TITLE : QUANTUM ALGORITHMS

" Solving mathematical problems with quantum systems "

Joonwoo Bae (QIT @ KAIST, EE, KAIST)

" What is quantum computation ? "

Lecture (the 8th School of Mesoscopic Physics)

- Basics of quantum information processing
- Computing with quantum systems
- Examples of quantum algorithms

$|0\rangle^{\otimes n}$

Quantum Computing

x_1 solution

x_2

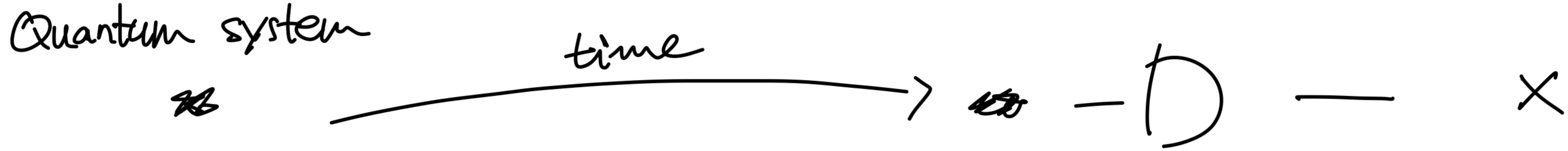
x_3

$\vdots$

x_n

I. Basics of Quantum Information Processing

Quantum theory is a mathematical model of the microscopic world.



	State	Dynamics	Measurement	Observable
Textbook.	$\psi(x,t)$	$i\partial_t\psi = H\psi$ $(\hbar=1)$	$\lvert\psi(x,t)\rvert^2 \sim p(x,t)$	$A = A^\dagger$
	Description of a quantum system	Eq. of motion for $\psi(x,t)$	Probabilistic nature of measurement outcomes	Characterization of the parameters that can be observed

	Quantum State	Dynamics	Measurement	Observable
Textbook.	$\psi(x,t)$	$i\,\partial_t \psi = H\psi$ $(\hbar = 1)$	$\lvert\psi(x,t)\rvert^2 \sim p(x,t)$	$A = A^\dagger$
	Description of a quantum system	Eq. of motion for $\psi(x,t)$	Probabilistic nature of measurement outcomes	Characterization of the parameters that can be observed

Recall.

$$\psi = \sum_n c_n \phi_n \rightsquigarrow \{\phi_n\} \text{ basis}$$

$$\psi \in \text{span}\{\phi_n\} = V \quad (\text{vector space})$$

inner product

$$\langle \psi, \varphi \rangle = \int d\mu(x)\, \psi^*(x)\, \varphi(x) \rightsquigarrow \lvert\psi\rvert^2$$

quantum measurement

Mathematical structure

- Quantum states introduce a vector space
- A quantum measurement introduces an inner product.

A vector space with an inner product ~ Hilbert space, $\mathcal{H}$

$\vec{x} \in \mathcal{H}$ element in $\mathcal{H}$

$(\vec{y})^\dagger = (\vec{y}^*)^T$ Hermitian conjugate

$\langle \vec{x} . \vec{y} \rangle = \vec{x}^\dagger . \vec{y}$ inner product

$\vec{y} = A\vec{x}$

$$A = \begin{bmatrix} \cdot & \cdot & \cdot & \cdot \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}$$

Matrix

Dirac notation

$|x\rangle \in \mathcal{H}$

$\langle y| = (|y\rangle)^\dagger$

$\langle x, y \rangle = \langle x|y\rangle$

$|y\rangle = A|x\rangle$

$$A = \sum_{ij} a_{ij} |i\rangle\langle j|$$

Reconstructing Quantum Theory

✓ State

$\psi(x,t)$

Description of a quantum system

✓ Dynamics

$i\partial_t\psi = H\psi$

$(\hbar = 1)$

Eq. of motion for $\psi(x,t)$

✓ Measurement

$|\psi(x,t)|^2 \sim p(x,t)$

Probabilistic nature of measurement outcomes

✓ Observable

$A = A^\dagger$

Characterization of the parameters that can be observed

$|\psi(x,t)\rangle \in \mathcal{H}$

$|\psi(t)\rangle = U(t)\,|\psi(t_0)\rangle$

U: unitary transformation

$UU^\dagger = U^\dagger U = I$

$|\langle\psi|i\rangle|^2$

(inner product)

Quantum measurement

a measurement in basis $\{|i\rangle\}_{i=1}^{n} = \{|1\rangle, |2\rangle, \cdots, |n\rangle\}$

$$p(i \mid \psi) = |\langle i|\psi\rangle|^2 = \langle i|\psi\rangle\langle i|\psi\rangle^*$$

$$= \langle\psi|i\rangle\langle i|\psi\rangle$$

$$1 = \sum_{i=1}^{n} p(i|\psi) = \langle\psi|\left(\sum_{i=1}^{n} |i\rangle\langle i|\right)|\psi\rangle = \langle\psi| I |\psi\rangle$$

note. trace

Def. $\operatorname{tr} A = \sum_i \langle i|A|i\rangle = \sum_i \lambda_i \quad , \quad \{\lambda_i\} = \operatorname{eig}(A)$

- $\operatorname{tr} AB = \operatorname{tr} BA \quad , \quad AB \neq BA$
- $\operatorname{tr} ABC = \operatorname{tr} CAB$

a measurement in a basis

$$p(i|\psi) = \langle\psi|i\rangle\langle i|\psi\rangle = \mathrm{tr}\left[\left(|\psi\rangle\langle\psi|\right)|i\rangle\langle i|\right]$$

a general description of a quantum measurement

$$\{M_i\}_{i=1}^{n} \quad \text{such that} \quad p(i|\psi) = \mathrm{tr}\left[|\psi\rangle\langle\psi|\, M_i\right]$$

i) $p(i|\psi) = \mathrm{tr}\left[|\psi\rangle\langle\psi|\, M_i\right] \geq 0 \iff M_i \geq 0$

note. $A \geq 0 \iff \forall |\psi\rangle,\ \mathrm{tr}\left[A\, |\psi\rangle\langle\psi|\right] \geq 0 \iff \mathrm{eig}\, A \geq 0$

ii) $1 = \sum_i p(i|\psi) = \mathrm{tr}[|\psi\rangle\langle\psi| \sum_i M_i] \iff \sum_i M_i = I$

A generalized measurement is described by positive-operator-valued-measure (POVM) elements $\{M_i\}$ satisfying $M_i \geq 0 \ \forall i$, $\sum_i M_i = I$.

Reconstructing Quantum Theory

State

$|\psi\rangle$

~ Physical interpretation ?

probabilities

$\mathrm{tr}[\,|\psi\rangle\langle\psi|\, M_i\,]$

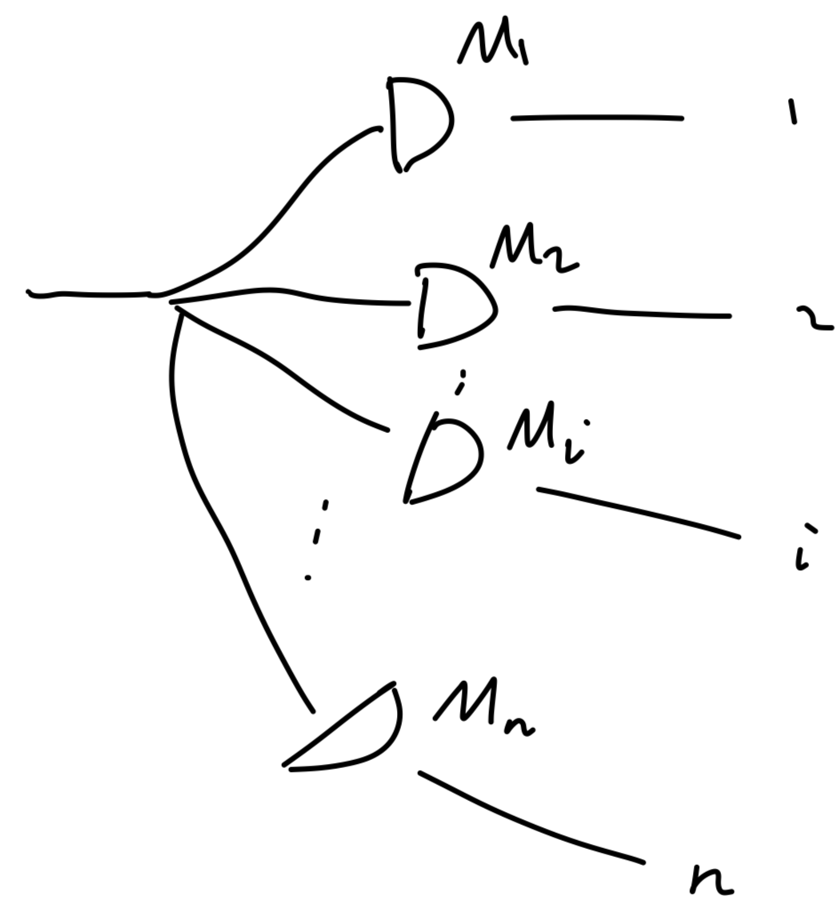
$|\psi\rangle \longrightarrow |\psi\rangle\langle\psi|$

Dynamics

Measurement

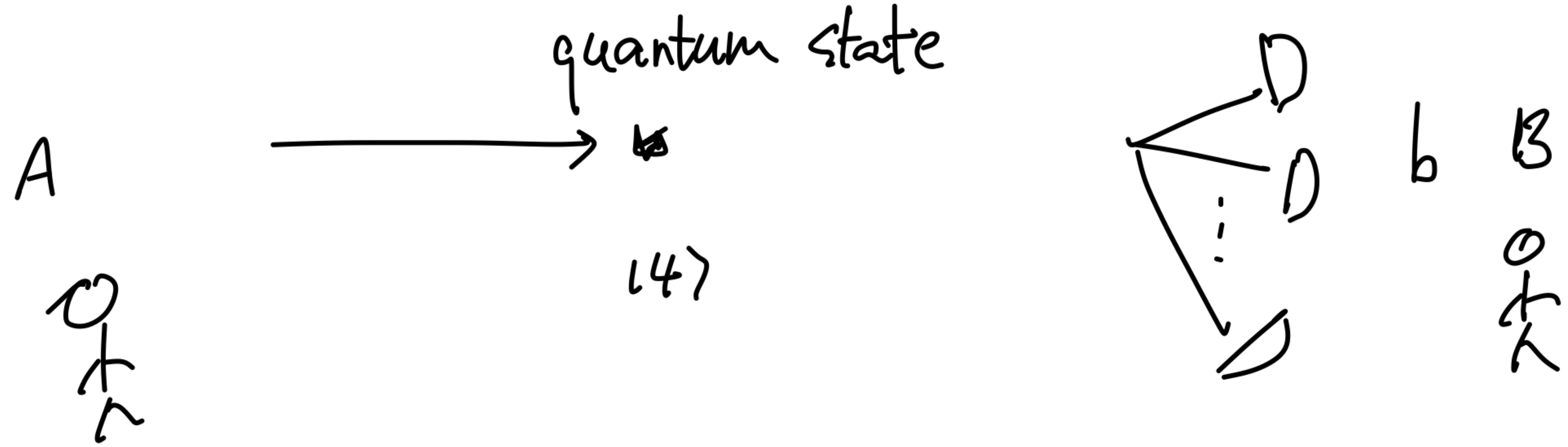
POVM $\{M_i\}$

$p(i|\psi) = \mathrm{tr}[\,|\psi\rangle\langle\psi|\, M_i\,]$



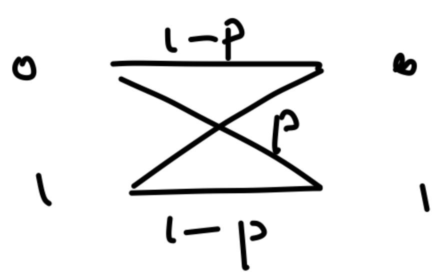
POVM

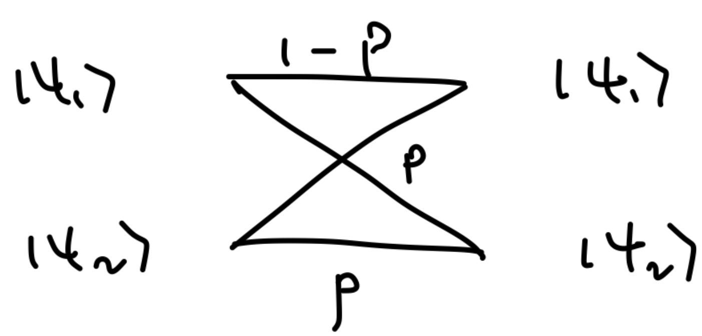
~ description of detectors in a quantum measurement a preparation game



