Quantum bits, gates & circuits; circuit model of quantum computation

qubit = quantum bit

= 2-state quantum syst

$$\begin{pmatrix}1\\0\end{pmatrix} = |0\rangle \qquad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

"computational states"

(orthogonal)

→ qubit state space: $\mathcal{H}_1 = \mathrm{Span}\{|0\rangle, |1\rangle\}$

$= \mathbb{C}^2$

- gen. pure q-bit state:

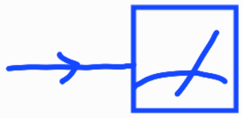
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- initial qubit states always computational states $|0\rangle$ or $|1\rangle$

  symbol: $\quad |i\rangle \rightarrow \quad i = 0,1$

- qubit measurements always w.r.t. computational base $|0\rangle, |1\rangle$

  symbol:



n-qubit register:

$$n \begin{cases} |i_{n-1}\rangle \\ |i_{n-2}\rangle \\ \vdots \\ |i_1\rangle \\ |i_0\rangle \end{cases}$$

state space: $\mathcal{H}_n = \mathcal{H}_1 \otimes \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_1 = \mathcal{H}_1^{\otimes n}$

$$\cong$$

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \cdots = \mathbb{C}^{(2^n)}$$

comp. base:

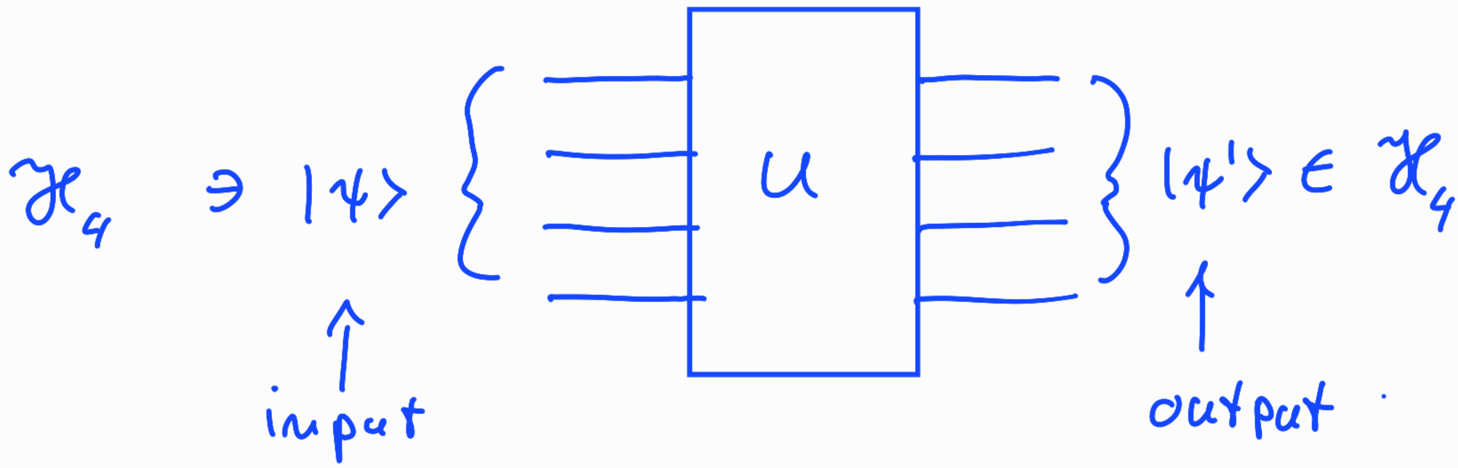
$$|00\ldots00\rangle = |0\rangle_n$$
$$|00\ldots01\rangle = |1\rangle_n$$
$$|00\ldots10\rangle = |2\rangle_n$$
$$\vdots$$
$$|11\ldots11\rangle = |2^n-1\rangle_n$$

$\rightarrow \quad \mathcal{H}_n = \text{Span}\{|i\rangle_n\}_{i=0,1,2,\ldots,2^n-1}$

k-qubit quantum gate:

implements unitary transformation on k qubits: $\mathcal{U} : \mathcal{H}_k \to \mathcal{H}_k$

symbol.:



$$|\psi'\rangle = \mathcal{U}\,|\psi\rangle$$

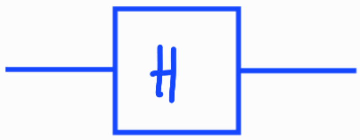
generally $\mathcal{U}$ represented as $k \times k$ matrix w.r.t. comp. base.

