Vedecká rada Fakulty matematiky, fyziky a informatiky
Univerzity Komenského v Bratislave

Mgr. Michal Sedlák

Autoreferát dizertačnej práce

Quantum theory of unambiguous measurements

na získanie akademickej hodnosti
philosophiae doctor
v študíjnom programe doktorandského štúdia
4.1.2 všeobecná fyzika a matematická fyzika

Bratislava, 2009

Dizertačná práca bola vypracovaná v dennej forme doktorandského štúdia v *Centre pre výskum kvantovej informácie* na Fyzikálnom ústave Slovenskej akadémie vied v Bratislave

Predkladateľ: Mgr. Michal Sedlák
Fyzikálny ústav SAV
Dúbravská cesta 9
845 11 Bratislava

Školiteľ: Prof. RNDr. Vladimír Bužek, DrSc.
Fyzikálny ústav SAV
Dúbravská cesta 9
845 11 Bratislava

Oponenti: Prof. RNDr. Anatolij Dvurečenskij, DrSc.
Matematický ústav SAV
Štefánikova 47
814 73 Bratislava

Prof. RNDr. Peter Prešnajder, DrSc.
Fakulta matematiky, fyziky a informatiky UK
Mlynská dolina F2
842 48 Bratislava

Dr. Mátyás Koniorczyk, PhD.
Institute of Physics, University of Pécs
H-7624 Pécs, Ifjúság útja 6
Hungary

Autoreferát bol rozoslaný: 11.9.2009

Obhajoba dizertačnej práce sa koná 22.10.2009 o 16:00 hod. pred komisiou pre obhajobu dizertačnej práce v študíjnom programe doktorandského štúdia vymenovanou predsedom spoločnej odborovej komisie 4.1.2, všeobecná fyzika a matematická fyzika na Fyzikálnom ústave SAV, Dúbravská cesta 9, 845 11 Bratislava.

Predseda spoločnej odborovej komisie
Prof. RNDr. Peter Prešnajder, DrSc.
FMFI UK, Mlynská dolina
842 48 Bratislava

Obsah

Úvod

V predkladanej dizertačnej práci formulujem matematický rámec, ktorý umožňuje jednotným spôsobom definovať kvantové úlohy bezchybného rozlišovania. Ukážem, že apriórna informácia o každej súčasti kvantového experimentu (stav, kanál, meranie) nám umožňuje preformulovať úlohy o rozlišovaní medzi konečným počtom alternatív na úlohy o rozlišovaní konečného počtu stredných stavov, kanálov, či meraní. S využitím uvedenej formulácie odvádzam riešenia viacerých úloh bezchybného rozlišovania.

1 Ciele dizertačnej práce

1. Vyriešiť úlohu bezchybného porovnávania dvoch konečných súborov kvantových stavov, preskúmať možnosti zlepšenia pre koherentné stavy a prípadne navrhnúť zodpovedajúci optický experiment.

2. Preskúmať riešiteľnosť úlohy bezchybnej identifikácie koherentných stavov a pokúsiť sa nájsť optimálne riešenie v rámci lineárnej optiky. Overiť klasické limity veľkého počtu neznámych stav, či referenčných stavov a kvantifikovať možnosti čiastočného obnovenia a opätovného použitia referenčných stavov pre ďalšiu bezchybnú identifikáciu. Ďalším cieľom je vyšetriť vplyv šumu na spoľahlivosť optimálneho merania.

3. Nájsť a charakterizovať všetky optimálne experimenty pre bezchybné porovnávanie dvojice unitárnych quditových kanálov a preskúmať využitie kvantového previazania (entanglementu) v nich.

4. Zadefinovať problém bezchybného porovnávania meraní. Zistiť pre aké druhy meraní má takáto úloha netriviálne riešenie a pokúsiť sa vyriešiť aspoň prípad dvojhladinových systémov (qubitov).

2 Model kvantového experimentu

Všeobecný experiment s kvantovým systémom môžeme popísať ako časovú následnosť troch udalostí: prípravy, vývoja a merania systému. Výsledným efektom týchto udalostí sú: príprava stavu ϱ, realizácia kvantového kanálu $\mathcal{E}$ (úplne pozitívnej, stopu zachovávajúcej lineárnej transformácie) a získanie klasickej informácie o výsledku merania k spojeného s efektom E_k. Kvantová mechanika predpovedá pravdepodobnosť namerania výsledku k známym Bornovým pravidlom $p_k = Tr(E_k\mathcal{E}(\varrho))$, pričom pozitivita a normalizácia pravdepodobností je zabezpečená pozitivitou POVM (positive operator valued measure) elementov E_k a ich normalizáciou $\sum_k E_k = I$. Namerané výsledky kvantového experimentu nám umožňujú doplniť chýbajúcu informáciu o jeho konštituentoch (preparátoroch, kanáloch a meraniach). V mojej dizertačnej práci sa venujem teoretickému návrhu takých experimentov, ktoré nám umožňujú bezchybne doplniť istý druh informácie o jednom z konštituentov uvažovaného experimentu. Matematicky sa dá takáto úloha, nazvaná *problém bezchybného rozlišovania*, sformulovať nasledovne:

Problém bezchybného rozlišovania (Unambiguous discrimination problem)

