

Přírodovědecká fakulta Univerzity Palackého

katedra optiky



# Rozlišení a odhad fyzikálního stavu systému

27. 4. 2003

Fyzikální základy fotoniky 2003

Miroslav Ježek

<mailto:jezek@optics.upol.cz>  
<http://optics.upol.cz/jezek>

**Rozlišení a odhad fyzikálního stavu systému**  
**©2003, Miroslav Ježek**

# Obsah

<b>1</b>	<b>Teorie pravděpodobnosti</b>	<b>1</b>
<b>2</b>	<b>Stav a měření v kvantové teorii</b>	<b>4</b>
2.1	Stav . . . . .	4
2.2	Transformační vlastnosti stavu . . . . .	5
2.3	Volné šíření . . . . .	7
2.4	Konečná apertura . . . . .	8
<b>3</b>	<b>Detekce</b>	<b>9</b>
<b>4</b>	<b>Odhad stavu</b>	<b>11</b>
4.1	Přímé metody . . . . .	11
4.2	Statistické metody . . . . .	12
4.3	Bayesovský odhad . . . . .	13
4.4	Extremalizace věrohodnosti . . . . .	15
4.5	Odhad vzájemné intenzity . . . . .	17
4.6	Poznámky . . . . .	19
<b>5</b>	<b>Rozlišení stavů</b>	<b>20</b>
5.1	Nejednoznačné rozlišení . . . . .	20
5.2	Jednoznačné rozlišení . . . . .	23
	<b>Literatura</b>	<b>24</b>



# Kapitola 1

## Teorie pravděpodobnosti

Při fyzikálním měření a jeho popisu se snažíme vždy dodržet princip „*ceteris paribus*“, tedy „ostatní se nemění“. Máme tím na mysli kontrolovatelnost a neměnnost podmínek za kterých pokus provádíme. Bez dodržení tohoto principu by bylo naše měření neopakovatelné, a tudíž nemělo žádnou hodnotu.

Známe experimenty, které při dodržení podmínek ( $\pm$  neurčitost) vedou vždy ke stejným závěrům ( $\pm$  neurčitost), jmenovitě stabilní systémy klasické fyziky. Nestabilními systémy rozumíme ty, u nichž malá změna počátečních podmínek vede k velkému rozdílu ve výsledném stavu, například systémy s mísením a deterministický chaos. Teoreticky, při přesném dodržení podmínek získáme stejný výsledek.

Existují také fyzikální systémy a měření vedoucí s různou pravděpodobností k různým výsledkům bez ohledu na dodržení stejných podmínek. Výsledek pokusu není jednoznačně určen podmínkami. Tato situace nastává u kvantově–mechanických systémů.

Pokud nedokážeme fyzikální systém dostatečně vymezit vzhledem k okolí, a tedy přesně kontrolovat podmínky, dochází také k různým výsledkům při jednotlivých realizacích pokusu. Tento případ se překrývá s případem deterministického chaosu.

Výše zmíněné pokusy, jejichž výsledek není jednoznačně předurčen kontrolovanými podmínkami, a které jsou (alespoň teoreticky) neomezeně opakovatelné, nazýváme *náhodnými pokusy*. Jakékoli tvrzení o výsledku náhodného pokusu, u kterého lze po provedení pokusu rozhodnout o pravdivosti, nazýváme *náhodný jev*.

Empirickým základem teorie pravděpodobnosti a základem pro klasickou definici pravděpodobnosti je *relativní četnost*. Studujme  $N$  realizací náhodného pokusu. Označme  $N_A$  počet realizací, při nichž nastal sledovaný náhodný jev  $A$ . Podíl

$$f_A = \frac{N_A}{N} \quad (1.1)$$

se nazývá relativní četnost jevu  $A$ . Snadno dokážeme, že relativní četnost leží v intervalu  $[0, 1]$ , relativní četnost sjednocení disjunktních jevů je rovna součtu relativních četností jednotlivých jevů a relativní četnost jistého jevu je rovna 1.

Stabilitou relativní četnosti rozumíme fakt, že relativní četnost náhodného jevu se po mnoha pokusech blíží určitému číslu,

$$\lim_{N \rightarrow \infty} \frac{N_A}{N} = P_A. \quad (1.2)$$

Hodnota  $P_A$  charakterizuje „častost“ jevu  $A$  a nazýváme ji *pravděpodobností*. Zřejmě pravděpodobnosti splňují stejné vlastnosti (formou axiomů) jako relativní četnosti.

Předchozí empirická definice pravděpodobnosti je nedostatečná pro korektní matematickou a fyzikální práci s náhodnými jevy. Proto byla vybudována axiomatická definice pravděpodobnosti, viz například [1, 2, 3]. Zde pouze nastíníme základní axiomy.

Nechť je dána množina  $S$  a systém  $\mathcal{A}$  podmnožin množiny  $S$  s následujícími vlastnostmi. Množina  $S$  je prvkem systému  $\mathcal{A}$ . Pro každou množinu  $A \in \mathcal{A}$  je také množina  $\bar{A} = S - A$  prvkem systému  $\mathcal{A}$ . Sjednocení množin ze systému  $\mathcal{A}$  je také prvkem systému  $\mathcal{A}$ . Dvojici  $\{S, \mathcal{A}\}$  nazýváme *jevovým polem* a prvky  $A$  systému  $\mathcal{A}$  *jevy* nebo *náhodnými jevy*.

Budiž  $P$  reálná nezáporná funkce definovaná na systému  $\mathcal{A}$ , která splňuje následující podmínky.  $P(S) = 1$ ,  $P(\bigcup_i A_i) = \sum_i P(A_i)$  pro disjunkttní systém množin  $A_i \in \mathcal{A}$ . Funkci  $P$  na  $\mathcal{A}$  nazýváme *pravděpodobnostní mírou* na  $\mathcal{A}$  a trojici  $\{S, \mathcal{A}, P\}$  *pravděpodobnostním polem*.

Nechť  $\{S, \mathcal{A}, P\}$  je pravděpodobnostní pole a  $B$  daná množina z  $\mathcal{A}$ . Potom  $\{B, \mathcal{B}\}$ ,  $\mathcal{B} = \{A \cap B | A \in \mathcal{A}\}$ , je jevovým polem a funkce

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \quad (1.3)$$

je pravděpodobnostní mírou na  $\mathcal{B}$ . Nazýváme ji *podmíněnou pravděpodobností*.

Poznámka. Pravděpodobnost  $P(A \cap B)$  současného výskytu (průniku) jevů  $A$  a  $B$  budeme dále značit stručně  $P(AB)$ . Přitom pro pravděpodobnost sjednocení jevů zřejmě platí  $P(A \cup B) = P(A) + P(B) - P(AB)$ .

Vztah (1.3) se často užívá ve tvaru

$$\begin{aligned} P(AB) &= P(A|B)P(B) \\ &= P(B|A)P(A) \end{aligned} \quad (1.4)$$

a nazývá se teorém o násobení pravděpodobnosti.

Uvažujme disjunkttní množinu jevů  $H_i$  pokrývající celý prostor jevů,  $P(\bigcup_i H_i) = 1$ . Jev  $A$  může nastat současně s jedním z jevů  $H_i$ ,  $A = \bigcup_i AH_i$ . Použijeme-li (1.4) získáme pro *úplnou pravděpodobnost* jevu  $A$  následující vztah,

$$P(A) = \sum_i P(A|H_i)P(H_i). \quad (1.5)$$

Uplatníme-li vztahy (1.4) na součin jevů  $A$  a  $H_i$ , získáme

$$P(H_i|A) = \frac{P(A|H_i)P(H_i)}{P(A)} = \frac{P(A|H_i)P(H_i)}{\sum_i P(A|H_i)P(H_i)}, \quad (1.6)$$

kde jsme užili (1.5). Vztah (1.6) mezi podmíněnými pravděpodobnostmi se nazývá *Bayesova věta*. Slovně ji můžeme vyjádřit následovně,

$$\text{posterior} = \frac{\text{likelihood} \times \text{prior}}{\text{evidence}}. \quad (1.7)$$

Disjunktní jevy  $H_i$  nazýváme *hypotézy*. Pojmem „posterior“ myslíme posteriorní pravděpodobnost hypotéz, „prior“ znamená priorní (apriorní) pravděpodobnost hypotéz, „likelihood“ znamená věrohodnost hypotéz a názvu „evidence“ se někdy používá pro úplnou pravděpodobnost (1.5).

Význam Bayesovy věty a názvosloví bude podrobněji vysvětleno v kapitole věnované odhadu stavu fyzikálního systému.

*Příklad.* Studujme nedokonalý komunikační kanál, tedy přenosovou soustavu, která na odeslaný znak (jev)  $H_i$  na straně odesilatele odpoví přijutím nějakého znaku  $A \in H_i$  na straně druhé. Přitom z vlastností kanálu, respektive z měření na něm, můžeme určit pravděpodobnost  $P(A^{\text{přijat}}|H_i^{\text{odeslán}})$ . Taktéž známe priorní pravděpodobnost  $P(H_i)$  odeslání jednotlivých znaků abecedy a celkovou pravděpodobnost  $P(A)$  přijutí znaku  $A$ . Nyní se můžeme ptát, co bylo vysláno, tedy jaký znak a s jakou pravděpodobností, když obdržíme znak  $A$ . Odpověď nám dává Bayesova věta

$$P(H_i^{\text{odeslán}}|A^{\text{přijat}}) = \frac{P(A^{\text{přijat}}|H_i^{\text{odeslán}}) P(H_i)}{P(A)}. \quad (1.8)$$

Vztah (1.8) určuje posteriorní pravděpodobnost hypotézy „byl odeslán znak  $H_i$ “ podmíněnou jevem „byl přijat znak  $A$ “.

*Historická poznámka.* Odhady s použitím Bayesovy věty jsou v literatuře poněkud rozporuplně hodnoceny. Některé prameny zdůrazňují schopnost začlenit priorní informaci, jiné oprávněně poukazují na problémy spojené s jejím výběrem [1]. Ani volba uniformní priorní pravděpodobnosti není spolehlivou cestou k vyjádření naší neznalosti, neboť poskytuje různé odhady v závislosti na parametrizaci. V každém případě termín „Bayesovská metoda“ je minimálně vágní a historicky neopodstatněný. Amatérský matematik reverend Thomas Bayes sice roku 1763 publikoval partikulární výsledek obrácení binomického rozdělení – odhad posteriorního rozdělení, avšak není autorem Bayesovy věty. Již například Bernoulli a de Moivre znali vztahy pro pravděpodobnost součinu, dávno před Bayesem. Za duchovního otce obecného tvrzení (1.6), základů teorie odhadu a myšlenky uniformní priorní pravděpodobnosti hypotéz by měl být považován Laplace [4], citováno v [2].

