PŘÍRODOVĚDECKÁ FAKULTA MASARYKOVY UNIVERZITY

Zdroje stlačení v kvantové optice

Diplomová práce

Brno 2007 Filip Zlámal

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně a s použitím uvedené literatury.

V Brně dne 21. května 2007

PODĚKOVÁNÍ

Chtěl bych velmi poděkovat vedoucímu diplomové práce ***Mgr. Tomáši Tycovi, PhD.*** *a též* ***prof. RNDr. Michalu Lencovi, PhD.*** *za cenné připomínky a rady.*

Obsah

Úvod

V současnosti hraje optická interferometrie důležitou roli v oblasti kvantové kryptografie. Neznámá informace ve formě kvantového stavu (tzv. kvantové tajemství) se prováže s pomocnými stavy (hráči) při průchodu optickou soustavou, což je soubor pasivních a aktivních optických prvků. K odprovázání tajemství se použije jiná optická soustava. Není však nutné, aby všichni hráči spolupracovali. Jako aktivní prvky (tj. stlačovače) se používají nelineární krystaly, které však v experimentech patří k nejnákladnějším. Při dekódování tajemství je proto snaha o optimalizaci jejich počtu.

Bylo již ukázáno [9], že v případě jednoho tajemství je možno jej odprovázat s použitím dvou stlačovacích prvků.

V této práci jsem se snažil o zobecnění tohoto výsledku, tj. o možnost odprovázání více kvantových tajemství najednou, nalezení extrakčního algoritmu a optimalizaci počtu stlačovačů.

Členění textu je následující. V 1. kapitole je popsána trocha historie z období tzv. staré kvantové teorie, jež ilustruje, že klasická fyzika není schopna některé jevy dostatečně vysvětlit. Následuje pak stručné shrnutí dnes používaného formálního přístupu ke kvantové teorii včetně postulátů. V 2. kapitole je kvantově popsán jeden z nejdůležitějších fyzikálních objektů - harmonický oscilátor. V kapitole následující jsou uvedeny vlastnosti a definice koherentních stavů, stlačených koherentních stavů a distribučních a kvazidistribučních funkcí. 4. kapitola se již zabývá způsobem popisu optických prvků a soustav a též velmi užitečným Braunsteinovým rozkladem. V 5. kapitole jsou uvedeny některé informace z oblasti kryptografie o sdílení tajemství a poslední kapitola je vlastní prací. V závěru jsou pak shrnuty dosažené výsledky.

Introduction

In these days the optical interferometry plays important role in the quantum cryptography. An uknown information in a form of a quantum state (quantum secret) is entangled with so called ancillary states (players) in an optical system, which consists of passive and active optical elements. Another optical system is used for the disentanglement. It is not necesarry for all players to collaborate. Nonlinear crystals are used as active elements (i.e. squeezers). But they are the most expensive parts in the experiments. That's way there is an effort for optimalization of their number.

It has already been shown [9] that in the case of one quantum secret the number of needed squeezers for disentanglement is two.

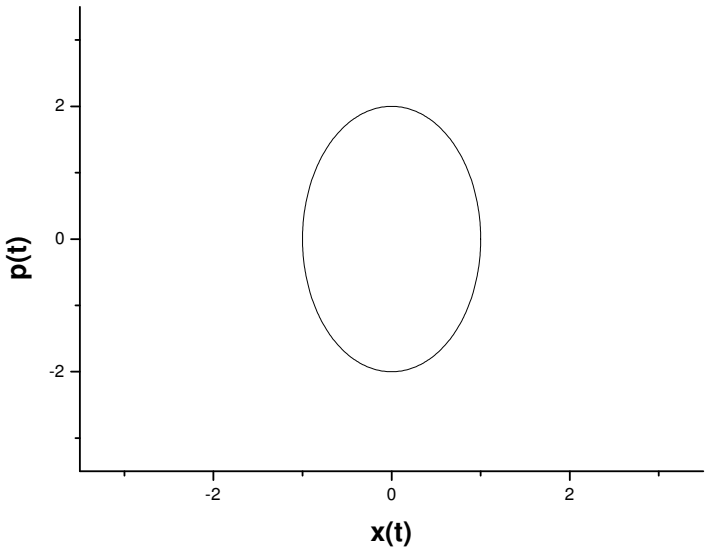
In this work I tried to generalize this result. It means to find out if it is possible to disentangle more than one quantum secret, to find extraction algorithm and the optimalized number of squeezers.

Text is organized as follows. A little bit old quantum history is described in the chapter 1. This illustrates the impossibility of classical physics to explain some features. Then the formal description of quantum physics with the postulates follows. In chapter 2 one of the most important physical object is treated quantum mechanicly - harmonic oscilator. The definitions and the properties of coherent states, squeezed coherent states and distributions and quasi-distributions are described in the folowing chapter. Chapter 4 shows how to describe optical elements and systems and also very important Braunstein decomposition. Some information about secret sharing can be found in chapter 5, next chapter is own work. In the end the results are specified.

Kapitola 1

Formalismus kvantové fyziky

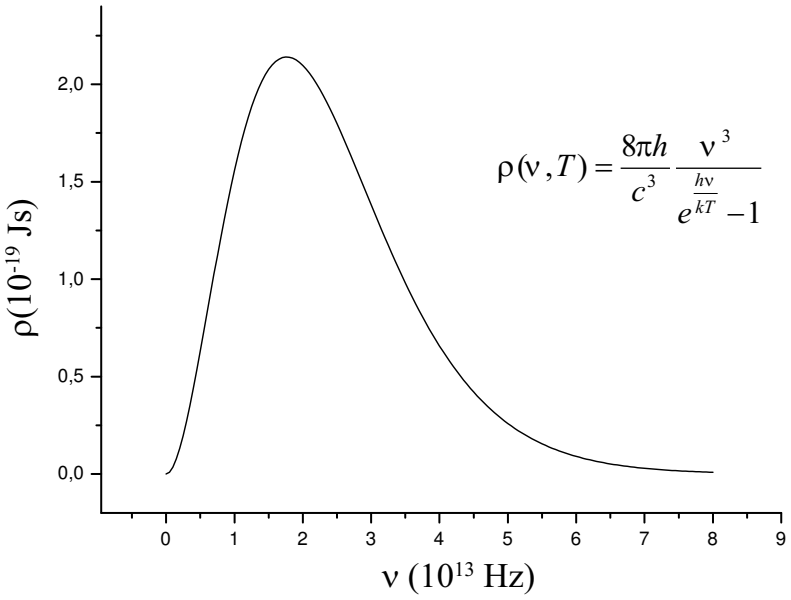
V klasické mechanice je stav jedné částice v časovém okamžiku t určen její polohou $\mathbf{r}(t)$ a hybností $\mathbf{p}(t)$ vyjádřenou v určitém souřadnicovém systému. Stav této částice tak charakterizuje šestice čísel a tu lze reprezentovat bodem ve fázovém prostoru s dimenzí 6. Obecně N–částicový systém je charakterizován bodem v $6N$–dimenzionálním fázovém prostoru. Pokud se tento systém vyvíjí v čase, tak jej ve fázovém prostoru charakterizuje fázová trajektorie.



Obrázek 1.1: Fázová trajektorie netlumeného harmonického oscilátoru.

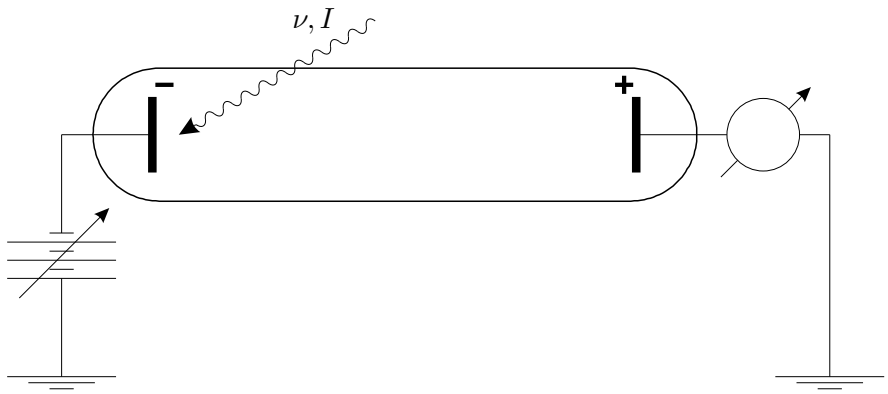
Klasicky je principiálně možné určit polohu a hybnost N–částicové soustavy s nekonečnou přesností. Jsme jen prakticky omezeni technickými a praktickými možnostmi měřících přístrojů.

Kvantová mechanika vznikla jako důsledek neschopnosti klasické fyziky teoreticky vysvětlit některé experimentální výsledky. Její počátek můžeme datovat do roku 1900. Tehdy se Maxu Planckovi podařilo teoreticky odvodit vztah pro spektrální hustotu záření absolutně černého tělesa. Byl však nucen přepokládat, že energie jednotlivých módů elektromagnetického pole záření vycházejícího z tohoto tělesa je úměrná jejich frekvenci, tj. je kvantovaná ($E = h\nu$, $h \approx 6,626.10^{-34}\, Js$ je Planckova konstanta). To bylo pochopitelně ve své době velmi zvláštní.



Obrázek 1.2: Spektrum absolutně černého tělesa pro $T = 300\,K$.

Dalším případem v pořadí byl fotoelektrický jev. Ten objevil v roce 1887 Heinrich Hertz, když náhodou zjistil, že se vodič, na nějž dopadá elektromagnetické vlnění, nabíjí kladně. Dále byly prováděny experimenty podle následujícího schématu.

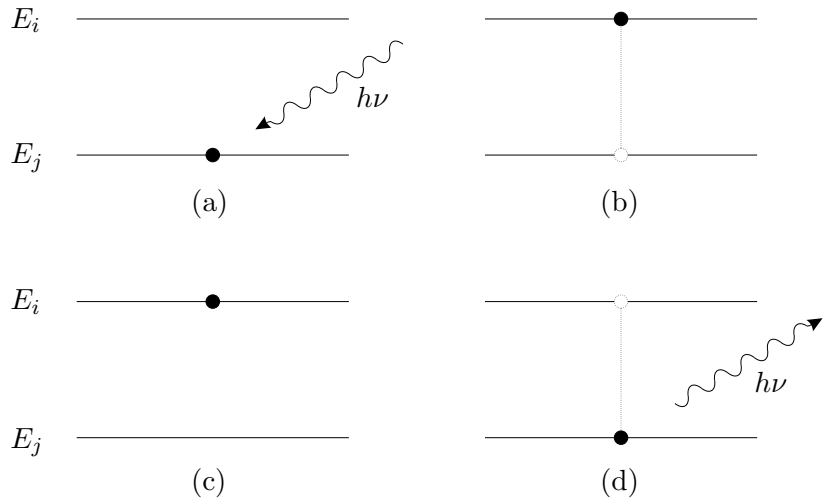


Obrázek 1.3: Experimentální schéma pro studium fotoelektrického jevu.

Na katodu dopadá elektromagnetické vlnění, charakterizované frekvencí ν a intenzitou I, to vyráží elektrony, které jsou elektrostaticky přitahovány k anodě a v trubici tak vzniká tzv. fotoproud. Podle klasické fyziky by k tomuto jevu mělo dojít. S rostoucí frekvencí by měla hustota fotoproudu růst, což se skutečně experimentálně potvrdilo. Co však už ne byla existence jevu od určité frekvence a závislost kinetické energie elektronů T a hustoty fotoproudu na frekvenci vlnění a nezávislost kinetické energie elektronů na intenzitě záření. Takže klasický pohled vylučuje vysvětlení tohoto jevu. Einstein proto předpokládal, že elektromagnetické vlnění (čili i světlo) může být absorbováno ve formě „balíčků“, tedy jednotlivých kvant energie, které byly

později nazvány fotony, a s pomocí tohoto náhledu již fotoelekrický jev úspěšně vysvětlil (1905). Energie absorbovaného záření $E = h\nu$ se spotřebuje na výstupní práci elektronu A, tj. energii potřebnou k tomu, aby elektron opustil kov, a zbytek se projeví ve formě kinetické energie elektronu, tedy $E = A + T$.

Dalším příkladem neúspěšnosti klasické fyziky byla snaha o vysvětlení diskrétních spekter atomů velmi zředěných plynů (tím jsou atomy plynu odprostěny od vzájemné interakce). Pro jednoduchost si můžeme představit atom vodíku. Ten se skládá z jednoho protonu, tvořící jádro, a jednoho elektronu. Klasicky jsou podrobeny elektrostatické interakci a vzájemně se přitahují. Elektron by se podle zákonů klasické fyziky měl krouživým pohybem stále přibližovat k jádru. Tento pohyb by měl být zrychlený, a proto by měl elektron vyzařovat elektromagnetické vlny spojitě a nakonec by měl spadnout na jádro. Atom by měl být nestabilní s dobou života řádově 10^{-9} s. Nicméně zkušenost ukazuje, že spektrum vodíku je diskrétní a že tyto atomy jsou stabilní. Niels Bohr, aby tuto podivnost vysvětlil, vytvořil nový model atomu (19??), který byl po něm později nazván. Je založen na následujících předpokladech: 1) elektrony se v atomu mohou nalézat jen v určitých stavech s určitými energiemi (energiové hladiny), 2) elektron může mezi jednotlivými energiovými hladinami E_i a E_j přecházet, přičemž při tomto přechodu přijme nebo vyzáří foton o frekvenci $\nu_{ij} = (E_i - E_j)/h$; pokud přechází elektron z hladiny nižší na vyšší, je foton elektronem absorbován, v opačném případě je foton vyzářen.



Obrázek 1.4: (a) Elektron s energií E_j absorbuje foton o energii $h\nu$, (b) elektron je excitován na energetickou hladinu $E_i = E_j + h\nu$; (c) elektron s energií E_i (d) klesá na energetickou hladinu E_j, přičemž vyzáří foton s energií $h\nu = E_i - E_j$.

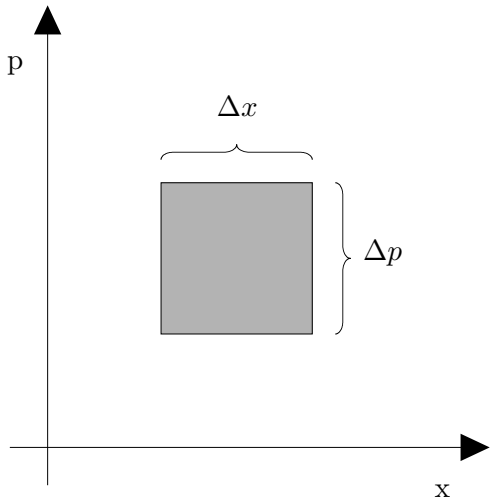
Ukazovalo se tedy, že světlo se za jistých okolností chová jako vlna (Thompsonův experiment) a jindy zase jako částice (fotoelektrický jev). V roce 1923 Louise de Broglie vyslovil hypotézu, že s každým objektem majícím hybnost p je možno spojit rovinnou monochromatickou vlnu, jejíž vlnová délka je dána vztahem $\lambda = h/p$. Pokud je to pravda, mělo by jít tuto vlnovou délku zjistit experimentálně.

V roce 1926 prováděli Davisson a Germer komerční experiment, v němž nechávali nízkoenergetické elektrony rozptylovat na povrchu jistého materiálu. Jeden vzorek však ztratil ochrannou atmosféru a na povrchu zoxidoval. Proto jej zahřáli, aby odstranili zoxidovanou vrstvu, a pak jej vložili znovu do ochranné atmosféry. Když však experiment provedli na tomto

vzorku, dostali difrakční obrazec. Chovali se tak podobně jako světlo při rozptylu na difrakční mřížce. Při zahřátí se totiž ze vzorku stal monokrystal a elektrony se na něm rozptýlili. Porovnali pak experimentálně získané výsledky a předpověď z de Broglieho hypotézy a dostali shodu.

Bylo tedy jasné, že klasická fyzika na vše nestačí a bylo třeba formulovat základy této nové fyzikální disciplíny, jež byla nazvána kvantová fyzika. K tomu došlo ve 20. a 30. letech 20. století zásluhou Diraca, Schrödingera, Heisenberga a dalších. Jako důsledky popisu se následně ukázaly např. relace neurčitosti nebo provázanost, které v klasické fyzice nemají obdoby.

Relace neurčitosti pro polohu a hybnost mají tvar $\Delta x \Delta p \geq \hbar/2$, kde Δx a Δp jsou po řadě neurčitosti v poloze a v hybnosti a $\hbar = h/(2\pi)$ je redukovaná Planckova konstanta. Tento vztah nám říká, že není principiálně možné určit neomezeně přesně polohu a hybnost nějakého objektu. Čím přesněji známe jednu veličinu, tím nepřesněji známe druhou, tj. čím lépe se snažíme zjistit, kde částice je (zmenšujeme Δx), tím neurčitější bude její hybnost (zvětšíme Δp). Proto charakterizovat kvantový systém prostřednictvím fázové trajektorie postrádá smysl.



Obrázek 1.5: Šedý čtverec je oblast minimální neurčitosti ve fázovém prostoru, $\Delta x = \Delta p = \sqrt{\hbar/2}$.

U objektů kvantové fyziky tak nelze obecně s jistotou říci, v jakém stavu se budou nacházet[1]. Můžeme to zjistit jen s určitou pravděpodobností. Z toho důvodu byla jako stavová veličina objektu zavedena tzv. vlnová funkce $\psi(x, y, z, t)$, která zcela charakterizuje příslušný objekt. Sama o sobě fyzikální význam nemá, avšak $|\psi(x, y, z, t)|^2$ udává pravděpodobnost toho, že se systém bude nacházet v bodě (x, y, z, t). Proto se vlnová funkce též nazývá amplituda pravděpodobnosti. Vlnová funkce je však konkrétním vyjádřením stavového vektoru v souřadnicové bázi. Stavové vektory tak mají obecnější charakter.

O matematickém formalismu a postulátech kvantové fyziky pojednávají následující dva odstavce.

1.1 Matematický aparát kvantové fyziky

Nechť $\mathbb{F}$ je pole skalárů (např. $\mathbb{R}$ nebo $\mathbb{C}$), jehož prvky nazýváme skaláry.

