

Eötvös Loránd Tudományegyetem
Természettudományi Kar

Kvantum-számításelmélet jegyzet (töredék)



Józsa Richárd előadásai nyomán készítette:

Gilyén András

Budapest, 2024

1. Végés dimenziós kvantummechanika és formalizmus

Ebben a szakaszban a kvantummechanika posztulátumait és a kapcsolódó alapvető lineáris algebrai fogalmakat tárgyaljuk röviden, valamint bevezetjük a kvantumfizikában használt Dirac-féle bra-ket jelölésrendszert.

1.1. Végés dimenziós Hilbert-terek

Egy n dimenziós \mathcal{H} Hilbert tér egy n dimenziós komplex vektortér ellátva egy $\langle \cdot | \cdot \rangle : \mathcal{H} \times \mathcal{H} \rightarrow \mathbb{C}$ pozitív definit (belső) skalárszorzattal:

- (i) $\langle \mathbf{w} | \mathbf{v} \rangle = \langle \mathbf{v} | \mathbf{w} \rangle^*$ (a $*$ komplex konjugáltat jelöl)
- (iia) $\langle \mathbf{w} | \alpha \mathbf{v}_1 + \beta \mathbf{v}_2 \rangle = \alpha \langle \mathbf{w} | \mathbf{v}_1 \rangle + \beta \langle \mathbf{w} | \mathbf{v}_2 \rangle$
(azaz lineáris a második változóban)
- (iib) $\langle \gamma \mathbf{w}_1 + \delta \mathbf{w}_2 | \mathbf{v} \rangle = \gamma^* \langle \mathbf{w}_1 | \mathbf{v} \rangle + \delta^* \langle \mathbf{w}_2 | \mathbf{v} \rangle$
(avagy konjugált lineáris az első változóban)
- (iii) $\langle \mathbf{v} | \mathbf{v} \rangle \in \mathbb{R}_0^+$ és $\langle \mathbf{v} | \mathbf{v} \rangle = 0 \iff \mathbf{v} = 0$ (pozitív definit)

További definíciók és tulajdonságok:

- Ha $\langle \mathbf{w}, \mathbf{v} \rangle = 0$, akkor a \mathbf{w} és \mathbf{v} vektorokat merőlegesnek (ortogonálisnak) nevezzük,
- Definiálható a vektorok normája: $\|\mathbf{v}\| = \sqrt{\langle \mathbf{v} | \mathbf{v} \rangle}$
- Teljesül a Cauchy-Schwartz egyenlőtlenség: $|\langle \mathbf{w}, \mathbf{v} \rangle| \leq \|\mathbf{w}\| \cdot \|\mathbf{v}\|$
- Van ONB (ortonormált bázis): $\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n : \langle \mathbf{e}_i | \mathbf{e}_j \rangle = \delta_{ij}$
($\delta_{ij} = 1$ ha $i = j$ különben 0.)
- Kifejtés ONB-ban: $\mathbf{v} = \sum_{i=1}^n \langle \mathbf{e}_i | \mathbf{v} \rangle \mathbf{e}_i$

Példa: Legyen $\mathcal{H} = \mathbb{C}^3$, és gondoljunk a vektorokra mint oszlopvektorokra. Ekkor a legtermészetesebb belső szorzat definíció a következő: $(\mathbf{w}, \mathbf{v} \in$

\mathcal{H}) $\langle \mathbf{w} | \mathbf{v} \rangle := \mathbf{w}^{*T} \cdot \mathbf{v}$. (A *T az oszlopvektor elemenként vett komplex konjugáltjának a transzponáltját jelöli.)

$$\text{Pl. } \mathbf{w} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}, \mathbf{v} = \begin{bmatrix} d \\ e \\ f \end{bmatrix}, \langle \mathbf{w} | \mathbf{v} \rangle = \begin{bmatrix} a^* \\ b^* \\ c^* \end{bmatrix}^T \begin{bmatrix} d \\ e \\ f \end{bmatrix} = a^*d + b^*e + c^*f.$$

