MTA DOKTORI ÉRTEKEZÉS TÉZISEI

Nemlokális kvantumkorrelációk vizsgálata

Vértesi Tamás Ferenc

MTA Atommagkutató Intézet

Debrecen

2018

dc_1476_17

A kutatások előzménye

A huszadik század elején a kvantummechanika megalkotásával sikerült az atomok és a fotonok (fény részecskéinek) különös hullám-részecske viselkedését leírni. Az 1920-as években felfedezett kvantumelmélet egyenletei kitűnő pontossággal írják le mind a mikrovilág, mind pedig a makroszkópikus méretű kvantumrendszerek viselkedését. A kvantummechanika a legsikeresebb tudományos elméletek egyike, amely a természetben előforduló teljes energia- és méretskálát felöleli. Érvényességi köre a legkisebb energiáktól egészen a nukleáris energiákon zajló folyamatokig, illetve az atomi méretektől az egész univerzum méretéig terjed. Ezen első kvantummechanikai forradalomnak nevezett időszakban sikerült az elmélet keretein belül számos alapvető jelenséget leírni, amelyre a klasszikus fizika képtelen volt magyarázatot adni. Sikerült leírni a félvezetőkben folyó áramot, a fénysugarat alkotó milliárdnyi foton viselkedését, a szilárdtestek mechanikai tulajdonságait, és a szupravezetés különös jelenségére is sikerült fényt deríteni.

Ezzel párhuzamosan a kvantumfizikának számos más tudomány fejlődésében is meghatározó szerepe volt. Itt említhetjük a számítástudományt, amelynek sikere az elektronikai kapcsolókat megvalósító tranzisztorok működésén alapszik, vagy a Földünket behálózó kommunikációt, amelynél optikai szálak közvetítik nagy távolságokban a fotonokat, illetve a sugárzásmentes képfeldolgozás úttörő módszereit, amelyek forradalmasították az orvosi képalkotást.

Ezen átütő sikerek ellenére még mindig hiányzik a kvantummechanikának mély és intuitív megértése, amelyet a gyakran paradoxonok formájában felbukkanó új kvantumeffektusok felismerése is mutat. A kvantummechanika első ilyen látszólagos paradox megnyilvánulását az EPR-gondolatkísérletben írták le. 1935-ben Einstein, Podolsky és Rosen azt posztulálták [23], hogy a kvantumelmélet leszármaztatható egy ún. lokális elméletből, ahol bizonyos – kísérletileg hozzá nem férhető – rejtett paramétereket átlagolunk össze. Három évtizeddel később azonban John Bell megcáfolta ennek lehetőségét [8]: amennyiben elfogadjuk a kvantummechanika matematikai formalizmusát, Bell tételéből következően a kvantumelmélet helyes leírását célul kitűző bármely rejtett paraméteres elméletnek szükségszerűen nemlokálisnak kell lennie.

Bell nevezetes tételét – amelyet egyenlőtlenség formájában fogalmazott meg – azóta számos kísérlet egyre nagyobb és nagyobb pontossággal igazolta [5]. Az első ilyen Bell-kísérletet – amelyben még számos technikai kiskapu jelentkezett – 1982-ben Aspect és munkatársai végezték [6]. A kvantumtechnológia fejlődésének köszönhetően a közelmúltban végül sikerült minden lényeges kiskapu egyidejű zárásával igazolni a Bell-egyenlőtlenségek sérülését. Ezen kiskapumentes Bell-kísérletet pár éven belül számos fizikai platformon elvégezték: fotonokkal [60, 26], elektronspinekkel [30]

és atomokkal [57] is. Ezen kísérletek már meggyőzően bizonyították a kvantummechanika nemlokális tulajdonságát, vagyis azt, hogy a kvantumrendszerek távoli szeparált részein elvégzett mérések eredményei olyan korrelációkat mutatnak, amilyeneket semmiféle klasszikus mechanizmus nem eredményezhet, azaz mintha az egymástól nagy távolságban levő kvantumobjektumok összehangolnák hatásukat. Ez a részrendszerek között működő erős nemlokális kapocs adja a kulcsot a fenti kísérletekben megfigyelt Bell-egyenlőtlenségek sérüléséhez.

Ugyanakkor az utóbbi évtizedek elméleti vizsgálatainak köszönhetően kiderült, hogy a kvantumeffektusokon alapuló informatikai eszközök sokkal hatékonyabbak lehetnek klasszikus társaiknál. Így született meg a kvantuminformatika tudománya, amely felöleli a kvantumalgoritmusok, a kvantumkommunikációs bonyolultság, és a kvantumtitkosítás területeit [42]. Az egyik ilyen úttörő alkalmazás a kvantumos kulcskiosztás, amelyre Bennett és Brassard 1984-ben megalkotta az első lehallgatásmentes kvantumprotokollt [11], és amelynek biztonsága azon alapszik, hogy a kvantumbitek (qubitek) nem klónozhatók [72]. Vagyis szemben a hagyományos kriptográfiai protokollokkal – ahol a biztonságot bizonyos matematikai műveletek bonyolultsága nyújtja – a kvantumos esetben a biztonság a kvantummechanika érvényességén alapul. Másik példaként a nagy számok faktorizálásának problémáját említem, amelyre Peter Shor találta meg 1994-ben az első hatékony (polinomrendű) kvantumalgoritmust [61], kiaknázva annak lehetőségét, hogy a kvantummechanika exponenciálisan sok különböző kvantumállapot egyidejű, egymással párhuzamosan történő időfejlődését is megengedi.

Célkitűzések

A kvantuminformatika tudományának fő célja a kvantummechanikai erőforrások hatékonyságának feltérképezése és minél jobb kiaknázása különböző számítási és kommunikációs feladatokban. Dolgozatomban ezen megközelítésből kiindulva egy különös kvantummechanikai erőforrást, az ún. Bell-nemlokális korrelációk erősségét térképezem fel. Túljutva a természet Bell-nemlokális tulajdonsága kérdésének az eldöntésén – amelyet a közelmúlt kísérletei már meggyőzően bizonyítottak – fő célom feltárni, hogy a kvantummechanika pontosan milyen mértékben mutat nemlokális viselkedést, és ezen nemlokális korrelációk milyen jellegű informatikai feladatokban válnak hasznosíthatóvá.

