

PÉCSI TUDOMÁNYEGYETEM

Fizika Doktori Iskola

Kvantumoptika és kvantuminformatika Program

Az egy- és kétrésű rendszerek nemklasszikus viselkedéséről

Doktori disszertáció

Bodor András

témavezető:

Dr. Koniorczyk Mátyás

habil. egyetemi docens



Pécs, 2022

Tartalomjegyzék

Tartalomjegyzék	2
1. Bevezetés	4
2. Előzmények	6
2.1. Kvantumállapotok megkülönböztetése	6
2.1.1. Bináris klasszifikáció	7
2.1.2. ROC görbék	8
2.1.3. Kvantumállapot megkülönböztetés	12
2.2. Kétrésztű korrelációk	12
2.2.1. Diszkrét geometriai áttekintés	12
2.2.2. Jelölések, fogalmak	13
2.2.3. A CHSH elrendezés	15
2.2.4. Kvantum korrelációk	20
2.3. Játékelméleti áttekintés	24
2.3.1. Bayes-i játékok és egyensúlyaik	28
3. Eredmények	33
3.1. Kvantumállapotok megkülönböztetése	33
3.1.1. Bhattacharyya-együttható a ROC görbéből	33
3.1.2. A kvantumállapotok ROC görbéje	35
3.1.3. Egy kvantum Bhattacharyya-együttható	39
3.1.4. Két qubit	41
3.1.5. Két tetszőleges kvantumállapot	42

3.1.6. A kvantum Bhattacharyya-együttható tulajdonságai	44
3.1.7. Egyértelmű kvantumállapot megkülönböztetés	46
3.2. Kétrészi korrelációk és Bayes-i játékok	47
3.2.1. Numerikus módszerek	48
3.2.2. A 2-2-3-3 politópok szerkezete	54
3.2.3. Kvantumelőnnel rendelkező játékok konstrukciója	56
3.2.4. Egy új játék	61
3.2.5. Egy kivétel: a Vértesi-Bene játék	63
4. Összefoglalás és kitekintés	67
5. Tézisek	69
6. Summary	70
7. Köszönetnyilvánítás	72
8. A disszertációhoz kapcsolódó publikációk	74
9. Irodalomjegyzék	75

1. fejezet

Bevezetés

Ha biztonságosan akarsz közlekedni,
be kell tartanod a fizika törvényeit.
Ha nem – akkor is.

Ebben a disszertációban tárgyalt eredmények két csoportra oszthatók. Az első csoportba a kvantumállapotok megkülönböztetésével kapcsolatos eredmények tartoznak. Ezek egyrészt kvantumrendszerekkel kapcsolatosak, legalábbis abban az értelemben, hogy nem vizsgáljuk az állapottér esetleges tenzorszorzat szerkezetét. A második csoportba olyan eredmények tartoznak, amelyeket kétrésztű kvantumrendszerek viselkedésének vizsgálata motivált. Az alkalmazott megközelítés a kétrésztű rendszerek statisztikai viselkedésének olyan tulajdonságait vizsgálja, amiket általános elvek (például a fénysebességnél gyorsabb kommunikáció tilalma) határozhatnak meg, nem a rendszer (hardver) konkrét fizikai felépítése. Ezeknek például az eszközfüggetlen kriptográfiában van nagy jelentősége.

A régóta és rendkívül alaposan kutatott kvantumállapot megkülönböztetés területén egy eddig nem vizsgált megközelítést alkalmaztunk. A klasszikus statisztikából ismert ROC (Receiver Operating Characteristic) görbe diszkriminátorok sokaságának jellemzésére szolgál. Bevezettük ennek kvantum változatát, és vizsgáltuk egyes tulajdonságait. Ennek eredményeképp a görbét számos kvantummos mennyiséggel tudtuk összefüggésbe hozni, szemléletes képet nyerve azok összefüggéseiről. Ezen kívül találtunk egy, a ROC görbe alakjából természetesen adódó mennyiséget, a kvantum-Bhattacharyya-együtthatót, ami kvantumállapotok hasonlóságának számszerűsítésére szolgálhat.

A kétrészű rendszerek nemklasszikus viselkedésének vizsgálata a kvantuminformatika egyik központi kérdésköre. Mind elméleti (pl. Tsirelson-sejtés), mind gyakorlati (praktikus kvantum titkosító eszközök) téren kiemelkedő jelentőségű. Ezen belül egy viszonylag új kutatási iránnyal: a játékelméleti megközelítéssel foglalkoztunk. Bayes-i játékok egyensúlyai és a kétrészű korrelációk kapcsolatát vizsgálva módszert találtunk nemklasszikus előnnyel rendelkező játékok konstruálására. Különböző egyensúlyfogalmak felhasználásával feltártuk a Bell-egyenlőtlenségek bizonyos strukturális tulajdonságait is.

A dolgozat felépítése a következő: A 2. fejezetben áttekintjük az eredmények szempontjából lényeges előismereteket, módszereket és a kutatás előzményeit. A 2.1. részben a klasszikus és kvantum bináris klasszifikáció témakörét tekintjük át és bemutatjuk a ROC görbét. A 2.2. részben a kétrészű korrelációk témakörével foglalkozunk. Ez tartalmaz a politópokkal kapcsolatos diszkrét geometriai áttekintést, a lokális és nemjelző politópok és a kvantum halmazok definícióját, és részletesebben foglalkozunk a CHSH elrendezéssel. A 2.3 rész tartalmaz egy általános játékelméleti áttekintést és a mi szempontunkból lényeges Bayes-i játékokat bemutató részt.

A 3. fejezetben a saját eredményeket írjuk le. A 3.1. részben a ROC görbék kvantum-állapotok megkülönböztetésében lehetséges szerepét mutatjuk be, és a segítségével bevezetett új mennyiség, a kvantum Bhattacharyya-együttható tulajdonságait vizsgáljuk. A 3.2. részben a játékelméleti eredményeket ismertetjük. Szisztematikus módszert mutatunk be kvantumelőnnyel rendelkező játékok szerkesztésére, részletesebben vizsgáljuk a 2-2-3-3 elrendezést, és Vértesi-Bene játékkal mutatunk egy példát, ami eltér az általános mintázattól.

A 4. fejezetben röviden összefoglaljuk a dolgozat eredményeit és kitekintést adunk a lehetséges és már megvalósult további kutatási irányokra. A dolgozat a szokásos módon tézisekkel (5. fejezet), angol nyelvű összefoglalóval (6. fejezet) és köszönetnyilvánítással (7. fejezet) zárul.

2. fejezet

Előzmények

2.1. Kvantumállapotok megkülönböztetése

A mindennapi életben és a tudományos, mérnöki, orvosi feladatok végrehajtása során is gyakran ütközünk a *klasszifikáció* problémájába, amikor valamiről a rendelkezésre álló információk alapján el kell dönteni, hogy (véges lehetőségek közül) micsoda.

A bináris klasszifikáció esetén két lehetőség közül kell választani. Például:

- Egy páciensről el kell dönteni, hogy egy bizonyos betegségben szenved-e vagy nem.
- Egy vádlottról el kell dönteni, bűnös, vagy ártatlan.
- Egy radarjelről el kell dönteni, ellenséges repülőgéphez tartozik-e vagy nem.

Az érdekes (és nehéz) esetekben a döntéshez csak korlátozott információ áll rendelkezésre, a tökéletes döntéshez szükséges minden adat valamiért elérhetetlen, például a rendelkezésre álló pénz, idő elégtelensége, etikai, jogi akadályok miatt, vagy a hiányzó információ elvileg is elérhetetlen.

Amikor egy ilyen helyzetben az ideális megoldást keressük, egy lényeges része a dolognak azt megvizsgálni, hogyan tudnánk még több információhoz hozzájutni, de ez helyzetről helyzetre különböző, ezért amikor általánosan vizsgáljuk a bináris klasszifikáció problémáját, úgy kell vennünk, hogy a rendelkezésre álló információmennyiség rögzített.

Ezért a továbbiakban mindig úgy vesszük, hogy a klasszifikálandó rendszer két teljesen

ismert állapot egyikében van, ahol az állapotok teljes ismerete azt jelenti, hogy egy klasszikus valószínűségeloszlással vagy egy kvantumállapottal írható le.

2.1.1. Bináris klasszifikáció

A klasszikus alapesetben azonos eseménytérre lévő valószínűségi változó két különböző valószínűségi mérték szerinti eloszlását kell megkülönböztetni¹. A megkülönböztetés szempontjából a valószínűségi változó konkrét értékei nem jelentősek, a lényeg az, hogy a mérés (a változó mintavétele) után a kapott érték alapján be tudjuk határolni az eseménytér valamely tartományát. Például egy kockadobás esetén az eseménytér egytől hatig az egész számok, a mintavétel (kockadobás) után a valószínűségi változónk értéke a kockadobás értéke. De amikor két valószínűségi mértéket akarunk megkülönböztetni (mondjuk cinkelt kocka – szabályos kocka) akkor a konkrét értékek, vagy például a hatos nagyobb mint az egyes, nem számítanak, a lényeg, hogy van egy hitelemű eseményterünk, és a kockadobás ennek egyetlen elemét jelöli ki. Tehát a rendelkezésre álló mérésekből csupán az eseménytér behatárolási képességük érdekes.

Most vizsgáljuk meg közelebbről két valószínűségeloszlás megkülönböztetését. Először vegyünk két bináris változót.

Két bináris változó Tegyük fel, hogy van egy bináris véletlen változónk (vagyis egy klasszikus bit) aminek lehetséges értékei: 0 és 1. A változó két lehetséges eloszlás egyikét követi:

$$(p, 1 - p) \quad \text{vagy} \quad (q, 1 - q), \quad (2.1)$$

ahol $p, q \in [0, 1]$. A két eloszlás előre ismert. Azt szeretnénk eldönteni, hogy a változó az első eloszlást követi-e. Ezt az eseményt \mathfrak{P} -vel (mint pozitív) jelöljük, míg a komplementer eseményt \mathfrak{N} -nel (negatív). Ezen kívül $\Pr(\mathfrak{P}) = \lambda \in [0, 1]$ szintén legyen előre ismert. (Ez utóbbi követelmény implicite azt is feltételezi, hogy létezik a „valószínűségeloszlások valószínűségeloszlása”, tehát hogy ténylegesen az első vagy második eloszlást követi-e a bináris változónk, az is egy „meta” valószínűségi változó.)

¹A valószínűségi változó fogalmába időnként az eloszlását is beleértik, ebben az értelemben ez két külön változónak számítana, de mi csak az eseményteret és az értékek hozzárendelését tekintjük rögzítettnek.

A döntési folyamat során először mérést kell végezni a valószínűségi változónkon. A mérés kétféle kimeneteléhez tartozó két eseményt a mért értékkel (0 és 1) jelöljük. Végül a mérési eredmények alapján meg kell tippelnünk, vajon melyik volt a tényleges eloszlás. A két lehetséges választásunkhoz tartozó eseményeket jelölje p (ha az elsőt választottuk) és n (ha a másodikat).

2.1.2. ROC görbék

Azt az eljárást, amivel a 0/1 mérésekből meghatározzuk a p/n döntésünket, klasszifikátornak nevezzük. (Bináris klasszifikáció esetén bináris klasszifikátorról beszélünk.)

A lehetséges klasszifikátorok tulajdonságait a ROC (Receiver Operating Characteristic²) téren tanulmányozhatjuk[2]: minden klasszifikátort egy pont jellemez itt, a függőleges tengelyen a $\Pr(p|\mathfrak{P})$ feltételes valószínűség, a vízszintesen $\Pr(p|\mathfrak{N})$. Ha a döntési eljárást megismételnénk egy nagy számú mintán, az első mennyiség a *valódi pozitív ráta*, a második a *hamis pozitív ráta* lenne.

Egy klasszifikátor esetén a „döntési folyamatot” az alábbi feltételes valószínűségekkel jellemezhetjük:

$$\begin{aligned} \Pr(p|0) &= p_{a,p}, \\ \Pr(n|1) &= p_{a,n}, \\ \Pr(n|0) &= 1 - p_{a,p}, \\ \Pr(p|1) &= 1 - p_{a,n}, \end{aligned} \tag{2.2}$$

ahol $p_{a,p}, p_{a,n} \in [0, 1]$ az *elfogadási valószínűségek*. A $p_{a,p} = p_{a,n} = 1$ eset például ahhoz a determinisztikus eljáráshoz tartozik, ahol 0-t \mathfrak{P} indikátorának, 1-et pedig \mathfrak{N} indikátorának tekintjük. De lehetséges probabilisztikus algoritmust is választani.

Vegyük észre, hogy a meta valószínűségeloszlás (más néven a prior) ($\mathfrak{P}/\mathfrak{N}$), majd a mérési eredmény (0/1), végül a döntés (p/n), mint véletlen változók egy Markov-láncot

²A ROC története a második világháborúba nyúlik vissza, amikor az Egyesült Államok hadserege a Pearl Harbor-i támadás után kutatni kezdte, hogyan lehetne nagyobb hatékonysággal azonosítani a japán repülőgépeket a visszavert radarjelük alapján. Ezért mérni kezdték a radarkezelők teljesítményét ezen a téren, ezt a mértéket nevezték Receiver Operating Characteristic-nek. [1].

alkotnak³.

Az adott helyzetben

$$\Pr(p|\mathfrak{F}) = \Pr(p|0, \mathfrak{F})\Pr(0|\mathfrak{F}) + \Pr(p|1, \mathfrak{F})\Pr(1|\mathfrak{F}). \quad (2.3)$$

A Markov-láncból tudjuk, hogy $\Pr(p|0, \mathfrak{F}) = \Pr(p|0)$ és $\Pr(p|1, \mathfrak{F}) = \Pr(p|1)$ és ezeket a valószínűségeket megkaphatjuk a (2.2) egyenletből, a többit pedig a (2.1) egyenletből, így

$$\Pr(p|\mathfrak{F}) = p_{a,p}p + (1 - p_{a,n})(1 - p). \quad (2.4)$$

A hamis pozitív ráta

$$\Pr(p|\mathfrak{N}) = \Pr(p|0, \mathfrak{N})\Pr(0|\mathfrak{N}) + \Pr(p|1, \mathfrak{N})\Pr(1|\mathfrak{N}), \quad (2.5)$$

amit hasonlóan kiszámítva kapjuk:

$$\Pr(p|\mathfrak{N}) = p_{a,p}q + (1 - p_{a,n})(1 - q). \quad (2.6)$$

Vagyis egy adott p és q esetére $p_{a,p}p + (1 - p_{a,n})(1 - p)$ értékét kell ábrázolni $p_{a,p}q + (1 - p_{a,n})(1 - q)$ függvényében minden lehetséges $(p_{a,p}, p_{a,n})$ elfogadási valószínűségekre mint paraméterre, hogy megkapjuk az összes lehetséges klasszifikátor ROC diagramját. Vegyük észre, hogy ez nem függ λ -tól. Ez a klasszifikátorokat a két megkülönböztetendő valószínűségeloszlás alapján jellemzi, nem azok prior eloszlása alapján.

A (2.6) és (2.4) egyenletek által meghatározott pontthalmaz ábrázolásához fejezzük ki $(1 - p_{a,n})$ -t a (2.6) egyenletből:

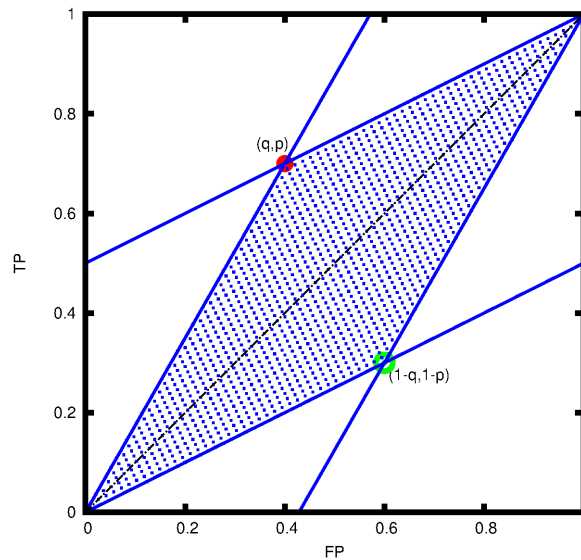
$$0 \leq (1 - p_{a,n}) = \frac{x - p_{a,p}q}{1 - q} \leq 1. \quad (2.7)$$

Ezt behelyettesítve (2.4)-be egy kis számolás után azt kapjuk, hogy

$$y = \frac{1 - p}{1 - q}x + \left(p - \frac{1 - p}{1 - q}q\right)p_{a,p} = Ax + Bp_{a,p}. \quad (2.8)$$

Kizártuk a triviális eseteket, amikor $p, q = 0$ vagy 1 . $p_{a,p} = 0$ esetére ez egy, az origón átmenő egyenest határoz meg a ROC téren. $p_{a,p} = 1$ esetére egy ezzel párhuzamos egyenest az első fölött vagy alatt B előjelétől függően. A megengedett régió ezen párhuzamos vonalakon

³A valószínűségszámítási és információelméleti fogalmakat Cover könyvében definiált módon használjuk [3].



2.1. ábra. Az elérhető ROC tartomány bináris valószínűségeloszlásokra $p = 0.7$, $q = 0.4$ esetén.

belül (vagy rajtuk) helyezkedik el. $p_{a,p}$ hasonlóan megszorítja az elérhető tartományt a (2.7) egyenlet alapján. Ismét két párhuzamos egyenest kapunk, melyek egyenlete:

$$y = \frac{p}{q}x \tag{2.9}$$

és

$$y = \frac{p}{q}x + (1-p) - \frac{p}{q}(1-q). \tag{2.10}$$

(Ezek közül az egyik a ROC tér „jobb felső sarkán”, az $(1, 1)$ ponton megy keresztül.) Vagyis a ROC tér elérhető tartománya egy paralelogramma, a $(0, 0)$, $(1, 1)$, (q, p) és $(1-q, 1-p)$ pontok konvex burka. Egy példa látható a 2.1 ábrán.

A ROC térben minél jobb egy klasszifikátor, annál közelebb van a hozzá tartozó pont a $(0, 1)$ ponthoz (ami 1 valódi pozitív és 0 hamis pozitív rátát jelent). Vagyis a ROC diagram legérdekesebb része a felső (konkáv) töröttvonal $(0, 0) \rightarrow \mathbf{P} \rightarrow (1, 1)$, ahol a \mathbf{P} pont vagy (q, p) , vagy $(1-q, 1-p)$. Az utóbbi esetben végrehajthatjuk a $p \rightarrow 1-p$ és $q \rightarrow 1-q$ cseréket, amivel ugyanazt az alakzatot kapjuk, de a két pont felcserélődik. Vagyis az általánosság megszorítása nélkül feltehetjük, hogy a $\mathbf{P} = (q, p)$ pont a felső töröttvonalon fekszik.

Vegyük észre, hogy a lehetséges legjobb klasszifikátorokat reprezentáló vonal, amit „optimális ROC görbének” is nevezhetünk, a két kumulatív eloszlás $(0, q, 1)$ és $(0, p, q)$ egymás

függvényében felrajzolt három pontját kötik össze.

Fontos megjegyezni, hogy a ROC tartomány konvex. Ha veszünk két pontot, amik két megvalósítható diszkriminátort jellemeznek, a kettőt összekötő szakasz minden pontja szintén megvalósítható diszkriminátorhoz tartozik. Ezeket úgy kaphatjuk, hogy a végpontokhoz tartozó diszkriminátorok közül egy bináris véletlen változó értéke alapján választunk [2]. A $p_{a,p}$ és $p_{a,n}$ paraméterek optimális megválasztása nem teljesen nyilvánvaló. A (q, p) pontban $p_{a,p} = p_{a,n} = 0$, ami azt jelenti, hogy determinisztikusan p -t választjuk, ha 1-et mértünk, és n -t, ha 0-át. Természetesen a valódi pozitív ráta ekkor p , a hamis pozitív pedig q . A $(0, 0)$ és $(1, 1)$ pontok rendre a $p_{a,p} = 0, p_{a,n} = 1$ és $p_{a,p} = 1, p_{a,n} = 0$ paraméterekhez tartoznak. Ebben az esetben a mérési eredménytől függetlenül mindig p -t illetve n -t választjuk.

Keressük meg azokat a pontokat a ROC térben, amik konstans hibázási valószínűséghez tartoznak feltéve, hogy adott a λ -val jellemzett prior eloszlás. A hibázás valószínűsége:

$$\begin{aligned} \Pr(\text{hiba}) &= \Pr(p, \mathfrak{N}) + \Pr(n, \mathfrak{P}) = \Pr(\mathfrak{N}) \Pr(p|\mathfrak{N}) + \Pr(\mathfrak{P}) \Pr(n|\mathfrak{P}) \\ &= (1 - \lambda) \Pr(HP) + \lambda(1 - \Pr(VP)). \end{aligned} \quad (2.11)$$

Vagyis egy adott $\Pr(\text{hiba})$ -hoz egy egyenes tartozik a ROC térben:

$$\Pr(VP) = \frac{\lambda - \Pr(\text{hiba})}{\lambda} + \frac{1 - \lambda}{\lambda} \Pr(HP), \quad (2.12)$$

aminek meredeksége $(1 - \lambda)/\lambda$.

Végezetül vizsgáljuk meg az N lehetséges értékkel rendelkező valószínűségi változók esetét. Meg lehet mutatni, hogy ekkor úgy kaphatjuk meg az optimális ROC görbét, ha a kimeneteket p_i/q_i szerint csökkenő sorrendbe rendezzük, majd az így rendezett halmazhoz tartozó kumulatív eloszlásokat egymás függvényében ábrázoljuk. Az így kapott pontok összekötésével kapjuk az optimális görbét. A továbbiakban ezt ROC görbének nevezzük. (Az irodalomban ehelyett sokszor egy folytonos paraméteres diszkriminátorhalmaz képét nevezik ROC görbének.)

Az optimális ROC görbe megadásának kiterjedt irodalma van, lásd például Medlock és Oppenheim cikkét [4] (akik megadnak egy új eljárást) és a cikkben lévő hivatkozásokat.

2.1.3. Kvantumállapot megkülönböztetés

Két kvantumállapot megkülönböztetése a kvantuminformáció-elmélet egyik központi, jól megértett problémája. Ha adott egy kvantumállapot és prior információ arról, hogy ez valamilyen valószínűséggel két adott állapot egyike, határozzuk meg olyan pontosan ahogy csak lehet, hogy a kettő közül melyik. Az ezzel kapcsolatos rengeteg eredményt például Bergou, Ulrike és Mark [5] vagy Bae és Kwek [6] áttekintő cikkéből lehet megismerni.

Mi itt most csak a legfontosabb alapesetet tekintjük át. Ha az ismeretlen állapot $p_{\mathfrak{P}}$ valószínűséggel $\rho_{\mathfrak{P}}$, $p_{\mathfrak{N}}$ valószínűséggel $\rho_{\mathfrak{N}}$, akkor a tévedés valószínűségét minimalizáló mérést a Hellstrom formulával kaphatjuk meg [7].

Ehhez venni kell a következő hermitikus, de nem pozitív definit operátort:

$$\Lambda = p_{\mathfrak{P}}\rho_{\mathfrak{P}} - p_{\mathfrak{N}}\rho_{\mathfrak{N}}. \quad (2.13)$$

A mérést alkotó két operátornak Λ pozitív sajátértékű illetve negatív sajátértékű saját altereire kell vetíteni, ezek automatikusan ortogonálisak, vagyis egy projektív mérést adnak. (Ha van, Λ nullterét bármelyik projektorhoz hozzávehetjük, az a tévedés valószínűségét nem befolyásolja.)

2.2. Kétrészi korrelációk

Ebben a fejezetben a nemklasszikus korrelációk elméletének szükséges részleteit ismertetem.