Ez a skalárszorzás definíció tulajdonképpen ekvivalens azzal, hogy ONB lesz a számítási bázis:

$$\left\{ \mathbf{e}_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \mathbf{e}_2 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}, \mathbf{e}_3 = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \right\}$$

De persze a számítási bázis mellett sok másik ONB is akad, pl.:

$$\left\{ \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix}, \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ e^i \end{bmatrix} \right\}$$

Ha a számítási bázis ONB, akkor a *T művelet megfelel az adjungálásnak. Az adjungálást \dagger (dagger)-rel jelöljük. Néhány fontos tulajdonsága: (ha *T -ként gondolunk rá, akkor könnyen látszanak)

- $\langle \mathbf{w} | \mathbf{v} \rangle = \mathbf{w}^\dagger \mathbf{v}$ és $(\mathbf{w}^\dagger)^\dagger = \mathbf{w}$
- $\langle \mathbf{w} | A\mathbf{v} \rangle = \langle \mathbf{w} A^\dagger | \mathbf{v} \rangle$ és $(A^\dagger)^\dagger = A$
- $(A\mathbf{v})^\dagger = \mathbf{v}^\dagger A^\dagger$ és $(AB)^\dagger = B^\dagger A^\dagger$
- $(\lambda \mathbf{w})^\dagger = \lambda^* \mathbf{w}^\dagger$ és $(\lambda A)^\dagger = \lambda^* A^\dagger$

A jegyzetben a vektorterek önmagukra menő lineáris leképezéseit egyszerűen csak (lineáris) operátoroknak fogjuk nevezni, és többször a lineáris jelzöt is le hagyjuk.

A legsűrűbben unitér operátorokkal fogunk majd foglalkozni. Definíció szerint az U operátor unitér, ha $U^{-1} = U^\dagger$, avagy $U^\dagger U = I$. Ezzel a definícióval ekvivalens, hogy mátrixának oszlopai (sorai) merőlegesek egymásra és bármely oszlopának (sorának) 1 a normája.

Az unitér operátorok talán legfontosabb tulajdonsága, hogy megtartják a skaláris szorzat értékét: $\langle U\mathbf{w} | U\mathbf{v} \rangle = \langle \mathbf{w} | U^\dagger U \mathbf{v} \rangle = \langle \mathbf{w} | I \mathbf{v} \rangle = \langle \mathbf{w} | \mathbf{v} \rangle$.

1.2. Vektorok és vektorterek tenzorszorzata

Legyen \mathcal{V} és \mathcal{W} egy n illetve m dimenziós vektortér és $\{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n\}$ illetve $\{\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_m\}$ a terek bázisai. Ekkor a \mathcal{V} és \mathcal{W} vektorterek tenzor szorzata egy $n \cdot m$ dimenziós vektortér, amit $\mathcal{V} \otimes \mathcal{W}$ -el jelölünk. Ezt a vektorteret tekinthetünk úgy mint az $\mathbf{e}_i \otimes \mathbf{f}_j$ ($0 \leq i, j \leq n, m$) „szimbólumokból” képzett $\left\{ \sum_{i,j}^{n,m} \gamma_{i,j} \cdot \mathbf{e}_i \otimes \mathbf{f}_j \mid \gamma_{i,j} \in \mathbb{C} \right\}$ formális lineáris kombinációk által alkotott vektorteret. Ez utóbbit pedig azonosíthatjuk a $\mathbb{C}^{n \cdot m}$ oszlopvektorok terével.

Például ha $\mathcal{V} = \mathcal{W} = \mathbb{C}^2$, akkor az azonosítást az alábbi „lexikografikus” elrendezésben szokás megtenni:

$$\mathbf{e}_1 \otimes \mathbf{f}_1 \leftrightarrow \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \mathbf{e}_1 \otimes \mathbf{f}_2 \leftrightarrow \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \mathbf{e}_2 \otimes \mathbf{f}_1 \leftrightarrow \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \mathbf{e}_2 \otimes \mathbf{f}_2 \leftrightarrow \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Vektorok tenzorszorzata alatt az alábbi $(\cdot, \cdot) : \mathcal{V} \times \mathcal{W} \mapsto \mathcal{V} \otimes \mathcal{W}$ bilineáris beágyazást értjük: $(\mathcal{V} \ni \mathbf{v} := \sum_{i=1}^n a_i \cdot \mathbf{e}_i, \mathcal{W} \ni \mathbf{w} := \sum_{j=1}^m b_j \cdot \mathbf{f}_j)$