Definice 1: Množinu $\mathbb{V}$ nazveme *vektorovým prostorem* nad $\mathbb{F}$, jestliže na $\mathbb{V}$ jsou definovány

[1] Pokud jsme na nich neprovedli měření.

operace $+ : \mathbb{V} \times \mathbb{V} \ni (\mathbf{u}, \mathbf{v}) \to +(\mathbf{u}, \mathbf{v}) \equiv \mathbf{u} + \mathbf{v} \in \mathbb{V}$ nazývaná sčítáním vektorů a operace $. : \mathbb{F} \times \mathbb{V} \ni (\alpha, \mathbf{u}) \to .(\alpha, \mathbf{u}) \equiv \alpha\mathbf{u} \in \mathbb{V}$ nazývaná násobením vektoru skalárem při splnění následujících axiomů:

1) $\forall \mathbf{u}, \mathbf{v} \in \mathbb{V}$	$\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$
2) $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{V}$	$\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$
3) $\exists \mathbf{0} \in \mathbb{V}, \forall \mathbf{u} \in \mathbb{V}$	$\mathbf{u} + \mathbf{0} = \mathbf{0} + \mathbf{u} = \mathbf{u}$
4) $\forall \mathbf{u} \in \mathbb{V}, \exists (-\mathbf{u}) \in \mathbb{V}$	$\mathbf{u} + (-\mathbf{u}) = (-\mathbf{u}) + \mathbf{u} = \mathbf{0}$
5) $\forall \alpha, \beta \in \mathbb{F}, \forall \mathbf{u} \in \mathbb{V}$	$\alpha(\beta\mathbf{u}) = (\alpha\beta)\mathbf{u}$
6) $\exists 1 \in \mathbb{F}, \forall \mathbf{u} \in \mathbb{V}$	$1\mathbf{u} = \mathbf{u}1 = \mathbf{u}$
7) $\forall \alpha, \beta \in \mathbb{F}, \forall \mathbf{u} \in \mathbb{V}$	$(\alpha + \beta)\mathbf{u} = \alpha\mathbf{u} + \beta\mathbf{u}$
8) $\forall \alpha \in \mathbb{F}, \forall \mathbf{u}, \mathbf{v} \in \mathbb{V}$	$\alpha(\mathbf{u} + \mathbf{v}) = \alpha\mathbf{u} + \beta\mathbf{v}$

Příklad 1:

- Množiny $\mathbb{R}^n$ a $\mathbb{C}^n$ tvoří vektorový prostor.
- Množina řešení diferenciální rovnice $y'' + y = 0$ tvoří vektorový prostor dimenze 2.

Prvky $\mathbb{V}$ se nazývají vektory. V dalším budeme pracovat s vektorovými prostory nad $\mathbb{C}$.

- Vektor $u_1\mathbf{e}_1 + \cdots + u_n\mathbf{e}_n$ je *lineární kombinace* vektorů $\mathbf{e}_1, \ldots, \mathbf{e}_n \in \mathbb{V}$ pro nějaké $u_1, \ldots, u_n \in \mathbb{C}$.
- Vektory $\mathbf{e}_1, \ldots, \mathbf{e}_n$ nazveme *lineárně nezávislé*, jestliže
$$u_1\mathbf{e}_1 + \cdots + u_n\mathbf{e}_n = 0 \qquad \Rightarrow \qquad u_1 = \cdots = u_n = 0.$$
- Vektory, které nejsou nelineárně nazávislé, nazýváme lineárně závislé.
- *Maximálně lineární nezávislý systém* je soubor vektorů $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ takový, že soubor $(\mathbf{e}_1, \ldots, \mathbf{e}_n, \mathbf{e}_{n+1})$ je již lineárně závislý pro libovolný $\mathbf{e}_{n+1} \in \mathbb{V}$.
- Počet těchto vektorů (n) nazýváme *dimenzí* $\mathbb{V}$, označme proto tento prostor jako $\mathbb{V}_n$, a vektory $\mathbf{e}_1, \ldots, \mathbf{e}_n$ *bází* prostoru $\mathbb{V}_n$.
- Libovolný $\mathbf{u} \in \mathbb{V}_n$ lze vyjádřit jako lineární kombinace bázových vektorů., tj. $\mathbf{u} = u_1\mathbf{e}_1 + \cdots + u_n\mathbf{e}_n$.
- Tento vektor obvykle reprezentujeme pomocí jeho *složek* $u_1, \ldots, u_n$ v bázi $\mathbf{e}_1, \ldots, \mathbf{e}_n$ ve tvaru matice $n \times 1$: $\mathbf{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$.

Definice 2: *Skalární součin* je zobrazení $\langle . | . \rangle : \mathbb{V} \times \mathbb{V} \ni (\mathbf{u}, \mathbf{v}) \to \langle \mathbf{u} | \mathbf{v} \rangle \in \mathbb{C}$, přičemž platí

1) $\forall \mathbf{u}, \mathbf{v} \in \mathbb{V}$	$\langle \mathbf{u} \vert \mathbf{v} \rangle = \langle \mathbf{v} \vert \mathbf{u} \rangle^*$
2) $\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{V}$	$\langle \mathbf{u} \vert \mathbf{v} + \mathbf{w} \rangle = \langle \mathbf{u} \vert \mathbf{v} \rangle + \langle \mathbf{u} \vert \mathbf{w} \rangle$
3) $\forall \mathbf{u} \in \mathbb{V}, \forall \alpha \in \mathbb{C}$	$\langle \mathbf{u} \vert \alpha \vert \mathbf{v} \rangle = \alpha \langle \mathbf{u} \vert \mathbf{v} \rangle$
4) $\forall \mathbf{u} \in \mathbb{V}$	$\langle \mathbf{u} \vert \mathbf{u} \rangle \geq 0,\ \langle \mathbf{u} \vert \mathbf{u} \rangle = 0 \Leftrightarrow \vert \mathbf{u} \rangle = \mathbf{0}$

Skalární součin umožňuje definovat velikost vektoru $\mathbf{u} \in \mathbb{V}$ jako $\sqrt{\langle \mathbf{u}|\mathbf{u}\rangle}$ a úhel φ mezi vektory $\mathbf{u}$ a $\mathbf{v}$ jako $\cos\varphi = \frac{\langle \mathbf{u}|\mathbf{v}\rangle}{\sqrt{\langle \mathbf{u}|\mathbf{u}\rangle}\sqrt{\langle \mathbf{v}|\mathbf{v}\rangle}}$.

V kvantové mechanice se používá k zápisu vektorů tzv. Diracova notace. Pomocí ní namísto vektoru $\mathbf{u}$ píšeme $|\mathbf{u}\rangle$, nazýváme jej ket vektor, a vektor k němu hermiteovsky sdružený[2] $\mathbf{u}^\dagger$ je zapisován jako $\langle \mathbf{u}|$, nazýváme jej bra vektor ($\langle \underbrace{\mathbf{u}}_{bra} | \underbrace{\mathbf{v}}_{ket} \rangle$, *bracket* znamená závorka). Tato notace umožňuje elegantně zapsat skalární součin dvou vektorů, viz příklad.

Definice 3: Vektory $|\mathbf{u}\rangle, |\mathbf{v}\rangle \in \mathbb{V}_n$ nazveme *ortogonální* právě tehdy, když $\langle \mathbf{u}|\mathbf{v}\rangle = 0$.

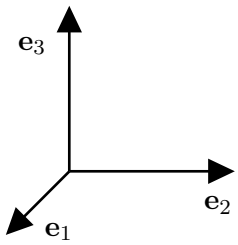
Ve $\mathbb{V}_2$ a $\mathbb{V}_3$ odpovídá pojem ortogonální pojmu kolmý. To je vidět z definice úhlu sevřeného dvěma vektory: pokud $\langle \mathbf{u}|\mathbf{v}\rangle = 0$, tak potom $\cos\varphi = 0$, tj. $\varphi = \frac{\pi}{2}$.

Definice 4: Řekneme, že vektor $|\mathbf{u}\rangle \in \mathbb{V}_n$ je *normovaný*, pokud $\langle \mathbf{u}|\mathbf{u}\rangle = 1$.

Tj. normovaný vektor má jednotkovou velikost.

Definice 5: Bázi $\mathbf{e}_1, \ldots, \mathbf{e}_n$ prostoru $\mathbb{V}_n$ nazveme *ortonormální* právě tehdy, když $\langle \mathbf{e}_i|\mathbf{e}_j\rangle = \delta_{ij}$, kde δ_{ij} je Kroneckerův symbol.

V $\mathbb{R}^3$ je ortonormální báze tvořena jednotkovými, na sebe vzájemně kolmými vektory.



Obrázek 1.6: Vektory ortonormální báze v $\mathbb{R}^3$.

Není těžké dokázat, že jestliže vektory $\mathbf{e}_1, \ldots, \mathbf{e}_n$ jsou ortogonální, tak potom jsou lineárně nezávislé.

Příklad 2: Pokud $|\mathbf{u}\rangle = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$, $|\mathbf{v}\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$ jsou vektory vyjádřené pomocí složek v ortonormální bázi prostoru $\mathbb{V}_n$, tak potom $\langle \mathbf{v}|\mathbf{u}\rangle = (v_1^* \ \cdots \ v_n^*) \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} = \sum_{i=1}^n v_i^* u_i$. Naopak, $|\mathbf{u}\rangle\langle \mathbf{v}| = \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix} (v_1^* \ \cdots \ v_n^*) = \begin{pmatrix} u_1 v_1^* & \cdots & u_1 v_n^* \\ \vdots & \ddots & \vdots \\ u_n v_1^* & \cdots & u_n v_n^* \end{pmatrix}$. Tzn. že $\langle \mathbf{v}|\mathbf{u}\rangle$ je číslo, $|\mathbf{u}\rangle\langle \mathbf{v}|$ je operátor.

[2]Hermiteovský znamená u matic transponovaný a komplexně sdružený.

Příklad 3: Mějme vektory $|\mathbf{u}\rangle = \begin{pmatrix} 1+\mathrm{i} \\ -2 \\ 2\mathrm{i} \end{pmatrix}$, $|\mathbf{v}\rangle = \begin{pmatrix} -3 \\ 3\mathrm{i} \\ -2+\mathrm{i} \end{pmatrix}$. Potom jejich skalární součin je $\langle \mathbf{u}|\mathbf{v}\rangle = (1-\mathrm{i}\ \ -2\ \ -2\mathrm{i}) \begin{pmatrix} -3 \\ 3\mathrm{i} \\ -2+\mathrm{i} \end{pmatrix} = -1+\mathrm{i}$. Dále je $|\mathbf{u}\rangle\langle\mathbf{v}| = \begin{pmatrix} 1+\mathrm{i} \\ -2 \\ 2\mathrm{i} \end{pmatrix} (-3\ \ -3\mathrm{i}\ \ -2-\mathrm{i}) =$
$= \begin{pmatrix} -3-3\mathrm{i} & 3-3\mathrm{i} & -1-3\mathrm{i} \\ 6 & 6\mathrm{i} & 4+2\mathrm{i} \\ -6\mathrm{i} & 6 & 2-4\mathrm{i} \end{pmatrix}$.

Definice 6: Na $\mathbb{V}_n$ definujme *normu* jakožto zobrazení $\|.\| : \mathbb{V}_n \ni \mathbf{u} \to \|\mathbf{u}\| \in \mathbb{R}$ takové, že

1) $\forall \mathbf{u}, \in \mathbb{V}$	$\|\mathbf{u}\| \geq 0, \|\mathbf{u}\| = 0 \Leftrightarrow \mathbf{u} = \mathbf{0}$
2) $\forall \mathbf{u} \in \mathbb{V}, \alpha \in \mathbb{F}$	$\|\alpha\mathbf{u}\| = \|\alpha\|.\|\mathbf{u}\|$
3) $\forall \mathbf{u}, \mathbf{v} \in \mathbb{V}$	$\|\mathbf{u}+\mathbf{v}\| \leq \|\mathbf{u}\| + \|\mathbf{v}\|$.

Ta na $\mathbb{V}$ intuitivně odpovídá pojmu velikost vektoru.

Příklad 4: Nejčastěji se lze setkat s těmito normami (pro libovolné $\mathbf{u} \in \mathbb{V}_n$):

- $\|\mathbf{u}\|_1 = \sum_{i=1}^n |u_i|$
- $\|\mathbf{u}\|_2 = \left(\sum_{i=1}^n |u_i|^2\right)^{1/2}$, tj. euklidovská norma
- $\|\mathbf{u}\|_\infty = \max\{|\mathrm{u}_1|, \ldots, |\mathrm{u}_\mathrm{n}|\}$, tj. maximální norma

Například pro vektor $|\mathbf{u}\rangle = \begin{pmatrix} 2 \\ 3\mathrm{i} \\ -1 \end{pmatrix}$ je $\|\mathbf{u}\|_1 = 2+3+1 = 6$, $\|\mathbf{u}\|_2 = (4+9+1)^{1/2} = \sqrt{14}$ a $\|\mathbf{u}\|_\infty = \max\{2,3,1\} = 3$.

Definice 7: *Prostor se skalárním součinem* $(\mathbb{V}, \langle.|.\rangle)$ je vektorový prostor $\mathbb{V}$, na němž je definován skalární součin $\langle.|.\rangle$.

Definice 8: *Normovaný vektorový (lineární) prostor* je vektorový prostor $\mathbb{V}$ s normou $\|.\|$.

Definice 9: Posloupnost $\{\mathbf{u}_n\}_{n=0}^\infty$ ($\mathbf{u}_n \in \mathbb{V}$, $\forall n \in \mathbb{N}_0$) nazveme *konvergentní* ve $(\mathbb{V}, \|.\|)$, jestliže $\exists \mathbf{u} \in \mathbb{V}$ tak, že $\forall \epsilon > 0$, $\exists n_0 \in \mathbb{N}$, $\forall n \in \mathbb{N}, n > n_0$ platí $\|\mathbf{u}_n - \mathbf{u}\| < \epsilon$.

Definice 10: Posloupnost $\{\mathbf{u}_n\}_{n=0}^\infty$ ($\mathbf{u}_n \in \mathbb{V}$, $\forall n \in \mathbb{N}_0$) nazveme *cauchyovskou* (ve $(\mathbb{V}, \|.\|)$), jestliže $\forall \epsilon > 0$, $\exists n_0 \in \mathbb{N}$, $\forall m, n \in \mathbb{N}$, $m, n > n_0$ platí $\|\mathbf{u}_m - \mathbf{u}_n\| < \epsilon$.

Není obtížné dokázat následující větu.

Věta 1: Každá konvergentní posloupnost je cauchyovská.

Obrácené tvrzení však obecně neplatí. Ukažme to na příkladu.

Příklad 5: Uvažujme normovaný vektorový prostor $(\mathbb{Q}, \|.\|)$ a cauchyovskou posloupnost $\{3; 3,1; 3,14; 3,141; 3,1415; \dots\}$. Její prvky jsou racionální čísla, posloupnost konverguje a její limitou je π, které však racionální není. Tzn. že prostor $(\mathbb{Q}, \|.\|)$ není úplný.

Definice 11: *Hilbertův prostor* je každý prostor se skalárním součinem, který je vzhledem k normě indukované skalárním součinem $\|\mathbf{u}\| = \sqrt{\langle \mathbf{u}|\mathbf{u}\rangle}$ úplný, tzn. že každá cauchyovská posloupnost v něm konverguje.

Každá cauchyovská posloupnost má v Hilbertově prostoru limitu patřící do tohoto prostoru. Méně přesně řečeno, úplný (tedy i Hilbertův) prostor je prostor, který nemá „díry“.

Definice 12: *Lineární operátor* $\hat{A}$ je zobrazení $\hat{A} : \mathcal{H} \ni |\mathbf{u}\rangle \to \hat{A}(|\mathbf{u}\rangle) \equiv \hat{A}|\mathbf{u}\rangle \in \mathcal{H}$ (tj. prvku Hilbertova prostoru je přiřazen opět prvek z téhož Hilbertova prostoru) takové, že toto zobrazení je lineární, tj. $\hat{A}(\alpha|\mathbf{u}\rangle + \beta|\mathbf{v}\rangle) = \alpha\hat{A}|\mathbf{u}\rangle + \beta\hat{A}|\mathbf{v}\rangle$ pro $\alpha, \beta \in \mathbb{C}$, $|\mathbf{u}\rangle, |\mathbf{v}\rangle \in \mathcal{H}$.

Příklad 6: Pokud třeba $\mathcal{H} = \mathbb{R}^n$, tak lineárním operátorem je matice $\mathbf{A} \in \mathbb{R}^{n\times n}$.

V dalším budeme pracovat jen s těmito operátory, proto budeme vynechávat přívlastek lineární.

V kvantové mechanice mají velký význam operátory hermiteovské a unitární. Uveďme jejich definice.

Definice 13: Nechť $|\mathbf{u}\rangle, |\mathbf{v}\rangle \in \mathcal{H}_S$ a nechť $\hat{A}$ je operátor, tzn. $|\mathbf{u}\rangle \to \hat{A}|\mathbf{u}\rangle$, $|\mathbf{v}\rangle \to \hat{A}|\mathbf{v}\rangle$. $\hat{A}$ nazveme *unitární* právě tehdy, když $\langle \mathbf{u}|\mathbf{v}\rangle = \langle \mathbf{u}|\hat{A}^\dagger\hat{A}|\mathbf{v}\rangle$. Operátor $\hat{A}$ nazveme *hermiteovský* právě tehdy, když $\langle \mathbf{u}|\hat{A}^\dagger|\mathbf{v}\rangle = \langle \mathbf{u}|\hat{A}|\mathbf{v}\rangle$.

Operátor, který daný stav transformuje identicky, se nazývá jednotkový a budeme ho značit $\hat{1}$. Tedy $\hat{1}|\mathbf{u}\rangle = |\mathbf{u}\rangle$.

Unitární operátor tak zachovává skalární součin a platí pro něj $\hat{A}^\dagger\hat{A} = \hat{1}$ neboli $\hat{A}^\dagger = \hat{A}^{-1}$. Pro hermiteovský operátor je pak $\hat{A}^\dagger = \hat{A}$.

Definice 14: Vektor $|\mathbf{u}\rangle \in \mathcal{H}$ nazveme *vlastním vektorem* operátoru $\hat{A}$ a číslo $\lambda \in \mathbb{C}$ jeho *vlastní hodnotou*, jestliže $\hat{A}|\mathbf{u}\rangle = \lambda|\mathbf{u}\rangle$.

Z definice plyne, že $(\hat{A} - \lambda\hat{1})|\mathbf{u}\rangle = \mathbf{0}$. V případě, že $\hat{A}$ je matice, tak máme rovnici, která je řešitelná právě tehdy, když $\det(\hat{A} - \lambda\hat{1}) = 0$, která se nazývá charakteristická a umožňuje získání souboru vlastních čísel $\{\lambda_1, \dots, \lambda_n\}$ zvaných spektrum. Vlastní vektory příslušné vlastní hodnotě λ_i dostaneme vyřešením rovnice $(\hat{A} - \lambda_i\hat{1}) = 0$. Pro hermiteovské a unitární operátory platí následující věta.

Věta 2: Nechť operátor $\hat{A}$ je unitární nebo hermiteovský. Potom vlastní vektory příslušné různým vlastním hodnotám jsou ortogonální. Navíc soubor těchto vlastních vektorů tvoří ortonormální bázi příslušného Hilbertova prostoru.

Věta 3: Vlastní čísla hermiteovského operátoru jsou reálná, vlastní čísla unitárního operátoru mají jednotkovou velikost.

Věta (o spektrálním rozkladu): Nechť $\hat{A}$ je hermiteovský nebo unitární operátor a nechť $\hat{A}|\mathbf{u}_i\rangle = \lambda_i|\mathbf{u}_i\rangle$ $(i = 1, \ldots, n)$. Potom

$$\hat{A} = \sum_{i=1}^{n} \lambda_i |\mathbf{u}_i\rangle\langle\mathbf{u}_i|.$$

Tzn. že takový operátor lze vždy vyjádřit pomocí jeho vlastních hodnot a vlastních vektorů.