# Kapitola 2

## Stav a měření v kvantové teorii

### 2.1 Stav

Jádrem kvantového popisu fyzikálních systémů je pouze několik málo axiomů. Jako nejdůležitější z nich se jeví princip superpozice. Matematický popis akceptující tyto axiomy musí být založen na struktuře, jíž je superpozice vlastní, která umožňuje zjišťovat „překryv“ stavů formou skalárního součinu, a která má další potřebné vlastnosti. Jako nejvhodnější se ukázal Hilbertův prostor a vyjadřování pomocí Diracovy symboliky [5].

Klíčový je pojem *čistého stavu*. Nekonečný soubor identicky připravených fyzikálních objektů, na kterém lze provést neomezený počet měření, představuje maximální dostupnou informaci o tomto objektu. Nazývá se čistým stavem a je reprezentován stavovým vektorem z Hilbertova prostoru. Lze sice použít i příslušný projektivní prostor [6, 7], ale prostor vektorový je vždy primární. Prakticky jedinou libovůli máme ve volbě tělesa. Je vybudována i kvaternionová kvantová teorie [8], ale obvykle se užívá těleso komplexních čísel dostačující k vysvětlení experimentálních výsledků – k zahrnutí fází do amplitud pravděpodobnosti. Vyvstává pouze otázka, jak upřesnit vágní pojem „identická příprava“. Přípravu vedoucí k čistému stavu lze operacionálně definovat existencí jistého maximálního testu (měření), jenž poskytne s jistotou vždy stejný výsledek a výsledky ostatních maximálních testů se řídí jednoznačnými pravděpodobnostmi, které nezávisí na detailech přípravy. Přitom každé měření s maximálním počtem možných výstupů ze všech možných měření nazýváme maximálním.

Jestliže se v diskutovaném souboru projeví jakékoli nepravidelnosti, nebo ztratíme-li jakoukoli informaci, hovoříme o *stavu smíšeném*. Například si můžeme představit zdroj, který vysílá čistý stav  $|\varphi_1\rangle$ , ale občas vlivem nedokonalostí a interakce s okolím emituje stav  $|\varphi_2\rangle$  s pravděpodobností  $\lambda_2$ , stav  $|\varphi_3\rangle$  s pravděpodobností  $\lambda_3$  atd. Naši neúplnou znalost popisujeme nekoherentní superpozicí čistých stavů – *operátorem hustoty*

$$\hat{\rho} = \sum_k \lambda_k |\varphi_k\rangle \langle \varphi_k|, \quad (2.1)$$

s vlastnostmi hermiteovskosti a nezápornosti (pozitivní semidefinitnosti),

$$\widehat{\rho}^+ = \widehat{\rho}, \quad \langle \psi | \widehat{\rho} | \psi \rangle \geq 0, \quad \forall |\psi\rangle. \quad (2.2)$$

Vztah (2.1) současně představuje obecnou parametrizaci neznámého kvantového stavu.

V reprezentaci dané veličiny nabývá popis stavu konkrétní podoby. Například v reprezentaci hybnosti je čistý stav popsán komplexní funkcí reálné proměnné  $p$ , v reprezentaci energetické je čistý stav vázaného systému popsán vektorem komplexních čísel a smíšený stav hermiteovskou maticí.

Dále zdůrazníme některé souvislosti mezi kvantově mechanickým popisem stavu a prostorovým popisem vlny ve skalární vlnové teorii. Užijeme tedy souřadnicovou  $x$ -reprezentaci. Použijeme-li projektor  $|x'\rangle\langle x|$  a (2.1), získáme pro  $x$ -reprezentaci operátoru hustoty

$$\text{Tr} [\widehat{\rho} |x'\rangle\langle x|] = \langle x | \widehat{\rho} | x' \rangle = \sum_k \lambda_k \langle x | \varphi_k \rangle \langle \varphi_k | x' \rangle = \sum_k \lambda_k \varphi_k(x) \varphi_k^*(x') = \langle \varphi^*(x') \varphi(x) \rangle, \quad (2.3)$$

kde  $\varphi_k(x) = \langle x | \varphi_k \rangle$  představuje (de Broglieovu) vlnovou funkci čistého stavu  $|\varphi_k\rangle$ .

Projektor  $|x'\rangle\langle x|$  lze považovat za „přeskokový“ operátor v  $x$ -bázi a formálně zavést bosonovské anihilační a kreační operátory  $|x'\rangle\langle x| = \widehat{\sigma}_{x'x} = \widehat{a}_{x'}^+ \widehat{a}_x$ ,  $[\widehat{a}_x, \widehat{a}_{x'}^+] = \delta(x - x')$ . Potom zřejmě matice hustoty v  $x$ -bázi je kvantová korelační funkce druhého řádu [9],

$$\text{Tr} [\widehat{\rho} |x'\rangle\langle x|] = \text{Tr} [\widehat{\rho} \widehat{a}_{x'}^+ \widehat{a}_x] = \Gamma(x, x', z) = \langle \psi^*(x', z) \psi(x, z) \rangle. \quad (2.4)$$

V kontextu klasické optiky jde o vzájemnou intenzitu [10]. Závislost na  $z$  zde specifikuje hodnotu evoluční proměnné, tj. určuje, v kterém místě na ose  $z$ , respektive v jakém čase zkoumáme  $\widehat{\rho}$ . Vlastnosti (2.2) se věrně kopírují do vlastností vzájemné intenzity,

$$\Gamma(x, x', z) = \Gamma^*(x', x, z), \quad \Gamma(x, x, z) \geq 0. \quad (2.5)$$

Místo fázového prostoru  $(x, x')$ , v němž může být vyjádření evoluce stavu poněkud obtížné, lze pracovat v  $(x, p)$ -reprezentaci, tj. ve fázovém prostoru  $(x, p)$ . Tato myšlenka je základem všech kvazidistribucí v kvantové teorii [11, 12, 13, 14, 15]. Pro své vlastnosti a použití i v jiných oblastech fyziky je důležitá reálná omezená symetrická Wignerova distribuce (Wigner [11], Ville [16]) nativně spojená s Weylovým symetrickým uspořádáním,

$$W(x, p, z) = \frac{1}{\pi} \int dx' e^{-i2px'} \langle x - x' | \widehat{\rho} | x + x' \rangle = \frac{1}{\pi} \int dx' e^{-i2px'} \Gamma(x + x', x - x', z). \quad (2.6)$$

Poznámka. Integrace je prováděna přes celý obor proměnné, pokud nejsou uvedeny explicitně meze.

## 2.2 Transformační vlastnosti stavu

Poznámka. Nebude-li řečeno jinak, jsou veličiny přeskálované tak, aby  $\hbar = \frac{1}{k} = \frac{\lambda}{2\pi} = 1$ , kde  $\hbar$  je Diracova konstanta,  $k$  vlnové číslo a  $\lambda$  vlnová délka.

Unitární evoluce (vývoj) obecného smíšeného stavu je řízen evolucí jeho složek – primární je evoluce čistého stavu. Naopak, neunitární evoluce znamená změnu složek a jejich pravděpodobností v rozkladu operátoru hustoty (2.1) – mění se „smíšenost“ stavu.

Předpokládáme-li lineárnost, kauzálnost a nedisperznost (lokálnost v evoluční proměnné), není obtížné napsat formální tvar unitární evoluční rovnice

$$\frac{\partial}{\partial z}|\psi(z)\rangle = \widehat{L}|\psi(z)\rangle, \quad (2.7)$$

případně

$$|\psi(z)\rangle = \widehat{T}(z)|\psi(0)\rangle, \quad \frac{\partial}{\partial z}\widehat{T}(z) = \widehat{L}\widehat{T}(z), \quad \widehat{T}(0) = \widehat{1}. \quad (2.8)$$

Zde  $|\psi(z)\rangle$  představuje vyvíjející se čistý stav,  $z$  je evoluční parametr (axiální souřadnice, čas),  $\widehat{T} = \widehat{T}(z; \dots)$  je evoluční, respektive transformační operátor závisující na parametrech evoluce a  $\widehat{L}$  je generátor této transformace. V dalším budeme pracovat výhradně s  $z$ -nezávislými generátory  $\widehat{L} \neq \widehat{L}(z)$ , pro než není obtížné nalézt formální řešení evoluční rovnice (2.8),

$$\widehat{T}(z) = e^{\widehat{L}z}. \quad (2.9)$$

V kvantové teorii je generátorem evoluce Hamiltonián  $\widehat{H}$ ,  $\widehat{L} = -i\widehat{H}$ , a (2.7) představuje Schrödingerovu rovnici pro čistý stav. Rovnice (2.8), řešení (2.9) a definice (2.1) specifikují evoluci smíšeného stavu

$$\widehat{\rho}_{\text{out}} = \widehat{T}\widehat{\rho}_{\text{in}}\widehat{T}^+, \quad \widehat{T} = \exp[-i\widehat{H}z]. \quad (2.10)$$

Ekvivalentně lze vyjádřit transformační účinky operátoru  $\widehat{T}$  v Heisenbergově obraze, zde konkrétně pro kanonické pozorovatelné *zobecněnou polohu* a *zobecněnou hybnost*,

$$\begin{pmatrix} \widehat{x}_{\text{out}} \\ \widehat{p}_{\text{out}} \end{pmatrix} = \widehat{T}^+ \begin{pmatrix} \widehat{x}_{\text{in}} \\ \widehat{p}_{\text{in}} \end{pmatrix} \widehat{T}. \quad (2.11)$$

Speciálně pro unitární evoluci generovanou Hamiltoniánem s nejvýše kvadratickou závislostí na kanonických pozorovatelných se tyto transformují mezi vstupní a výstupní rovinou lineárně,

$$\begin{pmatrix} \widehat{x}_{\text{out}} \\ \widehat{p}_{\text{out}} \end{pmatrix} = \widehat{T}^+ \begin{pmatrix} \widehat{x}_{\text{in}} \\ \widehat{p}_{\text{in}} \end{pmatrix} \widehat{T} = T \begin{pmatrix} \widehat{x}_{\text{in}} \\ \widehat{p}_{\text{in}} \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} \widehat{x}_{\text{in}} \\ \widehat{p}_{\text{in}} \end{pmatrix}. \quad (2.12)$$

Parametry  $A, B, C, D$  závisí příslušným způsobem na parametrech Hamiltoniánu. Lineární transformace operátorů  $(\widehat{x}, \widehat{p})$  indukuje evoluci Wignerovy funkce transformací jejich fázových proměnných

$$W(x, p, z) = W(Dx - Bp, -Cx + Ap, 0). \quad (2.13)$$

Tvrzení lze snadno dokázat užitím vztahu mezi Wignerovou funkcí a funkcí charakteristikou, Baker–Campbell–Hausdorffovy identity a unitarity evolučního operátoru,  $\widehat{T}\widehat{T}^+ = \widehat{1}$ .