2.2.1. Diszkrét geometriai áttekintés

A nemklasszikus korrelációk vizsgálatához szükségünk van a politópok elméletének [8, 9] egyes elemeire. A következőkben ezeket tekintjük át.

Intuitíve egy politóp a „sík lapokkal határolt test” általánosítása. Pontosán:

Egy (konvex) politóp a d dimenziós euklidészi tér egy olyan konvex kompakt részhalmaza, aminek csak véges sok extrémális pontja⁴ van.

⁴Egy konvex halmaz extrémális pontja a halmaz egy olyan eleme, ami nem áll elő más pontok konvex

Egy konvex politópot többféleképpen is meg lehet adni, ezek közül a két legfontosabb a csúcs- és a laprepresentáció. Csúcsrepresentációban a test extrémális pontjait adjuk meg, és a politóp ezek konvex burka. (Vehetjük tetszőleges ponthalmazok konvex burkát is de ekkor nem garantált, hogy mindegyik pont extrémális lesz. Ezeket utólag ki kell szűrni a representációból.)

Laprepresentációban a politópot határoló hipersíkokat adjuk meg lineáris egyenlőtlenségek formájában. Például két dimenzióban az $x \leq 1, y \geq 0, y - 2x \leq 1$ egy derékszögű háromszöget határoz meg. (Ha csak úgy vesszük egyenlőtlenségek egy halmazát, akkor egyrészt lehet, hogy nem mindegyik egyenlőség határozza meg a politóp valamelyik lapját, mert a többi egyenlőtlenség által behatárolt térrész teljesen ezen hipersík egyik oldalán fekszik, másrészt az is előfordulhat, hogy az egyenlőtlenségek nem egy véges átmérőjű részt jelölnek ki.)

A csúcsrepresentáció tipikusan a politóp definíciójánál hasznos, hiszen gyakran fel tudjuk sorolni az összes extrémális pontot. A laprepresentáció akkor jön jól, ha egy tetszőleges pontról el kell dönteni, hogy benne van-e a politópban, hiszen elegendő leellenőrizni, hogy a pont kielégíti-e az összes egyenlőtlenséget. Ezért fontos, hogy tudjunk váltogatni a két representáció között. Ez a legáltalánosabb esetben egy nemtriviális feladat például azért is, mert előfordulnak olyan politópok, amiknek sokkal több csúcsuk van, mint lapjuk, vagy fordítva.

2.2.2. Jelölések, fogalmak

Tekintsünk egy olyan kísérletet, amelyet két fél hajt végre, akár két különböző helyszínen. A feleket hagyományosan Alíznek és Bobnak hívjuk. A kísérlet egy körében mindketten egymástól függetlenül választhatnak egy mérést, amit végrehajtanak egy a rendelkezésükre álló fizikai rendszeren, és megkapják a mérési eredményt. Az Alíz és Bob által választható mérések halmazát rendre X és Y jelöli, a kapható mérési eredmények halmazát A és B , kombinációjaként. Az még általában nem elég, ha egy pont a halmaz határán van. Két dimenzióban egy háromszög extrémális pontjai a három csúcsa, az oldalak többi pontja előállítható a két csúcsuk konvex kombinációjaként. Egy kör esetén viszont minden határpont extrémális, hiszen minden érintője csak egy pontban érinti a kört.

amennyiben az egyik fél által végezhető méréseknek mind ugyanazok a lehetséges kimenetei, vagy A_x és B_y , ahol $x \in X, y \in Y$ az általános esetben.

Annak valószínűségét, hogy x és y mérés választása esetén az eredmények a és b

$$p(ab|xy) \quad x \in X, y \in Y, a \in A_x, b \in B_y \quad (2.14)$$

jelöli. A feltételek, hogy minden x, y -ra ezek valószínűségeloszlást alkossanak:

$$\forall x \in X, y \in Y : \sum_{a \in A_x, b \in B_y} p(ab|xy) = 1, \quad (2.15)$$

$$\forall x \in X, y \in Y, a \in A_x, b \in B_y : p(ab|xy) \geq 0, \quad (2.16)$$

vagy ha normalizáljuk az egyenlőtlenségeket:

$$\forall x \in X, y \in Y : \sum_{a \in A_x, b \in B_y} p(ab|xy) = 1, \quad (2.17)$$

$$\forall x \in X, y \in Y, a \in A_x, b \in B_y : p(ab|xy) + \frac{1}{|A_x||B_y| - 1} - \frac{1}{|A_x||B_y| - 1} \sum_{a' \in A_x, b' \in B_y, (a' \neq a \vee b' \neq b)} p(a'b'|xy) \geq 0. \quad (2.18)$$

($|A|$ az A halmaz számosságát jelenti). A $p(ab|xy)$ eloszlást *viselkedésnek* vagy egyszerűen *korrelációnak* is nevezzük a továbbiakban.

Természetesen merül fel a kérdés, hogy milyen megszorítások vonatkozhatnak a $p(ab|xy)$ együttes feltételes eloszlásra. Gyakori feltevés, amellyel élünk is a továbbiakban, hogy a két kísérletező egymástól függetlenül választhatja meg és hajthatja végre a mérését. A két mérés eseménye akár térszerűen elválasztott is lehet, ezért meg kell követelnünk, hogy a két szereplő közt ne lehessen információátvitel. Ezt *nemjelzési* (angolul *no-signaling*) feltételnek nevezzük; matematikai alakja a következő:

$$\begin{aligned} \forall x, x' \in X, y \in Y, b \in B_y : \sum_{a \in A_x} p(ab|xy) &= \sum_{a \in A_{x'}} p(ab|x'y), \\ \forall x \in X, y, y' \in Y, a \in A_x : \sum_{b \in B_y} p(ab|xy) &= \sum_{b \in B_{y'}} p(ab|xy'). \end{aligned} \quad (2.19)$$

Az első egyenlet azt fejezi ki, hogy Alíz nem küldhet információt Bobnak, a második az ellenkező irányra vonatkozik. A nemjelzési feltételekben nem teszünk fel semmit a rendszer belső működéséről. A fenti egyenletek nem zárják ki, hogy minden elektronban egy telepikus képességekkel rendelkező manó lakjon. Csupán annyit tiltunk meg, hogy maguk

a kísérletezők – valamilyen ravasz módon ezeket a kismanókat kihasználva – üzeneteket küldjenek *egymásnak*. Ehhez pedig az kell, hogy a rendszerből Bob által kinyerhető információt ne tudja befolyásolni Alíz. Mivel Alíz egyetlen lehetséges ráhatása a rendszerre a mérés megválasztása, ettől kell függetlennek lennie a Bob által kimérhető valószínűségeloszlásnak, ezt fejezik ki az egyenletek.

A $p(ab|xy)$ számokat tekinthetjük egy $\sum_{x,y} |A_x||B_y|$ dimenziós valós vektortér pontjának a szokásos metrikával ellátva. Ebben az esetben, mivel a pontok értékeit megszorító feltételek mind lineáris egyenlőtlenségek, és valószínűségek lévén az egység hiperkockán belül kell lenniük, ezért a nemjelző feltételnek eleget tevő pontok egy politópot alkotnak.

Az egyik fél által kimérhető eloszlást – vagyis a közös eloszlás marginálisát – így jelöljük:

$$p(a|xy) = \sum_{b \in B_y} p(ab|xy), \quad (2.20)$$

$$p(b|xy) = \sum_{a \in A_x} p(ab|xy). \quad (2.21)$$

Amikor a nemjelző politópon belül vagyunk, akkor Alíz marginálisja független y -tól, Bobé x -től (igazából ez a nemjelzés definíciója), ekkor egyszerűen $p(a|x)$ és $p(b|y)$ a jelölésük ⁵.

A véges halmazok elemeinek általában nullától kezdve a megfelelő számú természetes számot vesszük. Amikor egy konkrét elrendezés paramétereiről beszélünk, érdemes a valószínűségeket egy táblázatba rendezni. A következőkben bemutatunk néhány konkrét példát.

2.2.3. A CHSH elrendezés

A kétrészű rendszerek közül az a konfiguráció kapta a legtöbb figyelmet, ahol mindkét résztvevő két mérés közül választhat, és mindegyik mérésnek két lehetséges kimenete van. (Érthető, hiszen ez a lehető legegyszerűbb nemtriviális elrendezés. Megvizsgáltsága vetekszik az egy qbit állapotterével.) Ezt először Clauser, Horne, Shimony és Holt [10] vizsgálták. Két példa eloszlást láthatunk a 2.1. táblázatban.

Ahhoz, hogy egy ilyen rendszert statisztikailag leírassunk, 16 szám bizonyosan elegendő. Hiszen Alíz és Bob választásai alapján összesen négy lehetséges szituációval találkozhatja szemben magát a rendszer, és mindegyik esetben négy lehetséges válasza van.

⁵Ha a -t, b -t stb. konkrét értékekkel helyettesítjük, akkor nem lehet tudni, hogy pl. $p(0|1)$ mit jelent, ilyenkor így módosítjuk a jelölést: $p(a = 0|x = 1)$ vagy csak $p(0|x = 1)$ mert a már ebből kikövetkeztethető.

$x \downarrow y \rightarrow$		0		1	
		0	1	0	1
0	0	3/8	1/8	3/8	1/8
	1	1/8	3/8	1/8	3/8
1	0	3/8	1/8	1/8	3/8
	1	1/8	3/8	3/8	1/8

$x \downarrow y \rightarrow$		0		1	
		0	1	0	1
0	0	1/2	0	1/2	0
	1	0	1/2	0	1/2
1	0	1/2	0	0	1/2
	1	0	1/2	1/2	0

2.1. táblázat. *Két példa korreláció. A bal szélső oszlopban és a felső sorban X és Y elemei. A belső négy kis 2×2 mátrixban a négy eloszlás. Az első a lokális politóp egy felszíni (de nem extrémális) pontja, a második a nemjelző politóp híres extrémális pontja, a „PR-doboz” (Popescu-Rorhlich doboz).*

Természetesen ezt a 16 paramétert nyomban lecsökkenthetjük 12-re, hiszen a rendszer válasza négy külön valószínűségeloszlást képeznek. Sajnos még nem találtak igazán jó módszert arra, hogy egy d dimenziós diszkrét valószínűségeloszlás d paramétere (az események egyedi valószínűségei) közül hogyan szabaduljunk meg egytől, ezért legcélszerűbb nekünk is egy 16 dimenziós tér 12 dimenziós affin alterében maradni. További megszorítást jelent, hogy a valószínűségek nem lehetnek negatívak, de ez nem csökkenti a paramétertér dimenzióját, hanem egy politópot vág ki belőle.

Egy egyszerűbb példaként: a háromdimenziós valószínűségeloszlás \mathbb{R}^3 -ból a $p_0 + p_1 + p_2 = 1$ kétdimenziós síkot jelöli ki, és ebből a $p_i \geq 0$ feltételek egy egyenlő oldalú háromszöget vágnak ki. Négy dimenzióban (a mi esetünk) háromdimenziós affin alteren egy szabályos tetraéder (általános esetben pedig egy $d - 1$ dimenziós szabályos szimplex) lesz a paraméterek megengedett halmaza.

És itt belebotlunk az első technikai nehézségbe. Egy affin alteret majdnem bármilyen egyenlőtlenség két részre vág (kivéve az alterrel párhuzamos hipersíkokat), így jellemezni lehet velük a politóp egy lapját, de a politóp egy bizonyos lapját számos különböző egyenlőtlenség is meghatározhatja. (Ahhoz hasonlóan, hogy mindegy, milyen szögben tartjuk a ceruzát a vonalzóhoz, ugyanazt a vonalat lehet vele meghúzni.)

A dolgot egyértelművé tehetjük, ha megköveteljük, hogy az egyenlőtlenség által meghatározott hipersík merőleges legyen az affin alterre. A valószínűségi politóp esetén $p_i \geq 0$ helyett $dp_i - \sum_{j=1}^d p_j \geq -1$ ⁶. Tehát valószínűségszámítás órán ahelyett, hogy a valószínűségek nem negatívak, taníthatnánk azt is, hogy mindegyik valószínűség legfeljebb $\frac{1}{d-1}$ -el lehet kisebb, mint a többi valószínűség átlaga, de ezt valószínűleg jóval nehezebb lenne elmagyarázni a diákoknak.

A négy külön eloszlás által meghatározott négy tetraéder Descartes-szorzata az a tartomány, ami a CHSH elrendezésben vizsgálható rendszerek legáltalánosabb viselkedési lehetőségeit leírja. Aki innen kimozdul, annak számot kell adnia olyan dolgokról, mint például a negatív vagy egynél nagyobb valószínűségek lehetősége.

Ez a tartomány nem csak a lehetséges burkoló, ennek minden pontjához ténylegesen el

⁶Ez úgy jön ki, hogy a határoló hipersík normálvektorának merőlegesnek kell lennie a $\sum_{j=1}^d p_j = 1$ sík normálvektorára, ami $(1, 1, \dots, 1)$, ennek eléréséhez viszont szabadon hozzáadhatjuk a sík egyenletének szám-szorosát az egyenlőtlenséghez.

is tudunk készíteni az általa leírt viselkedést leíró fizikai rendszert. De ehhez az szükséges, hogy a mérési futam során valamilyen felsőbb hatóság begyűjtse mindkét résztvevőtől azt, hogy melyik mérést választották, majd a teljes információ birtokában a megfelelő valószínűségeloszlás szerint egy véletlen generátorral kiszámítsa Alíz és Bob mérési eredményeit. Ez csak akkor lehetséges, ha Alíz döntése és Bob mérési eredménye, illetve Bob döntése és Alíz mérési eredménye oksági kapcsolatban állhatnak egymással, vagyis – ha hiszünk a speciális relativitáselméletben – egymástól időszerűen elválasztottak.

A valóságban azonban – Alíz és Bob viszonylag nagy távolsága és gyors detektorok segítségével – viszonylag könnyen előállíthatunk egy olyan mérési elrendezést, ahol a fenti feltétel nem teljesül, Alíz döntése és Bob mérési eredménye térszerűen elválasztott lesz: a nemjelző politópba kerülünk. Matematikailag ez a (2.19) feltételek teljesülését jelenti. Ez az esetünkben újabb négy egyenlőséghez vezet, amik a valószínűségi politópból kimetszenek egy 8 dimenziós részt, a CHSH elrendezésben ez a nemjelző politóp.

Abban az esetben, ha a szereplők a méréseket egymástól térszerűen elválasztott tartományokban végzik, akkor a nemjelző politóp határait csupán egy fundamentális feltevés – a fénynél gyorsabb információtovábbítás lehetetlensége – jelöli ki. Viszont mai ismereteink szerint a fizika alaptörvényeinek engedelmességekkel ezen politóp nem minden pontjának megfelelő korrelációkat lehet megvalósítani.

A következő, kisebb tartomány lehetne a fizikailag megvalósítható tartomány. Ehhez persze rendelkezniünk kellene egy modellel, ami leírja a világegyetem működését (de ennek bemutatása meghaladja e dolgozat kereteit). A kutatások középpontjában ezért a nemrelativisztikus kvantummechanikai rendszerekkel megvalósítható korrelációk állnak, ezeket tekinthetjük a „fizikailag megvalósítható” korrelációknak. Ez bizonyosan nem politóp, „görbe” felületek is határolják, és valószínűleg rendkívül bonyolult határa van nagyobb dimenziós (értsd: több mérési lehetőség és több lehetséges kimenet) esetben. Sőt, igazából két különböző módon is értelmezhetjük azt, hogy mit jelent egy kvantumrendszer két részénél, hogy térszerűen el vannak választva, és ha a Tsirelson-sejtés [11, 12] nem igaz, akkor végtelen dimenziós Hilbert-térrel leírható rendszerek esetén ez a két értelmezés különböző alakú „fizikailag megvalósítható” tartományt ad. A szóban forgó tartomány ismert karakterizálására a 2.2.4 pontban még visszatérünk.

$x \downarrow y \rightarrow$		0		1	
		0	1	0	1
0	0	1	0	0	1
	1	0	0	0	0
1	0	1	0	0	1
	1	0	0	0	0

2.2. táblázat. A CHSH elrendezés lokális politópjának egy extrémális pontja.

Szépérezékünknek sokkal jobban megfelelne, ha a nemjelző politóphoz hasonlóan a „fizikailag megvalósítható” tartományt is definiálhatnánk valamilyen könnyen megérthető általános elvvel, ahelyett, hogy csak annyit mondunk: így működik a világ”. Noha sok érdekes eredmény mutat ebbe az irányba (ld. pl. [13]), idáig ilyen elvet nem sikerült találni.

A legkisebb figyelemreméltó tartomány a lokális politóp. Ezek azok a korrelációk, amik akkor lennének megvalósíthatók, ha a világ úgy működne, ahogyan azt Einstein szeretett volna [14]. Vagyis alapvetően nem egy statisztikus elmélet írná le, hanem az Alíz és Bob által vizsgált rendszerek eleve minden lehetséges mérésre „előre tudják” a mérési eredményt. Pontosabban: a világ működése teljesen determinisztikus, a méréseink bizonytalansága kizárólag a tudatlanságunkból ered, vagyis, hogy nem rendelkezünk az összes szükséges információval az eredmény megjóslásához, illetve, hogy a kísérletek megismétlésénél képtelenek vagyunk „tényleg” mindig ugyanabból a kezdőállapotból indítani a rendszert. (Az általunk nem ismert információt szokás rejtett paramétereknek hívni.)

A lokális politóp extrémális pontjai a lokális determinisztikus csatornák szorzatai, vagyis amikor minden mérés kimenete helyben előre meg van határozva. A nemjelző feltétel miatt elég külön-külön megadni Alíz és Bob mérési eredményeit. Így általában

$$\prod_{x \in X} |A_x| \prod_{y \in Y} |B_y| \quad (2.22)$$

lehetőség van. A CHSH esetben az extrémális pontok száma 16.

Ennek a politópnak az oldalait leíró egyenlőtlenségek a híres Bell-egyenlőtlenségek. Az összes oldalt először Arthur Fine találta meg 1982-ben [15]. A valószínűségi megszorítás-

kon kívül az alábbi 8 egyenlőtlenségnek kell teljesülnie (Fine jelölésével):

$$-1 \leq P(AB) + P(AB') + P(A'B') - P(A'B) - P(A) - P(B') \leq 0. \quad (2.23)$$

A másik hat egyenlőtlenséget A, A' , illetve B, B' felcserélésével kapjuk. Ugyanez a dolgot a dolgotat-beli jelöléssel:

$$-1 \leq p(00|00) + p(00|01) + p(00|11) - p(00|10) - p(0|x=0) - p(0|y=1) \leq 0. \quad (2.24)$$

2.2.4. Kvantum korrelációk

A nemjelző politóp leírásánál nem egy konkrét fizikai modellt vizsgáltunk, csak egy alapelv (nincs kommunikáció) teljesülését követeltük meg, amikor az elvileg lehetséges korrelációkat kerestük. Most nézzük meg, mit mondhatunk, ha Alíz és Bob rendszerei a kvantummechanika szabályai szerint viselkednek. A kérdést látszólag könnyen megfogalmazhatjuk, de hamarosan egy nem várt nehézségbe fogunk ütközni.

Ebben az esetben azt feltételezzük, hogy létezik egy kvantumrendszer, ami két részrendszerből áll. A teljes rendszer valamilyen ismert inicializálása után a két részrendszert Alíz és Bob birtokába adjuk, akik valahogy *egymástól függetlenül* információt nyernek ki a saját részrendszerükből.

Matematikailag megfogalmazva: létezik egy Hilbert-tér \mathcal{H} , ami két másik Hilbert-tér tenzorszorzataként áll elő: $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Az információkinyerés legáltalánosabb kvantummechanikai modellje az általánosított mérés. A POVM (pozitív operátor értékű mérték) minden $a \in A$ mérési kimenetelhez egy M_a pozitív szemidefinit operátort rendel oly módon, hogy

$$\sum_{a \in A} M_a = \mathbb{1}, \quad (2.25)$$

és az a kimenetet

$$p(a) = \text{Tr} \rho M_a \quad (2.26)$$

valószínűséggel adja a mérés [16]. Esetünkben tehát minden $x \in X$ -hez és $y \in Y$ -hoz létezik rendre egy $|A_x\rangle$ és $|B_y\rangle$ elemű POVM (M_a^x és M_b^y operátorokkal), és létezik egy \mathcal{H} -n

értelmezett ρ állapot, hogy a megadott korrelációkat a mérési eredmények valószínűségei adják:

$$p(ab|xy) = \text{Tr}(\rho M_a^x \otimes M_b^y). \quad (2.27)$$

Az általánosság megszorítása nélkül feltehetjük, hogy ρ tiszta állapot, a mérések pedig projektív mérések, ha nem bánjuk, hogy az eredetivel esetleg valamivel nagyobb Hilbert-térben kell dolgoznunk, hiszen minden kevert állapot és Naimark dilatációs tétele szerint minden POVM „felhígítható” egy nagyobb dimenziós térbeli tiszta állapottá és projektív méréssé [16, 17].

A Hilbert-terek mérete alapján a következőképp osztályozhatjuk a korrelációkat: Jelölje $C_q(n)$ az $n \times n$ dimenziós Hilbert-téren (a (2.27) értelemben) realizálható korrelációkat, $C'_q(n)$ az $n \times n$ dimenziós Hilbert-téren tiszta állapotokkal és projektív mérésekkel realizálható korrelációkat. A Hilbert-tér lehet szeparábilis végtelen dimenziós is, ezt jelöljük C_{qs} -sel. Ebben az esetben nem kell megkülönböztetnünk a tiszta és kevert esetet, mert a Hilbert-tér a higitás után is szeparábilis marad. A valamilyen véges dimenziós Hilbert-téren realizálható korrelációk az egyes $C_q(n)$ halmazok uniói, így legyen

$$C_q = \bigcup_{n \in \mathbb{N}} C_q(n), \quad (2.28)$$

$$C'_q = \bigcup_{n \in \mathbb{N}} C'_q(n). \quad (2.29)$$

Mivel $C'_q(n) \subseteq C_q(n) \subseteq C'_q(n^2 d)$, ahol $d = (\max_x |A_x|)(\max_y |B_y|)$, ezért C_q és C'_q egyenlő.

A $C_q(n)$ halmazok konvexek és zártak, és $C_q(n) \subseteq C_q(n+1)$, ezért az uniójuk is konvex, de mint kiderült, nem zárt. C_q lezártját jelöljük C_{qa} -val. C_{qs} lezártjáról kiderült, hogy az is C_{qa} -val egyenlő [18]. De ezzel a kvantumkorrelációs halmazok még nem fogytak el. Triviálisan adódnak az alábbi tartalmazások:

$$C_c \subseteq C_q \subseteq C_{qs} \subseteq C_{qa}. \quad (2.30)$$

A nevezetes Bell-tétel bizonyítja [19], hogy $C_c \subset C_q$. Itt C_c a lokális (vagy klasszikus, értsd: nem kvantum) korrelációk halmazát jelenti, vagyis a lokális determinisztikus csatornák szorzatainak konvex burkát.