Az utóbbi néhány évben fogalmazódott meg, hogy a Bell-egyenlőtlenségek kísérletekben kapott sérülése nemcsak koncepcionális szempontból érdekes, de emellett egy gyökeresen új lehetőségét adja a kvantuminformatika megközelítésének. Ezen megközelítést a kvantuminformáció elmélet ún. eszközfüggetlen keretének nevezzük,

amelyben a protokollban szereplő kvantumeszközöket – a külvilág felé klasszikus bemenettel és klasszikus kimenettel rendelkező – fekete dobozoknak tekintjük. Ezen eszközfüggetlen keretben az egymás után elvégzett mérések statisztikájából származó valószínűségi eloszlásból, vagyis korrelációkból nyerünk információt a kvantumeszközökre vonatkozóan. Konkrétan két felhasználó esetén az egyedüli rendelkezésünkre álló kísérleti adat a $P(a,b|x,y)$ közös feltételes valószínűségi eloszlás, amely annak a valószínűségét adja meg, hogy a két kísérletező fél x és y bemenetei mellett az a, illetve b kimenetel adódik.

Az eszközfüggetlen keret egyik fontos alapproblémája, valamint a jelen dolgozat egyik fő célkitűzése is annak megértése, hogy a kvantumelmélet absztrakt objektumai, mint például a kvantumállapot, a mérési operátorok, illetve a kvantumrendszer dimenzionalitása milyen kényszereket írnak elő a $P(a,b|x,y)$ korrelációk halmazára. Másképpen fogalmazva: a kísérletből származó $P(a,b|x,y)$ statisztikai adatból tudunk-e valamilyen információt kinyerni a kvantumprotokollban szereplő eszköz működésének a részleteiről.

A kvantummechanika matematikai formalizmusából adódóan léteznek olyan extremális $P(a,b|x,y)$ korrelációk, amelyeket csak egyedi kvantumállapotokon végzett mérések tudnak előállítani. Például az egyik legismertebb Bell-egyenlőtlenség, a CHSH-Bell-egyenlőtlenség [19] maximális, $2\sqrt{2}$ mértékű sérüléséhez tartozó $P(a,b|x,y)$ korreláció a maximálisan összefonódott szinglett állapoton ható mérési operátorokkal érhető csak el. A fenti Bell-nemlokális korrelációk megfigyelésén alapulva olyan eszközfüggetlen kvantuminformatikai protokollok előállítása válik lehetővé, amelyek működésének helyessége ellenőrizhető, ha a protokollban szereplő egyes kvantumeszközök működése nem megbízható, vagy olyan felhasználó működteti az eszközt, akiben nem bízunk meg. A fenti elméleti eredmények szellemes alkalmazásai közé tartozik a hitelesített véletlenszámok előállítása [54, 20], vagy a tökéletesen lehallgatásmentes kvantumos kulcs kiosztása [1]. Ezen feladatok elvégzéséhez egy jól megkonstruált Bell-egyenlőtlenség adott mértékű sérülésének a kísérleti igazolása szükséges.

Dolgozatomban a fenti eszközfüggetlen nézőpontot szem előtt tartva térképezem fel a többrészű kvantumrendszerekből származó Bell-féle nemlokális kvantumkorrelációkat. E célból új, hatékony numerikus módszerek kifejlesztésében veszek részt, amelyeket változatos elrendezésekben használok fel. A dolgozatban részletesen a kétfelhasználós esetben elért eredményeket mutatom meg, de a módszerek és eredmények egy része átültethető, illetve könnyen általánosítható kettőnél több felhasználós esetekre is. Bízom benne, hogy a nemlokális korrelációk struktúrájának jobb megértése gyümölcsözőnek bizonyul az eszközfüggetlen kvantuminformatika gyökeresen új alkalmazásainak feltárásában.

Vizsgálati módszerek

A kvantumelmélet eszközfüggetlen megközelítésében a protokollban szereplő eszközöket egymással nem kommunikáló fekete dobozoknak tekintjük, amelyek a külvilág felé klasszikus bemenettel $(x_1, x_2, \ldots x_n)$ és klasszikus kimenettel $(a_1, a_2, \ldots, a_n)$ rendelkeznek. Az egyedüli rendelkezésünkre álló adat a kísérletből származó $P(a_1, a_2, \ldots a_n|x_1, x_2, \ldots, x_n)$ feltételes eloszlás, vagy más néven korreláció. Azt vizsgáljuk, hogy ezen kísérleti statisztikából milyen információt tudunk kinyerni az eszközök – mint fekete dobozok – működéséről. A dolgozatban megoldott egyik ilyen alapfeladat a kvantumrendszerek dimenziójának a becslése volt, vagyis a kinyert korrelációkból annak meghatározása, hogy a kísérletben szereplő fekete dobozok egyenként legalább hány qubit információt tárolnak. Eszközeink dimenzionalitását ezáltal erőforrásként tudjuk használni, hiszen egy kvantumrendszer dimenziója szoros kapcsolatban áll a vele potenciálisan megvalósítható kvantumalgoritmusok hatékonyságával. A fentiek szemléltetéséhez bemutatok egy fontos technikai eszközt, az ún. dimenziótanút. Szorítkozzunk most kétrészű kvantumrendszerekre, és tegyük fel, hogy bármely kétrészű rendszeren felvett $P(a, b|x, y)$ korreláció, amely 4×4 dimenziós (azaz *ququart*) rendszereken végrehajtott mérésekből származik, kielégíti a következő egyenlőtlenséget:

$$\sum_{a,b,x,y} W_{a,b,x,y} P(a, b|x, y) \leq Q_D, \tag{1}$$

ahol $W_{a,b,x,y}$ tetszőleges valós együtthatók, és konkrét esetünkben a dimenzió $D = 4$. Ezen típusú egyenlőtlenségeket dimenziótanúnak nevezzük: amennyiben ezen egyenlőtlenséget egy kísérletből származó adott $P'(a, b|x, y)$ korrelációval sikerül megsérteni, vagyis $\sum_{a,b,x,y} W_{a,b,x,y} P'(a, b|x, y) > Q_4$, ebből arra tudunk következtetni, hogy a protokollban szereplő fekete dobozok négydimenziósnál magasabb dimenziós rendszert tároltak.

