

## 1. fejezet

# Elméleti Bevezető

### 1.1. Elméleti alapok

#### 1.1.1. Posztulátumok: [1]

1.állapotterés leírás: Egy zárt fizikai rendszer éppen aktuális állapota leírható egy  $\mathbf{V}$  Hilbert tér-beli egység-hosszú, komplex együtthatós állapotvektorral. Hilbert tér például egy komplex lineáris vektortér, amire értelmezve van a belső szorzat(skalárszorzat). Vegyünk példának egy két dimenziós Hilbert teret, ami egy egyszerű zárt fizikai rendszer jelképez. A rendszer állapotát le lehet írni egy két dimenziós vektorral, ahol:

$$v = \begin{bmatrix} a \\ b \end{bmatrix} = a\mathbf{0} + b\mathbf{1}, \text{ ahol } \mathbf{0} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \mathbf{1} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, a, b \in \mathbb{C}$$

Itt  $\mathbf{0}$  és  $\mathbf{1}$  az orthonormális(ortgonális és egység-hosszú) bázisvektorok. Mivel az állapotvektor egység-hosszú, ezért ki kell még kötni, hogy  $|a|^2 + |b|^2 = 1$ . Az együtthatókra szokás még valószínűségi amplitúdóként is hivatkozni(a Schrödinger hullámfüggvényben amplitúdóként jelennek meg).

2.Rendszerek időbeli fejlődése:Zárt fizikai rendszer időbeli fejlődése leírható csak változás kezdő- és végpontjától függő unitér transzformációval. Az előbbi jelölésrendszer segítségével leírva:

$$v'(t_2) = U(t_1, t_2)v(t_2), v' \in V$$

$U$  unitér operátor lineáris algebrai reprezentációja egy  $\mathbf{U}$  kvadratikus mátrix, melynek  $U_{ij}$  elemei a bemeneti  $\mathbf{j}$  orthonormális bázisvektor  $\mathbf{i}$  vektorral való kapcsolatát jelképező valószínűségi amplitúdókat jelölik.

3.Mérés: Méréseket leírhatunk  $M_m$  mérési operátorokkal, ahol  $m$  a lehetséges mérési eredményeket jelöli.  $m$  mérésének a valószínűsége, ha a rendszer  $\mathbf{v}$  állapotban van:

$$P(m|\mathbf{v}) = \mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v}$$

A rendszer állapota mérés után:

$$\mathbf{v}' = \frac{M_m \mathbf{v}}{\sqrt{\mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v}}}$$

Mivel a kimenetek összesített valószínűsége 1-el egyenlő.(a lehetséges kimenetek lefedik a teljes eseményteret):

$$\sum_m P(m|\mathbf{v}) = \sum_m \mathbf{v}^\dagger M_m^\dagger M_m \mathbf{v} \equiv 1$$

ami alapján:

$$\sum_m M_m^\dagger M_m \equiv I$$

A mérések nem visszafordíthatóak és viszonylag durvának tekinthetők abból a szempontból, hogy befolyásolják a mért rendszer állapotát a fentebb már leírt módon. Ugyanakkor velük teremthetjük meg a kapcsolatot a klasszikus és a kvantum világ között, mivel ők azok az eszközök, amikkel megfigyelhetjük mégiscsak mi történik a kvantum világban.

4.Összetett rendszerek: Egy  $W$  összetett fizikai rendszer állapota leírható az őt összetevő rendszerek tenzorszorzataként:  $W = V \otimes Y$ . Továbbá ha  $\mathbf{v} \in V$  és  $\mathbf{y} \in Y$  akkor a belőlük alkotott állapot:  $\mathbf{w} = \mathbf{v} \otimes \mathbf{y}$ . A kvantummechanikában a legkisebb információt hordozó elem a bit, amit kvantumbitnek, vagy röviden qubitnek szokás hívni. Egy qubit szokványos leírása:

$$|\psi\rangle = a|0\rangle + b|1\rangle = a \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$$

A klasszikus számítástechnikához hasonlóan  $n$  qubit felhasználásával építhetünk  $n$  bites kvantumregisztereket. Vizsgáljunk például egy két qubitből alkotott kvantumregisztert. Ekkor a teljes két qubites rendszer állapota:

$$|\psi\rangle \equiv |\psi_1\rangle |\psi_2\rangle \equiv |\psi_1, \psi_2\rangle \equiv |\psi_1 \psi_2\rangle$$