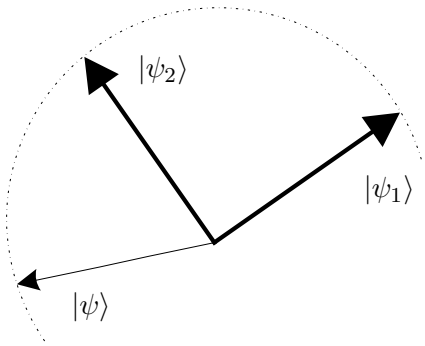
Příklad 7: Nalezněme vlastní čísla a vlastní vektory Pauliho matice $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Tato matice je zřejmě hermiteovská (a zároveň unitární). Charakteristická rovnice je $0 = \begin{vmatrix} 1-\lambda & 0 \\ 0 & -1-\lambda \end{vmatrix} = -(1-\lambda)(1+\lambda)$, tzn. že vlastní čísla matice σ_z jsou $\lambda_1 = 1$, $\lambda_2 = -1$. Nalezněme vlastní vektory. Označme $|\mathbf{u}_i\rangle$ vlastní vektor příslušný vlastnímu číslu λ_i $(i = 1, 2)$. Pro $\lambda_1 = 1$ máme soustavu $\begin{pmatrix} 0 & 0 \\ 0 & -2 \end{pmatrix} \sim \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, čili $|\mathbf{u}_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, a podobně $|\mathbf{u}_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Jak je vidět, tyto vektory jsou skutečně ortogonální. Podle věty o spektrálním rozkladu můžeme psát $\sigma_z = 1.\begin{pmatrix} 1 \\ 0 \end{pmatrix}(1\ \ 0) + (-1).\begin{pmatrix} 0 \\ 1 \end{pmatrix}(0\ \ 1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

1.2 Postuláty kvantové fyziky

V kvantové mechanice fyzikální systém S matematicky reprezentuje Hilbertův prostor $\mathcal{H}_S$ a její formální přístup je založen na dále zmíněných postulátech.

Postulát 1: Každý fyzikální stav systému S je kvantověmechanicky zastoupen vektorem $|\psi\rangle$ z příslušného Hilbertova prostoru $\mathcal{H}_S$ náležejícímu systému S.

- Předpokládejme, že máme $|\psi\rangle \in \mathcal{H}_S$. Nazýváme jej *stavový vektor* nebo též zkráceně *stav*.
- Jeho skalární součin $\langle\Phi|\psi\rangle$ s vektorem $|\Phi\rangle \in \mathcal{H}_S$ se nazývá *amplutida pravděpodobnosti*.
- Kvadrát modulu tohoto komplexního čísla $|\langle\Phi|\psi\rangle|^2$ udává pravděpodobnost toho, že když systém byl ve stavu $|\psi\rangle$, tak že bude ve stavu $|\Phi\rangle$, neboli určuje pravděpodobnost přechodu ze stavu $|\psi\rangle$ do stavu $|\Phi\rangle$.
- Jsou–li $|\psi_1\rangle$ a $|\psi_2\rangle$ dva stavové vektory patřící do téhož Hilbertova prostoru, tak i jejich lineární kombinace $|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle$ $(c_1, c_2 \in \mathbb{C})$ je stavovým vektorem patřícím do tohoto prostoru.
- Je zřejmé, že $|\langle\psi|\psi\rangle|^2 = 1$. To je *normovací podmínka*, kterou musí splňovat všechny fyzikální stavy, tedy i $|\psi_1\rangle$ a $|\psi_2\rangle$. Ta jistě omezuje možný výběr konstant c_1, c_2. Pokud $|\psi_1\rangle$ a $|\psi_2\rangle$ jsou ortogonální, dostáváme $|c_1|^2 + |c_2|^2 = 1$. To znamená, že všechny stavové vektory leží na jednotkové kouli v $\mathcal{H}_S$.



Obrázek 1.7: Lineární kombinace ortonormálních vektorů $|\psi_1\rangle$ a $|\psi_2\rangle$ v $\mathbb{R}^2$.

Postulát 2: Každá fyzikální veličina A je kvantověmechanicky reprezentována hermiteovským operátorem $\hat{A}$.

- Předpokládejme, že fyzikální veličina reprezentovaná hermiteovským operátorem $\hat{A}$ má vlastní stavy $|\psi_i\rangle$ s vlastními hodnotami λ_i, tj. $\hat{A}|\psi_i\rangle = \lambda_i|\psi_i\rangle$.
- Jak již víme, tento soubor vlastních stavů tvoří bázi celého Hilbertova prostoru $\mathcal{H}_S$ a tyto stavy jsou vzájemně ortogonální.
- To znamená, že libovolný $|\psi\rangle \in \mathcal{H}_S$ lze vyjádřit jako jejich lineární kombinaci, tj. $|\psi\rangle = \sum_i c_i|\psi_i\rangle$ (prostor může být i nekonečnědimenzionální, viz např. Fockovy stavy).
- Fyzikálně představuje vlastní stav $|\psi_i\rangle$ stav, na nějž se může $|\psi\rangle$ zobrazit jako důsledek provádění měření na $|\psi\rangle$, a to s amplitudou pravděpodobnosti c_i, čili s pravděpodobností $|c_i|^2$.
- Z normovací podmínky $|\langle\psi|\psi\rangle|^2 = 1$ dostáváme $\sum_i |c_i|^2 = 1$.
- Unitární operátory v kvantové fyzice realizují přechod mezi jednotlivými stavy, např. operátor časového vývoje.
- Pokud se systémy bude nacházet ve vlastním stavu, tak potom již nemůže přímo přejít do jiného vlastního stavu, protože tyto stavy jsou ortogonální a to znamená, že amplituda pravděpodobnosti tohoto přechodu je 0.

Báze

Uvažujme stav $|\psi\rangle \in \mathcal{H}_S$. Mějme nějakou bázi jako soubor $\{|\varphi\rangle\}$. Tato báze může být konečná, nekonečná spočetná a nekonečná nespočetná. Stav $|\psi\rangle$ pak vyjádříme v této bázi jako $|\psi\rangle = \sum_i \langle\varphi_i|\psi\rangle|\varphi_i\rangle$ v případě spočetné a $|\psi\rangle = \int \mathrm{d}\varphi \langle\varphi|\psi\rangle|\varphi\rangle$ v případě nespočetné báze.

- Příkladem konečné báze může být $\{|\uparrow\rangle, |\downarrow\rangle\}$ jako množina stavů se spinem nahoru a dolů. Pak $|\psi\rangle = \langle\uparrow|\psi\rangle|\uparrow\rangle + \langle\downarrow|\psi\rangle|\downarrow\rangle$.
- Jako nekonečnou spočetnou bázi lze uvést bázi Fockových stavů $\{|n\rangle\}_{n=0}^{\infty}$ (viz. dále). V ní $|\psi\rangle = \sum_{n=1}^{\infty}\langle n|\psi\rangle|n\rangle$.
- Nespočetnou bází je např. souřadnicová báze $\{|x\rangle\}_{x\in\mathbb{R}}$. Zde $|\psi\rangle = \int_{-\infty}^{\infty} \mathrm{d}x\, \langle x|\psi\rangle|x\rangle = \int_{-\infty}^{\infty} \mathrm{d}x\, \psi(x)|x\rangle$. $\psi(x)$ je vlnová funkce.

To vše je umožněno díky tomu, že $|\uparrow\rangle\langle\uparrow| + |\downarrow\rangle\langle\downarrow| = \hat{1}$, případně $\sum_{n=0}^{\infty}|n\rangle\langle n| = \hat{1}$, případně $\int_{-\infty}^{\infty} \mathrm{d}x\, |x\rangle\langle x| = \hat{1}$. Podobně lze pochopitelně přecházet i mezi jendotlivými bázemi.

Střední hodnoty a neurčitosti

Pokud máme systém v nějakém stavu, nelze obecně říci, v jakém stavu se systém ocitne, pokud na něj budeme aplikovat měření. Poté vždy systém přejde do jednoho ze svých vlastních stavů, a to s pravděpodobností danou jako kvadrát amplitudy pravděpodobnosti u vlastního stavu. Pokud jsme schopni vytvořit vhodným způsobem stav, který je vždy totožný, pak prakticky můžeme tyto pravděpodobnosti experimetnálně získat jako podíly četnosti výskytu systému v určitém vlastním stavu, do nějž by systém přešel po našem měření, a celkového počtu měření (v určité bázi). Na jednom stavu bychom provedli jedno měření, na dalším takovém stavu druhé měření atd. Výsledky měření jsou náhodné a mají tak určité pravděpodobnostní rozdělení.

Podobné je to s měřením fyzikálních veličin v určitém stavu. Pokud víme, v jakém stavu zjišťujeme hodnotu veličiny A, tak potom je možno výsledky teoreticky předpovědět. Střední hodnotu fyzikální veličiny A, zastoupenou hermiteovským operátorem $\hat{A}$, měřenou ve stavu $|\psi\rangle$ vypočteme jako

$$\langle \hat{A} \rangle = \langle \psi | \hat{A} | \psi \rangle. \tag{1.1}$$

Neurčitost této veličiny určíme ze vztahu známého z teorie pravděpodobnosti jako

$$\Delta A \equiv \sqrt{\langle (\Delta \hat{A})^2 \rangle} = \sqrt{\langle \hat{A}^2 \rangle - \langle \hat{A} \rangle^2} = \sqrt{\langle \psi | \hat{A}^2 | \psi \rangle - \langle \psi | \hat{A} | \psi \rangle^2}. \tag{1.2}$$

Lze ukázat, že pro relace neurčitosti dvou veličin A a B platí

$$\Delta A \Delta B = \sqrt{\langle \psi | \hat{A}^2 | \psi \rangle - \langle \psi | \hat{A} | \psi \rangle^2} \sqrt{\langle \psi | \hat{B}^2 | \psi \rangle - \langle \psi | \hat{B} | \psi \rangle^2} \geq \frac{1}{2} \left| \left\langle [\hat{A}, \hat{B}] \right\rangle \right|. \tag{1.3}$$

Například pro operátory polohy $\hat{x}$ a hybnosti $\hat{p}$ máme $[\hat{x}, \hat{p}] = i\hbar$, a tedy $\Delta x \Delta p \geq \hbar/2$, což je asi nejznámější relace neurčitosti. Pokud je komutátor operátorů nulový, tak se měření těchto dvou veličin v libovolném stavu neovlivňují. Například operátor z–vé složky momentu hybnosti $\hat{L}_z$ a operátor celkového momentu hybnosti $\hat{L}^2$ mají komutátor $[\hat{L}_z, \hat{L}^2] = 0$, proto $\Delta L_z \Delta L^2 = 0$, čili lze zároveň měřit hodnoty veličin L_z a L^2, aniž se vzájemně ovlivnili.

Kapitola 2

Časový vývoj, reprezentace, harmonický oscilátor

2.1 Časový vývoj v kvantové mechanice, reprezentace

Časový vývoj stavů

V kvantové mechanice je časový vývoj stavu $|\psi\rangle \in \mathcal{H}_S$ určen Schrödingerovou rovnicí

$$i\hbar \frac{\partial |\psi\rangle}{\partial t} = \hat{H}|\psi\rangle, \tag{2.1}$$

kde $\hat{H}$ je hamiltonián systému S. Pokud $|\psi_n\rangle$ je jeho vlastním stavem, tj.

$$\hat{H}|\psi_n\rangle = E_n|\psi_n\rangle,$$

tak potom

$$i\hbar \frac{\partial |\psi_n\rangle}{\partial t} = E_n|\psi_n\rangle,$$

a tedy

$$|\psi_n(t)\rangle = |\psi_n(0)\rangle e^{-\frac{i}{\hbar}E_n t}. \tag{2.2}$$

Tím je zadán časový vývoj vlastního stavu.
Lineární kombinací vlastních stavů, které tvoří ortonormální bázi $\mathcal{H}_S$, je opět stav z $\mathcal{H}_S$, tj.

$$|\phi(t)\rangle = \sum_n c_n(t)|\psi_n(t)\rangle, \tag{2.3}$$

jehož časový vývoj je podle (2.2)

$$|\phi(t)\rangle = \sum_n c_n(t)|\psi_n(0)\rangle e^{-\frac{i}{\hbar}E_n t}, \tag{2.4}$$

přičemž normovací podmínkou je

$$\sum_n |c_n(t)|^2 = 1 \tag{2.5}$$

v každém časovém okamžiku. Za předpokladu, že platí

$$\frac{\partial \hat{H}}{\partial t} = 0, \tag{2.6}$$

lze obecně pro stav $|\psi(t)\rangle$ psát (z (2.1))

$$|\psi(t)\rangle = \hat{U}(t)|\psi(0)\rangle, \tag{2.7}$$

kde

$$\hat{U}(t) = e^{-\frac{i}{\hbar}\hat{H}t} \tag{2.8}$$

se nazývá *operátor časového vývoje*. Ten je zřejmě unitární. Pokud ovšem vztah (2.6) neplatí, je v případě, že je splněno

$$[\hat{H}(t_1), \hat{H}(t_2)] = 0, \qquad t_1, t_2 \in (0, T),$$

nutno pro operátor časového vývoje psát

$$\hat{U}(t) = e^{-\frac{i}{\hbar}\int_0^T \hat{H}\mathrm{d}t}. \tag{2.9}$$

Časový vývoj kvantového stavu tak lze určit přímo ze Schrödingerovy rovnice nebo ekvivalentně pomocí operátoru časového vývoje. To však není jediný možný náhled.

Schrödingerova a Heisenbergova reprezentace

Pokud nás zajímá časový vývoj nějakého systému, tak můžeme pracovat

1) v reprezentaci, v níž jsou stavy na čase závislé a operátory se s časem nemění (to je tzv. *Schrödingerova reprezentace*),

$$|\psi_S(t)\rangle = \hat{U}(t)|\psi_S(0)\rangle \qquad \hat{A}_S(t) = \hat{A}_S(0)$$

2) v reprezentaci, v níž se stavy nemění a vyvíjejí se operítory (to je tzv. *Heisenbergova reprezantace*)

$$|\psi_H(t)\rangle = |\psi_H(0)\rangle \qquad \hat{A}_H(t) = \hat{U}^\dagger(t)\hat{A}_H(0)\hat{U}(t),$$

3) v reprezentaci, v níž se vyvíjejí stavy i operátory (to je tzv. *Diracova* nebo *interakční reprezentace*).

Ukažme, proč tomu tak je pro 1) a 2). Z fyzikálního hlediska výsledky měření nesmí záviset na zvolené reprezentaci. A fyzikálně měřitelné jsou střední hodnoty těchto veličin. Střední hodnota veličiny $\hat{A}_S$ ve Schrödingerově reprezentaci je

$$\begin{aligned}\langle\hat{A}_S(t)\rangle &= \langle\psi_S(t)|\hat{A}_S(t)|\psi_S(t)\rangle = \langle\psi_S(0)|\hat{U}^\dagger(t)\hat{A}_S(0)\hat{U}(t)|\psi_S(0)\rangle = \langle\psi_H(0)|\hat{A}_H(t)|\psi_H(0)\rangle = \\ &= \langle\psi_H(t)|\hat{A}_H(t)|\psi_H(t)\rangle = \langle\hat{A}_H(t)\rangle\end{aligned}$$

a je vidět, že střední hodnoty vypočtené ve Schrödingerově a Heisenbergově reprezentaci jsou skutečně totožné.

Časový vývoj operátoru

Časový vývoj operátoru $\hat{A}(t)$ je určen rovnicí:

$$\frac{\mathrm{d}}{\mathrm{d}t}\hat{A}(t) = \frac{1}{i\hbar}[\hat{A}, \hat{H}] + \frac{\partial}{\partial t}\hat{A}. \tag{2.10}$$

To lze odvodit z časového vývoje operátoru v Heisenbergově reprezentaci a užitím skutečnosti, že operátor časového vývoje komutuje s hamiltoniánem. Zde vidíme možný význam komutátoru, totiž že komutátor daného operátoru s hamiltoniánem určuje časový vývoj tohoto operátoru v Heisenbergově reprezentaci. Po určení komutátoru je pak pro určení $\hat{A}(t)$ třeba řešit diferenciální rovnici.
Pokud operátor $\hat{A}$ bude explicitně nezávislý na čase a pokud bude komutovat s hamiltoniánem $\hat{H}$, tak z (2.10) dostáváme, že veličina příslušející $\hat{A}$ bude integrálem pohybu.

Použitím Baker-Campbell-Hausdorffovy formule () pro $\hat{A}_H(t) = \hat{U}^\dagger(t)\hat{A}_h(0)\hat{U}(t)$ dostaneme

$$\hat{A}(t) = \hat{A} + \frac{1}{1!}\frac{it}{\hbar}[\hat{H}, \hat{A}] + \frac{1}{2!}\frac{i^2t^2}{\hbar^2}[\hat{H}, [\hat{H}, \hat{A}]] + \cdots + \frac{1}{n!}\frac{i^nt^n}{\hbar^n}[\hat{H}, [\ldots, [\hat{H}, \hat{A}]\ldots] + \cdots, \tag{2.11}$$

což je další užitečný vztah.

2.2 Hamiltonián harmonického oscilátoru, kreační a anihilační operátory

Hamiltonián harmonického oscilátoru má tvar

$$\hat{\mathcal{H}} = \frac{1}{2m}\hat{P}^2 + \frac{1}{2}m\omega^2\hat{X}^2. \tag{2.12}$$

Anihilační operátor $\hat{a}$ a *kreační operátor* $\hat{a}^\dagger$ jsou definovány jako

$$\hat{a} = \sqrt{\frac{m\omega}{2\hbar}}\,\hat{X} + i\sqrt{\frac{1}{2\hbar m\omega}}\,\hat{P} \tag{2.13}$$

$$\hat{a}^\dagger = \sqrt{\frac{m\omega}{2\hbar}}\,\hat{X} - i\sqrt{\frac{1}{2\hbar m\omega}}\,\hat{P}. \tag{2.14}$$

Použijme transformaci, která převádí proměnné X, P na proměnné s totožným rozměrem,

$$\hat{x} = \sqrt{\frac{m\omega}{\hbar}}\,\hat{X} \tag{2.15}$$

$$\hat{p} = \frac{1}{\sqrt{m\omega\hbar}}\,\hat{P}. \tag{2.16}$$

Tím dostaneme nový hamiltonián

$$\hat{H} = \frac{\hbar\omega}{2}(\hat{x}^2 + \hat{p}^2) \tag{2.17}$$

a kreační a anihilační operátory

$$\hat{a} = \frac{1}{\sqrt{2}}\,(\hat{x} + i\hat{p}) \tag{2.18}$$

$$\hat{a}^\dagger = \frac{1}{\sqrt{2}}\,(\hat{x} - i\hat{p}) \tag{2.19}$$

a odtud

$$\hat{x} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a}) \tag{2.20}$$

$$\hat{p} = \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a}). \tag{2.21}$$

Dále položme $\hbar = \omega = 1$. V nových proměnných máme

$$[\hat{x}, \hat{p}] = i\hat{1}. \tag{2.22}$$

Zřejmě platí

$$\hat{a}^\dagger = (\hat{a})^\dagger \tag{2.23}$$

a

$$[\hat{a}, \hat{a}^\dagger] = \hat{1}. \tag{2.24}$$

Pomocí (2.18) a (2.19) s použitím (2.24) lze (2.17) psát ve tvaru

$$\hat{H} = \frac{1}{2}\left(\hat{a}\hat{a}^\dagger + \hat{a}^\dagger\hat{a}\right) = \hat{a}^\dagger\hat{a} + \frac{1}{2}\cdot \tag{2.25}$$

Označme $\hat{a}^\dagger\hat{a} = \hat{n}$, $\hat{n}$ se nazývá *operátor počtu excitací*, s jehož pomocí je možno psát

$$\hat{H} = \hat{n} + \frac{1}{2}\cdot \tag{2.26}$$

Označme $|\psi_n\rangle$ vlastní stav hamiltoniánu $\hat{H}$ s vlastní hodnotou E_n, $|n\rangle$ vlastní stav operátoru $\hat{n}$ s vlastní hodnotou n, tak díky (2.26) platí

$$[\hat{H}, \hat{n}] = 0 \tag{2.27}$$

a

$$E_n = n + \frac{1}{2}, \tag{2.28}$$

kde $n = 0, 1, 2, \ldots$. Stav $|0\rangle$ je stav s 0 fotony (vakuum), $|1\rangle$ je stav s 1 fotonem atd. Tedy harmonický oscilátor se může nalézat jen ve stavech s určitými hodnotami energie dané ekvidistantní posloupností (2.28).

