



Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék

Összefonódás megosztásának vizsgálata kvantum alapú hálózatokban

SZAKDOLGOZAT

Készítette
Solymos Balázs

Konzulens
dr. Bacsárdi László

2017. december 1.

Tartalomjegyzék

Kivonat	4
Abstract	5
1. Bevezetés	6
1.1. Motiváció	6
2. Áttekintés	8
2.1. A kvantumkommunikáció napjainkig	8
2.2. Elméleti alapok	11
2.2.1. Posztulátumok:	11
2.3. Összefonódás megosztás	13
2.3.1. A jelenség bemutatása	13
2.3.2. Összefonódás megosztások összefűzése	16
2.3.3. A kvantum ismétlő	17
2.3.4. Néhány megvalósítás	20
2.4. Összefoglaló	23
3. Szimuláció	24
3.1. Választott környezet, eszközök	24
3.2. A szimuláció vezérlése	24
3.3. A kvantumos elemek reprezentációja	25
3.4. Az ismétlő protokoll elemei	25
3.5. Szimuláció működése	26
4. Szimulációs eredmények	30
4.1. Ismétlő protokoll és az egyszerű csatorna	30
4.2. Mérési sorrend	33
4.3. Összefonódott pár létrehozási sebesség hatása	35
4.4. A fogadott párok tisztasága	35
4.5. Tisztító stratégiák	35
4.6. Erőforrások elosztása	35
4.7. Egyéb megfontolandó paraméterek	35
4.7.1. Protokoll indulása	35

4.7.2. Kvantumos memóriák	35
Irodalomjegyzék	38
Függelék	39
F.1. Sűrűségmátrixos leírás	39
F.2. Összefonódás megosztás lépésről lépésre	39

HALLGATÓI NYILATKOZAT

Alulírott *Solymos Balázs*, szigorló hallgató kijelentem, hogy ezt a szakdolgozatot meg nem engedett segítség nélkül, saját magam készítettem, csak a megadott forrásokat (szakirodalom, eszközök stb.) használtam fel. Minden olyan részt, melyet szó szerint, vagy azonos értelemben, de átfogalmazva más forrásból átvettem, egyértelműen, a forrás megadásával megjelöltem.

Hozzájárulok, hogy a jelen munkám alapadatait (szerző(k), cím, angol és magyar nyelvű tartalmi kivonat, készítés éve, konzulens(ek) neve) a BME VIK nyilvánosan hozzáférhető elektronikus formában, a munka teljes szövegét pedig az egyetem belső hálózatán keresztül (vagy autentikált felhasználók számára) közzétegye. Kijelentem, hogy a benyújtott munka és annak elektronikus verziója megegyezik. Dékáni engedéllyel titkosított diplomatervek esetén a dolgozat szövege csak 3 év eltelte után válik hozzáférhetővé.

Budapest, 2017. december 1.

Solymos Balázs
hallgató

Kivonat

Dolgozatomban kvantum ismétlők, valamint a velük kapcsolatos megoldandó feladatok, kihívások vizsgálatával, szimulációjával foglalkozok.


A kvantum eszközök és eljárások számának növekedésével egyre nőnek a kvantum információs rendszerek felé támasztott igények is. A jelenkori megoldások teljesítményének komoly gátat szab a távolság növekedése. Erre kínálhatnak megoldást az „ún.” kvantum ismétlők.

Figyelembe véve, hogy a választott téma egy viszonylag fiatal kutatási területhez tartozik, dolgozatomat egy rövid áttekintéssel, valamint a későbbiek megértéséhez szükséges általános bevezetővel nyitom. Ennek felhasználásával az összefonódás megosztás és az ezt használó ismétlő protokoll pontosabb elméleti bemutatásával, valamint a felmerülő feladatok, nehézségek vizsgálatával folytatom. Ezután az általam készített szimuláció ismertetése következik. A dolgozatot az utolsó fejezetben már korábban említett problémák, feladatok szimulálásával, valamint a az így kapott eredmények értékelésével zárom.

Abstract

The purpose of my thesis is to describe the concept of the quantum repeater, further demonstrating its operation process and the associated challenges with a simulation.

With the growing number of quantum devices and protocols, comes the need for better and better quantum communication systems. For such systems today, the distance between the endpoints still poses a huge limiting factor. One possible solution for this can be the use of quantum repeaters.

Considering the nality of the field in question, I start my thesis with a brief historical overview, followed by a short introduction to the theoretical basics. I continue with describing the concept of entanglement swapping and exploring the possibility of a quantum repeater. Later I present the outline of my simulation. The thesis finishes with revisiting the challenges and problems related to the protocol by reviewing the simulation results.

1. fejezet

Bevezetés

1.1. Motiváció

A számítógépes rendszerek elterjedésének természetes következménye volt az őket összekötő hálózatok megjelenése és fejlődése. Napjainkban egyre kevesebb olyan eszközt találni, amely ne lenne alkalmas egy ilyen hálózathoz való csatlakozásra, rengetek alkalmazás és funkció van, ami valamilyen hálózatból kapott információra támaszkodik működése során. Tekintve a kvantummechanikára építő technológiai megoldások fejlődését, kísérleti kvantumszámítógépek jelenlegi állását [1][2], az ilyen kvantumos erőforrásokat használó eszközök összekötésére alkalmas hálózatokra is igény lesz. További motivációt jelent még, hogy ezen kvantumos információ továbbítására alkalmas hálózatok sok más felhasználási lehetőséget kínálnak a leendő kvantumszámítógépek összekapcsolásán túl. Ezek közül talán a legismertebb és legelterjedtebb a kvantum kulcsszétosztás, ahol kvantumos állapotokat használunk titkosított kulcsok bizonyítottan biztonságos megosztására [3]. Ezt a technológiát már a valós életben is használják, nem csak kutatási célokra [4]. Mindezek hatására egyre nő az egyre nagyobb ilyen hálózatokra való igény, egy jövőbeli kvantum internet [5] megvalósítására való törekvés. Ennek jelenleg a legnagyobb gátat a távolság jelenti. A klasszikus információval ellentétben a kvantumos információ nem másolható [6], emiatt a klasszikushoz hasonló erősítők sem alkalmazhatóak a kommunikációs csatorna által okozott veszteségek korrigálására. Ezt leküzdendő születtek meg különböző megvalósítások. Ezek egy csoportja az ún. kvantum ismétlők. Itt a fő cél a küldő és a fogadó állomás között összefonódott párok megosztása. Ezután az összefonódás különös tulajdonságait felhasználva a felek már különböző kvantumos műveletekre képesek. Tetszőleges kvantumbit küldése például a párok és egy klasszikus kommunikációs csatorna valamint a kvantum teleportációs protokoll [7] segítségével már megvalósítható. A kvantum ismétlő protokollok működése ugyan kvantumos alapokon nyugszik, a velük kapcsolatos megoldandó problémák jelentős része hasonlít a klasszikus hálózatokban felmerülőkhöz. Ezen protokollok hatékony megvalósításhoz is szükséges több elosztott erőforrás megfelelő együttműködése, itt is fontos szerepet kap például a hibakezelés, vagy éppen az adott lépések megfelelően összehangolt végrehajtási sorrendje. Dolgozatomban a protokoll ismertetésén túl ezen problémák vizsgálata a célom.

A továbbiakban a feladatkiírásnak megfelelően a dolgozatot egy gyors történeti áttekintés, majd egy hosszabb elméleti bevezető nyitja. Ezek után a készített szimuláció leírásával, majd végül a szimulációs eredmények és ezeken keresztül egyes technológiai megvalósítási lehetőségek áttekintésével zárul.

2. fejezet

Áttekintés

2.1. A kvantumkommunikáció napjainkig

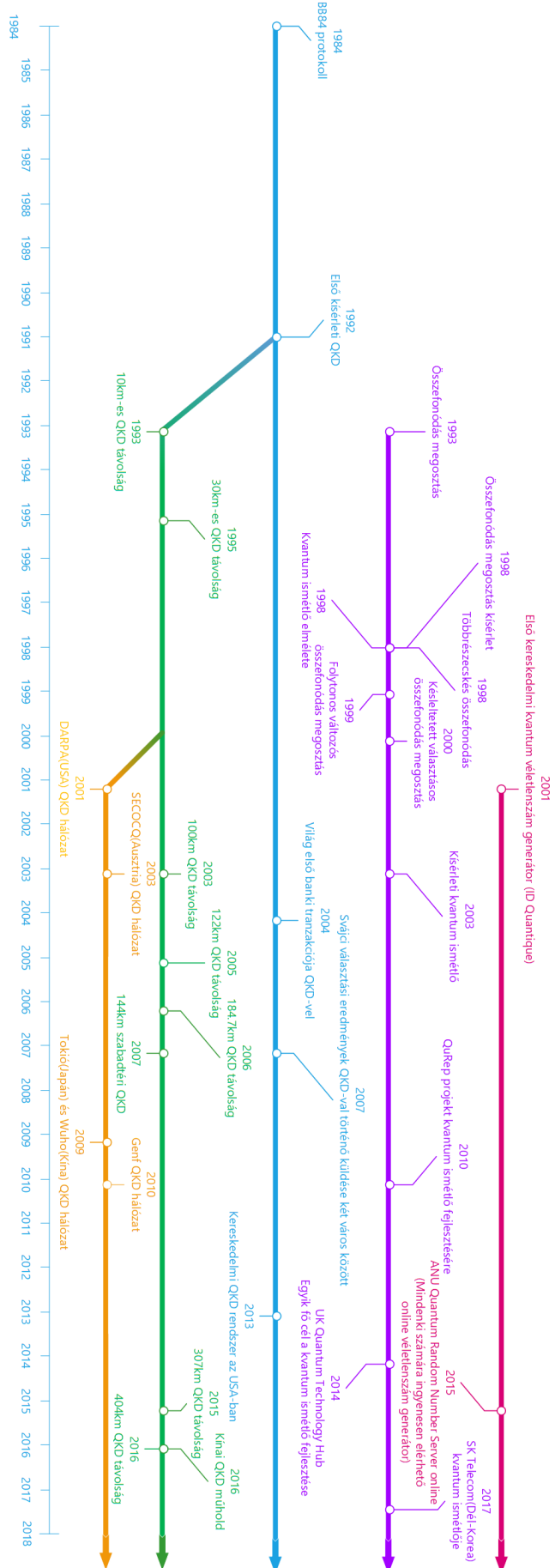
A kvantumkommunikációról valamint kvantuminformatikáról mint kutatási területről, valamikor a 90-es évek eleje-közepe óta beszélhetünk, habár az általa vizsgált és használt főbb jelenségekkel a fizika már az 1920-as években is foglalkozott. Elég csak azt tekinteni, hogy a kvantummechanika egyik mai meghatározó alapköve az 1926-ban publikált Schrödinger-egyenlet [8]. Az azóta eltelt időben a témához kapcsolható talán leghíresebb történet az 1980-as évekig az 1935-ös ún. EPR-paradoxon [9] valamint ennek kapcsán Bell 1964-es válasza [10]. Az EPR-paradoxonban Einsteinék összefonódott párok azon különleges tulajdonságát vizsgálták, hogy az egyik részecskén elvégzett véletlen eredményű mérés, hatással van az összefonódott pár másik tagjára is, távolságtól függetlenül. Mivel az azonnali információterjedés lehetősége a relativitáselméletben megismertekkel ellentézik, helyi rejtett, számunkra ismeretlen változók ötletével álltak elő ennek magyarázatára. Így ezekbe az ismeretlen változókba lehetséges lehetne előre eltárolni információt, ami alapján a számunkra véletlennek tűnő méréseknél a pár mégis korreláló eredményeket mutathat. Mivel a kvantummechanikában ilyen rejtett változók nincsenek, ezért szerintük a kvantummechanikának hiányosnak kellett lennie. Bell 1964-es írásában erre reflektál. Az általa levezetett egyenlőtlenség lehetővé tette ezen elméletek kísérleti tesztelését, melyek később a kvantummechanika jóslatait igazolták, a rejtett változós elképzeléssel szemben.