$$\text{prob}(b|\psi) = \text{tr}[M_b |\psi\rangle\langle\psi|]$$

Binary Symmetric Channel

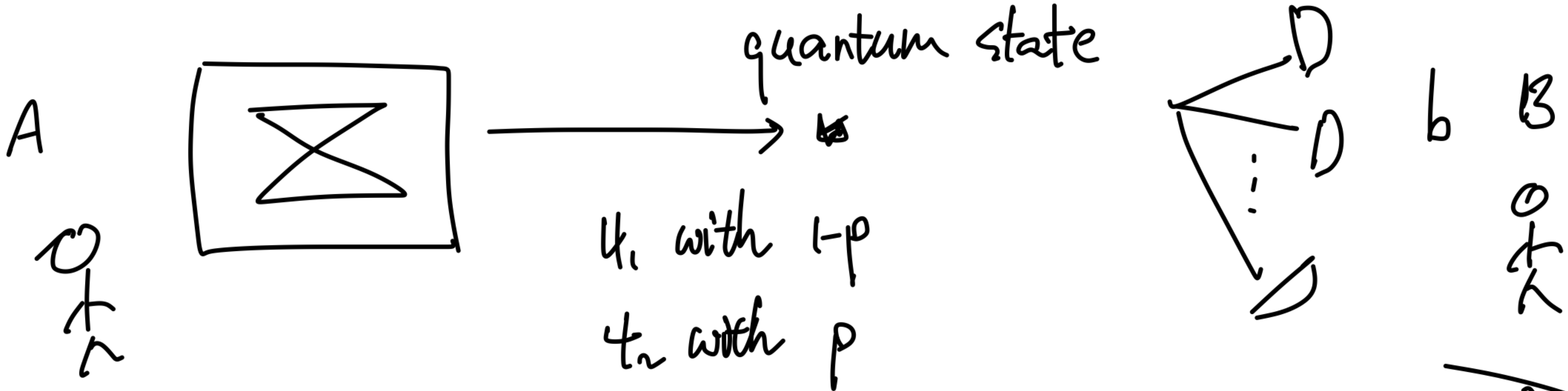




$|\psi_1\rangle$: $|\psi_1\rangle$ with prob $1-p$, $|\psi_2\rangle$ with prob p

$|\psi_2\rangle$: $|\psi_2\rangle$ with prob $1-p$, $|\psi_1\rangle$ with prob p

a preparation game



$\text{prob}(b|\psi) = \cancel{\mathrm{tr}[M_b |\psi\rangle\langle\psi|]}$

Note. $(1-p)|\psi_1\rangle\langle\psi_1| + p|\psi_2\rangle\langle\psi_2|$

state ψ_1 with prob $1-p$

ψ_2 with prob p $\Leftarrow$

$$\text{Prob}[b \mid \psi_1 \text{ with } 1-p,\ \psi_2 \text{ with } p]$$

$$= (1-p)\,\text{Prob}[b|\psi_1] + p\,\text{Prob}[b|\psi_2]$$

$$= (1-p)\,\mathrm{tr}[M_b |\psi_1\rangle\langle\psi_1|] + p\,\mathrm{tr}[M_b |\psi_2\rangle\langle\psi_2|]$$

$$= \mathrm{tr}[\underbrace{M_b}_{\text{POVM}} \underbrace{\left((1-p)|\psi_1\rangle\langle\psi_1| + p|\psi_2\rangle\langle\psi_2|\right)}_{\text{state}}]$$

A general description of a quantum state

$$\rho = p_1 |\psi_1\rangle\langle\psi_1| + p_2 |\psi_2\rangle\langle\psi_2| + \cdots = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

i) $\rho \geq 0$ ii) $\mathrm{tr}\,\rho = 1$

$\sum_i M_i = I.$ $\mathrm{tr}[\rho \sum_i M_i] = 1$ $\forall$ POVM

operational equivalence of quantum states

$$\rho = \sigma \quad \text{iff} \quad \forall M, \quad \mathrm{tr}[\rho M] = \mathrm{tr}[\sigma M]$$

$\Leftrightarrow$ ρ and σ cannot be distinguished, thus identical!

$$\rho \neq \sigma \iff \exists M \text{ such that } \mathrm{tr}[\rho M] \neq \mathrm{tr}[\sigma M]$$

Quantum Dynamics

$$\rho \longrightarrow U \rho U^{\dagger}, \quad U : \text{unitary transformation}$$

$$U U^{\dagger} = U^{\dagger} U = I$$

$|\psi\rangle$: $i \partial_t |\psi\rangle = H |\psi\rangle$

$$U = e^{-iHt} \quad H : \text{Hamiltonian}$$

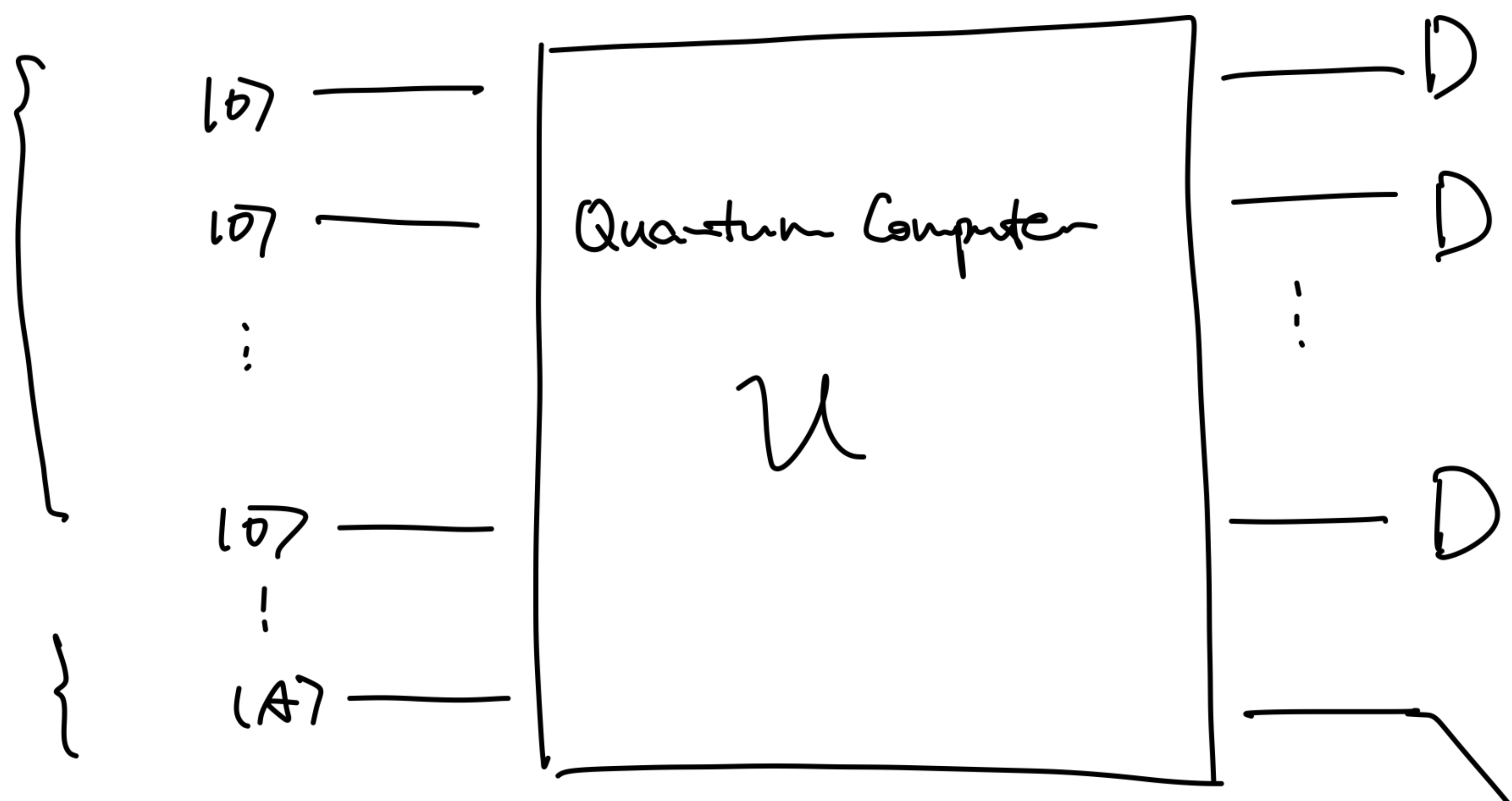
ρ : $\partial_t \rho(t) = -i [H(t), \rho(t)]$

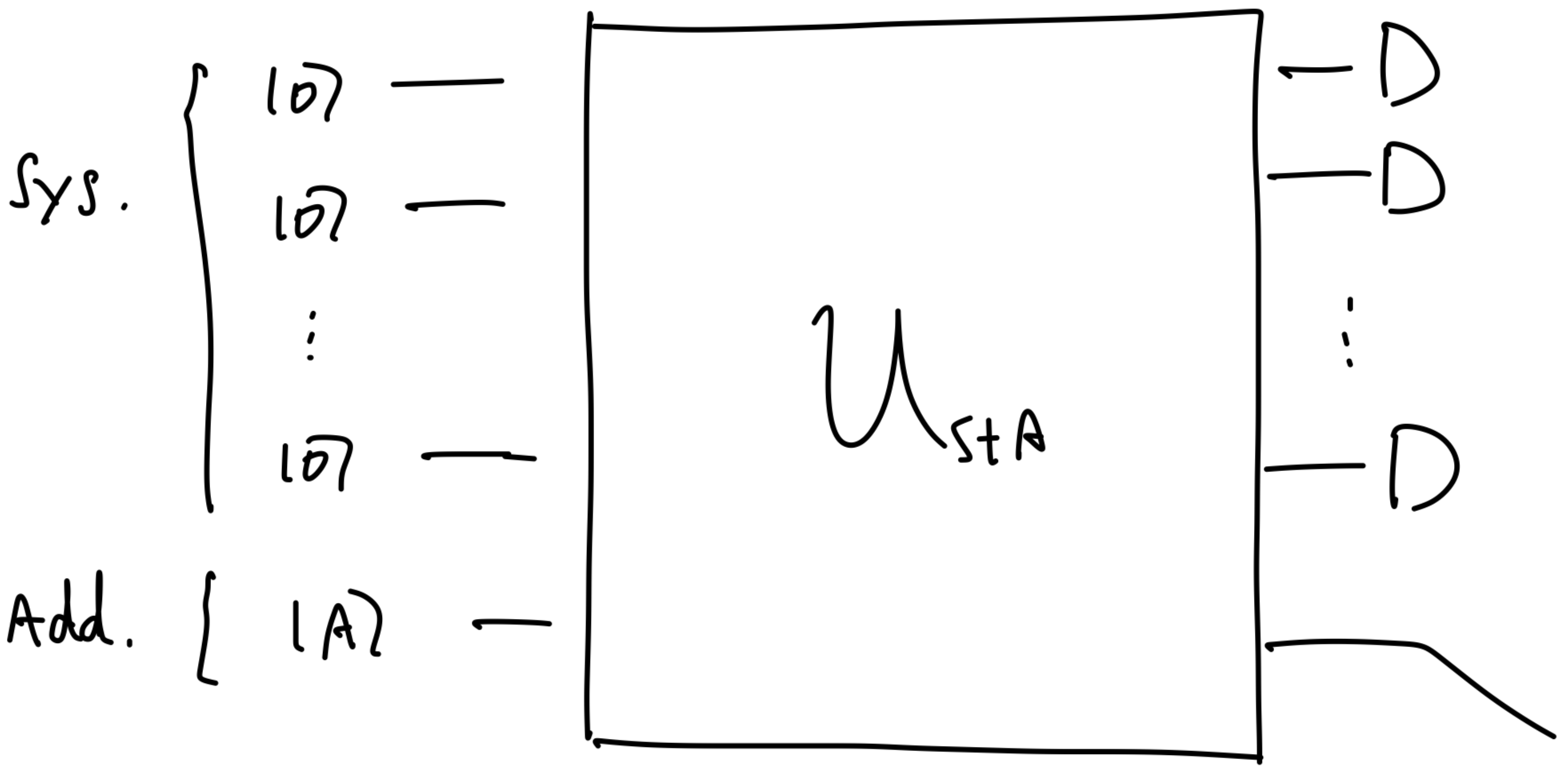
von Neumann eq.

