Budapesti Műszaki és Gazdaságtudományi Egyetem
Híradástechnikai Tanszék
Mobil és Kvantumtechnológiai Laboratórium

Zéró-kapacitású kvantumcsatornák információ-geometriai aktiválása

Tézisfüzet

Gyöngyösi László

Témavezető:

Prof. Dr. Imre Sándor

Budapest

2013

Kivonat

A szuperaktiválás segítségével, zéró kapacitással rendelkező kvantumcsatornák akár teljesen hibamentes információátvitelre használhatóak. A szuperaktiválás jelensége azonban csak bizonyos kvantumcsatorna kombinációk esetében lép fel. A szuperaktiválással kapcsolatos elméleti háttér teljes körűen nem bizonyított, így további olyan csatorna kombinációk is elképzelhetőek, amelyekkel a kvantumcsatornák kapacitása szuperaktiválható. Az elméleti úton igazolt csatorna kombinációkon túlmenően számos, jelenleg még felderítetlen kombináció létezhet. A Ph.D disszertációmban a kvantumcsatornák szuperaktiválási problémájára adtam algoritmikus megoldást. A kidolgozott módszerem segítségével, az elméleti úton jelenleg még nem igazolt szuperaktív csatorna kombinációk is nagy hatékonysággal feltárhatóak, azok információátviteli képessége pedig nagy pontossággal meghatározható.

A kvantumcsatornák szuperaktiválási lehetőségeinek vizsgálata egy gyakorlati rendszer esetében nagyszámú kvantumállapot vizsgálatát igényli, amely bonyolult feladat. A szuperaktivált csatornakapacitás vizsgálatát hatékony algoritmikus és információ geometriai módszerekkel hajtottam végre. A kvantumcsatornák kapacitásának meghatározása numerikus módszerekkel NP-teljes probléma. A kapacitás pontos kiszámítása már egy kisméretű kvantumrendszer esetében is kezelhetetlenné válik. A kifejlesztett információ-geometriai metódus segítségével a szuperaktiválható csatornakombinációk feltárása, valamint azok kapacitásának pontos meghatározása nagyméretű kvantumrendszer (gyakorlati rendszerek) esetében is hatékonyan végrehajtható.

A doktori disszertációmban kidolgozott geometriai eljárás segítségével válasz adható a kvantumcsatornák tulajdonságaival kapcsolatos – jelenleg is tisztázatlan – kérdésekre, illetve felderíthetőek a zéró-kapacitású kvantumcsatornákon keresztüli információátvitel megvalósításához szükséges peremfeltételek. A kutatási munka során kiemelten vizsgáltam a szuperaktiválás gyakorlati alkalmazhatóságát a jövő kommunikációs hálózataiban. Az elért elméleti jellegű eredményeinknek köszönhetően nagyságrendekkel hatékonyabb kommunikáció válhat elérhetővé a jövő kvantum-kommunikációs hálózataiban, lehetővé téve a nagy-hatótávolságú, biztonságos kvantum-kommunikációs hálózatok világszintű elterjedését.

Tézisek

1. Téziscsoport. *Bebizonyítottam, hogy tetszőleges dimenziószámú kvantumcsatornák szuperaktiválása leírható információ-geometriai eszközökkel. Bebizonyítottam, hogy a szuperaktiválás jelensége matematikailag információ-geometriai alapokra vezethető vissza.*

1.1. Tézis. *Igazoltam, hogy a szuperaktiválhatósága eldönthető egy absztrakt információ geometriai objektum, a kvantum információs szupergömb segítségével* [P1, P2, P3, B1, C1-C15], [Chapter 5, Appendix D, Appendix E].

1.2. Tézis. *Bebizonyítottam, a kvantum információs szupergömb sugara a tetszőleges dimenziószámú csatornákat tartalmazó kombinált csatornastruktúra szuperaktivált kapacitásával azonos* [P1, P2, P3, B1, C1-C15], [Chapter 5, Appendix D, Appendix E].

1.3. Tézis. *Bebizonyítottam, hogy a szuperaktiválható kvantumcsatornák halmazát a kvantum relatív entrópia függvény matematikai tulajdonságai határozzák meg* [P1, P2, P3, B1, C1-C15], [Chapter 5, Appendix D, Appendix E].

2 Téziscsoport. *Definiáltam egy hatékony algoritmust a kvantumcsatornák kvantumkapacitásának szuperaktiválására.*

2.1. Tézis. *Bebizonyítottam, a szuperaktiválható kvantumcsatorna kombinációk feltárása információ-geometriai eszközökkel végrehajtható* [P1, P2, P7, B1, C11-C15], [Chapter 6, Appendix D, Appendix E, Appendix F, Appendix G].

2.2. Tézis. *Igazoltam, hogy a felfedezett matematikai összefüggések felhasználhatóak hatékony információ-geometriai algoritmusok kifejlesztésére* [P1, P2, P7, P9, B1, C11-C15], [Chapter 6, Appendix D, Appendix E, Appendix F, Appendix G].

2.3. Tézis *Definiáltam a szuperaktiválható kvantumkapacitással rendelkező kvantumcsatorna-kombinációk feltárásához szükséges algoritmust* [P1, P2,P7, B1, C11-C15], [Chapter 6, Appendix D, Appendix E, Appendix F, Appendix G].

3. Téziscsoport. *Definiáltam egy polinomiális approximációra épülő információ geometriai algoritmust a kvantumcsatornák klasszikus perfekt kapacitás szuperaktiválhatóságának vizsgálatára. A módszer tetszőleges dimenziószámú kvantumcsatornák esetén alkalmazható, a numerikus módszerek esetében fennálló NP-teljes komplexitás nélkül.*

3.1. Tézis. *Bebizonyítottam, hogy a klasszikus perfekt kapacitás szuperaktiváláshoz szükséges peremfeltételek a kifejlesztett absztrakt geometriai struktúra segítségével feltárhatóak* [P3,B1, C1-C10], [Chapter 7, Appendix D, Appendix E, Appendix F, Appendix G].

3.2. Tézis. *Igazoltam, hogy a kifejlesztett információ-geometriai polinomiális approximációs algoritmus, minimális hibával képes a tetszőleges dimenziószámú kvantumcsatornákat tartalmazó kombinált struktúra szuperaktiválható csatornakapacitásának meghatározására* [P3, B1, C1-C10], [Chapter 7, Appendix D, Appendix E, Appendix F, Appendix G].

3.3. Tézis. *Igazoltam, hogy a bemeneti sűrűségmátrixok algoritmikus előszűrésével, valamint hatékony információ-geometriai megoldások alkalmazásával, a tetszőleges kvantumcsatornákból álló kombinált csatornastruktúra klasszikus perfekt csatornakapacitásának szuperaktiválása polinomiális komplexitás mellett végrehajtható* [P3, B1, C1-C10], [Chapter 7, Appendix D, Appendix E, Appendix F, Appendix G].

1 Bevezető

A kvantumcsatornák a hagyományos optikai szálakkal, illetve műhold-alapú, vezetéknélküli kommunikációs csatornákkal is megvalósíthatóak a *jelenlegi* – már kiépített – hagyományos hálózati architektúra felhasználásával. Ugyanakkor, a kvantum-kommunikációs csatornák tulajdonságai nem írhatóak le a hagyományos, klasszikus információelmélet eredményeivel [Shannon48]. A kvantumcsatornák kapacitásával kapcsolatban számos kérdés jelenleg is tisztázatlan. A Ph.D disszertációmban a kvantumcsatornák kapacitásával kapcsolatos, *jelenleg is nyitott* kérdéseket kutattam.

A *szuperaktiválás* segítségével, információátvitelre alkalmatlan kvantumcsatornák egymással kombinálva alkalmazhatóak információátvitelre [Brandao11], [Cubitt09], [Cubitt09a], [Cubitt10], [Duan09], [Smith08], [Smith11]. A szuperaktiválás alapját az ún. „*additivitási-tétel*" sérülése jelenti: két kvantumcsatorna kombinálásával, és azok együttes használatával több információ továbbítható, mint a két független csatornán átküldött információmennyiség összege. A szuperaktiválás az additivitási tétel *extrém* sérülése: a kombinált csatornamodellben található csatornák önmagukban nem képesek információátvitelre; - a kombinált struktúra kapacitása azonban mégis pozitívvá tehető. A szuperaktiválás jelensége ugyanakkor még elméletileg nem tisztázott, számos egyéb csatornakombináció is elképzelhető az eddig feltárt néhány kombináción túl. A célom a probléma algoritmikus úton történő megoldása volt. A *szuperaktiválás* jelensége, illetve a tökéletes információátvitel szuperaktiválásának lehetősége klasszikus (hagyományos, nem kvantum-alapú kommunikációs rendszerek) rendszerekben teljességgel elképzelhetetlen és megvalósíthatatlan.

A kutatási részfeladatok keretén belül egyesítettem az algoritmuselmélet, információelmélet, a számítógépes geometria, valamint a kvantum-információelmélet eredményeit. A kvantum-információelméleti, illetve hagyományos információelméleti és algoritmuselméleti eredmények közti kapcsolatok felhasználhatóak a kvantum-kommunikációs protokollok információelméleti tulajdonságainak analizálására, valamint hatékony kommunikációs kódolási eljárások kidolgozására.