Az 1980-as években már kezdték vizsgálni ezen jelenségek későbbi lehetséges alkalmazásait, 1982-ben született a később meghatározó „No Cloning Theorem” [6], ami a tetszőleges kvantumbit másolhatatlanságát mondja ki, továbbá 1984-ben merült fel az első kvantumkriptográfia protokoll ötlete is [3]. Az 1990-es évektől kezdődően pedig kísérleti megvalósításokkal is találkozhatunk. További meghatározó eljárások születtek, mint például a kvantumteleportációs protokoll [7], majd ennek későbbi kísérleti megvalósítása [11], vagy akár az elméletben RSA titkosítás törésére is használható Shor-algoritmus [12]. Kvantumkommunikációs szempontból 1992-ben először hajtottak végre sikerrel kvantum kulcsszétosztást [13], valamint 1993-ban felmerült az összefonódás megosztás ötlete [14], amit 1998-ban kísérletileg is megvalósítottak [15]. Fontos előrelépés volt még az első összefonódás tisztító eljárások [16][17] megjelenése is, később ezen újítások segítségével vázolták fel a kvantum

ismétlő ötletét [18].

Az elkövetkezendő években egyre hatékonyabb eljárások, valamint az új technológiák segítségével pontosabb és megbízhatóbb kísérletek készültek. Ezt bizonyítja, hogy a 2000-es évek közepétől kezdtek elérhetővé válni (főleg kvantumkriptográfiában) a nagyközönség számára is használható kvantumos termékek. A folyamatos fejlődés megfigyelhető a kapcsolódó kutatások növekedésén is, idővel egyre több helyen alakultak a témába vágó kutatóközpontok, valamint kísérleti kvantumhálózatok. Egyre közeledünk az előzetes kutatások iparban való felhasználhatóságához. Ezt mutatják a közelmúltban a témában elért eredmények is. Ezek közül az egyik talán legjelentősebb a kínaiak által 2016-ben ~~fellőtt~~ műhold [19] kvantum kulcsszétosztás tesztelésére, melyről már kísérleti eredmények is származnak [20]. Megemlítendő még, hogy felismerve a területben rejlő lehetőségeket, a kvantumos kutatások támogatása bekerült az Európai Unió fejlesztési tervébe is, amely keretében 1 milliárd euró értékben támogatnak kvantumtechnológiai kutatásokat és fejlesztéseket [21].

A „kvantum internet” [5][22] megvalósításához azonban még mindig le kell küzdeni a hozzáférési pontok közti távolságból adódó problémákat. Habár a kapcsolódó technológiák fokozatosan javultak az évek során, olyan megbízható, hibatűrő rendszer ami ehhez kéne még nincs. A közeljövőben erre két kutatási terület is kínálhat megoldást: egyes kvantum hibajavító kódok [23] melyek alkalmazhatóak hálózatokra is [24], valamint a kvantum ismétlők[25][26][27][28]. A dolgozat a továbbiakban ezek közül a kvantum ismétlőkkel foglalkozik.



2.1. ábra. Kvantumkommunikáció fejlődése 1984-től

2.2. Elméleti alapok

A dolgozatban használt terminológia, valamint a vizsgált rendszerek megértéséhez szükséges a kvantuminformatikában használt alapvető jelölések, valamint a kvantum állapotok alapvető tulajdonságainak és a rajtuk végzett mérések, műveletek hatásainak ismerete. Ehhez nyújt egy gyors áttekintést a következő rész. Megjegyzendő, hogy jelen esetben a rendszereket csak diszkrét időben vizsgáljuk, mivel a későbbiekben vizsgált események leírásához ez elégséges, valamint hogy a bevezető megfelelő lineáris algebrai előismeretekre is épít.

2.2.1. Posztulátumok:

A posztulátumokat a [29] irodalom alapján mutatom be.

1. posztulátum - állapotterez leírás: Egy zárt fizikai rendszer éppen aktuális állapota leírható egy \mathbf{V} Hilbert-térbeli 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 rendszert jelképez. A rendszer állapotát le lehet írni egy \mathbf{v} 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 (ortogonális 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. posztulátum - rendszer időbeli fejlődése Zárt fizikai rendszer időbeli fejlődése leírható csak a 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. posztulátum - 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 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. posztulátum - 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 (amelyek mellelleg 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 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-át 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:

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

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.

Megjegyzés: A kapcsolódó irodalmak olvasásához szükséges lehet még a sűrűségmátrixos leírás ismerete (lsd. F. 1.), viszont a dolgozat olvasáshoz nem, ezért ennek ismertetésétől eltekintettem.

2.3. Összefonódás megosztás

2.3.1. 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 állapotokat "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 [14] 2 összefonódott pár interakcióját vizsgáljuk egymással a következő módon. A példában tekintsünk kvantum információ hordozóira fotonokként, de természetesen minden fotonhoz hasonló kvantum információ hordozására alkalmas 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:

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

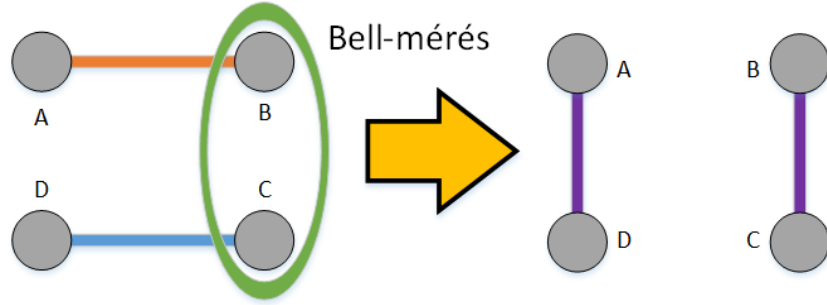
ahol Ψ^- a már fentebb említett Bell állapot, AB fotonpár van Alíznál és CB fotonpár pedig Bobnál. A teljes állapot felírható:

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

(Részletesebb magyarázatért lsd. F. 2.)

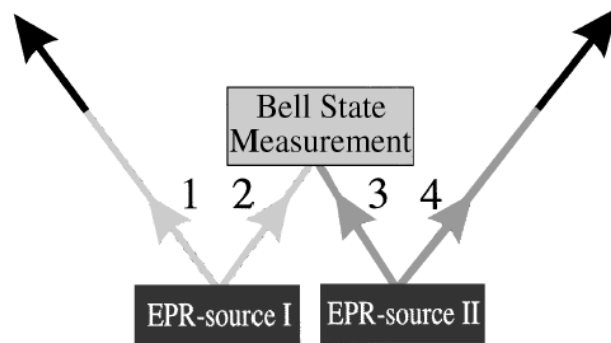
Alíz elküldi A fotont Bobnak, Bob pedig C fotont Alízna, tehát Alíznál lesz B és C, míg

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.



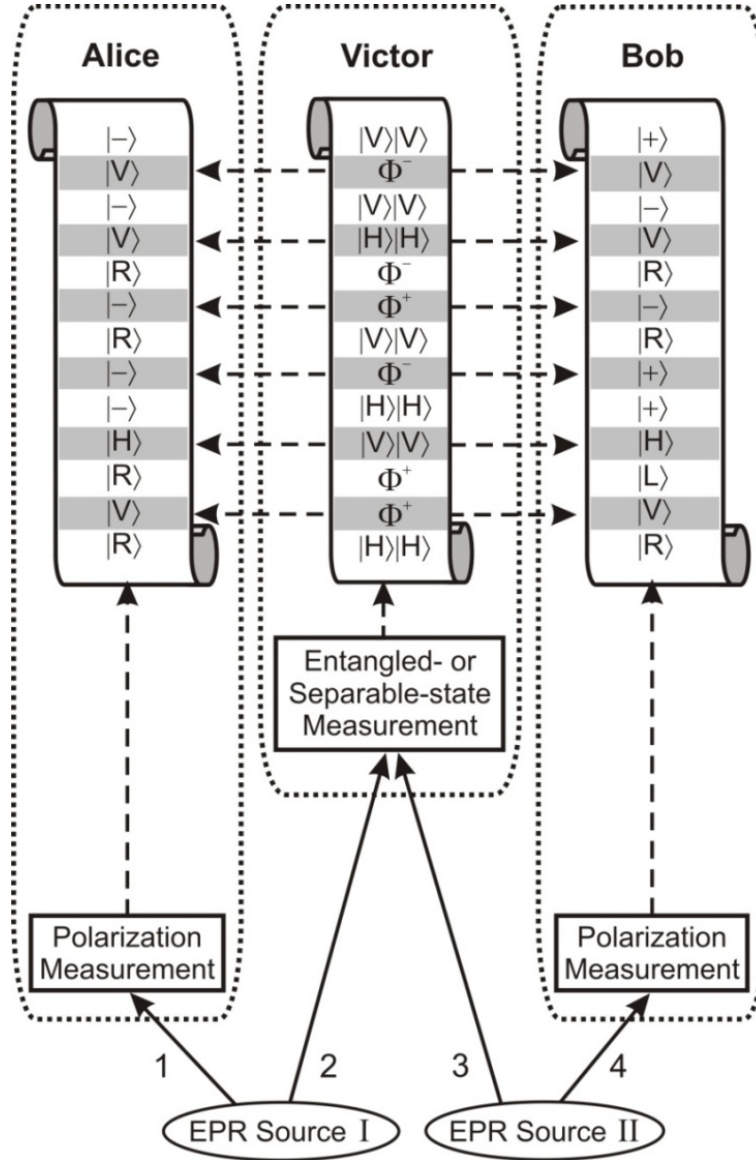
2.2. ábra. Összefonódás során a párok változása. Bal oldalt a Bell-mérés előtti állapot, jobb oldalt a mérés utáni. A mérést B és C biteken végezzük el.

A folyamatot lehet úgy is tekinteni, mintha a kvantumteleportációs protokoll [7] 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.



2.3. 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 [30] 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 [31].

