

Válaszok Diósi Lajos opponensi véleményére

Szeretném megköszönni Diósi Lajos professzor úrnak az értekezésem bírálataival kapcsolatos gondos munkáját, észrevételeit és értékes megjegyzéseit. A feltett kérdésekre az alábbiakban válaszolok.

1. kérdés: A mű megemlíti (26. old), hogy Gisin talált olyan állapotot, amely lokális, de lokális szűréssel nemlokálissá lesz. Tehát a szűretlen statisztika lokális, a szűrt már nem. Azt gondolnám, a korrelációk nemlokalitása abból következik, hogy egyes mérési adatok a szűrés miatt kiesnek. De ha ez megtehető, vagyis a mért statisztika előválogatható, akkor még egy teljesen korrelálatlan állapotban is kaphatnánk korrelációt, nemlokálisat is. A szűrt statisztika nemlokalitásából tehát nem következik az eredeti állapot nemlokalitása – szemben azzal, amit a példa sugallni látszik. Hányadik lépése hibás gondolatmenetnek?

Az opponensem által ismertetett ún. rejtett nemlokalitás jelenségének kimutatása során a két kísérletező személy, akiket nevezünk Alice-nak és Bobnak, a kiosztott kétrészes állapot részrendszerén egy-egy előzetes mérést hajtanak végre. Ezen szűrési eljárás során csak egy adott mérési eredményhez tartozó statisztikát tartanak meg. Ezen eljárással ún. előszűrjük az állapotukat, majd ezen az előszűrt állapotban végzik el a hagyományos Bell-kísérletet. A 90-es évek közepén egymástól függetlenül Sandu Popescu és Nicolas Gisin is megmutatta, hogy ezen módszerrel lokális modellel rendelkező kvantumállapotból is kaphatunk egy olyan szűrt állapotot, amely Bell-egyenlőtlenséget sért, azaz nemlokális.

A fenti szűrési művelet alkalmazásában az a megérzés vezet, hogy egy kezdeti szűretlen lokális állapot tekinthető több állapot statisztikai keverékének, amely állapotok közül több is mutathat nemlokalitást. Így az előszűrés feladata az, hogy legalább az egyik ilyen nemlokális állapotot kiszűrje a keverékből, majd ezen kiszűrt állapottal már Bell-egyenlőtlenséget lehet sérteni egy standard Bell-kísérlet során. Fontos még megemlíteni, hogy a tényleges Bell-kísérlet elvégzésére csakis a sikeres előszűrés után kerülhet sor, máskülönben megmutatható, hogy lokális stratégiák használatával hamisítani lehetne a Bell-sérülést.

Opponensem gondolatmenete szerint akár teljesen korrelálatlan állapotból is nyerhetünk ki nemlokális korrelációt a fenti előszűrés segítségével. Amint az alábbiakban megmutatjuk, ez azonban mégsem lehetséges. Kiindulási állapotként vegyünk egy szeparálható, vagyis nem összefonódott állapotot. Ezen állapot mindig felírható szorzatállapotok statisztikus keverékékként és csak klasszikus korrelációkat hordoz. Most Alice és Bob előszűrést végez ezen az állapotban, amelynek eredményeként a sikeres mérések esetén az előszűrt állapot továbbra is szeparálható marad. Ez azért igaz, mert az előszűrés egy ún. LOCC művelet, amely megtartja az állapot szeparálhatóságát. Mivel minden szeparálható állapothoz létezik lokális modell, ezért ilyen módon a szűrt állapottal Bell-sérülés sem érhető el. Tehát megállapíthatjuk, hogy a kezdeti állapotnak összefonódottnak kell lennie ahhoz, hogy az állapot az előszűrés művelete által felfedhető rejtett nemlokalitással rendelkezzen. Tudomásom szerint az egy régen nyitva álló probléma, hogy vajon minden összefonódott állapot rendelkezik-e rejtett nemlokalitással.

2. kérdés: A mű csökkent hatékonyságú detektálás esetére mutat dimenziótanút (67. old). Az ilyen detektálás, az előző kérdésben hivatkozott Gisin-féle szűréshez hasonlóan, inkonklúzív mérésekre

is vezet. Most azonban Vértesi a hatékonysággal paraméterezve módosítja a Bell-egyenlőtlenséget és (a doktori mű ezt nem említi, csak az eredeti [153] publikáció) az inkonkluzív mérési eredményeket kipótolja konstans -1-gyel. Ebben az esetben tehát meg van oldva, hogy a teljes statisztikát nem kell redukálni. Tehát elhárulnak az előző kérdésben felvetett kétségeim. Tudná-e Vértesi értelmezni, mi az itteni és a Gisin-féle statisztikacsökkentés viszonya, kell-e összevetnem őket, vagy nincs köze egyiknek a másikhoz?

