

Klasszikus vs kvantum

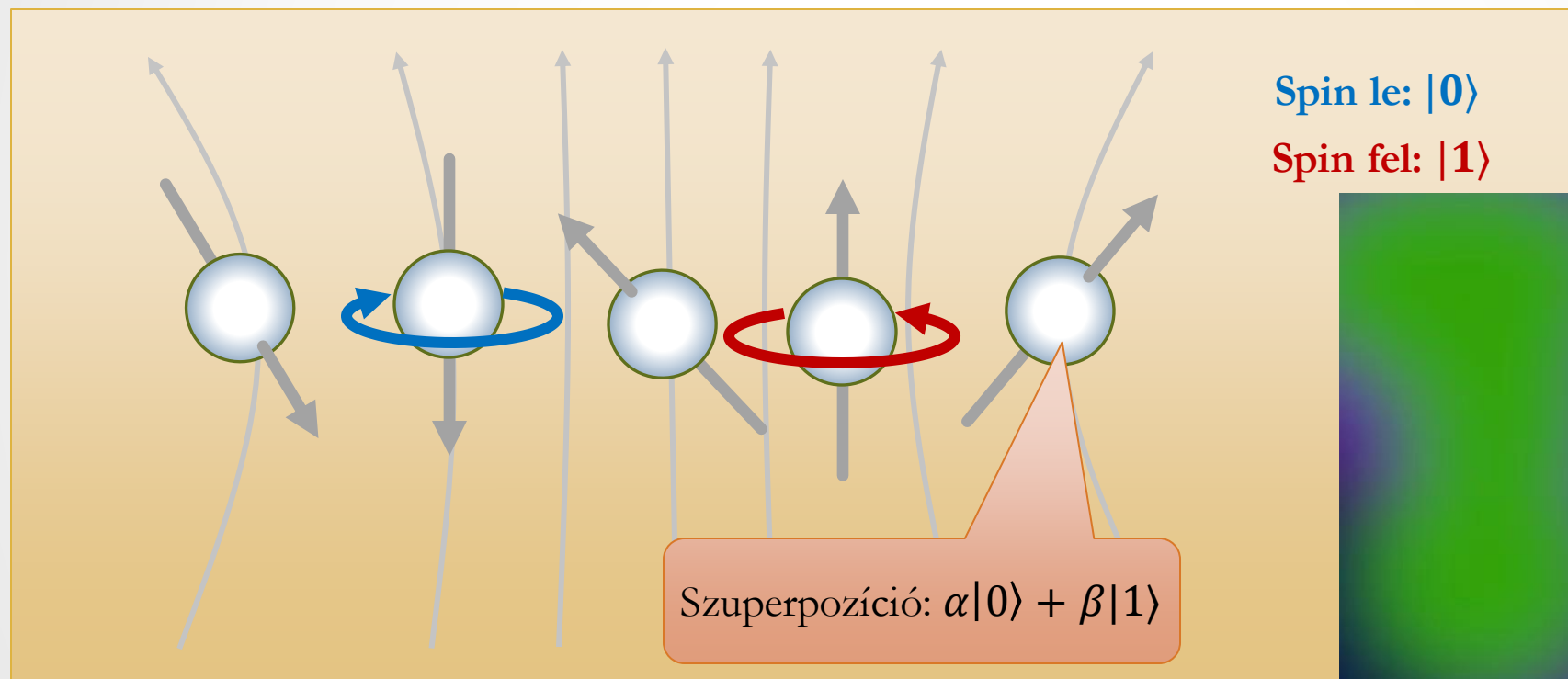
- A klasszikus számítógép
 - alap számítási egysége a **klasszikus bit**
 - egy (bitekből) álló regiszter manipulálásával csak **egy számot** (a regiszter tartalmát) képes változtatni
 - A számítás gyorsaságát gigaflops-ban mérjük (billions of floating-point operations per second)
- A kvantumszámítógép
 - alap számítási egysége a **kvantumbit**
 - egy kvantumbitekből álló regiszter manipulálásával **több számon** képes egyszerre számításokat végezni
 - Egy 30 kvantumbites kvantum számítógép sebessége megfelel egy 10 teraflops sebességű hagyományos számítógép sebességének

Mi tehát a kvantumbit?