Ami például hogyha:

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

akkor:

$$|\psi\rangle = \frac{|0\rangle\otimes|0\rangle+|0\rangle\otimes|1\rangle+|1\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle}{2} = \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2}$$

látszik, hogy az előbbi rendszer a 00,01,10,11 állapotok(ők mellesleg ortogonálisak egymásra,itt az állapottér bázisának tekinthetők) súlyozott(most itt mindegyik 1/2 -el de ez lehet bármilyen más komplex szám is, sőt akár 0 is.) összege, ezeket mind tartalmazza és jól látszik, hogy felbontható  $|\psi_1\rangle$  és  $|\psi_2\rangle$  tenzorszorzatára. Az ilyen állapotokat hívjuk szorzat állapotoknak.

Most vizsgáljuk a következő állapotot:

$$|\psi\rangle = a|00\rangle + b|11\rangle$$

Ezt nem tudjuk felbontani két qubit tenzorszorzatára. Az ilyen állapotokat hívjuk összefonódott állapotoknak. Vegyük észre ennek az állapotnak egy érdekes tulajdonságát. Ha megmérjük az egyik bitjét, akkor akkor valamilyen valószínűséggel 0-át vagy 1-et kapunk.

Viszont ha ezután megmérjük a másik bitet is, ha az első mérésünk eredménye 0 volt, akkor itt már csak 0 mérhetünk és ehhez hasonlóan 1-es eredmény esetén pedig csak 1-et. Továbbá kísérletileg bizonyított, hogy ez a jelenség akkor is fenn marad, ha a rendszer két qubitjét helyileg egymástól eltávolítjuk. Néhány nevezetes összefonódott állapot, amelyeket Bell-állapotoknak szokás nevezni:

$$\begin{aligned} |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|0_A 0_B\rangle - |1_A 1_A\rangle) \\ |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_A\rangle) \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|0_A 1_B\rangle - |1_A 0_A\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|0_A 1_B\rangle + |1_A 0_A\rangle) \end{aligned}$$

Figyeljük meg, hogy ezek az állapotok egymásra merőlegesek, az állapotérnek bázisai-ként szolgálhatnak. Ennek segítségével definiálhatjuk az ún. Bell mérést ami egy 2 qubites rendszer projektív mérése ezekben a bázisokban. Megjegyzendő még, hogy a mérés után a mérési posztulátumnak megfelelően a két qubit a négy Bell állapot egyikébe kerül. Ezeken felül, bár a továbbiakhoz nem feltétlen szükséges, viszont a hivatkozások olvasásához igen, ismerjünk meg a rendszerek egy másik lehetséges leírási módját a teljesség igénye nélkül, a sűrűségmátrixos leírást[2]. Ebben az esetben a rendszert a lehetséges állapotainak valószínűségeinek összegével jellemezzük:

$$p = \sum_i p_i |\phi\rangle \langle \phi_i|$$

ahol  $|\phi_i\rangle$  az  $i$ -edik rendszer állapot, melynek előfordulási valószínűsége  $p_i$  a sűrűségmátrixos leírás ilyen ún. tiszta állapotok valószínűségi elegyeként írja le a rendszert. Ezek alapján például a

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

rendszer sűrűségmátrixa a következőképpen számolható:

$$p = |\phi\rangle \langle \phi| = \begin{bmatrix} a \\ b \end{bmatrix} \begin{bmatrix} a^* & b^* \end{bmatrix} = \begin{bmatrix} aa^* & ab^* \\ a^* b & bb^* \end{bmatrix} = \begin{bmatrix} |a|^2 & ab^* \\ a^* b & |b|^2 \end{bmatrix}$$

Ezen felül definiáljuk még a “trace” (magyarul nyom) operátort a következőképpen. Egy  $n$ -szer  $n$ -es  $A$  mátrixra:

$$Tr(A) = a_{11} + a_{22} + \dots + a_{nn} = \sum_{i=1}^n a_{ii}$$

Továbbá említésre méltó még, hogy  $Tr(A)$  egyenlő  $A$  sajátértékeinek összegével.