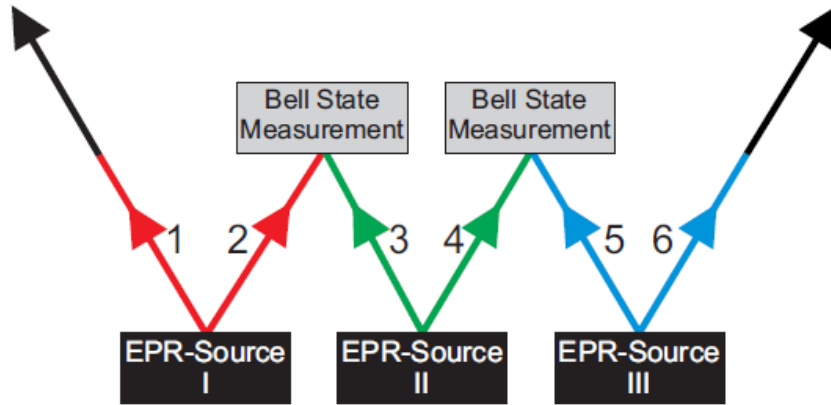


2.4. ábra. Elvi kísérleti összeállítás *delayed choice* (késleltetett döntéssel) összefonódás megosztás vizsgálatára. Az előzőekhez hasonlóan itt is két összefonódott pár forrás szolgáltatja a fotonpárokat, viszont a korábbiakkal ellentétben itt először az 1-es és 4-es foton állapotait nézzük meg, utána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

2.3.2. 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 (quantum repeaters). 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 információk a fogadó oldalra eredeti 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 távolságokként ismételnénk, eredeti állapotában mindig újra küldenénk tisztábban a küldendő bitet. 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 ha összefonódott párokat akarunk szétoztani ugyanúgy fennállnak az előzőleg említett problémák a csatornával, viszont tekintsük a következő esetet [32]: Ha az összefonódott párok közül az egyiket előzőleg összefonódás megosztásával hozzuk létre, könnyen elképzelhető, egy szabadon bővíthető 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 párajainkon. Ha a párajaink kezdetben 1-2 3-4 és 5-6, akkor Bell-méréseket hajtunk végre 2-3-on és 4-5-ön. Ennek eredményeként 1 és 6 kerül összefonódott állapotba.



2.5. 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.

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 az első Bell-mérés után összefonódott állapotba kerülnek a mérés eredményétől függetlenül. Az eredmény csak arról szolgáltat információt, hogy melyik összefonódott állapotban vannak, 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 párra, 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.

2.3.3. 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. 

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. Ezen felül 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 források maguk is sokféle karakterisztikával rendelkezhetnek. Adhat ki egy forrás kis sebességgel, nagy hibaszázalékkal közel teljesen tiszta állapotokat, vagy akár nagyobb sebességgel kisebb hibaszázalékkal több kevésbé tiszta állapotot is egyszerre.

A csatorna nem ideális átvitelével is foglalkozni kell, látható, hogy az továbbra is exponenciálisan fog romlani a csomópontok közötti hossz növelésével. Ennek kiküszöbölésére használhatunk valamilyen összefonódás tisztító eljárást.

Ezek jellemzően több nem teljesen tiszta összefonódott állapotból állítanak elő kevesebb, tisztább, jobban összefonódott állapotokat. Tipikusan van egy tisztasági határérték a felhasznált "koszos" összefonódott állapotokra ami fölött alkalmazhatóak, emiatt akár ezek paraméterei is támaszthatnak határokat a csatornaszakaszok hossza felé. Segítségükkel az átviteli sebesség kárára ugyan, de az átviteli folyamatok közé megfelelően beiktatva, kompenzálhatóak a csatornából származó veszteségek. Ennek szemléltetésére vizsgáljunk egy egyszerűbb ilyen eljárást.

Példa egy tisztító protokollra:

Egy lehetséges ilyen tisztító protokoll például a Bennett által javasolt[16] aminek folyamán helyben végzett transzformációk segítségével több nem teljesen "tiszta" 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 $F = \langle \Psi^- | M | \Psi^- \rangle$ segítségével fejezhetjük ki. Ezt akár értelmezhetjük azzal is ebben az esetben, hogy egy véletlenszerű bázisban végzett mérésnél mekkora valószínűséggel mérjük a vizsgált és a cél állapotot párhuzamosnak($P_{||}$). A protokoll lépései leegyszerűsítve:

Először végrehajtunk egy véletlenszerű bilaterális forgatást minden megosztott páron külön, aminek hatására következő forgásszimmetrikus állapothoz jutunk:

$$W_F = F \cdot \langle \Psi^- | + \frac{1-F}{3} \langle \Psi^+ | \Psi^+ \rangle + \frac{1-F}{3} \langle \Phi^+ | \Phi^+ \rangle + \frac{1-F}{3} \langle \Phi^- | \Phi^- \rangle$$

Az így kapott W_F Werner-állapot ugyanolyan F tisztaságú, mint a kiinduló M . A továbbiakban a következő műveletekre lesz szükségünk.:

-Unilaterális Pauli forgatások.: az összefonódott párban egy részecske π radiánnal való elforgatása az x,y, vagy z tengely körül. Ennek hatására a Bell állapotok egymásba mennek át:

$$\sigma_x : \Psi^\pm \leftrightarrow \Phi^\pm$$

$$\sigma_z : \Psi^\pm \leftrightarrow \Psi^\mp, \Phi^\pm \leftrightarrow \Phi^\mp$$

$$\sigma_y : \Psi^\pm \leftrightarrow \Phi^\mp$$

-Bilaterális $\pi/2$ forgatások B_x , B_y és B_z a pár mindkét tagjára megfelelően x,y és z szerint.
Hatása:

$$B_x : \Phi^+ \leftrightarrow \Psi^+$$

$$B_y : \Phi^- \leftrightarrow \Psi^+$$

$$B_y : \Phi^+ \leftrightarrow \Phi^-$$

-Kvantum XOR vagy CNOT bilaterálisan végrehajtva a mindkét megfigyelő által két megosztott pár megfelelő bitjein. A bilaterális XOR az hagyományos XOR-hoz hasonlóan működik. Alíz és Bob osztozzon 2 páron, Alíznál van 1 és 3, Bobnál 2 és 4. Ekkor egy 1, 2 forrású és 3,4 célú BXOR feltételesen fordítja a 3-as bitet, akkor és csak akkor, ha 1-es 1 (például elektronspinek esetében felfele áll, de ez hordozónként szabadon változhat.) és ehhez hasonlóan feltételesen fordítja a 4-es bitet, akkor és csak akkor, ha 2-es 1. A BXOR hatása Bell állapotokra:

Before		After (n.c. = no change)	
Source	Target	Source	Target
Φ^\pm	Φ^+	n.c.	n.c.
Ψ^\pm	Φ^+	n.c.	Ψ^+
Ψ^\pm	Ψ^+	n.c.	Φ^+
Φ^\pm	Ψ^+	n.c.	n.c.
Φ^\pm	Φ^-	Φ^\mp	n.c.
Ψ^\pm	Φ^-	Ψ^\mp	Ψ^-
Ψ^\pm	Ψ^-	Ψ^\mp	Φ^-
Φ^\pm	Ψ^-	Φ^\mp	n.c.

2.6. ábra. BXOR hatása Bell-állapotokra.

-Az előző unitér transzformációkon kívül alkalmazunk még egy mérést is, melyben Alíz és Bob a z tengely mentén mér (elektronok spinjeit), amivel megbízhatóan meg tudjuk különböztetni a Φ és Ψ állapotokat, viszont a „-” és „+” -t nem. Természetesen a mérés után a mért pár már nincs összefonódott állapotban. Ezen műveletek birtokában tekintsük az alábbi protokollt, melynek bemenetei valamilyen F tisztaságú Werner állapotok:

1. Egy unilaterális σ_y forgatást hajtunk végre mind a két páron, aminek hatására a többnyire Ψ^- Werner állapotból a többnyire Φ^+ Werner állapotba kerülnek.
2. Végrehajtunk egy BXOR-t a két nem tiszta Φ^+ állapoton és utána a célpárt megmérjük a z tengely mentén. Ha a mérési eredmények párhuzamosak, ami a Φ^+ állapotnak megfelelő, akkor a meg nem mért forráspárt megtartjuk, ellenkező esetben nem.

3. Végül, ha a forráspárt megtartottuk, egy többnyire Ψ^- állapotba visszaalakítjuk egy unilaterális σ_y forgatással, majd forgásszimmetrikussá tesszük egy véletlen bilaterális forgatással.

Ezen egyszerű protokoll ismétlésével lépésenként legalább $\frac{1}{4}$ -ed valószínűséggel növekvő F tisztaságot lehet elérni, amennyiben a felhasznált M párokra igaz, hogy $F_m > 1/2$. Továbbá a lépésenként így elért $F' > F$ kielégíti a következő egyenletet:

$$F' = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2}$$

A módszer ismételt elvégzésével a tiszta állapotot tetszőlegesen megközelítő állapot állítható elő, viszont a hatékonyság (nem tiszta bemenet/tiszta kimenet) a teljesen tiszta kimenet közelítésével a 0-hoz tart. Ennek a javítására szerencsére vannak módszerek, egy ilyen lehetőség például, ha nem egy forrást párt BXOR-olunk egy célpárral, hanem többet. Ennek az ötletnek egy továbbfejlesztése, amikor tiszta Φ^+ állapotokat használunk a BXOR céljaként a több nem tiszta forráspárhoz. Ezután megmérjük a célt. A fenti tábla alapján minden Ψ^+ vagy Ψ^- forráspár váltja a célt Φ^+ és Ψ^+ között, a forrásra való hatás nélkül. Ennek alapján a BXOR-t egyfajta paritás tesztként használva meg tudjuk állapítani, hogy a mért halmazban páratlan vagy páros számú Ψ állapot van. Ezután további BXOR-ok elvégzésével a részhalmazokon, kiválasztható az összes Ψ állapot és Φ állapotra javítható, majd hasonló módszerrel meg lehet találni a Φ^- állapotokat is és javítani a kívánt Φ^+ -ra. Természetesen léteznek más tisztítóprotokollok is más tulajdonságokkal, viszont a továbbiakhoz nem szükséges ezen terület mélyebb ismerete.

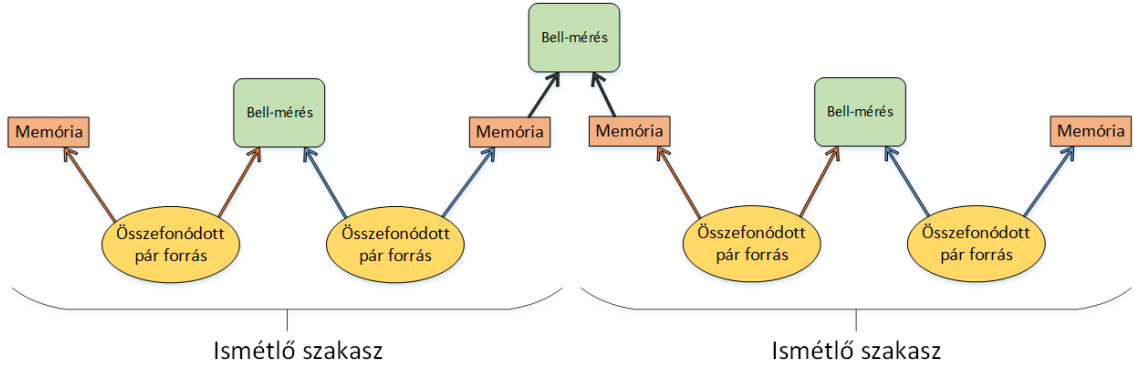
Az ismétlődő következő eleme maga a Bell-mérés aminek következtében maga az „összefonódás megosztás” nevű jelenség a párokon ténylegesen végbe megy. Megemlítendő, hogy amennyiben nem teljesen tiszta állapotokat mérünk ennek hatására a létrejövő új pár tisztasága is romlani fog, valamint magának a mérésnek is lehet egy hibaszázaléka [33], amiket a későbbi lépésekben ugyanúgy javítani kell.