Dolgozatom egyik részében általános $W_{a,b,x,y}$ együtthatókhoz tartozó dimenziótanúk szisztematikus előállítását végeztem el. Ezen optimalizációs feladat egzakt megoldásának számítási igénye még a legkisebb ($D = 2$) qubit rendszerek esetén is igen nagy, a lehetséges kvantumállapot és a mérési operátorok jellemzéséhez szükséges számtalan szabad paraméter miatt. Megmutattam, hogy adott $W_{a,b,x,y}$ esetén a Q_D határ felülről történő becslése visszavezethető egy szemidefinit programozási feladatra (ún. SDP-feladatra) [13]. A kidolgozott módszer SDP-feladatok hierarchiáját állítja elő, amelynek növelve a szintjét, egyre jobb közelítését kapjuk meg Q_D egzakt értékének.

Azonban növelve a fenti SDP-hierarchiában az (x, y) bemenetek számát vagy a D dimenziót, az optimalizálási feladat szuperszámítógépek használatával is hamar

megoldhatatlanná válik (pl. már $D = 4$ esetén, viszonylag alacsony hierarchia szinten és kevés számú x, y bemenet esetén is gyakran számítási nehézségekbe ütközünk). Ez problémás lehet más alkalmazásokban is, hiszen a kvantuminformatika számos alapfeladata SDP-módszerek használatára vezethető vissza. Ennek kezelésére kifejlesztettem egy iteratív algoritmust, amely hatékonyan tudja az ún. membership problémát megoldani. Vagyis adott a $P(a, b|x, y)$ korrelációk egy konvex halmaza (pl. azon korrelációk halmaza, amelyek megvalósíthatók négydimenziós állapoton történő mérésekkel). Ekkor azt kérdezzük, hogy egy adott $P'(a, b|x, y)$ korreláció – amelyet tekinthetünk a valószínűségi térben egy pontnak – vajon ezen halmazhoz tartozik-e. Egy iteratív algoritmus kifejlesztésével, amely a Gilbert-algoritmus [25] egy módosított változatának tekinthető, sikerült a fenti membership problémát visszavezetnem az (1) típusú kifejezés bal oldalának iteratív úton történő maximalizálására. Az irodalomban ezzel kapcsolatosan fellelhető algoritmusok óriási memóriaigényük miatt csak elméleti szempontból voltak érdekesek. Ezzel szemben az új algoritmus memóriaigénye csupán lineárisan függ a kérdéses konvex halmaz dimenziójától. Ezen előnyös tulajdonság miatt számos eddig megoldhatatlannak tűnő összefonódottsággal és nemlokalitással kapcsolatos problémát sikerült kezelnünk. Példaként a funkcionálanalízisben előforduló nevezetes konstans – a Grothendieck-együttható – véges dimenziós $n = 3, 4$ értékeinek a becslésén tudtunk lényegesen javítani.

A dolgozatban használt másik gyakran használt numerikus módszer a libikóka elvű variációs algoritmus [71], amelynek nagy hasznát vettem a kötötten összefonódott állapotok nemlokalitása és metrológiai teljesítőképessége közötti viszony felderítésében, továbbá a Peres-sejtés megcáfolásához szükséges ellenpélda előállításában is meghatározó szerepe volt. Ez egy olyan heurisztikus algoritmus, amelyben az eredeti nemkonvex optimalizálási problémát kisebb – gyakran SDP-elvű – hatékonyan megoldható részproblémák iteratív típusú optimalizálására vezetjük vissza. Bár nem garantált, hogy ezen algoritmus megadja a célfüggvény globális maximumát, gyakorlatban alkalmazva nagyon jó konvergencia tulajdonságokkal rendelkezik, aminek a megtalált ellenpéldákat is köszönhetjük.

Új tudományos eredmények

A dolgozatban a kvantumelmélet nemlokalitásának határait térképeztem fel különböző típusú és dimenziójú összefonódott kvantumállapotok esetén. Először a legegyszerűbb kétdimenziós kvantumrendszerek Bell-nemlokális viselkedését vizsgáltam, majd magasabb dimenziós, összetettebb rendszerek leírása felé haladtam. Téziseimben három különböző téma köré csoportosítva adom meg az elért eredményeimet:

1. *Werner-állapotok nemlokalitásának határai.*—A Werner-állapot a következő két-

qubites állapotcsaláddal írható le: $\rho_W(p) = p|\Psi_-\rangle\langle\Psi_-| + (1-p)\frac{\mathbb{I}}{4}$, amelyben a p paraméter a 0 és 1 között vehet fel értéket, és $|\Psi_-\rangle$ a szinglett állapotot jelöli. Legyen p_{crit} a p paraméter azon felső határa, amelyre a $\rho_W(p)$ állapot nem sérthet semmilyen Bell-egyenlőtlenséget, vagyis az $\langle A_x B_y\rangle = \mathrm{Tr}(\rho_W(p) A_x \otimes B_y)$ korreláció tetszőleges számú A_x, B_y projektív mérés esetén is szimulálható lokális modellel. A szakirodalomban közölt legszűkebb tartomány $0.66 < p_{crit} \leq 1/\sqrt{2}$ [2]. Ezzel kapcsolatosan elért eredményeim:

1.1 Megmutattam, hogy a kétqubites Werner-állapotok p_{crit} paraméter értékére fennáll a szigorú egyenlőtlenség: $p_{crit} < 1/\sqrt{2}$. Ennek bizonyításához kétrészű korrelációs Bell-egyenlőtlenségek egy osztályát állítottam elő [Tez1]. Az egyenlőtlenség bizonyításához egy 465-méréses Bell-egyenlőtlenségből származó korrelációkat használtam fel, továbbá a p_{crit} és a $K_G(3)$ harmadrendű Grothendieck-állandó értéke közötti szoros kapcsolatot is kihasználtam.