Quantum Computation

system

Additional





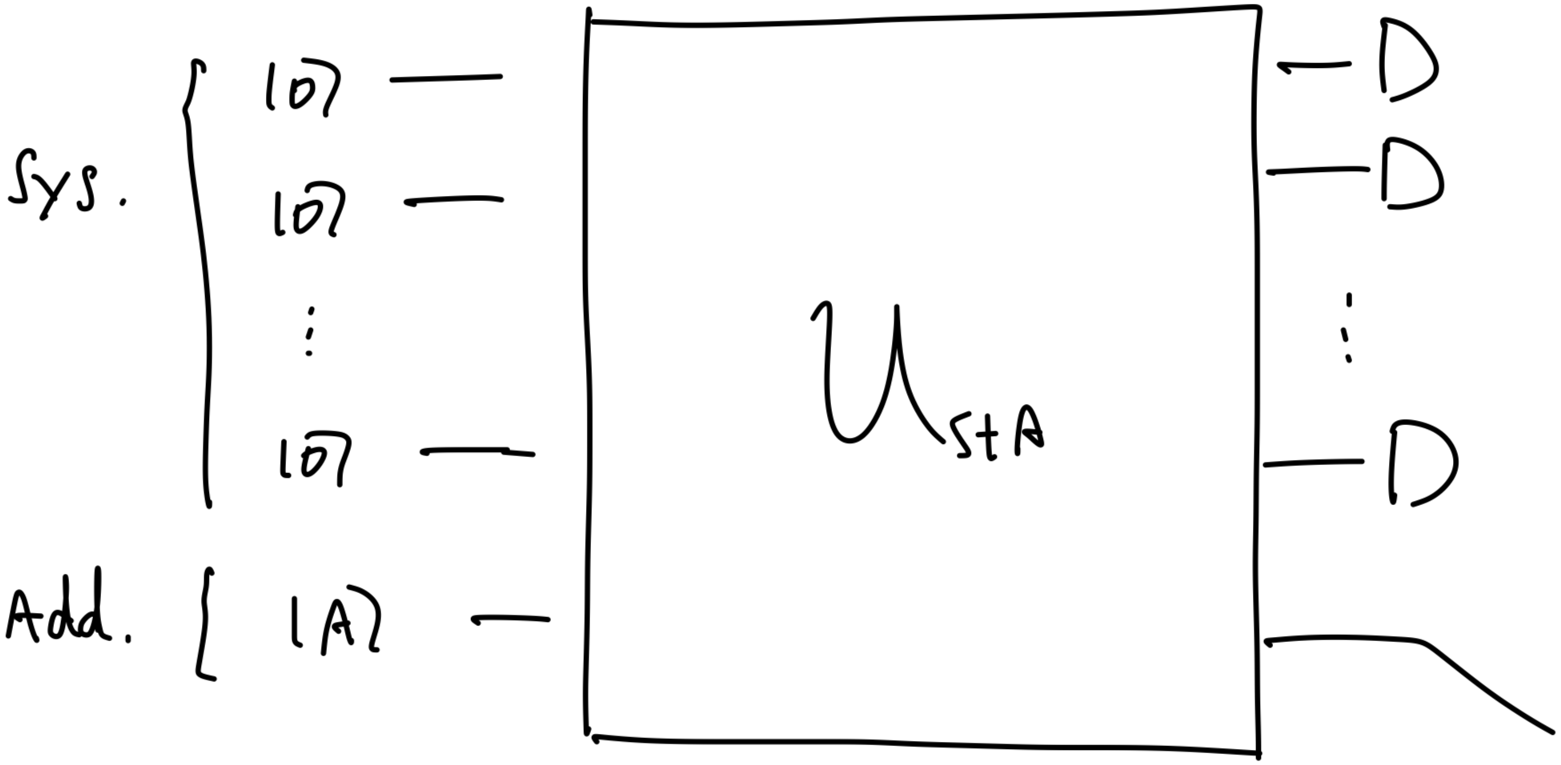
Dynamics of system qubits may not be unitary

$$U_{SA} \, \rho_S \otimes \rho_A \, U_{SA}^\dagger$$

discard A

tr : mathematical description of a measurement

$$\mathrm{tr}_A \, U_{SA} \, \rho_S \otimes \rho_A \, U_{SA}^\dagger$$



Dynamics of S : $\mathcal{E}(\rho_S) = \mathrm{tr}_A\, U_{SA}\, \rho_S \otimes |e\rangle\langle e|\, U_{SA}^\dagger$

$$= \sum_a {}_A\langle a|\, U_{SA}\, \rho_S \otimes |e\rangle\langle e|\, U_{SA}^\dagger\, |a\rangle$$

$$= \sum_a {}_A\langle a|\, U_{SA}\, |e\rangle\, \rho_S\, \langle e|\, U_{SA}^\dagger\, |a\rangle$$

$$\mathcal{E}(\rho_S) = \sum_a K_a\, \rho_S\, K_a^\dagger$$

$K_a = \langle a|\, U_{SA}\, |e\rangle$: Kraus operators

$$\sum_a K_a^\dagger K_a = \sum_a \langle e|\, U_{SA}^\dagger\, |a\rangle\langle a|\, U_{SA}\, |e\rangle = I_S$$

$$\mathcal{E}(\rho) = \sum_a K_a \rho K_a^\dagger$$: a quantum channel

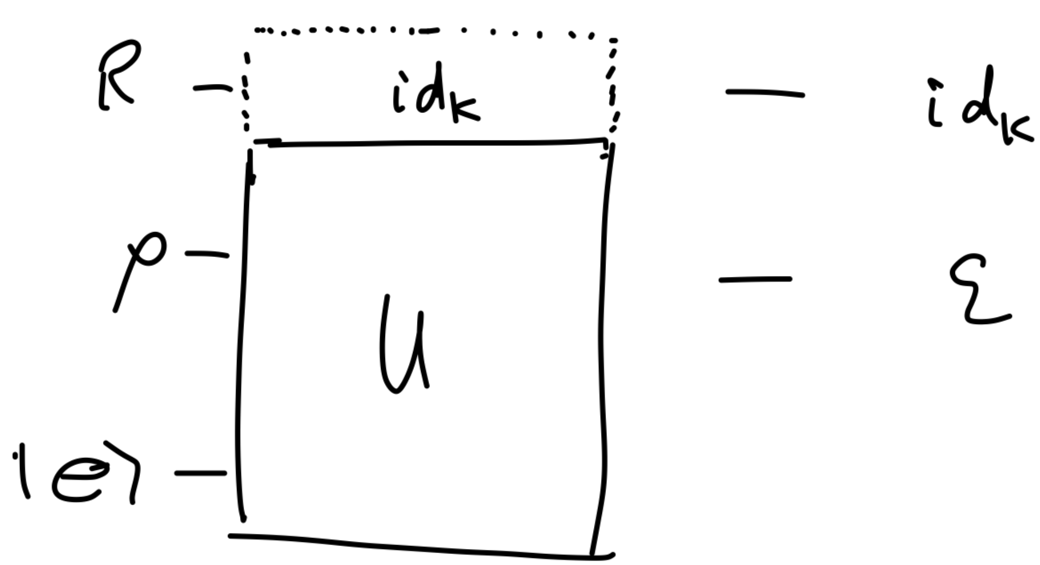
a dynamical map

a dynamical map $\rho(t+dt) = V(t)\,\rho(t)$, $V(t) = e^{\mathcal{L}t}$

$\mathcal{L}$: Lindblad generator   cf. $U = e^{-iHt}$

open problem : $\mathcal{E} \sim \mathcal{L}$?

$\mathcal{E} \geq 0$ if $\forall \rho \geq 0$, $\mathcal{E}(\rho) \geq 0$



$\mathcal{E} \geq 0$: $\mathcal{E}$ positive

$\forall K$, $id_K \otimes \mathcal{E} \geq 0$: $\mathcal{E}$ completely positive (CP)

A general description of a quantum dynamics

- Λ is a quantum channel.

  $\Lambda \geq 0$. $id \otimes \Lambda \geq 0$

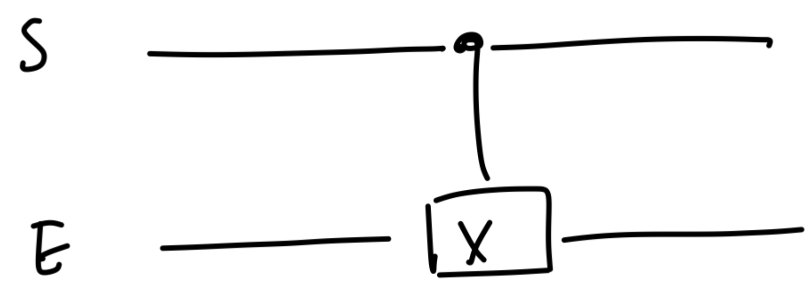
- $\Lambda \sim \{K_a\}$, $\Lambda(\rho) = \sum_a K_a \rho K_a^\dagger$

- $\Lambda(\rho) = tr_A\, U_{SA}\, \rho \otimes |e\rangle\langle e|\, U_{SA}^\dagger = V \rho V^\dagger$

  V : isometry

- a dynamical map, $\mathcal{L}$.

Example U_{CNOT}



$$|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle$$
$$|0\rangle|1\rangle \longrightarrow |0\rangle|1\rangle$$
$$|1\rangle|0\rangle \longrightarrow |1\rangle|1\rangle$$
$$|1\rangle|1\rangle \longrightarrow |1\rangle|0\rangle$$

$$U = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$\rho_s(t) = tr_E \, U_{CNOT} \; \rho \otimes |0\rangle\langle 0| \; U_{CNOT}^{\dagger}$$

$$= {}_E\langle 0| \, U_{CNOT} \; \rho \otimes |0\rangle\langle 0| \; U_{CNOT}^{\dagger} \, |0\rangle_E + {}_E\langle 1| \, U_{CNOT} \; \rho \otimes |0\rangle\langle 0| \; U_{CNOT}^{\dagger} \, |1\rangle_E$$

$$= {}_E\langle 0| U_{CNOT} |0\rangle_E \; \rho \; {}_E\langle 0| U_{CNOT}^{\dagger} |0\rangle_E + {}_E\langle 1| U_{CNOT} |0\rangle_E \; \rho \; \langle 0| U_{CNOT}^{\dagger} |1\rangle$$

$$\rho_s(t) = \mathrm{tr}_E\, U_{CNOT}\, \rho \otimes |0\rangle\langle 0|\, U_{CNOT}^\dagger$$

$$= {}_E\langle 0|\, U_{CNOT}\, \rho \otimes |0\rangle\langle 0|\, U_{CNOT}^\dagger\, |0\rangle_E + {}_E\langle 1|\, U_{CNOT}\, \rho \otimes |0\rangle\langle 0|\, U_{CNOT}^\dagger\, |1\rangle_E$$

$$= \underbrace{{}_E\langle 0|\, U_{CNOT}\, |0\rangle_E}_{K_0}\, \rho\, {}_E\langle 0|\, U_{CNOT}^\dagger\, |0\rangle_E + \underbrace{{}_E\langle 1|\, U_{CNOT}\, |0\rangle_E}_{K_1}\, \rho\, \langle 0|\, U_{CNOT}^\dagger\, |1\rangle$$

$$\rho_s(t) = K_0\, \rho\, K_0^\dagger + K_1\, \rho\, K_1^\dagger$$

$$K_0^\dagger K_0 + K_1^\dagger K_1 = {}_E\langle 0|\, U_{CNOT}^\dagger\, |0\rangle_E \langle 0|\, U_{CNOT}\, |0\rangle_E + {}_E\langle 0|\, U_{CNOT}^\dagger\, |1\rangle_E\langle 1|\, U_{CNOT}\, |0\rangle_E$$

$$= {}_E\langle 0|\, U_{CNOT}^\dagger\, \underbrace{\left(|0\rangle_E\langle 0| + |1\rangle_E\langle 1|\right)}_{I_E}\, U_{CNOT}\, |0\rangle_E$$

$$= {}_E\langle 0|\, \underbrace{U_{CNOT}^\dagger\, U_{CNOT}}_{I_{SE}}\, |0\rangle_E = I_S$$

A fundamental operational task : distinguishability

Problem statement

Suppose that ρ_1 is given with a priori prob $1/2$

ρ_2 is given with a priori prob $1/2$

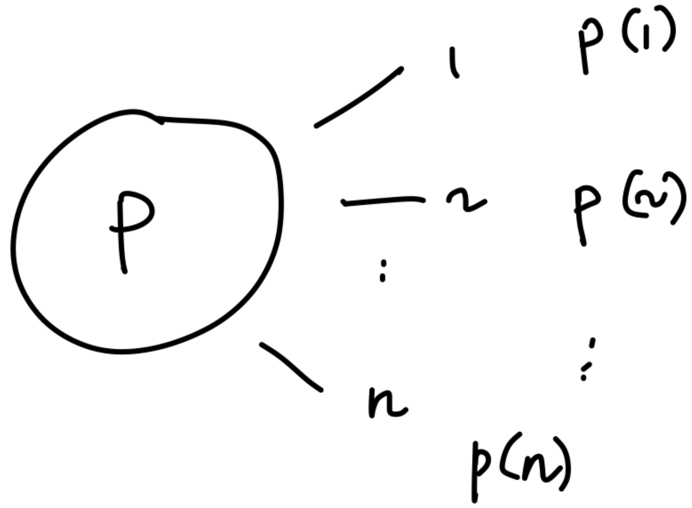
A measurement is given, you can optimize it.