Predpokladajme, že máme k dispozícii jeden z konštituentov kvantového experimentu t.j. máme zariadenie, ktoré realizuje prípravu stavu, kanál, alebo meranie. Na nešťastie máme o činnosti tohto zariadenia len čiastočnú informáciu. Napríklad, vieme len, že zariadenie implementuje unitárny kanál, no nevieme ktorý. Našou úlohou je z jediného použitia uvažovaného zariadenia zodpovedať otázku o jeho fungovaní. Naše odpovede musia byť buď bezchybné (správne), alebo náš test zariadenia môže zlyhať, pričom na kladenú otázku nedávame žiadnu odpoveď. Cieľom je navrhnúť taký test zariadenia, ktorý uspeje (t.j. dá správnu odpoveď), čo najčastejšie. Nech písmená P, C a M zodpovedajú príprave stavu, kanálu a meraniu. Množinu $S_{\mathsf{X}}(\mathcal{H})$ pre $\mathsf{X} \in \{\mathsf{P}, \mathsf{C}, \mathsf{M}\}$ budeme nazývať množinou všetkých konštituentov typu X pre Hilbertov priestor $\mathcal{H}$. Neúplná vedomosť o zariadení, ktoré testujeme, je odzrkadlená v pravdepodobnostnej miere dA definovanej na $S_{\mathsf{X}}(\mathcal{H})$, ktorá vyjadruje hustotu pravdepodobnosti, že testovaný konštituent je skutočne A ($\int_{S_{\mathsf{X}}(\mathcal{H})} dA = 1$). Aby bola kladená otázka pre náš problém zmysluplná, musia možné odpovede rozdeliť množinu $S_{\mathsf{X}}(\mathcal{H})$ na M disjunktných podmnožín S_i. Označme $p_j(A)$ pravdepodobnosť odpovede j ak testujeme konštituent $A \in S_{\mathsf{X}}(\mathcal{H})$. Pravdepodobnosť zlyhania testu pomenujeme $p_0(A)$, pričom $j = 0$ označuje nekonkluzívny výsledok. Požiadavka bezchybnosti výsledkov testu je matematicky vyjadrená nasledovnými rovnicami

$$\forall i, j \in \{1, \ldots, M\}, \quad i \neq j, \quad \forall A \in S_i; \quad p_j(A) = 0. \tag{1}$$

Našim cieľom je maximalizovať

$$P_{succ} = \sum_{i=1}^{M} \int_{S_i} p_i(A) dA \,, \tag{2}$$

pravdepodobnosť správneho zodpovedania skúmanej otázky o testovanom zariadení pri dodržaní bezchybnosti výsledkov. Takto nadefinovaný problém zahŕňa všetky úlohy, ktoré chceme riešiť.

Reformulácia problému bezchybného rozlišovania

Z všeobecného pohľadu je dôležité, že vďaka linearite je možné problém bezchybného rozlišovania ekvivalentne preformulovať na bezchybné rozlišovanie M stredných konštituentov

$$A_i = \frac{1}{\eta_i} \int_{S_i} A \; dA, \quad \eta_i = \int_{S_i} dA \tag{3}$$

toho istého druhu. Stredné konštituenty A_i sú korektnými preparátormi, kanálmi, či meraniami a musia pre ne platiť nasledovné rovnice zaručujúce bezchybnosť výsledkov

$$\forall i \neq j, \quad \forall A \in S_i : \quad p_j(A) = 0 \quad \Leftrightarrow \quad p_j(A_i) = \frac{1}{\eta_i} \int_{S_i} p_j(A) \; dA = 0. \tag{4}$$

Podobne aj pravdepodobnosť úspechu (správneho zodpovedania otázky) je ľahko vyjadriteľná pomocou A_i:

$$P_{succ} = \sum_{i=1}^{M} \int_{S_i} p_i(A) dA = \sum_{i=1}^{M} p_i \left(\int_{S_i} A \; dA \right) = \sum_{i=1}^{M} \eta_i p_i(A_i). \tag{5}$$

Pre jednotlivé typy konštituentov je teda možné previesť každý problém bezchybného rozlišovania na bezchybné rozlišovanie známych zmiešaných stavov, kanálov, či meraní. V prípade stavov potrebujeme optimalizovať výber merania, ktoré testuje výstup skúmaného zariadenia. Matematicky táto optimalizácia zodpovedá hľadaniu viazaných extrémov funkcie P_{succ} na množine pozitívnych operátorových mier (POVM) spojenej s Hilbertovým priestorom $\mathcal{H}$ a výsledkovým priestorom $\{0, 1, \ldots, M\}$. Vo všeobecnosti je na uvažovanej väzbe danej rovnicami (4) veľa maxím. Namiesto priameho riešenia je vhodné problém najprv zjednodušiť. Pre prípad bezchybného rozlišovania dvoch zmiešaných stavov možno použiť Raynalové redukčné teorémy [1], ktoré buď rozkladajú problém na viacero nezávisle riešiteľných častí alebo redukujú dimenziu Hilbertovho priestoru v ktorom treba robiť optimalizáciu. Podobne možno využiť aj výsledky M. Kleinmanna, H. Kampermanna a D. Bruss [2]. Pre všeobecné dva zmiešané stavy je problém bezchybného rozlišovania stále otvorený, no pre viacero typov stavov sú už optimálne riešenia známe.

V prípade bezchybného rozlišovania kvantových kanálov je situácia komplikovanejšia. Donedávna totiž neexistoval pre popis experimentov testujúcich kanály koncept podobný POVM. Množina všetkých prípustných testov je totiž veľmi veľká a mnohé z testov sú ekvivalentné. Naštastie, M. Ziman [3] navrhol koncept Process positive operator valued measure (PPOVM), ktorý systematicky berie ekvivalentnosť testov kanálov do úvahy. Podobne ako pri POVM je experiment testujúci kvantové kanály popísaný sadou pozitívnych operátorov $\{M_k\}$ avšak tieto pôsobia na $\mathcal{H} \otimes \mathcal{H}$ a na rozdiel od POVM je PPOVM aj inak normalizované ($\sum_k M_k = \xi^T \otimes I,\ \xi \in S_{\mathsf{P}}(\mathcal{H})$). Voľnosť v normalizácii PPOVM výrazne komplikuje optimalizáciu a neumožňuje priamo aplikovať poznatky z rozlišovania stavov na rozlišovanie kanálov.