$$(\mathbf{v}, \mathbf{w}) \rightarrow \mathbf{v} \otimes \mathbf{w} = \left(\sum_{i=1}^n a_i \cdot \mathbf{e}_i \right) \otimes \left(\sum_{j=1}^m b_j \cdot \mathbf{f}_j \right) := \sum_{i=1}^n \sum_{j=1}^m a_i b_j \cdot \mathbf{e}_i \otimes \mathbf{f}_j.$$

Tenzorszorzat az oszlopvektorok nyelvén az előbbi példával illusztrálva:

$$\begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \rightarrow \begin{bmatrix} a_1 \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \\ a_2 \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{bmatrix}$$

Megjegyzés: Sokszor hasznos a tenzorszorzatként kapott vektor együtthatóit táblázatos formában elképzelni:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow \begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix} \quad \text{Általánosan: } \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \otimes \begin{bmatrix} b_1 \\ b_2 \end{bmatrix} \rightarrow \begin{matrix} a_1 b_1 & a_1 b_2 \\ a_2 b_1 & a_2 b_2 \end{matrix}$$

A fenti alak jól mutatja, hogy nem minden $\mathcal{V} \otimes \mathcal{W}$ -beli vektor áll elő tenzorszorzatként. Azokat a vektorokat amelyek előállnak így, szorzatvektoroknak

nevezzük, amelyek nem állnak elő azokat pedig összefonódott (angolul: entangled) vektoroknak. (Meggondolható, hogy pontosan azok a szorzatvektorok, amelyek fenti táblázatos alakban írt koordinátái 1 rangú együtthatómátrixot alkotnak.)

Ha \mathcal{V} és \mathcal{W} is Hilbert-tér, akkor ez a Hilbert-tér struktúra természetes módon átörökíthető $\mathcal{V} \otimes \mathcal{W}$ -re. A szorzatvektorokon az alábbi módon definiálhatjuk a skaláris szorzást: (A $\langle \cdot | \cdot \rangle$ alsó index azt jelöli, hogy mikor melyik tér belső szorzatáról van szó.)

$$\langle \mathbf{v}_1 \otimes \mathbf{w}_1 | \mathbf{v}_2 \otimes \mathbf{w}_2 \rangle_{V \otimes W} := \langle \mathbf{v}_1 | \mathbf{v}_2 \rangle_V \cdot \langle \mathbf{w}_1 | \mathbf{w}_2 \rangle_W.$$

Így ha $\{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n\}$ és $\{\mathbf{f}_1, \mathbf{f}_2, \dots, \mathbf{f}_m\}$ ONB, akkor $\mathbf{e}_i \otimes \mathbf{f}_j$ is ONB lesz. Ezáltal pedig a definíció kiterjeszthető összefonott vektorokra is: tetszőleges $\mathbf{z} \in V \otimes W$ vektort kifejtethető $\sum_{i,j}^{n,m} \gamma_{i,j} \cdot \mathbf{e}_i \otimes \mathbf{f}_j$ alakban. Így definiálható

$$\langle \mathbf{z} | \mathbf{q} \rangle = \left\langle \sum_{i,j}^{n,m} \gamma_{i,j} \cdot \mathbf{e}_i \otimes \mathbf{f}_j \left| \sum_{k,l}^{n,m} \beta_{k,l} \cdot \mathbf{e}_k \otimes \mathbf{f}_l \right. \right\rangle := \sum_{i,j}^{n,m} \gamma_{i,j}^* \cdot \beta_{i,j}.$$

1.3. Operátorok (azaz lineáris leképezések) tenzorszorzata

Legyen $A : \mathcal{V} \rightarrow \mathcal{V}$ és $B : \mathcal{W} \rightarrow \mathcal{W}$ lineáris leképezés (avagy operátor). Ekkor az $A \otimes B : \mathcal{V} \otimes \mathcal{W} \rightarrow \mathcal{V} \otimes \mathcal{W}$ operátor szorzatvektorokon legyen az alábbi módon definiálva:

$$A \otimes B(\mathbf{v} \otimes \mathbf{w}) := A(\mathbf{v}) \otimes B(\mathbf{w})$$

Hasonlóan mint az előbb, a definíció lineárisan kiterjeszthető összefonott vektorokra is, mivel az $\mathbf{e}_i \otimes \mathbf{f}_j$ bázison már definiálva van a leképezést.