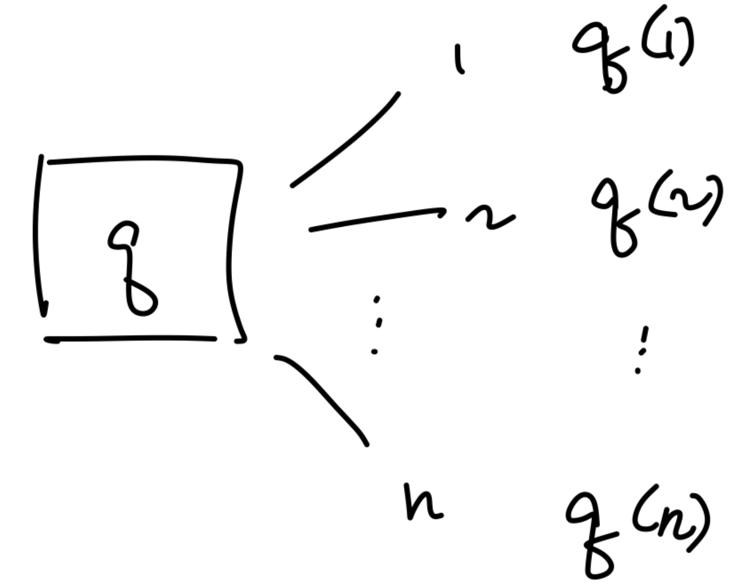
Find the highest probability you make a correct guess

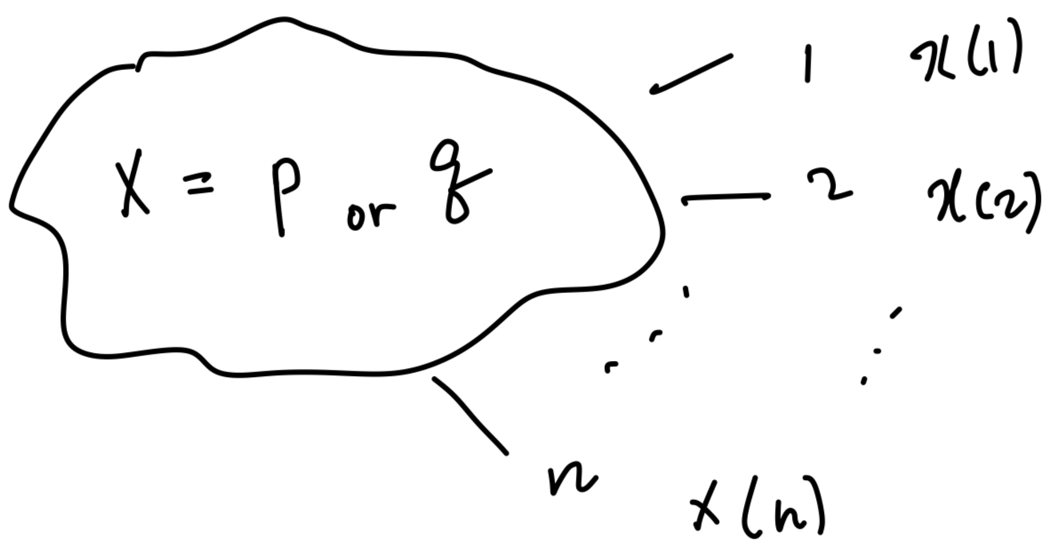
& an optimal measurement that achives the guessing probability.

In a classical scenario

two probabilistic systems

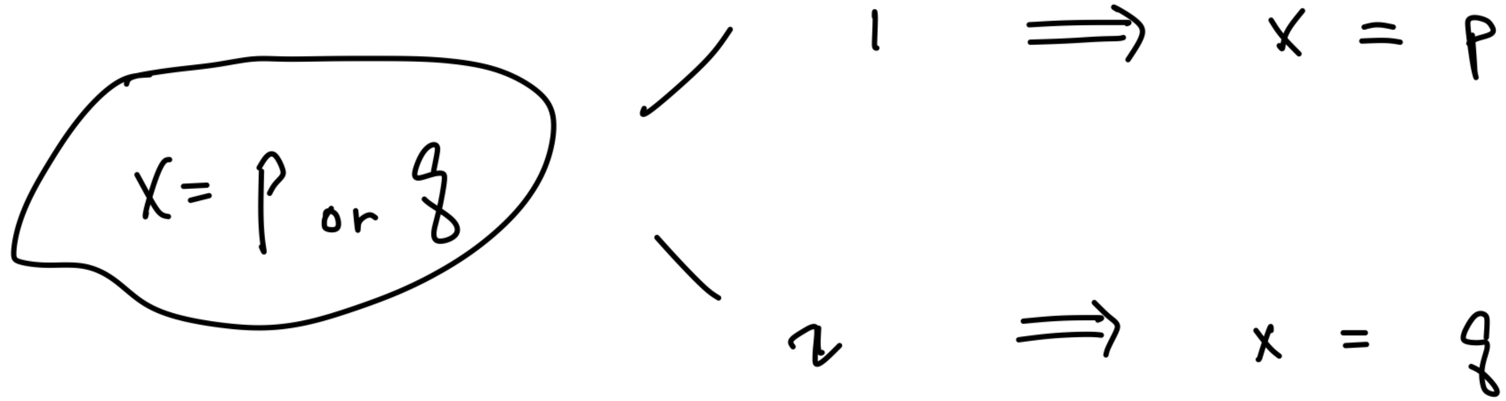




Given 

find $X=p$ or $X=q$?

e.g.



What is the optimal strategy to distinguish two probabilistic systems?

$$\delta(p, q) = \frac{1}{2} \sum_{x \in X} \left| p_x(x) - q_x(x) \right| \quad : \text{ variational distance}$$

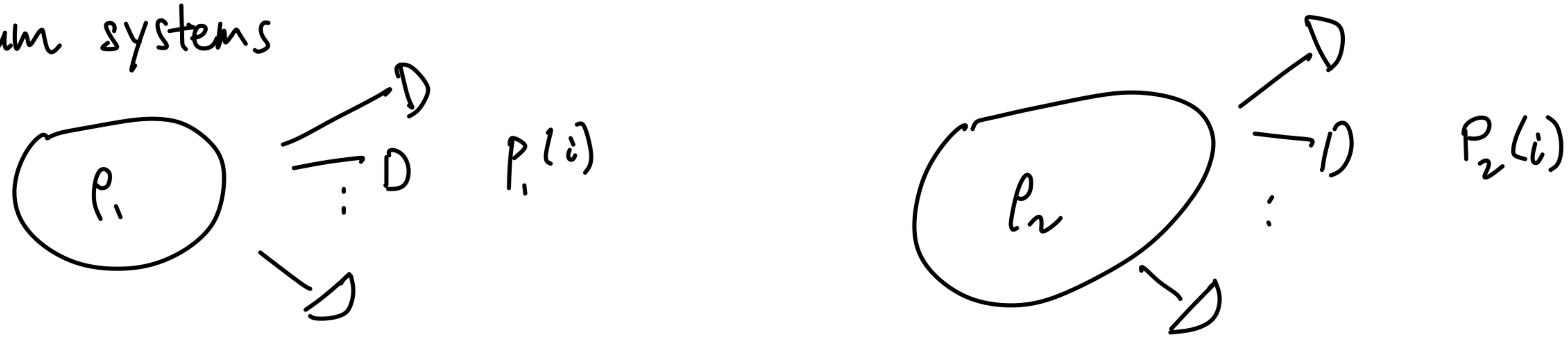
$$P_{guess} = \max_{S:\text{ strategy}} \frac{1}{2} \operatorname{Prob}[S = p \mid p] + \frac{1}{2} \operatorname{Prob}[S = q \mid q]$$

$$= \frac{1}{2} + \frac{1}{2} \delta(p, q) \quad : \text{ operational meaning of } \delta(p, q)$$

two probabilistic systems

$$P_{guess} = \frac{1}{2} + \frac{1}{2}\,\delta(p, q)$$

two quantum systems



$$P_{guess} = \max_{\substack{M:\ \mathrm{POVM} \\ S:\ \mathrm{Strategy}}} \frac{1}{2}\,\mathrm{Prob}_M[S = \rho_1 \mid \rho_1] + \frac{1}{2}\,\mathrm{Prob}_M[S = \rho_2 \mid \rho_2]$$

$$= \frac{1}{2} + \frac{1}{2}\,D(\rho_1, \rho_2)$$

$$D(\rho_1, \rho_2) = \frac{1}{2}\|\rho_1 - \rho_2\|_1 , \qquad \|A\|_1 = \mathrm{tr}\sqrt{A^\dagger A} = \sum_i |\mathrm{eig}(A)|$$

Problem statement

Suppose that ρ_1 is given with a priori prob $1/2$

ρ_2 is given with a priori prob $1/2$

A measurement is given, you can optimize it.

Find the highest probability you make a correct guess

& an optimal measurement that achives the guessing probability.

$$P_{guess} = \frac{1}{2} + \frac{1}{2} D(\rho_1, \rho_2), \quad D(\rho_1, \rho_2) = \frac{1}{2} \| \rho_1 - \rho_2 \|$$

opt $M \sim (\rho_1 - \rho_2)_\pm$, positive & negative projections

II. Quantum Computation

Quantum computation contains i) preparation ii) dynamics iii) measurements of quantum states

- Preparation of quantum states

$$|0\rangle^{\otimes n} \quad \text{or} \quad |\psi\rangle = \left[\bigotimes_{i=1}^{n} U_i\right]|0\rangle^{\otimes n} = U_1|0\rangle \otimes \cdots \otimes U_n|0\rangle$$

$|0\rangle^{\otimes n}$ and $|\psi\rangle$ are equivalent up to local unitary transformations

- Measurement

$$M = \{|0\rangle, |1\rangle\}_1 \otimes \{|0\rangle, |1\rangle\}_2 \otimes \cdots \otimes \{|0\rangle, |1\rangle\}_n$$