## 1.2. Összefonódás megosztás

(entanglement swapping)

### 1.2.1. A jelenség bemutatása

Az összefonódott állapotok érdekes tulajdonságait, természetesen igyekszünk kihasználni a kvantuminformatikában is, nem véletlen tehát, hogy magára az összefonódásra is mint egy

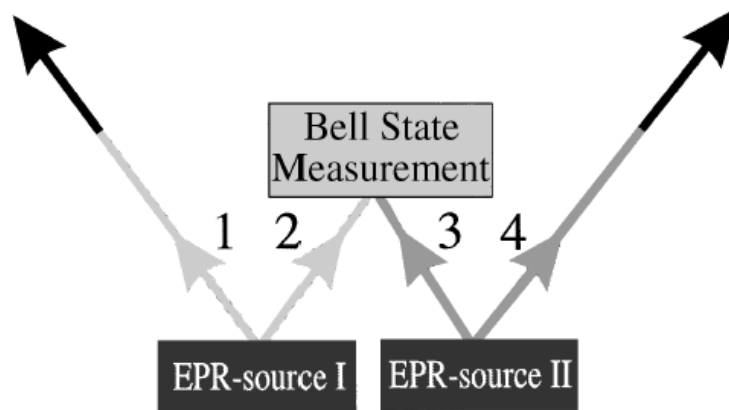
fontos erőforrásként tekinthetünk. Elég csak olyan, protokollokra gondolni, mint a szuper-sűrűségű kódolás, vagy a kvantumteleportáció, melyek mind összefonódott állapotok “használnak el” a működésük során. Nem csoda tehát, hogy egy adott helyen (vagy helyek között) való összefonódás létrehozásának képessége különös jelentőséggel bír. Ezzel kapcsolatban létezik szerencsére egy számunkra igen hasznos és viszonylag sokszor hasznosított jelenség, az összefonódás megosztás (entanglement swapping), mellyel egy összefonódott párok közötti érdekes interakciót írunk le. A már 1993-ban felvetett koncepció szerint [3] 2 összefonódott pár interakcióját vizsgáljuk egymással a következő módon. A példában tekintsünk kvantum információ hordozóira fotonokként hivatkozunk, de természetesen minden fotonhoz hasonló kvantum információ hordozására hasznos módszerre is az alábbiak szerinti a jelenség. Az összefonódott párajaink közül az egyik kezdetben legyen Alíznál, a másik pedig Bobnál. Legyen a rendszerünk kezdő állapota:

$$|\Psi_{kezd}^{-}\rangle = |\Psi^{-}\rangle_{AB} \otimes |\Psi^{-}\rangle_{CD}$$

ahol  $\Psi^{-}$  a már fentebb említett Bell állapot, AB fotonpár van Alíznál és CB fotonpár pedig Bobnál. A teljes állapot felírható:

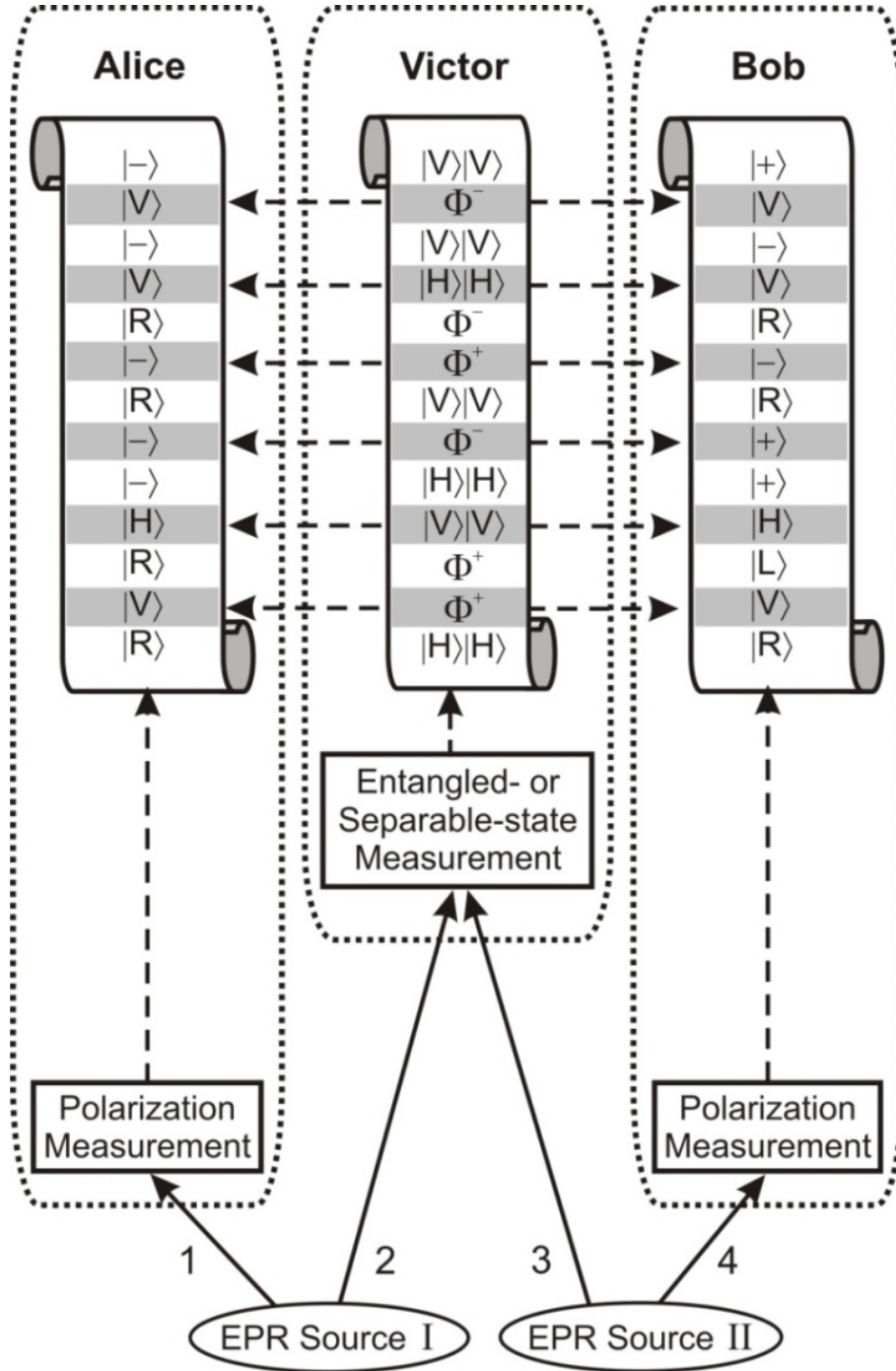
$$|\Psi_{kezd}^{-}\rangle = \frac{1}{2} \left( |\Psi^{+}\rangle_{AD} |\Psi^{+}\rangle_{BC} - |\Psi^{-}\rangle_{AD} |\Psi^{-}\rangle_{BC} - |\Phi^{+}\rangle_{AD} |\Phi^{+}\rangle_{BC} + |\Phi^{-}\rangle_{AD} |\Phi^{-}\rangle_{BC} \right)$$

Alíz elküldi A fotont Bobnak, Bob pedig C fotont Alíznek, tehát Alíznál lesz B és C, míg Bobnál A és D. Ha Alíz Bell mérést hajt végre BC fotonpárján és  $|\Psi^{-}\rangle_{BC}$  állapotban találja, akkor ha Bob is megméri a saját párját  $|\Psi^{-}\rangle_{AD}$  állapotot fog találni. Ha Alíz a mérése során a maradék három állapot közül találja valamelyiket, akkor Bob ennek megfelelő állapotokat fog találni az ő fotonpárja mérésénél is. Látszik, hogy a Bobnál előfordulható állapotok mind tiszta összefonódott állapotok, emiatt ha Alíz Bell mérést végez, tudhatjuk, hogy a Bobnál lévő fotonpár össze van fonódva Alíz mérési eredményének pontos ismerete nélkül. Érdekes megfigyelni, hogy a Bobnál lévő fotonok semmilyen közös múlttal nem rendelkeznek, mégis szert tettek egy közös tulajdonságra, összefonódott állapotba kerültek. A folyamatot lehet úgy is tekinteni, mintha a kvantumteleportációs protokoll [4] segítségével egy már kezdetben is összefonódott állapot egyik kvantumbitjét teleportáltuk volna, csak ebben az esetben nem a kiválasztott kvantumbit pontos átvitele a fontos, hanem csak az összefonódás, mint a két kvantumbites rendszerre jellemző állapot, továbbítása az. Alíz mérési eredményének pontos ismerete és a feltételes visszaállító transzformációk, továbbá az ehhez szükséges 2 klasszikus bitnyi információ itt nem is része a folyamatnak, mivel fentebb már megmutattuk, hogy az összefonódás léte (ami most minket érdekel) ezek nélkül is belátható.