Például legyen $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$ és $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$ ekkor $A \otimes B$ blokkmátrix alakú, azaz

$$A \otimes B = \begin{bmatrix} a_{11} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{12} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \\ a_{21} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} & a_{22} \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{bmatrix}$$

1.4. Dirac-féle bra-ket jelölés

Mostantól a \mathcal{H} Hilbert-tér elemeit \mathbf{v} helyett $|v\rangle$ -vel fogjuk jelölni (ezek a Dirac-féle jelölés ket vektorai), és úgy fogunk rájuk gondolni mint egy ONB-ben felírt oszlopvektorra. A számítási bázis elemeit pedig \mathbf{e}_{i+1} helyett egyszerűen $|i\rangle$ -vel fogjuk jelölni. A \mathbf{v}^\dagger adjungált (sor)vektor helyett pedig a $\langle v|$ bra vektor jelölést vezetjük be.

Például a $\dim(\mathcal{H}) = 2$ estben az új jelölés így váltja le a régít:

$$\mathbf{v} = a \cdot \mathbf{e}_1 + b \cdot \mathbf{e}_2 = \begin{bmatrix} a \\ b \end{bmatrix} = a |0\rangle + b |1\rangle = |v\rangle$$

$$\mathbf{v}^\dagger = a^* \cdot \mathbf{e}_1^\dagger + b^* \cdot \mathbf{e}_2^\dagger = [a^* \quad b^*] = a^* \langle 0| + b^* \langle 1| = \langle v|$$

Megjegyzés: A skalárok és operátorok kiemelésekor vigyázni kell, ugyanis míg $|\lambda v\rangle = \lambda \mathbf{v} = \lambda |v\rangle$ és $|A v\rangle = A \mathbf{v} = A |v\rangle$ addig a bra vektorokra $\langle \lambda v| = (\lambda \mathbf{v})^\dagger = \lambda^* \mathbf{v}^\dagger = \lambda^* \langle v|$ és $\langle A v| = (A \mathbf{v})^\dagger = \mathbf{v}^\dagger A^\dagger = \langle v| A^\dagger$.

A Dirac-féle jelölésrendszer szépségét az adja, hogy a skalárszorzat jelöléséhez tökéletesen illeszkedik, és így segít összevonni amit könnyen össze lehet:

$$\langle \mathbf{w} | \mathbf{v} \rangle = \mathbf{w}^\dagger \cdot \mathbf{v} = \langle w | \cdot |v \rangle.$$

Kényelmesen tudunk operátorokat is definiálni az új jelölés segítségével. Például maradva a $\dim(\mathcal{H}) = 2$ esetnél:

$$|0\rangle \langle 0| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \cdot [1 \quad 0] = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}; |0\rangle \langle 1| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \cdot [0 \quad 1] = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \dots$$

Így aztán tetszőleges M operátor kifejezhető az $|i\rangle \langle j|$ mátrixelemek segítségével:

$$M := \begin{bmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{bmatrix} = m_{00} |0\rangle \langle 0| + m_{01} |0\rangle \langle 1| + m_{10} |1\rangle \langle 0| + m_{11} |1\rangle \langle 1|.$$

Hasonlóan megy a dolog általános vektorokra is: vegyük most a $|v\rangle \langle w|$ szorzatot, ami ugyebár egy operátor (diád-mátrix). Hogyan hat ez az operátor a $|z\rangle$ vektoron? A választ gondolkodás nélkül megadja a Dirac-féle jelölésrendszer:

$$(|v\rangle \langle w|) |z\rangle = |v\rangle \langle w | z \rangle = |v\rangle \langle w | z \rangle = \langle w | z \rangle |v\rangle$$