$\{|0\rangle, |1\rangle\}_i$ — $x_1 = 0, 1$ all in the computational basis

— $x_2 = 0, 1$

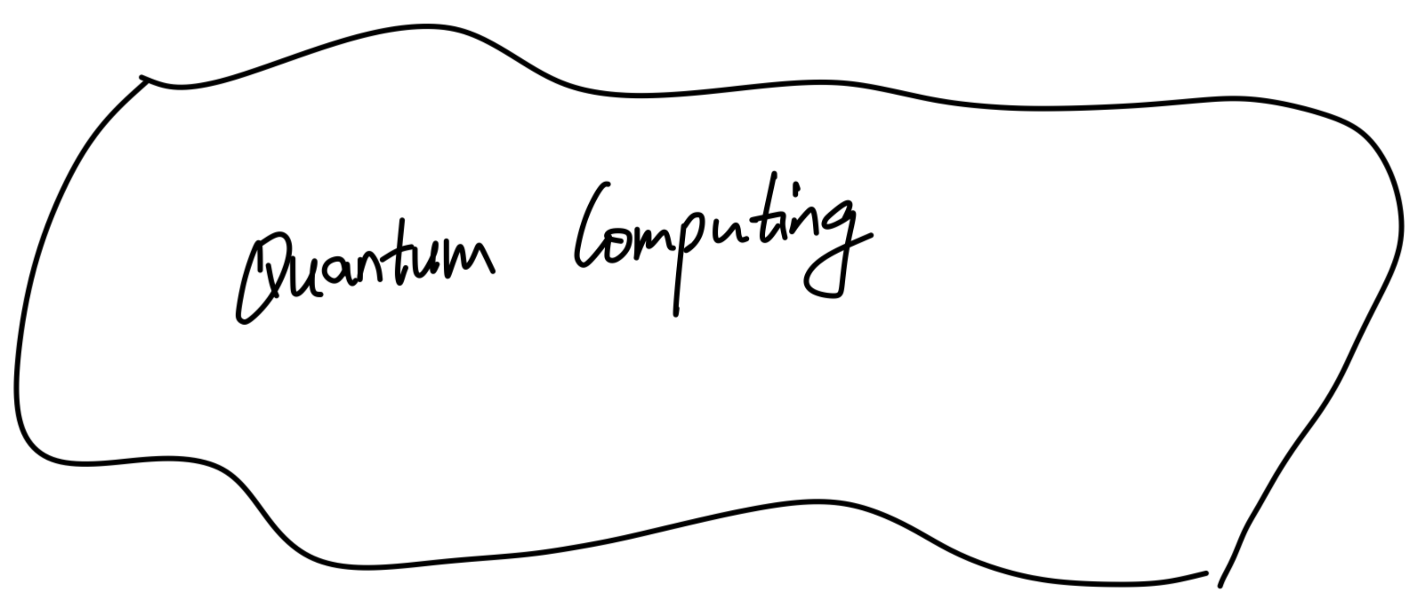
$\vdots$

— $x_n = 0, 1$

- dynamics ~ hybrid quantum and classical operations

~ manipulation of quantum states

$|0\rangle^{\otimes n}$



x_1 solution

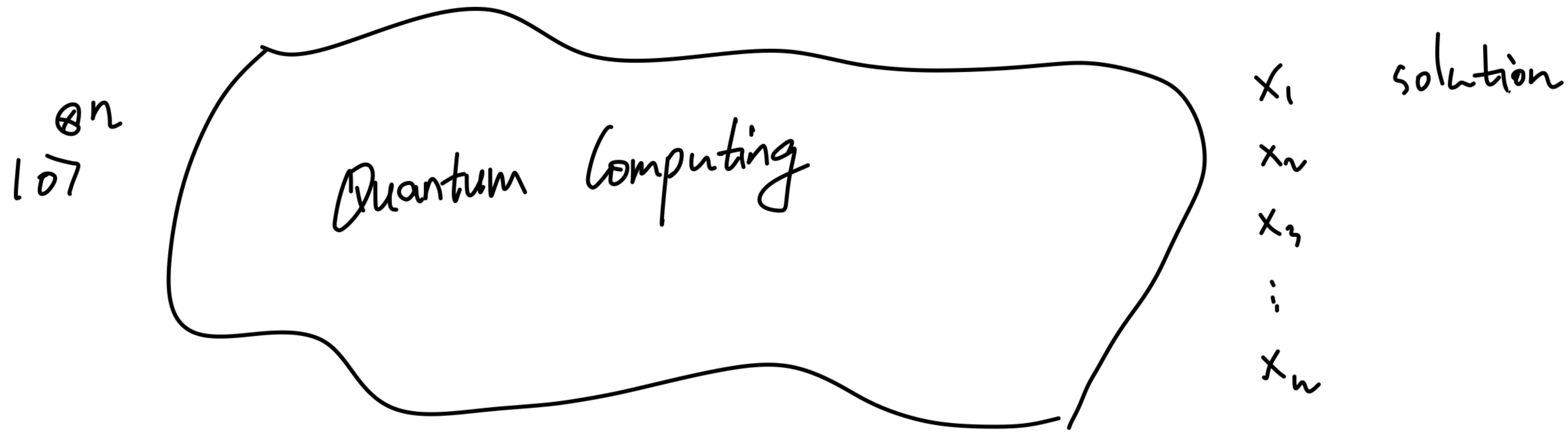
x_2

x_3

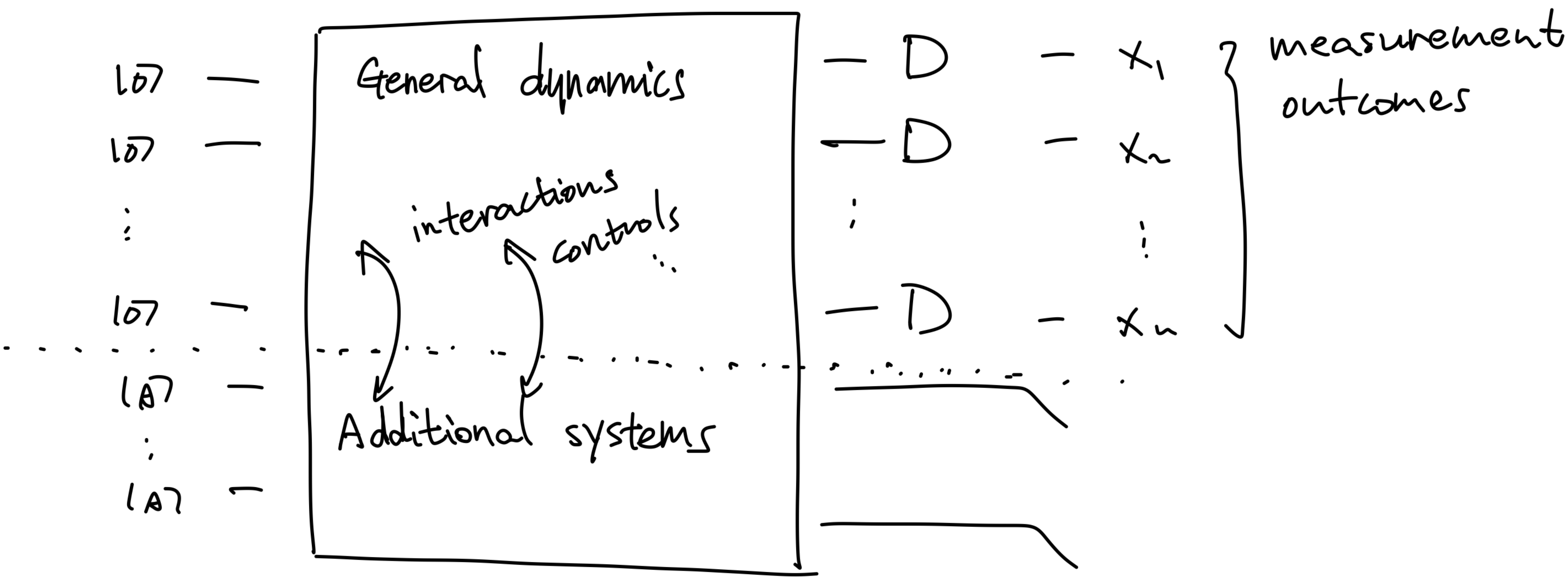
$\vdots$

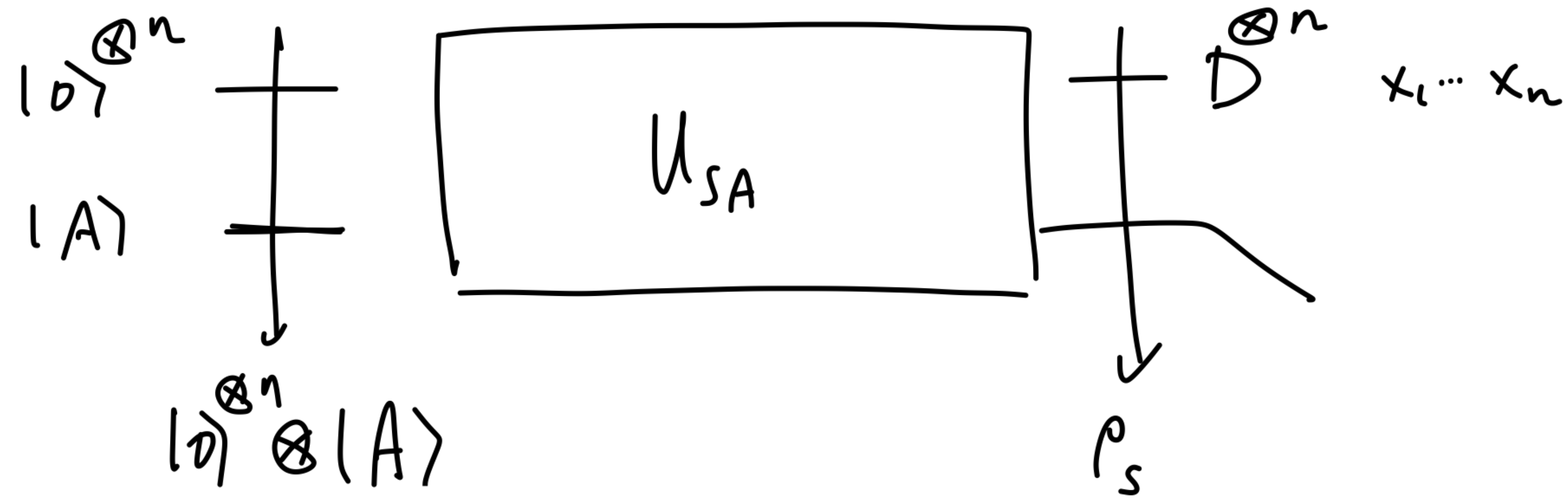
x_n

Dynamics in a quantum computer



Implementation





dynamics : $\mathrm{tr}_A\, U_{SA}\, |0\rangle\langle 0|^{\otimes n} \otimes |A\rangle\langle A|\, U_{SA}^{\dagger} = \rho_s$

measurement : $\mathrm{tr}[\, M_{x_1} \otimes M_{x_2} \otimes \cdots \otimes M_{x_n}\, \rho_s \,] = p(x_1 \cdots x_n \mid \rho_s)$

$x^n = x_1 x_2 \cdots x_n$ is obtained with probability

$$\mathrm{tr}[\, M_{x_1} \otimes M_{x_2} \otimes \cdots \otimes M_{x_n} \otimes I_A\, U_{SA}\, |0\rangle\langle 0|^{\otimes n} \otimes |A\rangle\langle A|\, U_{SA}^{\dagger} \,]$$

solutions of a mathematical problem

resources for computation

$|0\rangle^{\otimes n}$

Quantum Computing

x_1 solution

x_2

x_3

$\vdots$

x_n

$\underline{x^n = x_1 x_2 \cdots x_n}$ is obtained with probability

$$\mathrm{tr}\left[M_{x_1} \otimes M_{x_2} \otimes \cdots \otimes M_{x_n} \otimes I_A \, \underline{U_{SA}} \, |0\rangle\langle 0|^{\otimes n} \otimes \underline{|A\rangle\langle A|} \, \underline{U_{SA}^{\dagger}} \right]$$

solutions of a mathematical problem

resources for computation

U_{SA} and $|A\rangle$ are designed
such that the solution of a mathematical problem is provided by x^n
with finite resources (time, space, ⋯)

The main question to apply quantum theory to a computational task

X : a mathematical problem to solve

$x^n = x_1 x_2 \cdots x_n$ is a solution

F denotes a set of steps to find x^n, an algorithm

$$\underbrace{i^n = i_1 \cdots i_n}_{\text{trivial input}} \xrightarrow{\quad F \quad} \underbrace{F[x] \in \{0,1\}^n}_{\text{meaningful output}}$$

circuits, logic gates

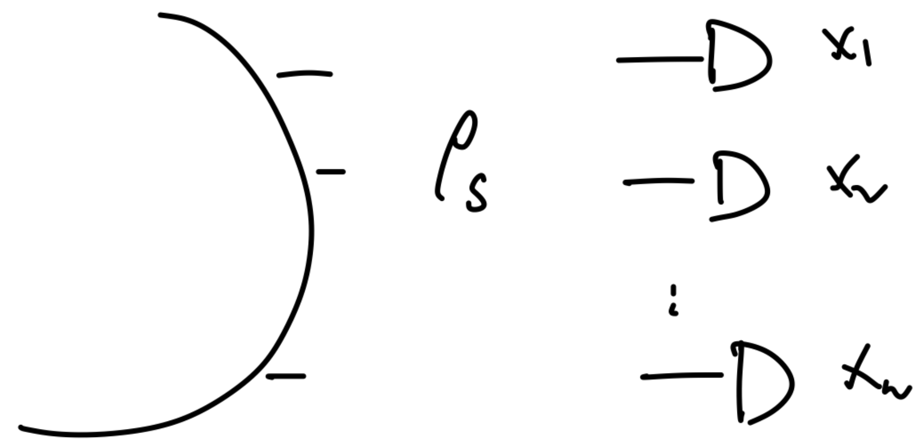
Algorithms, ...

$$\underline{\delta(F[x], x^n) < \epsilon \quad \forall \epsilon > 0}$$

$\iff$ F solves the problem

Design quantum steps to solve a mathematical problem

$$F_Q \sim \operatorname{tr}\left[M_{x_1} \otimes \cdots \otimes M_{x_n} \otimes I_A \; U_{SA} \, |0\rangle\langle 0|^{\otimes n} \otimes |A\rangle\langle A| \, U_{SA}^{\dagger} \right]$$



ρ_S such that

$$D\left[|x^n\rangle\langle x^n| , \; \operatorname{tr}_A U_{SA} \, |0\rangle\langle 0|^{\otimes n} \otimes |A\rangle\langle A| \, U_{SA}^{\dagger} \right] < \varepsilon$$

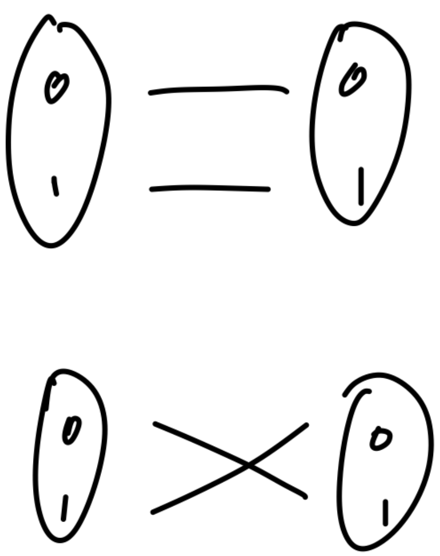
$$|0\rangle^{\otimes n} \xrightarrow{\text{quantum dynamics}} |x^n\rangle$$

$\sim$ state transformation

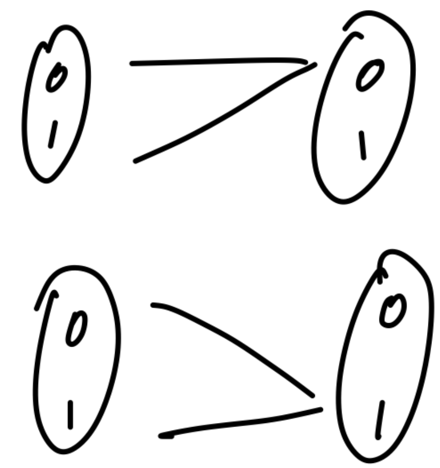
state manipulation

The Deutsch Problem

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



1-1 function
(balanced function)



constant function

Problem : Given a function $f : \{0,1\} \to \{0,1$
determine if f is constant or balanced.

classical solution : call $f(x)$ twice

quantum solution : call $f(x)$ once ✓

Problem : Given a function $f : \{0,1\} \to \{0,1\}$

determine if f is constant or balanced.