Ze vztahů (2.8) a (2.9) plynoucí evoluce čistého stavu  $|\psi_{\text{out}}\rangle = \widehat{T}|\psi_{\text{in}}\rangle$  nabývá v  $x$ -reprezentaci známého tvaru

$$\psi(x, z) = \langle x|\psi\rangle = \int dx_0 \langle x|\widehat{T}|x_0\rangle \langle x_0|\psi_0\rangle = \int dx_0 h(x, x_0; z, \dots) \psi(x_0, 0), \quad (2.14)$$

kde jsme využili relaci úplnosti souřadnicové  $x_0$ -báze ve vstupní rovině. Propagátor

$$h(x, x_0) = \langle x|\widehat{T}|x_0\rangle \quad (2.15)$$

v kvantové teorii je odezovou funkcí (point spread function, PSF) ve skalární vlnové teorii [17]. Dává do souvislosti bodový zdroj ve vstupní rovině s jeho obrazem v rovině výstupní. V případě nekonečné apertury je transformační systém ryze refraktivní, evoluce je unitární,  $\widehat{T}^+ = \widehat{T}^{-1}$ , a bod je zobrazen na bod. Naopak, v neunitárním transformačním systému s konečnou aperturou dojde k „rozmazání“ vlivem difrakce. Podobně vyjádříme-li (2.10) v  $x$ -reprezentaci obdržíme analog (2.14) pro vzájemnou intenzitu

$$\Gamma(x, x', z) = \iint dq dq' h(x, q) h^*(x', q') \Gamma(q, q', 0). \quad (2.16)$$

Při reprezentaci Wignerovou funkcí, tj. v  $(x, p)$ -doméně, vycházíme z definičního vztahu (2.6). Dosadíme-li za  $\widehat{\rho}$  propagovaný operátor hustoty  $\widehat{\rho}_{\text{out}}$ , získáme Wignerovu funkci  $W_{\text{out}}$  ve výstupní rovině.

## 2.3 Volné šíření

Pohyb volné částice, respektive neinteragujícího modu světla, je řízen Hamiltoniánem  $\frac{1}{2}\widehat{p}^2$ , tedy transformačním operátorem  $\widehat{T} = \widehat{F}(z) = \exp[-i\frac{z}{2}\widehat{p}^2]$ . Operátor hustoty se transformuje dle předpisu (2.10),  $\widehat{\rho}_{\text{out}} = \widehat{F}(z)\widehat{\rho}_{\text{in}}\widehat{F}^+(z)$ . Ekvivalentně lze vyjádřit transformační účinky operátoru  $\widehat{F}(z)$  v Heisenbergově obraze, zde konkrétně pro kanonické pozorovatelné

$$\begin{pmatrix} \widehat{x}_{\text{out}} \\ \widehat{p}_{\text{out}} \end{pmatrix} = \widehat{F}^+(z) \begin{pmatrix} \widehat{x}_{\text{in}} \\ \widehat{p}_{\text{in}} \end{pmatrix} \widehat{F}(z).$$

Zderivujeme-li předchozí vztah, získáme diferenciální rovnici pro vektor  $(\widehat{x}_{\text{out}}, \widehat{p}_{\text{out}})$

$$\frac{d}{dz} \begin{pmatrix} \widehat{x}_{\text{out}} \\ \widehat{p}_{\text{out}} \end{pmatrix} = \begin{pmatrix} \widehat{p}_{\text{out}} \\ \widehat{0} \end{pmatrix}.$$

Vidíme, že hybnost  $\widehat{p}$  je integrálem pohybu  $\widehat{p}_{\text{out}} = \widehat{p}_{\text{in}}$  a souřadnice  $\widehat{x}$  se mění lineárně s evolučním parametrem  $z$ ,

$$\begin{pmatrix} \widehat{x}_{\text{out}} \\ \widehat{p}_{\text{out}} \end{pmatrix} = \begin{pmatrix} \widehat{x}_{\text{in}} + z\widehat{p}_{\text{in}} \\ \widehat{p}_{\text{in}} \end{pmatrix} = F(z) \begin{pmatrix} \widehat{x}_{\text{in}} \\ \widehat{p}_{\text{in}} \end{pmatrix}. \quad (2.17)$$

Funkce bodové odezvy (propagátor)

$$h(x, x_0, z) = \langle x | \widehat{F}(z) | x_0 \rangle = \langle x | e^{-i\frac{z}{2}\widehat{p}^2} | x_0 \rangle = \langle x | \int dp e^{-i\frac{z}{2}p^2} | p \rangle \langle p | x_0 \rangle,$$

je známé jádro Fresnelovy difrakce [17],

$$h(x, x_0, z) \approx e^{\frac{i}{2z}(x-x_0)^2}, \quad (2.18)$$

kde jsme využili identity

$$\langle x | p \rangle = \frac{1}{\sqrt{2\pi}} e^{ixp}, \quad \int dp e^{-\alpha^2 p^2 + \beta p} = \frac{\sqrt{\pi}}{|\alpha|} e^{\frac{\beta^2}{4\alpha^2}}. \quad (2.19)$$

Volné šíření představuje kvadratický fázový filtr (QPF [18]). K podobnému závěru dospějeme i pro lineární  $ABCD$  evoluci (2.12),

$$h(x, x_0; z, \dots) \approx e^{\frac{i}{2B}(Dx^2 - 2xx_0 + Ax_0^2)}. \quad (2.20)$$

## 2.4 Konečná apertura

Vyskytnou-li se v transformačním systému ztráty, například částečně propustné stínítko, dochází k procesu měření a evoluce se stává neunitární. Můžeme si představit například vlnovou funkci dopadající na nepropustné stínítko s otvorem (aperturou) o velikosti  $2a$ . Toto zařízení provádí spektrální rozklad v bázi vlastních stavů  $|\xi\rangle$  souřadnice  $\widehat{x}$  v rovině stínítka a následnou projekci. Propuštěna je pouze ta část spektra, pro jejíž vlastní čísla platí  $\xi \in [-a, a]$ , kde  $2a$  je průměr apertury. Zbytek spektra je absorbován. Takovou neunitární evoluci popíšeme projekčním evolučním operátorem

$$\widehat{\chi}(2a) = \int_{-a}^a d\xi |\xi\rangle \langle \xi|. \quad (2.21)$$

Při reálném pozorování je vždy přítomné jisté omezení zorného pole, tedy konečná apertura, a transformační operátor  $\widehat{T}$  obsahuje projektor (2.21). Transformační systém reálného pozorovatele je tedy neunitární a po provedení transformace je nutné výstupní kvantový stav normalizovat pro zachování pravděpodobnosti,  $|\langle \psi_{\text{out}} | \psi_{\text{out}} \rangle|^2 = 1$

# Kapitola 3

## Detekce

V předchozí kapitole jsme zmínili kanonické pozorovatelné, tedy zobecněnou polohu a hybnost, a jejich vývoj v rámci unitární evoluce. Při popisu apertury jsme si rovněž všimli, že vlastní funkce a vlastní hodnoty pozorovatelné  $\hat{x}$  (souřadnice na stínítku) souvisí s měřením. Vlastní funkce  $|\xi\rangle$  operátoru  $\hat{x}$  nacházející se mimo aperturu jsou detekovány a nejsou zastoupeny ve vlnové funkci za rovinou apertury.

Obecně každá pozorovatelná  $\hat{O}$ , tj. pozitivně definitní operátor působící na Hilbertově prostoru  $\mathcal{H}$ , představuje měření v kvantové teorii. Výsledky měření jsou určeny spektrem pozorovatelné. Vlastní funkce reprezentují možné stavy kvantového systému po měření, vlastní hodnoty potom možné hodnoty pozorovatelné. Podrobněji viz učebnice kvantové teorie, například [5, 19, 20]. Vzhledem k hermiteovskosti pozorovatelné jsou její vlastní stavy ortogonální a tvoří úplný systém v  $\mathcal{H}$

$$\hat{O}|a\rangle = a|a\rangle, \quad \sum_a |a\rangle\langle a| = \hat{1}, \quad \langle a|a'\rangle = \delta_{aa'}. \quad (3.1)$$

Pravděpodobnost naměření vlastní hodnoty je dána překryvem příslušného vlastního stavu a měřeného stavu  $p_a = \text{Tr}[\hat{\rho}|a\rangle\langle a|]$ , střední hodnota pozorovatelné  $\langle\hat{O}\rangle = \text{Tr}[\hat{\rho}\hat{O}]$ . Úplnost v (3.1) zaručuje normování elementárních pravděpodobností  $\sum_a p_a = 1$ , ortogonalita implikuje exkluzivitu elementárních výstupů  $a$ .

Koncept *hermiteovských pozorovatelných* se ukázal jako nedostatečně obecný. Především výlučnost elementárních výstupů a „maximální rozlišovací schopnost“ pro danou veličinu nebývají v praxi splněny. Obecnějším přístupem je jakýkoli rozklad jednotky na pozitivně definitní operátory – *pozitivní operátorová míra* (POVM, POM, [21])

$$\hat{\Pi}_b \geq 0, \quad \sum_b \hat{\Pi}_b = \hat{1}. \quad (3.2)$$

Každý z operátorů  $\hat{\Pi}_b$  je tvořen určitou lineární kombinací projektorů  $|a\rangle\langle a|$  a vyjadřuje tak naši neschopnost rozlišovat mezi příslušnými elementárními výstupy. Pravděpodobnost výskytu „složeného“ výstupu  $b$  je  $p_b = \text{Tr}[\hat{\rho}\hat{\Pi}_b]$ .

Studujme prostorovou strukturu vlnové funkce, tedy stav kvantového systému (částice) v  $x$ -reprezentaci. Kvadrát absolutní hodnoty vlnové funkce představuje pravděpodobnost nalezení částice, například elektronu nebo fotonu, v daném místě. Pokud je zkoumaným systémem mod světla, vlnová funkce odpovídá amplitudě elektromagnetického pole ve skalární aproximaci a kvadrát její absolutní hodnoty odpovídá skalární optické intenzitě,

$$I(x) = p(x) = \text{Tr} [\hat{\rho}_{\text{out}} |x\rangle\langle x|] = \Gamma(x, x, z), \quad (3.3)$$

tedy vzájemné intenzitě (2.4) pro  $x' = x$ . Měření intenzity odpovídá pozorovatelné  $\hat{O}(x) = |x\rangle\langle x|$ .