Fontos kérdés, hogy hogyan lehet eldönteni egy pontról, hogy benne van-e valamelyik halmazban. A tartalmazás bizonyítására elegendő megadni egy, a mérési eredményekhez

tartozó operátorhalmazt és állapotot, ami a megadott valószínűségeket reprodukálja. Persze, mivel potenciálisan végtelen dimenziós vektorterekről és tetszőleges precízitású valószínűségekről van szó, a gyakorlatban ez sem egy triviális feladat. A nem tartalmazás bizonyítása már keményebb dió. Első eredmény a Tsirelson-határ [20] volt, amely a CHSH egyenlőtlenség maximális sérülését adja meg. Szemléletesen: megadja, hogy a CHSH klasszikus politóp CHSH egyenlőtlenség által meghatározott lapjától milyen messzire van a kvantum tartomány széle. Az eredmény néhány sorban is levezethető az „SOS” (sum-of-squares) módszer segítségével [21]. Ebben az esetben vegyük úgy, hogy Alíz és Bob mérései az 1 és -1 értéket vehetik fel. A mérésekhez tartozó hermitikus operátorok (melyek spektrális projektorai a mérést leíró operátorok) legyenek A_0, A_1, B_0, B_1 . Ekkor $A_x^2 = B_x^2 = 1$ és $[A_x, B_x] = 0$. A CHSH egyenlőtlenség bal oldalát ekkor a következő mérhető mennyiség várható értéke adja:

$$A_0B_0 + A_0B_1 + A_1B_0 - A_1B_1. \quad (2.31)$$

Ez klasszikusan nem lehet nagyobb, mint kettő. A (2.31) egyenlet ravaszul ilyen alakba írható:

$$\begin{aligned} & \frac{\sqrt{2}}{2} \left(B_0^2 + B_1^2 + A_0^2 + A_1^2 - \left(\frac{B_0 - 0 + B_1}{\sqrt{2}} - A_0 \right) - \left(\frac{B_0 - 0 - B_1}{\sqrt{2}} - A_1 \right) \right) = \\ & = \frac{\sqrt{2}}{2} (4 - X^2 - Y^2), \end{aligned} \quad (2.32)$$

ahol X és Y hermitikus operátorok, vagyis a kifejezés várható értéke semmiképp sem lehet nagyobb, mint $2\sqrt{2}$. A korlát éles, hiszen egy szinglett qbitpárral és a Bell által meghatározott méréssel is⁷ el lehet érni.

A jelenleg legjobb szisztematikus eljárást Navascués, Pironio és Acín [12, 23] találták meg. Módszerük lényege a következő. Ha egy korrelációt elő tudunk állítani kvantummérésekkel, akkor a (2.27) egyenlet kielégítéséhez létezik egy $\rho = |\psi\rangle\langle\psi|$ tiszta állapot és $M_a^x = E_a^x$, $M_b^y = E_b^y$ projektorok. Ezután vegyük a projektorok tetszőleges szorzataiból képzett szabad félcsoporthoz (egységelem az egységoperátor). Ezen félcsoporthoz tetszőleges véges

⁷A kvantuminformáció-elmélet bonyolultságát mutatja, hogy itt még az *is* szócskával is vigyázni kell. Vannak ugyanis úgynevezett öntesztelő korrelációk, amiket lényegében csak egyetlenegy közös állapottal és mérésekkel lehet létrehozni. A CHSH egyenlőtlenség maximális sértése is ilyen [22].

részhalmazával mint index halmazzal vehetjük az alábbi mátrixot:

$$\Gamma_{TS} = \langle \psi | T^\dagger \cdot S | \psi \rangle, \quad (2.33)$$

ahol T és S a részhalmaz elemei. (A hermitikus konjugálás itt annyit jelent, hogy fordított sorrendbe kell írni az operátorokat.) Egyrészt Γ pozitív definit, mert tetszőleges v_T komplex vektorra

$$v^\dagger \Gamma v = \sum_{TS} v_T^\dagger \langle \psi | T^\dagger \cdot S | \psi \rangle v_S = \langle \psi | V^\dagger \cdot V | \psi \rangle \geq 0, \quad (2.34)$$

ahol $V = \sum_S v_S S = \sum_T v_T T$.

Másfelől a Γ mátrix elemeinek különböző egyenlőségeknek kell megfelelniük. Egyrészt $\langle \psi | T^\dagger \cdot S | \psi \rangle = \langle \psi | T'^\dagger \cdot S' | \psi \rangle$, ha $T^\dagger \cdot S$ $T'^\dagger \cdot S'$ ekvivalensek egymással, másrészt a $\Gamma_{E_a^x E_b^y}$ mátrixelemeknek vissza kell adniuk a $p(ab|xy)$ valószínűségeket, a $\Gamma_{E_a^x \perp}$ és $\Gamma_{E_b^y \perp}$ elemeknek pedig a marginálisokat. Két operátorfüzér akkor ekvivalens, ha a kommutációs szabályokkal (Alíz és Bob operátorai és az egy mérésen belüli projektorok kommitálnak) vagy a projektor definíciója miatt (mindegyik projektor négyzete önmaga) egymásba átvihetők. Például, ha A_1, A_2, B_1, B_2 Alíz illetve Bob különböző méréseihez tartozó két-két projektora, akkor

$$B_2 A_1 A_2 B_1 \cdot B_1 B_2 A_1 A_2 A_1 \cong A_1 \cdot A_2 B_2 B_1 B_2 A_1 A_2 A_1. \quad (2.35)$$

A korreláció nem kvantumosságát tehát úgy lehet bizonyítani, hogy keresünk egy részhalmazt, amire nem létezik a fenti megszorításokat teljesítő pozitív szemidefinit mátrix. Ezt egy szemidefinit programmal lehet bizonyítani.

Navascuésék azt is bebizonyították, hogy ha minden véges részhalmaz esetén található egy megfelelő pozitív szemidefinit mátrix, akkor létezik egy Hilbert tér, azon egy tiszta állapot és lineáris operátorok, amik a fenti egyenleteket teljesítik. Fontos azonban megjegyezni, hogy a tétel csak olyan operátorok létezését bizonyítja, amikre Alíz és Bob operátorai kommutálnak egymással *ugyanazon* a Hilbert téren, nem pedig azt, hogy Alíz és Bob operátorai két Hilbert téren vannak értelmezve, az állapot pedig a két tér tenzorszorzatán, amint a nemrelativisztikus kvantummechanika előírná.

Tsirelson egy cikkében [11] bizonyítás nélkül kijelentette, hogy a két feltétel ekvivalens, de kiderült, hogy ezt csak véges dimenziós Hilbert terekre könnyű belátni⁸, majd Junge és

⁸Einstein után szabadon talán ezt nevezhetjük Tsirelson legnagyobb tévedésének [24].

munkatársai [25] a végtelen dimenziós esetet összefüggésbe hozták az operátoralgebrák egyik legjelentősebb nyitott problémájával, Connes beágyazási problémájával [26]. Vagyis lehetséges, hogy létezik a korrelációknak még egy osztálya (C_{co}), a kommutáló operátorokkal megvalósíthatóké. A tartalmazási láncunk ekkor így fest:

$$C_c \subseteq C_q \subseteq C_{qs} \subseteq C_{qa} \subseteq C_{co} \quad (2.36)$$

Olyan módszert, amivel azt lehetne bizonyítani, hogy egy korreláció nem eleme C_{qa} -nak anélkül, hogy azonnal C_{co} -ból is kizárnánk, még nem sikerült találni.

2020 januárjában Ji, Natarajan, Vidick, Wright és Yuen közöltek egy 169 oldalas preprintet [27] (amely a második verzióban 206 oldalra nőtt). Ebben bebizonyítják, hogy a két halamaz valóban különböző (és ezzel a Connes-problémát is negatívan válaszolják meg). E sorok írásáig a cikk még nem jelent meg referált folyóiratban.

2.3. Játékelméleti áttekintés

Időnként előfordul az emberrel, hogy döntéseinek következményei vannak. Gyakran több szereplő döntései is kihathatnak mindegyikőjükre. A játékelmélet ezeket a helyzeteket igyekszik modellezni, eléggé leegyszerűsítve ahhoz, hogy matematikailag kezelhetőek legyenek, de elég sok aspektusukat megtartva ahhoz, hogy az életre nézve valami hasznos tanulságot levonhassunk belőlük.

A játékelmélet egy egyszerűbb esetében két szereplőt vizsgálunk. (Ha csak egy szereplő van, azzal a döntéssel foglalkozik.) Mindkettőről feltesszük, hogy *racionális*. Ezen kívül egy igen fontos feltevés, hogy a szereplőket sújtó következményeket egy valós számmal jellemezhetjük⁹. Ez persze sok esetben nem életszerű. A játékelmélet használhatósága szoros összefüggésben van azzal, hogy egy területen mennyire számszerűsíthető a siker. Ez magyarázhatja a közgazdasági jelentőségét, ahol sok mindent pénzben mérünk, és azt, hogy

⁹Arról, hogy pontosan mit is jelent a racionális, önmagában is játékelméleti tankönyveket lehet megtölteni. Leegyszerűsítve: azt feltételezzük, hogy minden játékos kizárólag a saját célfüggvényének a maximalizálására törekszik és elég okos ahhoz hogy ténylegesen ki is tudja számolni, hogy ehhez a rendelkezésére álló információk alapján mit kell tennie. A következmények valós számmal való jellemzése mögött a Neumann-Morgenstein hasznossági tétel (utility theorem) áll [28], de ezek ismertetése meghaladja e dolgozat kereteit.

talán a legnagyobb sikereit az evolúciós biológiában aratta, ahol a siker egyetlen univerzális mértéke az utódok számának várható értéke.

Számos változata lehet annak, hogy a cselekedeteinktől hogyan jutunk el a következményekig. A legegyszerűbb modellben két játékos egymástól függetlenül dönthet arról, hogy mit csinál. A lehetőségeik egy véges halmazt alkotnak, ezeket nevezzük akcióknak. Adott még egy függvény, ami megadja, hogy az egyes választott akciópárokhoz milyen számszerűsíthető következmények tartoznak (játékosonként külön-külön), ezt nevezzük kifizetés-függvénynek.

A két játékosnak úgy kell eldöntenie, hogy melyik akciót választják, hogy közben nem tudják, a másik mit fog választani. Viszont teljes tudatában vannak annak, hogy az egyes lehetséges akciókhoz milyen kifizetések tartoznak. A racionális játékosoknak úgy kell megválasztaniuk az akciójukat, hogy a saját kifizetésüket maximalizálják, és egyáltalán ne törődjenek a másik kifizetésével.

Matematikailag egy kétszereplős (teljes információs) játék egy (A, B, u_A, u_B) négyes, ahol A és B az első, illetve a második játékos lehetséges akciói, és u_A és $u_B: A \times B \rightarrow \mathbb{R}$ függvények, rendre A és B játékos kifizetései.

Még egy további egyszerűsítési lehetőségünk van, ha feltesszük, hogy a játék során az egyik játékos pont annyit nyer, amennyit a másik veszít, vagyis $u_a = -u_b$. Ekkor a játékot zérus-összegűnek nevezzük.

A véges (véges akcióhalmazokkal rendelkező) kétszereplős játékokat bimátrix játékoknak hívjuk, és megadásukhoz elég egy párt, a két kifizetémátrixot megadni. Az akcióhalmazokat a mátrixok dimenziója kódolja. A zérus-összegű bimátrix játéknál elég az egyik mátrixot megadni. (Az ilyen játékot mátrixjátéknak hívjuk.) Zéró-összegű játéokra egy mindenki által ismert példa a Kő-papír-olló. Nem zéró-összegű játékra a példánk a „Nemek harca” játék. Itt Alíz és Bob számára az a legfontosabb, hogy együtt töltsék az estét, de Alíz ezt szívesebben tenné egy moziban, míg Bob egy meccsen. Erről reggel nem sikerült megállapodniuk, és napközben sajnos lemerült a telefonjuk, így mindkettejüknek magukban kell eldönteniük, hogy este a város egyik végén található mozi vagy a másik végén található sportcsarnok előtt váraкоzzanak abban reménykedve, hogy a másik is oda jön.

Kérdés, hogy mit tud tanácsolni a matematika annak, aki ilyen játékba keveredett. Aki-

$a \downarrow b \rightarrow$	kő	papír	olló
kő	(0, 0)	(-1, 1)	(1, -1)
papír	(1, -1)	(0, 0)	(-1, 1)
olló	(-1, 1)	(1, -1)	(0, 0)

$a \downarrow b \rightarrow$	mozi	meccs
mozi	(2, 1)	(0, 0)
meccs	(0, 0)	(1, 2)

2.3. táblázat. A „Kő-papír-olló” (balra) és a „Nemek harca” (jobbra) játék. A sorok és oszlopok a játékosok akcióinak felelnek meg, $a \in A$, $b \in B$, míg a táblázat számai a kifizetések $(u_{Alíz}(a, b), u_{Bob}(a, b))$ alakban.

nek van testvére, tudja, hogy nem mindig az történik, amit az ember akar (ha mégis, akkor kérdezze meg erről a testvérét), így a matematika sem tud az „optimális” megoldás megtalálásához segítséget nyújtani. Ehelyett egy másik fogalom bizonyult a probléma vizsgálatánál hasznosnak, ez a Nash-egyensúly.

Egy játék *tiszta* Nash-egyensúlya egy olyan akciópár, ahol egyik játékosnak sem éri meg egyoldalúan eltérni a saját egyensúlyi akciójától. Formálisan az (a, b) akciópár egy Nash-egyensúly, ha

$$\begin{aligned} (\forall a' \in A) \quad u_A(a', b) &\leq u_A(a, b), \\ (\forall b' \in B) \quad u_B(a, b') &\leq u_B(a, b). \end{aligned} \tag{2.37}$$

A Nemek harca játékban két ilyen egyensúly is van, az egyik a (mozi,mozi), a másik a (meccs,meccs). Ha csak az egyikük változtat, akkor nem találkoznak, és mindketten rosszabbul járnak, mint az egyensúlyban. Természetesen Alíz jobban örülne az első, míg Bob a második egyensúly megvalósulásának, ebből is látszik, hogy nehezen lehetne ezeket optimumnak nevezni.

Könnyen látható, hogy a Kő-papír-olló játék esetén tiszta Nash-egyensúly nem létezik a körbeverés miatt.

A játékosok nem csak determinisztikusan választhatnak akciót, hanem egy valószínűségi eloszlás szerint is. Ha $p_A(a)$ és $p_B(b)$ Alíz és Bob egymástól független eloszlásai, akkor kiszámolhatjuk a kifizetések várható értékét, a *várható kifizetést* a két eloszlás szorzat eloszlásából. A valószínűségeloszlásokat *kevert stratégiáknak* nevezzük a determinisz-

tikus „tisza” stratégiával ellentétben.¹⁰ Ekkor egy kevert Nash-egyesúly a játékosok olyan kevert-stratégia párja, amitől egyik játékosnak sem érdemes egyoldalúan eltérni. A Nash-tétel [29, 30] szerint minden véges játéknak létezik kevert Nash-egyesúlya. A Nemek harca játékban a két tiszta Nash-egyesúly mellett a $(p_A = (2/3, 1/3), p_B = (1/3, 2/3))$ kevert-stratégia pár a játék kevert egyensúlya. A Kő-papír-olló játékban az egyetlen kevert egyensúly a $(p_A = (1/3, 1/3, 1/3), p_B = (1/3, 1/3, 1/3))$ kevert-stratégia pár. Egy kevert egyensúlyban a saját stratégiától való eltérés nem növeli a várható kifizetést, de az eloszlás tartóján belül a valószínűségeket átcsoportosítva nem is csökkenti. (Addig, amíg a másik fél tényleg marad az egyensúlyi eloszlásánál.)

A kevert Nash-egyesúly egy általánosítása a korrelált egyensúly [31, 32]. Ebben az esetben a játékosok egy közös, nem feltétlenül szorzat alakú együttes eloszlás szerint választanak stratégiát. Úgy képzelhetjük, mintha egy megbízható harmadik fél egy ismert eloszlás szerint adna tanácsot a játékosoknak. (A tanácsot a játékosoknak külön-külön adja, azt egyiküknek sem árulja el, hogy a másiknak mit tanácsolt.) Például a Nemek harca játékban egy pénzt feldob, és ha fej, mindkettőjüknek mozi, ha írás, mindkettőjüknek meccset javasol. (Ebben az esetben az eloszlás speciális alakja miatt fölösleges a titkolózás, de általános esetben nagyon is fontos ahhoz, hogy a stratégia tényleg egyensúly legyen.)

A matematikai definíció:

$$\begin{aligned} (\forall a, a') \sum_b (u_A(a, b) - u_A(a', b))p(a, b) &\geq 0, \\ (\forall b, b') \sum_a (u_B(a, b) - u_B(a, b'))p(a, b) &\geq 0. \end{aligned} \tag{2.38}$$

A Nemek harca példánkban a fent említett korrelált egyensúly a következő: $p(\text{meccs, meccs}) = p(\text{mozi, mozi}) = 1/2$.

A fenti egyensúlyfogalmak közül talán ez a matematikailag legkönnyebben kezelhető, mert az egyensúlyi stratégiák egy konvex politópot alkotnak a valószínűségeloszlások terében. A nemek harca játékban a harmadik fél nem csak pénzfeldobással döntheti el, hogy mit tanácsoljon, hanem mondhat például állandóan meccset is.

Ennek az egyensúlynak is az az intuitív jelentése, hogy nem érdemes egyoldalúan eltérni a stratégiától. De míg a tartón belül a kevert Nash-egyesúlytól való eltérés az adott játékosnak nem oszt nem szoroz, addig korrelált egyensúly esetén ha valaki nem hallgat a

¹⁰Egészen pontosan a tiszta stratégiák halmaza a kevert stratégiák egy valódi részhalmaza.

harmadik fél tanácsára, akkor csökkenhet a várható kifizetése.

2.3.1. Bayes-i játékok és egyensúlyaik

Eddig teljes információs játékokról volt szó, vagyis mindkét játékos teljes mértékben tisztában volt a játszott játékkal. Ekkor az egyetlen bizonytalanság a másik játékos szabad döntése. Ilyenek például a fent vizsgált bimátrix játékok.

Gyakran azonban nem ez a helyzet. A legtöbb kártyajátékban rendkívül fontos jellemző, hogy a játékosok ismerik saját lapjaikat, de nem ismerik az ellenfelét.

Matematikailag ezt úgy modellezhetjük, hogy a játékosoknak típusaik vannak, minden játékos ismeri a saját típusát (privát információ), és a kifizetések nem csak az akcióktól, de a típusoktól is függenek. A játékosok nem befolyásolhatják, hogy mi legyen a típusuk, ha megtehetnék akkor az már a stratégia része lenne, nem a típusé. Legtöbbször feltesszük, hogy a lehetséges típusoknak van egy mindenki által ismert együttes valószínűségeloszlása. Ezt az együttes valószínűségeloszlást közös priornak nevezzük.

Mielőtt rátérnénk a pontos definícióra, vegyünk a módosított Nemek harca játékot mint példát[33]. Alíznek és Bobnak két típusa van: szerelmesek a másikba, vagy utálják. Aki szerelmes a másikba, az szeretne vele találkozni, aki utálja, az igyekszik elkerülni. Ekkor a kifizetések a 2.4. táblázatban láthatóak.

$x \downarrow y \rightarrow$		sz		u	
		mozi	meccs	mozi	meccs
sz	mozi	(2, 1)	(0, 0)	(2, 0)	(0, 1)
	meccs	(0, 0)	(1, 2)	(0, 2)	(1, 0)
u	mozi	(0, 1)	(2, 0)	(0, 0)	(2, 2)
	meccs	(1, 0)	(0, 2)	(1, 1)	(0, 0)

2.4. táblázat. A módosított nemek harca kifizetései. A táblázat Alíz és Bob típusai szerint blokkokba van rendezve.

Legyen mondjuk az ismert közös prior valószínűség: $p(sz, sz) = p(sz, u) = 2/6, p(u, sz) =$

$p(u, u) = 1/6$. Ekkor a $((\text{mozi}, \text{mozi}), (\text{mozi}, \text{meccs}))$ stratégia – vagyis, hogy Alíz mindig moziba megy, Bob pedig moziba, ha szerelmes Alízba és meccsre, ha nem – egy olyan egyensúly, amitől egyik félnek sem érdemes egyoldalúan eltérnie. Az könnyen látható, hogy Bobnak így kell tennie, ha Alíz mindenképp moziba megy. Hogy Alíznek sem érdemes eltérnie ettől, az a következőképpen látható be. Mivel Alíz ismeri a saját típusát, ezért számára Bob $1/2$ - $1/2$ valószínűséggel szerelmes vagy nem. (Ezt a prior feltételes valószínűségeiből számolta ki.) Ha Alíz szerelmes, akkor a moziban és a meccsen a várható kifizetése:

$$u_A(\text{mozi} | (\text{mozi}, \text{meccs})) = 1/2 \cdot 2 + 1/2 \cdot 0 = 1, \quad (2.39)$$

$$u_A(\text{meccs} | (\text{mozi}, \text{meccs})) = 1/2 \cdot 0 + 1/2 \cdot 1 = 1/2. \quad (2.40)$$

Ha nem szerelmes:

$$u_A(\text{mozi} | (\text{mozi}, \text{meccs})) = 1/2 \cdot 0 + 1/2 \cdot 2 = 1, \quad (2.41)$$

$$u_A(\text{meccs} | (\text{mozi}, \text{meccs})) = 1/2 \cdot 1 + 1/2 \cdot 0 = 1/2. \quad (2.42)$$

Tehát mindenképp a mozival jár jobban. Később kiszámoljuk, hogy mi a helyzet, ha Bob önzőzik, vagyis $((\text{meccs}, \text{mozi}), (\text{meccs}, \text{meccs}))$.

Most térjünk rá a pontos definíciókra. Ha A egy szigma algebrával ellátott halmaz, akkor $\Delta(A)$ jelölje az A fölötti valószínűségeloszlások halmazát. A szigma algebrát külön nem jelöljük, mert a dolgozatban az mindig a szokásos lesz. Ha $\{T_i\}_{i \in I}$ I szerint indexelt halmazcsalád, akkor T_{-i} jelölje a halmazok Descartes-szorzatát, amiből az i indexű elemet kihagytuk, vagyis $\prod_{j \in I, j \neq i} T_j$.

A Bayes-i játékok definíciójához szükség van a típustér fogalmára. Egy típustér alatt egy $(N, P, \{T_i\}_{i \in N}, \{\tau_i\}_{i \in N})$ négyest értünk, ahol

1. N a játékosok halmaza, véges, ezért általában $\{1, 2, \dots, n\}$ -nek vesszük,
2. P egy nemüres véges halmaz, a természet lehetséges állapotai,
3. T_i egy nemüres véges halmaz, az i játékos típusa halmaza,
4. $\tau_i : T_i \rightarrow \Delta(P \times T_{-i})$ az i játékos típusfüggvénye. Például $\tau_i(t)$ azt írja le, hogy az i játékos – amennyiben a típusa t – akkor mit gondol a többi játékos és a természet típusairól.

Az egyes játékosok típusfüggvényeinek nem kell egymással koherensnek lenni. Ha például $P = \{„A Föld lapos”, „A Föld kocka alakú”\}$, akkor megengedett, hogy az egyik játékos a Földet laposnak, a másik kocka alakúnak képzelje.

A típusfüggvényeket „kiegészíthetjük” egy-egy olyan valószínűségeloszlással, ami az összes játékos típusain van értelmezve. Ekkor azt követeljük meg a „kiegészített” eloszlástól, hogy a i játékos típusfüggvénye annak feltételes eloszlása legyen. Egy ilyen „kiegészítést” az i játékos *priorjának* nevezünk. A prior nem egyértelmű. Ha létezik olyan valószínűségeloszlás, ami az összes játékosnak priorja, ezt *közös priornak* nevezzük. Közös prior nem biztos, hogy létezik.

A fenti példánkban például feltehetjük hogy a temperamentumos Alíz szerint érzelmei mindig viszonzásra találnak, vagyis a típusfüggvénye

$$\begin{aligned} & (p(\text{sz}), p(\text{u})) \\ \text{sz} & \mapsto (1, 0) \\ \text{u} & \mapsto (0, 1) \end{aligned} \tag{2.43}$$

míg a szkeptikus Bob úgy gondolja, Alíz típusai a sajátjától függetlenül egyenlő valószínűségűek:

$$\begin{aligned} & (p(\text{sz}), p(\text{u})) \\ \text{sz} & \mapsto (1/2, 1/2) \\ \text{u} & \mapsto (1/2, 1/2). \end{aligned} \tag{2.44}$$

Könnyen látható, hogy ekkor közös prior nem létezik.