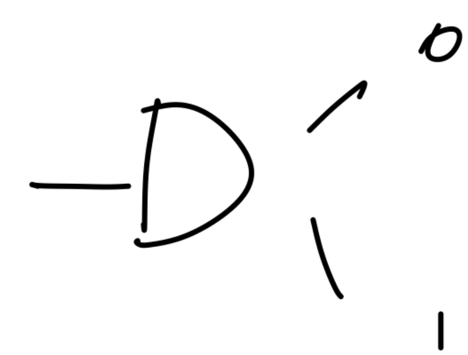
$$\iff \text{Find } f(0) + f(1) = \begin{cases} 0 & \text{iff } f \text{ is constant} \\ 1 & \text{iff } f \text{ is balanced} \end{cases}$$

Classical

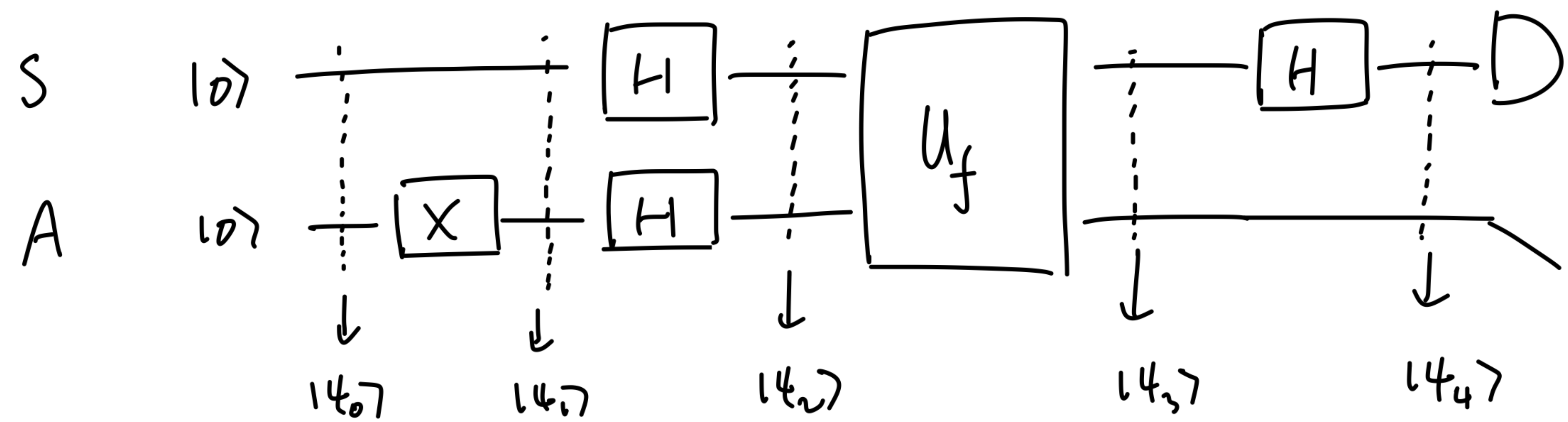
$$a \xrightarrow{F\,[\text{Deutsch}]} f(0) + f(1)$$: single bit

Quantum

$$|0\rangle \xrightarrow{F_Q\,[\text{Deutsch}]} |f(0)+f(1)\rangle$$



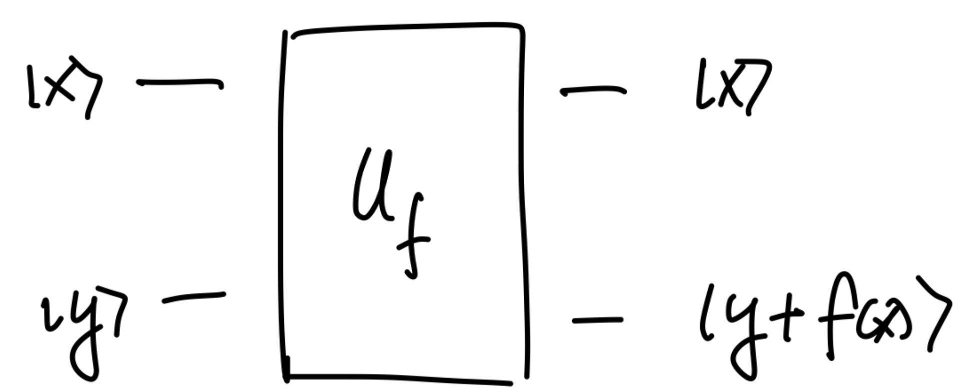
The Deutsch Algorithm



note. $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ $\quad$ $H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle)$ $\quad$ Hadamard gate

$H|1\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle)$

$$U_f |x\rangle|y\rangle = |x\rangle|y + f(x)\rangle$$

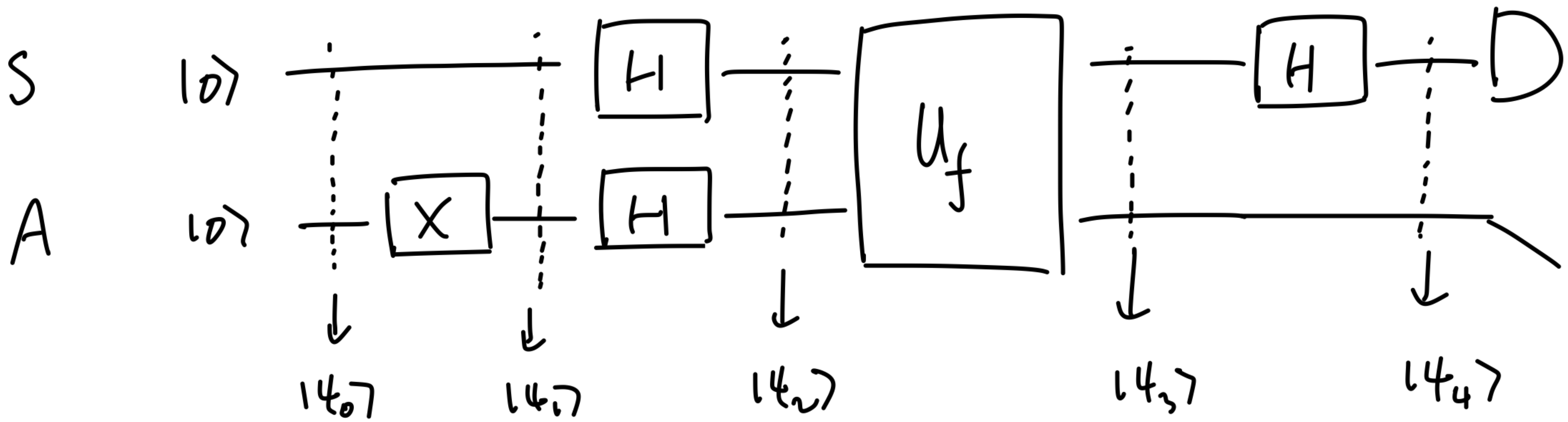


note. U_f is unitary

proof. (exercise)

$$U_f = \sum_{x,y} |x\rangle\langle x| \otimes |y+f(x)\rangle\langle y|$$

The Deutsch Algorithm



$$|\psi_0\rangle = |0\rangle_S |0\rangle_A$$

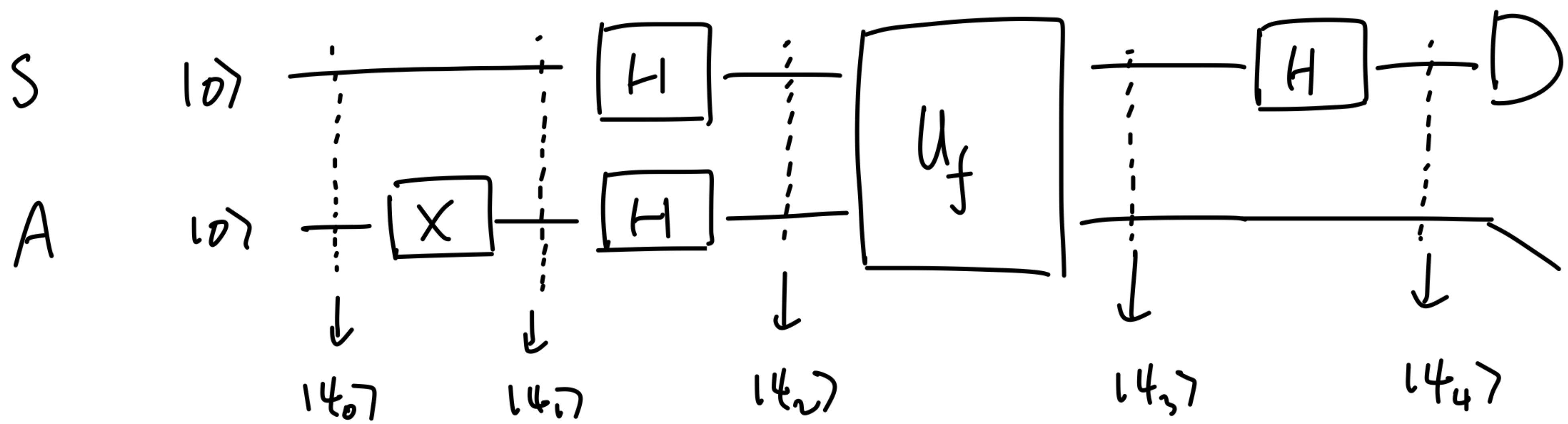
$$|\psi_1\rangle = |0\rangle|1\rangle \qquad |\psi_2\rangle = |+\rangle|-\rangle = \frac{1}{\sqrt{2}}|0\rangle|-\rangle + \frac{1}{\sqrt{2}}|1\rangle|-\rangle$$

note.
$$U_f|x\rangle|-\rangle = U_f\left(|x\rangle\frac{1}{\sqrt{2}}|0\rangle - |x\rangle\frac{1}{\sqrt{2}}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}}|x\rangle|f(x)\rangle - \frac{1}{\sqrt{2}}|x\rangle|1 \oplus f(x)\rangle$$

$$= \begin{cases} |x\rangle|-\rangle & \text{if } f(x)=0 \\ (-1)|x\rangle|-\rangle & \text{if } f(x)=1 \end{cases} = (-1)^{f(x)}|x\rangle|-\rangle$$

The Deutsch Algorithm



$$|\psi_0\rangle = |0\rangle_S |0\rangle_A$$

$$|\psi_1\rangle = |0\rangle|1\rangle$$

$$|\psi_2\rangle = |+\rangle|-\rangle = \frac{1}{\sqrt{2}}|0\rangle|-\rangle + \frac{1}{\sqrt{2}}|1\rangle|-\rangle$$

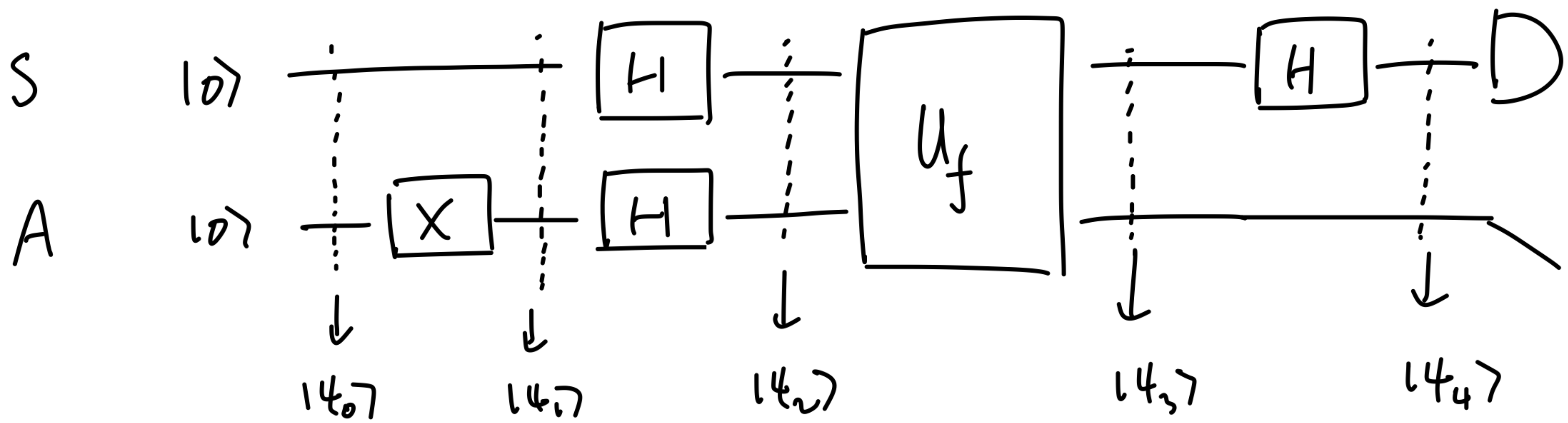
note. $U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$

$$|\psi_3\rangle = U_f|\psi_2\rangle = U_f|+\rangle|-\rangle = U_f\left(\frac{1}{\sqrt{2}}|0\rangle|-\rangle + \frac{1}{\sqrt{2}}|1\rangle|-\rangle\right)$$

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

$$= \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)|-\rangle$$

The Deutsch Algorithm



$$|\psi_0\rangle = |0\rangle_S |0\rangle_A$$

$$|\psi_1\rangle = |0\rangle|1\rangle$$

$$|\psi_2\rangle = |+\rangle|-\rangle = \frac{1}{\sqrt{2}}|0\rangle|-\rangle + \frac{1}{\sqrt{2}}|1\rangle|-\rangle$$

$$|\psi_3\rangle = \left(\frac{1}{\sqrt{2}}(-1)^{f(0)}|0\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|1\rangle\right)|-\rangle$$