Pro reálný detektor, například CCD kameru, vykazující konečnou prostorovou rozlišovací schopnost je však nutné provést diskretizaci vzhledem k pixelům. Pro  $i$ -tý pixel nabývá detekční operátor tvaru

$$\hat{O}_i = \int_{\Delta_i} dx |x\rangle\langle x|, \quad (3.4)$$

kde  $\Delta_i$  je plocha  $i$ -tého pixelu detektoru.

Představme si pozorovatele vybaveného pomocným optickým zařízením a intenzitním detektorem (3.4). Pozorovaný (vstupní) systém v kvantovém stavu  $\hat{\rho}_{\text{in}}$ , je transformován (2.10) zařízením  $\hat{T}$  a výstupní systém ve stavu  $\hat{\rho}_{\text{out}}$  je přiveden na detektor (3.4). Ten v každém svém pixelu načítá elementární detekční události během detekčního času. Výsledkem je vektor  $N_i$  celkového počtu událostí v každém z pixelů. Normováním obdržíme relativní četnosti (frekvence)  $f_i = N_i/N$ ,  $N = \sum_i N_i$ , jednotlivých výstupů. Tyto frekvence se blíží teoretickým intenzitám (pravděpodobnostem)

$$p_i = \text{Tr} [\hat{\rho}_{\text{out}} \hat{O}_i] = \text{Tr} [\hat{\rho}_{\text{in}} \hat{\Pi}_i], \quad \hat{\Pi}_i = \hat{T}^+ \hat{O}_i \hat{T}. \quad (3.5)$$

se vzrůstajícím počtem elementárních měření  $N$ , respektive s prodlužujícím se detekčním časem.

Operátory  $\hat{\Pi}_i$  reprezentují POVM našeho pozorovatele a kompletně popisují provedené měření. Zahrnují jak účinky transformačního systému  $\hat{T}$ , včetně jeho případné neunitárnosti, tak i vlastní detekci. Případné další vlivy, například statistiku detekce, lze zahrnout podobným způsobem.

# Kapitola 4

## Odhad stavu

### 4.1 Přímé metody

V předchozí kapitole jsme využili POVM  $\hat{\Pi}_i$  k popisu měření v rámci kvantové teorie. Aplikujeme-li toto měření na stav  $\hat{\rho}$ , získáme s pravděpodobností  $p_i$  výstup  $i$ ,  $N_i \rightarrow N_i + 1$ . Měřicí zařízení si můžeme představit jako skříňku (black box) s žárovkami a výstup  $i$  jako rozsvícení  $i$ -té žárovky. Po provedení  $N$  elementárních měření získáme relativní četnosti  $f_i = N_i/N$  jednotlivých výstupů. S ohledem na stabilitu relativních četností (1.2) můžeme pro dostatečně velké  $N$  ztotožnit relativní četnosti  $f_i$  s teoretickými pravděpodobnostmi  $p_i$  (3.5),

$$\text{Tr} [\hat{\rho} \hat{\Pi}_i] = f_i, \quad (4.1)$$

kde jsme pro jednoduchost vynechali index  $\text{in}$ .

Operátor hustoty  $\hat{\rho}$ , stejně jako element POVM  $\hat{\Pi}_i$ , jsou v konkrétní reprezentaci vyjádřeny pomocí pozitivně definitních hermiteovských matic. Levá strana  $i$ -té rovnice (4.1) je tedy lineární kombinací elementů matice hustoty. V Hilbertově prostoru  $\mathcal{H}$  dimenze  $\dim \mathcal{H}$  je operátor hustoty kompletně popsán (parametrizován) pomocí  $(\dim \mathcal{H})^2 - 1$  reálných čísel, kde bereme v úvahu  $\text{Tr} [\hat{\rho}] = 1$ . Aplikujeme-li známé měření  $\hat{\Pi}_i$  na neznámý stav  $\hat{\rho}$ , obdržíme čísla  $f_i$ . V případě stejného počtu výstupů  $\hat{\Pi}_i$  a neznámých parametrů operátoru hustoty představují rovnice (4.1) pro jednotlivé výstupy  $i$  nehomogenní soustavu lineárních rovnic. Řešením soustavy (4.1) získáme neznámé parametry, a tudíž i neznámý operátor hustoty  $\hat{\rho}$ . Popsaný postup založený na ztotožnění relativních četností a příslušných pravděpodobností je základem všech *přímých* rekonstrukčních metod. Rekonstruovaný operátor hustoty budeme nazývat *odhad* a značit  $\hat{\rho}_{\text{est}}$ , na rozdíl od skutečného operátoru hustoty  $\hat{\rho}$  někdy označovaného  $\hat{\rho}_{\text{true}}$ .

Přímé metody založené na (4.1) jsou spojené s celou řadou problémů, nicméně pro jejich přímočarost a výpočetní nenáročnost jsou velmi rozšířené ve výzkumu i v praxi. Snadno si můžeme všimnout, že v případě většího nebo menšího počtu výstupů měřicího přístroje získáme přeurčenou nebo naopak nedourčenou soustavu lineárních rovnic. Podobně, pro složitější tomografická měření, jako je výpočetní tomografie nebo homodynní detekce, je

řešení (inverze) soustavy (4.1) problematické a vyžaduje speciální regularizační postupy. Pokud je struktura měření ještě složitější a obsahuje neunitární evoluci, je nalezení inverzního vztahu prakticky nemožné. Přitom neunitární evoluce nemusí být nutně způsobená pouze konečnou aperturou nebo jinou „nedokonalostí“ pozorovacího systému. Může také jít o nativní součást metody, jako v případě zástinových metod (metoda Foucaultova nože, metoda Töplerova zástinu). Je také zřejmé, že rovnice (4.1) nezaručují pozitivní definitnost operátoru hustoty  $\hat{\rho}_{\text{est}}$  odhadovaného stavu. Na rozdíl od předchozích „technických“ problémů je tento problém fyzikální a vychází přímo z principu metody. Přímá rekonstrukční metoda nám poskytne odhad  $\hat{\rho}_{\text{est}}$ , který obecně nespĺňuje vlastnosti kvantového stavu.

Nutnost regularizačních postupů při řešení (4.1) a problémy s pozitivní definitností odhadnutého stavu souvisí s fyzikálně chybným předpokladem (4.1) rovnosti detekovaných relativních četností  $f_i$  a teoretických pravděpodobností  $p_i$ . I malý rozdíl mezi  $f_i$  a  $p_i$  může vést při určitém POVM k podstatným rozdílům mezi  $\hat{\rho}_{\text{est}}$  a skutečným  $\hat{\rho}_{\text{true}}$ , *šum je zesilován*. Stejně tak snadno může dojít i k překročení oblasti pozitivně definitních operátorů.

## 4.2 Statistické metody

Všechny uvedené problémy – nekorektnost požadavku přesné rovnosti detekčních pravděpodobností a frekvencí, nemožnost syntetizovat výsledky více rozličných pozorovatelů a zpracování dat z neunitárních pozorování – řeší statistické metody zpracování dat.

Jejich společným principem je sestavení funkcionálu nad prostorem možných stavů, který je současně funkcí naměřených frekvencí  $f_i$ . Tento funkcionál následně kvantifikuje „vzdálenost“ stavu a pozorovaných dat, tedy vyjadřuje míru (metriku), s jakou je schopen zkoumaný stav vyprodukovat daná data. Nepoužíváme výrazu pravděpodobnost, neboť zmíněná metrika nemusí být normovaná. Stav s největší hodnotou tohoto metrického funkcionálu (estimator) je schopen nejlépe, ne nutně dokonale, vygenerovat pozorovaná data. Takový stav nazýváme odhadem (estimate). Přístup založený na teorii odhadu nevyžaduje předpoklad přesné rovnosti teoretických pravděpodobností a experimentálních dat. Jedná se o metodu zpracování dat, jenž mohou být získána z libovolných experimentálních uspořádání. Hledaný stav není explicitně vyjádřen pomocí dat, pouze za předpokladu jistých pozorovaných dat je výsledkem extremalizačního postupu. Na rozdíl od přímých inverzí je matematická formulace obecná a je ve shodě se základními principy.

Statistické metody rekonstrukce jsou často používány pro zpracování signálu a obrazu (image reconstruction, image enhancement). Příkladem může být optická, a speciálně konfokální, mikroskopie. Rozdíly mezi různými statistickými přístupy spočívají v konkrétní volbě funkcionálu odhadu.

Příklad. Místo rovnosti (4.1) relativních četností a teoretických pravděpodobností požadujeme minimalizaci jejich rozdílů

$$\sum_i \left| f_i - \text{Tr} \left[ \hat{\rho} \hat{\Pi}_i \right] \right|. \quad (4.2)$$

Funkcionál (4.2) je spojen se statistickou metodou nejmenších čtverců. Minimalizace funkcionálu

$$-\sum_i f_i \ln \text{Tr} \left[ \hat{\rho} \hat{\Pi}_i \right] \quad (4.3)$$

vzhledem ke stavu  $\hat{\rho}$  je zase podstatou metody maximální věrohodnosti (MLE), viz oddíl 4.4.

### 4.3 Bayesovský odhad

Uvažujme množinu  $\mathcal{S}$  přípustných vstupních stavů  $\{\hat{\rho}\}$ , množinu detekovaných relativních četností  $\{f_i\}$  na výstupu měřicího přístroje a množinu  $\{\hat{T}\}$  možných konfigurací měřicího přístroje. Tedy názorněji  $\{f_{ij}\}$  a  $\{\hat{T}_j\}$ , kde  $i$  parametrizuje pixel a  $j$  konfiguraci transformačního systému. Věrohodnostní funkce (likelihood) odpovídá na otázku, *jak pravděpodobná jsou výstupní data  $f_i$  a nastavení měřicího přístroje  $\hat{T}$ , byl-li na vstupu stav  $\hat{\rho}$ ,*

$$\mathcal{L} = \mathcal{L}(\hat{\rho}|f_i) = p(f_i, \hat{T}|\hat{\rho}_{\text{in}}). \quad (4.4)$$

Zřejmě, při realizaci jevu  $(f_i, \hat{T})$ , neurčuje obecně věrohodnostní funkce pravděpodobnost hypotézy „na vstupu je stav  $\hat{\rho}$ “ a není vzhledem k těmto hypotézám normovaná.