2.2.1 Další vlastnosti kreačního a anihilačního operátoru

Kreační a anihilační operátory působí na vlastní stav $|n\rangle$ takto:

$$\hat{a}|n\rangle = \sqrt{n}\,|n-1\rangle \tag{2.29}$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}\,|n+1\rangle. \tag{2.30}$$

Čili anihilační operátor snižuje počet fotonů ve stavu o jeden, kreační operátor naopak zvyšuje počet fotonů o jeden. Vícenásobným aplikováním těchto operátorů dostaneme

$$(\hat{a})^k|n\rangle = \sqrt{n}\cdot\ldots\cdot\sqrt{n-k+1}\,|n-k\rangle \tag{2.31}$$

$$(\hat{a}^\dagger)^k|n\rangle = \sqrt{n+1}\cdot\ldots\cdot\sqrt{n+k}\,|n+k\rangle, \tag{2.32}$$

kde $k \in \mathcal{N}$, a speciálně pro $k = n$ v (2.31) a $n = 0$ v (2.32) dostaneme

$$|0\rangle = \frac{1}{\sqrt{n!}}(\hat{a})^n|n\rangle \tag{2.33}$$

$$|n\rangle = \frac{1}{\sqrt{n!}}(\hat{a}^\dagger)^n|0\rangle. \tag{2.34}$$

Takto lze z vakua dospět do stavu s libovolným počtem fotonů.

2.2.2 Časový vývoj vlastního stavu harmonického oscilátoru

Dosazením (2.28) do (2.4) při přeznačení $|\psi_n(t)\rangle \equiv |u_n(t)\rangle$, $|\Psi(t)\rangle \equiv |u(t)\rangle$ dostaneme

$$|u(t)\rangle = e^{-\frac{i}{2}t} \sum_n c_n(t)|u_n(0)\rangle e^{-int}. \tag{2.35}$$

Faktor $e^{-\frac{i}{2}t}$ je globální a lze se jej formálně zbavit tak, že všechny energiové hladiny harmonického oscilátoru posuneme o $\frac{1}{2}$ směrem dolů. Potom je $E_n = n$.

2.2.3 Souřadnicová repretentace vlastního stavu harmonického oscilátoru

Vyjdeme z nečasové Schrödingerovy rovnice pro harmonický oscilátor

$$\frac{1}{2}(\hat{p}^2 + \hat{x}^2)|u_n\rangle = E_n|u_n\rangle \tag{2.36}$$

a po jejím vyjádření v souřadnicové reprezentaci a úpravě dostaneme diferenciální rovnici

$$\frac{\mathrm{d}^2 u_n(x)}{\mathrm{d}x^2} + (2E_n - x^2)u_n(x) = 0 \tag{2.37}$$

s řešením [1]

$$u_n(x) = \frac{1}{\sqrt{2^n n! \sqrt{\pi}}} e^{-\frac{x^2}{2}} H_n(x), \tag{2.38}$$

kde $H_n(x)$ jsou Hermiteovy polynomy stupně n v proměnné x. Vlastní stavy harmonického oscilátoru $|n\rangle$ se nazývají Fockovy stavy a tvoří ortonormální bázi (jelikož hamiltonián je hermiteovský operátor) zvanou Fockova.

Střední hodnota počtu fotonů ve Fockově stavu $\langle n\rangle = n$ a neurčitost v počtu fotonů je $\Delta n = 0$. Relace neurčitosti jsou

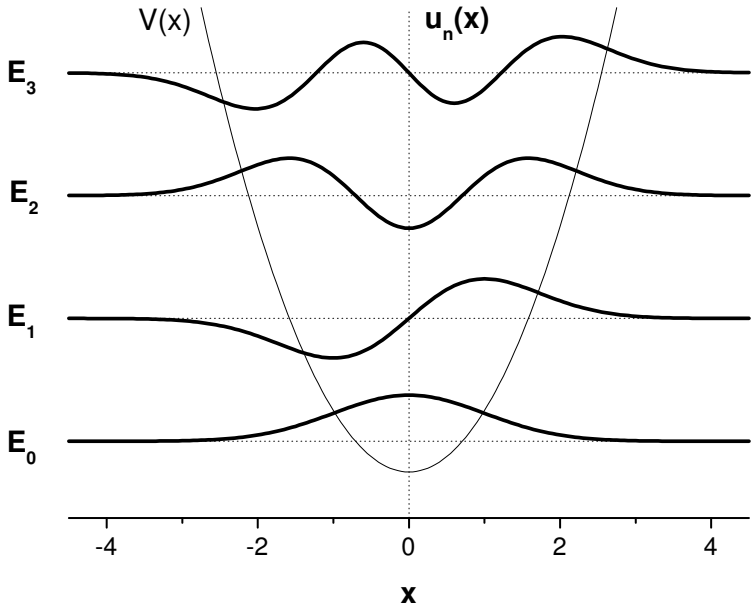
$$\Delta x \Delta p = \left(n + \frac{1}{2}\right).$$

Vakuum $|0\rangle$ tak splňuje mininální relaci neurčitosti.

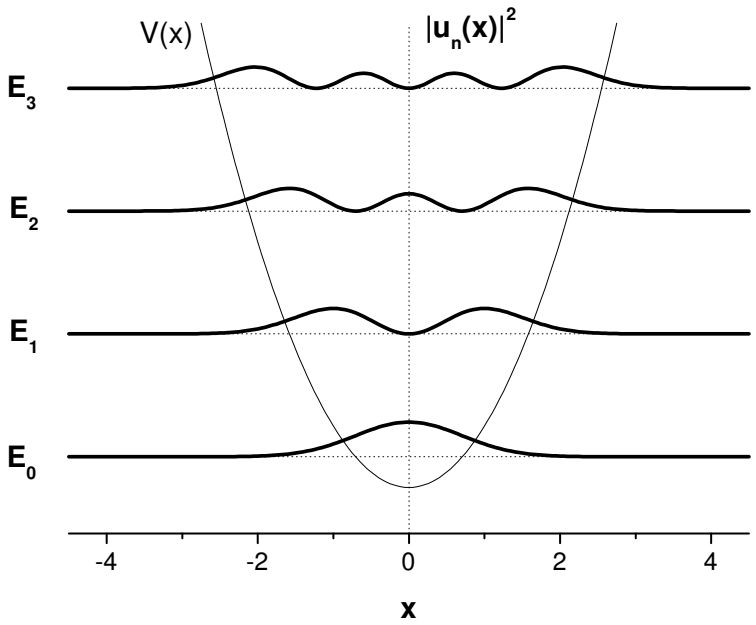
Souřadnicová reprezentace prvních čtyř Fockových stavů je uvedena v následující tabulce:

n	$u_n(x)$
0	$\frac{1}{\sqrt[4]{\pi}} e^{-\frac{x^2}{2}}$
1	$\frac{1}{\sqrt{2\sqrt{\pi}}} e^{-\frac{x^2}{2}}(2x)$
2	$\frac{1}{\sqrt{8\sqrt{\pi}}} e^{-\frac{x^2}{2}}(4x^2 - 2)$
3	$\frac{1}{\sqrt{48\sqrt{\pi}}} e^{-\frac{x^2}{2}}(8x^3 - 12x)$

Tabulka 2.1: Souřadnicová reprezentace základního a prvních tří excitovaných vlastních stavů harmonického oscilátoru.



Obrázek 2.1: Grafické vyjádření Fockových stavů $u_0(x)$, $u_1(x)$, $u_2(x)$ a $u_3(x)$.



Obrázek 2.2: Grafické vyjádření pravděpodobnostních funkcí pro Fockovy stavy $u_0(x)$, $u_1(x)$, $u_2(x)$ a $u_3(x)$.

Kapitola 3

Koherentní stavy, stlačené koherentní stavy a (kvazi)distribuční funkce

3.1 Koherentní stavy

Erwin Schrödinger ve svém článku [17] z roku 1926 hledal stavy, jež splňují minimální relace neurčitosti. Ukázal, že takovým stavem je vlastní stav bosonového anihilačního operátoru $\hat{a}$.

K hlubšímu zájmu a teoretickému rozvoji těchto stavů však došlo na počátku 60. let 20. století, a to zejména díky Royi Glauberovi (další např. Klauder, Sudarshan), který mj. ukázal [7], že koherentní stavy jsou vlastní stavy pozitivně-frekvenčního operátoru elektrického pole a zavedl posunovací operátor umožňující alternativní zavedení koherentního stavu. Je tak umožněno popsat elektrické pole právě pomocí koherentních stavů.

V současnosti se používají ke kvantověmechanickému popisu stavů generovaných lasery a můžeme se s nimi setkat též v teorii supravodivosti. Za zmínku stojí, že ze Schrödingerovy definice plyne, že anihilace fotonu nijak tento stav nemění, což má význam v oblasti detekce záření. Koherentní stavy slouží též jako základ pro studium širší třídy tzv. stlačených stavů, jimž je věnována podkapitola následující. Dá se ukázat, že klasický proud vyzařuje pole, které je právě v koherentním stavu [2].

V této podkapitole uvedeme jeho vlastnosti, ukážeme, že se jedná o posunutý základní stav harmonického oscilátoru.

Definice

Označme jako $|\alpha\rangle$ koherentní stav a definujme jej jako vlastní stav bosonového anihilačního operátoru $\hat{a}$

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle. \tag{3.1}$$

Jelikož operátor $\hat{a}$ není hermiteovský, je číslo α obecně komplexní. Hermitovským sdružením (3.2) dostaneme

$$\langle\alpha|\hat{a}^\dagger = \alpha^*\langle\alpha|, \tag{3.2}$$

takže kreační operátor $\hat{a}^\dagger$ je vlastním stavem $\langle\alpha|$.

Vyjádřeme koherentní stav v bázi Fockových stavů $\{|n\rangle\}_{n=0}^{\infty}$ pomocí jednotkového operátoru

$\hat{1} = \sum_{n=0}^{\infty} |n\rangle\langle n|$. Ten vložíme před $|\alpha\rangle$

$$|\alpha\rangle = \hat{1}|\alpha\rangle = \sum_{n=0}^{\infty} |n\rangle\langle n|\alpha\rangle = \sum_{n=0}^{\infty} |n\rangle\langle 0|\frac{\hat{a}^n}{\sqrt{n!}}|\alpha\rangle = \sum_{n=0}^{\infty} |n\rangle\langle 0|\frac{\alpha^n}{\sqrt{n!}}|\alpha\rangle = \langle 0|\alpha\rangle \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle.$$

Při úpravách jsme použili vyjádření Fockova stavu pomocí vakua a anihilačních operátorů () a definice koherentního stavu (). Z normovací podmínky $\langle\alpha|\alpha\rangle = 1$ zjistíme, že $\langle 0|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}}$. Celkem

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle. \tag{3.3}$$

Z definice (3.2) a ze vzorce (3.3) vyplývají další vlastnosti koherentního stavu.

Komplexní číslo α je tvaru

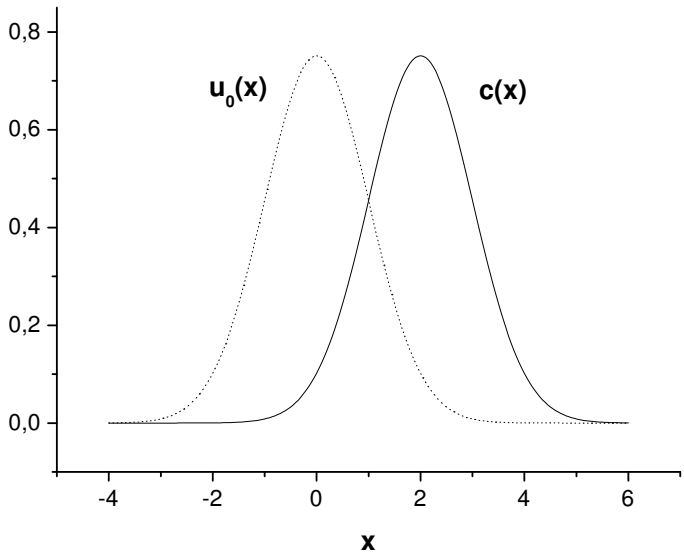
$$\alpha = \frac{\langle\hat{x}\rangle}{\sqrt{2}} + i\frac{\langle\hat{p}\rangle}{\sqrt{2}}. \tag{3.4}$$

Střední hodnoty souřadnice a hybnosti tak představují právě jeden koherentní stav.

Souřadnicová reprezentace koherentního stavu je

$$c(x) = \frac{1}{\sqrt[4]{\pi}} \exp\left(-\frac{1}{2}[(x - \langle\hat{x}\rangle) - i\langle\hat{p}\rangle]^2\right) \tag{3.5}$$

Při $\langle\hat{p}\rangle = 0$ je koherentní stav posunutým základním stavem harmonického oscilátoru.



Obrázek 3.1: Srovnání základního stavu harmonického oscilátoru $u_0(x)$ a koherentního stavu $c(x)$ v souřadnicové reprezentaci ($\langle\hat{x}\rangle = 2$, $\langle\hat{p}\rangle = 0$).

Vyjádření koherentního stavu ve Fockově bázi (3.3) umožňuje jeho alternativní zavedení, jako ukázal Glauber [7].

Posunovací operátor

Je definován [5] jako

$$\hat{D}(\alpha) = e^{\alpha\hat{a}^\dagger - \alpha^*\hat{a}}. \tag{3.6}$$

Koherentní stav matematicky dostaneme, když jej necháme zapůsobit na vakuum

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle \tag{3.7}$$

Z obrázku 2. je vidět, že tento operátor skutečně „posouvá“ vakuum. Posunovací operátor je unitární. Je totiž vidět, že

$$\hat{D}^\dagger(\alpha) = \hat{D}(-\alpha) = [\hat{D}(\alpha)]^{-1}. \tag{3.8}$$

Další pro výpočty užitečné vztahy jsou

$$\hat{D}^\dagger(\alpha)\hat{a}\hat{D}(\alpha) = \hat{a} + \alpha \tag{3.9}$$

$$\hat{D}^\dagger(\alpha)\hat{a}^\dagger\hat{D}(\alpha) = \hat{a}^\dagger + \alpha^*. \tag{3.10}$$

Díky unitaritě posuvného operátoru lze ukázat, že

$$\hat{D}^\dagger(\alpha)f(\hat{a},\hat{a}^\dagger)\hat{D}(\alpha) = f(\hat{a}+\alpha, \hat{a}^\dagger + \alpha^*), \tag{3.11}$$

kde operátor $f(\hat{a},\hat{a}^\dagger)$ je možno zapsat jako rozklad $f(\hat{a},\hat{a}^\dagger) = \sum_{m,n} c_{mn}\,\hat{a}^m(\hat{a}^\dagger)^n$, přičemž zde není podstatné uspořádání.

Dva koherentní stavy $|\alpha\rangle$ a $|\beta\rangle$ pro $\alpha \neq \beta$ nejsou ortogonální. Amplituda pravděpodobnosti přechodu od $|\beta\rangle$ k $|\alpha\rangle$ je

$$\langle\alpha|\beta\rangle = e^{-\frac{1}{2}(|\alpha|^2+|\beta|^2-2\alpha^*\beta)} \tag{3.12}$$

a pravděpodobnost tohoto přechodu je tak

$$|\langle\alpha|\beta\rangle|^2 = e^{-|\alpha-\beta|^2}. \tag{3.13}$$

Tzn. že čím jsou body Gaussovy roviny reprezentující koherentní stavy více vzdáleny, tím je pravděpodobnost přechodu od jednoho stavu k druhému menší.

Soubor koherentních stavů $\{|\alpha\rangle\}_{\alpha\in\mathbb{C}}$ tvoří bázi. Jednotkový operátor je vyjádřen jako

$$\hat{1} = \frac{1}{\pi}\int \mathrm{d}^2\alpha|\alpha\rangle\langle\alpha|, \tag{3.14}$$

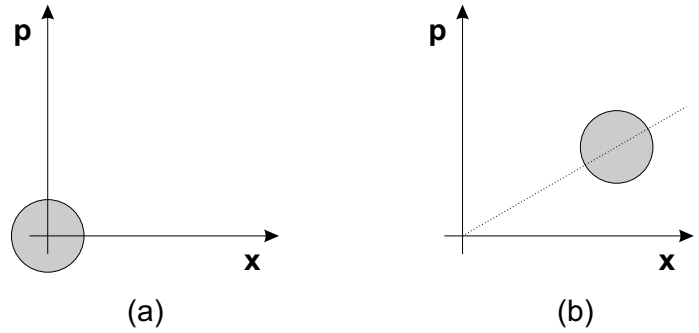
přičemž integrace probíhá přes celou komplexní rovinu. Soubor je však přeplněný a to má za následek, že libovolný stav není v bázi koherentních stavů rozložen jednoznačně.

Relace neurčitosti

Jednomódový koherentní stav splňuje minimální relaci neurčitosti

$$\Delta x\Delta p = \frac{1}{2}, \tag{3.15}$$

přičemž neurčitosti $\hat{x}$ a $\hat{p}$ jsou totožné, tj. $\Delta x = \Delta p = \frac{1}{\sqrt{2}}$. Tyto neurčitosti jsou s časem neproměnné. Taktéž je $(\Delta x)^2 + (\Delta p)^2 = 1$.



Obrázek 3.2: Srovnání oblastí neurčitosti (a) pro vakuum a (b) pro koherentní stav ve fázovém prostoru.

Fotonová statistika

Střední hodnota počtu fotonů $\langle \hat{n} \rangle$ v koherentním stavu je

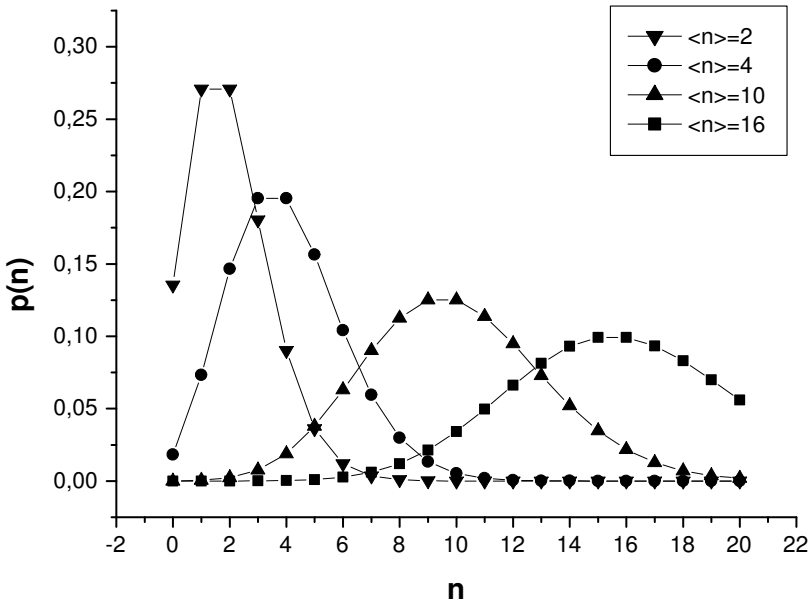
$$\langle \hat{n} \rangle = \langle \alpha | \hat{n} | \alpha \rangle = |\alpha|^2. \tag{3.16}$$

Odtud je zřejmý význam modulu komplexního čísla α, tj. jeho kvadrát udává střední hodnotu počtu fotonů ve stavu $|\alpha\rangle$.