1-qubit-gates:

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

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

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

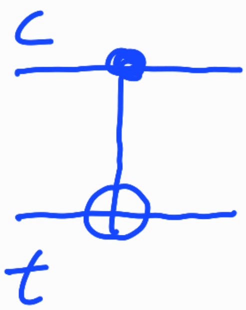


$H = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$: Hadamard

general unitary U on $\mathcal{H}_1$

2-qubit gates:

CNOT = controlled NOT:



$|c, t\rangle \longrightarrow |c, t \oplus c\rangle$

i.e.:

$|0\rangle = |00\rangle \rightarrow |00\rangle = |0\rangle$

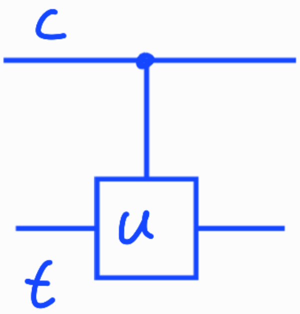
$|1\rangle = |01\rangle \rightarrow |01\rangle = |1\rangle$

$|2\rangle = |10\rangle \rightarrow |11\rangle = |3\rangle$

$|3\rangle = |11\rangle \rightarrow |10\rangle = |2\rangle$

$\rightarrow$ $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ (unitary!)

CU = controlled U:

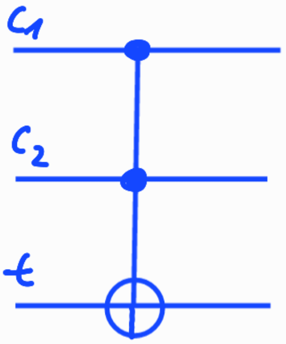


$$|0\rangle|t\rangle \longrightarrow |0\rangle|t\rangle$$

$$|1\rangle|t\rangle \longrightarrow |1\rangle\, U|t\rangle$$

$$\rightsquigarrow \quad CU = \begin{pmatrix} \mathbb{1}_2 & 0 \\ 0 & U \end{pmatrix}$$

3-qubit gate: CCNOT (Toffoli)



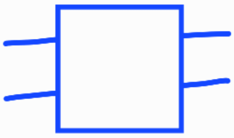
$$|c_1, c_2, t\rangle \longrightarrow |c_1, c_2, t \oplus (c_1 \text{ AND } c_2)\rangle$$

$$\rightsquigarrow \quad CCNOT = \begin{pmatrix} 1 &&&&&&& \\ & 1 &&&&&& \\ && 1 &&&&& \\ &&& 1 &&&& \\ &&&& 1 &&& \\ &&&&& 1 && \\ &&&&&& 0 & 1 \\ &&&&&& 1 & 0 \end{pmatrix}$$

classically universal!

Quantum circuit = directed, acyclic graph:

$\longrightarrow$ edge : qubit-channel

 knot : gate

$|i\rangle \longrightarrow$ ingoing edge :

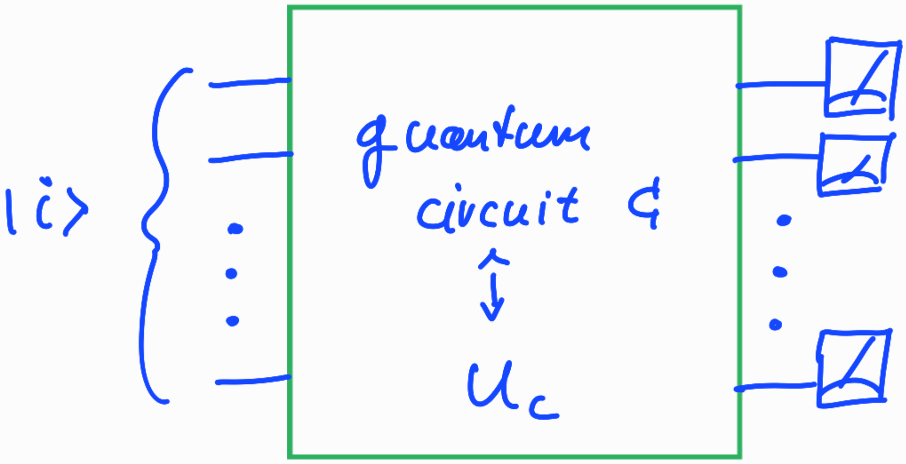
qubit in comp. stat $|i\rangle$

 outgoing edge :

qubit measurement w.r.t.