Pravděpodobnost hypotéz  $\hat{\rho}$  v závislosti na pozorovaných datech a nastavení měřicího přístroje určuje posteriorní pravděpodobnost  $p(\hat{\rho}|f_i, \hat{T})$ . Použijeme-li definici podmíněné pravděpodobnosti a jejího vztahu k pravděpodobnosti součinu, můžeme vyjádřit souvislost priorní pravděpodobnosti, posteriorní pravděpodobnosti a věrohodnosti (viz kapitolu 1) ve tvaru Bayesovy věty (1.6,1.7),

$$p(\hat{\rho}|f_i, \hat{T}) = \frac{p(f_i, \hat{T}|\hat{\rho}) p(\hat{\rho})}{p(f_i, \hat{T})}. \quad (4.5)$$

Úplná pravděpodobnost dat (1.5)

$$p(f_i, \hat{T}) = \int_{\hat{\rho} \in \mathcal{S}} d\hat{\rho} p(f_i, \hat{T}|\hat{\rho}) p(\hat{\rho}) \quad (4.6)$$

není v teorii odhadu příliš důležitá, neboť nezávisí na hypotézách a představuje pouhý normalizační faktor. Často se pro ni volí název evidence.

Poznámka. Rozklad (4.6) je založen na tvrzení o úplnosti a vzájemné výlučnosti hypotéz  $\hat{\rho} \in \mathcal{S}$ . Úplnost je zřejmá, neboť stojí přímo v definici množiny  $\mathcal{S}$ . Exkluzivita hypotéz značí, že na vstupu je buď stav  $\hat{\rho}^{(1)}$  nebo stav  $\hat{\rho}^{(2)}$ . Princip superpozice se nedá v tomto případě uplatnit, neboť lineární kombinace  $\lambda\hat{\rho}^{(1)} + (1-\lambda)\hat{\rho}^{(2)} = \hat{\rho}^{(3)}$  tvoří stav třetí, který je již v množině  $\mathcal{S}$  zastoupen, a je ve smyslu hypotéz exkluzivní s prvními dvěma stavy. Množina  $\mathcal{S}$  je tedy ve skutečnosti vektorový prostor všech fyzikálně přípustných operátorů hustoty.

V teorii odhadu se běžně vyskytuje několik postupů odhadu hypotézy o vstupním stavu. Lze maximalizovat její

1. posteriorní pravděpodobnost při určité dané priorní distribuci,
2. posteriorní pravděpodobnost při uniformní priorní distribuci,
3. věrohodnost,
4. logaritmus věrohodnosti;
5. řešit rekurentní rovnici pro hypotézu.

Naším cílem bude ukázat souvislost metod 2.–5.

Ekvivalence 2. a 3.

Tvrzení je zřejmé. Za předpokladu uniformní priorní informace nezávisí pravděpodobnost  $p(\hat{\rho})$  na hypotéze. Stejně tak evidence. Extrémy vzhledem k  $\hat{\rho}$  levé a pravé strany (4.5) jsou tedy identické.

Ekvivalence 3. a 4.

Opět zřejmé. Logaritmus je ryze monotonní funkce a zachovává extrémy.

Souvislost 4. a 5.

Nyní odvodíme rekurentní rovnici pro absolutní pravděpodobnost hypotézy „na vstupu je stav  $\hat{\rho}$ “, tedy jádro přístupu 5. K extremalizaci logaritmu věrohodnostní funkce přistoupíme v následující sekci a dokážeme ekvivalenci obou přístupů.

Vyjdeme ze vztahu pro úplnou pravděpodobnost  $p(\hat{\rho})$ ,

$$p(\hat{\rho}) = \sum_i p(\hat{\rho}|f_i, \hat{T}) p(f_i, \hat{T}), \quad (4.7)$$

do kterého dosadíme (4.5) společně s rozkladem (4.6). Tím „uzavřeme“ Bayesovu větu a obdržíme

$$p(\hat{\rho}) = R(\hat{\rho}) p(\hat{\rho}), \quad (4.8)$$

kde

$$R(\hat{\rho}) = \sum_i \frac{p(f_i, \hat{T})}{\int_{\hat{\rho}' \in \mathcal{S}} d\hat{\rho}' p(f_i, \hat{T}|\hat{\rho}') p(\hat{\rho}')} p(f_i, \hat{T}|\hat{\rho}). \quad (4.9)$$

Ještě jednou poznamenejme, že v přesnějším zápise by suma byla dvojná přes  $i, j$ , relativní četnosti  $f_{ij}$  a transformační operátory indexované  $\hat{T}_j$ . Řešení nelineární rovnice (4.8) je formálně totožné například s řešením

$$R(\hat{\rho}) = 1. \quad (4.10)$$

Jádro  $R$  nabývá hodnoty 1 na množině hypotéz, kterou považujeme za odhadnuté řešení  $\hat{\rho}_{\text{est}}$ . Prakticky nejvhodnější metodou řešení je metoda iterativní, která se přímo nabízí,

$$p(\hat{\rho}^{(n+1)}) = R(\hat{\rho}^{(n)}) p(\hat{\rho}^{(n)}). \quad (4.11)$$

Předchozí Bayesovský rekurentní algoritmus je snadno aplikovatelný na klasickou rekonstrukci obrazu v podobě Richardsonovy metody [22]. Předpokládáme-li totálně nekoherentní zobrazování (ignorujeme změny koherenčních vlastností při šíření), vstupní obrazovou intenzitu  $\hat{\rho} \rightarrow I$  a výstupní obrazovou intenzitu  $(f_i, \hat{T}) \rightarrow I_{\text{out}}$  degradovanou nekoherentní odezvou funkcí  $p(f_i, \hat{T}|\hat{\rho}) \rightarrow p(I_{\text{out}}|I) = p(S)$ ,  $I_{\text{out}} = S * I$ , lze dojít ke vztahům analogickým (4.8), (4.9), (4.10) a (4.11). Richardsonův postup spočívá na následující úvaze. Intenzitní distribuce reprezentují přímo nebo po vynormování pravděpodobnosti detekce, viz kapitolu 3. Můžeme tedy nahradit  $p(I) \rightarrow I$ ,  $p(I_{\text{out}}) \rightarrow I_{\text{out}}$  a  $p(I_{\text{out}}|I) \rightarrow S$  a získat z (4.8) a (4.9) extrémální rovnici pro vstupní intenzitu

$$I = R(I) I, \quad R(I) = \frac{\int_{I_{\text{out}}} I_{\text{out}}}{\int_I S I} S. \quad (4.12)$$

Poznámka. Symbol  $\int$  značí v (4.12) integraci přes spojitou oblast souřadnice  $x$ , respektive  $x_0$ , nebo sumaci přes pixely ve výstupní, popřípadě vstupní rovině. Nekoherentní odezvovalá funkce  $S = |h(x, x_0)|^2$ , kde  $h(x, x_0)$  je funkce bodové odezvy (2.15). Její Fourierova transformace je optická přenosová funkce, OTF, viz [17]. Explicitní diskrétní podobu vztahu (4.12) ve dvou dimenzích lze nalézt v Richardsonově práci [22].

Vezmeme-li v úvahu pozitivní definitnost operátorů hustoty a obecnou definici pravděpodobnostní míry jako zobrazení množiny stavů na množinu pozitivně definitních objektů zachovávající strukturu příslušných  $\sigma$ -algeber, můžeme v (4.8) a (4.9) nahradit  $p(\hat{\rho}) \rightarrow \hat{\rho}$ ,  $p(f_i, \hat{T}) \rightarrow f_i$ ,  $p(f_i, \hat{T}|\hat{\rho}) \rightarrow \hat{\Pi}_i$ , a dojít ke kvantovému analogu Richardsonova vztahu (4.12),

$$\hat{\rho} = \hat{R}(\hat{\rho}) \hat{\rho}, \quad \hat{R}(\hat{\rho}) = \sum_i \frac{f_i}{\text{Tr}[\hat{\Pi}_i \hat{\rho}]} \hat{\Pi}_i. \quad (4.13)$$

Zde  $\hat{\rho}$  odpovídá vstupnímu obrazu,  $f_i$  skutečně pozorovanému degradovanému výstupnímu obrazu,  $\hat{\Pi}_i$  odezvovalou funkci  $S$  a  $\text{Tr}[\hat{\Pi}_i \hat{\rho}] = p_i$  teoretickému degradovanému výstupnímu obrazu. Vztah (4.13) představuje významné zobecnění Richardsonova výsledku z úplně nekoherentního signálu na částečně koherentní (bude ukázáno dále) a současně z  $x$ -reprezentace na libovolnou reprezentaci, neboť je formulován na úrovni operátorů a kvantových stavů. V následující sekci odvodíme rekurentní rovnici (4.13) jednodušším způsobem, a to maximalizací věrohodnostní funkce.

## 4.4 Extremalizace věrohodnosti

Zkoumejme pravděpodobnost  $p(f_i, \hat{T}|p_i)$  jevu „při teoretických pravděpodobnostech  $p_i = \text{Tr}[\hat{\Pi}_i \hat{\rho}]$  výstupů  $\hat{\Pi}_i$  měřicího zařízení nastane konkrétní rozložení relativních četností  $f_i$  jednotlivých výstupů.“ Pravděpodobnost elementární detekce na prvním výstupu (pixelu)

je podle (3.5) rovna příslušné pravděpodobnosti (intenzitě)  $p_1$ . Pravděpodobnost zaregistrování  $N_1 = N f_1$  detekčních událostí je úměrná  $p_1^{N f_1}$ , s ohledem na zřejmou nezávislost jednotlivých detekcí. Vezmeme-li v úvahu nezávislost jednotlivých pixelů, pravděpodobnost realizace relativních četností  $f_i$  při teoretické intenzitě  $p_i$  udává multinomické rozdělení

$$p(f_i, \hat{T} | p_i) = p(f_i, \hat{T} | \hat{\rho}) \approx \prod_i p_i^{N f_i}, \quad (4.14)$$

které současně představuje nenormovanou věrohodnostní funkci (4.4). Užijeme (3.5), (4.4), (4.14), zanedbáme nedůležité konstantní faktory a získáme vyjádření pro *logaritmus věrohodnostní funkce*

$$\ln \mathcal{L}(\hat{\rho} | f_i) = \sum_i f_i \ln p_i = \sum_i f_i \ln \text{Tr} [\hat{\rho} \hat{\Pi}_i]. \quad (4.15)$$

Princip maximální věrohodnosti nám poskytne hledaný neznámý stav jako extrém věrohodnostního funkcionálu (4.15) na množině přípustných stavů

$$\hat{\rho}_{\text{est}} = \arg \max_{\hat{\rho} \in \mathcal{S}} \ln \mathcal{L}(\hat{\rho} | f_i). \quad (4.16)$$