Pre rozlišovanie meraní nebol vhodný popis všeobecného experimentu doteraz zavedený. Komplikáciou je hlavne nepriamy súvis výsledkov testovaného meracieho zariadenia s výsledkami samotného testu. Z tohto dôvodu sa v práci obmedzujem len na scenár pri ktorom sa na meranie používajú len testované meracie zariadenia.

3 Úlohy bezchybného rozlišovania pre stavy

Moje originálne výsledky v štvrtej kapitole predloženej práce zahŕňajú dve témy: Bezchybné porovnávanie dvoch konečných súborov kvantových stavov a bezchybnú identifikácie koherentných stavov.

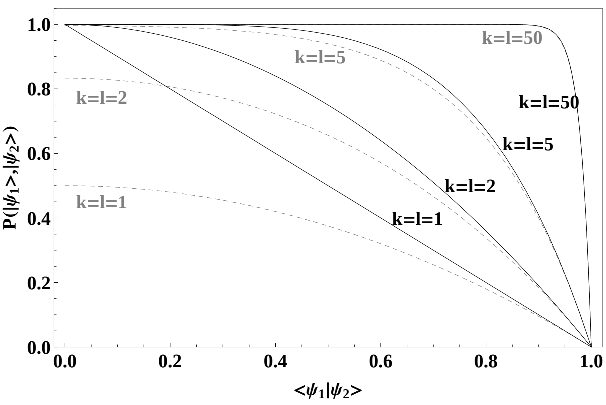
Porovnávanie dvoch preparátorov, ktoré pripravili k a l kópii dvoch neznámych stavov $|\psi_1\rangle$, $|\psi_2\rangle$ je ekvivalentné rozlišovaniu dvoch zmiešaných stavov (stredných konštituentov)

$$\begin{aligned}
\rho_1 &= \frac{1}{\eta_{same}} \int_{S_1} A dA = \int |\psi\rangle\langle\psi|^{\otimes k+l} d\psi = \frac{1}{d_{k+l}} P^{sym}_{1\ldots k+l} \,; \\
\rho_2 &= \frac{1}{\eta_{diff}} \int_{S_2} A dA = \int \psi_1^{\otimes k} \otimes \psi_2^{\otimes l}\, d\psi_1 d\psi_2 = \frac{1}{d_k d_l} P^{sym}_{1\ldots k} \otimes P^{sym}_{k+1\ldots k+l} \,,
\end{aligned}$$

kde $P^{sym}_{1\ldots k}$ je projektor na úplne symetrický podpriestor častí $1, \ldots, k$ systému a $d_k = Tr(P^{sym}_{1\ldots k})$. Keďže suport ρ_1 je podmnožinou suportu ρ_2 ($P^{sym}_{1\ldots k+l} \leq P^{sym}_{1\ldots k} \otimes P^{sym}_{k+1\ldots k+l}$), nie je možné bezchybne potvrdiť zhodnosť porovnávaných preparátorov stavov. Z tohto dôvodu je pravdepodobnosť úspechu

$$\begin{aligned}
P_{succ} \equiv P_{succ}(k,l) &= \eta_{same}.0 + \eta_{diff} \int_{S_{pure}} \int_{S_{pure}} d\psi_1 d\psi_2 P(|\psi_1\rangle, |\psi_2\rangle), \\
P(|\psi_1\rangle, |\psi_2\rangle) &= \langle\psi_1|^{\otimes k} \otimes \langle\psi_2|^{\otimes l} E_2 |\psi_1\rangle^{\otimes k} \otimes |\psi_2\rangle^{\otimes l}, \qquad (6)
\end{aligned}$$

priamo úmerná strednej podmienenej pravdepodobnosti odhalenia rozdielnosti preparátorov, ktoré sú rôzne a optimálne meranie je dané vzťahmi $E_2 = I - P^{sym}_{1\ldots k+l}$, $E_1 = 0$, $E_0 = P^{sym}_{1\ldots k+l}$. V práci odvádzam podmienenú



Obrázok 1: Optimálna pravdepodobnosť odhalenia rozdielnosti stavov $|\psi_1\rangle$, $|\psi_2\rangle$. Šedé prerušované čiary platia pre porovnávanie akýchkoľvek čistých stavov, zatiaľ čo čierne čiary platia len pre porovnávanie koherentných stavov. Každá čiara zodpovedá inému počtu kópii porovnávaných stavov.

pravdepodobnosť odhalenia rozdielnosti stavov

$$P(|\psi_1\rangle, |\psi_2\rangle) = 1 - \sum_{m=0}^{\min(k,l)} \frac{\binom{k}{m}\binom{l}{m}}{\binom{k+l}{k}} |\langle\psi_1|\psi_2\rangle|^{2m}, \tag{7}$$

pre ľubovoľné čisté stavy $|\psi_1\rangle, |\psi_2\rangle$. Táto pravdepodobnosť nezávisí na dimenzii porovnávaných kvantových systémov na rozdiel od strednej hodnoty

$$P_{succ}(k,l) = \eta_{diff}\left(1 - \frac{\dim(\mathcal{H}_{sym}^{\otimes k+l})}{\dim(\mathcal{H}_{sym}^{\otimes k})\dim(\mathcal{H}_{sym}^{\otimes l})}\right). \tag{8}$$

Ak je celkový počet kópii $N = k + l$ zafixovaný, je pravdepodobnosť úspechu maximalizovaná pre $k = l$, t.j. pre rovnaký počet kópii pripravených porovnávanými preparátormi. Pravdepodobnosť úspechu možno mierne zvýšiť na

$$P(|\alpha_1\rangle, |\alpha_2\rangle) = 1 - e^{-\frac{kl}{k+l}|\alpha_1-\alpha_2|^2}. \tag{9}$$

ak vieme, že porovnávané stavy $|\alpha_1\rangle, |\alpha_2\rangle$ sú koherentnými stavmi kvantovaných jednomódových elektro-magnetických (EM) polí. Zlepšenie je výrazné len pre malé k, l (pozri obrázok 1).