Fontos speciális eset amikor $\langle v | v \rangle = 1$, azaz $|v\rangle$ normált ($\|\mathbf{v}\| = 1$). Ilyenkor $|v\rangle \langle v| = \prod_v$, a $|v\rangle$ -re való merőleges vetítés operátora. A Dirac-féle jelölés

segítségével könnyű látni, hogy ez valóban egy vetítő operátor, avagy projektor:

$$\prod_v \prod_v = |v\rangle \langle v| |v\rangle \langle v| = |v\rangle \underbrace{\langle v|v\rangle}_{=1} \langle v| = |v\rangle \langle v| = \prod_v.$$

Megjegyzés: A tenzorszorzat jelét a Dirac-féle bra-ket jelölésekből el szokás hagyni. Vagyis $\mathbf{v} \otimes \mathbf{w}$ ket vektoros jelölésére $|v\rangle \otimes |w\rangle$ helyett csak egyszerűen $|v\rangle |w\rangle$ fogunk írni legtöbbször. A számítási bázisvektorok jelölésekor $|i\rangle |j\rangle$ helyett pedig sokszor még egyszerűbben csak $|ij\rangle$ -t fogunk írni.

1.5. A kvantummechanika posztulátumai

A mi esetünkben a vizsgált rendszereknek mindig véges sok szabadsági foka lesz, vagyis mi csak a véges dimenziós esettel fogunk foglalkozni.

(I) **Fizikai állapotok:** Egy izolált fizikai rendszer állapotait mindig leírhatjuk egy Hilbert-tér egységvektoraival. Két állapot akkor és csak akkor különböztethető meg teljes bizonyossággal, ha a megfelelő vektorok merőlegesek egymásra.

Qubitek: A két szabadsági fokú kvantumrendszereket qubiteknek fogjuk hívni, és a hozzá tartozó Hilbert-tér egy kitüntetett ONB-át számítási bázisnak fogjuk hívni elemeit pedig $\{|0\rangle, |1\rangle\}$ -el fogjuk jelölni.

(II) **Összetett rendszerek:** Ha két kvantumrendszer egyikét a \mathcal{H}_1 míg másikat a \mathcal{H}_2 Hilbert-tér írja le, akkor a két rendszer együttese által alkotott összetett rendszer lehetséges állapotait a $\mathcal{H}_1 \otimes \mathcal{H}_2$ tenzorszorzat egységvektorai írják le.

(III) **Időfejlődés:** A fizikai rendszer állapotainak véges idő alatt bekövetkező változását a Hilbert-tér valamely unitér operátora írja le.

(IV) **Rendszer mérése:** A rendszert valamilyen ONB-ban tudjuk megmérni. Legyen például $B = \{|e_1\rangle, \dots, |e_n\rangle\}$. Ekkor a $|\psi\rangle = \sum_{i=1}^n a_i |e_i\rangle$ állapotot a B ONB-ban mérve a mérés lehetséges eredményei: $1, \dots, n$. Annak a valószínűségét, hogy a mérési eredmény k lesz a Born szabály mondja meg:

$$P(\text{eredmény} = k) = |\langle e_k | \psi \rangle|^2 = |a_k|^2.$$

Ha a mérési eredmény k , akkor a rendszer a $|\psi\rangle$ állapotból „beugrik” az $|e_k\rangle$ állapota, vagyis a rendszer állapota végérvényesen megváltozik!

Részrendszer mérése (kiterjesztett Born szabály): Tegyük fel, hogy két rendszer együttes állapotát csak az egyik részrendszerben mérem meg. Ekkor a mérési valószínűségeket, és a mérés utáni állapotokat az úgynevezett részleges belső szorzat adja meg. Tegyük fel, hogy a másik részrendszerben $\{|f_1\rangle, |f_2\rangle, \dots, |f_m\rangle\}$ ONB. Legyen az összetett rendszerünk állapota $|\varphi\rangle = \sum_{i,j}^{n,m} \alpha_{i,j} \cdot |e_i\rangle |f_j\rangle$. Ekkor a mérési valószínűség és az új állapot:

$$P(\text{eredmény} = k) = \|(\langle e_k | \otimes I) |\varphi\rangle\|^2 = \sum_{j=1}^m |\alpha_{kj}|^2;$$

$$\text{mérés utáni állapot: } |e_k\rangle \frac{\sum_{j=1}^m \alpha_{kj} \cdot |f_j\rangle}{\sqrt{\sum_{j=1}^m |\alpha_{kj}|^2}}.$$