Fontos elemek még az állomásokon található kvantum állapotok tárolására képes memóriaegységek. Mivel a végső cél az ismétlődő két végén található memóriában tárolt qubit közötti összefonódás létrehozása, természetes feltétel az állapothű tároláson túl, hogy ezek a memóriák képesek legyenek megtartani a qubit állapotát a protokoll végigfutási ideje alatt. Az alkalmazható hibajavítási stratégiáknak ez is egyfajta gátat szab mint az összes rendszerben tölthető idő felső határa.

2.3.4. Néhány megvalósítás

A továbbiakban vizsgáljunk néhány mostani megvalósítást, ahol már láthatóak a technológia alkalmazásából származó előnyök valamint kihívások is.

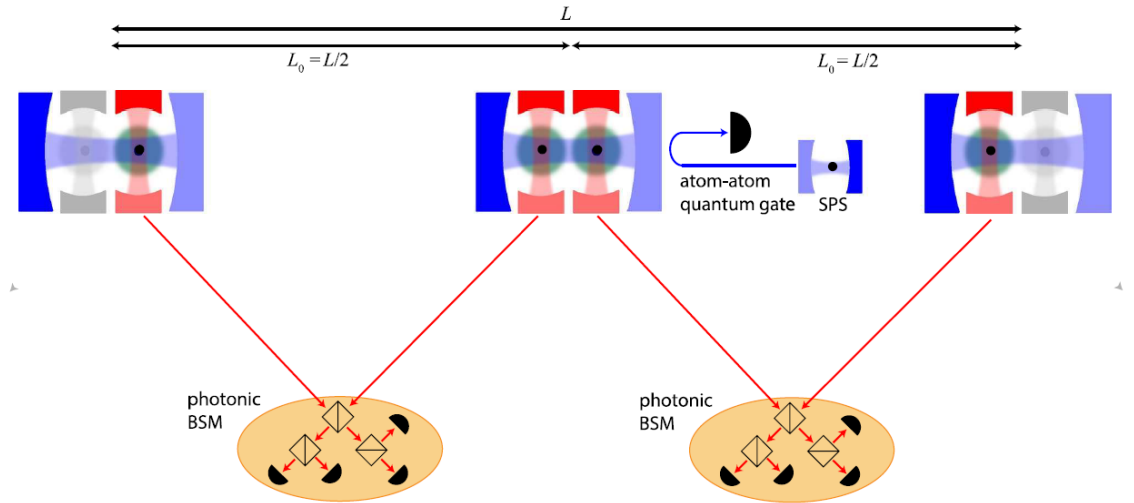
Egy 2016-os német tanulmányban[25] atom-foton összefonódott párokat használnak, melyeket optikai mikroüregekben található magányos atomok segítségével hoznak létre. Az összefonódás közvetlen az atomi kvantummemória és a foton között jön létre. További



2.7. ábra. Általános ismétlő rajza

A tisztító protokoll a képen nincs feltüntetve, tipikusan a Bell-mérések előtt alkalmazzák, habár ettől eltérő stratégiák is létezhetnek.

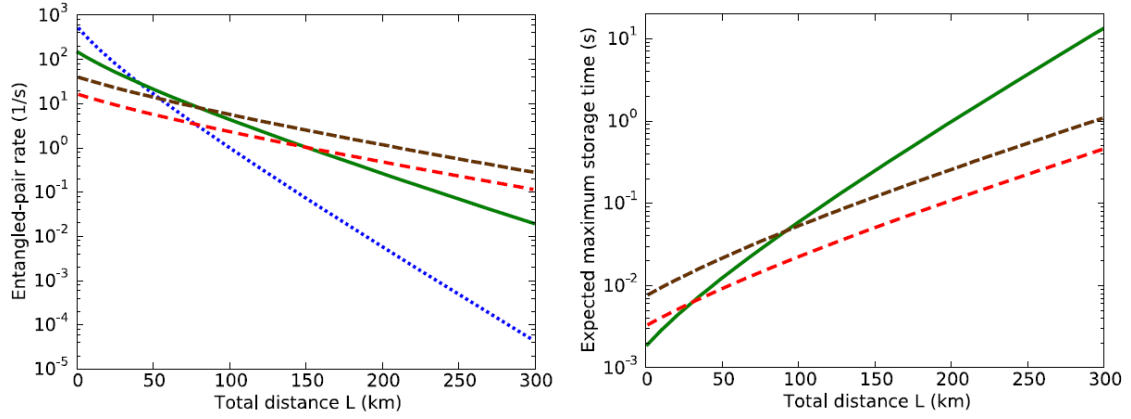
előny még, hogy ennek létrejöttét egy másik ún. “bejelentő” foton is jelzi és az összefonódást szállító foton olyan előnyös tulajdonságokkal rendelkezik (spektrum stb), hogy az egész elrendezés a szokványos telekommunikációs hullámhossztartományban használható. A további lépések az általános modellt követik, maga az összefonódás megosztás, fotonok közötti Bell-mérésekkel, és atom-atom kapuk alkalmazásával történik.



2.8. ábra. A 2016-os német tanulmány elvi rajza.

Egy ismétlő csomópont a “bejelentő” üregből(kék) és telekommunikációs hullámhosszú összefonó üregekből áll. Az atomokat (fekete pont) lézersugarakkal irányítjuk. Az $L/2$ távolságra lévő csomópontokat először összefonódott állapotba juttatjuk a fotonokon elvégzett ($L/4$ távolságnál) Bell-mérések segítségével. A csomópont párok között összefonódás megosztást a központi csomópontban elvégzett (atom-atom) művelettel valósítjuk meg.

A tanulmány szépen szemlélteti még a távolságból és a hibajavításból adódó problémák hatását.



2.9. ábra. A várható átviteli sebesség és tárolási idő alakulása az áthidalni kívánt távolság függvényében.

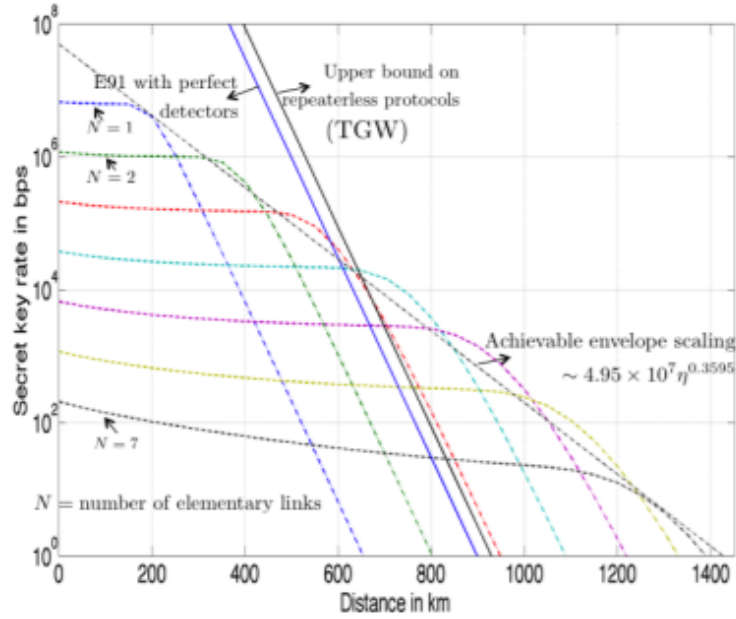
Kék pontozott vonal-> ismétlő nélküli eset; zöld folytonos vonal->2 szakasz esetén

piros szaggatott vonal-> 4 szakasz esetén, hibánál teljes újratekésztel

barna szaggatott vonal-> 4 szakasz hibánál a már összefonódott állapotok megtartásával

Látszik, hogy kis távolságoknál a közvetlen összeköttetés a legjobb egyszerűsége miatt, viszont 100km fölött már számottevően jobbak az ismétlős megoldások. A tárolási idő szempontjából látszik, hogy nagy távolságoknál a több részre felosztott rendszerek teljesítenek jobban. (Továbbá az is, hogy a hiba teljes újratekésztel való javítása is meglehetősen csökkenti a szükséges tárolási időt.)

Egy másik 2016-os tanulmány [26] az ún. „parametric down conversion” jelenséget és két foton interferenciát hasznosító összefonódott pár forrásokat használó jelen/közeli jövőbeli ismétlők lehetséges korlátjait vizsgálta, különös tekintettel az egyszerű megvalósíthatóságra a mai technológiákkal. Az ő szimulációjukból is látszik az ismétlők előnye nagyobb távolságok esetén:



2.10. ábra. A különböző számú kapcsolatokból álló ismétlőrendszerek átvitele és összehasonlításuk más ismétlő nélküli protokollok határaival (TGW vonal ezek felső határa).

Különböző ismétlő protokollok akár ionokkal való megvalósítási lehetőségét is vizsgálták [27] ugyancsak 2016-ban. Az általuk használt kísérleti összeállításban $^{40}\text{Ca}^+$ ionok segítségével már $F > 0.95$ esetén 100 állapot/s sebességet is elértek bizonyos protokollok esetén, azonban megfelelő változtatásokkal a több mint 750 állapot/s sebességet is elérhetőnek találták, az ionos megvalósítások esetében.

Egy negyedik, kínai tanulmány [28] pedig a kvantum pontok és optikai üregek használatával való megvalósítással foglalkozik. Ennek egyik érdekessége, hogy itt úgynevezett time-bin összefonódást hoznak létre, aminek folyamán a fotonoknak az időbeli szabadságfokát használják fel információtárolásra. A tanulmányban továbbá megmutatják, egy lehetséges N többfelhasználós kvantum ismétlő rendszer felépítését is.

2.4. Összefoglaló

Már az említett megvalósításokból is látszik, hogy a kísérleti kvantuminformációs megvalósítások hatékonysága, erőforrásigénye és megbízhatósága egyre inkább közelíti a gyakorlatban való eredményes használhatóságához szükséges feltételek teljesítését az információszétosztás területén is. Tekintve a terület gyors fejlődését, különösen, hogy a kvantum titkosítás és kulcsszétosztás már a jelenben is gyakorlati jelentőséggel bír, a kvantum ismétlők ipari megvalósítása nagy valószínűséggel már a közeljövőben is egy megoldandó mérnöki feladatot fog jelenteni. A fentebb szemléltetett tervezésnél megfontolandó nehézségek fényében döntöttem egy szimuláció elkészítése mellett, ahol a továbbiakban ezek hatását szemléltetem illetve vizsgálom.