Předloženou extrémální úlohu lze řešit derivací podle čistých stavů v rozkladu (2.1), tedy hledáním stacionárních bodů věrohodnosti [23, 24, 25], nebo ekvivalentně metodami variačního počtu. Předpokládejme variovaný extrémální stav

$${}^\nu \hat{\rho} = \hat{\rho} + \delta \hat{X}. \quad (4.17)$$

Operátor  $\hat{X}$  v předchozím je libovolný hermiteovský operátor s nulovou stopou pro zachování jednotkové stopy operátoru hustoty. Dosazením (4.17) do (4.15) najdeme příslušnou variaci věrohodnostního funkcionálu za dodatečné normovací podmínky  $G = \mu (\text{Tr} [\hat{\rho}] - 1) = 0$

$$\Delta = ({}^\nu \ln \mathcal{L} - {}^\nu G) - (\ln \mathcal{L} - G) = \sum_i \frac{f_i}{p_i} \text{Tr} [\hat{\Pi}_i \delta \hat{X}] - \mu \text{Tr} [\delta \hat{X}]. \quad (4.18)$$

Pro extrémálu  $\hat{\rho}$  nutně platí

$$\text{Tr} \left[ \left( \sum_i \frac{f_i}{p_i} \hat{\Pi}_i \right) \delta \hat{X} - \mu \delta \hat{X} \right] = 0. \quad (4.19)$$

Zavedeme označení  $\hat{R}$  pro extrémální operátor

$$\hat{R}(\hat{\rho}) = \sum_i \frac{f_i}{p_i} \hat{\Pi}_i, \quad (4.20)$$

identicky s (4.13). S pomocí (4.20) získáme pro odhadovaný operátor hustoty na extrémále

$$\text{Tr} \left[ \left( \hat{R} - \mu \hat{1} \right) \delta \hat{X} \right] = 0, \quad \forall \delta \hat{X},$$

což implikuje finální řešení extremalizační procedury

$$\widehat{R}(\widehat{\rho}) = \widehat{1}_{\widehat{\rho}}. \quad (4.21)$$

Index jednotkového operátoru zdůrazňuje, že nejde o absolutní jednotku, ale jednotku pouze na extrémále. Relace  $\mu = 1$  se snadno dokáže aplikováním stopy na vztah  $\widehat{R} = \mu \widehat{1}$  a použitím normovanosti vektoru frekvencí.

Poznámka. Podobný přechod od reálného funkcionalu odhadu k extrémální operátorové rovnici bychom mohli provést i pro jiné metriky, než věrohodnostní. Součet čtverců odchylek (4.2),  $\chi^2$ , modifikované  $\chi^2$ , Hellingerova vzdálenost a Haldeneova diskrepance mohou sloužit za příklad, viz [1]. Označíme-li  $\widehat{\Pi}'_i = \frac{f_i}{p_i} \widehat{\Pi}_i$  přeškálované POVM operátory (3.5) pozorování, uvědomíme-li si jejich pozitivní definitnost a připomeneme definici POVM (3.2), vidíme, že jednotkovost (4.21) extrémálního operátoru nad rekonstruovaným stavem vyjadřuje rozklad operátorové jednotky

$$\sum_i \widehat{\Pi}'_i = \widehat{1}_{\widehat{\rho}} \quad (4.22)$$

a soustava operátorů  $\widehat{\Pi}'_i$  splňuje všechny vlastnosti POVM. Toto *nové* POVM vytvořila metoda maximální věrohodnosti přeškálováním původního POVM, které popisuje ideálně náš měřicí přístroj a poskytuje teoretické pravděpodobnosti (3.5). Naproti tomu nové POVM popisuje konkrétní realizaci pozorování a vede ke skutečně naměřeným hodnotám

$$f_i = \text{Tr} \left[ \widehat{\rho} \widehat{\Pi}'_i \right]. \quad (4.23)$$

Lze dokázat, že věrohodnost je jedinou metrikou, která zachází s daty formou zobecněného POVM měření [25]. V tomto smyslu považujeme princip maxima věrohodnosti za výlučný.

Kvantové zobecnění (4.13) Richardsonova rekurentního vztahu pro klasickou priorní pravděpodobnost máme nyní exaktně dokázáno. Tím jsme uzavřeli důkaz ekvivalence bodů 4. a 5. z oddílu 4.2. Nepotřebnost priorní informace v přístupu 5. je zřejmá, neboť je to právě priorní rozdělení, jenž je hledáno. Díky ekvivalenci obou metod platí stejné tvrzení o principu maxima logaritmu věrohodnosti.

## 4.5 Odhad vzájemné intenzity

Jak již bylo řečeno, aplikací operátorové rovnice (4.21) věrohodnostní extrémály na prostor fyzikálně přípustných stavů  $\widehat{\rho} \in \mathcal{S}$  získáme operátorovou nelineární extrémální rovnici (4.13)

$$\widehat{R}(\widehat{\rho}) \widehat{\rho} = \widehat{\rho}, \quad (4.24)$$

popisující rekonstrukci vstupního operátoru hustoty jako zobecněné kvantové měření. Užitím úplnosti  $x$ -báze ve vstupní rovině lze operátorovou relaci (4.24) převést na rovnici nad prostorem funkcí, viz oddíl 2.1,

$$\int dx' \mathcal{R}(q, x') \Gamma(x', q', 0) = \Gamma(q, q', 0), \quad \mathcal{R}(q, x') = \sum_i \frac{f_i}{p_i} \mathcal{P}_i(q, x'). \quad (4.25)$$

Funkce

$$\mathcal{P}_i(q, x') = \int_{\Delta_i} dx h^*(x, q) h(x, x') \quad (4.26)$$

odpovídají elementům POVM  $\widehat{\Pi}_i$  v  $x$ -reprezentaci. Stejně jako v operátorovém případě, i zde je třeba zdůraznit nelinearitu rovnice (4.25), neboť detekční pravděpodobnosti  $p_i$  závisí na neznámé funkci  $\Gamma$ ,

$$p_i = \iint dq dq' \Gamma(q, q', 0) \mathcal{P}_i(q', q). \quad (4.27)$$

Pro úplnost připomeňme, že  $\Gamma(q, q', 0)$  označuje rekonstruovanou vzájemnou intenzitu ve vstupní rovině, viz oddíl 2.1, vztah (2.4), a  $h(x, x')$  značí odezvou funkci, viz oddíl 2.2, vztah (2.15).

Extremální rovnice (4.25) dává přirozeným způsobem do souvislosti rekonstruovaný signál s naměřenými daty a vlastnostmi měřícího přístroje. Neznámý stav je zastoupen korelační funkcí  $\Gamma(x, x')$  bez jakýchkoli předpokladů o jeho statistických vlastnostech. Rekonstrukční metoda tedy dovoluje stavu měnit své koherenční vlastnosti v procesu měření, jak je nutné pro její fyzikální bezspornost. Měřená data vstupují do rekonstrukční procedury jako frekvence  $f_i$ . Konečně vlastnosti optického transformačního systému jsou zahrnuty formou PSF  $h(x, x')$ . Vazba zmíněných faktorů je zřejmě neseparovatelná, především vzhledem k nelinearitě. Vyjadřuje neoddelitelnost stavu a jeho pozorování.

Popsaná metoda rekonstrukce operátoru hustoty  $\widehat{\rho}$  v  $x$ -reprezentaci představuje statistickou alternativu k přímým metodám rekonstrukce vzájemné intenzity a Wignerovy funkce v pracích [26, 27].

Poznámka. Richardsonův algoritmus (4.12) je ekvivalentní extremální rovnici (4.25) s dodatečným předpokladem totální nekoherence signálu v celém aktu pozorování. Omezíme-li rovnici (4.25) předpokladem  $\Gamma(q, q') = I(q) \delta(q - q')$ , obdržíme

$$\int dq' \mathcal{R}(q, q') I(q') = I(q).$$

Podobně (4.27) poskytne

$$p_i = \int dq \mathcal{P}_i(q, q) I(q).$$

Kombinací předchozích dvou vztahů získáme (4.12), a případnou diskretizací klasický Richardsonův vzorec [22] často používaný v různých modifikacích a optimalizovaných tvarech pro rekonstrukci obrazu.

## 4.6 Poznámky

Úzkou souvislost s metodou maxima věrohodnostní funkce (maximum likelihood estimation, MLE) má tzv. EM algoritmus (expectation—maximization algorithm) [28, 29]. Z pohledu kvantové teorie je zajímavé, že EM algoritmus lze doplnit dalším krokem, a to unitární evolucí. Takto vzniklý EMU algoritmus lze efektivně použít pro odhad kvantových stavů [30]. Metoda maximální věrohodnosti našla uplatnění také v odhadu kvantového měření [31], kvantového procesu [32] a v odhadu kvantového procesu pomocí neznámých testovacích stavů [33, 34]. V práci [34] lze najít také srovnání některých rekonstrukčních metod.

V některých případech může být zajímavou alternativou k odhadu stavu měření pouze jediné nebo několika charakteristik stavu [35, 36].

# Kapitola 5

## Rozlišení stavů

Rozlišení (diskriminace) stavů je v jistém směru jednodušší a blíží základním principům než odhad stavu. Úkolem je navrhnout měření, které nejlépe rozhoduje mezi stavy z dané množiny stavů fyzikálního systému [21]. Pro velký počet stavů, které pokrývají Hilbertův prostor systému, přechází problém rozlišení mezi stavy na problém odhadu stavu. Stejně jako odhad, má i rozlišení mezi stavy mnoho konkrétních aplikací. Zvláště můžeme jmenovat rozpoznávání cílů (target recognition), hledání vzorů (pattern matching), návrh detekčního zařízení pro klasické a kvantové komunikační kanály [37, 38], návrh útoků na kvantově kryptografické protokoly a hodnocení jejich bezpečnosti [39, 40], kvantové multimetry, atd.

### 5.1 Nejednoznačné rozlišení

Ortogonální čisté stavy  $|\psi\rangle$  a  $|\psi_\perp\rangle$  lze zřejmě rozlišit bez chyby, neboť přímo projektory  $|\psi\rangle\langle\psi|$  a  $|\psi_\perp\rangle\langle\psi_\perp|$  představují měření s výstupy  $\{1, 0\}$  a  $\{0, 1\}$ , jsou-li postupně aplikovány na rozlišované stavy.

První úvahy o rozlišitelnosti (distinguishability) dvou neortogonálních stavů pocházejí od von Neumanna [41]. Obecný problém diskriminace mezi několika smíšenými stavy s různou pravděpodobností formulovali Holevo a Helstrom [42, 21]. Explicitní řešení však bylo nalezeno pouze pro speciální případy, například pro dva a tři čisté stavy, nebo pro systém symetrických čistých stavů, a to vesměs pro systémy s nízkou dimenzí Hilbertova prostoru.