**1.1. ábra.** *Összefonódás megosztás elvi rajza: Két összefonódott pár forrás (EPR source I és II) összefonódott fotonpárokat bocsájt ki (1-2 és 3-4). Mindegyik párból 1-1 fotonnal (2 és 3) végrehajtunk egy közös Bell mérést, aminek hatására a maradék két foton (1 és 4) is összefonódott állapotba kerül.*

Megjegyzendő még érdekességként, hogy Peres elméletének megfelelően[5] az összefonódás megosztás akkor is végbemehet, ha a (jelen esetben Alíznál) Bell mérést csak azután hajtjuk végre, hogy Bobnál már megmértük a másik két (jelen példánál A és D) állapotokat. Ezt igazolja például egy 2012-es kísérlet is[6].



**1.2. ábra.** Elvi kísérleti összeállítás *delayed choice* (késleltetett döntéses) összefonódás megosztás vizsgálatára. Az előzőekhez hasonlóan itt is két összefonódott pár forrás szolgáltatja a fotonpárokat, viszont a korábbiakkal ellentétben itt először az 1-es és 4-es foton állapotait nézzük meg, utána véletlenszerűen döntünk, hogy Bell mérést, vagy valamilyen szétválasztható állapot szerinti mérést végzünk el. Ezek után Alice és Bob rendezni és vizsgálni tudja a már meglévő mérési adatait Victor döntése ismeretében. Azt kapjuk, hogy Alice és Bob fotonjai vagy összefonódott vagy szétválasztható állapotokként viselkednek, Victor mérési eredményeinek megfelelően.

### 1.2.2. Összefonódás megosztások összefűzése

Tekintve, hogy milyen fontos szerepe van az összefonódásnak a kvantumkommunikáció területén, az összefonódás megosztás is egy fontos eljárása, építőeleme számos kvantumkommunikációs protokollnak. Ezek közül talán az egyik legfontosabb ilyen felhasználási terület a kvantum ismétlők. A kvantumkommunikációs csatornák a valóságban nem tekinthetők tökéletesnek, hasonlóan a klasszikus összeköttetésekhez, itt is számolni kell például csillapítással(hosszabb távon komoly probléma például a fotonok elnyelődése, detektálásuk nehézsége), a környezet hatásaival, mint például dekoherencia,zaj. Ebből adódóan nem élhetünk azzal a feltételezéssel, hogy hosszabb kapcsolatoknál az elküldött információnk a fogadó oldalra eredet formájában jut el. A kvantum csatorna átvitelére jellemző exponenciális csökkenés pedig gyakorlatilag ellehetetleníti a hosszabb távokon át történő információátvitelt. Erre lehetne az egyik megoldás, a klasszikus kommunikációhoz hasonlóan, ha megfelelően nem túl nagy távolságoként ismételnénk, eredeti állapotában mindig újra küldenénk tisztábban. A klasszikus kommunikációban ez könnyedén megoldható, azonban a kvantum másolási tétel (No Cloning Theory) miatt nem lehet azt a megoldást teljes egészében lemásolni.Vegyük észre viszont, hogy a kvantum teleportációs protokoll segítségével tetszőleges állapotot tudunk elvinni egyik helyről a másikra, feltéve hogy a cél és a forrás rendelkezik egy összefonódott párral amin már előzőleg megosztottak.A problémát így módon vissza tudjuk vezetni összefonódott párok szétoztására(mert klasszikus információt már tudunk nagy távolságokra is szállítani).Összefonódott párokat különben sem csak a teleportációs protokoll használ működése során, két hely közötti összefonódásra tekinthetünk egy általában is értékes erőforrásként. Itt lehet segítségünkre az összefonódás megosztás jelentősége.