3. fejezet

Szimuláció

A szimuláció elsődleges célja egy általános kvantum ismétlő protokoll működésének vizsgálata. Ennek megfelelően a különböző fizikai megvalósítások pontos szimulációjától ezek sokszínűsége miatt a továbbiakban eltekintettem, helyette egy általánosított modellen vizsgáltam az egyes paraméterek hatását. A modell elemei a bevezetőnek megfelelően ismétlő állomások és csatornák. Az állomások rendelkeznek kvantum memóriákkal, képesek mérések, és helyi műveletek elvégzésére a memóriájukban tárolt qubitjeiken, valamint egy speciális állomásfajtának tekinthetjük az összefonódott pár forrásokat is. A csatornák az állomásokat összekötő kommunikációs összeköttetések, amelyeken keresztül a qubitjeinket az állomásoknak szétküldjük. Továbbá feltételezzük, hogy az egyes állomások képesek egymás közt hagyományos kommunikációra is.

3.1. Választott környezet, eszközök

A szimuláció C++ nyelven íródott(C++11-et használ), valamint az Eigen [34] lineáris algebra könyvtárt használja. Az elkészítésnél cél volt sokféle szimulációs elrendezés támogatása, emiatt használata a legtöbb esetben egy C++ könyvtárhoz hasonló. A legegyszerűbb esetben egy előre megírt függvény egyszeri meghívásával akár egy teljes szimuláció is futtatható, viszont a rendelkezésre álló eszközökkel lehetőség van teljesen egyedi szimulációs elrendezés készítésére is. Az egyes elemek 4 fő csoportba sorolhatók, melynek megfelelően az egyes funkciók 4 header fájlba kerültek szétosztásra. Ezek: a kvantum elemek reprezentációit tartalmazó, az ismétlő protokoll elemeit tartalmazó, a szimuláció vezérléséért felelős, valamint az előre megírt teszteseteket tartalmazó fájlok. A forrásfájlok a <https://github.com/SOlymi/szakdoga> oldalon elérhetőek.

3.2. A szimuláció vezérlése

A szimuláció vezérlése egy végrehajtási lista alapján történik, melynek kezelését a `SimRoot` és `SimItem` osztályok végzik. A lista `SimItem` típusú elemekből áll. Ebben az osztályban található információk az egyes elemek egymáshoz képesti viszonyáról a sorban, valamint a végrehajtandó lépéseket is itt tárolódnak. Egy ilyen lépést egy itt tárolt függvény (`std::function`) jelképez ami végrehajtáskor meghívódik. Ilyen függvény lehet például egy

Bell-mérés végrehajtása, vagy egy qubit átküldése egy csatornán. Ezen felül tárolva van még a végrehajtás tervezett ideje is. A listát kezelő `SimRoot` osztály ennek alapján új elem felvételénél a megfelelő helyre tudja rakni a tagokat ezzel egy idő szerint rendezett struktúrát hozva létre. A végrehajtásnál így már mindig csak a soron következő elemmel kell foglalkozni. Az objektumba felelős még a sor megfelelő ürítéséért is törlésnél, valamint itt található a szimuláció aktuális órája is. E két osztály a `Simulation.h` fájlban része.

3.3. A kvantumos elemek reprezentációja

A szimuláció során elemi kvantumos egységnek nem a kvantum bitet, hanem mivel minden esetben egy vagy több párral kell dolgozni a kvantum bitpárt választottam. Ennek leírására `qrep.h` fájlban található `QPair` osztály szolgál. Párt választani alapelemnek abból a szempontból is nagy könnyebbség, hogy a két részecske közti lehetséges összefonódást a bitek együttes állapota már tartalmazza, ezért annak külön kezelésével nem kell foglalkozni. Az együttes állapot leírására ennek megfelelően egy 4 dimenziós komplex vektor szolgál (a 2 bit egy 4 dimenziós állapotteret feszít ki). Ide sorolható továbbá még az egy bites kvantumos memóriát reprezentáló `QMem` osztály. Az egy qubitre való hivatkozáshoz itt tárolva van a pár címe, aminek a tárolt qubit a része, valamint egy index aminek segítségével a összetett páros állapotból ki tudjuk nyerni a számunkra érdekes qubitet. Az objektum tárolni tudja még ezen kívül egy adott qubit beérkezési idejét is, amiből így később számítható a bit teljes memóriában töltött ideje. A két osztály az említetteken túl egyéb szimulációt segítő segédváltozókat tartalmaz még.

3.4. Az ismétlő protokoll elemei

Az ismétlő protokoll működéséhez szükséges elemeket az `elements.h` fájl tartalmazza. Itt ~~vannak meghatározva~~ a csomópontok, csatornák, valamint az általuk használt eszközök, eljárások. Ezek közül egyik másik erősen épít egymásra. Az itt található fontosabb dolgok ezt is figyelembe véve:

`Pair2Measure` osztály ami párokon elvégzendő mérések megvalósítására szolgál. Jelen esetben csak a Bell-mérés megvalósítására szolgál, viszont megfelelő paraméterekkel más mérések is elvégezhetők. Mérést tud végezni 2 páron. Ehhez mivel a párok közötti összefonódással számolni is számolni kell létrehozza az így kialakuló mind a két párra kibővített teret és a továbbiakban azon dolgozik. Magát a mérést a bevezetőben leírtak szerint el lehet végezni. Továbbá tartalmaz állítható kisegítő mátrixokat is, amivel például egyszerűbb bázisváltás is végezhető, megfelelő beállításukkal a mérési folyamat tovább egyszerűsíthető. A beépített Bell-mérés (`.bmeasure()`) ezeket használja, emiatt a beállításuk fontos, viszont ez egyszerűen megtehető egy másik beépített függvénnyel (`.SetBellMeasure()`).

`EPR` osztály, ami összefonódott párok előállításáért felel. Benne állítható a létrehozni kívánt pár (ez bármilyen lehet) állapota, amit itt is egy 4 dimenziós komplex vektor ír le, valamint a kiadott pár ehhez képesti tisztasága, amivel egy ismeretlen zaj hatását lehet imitálni. Beállítható még a pár generálások közt eltelt idő, ami később a szimulációban kerül felhasználásra.

Channel osztály az egyes csomópontokat összekötő kvantum kommunikációs csatornák leírására. Az egyes csatornákat a hosszukkal, valamint csillapításukkal, amit itt egy „csillapítási hosszal” jellemzünk. A csatorna által okozott zavar/veszteség egy bit egyszeri átküldésénél a legtöbb esetben átviteli valószínűségként nyilvánul meg. Ennek értéke az előző jellemzőkkel leírva:

$$p = e^{-\frac{L}{L_{cs}}}, \text{ ahol } L \text{ a teljes hossz } L_{cs} \text{ pedig a „csillapítási hossz”}.$$

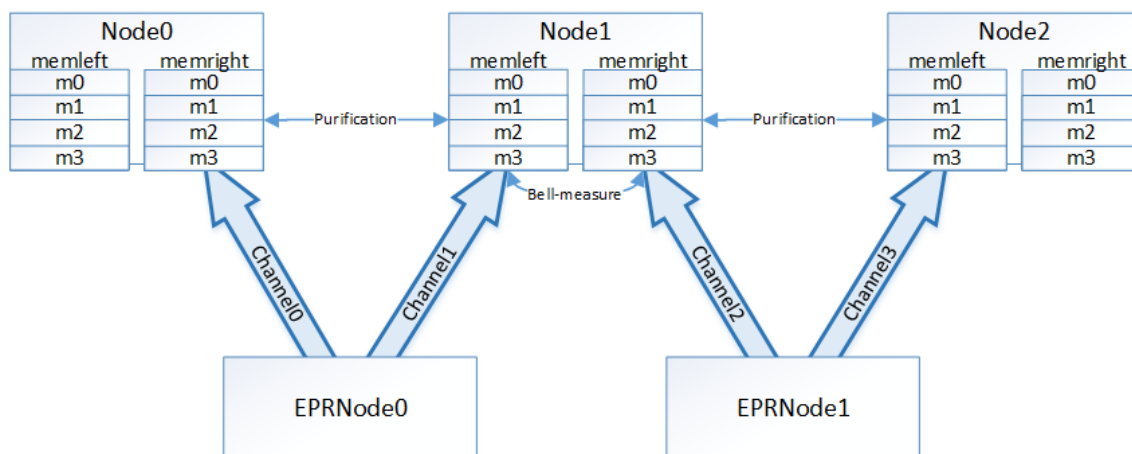
Ezekon felül az osztály tartalmaz még a szimulációt segítő egyéb változókat(pl.: melyik két csomópontot köti össze), valamint egy a szimulációs sorban végrehajtandó lépést is. A **SendThrough** függvény írja le azt, hogy mi történik a qubittel a csatornán való áthaladás során. A csatorna jellemzőinek megfelelően módosítja a qubitet tartalmazó pár állapotát, valamint lépteti tovább a szimulációt azáltal, hogy a végrehajtási sorba beütemezi a következő lépést.

Node osztály felelős a használt csomópontok leírásáért. ~~El vannak benne tárolva~~ a csomópont működéséhez szükséges információk: a csomópont helye a felépített kísérleti rendszerben(a többi csomóponthoz képest), a működése során felhasznált eszközök(Bell-mérés, pár létrehozás, pár tisztítás). Ezeken felül minden ilyen csomópont rendelkezik valamennyi memóriával is(**QMem** tömb) amiken keresztül működése során az egyes qubiteket manipulálni tudja. Az összefonódott párokat létrehozó egységeknél állítható plusz változó még az egyszerre létrehozandó párok száma, valamint a mérést végző egységek esetében a tisztító protokoll által elérendő tisztaság. Az osztályban ~~van még definiálva~~ a végrehajtási sorban fellelhető szimulációs lépések nagy része is.

3.5. Szimuláció működése

A szimuláció és az alkalmazott modell működésének bemutatásához tekintsük a következő egyszerű esetet. A vizsgált rendszerben két végpont között egy csomópont, valamint két összefonódott pár forrás segítségével szeretnénk összefonódott állapotokat megosztani. Így összesen 5 egységünk és 4 csatornánk van:3 hagyományos csomópont és 2 párt generáló, valamint az őket összekötő csatornák. A továbbiakban egy pár útját vizsgáljuk ahogy halad és változik a rendszerben. Ehhez kiindulásnak feltételezzük, hogy már vannak más párok is a rendszerben, viszont a vizsgált párunk számára is van még szabad memória.

