MATEMATICKO-FYZIKÁLNA FAKULTA
UNIVERZITY KOMENSKÉHO
BRATISLAVA

DIPLOMOVÁ PRÁCA

2000 Mário Ziman

MATEMATICKO-FYZIKÁLNA FAKULTA
UNIVERZITY KOMENSKÉHO
BRATISLAVA
Katedra teoretickej fyziky

Kapacita kvantových komunikačných kanálov pri hustom kódovaní

Bratislava, Marec 2000
Diplomant: Mário Ziman
Vedúci diplomovej práce: Prof. RNDr. Vladim´ ir Bužek, DrSc.

Čestne prehlasujem, že som diplomovú prácu vypracoval samostatne.

Aj touto cestou by som chcel vyslovit' pod'akovanie prof. Vladimírovi Bužekovi za povzbudzujúce slová, ktoré mi pomáhali pri písaní vo chvíl'ach najt' ažších a usmerňovali moje myšlienky tým správnym smerom, aby som sa vyvaroval zbytočných chýb.

Obsah

Kapitola 1

ÚVOD

Vznik *teórie informácie* sa datuje od roku 1948, kedy Shannon matematicky zadefinoval pojmy informácie, informačného zdroja a komunikačného kanála, čím položil jej základy. S informáciou môžeme v podstate robit' dve základné operácie, a síce môžeme ju menit' (transformovat'), alebo ju prenášat', či už časom (uchovávat' v pamäti), alebo priestorom (komunikácia). Na základe tohoto môžeme teóriu informácie rozdelit' na oblast', ktorá sa zaoberá počítaním (transformovaním informácie) a oblast' zaoberajúcu sa prenosom. Práve prenosom informácie sa zaoberá aj táto diplomová práca. Jej cieľom je spočítat' kapacity komunikačných kanálov pri stratégii *hustého kódovania*.

Všetky manipulácie s informáciou sa uskutočňujú na zariadeniach, ktoré pracujú na fyzikálnych princípoch. Pôvod tohoto faktu je v tom, že samotná informácia je zakódovaná do fyzikálnych syst 'emov. Je teda prirodzené, že fyzika má aj v tejto oblasti čo povedat'. Aj ked' teória informácie v jej klasickom podaní je natoľko abstraktná, že s týmito princípmi priamo nenarába. V nasledujúcich riadkoch sa pokúsime motivovat' zavedenie pojmu informácie a jeho fyzikálny obsah.

O čom vlastne hovoríme, ked' hovoríme o informácii? Našu otázku, koľko informácie obsahuje nejaký jav, musíme spresnit'. Môžeme sa síce spýtat', že koľko informácie obsahuje napríklad strom, ale odpoved', by sme hľadali asi dlho. Musíme sa pýtat' na kontext, o ktorom má informácia hovorit'. To znamená, že sa pýtame na množstvo informácie v nejakom jave o nejakom inom jave. Daný jav je vždy spojený s nejakým systémom a s nejakým pozorovaním na tomto systéme. Naša otázka na množstvo informácie je potom otázkou, koľko nám jedno pozorovanie hovorí o inom pozorovaní.

Neviem, či Shannon vychádzal z podobnej motivácie, ked' k opisu informácie použil teóriu pravdepodobnosti, ale mám pocit, že tieto úvahy k tomu priamo vedú. Stačí, ak pojem javu stotožníme s pojmom javu, ako sa vyskytuje v teórii pravdepodobnosti, a tým získame pravdepodobnostné rozdelenie na množine všetkých javov, ktoré môžeme stotožnit' s pojmom pozorovanie. To znamená, že sa zaujímame o množstvo informácie, ktorú obsahuje jedna pravdepodobnostná distribúcia (opisujúca pozorovanie) o inej.

Vo fyzike sa skôr ako pojem informácie zaviedol pojem neurčitosti (alebo neznalosti) fyzikálneho systému. Miera tejto neurčitosti sa nazýva *entropiou*. Vyjadruje vlastne informáciu, ktorá nám o systéme chýba, a ktorej dôsledkom je pravdepodobnostný opis takéhoto systému. Pod pravdepodobnostným opisom fyzikálneho systému rozumieme, že vieme určit' pravdepodobnostné rozdelenia výsledkov všetkých meraní. Takouto znalost'ou o systéme vieme všetko, čo podľa predchádzajúceho odstavca potrebujeme k definícii informácie. Bližšie sa tejto definícii venujeme v dodatkoch A a B.

Teóriu informácie môžeme rozdelit' na oblast', ktorá sa zaoberá počítačmi a oblast' zaoberajúcu sa komunikáciou. Práve komunikáciou, presnejšie prenosom informácie, sa zaoberá aj táto diplomová práca. Jej cieľom je spočítat' kapacity komunikačných kanálov pri stratégii hustého kódovania.

Hlavný rozdiel medzi klasickou a kvantovou teóriou je v štruktúre stavov klasických a kvantových systémov. Tento rozdiel sa prenáša aj do teórie informácie, lebo vieme, že vo fyzike stav určuje pravdepodobnostné distribúcie výsledkov všetkých meraní, t.j. objekty s ktorými teória informácie

pracuje. Môžeme povedat', že informácia je ukrytá v stavoch fyzikálneho systému a získavame ju vhodným meraním. Nie je to tak dávno, čo vznikla tzv. *kvantová teória informácie*, v ktorej je informácia práve v stavoch kvantového systému.

Prínos kvantovej teórie v teórii informácie je v zlepšení a zefektívnení niektorých manipulácií s informáciou. Napríklad v oblasti komunikácie ide o bezpečnejší prenos informácie. Kvantová teória ponúka niekoľko možností bezpečnejšieho prenosu informácie ako klasická teória.

Predstavme si, že chceme poslat' nejakú správu (reprezentovanú ret'azcom bitov) z miesta odosielateľa A na miesto príjemcu B a nechceme, aby niekto mohol túto správu (okrem príjemcu) prečítat'. Najlepšie kódovanie je pomocou kľúča, ktorý je rovnako dlhý ako posielaná správa. Posielanú správu s týmto kľúčom bitovo sčítame a posielame takto zakódovanú správu. Príjimateľ, ktorý samozrejme vlastní kľúč, sčíta prijatú správu s týmto kľúčom a získa tak pôvodnú správu. Problémom je bezpečné rozposlanie kľúča z miesta A na miesto B. Kvantová teória ponúka možnost' využitia existencie entanglovaných stavov k tzv. *EPR distribúcii kľúča*.

Odosielateľ a príjemca obdržia dvojhladinové častice (napr. fotóny), ktoré sú v úplne entanglovanom stave. Potom nech obidvaja robia na nich merania polarizácií do dvoch rôznych smerov. Výsledkom takýchto meraní je hodnota polarizácie, t.j. ± 1. Častice sú v stave, že merania na A a B sú v prípade, ak obaja merajú v tom istom smere, úplne korelované. Potom si nejakým verejným komunikačným spojením (napr. telefónom) vymenia informáciu o smeroch, do ktorých merania postupne volili. Poznamenajme, že si nevymenia výsledky svojich meraní. Ak zvolili obaja rovnaký smer, tak ich výsledky sú rovnaké. Ak nie, tak tieto výsledky zahadzujú. Zostávajúce výsledky tvoria postupnost' núl (výsledok -1) a jednotiek (1), t.j. tvoria prenesený kľúč.

Ako uvidíme v práci, využitie úplne entanglovaných stavov vedie k možnosti, ako jedným EPR párom preniest' metódou hustého kódovania dva bity klasickej informácie. V istom zmysle inverzným procesom je tzv. *kvantová teleportácia* opísaná v dodatku D. Pri tejto procedúre sa dá klasickým prenosom dvoch bitov informácie preniest' stav jedného qubitu z miesta odosielateľa na miesto prijímateľa. Treba poznamenat', že všetky tieto spomínané procedúry boli už aj prakticky realizované a k ich zavedeniu do praxe nemusí byt' až tak d'aleko.

Pri všetkých týchto procedúrach sa využíva *kvantové entanglovanie*. Systémy v entanglovanom stave sú kvantovo korelované a obsahujú informáciu, ktorá nemá klasický analóg. Práve táto informácia spôsobuje úspechy kvantového prenosu informácie pred klasickým prenosom. V súčasnosti je snaha zaviest' mieru, ktorá by číselne vyjadrovala množstvo entanglovania pre daný stav. Tejto problematike sa venujeme aj v tejto práci, ktorá práve končí takým pokusom o zavedenie miery entanglovania.

Štúdium tejto oblasti okrem iného je aj snahou lepšie pochopiť kvantovú teóriu. Priamo sa dotýka interpretácie kvantovej teórie, problému merania a ďalších fundamentálnych otázok.

Diplomová práca je rozdelená do šiestich kapitol a piatich dodatkov. Druhá až štvrtá kapitola sú úvodom do problematiky a 5. a 6.kapitola sa týkajú konkrétne kapacít komunikačných kanálov.

Kapitola 2

TEÓRIA PRENOSU INFORMÁCIE

2.1 ZÁKLADNÉ POJMY

V tejto kapitole sa budeme zaoberat' prenosom informácie zo zdroja informácie k nejakému fiktívnemu príjemcovi, ktorý môže s touto informáciou d'alej pracovat'. Informácia bude daná *správou*, ktorú tvorí postupnost' l'ubovol'ných znakov z nejakej fixnej množiny, v ktorých je informácia obsiahnutá. Znak budeme nazývat' *písmenom* a množinu písmen *abecedou*. Správa bude teda usporiadanou množinou písmen z abecedy. Pri prenose správy prichádza k jej skresleniu, lebo fyzikálne je každé prenášané písmeno správy stotožnené so stavom systému, ktorý je počas prenosu v interakcii s prostredím. Vplyvy prostredia nazývame spoločným názvom *šum*. Tento šum práve charakterizuje prenosové zariadenie, ktoré nazývame *komunikačným kanálom*. Z dôvodu existencie šumu je prirodzenou snahou prenášat' iba podstatnú informáciu, t.j. informáciu potrebnú pre vlastné rozhodovanie prijímatel'a. Napríklad namiesto správy $\mathbf{x}=(x_1,\ldots,x_N)$ nám stači poslat' hodnotu nejakej funkcie $T(\mathbf{x})$ na množine správ, pretože táto je podstatná pre prijímatel'a, aj ked' je nepochybne v celej správe informácie viac.

Celá situácia prenosu informácie sa dá opísat' nasledovne : Zo zdroja informácie získame správu v abecede $\mathbf{X}$ zdroja. Ked'že všeobecne nemusí platit' , že abeceda zdroja je zhodná so vstupnou abecedou komunikačného kanála $\mathbf{A}$, a teda musíme prepísat' správu z jednej abecedy do druhej. Tento prepis voláme *kódovanie*[1]. Podobná situácia nastáva aj na konci komunikačného kanála, kde musíme prepísat' výstupnú správu z výstupnej abecedy $\mathbf{B}$ do abecedy prijímatel'a $\mathbf{Y}$, čo nazývame *dekódovaním*.

Teraz matematicky popíšeme komunikačný kanál.

Definícia: Komunikačný kanál $\mathbf{K}$ definujeme, pre M=1,2,..., ako postupnost' trojíc $(\mathbf{A}^M, \mathbf{p}^M(.|.), \mathbf{B}^M)$, kde $\mathbf{A}$ je vstupná abeceda a $\mathbf{B}$ je vystupná abeceda komunikačného kanála. $\{\ p^M(.|\mathbf{a}) : \mathbf{a} \in \mathbf{A}^M\}$ je rodina pravdepodobnostných hustôt na množine $\mathbf{B}^M$ výstupných správ, pričom sa o nich predpokladá konzistentnost' v nasledovnom zmysle

$$p^M(b_1,\ldots,b_M|a_1,\ldots,a_M) = \sum_{b_{M+1}\in\mathbf{B}} p^{M+1}(b_1,\ldots,b_{M+1}|a_1,\ldots,a_{M+1})$$

pre všetky $\mathbf{a} \in \mathbf{A}^{M+1}$, $\mathbf{b} \in \mathbf{B}^M$.

V našej definícii predpokladáme, že počet písmen M v správe sa pri prenose nemení. Komunikačný kanál opisuje v jazyku teórie pravdepodobnosti (Dodatok A), ako sa vstupná správa $\mathbf{a}$ transformuje na výstupnú správu $\mathbf{b}$. Táto transformácia je deterministická iba v prípade, ak $p^M(\mathbf{b}|\mathbf{a}) = 1$ pre niektorú $\mathbf{b} = \mathbf{b}(\mathbf{a}) \in \mathbf{B}^M$. Všeobecne ide o stochastickú transformáciu opísanú hustotou pravdepodobnosti

[1] To znamená, že kódujeme nielen, ked' chceme správu utajit'.

$p^M(.|\mathbf{a})$ na $\mathbf{B}^M$. Samotné $p^M(\mathbf{b}|\mathbf{a})$ určuje pravdepodobnosť, že pri výstupnej správe $\mathbf{b}$ bola na vstupe správa $\mathbf{a}$.

Podmienka konzistencie spája hustoty pravdepodobností, ktoré definujú komunikačný kanál, pri prenosoch správ rôznych dĺžok. Ak by bola pravdepodobnosť naľavo väčšia, tak pri poslaním správy o jedno písmeno dlhšej by bola istá pravdepodobnosť, že na konci prenosu bude jedno písmeno chýbať. Naopak si predstavme, že sa nezaujímame o posledné písmeno správy. Pri opačnej nerovnosti by sme potom s väčšou pravdepodobnosťou určili o písmeno kratšiu správu, ako pri prenose iba tejto samotnej (kratšej) správy. Je rozumné takéto prenosy nepovažovať za prenosy cez komunikačný kanál.

Komunikačný kanál nazývame *bezpamäťový*, akk na výstupnej abecede $\mathbf{B}$ existuje rodina hustôt pravdepodobností $\{p(.|a) : a \in \mathbf{A}\}$, pre ktorú

$$p^M(\mathbf{b}|\mathbf{a}) = \prod_{i=1}^{M} p(b_i|a_i) \quad M = 1, 2, \ldots$$

Uvedená podmienka konzistencie je potom splnená a každý bezpamäťový kanál je určený trojicou ($\mathbf{A}$,p(.|.),$\mathbf{B}$). Bezpamäťovosť komunikačného kanála je v tom, že poslanie písmena neovplyvňuje jeho pôsobenie na neskoršie poslané písmená, t.j. nepamätá si, čo už preniesol. Alebo v reči pravdepodobnosti posielania písmen cez komunikačný kanál sú nezávislé javy a teda spoločná pravdepodobnosť javu (celej správy) sa rovná súčinu jednotlivých javov (písmen), čo je štatistickým vyjadrením nezávislosti. Takýto komunikačný kanál môžeme opísať maticou p(j|i), kde j=1,...,m a i=1,...,n, kde n je počet písmen v abecede $\mathbf{A}$ a m je počet písmen v abecede $\mathbf{B}$.

Ak na vstup príde správa $\mathbf{a}$, tak výstupná správa je náhodný vektor s výberovým priestorom $(\mathbf{B}^M, p^M(.|\mathbf{a}))$. Akákoľvek hustota π^M na množine vstupných správ $\mathbf{A}^M$ definuje náhodnú vstupnú správu s výberovým priestorom $(\mathbf{A}^M, p^M_\alpha(\mathbf{a}) = \pi^{\mathbf{M}}(\mathbf{a}))$. Na výstupe komunikačného kanála pozorujeme náhodné správy $\mathbf{b} \in \mathbf{B}^M$ s pravdepodobnosťou $p^M_\beta(\mathbf{b}) = \sum_{\mathbf{a}\in\mathbf{A}^M} p^M(\mathbf{b}|\mathbf{a})\pi^M(\mathbf{a})$. Pravdepodobnosť, že na vstupe je správa $\mathbf{a}$ a na výstupe je správa $\mathbf{b}$ je $p^M_{\alpha\beta}(\mathbf{a},\mathbf{b}) = p^M(\mathbf{b}|\mathbf{a})\pi^M(\mathbf{a})$. Teraz sa môžeme sa zaujímať o Shannonovu informáciu (B.8) o správach $\alpha \in \mathbf{A}^M$, ak na výstupe pozorujem správy $\beta \in \mathbf{B}^M$. Dosadením príslušných pravdepodobnostných distribúcií do (B.8) dostaneme pre Shannonovu informáciu

$$I(\alpha,\beta) = \sum_{\mathbf{a}\in\mathbf{A}^M} \sum_{\mathbf{b}\in\mathbf{B}^M} p^M(\mathbf{b}|\mathbf{a})\pi^M(\mathbf{a}) \log \frac{p^M(\mathbf{b}|\mathbf{a})}{p^M_\beta(\mathbf{b})}. \tag{2.1}$$

Treba poznamenať, že ide o globálnu mieru informácie, t.j. nič nám nehovorí o tom koľko informácie máme o konkrétnej vstupnej správe $\mathbf{a}$, ak na výstupe máme konkrétnu správu $\mathbf{b}$. Informácia je pre fixnú dĺžku správy M jednoznačne určená komunikačným kanálom (t.j. $p^M(\mathbf{b}|\mathbf{a})$) a vstupnou hustotou π^M.

Kódovanie sa uskutočňuje pomocou zariadenia, ktoré nazývame *kóder* a dekódujeme pomocou *dekodéra*. Kóder, prislúchajúci zdroju informácie s abecedou $\mathbf{X}$, komunikačnému kanálu a dĺžke správ M, je definovaný ako zobrazenie $\kappa : \mathbf{X}^N \to \mathbf{A}^M$. Naopak dekodér je zobrazenie $\delta : \mathbf{B}^M \to \mathbf{A}^M$ a závisí iba od komunikačného kanála a dĺžky správy. Zdroj informácie (odosielateľ) generuje správu $\mathbf{x} \in (\mathbf{X}^N, p^N)$, ktorú kóder zakóduje do vstupnej správy $\mathbf{a} = \kappa(\mathbf{x}) \in \mathbf{A}^M$ a spolu definujú vstupnú hustotu pravdepodobnosti $\pi^M(.) = p^N(\kappa^{-1}(.))$ na $\mathbf{A}^M$. Dekodér δ na základe výstupnej správy $\mathbf{b}$ určí vstupnú správu $\mathbf{a'} = \delta(\mathbf{b}) \in \mathbf{A}^M$. Adresát ale správe $\mathbf{a'}$ nerozumie, lebo nepozná kód, a tak sa mu musí dodať správa $\mathbf{x'} = \kappa^{-1}(\mathbf{a'}) \in \mathbf{X}^N$, čo znamená, že úplný dekodér je zobrazenie $\kappa^{-1}\delta : \mathbf{B}^M \to \mathbf{X}^N$. Pravdepodobnosť chyby, t.j. $\mathbf{x'} \neq \mathbf{x}$, je rovná pravdepodobnosti, že na výstupe je nesprávne určené $\mathbf{a'}$, t.j. $\mathbf{a'} \neq \mathbf{a}$. [2]

[2] Toto platí iba ak κ je prosté zobrazenie, lebo inak κ^{-1} nie je jednoznačne definované.

2.2 KAPACITA

V tejto časti zavedieme pojem kapacity komunikačného kanála. Malo by ísť o číselnú charakteristiku, ktorá určuje množstvo informácie prenesené poslaním jedného písmena daným komunikačným kanálom. Vieme, že informácia závisí od komunikačného kanála, dĺžky správy M a hustoty pravdepodobnosti π^{M} definovanej na vstupných správach, ktorá je určená kódovaním (viď koniec predchádzajúcej časti). Keďže my chceme kvantitu, ktorá závisí iba od komunikačného kanála, tak *kapacitu* zadefinujeme nasledovne

$$\mathrm{C} = \lim_{\mathrm{M}\to\infty} \frac{1}{\mathrm{M}} \sup_{\pi^{\mathrm{M}}} \mathrm{I}(\alpha_1, \dots \alpha_{\mathrm{M}}, \beta_1 \dots \beta_{\mathrm{M}}). \tag{2.2}$$

V tomto vzorci najprv robíme suprémum cez kódovania pri fixnej dĺžke správ M a potom limitu M idúce do nekonečna. Vyberáme teda najlepšie kódovanie v zmysle množstva prenesenej informácie. To znamená najmenšiu pravdepodobnosť chyby pri takomto prenose, lebo vtedy výstupná správa obsahuje v priemere najviac informácie o vstupnej správe pri fixovanom M. Predelenie informácie dĺžkou správy vyjadruje potom priemerné množstvo informácie pripadajúcej na jedno prenesené písmeno správy.

Uvažujme teraz, že $\pi^{\mathrm{M}}(\mathbf{a}) = \pi(\mathrm{a}_1)\dots\pi(\mathrm{a}_{\mathrm{M}})$, kde π je hustota pravdepodobnosti na abecede $\mathbf{A}$. Ďalej nech kanál je bezpamäťový, t.j. $\mathrm{p}^{\mathrm{M}}(\mathbf{b}|\mathbf{a}) = \sum_{\mathrm{i}=1}^{\mathrm{M}} \mathrm{p}(\mathrm{b_i}|\mathrm{a_i})$. Potom $(\alpha_1, \beta_1), \dots, (\alpha_{\mathrm{M}}, \beta_{\mathrm{M}})$ sú vzájomne nezávislé dvojice náhodných veličín so spoločným výberovým priestorom $(\mathbf{A}\times\mathbf{B}, \pi(.)\mathrm{p}(.|.))$. Informácia (2.1) prejde s využitím (B.9) na sumu informácií cez všetky dvojice náhodných veličín, pričom v tomto prípade ide o dvojice rovnakých veličín, t.j. v sume sú všetky členy rovnaké, takže

$$\mathrm{I}(\alpha, \beta) = \mathrm{MI}(\alpha_1, \beta_1).$$

Ak toto dosadíme do (2.2), tak dostaneme

$$\mathrm{C} = \sup_{\pi} \mathrm{I}(\alpha_1, \beta_1) = \sup_{\pi} \sum_{\mathrm{a}\in\mathbf{A}} \sum_{\mathrm{b}\in\mathbf{B}} \pi(\mathrm{a})\mathrm{p}(\mathrm{b}|\mathrm{a}) \log \frac{\mathrm{p}(\mathrm{b}|\mathrm{a})}{\mathrm{p}_{\beta_1}(\mathrm{b})}, \tag{2.3}$$

kde

$$\mathrm{p}_{\beta_1}(\mathrm{b}) = \sum_{\mathrm{a}\in\mathbf{A}} \mathrm{p}(\mathrm{b}|\mathrm{a})\pi(\mathrm{a}).$$

Kapacita bezpamäťového komunikačného kanála spĺňa nerovnosť

$$0 \le \mathrm{C} \le \log \mathrm{N},$$

kde N je počet písmen vo vstupnej abecede. Rovnosť na ľavej strane nastáva, akk sú všetky hustoty $\mathrm{p}(.|\mathrm{a}), \mathrm{a} \in \mathbf{A}$ rovnaké, t.j. α_1, β_1 sú nezávislé pri ľubovoľnej vstupnej hustote π. Rovnosť na pravej strane nastáva, akk $\mathrm{p}(\mathrm{b}|\mathrm{a}) = \delta_{\mathrm{ab}}$, t.j. keď výstupné písmeno jednoznačne určuje písmeno na vstupe.

Nezodpovedanou otázkou zostal výber základu v logaritme, ktorý súvisí s výberom jednotiek informácie. Štandardný výber je logaritmus so základom dva a jednotkou informácie je potom bit. Výber tejto jednotky súvisí s používaním dvojprvkovej (binárnej) abecedy v praxi. Jedným bitom informácie budeme nazývať maximálnu kapacitu ideálneho bezpamäťového komunikačného kanála, ktorý pri prenose používa binárnu abecedu, t.j. $\mathbf{A} = \mathbf{B} = \{0, 1\}$. V takomto prípade $\mathrm{p}(\mathrm{i}|\mathrm{j}) = \delta_{\mathrm{ij}}$ a kapacita je $\log_{\mathrm{z}} 2$. My chceme povedať, že takýto komunikačný kanál má kapacitu rovnú jednej, t.j $\log_{\mathrm{z}} 2 = 1$, čo platí ak základ logaritmu je práve dva.

Kapitola 3

KVANTOVÁ TEÓRIA

3.1 MATEMATICKÝ OPIS

3.1.1 Stav systému

V tejto kapitole zavedieme základné pojmy a matematický formalizmus vyskytujúce sa v kvantovej mechanike.

Kvantový fyzikálny systém A pri matematickom opise stotožňujeme s komplexným separabilným Hilbertovým priestorom H so skalárnym súčinom $\langle .|. \rangle$. My budeme uvažovať iba konečnorozmerné Hilbertove priestory. Znalosť systému znamená poznať všetky možné stavy tohoto systému. *Stavom* na tomto priestore nazveme lineárny operátor ϱ, ktorý má nasledujúce vlastnosti

1.$\varrho = \varrho^+$, t.j. *hermitoskosť*

2.$\varrho \geq 0$, t.j. $\forall |\psi\rangle \in$ H platí $\langle \psi|\varrho|\psi\rangle \geq 0$, t.j. *pozitívnosť*

3.Tr$\varrho = 1$

Takýto operátor nazývame *maticou hustoty*. Ak je matica hustoty projektorom, t.j. $\varrho = \varrho^2$, tak hovoríme, že systém je v *čistom stave*. Inak hovoríme, že je systém v *zmesi*. Každý čistý stav je jednoznačne určený jednotkovým vektorom, $||\psi|| = 1$, z Hilbertovho priestoru H. Teda množina čistých stavov je zhodná s množinou všetkých jednotkových vektorov z H. Matica hustoty pre čistý stav má tvar $|\psi\rangle\langle\psi|$ pre každé $\psi \in$ H, pre ktoré $||\psi|| = 1$. Množina stavov tvorí konvexnú množinu, t.j. platí ak ϱ_i sú stavy, $\lambda \in \mathbf{R}$, $\lambda_\mathrm{i} \geq 0$ a $\sum \lambda_\mathrm{i} = 1$, tak aj $\sum \lambda_\mathrm{i}\varrho_\mathrm{i}$ je stavom na tomto priestore, t.j. spĺňa všetky tri podmienky.

V prípade lineárnej kombinácie vektorových stavov $|\psi_\mathrm{i}\rangle \in$ H, $||\psi_\mathrm{i}|| = 1$

$$|\psi\rangle = \sum_\mathrm{i} \alpha_\mathrm{i}|\psi_\mathrm{i}\rangle,$$

takémuto súčtu hovoríme *superpozícia*, ktorá je opäť vektorovým (t.j. čistým) stavom. V tomto prípade, narozdiel od konvexnej kombinácie, $\alpha_\mathrm{i} \in \mathbf{C}$ a $\sum_\mathrm{i} |\alpha_\mathrm{i}|^2$=1. Vektorovým stavom nazývame vektorový zápis čistého stavu.

Rozšírením Hilbertovho priestoru H o nové stupne voľnosti vieme pre každú zmes nájsť čistý stav v tomto rozšírenom priestore, z ktorého čiastočnou stopou cez pridané stupne voľnosti dostaneme danú zmes. Procedúru nájdenia čistého stavu pre zmes nazývame *purifikácia* [1].

Rozoznávame dva druhy systémov: *otvorené* a *izolované*, podľa toho, či sú alebo nie sú ovplyvňované svojim okolím. V kvantovej teórii izolovaných systémov sa stavy menia dvoma rozdielnymi spôsobmi: pri meraní alebo evolúciou podľa Schröedingerovej rovnice. Ďalej zovšeobecníme tieto pojmy na otvorené systémy.

[1] z anglického purification, čo znamená očistenie

3.1.2 Meranie

Meranie opisujeme pre izolované systémy pomocou samozdruženého operátora $\mathbf{A} = \mathbf{A}^+$, pričom možné výsledky merania sú práve vlastné hodnoty takéhoto operátora, ktoré sú určené rovnicou

$$\mathbf{A}|\phi_a\rangle = a|\phi_a\rangle,$$

kde $|\phi_a\rangle$ sú vlastné stavy operátora $\mathbf{A}$. Tieto vlastné stavy tvoria úplný ortonormovaný systém, čo znamená, že ľubovolný stav $|\psi\rangle$ môžeme rozvinúť v tejto báze do Fourierovho radu

$$|\psi\rangle = \sum_a \langle\phi_a|\psi\rangle|\phi_a\rangle.$$

Každú meranú veličinu (*pozorovateľnú*) vieme zapísať v báze vlastných stavov tejto veličiny ako

$$\mathbf{A} = \sum_a a|\phi_a\rangle\langle\phi_a| = \sum_a a\mathbf{E}_a, \tag{3.1}$$

kde $\mathbf{E}_a$ je projektorom na H. Tento zápis nazývame spektrálny rozklad operátora. Takéto meranie nazývame *ortogonálne*.

Pri meraní nám kvantová mechanika určuje iba pravdepodobnostné rozdelenie výsledkov, ktoré je určené stavom, na ktorom meriame. Ak meriame veličinu $\mathbf{A}$ na stave ϱ, tak pravdepodobnostné rozdelenie výsledkov je určené vzťahom

$$\Pr(a) = \mathrm{Tr}(\varrho\mathbf{E}_a). \tag{3.2}$$

Stav kvantového systému môžeme teda chápať ako zobrazenie p, ktoré projektoru na H priradí číslo z intervalu $\langle 0, 1\rangle$, t.j. p je mierou na množine projektorou, a teda platí

1.p($\mathbf{0}$)=0; p($\mathbf{1}$)=1

2.ak $\mathbf{E}.\mathbf{F}=\mathbf{0}$, tak p($\mathbf{E}$+$\mathbf{F}$)=p($\mathbf{E}$)+p($\mathbf{F}$).