1.2 Az előző tézispontban kapott felső korlátot tovább javítottam az új korlátra: $p_{crit} \leq 0.6964$. Ezen új felső korlát eléréséhez nagyléptékű numerikus módszerek kifejlesztésére volt szükség, amelyben meghatározó szerepem volt [Tez2]. Az egyik módszer a videojátékok fejlesztésében kiválóan bevált Gilbert-algoritmus továbbfejlesztésén alapul, a másik módszer pedig az NP-nehéz problémák megoldása során gyakran használt *branch-and-bound* elvű algoritmusra épül. Mindkét algoritmus memóriaigénye elhanyagolható, és nagyon jól skálázik a vizsgált tér dimenziójával, így ezek használatával az irodalomban fellelhető eddigi módszereknél lényegesen jobb eredményeket lehetett elérni [Tez2].

1.3 Szisztematikus módszerek kidolgozásában vettem részt többrészű kvantumállapotok Bell-lokális modelljeinek meghatározására [Tez3]. A kidolgozott módszerek nem szorítkoznak qubites rendszerekre, elvben tetszőleges dimenziójú és számú részt tartalmazó állapotra is alkalmazhatók. Ezen numerikus módszerek hatékonyságát illusztráltam a kétqubites Werner-állapotok példáján [Tez4]. A módszer alkalmazásával a $p_{crit} > 0.6829$ alsó korlátot kapjuk (megjavítva az eddigi legjobb $p_{crit} > 0.66$ korlátot). Így a szakirodalomban szereplő eddigi legjobb $0.66 < p_{crit} \leq 1/\sqrt{2}$ korlátokat lényegesen megjavítva, a $0.6829 < p_{crit} < 0.6964$ intervallumra sikerült szűkíteni a kétqubites Werner-állapotcsalád p_{crit} értékét [Tez4].

2. *Dimenziótanúk előállítása.*—Ezen kutatásban azt vizsgáltam, hogy milyen nagyságú Hilbert-tér szükséges a természetben megvalósuló Bell-nemlokális kvantumkorrelációk előállításához. Célom annak eldöntése volt, hogy egy adott

$P(a,b|x,y)$ nemlokális korreláció megvalósítható-e kvantummechanikailag, ha a két kísérletező fél, szokásos nevükön Aliz és Bob, a méréseket egy-egy maximálisan D-dimenziós Hilbert-téren hajtja végre. Ehhez segítségül hívtam az (1) képlettel jellemzett dimenziótanút, amely alsó korlátot ad a $P(a,b|x,y)$ korreláció eléréséhez szükséges Hilbert-tér D dimenziójára. Alkalmazásával így eszközfüggetlen módon – vagyis a kísérletben szereplő mérőberendezések működésének részleteitől függetlenül – tudjuk többrészű kvantumállapotok dimenzióját becsülni. Az alábbiakban felsorolom a dolgozatban ezzel kapcsolatosan elért konkrét eredményeimet.

2.1 Munkatársammal közösen javasolt elrendezésben dimenziótanúk létezését bizonyítottam be a legegyszerűbb nemtriviális, $D > 2$ dimenziós kvantumrendszerek esetén. Ilyenkor azt láttam be, hogy egy adott $P(a,b|x,y)$ korreláció eléréséhez qubitnél magasabb dimenziós rendszerekre van szükség. Ezen eredménynél alkalmasan megválasztott kétkimenetelű korrelációs tagokon alapuló Bell-kifejezést használtam fel dimenziótanúként. [Tez5].

2.2 A D dimenzióhoz tartozó dimenziótanúk megalkotására szemidefinit programozáson (SDP) alapuló numerikus módszerek kidolgozását végeztem. Ezen SDP-hierarchián alapuló módszerek lehetőséget adnak adott D Hilbert-tér dimenzió esetén tetszőleges Bell-egyenlőtlenség maximális sérülésének felülről történő becslésére. A hierarchia szintjét növelve egyre jobb felső korlátokat kapunk. Két különböző módszer kifejlesztésében volt meghatározó szerepem. Az első módszer a mérési operátoroknak a kvantumállapot terébe való leképezésén alapszik [Tez6], amely gyakorlatban jól működik kettőnél több részrendszer esetén is, azonban egyelőre nem bizonyított, hogy az SDP-hierarchia minden esetben az egzakt megoldáshoz konvergál. A másik módszer a széles körben elterjedt, dimenzióra nem érzékeny ún. Navascues-Pironio-Acín (NPA) hierarchiát általánosítja véges dimenziós rendszerekre [Tez7]. Szemben az előző SDP-hierarchiával, ezen utóbbi módszer tetszőleges D dimenzió esetén konvergál. A módszerek hatékonyságát konkrét két- és kettőnél több részű dimenziótanúkon teszteltem. Numerikus tapasztalataim azt mutatják, hogy a fenti módszerek tipikusan $D \leq 4$ dimenzió esetén alkalmazhatók jól (kis számú x, y bemenet, illetve a, b kimenetel mellett) [Tez8].