V následujícím se pro jednoduchost omezíme na rozlišení dvou stavů (binary decision) vyskytujících se se stejnou pravděpodobností. Při *nejednoznačném* (ambiguous) rozlišení mezi stavy  $\hat{\rho}_A$  a  $\hat{\rho}_B$  navrhujeme POVM měření  $\{\hat{\Pi}_A, \hat{\Pi}_B\}$ ,  $\hat{\Pi}_A + \hat{\Pi}_B = \hat{1}$ , které s co největší pravděpodobností poskytne výstup  $A$ , je-li aplikováno na stav  $\hat{\rho}_A$ , a současně s co největší pravděpodobností poskytne výstup  $B$ , je-li aplikováno na stav  $\hat{\rho}_B$ . Snažíme se tedy maximalizovat pravděpodobnost úspěchu (success rate)

$$P_{\text{succ}} = \frac{1}{2}(P_{AA} + P_{BB}) = \frac{1}{2}\text{Tr}[\hat{\rho}_A\hat{\Pi}_A] + \frac{1}{2}\text{Tr}[\hat{\rho}_B\hat{\Pi}_B]. \quad (5.1)$$

Zbývající „křížové“ pravděpodobnosti (detekce  $B$ , byl-li na vstupu stav  $\hat{\rho}_A$ , a naopak) formují pravděpodobnost chyby (error rate),

$$P_{\text{err}} = \frac{1}{2}(P_{AB} + P_{BA}) = \frac{1}{2}\text{Tr} \left[ \hat{\rho}_A \hat{\Pi}_B \right] + \frac{1}{2}\text{Tr} \left[ \hat{\rho}_B \hat{\Pi}_A \right]. \quad (5.2)$$

Problém minimalizace chybovosti (5.2) je ekvivalentní problému maximalizace úspěšnosti (5.1), neboť

$$P_{\text{succ}} + P_{\text{err}} = 1. \quad (5.3)$$

Optimální POVM měření, které maximalizuje pravděpodobnost úspěchu (5.1), získáme derivací (přesněji variací) pravděpodobnosti (5.1) podle  $\hat{\Pi}_i$ ,  $i \in \{A, B\}$ , a položením těchto derivací současně rovno nule. Hledání stacionárních bodů na prostoru možných měření je podmíněno dodržením vlastnosti POVM,  $\sum_i \hat{\Pi}_i = \hat{1}$ . Toho snadno dosáhneme s pomocí operátorového Lagrangeova multiplikátoru  $\hat{\lambda}$ ,

$$\text{Tr} \left[ \hat{\lambda} \left( \sum_i \hat{\Pi}_i - \hat{1} \right) \right] = 0. \quad (5.4)$$

Extremalizací výsledného efektivního funkcionálu úspěchu,

$$\mathbb{F}[\hat{\Pi}_A, \hat{\Pi}_B] = \text{Tr} \left[ \hat{\rho}_A \hat{\Pi}_A \right] + \text{Tr} \left[ \hat{\rho}_B \hat{\Pi}_B \right] - \text{Tr} \left[ \hat{\lambda} (\hat{\Pi}_A + \hat{\Pi}_B) \right], \quad (5.5)$$

získáme extrémální rovnice

$$\begin{aligned} \hat{\rho}_A \hat{\Pi}_A &= \hat{\lambda} \hat{\Pi}_A, \\ \hat{\rho}_B \hat{\Pi}_B &= \hat{\lambda} \hat{\Pi}_B. \end{aligned} \quad (5.6)$$

Jejich součet vede k Lagrangeovu multiplikátoru

$$\hat{\rho}_A \hat{\Pi}_A + \hat{\rho}_B \hat{\Pi}_B = \hat{\lambda}, \quad (5.7)$$

kde jsme využili úplnosti POVM  $\hat{\Pi}_i$ . Rozdílem rovnic (5.6) a vyloučením Lagrangeova multiplikátoru (5.7) získáme

$$(\hat{\rho}_A - \hat{\rho}_B) \hat{\Pi}_A \hat{\Pi}_B = \hat{0} \quad (5.8)$$

a podobně rozdílem rovnic (5.6) a rovnic hermiteovsky sdružených obdržíme

$$\hat{\Pi}_B (\hat{\rho}_A - \hat{\rho}_B) \hat{\Pi}_A = \hat{0}. \quad (5.9)$$

Relaci (5.9) pro více diskriminovaných stavů odvodil Holevo [42, 21]. Snadno lze dokázat, že rovnice (5.6) a (5.7) nejsou nezávislé. Platí jak (5.6)  $\Rightarrow$  (5.7), tak i implikace opačná [43, 21].

Kromě řešení extrémálních rovnic (5.6) bychom měli specifikovat, zda řešení představuje maximum nebo minimum úspěšnosti. V maximu výstup  $B$  detektoru zareaguje s větší pravděpodobností na stav  $B$ ,  $P_{BB} - P_{AB} \geq 0$ . Úpravou  $\hat{\rho}_B \hat{\Pi}_B - \hat{\rho}_A \hat{\Pi}_B \geq \hat{0}$  získáme  $(\hat{\rho}_B -$

$\widehat{\rho}_A)\widehat{\Pi}_B \geq \widehat{0}$ , respektive  $\widehat{\lambda} - \widehat{\rho}_A \geq \widehat{0}$  s pomocí (5.7). Podobně pro rozdíl pravděpodobností  $P_{AA}$  a  $P_{BA}$ . Maximum úspěšnosti je tedy podmíněno nerovnostmi

$$\begin{aligned}\widehat{\lambda} - \widehat{\rho}_A &\geq \widehat{0}, \\ \widehat{\lambda} - \widehat{\rho}_B &\geq \widehat{0},\end{aligned}\tag{5.10}$$

respektive nerovnostmi

$$\begin{aligned}(\widehat{\rho}_A - \widehat{\rho}_B)\widehat{\Pi}_A &\geq \widehat{0}, \\ (\widehat{\rho}_B - \widehat{\rho}_A)\widehat{\Pi}_B &\geq \widehat{0}.\end{aligned}\tag{5.11}$$

Extremální rovnice (5.6) a nerovnice (5.10) kompletně určují optimální POVM  $\{\widehat{\Pi}_A, \widehat{\Pi}_B\}$  a současně představují formulaci *semidefinitního programu* [43, 44, 45]. S ohledem na lineárnost funkcionálu úspěšnosti se řešení nachází „na hranici“ definičního oboru podmíněného vazbou  $\sum_i \widehat{\Pi}_i = \widehat{1}$  a podmínky (5.10), respektive (5.11), jsou splněny rovností.

V případě dvou stavů lze uvést postup řešení soustavy (5.6),(5.10) [21]. Nalezneme vlastní čísla a vlastní stavy operátoru  $\widehat{\rho}_A - \widehat{\rho}_B$ , seskupíme je na pozitivně definitní a negativní a z odpovídajících vlastních stavů vytvoříme součtem POVM operátory  $\{\widehat{\Pi}_A, \widehat{\Pi}_B\}$ . Pro systémy s malou dimenzí Hilbertova prostoru lze postup explicitně provést. Podobně pro dva čisté stavy  $\widehat{\rho}_A = |\psi_A\rangle\langle\psi_A|$ ,  $\widehat{\rho}_B = |\psi_B\rangle\langle\psi_B|$  lze zkonstruovat optimální POVM měření a vyhodnotit minimální dosažitelnou chybovost

$$P_{\text{err}} = \frac{1}{2} \left( 1 - \sqrt{1 - |\langle\psi_A|\psi_B\rangle|^2} \right),\tag{5.12}$$

nazývanou *Helstromova mez*.

V případě rozlišení mezi smíšenými stavy složitějšího systému je nalezení analytického tvaru optimálního POVM problematické, ne-li nemožné, vzhledem k obtížnosti řešení vlastněhodnotového problému pro operátor  $\widehat{\rho}_A - \widehat{\rho}_B$ . Podobně v případě většího počtu nesy-metrických stavů je analytické řešení nedosažitelné. Byly navrženy dvě numerické metody pro nalezení optimálního POVM měření v případě obecného počtu smíšených kvantových stavů s různou priori pravděpodobností. Jednak formulace v podobě semidefinitního programu [43, 44] a řešení pomocí již existujícího aparátu *semidefinitního programování* (SDP). Druhá možnost spočívá v rekurentním řešení extremálních rovnic (5.6) při zachování pozitivní definitnosti elementů POVM [44].

Optimalita měření může být kvantifikována i jinou mírou, než je pravděpodobnost úspěchu. Uvažujme diskriminaci stavů  $\widehat{\rho}_i$  pomocí POVM měření  $\widehat{\Pi}_j$ . Diskriminace bude tím úspěšnější, čím budou teoretické pravděpodobnosti  $P_{ij} = \text{Tr}[\widehat{\rho}_i\widehat{\Pi}_j]$  blíže 1 pro  $i = j$  a 0 pro  $i \neq j$ . Požadujeme tedy co nejmenší vzdálenost pravděpodobností  $P_{ij}$  od „ideálních dat“  $F_{ij} \approx \delta_{ij}$ . Přitom vzdálenost můžeme kvantifikovat pomocí různých měř, stejně jako při odhadu stavu. I zde se však ukazují výhody logaritmu věrohodnosti (log likelihood)

$$\ln \mathcal{L}[\widehat{\Pi}_j] = \sum_{ij} F_{ij} \ln P_{ij} = \sum_{ij} \delta_{ij} \ln \text{Tr} [\widehat{\rho}_i\widehat{\Pi}_j] = \sum_i \ln \text{Tr} [\widehat{\rho}_i\widehat{\Pi}_i].\tag{5.13}$$

Aplikaci na nedokonalý kvantový komunikační kanál lze najít v práci [38].