A kvantum-repeaterek („kvantum-jelismétlők") tervezése és kifejlesztése alapvető fontosságú a jövő telekommunikációs hálózatainak hatékonysága szempontjából. Javaslatot tettem a kvantum-jelismétlők működési mechanizmusának, illetve azok strukturális felépítésének módosításaira. Az elért elméleti jellegű eredményeinknek köszönhetően nagyságrendekkel hatékonyabb kommunikáció válhat elérhetővé a jövő kvantum-kommunikációs hálózataiban, lehetővé téve a nagy-hatótávolságú, biztonságos kvantum-kommunikációs hálózatok világszintű elterjedését. A kutatási feladat keretén belül kiemelten vizsgáltam az eredmények gyakorlati alkalmazhatóságát a kvantum-kommunikációs hálózatokban.

Az Ph.D disszertáció tudományos eredményeit lektorált külföldi folyóiratcikkekben, konferencia kiadványokban, valamint könyvfejezetek és monográfiák formájában publikáltam.

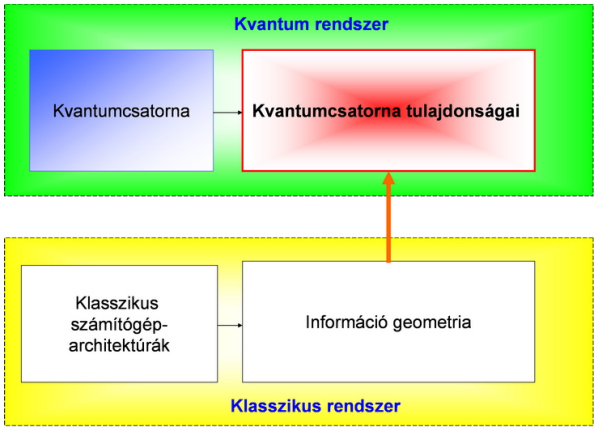
1.1 A kutatás kontextusának bemutatása

A Ph.D disszertáció elsődleges célja a jövő kvantum-kommunikációs hálózataiban rejlő lehetőségek feltérképezése. A Moore-törvény alapján, 2020-ra várhatóan egy bit információt egy atom tárol majd, így már néhány éven belül elérkezhet a kvantuminformatika világa. A kvantumszámítógépek támadásával szemben a jelenlegi, gyakorlatban alkalmazott klasszikus titkosítási és kriptográfiai algoritmusok legtöbbje védtelen. A kvantumszámítógép működése a kvantumelméletre épül, és alkalmas arra, hogy minden mai modern, feltörhetetlennek vélt kódot másodpercek alatt feltörjön [Shor94], [Grover96].

A kvantumszámítógépek napjainkban ugyan még nem állnak rendelkezésre, ellenük azonban csak a kvantumcsatornákon keresztüli kommunikáció nyújthat abszolút védelmet. A jövőbeni védelmi módszerek kidolgozása szempontjából így már ma alapvető fontosságú a kvantumcsatornákon keresztüli kommunikáció lehetőségeinek pontos megismerése és feltérképezése.

A kutatási munka keretén belül vizsgáltam a zajos kvantumcsatornák kapacitás visszaállíthatóságának kérdését, annak alkalmazhatóságát nagy-hatótávolságú kvantumkommunikáció területén, valamint hatékony algoritmusokat dolgoztam ki szuperaktiválási probléma elemzésére. Amíg klasszikus kommunikációs csatornák esetén egyetlen kapacitás (*klasszikus kapacitás*) áll rendelkezésünkre az információátvitel megvalósítására, addig a kvantumcsatornák esetében többféle csatornakapacitás (*klasszikus, kvantumalapú klasszikus, privát, tisztán kvantum*) közül választhatunk [Cortese02], [Cortese03], [Devetak03], [Hastings09], [Hayashi03], [Holevo98], [Imre05], [Imre12], [Lloyd97], [Mosca06], [Ruskai01], [Schumacher97], [Shor02], [Smith09b].

A Ph.D disszertációmban hatékony információ-geometriai módszerekkel adtam választ a kvantumcsatornák szuperaktiválására, valamint a további lehetséges – elméleti úton mindezidáig feltáratlan - csatornakombinációk megtalálására. Megmutattam, hogy a kvantum-információelméleti, illetve hagyományos információelméleti és algoritmuselméleti eredmények közti kapcsolatok felhasználhatóak a kvantumcsatornák szuperaktiválásának információelméleti tulajdonságainak analizálására, valamint hatékony kommunikációs kódolási eljárások kidolgozására (*1. ábra*). A geometria alapvető feladata a különböző térbeli kiterjedések, alakzatok leírása és modellezése. A számítógépes geometria napjainkra különálló tudományterületté vált, szerepe pedig alapvető fontosságú a számítógépes grafika, geográfiai rendszerek, mesterséges intelligencia, robotika, illetve számos egyéb kutatás területén [Ackermann08], [Chen07], [Feldman07], [Nielsen07], [Nielsen07a], [Nielsen08b], [Nielsen09].

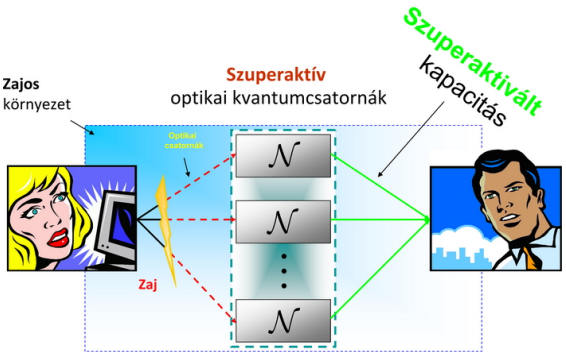


1. ábra. A kvantumcsatornák szuperaktiválására kidolgozott megoldás a klasszikus számítógépes architektúrákra épül. [L. Gyongyosi, S. Imre: Algorithmic Superactivation of Asymptotic Quantum Capacity of Zero-Capacity Quantum Channels, Information Sciences, Informatics and Computer Science Intelligent Systems Applications, ELSEVIER, ISSN: 0020-0255; 2011]

A Ph.D disszertáción belül elvégzett kutatásaim célja a jövő kvantum-kommunikációs hálózataiban rejlő lehetőségek feltérképezése, a zajos kvantumcsatornák szuperaktiválhatóságának, valamint a kvantum-csatornák fejlett (klasszikus kommunikációs rendszerek esetén elképzelhetetlen) tulajdonságainak vizsgálatán keresztül.

2 Eredmények

A kvantumcsatornák kapacitásával kapcsolatban számos kérdés jelenleg is tisztázatlan. A hagyományos információelméleti eredmények nem alkalmazhatóak a kvantumrendszerek leírására, számos jelenségre pedig klasszikus analógia sem állítható fel. Kutattam a kvantumcsatornák kapacitásával kapcsolatos nyitott kérdéseket, valamint az azokban rejlő forradalmi lehetőségeket. Az eredmények alapján kijelenthető, hogy a szuperaktiválás jelensége forradalmasíthatja a jövő tele-kommunikációs hálózatainak működését, általánossá téve a *szuperaktivált kapacitásokra* épülő világszintű kommunikációt (*2. ábra*).



2. ábra. Az optikai kvantumcsatornák szuperaktiválása forradalmasíthatja a jövő telekommunikációs hálózatait. A szuperaktiválás kiterjeszthető tökéletes (zero-error) információátvitelre is. [L. Gyongyosi, S. Imre: Information Geometric Superactivation of Classical Zero-Error Capacity of Quantum Channels, Progress in Informatics, Quantum Information Technology, Print ISSN : 1349-8614, Online ISSN : 1349-8606; 2011.]

Amint arra a Ph.D disszertációban kitértem, a kvantumcsatornák szuperaktiválási lehetőségeinek vizsgálata nagyszámú bemeneti kvantumállapot esetében bonyolult feladat. A szuperaktivált csatornakapacitást leíró absztrakt kvantum-információelméleti gömb meghatározását hatékony, algoritmikus geometriai módszerekre vezettem vissza.

A kvantumcsatornák kapacitásának meghatározása numerikus módszerekkel NP-teljes probléma [Beigi07]. Ennek következtében, a kapacitás meghatározása már egy kisméretű kvantumrendszer esetében lehetetlenné válik. A kifejlesztett információ-geometriai metódusunk segítségével azonban, - a numerikus úton NP-teljes probléma - kezelhetővé válik, megkerülhető, a kapacitás meghatározása pedig nagyméretű kvantumrendszerek (gyakorlati alkalmazások) esetében is nagy hatékonysággal végrehajtható.

A kvantumcsatornák szuperaktiválási tulajdonságának vizsgálatára kifejlesztett geometriai metódusom segítségével, a gyakorlati átvitel során alkalmazott kvantumcsatornák információelméleti tulajdonságai, illetve az azokkal kapcsolatos nyitott kérdések analizálhatóak.

Első téziscsoport

A Ph.D disszertációmban feltártam a kvantumcsatornák szuperaktiválhatóságának matematikai alapjait. Ezen eredményeket az 1. Téziscsoport tartalmazza.

1. Téziscsoport. Bebizonyítottam, hogy tetszőleges dimenziószámú kvantumcsatornák szuperaktiválása leírható információ-geometriai eszközökkel. Bebizonyítottam, hogy a szuperaktiválás jelensége matematikailag információ-geometriai alapokra vezethető vissza.