2.3 Magasabb (tipikusan $D > 4$) dimenziós tanúk esetén az előbbi tézispontban felsorolt numerikus módszerek a számítási kapacitás korlátossága miatt sajnos már nem használhatók. Így az a fontos nyitott kérdés maradt, hogy léteznek-e dimenziótanúk tetszőleges véges dimenzió esetén. Ehhez (1) alakú dimenziótanúkat konstruáltam analitikusan, amelyek Q_D korlátjára sejtést fogalmaztam meg tetszőleges D véges dimenzióban. Az első konstrukcióm kétkimenetelű

mérésekből származó korrelációkra épít. A sejtés alapja a $K_G(n)$, n-edrendű Grothendieck-állandó – tudomásunk szerint még nem bizonyított, de plauzibilisnek tűnő – szigorúan monoton növekvő tulajdonsága n függvényében. Ennek alátámasztására vonatkozóan sikerült belátni, hogy $K_G(4) > K_G(3)$ (a $K_G(3) > K_G(2)$ összefüggést pedig a [Tez1] cikkben bizonyítottam). Konkrétan a $K_G(3) \leq 1.4644$ korlátot találtam, amelyhez a [Tez4] tanulmányban kidolgozott numerikus eljárást használtam fel. Ugyanakkor, $K_G(4) \geq 1.4841$, amely eredmény a [Tez2] tanulmányból származik.

2.4 A második, ugyancsak analitikus konstrukcióm egy aszimmetrikus Bell-kifejezések családján alapul (itt Aliz detektorai tökéletesek, míg Bob detektorai véges η hatékonyságúak). Ezen Bell-egyenlőtlenség-család D-ik tagjáról bebizonyítottam, hogy sérthető $D \times D$ dimenziós állapottéren, Bob detektorainak $\eta > (1/D)$ hatékonysága mellett [Tez9]. Ahhoz, hogy a konstrukciót tetszőleges D esetén lehessen dimenziótanúként használni, még azt lenne szükséges belátni, hogy a család D-ik tagja nem sérthető Bob $\eta \leq 1/(D-1)$ hatékonyságú detektoraival a $(D-1) \times (D-1)$ téren. Ezen tulajdonságot sejtésként fogalmaztam meg.

2.5 A harmadik konstrukcióm az I_{3322} Bell-egyenlőtlenséget használja fel dimenziótanúként [Tez10]. $Q = 0.250\,875$ az NPA-módszerből származó felső korlát az I_{3322}-egyenlőtlenség maximális sértésére. Munkatársammal együtt sikerült ezen értéket reprodukálni konkrét mérési operátorokkal és állapottal, amelyekhez határesetben végtelen dimenziós állapottér tartozik. Azt a sejtést fogalmaztuk meg, hogy az I_{3322} egyenlőtlenség maximális sérülése csakis végtelen dimenziójú Hilbert-téren érhető el, amiből pedig tetszőleges véges dimenziós tanú létezése következne.

2.6 Annak az analitikus bizonyításában volt meghatározó szerepem, hogy bármely $D \geq 2$ véges dimenzió esetén létezik dimenziótanú [Tez11]. Ezen konstrukció kétkimenetelű korrelációs típusú Bell-kifejezések egy speciális osztályán alapszik, és D növelésével szükségszerűen növekszik a Bell-kifejezésben szereplő mérések száma is.

3. *Kötötten összefonódott állapotok és Bell-nemlokalitás.*—A természetben előforduló nagyon gyengén összefonódott kvantumállapotok az ún. kötötten összefonódott állapotok, amelyekből nem párolható le maximálisan összefonódott állapot a desztilláció művelete segítségével. Ezen nem-desztillálható állapotok fontos családja az ún. PPT-típusú állapotok. Asher Peres 1999-ben fogalmazta meg a PPT-típusú állapotok nemlokalitására vonatkozó nevezetes sejtését [53]. Állítása szerint PPT-típusú

állapotokkal semmilyen Bell-egyenlőtlenség nem sérthető. Azóta számos munkában próbálták ezen sejtést igazolni, illetve cáfolni. Egyik fontos lépésként sikerült belátni, hogy a CHSH-Bell-egyenlőtlenség [19] – a Bell-kísérletekben leggyakrabban használt egyenlőtlenség – kötötten összefonódott állapotokkal, így PPT-típusú állapotokkal sem sérthető [38]. A jelen dolgozatban tárgyalt tanulmányokban lépésről lépésre haladva cáfoltam meg Peres sejtését:

3.1 Háromrészű, bármely kétrészű osztás mentén PPT-tulajdonságú kvantumállapotot konstruáltam meg. Beláttam, hogy ezen állapot alkalmasan megválasztott mérések mellett sért egy adott Bell-egyenlőtlenséget [Tez12]. Ez Peres sejtését kettőnél többrészű rendszerek esetén cáfolja meg.

3.2 Bell-egyenlőtlenséget sértő kétrészű (3×3 dimenziós) PPT-típusú kötötten összefonódott kvantumállapotot konstruáltam meg. Ezen a konkrét példán keresztül sikerült megcáfolni Peres eredeti sejtését [Tez13]. Mivel a kötötten összefonódott állapotokból nem desztillálható összefonódottság, így egyúttal bizonyítást nyert, hogy a Bell-féle nemlokalitásból nem következik az összefonódottság desztillálhatósága.

3.3 Lényeges szerepem volt a fenti eredmény $d > 3$ dimenziós rendszerekre történő kiterjesztésében: egy d paramétertől függő Bell-egyenlőtlenséget sikerült megalkotni, amely tetszőleges $d \geq 3$ esetén sérthető speciális $d \times d$ dimenziós PPT-típusú állapottal. Azt a sejtést fogalmaztuk meg, hogy ezen Bell-egyenlőtlenség-család dimenziótanúként működik a PPT-típusú állapotok körében: Bármely rögzített $d \geq 3$ esetén létezik a családnak egy tagja, amelynek PPT-állapotokkal történő sértéséhez legalább $d \times d$ dimenzió szükséges [Tez14].

Tézispontokhoz kapcsolódó publikációk

[Tez1] T. Vértesi:
More efficient Bell inequalities for Werner states
Phys. Rev. A **78**, 032112 (2008).