Pre optimálne porovnávanie koherentných stavov módov EM poľa sa mi podarilo navrhnúť aj schému pre optický experiment. Táto schéma je pomerne ľahko realizovateľná, keďže využíva len $k + l - 1$ deličov zväzkov a jeden fotodetektor. Zmienená schéma zovšeobecňuje experiment navrhnutý E. Andersson et.al. [6].

V predkladanej práci je najväčší priestor venovaný identifikácii stavov, pričom moje vlastné výsledky sa vzťahujú hlavne k bezchybnej identifikácii koherentných stavov. V tejto úlohe máme k dispozícii kvantové systémy, ktoré sú pripravené v koherentných stavoch a sú označené ako neznámy stav, či referenčné stavy. Z definície úlohy vieme, že jeden z referenčných stavov je rovnaký ako neznámy stav. Našou úlohou je zistiť, ktorý to je, pričom náš záver musí byť neomylný a pravdepodobnosť zlyhania merania, čo najmenšia. Našou snahou teda je navrhnúť meranie, ktoré dokáže bezchybne odlíšiť nasledovných M typov stavov

$$|\Psi_i\rangle_{ABC\ldots} \equiv |\alpha_i\rangle_A^{\otimes n_A} \otimes |\alpha_1\rangle_B^{\otimes n_B} \otimes |\alpha_2\rangle_C^{\otimes n_C} \otimes \ldots , \tag{10}$$

pričom $n_A, n_B, n_C, \ldots$ označujú počet kópii neznámeho stavu a jednotlivých referenčných stavov. Konkrétny výber referenčných stavov nepoznáme, vieme len pravdepodobnostné rozdelenie xi podľa, ktorého sú referenčné stavy vybrané a našim cieľom je maximalizovať priemernú pravdepodobnosť úspechu

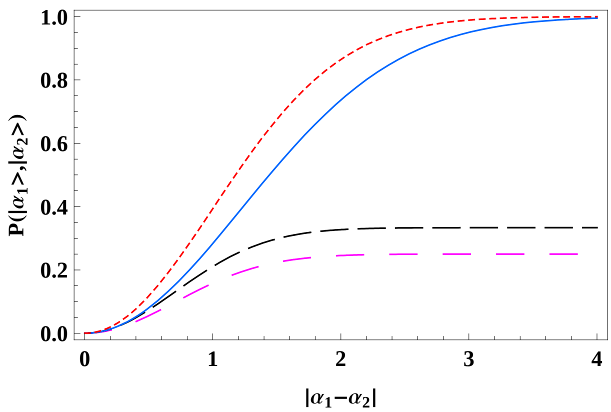
$$\overline{P(S_{coh})} = \int_{\mathbb{C}^M} P(|\alpha_1\rangle, \ldots, |\alpha_M\rangle)\chi(\alpha_1, \ldots, \alpha_M)\; d\alpha_1 \ldots d\alpha_M \; .$$

$$P(|\alpha_1\rangle, \ldots, |\alpha_M\rangle) = \sum_{k=1}^{M} \frac{1}{M} Tr(E_k |\Psi_k\rangle\langle\Psi_k|)$$

Ako prvou som sa zaoberal otázkou vplyvu apriórnej informácie o koherentnosti stavov na pravdepodobnosť úspechu bezchybnej identifikácie. Relevantnosť tejto apriórnej vedomosti som ilustroval tak, že som dokázal existenciu špecializovaného merania pre koherentné stavy, ktoré výrazne prekonáva univerzálne identifikačné meranie, t.j. meranie fungujúce bezchybne pre všetky čisté stavy. Zaujímavý kvalitatívny rozdiel medzi špecializovaným a univerzálnym identifikačným meraním je napríklad pre $M = 2, n_A = n_B = n_C = 1$ v pravdepodobnosti identifikácie takmer kolmých referenčných stavov. Zatiaľ čo špecializované meranie uspeje takmer s istotou (pozri obrázok 2), univerzálne meranie dosahuje pravdepodobnosť úspechu len 1/3.

Pre všeobecný prípad viacerých kópii neznámych a referenčných stavov som navrhol schému optického experimentu pre bezchybnú identifikáciu, ktorá využíva deliče zväzkov a fotodetektori. Hlavnou ideou pri návrhu tejto schémy je "koncentrácia"kópii jedného druhu stavov do koherentných stavov s väčšou amplitúdou ($|\alpha\rangle^{\otimes k} \mapsto |\sqrt{k}\alpha\rangle \otimes |0\rangle^{\otimes k-1}$) a ich následná identifikácia schémou pre jednu kópiou neznámeho i referenčných stavov. Schéma pre jednu kópiou neznámeho i referenčných stavov využíva inverznú operáciu ku

"koncetrácii", pričom vzniknuté kópie neznámeho stavu so skrátenou amplitúdou (presnejšie $|\lambda\alpha_?\rangle$) sú následne využité pri bezchybnom porovnávaní s jednotlivými referenčnými stavmi.