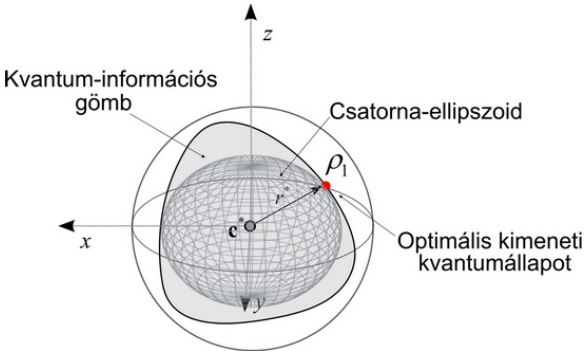
> **1.1. Tézis.** Bebizonyítottam, hogy a szuperaktiválhatósága eldönthető egy absztrakt információ geometriai objektum, a kvantum információs szupergömb segítségével *[P1, P2, P3, B1, C1-C15], [Chapter 5, Appendix D, Appendix E].*
>
> **1.2. Tézis.** Bebizonyítottam, a kvantum információs szupergömb sugara a tetszőleges dimenziószámú csatornákat tartalmazó kombinált csatornastruktúra szuperaktivált kapacitásával azonos *[P1, P2, P3, B1, C1-C15], [Chapter 5, Appendix D, E Függelék].*
>
> **1.3. Tézis.** Bebizonyítottam, hogy a kvantumcsatornák szuperaktiválhatósága a kvantum relatív entrópia függvény tulajdonságai által determinált [*P1, P2, P3, B1, C1-C15], [Chapter 5, Appendix D, E Függelék].*

Amíg a kvantumcsatornák kapacitásának meghatározása eddig numerikus úton nehéz feladatnak bizonyult, addig a kifejlesztett megoldás segítségével forradalmi lehetőségek

nyílhatnak meg a kvantumcsatornák kapacitásvizsgálatában. A kvantumcsatornák szuperaktiválásának kérdését az általunk kifejlesztett információ-geometriai megoldásra vezettük vissza.

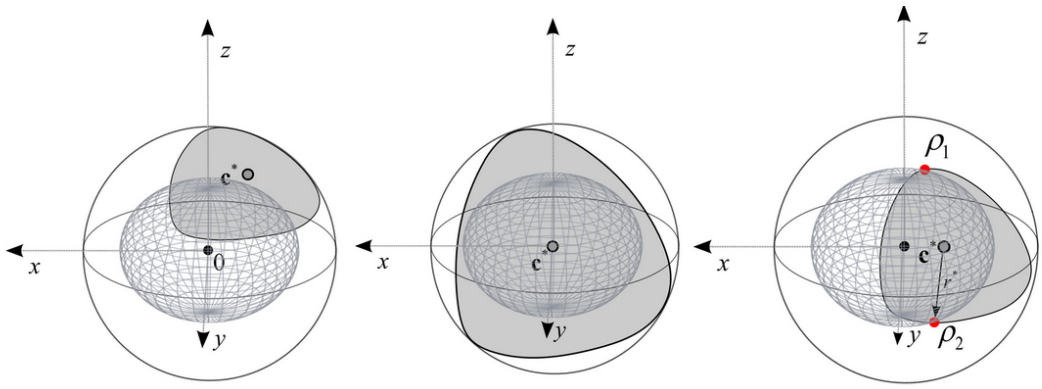
A kvantumcsatornák szuperaktiválási tulajdonságának vizsgálatára kifejlesztett algoritmusunk segítségével, a gyakorlati átvitel során alkalmazott kvantumcsatornák információelméleti tulajdonságai, illetve az azokkal kapcsolatos nyitott kérdések analizálhatóak. A kidolgozott geometriai eljárásom segítségével, a Ph.D disszertációmban választ adtam a zéró-kapacitású kvantumcsatornákon keresztüli információátvitel megvalósításához szükséges feltételek hatékony feltárására.

A kvantumcsatorna kapacitását leíró kvantum-információelméleti gömb sugarának meghatározásához, a kvantumállapotok közti információelméleti távolságot alkalmaztam (*3. ábra*).



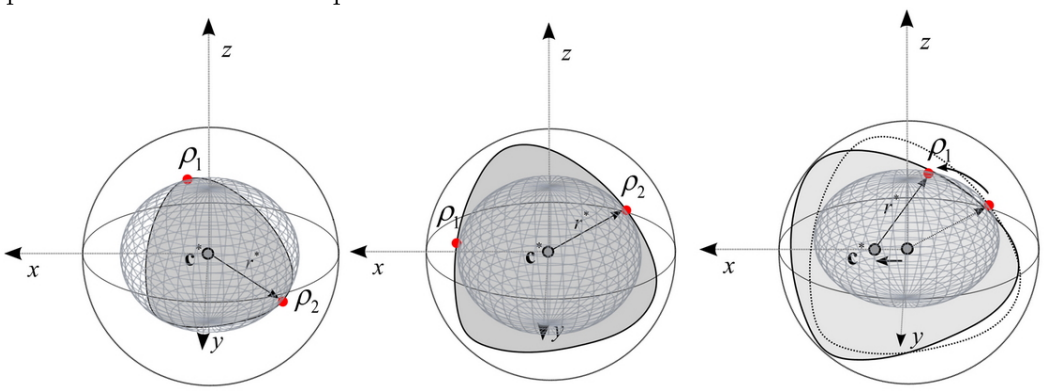
3. ábra. A csatornakapacitás leírható a kvantum-információs gömb segítségével. A torzult struktúra oka: nem alkalmazhatóak a hagyományos Euklideszi távolságok. [L. Gyongyosi, S. Imre: Informational Geometric Analysis of Superactivation of Zero-Capacity Optical Quantum Channels, SPIE Photonics West OPTO 2011, Advanced Quantum and Optoelectronic Applications, "Advances in Photonics of Quantum Computing, Memory, and Communication IV", Section on Quantum Communication, Jan. 2011, San Francisco, California, USA.]

A kvantumcsatornák szuperaktiválási lehetőségeinek vizsgálata során igazoltam a minimális entrópiájú kimeneti kvantumállapotok, valamint a szuperaktivált csatornakapacitás közti matematikai kapcsolatot. Elemeztem a kapcsolat jellemzőit különböző csatornamodellek esetén. A doktori munka keretében hatékony algoritmikus megoldást dolgoztam ki a szuperaktiválható kvantumcsatornák felderítésére (*4. ábra*).



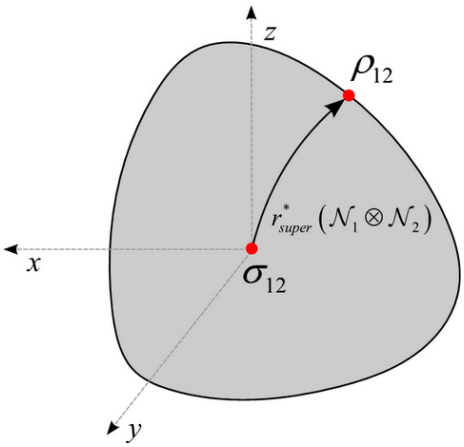
4. ábra. A kidolgozott algoritmus több iterációt hajt végre az optimális kimeneti kvantumállapot, valamint a kvantum-információs gömb meghatározásához. Ezen esetek egyike sem felel meg az algoritmussal szemben támasztott követelményeknek.

A hagyományos Euklideszi értelemben vett távolságszámítási metrikák nem alkalmazhatóak a kvantumállapotok közötti kvantum-információelméleti távolságok meghatározására, így ezen algoritmikus geometriai algoritmusok optimalizálását a kvantum-információelméleti térben hajtottam végre. A kidolgozott módszer segítségével nagy hatékonysággal határozhatóak meg a kimeneti kvantumállapotok közötti kvantum-információelméleti távolságok (*5. ábra*), valamint a csatornakombinációk szuperaktiválható csatornakapacitása.



5. ábra (a): Az iterációs lépések folytatásával az algoritmus meghatározza a kvantum-információelméleti gömböt. (b): az optimális megold (c) az átlagolt kvantumállapot módosításának hatása a kvantum-információelméleti gömb méretére.

A csatornakombinációk szuperaktiválhatóságának vizsgálatára bevezettem egy absztrakt információelméleti objektumot: a kvantum-információelméleti szupergömböt (*6.ábra*). ("*quantum superball*"), valamint igazoltam annak matematikai helyességét. A bevezetett geometriai struktúra a kombinált csatornastruktúra együttes szuperaktivált kapacitását határozza meg.



6. ábra. A szuperaktiválás kutatására kidolgozott absztrakt geometriai objektum: a "kvantum superball". [L. Gyongyosi, S. Imre: Information Geometric Superactivation of Zero-Capacity Quantum Channels, The Second International Conference on Quantum Information and Technology - New Trends in Quantum Information Technology (ICQIT2010), Quantum Information Science Theory Group (QIST), 2010, QIST, NII, Tokyo, Japan.]