comp. base

$\Rightarrow$ circuit model of quantum computation:



(I) $\longrightarrow$ (II) $\longrightarrow$ (III) $\longrightarrow$ (IV)

$\longrightarrow$

(I) preparation of initial comp. state:

$$|i\rangle \in \mathcal{H}_n \, , \quad i \in \{0, 1, \dots, 2^n - 1\}$$

(II) unitary transf. of $|i\rangle$ according to quantum circuit:

$$|i\rangle \xrightarrow{U_c} |\psi\rangle = U_c |i\rangle$$

(III) measurement w.r.t. comp base:

$$A = \sum_{l=0}^{2^n-1} l \, |l\rangle\langle l|$$

$\rightarrow$ result $l \in \{0, 1, \dots, 2^n - 1\}$ with probability

$$p_l = |\langle l|\psi\rangle|^2 = |\langle l| U_c |i\rangle|^2$$

(IV) evtl. classical post-processing of measurement outcomes

Rmrk.: any classical computation can be implemented in a quantum circuit!

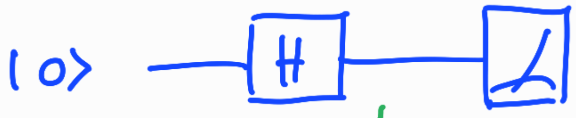
⌈ for two reasons:

(i) $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ can be made reversible!

$$\tilde{f}(x,y) := (x,\ y \oplus f(x))$$

(ii) quantum CCNOT $\overset{!}{=}$ classically universal gate! ⌋

Examples:

(i) 

:

$$|\psi\rangle = H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

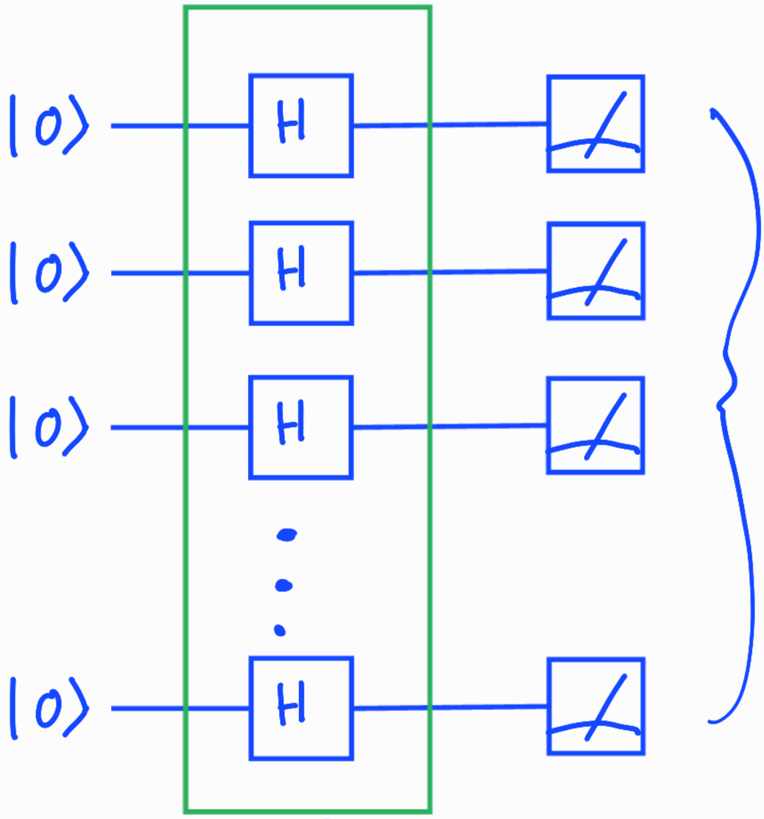
$0 : p_0 = \tfrac{1}{2}$

$1 : p_1 = \tfrac{1}{2}$

"true" 1-bit random number generator!