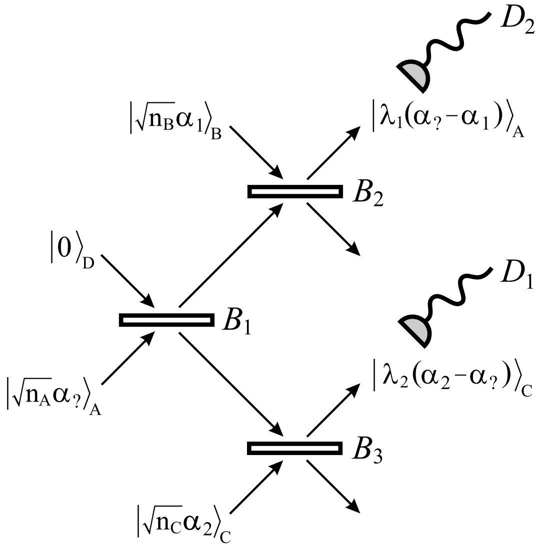
Obrázok 2: Pravdepodobnosť identifikácie $P(|\alpha_1\rangle, |\alpha_2\rangle)$ pre referenčné stavy $|\alpha_1\rangle$, $|\alpha_2\rangle$ ako funkcia skalárneho súčinu (udaného parametrom $|\alpha_1 - \alpha_2|$) pre tri identifikačné stratégie. Najspodnejšie dve krivky zodpovedajú univerzálnym bezchybným identifikačným meraniam (swap-based stratégia je zobrazená ružovou a optimálna stratégia čiernou farbou). Modrá krivka zodpovedá stratégii špeciálne navrhnutej pre koherentné stavy a využíva deliče zväzkov a fotodetektory. Najvrchnejšia červená krivka zodpovedá optimálnemu riešeniu situácie so známymi referenčnými stavmi , t.j. situácie kedy by sa z identifikácie stalo rozlišovanie medzi dvoma známymi koherentnými stavmi.

V prípade viacerých kópii neznámeho stavu a dvoch typov referenčných stavov ($M = 2, n_B = n_C$) som dokázal optimálnosť tejto schémy (obrázok 3) v rámci lineárnej optiky. Za uvedených okolností je optimálna pravdepodobnosť daná vzťahom

$$P(|\alpha_1\rangle, |\alpha_2\rangle) = 1 - e^{-\frac{n_A n_B}{n_A + 2n_B}|\alpha_1 - \alpha_2|^2}. \tag{11}$$

V limite $n_B = n_C \to \infty$ sa stávajú referenčné stavy známe. Preto musíme rozlíšiť v ktorom z dvoch možných stavov sa neznámy stav nachádza. Pravdepodobnosť úspechu navrhnutej identifikačnej schémy je v tomto prípade rovná optimálnej hodnote dosahovanej Ivanovic-Dieks-Peres meraním [5, 7]. Navrhnutá identifikačná schéma bola pre $M = 2, n_A = n_B = n_C = 1$ experimentálne zrealizovaná L. Bartůškovou et. al. [4].

Bezchybnú identifikáciu koherentných stavov môžeme považovať aj za vyhľadávanie v kvantovej databáze, ktorej elementami sú referenčné stavy a vyhľadávaný prvok je reprezentovaný neznámym stavom. Tento pohľad ma motivoval k dokázaniu možnosti čiastočného obnovenia a opätovného použitia referenčných stavov pre ďalšiu bezchybnú identifikáciu. Takýto postup je

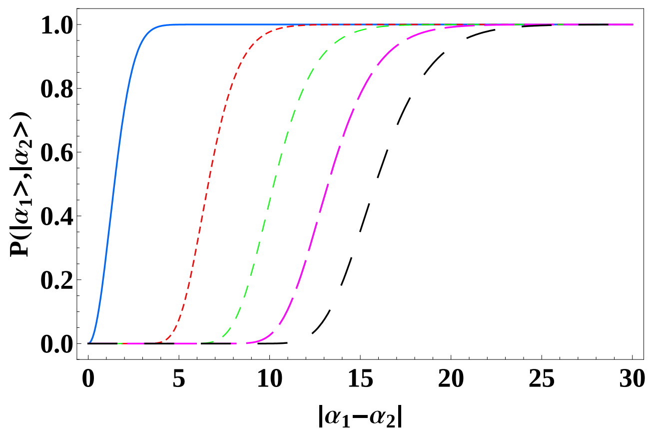


Obrázok 3: Schéma pre bezchybnú identifikáciu viacerých kópii dvoch typov koherentných referenčných stavov.

však možný len ak je výsledok všetkých predošlých identifikácii konkluzívny. Napriek tomu, ak majú referenčné stavy malý prekryv je pravdepodobnosť úspechu pre x-té kolo bezchybnej identifikácie pomerne vysoká (pozri obrázok 4). Ďalší aspekt úlohy, ktorý som skúmal, je vplyv šumu v príprave koherentných stavov na spoľahlivosť navrhnutej optickej schémy. Konkrétne som skúmal komunikačný scenár nazvaný "phase keying"($M = 2$, $n_A = n_B$, $|\alpha_2\rangle = |-\alpha_1\rangle$) s gausovským modelom šumu pôsobiacim nezávisle a rovnako na všetky stavy. Ukázalo sa, že spoľahlivosť výsledkov identifikácie závisí iba na pomere amplitúd signálu a šumu. Bohužiaľ pre nenulový šum už nie sú výsledky navrhnutej schémy bezchybné.

4 Úlohy bezchybného rozlišovania pre kanály

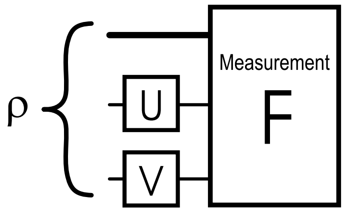
Cieľom piatej kapitoly predloženej práce bolo zhrnutie aktuálnych poznatkov o rozlišovaní kvantových kanálov a vyriešenie úlohy bezchybného porovnania dvoch neznámych unitárnych kanálov. Veľa experimentov testujúcich kvantové kanály je ekvivalentných vzhľadom k pravdepodobnostným distribúciam výsledkov, ktoré produkujú. Ak s touto ekvivalenciou nepracujeme systematicky, optimalizácia pre rozlišovacie problémy je veľmi zložitá, pretože musíme nezávisle variovať prípravu stavov i meranie. Z tohto dôvodu na štúdium uvedenej problematiky využívam popis pomocou *Process po-*