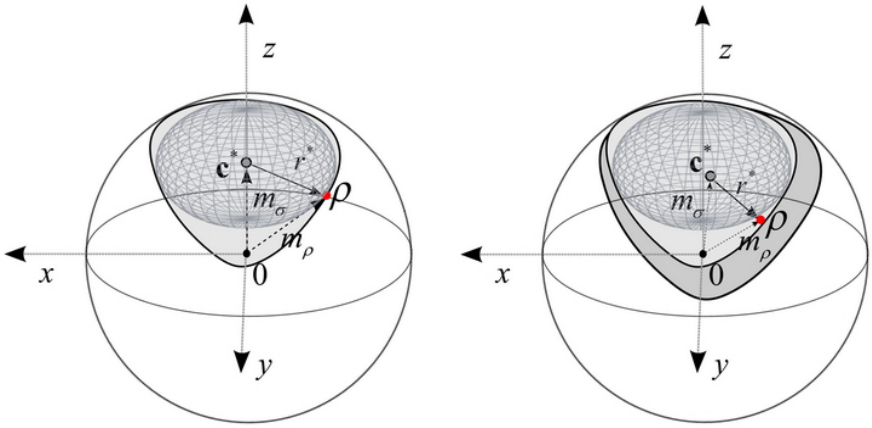
Második téziscsoport

A feltárt geometriai összefüggések segítségével a kvantumcsatornák szuperaktiválására hatékony információ-geometriai módszereket dolgoztam ki. Ezen eredményeket a 2. Téziscsoport tartalmazza.

2 Téziscsoport. *Definiáltam egy hatékony algoritmust a kvantumcsatornák kvantumkapacitásának szuperaktiválására.*

> **2.1. Tézis.** *Bebizonyítottam, a szuperaktiválható kvantumcsatorna kombinációk feltárása információ-geometriai eszközökkel végrehajtható [P1, P2, P7, B1, C11-C15], [Chapter 6, Appendix D, Appendix E, Appendix F, Appendix G].*
>
> **2.2. Tézis.** *Bebizonyítottam, hogy a felfedezett matematikai összefüggések felhasználhatóak hatékony információ-geometriai algoritmus konstruálására [P1, P2, P7, P9, B1, C11-C15], [Chapter 6, Appendix D, Appendix E, Appendix F, Appendix G].*
>
> **2.3. Tézis** *Definiáltam a szuperaktiválható kvantumkapacitással rendelkező kvantumcsatorna-kombinációk feltárásához szükséges algoritmust [P1, P2,P7, B1, C11-C15], [Chapter 6, Appendix D, Appendix E, Appendix F, Appendix G].*

A Ph.D disszertációban az optikai szálakkal megvalósított kvantumcsatornák szuperaktiválási lehetőségeit is kutattam (*7. ábra*). A vizsgálatok eredményeként megállapítottam, hogy a szuperaktiválás jelensége optikai kvantumcsatornákra is kiterjeszthető.



7. ábra. A kidolgozott geometriai eljárás segítségével, nagy hatékonysággal elemezhetőek az optikai kvantumcsatornák szuperaktiválásával kapcsolatos – jelenleg is tisztázatlan – problémák. [L. Gyongyosi, S. Imre: Information Geometrical Analysis of Additivity of Optical Quantum Channels, IEEE/OSA Journal of Optical Communications and Networking (JOCN), IEEE Photonics Society & Optical Society of America, ISSN: 1943-0620; 2010.]

A disszertációban igazoltam, hogy az információelméleti gömb sugarának meghatározására hatékony algoritmusok konstruálhatóak, a szuperaktiválás problémáját pedig a kvantumállapotok közti konvex burok meghatározására vezettem vissza.

A szuperaktiválható perfekt klasszikus kapacitással rendelkező csatornakombinációk felderítését hatékony információ-geometriai módszerrel hajtottam végre.

Harmadik téziscsoport

Az eredményeket kiterjesztettem a kvantumcsatornák klasszikus perfekt kapacitásának szuperaktiválására, amely probléma numerikus úton NP-teljes. A Ph.D disszertációmban adott megoldás polinom időben képes megtalálni a szuperkativálható klasszikus perfekt kapacitással rendelkező csatornákat. Ezen eredményeket a 3. Téziscsoport tartalmazza.

3. Téziscsoport. *Definiáltam egy polinomiális approximációra épülő információ geometriai algoritmust a kvantumcsatornák klasszikus perfekt kapacitás szuperaktiválhatóságának vizsgálatára. A módszer tetszőleges dimenziószámú kvantumcsatornák esetén alkalmazható, a numerikus módszerek esetében fennálló NP-teljesség nélkül.*

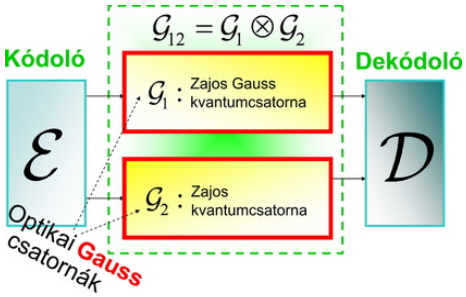
3.1. Tézis. *Bebizonyítottam, hogy a klasszikus perfekt kapacitás szuperaktiváláshoz szükséges peremfeltételek a kifejlesztett absztrakt geometriai struktúra segítségével feltárhatóak. [P3, B1, C1-C10], [Chapter 7, Appendix D, Appendix E, Appendix F, Appendix G].*

3.2. Tézis. *Bebizonyítottam, hogy a kifejlesztett információ-geometriai alapokra épülő polinomiális approximációs algoritmus minimális hiba mellett képes a tetszőleges dimenziószámú kvantumcsatornákat tartalmazó kombinált struktúra*

szuperaktiválható csatornakapacitásának meghatározására [P3, B1, C1-C10], [Chapter 7, Appendix D, Appendix E, Appendix F, Appendix G].

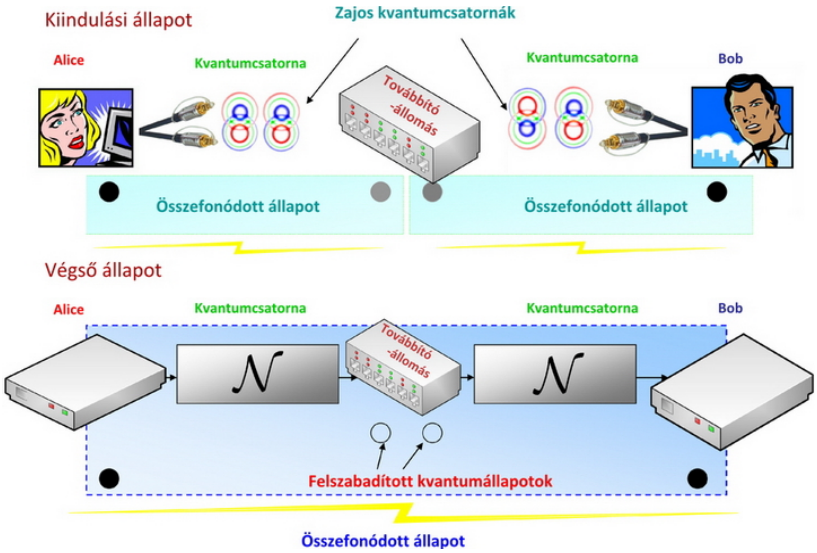
3.3. Tézis. *Bebizonyítottam, hogy a bemeneti sűrűségmátrixok algoritmikus előszűrésével, valamint hatékony információ-geometriai megoldások alkalmazásával, a tetszőleges kvantumcsatornákból álló kombinált csatornastruktúra klasszikus perfekt csatornakapacitásának szuperaktiválása polinomiális komplexitás mellett végrehajtható [P3, B1, C1-C10], [Chapter 7, Appendix D, Appendix E, Appendix F, Appendix G].*

A tökéletes információátvitel szuperaktiválásával forradalmi lehetőségek nyílhatnak meg a jövő kvantum-kommunikációs rendszereiben. A kvantum-repeaterek („kvantum-jelismétlők") tervezése és kifejlesztése alapvető fontosságú a jövő telekommunikációs hálózatainak hatékonysága szempontjából. A kvantum-jelismétlők nem valósíthatóak meg a hagyományos, klasszikus-jelismétlők esetében alkalmazott módszerekkel, ugyanis a kvantumállapotok nem másolhatóak, többszörözhetőek.
A kidolgozott metódusom segítségével megmutattam, hogy zajos, önmagában tökéletes információátvitelre alkalmatlan optikai Gauss kvantumcsatornák is szuperaktiválhatóak (*8. ábra*). A tökéletes információátvitel így az egyes kvantumcsatornák zajától függetlenül is megvalósítható.



8. ábra. Optikai Gauss kvantumcsatornák tökéletes információátvitelre. Önmagukban a kvantumcsatornák egyike sem képes tökéletes információátvitelre, a kombinált kapacitás azonban szuperaktiválható.

A megoldásunk forradalmasíthatja a jövő tele-kommunikációs hálózatainak kommunikációját. A kvantum-jelismétlők összefonódott állapotok, valamint a kvantum-teleportációs algoritmus segítségével kommunikálnak egymással. A jelenlegi megoldások kritikus része az összefonódott állapotok megosztása. A bázisállomások közti állapotmegosztás költséges és erőforrás igényes feladat. A zajos kvantumcsatornákon keresztül megosztott kvantumállapotok sérültek, zajosak (*9. ábra*).