- Kvantumbit tehát a kvantum információ **alapegysége**, egy két **állapotú kvantummechanikai rendszer**
 - Ez egy olyan rendszer mely képes a bázisállapotai bármilyen **szuperpozícióját** felvenni
 - A bázisállapotok szokásos jelölése: **$|0\rangle$** és **$|1\rangle$**
 - A bázisállapotok szuperpozíciója **$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$** ahol
 - α és β **valószínűségi amplitúdók** (α és β komplex számok)
 - $\alpha^2 + \beta^2 = 1$
 - például $|\psi\rangle = 0.8|0\rangle + 0.6|1\rangle$
 - Általában a **magasabb** energiaszintű bázisállapotot jelöli az **$|1\rangle$**
- Kvantumbit lehet például a foton, ahol a két bázisállapot a horizontális (**$|0\rangle$**) és a vertikális (**$|1\rangle$**) polarizáció

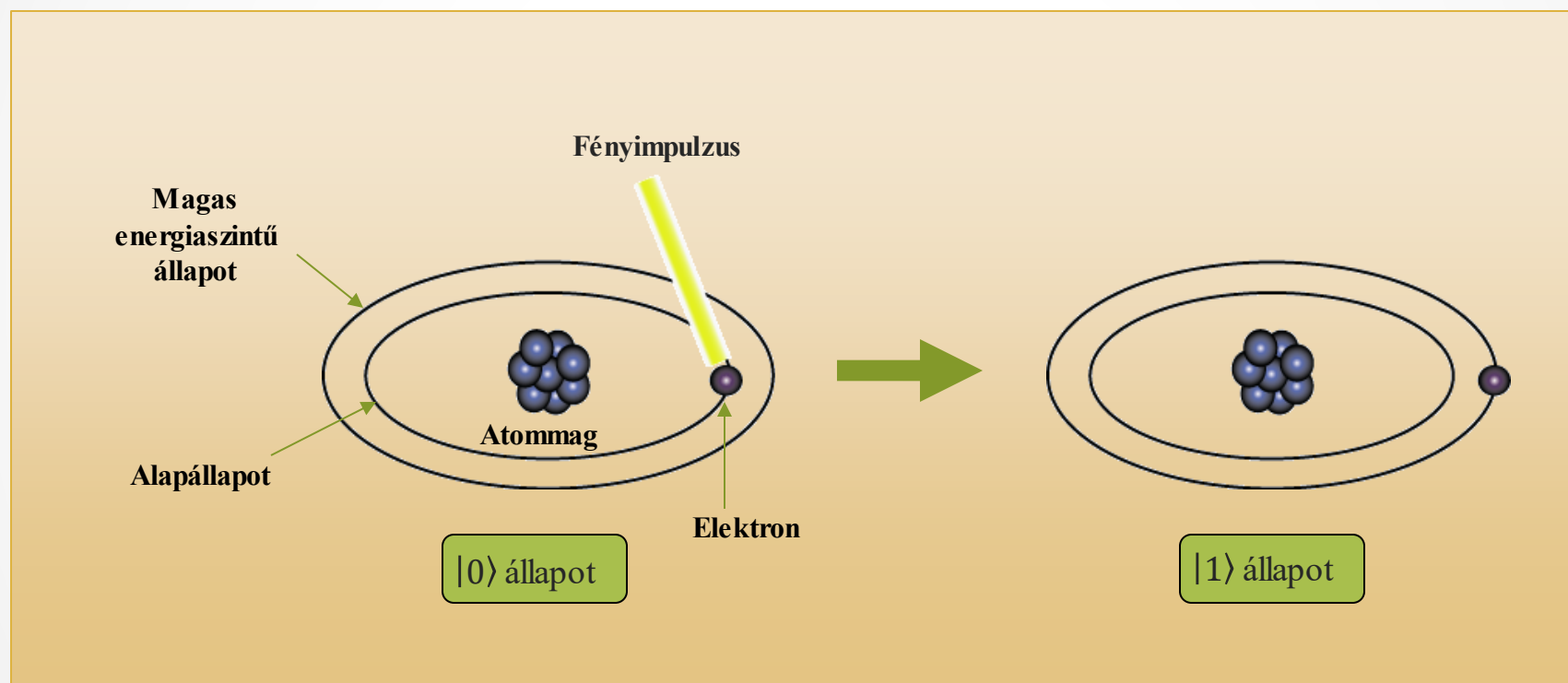
Miből lehet kvantumbit?