Gleasonov teorém hovorí, že pre dim(H)>2 pre každé p existuje matica hustoty ϱ taká, že

$$\mathrm{p}(\mathbf{E}) = \mathrm{Tr}(\varrho\mathbf{E}).$$

Zadefinujeme *zovšeobecnené meranie*, ktoré nazývame POVM[2] ako množinu operátorov $\{\mathbf{F_a}\}$ na systéme A, pre ktorú platí

1.$\mathbf{F}_a = \mathbf{F}_a^+$

2. ${}_{\mathrm{A}}\langle\psi|\mathbf{F}_a|\psi\rangle_{\mathrm{A}} \geq \mathbf{0}$

3.$\sum_a \mathbf{F}_a = \mathbf{1}_{\mathrm{A}}$

Narozdiel od ortogonálneho merania v tomto prípade $\mathbf{F}_a$ nemusia byť projekcie. Podľa *Neumarkovho teorému* môže byť každá POVM realizovaná v rozšírenom Hilbertovom priestore ortogonálnym meraním, pričom ak POVM obsahuje n operátorov $\mathbf{F}_a$, tak rozšírený Hilbertov priestor má dimenziu rovnú n.

Nech systém A je podsystém systému opísaného Hilbertovým priestorom $\mathrm{H}=\mathrm{H_A}\otimes\mathrm{H_B}$ a na tomto H robíme ortogonálne meranie, ktoré je určené projektormi $\mathbf{E}_a$, ktorých počet je práve dimenzia H. Pravdepodobnosť namerať výsledok a na celom H je daná vzťahom (3.2).Všimnime si pôsobenie týchto projektorov na podsystéme A, ktorého stav nech je $\varrho_{\mathrm{AB}} = \varrho_{\mathrm{A}} \otimes \varrho_{\mathrm{B}}$, t.j. systémy sú navzájom izolované. Pravdepodobnosť výsledku a je

$$\Pr(a) = \mathrm{Tr_A}(\mathrm{Tr_B}((\varrho_{\mathrm{A}} \otimes \varrho_{\mathrm{B}})\mathbf{E}_a)) = \mathrm{Tr_A}(\mathbf{F}_a\varrho_{\mathrm{A}}),$$

[2]Positive Operator Valued Measure

kde

$$(\mathbf{F}_a)_{\mathrm{ij}} = \sum_{\mu\nu} (\mathbf{E}_a)_{\mathrm{j}\nu,\mathrm{i}\mu} (\varrho_{\mathrm{B}})_{\mu\nu}.$$

Ak zadefinujeme projekciu $\mathbf{E}_{\mathrm{A}} : \mathrm{H} \to \mathrm{H}_{\mathrm{A}}$, tak operátory $\mathbf{F}_a$ tvoriace POVM môžeme formálne zapísat' aj takto

$$\mathbf{F}_a = \mathbf{E}_{\mathrm{A}} \mathbf{E}_a \mathbf{E}_{\mathrm{A}}.$$

Kvantová teória obmedzuje aj súčasné merania niektorých veličín. Zo spektrálneho rozkladu (3.1) vidno, že ak nemajú operátory diagonálny tvar v tej istej báze, t.j. nekomutujú, tak meranie jednej veličiny ovplyvňuje meranie druhej veličiny, lebo merania robia projekcie na rôzne vektory, čo znamená rôzne pravdepodobnostné distribúcie výsledkov (3.2). Strednú hodnotu operátora $\mathbf{A}$ v stave ψ definujeme nasledovne

$$\langle \mathbf{A} \rangle = \langle \psi | \mathbf{A} | \psi \rangle = \mathrm{Tr}(\varrho \mathbf{A})$$

a pre disperziu platí $\triangle \mathbf{A} = (\langle \mathbf{A^2} \rangle - \langle \mathbf{A} \rangle^{\mathbf{2}})^{\frac{1}{2}}$. Potom dostávame vzt'ah neurčitosti pre pozorovateľné **A**,**B**

$$\triangle \mathbf{A} \triangle \mathbf{B} \geq \frac{\mathbf{1}}{\mathbf{2}} \langle [\mathbf{A}, \mathbf{B}] \rangle,$$

odkiaľ tiež vidno význam komutátora. Ak je komutátor dvoch veličín nulový, tak potom tieto veličiny majú súčasne ostré hodnoty.

V kvantovej teórii treba mat' stále na pamäti, že ide o pravdepodobnostnú teóriu, v ktorej jedno meranie nemá veľký význam. V takomto duchu platí aj vzt'ah neurčitosti, t.j. netýka sa výsledkov jedného merania. Samozrejme, že môžeme **A** a **B** zmerat' súčasne, ale výsledky opakovaných meraní týchto veličín na rovnako pripravených stavoch budú vždy rozmazané bez závislosti na presnosti našich meracích prístrojov.

3.1.3 Evolúcia

Pre izolovaný systém je evolúcia vždy unitárna. Podobne ako v klasickej mechanike je generovaná Hamiltoniánom systému **H**, ktorý je zároveň aj operátorom celkovej energie. Samotnú evolúciu stavu popisuje Schrödingerova rovvnica

$$\mathrm{i}\hbar \partial_{\mathrm{t}} |\psi_{\mathrm{t}}\rangle = \mathbf{H} |\psi_{\mathbf{t}}\rangle \tag{3.3}$$

s počiatočnou podmienkou

$$|\psi_{t=0}\rangle = |\psi_0\rangle,$$

ktorej formálnym riešením je

$$|\psi_t\rangle = \exp(-\frac{\mathrm{i}}{\hbar} \mathbf{H} \mathrm{t}) |\psi_0\rangle.$$

Opät' sa pozrime ako sa vyvíja podsystém systému, ak sa celý systém vyvíja unitárne. Tento vývoj podsystému zadefinujeme ako zobrazenie \$, ktoré matici hustoty priradí inú maticu hustoty. Toto zobrazenie \$ budeme nazývat' *superoperátorom* a musí spĺňat'

1.\$ zachováva hermitovskost'

2.\$ zachováva stopu

3.\$ je úplne pozitívne, t.j. pre všetky rozšírenia z H_{A} na $\mathrm{H}_{\mathrm{A}} \otimes \mathrm{H}_{\mathrm{B}}$ je $\$_{\mathrm{A}} \otimes \mathbf{1}_{\mathrm{B}}$ pozitívne

4.\$ je lineárne

Prvé tri požiadavky sú z podmienky, aby $\$(\varrho)$ bola tiež matica hustoty. Požiadavka linearity je z dôvodu zachovania pravdepodobnostnej interpretácie, a síce pre nelineárne \$ by mohol závisiet' vývoj ϱ na spôsobe jeho prípravy.

Napríklad uvažujme zobrazenie $\$(\varrho) = \exp(\mathrm{i}\pi\sigma_1 \mathrm{Tr}(\sigma_1 \varrho)) \varrho \exp(-\mathrm{i}\pi\sigma_1 \mathrm{Tr}(\sigma_1 \varrho)))$, ktoré spĺňa prvé tri požiadavky. Nech $\varrho_1 = \frac{1}{2}\mathbf{1}$, t.j. $\varrho_1 = \frac{1}{2}|\mathrm{z}\rangle\langle \mathrm{z}| + \frac{1}{2}|-\mathrm{z}\rangle\langle -\mathrm{z}|$ a v tomto prípade je $\mathrm{Tr}(\sigma_1 \varrho_1) = 0$,čo

znamená, že evolúcia je triviálna. Teraz nech $\varrho_2 = \frac{1}{2}|\mathrm{x}\rangle\langle\mathrm{x}| + \frac{1}{2}|\mathrm{z}\rangle\langle\mathrm{z}|$. Pre takýto stav je $\mathrm{Tr}(\varrho_2\sigma_1) = \frac{1}{2}$, a potom $\$(\varrho_2) = \sigma_1\varrho\sigma_1$. Teda spin pripravený v stave $|\mathrm{z}\rangle$ sa v prvom prípade vyvinie na $|\mathrm{z}\rangle$ a v druhom prípade na $|-\mathrm{z}\rangle$, čo sú navzájom ortogonálne stavy a teda evolúcia závisí od prípravy, t.j. z akého ansámbla stavy pochádzajú.

Uvažujme unitárny vývoj stavu $\varrho_\mathrm{A} \otimes |0\rangle_{\mathrm{BB}}\langle 0|$ pomocou unitárneho operátora $\mathbf{U}_{\mathrm{AB}}$. Chceme vediet' maticu hustoty systému A, t.j. urobíme čiastočnú stopu cez B a evolúcia na systéme A potom vyzerá nasledovne

$$\varrho'_\mathrm{A} = \mathrm{Tr}_\mathrm{B}(\mathbf{U}_{\mathrm{AB}}(\varrho_\mathrm{A} \otimes |\mathbf{0}\rangle_{\mathrm{BB}}\langle\mathbf{0}|)\mathbf{U}^+_{\mathrm{AB}}) = \sum_\mu {}_\mathrm{B}\langle\mu|\mathbf{U}_{\mathrm{AB}}|\mathbf{0}\rangle_\mathrm{B}\ \varrho_\mathrm{A}\ {}_\mathrm{B}\langle\mathbf{0}|\mathbf{U}_{\mathrm{AB}}|\mu\rangle_\mathrm{B}$$

Zadefinujme operátor na systéme A

$$\mathbf{M}_\mu := {}_\mathrm{B}\langle\mu|\mathbf{U}_{\mathrm{AB}}|\mathbf{0}\rangle_\mathrm{B}.$$

Potom evolúcia na tomto systéme sa dá zapísat' pomocou tohto operátora ako

$$\varrho'_\mathrm{A} = \$(\varrho) = \sum_\mu \mathbf{M}_\mu\varrho_\mathrm{A}\mathbf{M}^+_\mu \tag{3.4}$$

Pre tieto operátory platí

$$\sum_\mu \mathbf{M}^+_\mu\mathbf{M}_\mu = \sum_\mu {}_\mathrm{B}\langle\mathbf{0}|\mathbf{U}^+_{\mathrm{AB}}|\mu\rangle_\mathrm{B}\ {}_\mathrm{B}\langle\mu|\mathbf{U}_{\mathrm{AB}}|\mathbf{0}\rangle_\mathrm{B} = {}_\mathrm{B}\langle\mathbf{0}|\mathbf{U}^+_{\mathrm{AB}}\mathbf{U}_{\mathrm{AB}}|\mathbf{0}\rangle_\mathrm{A} = \mathbf{1}_\mathrm{A},$$

lebo $\mathbf{U}^+_{\mathrm{AB}}\mathbf{U}_{\mathrm{AB}} = \mathbf{1}_{\mathrm{AB}}$. Takáto reprezentácia superoperátora pomocou operátorov $\mathbf{M}_\mu$, ktoré spĺňajú $\sum_\mu \mathbf{M}^+_\mu\mathbf{M}_\mu = \mathbf{1}_\mathrm{A}$, sa nazýva *Krausova reprezentácia*. Dá sa ukázat', že takto zadefinované zobrazenie je superoperátorom, t.j. spĺňa všetky štyri podmienky a implikácia platí aj naopak, t.j. pre každý superoperátor $\$ existuje Krausova reprezentácia tohto superoperátora. Táto Krausova reprezentácia superoperátora nie je určená jednoznačne, lebo môžeme urobit' čiastočnú stopu cez B v l'ubovolnej báze, pričom medzi bázami plati $|\nu\rangle_\mathrm{B} = \sum_\mu \mathbf{U}_{\nu\mu}|\mu\rangle_\mathbf{B}$. V dvoch Krausových reprezentáciach $\mathbf{M}_\mu, \mathbf{N}_\nu$ toho istého superoperátora sa jednotlivé operátory líšia unitárnou transformáciou $\mathbf{N}_\nu = \mathbf{U}_{\nu\mu}\mathbf{M}_\mu$.

Superoperátor nám poskytuje formalizmus pre opis dekoherencie, t.j. vývoj čistých stavov na zmesi. Unitárna evolúcia je špeciálnym prípadom, ak v Krausovej reprezentácii je iba jeden operátor. Ak je operátorov viac, tak z čistého stavu systému A sa stáva zmes, lebo cez $\mathbf{U}_{\mathrm{AB}}$ systém A interaguje s okolím, t.j. so systémom B a teda A sa správa ako otvorený systém.

Zložením dvoch superoperátorov $\$_1$ a $\$_2$ dostávame nový superoperátor $\$_1 \circ \$_2$. Otázkou je, či existuje aj inverzný superoperátor. Predstavme si, že čisté stavy v prípade dvojstavového systému sú reprezentované bodmi na dvojdimenzionálnej sfére (tzv. *Blochova sféra*). Stav reprezentovaný maticou hustoty je v tomto prípade

$$\varrho = \frac{1}{2}(\mathbf{1} + \vec{\mathrm{P}}.\vec{\sigma}),$$

kde $|\vec{\mathrm{P}}| \leq 1$ a $\vec{\sigma} = (\sigma_\mathrm{x},\ \sigma_\mathrm{y}, \sigma_\mathrm{z})$ sú Pauliho σ-matice, ktoré sú definované nasledovne

$$\sigma_\mathrm{x} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_\mathrm{y} = \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \quad \sigma_\mathrm{z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{3.5}$$

Pre čistý stav $|\vec{\mathrm{P}}| = 1$. Ak superoperátor opisuje evolúciu z čistého stavu do zmesi, tak to graficky v tomto prípade znamená zmenšovanie (kontrakciu) sféry. Otočenie kontrakcie (inflácia) je síce možné, ale toto otočenie nie je pozitívnym zobrazením. Odpoveď je kladná, iba ak superoperátor je unitárny, lebo vtedy neprichádza ku kontrakcii. Vo všeobecnosti superoperátor bežiaci späť v čase nie je superoperátorom. Superoperátory tvoria pologrupu.

Ešte zovšeobecníme Schrödingerovu rovnicu (3.3) pre otvorené systémy. Pre matice platí Schrödingerova rovnica v tomto tvare ($\hbar = 1$)

$$\dot{\varrho} = -\mathrm{i}[\mathbf{H}, \varrho]$$

s formálnym riešením

$$\varrho(t) = e^{-\mathrm{i}\mathbf{H}\mathrm{t}}\varrho(0)e^{\mathrm{i}\mathbf{H}\mathrm{t}},$$

kde $\mathbf{H}$ je časovo nezávislý hamiltonián systému A. Časový vývoj matice hustoty generovaný superoperátorom $\$_t$ je

$$\varrho(t) = \$_t(\varrho(0)) = \sum_\mu \mathbf{M}_\mu(\mathrm{t})\varrho(0)\mathbf{M}_\mu^+(\mathrm{t}) \tag{3.6}$$

$$\$_{t=0} = \mathbf{1}.$$

Uvažujme Markovovskú evolúciu, t.j. stav v čase t+dt je úplne určený iba stavom v čase t. Ak $\varrho(0) = \varrho(0) + \mathrm{O(dt)}$), tak jeden z Krausových operátorov bude mať tvar $\mathbf{M_0} = \mathbf{1} + (-\mathrm{i}\mathbf{H} + \mathbf{K})\mathrm{dt}$ a ostatné budú mať tvar $\mathbf{M}_\mu = \sqrt{\mathrm{dt}}\mathbf{L}_\mu$. Toto sú predpoklady priblíženia, ktoré vychádzajú z markovovosti systému. Použijeme Krausovu normalizačnú podmienku $\sum_\mu \mathbf{M}_\mu^+\mathbf{M}_\mu = \mathbf{1}$, tak dostaneme

$$\mathbf{K} = -\frac{1}{2}\sum_{\mu\neq 0}\mathbf{L}_\mu^+\mathbf{L}_\mu.$$

Dosadením do (3.6) v prvom ráde, t.j. $\varrho(0) = \varrho(0) + \dot{\varrho}(0)\mathrm{dt}$, dostaneme riešenie pre $\dot{\varrho}(0)$, čo zovšeobecníme na ľubovolný čas t

$$\dot{\varrho} = -\mathrm{i}[\mathbf{H}, \varrho] + \sum_{\mu\neq\mathbf{0}}(\mathbf{L}_\mu\varrho\mathbf{L}_\mu^+ - \frac{1}{2}\mathbf{L}_\mu^+\mathbf{L}_\mu\varrho - \frac{1}{2}\varrho\mathbf{L}_\mu^+\mathbf{L}_\mu) \tag{3.7}$$

Rovnicu nazývame *Lindbladovou rovnicou.* Operátory $\mathbf{L}_\mu$ nazávame Lindbladove operátory, alebo quantum jump operator. Prvý člen v Lindbladovej rovnici je obyčajný Schrödingerov člen generujúci unitárny vývoj. Druhý člen opisuje zmenu stavu okolia a jeho vplyv na systém A, o ktorý sa zaujímame. Lindbladova rovnica je všeobecnou formou Markovovskej evolúcie matíc hustoty, ktorú nazývame aj *master equation.*

3.1.4 Schmidtova dekompozícia

Čistý stav systému zloženého z dvoch podsystémov , $\mathrm{H_{AB}} = \mathrm{H_A} \otimes \mathrm{H_B}$, môžeme vyjadriť v tvare

$$|\psi\rangle_{\mathrm{AB}} = \sum_{\mathrm{i},\mu} a_{\mathrm{i}\mu}|\mathrm{i}\rangle_{\mathrm{A}}|\mu\rangle_{\mathrm{B}},$$

kde $|\mathrm{i}\rangle_{\mathrm{A}}$ a $|\mu\rangle_{\mathrm{B}}$ nemusia tvoriť ortonormálne systémy. Schmidtova dekompozícia je zápis takéhoto stavu v ortonormálnej báze celého systému $\mathrm{H_A} \otimes \mathrm{H_B}$.

Nech $|\mathrm{i}\rangle_{\mathrm{A}}$ je báza, v ktorej je ϱ_{A} diagoálne, t.j. $\varrho_{\mathrm{A}} = \sum_{\mathrm{i}} \mathrm{p_i}|\mathrm{i}\rangle_{\mathrm{AA}}\langle\mathrm{i}|$, a položme $|\tilde{\mathrm{i}}\rangle_{\mathrm{B}} = \sum_\mu a_{\mathrm{i}\mu}|\mu\rangle_{\mathrm{B}}$. Potom ${}_{\mathrm{B}}\langle\tilde{\mathrm{i}}|\tilde{\mathrm{j}}\rangle_{\mathrm{B}} = \mathrm{p_i}\delta_{\mathrm{ij}}$, t.j. tvoria ortogonálny systém. Keďže chceme ortonormálnu bázu na B, tak položme $|\mathrm{i}'\rangle = \mathrm{p_i}^{-\frac{1}{2}}|\tilde{\mathrm{i}}\rangle$ a tieto vektory $|\mathrm{i}'\rangle$ už tvoria ortonormálny systém a ľubovolný systém vieme zapísať

$$|\psi\rangle_{\mathrm{AB}} = \sum_{\mathrm{i}} \sqrt{\mathrm{p_i}}|\mathrm{i}\rangle_{\mathrm{A}}|\mathrm{i}'\rangle_{\mathrm{B}},$$

kde $|\mathrm{i}\rangle_{\mathrm{A}} \otimes |\mathrm{i}'\rangle_{\mathrm{B}}$ je časť ortonormálnej bázy v $\mathrm{H_A} \otimes \mathrm{H_B}$. Tento rozklad nazývame Schidtovou dekompozíciou a báza rozkladu čistého stavu závisí od tohto stavu.

Stav $\varrho_{\mathrm{B}} = \sum_{\mathrm{i}} \mathrm{p_i}|\mathrm{i}'\rangle_{\mathrm{BB}}\langle\mathrm{i}'|$, t.j. ϱ_{A} a ϱ_{B} majú rovnaké vlastné hodnoty, ale počet nulových sa môže líšiť, lebo $\mathrm{dim H_A} \neq \mathrm{dim H_B}$. Počet nenulových vlastných hodnôt ϱ_{A} alebo ϱ_{B} nazývame *Schmidtovým*

číslom. Lokálne unitárne transformácie nezvyšujú Schmidtovo číslo, lebo vlastné hodnoty operátora ϱ_A a $\mathbf{U}_A\varrho_A\mathbf{U}_A^+$ sú rovnaké [3].

Konkrétne pre podsystémy dim(H_A)=dim(H_B)=2 vieme každý čistý stav celého systému zapísat' v tvare

$$|\psi\rangle_{AB} = \alpha|0\rangle_A|\phi_0\rangle_B + \beta|1\rangle_A|\phi_1\rangle_B, \tag{3.8}$$

kde $\langle\phi_0|\phi_1\rangle = 0$.

Matemeticky je existencia Schmidtovej dekompozície ekvivalentná teorému: Pre danú obdĺžnikovú maticu A je vždy možné nájst' unitárne matice U_1 a U_2, aby obdĺžniková matica $B=U_1AU_2$ mala tvar $B_{mn} = \beta_m\delta_{mn}$.

3.1.5 Entropia

Pre meranie vieme predpovedat' iba pravdepodobnosti výsledkov, t.j. poznáme pravdepodobnostnú distribúciu výsledkov. Vieme, že pri n opakovaých meraniach na rovnako pripravených n systémoch, pre n dostatočne veľké, očakávame $n_i = np_i$ výsledkov typu i. Počet rôznych možností ako konkrétne vyzerajú jednotlivé výsledky pri n meraniach je $n!/(n_1!n_2!\ldots)$. Pre $n\to\infty$ a s použitím Stirlingovho vzorca dostávame

$$\log\frac{n!}{n_1!n_2!\ldots} = n\log n - n - \sum_i(n_i\log n_i - n_i) = -n\sum_i p_i\log p_i.$$

Výraz

$$S := -\sum_{i=1}^{N} p_i\log p_i \tag{3.9}$$

nazývame *entropiou* pravdepodobnostnej distribúcie $\{p_1\ldots p_N\}$. Táto kvantita vyjadruje mieru našej nevedomosti pre dané meranie a daný stav systému. Nezávisí od počtu n uskutočnených meraní. Dopredu nevieme aký výsledok konkrétne nameriame a pri n meraniach je počet rôznych možných postupností výsledkov rovný 2^{-nS}. Čím viacej rôznych postupností existuje, tým viac o systéme nevieme (alebo zanedbávame v prípade klasickej teórie).

Ak pravdepodobnostná distribúcia $p_i = 1/N$ pre všetky i=1,...,N, tak sa entropia rovná logN a je maximálna.

V kvantovej teórii sú pravdepodobnosti výsledkov určené vzťahom (3.2) a teda sú jednoznačne dané maticou hustoty. Maximálna hodnota entropie zodpovedá maximálnej zmesi. Opačným prípadom je prípad vlastného stavu pozorovatel'nej, kedy je entropia nulová, lebo vtedy meranie na systéme v takomto stave jednoznačne určuje tento čistý stav.

Zadefinujeme *entropiu prípravy* stavu, ako najnižšiu hodnotu (3.9) pre všetky ortogonálne merania.

Optimálnym meraním, ktoré minimalizuje S je meranie vo vlastných stavoch operátora matice hustoty, pre ktoré

$$S = -\sum_\mu \lambda_\mu\log\lambda_\mu,$$

kde λ_μ sú vlastné hodnoty tohto operátora. Matica hustoty opisujúca systém má v báze vlastných vektorov tvar

$$\varrho = \sum_\mu \lambda_\mu|\phi_\mu\rangle\langle\phi_\mu|$$

[3] ide o podobnostnú transformáciu matíc

Iné meranie je opísané množinou ortogonálnych projektorou $\{|\psi_1\rangle\langle\psi_1|,\ldots,|\psi_N\rangle\langle\psi_N|\}$. Ak robíme stopu v báze vlastných stavov matice hustoty, tak dostávame pre jednotlivé výsledky meraní a_i pre i=1,...,N

$$\mathrm{Pr}(a_\mathrm{i}) = \sum_\mu \lambda_\mu |\langle\psi_i|\phi_\mu\rangle|^2 = \sum_\mu \lambda_\mu \mathrm{p}_{\mu\mathrm{i}}.$$

Našou úlohou je porovnať entropiu pre meranie v báze vlastných stavov matice hustoty S=S(λ_μ) a entropiu pre ľubovoľné iné ortogonálne meranie S = S($\sum_\mu \lambda_\mu \mathrm{p}_{\mu\mathrm{i}}$).

Počítajme rozdiel

$$\mathrm{S}(\sum_\mu \lambda_\mu \mathrm{p}_{\mu\mathrm{i}}) - \mathrm{S}(\lambda_\mu) = \sum_\mu \lambda_\mu \log\lambda_\mu - \sum_\mathrm{i}\sum_\mu \lambda_\mu \mathrm{p}_{\mu\mathrm{i}} \log(\sum_\mu \lambda_\mu \mathrm{p}_{\mu\mathrm{i}}) =$$

$$= \sum_\mu \lambda_\mu (\log\lambda_\mu - \sum_\mathrm{i} \mathrm{p}_{\mu\mathrm{i}} \log(\mathrm{Pr}(a_\mathrm{i})) = \sum_{\mu,\mathrm{i}} \lambda_\mu \mathrm{p}_{\mu\mathrm{i}} \log(\lambda_\mu/\mathrm{Pr}(a_\mathrm{i})),$$

kde sme využili, že vďaka ortogonálnosti merania platí $\sum_\mathrm{i} \mathrm{p}_{\mu\mathrm{i}} = 1$. Ďalej platí $\log x \geq 1 - x^{-1}$ a

$$\mathrm{S}(\mathrm{Pr}(a_\mathrm{i})) - \mathrm{S}(\lambda_\mu) \geq \sum_{\mu,\mathrm{i}} \lambda_\mu \mathrm{p}_{\mu\mathrm{i}}(1 - \mathrm{Pr}(a_\mathrm{i})/\lambda_\mu) = 0.$$

Vidno teda, že meranie v báze vlastných stavov matice hustoty je optimálne v zmysle, že entropia pravdepodobnostnej distribúcie výsledkov je pri ňom najnižšia. Entropia prípravy, alebo entropia stavu ϱ, je teda

$$\mathrm{S} = -\mathrm{Tr}(\varrho\log\varrho) \tag{3.10}$$

Relatívnou entropiou S($\sigma||\varrho$) nazývame nasledujúci výraz

$$\mathrm{S}(\sigma||\varrho) = \mathrm{Tr}(\varrho(\log\varrho - \log\sigma)),$$

kde ϱ a σ sú dva stavy toho istého systému.

Uvedieme niektré matematické vlastnosti entropie:

1.Invariantnosť pri unitárnej transformácii S(UϱU$^+$) = S(ϱ).

2.Subaditívnosť

$$\mathrm{S}(\varrho_\mathrm{AB}) \leq \mathrm{S}(\varrho_\mathrm{A}) + \mathrm{S}(\varrho_\mathrm{B}),$$

kde $\varrho_\mathrm{A} = \mathrm{Tr}_\mathrm{B}(\varrho_\mathrm{AB})$ a $\varrho_\mathrm{B} = \mathrm{Tr}_\mathrm{A}(\varrho_\mathrm{AB})$. Rovnosť nastáva v prípade, akk $\varrho_\mathrm{AB} = \varrho_A \otimes \varrho_B$. Táto nerovnosť nám hovorí, že časť informácie je v koreláciach medzi systémami.

3.Araki-Liebova nerovnosť (trojuholníková nerovnosť)

$$\mathrm{S}(\varrho_\mathrm{AB}) \geq |\mathrm{S}(\varrho_\mathrm{A}) - \mathrm{S}(\varrho_\mathrm{B})|.$$

4.Silná subaditívnosť

$$\mathrm{S}(\varrho_\mathrm{ABC}) + \mathrm{S}(\varrho_\mathrm{B}) \leq \mathrm{S}(\varrho_\mathrm{AB}) + \mathrm{S}(\varrho_\mathrm{BC}).$$

3.2 ENTANGLOVANIE

3.2.1 EPR paradox

Ak sa systém skladá z podsystémov (*zložený systém*), H=H$_1\otimes\ldots\otimes$H$_\mathrm{k}$, a jeho stav ϱ_H sa dá zapísať ako váhovaný kartézsky súčin stavov jednotlivých podsystémov, t.j.

$$\varrho_\mathrm{H} = \sum_\mathrm{i} \mathrm{p}_\mathrm{i} \varrho^\mathrm{i}_{\mathrm{H}_1} \otimes \ldots \otimes \varrho^\mathrm{i}_{\mathrm{H}_\mathrm{k}},$$

tak tento stav ϱ_{H} nazývame *separabilný*. Povieme, že stav je *entanglovaný*, ak nie je separabilný. *Lokálnym unitárnym operátorom* nazveme unitárny operátor pôsobiaci iba na jednom z podsystémov celého systému, a ktorý sa na ostatných podsystémoch chová ako jednotkový operátor. Takýto unitárny operátor nijako nemení stavy na ostatných podsystémoch. Analogicky *lokálnym meraním* nazveme meranie uskutočnené iba na jednom podsystéme, ktoré matemeticky opisujeme samozdruženým operátorom, ktorý sa na ostatných podsystémoch správa ako jednotkový operátor.