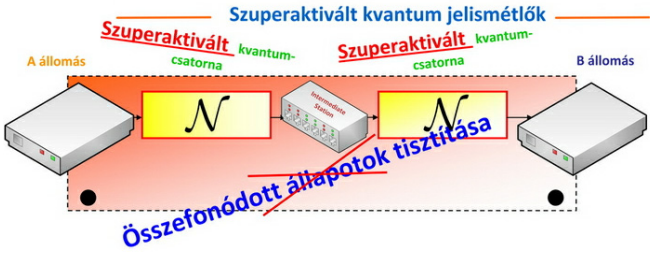


9. ábra. A kvantum-jelismétlők működési elve. A kommunikáció a bázisállomások között megosztott összefonódott állapotokra épül. [L. Gyongyosi, S. Imre: Efficient Quantum Repeaters without Entanglement Purification, International Conference on Quantum Information (ICQI) 2011, (The Optical Society of America (OSA), University of Rochester), Jun. 2011, University of Ottawa, Ottawa, Canada.]

Megállapítottam, hogy a jelenlegi megoldások kritikus része az összefonódott állapotok tisztása, ami nagyon erőforrás- és számításigényes feladat, a tisztítás sikervalószínűsége pedig a bementi állapotok sérülésének mértékétől függ (valószínűségi működés).

3 Implementáció és gyakorlati felhasználás

A doktori munka keretén belül javaslatot tettem a napjainkban ismert kvantum-jelismétlők működési mechanizmusának, illetve azok strukturális felépítésének módosításaira, amely módosításnak köszönhetően nagyságrendekkel hatékonyabb kommunikáció valósítható meg a jövő kvantum-kommunikációs hálózataiban.
A Ph.D disszertációmban definiáltam a „*szuperaktivált kvantum-jelismétlő*” fogalmát (*10. ábra*), valamint megadtam a kommunikáció információelméleti leírását és a jelismétlő architektúrális jellemzőit.



10. ábra. Szuperaktivált kvantum-jelismétlők. [L. Gyongyosi, S. Imre: Efficient Quantum Repeaters without Entanglement Purification, International Conference on Quantum Information (ICQI) 2011, (The Optical Society of America (OSA), University of Rochester), Jun. 2011, University of Ottawa, Ottawa, Canada.]

Kutattam a gyakorlati implementációk aktuális helyzetét is, amelynek eredményeképpen a következő megállapítást tettem. Annak ellenére, hogy a jelentős kutatási erőfeszítéseket tettek és néhány számos optikai szálas kísérleti összeköttetést is létrehoztak a gyakorlati implementációk megvalósítása terén, a hatékony, nagysebességű, nagytávolságú és flexibilis kvantumkommunikációs hálózat optimális megoldására számos kérdés még tisztázatlan. A kidolgozott eredmények felhasználásával lehetőség nyílt arra, hogy különféle kommunikációs eljárásokat vizsgáljunk, és a jelenlegieknél kedvezőbb megoldásokat találjunk. Az elméleti vizsgálatok eredményeit a későbbiekben laboratóriumban és valós hálózati körülmények között lehet ellenőrizni. A kvantum-repeaterek („kvantum-jelismétlők") tervezése és kifejlesztése alapvető fontosságú a jövő telekommunikációs hálózatainak működése szempontjából, - nélkülük ugyanis nem valósítható meg nagytávolságú információ átvitel a jövő kvantum-kommunikációs hálózataiban. Ugyanakkor, a kvantum-repeaterek nem valósíthatóak meg a hagyományos klasszikus jelismétlők esetében alkalmazott módszerekkel, mivel a kvantumállapotok nem másolhatóak, többszörözhetőek.

A későbbiekben tervezzük, hogy az elméleti kutatások eredményeként kapott szuperaktivációs technikák közül a passzív elemekkel megvalósíthatót megoldást a rendelkezésünkre álló laboratóriumban is demonstráljuk.

4 További kutatási eredmények

A Ph.D disszertációban bemutatott eredményeken túlmenően, a kvantumcsatornák kapacitás-visszaállításának kérdését kiterjesztettem a kvantumcsatornák *klasszikus* kapacitására, amely *jelentős elméleti áttörést* jelent a kvantumcsatornákon keresztüli információátvitel valódi információelméleti háttérének megismerése szempontjából. Kidolgoztam a zéró-kapacitású kvantumcsatornákon keresztüli klasszikus információátvitel megvalósításához szükséges elméleti modellt és igazoltam annak információelméleti helyességét.
Bevezettem egy új kvantum-kódolási eljárást, amellyel a szuperaktiválással egyenértékű eredmények érhetőek el. A módszer előnye, hogy a kvantumcsatornák kapacitás visszaállíthatósága a szuperaktiválás jelenségének eléréséhez szükséges kötöttségek és speciális peremfeltételek nélkül is megvalósítható. A módszer, - összehasonlítva a hagyományos szuperaktiválással - nagyságrendekkel hatékonyabb megoldást nyújt a kvantumcsatornák kapacitásának visszaállítására és erősítésére. A kidolgozott eljárásom neve *poláraktiválás*. A poláraktiválás segítségével tetszőleges, zéró kommunikációs kapacitással rendelkező kvantumcsatornák használhatóak információátvitelre, a módszer pedig – a gyakorlati megvalósítás szempontjából releváns - optikai kvantumcsatorna-modellek esetében is alkalmazható. A munka keretén belül kidolgoztam a poláraktiválás jelenségének eléréséhez szükséges matematikai hátteret, igazoltam annak információelméleti helyességét, valamint bizonyítottam a kidolgozott módszerünk hatékonyságát és alkalmazhatóságát. Megadtam a poláraktiválás eléréséhez szükséges csatornakódolási eljárást is, valamint javaslatot tettünk annak alkalmazhatóságára a jövő telekommunikációs rendszereiben.

A kvantumtitkosítás, kvantum-jelismétlők, valamint a kvantum-kommunikációs protokollok alapvető építőköve a *kvantum-összefonódottság*. Az összefonódottság átvitele és megosztása azonban problematikus, hiszen rendkívül érzékeny a kommunikációs csatorna zajára. A gyakorlatban a kommunikációs csatornák zajosak, az összefonódottság megőrzése pedig nehéz feladat. A megoldást az ideális, közel zajmentes kommunikációs csatornák jelentenék, ennek elérésére azonban a gyakorlatban nincs lehetőség. Bebizonyítottam, hogy a távoli pontok közti összefonódottság-megosztás megvalósítható a kvantum-összefonódottság tényleges átvitele nélkül. Bebizonyítottam, hogy a kvantum-összefonódottság klasszikus korrelációból is előállítható, - összefonódottság átvitelére önmagában alkalmatlan kommunikációs csatornák zaj-transzformációjának segítségével. A felfedezett jelenségnek a „korreláció konverzió" (*Correlation Conversion property – CC-property*) elnevezést adtam. Bebizonyítottam, hogy léteznek olyan kvantumcsatornák, amelyek rendelkeznek a CC-tulajdonsággal, és azok zaj-karakterisztikája önmagában alkalmas a távoli pontok közti összefonódottság-generálás végrehajtására.

Az eredmény új dimenziókat nyithat a jövő telekommunikációs hálózataiban, valamint jelentősen csökkenti a kvantum-kommunikációs hálózatok kialakításának költségeit.

Köszönetnyilvánítás

Köszönöm konzulensem, Prof. Dr. Imre Sándor támogatását. Szeretném megköszönni a Ph.D disszertáció bírálóinak a részletes és a Ph.D. disszertáció szakmai színvonalának növelését célzó észrevételeit, megjegyzéseit. Köszönöm a Magyar Tudományos Akadémia, Csibi Sándor ösztöndíj, TAMOP-4.2.1/B-09/1/KMR-2010-0002, 4.2.2.B-10/1--2010-0009, valamint a COST Action MP1006 támogatását.

5 Kutatási eredmények

A Ph.D kutatások eredményét lektorált külföldi folyóiratcikkek, konferencia kiadványok, könyvfejezetek, könyv és monográfiák formájában publikáltam.

Folyóirat publikációk

[P1] **Laszlo Gyongyosi**, Sandor Imre, "Algorithmic Superactivation of Asymptotic Quantum Capacity of Zero-Capacity Quantum Channels", Information Sciences, ELSEVIER, ISSN: 0020-0255; (Impact Factor: 3.28); (2011).

[P2] **Laszlo Gyongyosi**, Sandor Imre: Long-Distance Quantum Communications with Superactivated Gaussian Optical Quantum

Channels, SPIE Optical Engineering, ISSN: 0091-3286, E-ISSN: 1560-2303; USA, 2011. (Impact Factor: 0.9)

[P3] **Laszlo Gyongyosi**, Sandor Imre: Information Geometric Superactivation of Classical Zero-Error Capacity of Quantum Channels, Progress in Informatics, Quantum Information Technology, Quantum Information Science Theory Group, National Institute of Informatics, Tokyo, Japan, Print ISSN : 1349-8614, Online ISSN : 1349-8606; 2011.

[P4] **Laszlo Gyongyosi**, Sandor Imre: Algorithmical Analysis of Information-Theoretic Aspects of Secure Communication over Optical-Fiber Quantum Channels, Journal of Optical and Fiber Communications Research, Springer New York, ISSN 1867-3007 (Print) 1619-8638 (Online); 2010.

[P5] Sandor Imre, **Laszlo Gyongyosi**: Quantum-assisted and Quantum-based Solutions in Wireless Systems, with Lajos Hanzo, Harald Haas, Dominic O'Brien and Markus Rupp, in: "Wireless Myths, Realities and Futures: From 3G/4G to Optical and Quantum Wireless", Proceedings of the IEEE, Issue: Special Centennial Issue (100th Year Anniversary Celebration Volume of the Proceedings of the IEEE), ISSN: 0018-9219. (Impact Factor: 5.151, IEEE Highest), 2012.