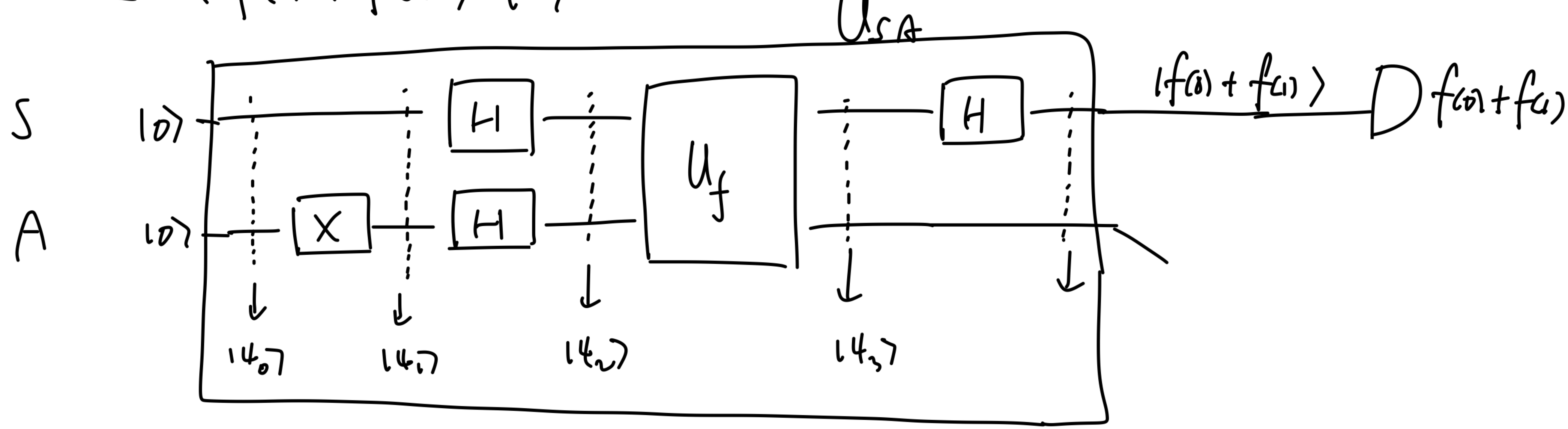
$$|\psi_4\rangle = \left(\frac{1}{\sqrt{2}}(-1)^{f(0)}|+\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|-\rangle\right)|-\rangle$$

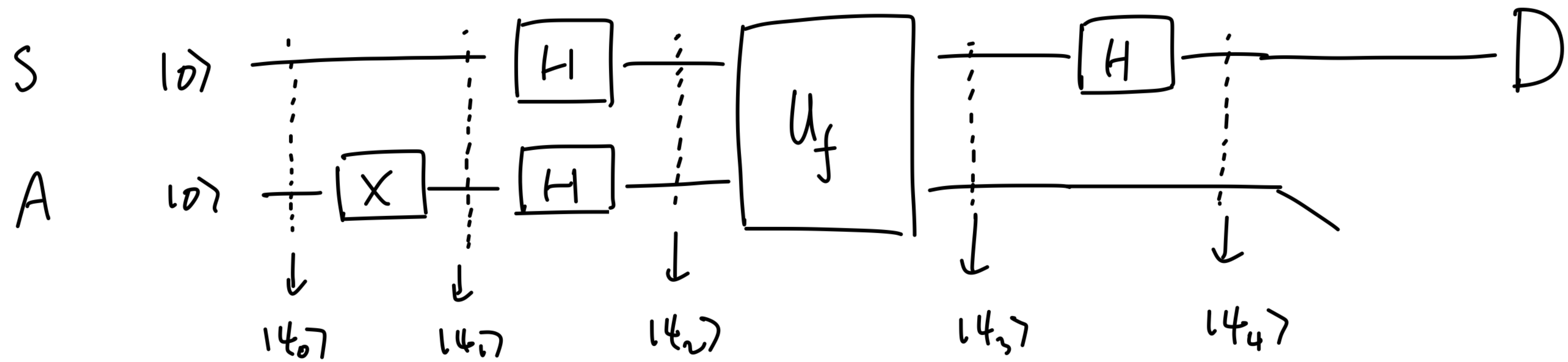
$$|\psi_4\rangle = \left(\frac{1}{\sqrt{2}}(-1)^{f(0)}|+\rangle + \frac{1}{\sqrt{2}}(-1)^{f(1)}|-\rangle\right)|-\rangle$$

$$= \left[\frac{1}{2}\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \frac{1}{2}\left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right]|-\rangle$$

$$= \begin{cases} |0\rangle & \text{if } f(0) = f(1) \iff f(0) + f(1) = 0 \\ |1\rangle & \text{if } f(0) \neq f(1) \iff f(0) + f(1) = 1 \end{cases} \quad |-\rangle$$

$$= |f(0) + f(1)\rangle\,|-\rangle$$





$$U_{SA} = (H \otimes I) U_f (H \otimes H)(I \otimes X)$$

$$\mathrm{tr}_A\, U_{SA} |0\rangle\langle 0| \otimes |0\rangle\langle 0| U_{SA}^\dagger = |f(0)+f(1)\rangle\langle f(0)+f(1)|$$

$$D\left[\, |f(0)+f(1)\rangle,\ \mathrm{tr}_A\, U_{SA} |0\rangle\langle 0| \otimes |0\rangle\langle 0| U_{SA}^\dagger \,\right] = 0$$

U_f is applied once !

Quantum Computing

Construct U_{SA} such that

$$\delta\left(x^n,\ \underline{\mathrm{tr}\, M_{x_1} \otimes M_{x_2} \otimes \cdots \otimes M_{x_n}} \otimes I_A\, U_{SA}\, |0\rangle\langle 0|^{\otimes n} \otimes |A\rangle\langle A|\, U_{SA}^{\dagger} \right) < \varepsilon$$

$f(0)+f(1)$

measurement in a computational basis

$$U_{SA} = (H \otimes I)\, U_f\, (H \otimes H)(1 \otimes X)$$

$$|0\rangle^{\otimes n} \xrightarrow[\underline{U},\ A,\ M]{} |\text{solution}\rangle$$

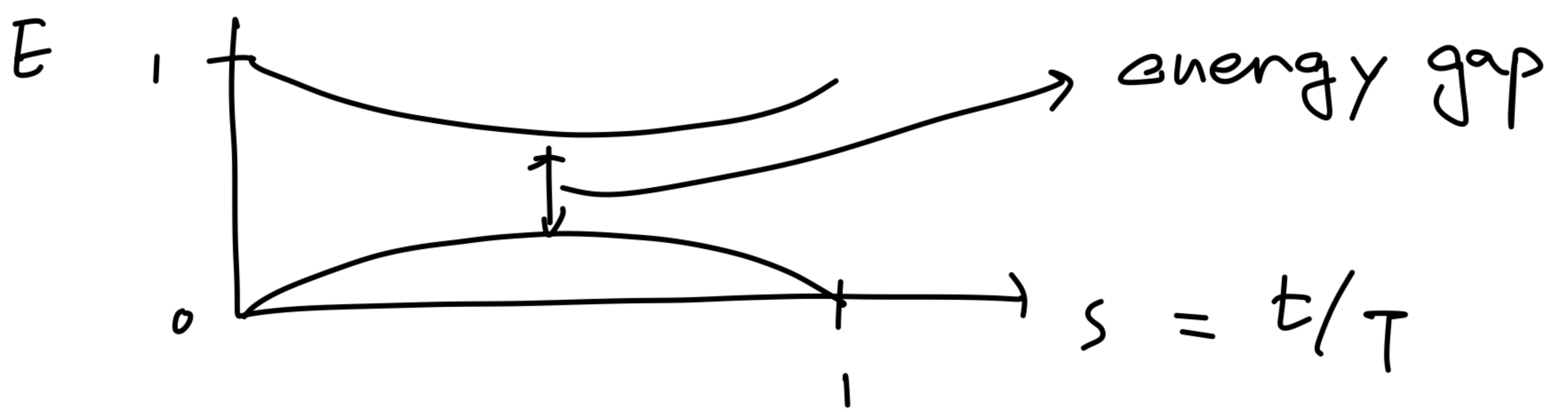
morale : universal transformation

- CNOT + all single-qubit operations are universal.
- CNOT + H. T = ($\pi/8$ gate) = $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

$$H(s) = (1-s) H_0 + s H_1 \qquad s = s(t)$$

$$H_0 = I - |\psi_0\rangle\langle\psi_0| \quad : \quad \text{ground state} \quad H_0|\psi_0\rangle = 0 \cdot |\psi_0\rangle$$

$$H_1 = I - |\psi_1\rangle\langle\psi_1| \quad : \quad \text{ground state} \quad H_1|\psi_1\rangle = 0 \cdot |\psi_1\rangle$$



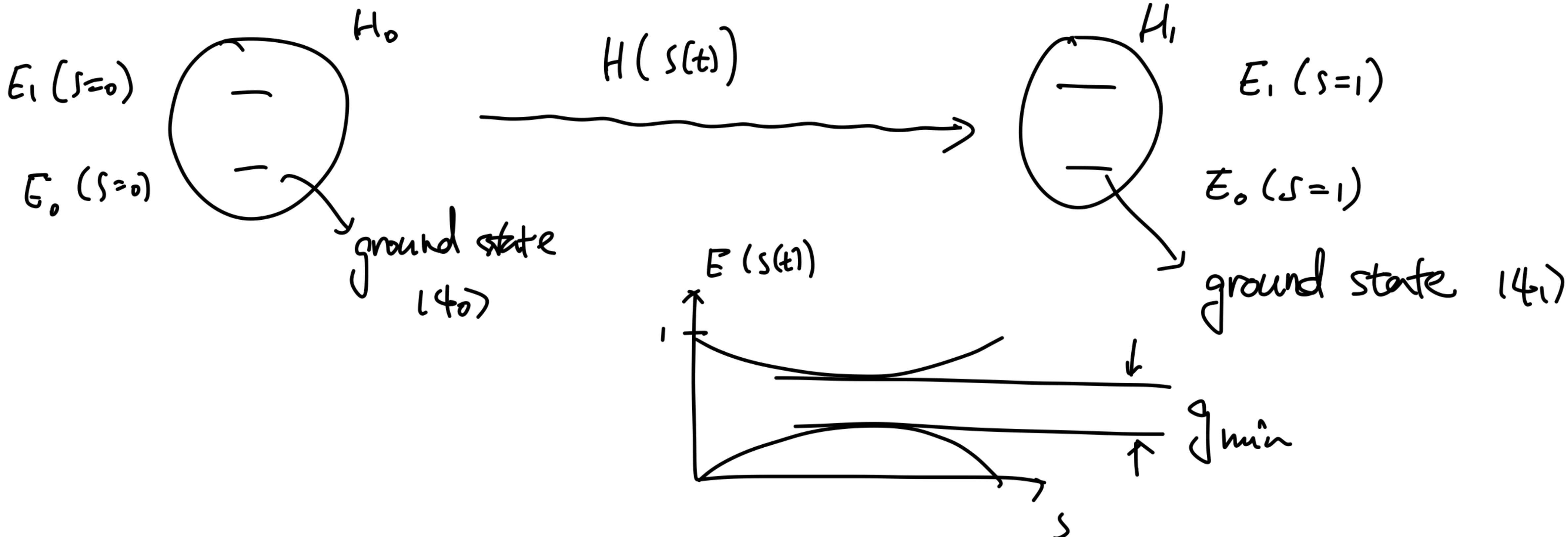
$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$$

f is constant $\Leftrightarrow$ $\alpha = 1$, $\beta = 0$

$$\alpha = \frac{1}{2}\left| (-1)^{f(0)} + (-1)^{f(1)} \right|$$

f is balanced $\Leftrightarrow$ $\alpha = 0$, $\beta = 1$

$$\beta = \frac{1}{2}\left| (-1)^{f(0)} - (-1)^{f(1)} \right|$$



Adiabatic theorem

$$g_{min} = \min_{0 \le s \le 1} \left(E_1(s) - E_0(s) \right)$$

provided that $\frac{1}{g_{min}^2} \left| \langle \frac{dH}{dt} \rangle \right| \le \varepsilon$, $\langle \frac{dH}{dt} \rangle = \langle E_1(s) | \frac{dH}{dt} | E_0(s) \rangle$

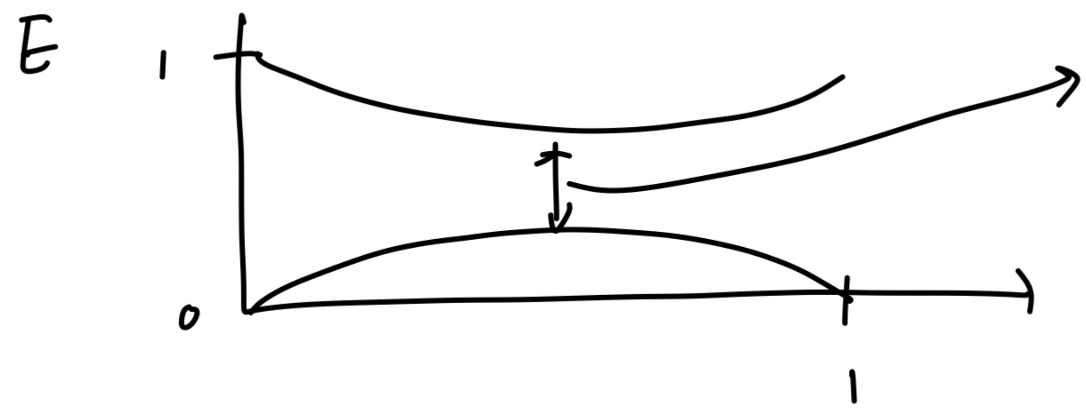
then $|\psi_0\rangle \longrightarrow |\psi_1\rangle$ with probability $(1-\varepsilon^2)^2$