Entanglované stavy sa asi dostali po prvýkrát do pozornosti vďaka EPR[4] paradoxu. Uvažujme dvojčasticový systém v entanglovanom stave

$$|\phi^+\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

kde každý zo systémov A,B je dvojstavový. Stavy na jednotlivých podsystémoch sú v prípade uvažovaného stavu matice hustoty $\frac{1}{2}\mathbf{1}$, čo sú *maximálne zmesi* v zmysle, že pre každé ortogonálne meranie na podsystéme sú všetky výsledky rovnako váhované, lebo

$$\mathrm{Tr}(\varrho \mathbf{E}_a) = \frac{1}{2}\mathrm{Tr}(\mathbf{E}_a) = \frac{1}{2}.$$

Takýto čistý stav, pre ktorý platí, že stavy podsystémov sú maximálne zmesi, nazývame *maximálne entanglovaný*.

Nech z nejakého miesta C sa entanglované častice v stave $|\psi\rangle$ pošlú jedna (systém A) na miesto A a druhá (systém B) na miesto B ($\neq$A). V týchto miestach nech prebieha meranie. Predstavme si , že A meria spin pozdĺž osi z a zo svojho výsledku vie určiť stav na B, ale ak B súčasne meria pozdĺž osi x, tak zistí velkosť spinu v tomto smere. Teda o B vieme hodnoty jeho spinu pozdĺž osi z a aj pozdĺž osi x. Ale v kvantovej teórii, nie je možná súčasná znalosť priemetu spinu do dvoch rôznych smerov. Chyba je v tejto úvahe v tom, že veličina, ktorú podľa kvantovej mechaniky skutočne meriame je $\sigma_{\mathrm{z}}^{\mathrm{A}} \otimes \sigma_{\mathrm{x}}^{\mathrm{B}}$ a vlastné hodnoty tejto veličiny ± 1 sú dvakát degenerované a nehovoria nám nič o konkrétnych hodnotách jednotlivých spinov, ale iba či majú rovnaké alebo opačné znamienka.

Výsledky merania σ_{z} na A a na B budú úplne korelované, t.j ak A nameria spin hore, tak aj B nameria spin hore (ak meria spin v tom istom smere). Teda A môže s určitosťou predpovedať výsledok tohto merania na B bez merania na tomto systéme. A tu vznikol EPR paradox.

Zmeraním spinu pozdĺž osi z určíme hodnotu spinu aj na B, podobne aj pre meranie v nejakom inom smere, napr. x, určíme hodnotu spinu B aj v tomto smere. Podľa Einsteina, ak vieme predikovať s určitosťou hodnotu fyzikálnej veličiny bez narušenia systému, tak existuje *element fyzikálnej reality*, ktorý zodpovedá tejto hodnote, t.j. systém je v stave, ktorý má túto hodnotu.

Vlastnosť znalosti stavu systému B po meraní na A podľa EPR narúša princíp *Einsteinovej lokálnosti*, t.j. hypotézy, že pre dva priestorovo separované systémy akcia robená na A nemôže okamžite meniť opis systému B. V našom prípade by potom mal mať systém B dopredu určené všetky hodnoty všetkých možných meraní priemetov spinu, čo v kvantovej teórii nie je možné. Toto viedlo EPR k tomu, že opis systému vlnovou funkciou nie je úplný, lebo úplná teória by podľa EPR mala spĺňať Einsteinovu lokálnosť. EPR navrhli existenciu parametrov systému, ktoré my síce zatiaľ nepoznáme a nevieme určiť, ale ktorých znalosť by nám jednoznačne a deterministicky určovala výsledky meraní, ako sme zvyknutí v klasickej mechanike. Takúto teóriu, ktorá by už vyhovovala Einsteinovej lokálnosti, nazývame teóriou so *skrytými parametrami*.

Otázkou zostala existencia teórie so skrytými parametrami, ktorá by bola lokálna a reprodukovala by výsledky kvantovej teórie, ak by sme vedeli aspoň pravdepodobnostnú distribúciu týchto parametrov (aj keď pri presnej znalosti hodnôt parametrov, by bola teóriou deterministickou, t.j. určovala by presne každý výsledok merania).

[4]Einstein-Podolsky-Rosen

Odpoveď našiel až Bell, ktorý zostrojil triedu teórií so skrytými lokálnymi parametrami (teda klasickú teóriu) a odvodil tzv. Bellove nerovnosti (Dodatok C), ktoré by mala každá takáto teória spĺňať. Tieto nerovnosti vôbec nepotrebujú existenciu kvantovej teórie a dajú sa merať experimentálne. Práve experiment v istých prípadoch potvrdzuje narušenie týchto nerovností a toto narušenie je v zhode s predpoveďami kvantovej teórie. Dá sa ukázať, že vďaka Gleasonovmu teorému, ktorý platí pre dimenzie väčšie alebo rovné trom, takéto teórie so skrytými parametrami neopisujú všetky javy kvantovej mechaniky, lebo existujú stavy systémov, ktoré narúšajú Bellove nerovnosti. Experiment teda vyvrátil Einsteinovu hypotézu o lokálnom opise prírody. Poznamenajme, že pre dimenziu rovnú dvom je takáto teória so skrytými parametrami možná[5].

Skúsme preniesť nejakú informáciu bez toho, aby sme fyzicky posielali nejakú časticu od A ku B, t.j. využime jav znalosti výsledku merania na B pri meraní na A. Meraním informáciu poslať nevieme, lebo výsledky našich meraní (na systéme A) sú úplne náhodné ako vždy pri meraní v kvantovej mechanike, t.j. nevieme dopredu aký výsledok nameria B. Iba jednotlivé výsledky meraní A a B budú navzájom štatisticky korelované.

Ďalšia možnosť je nech A urobí na svojej častici nejakú unitárnu operáciu, ktorá je ale nutne lokálna, a teda nijako nemení stav systému B. Teda žiadnu informáciu bez fyzického prenosu, ktorého rýchlosť už je ohraničená rýchlosťou svetla, poslať nevieme.

3.2.2 Miery entanglovania

Dva systémy v entanglovanom stave nemusia byť navzájom rovnako silne korelované. Uvažujme teraz trochu všeobecnejší stav

$$|\psi\rangle_{\mathrm{AB}} = \alpha|00\rangle + \beta|11\rangle,$$

ktorý je entanglovaný, akk $\alpha \neq 0$ alebo $\alpha \neq 1$. Ak pôjdeme s $\alpha \to 0$ alebo $\alpha \to 1$, tak z entanglovaného stavu sa nám stáva stav separabilný. Matice hustoty na systéme A a B sú opäť rovnaké

$$\varrho_{\mathrm{A}} = \varrho_{\mathrm{B}} = |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1|$$

a teda nie sú maximálne entanglované. Existuje nejaký rozdiel medzi takýmto stavom a stavom maximálne entanglovaným?

Tento rozdiel by malo byť vidieť v situáciach, kde je entanglovanie podstatné, ako napríklad pri Bellovych nerovnostiach (Dodatok C), kvantovej teleportácii (Dodatok D), alebo pri hustom kvantovom kódovaní, ktoré bude opísané v nasledujúcej kapitole. Vo všeobecnosti nie všetky entanglované stavy narúšajú Bellove nerovnosti, t.j. táto vlastnosť nie je dobrým kritériom pri určovaní množstva entanglovania. Niektoré entanglované stavy totiž nie sú v zmysle narúšania Bellovych nerovností odlíšiteľné od separabilných, ktoré nikdy tieto nerovnosti nenarúšajú.

Vychádzajúc z kvantovej teleportácie, pri ktorej separabilné stavy nemôžu byť použité, V.Vedral a M.B.Plenio[6] zadefinovali mieru entanglovania ako reálnu funkciu na množine stavov $\mathbf{S}$, pre ktorú platí

E1. $\mathrm{E}(\sigma)=0$ akk $\sigma \in \mathbf{S}$ je separabilný stav.

E2. $\mathrm{E}(\sigma)=\mathrm{E}(\mathrm{U_A} \otimes \mathrm{U_B}\sigma\mathrm{U_A^+} \otimes \mathrm{U_B^+})$, t.j. lokálne unitárne transformácie nechávajú mieru $\mathrm{E}(\sigma)$ invariantnú.

E3. Entanglovanie nemôže narastať pri procedúre zloženej z lokálneho zovšeobecneného merania (POVM), výmene informácie o meraní cez klasický komunikačný kanál a vhodnej lokálnej unitárnej

[5] viď napr. A.Perez : Quantum theory : Methods and Concepts, chapter 6

[6] M.B.Plenio and V.Vedral : Entanglement in Quantum Information Theory, xxx.lanl.gov/archive/quant-ph/9911...

operácii. Procedúra je spolu opísaná operátormi $\mathrm{V_i}$, pre ktoré $\sum_\mathrm{i} \mathrm{V_i^+ V_i} = \mathbf{1}$. Podmienka nenarastania množstva entanglovania má tvar

$$\sum \mathrm{Tr}(\sigma_\mathrm{i}) \mathrm{E}(\sigma_\mathrm{i}/\mathrm{Tr}(\sigma_\mathrm{i})) \leq \mathrm{E}(\sigma),$$

kde $\sigma_i = V_i \sigma V_i^+$.

E4. Pre dva páry entanglovaných častíc v stavoch σ_1 a σ_2 platí

$$\mathrm{E}(\sigma_1 \otimes \sigma_2) = \mathrm{E}(\sigma_1) + \mathrm{E}(\sigma_2).$$

Podmienka **E1** zabezpečuje, aby iba neentanglované stavy mali nulovú hodnotu entanglovania. Podmienka **E2** zabezpečuje, aby lokálne operácie nemenili mieru entanglovania. V podmienke **E3** sa zamedzuje zvyšovaniu miery entanglovania medzi systémami pri opísanej procedúre, ktorá popisuje kvantovú teleportáciu.

Predstavme si počiatočný stav $|0\rangle_\mathrm{A} \otimes (|0\rangle_\mathrm{B} + |1\rangle_\mathrm{B})/\sqrt{2}$. Tento stav je separabilný. Predpokladajme, že B uskutočňuje meranie v báze $|0\rangle$, $|1\rangle$ a klasickým komunikačným kanálom pošle A správu, ak nameria výsledok 1 a A zmení svoj stav na $|1\rangle_\mathrm{A}$. V prípade výsledku 0 nerobí A nič. Konečný stav je maximálnou zmesou

$$\varrho_\mathrm{AB} = \frac{1}{2}(|0\rangle_\mathrm{AA}\langle 0| \otimes |0\rangle_\mathrm{BB}\langle 0| + |1\rangle_\mathrm{AA}\langle 1| \otimes |1\rangle_\mathrm{BB}\langle 1|).$$

Tento stav je stále separabilný, ale čo sa týka klasickej korelácie (meranej množstvom vzájomnej informácie (B.3)), tak pôvodný stav je nekorelovaný, ale konečný stav už je klasicky korelovaný.

Otázkou je možnost' vzniku entanglovania zo separabilného stavu takouto procedúrou. Odpoved' je záporná, lebo tieto operácie sú čisto lokálne a teda separabilné stavy zostávajú separabilné. Jednoducho to vidiet', ak si uvedomíme tvar týchto operácií.

Situácia sa môže zmenit', ak na počiatku medzi systémami A a B je nejaké entanglovanie, t.j. stav systému A + B je entanglovaný. Entanglovanie môžeme touto procedúrou "skoncentrovat'" a získat' niekol'ko úplne entanglovaných stavov. Toto "skoncentrovanie" sa nazýva *purifikácia entanglovania.* Uvažujme N neúplne entanglovaných stavov $|\psi\rangle_\mathrm{AB}$, t.j. máme stav

$$|\psi_\mathrm{AB}^{\otimes \mathrm{N}}\rangle = \alpha^{2\mathrm{N}}|00\ldots00\rangle + \alpha^{2(\mathrm{N}-1)}\beta^2(|00\ldots0011\rangle + \ldots + |1100\ldots00\rangle) + \ldots \beta^{2\mathrm{N}}|11\ldots11\rangle.$$

A môže teraz robit' projekcie do stavov, v ktorých je nula stavov $|1\rangle$, dva stavy $|1\rangle$, štyri stavy $|1\rangle$, atd'. Výsledky svojich meraní môže klasickým komunikačným kanálom poslat' B. Pravdepodobnost', že pri meraní nameria A výsledok s 2k stavmi $|1\rangle$ je

$$\mathrm{P_{2k}} = \alpha^{2(\mathrm{N}-\mathrm{k})}\beta^{2\mathrm{k}} \begin{pmatrix} \mathrm{N} \\ \mathrm{k} \end{pmatrix}.$$

Dá sa ukázat', že počet maximálne entanglovaných stavov získatel'ných zo stavu, ktorý je získaný z takéhoto merania je zhruba $\ln(\binom{\mathrm{N}}{\mathrm{k}})$. Ak presumujeme cez všetky stavy, ktoré sú výsledkom merania na A, tak pre vel'ké N zistíme, že celkový počet maximálne entanglovaných stavov je $\mathrm{N.S}(\varrho_\mathrm{A})$, kde $\mathrm{S}(\varrho_\mathrm{A})$ je entropia stavu na systéme A získaným prestopovaním cez systém B[7].

Nech A a B zdiel'ajú Bellov stav $(|\phi^+\rangle_\mathrm{AB})^k$ a pomocou lokálnych operácii a klasickej komunikácie pripravím N kópií stavu $|\psi\rangle_\mathrm{AB}$, t.j. $(|\psi\rangle_\mathrm{AB})^N$. Aké je $\mathrm{k_{min}}$ Bellových párov, ktoré treba na túto úlohu?

Naopak predpokladajme, že máme N kópií stavu $|\psi\rangle_\mathrm{AB}$. Lokálnymi operáciami a klasickou komunikáciou chceme pripravit' k′ Bellovych stavov. Aký je maximálny počet, $\mathrm{k'_{max}}$, takýchto Bellovych

[7] viac už v spomínanom článku a v článkoch v ňom citovaných

párov? Táto opačná procedúra je práve purifikácia entanglovania a z predchádzajúceho vieme, že pre čisté stavy

$$k'_{max} = N.S(\varrho_A).$$

Keď že entanglovanie týmito operáciami nemôže narásť, tak $k'_{max} \leq k_{min}$.

Príklad ukazuje, že klasická korelovanosť môže lokálnymi operáciami a klasickou výmenou informácie narastať. Iba čisto klasicky korelovaný separabilný stav nemôže byť ale pri kvantovej teleportácii úspešný. Táto procedúra využíva korelácie medzi systémami, ktoré nie sú klasického pôvodu, lebo také môžu narastať. Preto hovoríme, že entanglovanie vyjadruje mieru kvantovej korelácie systémov. Práve schopnosť použitia stavu pre teleportáciu odlišuje klasickú a kvantovú koreláciu systémov. Hlavným problémom pri určení miery entanglovania je práve problém, ako odlíšiť kvantové korelácie od klasických. Tento príklad by mal byť motiváciou k zavedeniu podmienky **E3**.

Po purifikácii entanglovania získame zmes, v ktorej sa nachádza aj maximálne entanglovaný stav[8]. Po optimálnej purifikácii entanglovania chceme mať toľko maximálne entanglovaných stavov, kol'ko sa dá, t.j. množstvo entanglovania v iných stavoch tvoriacich konečnú zmes je nulové. Pravdepodobnosť maximálne entanglovaného stavu v konečnej zmesi je ohraničená

$$P_{max.ent.} \leq \frac{E(\sigma)}{E(\sigma_{max.ent.})}.$$

Každá miera entanglovania zhora ohraničuje kvantitu, ktorá hovorí o optimalite purifikácie entanglovania. Stav σ chápeme ako tenzorový súčin N stavov systému A + B, z ktorých sme optimálnou purifikáciou pripravili P_{max}.N maximálne entanglovaných stavov. Meraniami na každom stave systému A + B dostávame to isté, ako keby sme merali na stave, ktorý je v zmesi stavov tvoriacich stav σ. Váha každého z týchto stavov je daná početnosťou tohto stavu v tenzorovom súčine predelenou počtom všetkých stavov N, t.j. ide o zmes štatistickom zmysle.

Na tomto mieste vidíme rôzne chápanie zmesí v kvantovej teórii. Môžeme ich rozdeliť do dvoch skupín. Jednu skupinu tvoria *pravé zmesi*, ktoré popisujú stav, v ktorom sa systém môže nachádzať. Druhú skupinu tvoria štatistické zmesi, ktoré sa skladajú z množstva pravých zmesí, t.j. z množstva tých istých systémov, ktoré sa ale nachádzajú v rôznych stavoch a navzájom sa neovplyvňujú, ako je to uvedené aj v tomto príklade.

Pri argumentovaní, ktoré nás priviedlo k hornému ohraničeniu pre pravdepodobnosť výskytu maximálne entanglovaného stavu v zmesi (v tomto prípade štatistickej), sme teda skryte predpokladali, že miera entanglovania spĺňa práve podmienku **E4**.

Uveďme konkrétne príklady mier entanglovania:

- **entropia entanglovania**

$$E_v(|\psi\rangle_{AB}\langle\psi|) = S(Tr_A(|\psi\rangle_{AB}\langle\psi|)) = S(Tr_B(|\psi\rangle_{AB}\langle\psi|))$$

Táto miera je vhodná pre čisté stavy dvojzložkových systémov. Pre zmesi by aj v separabilnom prípade bola táto miera nenulová, čo je v spore s podmienkou **E1**.

Pre dvojzložkový systém je asymptotický prístup k zavedeniu miery entanglovania, ktorý vychádza práve z uvedeného príkladu.

- **entanglovanie formovania**

$$E_F(\varrho_{AB}) = \lim_{N\to\infty} \frac{k_{min}}{N}$$

- **entanglovanie destilovania**

$$E_D(\varrho_{AB}) = \lim_{N\to\infty} \frac{k'_{max}}{N}$$

[8] o to vlastne pri tejto purifikácii ide

Pre čisté stavy sa tieto dve miery rovnajú a platí

$$\mathrm{E_F} = \mathrm{E_D} = \mathrm{E_v} = \mathrm{S}(\varrho_\mathrm{A}) = \mathrm{S}(\varrho_\mathrm{B}).$$

V tomto prípade tieto miery určujú aj počet stavov, ktoré môžu byt' pravdivo teleportované pomocou $|\psi\rangle_{\mathrm{AB}}$, t.j. počet úplne entanglovaných stavov, ktoré vieme lokálnymi operáciami a klasickou komunikáciou pripravit'.

Stále je otvorenou otázkou nájst' "dobrú" miera entanglovania, ktorá by bola mierou aj pre zmesi. Dobrým adeptom je

- **relatívna entropia entanglovania**

$$\mathrm{E_R}(\sigma) = \min_{\varrho \in D} \mathrm{S}(\sigma || \varrho)$$

kde D je množina všetkých neentanglovaných stavov. Dôkaz, že takto zadefinovaná miera spĺňa **E1-E4** je urobený v článku "Entanglement measures and purification procedures[9]" od V.Vedrala a M.B.Plenia.

[9] publikovaný vo Phys. Rev. A 57, p.1619 (1998/March)

Kapitola 4

KVANTOVÁ TEÓRIA INFORMÁCIE

4.1 ANALÓGIA S KLASICKOU TEÓRIOU

V tejto kapitole spojíme znalosti z predošlých kapitol a budeme sa zaoberať prenosom informácie cez kvantový komunikačný kanál. Zovšeobecníme pojmy z kapitoly 2 na ich kvantovú verziu.

V klasickej teórii sa písmeno kóduje do stavu klasického fyzikálneho systému, ale tento fakt nie je pri vykladaní samotnej teórie informácie v klasickom ponímaní nejak významný. Všetky javy, ktoré s týmto faktom súvisia sú zahrnuté pod pojem šum a týkajú sa iba samotného prenosu.

Situácia sa zmení, ak písmená zakódujeme do stavov kvantového systému. Vtedy vstúpi do hry kvantová teória, v ktorej stavy nemusia byť úplne rozlíšiteľné. To znamená, že kým v klasickom prípade je abeceda zadaná počtom písmen, tak v kvantovom prípade treba konkretizovať aj jednotlivé stavy prislúchajúce písmenám. Dôvod tejto rozdielnosti je v štruktúre stavov klasickej a kvantovej teórie. V kvantovej teórii existuje možnosť superpozície stavov. Táto vlastnosť nemá klasický analóg. Jej dôsledkom je, že v klasickej teórii sa dá zmes zapísať jednoznačne ako konvexný súčet čistých stavov, kdežto v kvantovej teórii je takýchto zápisov nekonečne veľa. Súbor kvantových stavov je úplne rozlíšiteľný, ak je ortogonálny, lebo vtedy existuje meranie, ktoré medzi týmito stavmi jednoznačne rozlišuje. Ortogonálna abeceda je teda ekvivalentná klasickej.

Ako príklad si uveďme binárnu abecedu, zloženú v klasickej teórii z písmen 0 a 1. V kvantovej teórii označme tieto písmená $|0\rangle$ a $|1\rangle$, ktoré reprezentujú dvojrozmerný Hilbertov priestor. Objekty z dvojrozmerného Hilbertovho priestoru nazývame v kvantovej teórii informácie *qubity*. Už samotný názov naznačuje, že ide o kvantový analóg klasických bitov, čo sú písmená z binárnej abecedy. Prenosom jedného z nich prenesieme maximálne práve jeden bit informácie.

Z kapitoly 2 vieme, že prepis z abecedy zdroja Z do vstupnej abecedy komunikačného kanála, ktorej písmená sú reprezentované stavmi, nazývame kódovaním. V kvantovej teórii tomuto prepisu zodpovedá procedúra *prípravy stavu*, ktorý prenáša písmeno v ňom zakódované. Kódovanie spolu zo zdrojom informácie určuje pravdepodobnostnú distribúciu π_i na týchto kvantových stavoch ϱ_i. Túto distribúciu budeme ďalej nazývať kódovaním, lebo pre daný informačný zdroj je ním jednoznačne určená. Ak máme d-rozmernú abecedu, tak Hilbertov priestor H, do stavov ktorého kódujeme, bude tiež d-rozmerný.

Kvantový komunikačný kanál sa od klasického líši tým, že prenáša písmená zakódované v stavoch kvantového systému a nie klasického systému. Počas prenosu sa takýto stav vyvíja podľa zákonov kvantovej teórie. Evolúcia v nej je opísaná superoperátorom (3.4)

$$\varrho_i \to \$(\varrho_i) = \sum_\mu A_\mu \varrho_i A_\mu^+.$$

V prípade, ak je superoperátor unitárny, t.j. superoperátor obsahuje v Krausovej reprezentácii iba jeden operátor A, tak takýto kvantový komunikačný kanál budeme nazývať *ideálny*. Ideálny komunikačný kanál zachováva štruktúru vstupných stavov v zmysle ich skalárneho súčinu a vzájomnej rozlíšiteľnosti, čo je v zhode s klasickým prípadom, kde pod ideálnym komunikačným kanálom rozumieme taký komunikačný kanál, ktorý písmenu výstupnej abecedy, priradí jednoznačne písmeno z abecedy vstupnej, t.j. je bezšumový.

Výstupnú abecedu kvantového komunikačného kanála tvoria stavy $\mathrm{W_i} = \$(\varrho_\mathrm{i})$ a analógom dekódovania je meranie na výstupných stavoch, ktoré je v kvantovej teórii opísané POVM, t.j. pozitívnymi operátormi X_j, pre ktoré $\sum_j X_\mathrm{j} = \mathbf{1}_\mathrm{H}$ (viď 3.1.2). Pravdepodobnosť jednotlivých výsledkov POVM merania na stave ϱ je určená vzťahom

$$\mathrm{Pr(j)} = \mathrm{Tr}(\varrho \mathrm{X_j}).$$

Teraz sa pozrime na množstvo klasickej informácie (2.1) meranej v bitoch prenesenej takýmto kvantovým kanálom. Podmienená pravdepodobnosť, ktorá definuje komunikačný kanál je v tomto prípade

$$\mathrm{p(i|j)} = \mathrm{Tr}(\mathrm{W_i X_j}),$$

takže informácia prenesená kvantovým komunikačným kanálom \$ v prípade kódovania π_i a dekódovania $\mathrm{X_j}$ je

$$\mathrm{I_1}(\pi, \mathrm{X}) = \sum_{\mathrm{i,j}} \pi_\mathrm{i} \mathrm{Tr}(\mathrm{W_i X_j}) \log \left(\frac{\mathrm{Tr}(\mathrm{W_i X_j})}{\sum_\mathrm{k} \pi_\mathrm{k} \mathrm{Tr}(\mathrm{W_j X_k})} \right). \tag{4.1}$$

Táto kvantita určuje priemerné množstvo klasických bitov prenesených poslaním jedného písmena.

Pozrime sa na prenos správy zloženej z n písmen. V takomto prípade máme Hilbertov priestor $\mathrm{H}^{\otimes \mathrm{n}} = \mathrm{H} \otimes \ldots \otimes \mathrm{H}$. V stavoch tohoto systému

$$\varrho_\mathbf{i} = \varrho_{\mathrm{i}_1} \otimes \ldots \otimes \varrho_{\mathrm{i}_\mathrm{n}}$$

sú zakódované správy $\mathbf{i}=(\mathrm{i}_1, \ldots, \mathrm{i}_\mathrm{n})$, kde $\mathrm{i_k} \in \mathrm{Z}$ a $\varrho_{\mathrm{i_k}}$ sú stavy priradené písmenám z abecedy zdroja Z, t.j. tvoria vstupnú abecedu kvantového komunikačného kanála. Správy $\mathbf{i}$ môžeme chápať ako prvky abecedy $\mathrm{Z^n}$, t.j. písmená, na ktorých opäť máme zadefinovanú pravdepodobnostnú distribúciu (kódovanie)

$$\pi_\mathbf{i} = \prod_{\mathrm{k}=1}^{\mathrm{n}} \pi_{i_k}.$$

Prenos celej správy $\mathbf{i}$ je opísaný superoperátorom na celom priestore $\mathrm{H}^{\otimes \mathrm{n}}$. Ak tento superoperátor spĺňa

$$\$(\varrho_{i_1} \otimes \ldots \otimes \varrho_{i_n}) = \$(\varrho_{i_1}) \otimes \ldots \otimes \$(\varrho_{i_n}),$$

tak, analogicky s klasickým komunikačným kanálom, takýto kvantový komunikačný kanál nazveme *bezpamäťový*. Znamená to že stav na konci prenosu nebude v entanglovanom stave, t.j. komunikačný kanál skutočne pôsobí na každé písmeno zvlášť (t.j. lokálne).

Dekódovanie v tomto prípade je určené POVM meraním na celom priestore $\mathrm{H}^{\otimes \mathrm{n}}$. Takéto meranie môže byť vo všeobecnosti optimálnejšie v zmysle lepšieho určenia správy $\mathbf{i}$ z tohto globálneho merania, než osobitnými meraniami na každom písmene správy.

Informácia pri prenose správy dĺžky n je daná vzťahom analogickým ako (4.1)

$$\mathrm{I_n}(\pi, \mathrm{X}) = \sum_{\mathbf{i,j}} \pi_\mathbf{i} \mathrm{Tr}(\mathrm{W_i X_j}) \log \left(\frac{\mathrm{Tr}(\mathrm{W_i X_j})}{\sum_\mathbf{k} \pi_\mathbf{k} \mathrm{Tr}(\mathrm{W_j X_k})} \right), \tag{4.2}$$

kde π je kódovanie na vstupných správach a X označuje POVM meranie na výstupných stavoch $\mathrm{W_i}$ kvantového komunikačného kanála. Tieto stavy predstavujú správy zložené z n písmen, a ak dimZ=d, tak sú stavmi z $\mathrm{d^n}$-rozmerného Hilbertovho priestoru.

4.2 KVANTOVÉ HUSTÉ KÓDOVANIE

Kvantové husté kódovanie je príkladom využitia zvláštností kvantovej teórie. Využijeme informáciu skrytú v kvantových koreláciach medzi vzdialenými systémami, t.j. existenciu entanglovaných stavov, na prenos klasickej informácie.

Informáciu sa pokúsime prenášať nasledovnou procedúrou. Nech Alica a Bob[1] sú spojení kvantovým komunikačným kanálom a zdieľajú spolu dve dvojhladinové častice (qubity). Alica aplikuje na svoj qubit jednu zo štyroch ľubovoľných, ale fixných transformácii a takto pripravený qubit pošle kvantovým komunikačným kanálom Bobovi. Výberom transformácie Alica určuje posielané písmeno. Bob prijme qubit poslaný od Alici a prevedie meranie na obidvoch zdieľaných qubitoch. Z výsledku merania sa Bob pokúša určiť poslané písmeno. Túto procedúru nazývame *hustým kódovaním.*

V prípade, ak Bob robí merania iba na prijatom qubite, tak vieme, že maximum prenesenej informácie je jeden bit. Otázkou je ako sa zmení množstvo prenesenej informácie jedným qubitom, ak Alica a Bob využijú fakt, že qubit poslaný od Alici môže byť v entanglovanom stave s qubitom Bobovým. Hilbertov priestor dvoch qubitov je štvorrozmerný, t.j. abeceda môže byť tvorená štyrmi ortogonálnymi stavmi a prenesená informácia má v takomto prípade maximum $\log_2 4 = 2$ bity. Otázkou je, či Alica môže lokálnymi unitárnymi operáciami na svovom qubite pripraviť štyri ortogonálne stavy, ktoré by tvorili výstupnú abecedu.