[P6] Sandor Imre, **Laszlo Gyongyosi**: Introduction to Quantum-assisted and Quantum-based Solutions, with Lajos Hanzo, Harald Haas, Dominic O'Brien and Markus Rupp, in: "Prolog to the Section on Wireless Communications Technology", Proceedings of the IEEE, Issue: Special Centennial Issue (100th Year Anniversary Celebration Volume of the Proceedings of the IEEE), ISSN: 0018-9219. (Impact Factor: 5.151, IEEE Highest), 2012.

[P7] **Laszlo Gyongyosi**, Sandor Imre: Information Geometric Security Analysis of Differential Phase Shift Quantum Key Distribution Protocol, Security and Communication Networks, John Wiley & Sons, Ltd. ISSN: 1939-0114; 2010.

[P8] **Laszlo Gyongyosi**, Sandor Imre: Informational Geometric Analysis of Superactivation of Asymptotic Quantum Capacity of Zero-Capacity Optical Quantum Channels, Proceedings of SPIE Photonics West OPTO 2011, ISBN: 9780819484857, Vol: 7948.

[P9] **Laszlo Gyongyosi**, Sandor Imre: Superactivation of Quantum Channels is Limited by the Quantum Relative Entropy Function, Quantum Information Processing, Springer, ISSN: 1570-0755 (print version), ISSN: 1573-1332 (electronic version). 2012.

[P10] **Laszlo Gyongyosi**, Sandor Imre: Quasi-Superactivation of Classical Capacity of Zero-Capacity Quantum Channels, Journal of Modern

Optics, Taylor & Francis, 0950-0340 (Print), 1362-3044 (Online). 2012.

[P11] **Laszlo Gyongyosi**, Sandor Imre: Information Geometric Solution to Additivity of Amplitude-Damping Quantum Channel, AIP Conference Proceedings of QCMC 2010, American Institute of Physics, AIP Conference Proceedings Series (Library of Congress), 2011.

[P12] **Laszlo Gyongyosi**, Sandor Imre: Novel Quantum Information Solution to Copy-Protection and Secured Authentication, International Journal of Internet Technology and Secured Transactions (IJITST), ISSN (Online): 1748-5703, ISSN (Print): 1748-569X; 2011.

[P13] **Laszlo Gyongyosi**, Sandor Imre: Capacity Recovery of Very Noisy Optical Quantum Channels, International Journal of Applied Mathematics and Informatics, University Press, ISSN: 2074-1278, United Kingdom; 2011.

[P14] **Laszlo Gyongyosi**, Sandor Imre, Information Geometrical Analysis of Additivity of Optical Quantum Channels, IEEE/OSA Journal of Optical Communications and Networking (JOCN), IEEE Photonics Society & Optical Society of America, ISSN: 1943-0620; (2010). (Impact Factor: 1.2)

[P15] **Laszlo Gyongyosi**, Sandor Imre: Quantum Singular Value Decomposition Based Approximation Algorithm, Journal of Circuits, Systems, and Computers (JCSC), World Scientific, Print ISSN: 0218-1266, Online ISSN: 1793-6454; 2010.

[P16] **Laszlo Gyongyosi**, Sandor Imre: Quantum Informational Divergence in Quantum Channel Security Analysis, International Journal of Network Security, ISSN 1816-353X, ISSN 1816-3548; 2011.

[P17] **Laszlo Gyongyosi**, Sandor Imre: Efficient Computational Information Geometric Analysis of Physically Allowed Quantum Cloning Attacks for Quantum Key Distribution Protocols, WSEAS Transactions on Communications, ISSN: 1109-2742; 2010.

[P18] **Laszlo Gyongyosi**, Sandor Imre: Information Geometrical Approximation of Quantum Channel Security, International Journal on Advances in Security, Published by: International Academy, Research and Industry Association, ISSN: 1942-2636; 2010.

[P19] **Laszlo Gyongyosi**, Sandor Imre: Geometrical Estimation of Information Theoretical Impacts of Incoherent Attacks for Quantum Cryptography, International Review of PHYSICS, Print ISSN: 1971 - 680X; 2010.

[P20] **Laszlo Gyongyosi**, Sandor Imre: Quantum Information Theoretical Based Geometrical Representation of Eavesdropping Activity on the

Quantum Channel, Infocommunications Journal, Scientific Association for Infocommunications, ISSN 0018-2028; 2010.

[P21] **Laszlo Gyongyosi**, Sandor Imre: Quantum Protected Software, International Review on Computers and Software, ISSN:1828-6003, 1828-6011; 2009.

[P22] **Laszlo Gyongyosi**, Sandor Imre: Quantum cryptography based info-communication systems, Info-Communications Technology, Scientific Association for Infocommunications, BUTE, Faculty of Electrical Engineering and Informatics, Department of Telecommunications, 2008. ISSN 0018-2028; (**BEST PAPER AWARD 2009 - "POLLAK-VIRAG" - from the Scientific Association for Infocommunication, Hungary**).

[P23] **Laszlo Gyongyosi**: Quantum information in data privacy, Alma Mater series, Studies on Information and Knowledge Processes: Open Data, Protected Data 2, pages 341–378., BUTE, Faculty of Economic and Social Sciences, ISSN 1587-2386, ISBN 798-963-87788-5-7; 2008.

[P24] Sandor Szabo, **Laszlo Gyongyosi**, Sandor Imre, 'Performance Evaluation of Anycast-Based Micro-mobility Management', Int. J. of Mobile Network Design and Innovation (IJMNDI).

[P25] **Laszlo Gyongyosi**: TOR and Torpark: Functional and performance analyses of new generation anonymous browsers, Alma Mater series, Studies on Information and Knowledge Processes 11, pages 159-191., BUTE, Faculty of Economic and Social Sciences, 2007. ISSN 1587-2386, ISBN-10 963-421-429-0, ISBN-13 987-963-421-429-8. Published on-line: Hungarian privacy Enhancing Technologies portal.

Könyv

[B1] Sandor Imre and **Laszlo Gyongyosi**: Advanced Quantum Communications - An Engineering Approach, Publisher: Wiley-IEEE Press (New Jersey, USA), John Wiley & Sons, Inc., The Institute of Electrical and Electronics Engineers. (2012).

Könyvfejezet

[B2] **Laszlo Gyongyosi**, Sandor Imre: Quantum Mechanics based Communications, Research University series, Budapest University of Technology and Economics, 2012.

[B3] **Laszlo Gyongyosi**, Sandor Imre: Quantum Cryptographic Protocols and Quantum Security, in "Cryptography: Protocols, Design and Applications", Nova Science Publishers, (New York, USA), 2012.

[B4] **Laszlo Gyongyosi**, Sandor Imre: Secure Long-Distance Quantum Communication over Noisy Optical Fiber Quantum Channels, in "Optical Fibers", INTECH, ISBN 978-953-307-922-6; 2011.

[B5] **Laszlo Gyongyosi**, Sandor Imre: Quantum Cellular Automata Controlled Self-Organizing Networks, in "Cellular Automata", INTECH, ISBN 978-953-7619-X-X; 2010.

[B6] Laszlo Bacsardi, **Laszlo Gyongyosi**, Marton Berces, Sandor Imre: Quantum Solutions for Future Space Communication, in "Quantum Computers", Nova Science Publishers, 2010.

[B7] Sandor Szabo, **Laszlo Gyongyosi**, Karoly Lendvai, Sandor Imre: Overview of IP Multimedia Subsystem Protocols and Communication Services, in "Advanced Communication Protocol Technologies: Solutions, Methods and Applications", 2010.

Konferencia publikációk

[C1] **Laszlo Gyongyosi**, Sandor Imre: Superactivated Quantum Repeaters, Quantum Information Processing 2012 (QIP2012), Dec. 2011, University of Montreal, Quebec, Canada (**PHD GRANT AWARD OF QIP2012, UNIVERSITY OF MONTREAL**).

[C2] **Laszlo Gyongyosi**, Sandor Imre: On-the-Fly Quantum Error-Correction for Space-Earth Quantum Communication Channels, First NASA Quantum Future Technologies Conference (QFT 2012), Jan. 2012, Quantum Laboratory, Center for Applied Physics, NASA Ames Research Center, Moffett Field, California, USA.

[C3] **Laszlo Gyongyosi**, Sandor Imre: Pilot Quantum Error-Correction for Noisy Quantum Channels, Second International Conference on Quantum Error Correction (QEC11), Dec. 2011, University of Southern California, Los Angeles, USA (**PHD GRANT AWARD OF QEC2011, UNIVERSITY OF SOUTHERN CALIFORNIA**).

[C4] **Laszlo Gyongyosi**, Sandor Imre: Noisy Gaussian Quantum Channels with Superactivated Zero-Error Quantum Capacity, Frontiers in Quantum Information, Computing & Communication (QICC)-2011 Meeting, 'Quantum Systems to Qubits, Optics & Semiconductors', Sept. 2011, Massachusetts Institute of Technology (MIT), Cambridge, Massachusetts, USA.

[C5] **Laszlo Gyongyosi**, Sandor Imre: Classical and Quantum Communication with Superactivated Quantum Channels, PhD Workshop, TAMOP-4.2.2/B-10/1-2010-0009, March. 2012, Doctoral School on Computer Science and Information Technologies, Budapest University of Technology and Economics.