Egy Bayes-i játék alatt egy $(N, P, \{T_i\}_{i \in N}, \{\tau_i\}_{i \in N}, \{A_i(t)\}_{i \in N, t \in T_i}, \{u_i\}_{i \in N})$ hatost értünk, ahol

1. $(N, P, \{T_i\}_{i \in N}, \{\tau_i\}_{i \in N})$ egy típustér,
2. $A_i(t_i)$ egy nemüres véges halmaz, az i játékos akciói, ha a típusa t_i ,
3. $u_i : P \times \prod_{j \in N} \left(\sum_{t_j \in T_j} A_j(t_j) \right) \rightarrow \mathbb{R}$ az i játékos kifizetésfüggvénye, ami függ az összes játékos típusától és akciójától. Mivel egy játékos akcióhalmaza függhet a típusától, a kifizetésfüggvény értelmezési tartománya egy függő összeg¹¹.

¹¹A függő összeg a Descartes-szorzat általánosítása, elemei olyan rendezett párok, ahol az első elemtől függ, hogy a második elem milyen halmazból kerül ki. A függő függvény a függvény általánosítása, ahol nem csak

Itt jegyezzük meg, hogy szoros kapcsolat van a Bell-egyenlőtlenségek és a Bayes-i játékok között (lásd Brunner és Linden [36]).

A Bayes-i játék egyensúly fogalmának definiálásához a játékot át kell alakítanunk normál alakra. Az ex-ante normál alakban minden játékos számára kijelölünk egy priort, majd a játékos egy stratégiája egy olyan függvény, ami minden lehetséges típusához megad egy akciót; végül a kifizetését az eredeti játék kifizetéséből a megadott priorral számolt várható értéknek vesszük.

Vagyis egy $(N, \{S_i\}_{i \in N}, \{\bar{u}_i\}_{i \in N})$ normál formában felírt játék a $(N, P, \{T_i\}_{i \in N}, \{\tau_i\}_{i \in N}, \{A_i(t)\}_{i \in N, t \in T_i}, \{u_i\}_{i \in N})$ Bayes-i játék $\{\Pi_i\}_{i \in N}$ priorokkal vett ex-ante normál alakja, ha

1. $S_i = (\Pi_{t \in T_i} A_i(t))$, vagyis az i játékos stratégiái azok a függő függvények, amelyek T_i minden eleméhez a hozzá tartozó $A_i(t)$ egy elemét rendelik,
2. $\bar{u}_i : \prod_{i \in N} S_i \rightarrow \mathbb{R}$, $\bar{u}_i(\{s_j\}_{j \in N}) = \int_{P \times \prod_{j \in N} T_j} u_i(t_0, s_1(t_1), \dots, s_n(t_n)) d\Pi_i(t_0, t_1, \dots, t_n)$, vagyis a kifizetés az összes lehetséges típusra a priorjával számolt várható érték (hiszen esetünkben a normál alakban a játékosok stratégiái függvények, amik minden típusra megmondják, hogy milyen akciót választott volna az eredeti játékban).

Egy Bayes-i játék ex-ante Nash-egyensúlyának a játék ex-ante normál alakja Nash-egyensúlyát nevezzük. Az ex-ante normál alak függ a választott prioroktól.

A példajátékunk ex-ante normál alakjában mindkét játékosnak négy akciója van (hiszen négy különböző függvény létezik két kételemű halmaz között), és ha a példabeli közös priort vesszük mindkét játékosnak, akkor a kifizetések a 2.5. táblázatban láthatóak.

Látható, hogy a normál alakú játéknak a ((mozi,mozi),(mozi,meccs)) tiszta Nash-egyensúlya, hiszen a táblázat második oszlopában Alíznek az első sorban van a legnagyobb kifizetése, az első sorban pedig Bobnak a második oszlopban. Viszont a ((meccs,mozi),(meccs,meccs)) nem Nash-egyensúly, mert ebben az esetben Bobnak érdemes eltérni a (meccs,meccs) stratégiától.

A Bayes-i játékok ezen nagyon általános formája lehetőséget ad az olyan „Ki mit tud?” jellegű episztemiológia problémák vizsgálatára, mint például „Alíz tudja, hogy Bob tudja, a függvény értéke, de érkezési halmaza is függhet a bemenettől, például a benemet egy természetes szám, n , a kimenet pedig \mathbb{R}^n egy eleme. Bővebben lásd [34, 35]

Alíz ↓ Bob →	(mozi, mozi)	(mozi, meccs)	(meccs, mozi)	(meccs, meccs)
(mozi, mozi)	(4/3, 1/2)	(1, 7/6)	(1, 0)	(2/3, 2/3)
(mozi, meccs)	(5/3, 1/2)	(5/6, 2/3)	(5/6, 1/2)	(2/3, 2/3)
(meccs, mozi)	(0, 5/6)	(2/3, 1/2)	(2/3, 4/3)	(4/3, 1)
(meccs, meccs)	(1/3, 5/6)	(1/2, 0)	(1/2, 11/6)	(2/3, 1)

2.5. táblázat. A módosított Nemek harca kifizetései *ex-ante* normál alakban.

hogyc Cecil mit tud” [37, 38, 39], de ebben a dolgozatban csak olyan játékokat vizsgálunk, ahol létezik közös prior.

Az játékelméleti irodalomban három helyzetet különböztetünk meg az egyensúlyok tanulmányozása szempontjából. Az *ex-ante* helyzetben senki sem ismeri még saját típusát sem. Az *interim* helyzetben a játékosok ismerik saját típusukat, de a többiekére csak a priorjukból vett feltételes valószínűségekből következtethetnek. (Ez az a helyzet, amit magunk elé képzelünk, amikor Bayes-i játékokról gondolkozunk.) Az *ex-post* helyzetben a játékosok ismerik a többiek típusát is, vagyis olyan, mintha nyílt kártyákkal játszanának. Ismert, hogy az általunk tanulmányozott esetekben az *ex-ante* és az *interim* normál formákból kapott egyensúlyok egybeesnek, ezért külön az *interim* normál formával nem foglalkozunk. Az *ex-post* helyzetben a játékok szétesnek típusonként külön-külön teljes információs játékokra, amiknek egyenként meg lehet találni a (nem Bayes-i) egyensúlyait az $u_A(a, b, x, y)$, $u_B(a, b, x, y)$ kifizetések alapján, ahol x és y rögzítettek.

3. fejezet

Eredmények

3.1. Kvantumállapotok megkülönböztetése

A következőkben a kvantumállapotok megkülönböztetésének ROC térbeli leírásával kapcsolatos eredményeinket ismertetjük. A nem egyértelmű kvantumállapot megkülönböztetés ROC térbeli tárgyalása új intuitív képet szolgáltat a problémáról amely számos korábbi eredményt egységes szemléletbe helyez. Emellett módot ad kvantumállapotok egy új hasonlósági mérőszámának bevezetéséhez, amely műveleti jelentéssel is bír.

3.1.1. Bhattacharyya-együttható a ROC görbéből

Először térjünk vissza a klasszikus bináris klasszifikáció 2.1.2 fejezetben ismertetett ROC térbeli leírásához. Tehetünk egy olyan megfigyelést, amely a klasszikus ROC görbék irodalmában sem közismert eredményre vezet. Vegyük észre, hogy az (optimális) ROC görbe majdnem jellemzi a két eloszlást. Ha nincsenek pontok, amik azonos p_i/q_i arányhoz tartoznak, akkor a görbéből egyértelműen megkapható mindkét eloszlás. Csak az azonos p_i/q_i arányú pontok jelentenek kétértelműséget. Ezeket az egyik eloszlásban fel lehet cserélni, vagy össze lehet olvasztani egyetlen értéké. Ezen kívül bármelyik érték szétosztható több azonos p_i/q_i arányú pontra.

Az egyik széles körben használt eloszlás-hasonlósági mérték geometriailag megkapható

a ROC görbéből. Vegyük az alábbi koordináta transzformációt:

$$\begin{pmatrix} q \\ p \end{pmatrix} \rightarrow \begin{pmatrix} t \\ s \end{pmatrix} = \begin{pmatrix} \frac{p-q}{2} \\ \frac{p+q}{2} \end{pmatrix}, \quad (3.1)$$

vagyis $\pi/4$ -gyel elforgatjuk a koordinátarendszert, és összezsugorítjuk gyök kettédere. Ezután vegyük a következő Minkowski-metrikát az új koordinátarendszerben:

$$dl^2 = ds^2 - dt^2. \quad (3.2)$$

A speciális relativitáselmélet szóhasználatával az időtengely a ROC tér eredeti $(0, 0) \rightarrow (1, 1)$ átlója lesz, a tértengely pedig erre (Euklidészi-metrikában) merőleges. A teljes ROC tér ekkor a $(0, 0)$ pont jövőbeli és a $(1, 1)$ pont múltbeli fénykúpjában helyezkedik el.

Vegyük a következő kumulatív eloszlásokat:

$$P_k = \sum_{l=1}^k p_l \quad (3.3)$$

és

$$Q_k = \sum_{l=1}^k q_l \quad (3.4)$$

egymás függvényében felrajzolva, amivel az előző szakaszban leírt ROC görbét kapjuk. A töröttvonal k -dik szegmensének Minkowski-metrikában vett hosszánégyzete a (Q_k, P_k) és (Q_{k+1}, P_{k+1}) pontok között:

$$\ell_{k+1}^2 = -\left(\frac{P_{k+1} - Q_{k+1}}{2} - \frac{P_k - Q_k}{2}\right)^2 + \left(\frac{P_{k+1} + Q_{k+1}}{2} - \frac{P_k + Q_k}{2}\right)^2 \quad (3.5)$$

$$= -\left(\frac{p_{k+1} - q_{k+1}}{2}\right)^2 + \left(\frac{p_{k+1} + q_{k+1}}{2}\right)^2 = p_{k+1}q_{k+1}. \quad (3.6)$$

Vagyis a töröttvonal teljes hossza (sajátideje):

$$\ell = \sum_k \ell_k = \sum_k \sqrt{p_k q_k} = B(p, q), \quad (3.7)$$

ami éppen a statisztikai irodalomban széleskörben használt Bhattacharyya-együttható [40]. Ez két valószínűségeloszlás közötti hasonlóság egyik lehetséges mértéke.

3.1.2. A kvantumállapotok ROC görbéje

A nemegyértelmű kvantumállapot megkülönböztetés problémájában adott egy ismeretlen kvantumállapot, aminek λ valószínűséggel ρ_p a sűrűségmátrixa, $1 - \lambda$ valószínűséggel ρ_n (λ , ρ_p és ρ_n előre ismertek).

Az ismeretlen állapot egy példánya áll rendelkezésünkre, ezen egy tetszőleges POVM mérést hajthaunk végre, és a lehető legkisebb hibázási valószínűséggel meg kell állapítanunk, a két lehetséges állapot közül melyik volt a mintánk. A minimális hibavalószínűséget a jól ismert Helstrom-formula adja [7]:

$$P_{E, \min} = \frac{1}{2} (1 - \|\lambda \rho_p - (1 - \lambda) \rho_n\|_1). \quad (3.8)$$

A ROC vizsgálat során érdemes a mérést és az utána következő döntési algoritmust egye-
síteni a mérési operátorban, aminek így csak két lehetséges kimenete lesz, p (az állapot sze-
rintünk ρ_p volt) és n (az állapot szerintünk ρ_n volt). Mint a Helstrom-formulából kiderül,
az optimális mérés végül projektív lesz, a két altér az alábbi hermitikus operátor pozitív
illetve negatív sajátértékeihez tartozó altérek

$$\Lambda = \lambda \rho_p - (1 - \lambda) \rho_n. \quad (3.9)$$

Két tiszta állapot. Ebben a részben két tiszta állapot megkülönböztetését vizsgáljuk A
probléma eredendően kétdimenziós, mert elegendő a két állapot által kifeszített altérre
szorítkozni. Vagyis amíg nincsenek kevert állapotok, két qbit megkülönböztetése a legál-
talánosabb eset.

Vagyis van egy qbitünk az alábbi állapotok egyikében

$$|\Psi_p\rangle = \begin{pmatrix} \cos \frac{\theta_p}{2} \\ \sin \frac{\theta_p}{2} \end{pmatrix} \quad \text{vagy} \quad |\Psi_n\rangle = \begin{pmatrix} \cos \frac{\theta_q}{2} \\ \sin \frac{\theta_q}{2} \end{pmatrix} \quad (3.10)$$

mint „pozitív” és „negatív” eset. (A klasszikus esetet úgy kaphatjuk vissza, ha $p = \cos^2(\theta_p/2)$
és $q = \cos^2(\theta_q/2)$ a (2.1) egyenletben, és csak a z tengely menti mérést engedünk.) Szim-
metria okokból elég, ha valós vektorokat veszünk, de a θ_p és θ_q azimutiszögek a $[0, 2\pi[$ in-
tervallumban vehetnek fel értéket, így két tetszőleges állapotot kapunk a Bloch-gömb $x - z$
síkjában.

Válasszunk projektív mérést az alábbi (α -tól függő) bázisban

$$|\Phi_p\rangle = \begin{pmatrix} \cos \frac{\alpha}{2} \\ \sin \frac{\alpha}{2} \end{pmatrix}, \quad |\Phi_n\rangle = \begin{pmatrix} -\sin \frac{\alpha}{2} \\ \cos \frac{\alpha}{2} \end{pmatrix}, \quad \alpha \in [0, 2\pi[. \quad (3.11)$$

Továbbra is feltételezzük, hogy az esetleges klasszikus utófeldolgozás be van építve a kvantummérésbe, vagyis $|\Phi_p\rangle$ esetén úgy döntünk, $|\Psi_q\rangle$ volt az állapot, $|\Phi_n\rangle$ esetén pedig $|\Psi_n\rangle$: a mérést nem követi további utófeldolgozás.

A ROC görbe kiszámításához szükségünk van a valódi pozitív és hamis pozitív valószínűségekre, amit könnyen megkaphatunk néhány skalárszorzás elvégzésével

$$\begin{aligned} \Pr(VP) &= |\langle \Phi_p | \Psi_q \rangle|^2 = \frac{1 + \cos(\alpha - \theta_p)}{2}, \\ \Pr(HP) &= |\langle \Phi_p | \Psi_n \rangle|^2 = \frac{1 + \cos(\alpha - \theta_q)}{2}. \end{aligned} \quad (3.12)$$

A klasszikus ROC görbéhez hasonlóan ez is független a priortól. Az eredmény egy ellipszis paraméteres egyenlete, amit a 3.1. ábrán ábrázoltunk. Az ellipszisünk nagytengelye a $(0, 0) \rightarrow (1, 1)$ diagonálison fekszik. A klasszikus ROC tartomány extrémális pontjai, (q, p) és $(1 - q, 1 - p)$ is rajta vannak az ellipszisen, ami azt jelenti, a

$$\begin{aligned} \cos\left(\frac{\theta_p}{2}\right)^2 &= \frac{1 + \cos(\alpha - \theta_p)}{2}, \\ \cos\left(\frac{\theta_q}{2}\right)^2 &= \frac{1 + \cos(\alpha - \theta_q)}{2} \end{aligned} \quad (3.13)$$

egyenleteknek valóban van megoldásuk α -ra.

Most vizsgáljuk azokat a pontokat, ahol az ellipszis érinti a ROC négyzet oldalait. A valódi pozitív ráta egy, ha $\alpha - \theta_p = 0$, vagyis ha $|\Phi_p\rangle = |\Psi_q\rangle$. A hamis pozitív ráta ekkor éppen a két megkülönböztetendő állapot egy ismert hasonlósági mértékével, a fidelity-vel egyezik meg [41]:

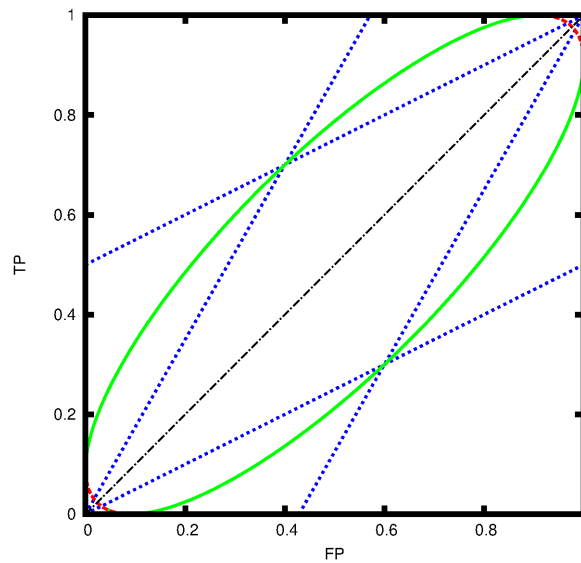
$$\mathcal{F}(\Psi_n, \Psi_q) = |\langle \Psi_q | \Psi_n \rangle|^2 = |\langle \Phi_p | \Psi_n \rangle|^2. \quad (3.14)$$

A hamis pozitív ráta értéke egy, ha $\alpha - \theta_q = 0$, ekkor $|\Phi_p\rangle = |\Psi_n\rangle$, és ismét a fidelity-t kapjuk:

$$\mathcal{F}(\Psi_n, \Psi_q) = |\langle \Psi_q | \Psi_n \rangle|^2 = |\langle \Psi_q | \Phi_p \rangle|^2. \quad (3.15)$$

A valódi pozitív ráta nulla, ha $\alpha - \theta_p = \pi$, vagyis $\alpha = \pi + \theta_p$. Ekkor $|\Phi_p\rangle = |\Psi_q^\perp\rangle$, ahol $|\Psi_q^\perp\rangle$ egy $|\Psi_q\rangle$ -re merőleges állapot a Hilbert-térben. A hamis pozitív rátára a következőt kapjuk:

$$|\langle \Phi_p | \Psi_n \rangle|^2 = |\langle \Psi_q^\perp | \Psi_n \rangle|^2 = 1 - \mathcal{F}(\Psi_n, \Psi_q). \quad (3.16)$$



3.1. ábra. Két tiszta állapot ROC görbéje. Az analóg klasszikus eset paraméterei $p = 0.7$, $q = 0.4$. A kvantum ROC görbe az ellipszis. Összehasonlításképp a klasszikus görbét is felrajzoltuk. A $(0, 0)$ ponttól a tengelyek és az ellipszis piros szaggatott vonallal jelzett szakasza által határolt terület, és az $(1, 1)$ pontnál lévő tükörképe nem érhető el a Helstrom-formulával megadott optimális állapotdiszkriminátorral.

A pont, ahol a hamis pozitív ráta nulla, $\alpha = \theta_n + \pi$ -nál van. A fentiekhez hasonlóan belátható, hogy itt a valódi pozitív ráta $1 - \mathcal{F}(\Psi_{\eta}, \Psi_{\eta})$. Vagyis két tiszta állapot esetén a fidelity a ROC görbéről azonnal leolvasható.

A klasszikus utófeldolgozás, amikor definiálunk elfogadási és elvetési valószínűségeket a kvantumérés eredményéhez, az ellipszisen belüli pontokat eredményez, így annak teljes területe elérhető valamilyen elrendezéssel. Ez annyiban nem egyértelmű, hogy különböző mérések és utófeldolgozások együttese ugyanazt a pontot is adhatja a ROC térben.

Egy másik megközelítést is alkalmazhatunk. A megkülönböztetendő állapotok és a prior valószínűség (λ) ismeretében meghatározhatjuk az ideális projektorokat és mérést a (3.9) egyenletből. Ebben az esetben a közvetlen α paraméter helyett λ -t használjuk. λ függvényében felrajzolva a pontokat a ROC síkon az ellipszis felső és alsó részét kapjuk, ahogy a 3.1. ábrán látható. A hiányzó darabok (az ábrán szaggatott piros vonal) az „átlagos” sűrűségmátrix spektrális projektoraival kaphatók meg. Az „átlagos” sűrűségmátrix:

$$\rho = \lambda \rho_{\eta} + (1 - \lambda) \rho_{\eta}. \quad (3.17)$$

Vagyis két lehetséges megközelítésünk van. Ha adott két állapot, vehetjük az α -val paraméterezett összes mérést, és megkapjuk az ellipszist, vagy vehetjük a prior (λ) által meghatározott optimális méréseket, amik az ellipszis felső és alsó részét adják.

Hogy meghatározzuk a prior λ valószínűséget, amihez az optimális ROC görbe egy pontja tartozik, vegyük észre, hogy a konstans hibavalószínűséghez tartozó pontok a (2.12) egyenlet által meghatározott egyenesek. Tegyük fel, hogy az ellipszis felső részén vagyunk. Egy pont akkor optimális, ha a lehető legközelebb van a $(0, 1)$ ponthoz. Ehhez az kell, hogy a rajta átmenő konstans hibavalószínűség egyenes másik oldalán ne legyen pont, vagyis az egyenes az ellipszis érintője kell legyen. Másfelől, az ellipszis érintője az adott pontban:

$$\frac{\lambda}{1 - \lambda} = \frac{d \Pr(VP)}{d\alpha} \left(\frac{d \Pr(HP)}{d\alpha} \right)^{-1} = \frac{\sin(\theta_p - \alpha)}{\sin(\theta_q - \alpha)}. \quad (3.18)$$

Ez az összefüggés összeköti a két megközelítésünkben szereplő α és λ paramétereket. Egyben egy műveleti jelentést is ad a ROC görbe érintőinek, ami valójában az optimális ROC görbe teljesen általános tulajdonsága: adott prior esetén így kaphatjuk meg az optimális diszkriminátorhoz tartozó rátákat.

Számoljuk ki a klasszikus Bhattacharyya-együtthatót a $\Pr(VP)$, $1 - \Pr(VP)$ és $\Pr(HP)$, $\Pr(1 - HP)$ eloszlásokra! Ezeket a valószínűségeket a (3.12) egyenletből a (3.7) egyenletbe kell

behelyettesíteni. Az ellipszis felső szakaszának pontjaira azt kapjuk, hogy a klasszikus Bhattacharyya-együttható állandó. Vagyis a két tiszta állapot optimális megkülönböztetését leíró ROC görbe egyben egy izo-Bhattacharyya-együttható vonal.

3.1.3. Egy kvantum Bhattacharyya-együttható

Most idézzük fel a 3.1.1 pontban kapott eredményünket, miszerint a Bhattacharyya-együttható megkapható mint az optimális ROC görbe Minkowski-metrika szerinti hossza. Joggal merülhet fel a kérdés, miszerint ez a görbe menti integrál milyen információt szolgáltat kvantumállapotok esetében. Elegendő azon pontok között integrálnunk, ahol a görbe a függőleges tengelyt és a $(0, 1) - (1, 1)$ egyenest érinti, hiszen a függőleges és vízszintes szakaszok Minkowski hossza nulla.