Prípad, ak zdieľaný stav je ľubovoľný, je predmetom tejto diplomovej práce. Teraz si uvedieme špeciálny prípad stavu

$$|\psi\rangle_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B),$$

ktorý je maximálne entanglovaný. Budeme predpokladať, že kvantový komunikačný kanál je triviálny, t.j. nijako nepôsobí na vstupné stavy. Uvedieme príklad voľby Aliciných lokálnych unitárnych operácií:

$$\mathbf{1}_{\mathrm{A}}(\text{nulová rotácia}), \text{t.j.} \phi^+ \to \phi^+$$
$$\sigma_1(180^o \text{ rotácie okolo x}), \text{t.j.} \phi^+ \to \psi^+$$
$$\sigma_2(180^o \text{ rotácie okolo y}), \text{t.j.} \phi^+ \to \psi^-$$
$$\sigma_3(180^o \text{ rotácie okolo z}), \text{t.j.} \phi^+ \to \phi^-,$$

kde

$$|\phi^{\pm}\rangle_{\mathrm{AC}} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$$
$$|\psi^{\pm}\rangle_{\mathrm{AC}} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle), \tag{4.3}$$

tvoria ortonormálny systém, a teda bázu spoločného Hilbertovho priestoru. To znamená, že existuje ortogonálne meranie (*Bellove meranie*), ktoré úplne rozlišuje medzi týmito stavmi, ktoré tvoria ortogonálnu abecedu. Bob prevedením Bellovho merania získa úplnú informáciu o poslanom písmene, t.j. dva bity informácie.

Môžeme povedať, že poslaním jedného qubitu sa preniesli dva bity klasickej informácie. Samozrejme, že v skutočnosti sme zamlčali počiatočné rozposlanie entanglovaných qubitov z nejakého zdroja, jeden Alici a druhý Bobovi. Takže qubity v skutočnosti spolu prejdú dvakrát vzdialenosť medzi Alicou a Bobom. Napríklad môže byť zdrojom Alica a posielať priamo dva entanglované qubity, pričom iba na jednom urobila dané lokálne operácie.

Môže to byť aj tak, že Alica a Bob boli v minulosti spolu a vtedy previazali svoje qubity, t.j qubity sa neprenášali žiadnym komunikačným kanálom. A práve o takomto prípade hovoríme, t.j.

[1] štandartní experimentátori v kvantovej teórii informácie

keď sa rozposlanie qubitov nedialo prostredníctvom nášho kvantového komunikačného kanála, a v tomto zmysle hovoríme, že poslaním jedného qubitu cez komunikačný kanál prenášame dva bity klasickej informácie.

Alica a Bob sa v tomto prípade vôbec nemusia obávať odpočúvania. Qubit posielaný komunikačným kanálom sa totiž pri každej voľbe písmena nachádza v maximálnej zmesi $\frac{1}{2}\mathbf{1}$. Potencionálny narušiteľ by meraním na tomto qubite nezistil nič o prenášanom písmene. Môžeme povedať, že Bobov qubit slúži ako kľúč k získaniu informácie. Opísaný príklad sa zvykne nazývať aj *superhustým kódovaním.*

4.3 DEFINÍCIA KAPACITY

Kapacitu kvantového komunikačného kanála zadefinujeme podobne ako v klasickej teórii (2.2) ako stredný počet prenesených bitov na jedno prenesené písmeno. V podstate ide opäť o stredovanie prenesenej informácie cez dĺžky správ. Teda

$$\mathrm{C} = \lim_{\mathrm{n}\to\infty} \frac{1}{\mathrm{n}} \sup_{\pi,\mathrm{X}} \mathrm{I_n}(\pi, \mathrm{X}), \tag{4.4}$$

kde $\mathrm{I_n}$ je množstvo prenesenej informácie pri posielaní správy dĺžky n (4.2). Suprémum je robené cez všetky možné POVM merania a všetky možné kódovania. Pre bezpamäťový komunikačný kanál je $\mathrm{I_n} = \mathrm{nI_1}$ a pre kapacitu platí

$$\mathrm{C} = \sup_{\pi,\mathrm{X}} \mathrm{I_1}(\pi, \mathrm{X}) \tag{4.5}$$

Počítať kapacitu priamo z tejto definície je dosť zložité. Preto si uvedieme jednoduchší vzťah

$$\mathrm{C} = \max_{\pi} \left[\mathrm{S}(\sum \pi_\mathrm{i} \mathrm{W_i}) - \sum \pi_\mathrm{i} \mathrm{S}(\mathrm{W_i}) \right], \tag{4.6}$$

kde stavy $\mathrm{W_i}$ tvoria výstupnú abecedu.

V tomto vzťahu už vôbec netreba uvažovať POVM merania na výstupných stavoch. Samotný dôkaz ekvivalencie týchto dvoch vyjadrení pre kapacitu kvantového komunikačného kanála bol podaný A.S.Holevom v [6]. Dovtedy bol tento výraz uvádzaný iba ako horné ohraničenie pre kapacitu. Holevo dokázal aj opačnú nerovnosť.

Dôkaz opačnej nerovnocti je založený na tzv. *kódovacej teoréme.* Táto teoréma hovorí, že pravdepodobnosť chyby pri prenose cez komunikačný kanál rastie s počtom prenesených písmen n ako $2^{-\mathrm{nC}+\delta}$, kde C je práve kapacita komunikačného kanála definovaná cez Shannonovu informáciu. Holevo ukázal, že pre bezpamäťový komunikačný kanál vzťah (4.6) spĺňa túto teorému.

Niektorí autori berú (4.6) za definičný vzťah pre kapacitu a my budeme v ďalšom samozrejme tiež pracovať s týmto vyjadrením pre kapacitu kvantového komunikačného kanála.

Kapitola 5

KAPACITA BINÁRNYCH KVANTOVÝCH KOMUNIKAČNÝCH KANÁLOV

5.1 KAPACITA IDEÁLNEHO KVANTOVÉHO KOMUNIKAČNÉHO KANÁLA

5.1.1 Prípad všeobecnej abecedy

Teraz spočítame kapacitu ideálneho kvantového komunikačného kanála pre ľubovoľnú binárnu abecedu. Vieme, že všeobecný stav dvojdimenzionálneho Hilbertovho priestoru sa dá zapísať v nasledovnom tvare

$$\varrho(\vec{\mathrm{m}}) = \frac{1}{2}(\mathbf{1} + \vec{\mathrm{m}}.\vec{\sigma}).$$

Binárna abeceda bude teda jednoznačne určená dvomi vektormi $\vec{\mathrm{m}}$, $\vec{\mathrm{n}}$, ktorých norma nie je väčšia ako jedna. Kapacita (4.6) potom bude rovná

$$\mathrm{C} = \max_{\pi_1}[\mathrm{S}(\varrho) - \pi_1 \mathrm{S}(\varrho(\vec{\mathrm{m}})) - \pi_2 \mathrm{S}(\varrho(\vec{\mathrm{n}}))],$$

kde $\pi_2 = 1 - \pi_1$ a $\varrho = \pi_1\varrho(\vec{\mathrm{m}}) + \pi_2\varrho(\vec{\mathrm{n}})$.

Vlastné hodnoty matice hustoty $\varrho(\vec{\mathrm{m}})$ sú $\lambda_\pm = (1 \pm |\vec{\mathrm{m}}|)/2$ a entropia takéhoto stavu je potom

$$\mathrm{S}(|\vec{\mathrm{m}}|) = 1 - \frac{1}{2}[(1 + |\vec{\mathrm{m}}|)\log(1 + |\vec{\mathrm{m}}|) + (1 - |\vec{\mathrm{m}}|)\log(1 - |\vec{\mathrm{m}}|)], \tag{5.1}$$

kde sme pre jednoduchosť zápisu $\mathrm{S}(\varrho(\vec{\mathrm{m}}))$ označili ako $\mathrm{S}(|\vec{\mathrm{m}}|)$. Ďalej prepíšme maticu hustoty ϱ do tvaru

$$\varrho = \pi_1\varrho(\vec{m}) + \pi_2\varrho(\vec{n}) = \pi_1\frac{1}{2}(\mathbf{1} + \vec{\mathrm{m}}.\vec{\sigma}) + \pi_2\frac{1}{2}(\mathbf{1} + \vec{\mathrm{n}}.\vec{\sigma}) =$$

$$= \frac{1}{2}(\mathbf{1} + (\pi_1\vec{\mathrm{m}} + \pi_2\vec{\mathrm{n}}).\vec{\sigma}),$$

odkiaľ vidno vektor, ktorý nám stav ϱ určuje.

V novom označení môžeme teraz kapacitu prepísať ako

$$\mathrm{C} = \max_{\pi_1}[\mathrm{S}(|\pi_1\vec{\mathrm{m}} + \pi_2\vec{\mathrm{n}}|) - \pi_1 \mathrm{S}(|\vec{\mathrm{m}}|) - \pi_2 \mathrm{S}(|\vec{\mathrm{n}}|)]. \tag{5.2}$$

Ostáva už iba určit' optimálne kódovanie, t.j. optimálnu hodnotu π_1. Zderivovaním 5.2 podľa π_1 dostaneme

$$\frac{\partial \mathrm{C}}{\partial \pi} = \mathrm{S}(|\vec{\mathrm{n}}|) - \mathrm{S}(|\vec{\mathrm{m}}|) - \frac{1}{2}\left\{\frac{\pi(\mathrm{m}^2+\mathrm{n}^2-2\mathrm{mn}\cos\phi)+\mathrm{mn}\cos\phi-\mathrm{n}^2}{|\pi\vec{\mathrm{m}}+(1-\pi)\vec{\mathrm{n}}|}\log\frac{1+|\pi\vec{\mathrm{m}}+(1-\pi)\vec{\mathrm{n}}|}{1-|\pi\vec{\mathrm{m}}+(1-\pi)\vec{\mathrm{n}}|}\right\},$$

kde sme položili $\pi_1 = \pi$, $|\vec{\mathrm{m}}| = \mathrm{m}$, $|\vec{\mathrm{n}}| = \mathrm{n}$ a ϕ je uhol, ktorý zvierajú vektory $\vec{\mathrm{m}}$ a $\vec{\mathrm{n}}$. Pre konkrétne dva stavy určené vektormi $\vec{\mathrm{m}}$ a $\vec{\mathrm{n}}$ by sme vedeli optimálne kódovanie π nájst'. Vo všeobecnosti to však určit' nevieme, lebo ide o transcendentnú rovnicu.

5.1.2 Špeciálne binárne abecedy

Uvažujme, že Alica pripravuje stavy vstupnej abecedy unitárnymi operáciami pôsobiacimi na nejaký fixný stav, t.j. stavy, ktoré vstupujú do komunikačného kanála majú rovnakú entropiu. Keďže entropia je v prípade stavov z dvojrozmerného Hilbertovho priestoru určená jednoznačne veľkost'ou vektora, ktorý tento stav zadáva, tak pre takto generované písmená $|\vec{\mathrm{m}}| = |\vec{\mathrm{n}}| = \mathrm{m}$. Ak si uvedomíme, že v tomto prípade platí

$$|\pi\vec{\mathrm{m}} + (1-\pi)\vec{\mathrm{n}}| = \mathrm{m}\sqrt{1+2(1-\cos\phi)(\pi^2-\pi)},$$

tak podmienka extrému kapacity, t.j. $\frac{\partial \mathrm{C}}{\partial \pi} = 0$, prejde na rovnicu

$$-\frac{1}{2}\frac{\mathrm{m}(2\pi-1)(1-\cos\phi)}{\sqrt{1+2(1-\cos\phi)(\pi^2-\pi)}}\log\frac{1+\mathrm{m}\sqrt{1+2(1-\cos\phi)(\pi^2-\pi)}}{1-\mathrm{m}\sqrt{1+2(1-\cos\phi)(\pi^2-\pi)}} = 0,$$

čo nastáva v prípade[1], ak $\pi = 1/2$. Ak m=0, tak kapacita je nulová, lebo v tomto prípade je abeceda tvorená úplnou zmesou, t.j. iba jedným písmenom. V prípade $\cos\phi = 1$ to znamená, že uhol medzi vektormi je nulový, t.j. ide o tie isté vektory, a teda aj stavy, ktoré určujú, sú rovnaké. Pre kapacitu opäť platí C=0.

Kapacita sa dá v tomto prípade ($|\vec{\mathrm{m}}| = |\vec{\mathrm{n}}| = \mathrm{m}$) s uvážením $\pi = 1/2$ vyjadrit' nasledovne

$$\mathrm{C} = \mathrm{S}(\mathrm{m}\sqrt{(1+\cos\phi)/2}) - \mathrm{S}(\mathrm{m}). \tag{5.3}$$

Pre konkrétne m je kapacita iba funkciou uhlu ϕ medzi vektormi určujúcimi stavy. Minimálna hodnota kapacity je pre uhol $\phi = 0$, kedy $\mathrm{C} = \mathrm{S}(\mathrm{m}) - \mathrm{S}(\mathrm{m}) = 0$. Maximum kapacita nadobúda pre hodnotu uhla $\phi = 180°$, kedy je $\cos\phi = -1$, t.j.

$$\mathrm{C} = \mathrm{S}(0) - \mathrm{S}(\mathrm{m}) = \log 2 - \mathrm{S}(\mathrm{m}) = 1 - \mathrm{S}(\mathrm{m}),$$

kde S(m) je dané vzt'ahom (5.1).

Ak položíme $|\alpha|^2 = (1+\mathrm{m})/2$ a $|\beta|^2 = (1-\mathrm{m})/2$, tak vstupná abeceda je tvorená stavmi, ktoré majú vo vhodnej báze tvar

$$\begin{aligned}\mathrm{W}_1 &= |\alpha|^2|0\rangle\langle 0| + |\beta|^2|1\rangle\langle 1| \\ \mathrm{W}_2 &= |\beta|^2|0\rangle\langle 0| + |\alpha|^2|1\rangle\langle 1|\end{aligned} \tag{5.4}$$

Kapacita pri takejto vol'be abecedy je potom

$$\mathrm{C} = 1 + |\alpha|^2\log|\alpha|^2 + |\beta|^2\log|\beta|^2. \tag{5.5}$$

V limite pre čisté stavy ($\mathrm{m} = 1$, t.j. $\alpha = 1$) abecedu tvoria ortogonálne stavy a C=1.

[1] v prípade, že je pod odmocninou nula, tak síce dostávame $\log 1 = 0$, ale táto odmocnina nám vystupuje aj v menovateli pred logaritmom

5.2 PAULIHO KVANTOVÝ KOMUNIKAČNÝ KANÁL

Začnime definíciou Pauliho kvantového komunikačného kanála na vstupný stav ϱ_i

$$\varrho_i \to \varrho_i' = (1-p)\varrho_i + p_x\sigma_x\varrho_i\sigma_x + p_y\sigma_y\varrho_i\sigma_y + p_z\sigma_z\varrho_i\sigma_z, \tag{5.6}$$

kde $p = p_x + p_y + p_z$.

Najprv si ukážme, že tento komunikačný kanál je skutočne superoperátorom. Zo zápisu (5.6) ľahko vidno štyri operátory vystupujúce v Krausovej reprezentácii, a síce $\sqrt{1-p}\mathbf{1}, \sqrt{p_x}\sigma_x, \sqrt{p_y}\sigma_y, \sqrt{p_z}\sigma_z$. Využitím $\sigma_i^+\sigma_i = \sigma_i^2 = \mathbf{1}$ pre i=x,y,z, overíme Krausovu normalizačnú podmienku, t.j.

$$\sum_\mu A_\mu^+ A_\mu = (1 - p + p_x + p_y + p_z)\mathbf{1} = \mathbf{1}.$$

Vidno teda, že Pauliho kanál je superoperátorom.

Pôsobenia jednotlivých Krausových operátorov, t.j. σ-matíc, interpretujeme ako chyby, ktoré počas prenosu nastávajú.

- **otočenie bitu**

$$\sigma_x \ : \quad \begin{array}{l} |0\rangle \to |1\rangle \\ |1\rangle \to |0\rangle \end{array}$$

- **zmena fázy**

$$\sigma_z \ : \quad \begin{array}{l} |0\rangle \to |0\rangle \\ |1\rangle \to -|1\rangle \end{array}$$

- **kombinácia obidvoch**

$$\sigma_y \ : \quad \begin{array}{l} |0\rangle \to i|1\rangle \\ |1\rangle \to -i|0\rangle \end{array}$$

Jeho pôsobenie na vstupný stav v tvare

$$\varrho(\vec{m}) = \frac{1}{2}(\mathbf{1} + \vec{m}.\vec{\sigma})$$

vyzerá nasledovne

$$\varrho' = (1-p)\frac{1}{2}(\mathbf{1} + \vec{m}.\vec{\sigma}) + \sum_\mu p_\mu\sigma_\mu\frac{1}{2}(\mathbf{1} + \vec{m}.\vec{\sigma})\sigma_\mu =$$

$$= \frac{1}{2}(\mathbf{1} + \vec{m'}.\vec{\sigma}),$$

kde

$$\vec{m'} = ((1-2(p_y+p_z))m_x, (1-2(p_x+p_z))m_y, (1-2(p_x+p_y))m_z) \tag{5.7}$$

Vidno, že pre $p_x = p_y = p_z = 1/4$, dostávame pre ľubovoľný vstupný stav na konci komunikačného kanála úplnú zmes $\frac{1}{2}\mathbf{1}$, čo znamená, že nemáme žiadnu šancu určiť stav na vstupe, a teda neprenesieme v tomto prípade žiadnu informáciu. V prípade $p_x = p_y = p_z = p/3 = q$ takýto komunikačný kanál nazývame *depolarizačný* a $\vec{m'} = (1-4q)\vec{m}$.

Pri výpočte kapacity môžeme použiť výsledky z predchádzajúcej časti. Ak na vstupe máme dva stavy určené vektormi $\vec{m}$, $\vec{n}$, tak na výstupe Pauliho kanála máme stavy $\vec{m'}$, $\vec{n'}$ určené rovnicou (5.7). Ak Alica kóduje unitárnymi operáciami, t.j. generuje stavy s rovnakou entropiou, tak stavy na konci vo všeobecnosti už rovnakú entropiu (5.1) mať nemusia. Práve iba v prípade depolarizačného kanála bude entropia stavov na výstupe rovnaká, aj keď menšia ako na začiatku. Kapacitu Pauliho kanála v takomto prípade máme určenú vzťahom (5.3).

Kapitola 6

POUŽITIE NEÚPLNE ENTANGLOVANÝCH STAVOV PRI KOMUNIKÁCII

6.1 KAPACITA PRE NEÚPLNE ENTANGLOVANÉ ČISTÉ STAVY PRI HUSTOM KÓDOVANÍ

Situácia sa trochu skomplikuje v prípade, ak qubit vstupujúci do kvantového komunikačného kanála je v entanglovanom stave so systémom prijímateľa, t.j. máme situáciu hustého kódovania opísaného v kapitole 4. Komunikačným kanálom sa prenáša iba jeden qubit, ktorý je z dvojrozmerného kvantového systému, ale vstupná aj výstupná abeceda sú štvorrozmerné Hilbertove priestory. Doteraz komunikačný kanál prenášal každé písmeno zvlášť. V tomto prípade akoby prenášal jedným písmenom písmená dve.

Kvantový komunikačný kanál, ktorého kapacita nás zaujíma, pôsobí iba na jeden qubit, t.j. jeho pôsobenie je lokálne a v prípade hustého kódovania, opísaného v kapitole 4, aj ideálne. Vieme, že pri tomto prenose je prenášaný qubit v maximálnej zmesi, a teda unitárna transformácia jeho stav nijako nemení. Takýto pohľad je ale nesprávny, lebo neberie do úvahy kvantové korelácie (entanglovanie) a práve v nich je skrytá prenášaná informácia. Ak by sme do výrazu pre kapacitu dosadili výstupné stavy prenášaného qubitu, ktoré sú maximálnymi zmesami, tak nepreniesieme žiadnu informáciu. Tento postup zodpovedá Bobovmu meraniu iba na jednom qubite. Nás ale nezaujíma stav jedného qubitu, ale stav oboch qubitov. Takže za výstupnú abecedu kanála budeme brať štyri výsledky Bellových meraní.

Kapacitu teda budeme počítať pre výstupné Bellove stavy $\phi^{\pm}, \psi^{\pm}$. Ak uvážime, že entropia čistých stavov je nulová a optimálne kódovanie je $\pi_{\mathrm{i}} = \frac{1}{4}$, tak

$$\mathrm{C} = \mathrm{S}(\frac{1}{4} \sum_{\mathrm{Bell.stavy}} |\psi_{\mathrm{i}}\rangle\langle\psi_{\mathrm{i}}|) = \mathrm{S}(\frac{1}{4}\mathbf{1}) = \log_2 4 = 2.$$

Tento výsledok sa zhoduje s množstvom prenesenej informácie 2 bitov získanej v 4.2. Poznamenajme, že kapacita je priemerné množstvo prenesenej informácie na jedno prenesené písmeno a teda samotná informácia ohraničuje kapacitu zdola. V tomto prípade je kapacita vypočítateľná aj z prvej definície, pričom optimálne meranie je práve Bellove meranie a optimálne kódovanie je $\pi_{\mathrm{i}} = 1/4$. V tomto prípade jedno binárne písmeno (jeden qubit) prenieslo dva bity informácie, čo už bolo diskutované v spomínanej kapitole 4.

Teraz sa pozrieme najprv na prípad nie úplne entanglovaných čistých stavov. Zo Schmidtovej dekompozície vyplýva, že čistý stav dvojzložkového systému, ktorého podsystémy sú dvojdimen-

zionálne Hilbertove priestory, sa dá zapísat' v nasledovnom tvare

$$|\psi_0\rangle_{\mathrm{AB}} = \alpha|0\rangle_A \otimes |\phi_0\rangle_B + \beta|1\rangle_A \otimes |\phi_1\rangle_B,$$

kde $\langle\phi_1|\phi_0\rangle = 0$ a $|\alpha|^2 + |\beta|^2 = 1$. Pre jednoduchost' budeme v d'al'šom označovat'

$$|0\rangle_{\mathrm{B}} = |\phi_0\rangle_{\mathrm{B}}$$

$$|1\rangle_{\mathrm{B}} = |\phi_1\rangle_{\mathrm{B}}$$

Otázkou je, či opät' existujú lokálne unitárne transformácie na A (Alica), ktoré by dávali štyri rovnako rozlíšitel'né stavy v zmysle prekryvu (E.1), ktoré by v najlepšom mohli byt' kolmé. Dôvodom, prečo sa zaujímame o takéto stavy, je intuitívny predpoklad, že abeceda zložená z takýchto štyroch stavov je najlepšie rozlíšitel'ná, a teda pomocou nej sme schopný preniest' najviac informácie cez ideálny kvantový komunikačný kanál.

Všeobecná lokálna unitárna transformácia na dvojdimenzionálnom priestore je vyjadrená maticou zo štvorparametrickej grupy U(2) a má tvar

$$\mathrm{U_i} = \mathrm{e}^{\mathrm{ik_i}}(\cos\psi_{\mathrm{i}}\mathbf{1} + \mathrm{i}\sin\psi_{\mathrm{i}}(\vec{\mathrm{n_i}}.\vec{\sigma})), \tag{6.1}$$

kde $\vec{\mathrm{n_i}} = (\sin\theta_{\mathrm{i}}\cos\phi_{\mathrm{i}}, \sin\theta_{\mathrm{i}}\sin\phi_{\mathrm{i}}, \cos\theta_{\mathrm{i}})$ je jednotkový vektor okolo ktorého rotujeme o uhol ψ_{i}[1].

Úlohou je nájst' štyri lokálne unitárne transformácie $\mathrm{U_i}\otimes\mathbf{1}$, ktorými zo stavu $|\psi_0\rangle = \alpha|00\rangle + \beta|11\rangle$ dostaneme štyri stavy $|\psi_{\mathrm{i}}\rangle = \mathrm{U_i}\otimes\mathbf{1}|\psi_{\mathbf{0}}\rangle$, pre ktoré platí

$$|\langle\psi_{\mathrm{i}}|\psi_j\rangle|^2 = \text{minimum} =$$

$$= |\langle\psi_0|\mathrm{U_i^+U_j}|\psi_0\rangle|^2 = |\ |\alpha|^2\langle 0|\mathrm{U_i^+U_j}|0\rangle + |\beta|^2\langle 1|\mathrm{U_i^+U_j}|1\rangle|^2 =$$

$$= |\ |\alpha|^2(\mathrm{W_{ij}})_{00} + |\beta|^2|^2(\mathrm{W_{ij}})_{11}|^2, \tag{6.2}$$

kde

$$\mathrm{W_{ij}} = \mathrm{U_i^+U_j},$$

čo pri neuvažovaní fázového faktoru $e^{\mathrm{ik_i}}$ v (6.1) dáva

$$\mathrm{W_{ij}} = \mathbf{1}(\cos\psi_{\mathrm{i}}\cos\psi_{\mathrm{j}} + \vec{\mathrm{n_i}}.\vec{\mathrm{n_j}}\sin\psi_{\mathbf{i}}\sin\psi_{\mathbf{j}}) + i\vec{\sigma}.(\sin\psi_{\mathrm{i}}\sin\psi_{\mathbf{j}}(\vec{\mathrm{n_i}}\times\vec{\mathrm{n_j}}) - \sin\psi_{\mathbf{i}}\cos\psi_{\mathbf{j}}\vec{\mathrm{n_i}} + \sin\psi_{\mathbf{j}}\cos\psi_{\mathbf{i}}\vec{\mathrm{n_j}}),$$

kde sme využili vzt'ah

$$\sigma_{\mathrm{i}}\sigma_{\mathrm{j}} = \delta_{\mathrm{ij}}\mathbf{1} + i\varepsilon_{\mathrm{ijk}}\sigma_{\mathrm{k}}.$$

Z (6.2) vidno, že nám stačia iba diagonálne elementy $\mathrm{W_{ij}}$ a teda sa zo σ-matíc uplatní iba σ_3, lebo iba tá má nenulové diagonálne elementy. Takisto nám stačí vediet' len z-ové zložky vektorov $\vec{\mathrm{n_i}}$, $\vec{\mathrm{n_j}}$, $(\vec{\mathrm{n_i}}\times\vec{\mathrm{n_j}})$.

Pri označení

$$a_{ij} = \cos\psi_{\mathrm{i}}\cos\psi_{\mathrm{j}} + \vec{\mathrm{n_i}}.\vec{\mathrm{n_j}}\sin\psi_i\sin\psi_j$$

$$b_{ij} = \sin\psi_{\mathrm{i}}\sin\psi_j(\vec{\mathrm{n_i}}\times\vec{\mathrm{n_j}})_{\mathrm{z}} - \sin\psi_i\cos\psi_j(\vec{\mathrm{n_i}})_z + \sin\psi_j\cos\psi_i(\vec{\mathrm{n_j}})_z$$

kde

$$\vec{\mathrm{n_i}}\vec{\mathrm{n_j}} = \cos\theta_i\cos\theta_j + \sin\theta_i\sin\theta_j\cos(\phi_j - \phi_i)$$

a

$$(\vec{\mathrm{n_i}}\times\vec{\mathrm{n_j}})_{\mathrm{z}} = \sin\theta_{\mathrm{i}}\sin\theta_j\sin(\phi_{\mathrm{j}} - \phi_{\mathrm{i}})$$

[1] ψ označujeme aj stav, aj uhol, ale z kontextu by malo byt' vždy jasné, o ktorý význam ide

platí

$$(\mathrm{W_{ij}})_{00} = a_{\mathrm{ij}} + \mathrm{i}b_{\mathrm{ij}}$$

$$(\mathrm{W_{ij}})_{11} = a_{\mathrm{ij}} - \mathrm{i}b_{\mathrm{ij}}.$$

Potom z (6.2) dostaneme

$$|\ |\alpha|^2(a_{\mathrm{ij}} + \mathrm{i}b_{\mathrm{ij}}) + |\beta|^2(a_{\mathrm{ij}} - \mathrm{i}b_{\mathrm{ij}})|^2 = (a_{\mathrm{ij}} - \mathrm{i}b_{\mathrm{ij}}(|\alpha|^2 - |\beta|^2))(a_{\mathrm{ij}} + \mathrm{i}b_{\mathrm{ij}}(|\alpha|^2 - |\beta|^2))$$

t.j.

$$|\langle\psi_{\mathrm{i}}|\psi_{\mathrm{j}}\rangle|^2 = a_{\mathrm{ij}}^2 + b_{\mathrm{ij}}^2(|\alpha|^2 - |\beta|^2)^2 = \mathrm{minimum} \tag{6.3}$$

Jednu z transformácií vyberieme ako triviálnu, t.j. $\mathrm{U_0} = \mathbf{1_A}$. Po jej aplikovaní stav nijako nezmeníme a podmienka pre minimum medzi pôvodným stavom a stavmi získanými operáciami pre i=1, 2, 3 má tvar

$$|\langle\psi_0|\psi_{\mathrm{i}}\rangle|^2 = \cos^2\psi_{\mathrm{i}} + \sin^2\psi_{\mathrm{i}}\cos^2\theta_{\mathrm{i}}(|\alpha|^2 - |\beta|^2)^2 = \mathrm{minimum} \tag{6.4}$$

Využijeme teraz výsledok pre Bellov stav $|\phi^+\rangle$, ktorý sme opisovaliv časti 4.2 ako príklad superhustého kódovania, pri ktorom minimum=0. Keďže chceme, aby naše transformácie pre $\alpha = \beta$ dávali tiež minimum=0, tak nutne

$$\cos^2\psi_{\mathrm{i}} = 0$$

$$a_{\mathrm{ij}} = 0$$

t.j. $\psi_{\mathrm{i}} = \pm\frac{\pi}{2}$ odkiaľ vyplýva, že $|\sin\psi_{\mathrm{i}}| = 1$. Ak toto dosadíme do a_{ij}, tak nutne $\vec{\mathrm{n}_{\mathrm{i}}}.\vec{\mathrm{n}_{\mathrm{j}}} = 0$, t.j. smery okolo ktorách rotujeme o uhol $\psi_{\mathrm{i}} = \pm\frac{\pi}{2}$ sú na seba kolmé. Zhrňme si podmienky, ktoré musia byť splnené, ak platí limita Bellových stavov

$$\psi_{\mathrm{i}} = \pm\frac{\pi}{2} \tag{6.5}$$

$$\vec{\mathrm{n}_{\mathrm{i}}}.\vec{\mathrm{n}_{\mathrm{j}}} = \delta_{\mathrm{ij}} \tag{6.6}$$

Zapíšme si ako vyzerajú rovnice (6.3-6.4) po dosadení týchto podmienok. Najprv si vyjadrime b_{ij}

$$b_{\mathrm{ij}} = \sin\psi_{\mathrm{i}}\sin\psi_j(\vec{\mathrm{n}_{\mathrm{i}}} \times \vec{\mathrm{n}_{\mathrm{j}}})_{\mathrm{z}},$$

kde ostatné výrazy sú nulové, lebo obsahujú výraz $\cos\psi_i = 0$ a označme

$$\triangle^2 = (|\alpha|^2 - |\beta|^2)^2.$$

Potom tieto rovnice majú nasledujúci tvar

$$\mathrm{minimum} = \sin^2\psi_{\mathrm{i}}\sin^2\psi_{\mathrm{j}}(\vec{\mathrm{n}_{\mathrm{i}}} \times \vec{\mathrm{n}_{\mathrm{j}}})_{\mathrm{z}}^2\triangle^2 = (\vec{\mathrm{n}_{\mathrm{i}}} \times \vec{\mathrm{n}_{\mathrm{j}}})_{\mathrm{z}}^2\triangle^2 \tag{6.7}$$

$$\mathrm{minimum} = \cos^2\theta_{\mathrm{i}}\triangle^2. \tag{6.8}$$

Predpokladajme, že transformácie $\mathrm{U_i}$ môžu závisieť aj od α a β. Ak porovnáme rovnice (6.7) a (6.8), tak dostaneme rovnicu, v ktorej nám α a β nevystupujú

$$\cos^2\theta_i = (\vec{\mathrm{n}_{\mathrm{i}}} \times \vec{\mathrm{n}_{\mathrm{j}}})_{\mathrm{z}}^2 = \sin^2\theta_{\mathrm{i}}\sin^2\theta_j\sin^2(\phi_{\mathrm{j}} - \phi_{\mathrm{i}}). \tag{6.9}$$

Označme $\cos^2\theta_i = \mathrm{F}^2$, lebo $\cos^2\theta_i$ sú z (6.8) pre všetky i rovnaké. Potom dostávame formálne sústavu dvoch rovníc

$$(1 - \mathrm{F}^2)^2\sin^2(\phi_{\mathrm{j}} - \phi_{\mathrm{i}}) = \mathrm{F}^2 \tag{6.10}$$

$$\vec{n_i}.\vec{n_j} = (1 - F^2)\cos(\phi_j - \phi_i) \pm F^2 = 0, \tag{6.11}$$

kde $\pm$ je znamienko súčinu $\cos\theta_i \cos\theta_j$, pričom výraz $\sin\theta_i \sin\theta_j$ má vždy kladné znamienko, lebo $\theta_i \in (0, \pi)$.