Természetesen az összefonódott párokat akarunk szétoztani ugyanúgy fennállnak az előzőleg említett problémák a csatornával, viszont tekintsük a következő esetet[7]: Ha az összefonódott párok közül az egyiket előzőleg összefonódás megosztásával hozzuk létre, könnyen elképzelhető, egy szabadon bővíthet séma, ahol a nagy átviteli távolságot, többszöri összefonódás megosztásával több kisebb szakaszra lehet bontani. Vizsgáljuk meg azt az esetet amikor ezt a hosszabb távot két részre osztjuk fel. Ilyenkor kétszer kell összefonódást megosztani, három összefonódás forrásunk van, és két Bell mérést hajtunk végre a párjaink. Ha a párjaink kezdetben 1-2 3-4 és 5-6, akkor a Bell méréseket hajtunk végre 2-3-on és 4-5-ön. Ennek eredményeként 1 és 6 kerül összefonódott állapotba.

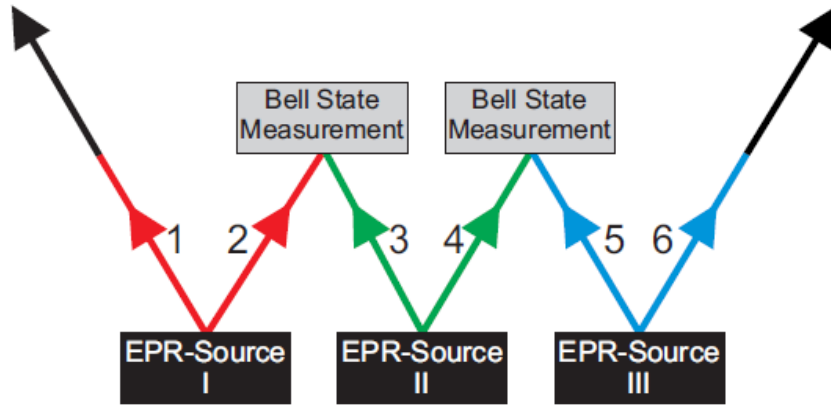
Felírva a rendszer állapotát:

$$|\Psi\rangle_{123456} = |\Psi^-\rangle_{12} \otimes |\Psi^-\rangle_{34} \otimes |\Psi^-\rangle_{56}$$

Ez átírható a következő alakra:

$$|\Psi\rangle_{123456} = \frac{1}{2} \left[ |\Psi^+\rangle_{14} |\Psi^+\rangle_{23} - |\Psi^-\rangle_{14} |\Psi^-\rangle_{23} - |\Phi^+\rangle_{14} |\Phi^+\rangle_{23} + |\Phi^-\rangle_{14} |\Phi^-\rangle_{23} \right] \otimes |\Psi^-\rangle_{56}$$

A korábbi két fotonpáros esethez hasonlóan itt is megfigyelhető, hogy az 1-es és 4-es fotonok a Bell mérés után összefonódott állapotban lesznek a mérés eredményétől függetlenül. Az eredmény csak arról szolgáltat információt, hogy melyik összefonódott állapotban vannak,,



**1.3. ábra.** Többlépcsős összefonódás megosztás elvi felépítése:  
A források által (EPR-Source I-II-III) kiadott kezdeti összefonódott párok: 1-2, 3-4, 5-6. 2 és 3-on majd 4 és 5-ön elvégezzük a Bell mérést. A két Bell mérés hatására végül 1 és 6 kerül összefonódott állapotba.

mivel az most is egyezik 2-3 közös mért állapotával. Ha feltesszük, hogy 2-3-as fotonpárnál  $|\Phi^-\rangle$  állapotot mértünk, a fennmaradó 4 fotonos rendszer a továbbiakban a következő formában írható fel:

$$|\Psi\rangle_{1456} = \frac{1}{2} \left[ |\Psi^+\rangle_{16} |\Phi^-\rangle_{45} + |\Psi^-\rangle_{16} |\Phi^+\rangle_{45} - |\Phi^+\rangle_{16} |\Psi^-\rangle_{45} - |\Phi^-\rangle_{16} |\Psi^+\rangle_{45} \right]$$

Hasonlóan az előzőekhez, elvégezzük a Bell mérést 4-5-ön, aminek hatására 1 és 6 összefonódott állapotba kerül. A mérési eredménynek megfelelően például, ha a Bell mérésnél  $|\Phi^-\rangle$  állapotot mérünk, akkor 1-6-nak az állapota:  $|\Psi^+\rangle$ .