Ennek kiszámításához végrehajtjuk ugyanazt a koordinátatranszformációt, amit a (3.1) egyenletben.

$$\begin{pmatrix} \Pr(HP) \\ \Pr(VP) \end{pmatrix} \rightarrow \begin{pmatrix} t \\ s \end{pmatrix} = \begin{pmatrix} \frac{\Pr(VP) - \Pr(HP)}{2} \\ \frac{\Pr(VP) + \Pr(HP)}{2} \end{pmatrix}, \quad (3.19)$$

és behelyettesítjük a (3.12) egyenletek baloldalait. Az eredmény:

$$\begin{aligned} t &= \frac{1}{4} ((\cos(\theta_p) - \cos(\theta_q)) \cos(\alpha) + (\sin \theta_p) - \sin(\theta_q)) \sin(\alpha) \\ s &= \frac{1}{4} ((\cos(\theta_p) + \cos(\theta_q)) \cos(\alpha) + (\sin \theta_p) + \sin(\theta_q)) \sin(\alpha). \end{aligned} \quad (3.20)$$

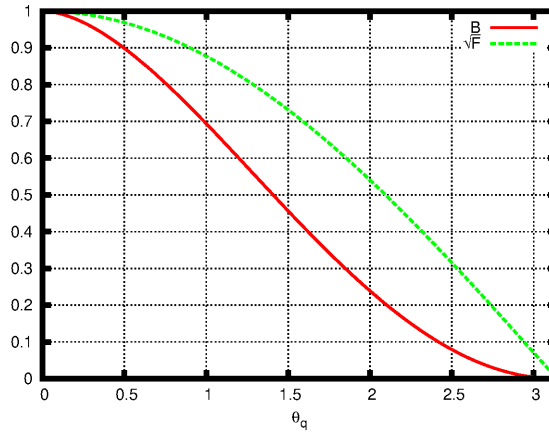
A görbe hossza Minkowski-metrikában így kapható:

$$B(|\Psi_{\eta}\rangle, |\Psi_{\eta}\rangle) = \int_{\text{felső görbe}} \sqrt{\left(\frac{ds}{d\alpha}\right)^2 - \left(\frac{dt}{d\alpha}\right)^2} d\alpha. \quad (3.21)$$

Az integrálás során az α értéke $\Pr(HP) = 0$ és $\Pr(VP) = 1$ között változik. A konkrét esetben az integrálási tartomány megválasztásánál ügyelni kell rá, hogy a felső görbén és a megfelelő irányban menjünk végig.

Némi számolás után azt kapjuk:

$$B(|\Psi_{\eta}\rangle, |\Psi_{\eta}\rangle) = \frac{\sqrt{2}}{4} \int_{\text{felső görbe}} \sqrt{\cos(\theta_q + \theta_p) - \cos(\theta_q + \theta_p - 2\alpha)} d\alpha. \quad (3.22)$$



3.2. ábra. A (3.21) egyenlet szerinti kvantum-Bhattacharyya-együttható és a fidelity négyzetgyöke $\theta_p = 0$ esetén θ_q függvényében.

Ez elliptikus integrálokra vezet, amiket általában csak numerikusan lehet kiszámítani. A mi esetünkben viszont, ha $\theta_p = 0$ és $\theta_q \in [0, \pi]$, vagyis a pozitív állapot felfelé áll, a negatív pedig tetszőleges irányban a Bloch-gömb $x - z$ síkjában, akkor lényegében az összes esetet lefedtük. Ebben az esetben a (3.22) integrálunk ilyen alakú:

$$B(|\Psi_{\mathfrak{F}}\rangle, |\Psi_{\mathfrak{T}}\rangle) = \frac{\sqrt{2}}{4} \int_{\theta_q + \pi}^{2\pi} \sqrt{\cos(\theta_q) - \cos(2\alpha - \theta_q)} d\alpha. \quad (3.23)$$

Amit zárt alakban ki lehet fejezni:

$$B(|\Psi_{\mathfrak{F}}\rangle, |\Psi_{\mathfrak{T}}\rangle) = \frac{1}{4} \left[\frac{2E(x|k) - (1 - \cos \theta)F(x|k)}{\sin\left(\frac{\theta}{2} - \alpha\right)} \right]_{\theta_q + \pi}^{2\pi}, \quad (3.24)$$

ahol

$$x = \cos\left(\frac{\theta}{2} - \alpha\right) \sqrt{1 + \cos \theta}, \quad (3.25)$$

és

$$k = \frac{\sqrt{2}}{2} \sqrt{1 + \cos \theta}, \quad (3.26)$$

és $F(x|k)$ és $E(x|k)$ rendre az első és másodfajú nem teljes elliptikus integrálok.

A B értékének θ_q függését a 3.2 ábrán rajzoltuk fel. A két állapot fidelity négyzetgyökét szintén kirajzoltuk. Látható, hogy a fidelity négyzetgyöke nagyobb vagy egyenlő, mint a kvantum-Bhattacharyya-együttható. A θ_q 0 és 1 értékeinél egyenlők. Mindkét függvény monoton csökkenő. Tehát – legalábbis tiszta állapotok esetén – a kapott B mennyiség valóban jellemzi a kvantumállapotok hasonlóságát.

3.1.4. Két qubit

Most kiterjesztjük a fogalmainkat a legáltalánosabb kétdimenziós esetre, amikor mindkét állapot egy-egy kevert qubit lehet, amiket a $\rho_{\mathfrak{P}}$ és $\rho_{\mathfrak{N}}$ kétdimenziós sűrűségmátrixok írják le. A Bloch-gömbön ezeket $\rho = 1/2(\hat{1} + \mathbf{r}\sigma)$ alakba írhatjuk, ahol \mathbf{r} egy valós háromdimenziós vektor, ami az állapotot jellemzi, míg σ a három Pauli-mátrixot tartalmazza. Tiszta állapotok esetén \mathbf{r} egy egységvektor, egyébként egynél rövidebb. A ROC görbe koordinátái:

$$\begin{aligned}\Pr(VP) &= \text{Tr}(M_p \rho_{\mathfrak{P}}), \\ \Pr(HP) &= \text{Tr}(M_p \rho_{\mathfrak{N}}),\end{aligned}\tag{3.27}$$

ahol M_p a pozitív döntéshez tartozó mérési operátor. Mivel a nyom lineáris, ezért ezek a kifejezések a Bloch-vektorok ($\mathbf{r}_{\mathfrak{P}}$ és $\mathbf{r}_{\mathfrak{N}}$) inhomogén lineáris függvényei. Vagyis a tiszta esetben kapott ellipszis csupán anizotróp módon összehúzódik a $(1/2, 1/2)$ pont felé. (Az összehúzódási arányokat a megfelelő Bloch-vektorok hossza adja.) Kevert állapotokra az ellipszis többé nem érinti a ROC tér szélét, de mivel a $(0, 0) \rightarrow (1, 1)$ egyenes szükségképpen az elérhető ROC tartomány része, ezért a ROC görbe felső része a (összehúzott) ellipszis és a $(0, 0)$ és $(1, 1)$ pontok konvex burkának felső szélé lesz.

Emlékezzünk rá, hogy a tiszta esetben (lásd a 3.1.2 pontban) az ellipszis egy izo-Bhattacharyya-vonal, és a koordinátatengelyekkel vett érintési pontja éppen a fidelity négyzetgyökét adja. Általános esetben a fidelity négyzetgyöke úgy is megkapható, hogy az összes lehetséges mérés Bhattacharyya-együtthatójának minimumát vesszük [41, 42]. Mivel tiszta állapotok esetén az ellipszis minden pontján azonos a Bhattacharyya-együttható értéke, és ez minimális, ezért az ellipszis nem csak izo-Bhattacharyya-vonal, hanem egyben izo-fidelity vonal is. A kevert esetben a ROC görbe már nem izo-Bhattacharyya-vonal, de megkereshetjük azt az izo-Bhattacharyya-ellipszist, ami ezt érinti, és az érintési pont megadja egyben a fidelity kiszámításához optimális mérést is. Sajnos a fenti gondolatmenet csak kétdimenziós esetben érvényes, mert magasabb (d) dimenzióban a fidelity kiszámításához szükséges optimális mérésnek d kimenete van, míg a ROC görbe pontjait adó méréseknek csak kettő, ezért nem feleltethetők meg egymásnak.

3.1.5. Két tetszőleges kvantumállapot

Most vegyük a legáltalánosabb esetet, és $\rho_{\mathfrak{p}}$ és $\rho_{\mathfrak{n}}$ legyenek tetszőleges kvantumállapotok a Hilbert-tér dimenziójának megszorítása nélkül. Ebben az esetben is végül egy konvex tartományt kapunk, aminek a felső széle az optimális diszkriminátorokhoz tartozik.

Ezt az optimális ROC görbét megkaphatjuk például úgy, hogy a különböző λ prior valószínűségekhez tartozó, Helstrom-formulából kapott optimális méréshez tartozó pontok konvex burkát vesszük. A mérés projektorai ($M_{\mathfrak{p}}, M_{\mathfrak{n}}$) a (3.9) egyenletben szereplő Λ mátrix pozitív és negatív sajátértékeihez tartozó alterekre vetítenek. Ezért a Helstrom-formulához tartozó pontok halmaza egy görbe, aminek általában szakadásai vannak ott, ahol $M_{\mathfrak{p}}$ rangja ugrik. (Ez akkor következik be, amikor λ növelésével Λ egyik sajátértéke előjelet vált.)

Egy másik lehetőség, hogy vesszük az összes ortogonális projektorpárhoz tartozó pontot a ROC térben. Ha a Hilbert-tér (vagy a két sűrűségmátrix közös tartójának) dimenziója d , akkor a projektorok rangja 0 és d változik. Mindegyik ranghoz egy a $(0, 0), (1, 1)$ vonalra szimmetrikus „pacát” kapunk a ROC síkon. (0 és d rang esetén rendre a $(0, 0)$ és $(1, 1)$ pontot kapjuk mint pacát.) A pacák konvex burka ismét az elérhető ROC tartományt adja, és ennek felső széle az optimális ROC görbét. Ezt a 3.3 ábrán ábrázoltuk.

A görbe érintőinek ugyanaz a műveleti jelentése, mint a korábbi fejezetben láttuk: az érintési pont adja az optimális mérést az érintő meredeksége által meghatározott priorhoz.

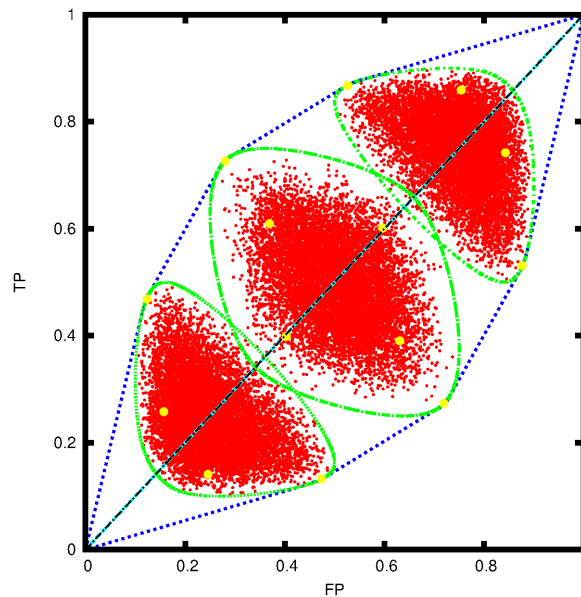
A trace distance

Kvantumállapotok különbözőségének egy másik ismert mértéke a *trace distance* [41]:

$$d_{\text{tr}}(\rho_{\mathfrak{p}}, \rho_{\mathfrak{n}}) = \frac{1}{2} \text{Tr} |\rho_{\mathfrak{p}} - \rho_{\mathfrak{n}}|. \quad (3.28)$$

(Azt a definíciót használjuk, amelyik tartalmaz egy $1/2$ faktort.) A ROC görbe a trace distance-nek is ad egy geometriai jelentést. Tegyük fel, hogy egyenlő prior valószínűségeink vannak, tehát $\lambda = 1/2$. A (3.18) egyenlet szerint az optimális diszkriminátorhoz tartozó pontnál a görbe érintője 45 fokos, vagyis a $(0, 0) - (1, 1)$ egyenessel párhuzamos. Másfelől a diszkriminátort a Helstrom-formulából is megkaphatjuk. Λ ebben az esetben éppen

$$\Lambda = \frac{1}{2} (\rho_{\mathfrak{p}} - \rho_{\mathfrak{n}}), \quad (3.29)$$



3.3. ábra. ROC tér két véletlenszerűen választott négydimenziós sűrűségmátrixhoz. A zárt zöld görbék az 1, 2 és 3 rangú projektorokkal elérhető tartományok. A kék görbe a tényleges optimális ROC görbe a Helstrom-formula alapján. A sok piros pont a Haar-mérték szerint választott véletlenszerű projektorokhoz tartozik. (Látható, hogy a pontok sűrűsége csökken a paca széléhez közeledve, ezért numerikusan nem így érdemes megkeresni a határait.) A nagyobb sárga pontok közül a ROC görbén fekvők a fidelity kiszámításához optimális mérés valószínűségeloszlásaihoz tartozó pontok (lásd a (3.33) egyenletet). A három sárga pont által alkotott töröttvonal viszont meghatároz két klasszikus valószínűségeloszlást, amikhez összesen 16 projektív diszkriminátort rendelhetünk, a 14 sárga pont és a két sarok ezeket a diszkriminátorokat jelöli. A ROC görbe belsejében levő 8 pont nem optimális diszkriminátorokat jelöl.

vagyis a két sűrűségmátrix különbségével arányos. A trace distance definíciója (3.28) alapján:

$$d_{\text{tr}}(\rho_{\mathfrak{P}}, \rho_{\mathfrak{N}}) = \text{Tr} |\Lambda|. \quad (3.30)$$

Ezt úgy is írhatjuk, mint

$$2d_{\text{tr}}(\rho_{\mathfrak{P}}, \rho_{\mathfrak{N}}) = \text{Tr}(M_{\text{p}}(\rho_{\mathfrak{P}} - \rho_{\mathfrak{N}})) - \text{Tr}(M_{\text{n}}(\rho_{\mathfrak{P}} - \rho_{\mathfrak{N}})). \quad (3.31)$$

Mivel Λ nyoma most nulla, a két tag abszolút értéke a jobb oldalon egyenlő, ezért

$$d_{\text{tr}}(\rho_{\mathfrak{P}}, \rho_{\mathfrak{N}}) = \text{Tr}(M_{\text{p}}(\rho_{\mathfrak{P}} - \rho_{\mathfrak{N}})) = \text{Pr}(TP) - \text{Pr}(FP). \quad (3.32)$$

Ez éppen a 45 fokos érintő metszéspontja a valódi pozitív tengellyel. Vagyis a trace distance is közvetlenül leolvasható a ROC diagramról.

3.1.6. A kvantum Bhattacharyya-együttható tulajdonságai

Az előző rész gondolatmenetét követve végül megvizsgáljuk a lehetőségét egy kvantum Bhattacharyya-együttható bevezetésének, ahogy azt tiszta állapotokra tettük (3.1.3). A ROC görbe konkrét alakján kívül semmit nem használtunk ki a kvantumállapotok tulajdonságaiból, így most is nevezhetjük a ROC görbe Minkowski-metrikában vett hosszát kvantum Bhattacharyya-együtthatónak. Ez egy új mennyiség, ami kvantumállapotok hasonlóságát méri. Konkrét esetekben leginkább numerikusan számítható ki egyszerű, de némileg számításigényes módon. Az alábbiakban az általános tulajdonságait vizsgáljuk.

1. Állítás. *A kvantum Bhattacharyya-együttható akkor és csak akkor nulla, ha a két állapot bizonyosan megkülönböztethető, vagyis a sűrűségmátrixok tartói diszjunktak; akkor és csak akkor egy, ha a két állapot megegyezik.*

Bizonyítás. Az első esetben a ROC görbe a $(0-0) \rightarrow (0,1) \rightarrow (1,1)$ töröttvonal, ami az egyetlen nulla hosszúságú görbe $(0-0)$ -tól $(1,1)$ -ig ebben a metrikában, míg a második esetben ez a $(0,0) \rightarrow (1,1)$ egyenes, ami a szigorúan leghosszabb (mert geodetikus) út a két pont között. \square

Szükségünk lesz az alábbi lemmára.

1. Lemma. *Ha adott két konvex görbe a ROC tér felső háromszögében, és az egyik a másik fölött halad, akkor a fölül haladó Minkowski hossza kisebb vagy egyenlő, mint az alul haladóé.*

Bizonyítás. Vegyünk egy olyan pontot az alsó görbén, ami nincs rajta a felsőn. Az e pontban vett érintő két ponton metszi a felsőt, hiszen az is konvex. A felső görbe két metszéspont közötti szakaszát helyettesítsük az érintő megfelelő szakaszával, így a felső görbe hosszát megnöveltük. Az alsó görbén elég sűrűn ilyen pontokat választva, és a felső görbét átszabva, így a felső görbe hosszának növelésével tetszőleges pontossággal megközelíthetjük az alsó görbét, így a közelítő görbe hosszának is az alsó görbe hosszához kell tartania. Egy monoton csökkenő sorozat első eleme feltétlenül nagyobb vagy egyenlő, mint a határérték. \square

2. Állítás. *A kvantum Bhattacharyya-együttható kisebb vagy egyenlő, mint a fidelity négyzetgyöke. A kettő egyenlő, ha a két sűrűségmátrix kommutál.*

Bizonyítás. Ismert, hogy létezik egy optimális projektív mérés aminek a valószínűségeloszlásaihoz tartozó Bhattacharyya-együttható éppen a fidelity négyzetgyökét adja. A mérőoperátor konkrétan meg is határozható:

$$M = \frac{1}{\sqrt{\rho_{\mathfrak{A}}}} \sqrt{\sqrt{\rho_{\mathfrak{A}}}\rho_{\mathfrak{B}}\sqrt{\rho_{\mathfrak{A}}}} \frac{1}{\sqrt{\rho_{\mathfrak{A}}}}, \quad (3.33)$$

lásd például a (13.54) egyenletet [41]-ban.

Ez meghatároz $d + 1$ pontot az elérhető ROC tartományban, ahol d a sűrűségmátrixok közös tartójának dimenziója. (Egy érdekes nyitott kérdés, hogy ezek a pontok vajon rajta vannak-e az optimális kvantum ROC görbén. Azt sejtjük, hogy igen.) Az ezek által a pontok által meghatározott $(0, 0)$ és $(1, 1)$ közötti töröttvonal Minkowski hossza éppen a mérés klasszikus Bhattacharyya-együtthatója, vagyis a fidelity négyzetgyöke. Ez is nyilvánvalóan konvex, és az elérhető ROC tartományban fut, vagyis az optimális kvantum ROC görbe alatt fut. Ha a két sűrűségmátrix kommutál, akkor a ROC görbe egybeesik ezzel a töröttvonallal, mert a mérés maga klasszikussá válik. Ezután az állítás következik az 1 lemmából. \square

Plauzibilisnek tűnik, hogy nem csak a kommutativitásból következik a két mennyiség egyenlősége, hanem fordítva is, a két mennyiség csak kommutáló sűrűségmátrixok esetén lehetne egyenlő. Ez abból adódhatna, hogy a pacák konvex burkaként előálló ROC görbe mindenképpen a fidelityt meghatározó görbevonallal fölött fut, mert azok a húrjai. Ez igaz

lenne, ha bizonyítani tudnánk, hogy a pacák határa deriválható, nincsenek benne törések. Ezt sajnos nem tudtuk kizárni. A pacákat a Helstrom formulában lévő paraméteres mátrix sajátvektoraiból kapjuk, és bár általában a paramétertől simán függenek a sajátvektorok, ugrások előfordulhatnak sajátérték keresztezések esetén.

3. Állítás. *A kvantum Bhattacharyya-együttható monoton teljesen pozitív leképezésekre. Vagyis, ha C egy tetszőleges teljesen pozitív leképezés, akkor*

$$\forall \rho_1, \rho_2, B(\rho_1, \rho_2) \leq B(C\rho_1, C\rho_2). \quad (3.34)$$

Bizonyítás. A bizonyításhoz vennünk kell az összes lehetséges POVM által kitöltött ROC tartományt (aminek a ROC görbe a felső széle). Heisenberg képben a teljesen pozitív leképezés a mérési operátort leképezi egy másik legális POVM operátorára, míg a sűrűségmátrixokat helyben hagyja. Mivel a korábbi tartomány az összes POVM-et tartalmazza, a leképezett POVM-hez tartozó pontnak is a tartományban kell maradnia. Vagyis a ROC tartomány nem növekedhet, de esetleg összemehet. Ezen kívül az új tartomány is konvex, hiszen Schrödinger képben éppen a transzformált állapotokon végezhető összes mérést reprezentálja. Vagyis a transzformált ROC görbének az eredeti alatt kell húzódnia, tehát az 1. lemma alapján hosszabbnak kell lennie. \square

Megjegyezzük, hogy a rögzített rangú projektorokhoz tartozó pacák önmagukban nem húzódnak össze. Ez például onnan is látható, hogy a pacák baloldali (függőleges) és felső (vízszintes) érintőinek helyét az első és a második állapot kumulatív sajátértékösszegeik adják. Egy teljesen pozitív leképezés a sajátértékeket növelheti és csökkentheti is, így az érintők mindkét irányban elmozdulhatnak. Sejtésünk szerint viszont unitális leképezésekre a pacák is kontrahálódnak.

3.1.7. Egyértelmű kvantumállapot megkülönböztetés

A fent ismertetett ROC technikát az egyértelmű kvantumállapot megkülönböztetésben is használhatjuk. Ismét tekintsünk két kvantumállapotot, egy „pozitívat” és egy „negatívát”. (Nem kell, hogy tiszták legyenek, vagy megegyezzen a tartójuk.) A feladat most három POVM operátort találni: ha az eredmény M_p , az állapot bizonyosan pozitív, ha M_n , akkor

negatív. És sajnos kell egy harmadik operátor is, hogy a POVM teljes legyen: ha $M_? = \hat{1} - M_p - M_n$ az eredmény, akkor az állapot ismeretlen (inkonklúzív eset).

Az első ötlet, hogy az inkonklúzív esetet egybevonjuk az egyik konklúzívvval. Ha a negatívval vonjuk össze, egy olyan diszkriminátort kapunk, aminek a valódi pozitív rátája egy, vagyis a hozzá tartozó pont a ROC térben a $(0, 1) \rightarrow (1, 1)$ vonalon fekszik. Ha a pozitívval vonjuk össze, a hamis pozitív ráta lesz nulla, vagyis a pont az y tengelyen lesz. Vagyis az egyértelmű kvantumállapot megkülönböztetés szükséges feltétele, hogy az állapotok optimális ROC görbéje érintse az y tengelyt és a $(0, 1) \rightarrow (1, 1)$ vonalat is (a $(0, 0)$ és $(1, 1)$ pontokon kívül).

Ezután megmutatjuk, hogy ez elégséges is. Vegyünk egy állapotpárt, amik teljesítik a fenti feltételeket. Mindkét érintési ponthoz tartozik egy-egy optimális mérés azzal a tulajdonsággal, hogy az egyik állapotot bizonyossággal detektálják, mivel a másik sűrűségmátrix nullterére vetítenek. Például a Helstrom-formulából megkaphatjuk ezeket a projektorokat, amiket jelöljünk \tilde{M}_p -vel és \tilde{M}_n -nel. Ezt a két operátort még nem lehet egy POVM mérésbe összerakni, mert az összegüknek lehet egynél nagyobb sajátértéke, de léteznek $\lambda_1, \lambda_2 \in]0, 1]$ számok, hogy $\lambda_1 \tilde{M}_p + \lambda_2 \tilde{M}_n \leq \hat{1}$. ($\lambda_1 = \lambda_2 = 1/2$ például biztosan egy megfelelő választás.) A λ -k hangolásával növelhetjük az egyik állapot felismerési valószínűségét a másik kárára. Végül $\tilde{M}_? = \hat{1} - \tilde{M}_p - \tilde{M}_n$ lesz az inkonklúzív operátor, amivel teljes a háromelemű POVM-ünk, ami megvalósítja az egyértelmű kvantumállapot megkülönböztetést, bár nem biztos, hogy optimálisan.

