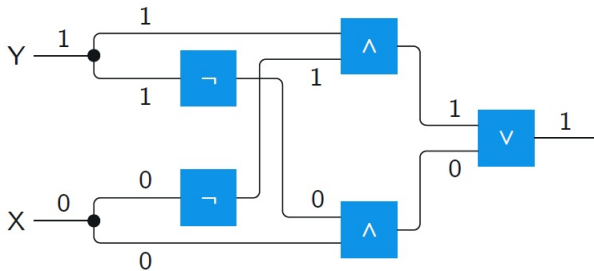


Kvantumalgoritmusok

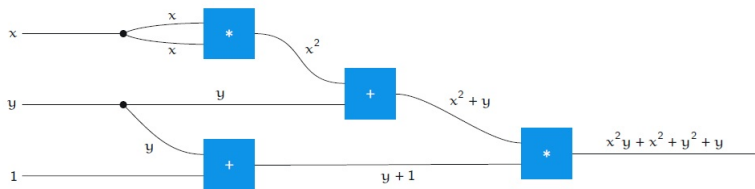
Kvantum áramkörök, kapuk, teleportáció

Áramkörök

Áramkörök számítási modellek, információ balról jobbra folyik.
A vonalak (wires) információt hordanak, a kapuk (gates)
leképezéseket reprezentálnak.



Áramkörök



Kvantum áramkörök

Kvantum áramkörben egy kapu (gate) unitér leképezést és mérést reprezentál.

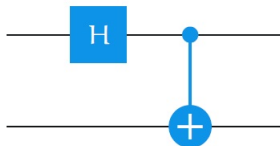
$$|0\rangle \text{ --- } \boxed{\text{H}} \text{ --- } \boxed{\text{S}} \text{ --- } \boxed{\text{H}} \text{ --- } \boxed{\text{T}} \text{ --- } \frac{1+i}{2}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \quad S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & \frac{1+i}{\sqrt{2}} \end{pmatrix}$$

$$THSH = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \end{pmatrix}$$

Példa

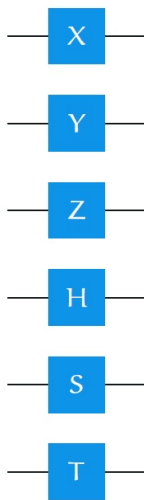
Qiskit rendezés: alulról-felfelé egyenlő a műveletek elvégzésével
balról-jobbra



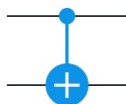
$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \end{pmatrix}$$

Gates

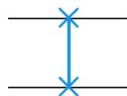
Single-qubit gates



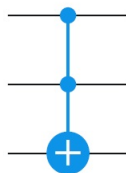
Controlled-NOT



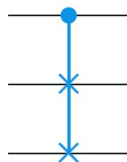
Swap gate



Toffoli gate

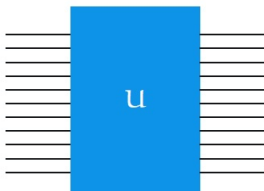


Fredkin gate

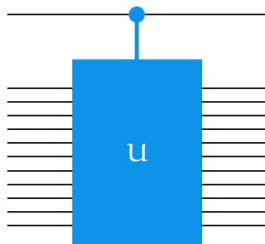


Unitér leképezések

Unitary operation



Controlled-unitary operation



SWAP leképezés

$$\text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\text{SWAP}|\phi^+\rangle = |\phi^+\rangle$$

$$\text{SWAP}|\phi^-\rangle = |\phi^-\rangle$$

$$\text{SWAP}|\psi^+\rangle = |\psi^+\rangle$$

$$\text{SWAP}|\psi^-\rangle = -|\psi^-\rangle$$

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

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|11\rangle$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle$$

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

Fredkin gate

A Fredkin gate egy controlled-SWAP leképezés három qubiton.

$$|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \text{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Toffoli gate

A Toffoli gate egy controlled-controlled-NOT leképezés három qubiton.

$$|0\rangle\langle 0| \otimes \mathbb{1} \otimes \mathbb{1} + |1\rangle\langle 1| \otimes (|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_x)$$

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

Még több kapu

Controlled-NOT leképezés

$$|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_x = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Controlled-Z leképezés

$$|0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_z = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

Teleportáció

Egy példa összefonódott állapotra (entangled state):

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

Azt mondjuk, hogy Alice és Bob-nak van egy *e-bit*jük, ha Alice-nak van qubit A és Bob-nak van qubit B , és együtt a pár (A, B) a $|\phi^+\rangle$ állapotban van.

Teleportáció protokoll

Alice és Bob osztózik egy e -biten, továbbá Alice szeretne a Q qubitet elküldeni Bobnak.

1. Alice elvégző egy controlled-NOT, ahol Q a kontrol és A a cél (target).
2. Alice elvégző egy Hadamard leképezést Q -n.
3. Alice méri A -t és Q -t, és kap két bináris kimenetet a és b .
4. Alice küldi a -t és b -t Bobnak.
5. Bob a következő két lépést hajt végre: Ha $a = 0$, akkor Bob elvégző egy X leképezést a B qubiten. Ha $b = 1$, akkor Bob elvégző egy Z leképezést a B qubiten.