1.6. Példa: kvantumteleportáció

Tegyük fel, hogy adott a térben egymástól távol két jó barát Alice és Béla, akik barátságuk jeléül korábban létrehoztak egy összefonódott EPR párt és magukkal vitték egy-egy qubitjét:

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

Tegyük fel, hogy Alice-nak van egy másik qubitje valamilyen $|\psi\rangle$ állapotban, és ezt a qubit állapotot szeretné eljuttatni Bélának. Hogyan küldheti el? Lehet, hogy még az állapot $|\psi\rangle$ leírását sem ismeri, és a kvantummérési elmélete szerint képtelen többet megtudni róla, mint egy kis mennyiségű információt, mielőtt teljesen megsemmisítené! Elhelyezheti a qubit állapotot megtestesítő (fizikai rendszert) egy "dobozba", és fizikailag átviheti Bélához. De van-e más mód? Mi van akkor, ha az A és B közötti térrész ellenséges és veszélyes hely? A kvantum teleportáció egy alternatív módszert kínál az állapot átvitelére, amely kihasználja az $|EPR\rangle$ pár állapotban lévő összefonódást.

Az együttes kvantumállapot ekkor $|\psi\rangle |EPR\rangle$, ahol Alice az első két kvantumbithez fér hozzá, Béla pedig a harmadikhoz.

A kvantumteleportáció protokollja a következő négy lépésből áll:

- (i) Alice alkalmazza a CNOT (kontrollált-NOT) műveletet a két qubitjére.

- (ii) Alice alkalmazza a H (Hadamard) kaput az első qubitjére.
- (iii) Alice megméri a két qubitjét (a számítási bázisban) és a kapott 2 bites (xy) karakterláncot elküldi Bélának (azaz 2 bit klasszikus információt küld).
- (iv) Az xy fogadásakor Béla alkalmazza a $Z^x X^y$ unitér műveletet (ami az $X^y Z^x$ inverze) a saját qubitjére, amely ezután garantáltan a $|\psi\rangle$ állapotban lesz.

A fenti protokoll helyességét az alábbi számítás mutatja:

$$\begin{aligned}
|\psi\rangle |EPR\rangle &= (\alpha |0\rangle + \beta |1\rangle) \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\
&= \frac{\alpha}{\sqrt{2}} |000\rangle + \frac{\alpha}{\sqrt{2}} |011\rangle + \frac{\beta}{\sqrt{2}} |100\rangle + \frac{\beta}{\sqrt{2}} |111\rangle \\
&\xrightarrow{CNOT} \frac{\alpha}{\sqrt{2}} |000\rangle + \frac{\alpha}{\sqrt{2}} |011\rangle + \frac{\beta}{\sqrt{2}} |110\rangle + \frac{\beta}{\sqrt{2}} |101\rangle \\
&\xrightarrow{H} \frac{1}{2} |00\rangle (\alpha |0\rangle + \beta |1\rangle) \\
&\quad + \frac{1}{2} |01\rangle (\alpha |1\rangle + \beta |0\rangle) \\
&\quad + \frac{1}{2} |10\rangle (\alpha |0\rangle - \beta |1\rangle) \\
&\quad + \frac{1}{2} |11\rangle (\alpha |1\rangle - \beta |0\rangle). \\
&\qquad\qquad\qquad \underbrace{\hspace{2cm}}_{\text{Alice}} \quad \underbrace{\hspace{2cm}}_{\text{Béla}}
\end{aligned}$$

Hivatkozások

- [1] Michael A. Nielsen, Isaac L. Chuang: Quantum Computation and Quantum Information, Cambridge University Press. (2000);
- [2] Richard Jozsa: Quantum Computation lecture notes, Cambridge;
- [3] Scott Aaronson: Complexity Zoo;