- Az egyik leggyakrabban használt fizikai kvantumbit-reprezentáció az elektron spin-je, ahol a bázisállapotok a spin irányai:



Miből lehet kvantumbit?

- Vagy lehet használni kvantumbitnek az elektron pályáját az atommag körül:



Kvantum regiszter

- Egy $\alpha|0\rangle + \beta|1\rangle$ kvantumbit **két számot** reprezentál: α -t és a β -t
- A kvantumbitekben rejlő hatalmas számítási potenciál csak akkor jelenik meg ha **egyszerre több** kvantumbitet, azaz egy **kvantum regisztert** használunk
- Két kvantumbitnek már **négyféle** bázisállapota van: $|00\rangle$, $|01\rangle$, $|10\rangle$ és $|11\rangle$
 - Két kvantumbit ezen négy bázis állapot **szuperpozíciójában** lehet:
$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$
 - Azaz két kvantumbittel már **négy számot** tudunk reprezentálni: α, β, γ és δ
 - Most is igaz, hogy $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1$
- Következik, hogy n kvantumbittel **2^n számot** lehet reprezentálni
- Ehhez képest n (klasszikus) biten **egy számot** tudunk csak reprezentálni (a lehetséges 2^n szám közül)

Kvantumbit mérése

- A kvantumszámítógép egy olyan gép ami képes egy n bites **kvantum regiszteren** műveletet végezve **egyszerre 2^n számot manipulálni**
- A gond az, hogy a kvantumrendszer által tárol számokat **nem lehet egyszerűen kiolvasni**
- Ha megmérünk egy $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ kvantumbitet, akkor α^2 valószínűséggel a $|0\rangle$, β^2 valószínűséggel pedig az $|1\rangle$ bázisállapotot kapjuk
 - Emlékezzünk vissza **a kalcit kristályos** kísérletre
 - Láttuk, hogy az első kristályból kilépve a foton hullámtermészete megmaradt
 - Viszont ha ekkor megmértük a foton polarizációját, akkor **50%** eséllyel horizontális, **50%** eséllyel pedig vertikális polarizációt mértünk
 - Valójában itt a fotonok az $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}i|1\rangle$ szuperpozícióban voltak