3.2. Kétrésű korrelációk és Bayes-i játékok

Ebben a fejezetben a nem klasszikus kétrésű korrelációkkal kapcsolatos eredményeimet ismertetem. Először illusztrálom azokat a numerikus eszközöket, amiket illetve amelyekhez hasonlókat az eredmények kidolgozásához használtunk. A módszerek ismertetését nem klasszikus illetve esetenként kvantum előnnyel rendelkező játékok egy általunk felismert általános konstrukciójának bemutatása követi. Végül kitérünk egy esetre amely nem illeszkedik ebbe a sémába.

3.2.1. Numerikus módszerek

Manapság számos programcsomag áll rendelkezésre a poliéderekkel kapcsolatos számítások elvégzéséhez. Így Fine eredményét is könnyen reprodukálhatjuk, például a Parma Polyhedra Library [43] programcsomag segítségével, Python nyelven a következőképpen:

```
#!/usr/bin/env python3

from ppl import Variable, Generator_System, C_Polyhedron, point
import ppl

v = [[[[ Variable(a+2*b+4*x+8*y) for y in range(2)] for x in range(
                2)]
      for b in range(2) ] for a in range(2)]

gs = Generator_System()

# A különbozo determinisztikus korelaciok:
#aX: Aliz kimenetei, bX: Bob kimenetei
for a0 in range(2):
    for a1 in range(2):
        for b0 in range(2):
            for b1 in range(2):
                gs.insert(point(v[a0][b0][0][0]+
                                v[a0][b1][0][1]+
                                v[a1][b0][1][0]+
                                v[a1][b1][1][1]))

polygs = C_Polyhedron(gs)

print(polygs.minimized_constraints())
```

A program a következő eredményt adja:

```
Constraint_System {x12+x13+x14+x15 -1==0,
    x0+x1 -x4+x7 -x13 -x15==0,  x0+x2+x9+x11 -1==0,
    x10+x11 -x14 -x15==0,  x0+x1+x2+x3 -1==0,
    x0+x2 -x8+x11 -x14 -x15==0,  x0+x1 -x4 -x5==0,
```


$x \downarrow y \rightarrow$		0		1	
		$a \downarrow$	$b \rightarrow$	0	1
0	0	x_0	x_2	x_8	x_{10}
	1	x_1	x_3	x_9	x_{11}
1	0	x_4	x_6	x_{12}	x_{14}
	1	x_5	x_7	x_{13}	x_{15}

3.1. táblázat. A változók a Python kódban.

$$\begin{aligned}
&x_4 + x_6 + x_{13} + x_{15} - 1 = 0, \quad -x_4 - x_{13} - x_{15} + 1 \geq 0, \quad x_2 \geq 0, \\
&-x_0 - x_1 - x_2 + 1 \geq 0, \quad -x_0 - x_1 + x_4 + x_{13} + x_{15} \geq 0, \\
&-x_0 - x_2 - x_{11} + 1 \geq 0, \quad x_1 \geq 0, \quad x_{11} \geq 0, \quad x_{13} \geq 0, \quad x_{15} \geq 0, \\
&x_{14} \geq 0, \quad -x_{11} + x_{14} + x_{15} \geq 0, \quad x_0 + x_1 - x_4 \geq 0, \quad x_4 \geq 0, \quad x_0 \geq 0, \\
&-x_1 + x_4 + x_{11} + x_{13} \geq 0, \quad -x_{13} - x_{14} - x_{15} + 1 \geq 0, \\
&x_0 + x_2 + x_{11} - x_{14} - x_{15} \geq 0, \quad -x_0 - x_1 - x_2 + x_4 - x_{11} + x_{15} + 1 \geq 0, \\
&x_2 + x_4 + x_{11} - x_{14} \geq 0, \quad x_0 - x_4 + x_{11} - x_{13} - x_{14} - x_{15} + 1 \geq 0, \\
&x_0 + x_1 + x_2 - x_4 + x_{11} - x_{15} \geq 0, \quad x_1 - x_4 - x_{11} - x_{13} + 1 \geq 0, \\
&-x_2 - x_4 - x_{11} + x_{14} + 1 \geq 0, \quad -x_0 + x_4 - x_{11} + x_{13} + x_{14} + x_{15} \geq 0 \}
\end{aligned}$$

Mivel a feltételek legkisebb halmazát kapjuk, minden egyenlőtlenség egy oldalnak felel meg. Látható, hogy 8 egyenlőség és 24 egyenlőtlenség határozza meg a lokális politópot. Várakozásunk szerint a 24 oldalból 16 $x_i \geq 0$ alakú valószínűségi megszorítás, a maradék nyolc pedig a Fine által felsorolt egyenlőtlenségek. Ezeket azonban a fenti eredményben első látásra nem találjuk meg. De mivel bármelyik egyenlőtlenséghez hozzá lehet adni az egyenlőségek tetszőleges lineárkombinációját, ezért a gép nem az általunk elvárt könnyen átlátható alakban adta meg az eredményt. Például az $x_6 \geq 0$ feltételt az $x_4 + x_{12} - x_{14} \geq 0$ és az $x_4 - x_6 + x_{12} - x_{14} = 0$ feltételek különbségeként kaphatjuk meg.

Megjegyezzük, hogy nagyobb problémák (több ki- és bemenet esetén) a csúcspont alapján a lapok numerikus meghatározása már akadályokba ütközik, mert a használt ún. Fourier-Motzkin algoritmus rosszul skálázódik. Ilyen kisméretű problémánál viszont még azt is

megtehetjük, és talán tanulságos is, hogy megnézzük, melyik oldalon mely csúcsok találhatóak. Az eredmények a 3.2 táblázatban találhatóak. (A programcsomag segítségével ez is könnyen meghatározható, a részleteket itt nem közöljük.) Látható, hogy a valószínűségi feltételekhez tartozó oldalakra 12 csúcs illeszkedik (ami logikus, hiszen mindegyik változó a csúcsok egynegyedében 1, háromnegyedében 0), a Bell-egyenlőtlenségekhez tartozókra pedig 8.

Jelentősen egyszerűsödik a helyzet, ha csak olyan eloszlásokat nézünk, ahol az összes marginális az egyenletes eloszlás. Ekkor csak 4 dimenzió, 8 csúcs és 16 oldal marad. A csúcsok mindegyike négy darab $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ vagy $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ blokkot tartalmaz. Ezekből három szabadon választható, a negyediket meghatározza a nemjelző feltétel. A csúcsokat jellemezhetjük a négy blokk bal felső sarkában lévő értékkel, ami vagy nulla vagy egykettő (a táblázatban a helykitöltés miatt egy). Bár a számítógép kissé összekeverte a csúcsokat és oldalakat, látható, hogy a csúcsokat 4 párba rendezhetjük. Ha a $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ blokkot feketével, a $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ blokkot fehérrel jelöljük, akkor vízszintes, függőleges, átlós és teljes mintákat kapunk. Mindegyik páros közül mindegyik oldalon pontosan egy csúcs található, az összes lehetséges kombináció adja ki a 16 oldalt. Ha így rendezzük őket párba:

+	$\begin{pmatrix} X & X \\ & \end{pmatrix}$	$\begin{pmatrix} X \\ & X \end{pmatrix}$	$\begin{pmatrix} X & \\ & X \end{pmatrix}$	$\begin{pmatrix} X & X \\ X & X \end{pmatrix}$
-	$\begin{pmatrix} & \\ X & X \end{pmatrix}$	$\begin{pmatrix} X \\ X \end{pmatrix}$	$\begin{pmatrix} & X \\ X & \end{pmatrix}$	$\begin{pmatrix} & \\ & \end{pmatrix}$

akkor a páros paritású oldalak (pl. ++++) Bell-egyenlőtlenségekhez, a páratlan paritásúak valószínűségi megszorításokhoz tartoznak.

Megjegyezzük, hogy a politóp struktúrájának megértéséhez érdemes átgondolni a szimmetriákat is. Egy Bell-elrendezés szimmetriái általában: felcserélhetők a résztvevők, permutálhatók egy résztvevő mérései és bármelyik mérésre permutálhatók a lehetséges kimenetek. Így a CHSH elrendezésben bármelyik két Bell-egyenlőtlenség oldala felcserélhető, és a valószínűségi megszorítások is felcserélhetők. Bonyolultabb elrendezésben ez már nincs így,

$P(a = 1 x = 0)$	0 1 0 1	0 1 0 1	0 1 0 1	0 1 0 1
$P(a = 1 x = 1)$	0 0 1 1	0 0 1 1	0 0 1 1	0 0 1 1
$P(b = 1 y = 0)$	0 0 0 0	1 1 1 1	0 0 0 0	1 1 1 1
$P(b = 1 y = 1)$	0 0 0 0	0 0 0 0	1 1 1 1	1 1 1 1
$-x_4 - x_{13} - x_{15} + 1 \geq 0$	X X	X X X X	X X	X X X X
$x_2 \geq 0$	X X	X X	X X X X	X X X X
$-x_0 - x_1 - x_2 + 1 \geq 0$	X X X X	X X X X	X X	X X
$-x_0 - x_1 + x_4 + x_{13} + x_{15} \geq 0$	X X X X	X X	X X X X	X X
$-x_0 - x_2 - x_{11} + 1 \geq 0$	X X X X	X X X X	X X	X X
$x_1 \geq 0$	X X X X	X X X X	X X	X X
$x_{11} \geq 0$	X X X X	X X X X	X X	X X
$x_{13} \geq 0$	X X X X	X X	X X X X	X X
$x_{15} \geq 0$	X X X X	X X	X X X X	X X
$x_{14} \geq 0$	X X	X X X X	X X	X X X X
$-x_{11} + x_{14} + x_{15} \geq 0$	X X	X X	X X X X	X X X X
$x_0 + x_1 - x_4 \geq 0$	X X X X	X X	X X X X	X X
$x_4 \geq 0$	X X	X X X X	X X	X X X X
$x_0 \geq 0$	X X	X X	X X X X	X X X X
$-x_1 + x_4 + x_{11} + x_{13} \geq 0$	X X	X X	X X	X X
$-x_{13} - x_{14} - x_{15} + 1 \geq 0$	X X	X X X X	X X	X X X X
$x_0 + x_2 + x_{11} - x_{14} - x_{15} \geq 0$	X X	X X	X X X X	X X X X
$-x_0 - x_1 - x_2 + x_4 - x_{11} + x_{15} + 1 \geq 0$	X X	X X	X X	X X
$x_2 + x_4 + x_{11} - x_{14} \geq 0$	X X	X X	X X	X X
$x_0 - x_4 + x_{11} - x_{13} - x_{14} - x_{15} + 1 \geq 0$	X X	X X	X X	X X
$x_0 + x_1 + x_2 - x_4 + x_{11} - x_{15} \geq 0$	X X	X X	X X	X X
$x_1 - x_4 - x_{11} - x_{13} + 1 \geq 0$	X X	X X	X X	X X
$-x_2 - x_4 - x_{11} + x_{14} + 1 \geq 0$	X X	X X	X X	X X
$-x_0 + x_4 - x_{11} + x_{13} + x_{14} + x_{15} \geq 0$	X X	X X	X X	X X

3.2. táblázat. Oldalak és csúcsok a CHSH elrendezés lokális politópjában.

$2p(00 00)$	0 1 1 1	0 1 0 0
$2p(00 01)$	0 0 0 1	1 1 0 1
$2p(00 10)$	1 0 1 1	1 0 0 0
$2p(00 11)$	1 1 0 1	0 0 0 1
$x_0 \geq 0$	X	X X X
$x_0 + x_4 - x_8 + x_{12} \geq 0$		X X X X
$x_4 \geq 0$	X	X X X
$-2 * x_8 + 1 \geq 0$		X X X
$-x_0 + x_4 - x_8 - x_{12} + 1 \geq 0$	X X	X X
$x_0 + x_4 + x_8 - x_{12} \geq 0$	X X	X X
$x_0 - x_4 - x_8 - x_{12} + 1 \geq 0$	X X	X X
$-2 * x_4 + 1 \geq 0$	X X X	X
$x_{12} \geq 0$	X	X X X
$-2 * x_{12} + 1 \geq 0$	X X X	X
$x_8 \geq 0$	X X X	X
$-2 * x_0 + 1 \geq 0$	X X X	X
$-x_0 + x_4 + x_8 + x_{12} \geq 0$	X X	X X
$-x_0 - x_4 - x_8 + x_{12} + 1 \geq 0$	X X	X X
$x_0 - x_4 + x_8 + x_{12} \geq 0$	X X	X X
$-x_0 - x_4 + x_8 - x_{12} + 1 \geq 0$	X X X X	

3.3. táblázat. Oldalak és csúcok a CHSH elrendezés lokális politópjában egyenletes marginálisok esetén.

p(ab 00)	b b b b	d d d d	c c c c	\emptyset a \emptyset a	a \emptyset a \emptyset	\emptyset \emptyset \emptyset \emptyset
p(ab 01)	a b a b	c d d c	d c c d	\emptyset a \emptyset b	b \emptyset a \emptyset	\emptyset \emptyset \emptyset \emptyset
p(ab 10)	d d b b	b d b d	a c a c	\emptyset c \emptyset c	a \emptyset a \emptyset	\emptyset \emptyset \emptyset \emptyset
p(ab 11)	c d a b	a d b c	b c a d	\emptyset c \emptyset d	b \emptyset a \emptyset	\emptyset \emptyset \emptyset \emptyset
x0>=0	X X X X	X X X X	X X X X			X X X X
-x4-x6-x8-x9+x12+1>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
x4+x6-x12>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
x8+x9-x12>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
x12>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
-x0-x2-x9+1>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
x0+x2-x8>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
x9>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
x8>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
-x0-x1-x6+1>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
x6>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
x0+x1-x4>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
x4>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
-x0-x1-x2+1>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
x2>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X
x1>=0	X X X X	X X X X	X X X X	X X X X	X X X X	X X X X

3.4. táblázat. Oldalak és csúcsok a CHSH elrendezés nemjelző politópjában. A marginálisokra nincs megkötés. A betűkkel jelölt csúcsok a lokális politóp csúcsai, a szellemek PR-dobozok.

2p(00 00)	0 0 0 0	0 0 0 0	1 1 1 1	1 1 1 1
2p(00 01)	0 1 0 0	1 1 1 0	0 0 1 0	0 1 1 1
2p(00 10)	1 0 0 0	0 1 1 1	1 1 0 0	0 0 1 1
2p(00 11)	0 1 1 0	0 0 1 1	1 0 1 1	0 0 0 1
-2 * x0 + 1 >= 0			X X X X	X X X X
x12 >= 0	X X X X	X X X X	X X X X	X X X X
-2 * x12 + 1 >= 0	X X X X	X X X X	X X X X	X X X X
x8 >= 0	X X X X	X X X X	X X X X	X X X X
-2 * x8 + 1 >= 0	X X X X	X X X X	X X X X	X X X X
x4 >= 0	X X X X	X X X X	X X X X	X X X X
-2 * x4 + 1 >= 0	X X X X	X X X X	X X X X	X X X X
x0 >= 0	X X X X	X X X X	X X X X	X X X X

3.5. táblázat. Oldalak és csúcsok a CHSH elrendezés nemjelző politópjában egyenletes marginálisok esetén.

ott léteznek egymással nem ekvivalens Bell-egyenlőtlenségek is.

Ennek a politópnak azonban egy plusz szimmetriája is van: Az egyenletes marginálisú lokális politópban a Bell- és valószínűségi oldalakat is felcserélhetjük egymással. Ehhez csak egy vagy három párnál fel kell cserélni a párt alkotó két csúcsot.¹

Például a

$$\begin{pmatrix} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \end{pmatrix} \quad (3.35)$$

irányra merőleges 15 dimenziós síkra tükröző operátor felcseréli az utolsó két párt, a többi helyben hagyja.

3.2.2. A 2-2-3-3 politópok szerkezete

A 3.2.4 pontban szükségünk lesz a $|X| = |Y| = 2$, $|A| = |B| = 3$ eset nemjelző politópjának egy csúcsára, ezért most megvizsgáljuk ezen lokális és nemjelző politópok szerkezetét. A 3.2.1 pontban ismertetett módszerekkel ebben az esetben még könnyen kiszámíthatók a lapok és a csúcsok. A lokális politópnak 81 csúcsa és 1116 lapja, a nemjelző politópnak pedig 36 lapja és 1161 csúcsa van. (Érdekes megjegyezni, hogy ha további feltételként azt is megköveteljük, hogy a lokális marginális eloszlások egyenletesek legyenek, a nemjelző politóp esetében 36 lapot és 1296 csúcsot kapunk, de a lokális politóp esetén már beleütközünk a politóp reprezentációváltásának számítási nehézségébe: a program néhány nap alatt nem fut le.)

A numerikus eredmények azt adják, hogy a lokális politópnak 4 fajta lapja van. A lapokra illeszkedő csúcsok száma rendre 72, 45, 36 és 30. A lapok numerikusan kapott együtthatói az ismert többértelműség miatt első ránézésre elég nehezen értelmezhetők, de a szimmetriák felfedezéséhez sokat segít, ha átlagoljuk a lapra illeszkedő pontokat (ami a lap súlypontját adja). Ez alapján a lapokat a 3.6 táblázat szerinti alakra lehet hozni:

- Az első (36 darab) a valószínűségi megszorításokhoz tartozó típus.

¹Igazából ez egy 4 dimenziós oktaéder.

$x \downarrow y \rightarrow$		0			1		
$a \downarrow b \rightarrow$		0	1	2	0	1	2
0	0	-1	0	0	0	0	0
	1	0	0	0	0	0	0
	2	0	0	0	0	0	0
1	0	0	0	0	0	0	0
	1	0	0	0	0	0	0
	2	0	0	0	0	0	0

$x \downarrow y \rightarrow$		0			1		
$a \downarrow b \rightarrow$		0	1	2	0	1	2
0	0	-1	-1	1	-1	-1	1
	1	-1	-1	1	-1	-1	1
	2	1	1	-1	1	1	-1
1	0	-1	-1	1	1	1	-1
	1	-1	-1	1	1	1	-1
	2	1	1	-1	-1	-1	1

$x \downarrow y \rightarrow$		0			1		
$a \downarrow b \rightarrow$		0	1	2	0	1	2
0	0	1	1	-1	1	1	-1
	1	1	1	-1	1	1	-1
	2	-1	-1	1	-1	-1	1
1	0	1	1	-1	-1	-1	1
	1	1	1	-1	-1	-1	1
	2	-1	-1	1	1	1	-1

$x \downarrow y \rightarrow$		0			1		
$a \downarrow b \rightarrow$		0	1	2	0	1	2
0	0	1	0	-1	1	-1	0
	1	-1	1	0	0	1	-1
	2	0	-1	1	-1	0	1
1	0	1	-1	0	-1	1	0
	1	0	1	-1	0	-1	1
	2	-1	0	1	1	0	-1

3.6. táblázat. A „két bemenet, három kimenet” elrendezés összes oldala. Az első a valószínűségi megszorítás, a második (36 pontos) és harmadik (45 pontos) a CHSH egyenlőtlenség kiterjesztései, a negyedik a CGLMP egyenlőtlenség $d = 3$ -ra.

- A következő kettő (324, 324 darab) a CHSH egyenlőtlenség kiterjesztése úgy, hogy a 2 kimenetes változatból minden bemenetnél egy kimenetet „megduplázunk”, vagyis az új kimenet együtthatói mindkét bemenet esetén az egyik eredeti kimenet együtthatóival azonosak. Tehát minden bemenet esetén az első két sor, illetve oszlop azonos, és az azonosak egyikét elhagyva visszakapjuk a CHSH politóp egy lapját. Ezt kétféleképpen tehetjük meg, a két lehetőség együtthatója egymás -1-szerese. A több negatív együtthatót tartalmazó lapokra 36 csúcs, a több pozitív együtthatót tartalmazókra 45 csúcs illeszkedik.
- A negyedik (432 darab) pedig az ún. Collins-Gisin-Linden-Massar-Popescu (CGLMP) típusú egyenlőtlenség.; ezekre rövidesen visszatérünk.

A CGLMP egyenlőtlenség. A CGLMP egyenlőtlenséget Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar és Sandu Popescu fedezték fel [44]. Az egyenlőtlenség a két bemenetű, d kimenetű elrendezés egy Bell-egyenlőtlensége. Lluís Masanes [45] bebizonyította, hogy az egyenlőtlenség minden d esetén szoros, azaz a lokális politóp egy oldalát határozza meg. Az alakja:

$$I_d = \sum_{k=0}^{\lfloor d/2-1 \rfloor} \left(1 - \frac{2k}{d-1}\right) \sum_{c=0}^{d-1} (p(c, c+k|00) - p(c, c-k-1|00) + p(c, c-k|01) - p(c, c+k+1|01) + p(c, c-k-1|10) - p(c, c+k|10) + p(c, c+k|11) - p(c, c-k-1|11)) \leq 2, \quad (3.36)$$

ahol $p(c, c+k|00)$ jellegű kifejezésekben az összeadás modulo d értendő. Vegyük észre, hogy $d = 2$ esetben a CGLMP egyenlőtlenség maga a CHSH egyenlőtlenség.

Tehát a 2-2-3-3 esetben kapott eredményünk azt mutatja, hogy a lokális politóp lapjait a valószínűségi megszorítások, a $d = 2$ eset CGLMP egyenlőtlenségeiből a leírt „duplázási” eljárással kapott lapok, és a $d = 3$ -hoz tartozó „natív” CGLMP egyenlőtlenségek által definiált lapok összessége adja.

Sejtésünk, hogy ez minden két bemenetes elrendezésre általánosítható: a lokális politóp minden lapját az alacsonyabb d -hez tartozó CGLMP egyenlőtlenségekből sorok és oszlopok másolásával lehet megkapni.

Végül térjünk vissza a nemjelző politóp szerkezetére. A numerikus számítás alapján ennek 36 oldala és 1161 csúcsa van. Ebből 81 lokális, 648 olyan, ahol egy PR dobozt helyezünk el a táblázatban, és 432 (éppen annyi, mint ahány ún. CGLMP egyenlőtlenség van) olyan nemjelző csúcs, amelyek lokális marginálisai egyenletes eloszlások. Ez utóbbiak mind megkaphatók egymásból szimmetriatranszformációval; egyiküket fogjuk használni a 3.2.4. pontban, alakját is ott ismertetjük.

3.2.3. Kvantumelőnnyel rendelkező játékok konstrukciója

A 2.3.1. pontban áttekintettük a Bayes-i játékok egyensúlyával kapcsolatos alapfogalmakat. Kérdés, hogy mi köze ennek a 2.2. pontban ismertetett kétrészes korrelációkhoz. Mint láttuk, a teljes információs játékoknál a korrelált egyensúlyt (előzetes megegyezés hiányában) egy megbízható harmadik fél segítségével lehetett létrehozni. De a tanácsadás-

hoz csak a kifizetések ismeretére volt szüksége. Bayes-i esetben mindkét játékos típusára is szükség van az optimális döntéshez, tehát ekkor a játékosoknak előbb el kell árulniuk a saját típusukat a harmadik félnek, és ezután kapják meg a jótanácsot. Vagyis a harmadik fél egy többkomponensű rendszernek tekinthető, amin a játékosok különböző méréseket végezhetnek: bemenetként elárulják a típusukat (vagy hazudnak róla), kimenetként várják a tanácsot. Ha plusz feltételként megszabjuk, hogy a játékosok a kapott tanácsból semmilyen információhoz ne jussanak a másik típusáról, máris azt kapjuk, hogy a harmadik fél válaszainak egy nemjelző korreláció eloszlásai szerint kell alakulniuk.