Az optikai Bell-kísérletekben gyakoriak a fotonveszteségek, ami miatt a detektorok sokszor nem adnak érvényes kimenetet. Ekkor a mérési adatok kezelésének egyik legegyszerűbb módja, hogy a felvett statisztikából eltávolítjuk a sikertelen detektálási eseményeket, ezzel csökkentve a statisztikai minta nagyságát. Azonban szemben a rejtett nemlokalitás észlelésénél alkalmazott előválogatás eljárásával, amely ugyancsak csökkenti a statisztikát, itt komoly elvi nehézségek léphetnek fel. Ugyanis ezen statisztikacsökkentési eljárást csak akkor alkalmazzuk helyesen, ha megbízunk abban, hogy a statisztikában megtartott események hűen reprezentálják azt a statisztikát, amit tökéletes hatékonyságú detektorokkal kaptunk volna. Amennyiben ez a feltétel nem teljesül, lokális modellekben kihasználható, hogy a nem detektált kimenetel előfordulása függhet a mérési bázistól, és így hamis Bell-sérülést kaphatunk. Ez az utólagos szelekció vagy másképpen posztszelekció egyik példája.

3. kérdés: A mű a Popescu-Rohrlich-dobozt idézi (20. oldal), hogy a neki megfelelő – mai tudásunk szerint szürreális – nemlokális korrelációk elképesztő erejű kommunikációs erőforrások lehetnének. A gyengébb, de kvantumrendszerekben realizálható nemlokális korrelációkról magukról, tehát a mű által is használt eszközfüggetlen módon, bizonyítható-e, hogy bárminek is erőforrásai?

A nemlokális kvantumkorrelációk többféle alkalmazásban is hasznos erőforrásnak bizonyulnak. Ezen korrelációk teljesítik az ún. nemjelző feltételeket, ami lényeges korlátozást jelent, hiszen nem lehet segítségükkel pillanatszerűen információt továbbítani. Ugyanakkor a nemjelző feltételek teljesülésének köszönhetően a nemlokális korrelációkhoz tartozó mérési kimenetek nem lehetnek a bemenetek determinisztikus függvényei. Tehát szükségszerű, hogy a kimenetek valamilyen mértékű valódi véletlenszerűséget hordozzanak. Ez az intuíció húzódik a kvantumkommunikációt biztonságossá tevő ún. eszközfüggetlen kriptográfia működése mögött is. Ilyenkor a technikai kikapuktól mentes kísérleti Bell-sérülés nagysága garantálja a kriptográfiai kulcsok lehallgatásmentes előállítását. Tehát ezen kulcskiosztási protokollokban a nemlokális korrelációk hasznos erőforrásként viselkednek, és ilyenkor szükséges, hogy teljesüljenek a nemjelző feltételek. További érdekes alkalmazások, amelyekben a nemlokális korrelációk erőforrásként használhatók, a kvantumhitelesítés művelete, illetve különböző elosztott számítási problémák. Az alábbiakban ezen alkalmazásokat mutatom be röviden.

A kvantumhitelesítés során pusztán a Bell-egyenlőtlenség sérülésének mértékéből következtetünk a forrás által kibocsátott állapotra, illetve a mérési eszközök jellemzőire. Ismeretes, hogy Bell-egyenlőtlenség sértése csakis összefonódott állapotokkal történhet. Vagyis egy sikeres Bell-kísérlet eszközfüggetlen módszer az összefonódottság detektálására. De vannak olyan esetek, amikor ennél többet is mondhatunk az eszközökről. Ilyenkor felhasználjuk, hogy bizonyos kvantumkorrelációk konkrét összefonódott állapotokon elvégzett jól meghatározott mérésekkel állíthatók csak elő. Például a CHSH-egyenlőtlenség maximális sérülése csakis olyan

állapottal történhet, amely ekvivalens a kétqubités maximálisan összefonódott állapottal, Alice és Bob mérési operátorainak pedig antikommutálniuk kell. Kvantumhitelesítéssel azt is becsülni tudjuk, hogy milyen messze van a kísérletileg előállított állapot a célállapottól, illetve milyen mértékben sikerült megközelíteni az elvégzett mérésekkel az ideális esetet.