→

(2) <u>n-bit random number generator:</u>



$\hat{=} H^{\otimes n}$

n random bits $b_1, b_2, \dots, b_n$

$\stackrel{!}{=}$

1 n-bit random number

$r = (b_1 b_2 \dots b_n)$

<u>alternative view:</u> $|\psi\rangle = H^{\otimes n} |0\rangle_n = ?$

Hadamard on <u>single</u> qubit state $|0\rangle$:

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

$$\rightarrow \quad |\psi\rangle = \left(H|0\rangle\right)^{\otimes n} = \frac{1}{2^{n/2}}\left(|0\rangle + |1\rangle\right)^{\otimes n}$$

$$= \frac{1}{2^{n/2}}\left(|0\rangle + |1\rangle\right) \otimes \left(|0\rangle + |1\rangle\right) \otimes \dots$$

$$\rightarrow \quad |\psi\rangle = \frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} |i\rangle_n \quad \hat{=}$$

superposition of <u>all</u> comp. states with equal weight!

$\to$ measurement outcome $\ell \in \{0, \dots, 2^n - 1\}$

with $p_\ell = \frac{1}{2^n}$ ✓

<u>problem:</u> output of n-fold Hadamard on general input $|i\rangle$:

$$H^{\otimes n} |i\rangle = ?$$

<u>usefull:</u>

- <u>field</u> $\mathbb{F}_2 = (\mathbb{Z}_2, \oplus, \cdot)$

$\oplus$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$\to$ $\mathbb{Z}_2^n$ = n - dim. vector space over $K = \mathbb{F}_2$:

$$i \oplus j = (i_1 \oplus j_1, \dots, i_n \oplus j_n)$$

$$\underset{\in \mathbb{F}_2}{\lambda} i = (\lambda i_1, \dots, \lambda i_n$$

- standard inner product on $\mathbb{Z}_2^n$:

$$i \cdot j = \bigoplus_{l=1}^{n} i_l \cdot j_l$$

$$= \left(\sum_{l=1}^{n} i_l \cdot j_l \right) \bmod 2$$

.

then:

$$H \, |i\rangle_1 \stackrel{!}{=} \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^i \, |1\rangle \right)$$

$$\rightarrow \quad H^{\otimes} \, |i\rangle_n = \bigotimes_{l=1}^{n} \frac{1}{\sqrt{2}} \left(|0\rangle + (-1)^{i_l} \, |1\rangle \right)$$

$$= \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} (-1)^{\sum_l i_l j_l} \, |j\rangle$$

$$\rightarrow \quad \boxed{H^{\otimes} \, |i\rangle_n \stackrel{!}{=} \frac{1}{2^{n/2}} \sum_{j=0}^{2^n-1} (-1)^{i \cdot j} \, |j\rangle}$$

↑ closely related to ⟶

Discrete Fourier Transformation over $\mathbb{Z}_2^n$

(DFT)

$$
\begin{aligned}
f : \mathbb{Z}_2^n &\longrightarrow \mathbb{C} \\
i &\longmapsto f_i
\end{aligned}
$$

$$\Big\downarrow \mathcal{F}$$

$$
\begin{aligned}
\mathcal{F}[f] = \hat{f} : \mathbb{Z}_2^n &\longrightarrow \mathbb{C} \\
j &\longmapsto \hat{f}_j
\end{aligned}
$$

with

$$\boxed{\hat{f}_j := \frac{1}{2^{n/2}} \sum_{i=0}^{2^n-1} f_i \, (-1)^{i \cdot j}}$$

discrete version of continuous F.T:

- $\hat{f}(\vec{k}) = \int_{\mathbb{R}^n} d^n\vec{x} \; f(\vec{x}) \, e^{-i\vec{k}\cdot\vec{x}}$

- $(-1)^{i \cdot j} = e^{i\pi \, i \cdot j}$

in fact:

$$H^{\otimes n} \sum_i f_i |i\rangle = \sum_i f_i H^{\otimes n} |i\rangle$$

$$= \frac{1}{2^{n/2}} \sum_i f_i \sum_j (-1)^{i \cdot j} |j\rangle$$

$$= \sum_j \underbrace{\frac{1}{2^{n/2}} \sum_i f_i (-1)^{i \cdot j}}_{\stackrel{!}{=} \hat{f}_j} |j\rangle$$

hence:

$$\sum_i \underline{\underline{f_i}} |i\rangle \xrightarrow{\underline{\underline{H^{\otimes n}}}} \sum_j \underline{\underline{\hat{f}_j}} |j\rangle$$

$\blacksquare$