[Tez2] P. Diviánszky, E. Bene, and T. Vértesi:
Qutrit witness from the Grothendieck constant of order four
Phys. Rev. A **96**, 012113 (2017).

[Tez3] F. Hirsch, M. T. Quintino, T. Vértesi, M. F. Pusey, and N. Brunner:
Algorithmic construction of local hidden variable models for entangled quantum states
Phys. Rev. Lett. **117**, 190402 (2016).

[Tez4] F. Hirsch, M. T. Quintino, T. Vértesi, M. Navascués, and N. Brunner:
Better local hidden variable models for two-qubit Werner states and an upper bound on the Grothendieck constant $K_G(3)$
Quantum **1**, 3 (2017).

[Tez5] T. Vértesi, K. F. Pál:
Generalized Clauser-Horne-Shimony-Holt inequalities maximally violated by higher-dimensional systems
Phys. Rev. A **77**, 042106 (2008).

[Tez6] M. Navascués, de la T. Gonzalo, and T. Vértesi:
Characterization of quantum correlations with local dimension constraints and its device-independent applications
Phys. Rev. X **4**, 011011 (2014).

[Tez7] M. Navascués and T. Vértesi:
Bounding the set of finite dimensional quantum correlations
Phys. Rev. Lett. **115**, 020501 (2015).

[Tez8] M. Navascués, A. Feix, M. Araújo, and T. Vértesi:
Characterizing finite-dimensional quantum behavior
Phys. Rev. A **92**, 042117 (2015).

[Tez9] T. Vértesi, S. Pironio, and N. Brunner:
Closing the detection loophole in Bell experiments using qudits
Phys. Rev. Lett. **104**, 060401 (2010).

[Tez10] K. F. Pál and T. Vértesi:
Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems
Phys. Rev. A **82**, 022116 (2010).

[Tez11] T. Vértesi and K. F. Pál:
Bounding the dimension of bipartite quantum systems
Phys. Rev. A **79**, 042106 (2009).

[Tez12] T. Vértesi and N. Brunner:
Quantum nonlocality does not imply entanglement distillability
Phys. Rev. Lett. **108**, 030403 (2012).

[Tez13] T. Vértesi and N. Brunner:
Disproving the Peres conjecture by showing Bell nonlocality from bound en-

tanglement
Nature Communications **5**, 5297 (2014).

[Tez14] K. F. Pál and T. Vértesi:
Family of Bell inequalities violated by higher-dimensional bound entangled states
Phys. Rev. A **96**, 022123 (2017).

Tézispontokban nem említett, de a témához kapcsolódó eredmények és publikációk

A fenti tézispontokban nem tárgyalt, de a témához kapcsolódóan számos más eredmény elérésében volt meghatározó szerepem. Ezen eredményeket röviden pontokba szedve foglalom össze:

- Sokrészű kvantumrendszerekben korlátok megadása a Bell-egyenlőtlenségek sérthetőségének mértékére véges hatékonyságú detektorok mellett [50],[49],[48],[34].
- Sokrészű kvantumrendszerekben a Bell-féle nemlokalitás zajtűrésének mértékére új fogalmak [17],[36] és módszerek [14] bevezetése, amelyekkel sikerült kibővíteni közismert többrészűen összefonódott állapotok (pl. Dicke-, GHZ-állapotok) nemlokalitási tartományát [70],[22],[14].
- Hitelesítési feladatok megvalósítása a kvantuminformatika eszközfüggetlen keretében. Meghatároztuk a kétqubites állapotokból kinyerhető valódi véletlenszerűség nagyságát [3], valódi többrészű összefonódottság meglétét igazoltuk [47], többrészű rendszerek összefonódottságának a struktúráját jellemeztük [16], háromrészű rendszerek eszközfüggetlen tomográfiáját végeztük el [51], kvantumeszközök zajtűrő öntesztjére dolgoztunk ki új algoritmusokat [74],[7].
- A kvantuminformatika féleszközfüggetlen keretében mérések hitelesítését végeztük el [62], egyrészű rendszerekre dimenziótanúkat alkottunk [15], kétrészű összefonódottság mértékét jellemeztük [37], általános POVM-típusú méréseket észleltünk [67],[28], illetve többrészű rendszereken elvégzett mérések összefonódottságát igazoltuk [69],[10].
- Az együttes mérhetőség, az EPR-steering és a Bell-nemlokalitás jelenségei közötti kapcsolatok feltárása [55],[12],[56],[58],[29],[31],[9].
- Véletlen mérések, illetve vonatkoztatási rendszerek nélküli Bell-egyenlőtlenségek sérthetőségének vizsgálata [59],[21],[24].

- A nemlokális kvantumkorrelációk információelméleti elvekből történő megalapozása [4],[35],[33],[32].
- Numerikus eszközök kidolgozása nemlokális korrelációk aktiválhatóságának a kimutatására [40],[18].
- PPT kötötten összefonódott állapotok nemlokalitása és metrológiai hasznossága közötti összefüggések feltárása [63].
- A nemlokális korrelációk kommunikációs [66],[39] és számítási komplexitási problémákban [52] történő hasznosítása.
- A kvantumkorrelációk halmaza geometriai struktúrájának feltérképezése különböző elrendezésekben [43],[45],[44],[46],[27].
- Kéttestkorrelációkon alapuló sokrészecskés Bell-egyenlőtlenségek megkonstruálása, amelyek képesek nemlokalitást detektálni ezen egyenlőtlenségek sérülése révén [64],[65],[73],[68],[41].
- Olyan eszközfüggetlen algoritmusok kifejlesztése, amelyeket fotonikai kísérletben is sikerült megvalósítani [59],[10],[29],[28],[32].

Irodalomjegyzék

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[2] A. Acín, N. Gisin, and B. Toner. Grothendieck's constant and local models for noisy entangled quantum states. *Physical Review A*, 73(6):062105, 2006.