Nemlokális korrelációk másik lehetséges alkalmazása a különböző elosztott számítási problémák területe. Ezen típusú problémákban két különböző helyen tartózkodó résztvevő szeretne adott $f(a,b)$ függvényt kiszámolni minél kevesebb számú bit kicserélésével, ahol a Alice, b pedig Bob változóit jelöli. Cleve és Buhrman 1997-ben közölt eredménye alapján (Physical Review A 56, 1201), ha Alice és Bob nemlokális kvantumrendszereket osztanak meg egymás között, bizonyos $f(a,b)$ függvényeket kevesebb kommunikációval is ki tudnak számolni, mint a nemlokális korrelációk hiányában. Persze az előny ilyenkor nem olyan látványos, mint az opponensem által megemlített PR-doboz esetén, amikor is csupán 1 bit kommunikáció elegendő bármely $f(a,b)$ függvény kiszámításához, amennyiben Alice és Bob tetszőleges számú PR-dobozhoz férhet hozzá.

4. kérdés: Bell mértéket is adott a nemlokalitásra. A mérték, az egyenlőtlenségek sérülésének értéke, mindaddig csupán egy heurisztikus skála, amíg a sérülés értékét nem tudjuk valamely független tulajdonság értékéhez hozzákötni. Van-e ilyen eredmény, legalább kilátás fél évszázaddal Bell felfedezése után?

Az értekezés fő témája kvantumrendszerekből származó korrelációk karakterizációja, beleértve annak eldöntését, hogy egy adott P korreláció nemlokális-e. Ugyanakkor kevés szó esett arról, hogy lehet-e a nemlokális korrelációkhoz mértéket rendelni. Ahogy opponensem megjegyezte, egy adott Bell-egyenlőtlenség sérülésének nagysága, mint mérték nem egyértelmű. Valóban, megmutatható, hogy egy egyszerű skálázással például a CHSH-Bell-egyenlőtlenség sértése akármilyen nagyra tehető. Azonban a Bell-egyenlőtlenségek jól megválasztott normálásával ilyenkor is értelmezhető egy alkalmas mértéke a nemlokalitásnak, amelyet Pérez-Garcia és munkatársai mutattak meg (D. Pérez-Garcia et al., Comm. Math. Phys. 279, 455 (2008)). Ezen kívül léteznek más használatos mértékei is a nemlokalitásnak, amelyeket az alábbiakban ismertetek.

Jó mérték definiálható a nemlokális korreláció különböző zajokra, mint például a fehér zajra és lokális zajra vonatkozó érzékenységből. Fehér zaj esetén például, ha adott a P korreláció, azt kérdezzük, hogy mi az a legnagyobb érték q -nak, aminek arányában P -hez hozzákeverve a teljesen korrelálatlan I fehér zajt, a $P' = (1-q)P + qI$ korreláció még mindig nemlokális. Megjegyezzük, hogy ezen q érték hatékonyan számolható lineáris programozás segítségével. Emellett a detektorhatékonysági küszöb nagysága is alkalmas nemlokalitási mérték meghatározására. Ennek a kiszámításánál a nem detektálási eseményt egy külön mérési kimenetelként vesszük figyelembe.

Egy másik érvényes mérték azon a megfigyelésen alapszik, hogy bármely nemlokális korreláció reprodukálható lokális modellel, ha a lokális modellt a Bell-kísérlet két szárnya közötti klasszikus kommunikációval egészítjük ki. Ilyenkor a reprodukáláshoz szükséges minimális klasszikus kommunikáció nagysága tekinthető egy nemlokalitás mértéknek. Ezzel kapcsolatosan Toner és Bacon 2003-ban megmutatta (Phys. Rev. Lett. 91, 187904), hogy maximálisan összefonódott

qubitpáron történt projektív mérésekből származó korrelációk reprodukálásához mindig elegendő 1 bit kommunikációval kiegészítünk a lokális modellt.

Végül a P korreláció statisztikus erőssége is használható nemlokalitási mérték definiálására. Ilyenkor a mérték annak a bizonytalansága, hogy a végtelen számú minta helyett adott véges számú mintát veszünk fel a Bell-kísérletben, és ebből kifolyólag egy lokális modellel leírható P korrelációt helytelenül nemlokálisnak azonosítunk be. Matematikailag ekkor a P pontnak a lokális halmaztól vett Kullback-Leibler távolsága használható mértékül.

Debrecen, 2020. január 27.

Vértesi Tamás