Obrázok 4: Úspešnosť schémy pre obnovu referenčných stavov. Na zvislej osi je pravdepodobnosť identifikácie $P(|\alpha_1\rangle, |\alpha_2\rangle)$ pre referenčné stavy $|\alpha_1\rangle$, $|\alpha_2\rangle$ ako funkcia skalárneho súčinu (udaného parametrom $|\alpha_1 - \alpha_2|$) zobrazená pre rôzne kolá bezchybnej identifikácie. Krivka pre prvé kolo je úplne vľavo. Ostatné krivky zodpovedajúce 20, 40, 60 a 80-temu kolu sa nachádzajú viac a viac vpravo.

sitive operator valued measure (PPOVM), ktoré bolo zavedené M.Zimanom [3]. Experiment testujúci kanál $\mathcal{E} : S_{\mathsf{P}}(\mathcal{H}) \mapsto S_{\mathsf{P}}(\mathcal{H})$ je pomocou PPOVM popísaný sadou pozitívnych operátorov $\{M_k\}$, ktoré pôsobia na $\mathcal{H} \otimes \mathcal{H}$, a operátorom $\omega_{\mathcal{E}} = I \otimes \mathcal{E}(|\Psi_+\rangle\langle\Psi_+|)$, pričom $\sum_k M_k = \xi^T \otimes I$, $\xi \geq 0$, $Tr(\xi) = 1$ a $|\Psi_+\rangle = \sum_{i=1}^{\dim \mathcal{H}} |i\rangle \otimes |i\rangle$. Operátor $\omega_{\mathcal{E}}$ sa nazýva *proces stav* a spolu s operátorom M_k udáva pravdepodobnosť výskytu udalosti k vzťahom $p_k = Tr(M_k \omega_{\mathcal{E}})$. Udalosť, ktorú môžeme pri experimente testujúcom kanál pozorovať pozostáva z prípravy testovacieho stavu ϱ a z pozorovania efektu E_j v meraní výsledného stavu. Bezchybné rozlišovanie bolo pre kanály ďaleko menej študované ako pre stavy. Úvodná časť kapitoly sa snaží do rozlišovania kanálov vniesť viac svetla práve PPOVM prístupom v ktorom som nadefinoval všeobecný problém a poskytol bližší rozbor pre unitárne kanály. Ťažiskom kapitoly je riešenie problému bezchybného porovnania dvoch neznámych unitárnych kanálov. Presnejšie, snažili sme sa zistiť, či paralelné použitie porovnávaných kanálov vytvára kanál typu $\mathcal{E}\otimes\mathcal{E}$, alebo $\mathcal{E}\otimes\mathcal{F}$. Schéma experimentov tohto typu je znázornená na obrázku 5. Pomocou PPOVM som dokázal nájsť nielen optimálnu strednú podmienenú pravdepodobnosť úspechu $\overline{p}_{\text{success}} = (d+1)/(2d)$, ale i nutnú formu optimálneho experimentu. Optimálne PPOVM má tvar

$$M_{\text{diff}} = \xi^T \otimes P^{sym}, \quad M_0 = \xi^T \otimes P^{asym}, \quad M_{same} = 0, \quad \xi \leq P^{asym}, \qquad (12)$$



Obrázok 5: Experiment porovnávajúci dva unitárne kanály $\mathcal{E}_U, \mathcal{E}_V$.

čo zodpovedá experimentu s antisymetrickým test stavom ξ, ktorého obe časti sú po akcii porovnávaných kanálov podrobené finálnemu meraniu rozlišujúcemu symetrickosť výstupného stavu[1]. Ako antisymetrický stav označujem ľubovoľný dvojčasťový stav, ktorého suport je len na antisymetrickom podpriestore daných dvoch častí systému. Ak sú porovnávané dva unitárne kanály rovnaké takýto stav zostáva antisymetrický a dostaneme vždy nekonkluzívny výsledok. Naopak ak sú kanály rôzne, potom časť výstupného stavu má prekryv aj so symetrickým podpriestorom, ktorý bezchybne indikuje rozdielnosť kanálov. Rovnako ako v prípade stavov ani pre neznáme kanály nie je možné bezchybne potvrdiť ich zhodnosť. Pre realizáciu popísaného optimálneho experimentu je nevyhnutné kvantové previazanie nielen pri záverečnom meraní ale i pri príprave testovacieho stavu. Každý (i zmiešaný) antisymetrický stav je totiž kvantovo previazaný.

5 Úlohy bezchybného rozlišovania pre kvantové merania

V kapitole šesť predloženej dizertačnej práce študujem úlohy bezchybného rozlišovania kvantových meraní. Na rozdiel od stavov a kanálov merania pôsobia nielen kvantovo ale i klasicky, keďže musia signalizovať nameraný výsledok. Práve apriórna informácia o signalizácii výsledkov merania nás motivuje rozlišovať dva typy ekvivalencie medzi meraniami. Merania nazývame *identické* ak sú ich výsledky označené rovnakým spôsobom a produkujú rovnaké pravdepodobnostné distribúcie pre každý meraný stav. Merania nazývame *ekvivalentné* ak je možné spraviť ich identickými vhodným premenovaním výsledkov. Bohužiaľ neexistuje vhodný všeobecný matematický rámec na popis experimentov rozlišujúcich merania. Z tohto dôvodu sa venujem len štúdiu experimentov, kde sa používajú iba práve testované merania a operácie podmienené výsledkami predošlých meraní nie sú povolené. V

[1] Jedná sa o experiment bez použitia pomocného systému.