A folyamat a fentiekből kiindulva általánosítható több tetszőleges számú összefonódott párral, tetszőleges számú Bell-méréssel, amivel az áthidalni kívánt távolság is tetszőleges számú szakaszra bontható fel.

A itt ábrázolt módszer is még idealizált csatornákkal dolgozik, magában nem oldja az előzőleg említett problémákat, mégis egy fontos építőeleme a későbbi ismétlődő létrehozására irányuló modelleknek.

### 1.2.3. A kvantum ismétlő

A kvantum ismétlő megvalósítására törekvő modellek túlnyomó része három fő építőelem-ből áll, és jellemzően e három építőelem más és más megvalósításában tér el egymástól. Egy jellemző általános megvalósítás az alábbi: A nagy távolságon jelentkező romlás elkerülése végett, ezt a távolságot felosztjuk több kisebbre, amik között a fentebb részletezett módon összefonódás megosztással teremtünk kapcsolatot. A felosztott kis távolságok között állomásokat alakítunk ki (ismétlőket), itt végezzük el az összefonódás megosztáshoz szükséges Bell méréseket. Továbbá minden szakaszhoz (minden összefonódás megosztási lépcsőhöz) létre kell hoznunk plusz összefonódott párokat amiket a folyamat során elhasználunk. Ehhez szükségünk van egy összefonódott pár forrásra, ami manapság már igen sokféle lehet. Ez



az egyik fő hasonlóság és egyben különbség is a legtöbb megvalósításban. A csatorna nem ideális átvitelével még mindig nem foglalkoztunk, pedig látható, hogy az továbbra is exponenciálisan fog romlani a csomópontok és a hossz növelésével. Ennek kiküszöbölésére használhatunk valamilyen összefonódás tisztító eljárást. Ezek jellemzően több nem teljesen tiszta összefonódott állapotból állítanak elő kevesebb, tisztább, jobban összefonódott állapotok. Tipikusan van egy tisztasági határérték a felhasznált “koszos” összefonódott állapotokra ami fölött alkalmazhatóak, emiatt akár ezek paraméterei támaszthatnak határokat a csatornaszakaszok hossza felé. Segítségükkel az átviteli sebesség kárára ugyan, de az átviteli folyamatok közé megfelelően beiktatva, kompenzálhatóak a csatornából származó veszteségek.

#### Példa egy tisztító protokollra

Egy lehetséges ilyen tisztító protokoll például a Bennett által javasolt [8] aminek folyamán helyben végzett transzformációk segítségével több nem teljesen “tiszt” összefonódott párból kevesebb jobban összefonódott állapot hozható létre. (Megemlítendő, hogy eredetileg elektronspinekre írták le, de természetesen megvalósítható más hordozók esetén is.) Legyen  $M$  egy “kevert” (nem tiszta) állapot amiből tisztább, jobban összefonódott állapotokat szeretnénk létrehozni. (Ilyen lehet például egy zajos csatornán megosztott  $|\Psi^-\rangle$  pár.) Ilyenkor  $M$  tisztaságát az eredeti teljesen összefonódott állapothoz képest

# Irodalomjegyzék

- [1] I. Sándor and F. Balázs, *Quantum Computing and Communications: an engineering approach*. John Wiley & Sons, 2005.
- [2] S. Imre and L. Gyongyosi, *Advanced quantum communications: an engineering approach*. John Wiley & Sons, 2012.
- [3] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, „" event-ready-detectors" bell experiment via entanglement swapping,” *Physical Review Letters*, vol. 71, no. 26, pp. 4287–4290, 1993.
- [4] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, „Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels,” *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.
- [5] A. Peres, „Delayed choice for entanglement swapping,” *Journal of Modern Optics*, vol. 47, no. 2-3, pp. 139–143, 2000.
- [6] X.-s. Ma, S. Zotter, J. Kofler, R. Ursin, T. Jennewein, Č. Brukner, and A. Zeilinger, „Experimental delayed-choice entanglement swapping,” *Nature Physics*, vol. 8, no. 6, pp. 479–484, 2012.
- [7] A. M. Goebel, C. Wagenknecht, Q. Zhang, Y.-A. Chen, K. Chen, J. Schmiedmayer, and J.-W. Pan, „Multistage entanglement swapping,” *Physical Review Letters*, vol. 101, no. 8, p. 080403, 2008.