Pravděpodobnost $p(n)$ nalezení n fotonů v koherentním stavu je

$$p(n) = |\langle n | \alpha \rangle|^2 = e^{-\langle n \rangle} \frac{\langle n \rangle^n}{n!}, \tag{3.17}$$

což je Poissonova rozdělovací funkce.



Obrázek 3.3: Rozdělení počtu fotonů v koherentním stavu pro některé hodnoty $\langle n \rangle$.

Pro Poissonovo rozdělení obecně platí, že střední hodnota náhodné veličiny v tomto stavu je rovna střední kvadratické odchylce[1] (neurčitosti), tj.

$$\Delta n = \langle \hat{n} \rangle. \tag{3.18}$$

Časový vývoj koherentního stavu

Díky vyjádření koherentního stavu ve Fockově bázi (3.3) a časového vývoje Fockova stavu (2.35) lze s využitím (2.2) a (2.28) psát

$$|\alpha(t)\rangle = e^{-\frac{i}{2}t} e^{-\frac{|\alpha(0)|^2}{2}} \sum_{n=0} \frac{\alpha(0)^n}{\sqrt{n!}} e^{-int} |n(0)\rangle = e^{-\frac{i}{2}t} |\alpha(0) e^{-it}\rangle \tag{3.19}$$

To znamená, že časová závislost koherentního přechází na komplexní číslo α, které tak periodicky obíhá kolem počátku Gaussovy roviny s jednotkovou frekvencí. Fázový faktor $e^{-\frac{i}{2}t}$ určuje globální fázi a lze jej formálně odstranit tak, že posuneme všechny energiové hladiny harmonického oscilátoru o $\frac{1}{2}$ směrem „dolů“, tj. $E_n = n$, a pak

$$|\alpha(t)\rangle = |\alpha(0) e^{-it}\rangle. \tag{3.20}$$

Pokud $\alpha(t)$ nahradíme intenzitou elektrického pole $E(t)$, tak dostaneme přesně časový vývoj jednoho módu elektrického pole. Koherentní stav tak kvantověmechanicky umožňuje popsat eletrické pole kvantověmechanicky.

Interpretace

Mějme klasickou částici o hmotnosti m a elektrickém náboji e nacházející se v rovnovážné poloze v oblasti harmonickém potenciálu $V(x)$ (viz obr.).
Hamiltonián této částice je zřejmě

$$H = \frac{p^2}{2m} + \frac{1}{2} k x^2. \tag{3.21}$$

Působme nyní na tuto částici elektrickou silou o intenzitě E. Pak je hamiltonián

$$H = \frac{p^2}{2m} + \frac{1}{2} k x^2 - eEx, \tag{3.22}$$

což lze upravit na tvar

$$H = \frac{p^2}{2m} + \frac{1}{2} k \left(x - \frac{eE}{k} \right)^2 - \frac{1}{2} k \left(\frac{eE}{k} \right)^2. \tag{3.23}$$

Získáme tak opět částici v oblasti harmonického potenciálu s novou rovnovážnou polohou. Dostaneme tak posunutý základní stav. Jestliže nyní vypneme pole E (tj. $E = 0$), tak získáme koherentní stav $|\alpha\rangle$.

[1] Obecně množina všech rozdělení splňující (3.18) se nazývá *poissonovská* a lze definovat další dvě kategorie statistických rozdělení: *superpoissonovská*, pro něž $\Delta n \geq \langle \hat{n} \rangle$, a *subpoissonovská*, pro než $\Delta n \leq \langle \hat{n} \rangle$.

n–módový koherentní stav

Není problém popsat pole skládající se z více módů, řekněme n, rozšířením definice koherentního stavu. n–módový koherentní stav je pomocí posunovacího operátoru definován jako

$$|\alpha_1, \ldots, \alpha_n\rangle = \prod_{i=1}^{n} \hat{D}(\alpha_i)|0, \ldots, 0\rangle, \tag{3.24}$$

přičemž $|0, \ldots, 0\rangle$ je n–módové vakuum. Odtud lze analogickým způsobem jako u jednoho módu získat vlastnosti $|\alpha_1, \ldots, \alpha_n\rangle$.

Operátor elektrického pole (s frekvencí ω) je

$$\hat{\mathbf{E}}(\mathbf{r}, t) = \frac{1}{L^{3/2}} \sum_{\mathbf{k}} l(\omega)\epsilon_{\mathbf{k}}[\hat{a}_{\mathbf{k}} e^{i(\mathbf{kr}-\omega t)} + \hat{a}^{\dagger}_{\mathbf{k}} e^{-i(\mathbf{kr}-\omega t)}], \tag{3.25}$$

kde $\epsilon_{\mathbf{k}}$ je jednotkový vektor polarizace ortogonální ke $\mathbf{k}$, $l(\omega)$ je funkce frekvence. Tento operátor je vhodné přepsat na

$$\hat{\mathbf{E}}(\mathbf{r}, t) = \hat{\mathbf{E}}^{+}(\mathbf{r}, t) + \hat{\mathbf{E}}^{-}(\mathbf{r}, t), \tag{3.26}$$

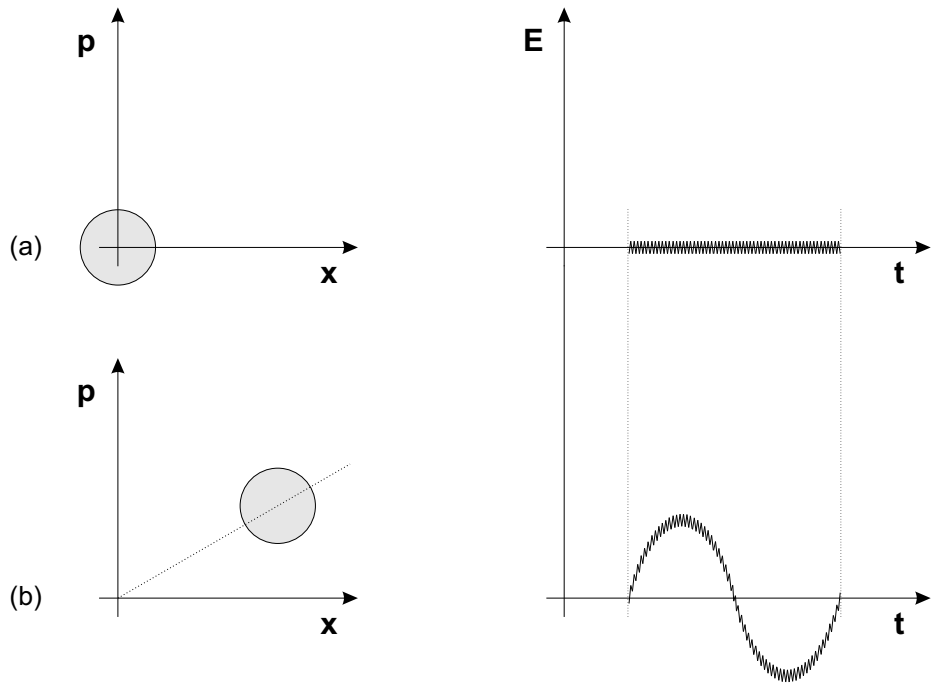
přičemž $\hat{\mathbf{E}}^{+}(\mathbf{r}, t)$ je tzv. pozitivně-frekvenční operátor elektrického pole

$$\hat{\mathbf{E}}^{+}(\mathbf{r}, t) = \frac{1}{L^{3/2}} \sum_{\mathbf{k}} l(\omega)\epsilon_{\mathbf{k}} \hat{a}_{\mathbf{k}} e^{i(\mathbf{kr}-\omega t)}. \tag{3.27}$$

Nahrazením $\hat{a}_{\mathbf{k}}$, $\hat{a}^{\dagger}_{\mathbf{k}}$ operátory $\hat{x}_{\mathbf{k}}$, $\hat{p}_{\mathbf{k}}$ máme

$$\hat{\mathbf{E}}(\mathbf{r}, t) = \frac{1}{L^{3/2}} \sum_{\mathbf{k}} l(\omega)[\hat{x}_{\mathbf{k}} \cos(\mathbf{kr} - \omega t) - \hat{p}_{\mathbf{k}} \sin(\mathbf{kr} - \omega t)] \tag{3.28}$$

Je tak vidět, že $\hat{\mathbf{E}}^{+}(\mathbf{r}, t)$, obsahující n módům, je vlastním stavem n–módového koherentního stavu $|\alpha_1, \ldots, \alpha_n\rangle$ s vlastní hodnotou $\frac{1}{L^{3/2}} \sum_{\mathbf{k}} l(\omega)\alpha_{\mathbf{k}}\epsilon_{\mathbf{k}} e^{i(\mathbf{kr}-\omega t)}$. Podobně $\hat{\mathbf{E}}^{-}(\mathbf{r}, t)$ je vlastním stavem $\langle\alpha_1, \ldots, \alpha_n|$.



Obrázek 4.: Ilustrace relace mezi rozložením elektrického pole ve fázovém prostoru a jeho fluktuacemi pro (a) vakuum a (b) koherentní stav.

3.2 Stlačené koherentní stavy

Zájem o stlačené stavy začal ve stejné době jako tomu bylo u koherentních stavů [6], [8]. Matematicky jsou definovány prostřednictvím stlačovacího operátoru $\hat{S}(\xi)$ [5], jež, podobně jako u koherentních stavů, číslo ξ je komplexní. Stlačený stav vznikne, když jej aplikujeme na koherentní stav. Ten je pak speciálním případem stlačeného stavu.

Když laserový svazek (který je v koherentním stavu) prochází nelineárním krystalem, dochází k procesům [5], jež koherentní stav transformují právě na stlačený stav. Pro tyto stavy je charakteristické, že jedna z neurčitostí (Δx nebo Δp) je redukována pod $1/\sqrt{2}$. To však neporušuje Heisenbergovy relace neurčitosti, neboť u konjugované veličiny se naopak neurčitost zvětší. Tato vlastnost má pochopitelně své využití, např. v oblasti optické komunikace, fotonové detekce, detekce gravitačních vln.

Stlačené stavy též mohou splňovat subpoissonovskou statistiku, tzn. že střední hodnota počtu fotonů je menší než neurčitost v jejich počtu, což je typický znak neklasičnosti.

Koherentní stav je možno si představit klasicky jako částici pohybující se v oblasti kvadratického potenciálu. Její hamiltonián byl (3.22). Nyní oblast výskytu částice zmenšíme přidáním dosatečného potenciál bx^2. Hamiltonián pak bude

$$H = \frac{p^2}{2m} + \frac{1}{2}kx^2 - eEx + bx^2 = \frac{p^2}{2m} + \frac{1}{2}(k+b)x^2 - eEx. \tag{3.29}$$

Přidáním potenciálu bx^2 tak kvantově znamená příspěvky operátorů $\hat{a}^2$ a $(\hat{a}^\dagger)^2$, které jsou důležité při přípravě stlačeného koherentního stavu. Definujme jej tak proto prostřednictvím *stlačovacího hamiltoniánu*

$$\hat{H}_S = \frac{i}{2}(\xi\hat{a}^\dagger\hat{a}^\dagger - \xi^*\hat{a}\hat{a}), \tag{3.30}$$

jež vede k definici *stlačovacího operátoru*

$$\hat{S}(\xi) = e^{i\hat{H}_S} = \exp\left[\frac{1}{2}(\xi^*\hat{a}\hat{a} - \xi\hat{a}^\dagger\hat{a}^\dagger)\right]. \tag{3.31}$$

Stlačený koherentní stav[2] $|\xi, \alpha\rangle$ tak dostaneme, když zapůsobíme tímto operátorem na koherentní stav:

$$|\xi, \alpha\rangle = \hat{S}(\xi)|\alpha\rangle = \hat{S}(\xi)\hat{D}(\alpha)|0\rangle. \tag{3.32}$$

Číslo $\xi = re^{i\theta}$ je obecně komplexní a jeho modul r vyjadřuje míru stlačení. Uveďme některé důležité vlastnosti stlačeného stavu.

Vlastnosti stlačovacího operátoru

Ze (3.31) je vidět, že, podobně jako posunovací operátor, je i tento unitární, tj.

$$\hat{S}^\dagger(\xi) = \hat{S}(-\xi) = [\hat{S}(\xi)]^{-1}. \tag{3.33}$$

S využitím (6.7) lze dostat

$$\hat{S}^\dagger(\xi)\hat{a}\hat{S}(\xi) = \hat{a}\cosh r - \hat{a}^\dagger e^{i\theta}\sinh r \tag{3.34}$$

$$\hat{S}^\dagger(\xi)\hat{a}^\dagger\hat{S}(\xi) = \hat{a}^\dagger\cosh r - \hat{a}e^{-i\theta}\sinh r, \tag{3.35}$$

[2] Budeme dále namísto pojmu stlačený koherentní stav používat kratšího termínu stlačený stav.

Odtud zřejmě pro libovolný operátor ve tvaru $f(\hat{a}, \hat{a}^\dagger) = \sum_{m,n} c_{mn}\, \hat{a}^m (\hat{a}^\dagger)^n$ dostaneme, že

$$\hat{S}^\dagger(\xi) f(\hat{a}, \hat{a}^\dagger) \hat{S}(\xi) = f(\hat{a}\cosh r - \hat{a}^\dagger e^{i\theta} \sinh r, \hat{a}^\dagger \cosh r - \hat{a} e^{-i\theta} \sinh r) \tag{3.36}$$

bez ohledu na pořadí operátorů v $f(\hat{a}, \hat{a}^\dagger)$.

Užitečný je též faktorizace stlačovacího operátoru [12]

$$\begin{aligned} \hat{S}(\xi) &= \exp\left[\frac{1}{2}(\xi^* \hat{a}\hat{a} - \xi \hat{a}^\dagger \hat{a}^\dagger)\right] = \\ &= \exp\left[\frac{1}{2}(e^{-i\theta} \tanh r)\hat{a}^\dagger \hat{a}^\dagger\right] \exp\left[-2\ln(\cosh r)\left(\frac{1}{2}\hat{a}^\dagger \hat{a} + \frac{1}{4}\right)\right] \exp\left[-\frac{1}{2}(e^{-i\theta} \tanh r)\hat{a}\hat{a}\right] \end{aligned} \tag{3.37}$$

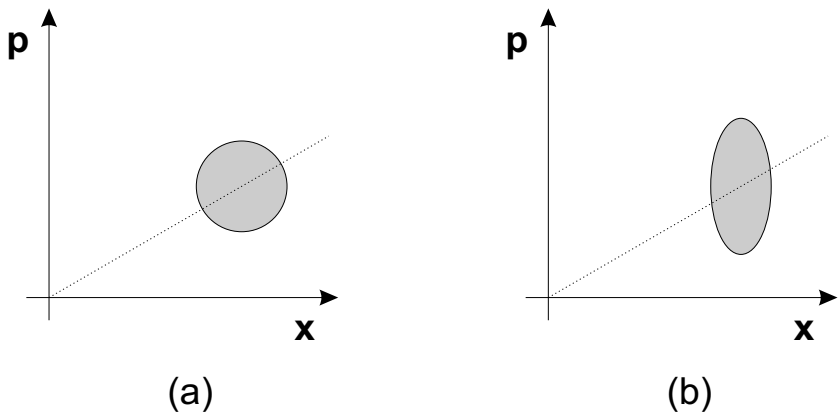
Obecně stlačovací a posunovací operátory nekomutují, tj. $\hat{S}(\xi)\hat{D}(\alpha) \neq \hat{D}(\alpha)\hat{S}(\xi)$, což znamená, že $|\xi, \alpha\rangle \neq |\alpha, \xi\rangle$.

Relace neurčitosti

Můžeme vypočítat s pomocí (3.34) a (3.35) relace neurčitosti stlačeného stavu. Dostaneme

$$\Delta x = \frac{1}{2} e^{-r}$$
$$\Delta p = \frac{1}{2} e^{r}$$

Tím pádem stlačený koherentní stav splňuje minimální relace neurčitosti $\Delta x \Delta p = \frac{1}{2}$, ovšem s tím, že neurčitost jedné z veličin je $< \frac{1}{2}$. Kolikrát je jedna neurčitost redukována, tolikrát je ta druhá zvětšena. Proto se každý stav s touto vlastností nazývá stlačený [2].



Obrázek 3.5: Oblast neurčitosti ve fázovém prostoru pro (a) koherentní stav a (b) stlačený stav s redukovanou neurčitostí v x.