"Adiabatic evolution"

$$H(s) = (1-s)H_0 + sH_1 \qquad s = s(t)$$

$$H_0 = I - |\psi_0\rangle\langle\psi_0| \quad : \text{ ground state} \quad H_0|\psi_0\rangle = 0\cdot|\psi_0\rangle$$

$$H_1 = I - |\psi_1\rangle\langle\psi_1| \quad : \text{ ground state} \quad H_1|\psi_1\rangle = 0\cdot|\psi_1\rangle$$



energy gap

$$s = t/T$$

$\boxed{\begin{array}{l} \text{Adiabatic theorem} \\ T \geq \dfrac{1}{\varepsilon} \\ |\psi_0\rangle \longrightarrow |\psi_1\rangle \text{ with prob. } (1-\varepsilon^2)^2 \end{array}}$

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$$

f is constant $\Leftrightarrow$ $\alpha = 1$, $\beta = 0$

f is balanced $\Leftrightarrow$ $\alpha = 0$, $\beta = 1$

$$\left(\begin{array}{l} \alpha = \dfrac{1}{2}\left|(-1)^{f(0)} + (-1)^{f(1)}\right| \\[2ex] \beta = \dfrac{1}{2}\left|(-1)^{f(0)} - (-1)^{f(1)}\right| \end{array}\right.$$

The Deutsch-Jozsa Problem

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

f is constant if $f(x) = f(y) \quad \forall x, y \in \{0,1\}^n$

f is balanced if $|f^{-1}(0)| = |f^{-1}(1)|$

The Deutsch-Jozsa Problem

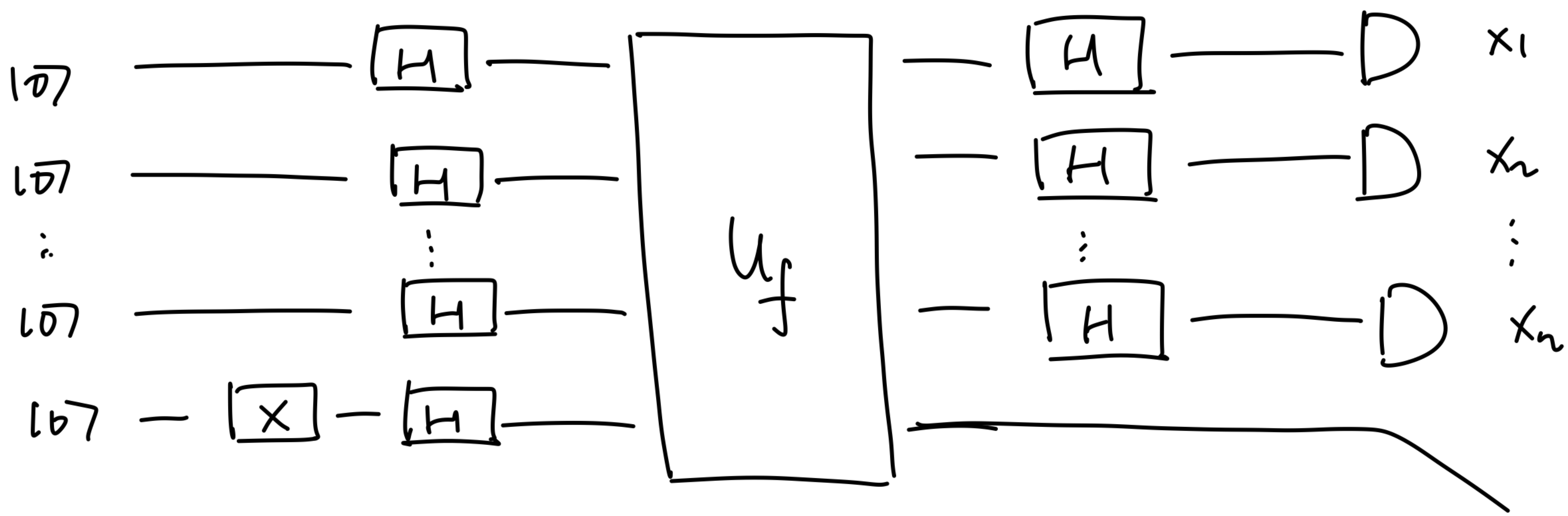
Given $f : \{0,1\}^n \longrightarrow \{0,1\}$
determine if f is constant or balanced

classical strategy $2^n/2$

Quantum algorithm $U_f \, |x\rangle|y\rangle = |x\rangle|y+f(x)\rangle$

✓ $U_f \, |x^n\rangle|y\rangle = |x^n\rangle|y+f(x^n)\rangle$

The Deutsch-Jozsa algorithm



f is constant $\Longleftrightarrow$ $x_1 x_2 \cdots x_n = 0 0 \cdots 0$

exercise. quantum state transformation from gates to gates

Remark. f is called only once.

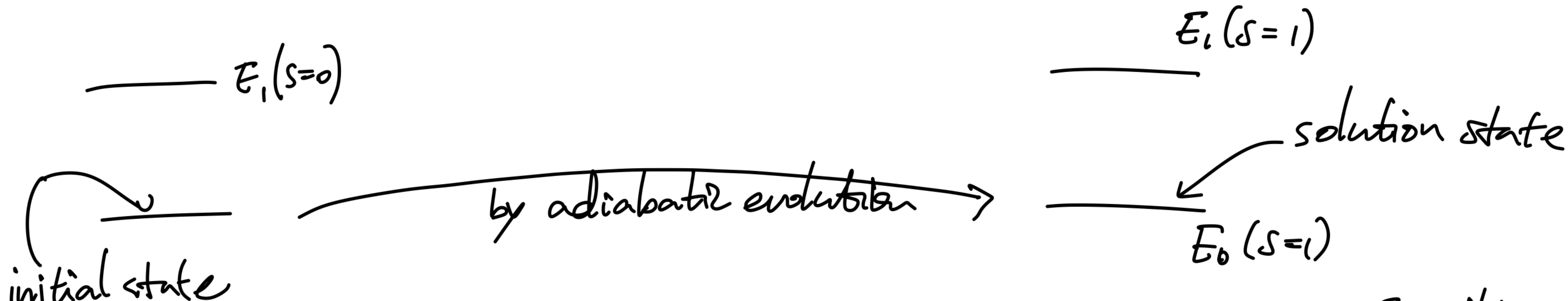
The Deutsch-Jozsa Algorithm in adiabatic evolution

$$D\left[|sol\rangle\langle sol|,\ \mathrm{tr}_A\, U_{SA}\, |0\rangle\langle 0|^{\otimes n} \otimes |A\rangle\langle A|\, U_{SA}^{\dagger} \right] < \varepsilon$$

dynamics performs computation

$H_0 = I - |\psi_0\rangle\langle\psi_0|$ $\qquad$ $H_1 = I - |\psi_1\rangle\langle\psi_1|$

$H(s) = (1-s)H_0 + sH_1$



$|\psi_0\rangle = |+\rangle^{\otimes n}$

f const. $\Leftrightarrow |\psi_1\rangle = |0\rangle$

$$|\psi_1\rangle = \alpha|0\rangle + \frac{\beta}{\sqrt{N-1}}\sum_{k=1}^{N-1}|k\rangle$$

$$\alpha = \frac{1}{N}\left|\sum_{x\in\{0,1\}^n}(-1)^{f(x)}\right|$$

$$\beta = 1-\alpha$$

Adiabatic theorem

$$\boxed{T \geq \sqrt{N}/\varepsilon}$$

$$H_0 = I - |\psi_0\rangle\langle\psi_0| \qquad H_1 = I - |\psi_1\rangle\langle\psi_1|$$

$$H(s) = (1-s)H_0 + sH_1$$

$E_1(s=0)$ $\qquad s(t) = t/T \qquad$ $E_1(s=1)$

solution state

initial state $\qquad$ by adiabatic evolution $\qquad$ $E_0(s=1)$

$$|\psi_0\rangle = |+\rangle^{\otimes n}$$

$$|\psi_1\rangle = \frac{\alpha}{\sqrt{N/2}} \sum_{k=0}^{N/2-1} |2k\rangle + \frac{1-\alpha}{\sqrt{N/2}} \sum_{i=0}^{N/2-1} |2i+1\rangle$$

$$\alpha = \frac{1}{N} \left| \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \right|$$

Adiabatic theorem

$$T \geq 4/\varepsilon \sim O(1)$$

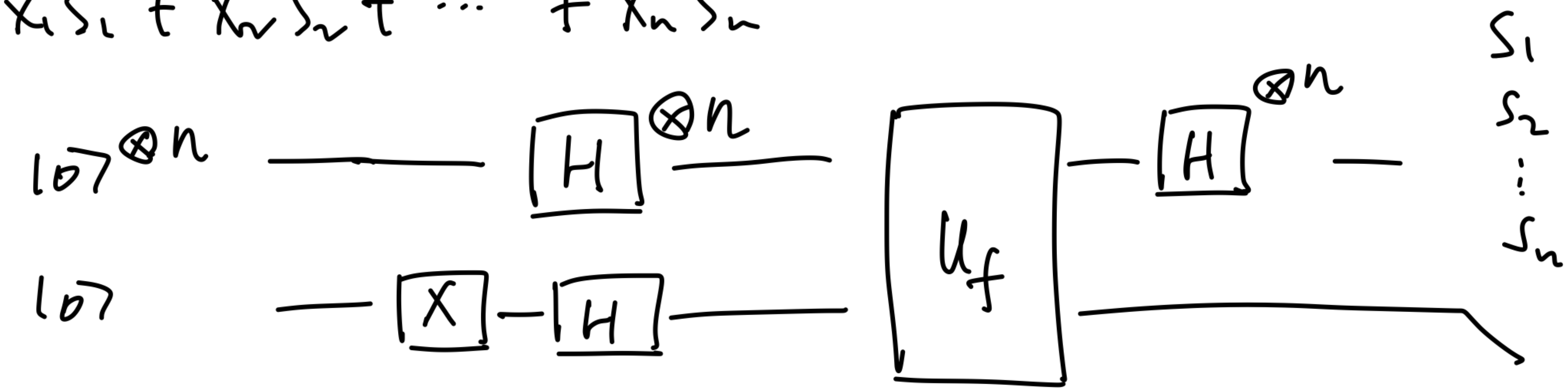
"no factor with n or N"

Bernstein-Vazirani algorithm

$$f_s(x) = x \cdot s \quad : \quad \{0,1\}^n \longrightarrow \{0,1\}$$

$$x \cdot s = x_1 s_1 + x_2 s_2 + \cdots + x_n s_n$$

Find s.



$$U_f |x\rangle|y\rangle = |x\rangle|y + f(x)\rangle$$

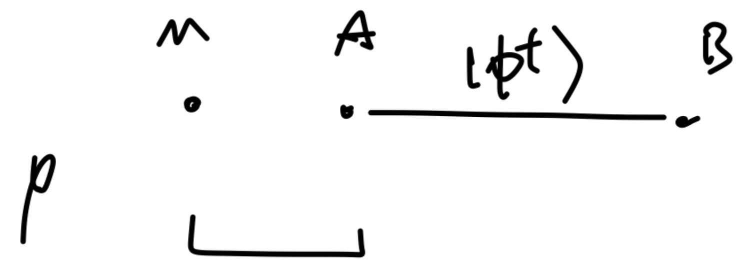
$$= |x\rangle|y + x \cdot s\rangle$$

Exercise. State transformation from a gate to a gate.

Measurement-Based Quantum Computation

Recall. Quantum teleportation

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$



$|\phi_1\rangle \cdots\cdots\rightarrow \rho$

$|\phi_2\rangle \cdots\cdots\rightarrow \sigma_z \rho \sigma_z$

$|\phi_3\rangle \cdots\cdots\rightarrow \sigma_x \rho \sigma_x$

$|\phi_4\rangle \cdots\cdots\rightarrow \sigma_y \rho \sigma_y$

$$|\phi_1\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\phi_2\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$|\phi_3\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$|\phi_4\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

$$\Rightarrow \quad \underset{\substack{\uparrow \\ \text{single-qubit} \\ \text{dynamics}}}{\Lambda_i[\rho]} = 4\, \mathrm{tr}_{MA}\left(\rho_M \otimes |\phi^+\rangle\langle\phi^+|_{AB}\right) |\phi_i\rangle\langle\phi_i|_{MA}$$

measurement on entangled states

Recall. CNOT + single-qubit operations ~ universal quantum computation

exercise

~ quantum teleportation.

$\Rightarrow$ Universal quantum computation can be realized by entangled states and measurements.

Quantum Algorithms : Solving mathematical problems with quantum systems

- Basics of Quantum Information Processing
- Idea of quantum computation
- Some Algorithms & Models
  - DJ algorithm   i) circuit models   ii) Adiabatic.