A vizsgált párt az egyik párokat generáló csomópont hozza létre a **GenEPR** lépés segítségével, ami végrehajtása során a pár létrehozásán túl késleltetve ütemezi a következő generálást. Ezen felül ütemezi a hozzá tartozó két csatornán a qubitek átküldésére szolgáló, egyes összekötő csatornák által tárolt **SendThrough** lépést, a pár megfelelő indexeivel meghívva. Amennyiben a bit átjut a csatornán, a csatorna típusának és hosszának megfelelő késleltetéssel ütemezve lesz a következő lépés ami az egyes csatornák végpontjaihoz tartozó hagyományos csomópontokon végrehajtott **ReceiveFromCh**. Itt kizárólag azt vizsgáljuk, hogy az éppen beérkező qubit számára van-e hely az egység memóriájában. Amennyiben nincs, a párt megfelelően törli, ha van, akkor pedig berakja az üres memóriába, és ütemezi



3.1. ábra. Példa modell egy kisebb hálózatra

A vizsgált párt generálja EPRNode0. Ennek megfelelően a hozzá kapcsolódó lépések egy lehetséges sora:

1. EPRNode0->GenEPR : A párt létrehozza a forrás.
2. Channel0->SendThrough és Channel1->SendThrough: Csatornákon való átküldés
3. Node0->ReceiveFromCh és Node1->ReceiveFromCh: Pár qubitjeinek fogadása memóriába
4. Node0->ReceiveFromChSuccess és Node1->ReceiveFromChSuccess: Megbizonyosodik arról, hogy mindkét oldal fogadni tudta a pár bitjeit
5. Node0->Updateformeasure és Node1->Updateformeasure: Tartalmazó állomások frissítése. Mivel Node0 az egész rendszer egyik végpontja, ezért vele nem lesz több lépés, kívülről vizsgálható, hogy elkészült-e már benne a kívánt összefonódott pár.
- 6/a. Node1-> Bellmeasure: Bell mérés, ha a kétoldali memóriák állapota megfelelő
- 7/a. CorrectAfterMeasure: A pár állapotának javítása a mérési eredménynek megfelelően.
- 8/a. Node0->Updateformeasure és Node2->Updateformeasure: Az új párt tartalmazó két állomás frissítése.
- 6/b. Node1->purification: A memóriák megfelelő állapota esetén az állomáshoz tartozó tisztító protokoll elvégzése.
- 7/b. Node1->Updateformeasure: Állomás frissítése tisztítás után.

a következő teendőt, valamint a csomópont struktúrában elfoglalt helyének megfelelően állítja a memória szimulációs állapotát. Mivel a párral csak akkor tudunk a továbbiakban dolgozni, ha mind a két bitjét sikerrel fogadtuk, ezért a két fogadó csomópontnak ezt a tényt le kell kommunikálniuk klasszikus kommunikációs csatornák segítségével. Ezt a folyamatot jelképezi a megfelelő késleltetéssel ütemezett **ReceiveFromChSuccess**. Ha mindkét bit sikeresen bekerült a hozzá tartozó memóriába, állít a memória szimulációs állapotán, valamint ütemezi a következő lépést. Ez az **Updateformeasure** ami egy a csomópontot elvégzett frissítés. Azt nézi, hogy memóriákon végrehajtható-e már a Bell-mérés, valamint hogy mely tárolt párokon szükséges tisztítóprotokollt végrehajtani. Ennek megfelelően Bell-mérés elvégzést ütemez, vagy tisztítóprotokoll elvégzést ütemez. A Bell-mérés elvégzését a **Bellmeasure** lépéssel lehet elvégezni. Ennek során a bevezetőben leírtak alapján két páron megtörténik a Bell-mérés. Végeredményül az egyik új pár(a mért bitekből keletkezett) törlődik, míg a két távoli állomás bitjei között új összefonódás keletkezik. A mérésnek 4 eredménye lehet, de mivel a protokoll során mi egy bizonyos állapotot szeretnénk szétosztani szükség van egy mérés utáni korrekcióra. Ehhez szükség van a mérés eredményére, valamint az új pár qubitjein kell elvégezni, ezért itt is fellép a csomópontok között szükséges klasszikus kommunikációból adódó késleltetés. Ez a **CorrectAfterMeasure** megfelelő időre történő ütemezésével szimulálható. Maga a korrekció elvégezhető a qubiteken történő helyi műveletek végrehajtásával a teleportációs protokoll [7] idevágó lépéséhez hasonlóan Pauli X és Z kapuk segítségével. Legyen a cél állapotunk $|\Phi^+\rangle$. Ekkor a mérés után lehetséges 4 Bell állapotból ez csupán az első biten végrehajtott műveletekkel a következő módon előállítható:

$$\begin{aligned} |\Phi^+\rangle &\rightarrow |\Phi^+\rangle \\ Z|\Phi^-\rangle &\rightarrow |\Phi^+\rangle \\ X|\Psi^+\rangle &\rightarrow |\Phi^+\rangle \\ ZX|\Psi^-\rangle &\rightarrow |\Phi^+\rangle \end{aligned}$$

Ez után a párt tartalmazó memóriák állapotának frissítése történik, majd a pár qubitjeit tartalmazó állomások frissítése(**Updateformeasure**). Figyeljük meg, hogy ez a frissítés már a mérés utáni párt tartalmazó állomásokat frissíti, ezáltal az ismétlődő protokollban soron következő mérés elvégezhetőségét ezzel a frissítéssel már vizsgáljuk. Ha egy állomáson elég memória foglalt már, valamint a memóriákhoz tartozó párok tisztasága a mérés előtti előírtánál kisebb, a frissítés ütemezi az állomáshoz tartozó tisztító protokoll elvégzését. Mivel ennek elvégzéséhez két állomás együttműködésére is szükség van, itt is lehet számolni az ebből származó késleltetéssel, továbbá a tisztítás folyamata alatt az érintett memóriákon más feladatot sem végezhetünk. Ezt a programban a tisztítani kívánt memóriák lefoglalásával, majd a tisztítás megfelelő késleltetéssel történő ütemezésével lehet elérni. Ennek megtörténte után az állomás újbóli frissítése következik.

A működésről általánosan elmondható, hogy alulról fölfele építkezik. Az összes lépés eredő kiváltó ingere az összefonódott párok periodikus létrehozása, amiket a rendszer utána vagy kezel, vagy nem. Egy másik lehetséges megközelítés lehetne, hogy az állomások folyamatosan szabad erőforrásaiknak megfelelően kérnek párokat a forrásoktól, viszont így

szükség lenne további klasszikus kommunikáció lebonyolítására, ezért ettől a továbbiakban eltekintettem.

4. fejezet

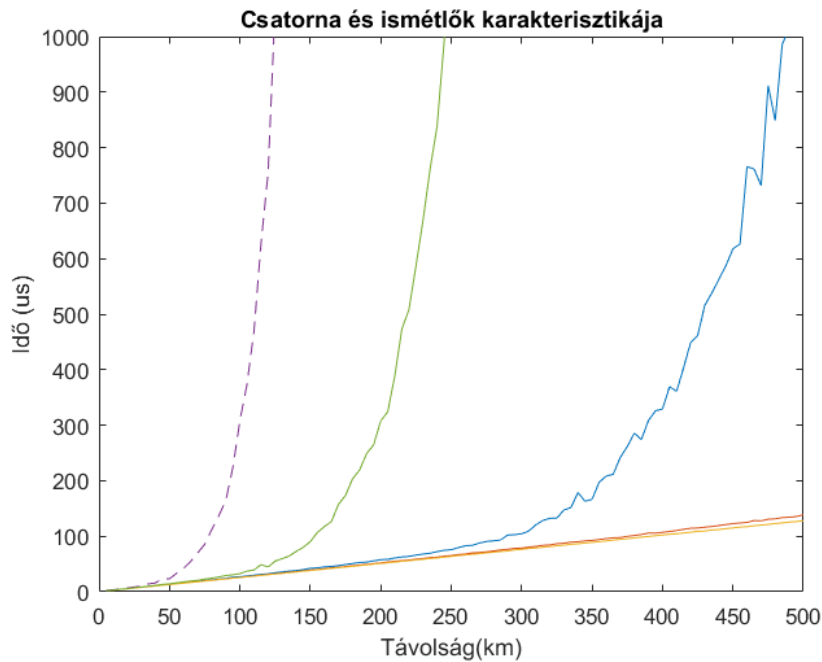
Szimulációs eredmények

Az elkészült szimuláció működésének ellenőrzésére a legegyszerűbb módszer, az általa szolgáltatott eredmények vizsgálata. Helyes működés esetén az így kapott eredmények használhatóak továbbá az ismétlő protokoll pontosabb bemutatására is. Mivel egy általánosított modellt szimulálok, a teszteseténél a program felé elvárás az adott esethez várt általános jelleg produkálása. Ennek előzetes meghatározásához használhatjuk az elméleti bevezetőben már megismerteket, valamint a szakirodalomban megtalálható egyéb szimulációkat, tanulmányokat [18][35][36]. A vizsgált esetekben, amennyiben nincsen másképp említve, a következő adatokat tekintettem alapértelmezésnek. Az összefonódott párok előállításáért felelős állomások $10\mu s$ -ként egyszerre 5 darab 0.7-es tisztaságú párt állítanak elő. Az egyes csatornákra jellemző „csillapítás hossz” 20km. A méréseket végző csomópontok mindkét beérkező csatorna felé 20 memória egységgel (összesen 40) rendelkeznek, valamint az egyes mérések előtt 0.98-as előírt tisztaságig tisztítatják a párokat. Az alapértelmezetten használt tisztító protokoll egy a bevezetőben már ismertetetthez hasonló [17] néhány későbbiekben javasolt változtatással [18]. Ennek lépései a programban teljes egészében, közelítések nélkül vannak szimulálva. Az egyes tisztítások sorrendjének meghatározásához használt alapértelmezett stratégia az ún. „greedy bottom up”, aminek pontos leírásával majd a későbbiekben foglalkozom. Az egyes mérések elvégzése egy a későbbiekben tárgyalt faszerű struktúra szerint történik. A vizsgált esetek teljesítményét az egységnyi idő alatt sikeresen megosztott párok számával mérjük.

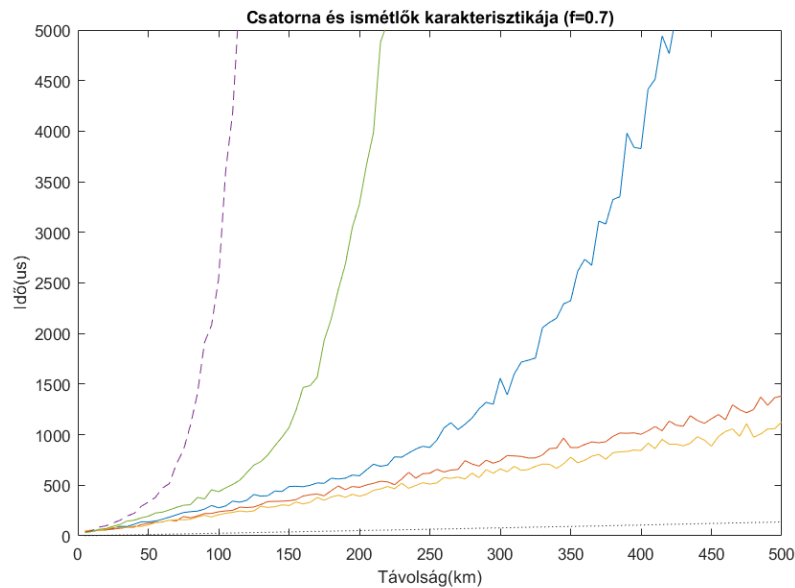
4.1. Ismétlő protokoll és az egyszerű csatorna

Első tesztesetnek azt vizsgáltam milyen távolság fölött kezd egyáltalán előnyt nyújtani a protokoll az ismétlő nélküli csatornával szemben. Tudván, hogy a csatorna átvitele a távolsággal exponenciálisan csökken, míg az ismétlőé csak polinomiálisan [18] azt várom, hogy kis távolságoknál egyszerűsége miatt a csatorna mutat jobb teljesítményt, míg egy bizonyos távolság felett az ismétlő. Szimulációval 5-500km-es távolságig vizsgáltam az egyes esetek teljesítményét. Először azt az idealizált esetet tekintve, ahol csak a párok elvesztésével kell számolni, a tisztaságukkal nem (szétosztott párok tisztasága = 1), később a csatorna esetén a végpontokban, az ismétlőknél pedig a köztes állomásokon elvégzendő tisztítás hatását is

figyelembe véve.