Umocnením rovnice (6.11) a dosadením

$$\cos^2(\phi_j - \phi_i) = \frac{F^4}{(1 - F^2)^2}$$

do rovnice (6.10) dostaneme rovnicu

$$(1 - F^2)^2(1 - \frac{F^4}{(1 - F^2)^2}) = F^2, \tag{6.12}$$

ktorej riešením je

$$F^2 = \frac{1}{3}.$$

Zhrňme výsledky

$$\cos^2\theta_j = \frac{1}{3}$$

$$\cos^2\psi_j = 0$$

$$\cos(\phi_j - \phi_i) = \frac{\mp F^2}{1 - F^2} = \mp\frac{1}{2}$$

Voľba ψ_i je ľubovoľná z možností (6.5), lebo od tejto hodnoty vôbec výsledok nezávisí. Riešenie pre θ_i a ϕ_i sú spolu zviazané, lebo $\mp = \mathrm{Sgn}(\cos\theta_i \cos\theta_j)$. Pôvod tejto väzby je v (6.6).

Vyberme $\psi_i = \pi/2$, t.j. $\sin\psi_i = 1$, potom

$$U_i = i(\vec{n_i}.\vec{\sigma}).$$

Vidno, že pre $\cos\theta_i$ nemôže byť pre všetky i=1,2,3 tá istá hodnota. Pre jedno i musí byť jedna hodnota opačná ako pre zvyšné dve, aby sme dostali tri rôzne transformácie. Zvoľme

$$\cos\theta_1 = \cos\theta_2 = \sqrt{\frac{1}{3}}$$

$$\cos\theta_3 = -\sqrt{\frac{1}{3}}$$

Potom nevyhnutne

$$\cos(\phi_1 - \phi_2) = -1/2$$

$$\cos(\phi_1 - \phi_3) = \cos(\phi_2 - \phi_3) = 1/2,$$

čo platí pre $\phi_1 = \phi$, $\phi_2 = \frac{2}{3}\pi + \phi$, $\phi_3 = \frac{\pi}{3} + \phi$. To znamená, že je voľnosť vo výbere jedného parametra ϕ, čo je ale iba vyjadrením rotačnej symetrie okolo osi, ku ktorej sa volí báza, čo je v našom prípade os z.

Ak zvolíme $\phi = 0$, tak dostávame

$$\vec{n_1} = (\sqrt{\frac{2}{3}}, 0, \sqrt{\frac{1}{3}})$$

$$\vec{n_2} = (-\sqrt{\frac{1}{6}}, \frac{\sqrt{2}}{2}, \sqrt{\frac{1}{3}}) \tag{6.13}$$

$$\vec{n_3} = (\sqrt{\frac{1}{6}}, \frac{\sqrt{2}}{2}, -\sqrt{\frac{1}{3}}).$$

Aké je vlastne naše nájdené minimum? Dosaďme do (6.7) alebo (6.8) a ľahko zistíme, že

$$\text{minimum} = \frac{1}{3}\triangle^2 = \frac{1}{3}(|\alpha|^2 - |\beta|^2)^2.$$

Pre štvorce skalárnych súčinou teda platí

$$|\langle\psi_i|\psi_j\rangle|^2 = \begin{cases} 1 & \text{ak } i = j \\ \frac{1}{3}\triangle^2 & \text{ak } i \neq j \end{cases} \tag{6.14}$$

kde

$$|\psi_i\rangle = \mathrm{U_i} \otimes \mathbf{1}|\psi_0\rangle.$$

Tvar matice lokálnej unitárnej transformácie $\mathrm{U_i}$ je

$$\mathrm{U_i} = \vec{n_i}.\vec{\sigma},$$

kde σ-matice sú definované vzhľadom k báze určenej vektormi[2] $|0\rangle_\mathrm{A}, |1\rangle_\mathrm{A}$, v ktorej majú tvar (3.5).

Explicitne vypíšeme vektory $|\psi_i\rangle$ v Schmidtovej báze

$$\begin{aligned} &\{|00\rangle, |10\rangle, |01\rangle, |11\rangle\} \\ |\psi_0\rangle &= (\alpha, 0, 0, \beta) \\ |\psi_1\rangle &= \left(\sqrt{\tfrac{1}{3}}\alpha, \sqrt{\tfrac{2}{3}}\alpha, \sqrt{\tfrac{2}{3}}\beta, -\sqrt{\tfrac{1}{3}}\beta\right) \\ |\psi_2\rangle &= \left(\sqrt{\tfrac{1}{3}}\alpha, (-\sqrt{\tfrac{1}{6}} + i\sqrt{\tfrac{1}{2}})\alpha, (-\sqrt{\tfrac{1}{6}} - i\sqrt{\tfrac{1}{2}})\beta, -\sqrt{\tfrac{1}{3}}\beta\right) \\ |\psi_3\rangle &= \left(-\sqrt{\tfrac{1}{3}}\alpha, (\sqrt{\tfrac{1}{6}} + i\sqrt{\tfrac{1}{2}})\alpha, (\sqrt{\tfrac{1}{6}} - i\sqrt{\tfrac{1}{2}})\beta, \sqrt{\tfrac{1}{3}}\beta\right) \end{aligned} \tag{6.15}$$

Vidno, že v limite $\alpha = \beta$, t.j. na počiatku máme Bellov stav ϕ^+, nedostávame v našom prípade ostatné Bellove stavy. Naše transformácie sú nezávislé od α a β.

Pozrime sa, čo sa stane, ak budeme týmito transformáciami pôsobiť na niektorý zo stavov $|\psi_\mathrm{i}\rangle$ pre i=1,2,3, t.j.

$$\vec{n_j}.\vec{\sigma}|\psi_\mathrm{i}\rangle = (\vec{n_j}.\vec{\sigma})(\vec{n_i}.\vec{\sigma})|\psi_0\rangle = \mathrm{i}(\vec{n_j} \times \vec{n_i}).\vec{\sigma}|\psi_0\rangle.$$

Naše tri transformácie (okrem triviálnej) sú určené troma navzájom kolmými vektormi $\vec{n_\mathrm{i}}$ v trojrozmernom reálnom vektorovom priestore. Z toho vyplýva, že vektorový súčin dvoch z nich dáva až na násobok ± 1 tretí z nich

$$\vec{n_j} \times \vec{n_i} = \varepsilon_{jik}\vec{n_k}$$

pre $j \neq i$. Triviálna transformácia samozrejme stav nemení, a teda až na fázový faktor sú naše stavy navzájom spojené týmito štyrmi transformáciami.

Skúsme pre tieto stavy zrátať výraz pre kapacitu ideálneho kvantového komunikačného kanála pri hustom kódovaní. Keďže ide opäť o čisté stavy, pre ktoré je entropia nulová, tak druhý člen v (4.6) bude analogicky ako v prípade Bellových stavov nulový. Numericky sa dá zistiť optimálne kódovanie, ktoré je $\pi_\mathrm{i} = \frac{1}{4}$. Pri takomto kódovaní treba zrátať maticu

$$\varrho = \sum_\mathrm{i} \pi_i \varrho_i = \sum_i \pi_i |\psi_i\rangle\langle\psi_i| = \frac{1}{4}\sum_i |\psi_i\rangle\langle\psi_i|,$$

ktorej entropia vystupuje ako prvý výraz v (4.6). Po zrátaní dostaneme celkom jednoduché vyjadrenie pre ϱ

$$\varrho = \frac{|\alpha|^2}{2}(|00\rangle\langle 00| + |10\rangle\langle 10|) + \frac{|\beta|^2}{2}(|01\rangle\langle 01| + |11\rangle\langle 11|),$$

teda dostávame diagonálnu maticu, ktorej entropiu vypočítame jednoducho a dostaneme pre kapacitu

$$\mathrm{C} = 1 - (|\alpha|^2 \log|\alpha|^2 + |\beta|^2 \log|\beta|^2). \tag{6.16}$$

[2] Smer týchto vektorov chápeme ako smer z.

6.2 EKVIVALENTNÉ ABECEDY

V predošlej časti sme predpokladali, že rovnako vzdialené stavy budú najlepšie v zmysle kapacity ideálneho kvantového komunikačného kanála.

Čo by sa stalo, ak by sme namiesto $\mathrm{U_i}$ uvažovali transformácie, ktoré vedú v prípade Bellových stavov k Bellovym meraniam, t.j. použit' ako lokálne transformácie $\mathbf{1}, \sigma_\mathrm{x}, \sigma_\mathrm{y}, \sigma_\mathrm{z}$ (vid' 4.2).

Pre takto získané stavy

$$|\phi_0\rangle = |\psi_0\rangle$$

$$|\phi_\mathrm{i}\rangle = \sigma_\mathrm{i} \otimes \mathbf{1}|\psi_\mathbf{0}\rangle$$

platí

$$|\langle\phi_\mathrm{i}|\phi_\mathrm{j}\rangle|^2 = \begin{cases} 1 & \text{ak } i = j \\ \triangle^2 & \text{ak } ij = 01, 10, 23, 32 \\ 0 & \text{inak} \end{cases} \tag{6.17}$$

Z tohoto a z (6.14) vidno, že transformácie $\mathrm{U_i}$ a σ_i dávajú množiny stavov, označme ich $\{\varrho_\mathrm{i}\}$ a $\{\mathrm{W_i}\}$, ktoré majú odlišnú štruktúru, t.j. nie sú navzájom zviazané iba jednou unitárnou transformáciou, t.j. neexistuje $\mathrm{U}|\psi_\mathrm{i}\rangle = |\phi_\mathrm{i}\rangle$ pre i=0,1,2,3.

Napriek tomu by sme pri počítaní kapacity dostali ten istý výsledok ako aj predtým. Skúsme sa bližšie pozriet' na dôvod, prečo sú tieto zjavne rôzne abecedy, čo sa týka kapacity ideálneho komunikačného kanála rovnaké.

Spoločná vlastnost' týchto množín stavov je *Bellova limita*, t.j. fakt, že pri $\alpha = \beta = \frac{1}{\sqrt{2}}$, dostávame ortonormálnu množinu. Vieme, že podmienka Bellovej limity implikuje pre tri lokálne transformácie (6.1) tieto dve vlastnosti

$$\cos^2\psi_\mathrm{i} = 0$$

$$\vec{\mathrm{n}_\mathrm{i}}.\vec{\mathrm{n}_\mathrm{j}} = \delta_\mathrm{ij},$$

pričom štvrtú transformáciu berieme ako jednotkový operátor. Keďže tieto transformácie sú unitárne, tak dostávame po ich aplikácii na ψ_0 štyri čisté stavy. Pri počítaní kapacity pre takéto stavy opät' stačí spočítat' entropiu zmesi týchto stavov s rovnakou váhou $\pi_\mathrm{i} = 1/4$, t.j. maticu hustoty

$$\varrho = \frac{1}{4}\sum_\mathrm{i}\varrho_i = \frac{1}{4}\sum_i \mathrm{U_i} \otimes \mathbf{1}|\psi_\mathbf{0}\rangle\langle\psi_\mathbf{0}|\mathrm{U_i^+} \otimes \mathbf{1}, \tag{6.18}$$

kde

$$\mathrm{U_i} = \vec{\mathrm{n}_\mathrm{i}}.\vec{\sigma} \text{ pre i} = 1, 2, 3$$

$$\mathrm{U_0} = \mathbf{1}. \tag{6.19}$$

Otázkou je, či kapacita bude stále rovnaká pri týchto transformáciach, ak platí podmienka $\vec{\mathrm{n}_\mathrm{i}}.\vec{\mathrm{n}_\mathrm{j}} = 0$.

Matica hustoty, ktorej entropiu treba spočítat' má tvar

$$\frac{1}{4}\begin{pmatrix} |\alpha|^2(1+\sum_\mathrm{i}\mathrm{n_i^z}) & |\alpha|^2\sum_\mathrm{i}(\mathrm{n_i^x}-\mathrm{in_i^y}) & \alpha\beta^*\sum_\mathrm{i}(\mathrm{n_i^x}+\mathrm{in_i^y}) & \alpha\beta^*(1-\sum_\mathrm{i}\mathrm{n_i^z}) \\ |\alpha|^2\sum_\mathrm{i}(\mathrm{n_i^x}+\mathrm{in_i^y}) & |\alpha|^2\sum_\mathrm{i}(\mathrm{n_i^y}.\mathrm{n_i^y}+\mathrm{n_i^x}.\mathrm{n_i^x}) & \alpha\beta^*\sum_\mathrm{i}(\mathrm{n_i^x}+\mathrm{in_i^y})(\mathrm{n_i^x}+\mathrm{in_i^y}) & \alpha\beta^*\sum_\mathrm{i}(\mathrm{n_i^x}-\mathrm{in_i^y}) \\ \alpha^*\beta\sum_\mathrm{i}\mathrm{n_i^z}(\mathrm{n_i^x}-\mathrm{in_i^y}) & \alpha^*\beta\sum_\mathrm{i}(\mathrm{n_i^x}-\mathrm{in_i^y})(\mathrm{n_i^x}-\mathrm{in_i^y}) & |\beta|^2\sum_\mathrm{i}(\mathrm{n_i^y}.\mathrm{n_i^y}+\mathrm{n_i^x}.\mathrm{n_i^x}) & |\beta|^2\sum_\mathrm{i}\mathrm{n_i^z}(\mathrm{n_i^x}+\mathrm{in_i^y}) \\ \alpha^*\beta(1-\sum_\mathrm{i}\mathrm{n_i^z}.\mathrm{n_i^z}) & \alpha^*\beta\sum_\mathrm{i}\mathrm{n_i^z}(\mathrm{n_i^x}+\mathrm{n_i^y}) & |\beta|^2\sum_\mathrm{i}\mathrm{n_i^z}(\mathrm{n_i^x}-\mathrm{in_i^y}) & |\beta|^2(1+\sum_\mathrm{i}\mathrm{n_i^z}.\mathrm{n_i^z}) \end{pmatrix}$$

kde $\mathrm{n_i^j}$ je j-ta komponenta vektora $\mathrm{n_i}$. Tieto vektory tvoria úplný ortonormálny systém, t.j. platí aj podmienka úplnosti

$$\sum_\mathrm{i}\mathrm{n_i^j n_i^k} = \delta^\mathrm{jk},$$

kde j,k=x,y,z. Po dosadení tejto vlastnosti do matice dostaneme diagonálnu maticu

$$\varrho = \begin{pmatrix} \frac{|\alpha|^2}{2} & 0 & 0 & 0 \\ 0 & \frac{|\alpha|^2}{2} & 0 & 0 \\ 0 & 0 & \frac{|\beta|^2}{2} & 0 \\ 0 & 0 & 0 & \frac{|\beta|^2}{2} \end{pmatrix} \tag{6.20}$$

z ktorej pre kapacitu kvantového komunikačného kanála dostávame výsledok zhodný s (6.16).

Dostali sme teda celú triedu transformácii určujúcich vstupné abecedy, pre ktoré je kapacita ideálneho kvantového komunikačného kanála rovnaká. Náš intuitívny predpoklad, že pre rovnako vzdialené stavy bude kapacita najväčšia, bol nesprávny. Poznamenajme, že naše transformácie dávajú stavy, ktoré rozkladajú tú istú maticu hustoty s tou istou váhou pre každý stav.

Treba poznamenat', že definícia σ-matíc je závislá na voľbe Schmidtovej bázy a teda aj tieto transformácie, keďže sú vyjadrené cez σ-matice, sú na tejto voľbe závislé. To znamená, že ak zafixujeme transformácie v nejakej báze, tak v inej báze budú vyzerať inak, ak ich budeme chciet' vyjadrit' cez σ-matice definované vzhľadom k tejto inej báze. Stavy, ktoré takto získame, už nebudú navzájom rovnako rozlíšiteľné. Práve fakt ekvivalentných abecied však zabezpečuje universalitu vybratých transformácii, čo sa týka dosiahnutej kapacity. Pre zhodnosť kapacity je podstatná podmienka ortogonálnosti vektorov $\vec{n}_i$. Tieto tri vektory si môžeme predstavit'zakreslené v trojrozmernom priestore spolu s Blochovou sférou. Stav $|0\rangle$ zodpovedá smeru z, ktorý je vlastným vektorom matice σ_z. Vlastné vektory zvyšných Pauliho matíc zodpovedajú smerom x a y. Vlastné vektory matice $\vec{n}.\vec{\sigma}$ sú takisto v smere $\vec{n}$. Zmena Schmidtovej bázy zodpovedá zmene smeru z a tým aj ku zmene osí x a y. Ak zafixujeme niektorú trojicu ortonormálnych vektorov $\vec{n}_i$, tak zmena bázy nezmení ich ortonormálnost'.

Vlastnosť, že transformácie (6.19) dávajú vektory medzi ktorými sa môžeme pohybovat' iba pomocou týchto transformácií, sa týka úplne všetkých stavov (aj matíc hustoty). Pôsobením transformácií U_j na stavoch $\varrho_i = U_i \varrho_0 U_i^+$ dostávam opäť iba stav z tejto množiny, t.j. táto množina je vzhľadom k týmto transformáciam invariantná. Takúto množinu môžeme prisúdit' ľubovoľnému stavu ϱ_0. Pôvod tejto vlastnosti je v platnosti vzťahu $U_i U_j = i\varepsilon_{kij} U_k$, ktorý nemá nič spoločné s nejakým konkrétnym stavom.

6.3 KAPACITA PRE ZMESI A NEIDEÁLNY KVANTOVÝ KOMUNIKAČNÝ KANÁL

Pokúsme sa zovšeobecnit' výsledky aj na zmesi. Opäť vyjdeme z jedného stavu ϱ_0, na ktorý Alica pôsobí štyrmi unitárnymi operáciami a generuje tak štyri písmená abecedy. Každú zmes vieme vyjadrit' ako konvexnú kombináciu čistých ortogonálnych stavov[3], t.j. v diagonálnom tvare

$$\varrho_0 = \sum_{i=1}^{4} \lambda_i |\psi_i^0\rangle\langle\psi_i^0| \tag{6.21}$$

Každý čistý stav $|\psi_i^0\rangle$ dvojzložkového systému vieme vyjadrit' v Schmidtovej báze (Schmidtovej dekompozícii). Otázkou je, či pre navzájom kolmé vektory existuje tá istá Schmidtova báza. Vyjadrime jeden z vektorov v Schmidtovej báze

$$|\psi_1^0\rangle = \alpha|0\rangle_A|0\rangle_B + \beta|1\rangle_A|1\rangle_B.$$

[3]každá maticu hustoty môžeme chápat' ako pozorovateľnú, alebo hermitovský lineárny operátor, pre ktorý existuje spektrálny rozklad

Teraz sa pozrime ako by mali vyzerať zvyšné vektory v tejto Schmidtovej báze. Schmidtova dekompozícia je unitárna transformácia, a teda aj v Schmidtovej báze musia byť všetky vektory navzájom kolmé, t.j. jeden z nich (označme ho indexom i=2) musí mať tvar

$$|\psi_2^0\rangle = \beta^*|0\rangle_A|0\rangle_B - \alpha^*|1\rangle_A|1\rangle_B$$

a zvyšné dva

$$|\psi_3^0\rangle = \gamma|0\rangle_A|1\rangle_B + \delta|1\rangle_A|0\rangle_B$$
$$|\psi_4^0\rangle = \delta^*|0\rangle_A|1\rangle_B - \gamma^*|1\rangle_A|0\rangle_B.$$

Vidno,že každý z nich je zapísaný v Schmidtovej dekompozícii v tej istej báze, čo sme chceli.

Teraz na takto zapísanú zmes použijeme lokálne unitárne transformácie $U_j = \vec{n}_j\vec{\sigma} \otimes \mathbf{1}$, čím dostaneme štyri stavy $\varrho_j = U_j\varrho_0 U_j^+$. Na výpočet kapacity pre takto získanú abecedu využijeme znalosti z predošlej časti tejto kapitoly. Zrátajme najskôr $S(\varrho_j)$. Keďže naše transformácie sú unitárne, tak entropia všetkých je rovnaká a druhý člen v (4.6) je rovný

$$S(\varrho_0) = -\sum_i \lambda_i \log \lambda_i.$$

V ďalšom spočítame entropiu stavu

$$\varrho = \frac{1}{4}\sum_{j=0}^{3} U_j\varrho_0 U_j^+ = \frac{1}{4}\sum_{j=0}^{3} U_j \left(\sum_{i=1}^{4} \lambda_i|\psi_i^0\rangle\langle\psi_i^0|\right) U_j^+,$$

čo vďaka linearite U_j môžeme prepísať na

$$\varrho = \sum_{i=1}^{4} \lambda_i \frac{1}{4}\sum_{j=0}^{3} U_j|\psi_i^0\rangle\langle\psi_i^0|U_j^+.$$

Výraz

$$\frac{1}{4}\sum_{j=0}^{3} U_j|\psi_i^0\rangle\langle\psi_i^0|U_j^+$$

je pre každé i=1,2,3,4, zhodný s (6.18). Práve teraz využijeme, že zápis našich stavov je v Schmidtovej báze, lebo to bola podmienka, z ktorej sme vychádzali pri výpočtoch ďalej. Poznamenajme, že táto podmienka nijako neobmedzuje triedu stavov, ktoré môžeme uvažovať, lebo pre každý čistý stav existuje zápis v Schmidtovej báze. Výsledkom z predošlej časti tejto kapitoly je fakt, že celý takýto výraz je diagonálny v Schmidtovej báze a ak k tomu pridáme, že pre všetky i=1,2,3,4 sú v tej istej Schmidtovej báze, tak prídeme k tomu, že celé ϱ je diagonálne v jednej báze, a teda nie ja problém spočítať entropiu takéhoto stavu. Matica ϱ má tvar

$$\varrho = \frac{1}{2}(|\alpha|^2\lambda_1 + |\beta|^2\lambda_2 + |\gamma|^2\lambda_3 + |\delta|^2\lambda_4)(|00\rangle\langle 00| + |10\rangle\langle 10|) +$$
$$+\frac{1}{2}(|\alpha|^2\lambda_2 + |\beta|^2\lambda_1 + |\gamma|^2\lambda_4 + |\delta|^2\lambda_3)(|01\rangle\langle 01| + |11\rangle\langle 11|).$$

Ostáva už iba určiť $\alpha, \beta, \gamma, \delta$ pre nejaké konkrétne ϱ_0, pričom platí

$$|\alpha|^2 + |\beta|^2 = |\gamma|^2 + |\delta|^2 = 1.$$

Pre takúto abecedu je kapacita ideálneho kvantového komunikačného kanála

$$C = \sum_i \lambda_i \log \lambda_i + 1 - x \log x - y \log y, \tag{6.22}$$

kde

$$\mathrm{x} = |\alpha|^2(\lambda_1 - \lambda_2) + |\gamma|^2(\lambda_3 - \lambda_4) + \lambda_2 + \lambda_4$$
$$\mathrm{y} = |\alpha|^2(\lambda_2 - \lambda_1) + |\gamma|^2(\lambda_4 - \lambda_3) + \lambda_1 + \lambda_3. \tag{6.23}$$

Všimnime si niektoré špeciálne prípady. Ak $\lambda_\mathrm{i} = 1/4$, tak kapacita C = 0, čo je pochopiteľné, lebo v tomto prípade stav ϱ_0 a tým aj všetky ostatné písmená abecedy sú úplnýni zmesami. Uvážme prípad čistého stavu, t.j. napríklad pre $\lambda_1 = 1$ a ostatné $\lambda_\mathrm{i} = 0$ pre i=2,3,4. V tomto prípade dostaneme vzťah zhodný so vzťahom (6.16), lebo prvý člen z rovnice vypadne, $\mathrm{x} = |\alpha|^2$ a $\mathrm{y} = |\beta|^2$.

Uvažujme počiatočný stav v špeciálnom tvare

$$\tilde{\varrho}_0 = s|\psi_0\rangle\langle\psi_0| + \frac{1-s}{4}\mathbf{1}.$$

Aplikujme na tento stav naše štyri transformácie $\mathrm{U_i}$. Dostaneme štvoricu stavov

$$\tilde{\varrho}_\mathrm{i} = s|\psi_\mathrm{i}\rangle\langle\psi_\mathrm{i}| + \frac{1-s}{4}\mathbf{1} = \mathrm{s}\varrho_\mathrm{i} + \frac{1-\mathrm{s}}{4}\mathbf{1} \tag{6.24}$$

pre i=0,1,2,3, $|\psi_\mathrm{i}\rangle = \mathrm{U_i}|\psi_0\rangle$.

Zrátajme kapacitu ideálneho kvantového komunikačného kanála pre abecedu tvorenú stavmi $\tilde{\varrho}_\mathrm{i}$

$$\mathrm{C} = \mathrm{S}(\tilde{\varrho}) - \frac{1}{4}\sum_\mathrm{i}\mathrm{S}(\tilde{\varrho}_\mathrm{i}),$$

kde

$$\tilde{\varrho} = \frac{1}{4}\sum_\mathrm{i}\tilde{\varrho}_\mathrm{i} = s\varrho + \frac{1-s}{4}\mathbf{1},$$

čo je diagonálna matica (ϱ je matica hustoty (6.20)). Pri počítaní $\mathrm{S}(\tilde{\varrho}_\mathrm{i})$ zvoľme ortonormálnu bázu $\{\psi_\mathrm{i}, \phi_1, \phi_2, \phi_3\}$, v ktorej je matica ϱ_i diagonálna, t.j. keďže ide o čistý stav má vlastnú hodnotu rovnú jednej, ($\mathbf{1}$ je v každej báze diagonálna). Dostávame diagonálnu maticu hustoty

$$\tilde{\varrho}_\mathrm{i} = \begin{pmatrix} \frac{3\mathrm{s}+1}{4} & 0 & 0 & 0 \\ 0 & \frac{1-\mathrm{s}}{4} & 0 & 0 \\ 0 & 0 & \frac{1-\mathrm{s}}{4} & 0 \\ 0 & 0 & 0 & \frac{1-\mathrm{s}}{4} \end{pmatrix}$$

ktorá je pre všetky i=0,1,2,3 rovnaká, aj keď pre rôzne i je vyjadrená v rôznych ortonormálnych bázach.