Vegyük a következő játékot [36]. Alíznek és Bobnak két-két típusa lehet, és minden esetben két akciója, amiket mind egy bittel jellemezünk. Az eddigi jelölésekhez hasonlóan Alíz és Bob típusát x és y , az akciójukat a és b jelölje. A kifizetés mindkettőjük számára 1, ha $a \otimes b = x \wedge y$, -1 egyébként (lásd a 3.7. táblázatot). Ezt CHSH játéknak nevezzük a CHSH elrendezéshez hasonló struktúrája miatt. Mivel a kifizetések azonosak, Alíz és Bob itt nem ellenfelek, hanem az ulthoz hasonlóan együtt küzdenek egy nem konkretizált harmadik féllel szemben. A kifizetés bináris, amit megfeleltethetünk annak a két esetnek, hogy Alízék vagy győznek, vagy veszítenek.

A várható kifizetés, ha egyenletes priort tételezünk fel:

$$U = \frac{1}{4} \sum_{x,y} \sum_{a,b} u(a, b, x, y) P(a, b|x, y), \quad (3.37)$$

vagyis a stratégiát jellemző feltételes valószínűségek (a viselkedés) lineáris függvénye.

A várható kifizetés attól függően, hogy mit tételezünk fel a valószínűségekről (vagy mit engedünk meg a játékosoknak), különböző maximumokat vehet fel.

Egy lehetséges feltételezés, hogy a játékosok lokális, klasszikusan viselkedő erőforrások birtokában vannak csak. Ez praktikusán annyit jelent, hogy a játék kezdete előtt összebe-szélhetnek, de a típusuk megismerése után nem csak, hogy nem kommunikálhatnak, de semmilyen különleges berendezés segítségét sem vehetik igénybe. Ekkor a viselkedésüknek a már bemutatott lokális politópon belül kell maradnia. Az optimumot egy lineáris program adja, ahol a megoldásnak teljesítenie kell a $P(a, b|x, y) \in \mathcal{P}_L$ megszorítást (\mathcal{P}_L a lokális politóp). A célfüggvény viszont éppen a CHSH egyenlőtlenség, vagyis ennek maximális értéke $1/2$. A gyakorlatban ezt például úgy lehet elérni, hogy mindig a $(0, 0)$ akciót választják. Mivel két egyenletes eloszlású bit logikai és függvénye 3 esetben 0, így $3/4$ valószínűséggel

$x \downarrow y \rightarrow$		0		1	
		$a \downarrow$	$b \rightarrow$		
0	0	1	-1	1	-1
	1	-1	1	-1	1
1	0	1	-1	-1	1
	1	-1	1	1	-1

$x \downarrow y \rightarrow$		0		1	
		$a \downarrow$	$b \rightarrow$		
0	0	1/2	0	1/2	0
	1	0	1/2	0	1/2
1	0	1/2	0	0	1/2
	1	0	1/2	1/2	0

3.7. táblázat. A CHSH játék kifizetésfüggvénye (fent) és a PR-doboz, ami az optimális nemjelző viselkedés (lent). Mivel Alíz és Bob kifizetései megegyeznek, minden pozícióban csak egy szám szerepel.

győznek. (De más optimális stratégiák is vannak.) Mivel itt várható kifizetést számolunk, ezért kaptuk a hagyományos 2 érték negyedét.

Vizsgálhatjuk azt az esetet is, amikor a játékosok egy megosztott kvantumrendszer rájuk eső részén végezhetnek méréseket a típusuk megismerése után, ekkor az optimalizációt a választott (2.2.4. fejezetben megismert) valamelyik kvantumos halmazra kell elvégezni. Amennyiben legalább az egyik játékosnak csak két típusa és két akciója van – a CHSH játékban ez a helyzet –, akkor az összes fent említett kvantumos halmaz egybeesik [46, 18]. A heurisztikusan megállapított maximális érték $\sqrt{2}/2$, ami a Tsirelson-határ.

A következő logikus lépés, hogy a nemjelző politópon belül keressük az optimumot, vagyis az egyetlen megszorítás, hogy a játékosok nem használhatnak klasszikus információ átadására alkalmas eszközt. Ha játékosok egymás fénykúpján kívül tartózkodnak a típusuk megismerése és az akció kiválasztása között, akkor a fizika mai állása szerint nem lehetséges a fenti feltétel által megengedett összes korreláció realizálása, de gyakorlatilag megvalósítható, ha valamilyen kontrollált kommunikációt megengedünk a szereplők között. Persze ekkor a csalások megakadályozásában nem hagyatkozhatunk pusztán a relativitáselméletre.

Ha megoldjuk azt a lineáris programot, ahol a célfüggvény (3.37) jobb oldala és a feltétel az, hogy $P(a, b|x, y) \in \mathcal{P}_{\text{NJ}}$ (\mathcal{P}_{NJ} a nemjelző politóp), akkor azt kapjuk, hogy az optimum 1. (Ismét, a Bell-egyenlőtlenségek szakirodalmában ez 4-nek felel meg.) A célfüggvény az optimumot a nemjelző politóp egy olyan csúcsán veszi fel, ami mind a lokális, mind a kvantum tartományon kívül esik. A megoldás a 3.7. táblázat lenti részén látható, ez nem más, mint a Popescu-Rorhlich (PR) doboz [47, 48, 49, 50].

Itt nem feltétlenül kell megállni. Az információ kauzalitás ([13]) definíciójában például Alíz átküldhet megszabott számú klasszikus bitet Bobnak, de ezzel az iránnyal ebben a dolgozatban nem foglalkozunk.

Itt két fontos megjegyzést kell tennünk. Először, mivel Alíz és Bob kifizetései megegyeznek, ezért a kifizetések maximalizálása szükségszerűen egy ex-ante egyensúlyhoz vezet. Ha nem egyensúly lenne, akkor az egyik játékosnak megérné eltérnie, amivel növelné a saját és jelen esetben a másik kifizetését, vagyis nem lehattunk a kifizetés maximumában. Másodszor, ha egyszer (x, y) rögzítettek (kiderült a típus), akkor az ex-post helyzetben a kifizetés

csakis az akcióktól függ, és az ex-ante egyensúly megfelelő blokkjához tartozó $P(a, b|x, y)$ (esetleg korrelált) valószínűségeloszlás egy lehetséges stratégiává válik az (x, y) -hoz tartozó teljes információs (rész)játék számára. Ekkor feltehetjük a kérdést, hogy ez a stratégia egyensúly-e ennek a bimátrix játéknak. *A CHSH játék esetén az optimális nemjelző viselkedéshez tartozó eloszlások az összes (x, y) típusok esetén korrelált egyensúlyok.* Más szóval egy ex-post egyensúlyt értünk el. Intuitíve ez a következőt jelenti: A Bayes-i játékokban egy fontos feltevés, hogy a játékosok nem ismerik egymás típusát, és itt is egy PR-dobozt használunk ahhoz, hogy a játékosok az optimális stratégiát alkalmazhassák. De a megfigyelésünkből az következik, hogy a játékosoknak akkor sem érdemes eltérniük a PR-doboz által javasolt akciótól, ha megismernék a másik típusát, ami az ex-post helyzet. Ugyanez igaz akkor is, ha kvantum korrelációkat engedünk, mert a kvantum optimum a PR-doboz és az egyenletes eloszlás konvex kombinációja.

A CHSH játék konstrukcióját vizsgálva még egy megfigyelést tehetünk. Ha egy nemlokális erőforrások szempontjából érdekes játékot keresnénk, és nem ismernénk a CHSH játékot, a következőképp is eljuthatunk volna hozzá: először vegyük a nemjelző politóp (\mathcal{P}_{NJ}) egyik nemlokális csúcsát, ez definiál egy viselkedést. Ezután a kifizetéseket úgy adjuk meg, hogy az összes (x, y) típushoz tartozó blokkban a hozzátartozó valószínűségeloszlás a kifizetés egy korrelált egyensúlya legyen a (2.38) egyenlet szerint. A (2.38) egyenlet egy rögzített $p(a, b)$ eloszláshoz egy nemüres poliédert definiál a kifizetémátrixok terében, vagyis végtelen sok választásunk lehet. Ezen kívül a kifizetéseket úgy kell megválasztani, hogy egy adott prior (pl. egyenletes eloszlás) esetén a lokális politópra vett maximuma kisebb legyen, mint a nemlokális csúcsban felvett értéke. A konkrét példánkban a CHSH játék legyártható a PR-dobozból, ami (szimmetriák erejéig) az egyetlen nemtriviális nemlokális csúcs a két bemenet, két kimenet elrendezésben. Mivel a várható kifizetés egy lineáris függvény, és a kvantum tartomány egy konvex halmaz valahol a lokális és a nemjelző között, ezzel a módszerrel jó eséllyel olyan játékokhoz jutunk, amik kvantumelőnnyel rendelkeznek.

Az összes kvantumelőnnyel rendelkező játék, amiről tudomásunk van, előállítható ezzel a módszerrel. Példaként megemlíthetjük Brandenburger és La Mura nagysebességű tőzsdejátékát ([51]), és Bruckner térbeli tájékozódási játékát ([52]), két játékot, amit heurisztikusan fedeztek fel egymástól függetlenül. A két különböző kifizetés levezethető ugyanabból

a csúcsból. Az érdekütközéses játék ([53]), habár nem egy koordinációs játék (Alíz és Bob kifizetései különböznek), szintén követi ezt a sémát, ugyanazzal a csúccsal, mint a CHSH játék. De ezzel a módszerrel további játékok is konstruálhatók.

3.2.4. Egy új játék

Konstrukciónk alkalmazásával bemutatunk egy olyan játékot, amellyel az irodalomban még nem találkoztunk. Tekintsük azt az esetet, amikor mindkét félnek két típusa (bemenet) és három lehetséges eredménye (kimenet) van, vagyis $|X| = |Y| = 2$ $|A| = |B| = 3$. A lokális és nemjelző politópok szerkezetét a 3.2.2 pontban már ismertettük. Vegyük ezek közül a 3.8 táblázatban szereplő, CGLMP típusú csúcsot. Alkalmazzuk erre a 3.2.3 pontban leírt konstrukciónkat. Az egyszerűség kedvéért a kifizetés függvény együtthatói legyenek maguk a 3.8 táblázat valószínűségei. Könnyen belátható, hogy ebben az esetben maga a csúcs minden bemenet-párra korrelált egyensúlyt ír le. Ezt a játékot az „Egy közelebből meg

$x \downarrow y \rightarrow$		0			1		
		0	1	2	0	1	2
0	0	0	0	1/3	1/3	0	0
	1	1/3	0	0	0	1/3	0
	2	0	1/3	0	0	0	1/3
1	0	1/3	0	0	0	0	1/3
	1	0	1/3	0	1/3	0	0
	2	0	0	1/3	0	1/3	0

3.8. táblázat. A nemlokális politóp egy csúcsa, amit egyben a „Titkárnök játék” kifizetéseinek veszünk.

nem nevezett távolkeleti ország nagyon konzervatív cégének titkárnöje” játéknak nevezzük. (Röviden „Titkárnök játék”.)

A mögötte álló történet szerint Bob és Alíz egy nagyon konzervatív cég középvezetője és annak titkárnöje. (A nagyon konzervatív felsővezetésben fel sem merül annak lehetősége, hogy Alíz legyen a középvezető, és Bob az asszisztense. [54]) A cég irodaépületébe két be-

járaton lehet bejutni, és reggel három lehetséges érkezési időpont van, 8:00, 8:03 és 8:06 (amiket mint akciókat továbbra is 0, 1, 2-vel jelölünk). A cég nagyon paranoid biztonsági főnöke minden reggel elárulja az alkalmazottaknak, hogy aznap melyik véletlenszerűen kiválasztott bejáraton kell bemenniük, ezt természetesen nem árulhatják el másnak. Ezután Alíz és Bob eldönti, hogy mikor érkezzen. A pontozás a következőképp alakul: ha külön bejáratot használnak, akkor egyszerre kell érkezniük, hogy Alíz Bob munkakezdésének pillanatában már rendelkezésére álljon, de ne fogyassza fölöslegesen az áramot az épületben, ha a főnöke még nincs ott. Ha ugyanazt a bejáratot használják, akkor semmiképp sem érkezhetnek egyszerre biztonsági okokból. Ekkor Alíznek lehetőleg Bob előtt kellene megérkeznie, de nem érkezhethet közvetlenül előtte, mert ebben a nagyon konzeratív cégben nagy sértésnek számít közvetlenül a főnök előtt bemenni. Így Alíz csak akkor érkezhethet előbb, ha Bob 8:06-kor érkezik. Egyébként közvetlenül utána kell érkeznie, hogy Bobnak csak minimálisan kelljen várnia rá.

Alíz és Bob nyernek, ha sikerül betartaniuk a szabályokat ($1/3$ pont), veszítenek, ha nem (0 pont).

Könnyen látható, hogy tiszta lokális stratégiák esetén a négy típuskombináció közül legfeljebb 3-ban tud Alíz és Bob nyerni, a negyedikben veszítenek, ezért lokális stratégiák esetén a kifizetés várható értéke legfeljebb $1/4$. Nemjelző stratégiák esetén természetesen semmi akadály, hogy a játékosok mindig nyerjenek, ezért a várható kifizetés ekkor $1/3$.

A lokális politópnak összesen 12 olyan csúcsa van, ami eléri a maximális várható kifizetést. De ez a 12 csúcs nem alkotja a lokális politóp egyik oldalát, vagyis ennek a játéknak a várható kifizetését nem lehet Bell-egyenlőségnek használni. Az a lap ugyanis, amelyikhez ez a 12 csúcs tartozik, összesen 30 csúcst tartalmaz, mégpedig azokat a csúcsokat, amikre a várható kifizetés legalább $1/6$, vagyis ahol Alíz és Bob $1/2$ valószínűséggel nyer. Ezt a lapot a CGLMP-egyenlőtlenség [44, 45] határozza meg, melynek együtthatóit a 3.9 táblázat tartalmazza. Lokális korrelációk esetén ennek maximális értéke 2. (Ezt azzal a megfontolással is megkaphatjuk, hogy egy egyenlőségbe szeretnénk vonni azokat a csúcsokat, amik két, illetve három ponton „találnak bele” nemnulla együtthatókba. Ehhez a három találatos csúcsok negyedik sarkához be kell írni egy -1-es együtthatót, ami a hármat rögtön kétféle csökkenti, és szerencsére a kéttalálatos csúcsokat nem rontja el. Ez a heurisztikus megoldás csak három

kimenet esetén működik, több dimenzióban a CGLMP-egyenlőség bonyolultabb.) Ezek az

$x \downarrow y \rightarrow$		0			1		
		0	1	2	0	1	2
0	0	0	-1	1	1	-1	0
	1	1	0	-1	0	1	-1
	2	-1	1	0	-1	0	1
1	0	1	-1	0	0	-1	1
	1	0	1	-1	1	0	-1
	2	-1	0	1	-1	1	0

3.9. táblázat. A CGLMP egyenlőtlenség együtthatói három kimenet esetén.

együtthatók már nem feleltethetők meg egy nemjelző csúcshoz, de ezeket is vehetjük egy módosított Titkárnyó játék kifizetéseinek, ahol egyes hibákat szigorúbban büntetnek, mint másikat.

Miután a módosított Titkárnyó játék egy Bell-egyenlőtlenségnek felel meg, nyilvánvaló, hogy kvantumelőnyvel rendelkezik. Az eredeti játék esetén ez már nem magától értetődik, bár mégis így van. Ez ugyanis a CGLMP cikkben [44] szereplő I korreláció, és ugyanebben a cikkben kimutatják, hogy ezt is meg lehet sérteni kvantummechanikával.

3.2.5. Egy kivétel: a Vértesi-Bene játék

Természetesen felvetődik a kérdés, hogy van-e példa olyan nemlokális előnyvel rendelkező Bayes-i játékra, ami nem követi a konstrukciónkat. Ennek megválaszolásához vizsgáljuk meg a Vértesi és Bene ([55]) által vizsgált Bell-féle szituációt, amit arra használtak, hogy bemutassák a POVM mérések lehetséges nemtriviális szerepét Bell-egyenlőtlenségeknél. A példa különlegessége, hogy Alíznek három típusa (vagy mérése) lehet, és csak a harmadik esetben három akciója (vagy mérési eredménye). Az első két esetben az akciók száma kettő. Bobnak két típusa és két akciója van.

A kifizetés a 3.10. táblázatban látható, $c > 0$ egy paraméter. Ennek a lokális optimuma 1, amit a 3.11. táblázatban megadott lokális csúcson vesz fel, függetlenül c értékétől. Vegyük

$x \downarrow y \rightarrow$		0		1	
		0	1	0	1
0	0	0	$-c/2$	$c/2$	$-c/2$
	1	$-c/2$	0	0	0
1	0	$c/2$	0	$-c$	0
	1	$-c/2$	0	0	0
2	0	$1/2$	$-1/2$	$1/2$	$-1/2$
	1	$\frac{\sqrt{2}+2}{4}$	$\frac{\sqrt{2}-2}{4}$	$\frac{\sqrt{2}-6}{4}$	$\frac{\sqrt{2}-2}{4}$
	2	0	0	0	0

3.10. táblázat. A Vértesi-Bene játék kifizetései. $c > 0$ egy paraméter.

észre, hogy a félkövérrel szedett blokkok nem korrelált egyensúlyai a megfelelő játéknak, vagyis a várható kifizetést maximalizáló lokális csúcs nem ex-post egyensúly.

$x \downarrow y \rightarrow$		0		1	
		0	1	0	1
0	0	1	0	1	0
	1	0	0	0	0
1	0	1	0	1	0
	1	0	0	0	0
2	0	1	0	1	0
	1	0	0	0	0
	2	0	0	0	0

3.11. táblázat. Egy optimális lokális viselkedés a 3.10. táblázatban látható játékhoz. A félkövérrel szedett blokkok nem korrelált egyensúlyai a megfelelő bimátrix játéknak.

Most hagyjuk el a lokális politópot, és nézzük meg a nemjelző esetet. Ebben az esetben is egy lineáris programozási problémát kell megoldani egy rögzített priorral (nálunk az egyenletes eloszlás). A célfüggvény természetesen a várható kifizetés, az elérhető tartomány pedig \mathcal{P}_{NS} , a (2.19) egyenletek által meghatározott politóp. $c > 1$ esetén az optimumot a 3.12.

táblázatban megadott csúcson veszi fel a célfüggvény. Vegyük észre, hogy az egyik blokkban (Alíz harmadik és Bob első típusához tartozóban) a valószínűségeloszlás nem korrelált egyensúlya a játéknak. *Vagyis az ex-ante és az ex-post egyensúlyok különböznek.*

Más hasonló játékok esetén (pl. a CHSH játék) egy optimális nemjelző dobozhoz való hozzáférés elég ahhoz, hogy elérjük azt az egyensúlyt, amit már azzal sem lehetne javítani, ha a szereplők megismernék egymás típusát (nyílt kártyákkal játszanának). Ezzel ellentétben a Vértesi-Bene féle játékban, bár egy nemlokális erőforrás növeli a játékosok nyeresi esélyeit, de még nagyobb lenne a várható kifizetésük, ha valamilyen kommunikációs csatornán információt szereznének egymás típusáról. Ez az effektus a korábban vizsgált kétszereplős nemlokális játékoknál nincs jelen.

$x \downarrow y \rightarrow$		0		1	
		$a \downarrow$	$b \rightarrow$	$a \downarrow$	$b \rightarrow$
0	0	1/2	0	1/2	0
	1	0	1/2	0	1/2
1	0	1/2	0	0	1/2
	1	0	1/2	1/2	0
2	0	1/2	0	1/2	0
	1	0	0	0	0
	2	0	1/2	0	1/2

3.12. táblázat. Az optimális nemjelző viselkedés a 3.10. táblázatban látható játékhoz $c > 1$ esetén. A félkövérrel szedett blokk nem korrelált egyensúlya a megfelelő bimátrix játéknak.

Mi történik, ha a játékosok egy kvantumdobozt használhatnak? Vértesiék cikke [55] tartalmaz egy példát egy olyan kvantum viselkedésre, ami meghaladja a lokális maximumot, bár nincs bizonyítva, hogy ez optimális lenne a kvantumkorrelációk között. Ez a 3.13. táblázatban látható. Alíz első két típusa esetén a CHSH szituáció ismétlődik, míg a harmadik típusnál numerikusan kiértékeljük az [55] cikkben megadott konstrukciót. Érdekes módon most Alíz harmadik típusához tartozó egyik blokk sem korrelált egyensúly (félkövérrel szedve), vagyis ez a viselkedés nem *ex-post* egyensúly, de egyszerű számítással meg lehet

$x \downarrow y \rightarrow$		0		1	
		0	1	0	1
0	0	$\frac{2+\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$
	1	$\frac{2-\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$
1	0	$\frac{2+\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$
	1	$\frac{2-\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$	$\frac{2+\sqrt{2}}{8}$	$\frac{2-\sqrt{2}}{8}$
2	0	0.30602	0.12925	0.41652	0.01875
	1	0.18243	0.11444	0.00395	0.29293
	2	0.01155	0.25630	0.07953	0.18832

3.13. táblázat. [55]-ben ismertetett, a lokális optimumhoz képest előnnyel rendelkező kvantumviselkedés. Az értékeket a cikkbeli eredmények numerikus kiértékelésével kaptuk. A félkövérrel szedett blokkok nem korrelált egyensúlyai a 3.10. táblázatban szereplő játék megfelelő bimátrix blokkjainak.

győződni róla, hogy *ex-ante* egyensúly.

4. fejezet

Összefoglalás és kitekintés

A dolgozatban bemutatott eredmények két fő csoportba oszthatók: az egyrészt kvantumrendszerekkel kapcsolatban az állapotmegkülönböztetés egy alternatív tárgyalását adtuk, míg a kétrészt rendszerek esetében a nemlokális korrelációk és a játékelmélet kapcsolatával foglalkoztunk.

Az első részben a ROC görbe kvantumállapotokra való alkalmazhatóságát vizsgáltuk. Megmutattuk, hogyan lehet összefüggésbe hozni néhány távolság mérőszámmal, és bevezettünk egy új a fidelityhez hasonló hasonlósági mértéket, a kvantum-Bhattacharyya-együtthetőt. A legjelentősebb nyitott kérdés ezzel kapcsolatban a sejtésünk, miszerint két sűrűségmátrix akkor és csak akkor kommutál, ha a fidelity és a kvantum-Bhattacharyya-együtthető egyenlők.

A kvantumállapot-megkülönböztetésről szóló cikkünk [56] megjelenése után eredményeinket Catherine Medlock, Alan Oppenheim, Isaac Chuang és Qi Ding (valamennyien a Massachusetts Institute of Technology munkatársai) általánosították [4, 57].

A szerzők részben a jelfeldolgozás, részben a kvantummechanika területéről érkeztek, de inkább az előbbi területnek címezték a munkájukat, ezért elég részletesen mutatják be a kvantummechanikai háttérrel. A gyakorlati életben gyakran előforduló azon helyzettel foglalkoznak főként, amikor a diszkrimináció két élesen elkülöníthető fázisra bontható, egy fizikai mérés/adatgyűjtés részre, és egy az adatok alapján tisztán informatikailag meghozott döntési részre. Az első rész eredménye gyakran egyetlen valós szám (score variable). A döntés ezután lehet például egy küszöbérték szerinti döntés (scorevariable threshold test –

SVT) vagy egy likelihood alapú (likelihoodratio test – LRT), ez utóbbi optimális, ha az első fázis rögzített.

A kvantum esetben is lehetséges egy olyan forgatókönyv, ahol rögzített a (kettőnél több értékű) mérési operátor, és az utófeldolgozást változtathatjuk. Az így kapott karakterisztikát elnevezik *Quantum decision operating characteristic*-nek (QDOC). A másik lehetőség a mérés változtatása, így kaphatjuk a *Quantum measurement operating characteristic*-et (QMOC). A QDOC esetben ismét megkülönböztethetjük az SVT és LRT döntési eljárásokat, és megmutatják, hogy az SVT karakterisztika bár nem optimális, de megkapható belőle egyéb input nélkül az LRT karakterisztika.