4.1. ábra. Csatorna és különböző ismétlők átvitele a távolság függvényében:
 Az y tengelyen az egy pár megosztásához szükséges átlagos időt mérjük.
 Lila szaggatott vonal: egyszerű csatorna.
 zöld, kék, piros, narancs vonalak: 2, 4, 8 valamint 16, köztes létrehozó állomásból álló ismétlő rendszerek.
 A szimuláció során kizárólag az átvitel során történő pár veszteséget vizsgáltam (megosztott párok tisztasága 1-> nem kell tisztítani).
 A csatorna és a 2 generátoros rendszer esetében a szimulációt idő előtt leállítottam a veszteségek miatt megnövekedett szükséges számítási kapacitás miatt.



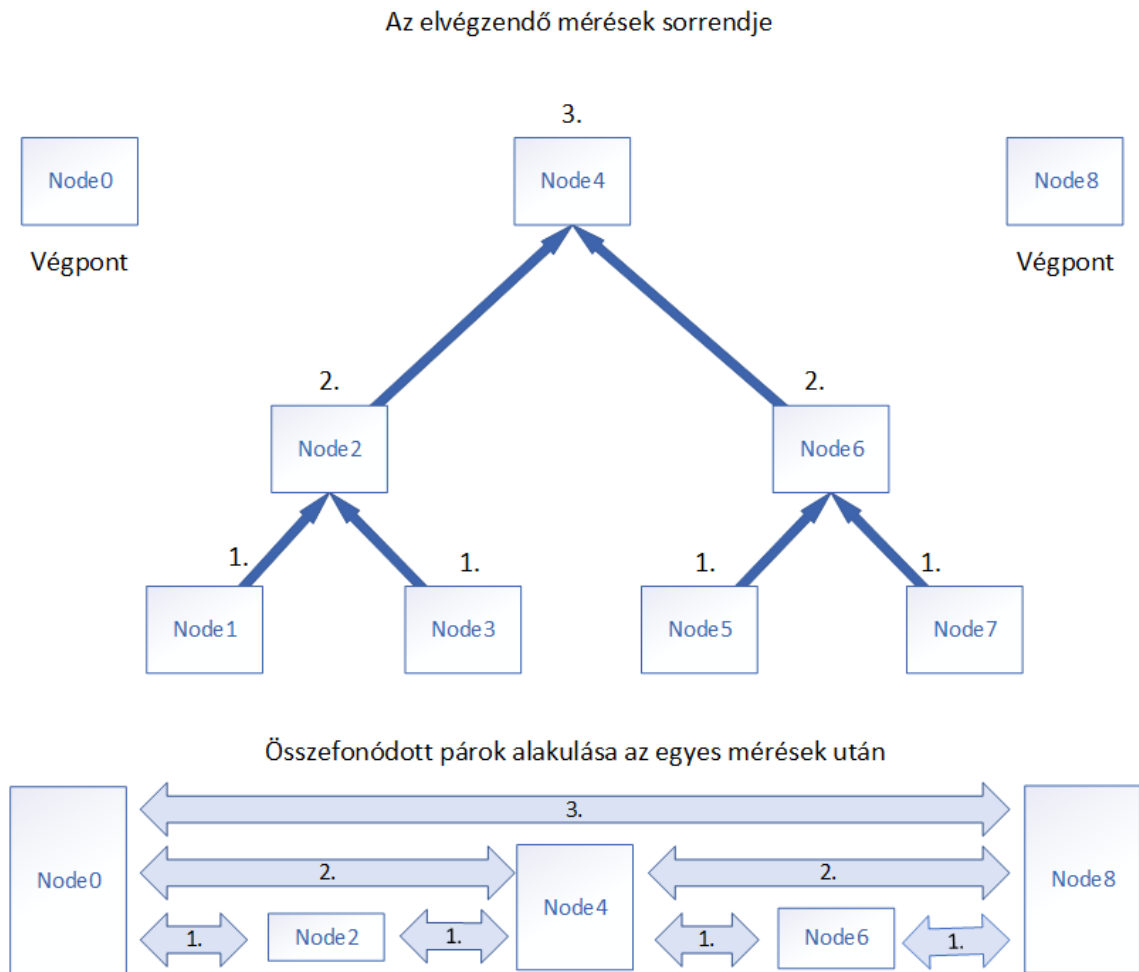
4.2. ábra. Csatorna és különböző ismétlők átvitele a távolság függvényében:
 Az y tengelyen az egy pár megosztásához szükséges átlagos időt mérjük.
 Lila szaggatott vonal: egyszerű csatorna.
 Zöld, kék, piros, narancs vonalak: 2, 4, 8 valamint 16, köztes létrehozó állomásból álló ismétlő rendszerek.
 Alsó fekete pontozott vonal: 8 köztes állomásból álló rendszer teljes tisztaság esetén.
 A szétozott párok ebben az esetben nem ideálisak, a tisztaságuk 0.7-es. Ennek következtében szükség van a tisztító eljárások végrehajtására. (egyszerű csatorna esetében ez a végpontokon történik.)
 A csatorna és a 2 generátoros rendszer esetében a szimulációt itt is idő előtt leállítottam a veszteségek miatt megnövekedett szükséges számítási kapacitás miatt.

Az egyes esetek teljesítményét az egy pár megosztásához szükséges átlagos idővel mértem (200 megosztott párból számolva). Látható a csatorna átvitelének exponenciális romlása, valamint nagyobb távolságok esetén az ismétlő elrendezések is ezt a jelleget mutatják. Ennek oka, hogy az egyes állomásokat is exponenciálisan romló csatornák kötik össze. A protokoll fő előnye, hogy egy nagy ilyen szakasz helyett használhatunk több kisebbet. A tisztaság rontásának hatása is megfigyelhető: a teljesen tiszta esethez képest ilyenkor a tisztítás miatt több párt kell felhasználni egy tiszta pár létrehozásához a végpontok között. A görbék jellege nem változott viszont az átlagos idő nőtt.

Az ismétlő protokollok természetesen több erőforrást használ mint csupán egy csatorna, viszont ezzel az előzőekben nem foglalkoztam. Ennek figyelembevételre tekintettem a következő eseteket: Álljon rendelkezésre egy 8 generátoros, állomásonként 8x5 memóriaegységgel rendelkező rendszer megvalósításához szükséges erőforráshalmaz. Ebből készíthető egy generátoros esetben egy 8-szor gyorsabb párgenerátor, valamint egyenként 8x5 pár kezelésére alkalmas végpont. Ezen logika mentén elkészíthető még 2 generátoros rendszer, 4-szer gyorsabb generátorokkal és 4x5 memóriával rendelkező állomásokkal, valamint hasonló logika alapján egy 4 generátoros rendszer is. Ezek egymáshoz képesti teljesítménye:

4.2. Mérési sorrend

A protokoll működése során fontos szerepe van az egyes mérések elvégzési sorrendjének is. A következőkben két különböző stratégiát vizsgálunk. Az egyik stratégia a többi vizsgálatnál általam alapértelmezettnek használt, ahol a mérések sorrendjét egy faszerű struktúra határozza meg. Itt a hálózat tipikusan $2^n + 1$ elemből áll (bár a végpontoknak csak az egyik felét használjuk). Két azonos szinten lévő csomópont között a kapcsolatot mindig a közöttük félúton lévő állomáson elvégzett mérés hozza létre. Ennek megfelelően egy egyszerű hálózatra ez a következőt jelenti:

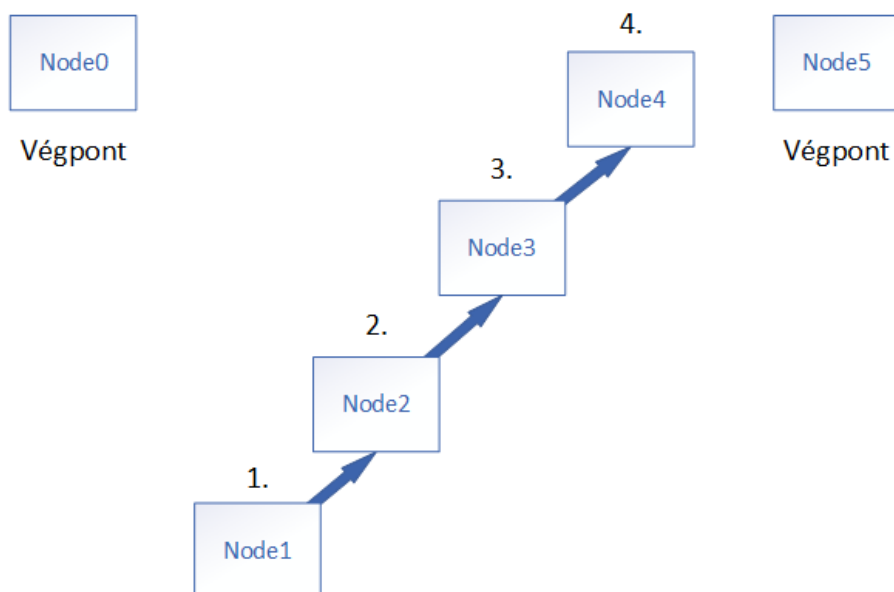


4.3. ábra. Az egyes számok a mérések elvégzési sorrendjét jelölik (feltételezzük, hogy minden állomáson rendelkezésre állnak az ehhez szükséges generátorok által küldött párok). A nyílak a sorban következő elvégzendő mérést jelölik, valamint az alsó ábrán az állomások közötti összefonódásokat.

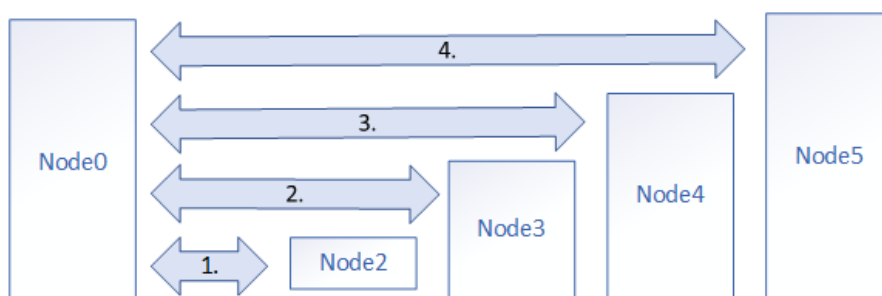
Az elrendezésből látszik, hogy ez a stratégia akkor a leghatékonyabb, ha $2^n - 1$ közbenső állomás van (+2 végponttal lesz így $2^n + 1$ állomás összesen).