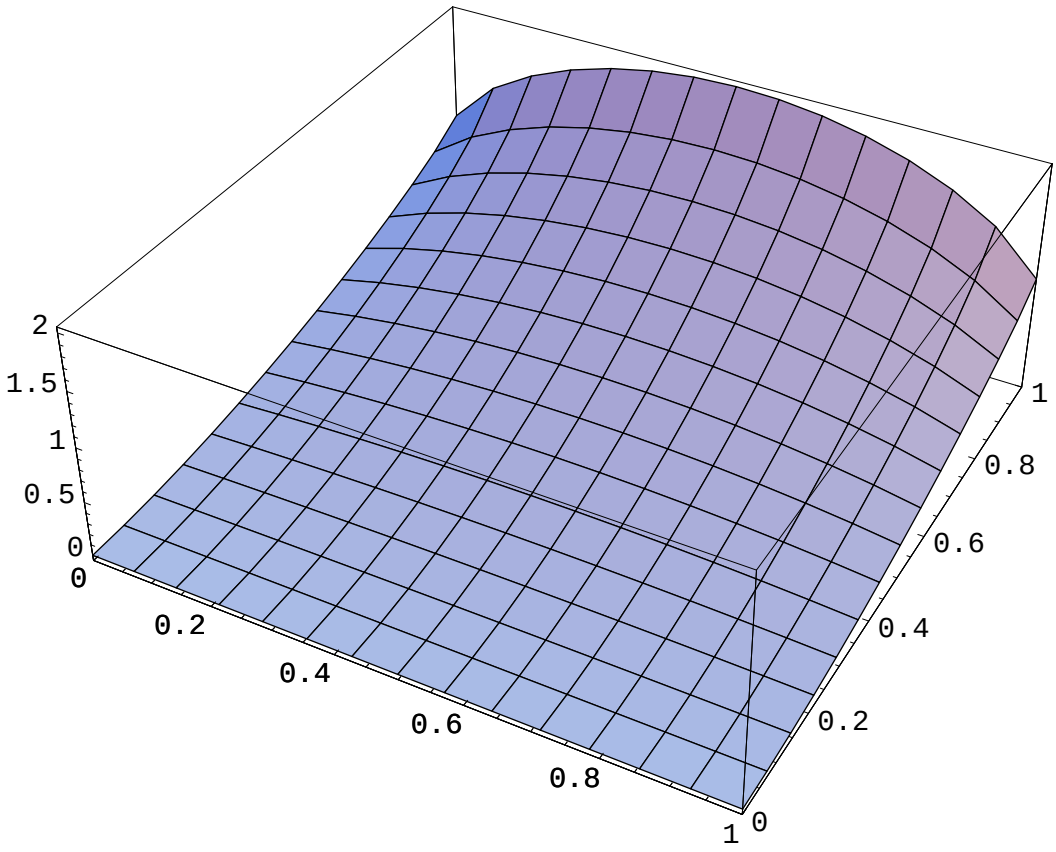
Matice, z ktorých počítame entropiu máme v diagonálnej forme. Teda dostávame pre kapacitu

$$\mathrm{C} = -\frac{\mathrm{s}(2|\alpha|^2-1)+1}{2}\log\left(\frac{\mathrm{s}(2|\alpha|^2-1)+1}{4}\right) - \frac{\mathrm{s}(2|\beta|^2-1)+1}{2}\log\left(\frac{\mathrm{s}(2|\beta|^2-1)+1}{4}\right) + \\ + \frac{3s+1}{4}\log\left(\frac{3s+1}{4}\right) + \frac{3(1-s)}{4}\log\left(\frac{1-s}{4}\right)$$

Graf tejto funkcie je zobrazený na obrázku 6.1. Výsledok môžeme jednoducho overiť, ak položíme s=1, tak dostávame výsledok zhodný s (6.16). Naopak pre s=0, čo je prípad abecedy zloženej z jedného písmena (úplnej zmesi), bude kapacita nulová.

Pre isté hodnoty s a α je stav $\tilde{\varrho}_0$ separabilný. Na určenie kritických hodnôt, pri ktorých sa z entanglovaného stavu, stáva separabilný, použijeme metódu čiastočne transponovanej matice.

Ak čiastočne transponovaná matica hustoty je pozitívne semidefinitná, t.j. $\varrho^{\mathrm{partialT}} \geq 0$, tak stav opísaný maticou hustoty pre dvojqubitový systém je separabilný. Poznamenajme (viď [8]), že toto tvrdenie vyjadruje nutnú a postačujúcu podmienku separability iba pre 2x2 a 2x3 systémi a neplatí pre ľubovoľné zložené systémy, kedy vyjadruje iba nutnú podmienku, t.j. existujú v



Obrázok 6.1: Graf kapacity kvantového komunikačného kanála so vstupnou abecedou generovanou stavom $\tilde{\varrho}_0 = s|\psi_0\rangle\langle\psi_0| + \frac{1-s}{4}\mathbf{1}$ v závislosti od parametrov $|\alpha|^2$ a s.

takýchto systémoch aj entanglované stavy s pozitívne semidefinitnou čiastočne transponovanou maticou. Čiastočne transponovanú maticu $\varrho^{\text{partial T}}$ definujeme na dvojzložkovom systéme, kde báza v A je určená latinskými písmenami $|\mathrm{i}\rangle$ a báza v B gréckymi písmenami $|\mu\rangle$. Matica hustoty je $\varrho_{\mathrm{ij},\mu\nu}$ a

$$\varrho^{\text{partial T}}_{\mathrm{i}\mu,\mathrm{j}\nu} = \varrho_{\mathrm{i}\nu,\mathrm{j}\mu}$$

je potom čiastočne transponovaná matica cez systém B. V našom prípade

$$\tilde{\varrho}_0^{\text{partial T}} = \begin{pmatrix} \frac{\mathrm{s}(4|\alpha|^2-1)+1}{4} & 0 & 0 & 0 \\ 0 & \frac{1-\mathrm{s}}{4} & \mathrm{s}\alpha\beta^* & 0 \\ 0 & \mathrm{s}\alpha^*\beta & \frac{1-\mathrm{s}}{4} & 0 \\ 0 & 0 & 0 & \frac{\mathrm{s}(3-4|\alpha|^2)+1}{4} \end{pmatrix}$$

Vlastné hodnoty tejto matice sú

$$\begin{aligned} \lambda_1 &= \tfrac{\mathrm{s}(4|\alpha|^2-1)+1}{4} \geq 0 \\ \lambda_2 &= \tfrac{\mathrm{s}(3-4|\alpha|^2)+1}{4} \geq 0 \\ \lambda_3 &= \tfrac{1-\mathrm{s}+4\mathrm{s}|\alpha||\beta|}{4} \geq 0 \\ \lambda_4 &= \tfrac{1-\mathrm{s}-4\mathrm{s}|\alpha||\beta|}{4} \end{aligned}$$

kde iba posledná vlastná hodnota je menšia ako nula (t.j. stav je entanglovaný) práve vtedy, ak

$$\mathrm{s} > \frac{1}{1+4|\alpha||\beta|} \tag{6.25}$$

V prípade rovnosti nastáva prechod medzi separabilnými a neseparabilnými stavmi. V reči kvantovej komunikácie to znamená prechod medzi množinami stavov použiteľných na husté kódovanie a stavov nepoužiteľných. Pozrime sa ako vyzerá kapacita kvantového komunikačného kanála práve v prípade rovnosti. Pre jednoduchosť zápisu položme $|\alpha| = \alpha$ a $|\beta| = \beta$ a pre kapacitu dostaneme

$$\mathrm{C} = \tfrac{1}{1+4\alpha\beta}\{2\alpha\beta\log(1+4\alpha\beta) - (\alpha^2+2\alpha\beta)\log(\alpha^2+2\alpha\beta) - \\ -(\beta^2+2\alpha\beta)\log(\beta^2+2\alpha\beta) + (1+\alpha\beta)\log(1+\alpha\beta) + \alpha\beta\log\alpha\beta\}.$$

Minimum nastáva v prípade Bellovych stavov, kedy

$$\mathrm{C} = \frac{1}{2}\log\frac{4}{3}.$$

Toto nie je až také prekvapujúce, ak si uvedomíme, že v tomto prípade je šum, t.j. výraz $1 - \mathrm{s}$, maximálny. Maximum nastáva v prípade $\alpha = 1$, kedy s=1 a C=1, čo je v zhode s očakávaním, lebo v tomto prípade ide o ideálny komunikačný kanál pre čistý separabilný stav. Abeceda je tvorená z dvojíc rovnakých stavov, pričom tieto dvojice sú navzájom ortogonálne. Teda abeceda je v skutočnosti binárna ortogonálna, pre ktorú je kapacita C=1 (vid' časť 5.2).

Poznamenajme, že rovnicu (6.24) môžeme chápať aj ako pôsobenie kvantového komunikačného kanála na vstupné stavy $|\psi_\mathrm{i}\rangle\langle\psi_i|$, pričom $\tilde{\varrho}_\mathrm{i}$ sú výstupné stavy, ktoré vystupujú vo výraze pre kapacitu, t.j.

$$|\psi_\mathrm{i}\rangle\langle\psi_i| = \varrho_\mathrm{i} \to \tilde{\varrho}_\mathrm{i}$$

Takýto kvantový komunikačný kanál budeme nazývať *šumový*.

6.4 KAPACITA PRE NxN ENTANGLOVANÉ STAVY

Predstavme si tú istú situáciu s tým rozdielom, že Hilbertove priestory Alici a Boba nie sú dvojrozmerné, ale N-rozmerné, a stavy na týchto priestoroch budeme nazývať *quNity*. Na N×N zloženom systéme môžeme zadefinovať analóg Bellových stavov (maximálne entanglovaných stavov, ktoré tvoria ortonormálnu bázu na $\mathrm{H_A} \otimes \mathrm{H_B}$) nasledovne

$$|\psi_\mathrm{mn}\rangle_\mathrm{AB} = \frac{1}{\sqrt{N}}\sum_{\mathrm{j}=0}^{\mathrm{N}-1} \mathrm{e}^{2\pi\mathrm{i}(\mathrm{jn}/\mathrm{N})}|\mathrm{j}\rangle_\mathrm{A}|(\mathrm{j}+\mathrm{m})\,mod\mathrm{N}\rangle_\mathrm{B},$$

kde $|\mathrm{j}\rangle_\mathrm{A(B)}$ je nejaká ortonormálna báza na A(B) a m,n=0,...N−1 označujú N^2 bázových Bellových stavov.

Schmidtovou dekompozíciou vieme každý čistý stav $|\phi_{00}\rangle_\mathrm{AB}$ previesť na tvar

$$|\phi_{00}\rangle_\mathrm{AB} = \sum_{\mathrm{j}=0}^{\mathrm{N}-1} \alpha_\mathrm{j}|\mathrm{jj}\rangle_\mathrm{AB},$$

kde $|\mathrm{jj}\rangle = |\mathrm{j}\rangle_\mathrm{A}|\mathrm{j}\rangle_\mathrm{B}$. Teraz hľadáme N^2 lokálnych unitárnych transformácii, t.j. $\mathrm{U_j} = \mathrm{U_j} \otimes \mathbf{1}_\mathrm{B}$, ktoré spĺňajú *Bellovu limitu*, t.j. pre $\alpha_\mathrm{j} = 1/\sqrt{N}$ pre všetky j dostávame N^2 navzájom kolmých stavov.

Všeobecná lokálna unitárna transformácia na N-rozmernom priestore je

$$\mathrm{U_j} = \exp(\mathrm{i}\sum_\mathrm{k} \mathrm{n_j^k A_k}),$$

kde $\mathrm{A_k}$ sú bázové prvky Lieovej algebry su(N). Stačí nám uvažovať Lieovu algebru su(N) namiesto u(N), lebo u(N)=su(N)⊕u(1), čo znamená, že unitárna transformácia sa dá zapísať ako súčin komplexného čísla s jednotkovou normou a matice z SU(N). Naviac my dávame $\mathrm{U_0} = \mathbf{1}_\mathrm{A}$ a teda hľadáme už len $\mathrm{N}^2 - 1$ lokálnych unitárnych matíc, čo je práve dimenzia su(N).

Uvažujme lokálne unitárne transformácie

$$\mathrm{U_{mn}} = \sum_{\mathrm{k}=0}^{\mathrm{N}-1} e^{2\pi \mathrm{i}(\mathrm{kn}/\mathrm{N})} |\mathrm{k}+\mathrm{m}\rangle_{\mathrm{A}}\langle \mathrm{k}|,$$

pre ktoré platí

$$|\psi_{\mathrm{mn}}\rangle_{\mathrm{AB}} = \mathrm{U_{mn}}|\psi_{00}\rangle_{\mathrm{AB}}.$$

Zapôsobme týmito transformáciami na ľubovoľný čistý stav $|\phi_{00}\rangle_{AB}$ zapísaný v Schmidtovej báze. Označme

$$|\phi_{\mathrm{mn}}\rangle_{\mathrm{AB}} = \mathrm{U_{mn}}|\phi_{00}\rangle_{\mathrm{AB}}.$$

Pre určenie kapacity potrebujeme spočítať maticu hustoty

$$\varrho_{\mathrm{AB}} = \frac{1}{\mathrm{N}^2} \sum_{\mathrm{m,n}=0}^{\mathrm{N}-1} |\phi_{\mathrm{mn}}\rangle\langle\phi_{\mathrm{mn}}|,$$

lebo vo výraze pre kapacitu (4.6) vystupuje z dôvodu, že $|\phi_{\mathrm{mn}}\rangle$ sú čisté stavy, iba prvý člen, t.j. entropia tejto zmesi.

$$\varrho_{\mathrm{AB}} = \frac{1}{\mathrm{N}^2} \sum_{\mathrm{mnst}} e^{\frac{2\pi \mathrm{i}}{\mathrm{N}}(\mathrm{s}-\mathrm{t})\mathrm{n}} (|\mathrm{s}+\mathrm{m}\rangle\langle \mathrm{s}| \otimes \mathbf{1}_{\mathrm{B}})|\phi_{00}\rangle\langle\phi_{00}|(|\mathrm{t}\rangle\langle \mathrm{t}+\mathrm{m}| \otimes \mathbf{1}_{\mathrm{B}}) =$$

$$= \frac{1}{\mathrm{N}^2} \sum_{\mathrm{mnstpq}} \alpha_{\mathrm{p}}\alpha_{\mathrm{q}}^{*} e^{\frac{2\pi \mathrm{i}}{\mathrm{N}}(\mathrm{s}-\mathrm{t})\mathrm{n}} |\mathrm{s}+\mathrm{m}\rangle\langle \mathrm{s}|\mathrm{p}\rangle\langle \mathrm{q}|\mathrm{t}\rangle\langle \mathrm{t}+\mathrm{m}| \otimes |\mathrm{p}\rangle\langle \mathrm{q}|,$$

kde sme dosadili za $|\phi_{00}\rangle$. Teraz využijeme vzťah

$$\sum_{\mathrm{n}=0}^{\mathrm{N}-1} e^{\frac{2\pi \mathrm{i}}{\mathrm{N}}(\mathrm{s}-\mathrm{t})\mathrm{n}} = \mathrm{N}\delta_{\mathrm{st}}$$

a dostaneme

$$\varrho_{\mathrm{AB}} = \frac{1}{\mathrm{N}} \sum_{\mathrm{mp}} |\alpha_{\mathrm{p}}|^2 |\mathrm{p}+\mathrm{m}\rangle\langle \mathrm{p}+\mathrm{m}| \otimes |\mathrm{p}\rangle\langle \mathrm{p}| = \sum_{\mathrm{p}=0}^{\mathrm{N}-1} \frac{|\alpha_{\mathrm{p}}|^2}{\mathrm{N}} \left[\sum_{\mathrm{m}=0}^{\mathrm{N}-1} |\mathrm{p}+\mathrm{m}\rangle\langle \mathrm{p}+\mathrm{m}| \right] \otimes |\mathrm{p}\rangle\langle \mathrm{p}|.$$

Vidíme, že ϱ je vlastne diagonálna matica $\mathrm{N}^2 \times \mathrm{N}^2$

$$\begin{pmatrix} \frac{|\alpha_0|^2}{\mathrm{N}}\mathbf{1}_{\mathrm{N}\times\mathrm{N}} & \dots\dots\dots & 0 \\ 0 & \dots\dots\dots\dots & 0 \\ 0 & \dots\dots\dots & \frac{|\alpha_0|^2}{\mathrm{N}}\mathbf{1}_{\mathrm{N}\times\mathrm{N}} \end{pmatrix}$$

Pre kapacitu teda dostávame

$$\mathrm{C} = \log_2 \mathrm{N} - \sum_{\mathrm{i}=0}^{\mathrm{N}-1} |\alpha_{\mathrm{i}}|^2,$$

čo je prirodzeným rozšírením kapacity dvojdimenzionálneho prípadu.

6.5 PAULIHO KANÁL PRE ENTANGLOVANÉ STAVY

V tejto časti bude Alica Pauliho komunikačným kanálom posielať qubit entanglovaný s Bobovým qubitom. Pôsobenie na stav ϱ_i^{AB} vyzerá nasledovne

$$\varrho_i \to \varrho_i' = (1-p)\varrho_i + p_x\sigma_x \otimes \mathbf{1}_B\varrho_i\sigma_x \otimes \mathbf{1}_B + p_y\sigma_y \otimes \mathbf{1}_B\varrho_i\sigma_y \otimes \mathbf{1}_B + p_z\sigma_z \otimes \mathbf{1}_B\varrho_i\sigma_z \otimes \mathbf{1}_B, \qquad (6.26)$$

kde používame označenia z (5.6) a

$$\varrho_i = U_i\varrho_0 U_i^+,$$

kde U_i sú štyri Alicine transformácie (6.19), pomocou ktorých kóduje.

Opäť pre $p_i = q$ takýto kanál nazývame depolarizačný.

K určeniu kapacity treba (4.6) spočítať pre stavy ϱ_i', t.j. pre výstupné stavy. Pôsobenie jednotlivých Krausových operátorov vyzerá nasledovne

$$\sigma_\mu\varrho_i\sigma_\mu = (n_i^\mu)^2\varrho_0 + i.n_i^\mu[(\vec{n_\mu} \times \vec{n_i})\vec{\sigma}, \varrho_0] + ((\vec{n_\mu} \times \vec{n_i})\vec{\sigma})\varrho_0((\vec{n_\mu} \times \vec{n_i})\vec{\sigma})$$

kde $\vec{n_\mu}$ je jednotkový vektor, ktorý má na μ-tom mieste jednotku, a pre jednoduchosť pri zápise vynechávame kartézsky súčin s jednotkovým operátorom na systéme B.

Výstupný stav bude sčítaním cez stavy získané pôsobením jednotlivých Krausovych operátorov, t.j.

$$\varrho_i' = (1-p)\sum_{\mu,\nu=1}^{3}\sigma_\mu\varrho_0\sigma_\nu n_i^\mu n_i^\nu + \sum_{\mu=1}^{3} p_\mu\{(n_i^\mu)^2\varrho_0 + i.n_i^\mu[(\vec{n_\mu} \times \vec{n_i})\vec{\sigma}, \varrho_0] + ((\vec{n_\mu} \times \vec{n_i})\vec{\sigma})\varrho_0((\vec{n_\mu} \times \vec{n_i})\vec{\sigma})\}.$$

Chceme spočítať maticu hustoty

$$\varrho = \frac{1}{4}\sum_i \varrho_i'.$$

Nič nás samozrejme neoprávňuje k voľbe kódovania $\pi_i = 1/4$, ale ani numericky nie je úloha ľahko zvládnuteľná kvôli veľkému počtu parametrov. Náš výsledok bude prinajhoršom dolným ohraničením pre kapacitu. Po využití úplnosti systému vektorov $\vec{n_i}$ dostaneme

$$\varrho = \frac{1}{4}[(1-p)(\varrho_0 + \sum_\mu \sigma_\mu\varrho_0\sigma_\mu) + \sum_\mu p_\mu(\varrho_0 + \sum_{\nu\neq\mu}\sigma_\nu\varrho_0\sigma_\nu)],$$

čo je nezávislé od voľby Aliciných transformácii určených trojicou navzájom kolmých jednotkových vektorov.

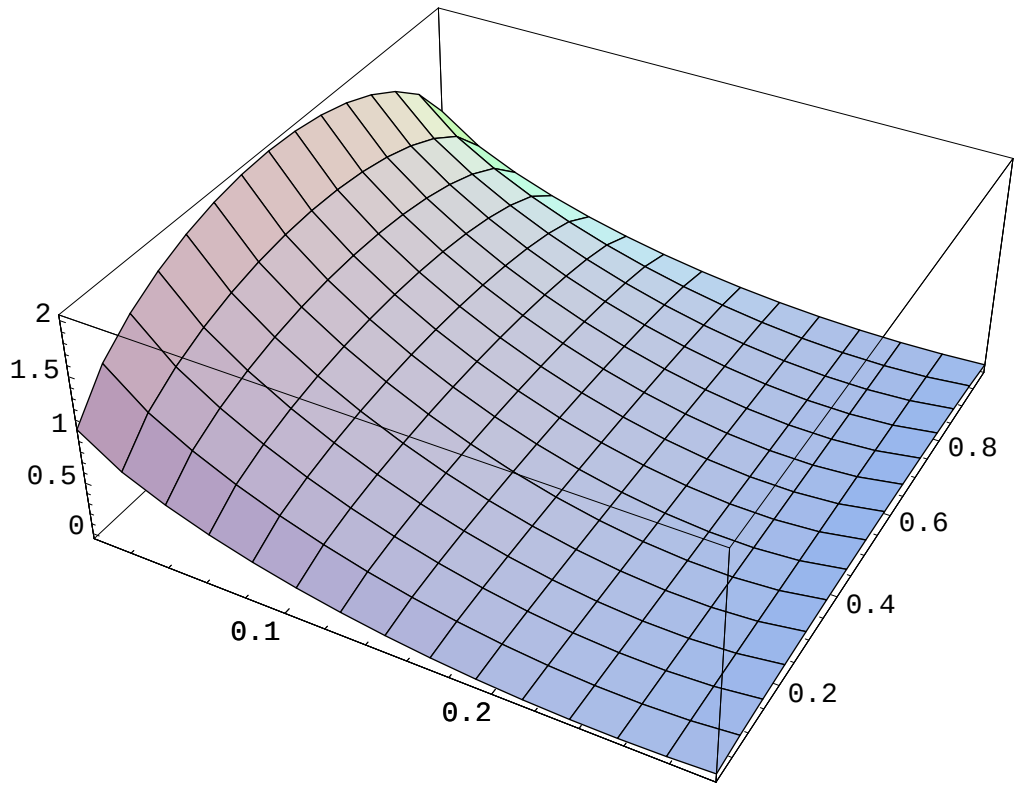
Kapacita

$$C = S(\varrho) - S(\frac{1}{4}\sum_i \varrho_i')$$

však už pre ľubovoľný kanál nemusí byť vôbec rovnaká pre rôzne voľby Aliciných transformácii. Aj keď zdanlivo nevystupujú v prvom výraze, tak v druhom určite vystupujú. Práve je otázkou, pri ktorých Pauliho komunikačných kanáloch je kapacita rovnaká pri rôznych voľbách Aliciných transformácii.

Pozrime sa, čo dostaneme pre kapacitu v prípade depolarizačného komunikačného kanála, t.j. $p_\mu = q$. V prípade binárnej abecedy mali výstupné stavy stále rovnakú entropiu. Predpokladajme dve rôzne abecedy určené voľbou Aliciných transformácií. Zvoľme lokálne unitárne transformácie, ktoré dávajú navzájom rovnako vzdialené stavy (6.14) a transformácie, ktoré sú určené σ-maticami (6.17). Tieto transformácie aplikujeme na stav

$$|\psi_0\rangle = \alpha|00\rangle + \beta|11\rangle$$



Obrázok 6.2: Závislosť kapacity depolarizačného kvantového komunikačného kanála od parametra q, ktorý charakterizuje tento komunikačný kanál, a od $|\alpha|^2$.

a získavame tak vstupné stavy komunikačného kanála. Numericky sme spočítali vlastné hodnoty matíc hustoty vystupujúcich vo výraze pre kapacitu, t.j. opisujúcich výstupné stavy, ktoré vyšli v obidvoch prípadoch rovnaké, a síce

$$\begin{aligned}
\lambda_1 &= 2q|\alpha|^2 \\
\lambda_2 &= 2q|\beta|^2 \\
\lambda_3 &= \tfrac{1}{2}(1-2q+\sqrt{(1-2q)^2-16q|\alpha|^2|\beta|^2(1-3q)}) \\
\lambda_3 &= \tfrac{1}{2}(1-2q-\sqrt{(1-2q)^2-16q|\alpha|^2|\beta|^2(1-3q)}).
\end{aligned} \tag{6.27}$$

To znamená, že aj entropia týchto výstupných stavov je rovnaká.

Ďalej platí

$$\varrho = \frac{1}{4}(\varrho_0 + \sum_\mu \sigma_\mu \varrho_0 \sigma_\mu),$$

čo je vlastne stav (6.20). Kapacita $C = S(\varrho) - S(\varrho'_i)$ je potom tiež rovnaká pri obidvoch abecedách. Po dosadení dostávame

$$C = 1 - (|\alpha|^2 \log|\alpha|^2 + |\beta|^2 \log|\beta|^2) - \sum_i \lambda_i \log \lambda_i. \tag{6.28}$$

Graf tejto funkcie je na obrázku 6.2, kde vidno, že pre q=0 dostávame kapacitu ideálneho komunikačného kanála pre čisté entanglované stavy (6.16).

6.6 HUSTÉ KÓDOVANIE A MIERY ENTANGLOVANIA

Pokúsime sa zaviest' mieru entanglovania. Pri jej zavedení sa pokúsime využit' jav zväčšenia kapacity binárneho kanála, ak sa používa tzv. husté kódovanie.

Niekto posiela qubity Alici a Bobovi. Tieto qubity tvoria spolu štvorrozmerný Hilbertov priestor a všeobecne sú opísané maticou hustoty ϱ_{AB}. Alica svojimi lokálnymi transformáciami pripravuje písmená abecedy, ktoré sa prenášajú komunikačným kanálom. Na druhej strane čaká Bob a každý prichádzajúci qubit spojí so svojim qubitom a na tomto páre qubitov robí meranie s cieľom zistit' posielaný stav. Kapacita je kvantita, ktorá hovorí ako najúspešnejšie môže rozoznat' Alicinu správu. Takýto prenos nazývame hustým kódovaním.

Predpokladajme, že máme stav ϱ_{AB}, ktorý zdieľajú Alica a Bob. V tomto prípade vieme určit' kapacitu ideálneho komunikačného kanála. Budeme ju označovat' $C^{ent}_{A\to B}$, kde $A \to B$ označuje smer posielania správy. Podl'a (6.22) platí

$$C^{ent}_{A\to B} = 1 + S(\varrho_A) - S(\varrho_{AB}),$$

kde

$$\varrho_A = Tr_B(\varrho_{AB}) = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$$

a x,y sú dané rovnicami (6.23).

Za povšimnutie stojí fakt, že kapacita závisí od toho, či posiela Alica alebo Bob. Dôvod je v tom, že vo všeobecnosti $\varrho_A \neq \varrho_B$. Vidno to aj z vyjadrení x a y (6.23), v ktorých stačí zamenit' λ_3 za λ_4 a dostávame x', y', ktoré tvoria diagonálne prvky ϱ_B. Kapacita teda pre niektoré zmesi, ktoré Alica a Bob zdieľajú môže spĺňat' nerovnost'

$$C^{ent}_{A\to B} \neq C^{ent}_{B\to A}.$$

Pre čisté stavy platí v tomto vzt'ahu vždy rovnost', lebo každý čistý stav vieme zapísat' v Schmidtovej dekompozícii.

Pri čistom binárnom prenose Alica pripravuje stavy iba dva a Bob odhaduje poslaný qubit iba meraniami na ňom samotnom. Alica pripravuje stavy s rovnakou entropiou. Uvažujme iba ideálny komunikačný kanál a vieme (Kapitola 5), že v tomto prípade je (5.4) abecedou, ktorá maximalizuje komunikačný kanál, ak jeden zo stavov máme zadaný. Túto kapacitu budeme označovat' $C^{bin}_{A\to B}$ a platí

$$C^{bin}_{A\to B} = 1 + |\alpha|^2 \log |\alpha|^2 + |\beta|^2 \log |\beta|^2.$$

Problém je ako porovnat' tieto dva druhy prenosu, alebo aký stav priradit' Alici (Bobovi) pri binárnom prenose, ak máme daný stav ϱ_{AB}, ktorého miera entanglovania nás zaujíma.