Stlačovat však můžeme i ve fázi a amplitudě. Zaveďme nové operátory $\hat{x}'$, $\hat{p}'$:

$$\hat{x}' = \frac{1}{\sqrt{2}}(\hat{a}^\dagger e^{i\beta} + \hat{a} e^{-i\beta}) \tag{3.38}$$

$$\hat{p}' = \frac{i}{\sqrt{2}}(\hat{a}^\dagger e^{i\beta} - \hat{a} e^{-i\beta}) \tag{3.39}$$

pro nějaký úhel β. Tato transformace neporušuje komutační relace $[\hat{x}', \hat{p}'] = i\hat{1}$. $\hat{x}'$, $\hat{p}'$ jsou tak zobecněním operátorů $\hat{x}$, $\hat{p}$. Elektrické pole z (3.28) takto transformované do x', p' je

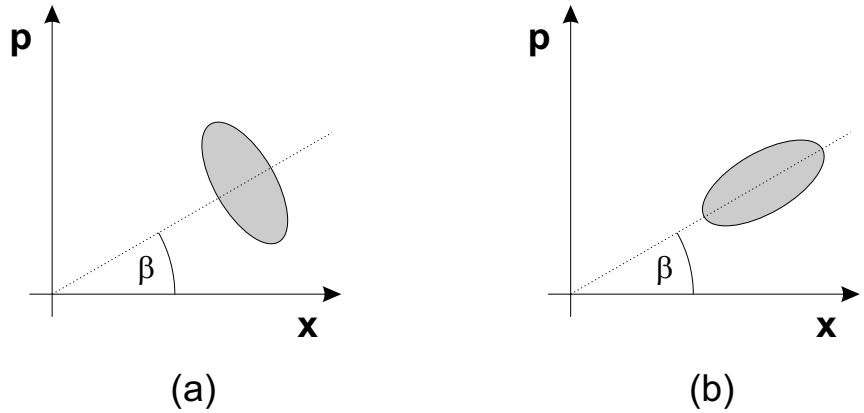
$$\hat{\mathbf{E}}(\mathbf{r}, t) = \frac{1}{L^{3/2}} \sum_{\mathbf{k}} l(\omega)[\hat{x}'_{\mathbf{k}} \cos(\mathbf{kr} - \omega t + \beta) - \hat{p}'_{\mathbf{k}} \sin(\mathbf{kr} - \omega t + \beta)]. \tag{3.40}$$

Pro relace neurčitosti lze dostat

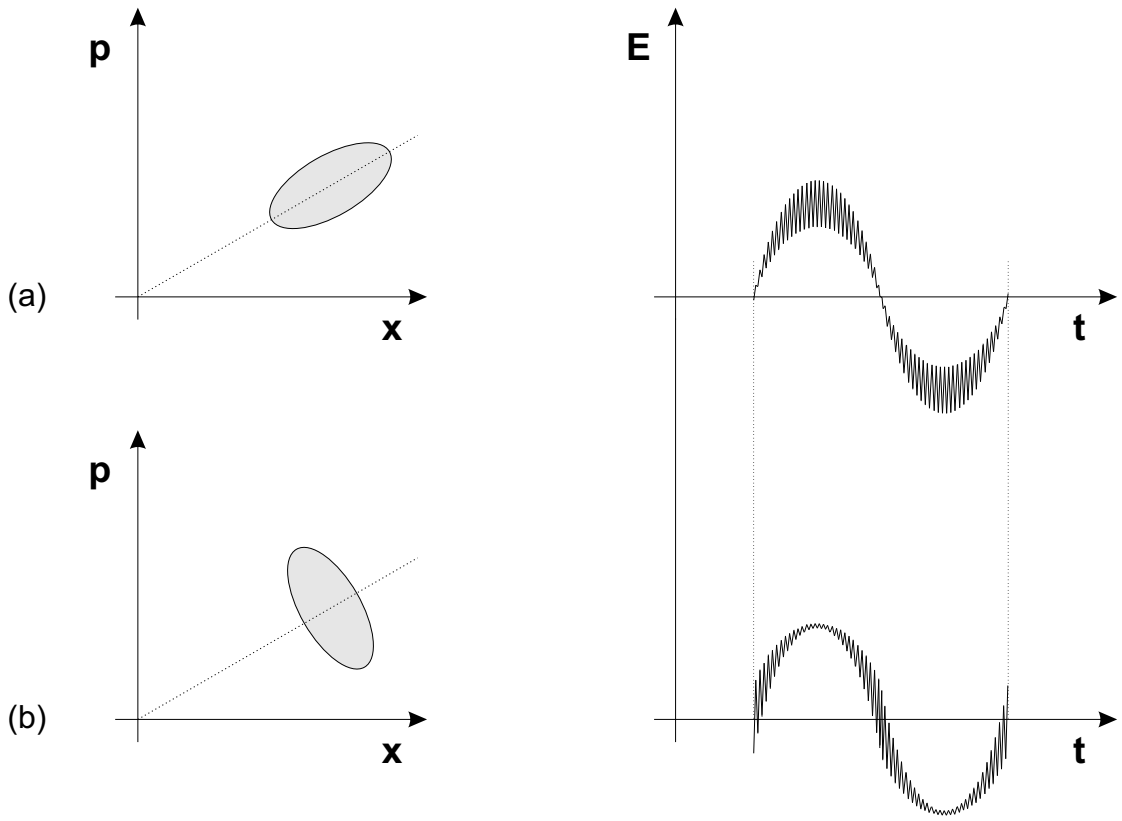
$$\Delta x' = \Delta x \cos\beta + \Delta p \sin\beta \tag{3.41}$$

$$\Delta p' = -\Delta x \sin\beta + \Delta p \cos\beta. \tag{3.42}$$

Transformace (3.38) a (3.39) tak má za následek natočení oblasti neurčitosti o úhel β.



Obrázek 3.6: Oblast neurčitosti ve fázovém prostoru pro (a) amplitudově a (b) fázově stlačený stav.



Obrázek 3.7: Ilustrace relace mezi rozložením elektrického pole ve fázovém prostoru a jeho fluktuacemi pro (a) fázově a (b) amplitudově stlačený koherentní stav.

Stlačený stav je zastoupen dvojicí komplexních čísel (ξ, α). α říká, kam se má posunout vakuum a ξ jak se má „stlačit“.

Soubor stlačených stavů je, podobně jako koherentní stavy, přeplněný. Jednotkový operátor je v něm

$$\hat{1} = \frac{1}{\pi} \int \mathrm{d}^2\alpha \, |\xi, \alpha\rangle\langle\xi, \alpha|. \tag{3.43}$$

Fotonové statistiky

Lze ukázat [2], že pravděpodobnost nalezení n fotonů ve $|\xi, \alpha\rangle$ je

$$p(n) = \frac{(\tanh r)^n}{2^n n! \cosh r} \exp\left\{-|\alpha|^2 + \frac{1}{2}\left[e^{-i\theta}\alpha^2 + e^{i\theta}(\alpha^*)^2\right]\tanh r\right\} \times \left|H_n\left(\frac{\alpha e^{-i\theta/2}}{\sqrt{2\cosh r \sinh r}}\right)\right|^2, \tag{3.44}$$

střední hodnota počtu fotonů

$$\langle\hat{n}\rangle = \langle\xi, \alpha|\hat{n}|\xi, \alpha\rangle = |\alpha|^2 + \sinh^2 r - \sinh r \cosh r \left[e^{i\theta}\alpha^2 + e^{-i\theta}(\alpha^*)^2\right] \tag{3.45}$$

a neurčitost v počtu fotonů

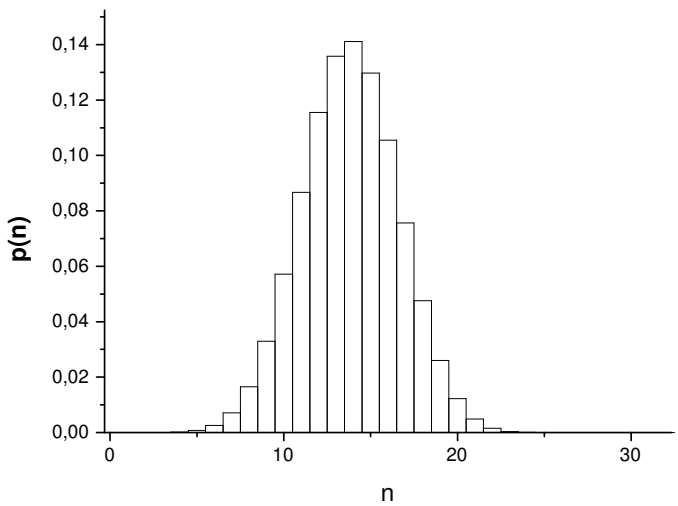
$$\Delta n = (|\alpha|^2[\cosh 4r - \cos(\theta - 2\phi)\sinh 4r] + 2\sinh^2 r \cosh^2 r)^{1/2} \tag{3.46}$$

($\alpha = |\alpha|e^{i\phi}$). Pokud je $r = 0$, dostáváme $|\alpha|^2 = \Delta n = \langle\hat{n}\rangle$, což je přesně výsledek, který platí pro koherentní stav.

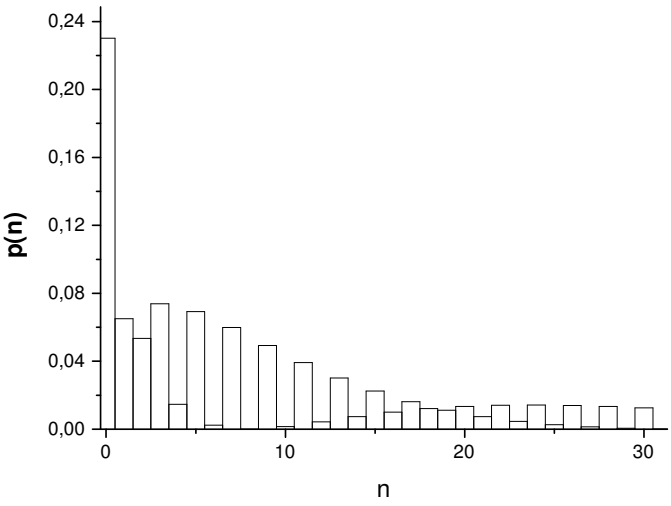
Speciálně, položíme–li $\alpha = 0$, dostaneme $|\xi, 0\rangle = \hat{S}(\xi)|0\rangle$, což je stlačené vakuum. Pokud použijeme (3.37), dostaneme

$$p(n) = \langle n|\hat{S}(\xi)|0\rangle = \begin{cases} \frac{(\tanh r)^n}{2^n}\sqrt{\frac{n!}{\cosh r}} & \text{pro } n \text{ sudé} \\ 0 & \text{pro } n \text{ liché} \end{cases} \tag{3.47}$$

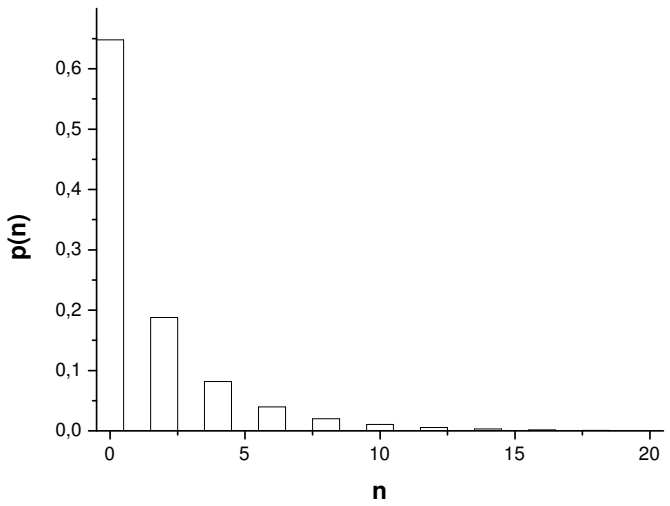
Takže ve stlačeném vakuu nalezneme vždy pouze sudý počet fotonů.



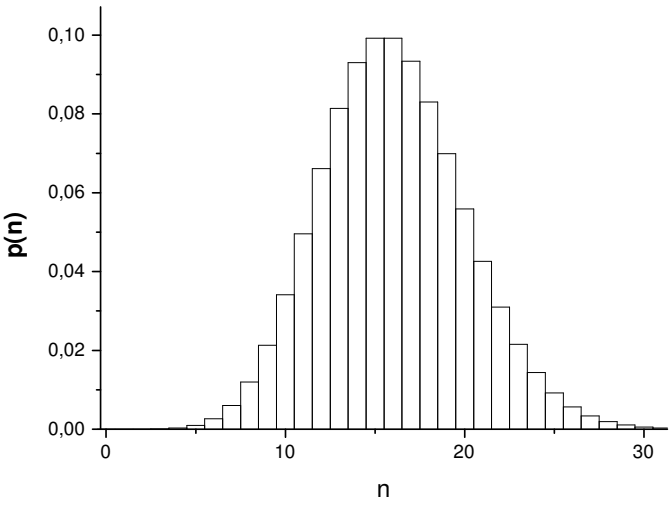
Obrázek 3.8: Rozdělení počtu fotonů pro stav s $r = 0,3$, $\alpha = 5$.



Obrázek 3.9: Rozdělení počtu fotonů pro stav s $r = 2$, $\alpha = 2$.



Obrázek 3.10: Rozdělení počtu fotonů pro stav s $r = 1$, $\alpha = 0$ - stlačené vakuum.



Obrázek 11.: Rozdělení počtu fotonů pro stav s $r = 0$, $\alpha = 4$ - koherentní stav.

3.3 Distribuční a kvazidistribuční funkce v kvantové fyzice

Operátor (matice) hustoty

Mějme systém, jež je možné charakterizovat fyzikální veličinou O, jíž přísluší operátor $\hat{O}$. Předpokládejme, že systém je ve stavu $|\psi\rangle$. Pak střední hodnota veličiny O v tomto stavu je dána vztahem

$$\langle O\rangle_\psi = \langle\psi|\hat{O}|\psi\rangle. \tag{3.48}$$

Ovšem to, že systém je ve stavu $|\psi\rangle$, nemusí být známo. Předpokládejme však, že je známa pravděpodobnost P_ψ nalezení systému v tomto stavu. Pak

$$\langle\langle O\rangle_\psi\rangle_{\text{soubor}} = \sum_\psi P_\psi\langle\psi|\hat{O}|\psi\rangle. \tag{3.49}$$

Nyní vložením jednotkového operátoru $\sum_n |n\rangle\langle n| = \hat{1}$ dostaneme

$$\langle\langle O\rangle_\psi\rangle_{\text{soubor}} = \sum_n\sum_\psi P_\psi\langle\psi|\hat{O}|n\rangle\langle n|\psi\rangle = \sum_n\sum_\psi P_\psi\langle n|\psi\rangle\langle\psi|\hat{O}|n\rangle$$

a zavedením *operátoru (matice) hustoty*

$$\hat{\rho} = \sum_\psi P_\psi|\psi\rangle\langle\psi| \tag{3.50}$$

dostaneme

$$\langle\langle O\rangle_\psi\rangle_{\text{soubor}} = \sum_n\langle n|\hat{\rho}\hat{O}|n\rangle. \tag{3.51}$$

Odtud

$$\langle O\rangle = \mathrm{Tr}(\hat{\rho}\hat{O}). \tag{3.52}$$

Vztah (3.52) má obecnou platnost.

Vlastnosti operátoru hustoty

Z (3.50) je zřejmé, že

$$\hat{\rho} = \hat{\rho}^\dagger \tag{3.53}$$

$$\mathrm{Tr}(\hat{\rho}) = 1, \tag{3.54}$$

tj. operátor hustoty je hermitovský a má jednotkovou stopu.

Další vyjádření operátoru hustoty

Pro čistý stav $|\psi\rangle$ je

$$\hat{\rho} = |\psi\rangle\langle\psi|. \tag{3.55}$$

Operátor hustoty je možno vyjádřit v bázi Fockových stavů jako

$$\hat{\rho} = \sum_{n,m} |n\rangle\langle n|\hat{\rho}|m\rangle\langle m| = \sum_{n,m} \rho_{nm}|n\rangle\langle m| \tag{3.56}$$

nebo v bázi koherentních stavů ve tvaru

$$\hat{\rho} = \int\int \frac{\mathrm{d}^2\alpha}{\pi}\frac{\mathrm{d}^2\beta}{\pi}|\alpha\rangle\langle\alpha|\hat{\rho}|\beta\rangle\langle\beta|. \tag{3.57}$$

V obou případech jsme $\hat{\rho}$ obložili příslušnými jednotkovými operátory.

Vztahy (3.55)-(3.57) vyjadřují spektrální reprezentaci matice hustoty v příslušném souboru bazí.

V klasické fyzice slouží rozdělovací funkce mimo jiné k určení středních hodnot fyzikálních veličin. Totéž bychom chtěli umět v kvantové fyzice pomocí vhodných rozdělovacích funkcí. Ty zde mají jednak atributy pravděpodobnostní distribuce, jednak, jak se ukáže dále na příkladech, mohou nabývat i záporných hodnot nebo být „singulárnější“ než δ-funkce - pak o příslušném rozdělení hovoříme jako o *kvazidistribuční funkci* (nebo zkráceně jako o *kvazidistribuci*). Chování těchto funkcí slouží jako indikátor toho, zda má daný kvantový stav svůj klasický protějšek (jsou nezáporné a „nejvýše“ δ-funkce) nebo jej nemají (v jiném případě) - to platí pro funkci P a pro Wignerovu funkci. Slouží též k výpočtu středních hodnot operátorů.

3.3.1 Glauber-Sudarshanova P-reprezentace

Zaveďme operátor v normálním uspořádání, tj. všechny kreační operátory jsou vlevo a všechny anihilační operátory jsou vpravo,

$$\hat{O}_N(\hat{a},\hat{a}^\dagger) = \sum_{n,m} c_{nm}(\hat{a}^\dagger)^n\hat{a}^m. \tag{3.58}$$

Podle vztahu (3.52) je střední hodnota tohoto operátoru

$$\langle\hat{O}_N(\hat{a},\hat{a}^\dagger)\rangle = \mathrm{Tr}\left[\hat{\rho}\hat{O}_N(\hat{a},\hat{a}^\dagger)\right] = \int \mathrm{d}^2\alpha\, P(\alpha,\alpha^*)O_N(\alpha,\alpha^*), \tag{3.59}$$

kde

$$P(\alpha,\alpha^*) = \mathrm{Tr}\left[\hat{\rho}\delta(\alpha^* - \hat{a}^\dagger)\delta(\alpha - \hat{a})\right] \tag{3.60}$$

je *Glauber-Sudarshanova P-reprezentace* nebo též *reprezentace koherentního stavu.*

Diagonální reprezentace koherentního stavu

Operátor hustoty je možno vyjádřit v bázi koherentních stavů jako

$$\hat{\rho} = \int P(\alpha, \alpha^*) |\alpha\rangle\langle\alpha| \, \mathrm{d}^2\alpha. \tag{3.61}$$

Vzhledem k vlastnostem operátoru hustoty je funkce $P(\alpha, \alpha^*)$ reálná a normovaná, tedy

$$\begin{aligned} P(\alpha, \alpha^*) &= [P(\alpha, \alpha^*)]^* \\ \int P(\alpha, \alpha^*) \, \mathrm{d}^2\alpha &= 1. \end{aligned}$$

Dále je otázkou, jak „vyextrahovat“ funkci $P(\alpha, \alpha^*)$ ze vztahu (3.61). K její rozřešení určíme

$$\begin{aligned} \langle -\beta|\hat{\rho}|\beta\rangle &= \int P(\alpha, \alpha^*) \langle -\beta|\alpha\rangle\langle\alpha|\beta\rangle \, \mathrm{d}^2\alpha \\ &= e^{-|\beta|^2} \int P(\alpha, \alpha^*) e^{-|\alpha|^2} e^{\beta\alpha^* - \alpha\beta^*} \, \mathrm{d}^2\alpha. \end{aligned} \tag{3.62}$$

Na prvním řádku jsme využili relace (3.12), z druhého je pak vidět, že funkce $P(\alpha, \alpha^*) \, e^{-|\alpha|^2}$ je dvourozměrnou Fourierovou transformací funkce $e^{|\beta|^2} \langle -\beta|\hat{\rho}|\beta\rangle$, tedy máme hledané vyjádření

$$P(\alpha, \alpha^*) = \frac{e^{|\alpha|^2}}{\pi^2} \int e^{|\beta|^2} \langle -\beta|\hat{\rho}|\beta\rangle e^{-\beta\alpha^* + \alpha\beta^*} \, \mathrm{d}^2\beta. \tag{3.63}$$

Příklady P-funkce

Koherentní stav

Pro koherentní stav $|\beta\rangle$ je $\hat{\rho} = |\beta\rangle\langle\beta|$ a s použitím (3.63) dosteneme

$$P(\alpha, \alpha^*)_{|\beta\rangle} = \delta^2(\alpha - \beta), \tag{3.64}$$

kde $\delta^2(\alpha - \beta)$ je dvourozměrná delta funkce.

Fockův stav

Pro Fockův stav $|n\rangle$ je $\hat{\rho} = |n\rangle\langle n|$ a s použitím (3.63) dosteneme

$$P(\alpha, \alpha^*)_{|n\rangle} = \frac{e^{|\alpha|^2}}{n!} \frac{\partial^{2n}}{\partial\alpha^n \partial(\alpha^*)^n} \delta^2(\alpha). \tag{3.65}$$

Speciálně pro vakuum $|0\rangle$ je

$$P(\alpha, \alpha^*)_{|0\rangle} = \delta^2(\alpha). \tag{3.66}$$

Termální pole

Jedná se o pole generované zdrojem, jež je v ternodynamické rovnováze při teplotě T[3]. Matice hustoty takového systému má tvar

$$\hat{\rho} = \frac{e^{-\hat{H}/k_B T}}{\mathrm{Tr}\left[e^{-\hat{H}/k_B T}\right]}, \tag{3.67}$$

[3] Takovým zdrojem může být třeba žárovka.

kde $\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)$. Opět lze analogicky dostat

$$P(\alpha, \alpha^*) = \frac{1}{\pi\langle n\rangle} e^{-\frac{|\alpha|^2}{\langle n\rangle}}. \tag{3.68}$$

Jak je vidět, tak pro koherentní stav, vakuum a stav termálního pole existuje analogie v klasické fyzice, kdežto Fockův stav $|n\rangle$ s $n \geq 1$ ji nemá.