A kvantumbitek matematikai leírása

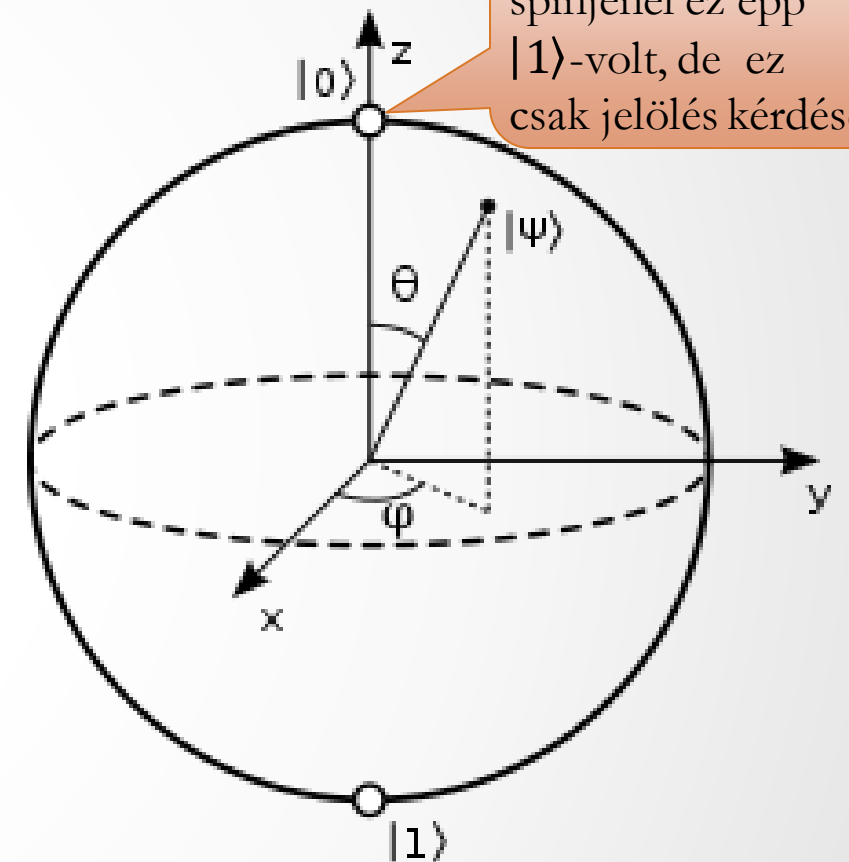
- A kvantumbiteken **kvantum kapuk** segítségével végezhetünk műveleteket
- A kvantum kapuk modellezhetők **mátrixokkal**
- Először nézzük meg, hogy hogyan reprezentálhatók a **kvantumbitek vektorokként**
- Legyen $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ egy kvantumbit
- $|0\rangle$ és $|1\rangle$ tekinthető két, egymásra merőleges **bázisvektornak**:
 - $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ és $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$
- $|\psi\rangle$ pedig megfelel a $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ vektornak
- Néhány nevezetes **szuperpozíció**:
 - $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$
 - $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$
 - $|i+\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}$

A Bloch gömb

- Emlékezzünk vissza arra, hogy a
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$
szuperpozícióban α és β **komplex számok**
- Így $|\psi\rangle$ ábrázolható az úgynevezett **Bloch gömbön** is:
- $$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