Predpokladajme, že medzi systémami nie je žiadna klasická korelácia. Stav, ktorý príde k Alici (Bobovi), je potom $\varrho_A(\varrho_B)$. Tento stav môžu použit', buď na husté kódovanie, alebo na prenos binárny. Keďže sme vylúčili možnost' klasickej korelácie, tak všetka korelácia medzi systémami je kvantová, t.j. entanglovanie. Rozdiel kapacít medzi prenosom hustým a binárnym by mohol vyjadrovat' číselne entanglovanie (označme E) v stave ϱ_{AB}. Treba vziat' do úvahy fakt, že kapacita v hustom prípade závisí od odosieľateľa. Zadefinujme

$$E(\varrho_{AB}) = \frac{1}{2}(C^{ent}_{A\to B} + C^{ent}_{B\to A} - C^{bin}_{A\to B} - C^{bin}_{B\to A})$$

Po dosadení dostávame vzt'ah, ktorý vyzerá veľmi jednoducho

$$E = S(\varrho_A) + S(\varrho_B) - S(\varrho_{AB}).$$

Je to vlastne iba veľmi známa vlastnosť entropie známa ako subaditívnosť (viď časť Entropia). Je známe, že E vyjadruje mieru korelácii medzi podsystémami. My sme ju dostali ako rozdiel kapacít ideálneho binárneho kanála pri hustom a obyčajnom kódovaní. Vidno, že E = 0, akk $\varrho_{AB} = \varrho_A \otimes \varrho_B$, t.j. sú separabilné, ale aj klasicky nekorelované. Existujú separabilné stavy, pre ktoré by E $\neq$ 0. Pre čisté stavy $E = 2S(\varrho_{A(B)})$, čo je známa miera na čistých stavoch.

Problém je, ak klasický stav je aj klasicky korelovaný. Skúsme sa pozrieť na separabilitu ľubovoľného stavu ϱ_{AB} metódou čiastočne transponovanej matice. Každý stav môžeme zapísať v spektrálnom tvare (6.21)

$$\varrho_0 = \sum_{i=1}^{4} \lambda_i |\psi_i^0\rangle\langle\psi_i^0|.$$

Zapísaný v Schmidtovej báze je určený parametrami $\alpha, \beta, \gamma, \delta, \lambda_i$ pre i = 1, 2, 3, 4, z ktorých je 5 nezávislých. Po transponovaní cez systém B má tvar

$$\varrho_{AB}^{T_B} = \begin{pmatrix} \lambda_1|\alpha|^2 + \lambda_2|\beta|^2 & 0 & 0 & \gamma\delta(\lambda_3 - \lambda_4) \\ 0 & \lambda_3|\delta|^2 + \lambda_4|\gamma|^2 & \alpha\beta(\lambda_1 - \lambda_2) & 0 \\ 0 & \alpha\beta(\lambda_1 - \lambda_2 & \lambda_4|\delta|^2 + \lambda_3|\gamma|^2 & 0 \\ \gamma\delta(\lambda_3 - \lambda_4) & 0 & 0 & \lambda_2|\alpha|^2 + \lambda_1|\beta|^2 \end{pmatrix}. \tag{6.29}$$

Pre vlastné hodnoty takejto matice platí

$$\begin{aligned} \kappa_1 &= \tfrac{1}{2}(\lambda_1 + \lambda_2 - \sqrt{P}) \\ \kappa_2 &= \tfrac{1}{2}(\lambda_1 + \lambda_2 + \sqrt{P}) \\ \kappa_3 &= \tfrac{1}{2}(\lambda_3 + \lambda_4 - \sqrt{Q}) \\ \kappa_4 &= \tfrac{1}{2}(\lambda_3 + \lambda_4 + \sqrt{Q}), \end{aligned} \tag{6.30}$$

kde

$$P = 4|\gamma|^2|\delta|^2(\lambda_3 - \lambda_4)^2 + (\lambda_1 - \lambda_2)^2(1 - 4|\alpha|^2|\beta|^2)$$
$$Q = 4|\alpha|^2|\beta|^2(\lambda_1 - \lambda_2)^2 + (\lambda_3 - \lambda_4)^2(1 - 4|\gamma|^2|\delta|^2).$$

Ak niektoré vlastné čísla sú záporné, tak potom tento stav je neseparabilný, V našom prípade sú κ_2, κ_4 vždy kladné. Podmienky, za ktorých sú zvyšné dve vlastné hodnoty kladné sú

$$(1 - 4|\alpha|^2|\beta|^2) \leq \frac{(\lambda_1 + \lambda_2)^2 - 4|\gamma|^2|\delta|^2(\lambda_3 - \lambda_4)^2}{(\lambda_1 - \lambda_2)^2}$$

$$(1 - 4|\gamma|^2|\delta|^2) \leq \frac{(\lambda_3 + \lambda_4)^2 - 4|\alpha|^2|\beta|^2(\lambda_1 - \lambda_2)^2}{(\lambda_3 - \lambda_4)^2}.$$

Pre konkrétne zadaný stav by sme teda vedeli určiť, kedy je separabilný a kedy je entanglovaný. Stále však E nevyjadruje mieru entanglovania, lebo entanglovaný stav môže byť aj klasicky korelovaný. Tu sme vlastne v jadre problému pri určovaní miery entanglovania. Nie je známa operácia, ktorá by oddelila klasickú koreláciu od entanglovania. Urobením čiastočnej stopy ignorujeme všetky korelácie. Čiastočnou transpozíciou rozlíšime "iba" medzi separabilnými a entanglovanými stavmi.

Ak by sme chceli, aby naše E pre separabilné stavy $\varrho_{AB} = \sum_i p_i \varrho_A^i \otimes \varrho_B^i$ dávalo nulu, tak môžeme zadefinovať

$$E(\varrho_{AB}) = \min_{rozklady} \left[\sum_i p_i (S(\varrho_A^i) + S(\varrho_B^i)) - \sum_i p_i S(\varrho_{AB}^i) \right],$$

čo by mohla byť miera entanglovania. Podmienky **E1,E2,E4** sú splnené. Problém je s podmienkou **E3**.

Pôvodnou snahou bolo zaviesť mieru, ktorá by sa dala jednoducho aj spočítať. Táto "miera" túto vlastnosť nespĺňa.

Kapitola 7

ZÁVER

Výsledky diplomovej práce sú v kapitole 6, kde sa podarilo spočítat' kapacitu ideálnych kvantových komunikačných kanálov pri hustom kódovaní pre l'ubovol'ný stav, ktorý pri tejto procedúre používame. Zároveň sme našli triedu transformácii, ktoré generujú abecedy, ktoré sú, čo sa kapacity týka, ekvivalentné. Pre triedy stavov vyjadrených v Schmidtovej dekompozícii v nejakej báze (*Schmidtovej*) sme našli lokálne unitárne transformácie, ktoré transformujú tento stav na stavy, ktoré sú navzájom rovnako rozlíšitel'né v zmysle prekryvov (*overlap*). Tieto transformácie sú univerzálne pre danú Schmidtovu bázu. Ďalej sme husté kódovanie rozšírili na N × N systémy, kde sme tiež spočítali kapacitu v prípade čistých stavov. Rozoberali sme prípady *šumového* a *Pauliho* komunikačného kanála (špeciálne *depolarizačného*). Na záver sme sa pokúsili zaviest' mieru entanglovania motivovanú hustým kódovaním. Toto sa nepodarilo dotiahnut' do úspešného konca. Popritom sa ukázala nesymetria kapacity komunikačného kanála pri zmene odosiel'ateľa a príjemcu.

Problémom pri určení kapacity (4.6) je nájst' najoptimálnejšie kódovanie π. Väčšinou stavy, z ktorých sa kapacita počítala, mali rovnakú entropiu. Pre N=2, sme v takomto prípade stavov dokázali , že optimálnym je kódovanie $\pi = 1/2$. Pre husté kódovanie s neúplne entanglovanými čistými stavmi sme to v našom prípade numericky spočítali, že optimálne je $\pi_{\mathrm{i}} = 1/4$. Ak je entropia stavov rovnaká, tak druhý člen je nezávislý od kódovania. Maximalizovat' kapacitu znamená maximalizovat' entropiu zmesi vystupujúcej v prvom člene. Vyslovíme nasledujúcu hypotézu:

Ak je zmes ϱ tvorená N stavmi s rovnakou entropiou, tak entropia tejto zmesi je maximálna, akk kódovanie bude práve $\pi_{\mathrm{i}} = 1/\mathrm{N}$. Inými slovami

$$\max_{\pi} S(\sum_i \pi_i \varrho_i) = S(\frac{1}{N} \sum_i \varrho_i).$$

Intuitívnym dôvodom, podporujúcim túto hypotézu, je interpretácia entropie ako miery našej neznalosti o systéme v danom stave. Nie je žiadny dôvod, prečo by niektorý z týchto stavov, mal byt' pri prenose uprednostňovaný.

Dodatok A

TEÓRIA PRAVDEPODOBNOSTI

Definícia: Nech $\mathbf{X}$ je množina a S je systém podmnožín taký, že
(i)$\emptyset, \mathbf{X} \in$ S
(ii)$\{\mathrm{E_j}\}_{\mathrm{j}\in\mathrm{J}} \in \mathrm{S} \Rightarrow \bigcup\limits_{\mathrm{j}\in\mathrm{J}} \mathrm{E_j} \in \mathrm{S}$
(iii)$\mathrm{E} \in \mathrm{S} \Rightarrow \mathbf{X} \setminus \mathrm{E} \in$S
Systém podmnožín nazývame σ-algebrou.

Definícia: Funkciu $\mu : S \to \mathbf{R}^+$ s vlastnost'ami
(i)$\mu(\emptyset) = 0$
(ii)$\{\mathrm{E_j}\}_{\mathrm{j}\in\mathrm{J}} \in \mathrm{S},\ \mathrm{E_j} \cap \mathrm{E_k} = \emptyset$ pre $\mathrm{j} \neq \mathrm{k} \Rightarrow \mu(\bigcap\limits_{\mathrm{j}\in\mathrm{J}}) = \sum\limits_{\mathrm{j}\in\mathrm{J}} \mu(\mathrm{E_j})$
(iii)$\mu(\mathbf{X}) = 1$
nazývame pravdepodobnostnou mierou μ na množine $\mathbf{X}$.Vlastnost' (ii) nazývame σ-aditívnost'.

Definícia:*Pravdepodobnostný priestor* je trojica ($\mathbf{X}$,S,μ), kde $\mathbf{X}$ je množina, na ktorej je definovaná σ-algebra S a pravdepodobnostná miera μ. Prvky z S nazývame náhodné udalosti.

Pre konečnú množinu je σ-algebra generovaná samotnými prvkami množiny a pravdepodobnostnú mieru stačí zadefinovat' tiež na týchto prvkoch (vid' definíciu hustoty pravdepodobnosti).

Definícia: Ak $\mathbf{X}$=$\mathbf{R}^{\mathrm{N}}$, (resp. $\mathbf{X}$ je spočítateľná množina), tak *hustotou pravdepodobnosti* nazveme funkciu p: $\mathbf{X}\to\langle 0,\infty)$, ktorá spĺňa nasledovný vzt'ah

$$\int_{\mathbf{X}} \mathrm{p(x)dx} = 1,\ (\mathrm{resp.} \sum_{\mathrm{x}\in\mathbf{X}} \mathrm{p(x)} = 1),$$

kde dx je Lesbeguova miera na $\mathbf{R}^{\mathrm{N}}$. Každá hustota pravdepodobnosti definuje pravdepodobnostnú mieru na $\mathbf{R}^{\mathrm{N}}$(resp. $\mathbf{X}$).

Definícia: Budeme hovorit' , že zobrazenie $\xi : \mathbf{X} \to \mathbf{R}$ je *náhodná veličina* na pravdepodobnostnom priestore ($\mathbf{X}$,S,μ), akk $\xi^{-1}(\mathbf{I}(\mathrm{a,b})) \in$ S pre všetky intervaly $\mathbf{I}$(a,b)$\subset \mathbf{R}$.

Definícia: Každá náhodná veličina ξ jednoznačne definuje *výberový pravdepodobnostný priestor* ($\mathbf{R}$,B,P_ξ), kde $\mathrm{P}_\xi(\mathbf{I}(\mathrm{a,b})) = \mu(\xi^{-1}(\mathbf{I}(\mathrm{a,b})))$ pre všetky intervaly.Systém intervalov tvorí σ-algebru $\mathbf{B}$ na $\mathbf{R}$.

Ak $\xi(\mathbf{X}) \subset \mathbf{R}$ je spočítateľná množina,tak ξ je diskrétna náhodná veličina. Zrejme existuje

hustota pravdepodobnosti p_ξ na $\xi(\mathbf{X})$ taká, že platí

$$\mathrm{P}_\xi(\mathrm{E}) = \sum_{\mathrm{x}\in\mathrm{E}} \mathrm{p}_\xi(\mathrm{x}) \text{ pre všetky } \mathrm{E} \subset \xi(\mathbf{X}).$$

Podobne, ak $\xi(\mathbf{X})$ je spojitý (nespočítateľný) priestor, tak existuje hustota p_ξ na $\mathbf{X}$ taká, že

$$\mathrm{P}_\xi(\mathrm{E}) = \int_{\mathrm{E}} \mathrm{p}_\xi(\mathrm{x})\mathrm{dx} \text{ pre všetky } \mathrm{E} \subset \xi(\mathbf{X}).$$

V tomto prípade hovoríme, že ξ je spojitá náhodná veličina.

Definícia:*Distribučná funkcia* F:$\mathbf{R}\to\mathbf{R}$ *náhodnej premennej* ξ je definovaná rovnosťou

$$\mathrm{F}(\mathrm{x}) = \mathrm{P}_\xi(\{\mathrm{y} : \xi(\mathrm{y}) < \mathrm{x}\}).$$

Definícia: Množinu $\{\xi_\mathrm{i} : \mathrm{i} = 1,\ldots,\mathrm{N}\}$, kde každá ξ_i je náhodná veličina na ($\mathbf{X}$,S,μ), nazveme *systémom náhodných veličín* na tomto pravdepodobnostnom priestore. Výberový pravdepodobnostný priestor systému $\{\xi_\mathrm{i} : \mathrm{i} = 1,\ldots,\mathrm{N}\}$ definujeme ako trojicu $(\mathbf{R}^\mathrm{N}, \mathbf{\Omega}, \mathrm{P})$, kde Ω je σ-algebra na kartézskom súčine $\mathbf{R}^\mathrm{N}$, ktorej prvky sú kartézske súčiny prvkov zo $\sigma-$algebier Ω_i výberových priestorov jednotlivých ξ_i. Pravdepodobnosť P je definovaná vzťahom

$$\mathrm{P}(\mathbf{K}) = \mu(\bigcap_{\mathrm{i}=1}^{\mathrm{N}} \xi_\mathrm{i}^{-\mathbf{1}}(\mathrm{K_i}))$$

pre všetky $\mathbf{K} \subset \mathbf{\Omega}$, $\mathbf{K}$=$\mathrm{K}_1 \times \ldots \times \mathrm{K}_\mathrm{N}$, kde $\mathrm{K_i} \subseteq \Omega_\mathrm{i}$.

Definícia: Nech $\xi_1,\ldots,\xi_\mathrm{N}$ je systém náhodných veličín s výberovým priestorom $(\mathbf{X}, \mathbf{\Omega}, \mathrm{p}_{\xi_1\ldots\xi_\mathrm{N}})$, kde $\mathbf{X}\subseteq \mathbf{R}^\mathrm{N}$. Uvažujme podsystém systému náhodných veličín $\mathbf{B}$=$\{\xi_\mathrm{i} : \mathrm{i} \in \mathrm{B}\}$, kde B je podmnožina množiny indexov {1,...,N}. Výberový priestor podsystému $\mathbf{B}$ je $(\mathbf{X}^{\mathrm{card\ B}}, \mathbf{\Omega} \cap \mathbf{X}^{\mathrm{card\ B}}, \mathrm{P}^\mathrm{B})$, kde P^B je dané hustotou *marginálnej* pravdepodobnosti

$$\mathrm{p}_\mathbf{B}(\{\mathrm{x_i} : \mathrm{i} \in \mathrm{B}\}) = \sum_{\mathrm{i}\notin\mathbf{B}} \sum_{\mathrm{x_i}\in\mathbf{X}} \mathrm{p}_{\xi_1\ldots\xi_\mathrm{N}}(\mathrm{x}_1,\ldots \mathrm{x}_\mathrm{N}).$$

V prípade, ak je náhodná veličina ξ_i spojitá , tak suma pre toto i prechádza na integrál.

Definícia: Náhodné udalosti A,B sa nazývajú *nezávislé*, ak

$$\mathrm{P}(\mathrm{A} \cap \mathrm{B}) = \mathrm{P}(\mathrm{A})\mathrm{P}(\mathrm{B}).$$

Náhodné veličiny $\xi, \eta : \mathbf{X} \to \mathbf{R}$ sa nazývajú *nezávislé*, ak sú nezávislé udalosti $\xi^{-1}(\mathrm{E}), \eta^{-1}(\mathrm{F})$ pre všetky intervaly E,F, t.j

$$\mathrm{P}(\xi^{-1}(\mathrm{E}) \cap \eta^{-1}(\mathrm{F})) = \mathrm{P}(\xi^{-1}(\mathrm{E}))\mathrm{P}(\eta^{-1}(\mathrm{F})).$$

V tejto definícii je istá jemnosť v chápaní náhodných udalostí. Vieme, že náhodné udalosti sú prvky zo σ-algebry definovanej na nejakej množine X. Ak vyjdeme z definície pravdepodobnosti, tak je zrejmé, že pre dva prvky σ-algebry platí $\mathrm{P}(\mathrm{A} \cap \mathrm{B}) = 0$, ak je prienik týchto množín prázdna

množina. Nie je žiadny dôvod, prečo by takéto dva javy mali mať nulovú pravdepodobnosť, a ani to nezodpovedá našej skúsenosti.

Vtip je v tom, že nezávislosť sa týka dvoch udalostí, ale v rôznych časoch. Pravdepodobnosť dvoch takýchto udalostí bude definovaná na kartézskom súčine $X \times X$. Všetky možnosti, o ktoré sa môžeme zaujímať sú prvky σ-algebry na kartézskom súčine, ktorá je definovaná cez σ-algebru na množine X. V tejto definícii je pravdepodobnosť definovaná na kartézskom súčine $X \times X$. Množinu A chápeme ako $A \times X$ a B ako $X \times B$.

Pre systém náhodných veličín táto definícia hovorí , že hustota pravdepodobnosti $p_{\xi_1,\ldots,\xi_N}$, ktorá je definovaná na $\mathbf{R}^N$ analogicky ako p_ξ v jednorozmernom prípade, (t.j. $P(\mathbf{K})=\int_{\mathbf{K}} p_{\xi_1,\ldots,\xi_N}(x)dx$), sa dá zapísať ako súčin jednorozmerných hustôt pravdepodobností pre jednotlivé náhodné veličiny p_{ξ_i}, t.j.

$$p_{\xi_1,\ldots,\xi_N}(x_1,\ldots,x_N) = \prod_{i=1}^{N} p_{\xi_i}(x_i),$$

tak systém náhodných veličín je nezávislý.

Teraz sa pokúsime zaviesť pojem *podmienenej pravdepodobnosti.* Začneme s príkladom:

Nech N je počet ľudí v skupine, medzi ktorými je m mužov a z nich je k vysokých. Aká je pravdepodobnosť $P(V|M)$, že v tejto skupine je náhodne vybratý muž vysoký? Zrejme

$$P(V|M) = \frac{k}{m} = \frac{\frac{k}{N}}{\frac{m}{N}} = \frac{P(V \cap M)}{P(M)}.$$

Dostali sme teda pravdepodobnosť, že ak jav spĺňa podmienku M, tak bude spĺňať aj podmienku V. Čo je v tomto prípade výberový priestor $\mathbf{X}$ a aká je σ-algebra, na ktorej je definovaná pravdepodobnostná miera? Aké možnosti vlastne pri tomto probléme uvažujeme? Máme štyri možnosti: vysoký muž, malý muž, vysoká žena, malá žena. Toto je náš výberový priestor $\mathbf{X}$. Keďže ide o konečnú množinu, tak za σ-algebru môžeme vziať množinu všetkých podmnožín množiny $\mathbf{X}$.

Vlastne kvôli prípadom, keď množina nie je spočítateľná, potrebujeme objekt σ-algebry, na ktorom definujeme pravdepodobnostnú mieru, lebo nie vždy má zmysel definícia pravdepodobnostnej miery na jednotlivých prvkoch $\mathbf{X}$. Ide práve o prípad, ak $\mathbf{X}$ je spojitá množina, na ktorej ak by mal jeden bod nenulovú pravdepodobnostnú mieru, tak celý priestor by mal mieru ∞.

Na tomto našom priestore si môžeme zadať štyri podmienky (poprípade ich kombinácie):vybratý prvok, t.j. človek, je muž, je žena, je vysoký, je malý, pričom vidno, že každá z týchto podmienok vlastne rozdeľuje $\mathbf{X}$ na dva podpriestory, z ktorých každý je prvkom σ-algebry, t.j. má určenú aj pravdepodobnosť. Podmienená pravdepodobnosť nie je pravdepodobnosť určená jednou podmienkou (napr. človek je vysoký muž), lebo hodnota tejto pravdepodobnosti je určená hneď, ak si uvedomíme, že táto podmienka vlastne určuje prvok zo σ-algebry, ktorého pravdepodobnosť je známa. Podmienená pravdepodobnosť je spojenie dvoch podmienok, ktoré určujú dva prvky zo σ-algebry. To spojenie má vyjadrovať pravdepodobnosť splnenia jednej podmienky, ak druhá už platí. To jest druhá podmienka nám už rozdelila $\mathbf{X}$ na dva podpriestory a mňa zaujíma pravdepodobnosť prvej podmienky iba na podpriestore, kde druhá podmienka platí, čo sa dá zapísať práve tým vzťahom, ktorý je uvedený ako posledný.

Výsledky z predchádzajúceho príkladu sa dajú rozšíriť na ľubovoľnú množinu $\mathbf{X}$ s definovanou σ-algebrou S a pravdepodobnostnou mierou P. Ďalej majme množinu podmienok M, ktorá nám určuje, ktorý prvok z S máme brať do úvahy, ak sa zaoberáme podmienenou pravdepodobnosťou za podmienok M. Tento prvok $\mathbf{X}_M$ zo σ-algebry tvorí nový výberový priestor, na ktorom je σ-algebra S_M definovaná množinami, ktoré vzniknú ako prienik $\mathbf{X}_M$ s množinami z pôvodnej σ-algebry S. Vidno, že takto definované S_M je skutočne σ-algebrou na $\mathbf{X}_M$. Pravdepodobnostná miera P_M na S_M je tiež jednoznačne určená z P vzťahom $P_M(E)=P(E)/P(\mathbf{X}_M)$ pre všetky $E \in S_M$. Analogicky ako v príklade platí, že P_M nie je ešte podmienenou pravdepodobnosťou. Potrebujeme nejaké iné

podmienky V, ktorých pravdepodobnosť splnenia, ak sú už podmienky M splnené, nás zaujíma. Podmienky V takisto určia trojicu$(\mathbf{X}_V, S_V, P_V)$ podobne ako pre M. Podmienená pravdepodobnosť je potom

$$P(V|M) = P_M(\mathbf{X}_V \cap \mathbf{X}_M) = \frac{P(\mathbf{X}_V \cap \mathbf{X}_M)}{P(\mathbf{X}_M)}. \tag{A.1}$$

Definícia:*Hustotou podmienenej pravdepodobnosti* nazveme nezápornú funkciu $p_{V|M}$, ktorá spĺňa $P(V|M)=\int_{\mathbf{X}_V \cap \mathbf{X}_M} p_{V|M} dx_M$ pre spojitý prípad. V diskrétnom prípade integrál nahradíme sumou.

Uvažujme systém náhodných veličín $\xi_1, \ldots, \xi_N$, z ktorých vyberme podmnožinu $\mathbf{B}$ náhodných veličín. Pomocou tejto podmnožiny môžeme zadať podmienku, napr. v prípade diskrétnych náhodných veličín aby $\xi_i = x_i$ pre všetky $\xi_i \in \mathbf{B}$. Uvedomme si, že celý výberový priestor tvorí kartézsky súčin výberových priestorov jednotlivých náhodných veličín ξ_i, takže daná podmienka je splnená na kartézskom súčine, v ktorom sú zafixované niektoré súčinitele práve touto podmienkou. Takto vzniknutá množina tvorí nový výberový priestor, na ktorom skúmame druhú podmienku C, ktorá môže byť určená fixnými hodnotami nejakých ešte nezafixovaných náhodných veličín, t.j. pre $\xi_i \notin \mathbf{B}$. Hustota podmienenej pravdepodobnosti je v špeciálnom prípade $\mathbf{C} = \mathbf{B}^C$, kde $\mathbf{B}^C$ je množina všetkých $\xi_i \notin \mathbf{B}$, určená vzťahom

$$p_{\mathbf{B}^C|\mathbf{B}}(x_i \in \mathbf{B}^C) = \frac{p_{\xi_1 \ldots \xi_N}(x_1, \ldots, x_N)}{p_{\mathbf{B}}(\{x_i : \ i \in B\})}, \text{ ak } p_{\mathbf{B}}(\{x_i : \ i \in B\}) \neq 0. \tag{A.2}$$

Teraz sa ešte oboznámime s *Bayesovým zákonom pre podmienenú pravdepodobnosť.* Tento zákon súvisí s pohľadom na samotný pojem pravdepodobnosti. Niekedy sa pravdepodobnosť chápe ako relatívna frekvencia, čo má význam, ak počet opakovaní pokusu je nekonečný, čo ale nezodpovedá úplne realite. Samotný zákon je vyjadrený nasledovne

$$P(A|B) = P(B|A)P(A)/P(B). \tag{A.3}$$

Tento zákon má význam v samotnej interpretácii merania. Dá sa dostať dosť triviálne zo samotnej definície podmienenej pravdepodobnosti (A.1) porovnaním $P(A|B)$ a $P(B|A)$.

Dodatok B

POJMY f-DIVERGENCIE, f-ENTROPIE, f-INFORMÁCIE

Motiváciou k zavedeniu pojmu f-divergencie je problém kvantitatívneho posúdenia podobnosti dvoch pravdepodobnostných modelov toho istého reálneho systému. Pri pevnom $\mathbf{X}$ ide o rozlíšiteľnosť hustôt pravdepodobností, alebo im príslušných pravdepodobností.

Definícia:*f-divergenciu* budeme označovať $D_f(P_1, P_2)$ a definovať pre ľubovoľnú *konvexnú* funkciu f, t.j. f(z) je spojitá a ku každému z_0 existuje $\lambda(z_0)$ také, že platí $f(z) \geq f(z_0)+\lambda(z_0)(z-z_0)$ pre $z \neq z_0$, definovanú na $(0,\infty)$, ktorá je naviac *striktne konvexná* v bode z=1, t.j. $f(z)>f(1)+\lambda(z-1)$ pre $z\neq 1$, výrazom

$$D_f(P_1, P_2) = \sum_{x\in\mathbf{X}} p_2(x) f\left(\frac{p_1(x)}{p_2(x)}\right). \tag{B.1}$$

Za maximálne divergentné (nepodobné) je prirodzené považovať také modely, v ktorých sú pravdepodobnosti P_1 a P_2 *ortogonálne*, t.j. existujú disjunktné podmnožiny $E,F\subset\mathbf{X}$, pre ktoré platí $P_1(E) = 1$ a $P_2(F) = 1$.

Ak zadefinujeme funkciu $\tilde{f}(z)=f(z)-f(1)$, tak pre f je konvexnú a striktne konvexnú v z=1 tieto vlastnosti má aj $\tilde{f}$, pričom $\tilde{f}(1)=0$. Teda môžeme bez narušenia všeobecnosti definície f-divergencie predpokladať, že f(1)=0.

Pre f-divergenciu platia tieto nerovnosti

$$0 \leq D_f(P_1, P_2) \leq f(0) + \lim_{z\to\infty} \frac{f(z)}{z}$$

kde ľavá rovnosť platí, akk $P_1 = P_2$, lebo vtedy $\frac{p_1}{p_2} = 1$ a f(1)=0. Pravá rovnosť, ak (v prípade $f(0)+\lim_{z\to\infty} \frac{f(z)}{z} < \infty$ práve vtedy, keď) sú navzájom ortogonálne. Uvedieme si niekoľko príkladov f-divergencií:

- **I-divergencia**: f(z)=zlog(z) a analytické vyjadrenie

$$I(P_1, P_2) = \sum_{x\in\mathbf{X}} p_1(x) \log \frac{p_1(x)}{p_2(x)}$$

- β**-divergencia**: $f(z)=|z^\beta-1|^{1/\beta}$ pre $\beta \in (0, 1)$, ktorá sa pre β=2 nazýva *Hellingerova vzdialenosť* a má nasledovné analytické vyjadrenie

$$D_{1/2} = 2(1 - \sum_{x\in\mathbf{X}} (p_1(x)p_2(x))^{1/2}$$

- α-**divergencia**: f(z)=sign$(\alpha-1)(z^\alpha-1)$ pre $\alpha\in(0,\infty)$
- χ-**divergencia**: f(z)=$|z-1|^\alpha$, ktorá sa pre $\alpha=1$ nazýva *totálnou variáciou* a má tvar

$$\chi^1(p_1,p_2)=\sum_{x\in X}|p_1(x)-p_2(x)|$$

Uvažujme teraz, že $P_{\xi\eta}$ je výberová pravdepodobnosť dvoch náhodných veličín ξ,η, t.j máme $p_{\xi\eta}$ na výberovom priestore X×Y, kde X,Y sú výberové priestory jednotlivých veličín. Zadefinujme marginálne pravdepodobnosti

$$p_\xi(x):=\sum_{y\in Y}p_{\xi\eta}(x,y)$$

$$p_\eta(y):=\sum_{x\in X}p_{\xi\eta}(x,y).$$

V prípade, že niektorý z výberových priestorov z X,Y je spojitý, t.j. interval z $\mathbf{R}$, tak príslušné sumy prejdú na integrály podľa pravidla $\sum_{x\in X}\to\int_X dx$. Pravdepodobnosť $P_{\xi\eta}$ bude hrať úlohu P_1 v predošlom a úlohu P_2 bude hrať $P_\xi\times P_\eta$, t.j. máme určené všetky objekty, ktoré vystupujú v definícii f-divergencie a teda f-divergencia nám určuje mieru nezávislosti dvoch náhodných veličín, lebo pre nezávislé veličiny platí $p_{\xi\eta}(x,y)=p_\xi(x)p_\eta(y)$ a teda $D_f(P_{\xi\eta},P_\xi\times P_\eta)=0$.