A másik vizsgált stratégiánál egyszerűen sorban végezzük el a méréseket. Ez a következőképp néz ki:

Az elvégzendő mérések sorrendje



Összefonódott párok alakulása az egyes mérések után



4.4. ábra. Az egyes számok itt is a mérések elvégzési sorrendjét jelölik (feltételezzük, hogy minden állomáson rendelkezésre állnak az ehhez szükséges generátorok által küldött párok). A nyilak a sorban következő elvégzendő mérést jelölik, valamint az alsó ábrán az állomások közötti összefonódásokat.

4.3. Összefonódott pár létrehozási sebesség hatása

4.4. A fogadott párok tisztasága

4.5. Tisztító stratégiák

4.6. Erőforrások elosztása

4.7. Egyéb megfontolandó paraméterek

4.7.1. Protokoll indulása

Az előzőekben kizárólag a hosszabb működés alatti átlagteljesítményt vizsgáltam, azonban meg kell említeni, hogy a rendszerek rendelkeznek egy úgymond telítődési idővel is ami indulásnál az egyes állomások kezdetben üres memóriáinak megfelelő állapotú párokkal való feltöltődésének ideje. Ennek szemléltetésére vizsgáltam a következőkben az indulástól számított első néhány sikeres megosztásig eltelt időt....

4.7.2. Kvantumos memóriák

Az előzőekben az egyes állomásokon a biteket tároló memóriákat ideálisnak tekintettük, azonban a való életben ezek korántsem azok. Határaik és tökéletlenségeik komoly limitáló tényezőt jelenthetnek. A legjobb tárolási minőségre, valamint a legnagyobb tárolási időre, a végpontokban van szükség, mivel az itt tárolt bitek állapotának fent kell maradni mialatt az összes hozzájuk tartozó mérést elvégezzük. Ennek az időnek az alakulását vizsgálom az alábbi szimulációkban.

Irodalomjegyzék

- [1] IBM, „Ibm announces advances to ibm quantum systems & ecosystem.” <http://www-03.ibm.com/press/us/en/pressrelease/53374.wss>, 2017.
- [2] C. Neill, P. Roushan, K. Kechedzhi, S. Boixo, S. Isakov, V. Smelyanskiy, R. Barends, B. Burkett, Y. Chen, Z. Chen, *et al.*, „A blueprint for demonstrating quantum supremacy with superconducting qubits,” *arXiv preprint arXiv:1709.06678*, 2017.
- [3] C. H. Bennett and G. Brassard, „Quantum cryptography:public-key distribution and coin tossing,” *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984.
- [4] P. Marks, „Quantum cryptography to protect swiss election.” <https://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/>, 2007.
- [5] H. J. Kimble, „The quantum internet,” *Nature*, vol. 453, no. 7198, pp. 1023–1030, 2008.
- [6] W. K. Wootters and W. H. Zurek, „A single quantum cannot be cloned,” *Nature*, vol. 299, no. 5886, pp. 802–803, 1982.
- [7] 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.
- [8] E. Schrödinger, „An undulatory theory of the mechanics of atoms and molecules,” *Physical Review*, vol. 28, no. 6, p. 1049, 1926.
- [9] A. Einstein, B. Podolsky, and N. Rosen, „Can quantum-mechanical description of physical reality be considered complete?,” *Physical review*, vol. 47, no. 10, p. 777, 1935.
- [10] J. Bell, „On the einstein podolsky rosen paradox,” 1964.
- [11] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, „Experimental quantum teleportation,” *Nature*, vol. 390, no. 6660, pp. 575–579, 1997.
- [12] P. W. Shor, „Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM review*, vol. 41, no. 2, pp. 303–332, 1999.

- [13] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, „Experimental quantum cryptography,” *Journal of cryptology*, vol. 5, no. 1, pp. 3–28, 1992.
- [14] 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.
- [15] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, „Experimental entanglement swapping: entangling photons that never interacted,” *Physical Review Letters*, vol. 80, no. 18, p. 3891, 1998.
- [16] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, „Purification of noisy entanglement and faithful teleportation via noisy channels,” *Physical review letters*, vol. 76, no. 5, p. 722, 1996.
- [17] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, „Quantum privacy amplification and the security of quantum cryptography over noisy channels,” *Physical review letters*, vol. 77, no. 13, p. 2818, 1996.
- [18] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, „Quantum repeaters: the role of imperfect local operations in quantum communication,” *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.
- [19] R. Bandom, „China’s new satellite would create the world’s largest quantum network.” <https://www.theverge.com/2016/8/15/12489914/china-satellite-quantum-encryption-network-launch>, 2017.
- [20] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, *et al.*, „Satellite-based entanglement distribution over 1200 kilometers,” *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.
- [21] „Quantum manifesto endorsement.” <http://quope.eu/manifesto>, 2016.
- [22] S. Pirandola and S. L. Braunstein, „Unite to build a quantum internet,” *Nature*, pp. 169–171, 2016.
- [23] D. A. Lidar and T. A. Brun, *Quantum error correction*. Cambridge University Press, 2013.
- [24] J. Zhang, Y.-x. Liu, Ş. K. Özdemir, R.-B. Wu, F. Gao, X.-B. Wang, L. Yang, and F. Nori, „Quantum internet using code division multiple access,” *Scientific reports*, vol. 3, 2013.
- [25] M. Uphoff, M. Brekenfeld, G. Rempe, and S. Ritter, „An integrated quantum repeater at telecom wavelength with single atoms in optical fiber cavities,” *Applied Physics B*, vol. 122, no. 3, p. 46, 2016.

- [26] H. Krovi, S. Guha, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, „Practical quantum repeaters with parametric down-conversion sources,” *Applied Physics B*, vol. 122, no. 3, p. 52, 2016.
- [27] A. D. Pfister, M. Salz, M. Hettrich, U. G. Poschinger, and F. Schmidt-Kaler, „A quantum repeater node with trapped ions: a realistic case example,” *Applied Physics B*, vol. 122, no. 4, p. 89, 2016.
- [28] T. Li, G.-J. Yang, and F.-G. Deng, „Heralded quantum repeater for a quantum communication network based on quantum dots embedded in optical microcavities,” *Physical Review A*, vol. 93, no. 1, p. 012302, 2016.
- [29] I. Sándor and F. Balázs, *Quantum Computing and Communications: an engineering approach*. John Wiley & Sons, 2005.
- [30] A. Peres, „Delayed choice for entanglement swapping,” *Journal of Modern Optics*, vol. 47, no. 2-3, pp. 139–143, 2000.
- [31] 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.
- [32] 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.
- [33] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, „Bell measurements for teleportation,” *Physical Review A*, vol. 59, no. 5, p. 3295, 1999.
- [34] „Eigen c++ library.” eigen.tuxfamily.org/.
- [35] R. Van Meter, T. D. Ladd, W. Munro, and K. Nemoto, „System design for a long-line quantum repeater,” *IEEE/ACM Transactions on Networking (TON)*, vol. 17, no. 3, pp. 1002–1013, 2009.
- [36] N. K. Bernardes, L. Praxmeyer, and P. van Loock, „Rate analysis for a hybrid quantum repeater,” *Physical Review A*, vol. 83, no. 1, p. 012323, 2011.
- [37] S. Imre and L. Gyongyosi, *Advanced quantum communications: an engineering approach*. John Wiley & Sons, 2012.

Függelék

F.1. Sűrűségmátrixos leírás

Az [37] alapján: Ennél a leírásnál a rendszert a lehetséges állapotainak valószínűségeinek összegével jellemezzük:

$$\rho = \sum_i p_i |\phi_i\rangle \langle \phi_i|$$

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:

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

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

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

Továbbá említésre méltó még, hogy $\text{Tr}(A)$ egyenlő A sajátértékeinek összegével.

F.2. Összefonódás megosztás lépésről lépésre

Vizsgáljuk a következőt :

$$\begin{aligned} |\Psi^+\rangle \otimes |\Psi^+\rangle - |\Psi^-\rangle \otimes |\Psi^-\rangle &= \frac{1}{2} \left((|01\rangle + |10\rangle) \otimes (|01\rangle + |10\rangle) - (|01\rangle - |10\rangle) \otimes (|01\rangle - |10\rangle) \right) = \\ &= \frac{1}{2} \left(|0101\rangle + |0110\rangle + |1001\rangle + |1010\rangle - |0101\rangle + |0110\rangle + |1001\rangle - |1010\rangle \right) = \\ &= \frac{1}{2} (2|0110\rangle + 2|1001\rangle) = |0110\rangle + |1001\rangle \end{aligned}$$

hasonlóan:

$$\begin{aligned} |\Phi^+\rangle \otimes |\Phi^+\rangle - |\Phi^-\rangle \otimes |\Phi^-\rangle &= \frac{1}{2} \left((|00\rangle + |11\rangle) \otimes (|00\rangle + |11\rangle) - (|00\rangle - |11\rangle) \otimes (|00\rangle - |11\rangle) \right) = \\ &= \frac{1}{2} \left(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle - |0000\rangle + |0011\rangle + |1100\rangle - |1111\rangle \right) = \\ &= \frac{1}{2} (2|0011\rangle + 2|1100\rangle) = |0011\rangle + |1100\rangle \end{aligned}$$

Ezek felhasználásával már egyszerűen levezethető hogy:

$$\begin{aligned}
|\Psi_{kezd}^-\rangle &= |\Psi^-\rangle_{AB} \otimes |\Psi^-\rangle_{CD} = \frac{1}{\sqrt{2}}(|0_A 1_B\rangle - |1_A 0_B\rangle) \frac{1}{\sqrt{2}}(|0_C 1_D\rangle - |1_C 0_D\rangle) = \\
&\frac{1}{2}(|0_A 1_B 0_C 1_D\rangle - |0_A 1_B 1_C 0_D\rangle - |1_A 0_B 0_C 1_D\rangle + |1_A 0_B 1_C 0_D\rangle) = \\
&\frac{1}{2}(|0_A 1_D 1_B 0_C\rangle - |0_A 0_D 1_B 1_C\rangle - |1_A 1_D 0_B 0_C\rangle + |1_A 0_D 0_B 1_C\rangle) = \\
&\frac{1}{2}(|0_A 1_D 1_B 0_C\rangle + |1_A 0_D 0_B 1_C\rangle - (|0_A 0_D 1_B 1_C\rangle + |1_A 1_D 0_B 0_C\rangle)) = \\
&\frac{1}{2}(|\Psi^+\rangle_{AD} |\Psi^+\rangle_{BC} - |\Psi^-\rangle_{AD} |\Psi^-\rangle_{BC} - |\Phi^+\rangle_{AD} |\Phi^+\rangle_{BC} + |\Phi^-\rangle_{AD} |\Phi^-\rangle_{BC})
\end{aligned}$$