θ -t osztjuk 2-vel, mert a két bázis igazából csak 90 fokot zár be

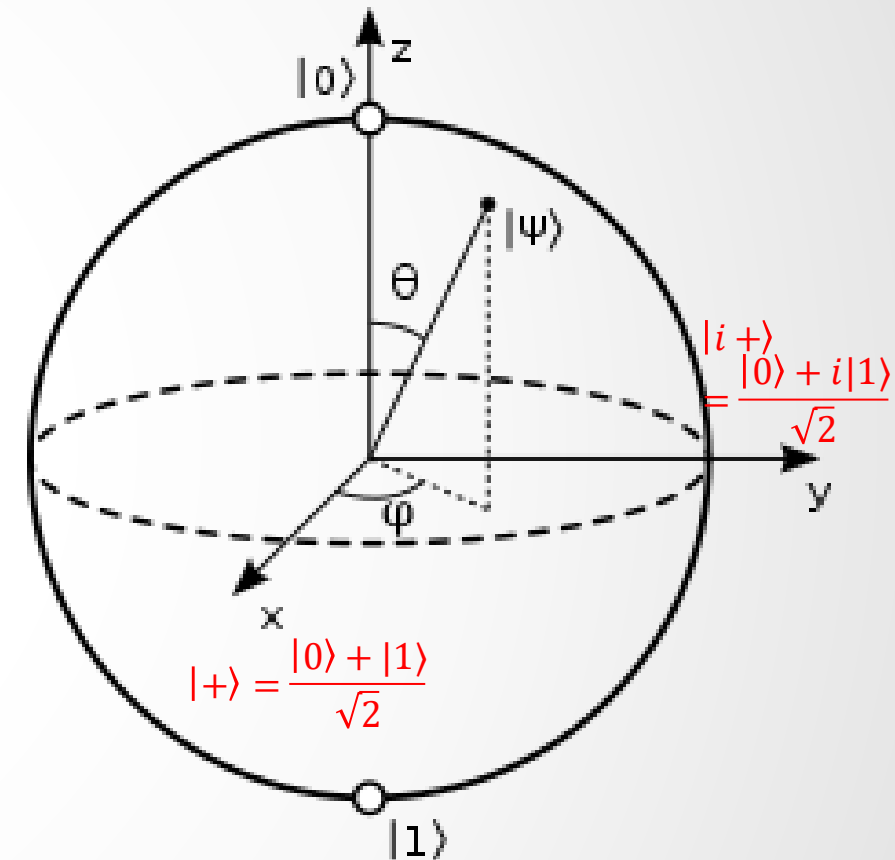
$$e^{ia\pi} = (-1)^a$$



A Bloch gömb

- Például ha θ 90 fok, φ pedig szintén 90 fok:
 - $|i+\rangle =$
$$= (\cos 45)|0\rangle + ((-1)^{\frac{1}{2}} \sin 45)|1\rangle =$$
$$= \frac{1}{\sqrt{2}}|0\rangle + i \frac{1}{\sqrt{2}}|1\rangle =$$
$$= \frac{|0\rangle + i|1\rangle}{\sqrt{2}}$$
- Hogyan **számoljuk ki** a bázisállapotok valószínűségét **komplex együtthatók** esetén?
 - Legyen $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$
 - $|\alpha|^2 = \bar{\alpha}\alpha$ és $|\beta|^2 = \bar{\beta}\beta$, ahol $\bar{}$ a **komplex konjugáltat** jelöli

Egy $\alpha = a + bi$ komplex szám
komplex konjugáltja $\bar{\alpha} = a - bi$



A Bloch gömb

- Az $|\alpha|^2$ és $|\beta|^2$ értékeket érdemes **mátrixszorzással** kiszámolni

- Például $|i+\rangle$ esetén $\alpha = \frac{1}{\sqrt{2}} + 0i$ és $\beta = 0 + \frac{1}{\sqrt{2}}i$

- A vektorok:

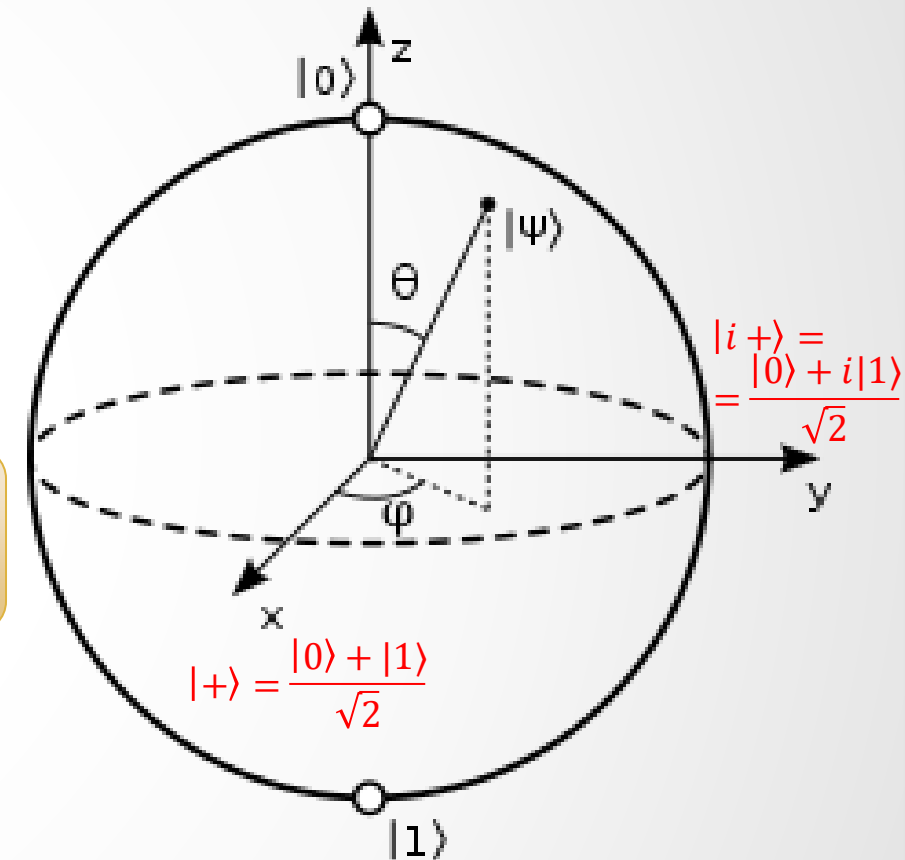
- $\alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}$ és $\beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}}i \end{bmatrix}$

- A szorzatok:

- $\bar{\alpha}\alpha = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \frac{1}{2} + 0 = \frac{1}{2}$

- $\bar{\beta}\beta = \begin{bmatrix} 0 & -\frac{1}{\sqrt{2}}i \end{bmatrix} \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}}i \end{bmatrix} = 0 + \frac{1}{2} = \frac{1}{2}$

Egyenlő
valószínűségek és
az összegük 1



Műveletek kvantumbiteken

- Hogyan lehet műveletet végezni egy kvantumbiten?