Definícia:*f-informáciou* vo veličine η o veličine ξ nazveme funkciu definovanú nasledovne

$$I_f(\xi,\eta):=D_f(P_{\xi\eta},P_\xi\times P_\eta) \tag{B.2}$$

Tento vzťah vyjadruje intuitívne chápanie: čím väčšia je štatistická väzba medzi ξ a η, tým viacej informácie musí niesť η o ξ a aj naopak, pričom platí

$$I_f(\xi,\eta)=I_f(\eta,\xi).$$

Ku každej f-divergencii je priamo z definície priradená f-informácia. My si uvedieme iba Shannonovu informáciu, ktorá prislúcha I-divergencii:

$$I(\xi,\eta)=\sum_{x\in X}\sum_{y\in Y}p_{\xi\eta}(x,y)\log\frac{p_{\xi\eta}(x,y)}{p_\xi(x)p_\eta(y)} \tag{B.3}$$

Každú $I_f(\xi,\eta)$ môžeme chápať ako mieru množstva informácie, ktoré získame o realizácii ξ, ak pozorujeme realizáciu η za predpokladu, že obidve tieto realizácie boli získané pri náhodnom pokuse, ktorý sa riadi pravdepodobnosťou $P_{\xi\eta}$ na X×Y. Všimnime si , že nehovoríme o konkrétnych realizáciach ξ alebo η. Takže ide o globálnu mieru informácie, ktorá ale nič nehovorí o tom, že ak pri realizácii η nameriam konkrétne y∈Y, tak koľko informácie mám o nejakom konkrétnom x∈X.

Definícia:*f-informáciou v realizácii $\eta=y$ o realizácii $\xi=x$* nazveme funkciu

$$I_f(x,y)=\frac{p_\xi(x)p_\eta(y)}{p_{\xi\eta}(x,y)}f\left(\frac{p_{\xi\eta}(x,y)}{p_\xi(x)p_\eta(y)}\right).$$

Táto funkcia síce môže byt' záporná, ale je nulová, ak sú javy ξ=x a η=y nezávislé, t.j. platí $p_\xi(x)p_\eta(y) = p_{\xi\eta}(x,y)$. Pre $I_f(\xi,\eta)$ potom platí

$$I_f(\xi,\eta) = \sum_{x\in X}\sum_{y\in Y} I_f(x,y)p_{\xi\eta}(x,y)$$

Definícia: Pre diskrétnu náhodnú veličinu ξ s výberovým pravdepodobnostným priestorom (X,p_ξ) a pre každú konvexnú funkciu f(u) s f(1)=0, f(0)$<\infty$ a $\lim_{u\to\infty}\frac{f(u)}{u^2} = 0$ definujeme *f-entropiu* ako nasledovnú funkciu

$$H_f(\xi) = \sum_{x\in X} p_\xi(x)^2 f\left(\frac{1}{p_\xi(x)}\right) + f(0)\sum_{x\in X} p_\xi(x)(1-p_\xi(x)), \tag{B.4}$$

kde $0^2 f(\frac{1}{0}) = 0$.

Dá sa ukázat', že pre ξ a η diskrétne platí $I_f(\xi,\eta) \le H_f(\xi)$, odkial' vyplýva $I_f(\xi,\xi) = H_f(\xi)$. Takže z tohto vzt'ahu vidno interpretáciu H_f, ktorý nám teda určuje množstvo informácie, ktoré o ξ získame, ked' pozorujeme priamo ξ. Táto informácia môže byt' aj mierou neurčitosti náhodnej veličiny ξ (neurčitosti systému opísaného pravdepodobnost'ou P_ξ), kde pod neurčitost'ou rozumieme t'ažkost' predpovede o realizácii veličiny ξ na základe znalosti pravdepodobnosti P_ξ, lebo t'ažkost' takejto predpovede by mala byt' úmerná informácii získanej realizáciou (pozorovaním) ξ.

Pre spojité náhodné veličiny je $I_f(\xi,\xi)$ konštanta f(0)+$\lim_{u\to\infty}\frac{f(u)}{u}$, ktorá nám nič nehovorí o ξ. Ak formálne prepíšeme B.4 pre spojitý prípad, tak dostaneme

$$H_f(\xi) = \int_{-\infty}^{\infty} p_\xi(x)^2 f\left(\frac{1}{p_\xi(x)}\right)dx \; + f(0)\int_{-\infty}^{\infty} p_\xi(x)(1-p_\xi(x))dx,$$

ktorý má stále pre nejaké f charakter miery neurčitosti, ale neplatí $I_f(\xi,\xi) = H_f(\xi)$.

Majme dve diskrétne náhodné veličiny ξ, η na (X×Y, $p_{\xi\eta}$). Pozrime sa na hodnotu f-entropie veličiny ξ, ak je daná nejaká pevná hodnota $\eta = y \in Y$. To znamená, že máme danú akúsi podmienku, ktorá nám výberový pravdepodobnosný priestor redukuje na množinu X×y, čo je prvok zo σ-algebry, na ktorom platí táto podmienka, a s hustotou pravdepodobnosti (A.2)

$$p_{\xi|y} = \frac{p_{\xi\eta}(x,y)}{p_\eta(y)}, \text{ ak } p_\eta(y) > 0.$$

Ak $p_\eta(y) = 0$, tak podmienená pravdepodobnost' je určená l'ubovol'ne.

Definícia: Príslušnú f-entropiu ku $p_{\xi|y}$ budeme nazývat' *podmienená f-entropia* náhodnej veličiny ξ za podmienky η=y, pričom pre ňu platí

$$H_f(\xi|\eta = y) = \sum_{x\in X} p_{\xi|y}(x)^2 f\left(\frac{1}{p_{\xi|y}(x)}\right) + f(0)\sum_{x\in X} p_{\xi|y}(x)(1-p_{\xi|y}(x)).$$

Strednú podmienenú f-entropiu zadefinujeme nasledovne

$$H_f(\xi|\eta) = \sum_{y\in Y} H_f(\xi|\eta = y)p_\eta(y). \tag{B.5}$$

Medzi podmienenou hustotou $p_{\xi|y}$ a nepodmienenou hustotou p_ξ neexistuje nijaká závislost', z ktorej by vyplývala nerovnost' $H_f(\xi) \geq H_f(\xi|\eta = y)$. Opačná ostrá nerovnost' pre všetky y by znamenala, že je t'ažšie predpovedat' realizáciu ξ pri znalosti podmienenej pravdepodobnosti, čo odporuje našej intuitícii.Dá sa ukázat' pre určité f, že aspoň v priemere platí správna nerovnost'.

Rozdiel $H_f(\xi) - H_f(\xi|\eta)$ medzi nepodmienenou a podmienenou entropiou veličiny ξ sa dá považovat' za mieru informácie v η o ξ. Ostáva nevyriešená otázka, pre ktoré f platí rovnica

$$H_f(\xi) - H_f(\xi|\eta) = I_f(\xi, \eta) \tag{B.6}$$

Ako príklad si uvedieme Shannonovu entropiu definovanú na náhodných veličinách $\xi_1, \ldots, \xi_N$

$$H(\xi_1, \ldots, \xi_N) = \sum_{\mathbf{x} \in \mathbf{X}^N} p_{\xi_1,\ldots,\xi_N}(\mathbf{x}) \log \frac{\mathbf{1}}{p_{\xi_1,\ldots,\xi_N}(\mathbf{x})}, \tag{B.7}$$

pre ktorú uvedená rovnost'(B.6) platí, a ktorá sa vo fyzike vyskytuje najčastejšie. Je odvodená zo Shannonovej informácie (B.3) definovanej na diskrétnych veličinách $\xi_1, \ldots, \xi_N, \eta_1, \ldots, \eta_M$ vzt'ahom

$$I(\xi_1, \ldots, \eta_M) = \sum_{\mathbf{x} \in \mathbf{X}^N} \sum_{\mathbf{y} \in \mathbf{Y}^M} p_{\xi_1,\ldots,\eta_M}(\mathbf{x}, \mathbf{y}) \log \frac{p_{\xi_1,\ldots,\eta_M}(\mathbf{x}, \mathbf{y})}{p_{\xi_1,\ldots,\xi_N}(\mathbf{x}) p_{\eta_1,\ldots\eta_M}(\mathbf{y})}. \tag{B.8}$$

Podmienená pravdepodobnost'v tomto prípade je

$$H(\xi_1, \ldots, \xi_N|\eta_1, \ldots, \eta_M) = \sum_{\mathbf{y} \in \mathbf{Y}^M} p_{\eta_1,\ldots,\eta_M}(\mathbf{y}) H(\xi_1, \ldots, \xi_N|(\eta_1, \ldots, \eta_M) = \mathbf{y}),$$

kde

$$H(\xi_1, \ldots, \xi_N|(\eta_1, \ldots, \eta_M) = \mathbf{y}) = \sum_{\mathbf{x} \in \mathbf{X}^N} p_{\xi_1,\ldots,\xi_N|(\eta_1,\ldots,\eta_M)=\mathbf{y}}(\mathbf{x}) \log \frac{\mathbf{1}}{p_{\xi_1,\ldots,\xi_N|(\eta_1,\ldots,\eta_M)=\mathbf{y}}(\mathbf{x})}.$$

Ďalej platí

$$I(\xi_1, \ldots, \xi_N, \eta_1, \ldots, \eta_M) = H(\xi_1, \ldots, \xi_N) - H(\xi_1, \ldots, \xi_N|\eta_1, \ldots, \eta_M),$$

čo je práve analóg vzt'ahu (B.6). Dôležitá vlastnost' entropie je jej *aditívnost'*

$$H(\xi_1, \ldots, \xi_N) \leq H(\xi_1) + \ldots + H(\xi_N),$$

pričom rovnost' nastáva v prípade, akk $\xi_1, \ldots, \xi_N$ sú navzájom nezávislé náhodné veličiny.

Nech teraz $\xi_1, \ldots, \xi_N, \eta_1, \ldots, \eta_N$ je taký systém, že dvojice $(\xi_1, \eta_1), \ldots, (\xi_N, \eta_N)$ tvoria navzájom nezávislé podsystémy. Potom

$$I(\xi_1, \ldots, \xi_N, \eta_1, \ldots, \eta_N) = \sum_{i=1}^{N} (H(\xi_i) - H(\xi_i|\eta_i)),$$

alebo, čo môžeme prepísat' aj takto

$$I(\xi_1, \ldots, \xi_N, \eta_1, \ldots, \eta_N) = \sum_{i=1}^{N} I(\xi_i, \eta_i), \tag{B.9}$$

čo nazveme *aditívnost' informácie.*

Dodatok C

BELLOVE NEROVNOSTI

Uvažujme dvojicu fotónov, ktoré sa šíria v opačných smeroch a dvoch experimentátorov, ktorí merajú ich lineárnu polarizáciu. Pomenujme týchto experimentátorov Alica a Bob.

Predpokladajme, že každý z nich si vyberá z dvoch smerov, v ktorých zisťuje polarizáciu toho svojho fotónu. Nech Alica si vyberá merania v smeroch určenými uhlami α a γ a Bob do smerov β a γ. Pre ľubovoľnú orientáciu polarizátora sú dva možné výsledky merania, označme ich ± 1. Výsledky meraní pre jednotlivé smery α, β, γ označme a, b, c a môžu mať iba hodnoty ± 1.

Hypotéza, ktorú testujeme, je, že Alicine (Bobove) výsledky sú jednoznačne určené lokálnymi skrytými parametrami, ktoré síce nepoznáme, ale vzťahujú sa iba k Alicinmu (Bobovmu) fotónu a polarizátoru. Podmienka Einsteinovej lokálnosti je podmienkou nezávislosti Aliciných výsledkov od Bobových lokálnych parametrov, t.j.výsledok Alicinho merania nezávisí od smeru, v ktorom meria Bob.

Vieme, že merania Alici a Boba v tom istom smere γ sú úplne korelované, t.j. ak Alica nameria c, tak aj Bob nameria c. Poznamenajme, že tieto korelácie nemajú nič spoločné s ovplyvňovaním výsledkov Alicinho merania Bobovým výberom smeru merania. Bob môže merať v ľubovoľnom smere β a výsledky Alicinho merania γ neovplyvní. Toto je vyjadrením faktu, že výsledky merania závisia iba od lokálnych skrytých parametrov, v čom je skrytá podmienka Eisteinovej lokálnosti.

Pre ľubovoľné hodnoty a, b, c platí

$$a(b-c) = \pm(1-bc),$$

lebo ak $b = c$, tak sú obidve strany nulové a pre $b \neq c$ sú rovné ± 2. Pamätajme, že v skutočnosti iba dva z týchto troch možných experimentov môžu byť uskutočnené na jednom páre fotónov.

Predstavme si, že merania opakujeme viackrát. Keďže skryté parametre nemáme pod kontrolov, tak výsledky, ktoré sú nimi určené, sú náhodné. Stále však pre každé meranie platí uvedený vzťah. Môžeme sa zaujímať o stredné hodnoty cez tieto skryté parametre. Dostaneme tak Bellovu nerovnosť

$$|\langle ab\rangle - \langle ac\rangle| \leq 1 - \langle bc\rangle.$$

Vidno, že pri jej odvodzovaní, sme nikde nepoužili nejakú konkrétnu fyzikálnu teóriu. Použili sme iba podmienku Einsteinovej lokálnosti. Na konkrétnej teórii je určiť aké sú stredné hodnoty vystupujúce v tejto nerovnosti. Tieto stredné hodnoty môžu byť určené aj experimentálne. Teda experiment môže otestovať Bellovu nerovnosť.

Kvantová teória síce nevie určiť konkrétne výsledky pre konkrétny pár, ale vie určiť stredné hodnoty. V prípade polarizovaných fotónov v stave

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|\mathrm{xx}\rangle + |\mathrm{yy}\rangle),$$

kde $|\mathrm{x}\rangle$ je stav jedného fotónu polarizovaného v smere osi x (ak smer šírenia je smer z) a $|\mathrm{y}\rangle$ je stav fotónu polarizovaného v smere y. Stredná hodnota

$$\langle ab\rangle = \langle\phi^+|\sigma_\alpha \otimes \sigma_\beta|\phi^+\rangle = \cos 2(\alpha-\beta),$$

kde

$$\sigma_\alpha = |\mathrm{x}(\alpha)\rangle\langle\mathrm{x}(\alpha)| - |\mathrm{y}(\alpha)\rangle\langle\mathrm{y}(\alpha)|$$

a

$$|\mathrm{x}(\alpha)\rangle = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix} \qquad |\mathrm{y}(\alpha)\rangle = \begin{pmatrix} -\sin\alpha \\ \cos\alpha \end{pmatrix}$$

Ak dosadíme výsledok kvantovej teórie do Bellovej nerovnosti, tak dostaneme

$$|\cos 2(\alpha-\beta) - \cos 2(\alpha-\gamma)| + \cos 2(\beta-\gamma) \leq 1.$$

Nech

$$\alpha-\beta = \beta-\gamma = 30^\mathrm{o}$$

$$\alpha-\gamma = 60^\mathrm{o}$$

tak prídeme k sporu

$$|\frac{1}{2} - (-\frac{1}{2})| + \frac{1}{2} = \frac{3}{2} \leq 1.$$

Preto hovoríme, že kvantová teória narúša Bellove nerovnosti. Táto predpoveď kvantovej teórie je v zhode s experimentom, a teda hovoríme, že priamo experiment vyvracia Einsteinovu lokálnosť.

Uvedieme si este ako príklad aj inú Bellovu nerovnosť, ktorá je známa ako CHSH nerovnosť.

Zovšeobecnenie je v tom, že Bob nebude vyberať z meraní určenými β, γ, ale z meraní β, δ, t.j. nebude robiť meranie v tom istom smere ako Alica. Výsledky merania δ sú analogicky ako predtým $d = \pm 1$. Výsledky a, b, c, d potom spĺňajú

$$(a+c)b + (a-c)d = \pm 2,$$

pretože buď $a+c=0$ a $a-c=\pm 2$, alebo $a-c=0$ a $a+c=\pm 2$.

Po ustrednení cez skryté parametre dostávame CHSH nerovnosť

$$|\langle ab\rangle + \langle bc\rangle + \langle cd\rangle - \langle ad\rangle| \leq 2.$$

K narušeniu tejto nerovnosti kvantovou teóriou použijeme merania, pre ktoré

$$\alpha-\beta = \beta-\gamma = \gamma-\delta = 22.5^\mathrm{o}$$

$$\alpha-\delta = 67.5^\mathrm{o}.$$

Dosadením do CHSH nerovnosti prídeme k sporu

$$|\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} - (-\frac{1}{\sqrt{2}})| = 2\sqrt{2} \leq 2.$$

Keďže prichádzame k sporom, tak niečo musí byť zle (v zmysle nefyzikálne alebo fyzikálne nesprávne) pri odvádzaní týchto nerovností.

Nefyzikálny je zrejme predpoklad, že je možné naraz uvažovať o výsledkoch viacerých meraní, pričom k týmto meraniam ani neprichádza.

Dodatok D

KVANTOVÁ TELEPORTÁCIA

Ide o spôsob ako preniesť kvantový stav pomocou prenosu klasickej informácie a lokálnymi operáciami.

Nech Alica má stav

$$|\psi\rangle_{\mathrm{C}} = a|0\rangle_{\mathrm{C}} + b|1\rangle_{\mathrm{C}},$$

ktorý chce poslať Bobovi, ale sú od seba vzdialený a Alica môže poslať iba klasickú informáciu. Nech ale obidvaja zdieľajú maximálne entanglovaný stav dvoch qubitov $|\phi^+\rangle_{\mathrm{AB}}$. Alica spojí stav $|\psi\rangle_{\mathrm{C}}$ s jej časťou entanglovaného stavu a na tejto dvojici qubitov spraví *Bellove meranie*, ktorého výsledkom sú Bellove stavy (4.3). Informáciu o výsledku svojho merania pošle cez klasický komunikačný kanál Bobovi (ide o prenos dvoch bitov informácie), ktorý podľa prijatej správy urobí na svojom qubite z entanglovaného páru unitárne operácie podľa nasledujúceho pravidla

$$|\phi^+\rangle_{\mathrm{AC}} \to \mathbf{1}_{\mathrm{B}}$$
$$|\psi^+\rangle_{\mathrm{AC}} \to \sigma_1^{(\mathrm{B})}$$
$$|\psi^-\rangle_{\mathrm{AC}} \to \sigma_2^{(\mathrm{B})}$$
$$|\phi^-\rangle_{\mathrm{AC}} \to \sigma_3^{(\mathrm{B})}$$

a dostane u seba stav $|\psi\rangle$. Táto procedúra sa nazýva kvantová teleportácia. Zdanlivo je to v rozpore z no-cloning teorémom, ale Alica meraním svoj stav, ktorý teleportuje Bobovi, zničí.

Ukážme si ako to funguje. Rozpíšme si počiatočný stav nášho celkovo trojčasticového systému, kde systém teleportovaného stavu označme písmenom C

$$|\psi\rangle_{\mathrm{C}} \otimes |\phi^+\rangle_{\mathrm{AB}} = (a|0\rangle_{\mathrm{C}} + b|1\rangle_{\mathrm{C}}) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{\mathrm{AB}} = \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle)_{\mathrm{CAB}} =$$

$$= \frac{1}{2}a\{(|\phi^+\rangle + |\phi^-\rangle)_{\mathrm{AC}}|0\rangle_{\mathrm{B}} + (|\psi^+\rangle + |\psi^-\rangle)_{\mathrm{AC}}|1\rangle_{\mathrm{B}}\} + \frac{1}{2}b\{(|\phi^+\rangle - |\phi^-\rangle)_{\mathrm{AC}}|1\rangle_{\mathrm{B}} + (|\psi^+\rangle - |\psi^-\rangle)_{\mathrm{AC}}|0\rangle_{\mathrm{B}}\} =$$

$$= \frac{1}{2}(|\phi^+\rangle_{\mathrm{AC}}(a|0\rangle_{\mathrm{B}} + b|1\rangle_{\mathrm{B}}) + |\psi^+\rangle_{\mathrm{AC}}(a|1\rangle_{\mathrm{B}} + b|0\rangle_{\mathrm{B}}) + |\phi^-\rangle_{\mathrm{AC}}(a|1\rangle_{\mathrm{B}} - b|0\rangle_{\mathrm{B}}) + |\phi^-\rangle_{\mathrm{AC}}(a|0\rangle_{\mathrm{B}} - b|1\rangle_{\mathrm{B}})) =$$

$$= \frac{1}{2}|\phi^+\rangle_{\mathrm{AC}}|\psi\rangle_{\mathrm{B}} + \frac{1}{2}|\psi^+\rangle_{\mathrm{AC}}\sigma_1|\psi\rangle_{\mathrm{B}} + \frac{1}{2}|\psi^-\rangle_{\mathrm{AC}}(-i\sigma_2)|\psi\rangle_{\mathrm{B}} + \frac{1}{2}|\phi^-\rangle_{\mathrm{AC}}\sigma_3|\psi\rangle_{\mathrm{B}},$$

odkiaľ vidno dôvod voľby Bobových operácii v závislosti od prijatej správy od Alice, resp. Alicinho výsledku merania.

Čo by sa stalo v prípade, že by Alica a Bob nezdieľali úplne entanglovaný stav, alebo by zdieľali separabilný stav?

V prípade separabilného stavu by sme touto procedúrou nijako neovplyvnili stav systému B, a teda by k žiadnej teleportácii prísť nemohlo. Vlastne všetky tri systémy A,B,C by boli separabilné a aj po urobení Bellovho merania na A+C, by A+C a B zostali separované.

Dodatok E

MIERY ROZLÍŠITEĽNOSTÍ

Problém, ktorý vzniká pri dekódovaní, je v kvantovom prípade problémom rozlíšiteľnosti kvantových stavov z Bobovho merania. V tomto dodatku zavedieme niektoré miery rozlíšiteľností vyskytujúce sa v kvantovej teórii. Ide o analogický pojem ku f-divergencii pravdepodobnostných distribúcií zavedenej v dodatku B. Zdrojom k tomuto dodatku je článok [7].

•Pravdepodobnosť chyby

Po meraní máme rozhodnúť, ktorej pravdepodobnostnej distribúcii, p_1 alebo p_2, výsledok x zodpovedá. Pri rozhodovaní používame tzv. Bayesovu stratégiu, ktorá vychádza z Bayesovho zákona (A.3). Pravdepodobnosť, že pri výsledku x sa realizovala niektorá z pravdepodobnostných distribúcii p_k, k=0,1, bude

$$\Pr(\text{výsledok} = x \Rightarrow \text{distribúcia} = k) = \Pr(k)p_k(x)/\Pr(x)$$

kde Pr(x) označuje pravdepodobnostnú distribúciu, ktorá je získaná z merania a Pr(k) je pravdepodobnosť, s akou sa vyskytuje distribúcia p_k, čo je v našom prípade, keďže o tom nemáme žiadnu informáciu úplne náhodné, a teda Pr(k)=1/2. Dopíšeme pravú stranu

$$\Pr(x \Rightarrow p_k) = \frac{1}{2}p_k(x)/p(x).$$

Danému výsledku x priradíme distribúciu p_k ako maximum z množiny

$$\{\Pr(\text{výsledok} = x \Rightarrow \text{distribúcia} = k)\}_{k=1,2}$$

Priemerná pravdepodobnosť úspechu, t.j. správneho rozhodnutia, je potom

$$\sum_{x\in X} p(x)\max\{\Pr(x \Rightarrow p_1), \Pr(x \Rightarrow p_2)\} = \frac{1}{2}\sum_{x\in X}\max\{p_1(x), p_2(x)\}.$$

Priemerná pravdepodobnosť chyby nášho rozhodovania je

$$\mathrm{PE}(p_1, p_2) = \frac{1}{2}\sum_{x\in X}\min\{p_1(x), p_2(x)\},$$

kde X je množina možných výsledkov merania. Pre identické distribúcie PE=$\frac{1}{2}$, a pre ortogonálne PE=0. Kvantový analóg má istú jemnosť v tom, že robíme minimum cez všetky POVM merania, t.j. vyberáme najoptimálnejšie meranie, pri ktorom je priemerná chyba minimálna. Dá sa ukázať, že najoptimálnejším meraním je ortogonálne meranie v báze vlastných vektorov matice $|\varrho_1 - \varrho_2|$, t.j.

$$\mathrm{PE}(\varrho_1, \varrho_2) = \frac{1}{2} - \frac{1}{4}\mathrm{Tr}|\varrho_1 - \varrho_2|.$$

•Kolgomorova vzdialenosť

Opäť začnime klasickou definíciou

$$\mathrm{K}(\mathrm{p}_1, \mathrm{p}_2) = \frac{1}{2} \sum_{\mathrm{x} \in \mathrm{X}} |\mathrm{p}_1 - \mathrm{p}_2|.$$

Táto funkcia, narozdiel od predošlej, už vyjadruje vzdialenosť, lebo pre dve identické distribúcie K=0. Pre ortogonálne K=1. Kolmogorova vzdialenosť je až na násobok totálnou variáciou (vid' dodatok B). Medzi pravdepodobnosťou chyby a Kolmogorovou vzdialenosťou existuje nasledovný vzťah

$$\mathrm{PE}(\mathrm{p}_1, \mathrm{p}_2) = \frac{1}{2}(1 - \mathrm{K}(\mathrm{p}_1, \mathrm{p}_2))$$

Kvantový analóg Kolmogorovej vzdialenosti medzi stavmi definujeme ako maximum klasickej Kolmogorovovej vzdialenosti cez všetky POVM merania. Z predchádajúceho vzťahu vidno, že meranie, ktoré minimalizuje PE maximalizuje K, t.j.

$$\mathrm{K}(\varrho_1, \varrho_2) = \frac{1}{2}\mathrm{Tr}|\varrho_1 - \varrho_2|,$$

čo je až na násobok Trace-vzdialenosť na operátoroch.

•Bhattacharyyaov koeficient

$$\mathrm{B}(\mathrm{p}_1, \mathrm{p}_2) = \sum_{\mathrm{x} \in \mathrm{X}} \sqrt{\mathrm{p}_1(\mathrm{x})\mathrm{p}_1(\mathrm{x})}$$

Pre B=1 sú distribúcie identické a pre B=0 sú ortogonálne, t.j. nejde o funkciu vzdialenosti na množine distribúcii. Môže však byť chápaná ako skalárny súčin medzi pravdepodobnostnými distribúciami, ktoré interpretujeme ako vektory v dim(X)=m-dimenzionálnom priestore. Kvantový analóg definujeme v tomto prípade ako minimum cez všetky POVM merania a dá sa vyjadriť vzťahom

$$\mathrm{B}(\varrho_1, \varrho_2) = \mathrm{Tr}\left(\sqrt{\sqrt{\varrho_1}\varrho_2\sqrt{\varrho_1}}\right)$$

Na množine čistých stavov je Bhattacharyyaov koeficient ekvivalentný prekryvu, ktorý je definovaný cez skalárny súčin

$$\mathit{prekryv}(|\psi_1\rangle, |\psi_2\rangle) = |\langle\psi_1|\psi_2\rangle|. \tag{E.1}$$

Ako ho ale definovať pre zmesi?

Odpoveď je v možnosti purifikácie, kde $|\psi_1\rangle$ je purifikáciou ϱ_1 a $|\psi_2\rangle$ je purifikáciou ϱ_2.

$$\mathit{prekryv}(\varrho_1, \varrho_2) = \max |\langle\psi_1|\psi_2\rangle|,$$

kde maximum berieme cez všetky purifikácie. Dá sa ukázať, že

$$\mathit{prekryv}(\varrho_1, \varrho_2) = \mathrm{B}(\varrho_1, \varrho_2)$$

Na záver poznamenajme, že všetky tieto funkcie rozlíšiteľnosti sa nemenia pri unitárnej transformácii stavov.

Bibliography

[1] A.Perez, *Quantum Theory:Concepts and Methods,* 1993, Kluwer, Dordrecht

[2] I.Vajda, *Teória informácie a štatistického rozhodovania,* 1982, SNTL,

[3] J.Preskill, *Lectures Notes on Physics 229:Quantum Information and Computation,* 1998, www.theory.caltech.edu/people/preskill/ph229/notes

[4] M.B.Plenio,V.Vedral, *Entanglement in Quantum Information Theory,* 1999, xxx.lanl.gov/archive/quant-ph/9911??

[5] V.Vedral,M.B.Plenio, *Entanglement measures and purification procedures,* 1998, Phyz.Rev.A 57, str.1619

[6] A.S.Holevo, *The Capacity of Quantum Channel with General Signal States,* 1996, xxx.lanl.gov/archive/quant-ph/9611023

[7] Ch.A.Fuchs and J.van der Graaf, *Cryptographic Distinguishability Measures for Quantum Mechanical States,* 1997, xxx.lanl.gov/archive/quant-ph/9712042

[8] M.Horodecki,P.Horodecki,R.Horodecki, *Separability of mixed states: necessary and sufficient conditions,* 1996, xxx.lanl.gov/archive/quant-ph/9605038