3.3.2 Q-reprezentace

V analogii s (3.60) definujme funkci

$$Q(\alpha, \alpha^*) = \mathrm{Tr}\left[\hat{\rho}\delta(\alpha - \hat{a})\delta(\alpha^* - \hat{a}^\dagger)\right] \tag{3.69}$$

Vložíme jednotkový operátor ve tvaru (3.14) a dostaneme [2]

$$Q(\alpha, \alpha^*) = \frac{1}{\pi}\langle\alpha|\hat{\rho}|\alpha\rangle, \tag{3.70}$$

tj. funkce $Q(\alpha, \alpha^*)$ je úměrná diagonálnímu elementu operátoru hustoty v reprezentaci koherentního stavu.

Funkce $Q(\alpha, \alpha^*)$ je normovaná, tzn. že

$$\int Q(\alpha, \alpha^*)\,\mathrm{d}^2\alpha = 1, \tag{3.71}$$

a reálná.

Mějme operátor v antinormálním uspořádáním

$$\hat{O}_A(\hat{a}, \hat{a}^\dagger) = \sum_{n,m} d_{nm}\hat{a}^n(\hat{a}^\dagger)^m. \tag{3.72}$$

Ukážeme, že Q-funkce ze vztahu (3.70) slouží k výpočtu střední hodnoty operátoru $\hat{O}_A$ podobně, jako je tomu u P-funkce a operátoru $\hat{O}_N$. Vyjádřeme střední hodnotu tohoto operátoru podle vztahu (3.52). Dostaneme

$$\langle\hat{O}_A(\alpha, \alpha^*)\rangle = \int \mathrm{d}^2\alpha\, Q(\alpha, \alpha^*)O_A(\alpha, \alpha^*). \tag{3.73}$$

Vložením (3.50) do (3.70) dostaneme

$$Q(\alpha, \alpha^*) = \frac{1}{\pi}\sum_\psi P_\psi|\langle\psi|\alpha\rangle|^2. \tag{3.74}$$

Poněvadž $|\langle\psi|\alpha\rangle|^2 \leq 1$, tak

$$Q(\alpha, \alpha^*) \leq \frac{1}{\pi}. \tag{3.75}$$

Jelikož $\hat{O}_N$ lze transformovat na $\hat{O}_A$ pomocí komutační relace (2.24), tak lze očekávat, že bude existovat transformace mezi Q a P. Stačí vložit (3.61) do (3.70), upravit a dostaneme

$$Q(\alpha, \alpha^*) = \frac{1}{\pi}\int \mathrm{d}^2\alpha'\, P(\alpha', \alpha'^*)e^{-|\alpha-\alpha'|^2}. \tag{3.76}$$

Q-funkce je tedy konvolucí P-funkce a Gaussovy křivky.

Příklady Q-funkce

Koherentní stav

Pro koherentní stav $|\beta\rangle$ je s použitím (3.70)

$$Q(\alpha,\alpha^*)_{|\beta\rangle} = \frac{1}{\pi}\, e^{-|\alpha-\beta|^2}. \tag{3.77}$$

Fockův stav

Pro Fockův stav $|n\rangle$ je s použitím (3.70)

$$Q(\alpha,\alpha^*)_{|n\rangle} = \frac{1}{\pi}\, e^{-|\alpha|^2}\, \frac{|\alpha|^{2n}}{n!}. \tag{3.78}$$

Speciálně pro vakuum $|0\rangle$ je

$$Q(\alpha,\alpha^*)_{|0\rangle} = \frac{1}{\pi}\, e^{-|\alpha|^2}. \tag{3.79}$$

3.3.3 Wignerova distribuce

V roce 1932 zavedl Wigner distribuční funkci $W(x,p)$, později po něm nazvánu Wignerova, jako důsledek snahy charakterizovat kvantový stav $|\psi\rangle$ funkcí ve fázovém prostoru. Jestliže $\hat{\rho}$ je operátorem hustoty systému a $|x\rangle$ resp. $|p\rangle$ označuje stav polohy resp. hybnosti, tak potom je Wignerova distribuce tohoto stavu definována jako

$$W(x,p) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \langle x+\frac{1}{2}\hbar y|\hat{\rho}|x-\frac{1}{2}\hbar y\rangle e^{\mathrm{i}yp}\,\mathrm{d}y. \tag{3.80}$$

Pro čístý stav je $\hat{\rho} = |\psi\rangle\langle\psi|$, a tedy

$$W(x,p) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \psi^*\left(x+\frac{1}{2}\hbar y\right)\psi\left(x-\frac{1}{2}\hbar y\right) e^{\mathrm{i}yp}\,\mathrm{d}y. \tag{3.81}$$

Tak jako funkce P resp. funkce Q slouží mj. k výpočtu střední hodnoty operátoru v normálním resp. antinormálním uspořádání, tak i Wignerova funkce má analogický význam. Pomocí ní lze vypočítat střední hodnotu symetricky uspořádané funkce[4]

$$F_S(\hat{x},\hat{p}) = \sum_{n,m} s_{nm}\hat{x}^n\hat{p}^m, \tag{3.82}$$

tedy

$$\langle F_S(\hat{x},\hat{p})\rangle = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} F_S(x,p)W(x,p)\,\mathrm{d}x\,\mathrm{d}p. \tag{3.83}$$

Wignerova funkce může nabývat i záporných hodnot, je to tedy kvazidistribuce. Nezastupuje ani přímo měřitelnou veličinu. Nicméně vypočítejme marginální integrál

$$\begin{aligned}\int_{-\infty}^{\infty} W(x,p)\,\mathrm{d}p &= \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \psi^*\left(x-\frac{1}{2}\hbar y\right)\psi\left(x+\frac{1}{2}\hbar y\right) e^{\mathrm{i}yp}\,\mathrm{d}y\,\mathrm{d}p = \\ &= \int_{-\infty}^{\infty} \psi^*\left(x-\frac{1}{2}\hbar y\right)\psi\left(x+\frac{1}{2}\hbar y\right)\delta(y)\,\mathrm{d}y = \\ &= \psi^*(x)\psi(x),\end{aligned} \tag{3.84}$$

[4] tj. funkce se symetricky uspořádanými operátory $\hat{x}$ a $\hat{p}$ s ohledem na jejich pořadí, např. $\hat{x}\hat{p}+\hat{p}\hat{x}$, $\hat{x}^2\hat{p}+\hat{x}\hat{p}\hat{x}+\hat{p}\hat{x}^2$

čili integrací Wignerovy funkce přes všechny hybnosti dostaneme pravděpodobnostní funkci pro polohu. Podobně lze ukázat, že

$$\int_{-\infty}^{\infty} W(x,p)\,\mathrm{d}x = \psi^*(p)\psi(p), \tag{3.85}$$

což je pravděpodobnostní funkce pro hybnosti.

Kapitola 4

Symplektická transformace a optické prvky

Kvantový stav $|\psi\rangle$ se pod vlivem interakce s ostatními systémy vyvíjí. Informace o interakci je obsažena v hamiltoniánu $\hat{H}$. V kapitole 2 jsme ze Schrödingerovy rovnice

$$i\frac{\partial|\psi\rangle}{\partial t} = \hat{H}|\psi\rangle \qquad (\hbar = 1),$$

která popisuje časový vývoj stavu, dostali ekvivalentní vyjádření

$$|\psi(t)\rangle = \hat{U}(t)|\psi(0)\rangle. \tag{4.1}$$

Vývoj je tak popsán prostřednictvím unitárního operátoru časového vývoje $\hat{U}(t) = e^{-i\hat{H}t}$, který je určen hamiltoniánem systému $\hat{H}$. Tím pádem $\hat{H}$ nám říká, jakým způsobem a do jakého stavu systém dospěje za určitý času. To je již zmíněná Schrödingerova reprezentace, v níž se vyvíjí stavy a operátory ne.

Optický prvek je zařízení, které mění vlastnosti světelného svazku, který jím prochází.

Každému takovému prvku bychom pak mohli prostřednictvím hamiltoniánu přiřadit unitární operátor $\hat{U}$, pomocí něhož bychom byli schopni podle výše uvedené rovnice určit výsledek transformace stavu při jeho průchodu tímto prvkem.

Další možný přístup, který se ukazuje jako výhodnější, je pracovat v Heisenbergově reprezantaci, v níž se naopak vyvíjí operátory a stavy zůstávají neměnné. Transformace operátoru $\hat{A}$ při průchodu optickým prvkem je potom dána rovnicí

$$\hat{A}(t) = \hat{U}^\dagger(t)\hat{A}(0)\hat{U}(t)$$

nebo ekvivalentně

$$\frac{\mathrm{d}}{\mathrm{d}t}\hat{A}(t) = \frac{1}{i}[\hat{A}, \hat{H}], \tag{4.2}$$

pokud $\hat{A}$ explicitně nezávisí na čase, tj. $\frac{\partial}{\partial t}\hat{A} = 0$.

Optické prvky mají obvykle jeden nebo dva vstupy a jeden nebo dva výstupy a můžeme je rozdělit na dvě kategorie:

- pasivní - zachovávají počet fotonů (dělič svazku, posouvač fáze)
- aktivní - nezachovávají počet fotonů (stlačovač).

Cílem této kapitoly je ukázat, jak se obecně n–módový stav transformuje při průchodu jednotlivými prvky a na souboru optických prvků (tj. optickou soustavou) a jaké vztahy platí pro tuto transformaci.

4.1 Symplektická transformace

Elektromagnetické pole je kvantověmechanicky popsáno mj. souborem bosonových kreačních a anihilačních operátorů $\{\hat{a}_i\}$ a $\{\hat{a}_i^\dagger\}$, které splňují komutační relace

$$[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij} \tag{4.3}$$

$$[\hat{a}_i, \hat{a}_j] = 0 \tag{4.4}$$

$$[\hat{a}_i^\dagger, \hat{a}_j^\dagger] = 0, \tag{4.5}$$

nebo ekvivalentně souborem operátorů polohy $\{\hat{x}_i\}$ a hybnosti $\{\hat{p}_i\}$ splňující komutační relace

$$[\hat{x}_i, \hat{p}_j] = i\hat{1} \tag{4.6}$$

$$[\hat{x}_i, \hat{x}_j] = 0 \tag{4.7}$$

$$[\hat{p}_i, \hat{p}_j] = 0. \tag{4.8}$$

Index u operátoru značí příslušný mód elektromagnetického pole a platí transformace

$$\hat{a}_i = \frac{1}{\sqrt{2}}(\hat{x}_i + i\hat{p}_i) \tag{4.9}$$

$$\hat{a}_i^\dagger = \frac{1}{\sqrt{2}}(\hat{x}_i - i\hat{p}_i). \tag{4.10}$$

Uvažujme, že máme takových módů n a optickou soustavu umožňující transformovat soubor operátorů $\{\hat{a}_i\}$,$\{\hat{a}_i^\dagger\}$ na jiný soubor $\{\hat{b}_i\}$, $\{\hat{b}_i^\dagger\}$ lineárně, tj.

$$\hat{b}_i = \sum_{j=1}^{n}(A_{ij}\hat{a}_j + B_{ij}\hat{a}_j^\dagger) \tag{4.11}$$

$$\hat{b}_k^\dagger = \sum_{l=1}^{n}(B_{kl}^*\hat{a}_l + A_{kl}^*\hat{a}_l^\dagger) \tag{4.12}$$

nebo když dané soubory reprezentujeme sloupcovými vektory $(\hat{a}_1, \ldots, \hat{a}_n, \hat{a}_1^\dagger, \ldots, \hat{a}_n^\dagger)^{\mathbf{T}}$ a $(\hat{b}_1, \ldots, \hat{b}_n, \hat{b}_1^\dagger, \ldots, \hat{b}_n^\dagger)^{\mathbf{T}}$, tak maticově je transformaci možno zapsat jako

$$\begin{pmatrix} \hat{b}_1 \\ \vdots \\ \hat{b}_n \\ \hat{b}_1^\dagger \\ \vdots \\ \hat{b}_n^\dagger \end{pmatrix} = (\mathbf{G}) \begin{pmatrix} \hat{a}_1 \\ \vdots \\ \hat{a}_n \\ \hat{a}_1^\dagger \\ \vdots \\ \hat{a}_n^\dagger \end{pmatrix},$$

přičemž $\mathbf{G} \in \mathbb{C}^{2n\times 2n}$ je čtvercová matice řádu $2n$ tvaru

$$\mathbf{G} = \left(\begin{array}{c|c} \mathbf{A} & \mathbf{B} \\ \hline \mathbf{B}^* & \mathbf{A}^* \end{array}\right),$$

tj. matice $\mathbf{A} = (A_{ij})$ vyjadřuje, jak se transformují anihilační operátory na anihilační operátory, matice $\mathbf{B} = (B_{ij})$ vyjadřuje transformaci kreačních operátorů na anihilační operátory apod. $(\mathbf{A}, \mathbf{B} \in \mathbb{C}^{n\times n})$. Matice $\mathbf{G}$ tak reprezenzuje příslušnou optickou soustavu. Jelikož soubor $\{\hat{b}_i\}$,

$\{\hat{b}_i^\dagger\}$ jsou opět bosonové anihilační a kreační operátory, musí splňovat komutační relace jako (4.3)-(4.5), tedy

$$[\hat{b}_i, \hat{b}_j^\dagger] = \delta_{ij} \tag{4.13}$$

$$[\hat{b}_i, \hat{b}_j] = 0 \tag{4.14}$$

$$[\hat{b}_i^\dagger, \hat{b}_j^\dagger] = 0. \tag{4.15}$$

To jistě klade podmínky na tvar matic $\mathbf{A}$ a $\mathbf{B}$. Tyto podmínky dostaneme, když dosadíme (4.11) a (4.12) postupně do (4.13)-(4.15). Tím dostaneme

$$\sum_j [A_{ij} A_{jk}^\dagger - B_{ij} B_{jk}^\dagger] = \delta_{ik}$$

nebo maticově

$$\mathbf{A}\mathbf{A}^\dagger - \mathbf{B}\mathbf{B}^\dagger = \mathbf{E}. \tag{4.16}$$

Další rovnice dá

$$\sum_j [A_{ij} B_{jk}^{\mathbf{T}} - B_{ij} A_{jk}^{\mathbf{T}}] = 0$$

nebo v maticovém zápisu

$$\mathbf{A}\mathbf{B}^{\mathbf{T}} = \mathbf{B}\mathbf{A}^{\mathbf{T}} = (\mathbf{A}\mathbf{B}^{\mathbf{T}})^{\mathbf{T}}. \tag{4.17}$$

Ekvivalentně lze lineárně transformovat operátory $\{\hat{x}_i\}$, $\{\hat{p}_i\}$ na $\{\hat{x}_i'\}$, $\{\hat{p}_i'\}$ vztahy

$$\hat{x}_i' = \sum_{j=1}^{n} (R_{ij}\hat{x}_j + S_{ij}\hat{p}_j) \tag{4.18}$$

$$\hat{p}_k' = \sum_{l=1}^{n} (T_{kl}\hat{x}_l + W_{kl}\hat{p}_l) \tag{4.19}$$

($\hat{x}_i'$ a $\hat{p}_i'$ souvisí s $\hat{b}_i$ a $\hat{b}_i^\dagger$ stejně jako $\hat{x}_i$ a $\hat{p}_i$ s $\hat{a}_i$ a $\hat{a}_i^\dagger$) nebo maticově

$$\begin{pmatrix} \hat{x}_1' \\ \vdots \\ \hat{x}_n' \\ \hat{p}_1' \\ \vdots \\ \hat{p}_n' \end{pmatrix} = (\mathbf{S}_p) \begin{pmatrix} \hat{x}_1 \\ \vdots \\ \hat{x}_n \\ \hat{p}_1 \\ \vdots \\ \hat{p}_n \end{pmatrix},$$

přičemž matice $\mathbf{S}_p$ je opět čtvercová matice řádu $2n$ tvaru

$$\mathbf{S}_p = \left(\begin{array}{c|c} \mathbf{R} & \mathbf{S} \\ \hline \mathbf{T} & \mathbf{W} \end{array}\right),$$

a nazývá se *symplektrická*, $\mathbf{R}, \mathbf{S}, \mathbf{T}, \mathbf{W} \in \mathbb{R}^{n\times n}$. Množina matic tohoto typu tvoří grupu $Sp(2n, \mathbb{R})$, která je podgrupou grupy $GL(2n, \mathbb{R})$. Lze ukázat, že symplektická matice musí splňovat vlastnost

$$\mathbf{S}_p^{\mathbf{T}} \Omega \mathbf{S}_p = \Omega, \tag{4.20}$$

kde

$$\Omega = \left(\begin{array}{c|c} \mathbf{0} & \mathbf{E} \\ \hline -\mathbf{E} & \mathbf{0} \end{array}\right).$$

Vzhledem k závislostem mezi kreačními a anihilačními operátory a operátory polohy a hybnosti vyjádřené rovnicemi (4.3)-(4.5) lze očekávat i souvislost mezi maticemi $\mathbf{A}$, $\mathbf{B}$ a $\mathbf{R}$, $\mathbf{S}$, $\mathbf{T}$, $\mathbf{W}$. Opět není těžké s použitím výše uvedených rovnic dostat

$$\mathbf{A} + \mathbf{B} = \mathbf{R} + i\mathbf{T} \tag{4.21}$$

$$\mathbf{A} - \mathbf{B} = \mathbf{W} - i\mathbf{S}. \tag{4.22}$$

Máme tak vše připraveno k popisu jednotlivých optických prvků.

4.2 Pasivní optické prvky

Pro tyto prvky je charakteristické, že zachovávají celkový počet fotonů, které jimi procházejí. Tzn. že $\sum_i \hat{a}_i^\dagger \hat{a}_i = \sum_i \hat{b}_i^\dagger \hat{b}_i = konst.\hat{1}$. Odtud s použitím (4.11) a (4.12) lze dostat, že

$$\mathbf{A}\mathbf{A}^\dagger = \mathbf{0}$$
$$\mathbf{B} = \mathbf{0}$$

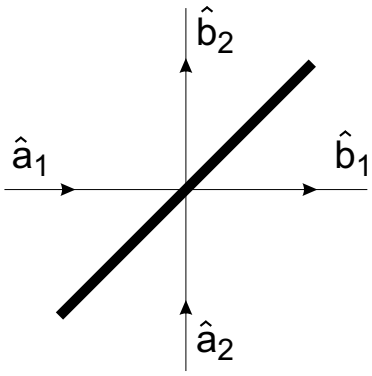
Matice $\mathbf{A}$ je tím pádem unitární. Dále díky tomu, že $\mathbf{B} = \mathbf{0}$, je $\mathbf{W} - i\mathbf{S} = \mathbf{A} = \mathbf{R} + i\mathbf{T}$, a tedy $\mathbf{R} = \mathbf{W}$, $\mathbf{T} = -\mathbf{S}$. Celkem matice $\mathbf{G}$ a $\mathbf{S}_p$ mají tvar

$$\mathbf{G} = \left(\begin{array}{c|c} \mathbf{A} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{A}^* \end{array}\right) \qquad \mathbf{S}_p = \left(\begin{array}{c|c} \mathbf{R} & \mathbf{S} \\ \hline -\mathbf{S} & \mathbf{R} \end{array}\right).$$

Při pasivní transformaci se tak mění pouze anihilační operátory na anihilační operátory a kreační operátory na kreační operátory. Mezi pasivní optické prvky patří dělič svazku a posouvač fáze.