[3] A. Acín, S. Pironio, T. Vértesi, and P. Wittek. Optimal randomness certification from one entangled bit. *Physical Review A*, 93(4):040102, 2016.

[4] J. Allcock, N. Brunner, N. Linden, S. Popescu, P. Skrzypczyk, and T. Vértesi. Closed sets of nonlocal correlations. *Physical Review A*, 80(6):062107, 2009.

[5] A. Aspect. Quantum mechanics: to be or not to be local. *Nature*, 446(7138):866, 2007.

[6] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein-Podolsky-Rosen-Bohm gedankenexperiment: a new violation of Bell's inequalities. *Physical Review Letters*, 49(2):91, 1982.

[7] J.-D. Bancal, M. Navascués, V. Scarani, T. Vértesi, and T. H. Yang. Physical characterization of quantum devices from nonlocal correlations. *Physical Review A*, 91(2):022115, 2015.

[8] J. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[9] E. Bene and T. Vértesi. Measurement incompatibility does not give rise to Bell violation in general. *New Journal of Physics*, 20(1):013021, 2018.

[10] A. Bennet, T. Vértesi, D. J. Saunders, N. Brunner, and G. J. Pryde. Experimental semi-device-independent certification of entangled measurements. *Physical Review Letters*, 113(8):080405, 2014.

[11] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.*, 560(P1):7–11, 2014.

[12] J. Bowles, T. Vértesi, M. T. Quintino, and N. Brunner. One-way Einstein-Podolsky-Rosen steering. *Physical Review Letters*, 112(20):200402, 2014.

[13] S. Boyd and L. Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[14] S. Brierley, M. Navascues, and T. Vértesi. Convex separation from convex optimization for large-scale problems. *arXiv preprint arXiv:1609.05011*, 2016.

[15] N. Brunner, M. Navascués, and T. Vértesi. Dimension witnesses and quantum state discrimination. *Physical Review Letters*, 110(15):150501, 2013.

[16] N. Brunner, J. Sharam, and T. Vértesi. Testing the structure of multipartite entanglement with Bell inequalities. *Physical Review Letters*, 108(11):110501, 2012.

[17] N. Brunner and T. Vértesi. Persistency of entanglement and nonlocality in multipartite quantum systems. *Physical Review A*, 86(4):042113, 2012.

[18] D. Cavalcanti, A. Acín, N. Brunner, and T. Vértesi. All quantum states useful for teleportation are nonlocal resources. *Physical Review A*, 87(4):042104, 2013.

[19] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880, 1969.

[20] R. Colbeck and A. Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[21] A. de Rosier, J. Gruca, F. Parisio, T. Vértesi, and W. Laskowski. Multipartite nonlocality and random measurements. *Physical Review A*, 96(1):012101, 2017.

[22] P. Diviánszky, R. Trencsényi, E. Bene, and T. Vértesi. Bounding the persistency of the nonlocality of W states. *Physical Review A*, 93(4):042113, 2016.

[23] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[24] A. Fonseca, A. de Rosier, T. Vértesi, W. Laskowski, and F. Parisio. Survey on the Bell nonlocality of a pair of entangled qudits. *arXiv preprint arXiv:1805.09451*, 2018.

[25] E. G. Gilbert. An iterative procedure for computing the minimum of a quadratic form on a convex set. *SIAM Journal on Control*, 4(1):61–80, 1966.

[26] M. Giustina, M. A. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-$\mathcal{A}$. Larsson, C. Abellán, et al. Significant-loophole-free test of Bell's theorem with entangled photons. *Physical Review Letters*, 115(25):250401, 2015.

[27] K. T. Goh, J. Kaniewski, E. Wolfe, T. Vértesi, X. Wu, Y. Cai, Y.-C. Liang, and V. Scarani. Geometry of the set of quantum correlations. *Physical Review A*, 97(2):022104, 2018.

[28] E. S. Gómez, S. Gómez, P. González, G. Cañas, J. F. Barra, A. Delgado, G. B. Xavier, A. Cabello, M. Kleinmann, T. Vértesi, et al. Device-independent certification of a nonprojective qubit measurement. *Physical Review Letters*, 117(26):260401, 2016.

[29] T. Guerreiro, F. Monteiro, A. Martin, J. Brask, T. Vértesi, B. Korzh, M. Caloz, F. Bussières, V. Verma, A. Lita, et al. Demonstration of Einstein-Podolsky-Rosen steering using single-photon path entanglement and displacement-based detection. *Physical Review Letters*, 117(7):070404, 2016.

[30] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán, et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682, 2015.

[31] F. Hirsch, M. T. Quintino, J. Bowles, T. Vértesi, and N. Brunner. Entanglement without hidden nonlocality. *New Journal of Physics*, 18(11):113019, 2016.

[32] X.-M. Hu, B.-H. Liu, Y. Guo, G.-Y. Xiang, Y.-F. Huang, C.-F. Li, G.-C. Guo, M. Kleinmann, T. Vértesi, and A. Cabello. Observation of stronger-than-binary correlations with entangled photonic qutrits. *Physical Review Letters*, 120(18):180402, 2018.

[33] M. Kleinmann, T. Vértesi, and A. Cabello. Proposed experiment to test fundamentally binary theories. *Physical Review A*, 96(3):032104, 2017.

[34] K. Kostrzewa, W. Laskowski, and T. Vértesi. Closing the detection loophole in multipartite Bell experiments with a limited number of efficient detectors. *arXiv preprint arXiv:1805.05106*, 2018.

[35] B. Lang, T. Vértesi, and M. Navascués. Closed sets of correlations: answers from the zoo. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424029, 2014.

[36] W. Laskowski, T. Vértesi, and M. Wieśniak. Highly noise resistant multiqubit quantum correlations. *Journal of Physics A: Mathematical and Theoretical*, 48(46):465301, 2015.

[37] Y.-C. Liang, T. Vértesi, and N. Brunner. Semi-device-independent bounds on entanglement. *Physical Review A*, 83(2):022108, 2011.