- Például mátrixszorzással:

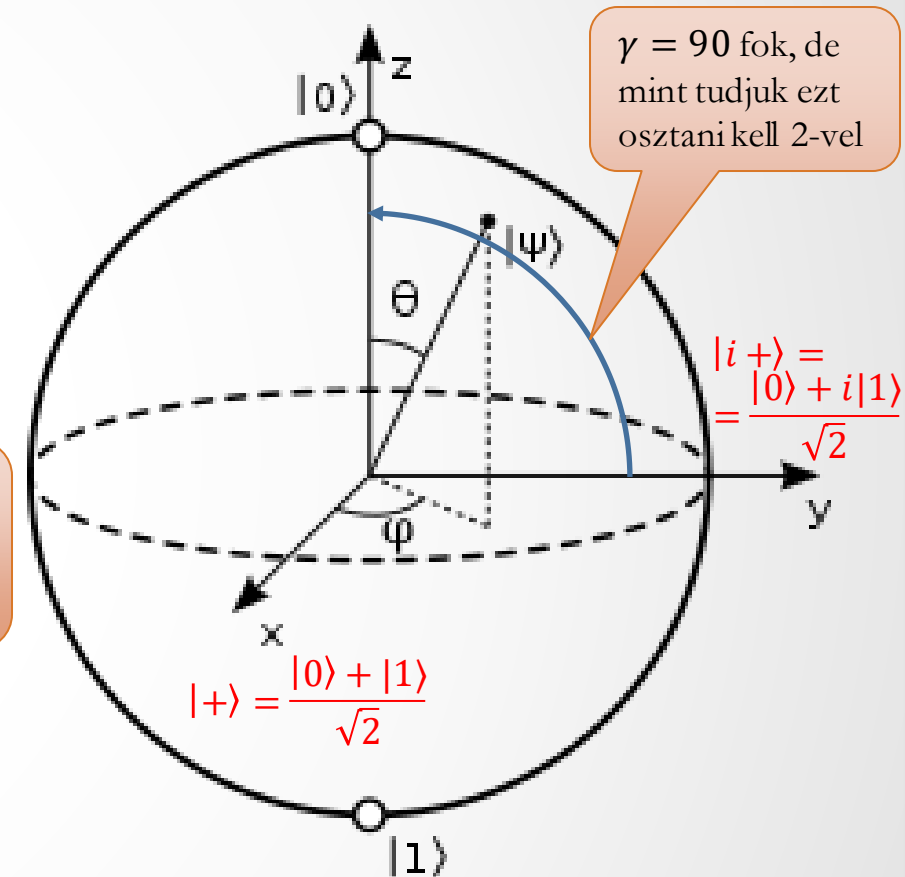
- Legyen pl. $U = \begin{bmatrix} \cos \frac{\gamma}{2} & -i \sin \frac{\gamma}{2} \\ -i \sin \frac{\gamma}{2} & \cos \frac{\gamma}{2} \end{bmatrix}$, ami megfelel az x tengely

körüli γ fokkal történő (óramutató irányával ellentétes) elforgatásnak

- Ha $\gamma = 90$, akkor $U = \begin{bmatrix} \frac{1}{\sqrt{2}} & -i \frac{1}{\sqrt{2}} \\ -i \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$

U egy unitér mátrix
Unitér: $U^*U = UU^* = I$
 U^* : U transzponált konjugáltja
 I : egységmátrix

- Akkor $U|i+\rangle = U \begin{bmatrix} \frac{1}{\sqrt{2}} \\ i \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} + \frac{1}{2} \\ -i \frac{1}{\sqrt{2}} + i \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$