[C6] **Laszlo Gyongyosi**, Sandor Imre: Zero-Error Transmission of Classical Information over Superactivated Optical Quantum Channels, International Conference on Quantum, Atomic, Molecular and Plasma Physics, Section on Quantum Information and Computing, Sept. 2011., Clarendon Laboratory, University of Oxford, Oxford, United Kingdom.

[C7] **Laszlo Gyongyosi**, Sandor Imre: High Performance Quantum Repeaters with Superactivated Gaussian Quantum Channels, IONS North America, IONS-NA-3, (Stanford Optical Society, Stanford Photonics Research Center), Oct. 2011, Stanford University, Stanford, California, USA (**PHD GRANT AWARD OF STANFORD UNIVERSITY, STANFORD OPTICAL SOCIETY**).

[C8] **Laszlo Gyongyosi**, Sandor Imre: Perfect Quantum Communication with Very Noisy Gaussian Optical Fiber Channels, Frontiers in Optics (FiO) 2011, OSA's 95th Annual Meeting, Section on Quantum Computation and Communication, (American Physical Society, Optical Society of America) Oct. 2011, San Jose, California, USA.

[C9] **Laszlo Gyongyosi**, Sandor Imre: Efficient Quantum Repeaters without Entanglement Purification, International Conference on Quantum Information (ICQI) 2011, (The Optical Society of America (OSA), University of Rochester), Jun. 2011, University of Ottawa, Ottawa, Canada.

[C10] **Laszlo Gyongyosi**, Sandor Imre: Channel Capacity Restoration of Noisy Optical Quantum Channels, ICOAA '11 Conference, Section on Optical Quantum Communications, Febr. 2011, University of Cambridge, Cambridge, United Kingdom.

[C11] **Laszlo Gyongyosi**, Sandor Imre: Informational Geometric Analysis of Superactivation of Zero-Capacity Optical Quantum Channels, SPIE Photonics West OPTO 2011, Advanced Quantum and Optoelectronic Applications, "Advances in Photonics of Quantum Computing, Memory, and Communication IV", Section on Quantum Communication, Jan. 2011, The Moscone Center, San Francisco, California, USA.

[C12] **Laszlo Gyongyosi**, Sandor Imre: Algorithmic Solution to Superactivation of Zero-Capacity Optical Quantum Channels, Photonics Global Conference (PGC) 2010, Nanyang Technological University, IEEE Photonics Society, 2010, Suntec City, Singapore.

[C13] **Laszlo Gyongyosi**, Sandor Imre: Information Geometric Superactivation of Zero-Capacity Quantum Channels, The Second International Conference on Quantum Information and Technology - New Trends in Quantum Information Technology (ICQIT2010), Quantum Information Science Theory Group (QIST), National Insti-

tute of Informatics (NII), National Institute of Information and Communications Technology (NICT), 2010, QIST, NII, Tokyo, Japan.

[C14] **Laszlo Gyongyosi**, Sandor Imre: Capacity Recovery of Useless Photonic Quantum Communication Channels, ALS Conference, 2010, Lawrence Berkeley National Laboratory (Berkeley Lab), University of California, Berkeley, California, USA.

[C15] **Laszlo Gyongyosi**, Sandor Imre: Method for Discovering of Superactive Zero-Capacity Optical Quantum Channels, IONS-NA Conference, 2010, University of Arizona, Tucson (Arizona), USA. (**PHD GRANT AWARD OF UNIVERSITY OF ARIZONA, USA**).

[C16] **Laszlo Gyongyosi**, Sandor Imre: Information Geometrical Solution to Additivity of Non-Unital Quantum Channels, QCMC 2010, 10th Quantum Communication, Measurement & Computing Conference, Section on Quantum Computing and Quantum Information Theory (Centre for Quantum Computer Technology) July 2010, University of Queensland, Brisbane, Queensland, Australia.

[C17] **Laszlo Gyongyosi**, Sandor Imre: Computational Information Geometric Analysis of Quantum Channel Additivity, Photon10 Conference, Quantum Electronics Group (QEP-19), Section on Quantum information, University of Southampton, Institute of Physics (IOP) Optics and Photonics Division, 2010, University of Southampton, Southampton, UK.

[C18] **Laszlo Gyongyosi**, Sandor Imre: Novel Geometrical Solution to Additivity Problem of Classical Quantum Channel Capacity, The 33rd IEEE Sarnoff Symposium - 2010, IEEE Princeton/Central Jersey Section, Apr. 2010, Princeton University, Princeton, New Jersey, USA.

[C19] **Laszlo Gyongyosi**, Sandor Imre: Computational Geometric Analysis of Physically Allowed Quantum Cloning Transformations for Quantum Cryptography, International Conference on Computer Engineering and Applications, Section on Quantum Computing, (CEA '10), 2010, University of Harvard, Cambridge (Massachusetts), USA. (**BEST PAPER AWARD 2010, HARVARD UNIVERSITY, CAMBRIDGE, USA.**)

[C20] **Laszlo Gyongyosi**, Sandor Imre: Quantum Informational Geometry for Secret Quantum Communication, The First International Conference on Future Computational Technologies and Applications, FUTURE COMPUTING 2009, Section on Quantum Computing, International Academy, Research and Industry Association, 2009,

Athens, Greece. (**FUTURE COMPUTING 2009: BEST PAPER AWARD**).

[C21] Laszlo Bacsardi, **Laszlo Gyongyosi**, Sandor Imre: Using Redundancy-free Quantum Channels for Improving the Satellite Communication, PSATS 2010, 2nd International ICST Conference on Personal Satellite Services, Section on Satellite Quantum Communications, 4-6 February 2010, Rome, Italy. In: Lecture Notes of The Institute for Computer Sciences Social-Informatics and Telecommunications Engineering (ISSN: 1867-8211) (2010).

[C22] **Laszlo Gyongyosi**, Laszlo Bacsardi, Sandor Imre: Novel Approach for Quantum Mechanical Based Autonomic Communication, The First International Conference on Future Computational Technologies and Applications, FUTURE COMPUTING 2009, Section on Quantum Computing, International Academy, Research and Industry Association, 2009., Athens, Greece.

[C23] Laszlo Bacsardi, **Laszlo Gyongyosi**, Sandor Imre: Solutions For Redundancy-free Error Correction In Quantum Channel, International Conference on Quantum Communication and Quantum Networking, October 26 – 30, 2009, Vico Equense, Sorrento peninsula, Naples, Italy.

[C24] **Laszlo Gyongyosi**, Sandor Imre: Quantum Divergence based Quantum Channel Security Estimation, N2S'2009 International Conference on Network and Service Security, Section on Quantum Cryptography and QKD, IFIP TC6 WG, IEEE France, June, 2009. Paris, France.

[C25] **Laszlo Gyongyosi**, Sandor Imre: Unduplicable Quantum Data Medium Based Secret Decryption and Verification, The 4th International Conference for Internet Technology and Secured Transactions (ICITST-2009), November 9-12, 2009, IEEE UK & RI, London, United Kingdom.

[C26] **Laszlo Gyongyosi**, Sandor Imre: Fidelity Analysis of Quantum Cloning Attacks in Quantum Cryptography, ConTEL 2009 International Conference on Telecommunications, IEEE Communications Society, 2009. Zagreb, Croatia.

[C27] **Laszlo Gyongyosi**: Really unbreakable? The Security Analysis of Quantum Cryptography, Hacktivity conference 2008, Budapest.

[C28] **Laszlo Gyongyosi**, Sandor Imre: Polaractivation of Quantum Channels, The 11th International Conference on Quantum Communication, Measurement and Computing (QCMC 2012), Section on Quantum Information and Communication Theory, 30

July - 3 August 2012, Vienna University of Technology, Vienna, Austria.

[C29] **Laszlo Gyongyosi**, Sandor Imre: Quantum Polar Coding for Probabilistic Quantum Relay Channels, The 11th International Conference on Quantum Communication, Measurement and Computing (QCMC 2012), Section on Quantum Information and Communication Theory, 30 July - 3 August 2012, Vienna University of Technology, Vienna, Austria.

[C30] **Laszlo Gyongyosi**, Sandor Imre: On the Mathematical Boundaries of Communication with Zero-Capacity Quantum Channels, The Alan Turing Centenary Conference (Turing-100), June 22-25, 2012, University of Manchester, Manchester, United Kingdom.

[C31] **Laszlo Gyongyosi**, Sandor Imre: Secure Communication over Zero Private-Capacity Quantum Channels, The Alan Turing Centenary Conference (Turing-100), June 22-25, 2012, University of Manchester, Manchester, United Kingdom.

[C32] **Laszlo Gyongyosi**, Sandor Imre: Quantum Polar Coding for Noisy Optical Quantum Channels, APS DAMOP 2012 Meeting, The 43rd Annual Meeting of the APS Division of Atomic, Molecular, and Optical Physics, (American Physical Society), Jun. 2012, Anaheim, California, USA. **(PHD GRANT AWARD OF APS DAMOP12, AMERICAN PHYSICAL SOCIETY, CALIFORNIA, USA)**.