[38] L. Masanes. Asymptotic violation of Bell inequalities and distillability. *Physical review letters*, 97(5):050503, 2006.

[39] S. Nagy and T. Vértesi. EPR steering inequalities with communication assistance. *Scientific Reports*, 6:21634, 2016.

[40] M. Navascués and T. Vértesi. Activation of nonlocal quantum resources. *Physical Review Letters*, 106(6):060403, 2011.

[41] M. Navascues and T. Vértesi. Bond dimension witnesses and the structure of homogeneous matrix product states. *Quantum*, 2:50, 2018.

[42] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[43] K. F. Pál and T. Vértesi. Efficiency of higher-dimensional Hilbert spaces for the violation of Bell inequalities. *Physical Review A*, 77(4):042105, 2008.

[44] K. F. Pál and T. Vértesi. Concavity of the set of quantum probabilities for any given dimension. *Physical Review A*, 80(4):042114, 2009.

[45] K. F. Pál and T. Vértesi. Quantum bounds on Bell inequalities. *Physical Review A*, 79(2):022120, 2009.

[46] K. F. Pál and T. Vértesi. Maximal violation of a bipartite three-setting, two-outcome Bell inequality using infinite-dimensional quantum systems. *Physical Review A*, 82(2):022116, 2010.

[47] K. F. Pál and T. Vértesi. Multisetting Bell-type inequalities for detecting genuine multipartite entanglement. *Physical Review A*, 83(6):062123, 2011.

[48] K. F. Pál and T. Vértesi. Bell inequalities violated using detectors of low efficiency. *Physical Review A*, 92(5):052104, 2015.

[49] K. F. Pál and T. Vértesi. Closing the detection loophole in tripartite Bell tests using the W state. *Physical Review A*, 92(2):022103, 2015.

[50] K. F. Pál, T. Vértesi, and N. Brunner. Closing the detection loophole in multipartite Bell tests using Greenberger-Horne-Zeilinger states. *Physical Review A*, 86(6):062111, 2012.

[51] K. F. Pál, T. Vértesi, and M. Navascués. Device-independent tomography of multipartite quantum states. *Physical Review A*, 90(4):042340, 2014.

[52] M. Pawłowski, T. Vértesi, A. Grudka, M. Horodecki, R. Horodecki, et al. Absolute nonlocality via distributed computing without communication. *Physical Review A*, 92(3):032122, 2015.

[53] A. Peres. All the Bell inequalities. *Foundations of Physics*, 29(4):589–614, 1999.

[54] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, et al. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021, 2010.

[55] M. T. Quintino, T. Vértesi, and N. Brunner. Joint measurability, Einstein-Podolsky-Rosen steering, and Bell nonlocality. *Physical Review Letters*, 113(16):160402, 2014.

[56] M. T. Quintino, T. Vértesi, D. Cavalcanti, R. Augusiak, M. Demianowicz, A. Acín, and N. Brunner. Inequivalence of entanglement, steering, and Bell nonlocality for general measurements. *Physical Review A*, 92(3):032107, 2015.

[57] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter. Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. *Physical Review Letters*, 119(1):010402, 2017.

[58] A. B. Sainz, N. Brunner, D. Cavalcanti, P. Skrzypczyk, and T. Vértesi. Postquantum steering. *Physical Review Letters*, 115(19):190403, 2015.

[59] P. Shadbolt, T. Vértesi, Y.-C. Liang, C. Branciard, N. Brunner, and J. L. O'brien. Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices. *Scientific Reports*, 2:470, 2012.

[60] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, et al. Strong loophole-free test of local realism. *Physical Review Letters*, 115(25):250402, 2015.

[61] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[62] A. Tavakoli, J. Kaniewski, T. Vertesi, D. Rosset, and N. Brunner. Self-testing quantum states and measurements in the prepare-and-measure scenario. *arXiv preprint arXiv:1801.08520*, 2018.

[63] G. Tóth and T. Vértesi. Quantum states with a positive partial transpose are useful for metrology. *Physical Review Letters*, 120(2):020506, 2018.

[64] J. Tura, R. Augusiak, A. B. Sainz, T. Vértesi, M. Lewenstein, and A. Acín. Detecting nonlocality in many-body quantum states. *Science*, 344(6189):1256–1258, 2014.

[65] J. Tura, A. B. Sainz, T. Vértesi, A. Acín, M. Lewenstein, and R. Augusiak. Translationally invariant multipartite Bell inequalities involving only two-body correlators. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424024, 2014.

[66] T. Vértesi and E. Bene. Lower bound on the communication cost of simulating bipartite quantum correlations. *Physical Review A*, 80(6):062316, 2009.

[67] T. Vértesi and E. Bene. Two-qubit Bell inequality for which positive operator-valued measurements are relevant. *Physical Review A*, 82(6):062115, 2010.

[68] T. Vértesi, W. Laskowski, and K. F. Pál. Certifying nonlocality from separable marginals. *Physical Review A*, 89(1):012115, 2014.

[69] T. Vértesi and M. Navascués. Certifying entangled measurements in known Hilbert spaces. *Physical Review A*, 83(6):062112, 2011.

[70] T. Vértesi and K. F. Pál. Nonclassicality threshold for the three-qubit Greenberger-Horne-Zeilinger state. *Physical Review A*, 84(4):042122, 2011.

[71] R. F. Werner and M. M. Wolf. Bell inequalities and entanglement. *arXiv preprint quant-ph/0107093*, 2001.

[72] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[73] L. E. Würflinger, J.-D. Bancal, A. Acín, N. Gisin, and T. Vértesi. Nonlocal multipartite correlations from local marginal probabilities. *Physical Review A*, 86(3):032117, 2012.

[74] T. H. Yang, T. Vértesi, J.-D. Bancal, V. Scarani, and M. Navascués. Robust and versatile black-box certification of quantum devices. *Physical Review Letters*, 113(4):040401, 2014.