## 5.2 Jednoznačné rozlišení

Předchozí nejednoznačné rozlišení stavů nemusí být pro některé aplikace vhodné, neboť nemáme jistotu, že výsledek rozhodování je správný. Kdykoli může dojít k chybě, a to s pravděpodobností  $P_{\text{err}}$ . Zajímavou alternativu proto představuje *jednoznačné* (unambiguous) rozlišení [46, 47, 48]. V případě rozlišení dvou stavů  $\hat{\rho}_A, \hat{\rho}_B$  má POVM měření tři elementy,  $\{\hat{\Pi}_A, \hat{\Pi}_B, \hat{\Pi}_?\}$ . Zareaguje-li výstup  $A$  (respektive  $B$ ), víme jistě, že na vstupu byl stav  $\hat{\rho}_A$  (respektive  $\hat{\rho}_B$ ). Chybovost je tudíž nulová,  $P_{\text{err}} = 0$ , ale s pravděpodobností

$$P_{\text{inc}} = \frac{1}{2}(P_{A?} + P_{B?}) = \frac{1}{2}\text{Tr} [\hat{\rho}_A \hat{\Pi}_?] + \frac{1}{2}\text{Tr} [\hat{\rho}_B \hat{\Pi}_?] \quad (5.14)$$

nastávají neprůkazné (inconclusive) případy, kdy nedokážeme mezi stavy rozhodnout. Jednoznačné rozlišení je jednoduchým příkladem tzv. *pravděpodobnostního protokolu*, který pracuje jen někdy, ale pokud pracuje, tak bez chyby. Optimální diskriminační POVM minimalizuje pravděpodobnost  $P_{\text{inc}}$  neprůkazného výsledku, respektive maximalizuje úspěšnost  $P_{\text{succ}}$ , ovšem za podmínky  $P_{\text{err}} = 0$ . Zřejmě platí  $P_{\text{succ}} + P_{\text{inc}} = 1$ , neboť  $\hat{\Pi}_A + \hat{\Pi}_B + \hat{\Pi}_? = \hat{1}$ . Jednoznačné rozlišení navrhl v roce 1987 Ivanovič [46], dále jej studoval Dieks [47] a optimální řešení pro dva čisté stavy se stejnou priorní pravděpodobností našel Peres [48]. Podle těchto autorů se často užívá pro jednoznačné rozlišení názvu IDP diskriminace. Pravděpodobnost neprůkazného výsledku je dána překryvem rozlišovaných čistých stavů,

$$P_{\text{inc}} = |\langle \psi_A | \psi_B \rangle|. \quad (5.15)$$

Každá implementace jednoznačné diskriminace je tedy současně měřením překryvu rozlišovaných stavů.

Pro více nesymetrických stavů, případně pro stavy smíšené, je stejně jako v případě nejednoznačného rozlišení prakticky nemožné najít optimální POVM měření analyticky. Pro smíšené stavy navíc existuje jistá míra chybovosti daná „překryvem“ jejich spekter. Například nelze bez chyby rozlišit dva stavy světla, které oba obsahují podíl termálního záření. Bezchybného IDP rozlišení lze ve skutečnosti dosáhnout pouze pro lineárně nezávislé čisté stavy a triviální případy stavů smíšených. Lze ovšem zafixovat jistou hodnotu pravděpodobnosti  $P_{\text{inc}}$  a minimalizovat chybovost  $P_{\text{err}}$ , nebo naopak. Toto kombinované schéma diskriminace může být uplatněno i na stavy smíšené a zavádí relaci (trade-off) mezi pravděpodobností neprůkazného výsledku a pravděpodobností chyby [49].

Poznámka. V poslední době je rozlišení kvantových stavů intenzivně zkoumáno jak teoreticky (smíšené stavy, SDP, spojité systémy), tak experimentálně [50, 51, 52, 53].

# Literatura

- [1] C. R. Rao. *Linear Statistical Inference and Its Applications*. John Wiley, New York, 2nd ed. 1973.
- [2] E. T. Jaynes. *Probability Theory: The Logic of Science*. Washington University, fragmentary ed. 1994. Download is possible from <http://omega.albany.edu/JaynesBook.html> and <http://bayes.wustl.edu/etj/prob/book.pdf.tar.gz>.
- [3] W. Feller. *An Introduction to Probability Theory and Its Applications*. John Wiley, New York.
- [4] P. S. Laplace. Mémoire sur la probabilité des causes par les évènements. *Mémoires de l'Académie royale des sciences*, 6:321–656, 1774.
- [5] P. A. M. Dirac. *The Principles of Quantum Mechanics*. Clarendon Press, Oxford, 3rd ed. 1958. 1st ed. 1930.
- [6] T. W. B. Kibble. Geometrization of quantum mechanics. *Commun. Math. Phys.*, 65:189–201, 1979.
- [7] D. C. Brody and L. P. Hughston. Geometry of quantum statistical inference. *Phys. Rev. Lett.*, 77:2851–2854, 1996.
- [8] D. Finkelstein, J. M. Jauch, S. Schiminovich, and D. Speiser. Foundations of quaternion quantum mechanics. *J. Math. Phys.*, 3:207–220, 1962.
- [9] J. Peřina. *Quantum Statistic of Linear and Nonlinear Optical Phenomena*. Informatorium, 1989.
- [10] J. Peřina. *Coherence of Light*. D. Reidel Publ. Comp., Dordrecht, 2nd ed. 1985.
- [11] E. Wigner. On the quantum correction for thermodynamic equilibrium. *Phys. Rev.*, 40:749–759, 1932.
- [12] K. Husimi. Some formal properties of the density matrix. *Proc. Phys. Math. Soc. Japan*, 22:264, 1940.

- [13] R. J. Glauber. *Phys. Rev.*, 131:2766, 1963.
- [14] R. J. Glauber. *Phys. Rev. Lett.*, 10:84, 1963.
- [15] E. C. G. Sudarshan. *Phys. Rev. Lett.*, 10:277, 1963.
- [16] J. Ville. Theorie et applications de la notion de signal analytique. *Cables et Transmission*, 2A:61–74, 1948.
- [17] J. W. Goodman. *Introduction to Fourier Optics*. McGraw-Hill, 2nd ed. 1996.
- [18] A. Papoulis. Pulse compression, fiber communications, and diffraction: A unified approach. *J. Opt. Soc. Am. A*, 11:3–13, 1994.
- [19] D. I. Blochincev. *Základy kvantové mechaniky*. ČSAV, Praha, 1955.
- [20] J. J. Sakurai. *Modern Quantum Mechanics*. Addison-Wesley Publ. Comp., revised ed. 1994.
- [21] C. W. Helstrom. *Quantum Detection and Estimation Theory*. Academic Press, New York, 1976.
- [22] W. H. Richardson. Bayesian-based iterative method of image restoration. *J. Opt. Soc. Am.*, 62:55–59, 1972.
- [23] Z. Hradil. Quantum-state estimation. *Phys. Rev. A*, 55:R1561, 1997.
- [24] Z. Hradil, J. Summhammer, and H. Rauch. Quantum tomography as normalization of incompatible observation. *Phys. Lett. A*, 261:20, 1999.
- [25] Z. Hradil and J. Summhammer. Quantum theory of incompatible observations. *J. Phys. A: Math. Gen.*, 33:7607, 2000.
- [26] M. G. Raymer, M. Beck, and D. F. McAlister. Complex wave-field reconstruction using phase-space tomography. *Phys. Rev. Lett.*, 72:1137, 1994.
- [27] Ch. Kurtsiefer, T. Pfau, and J. Mlynek. Measurement of the Wigner function of an ensemble of helium atoms. *Nature*, 386:150, 1997.
- [28] A. P. Dempster, N. M. Laird, and D. B. Rubin. Maximum likelihood from incomplete data via the EM algorithm. *J. R. Statist. Soc. B*, 39:1–38, 1977.
- [29] Y. Vardi and D. Lee. From image deblurring to optimal investments: Maximum likelihood solutions for positive linear inverse problems. *J. R. Statist. Soc. B*, 55:569–612, 1993.
- [30] J. Řeháček, Z. Hradil, and M. Ježek. Iterative algorithm for reconstruction of entangled states. *Phys. Rev. A*, 63:040303(R), 2001.

- [31] J. Fiurášek. Maximum-likelihood estimation of quantum measurement. *Phys. Rev. A*, 64:024102, 2001.
- [32] J. Fiurášek and Z. Hradil. Maximum-likelihood estimation of quantum processes. *Phys. Rev. A*, 63:020101(R), 2001.
- [33] M. Ježek. Generalized measurement of process and states. In J. Peřina, Jr., M. Hrabovský, and J. Křepelka, editors, *First International Workshop on Classical and Quantum Interference*, Proceedings of SPIE, volume 4888, pages 84–92, 2002.
- [34] M. Ježek, J. Fiurášek, and Z. Hradil. Quantum inference of states and processes. Will be published in *Phys. Rev. A*, 2003. arXiv:quant-ph/0210146.
- [35] R. Filip. Overlap and entanglement-witness measurements. *Phys. Rev. A*, 65:062320, 2002.
- [36] A. K. Ekert, C. M. Alves, D. K. L. Oi, M. Horodecki, P. Horodecki, and L. C. Kwek. Direct estimations of linear and nonlinear functionals of a quantum state. *Phys. Rev. Lett.*, 88:217901, 2002.
- [37] M. Sasaki, K. Kato, M. Izutsu, and O. Hirota. Quantum channels showing superadditivity in classical capacity. *Phys. Rev. A*, 58:146, 1998.
- [38] M. Ježek. Discrimination between non perfectly known states. *Phys. Lett. A*, 299:441, 2002.
- [39] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres. Eavesdropping on quantum-cryptographical systems. *Phys. Rev. A*, 50:1047, 1994.
- [40] M. Dušek, M. Jahma, and N. Lütkenhaus. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Phys. Rev. A*, 62:022306, 2000.
- [41] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton Univ. Press, Princeton, 1955.
- [42] A. S. Holevo. Statistical decision theory for quantum systems. *J. Multivar. Anal.*, 3:337, 1973.
- [43] H. P. Yuen, R. S. Kennedy, and M. Lax. Optimum testing of multiple hypotheses in quantum detection theory. *IEEE Trans. Inform. Theory*, IT-21:125, 1975.
- [44] M. Ježek, J. Řeháček, and J. Fiurášek. Finding optimal strategies for minimum-error quantum-state discrimination. *Phys. Rev. A*, 65:060301(R), 2002.
- [45] Y. C. Eldar, A. Megretski, and G. C. Verghese. Designing optimal quantum detectors via semidefinite programming. *IEEE Trans. Inform. Theory*, 2002. arXiv:quant-ph/0205178.

- [46] I. D. Ivanovic. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 123:257, 1987.
- [47] D. Dieks. Overlap and distinguishability of quantum states. *Phys. Lett. A*, 126:303, 1988.
- [48] A. Peres. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 128:19, 1988.
- [49] J. Fiurášek and M. Ježek. Optimal discrimination of mixed quantum states involving inconclusive results. *Phys. Rev. A*, 67:012321, 2003.
- [50] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin. Unambiguous quantum measurement of nonorthogonal states. *Phys. Rev. A*, 54:3783, 1996.
- [51] S. M. Barnett and E. Riis. Experimental demonstration of polarization discrimination at the Helstrom bound. *J. Mod. Opt.*, 44:1061, 1997.
- [52] R. B. M. Clarke, A. Chefles, S. M. Barnett, and E. Riis. Experimental demonstration of optimal unambiguous state discrimination. *Phys. Rev. A*, 63:040305(R), 2001.
- [53] R. B. M. Clarke, V. M. Kendon, A. Chefles, S. M. Barnett, E. Riis, and M. Sasaki. Experimental realization of optimal detection strategies for overcomplete states. *Phys. Rev. A*, 64:012303, 2001.