práci som vyriešil problém bezchybného porovnania nedegenerovaných projektívnych meraní (sharp non-degenerate observables). Je dôležité poznamenať, že bez obmedzenia sa na istú podmnožinu všetkých meraní nemá úloha bezchybného porovnania riešenie. Uvažoval som dva typy meracích zariadení, podľa toho, či ich výsledky merania sú apriori označené alebo nie. V práci prezentujem riešenie porovnania pomenovaných meraní z jedného ich použitia pre ľubovoľnú dimenziu zodpovedajúceho Hilbertovho priestoru. Pre merania s nepomenovanými výsledkami jedno použitie meraní pre bezchybné porovnanie nestačí. Preto pre dvojnásobné použitie každého z porovnávaných qubitových meraní odvádzam optimálnu stratégiu. Pre oba druhy meracích zariadení nie je možné bezchybne potvrdiť zhodnosť realizovaných meraní. Podobne ako pre stavy a unitárne kanály môžeme pri porovnaní nedegenerovaných projektívnych meraní bezchybne detekovať iba rozdielnosť týchto meraní. Optimálna stratégia pre porovnanie pomenovaných meracích zariadení využíva antisymetrické test stavy. Obe časti ľubovoľného antisymetrického test stavu zmeriame porovnávanými meraniami, pričom zhodnosť ich výsledkov bezchybne signalizuje rozdielnosť meraní s optimálnou podmienenou pravdepodobnosťou $\overline{q}_{\text{success}}(\mathcal{A} \neq \mathcal{B}) = 1/d$. Pre uvažované porovnanie nepomenovaných qubitových meracích zariadení existuje len jeden optimálny test stav. Tento stav

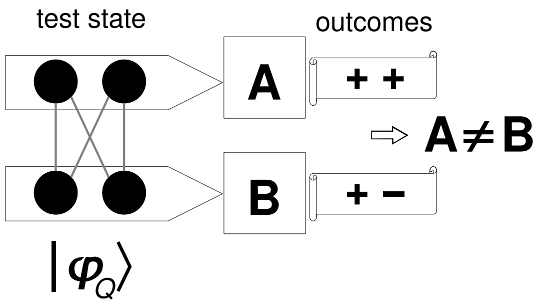
$$|\varphi_Q\rangle = \frac{1}{\sqrt{3}}(|\psi^-_{13} \otimes \psi^-_{24}\rangle + |\psi^-_{14} \otimes \psi^-_{23}\rangle)\,, \tag{13}$$

má tiež istú formu antisymetrie, vďaka stavom $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$ z ktorých je poskladaný. Rozdielnosť meraní je odhalená ak na jednom zo zariadení nájdeme rovnaké výsledky a na druhom zariadení rôzne výsledky merania (pozri obrázok 6). Stredná podmienená pravdepodobnosť odhalenia rozdielnosti meraní je v tomto prípade $\overline{p}_{\text{success}}(\mathcal{A} \neq \mathcal{B}) = 4/9$.

Na záver zrekapitulujme podmienené pravdepodobnosti úspechu porovnania čistých stavov, unitárnych kanálov a projektívnych meraní. Pre jediné použitie porovnávaných zariadení máme $\overline{p}_{\text{state}} = (d-1)/2d$, $\overline{p}_{\text{unitary}} = (d+1)/2d$, $\overline{p}_{\text{meas}} = 1/d$. Vidíme, že na rozdiel od stavov a kanálov pravdepodobnosť úspechu pre porovnanie pomenovaných meracích zariadení ide k nule s narastajúcou dimenziou kvantového systému.

Referencie

[1] P. Raynal, N. Lutkenhaus, and S. van Enk, "Reduction theorems for optimal unambiguous state discrimination of density matrices", Phys. Rev. A 68, 022308 (2003)



Obrázok 6: Ilustrácia optimálnej schémy pre bezchybné porovnanie qubitových meracích zariadení. Táto schéma vedie k odhaleniu rozdielnosti meraní so strednou podmienenou pravdepodobnosťou 4/9.

[2] M. Kleinmann, H. Kampermann, and D. Bruss, "Structural approach to unambiguous discrimination of two mixed states", arXiv:0803.1083v1 [quant-ph]

[3] M.Ziman, "Process POVM: A mathematical framework for the description of process tomography experiments", Phys. Rev. A **77**, 062112 (2008)

[4] L. Bartůšková, A. Černoch, J. Soubusta, and M. Dušek, "Programmable discriminator of coherent states: Experimental realization", Phys. Rev. A **77**, 034306 (2008)

[5] I. D. Ivanovic, "How to differentiate between non-orthogonal states", Phys. Lett. A, 123:257 (1987), D. Dieks, Överlap and distinguishability of quantum states", Phys. Lett. A, 126:303 (1988), A. Peres, "How to differentiate between non-orthogonal states", Phys. Lett. A, 128:19 (1988)

[6] E. Andersson, M. Curty and I. Jex, ”Experimentally realizable quantum comparison of coherent states and its applications“, Phys. Rev. A **74**, 022304 (2006)

[7] K. Banaszek, ”Optimal receiver for quantum cryptography with two coherent states“, Phys.Lett.A **253**, 12 (1999)

6 Zoznam publikácií

1. **M. Sedlák**, M. Ziman, O. Přibyla, V. Bužek, and M. Hillery
   Unambiguous identification of coherent states: Searching a quantum database
   Phys. Rev. A **76**, 022326 (2007)

2. **M. Sedlák**, M. Ziman, V.Bužek and M. Hillery
   Unambiguous comparison of ensembles of quantum states
   Phys. Rev. A **77**, 042304 (2008)

3. **M. Sedlák** and M.Ziman
   Unambiguous comparison of unitary channels
   Phys. Rev. A **79**, 012303 (2009)

4. **M. Sedlák**, M.Ziman, V .Bužek and M .Hillery
   Unambiguous identification of coherent states II: Multiple resources
   Phys. Rev. A **79**, 062305 (2009)

5. M.Ziman, **M. Sedlák**
   Single-shot discrimination of quantum unitary processes
   prijaté na publikáciu v Journal of Modern Optics.