Tehát a következő esetek fordulhatnak elő Bob számára:

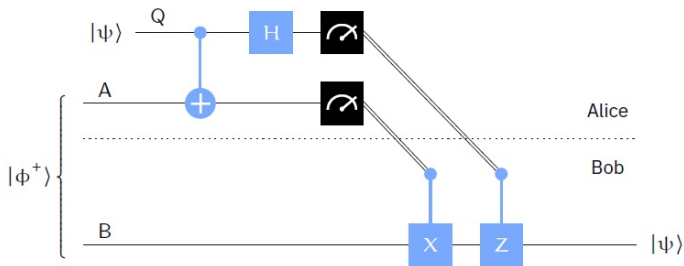
$$ab = 00 \Leftrightarrow \mathbb{I}$$

$$ab = 01 \Leftrightarrow Z$$

$$ab = 10 \Leftrightarrow X$$

$$ab = 11 \Leftrightarrow ZX$$

Teleportáció áramkör



E-bit megosztás és kvantumösszefonódás

- ▶ A kvantuminformáció törékenny.

E-bit megosztás és kvantumösszefonódás

- ▶ A kvantuminformáció törékeny.
- ▶ A kvantumállapot nem másolható (no-cloning tétel).

E-bit megosztás és kvantumösszefonódás

- ▶ A kvantuminformáció törékeny.
- ▶ A kvantumállapot nem másolható (no-cloning tétel).
- ▶ A klasszikus korreláció nem elegendő kvantumprotokollokhoz.

E-bit megosztás és kvantumösszefonódás

- ▶ A kvantuminformáció törékeny.
- ▶ A kvantumállapot nem másolható (no-cloning tétel).
- ▶ A klasszikus korreláció nem elegendő kvantumprotokollokhoz.
- ▶ Megoldás: **kvantumösszefonódás**.

Mi az az e-bit?

E-bit (entangled bit) = maximálisan összefonódott két-kubit állapot.

Leggyakoribb példa (Bell-állapot):

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

Mi az az e-bit?

E-bit (entangled bit) = maximálisan összefonódott két-kubit állapot.

Leggyakoribb példa (Bell-állapot):

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

Tulajdonságok:

- ▶ Nem szeparálható szorzatállapotra.
- ▶ Méréskor erős korreláció jelenik meg.
- ▶ A teljes rendszer tiszta, a részrendszer kevert.

Mi az összefonódás?

Egy két-részecske rendszer **összefonódott**, ha az állapota nem írható fel így:

$$|\psi\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$$

Mi az összefonódás?

Egy két-részecske rendszer **összefonódott**, ha az állapota nem írható fel így:

$$|\psi\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$$

Fontos jellemzők:

- ▶ Nem-klasszikus korreláció
- ▶ Bell-egyenlőtlenségek sértése
- ▶ Erőforrás kvantumkommunikációhoz

E-bit megosztásának folyamata

Általános lépések:

1. Összefonódott pár létrehozása
2. A két részecske fizikai szétválasztása
3. Küldés optikai szálon vagy szabad térben
4. Mérés és Bell-teszt

Kulcskérdés: fennmarad-e az összefonódás nagy távolságon?

Fizikai megvalósítások

Összefonódás létrehozása:

- ▶ Spontán paraméteres lesugárzás (SPDC)
- ▶ Csapdázott ionok
- ▶ Szupravezető qubitek
- ▶ Nitrogén-vakancia centrumok gyémántban

Kísérleti mérőföldkövek

- ▶ 1990-es évek: első km-es foton-összefonódás
- ▶ 2015: loophole-free Bell tesztek
- ▶ 2017: műholdas összefonódás több mint 1000 km-en
- ▶ Föld–műhold kvantumteleportáció

Műholdas e-bit megosztás

Eredmények:

- ▶ Összefonódott fotonpárok létrehozása műholdon
- ▶ Szétküldés két földi állomásra
- ▶ Több mint 1200 km távolság
- ▶ Bell-egyenlőtlenség sértés igazolása (A kvantumösszefonódás erősebb korrelációt hoz létre, mint amit bármilyen klasszikus, lokális modell megengedne.)

Jelentőség:

- ▶ Globális kvantuminternet alapja

Kvantumteleportáció

Teleportáció protokoll:

1. Alice és Bob megoszt egy e-bitet
2. Alice Bell-mérést végez
3. Klasszikus bitet küld Bobnak
4. Bob rekonstruálja az állapotot

Kvantumteleportáció

Teleportáció protokoll:

1. Alice és Bob megoszt egy e-bitet
2. Alice Bell-mérést végez
3. Klasszikus bitet küld Bobnak
4. Bob rekonstruálja az állapotot

Fontos: az e-bit valós fizikai erőforrás.

Mit tudunk ma?

- ▶ E-bitek laboratóriumban rutinszerűen létrehozhatók

Mit tudunk ma?

- ▶ E-bitek laboratóriumban rutinszerűen létrehozhatók
- ▶ Több száz km-es optikai szálak terjesztés működik

Mit tudunk ma?

- ▶ E-bitek laboratóriumban rutinszerűen létrehozhatók
- ▶ Több száz km-es optikai szálak terjesztés működik
- ▶ Műholdas elosztás demonstrálva

Mit tudunk ma?

- ▶ E-bitek laboratóriumban rutinszerűen létrehozhatók
- ▶ Több száz km-es optikai szálak terjesztés működik
- ▶ Műholdas elosztás demonstrálva
- ▶ Kvantumkulcs-megosztás működő technológia

Nyitott problémák

- ▶ Kvantumismétlők (quantum repeaters)
- ▶ Hosszú idejű kvantummemória
- ▶ Skálázható kvantuminternet
- ▶ Hibajavítás integrálása hálózatba

Összefoglalás

- ▶ Az e-bit valós, kísérletileg igazolt jelenség.
- ▶ Az összefonódás nem klasszikus korreláció.
- ▶ Nagy távolságon is megvalósítható.
- ▶ A kvantumkommunikáció alapvető erőforrása.