Kvantum regiszterek

- Több kvantumbit szuperpozíciója is reprezentálható mátrixszal
- Legyen $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ és $|\phi\rangle = \gamma|0\rangle + \delta|1\rangle$

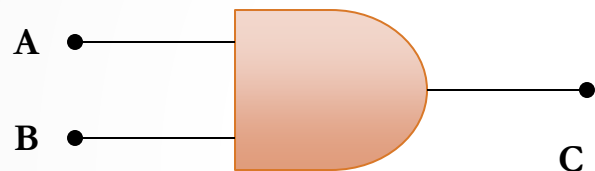
- Ekkor $|\psi\phi\rangle = \left[\begin{array}{c} \alpha\gamma \\ \alpha\delta \\ \beta\gamma \\ \beta\delta \end{array} \right] \} |\psi\rangle \otimes |\phi\rangle$ (tenzorszorzat)

- Általánosítható több kvantumbitre
- Példa:

- $|101\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0]^T$
- $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |111\rangle)$

Kvantum kapuk

- Milyen kapukat engedhetünk a kvantumszámítógépekben?
- Vizsgáljuk meg a klasszikus AND kaput



Input		Output
A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

Itt információvesztés
történik

- Az AND kapu kimenetéből nem lehet megállapítani, hogy mi volt a bemenet
- Az ilyen kapukkal tehát **információt veszítünk**
- A kvantumfizika természete alapján az információvesztés **hő termelésével** jár, ami elronthatja az állapotok szuperpozícióját

Műveletek kvantumbiteken – a megfordítható logika

- A kvantumszámítógépekben tehát csak olyan kapukat használunk melyek alkalmazása **nem jár információvesztéssel**
- Az **unitér mátrixokkal** megvalósított műveletek nem járnak információvesztéssel, mert a művelet „**megfordítható**”:

$$U^*U|\varphi\rangle = I|\varphi\rangle = |\varphi\rangle$$

- A kvantumszámítógépekben tehát **unitér mátrixokkal megvalósítható kapukat** használunk
- Következik, hogy egy számítás csak akkor valósítható meg egy kvantumszámítógéppel, ha **megfordítható**
- Ismert, hogy minden determinisztikus számítás **megfordíthatóvá** tehető (Charles Bennet, 1973)

Kvantum kapuk – a Hadamard kapu

- Az egyik legegyszerűbb kvantum kapu a **Hadamard** kapu, melynek mátrixa:

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

$H^* = H$, azaz H egy hermitikus mátrix

- A Hadamard mátrix unitér:

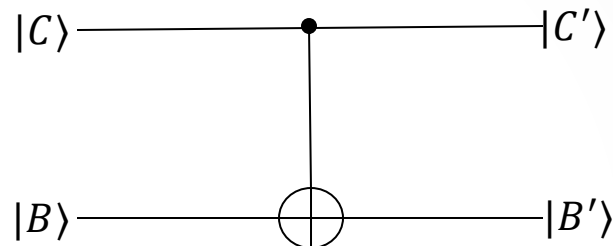
$$H^*H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

- A segítségével kvantum bázisok **egyenlő valószínűségű** szuperpozíciója állítható elő:

$$H|0\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$$

Kvantum kapuk - Kontrollált NOT

- A **kontrollált NOT** (CNOT) kapunak két kvantumbit a bemenete



- A CNOT mátrixa:
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- Legyen például $|C\rangle = |1\rangle$ és $|B\rangle = |0\rangle$

- $$|C\rangle \otimes |B\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \text{ és } \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |1\rangle \otimes |1\rangle$$