A QMOC a közvetlen általánosítása az általunk vizsgált ROC görbének. A szerzők bebizonyítják, hogy kétdimenziós Hilbert-tér esetén a QMOC egy ellipszis, nagyobb dimenzióban a projektív mérésekhez tartozó diszjunkt görbedarabok, amiket utófeldolgozással kiegészíthetünk a konvex burkára. Azt is megvizsgálták, hogy adott (nem mindig optimális) mérési szituációkhoz hogyan lehet olyan ekvivalens POVM-et találni, ami Parseval-frame-ek segítségével 1-rangú operátorokat használ.

A dolgozat második részében a kétrészes nemlokális korrelációk és a Bayes-i játékok elméletének összefüggéseivel foglalkoztunk. Részletesebben elemeztük a 2-2-3-3 politóp szerkezetét, egy szisztematikus eljárást adtunk nemlokális előnnyel rendelkező játékok előállítására, amivel az irodalomban talált (általában magasfokú szimmetriával rendelkező) esetek többségét le tudtuk fedni. De egy kivételt is találtunk, Vértesi és Bene korrelációját, amit a szerzők nem kvantumelőnyös játék céljából vizsgáltak, hanem hogy bemutassák, rögzített Hilbert-tér dimenzió esetén általános POVM-ek előnnyel rendelkezhetnek a projektív mérésekkel szemben a Bell-egyenlőtlenségek sértése szempontjából.

A dolgozat második részének alapjául szolgáló cikk a disszertáció elkészítése előtt nem sokkal jelent meg, ezért a hatásáról még kevesebb az információ. Az általunk adott konstrukció lehetővé teszi a nemklasszikus korrelációk újabb alkalmazásainak szisztematikus keresését. A Vértesi-Bene játék általunk bemutatott tulajdonsága arra utal, hogy a nem szimmetrikus akcióhalmazokkal rendelkező Bayes-i játékok további kutatásokat igénylő strukturális tulajdonságokkal rendelkeznek.

5. fejezet

Tézisek

1. Bevezettem a kvantum ROC görbe fogalmát. Ez a klasszikus ROC görbe általánosítása, amely részletes képet ad két kvantumállapot megkülönböztethetőségéről. (IV. publikáció)
2. Definiáltam a *kvantum-Bhattacharyya-együtthatót*, amely a fidelity-hez hasonlóan egy hasonlósági mérték. Bebizonyítottam, hogy ez a mennyiség teljesen pozitív leképezésekre monoton nő. (IV. publikáció)
3. Konstruktív eljárást adtam nemlokális előnnyel rendelkező Bayes-i játékok előállítására. Az eljárás az irodalomban előforduló legtöbb játék esetét lefedi. (I., II., III. publikációk)
4. A 2-2-3-3 nemjelző politóp elemzésével bevezettem egy új nemlokális előnnyel rendelkező Bayes-i játékot (EKMNNTKONKCT vagy Titkárno játék). (I., II., III. publikációk)
5. Megmutattam, hogy a Vértesi-Bene Bell-egyenlőtlenség alapján definiált játék *ex-ante* és *ex-post* egyensúlyai különböznek. A többi, az irodalomból ismert játék esetén ezek az egyensúlyok egybeesnek. (I., II., III. publikációk)

6. fejezet

Summary

The results presented in this thesis can be divided into two groups. Concerning the single component quantum systems we have presented an alternative view of state discrimination, while for bipartite quantum states we have considered the connection between nonlocal correlations and game theory.

In the first part we have investigated the applicability of ROC analysis to quantum state discrimination. We have shown the correspondence between the ROC curve and a few distance measures, and have introduced a new similarity measure similar to the fidelity: the quantum Bhattacharyya coefficient. The most important open question in this part is our conjecture that two density matrices commute if and only if their fidelity and quantum Bhattacharyya coefficient are equal.

Since the publication of our article about quantum state discrimination our results were generalized by Catherine Medlock, Alan Oppenheim, Isaac Chuang and Qi Ding (affiliated at the Massachusetts Institute of Technology) [4, 57]. The authors' background is partly in signal processing, partly in quantum mechanics; their work in argument adopts dominantly the to the former perspective (and therefore they present the quantum mechanical background in detail). They investigate the case — often occurring in practice — when the process of quantum state discrimination can be divided into two clearly distinguishable parts, the first is the physical measurement/data collection phase, the second is the decision making based on the data. The result of the first phase is often a single real value (score variable). The decision then may depend on a single threshold value (scorevariable threshold test –

SVT) or a likelihood based one (likelihood ratio test – LRT), the latter is optimal if the first phase is fixed.

In the quantum case it is also possible to address the scenario when a measurement operator with more than two outcomes is fixed and the means of postprocessing can vary. In the cited work resulting characteristics are termed as *Quantum decision operating characteristic* (QDOC). The other possibility is to let the measurement operator vary; then the *Quantum measurement operating characteristic* (QMOC) is obtained. In the QDOC case one can again distinguish between the SVT and LRT decision procedures; the authors show that although the SVT characteristic is not optimal, one can obtain without any further input the LRT characteristic from it.

The QMOC is the direct generalization of our optimal ROC curve. The authors prove that in case of a two-dimensional Hilbert space the QMOC is an ellipse, in higher dimensions disjoint pieces of curves that can be extended to their convex hull by postprocessing.

In the second part of the dissertation we have investigated the correspondence between two-party nonlocal correlations and Bayesian games. We have analysed in detail the structure of the 2-2-3-3 polytope. A systematic method for generating games with nonlocal advantage has been introduced that covers most of the cases found in the literature. Meanwhile, an exception is also found: the correlation discovered originally by Vértesi and Bene. The authors did not investigate this correlation from the game theoretic point of view, their intention was to demonstrate that if the dimension of the Hilbert space is bounded, general POVM-s may have advantage over projective measurement with respect to violating Bell's inequalities.

As the results of the second part were only published recently, we cannot assess yet their scientific impact. Nevertheless, our construction introduces a new possibility of systematically searching for new applications of nonclassical correlations. The property of the Vértesi-Bene game demonstrated by us suggests, that games with nonsymmetric action sets have structural properties that need further investigation.

7. fejezet

Köszönetnyilvánítás

Szeretnék köszönetet mondani az ELTE Komplex Rendszerek Fizikája Tanszék munkatársainak, különösen Csabai Istvánnak, A PTE Matematikai és Informatikai Intézetének munkatársainak, különösen Pinczehelyi Eszternek, a Wigner Fizikai Kutatóközpont Kvantuminformatika csoport munkatársainak, különösen Kiss Tamásnak, a BME Differenciálegyenletek Tanszékének, különösen Pintér Miklósnak a támogatásukért.

Köszönöm a segítséget, illetve a jó társaságot a következőknek: Ádám Péter, Berkics Péter, Cserti József, Csordás András, Dávid Gyula, Dombóvári József, Domokos Péter, Eisner Tímea, Gimesi László, Gnädig Péter, Horváth Zoltán, Jenák Ildikó, Jenei Sándor, Kálmán Orsolya, Kallus Zsófia, Kilián Imre, Király Balázs, Kiss-Vincze Tamás, Koncz Gabriella, Kondor Dániel, Kumar Preetam, Laczkó József, Li Shuang, Nagy-Csiha Zsuzsanna, Pap Margit, Papp Ágnes, Peyer Zoltán, Rajkó Róbert, Rébay Viktor, Reibling Tamás, Simon Ilona, Solymosi Norbert, Spisák Sándor, Stéger József, Szabó Sándor, Tolnai Balázs, Varga Ibolya, Vattay Gábor, Vella Péter, Völgyiné Mirbach Rita, Zaválnij Bogdán, Zheng Tonglin.

Köszönöm (a jó társaságon túl) Zentai Norbertnek a kézirat nyelvi lektorálását, Frigyük Andrásnak és Zimborás Zoltánnak a házivédésen az előbírálatot.

Szeretnék köszönetet mondani témavezetőmnek, Koniorczyk Mátyásnak, a tudományos együttműködésünk mellett a magánéleti támogatásáért (melyből családja, Alíz¹, Lilla és Emese is kivette részét), és hogy végül kipróbálta belőlem ezt a dolgozatot.

Végezetül köszönöm Diósi Lajosnak és Geszti Tamásnak a több évtizedes közös munkát,

¹Egy játékelméleti írásban illendő külön köszönetet mondani *Alíz*nak.

támogatásukat és a bölcs tanácsokat. (Mellesleg mindketten írtak egy-egy remek kvantummechanika tankönyvet is [16],[58].)

8. fejezet

A disszertációhoz kapcsolódó publikációk

- I. Koniorczyk Mátyás, Bodor András and Pintér Miklós Péter. Ex ante versus ex post equilibria in classical Bayesian games with a nonlocal resource. *PHYSICAL REVIEW A*, **101**(2020). ISSN 1050-2947. doi:10.1103/PhysRevA.101.062115.
- II. Koniorczyk Mátyás, Bodor András and Pintér Miklós Péter. Nemklasszikus korrelációk Bayes-i játékokban. In *XXXIII. MAGYAR OPERÁCIÓKUTATÁSI KONFERENCIA: Program és előadáskivonatok*. 2019.
- III. Koniorczyk Mátyás and Bodor András. No-Signaling in Quantum Mechanics. *JOURNAL OF RUSSIAN LASER RESEARCH*, **39**(2018):376–381. ISSN 1071-2836. doi:10.1007/s10946-018-9731-3.
- IV. Bodor András and Koniorczyk Mátyás. Receiver Operation Characteristics of Quantum State Discrimination. *JOURNAL OF RUSSIAN LASER RESEARCH*, **38**(2017):150–163. ISSN 1071-2836. doi:10.1007/s10946-017-9629-5:.

9. fejezet

Irodalomjegyzék

- [1] Wikipedia. Receiver operating characteristic — Wikipedia, The Free Encyclopedia, 2004. [Online; letöltve 2020.11.26.], URL https://en.wikipedia.org/wiki/Receiver_operating_characteristic.
- [2] Fawcett, Tom. Introduction to ROC Analysis. *Pattern Recogn. Lett.*, **27**(2006):861–874. ISSN 0167-8655.
- [3] Cover, Thomas M. and Thomas, Joy A. *Elements of Information Theory*. Wiley, 2005 April. doi:10.1002/047174882x. URL <https://doi.org/10.1002/047174882x>.
- [4] Medlock, Catherine and Oppenheim, Alan. Optimal ROC Curves from Score Variable Threshold Tests. In *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pages 5327–5330. 2019. doi:10.1109/ICASSP.2019.8683187.
- [5] Bergou, János A., Herzog, Ulrike and Hillery, Mark. 11 Discrimination of Quantum States. In *Quantum State Estimation*, pages 417–465. Springer Berlin Heidelberg, 2004 August. doi:10.1007/978-3-540-44481-7_11. URL https://doi.org/10.1007/978-3-540-44481-7_11.
- [6] Bae, Joonwoo and Kwek, Leong-Chuan. Quantum State Discrimination and its Applications. *Journal of Physics A: Mathematical and Theore-*

tical, **48**(2015)(8):083001. doi:10.1088/1751-8113/48/8/083001. URL <https://doi.org/10.1088/1751-8113/48/8/083001>.

- [7] Helstrom, Carl Wilhelm. *Quantum Detection and Estimation Theory*. Math. Sci. Eng. Academic Press, New York, NY, 1976. URL <https://cds.cern.ch/record/110988>.
- [8] Ziegler, G.M. *Lectures on Polytopes*, volume 152 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 1995.
- [9] Grünbaum, Branko. *Convex Polytopes*. 2003 Oct. ISBN 9780387404097.
- [10] Clauser, John F, Horne, Michael A., Shimony, Abner and Holt, Richard A. Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.*, **23**(1969):880–884. doi:10.1103/PhysRevLett.23.880. URL <https://link.aps.org/doi/10.1103/PhysRevLett.23.880>.
- [11] Tsirelson, B. S. Some Results and Problems on Quantum Bell-type Inequalities. *Hadronic J. Suppl.*, **8**(1993)(4):329–345.
- [12] Navascués, Miguel, Pironio, Stefano and Acín, Antonio. Bounding the Set of Quantum Correlations. *Phys. Rev. Lett.*, **98**(2007):010401. doi:10.1103/PhysRevLett.98.010401. URL <http://link.aps.org/doi/10.1103/PhysRevLett.98.010401>.
- [13] Pawłowski, Marcin, Paterek, Tomasz, Kaszlikowski, Dagomir, Scarani, Valerio, Winter, Andreas and Żukowski, Marek. Information Causality as a Physical Principle. *Nature*, **461**(2009)(7267):1101–1104. doi:10.1038/nature08400. URL <https://doi.org/10.1038/nature08400>.
- [14] Einstein, A., Podolsky, B. and Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.*, **47**(1935):777–780. doi:10.1103/PhysRev.47.777. URL <https://link.aps.org/doi/10.1103/PhysRev.47.777>.
- [15] Fine, Arthur. Hidden Variables, Joint Probability, and the Bell Inequalities. *Phys. Rev. Lett.*, **48**(1982):291–295. doi:10.1103/PhysRevLett.48.291. URL <https://link.aps.org/doi/10.1103/PhysRevLett.48.291>.

- [16] Diósi, Lajos. *A Short Course in Quantum Information Theory*. Springer Berlin Heidelberg, 2011. doi:10.1007/978-3-642-16117-9. URL <https://doi.org/10.1007/978-3-642-16117-9>.
- [17] I. Gelfand, M. Neumark. On the Imbedding of Normed Rings into the Ring of Operators in Hilbert Space. *Rec. Math. [Mat. Sbornik] N.S.*, **12(54)**(1943):197–217.
- [18] Scholz, Volkher B. and Werner, Reinhard F. Tsirelson’s Problem, 2008. arXiv:0812.4305.
- [19] Bell, John Stewart. On the Einstein Podolsky Rosen Paradox. *Physics*, **1**(1964)(3):195–200. doi:10.1103/physicsphysiquefizika.1.195. URL <https://doi.org/10.1103/physicsphysiquefizika.1.195>.
- [20] Cirel’son, B. S. Quantum Generalizations of Bell’s Inequality. *Lett. Math. Phys.*, **4**(1980)(2):93–100. doi:10.1007/bf00417500. URL <https://doi.org/10.1007/bf00417500>.
- [21] Bamps, Cédric and Pironio, Stefano. Sum-of-squares Decompositions for a Family of Clauser-Horne-Shimony-Holt-like Inequalities and their Application to Self-testing. *Phys. Rev. A*, **91**(2015):052111. doi:10.1103/PhysRevA.91.052111. URL <https://link.aps.org/doi/10.1103/PhysRevA.91.052111>.
- [22] Šupić, Ivan and Bowles, Joseph. Self-testing of Quantum Systems: a Review. *Quantum*, **4**(2020):337. ISSN 2521-327X. doi:10.22331/q-2020-09-30-337. URL <https://doi.org/10.22331/q-2020-09-30-337>.
- [23] Navascués, Miguel, Pironio, Stefano and Acín, Antonio. A Convergent Hierarchy of Semidefinite Programs Characterizing the Set of Quantum Correlations. *New J. Phys.*, **10**(2008)(7):073013. URL <http://stacks.iop.org/1367-2630/10/i=7/a=073013>.
- [24] Tsirelson, Boris. Bell inequalities and operator algebras, ismeretlen dátum. [Online; letöltve 2021.04.22.], URL <http://www.math.tau.ac.il/~tsirel/download/bellopalg.pdf>.

- [25] Junge, M., Navascues, M., Palazuelos, C., Perez-Garcia, D., Scholz, V. B. and Werner, R. F. Connes' Embedding Problem and Tsirelson's Problem. *Journal of Mathematical Physics*, **52**(2011)(1):012102. doi:10.1063/1.3514538. URL <https://doi.org/10.1063/1.3514538>.
- [26] Connes, Alain. Classification of Injective Factors Cases II_1 , II_∞ , III_λ , $\lambda \neq 1$. *The Annals of Mathematics*, **104**(1976)(1):73. doi:10.2307/1971057. URL <https://doi.org/10.2307/1971057>.
- [27] Ji, Zhengfeng, Natarajan, Anand, Vidick, Thomas, Wright, John and Yuen, Henry. $MIP^*=RE$, 2020. arXiv:2001.04383.
- [28] von Neumann, John and Morgenstern, Oskar. *Theory of Games and Economic Behavior*. Princeton University Press, Princeton, 1953.
- [29] Nash, John. Equilibrium points in n-person games. *Proceedings of the National Academy of Sciences*, **36**(1950)(1):48–49.
- [30] Nash, John. Non-Cooperative Games. *The Annals of Mathematics*, **54**(1951)(2):286–295.
- [31] Aumann, Robert J. Subjectivity and Correlation in Randomized Strategies. *Journal of Mathematical Economics*, **1**(1974)(1):67–96. doi:10.1016/0304-4068(74)90037-8. URL [https://doi.org/10.1016/0304-4068\(74\)90037-8](https://doi.org/10.1016/0304-4068(74)90037-8).
- [32] Aumann, Robert J. Correlated Equilibrium as an Expression of Bayesian Rationality. *Econometrica*, **55**(1987)(1):1–18. ISSN 00129682, 14680262. URL <http://www.jstor.org/stable/1911154>.
- [33] Huang, Haifeng. Introduction to Game Theory Lecture 7: Bayesian Games. <https://sites.duke.edu/niou/files/2011/05/Lecture-7-Bayesian-Games1.pdf>. [Online; letöltve: 2021.01.14.].
- [34] Wikipedia. Dependent type — Wikipedia, The Free Encyclopedia, 2004. [Online; letöltve 2021.04.07.], URL https://en.wikipedia.org/wiki/Dependent_type.

- [35] Chlipala, Adam. An Introduction to Programming and Proving with Dependent Types in Coq. *Journal of Formalized Reasoning*; Vol 3, (2010):No 2 (2010): Special Issue: User Tutorials I; 1–93. doi:10.6092/ISSN.1972-5787/1978. URL <http://jfr.unibo.it/article/view/1978>.
- [36] Brunner, Nicolas and Linden, Noah. Connection between Bell Nonlocality and Bayesian Game Theory. *Nature Commun.*, 4(2013)(July):2057. ISSN 20411723. doi:10.1038/ncomms3057.
- [37] Ternovszky Béla, Nepp József et al. Macskafogó, 1986. 0:49:10, URL <https://www.imdb.com/title/tt0179955>.
- [38] Munroe, Randall. Blue Eyes: The Hardest Logic Puzzle in the World, ismeretlen dátum. [Online; letöltve 2021.04.07.], URL https://xkcd.com/blue_eyes.html.
- [39] Michael Lembeck et al. Friends — The One Where Everybody Finds Out, 1999. [Online; letöltve 2021.04.07., <https://www.youtube.com/watch?v=LUN2YN0bOi8>], URL <https://www.imdb.com/title/tt0583452>.
- [40] Bhattacharyya, A. On a Measure of Divergence between two Statistical Populations Defined by their Probability Distributions. *Bull. Calcutta Math. Soc.*, 35(1943):99–109. ISSN 0008-0659.
- [41] I, Bengtsson and K, Życzkowski. *Geometry of Quantum States*. Cambridge University Press, Cambridge, 2006. ISBN 9780511535048.
- [42] Barnum, Howard, Caves, Carlton M., Fuchs, Christopher A., Jozsa, Richard and Schumacher, Benjamin. Noncommuting Mixed States Cannot Be Broadcast. *Phys. Rev. Lett.*, 76(1996):2818–2821.
- [43] PPL development team. Parma Polyhedra Library. [Online; letöltve: 2020.12.16.], URL <https://www.bugseng.com/parma-polyhedra-library>.
- [44] Collins, Daniel, Gisin, Nicolas, Linden, Noah, Massar, Serge and Popescu, Sandu. Bell Inequalities for Arbitrarily High-Dimensional Systems. *Physical Review Letters*,

- 88**(2002)(4). doi:10.1103/physrevlett.88.040404. URL <https://doi.org/10.1103/physrevlett.88.040404>.
- [45] Masanes, Lluís. Tight Bell inequality for d-outcome measurements correlations. *Quantum Information and Computation*, **3**(2003)(4):345–358. arXiv:quant-ph/0210073.
- [46] Navascués, M., Cooney, T., Pérez-García, D. and Villanueva, N. A Physical Approach to Tsirelson’s Problem. *Foundations of Physics*, **42**(2012)(8):985–995. doi:10.1007/s10701-012-9641-0. URL <https://doi.org/10.1007/s10701-012-9641-0>.
- [47] Rastall, Peter. Locality, Bell’s Theorem, and Quantum Mechanics. *Found. Phys.*, **15**(1985)(9):963–972. doi:10.1007/bf00739036. URL <https://doi.org/10.1007/bf00739036>.
- [48] Khalfin, L.A. and Tsirelson, B.S. Quantum and Quasi-classical Analogs of Bell Inequalities. In Lahti, Pekka and Mittelstaedt, Peter, editors, *Symposium on the Foundations of Modern Physics*, pages 441–460. World. Sci. Publ., 1985.
- [49] Popescu, Sandu and Rohrlich, Daniel. Generic Quantum Nonlocality. *Phys. Lett. A*, **166**(1992)(5-6):293–297. ISSN 03759601. doi:10.1016/0375-9601(92)90711-T.
- [50] Popescu, Sandu and Rohrlich, Daniel. Quantum nonlocality as an axiom. *Found. Phys.*, **24**(1994)(3):379–385. doi:10.1007/bf02058098. URL <https://doi.org/10.1007/bf02058098>.
- [51] Brandenburger, Adam and Mura, Pierfrancesco La. Team Decision Problems with Classical and Quantum Signals. *Phil. Trans. R. Soc. A*, **374**(2016)(2058):20150096. ISSN 1364503X. doi:10.1098/rsta.2015.0096.
- [52] Brukner, Časlav, Paunković, Nikola, Rudolph, Terry and Vedral, Vlatko. Entanglement-assisted orientation in space. *International Journal of Quantum Information*, **04**(2006)(02):365–370. doi:10.1142/s0219749906001839. URL <https://doi.org/10.1142/s0219749906001839>.

- [53] Pappa, Anna, Kumar, Niraj, Lawson, Thomas, Santha, Miklos, Zhang, Shengyu, Diamanti, Eleni and Kerenidis, Iordanis. Nonlocality and Conflicting Interest Games. *Phys. Rev. Lett.*, **114**(2015)(2):020401. ISSN 0031-9007. doi:10.1103/PhysRevLett.114.020401. URL <https://link.aps.org/doi/10.1103/PhysRevLett.114.020401>.
- [54] Bellanger, Anthony. Japon : les femmes assisteront ses messieurs. <https://www.franceinter.fr/emissions/les-histoires-du-monde/les-histoires-du-monde-18-fevrier-2021>. [Online; letöltve: 2021.02.20.].
- [55] Vértesi, T. and Bene, E. Two-qubit Bell Inequality for which Positive Operator-valued Measurements are Relevant. *Phys. Rev. A*, **82**(2010):062115. doi:10.1103/PhysRevA.82.062115. URL <https://link.aps.org/doi/10.1103/PhysRevA.82.062115>.
- [56] Bodor, András and Koniorczyk, Mátyás. Receiver Operation Characteristics of Quantum State Discrimination. *Journal of Russian Laser Research*, **38**(2017)(2):150–163. doi:10.1007/s10946-017-9629-5. URL <https://doi.org/10.1007/s10946-017-9629-5>.
- [57] Medlock, Catherine, Oppenheim, Alan, Chuang, Isaac and Ding, Qi. Operating Characteristics for Binary Hypothesis Testing in Quantum Systems. In *2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1136–1145. 2019. doi:10.1109/ALLERTON.2019.8919700. arXiv:2012.08081.
- [58] Geszti, Tamás. *Kvantummechanika*. Typotex, Budapest, 2007. ISBN 978-963-2793-83-2.