[C33] **Laszlo Gyongyosi**, Sandor Imre: Classical Communication with Stimulated Emission over Zero-Capacity Optical Quantum Channels, APS DAMOP 2012 Meeting, The 43rd Annual Meeting of the APS Division of Atomic, Molecular, and Optical Physics, (American Physical Society), Jun. 2012, Anaheim, California, USA. **(PHD GRANT AWARD OF APS DAMOP12, AMERICAN PHYSICAL SOCIETY, CALIFORNIA, USA).**

[C34] **Laszlo Gyongyosi**, Sandor Imre: Private Classical Communication over Zero-Capacity Quantum Channels Using Quantum Polar Codes, The 7th Conference on Theory of Quantum Computation, Communication, and Cryptography (TQC 2012), Jun. 2012, The University of Tokyo, Tokyo, Japan.

[C35] **Laszlo Gyongyosi**, Sandor Imre: Classical Communication with Zero-Capacity Quantum Channels, The 7th Conference on Theory of Quantum Computation, Communication, and Cryptography (TQC 2012), Jun. 2012, The University of Tokyo, Tokyo, Japan.

Díjak

- SPIE Photonics West OPTO 2013 Award, Advances in Photonics of Quantum Computing, Memory, and Communication, San Francisco, California, USA
- Incubic/Milton Chang Award, The Optical Society of America, Rochester, New York, USA, 2012.
- BMe Kutatói Pályázat 2012, Budapesti Műszaki és Gazdaságtudományi Egyetem
- PhD Student Grant Award of Columbia University, New York, USA, 2012.
- PhD Student Grant Award of QCRYPT 2012, The 2nd Annual Conference on Quantum Cryptography (Centre for Quantum Technologies), National University of Singapore, Singapore, 2012.
- PhD Student Grant Award of APS DAMOP 2012 (DAMOP12), APS Division of Atomic, Molecular, and Optical Physics, American Physical Society (APS), California, USA, 2012.
- PhD Student Grant Award of Quantum Information Processing 2012 (QIP2012), University of Montreal, Canada
- PhD Student Grant Award of The Second International Conference on Quantum Error Correction (QEC2011), University of Southern California (USC), 2011, USA
- PhD Student Grant Award of Stanford University, Stanford Optical Society, 2011, USA
- Doktorjelölti Ösztöndíj 2011, BME Villamosmérnöki és Informatikai Kar
- BMe Kutatói Pályázat 2011, Budapesti Műszaki és Gazdaságtudományi Egyetem
- PhD Student Grant Award of University of Arizona, Optical Society of America (OSA), 2010, USA
- BMe Kutatói Pályázat 2010, Budapesti Műszaki és Gazdaságtudományi Egyetem
- CSIBI SÁNDOR ösztöndíj 2010, PhD Kutatói ösztöndíj, Pro Progressio, Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosmérnöki és Informatikai Kar
- BEST PAPER AWARD 2010, Harvard University, Cambridge, USA
- BEST PAPER AWARD 2009, FUTURE COMPUTING, The First International Conference on Future Computational Technologies and Applications, 2009.
- Pollák-Virág díj, Hírközlési és Informatikai Tudományos Egyesület, 2009.
- Köztársasági Ösztöndíj, Budapesti Műszaki és Gazdaságtudományi Egyetem

- Szakmai Kari BME ösztöndíj, BME Villamosmérnöki és Informatikai Kar, A kategória
- Egyetemi BME Ösztöndíj, Budapesti Műszaki és Gazdaságtudományi Egyetem, A kategória

Irodalomjegyzék

[**Ackermann08**] M. Ackermann, J. Blömer, and C. Sohler. Clustering for metric and non-metric distance measures. In *Proceedings of the 19th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA '08),* pages 799–808. Society for Industrial and Applied Mathematics, (2008).

[**Beigi07**] S. Beigi and P. W. Shor, On the Complexity of Computing Zero-Error and Holevo Capacity of Quantum Channels, arXiv:0709.2090 [quant-ph] (2007).

[**Brandao11**] F. G.S.L. Brandao, J. Oppenheim and S. Strelchuk, "When does noise increase the quantum capacity?", arXiv:1107.4385v1 [quant-ph] (2011).

[**Chen07**] K. Chen. On k-median and k-means clustering in metric and Euclidean spaces and their applications. Manuscript, available at:http://ews.uiuc.edu/~kechen/, (2007).

[**Cortese02**] J. Cortese, "The Holevo-Schumacher-Westmoreland Channel Capacity for a Class of Qudit Unital Channels", LANL ArXiV e-print quant-ph/0211093, (2002).

[**Cortese03**] J. Cortese, "Classical Communication over Quantum Channels". PhD Thesis by. John A. Cortese. California Institute of Technology (2003).

[**Cubitt09**] T. Cubitt, J. X. Chen, and A. Harrow, Superactivation of the Asymptotic Zero-Error Classical Capacity of a Quantum Channel, arXiv: 0906.2547. (2009).

[**Cubitt09a**] T. Cubitt, G. Smith, Super-Duper-Activation of Quantum Zero-Error Capacities, arXiv:0912.2737v1. (2009).

[**Cubitt10**] T. Cubitt, D. Leung, W. Matthews and A. Winter, Improving Zero-Error Classical Communication with Entanglement, Phys. Rev. Lett. 104, 230503, arXiv:0911.5300, (2010).

[**Devetak03**] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," IEEE Trans. Inf. Theory, vol. 51, pp. 44–55, arXiv:quant-ph/0304127, (2005).

[**Duan09**] R. Duan, Superactivation of zero-error capacity of noisy quantum channels.arXiv:0906.2527, (2009).

[**Feldman07**] D. Feldman, M. Monemizadeh, and C. Sohler. A PTAS for k-means clustering based on weak coresets. In Proceedings of the 23rd ACM Symposium on Computational Geometry (SCG'07), pages 11–18, (2007).

[**Grover96**] Grover L.K.: A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212

[**Hastings09**] M. Hastings, "A Counterexample to Additivity of Minimum Output Entropy" Nature Physics 5, 255, arXiv:0809.3972, (2009).

[**Hayashi03**] M. Hayashi and H. Nagaoka, "General formulas for capacity of classical-quantum channels," IEEE Transactions on Information Theory, Vol.49, No.7, pp.1753-1768 (2003).

[**Holevo98**] A. Holevo, "The capacity of the quantum channel with general signal states", IEEE Trans. Info. Theory 44, 269 - 273 (1998).

[**Imre05**] S. Imre, F. Balázs: Quantum Computing and Communications – An Engineering Approach, Published by John Wiley and Sons Ltd, (2005).

[**Imre12**] S. Imre, L. Gyongyosi: Advanced Quantum Communications – An Engineering Approach, Published by Wiley-IEEE Press, (2012).

[**Mosca06**] M. Mosca and D. Stebila. Uncloneable quantum money. In Canadian Quantum Information Students' Conference (CQISC) 2006, Calgary, Alberta, August 2006. url http://www.iqis.org/events/cqisc06/papers/Mon-1130-Stebila.pdf. (2006).

[**Lloyd97**] S. Lloyd, "Capacity of the noisy quantum channel," Phys. Rev. A, vol. 55, pp. 1613–1622, (1997).

[**Nielsen07**] F. Nielsen, J.-D. Boissonnat, and R. Nock. On Bregman Voronoi diagrams. *In Proceedings of the 18th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'07),* pages 746–755, Philadelphia, PA, USA, Society for Industrial and Applied Mathematics, (2007).

[**Nielsen07a**] F. Nielsen, J. D. Boissonnat, R. Nock, Bregman Voronoi Diagrams: Prop erties, arXiv:0709.2196v1, (2007).

[**Nielsen08b**] F. Nielsen, R. Nock: Quantum Voronoi Diagrams and Holevo Channel Capacity for 1-Qubit Quantum States, ISIT 2008, (2008).

[**Nielsen09**] F. Nielsen, R. Nock: Approximating Smallest Enclosing Balls with Application to Machine Learning, International Journal on Computational Geometry and Applications (IJCGA'09), (2009).

[**Ruskai01**] M. Ruskai, S. Szarek, and E. Werner, "An Analysis of Completely-Positive Trace Preserving Maps on 2 by 2 Matrices", LANL ArXiV e-print quant-ph/0101003, (2001).

[**Schumacher97**] B. Schumacher and M. Westmoreland, "Sending classical information via noisy quantum channels," Phys. Rev. A, vol. 56, no. 1, pp. 131–138, (1997).

[**Shannon48**] C. Shannon, „A mathematical theory of communication", Bell System Tech. J. 27, 379 - 423, 623 - 656 (1948).

[**Shor02**] P. Shor, "The quantum channel capacity and coherent information." lecture notes, MSRI Workshop on Quantum Computation, Available online at http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/. (2002).

[**Shor94**] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In Proc. 35th Ann. IEEE Symp. Foundations of Comp. Sci., pp. 124–134. IEEE Press, doi:10.1109/SFCS.1994.365700. eprint arXiv:quant-ph/9508027, (1994).

[**Smith08**] G. Smith, J. Yard, Quantum Communication with Zero-capacity Channels. Science 321, 1812-1815 (2008).

[**Smith09b**] G. Smith and J. A. Smolin, "Extensive Nonadditivity of Privacy," Physical Review Letters, vol. 103, no. 12, p. 120503, Sep. arXiv:0904.4050. (2009).

[**Smith11**] G. Smith, J. A. Smolin and J. Yard, Gaussian bosonic synergy: quantum communication via realistic channels of zero quantum capacity, arXiv:1102.4580v1, (2011).