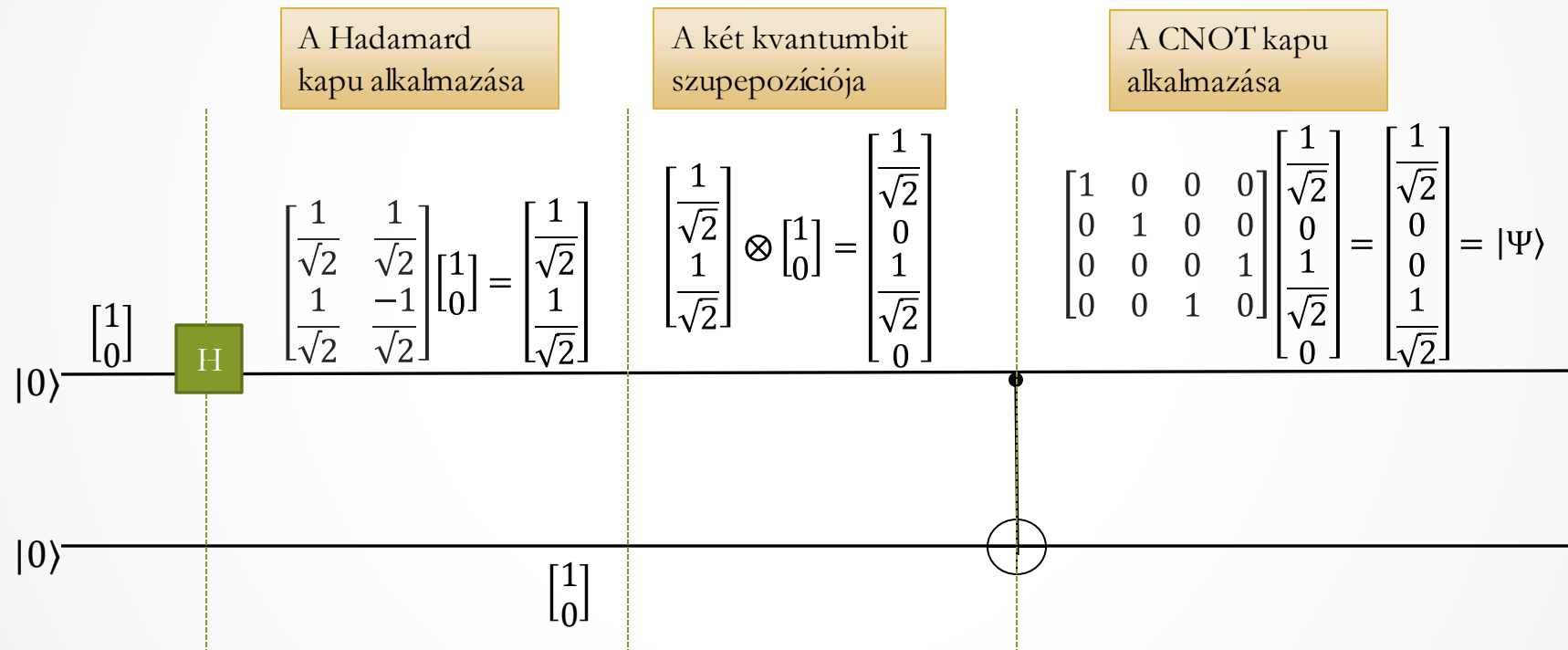
Bemenet		Kimenet	
C	B	C'	B'
$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$
$ 1\rangle$	$ 1\rangle$	$ 1\rangle$	$ 0\rangle$

$|C\rangle \oplus |B\rangle$
kizáró vagy

Ha $|C\rangle$ fixen $|1\rangle$
akkor a CNOT a
klasszikus tagadás

Kvantum-kapuk

Állítsuk elő a $|\Psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ két kvantumbites szuperpozíciót:



Kvantum-összefonódás

- A **kvantum-összefonódás** az a jelenség amikor két kvantumbit szuperpozícióját nem lehet a kvantumbitek szorzatával leírni
- Például a $|\Psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ állapot **összefonódott** mert
$$|\Psi\rangle \neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$$
- Ha $|\Psi\rangle$ -ben az első kvantumbitet $|0\rangle$ -nak mérjük, akkor a második kvantumbit is beesik ugyanebbe a bázisállapotba, ha viszont $|1\rangle$ -nek mérjük, akkor a másik is ebbe a bázisállapotba esik
- Ez akkor is teljesül ha két összefonódott kvantumrészecskét téreben eltávolítjuk egymástól
 - A távolságtól függetlenül a két részecske ugyanabban az időben fogja felvenni a két ellentétes bázisállapotot
 - Einstein: Spooky action at a distance