6. M. Ziman, T. Heinosaari, and **M. Sedlák**
   Unambiguous comparison of quantum measurements
   zaslané do Phys. Rev. A

7 Zoznam citácií

M. Sedlák, M. Ziman, O. Přibyla, V. Bužek, and M. Hillery
Unambiguous identification of coherent states: Searching a quantum database
Phys. Rev. A **76**, 022326 (2007)

1. L. Bartůšková, A. Černoch, J. Soubusta, and M. Dušek
   Programmable discriminator of coherent states: Experimental realization, Phys. Rev. A **77**, 034306 (2008)

2. Bing He and J. Bergou
   Coherent-states engineering with linear optics: Possible and impossible tasks, Phys. Rev. A 77, 053818 (2008)

3. M. Mičuda, M. Ježek, M. Dušek, and J. Fiurášek
   Experimental realization of a programmable quantum gate, Phys. Rev. A 78, 062311 (2008)

4. C. S. Hamilton, H. Lavička,E. Andersson, J. Jeffers, and I. Jex,
   Quantum public key distribution with imperfect device components, Phys. Rev. A 79, 023808 (2009)

5. R. V. Ramos, F. A. Mendonca,
   Quantum bit commitment protocol without quantum memory, arXiv:0801.0690 (2008)

6. J. Bergou
   Discrimination of Quantum States: A Tutorial Review, accepted to special issue of Journal of Modern Optics: "State&process discrimination"

M. Sedlák, M. Ziman, V.Bužek and M. Hillery
Unambiguous comparison of ensembles of quantum states
Phys. Rev. A **77**, 042304 (2008)

1. C. S. Hamilton, H. Lavička,E. Andersson, J. Jeffers, and I. Jex,
   Quantum public key distribution with imperfect device components
   Phys. Rev. A 79, 023808 (2009)

8 Príspevky na konferenciách

1. **M. Sedlák**
   Unambiguous coherent state identification (prednáška)
   Young European Physicists meeting, Budmerice, 11.- 15.12.2006

2. **M. Sedlák**, O. Přibyla, M. Ziman, V. Bužek, and M. Hillery
   Unambiguous coherent state identification (poster)
   QUROPE Winter School, 18. - 24.2.2007, Obergurgl, Austria

3. **M. Sedlák**
   Unambiguous identification of coherent states (prednáška)
   Informal Quantum Information Gathering (IQING), Innsbruck, 11. - 14.4.2007

4. **M. Sedlák**
   Unambiguous identification of coherent states (prednáška)
   Identifying quantum states and operations, 20. - 24.6.2007, Budmerice, Slovakia

5. **M. Sedlák**, M. Ziman, O. Přibyla, V. Bužek, and M. Hillery
   Unambiguous identification of coherent states: Searching a quantum

database (poster)
International Summer School in Quantum Information Processing and Control (QUIC 2007), 26. - 31.8.2007, Maynooth, Ireland

6. **M. Sedlák**
Unambiguous identification of coherent states (prednáška)
Young European Physicists meeting, 17. - 21.9.2007, Frauenchiemsee, Germany

7. **M. Sedlák**, M. Ziman, V. Bužek, and M. Hillery
Unambiguous comparison of ensembles of quantum states (poster)
5th Central European Quantum Information Processing Workshop, 5. - 8.6.2008, Telč, Czech Republic

8. **M. Sedlák**, M. Ziman, V. Bužek, and M. Hillery
Unambiguous comparison of ensembles of quantum states (poster)
QICS Workshop on Foundational Structures for Quantum Information and Computation, 14. - 20.9.2008, Obergurgl, Austria

9. **M. Sedlák**
Unambiguous comparison of Unitary Channels (prednáška)
6th Central European Quantum Information Processing Workshop, 1. - 4.6.2009, Jindřichuv Hradec, Czech Republic

10. **M. Sedlák**, M. Ziman, V. Bužek, and M. Hillery
Unambiguous identification of coherent states: Multiple resources, repeated use & optimality (poster)
Quantum Optics VII:Quantum Engineering of Atoms and Photons, 8. - 12.6.2009, Zakopane, Poland

9 Summary

In the present thesis I formulate a framework that accommodates many unambiguous discrimination problems. I show that the prior information about any type of constituent (state, channel, or observable) allows us to reformulate the discrimination among finite number of alternatives as the discrimination among finite number of average constituents. Using this framework I solve several unambiguous tasks:

1. *Optimal unambiguous comparison of two ensembles of unknown quantum states.* I consider two cases: 1) The two unknown states are arbitrary pure states of qudits. 2) Alternatively, they are coherent states of single-mode optical fields. For this case I propose simple and optimal experimental setup composed of beam-splitters and a photodetector.

2. *Unambiguous identification (UI) of coherent states.* In this task identical quantum systems are prepared in coherent states and labeled as unknown and reference states, respectively. The promise is that one reference state is the same as the unknown state and the task is to find out unambiguously which one it is. The particular choice of the reference states is unknown to us, and only the probability distribution describing this choice is known. In a general case when multiple copies of unknown and reference states are available I propose a scheme consisting of beamsplitters and photodetectors that is optimal within linear optics. UI can be considered as a search in a quantum database, whose elements are the reference states and the query is represented by the unknown state. This perspective motivated me to show that reference states can be recovered after the measurement and might be used (with reduced success rate) in subsequent UI. Moreover, I analyze the influence of noise in preparation of coherent states on the performance of the proposed setup.

3. *Unambiguous comparison of a pair of unknown qudit unitary channels.* I characterize all solutions and identify the optimal ones. I prove that in optimal experiments for comparison of unitary channels the entanglement is necessary.

4. *Unambiguous comparison of unknown non-degenerate projective measurements.* I distinguish between measurement devices with apriori labeled and unlabeled outcomes. In both cases only the difference of the measurements can be concluded unambiguously. For the labeled case I derive the optimal strategy if each unknown measurement is

used only once. However, if the apparatuses are not labeled, then each measurement device must be used (at least) twice. In particular, for qubit measurement apparatuses with unlabeled outcomes I derive the optimal test state in the two-shots scenario.