Dělič svazku (beam splitter)

Je to pasivní optický prvek se dvěma vstupy a dvěma výstupy. Označme vstupní módy $\hat{a}_1$, $\hat{a}_2$ a výstupní módy $\hat{b}_1$, $\hat{b}_2$.



Obrázek 4.1: Schematická značka děliče svazku s módy.

Interakce mezi dvěma svazky $\hat{a}_1$ a $\hat{a}_2$ je popsána pomocí hamiltoniánu

$$\hat{H}_{BS} = i(\hat{a}_1\hat{a}_2^\dagger - \hat{a}_1^\dagger\hat{a}_2). \tag{4.23}$$

Z něj nyní dostaneme tvar transformovaných módů s použitím Heisenbergovy rovnice (4.2)

$$\begin{aligned}\dot{\hat{a}}_1 &= -i[\hat{a}_1, \hat{H}_{BS}] = -\hat{a}_2\\ \dot{\hat{a}}_2 &= -i[\hat{a}_2, \hat{H}_{BS}] = \hat{a}_1\end{aligned}$$

s řešením

$$\begin{aligned}\hat{a}_1(t) &= \cos(t)\hat{a}_1(0) - \sin(t)\hat{a}_2(0)\\ \hat{a}_2(t) &= \sin(t)\hat{a}_1(0) + \cos(t)\hat{a}_2(0).\end{aligned}$$

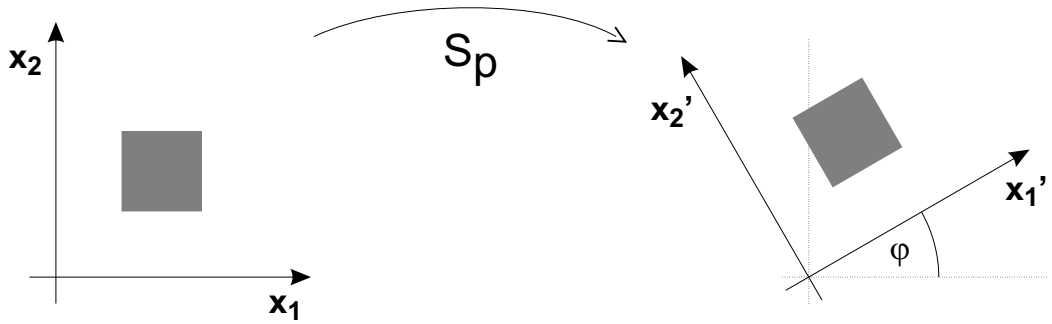
$\hat{a}_1(0)$ a $\hat{a}_2(0)$ jsou módy před transformací na děliči svazku, $\hat{a}_1(t)$ a $\hat{a}_2(t)$ jsou již transformované módy, tak $\hat{a}_1(t) = \hat{b}_1$ a $\hat{a}_2(t) = \hat{b}_2$ a

$$\begin{pmatrix} \hat{b}_1 \\ \hat{b}_2 \end{pmatrix} = \underbrace{\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}}_{\mathbf{A}} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix}. \tag{4.24}$$

$\varphi = t$ je formální přeznačení, parametr φ charakterizuje příslušný dělič svazku. Je vidět, že $\mathbf{A}$ je skutečně unitární. Pro zjištění transformace souřadnic a hybností stačí tuto matici $\mathbf{A}$ rozdělit na reálnou a imaginární část, čímž dostaneme, že $\mathbf{R} = \mathbf{A}$ a $\mathbf{S} = \mathbf{0}$. Proto

$$\begin{pmatrix} \hat{x}_1' \\ \hat{x}_2' \end{pmatrix} = \underbrace{\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}}_{\mathbf{A}} \begin{pmatrix} \hat{x}_1 \\ \hat{x}_2 \end{pmatrix} \quad , \quad \begin{pmatrix} \hat{p}_1' \\ \hat{p}_2' \end{pmatrix} = \underbrace{\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}}_{\mathbf{A}} \begin{pmatrix} \hat{p}_1 \\ \hat{p}_2 \end{pmatrix}.$$

Dělič svazku tak transformuje fázový prostor dvou módů otáčením jeho podprostorů (x_1, x_2) a (p_1, p_2) o stejný úhel φ.



Obrázek 4.2: Transformace módu ve fázovém prostoru při průchodu děličem svazku.

V praxi se často používá dělič svazku, pro který $\varphi = \pi/4$. Pak

$$\mathbf{A} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Posouvač fáze (phase shifter)

Jedná se o jednomódový pasivní optický prvek s jedním vstupem a jedním výstupem.

Obrázek 4.3: Schematická značka posouvače fáze s módy.

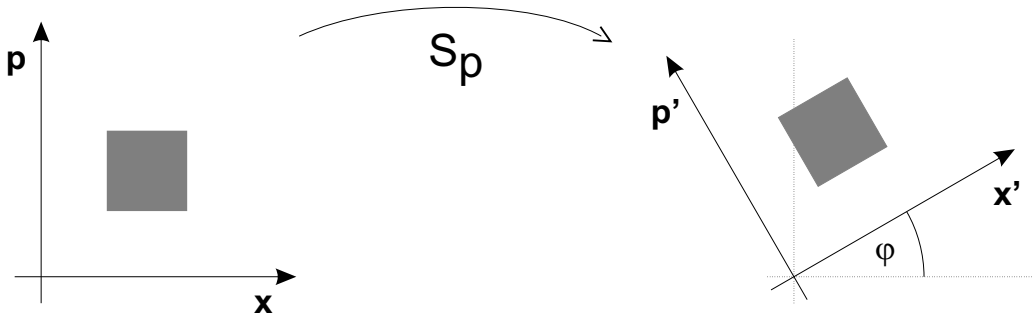
Pokud označíme $\hat{a}$ vstupní a $\hat{b}$ výstupní mód, tak

$$\hat{b} = e^{i\varphi}\hat{a}. \tag{4.25}$$

Podobně jako v předchozím případě lze odtud dostat vztah pro transformaci mezi souřadnicemi a hybnostmi

$$\begin{pmatrix} \hat{x}' \\ \hat{p}' \end{pmatrix} = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} \hat{x} \\ \hat{p} \end{pmatrix} \tag{4.26}$$

Posouvač fáze tak otáčí celý fázový prostor příslušný módu, jež transformuje, o úhel φ.



Obrázek 4.4: Transformace módu ve fázovém prostoru při průchodu posouvačem fáze.

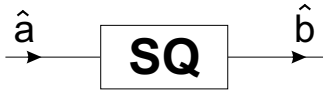
Soubor pasivních optických prvků, jež tvoří děliče svazku a posouvače fáze, zastupuje matice $\mathbf{G}$, která je unitární. V případě symplektické matice, pokud $\mathbf{S} = \mathbf{0}$, tak $\mathbf{R}$ je ortogonální.

4.3 Aktivní optické prvky

Tyto prvky nezachovávají celkový počet fotonů ve stavech, jež transformuje, tj. $\sum_i \hat{a}_i^\dagger \hat{a}_i \neq \sum_i \hat{b}_i^\dagger \hat{b}_i$. Lze jej poznat tak, že aspoň jeden transformovaný anihilační operátor $\hat{b}_i$ vyjádřený pomocí netransformovaných operátorů obsahuje alespoň jeden netransformovaný kreační operátor nějakého módu. Zástupcem skupiny aktivních prvků je stlačovací prvek. Prakticky jsou realizovány nelineárními krystaly. V laserovém svazku, který prochází takovým krystalem, dochází procesem optické harmonické generace k přeměně dvou fotonů téže frekvence na jeden foton frekvence dvojnásobné nebo procesem parametrické konverze dolů k přeměně jednoho fotonu dané frekvence na dva fotony, každý s poloviční frekvencí.

Jednomódový stlačovač (one–mode squeezer)

Tento prvek má jeden vstup a jeden výstup.



Obrázek 4.5: Schematická značka jednomódového stlačovače s módy.

Jeho působení lze popsat pomocí hamiltoniánu

$$\hat{H}_{SO} = \frac{i}{2}(\hat{a}^\dagger\hat{a}^\dagger - \hat{a}\hat{a}). \tag{4.27}$$

Pomocí Heisenbergovy rovnice dostaneme

$$\dot{\hat{a}} = -i[\hat{a}, \hat{H}_{SO}] = \hat{a}^\dagger$$

s řešením

$$\hat{a}(t) = \cosh(t)\hat{a}(0) + \sinh(t)\hat{a}^\dagger(0).$$

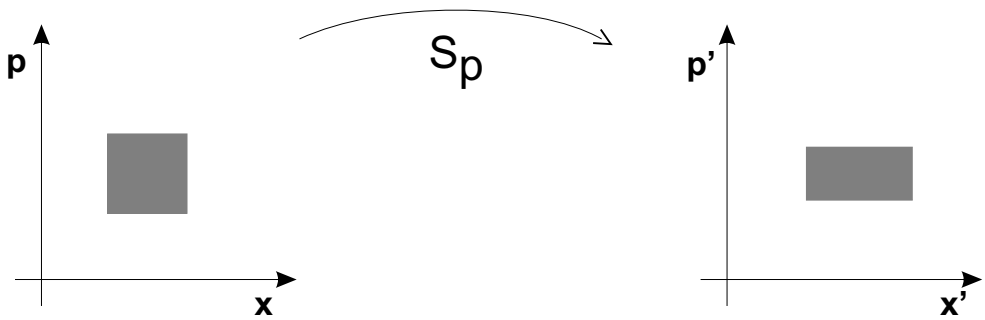
Podobně jako u děliče svazku $\hat{a}(t) \equiv \hat{b}$, $\hat{a}(0) \equiv \hat{a}$ a $t \equiv \xi$. Maticově tak transformaci vyjádříme jako

$$\begin{pmatrix} \hat{b} \\ \hat{b}^\dagger \end{pmatrix} = \underbrace{\begin{pmatrix} \cosh\xi & \sinh\xi \\ \sinh\xi & \cosh\xi \end{pmatrix}}_{\mathbf{G}} \begin{pmatrix} \hat{a} \\ \hat{a}^\dagger \end{pmatrix}. \tag{4.28}$$

ξ je reálný parametr zvaný *parametr stlačení*. Uvidíme proč. Z transformací (4.21) a (4.22) dostáváme $\mathbf{R} = e^\xi$, $\mathbf{S} = \mathbf{T} = 0$, $\mathbf{W} = e^{-\xi}$, čili

$$\begin{pmatrix} \hat{x}' \\ \hat{p}' \end{pmatrix} = \underbrace{\begin{pmatrix} e^\xi & 0 \\ 0 & e^{-\xi} \end{pmatrix}}_{\mathbf{S}_p} \begin{pmatrix} \hat{x} \\ \hat{p} \end{pmatrix}. \tag{4.29}$$

Jednomódový stlačovací prvek tak reprezentuje diagonální symplektická matice taková, že součin jejích pvků je 1. Čím je ξ větší, tím více se nová souřadnice „natáhne“ a nová hybnost „zúží“.



Obrázek 4.6: Transformace módu ve fázovém prostoru při průchodu jednomódovým stlačovačem.

Dvoumódový stlačovač (two–mode squeezer)

Tento prvek má dva vstupy a dva výstupy a je popsán hamiltoniánem

$$\hat{H}_{ST} = \frac{i}{2}(\hat{a}_1^\dagger \hat{a}_2^\dagger - \hat{a}_1 \hat{a}_2). \tag{4.30}$$

Postup bude analogický jako v předchozím případě. Pomocí Heisenbergovy rovnice dostaneme

$$\begin{aligned} \dot{\hat{a}}_1 &= -i[\hat{a}_1, \hat{H}_{ST}] = \hat{a}_2^\dagger \\ \dot{\hat{a}}_2 &= -i[\hat{a}_2, \hat{H}_{ST}] = \hat{a}_1^\dagger \end{aligned}$$

s řešením

$$\begin{aligned} \hat{a}_1(t) &= \cosh(t)\hat{a}_1(0) + \sinh(t)\hat{a}_2^\dagger(0) \\ \hat{a}_2(t) &= \cosh(t)\hat{a}_2(0) + \sinh(t)\hat{a}_1^\dagger(0) \end{aligned}$$

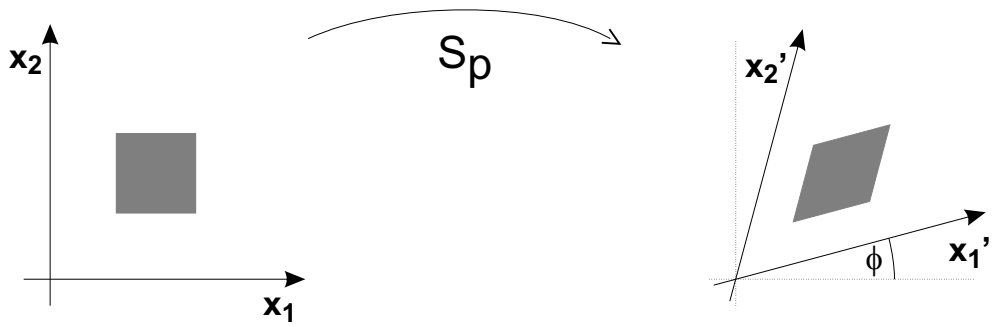
a po přeznačení $\hat{a}_i(t) \equiv \hat{b}_i$, $\hat{a}_i(0) \equiv \hat{a}_i$, $t \equiv \xi$ máme

$$\begin{pmatrix} \hat{b}_1 \\ \hat{b}_2 \\ \hat{b}_1^\dagger \\ \hat{b}_2^\dagger \end{pmatrix} = \underbrace{\left(\begin{array}{cc|cc} \cosh\xi & 0 & 0 & \sinh\xi \\ 0 & \cosh\xi & \sinh\xi & 0 \\ \hline 0 & \sinh\xi & \cosh\xi & 0 \\ \sinh\xi & 0 & 0 & \cosh\xi \end{array}\right)}_{\mathbf{G}} \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \\ \hat{a}_1^\dagger \\ \hat{a}_2^\dagger \end{pmatrix} \tag{4.31}$$

a s použitím (4.21) a (4.22)

$$\begin{pmatrix} \hat{x}_1' \\ \hat{x}_2' \\ \hat{p}_1' \\ \hat{p}_2' \end{pmatrix} = \underbrace{\left(\begin{array}{cc|cc} \cosh\xi & \sinh\xi & 0 & 0 \\ \sinh\xi & \cosh\xi & 0 & 0 \\ \hline 0 & 0 & \cosh\xi & -\sinh\xi \\ 0 & 0 & -\sinh\xi & \cosh\xi \end{array}\right)}_{\mathbf{S}_p} \begin{pmatrix} \hat{x}_1 \\ \hat{x}_2 \\ \hat{p}_1 \\ \hat{p}_2 \end{pmatrix} \tag{4.32}$$

Dvoumódový stlačovač transformuje podprostor souřadnic a podprostor hybností, vzájemně je nepromíchává a tuto transformaci reprezentuje jeden reálný stlačovací parametr ξ.



Obrázek 4.7: Transformace módu v podprostoru fázového prostoru (x_1, x_2) při průchodu dvoumódovým stlačovačem; $\Phi = \arctan(-\tanh\xi)$.

4.4 Braunsteinův rozklad

Podle Braunsteina [13] existuje rozklad matic $\mathbf{A}$ a $\mathbf{B}$ na

$$\mathbf{A} = \mathbf{U}\mathbf{A_D}\mathbf{V}^*, \qquad \mathbf{B} = \mathbf{U}\mathbf{B_D}\mathbf{V}, \tag{4.33}$$

přičemž $\mathbf{U}$ a $\mathbf{V}$ jsou matice unitární, tj. $\mathbf{U}\mathbf{U}^\dagger = \mathbf{E}$ a $\mathbf{V}\mathbf{V}^\dagger = \mathbf{E}$. Celkem tak můžeme psát

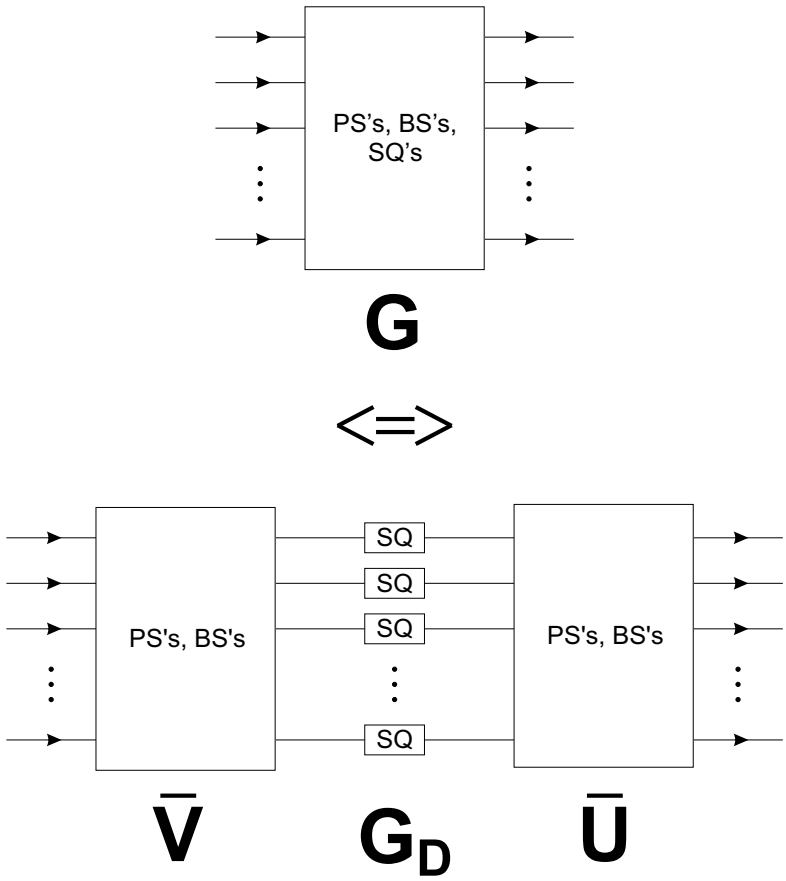
$$\mathbf{G} = \left(\begin{array}{c|c} \mathbf{A} & \mathbf{B} \\ \hline \mathbf{B}^* & \mathbf{A}^* \end{array}\right) = \underbrace{\left(\begin{array}{c|c} \mathbf{U} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{U}^* \end{array}\right)}_{\equiv\bar{\mathbf{U}}} \underbrace{\left(\begin{array}{c|c} \mathbf{A_D} & \mathbf{B_D} \\ \hline \mathbf{B_D^*} & \mathbf{A_D^*} \end{array}\right)}_{\equiv\mathbf{G_D}} \underbrace{\left(\begin{array}{c|c} \mathbf{V}^* & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{V} \end{array}\right)}_{\equiv\bar{\mathbf{V}}}$$

Matice $\bar{\mathbf{U}}$ a $\bar{\mathbf{V}}$ jsou zřejmě unitární a každá zastupuje soubor pasivních optických prvků. Dále dosazením (4.33) do (4.16) dostáváme

$$\mathbf{A_D^2} - \mathbf{B_D^2} = \mathbf{E}. \tag{4.34}$$

To znamená, že i–tý prvek diagonálních matic $\mathbf{A_D}$ resp. $\mathbf{B_D}$ má tvar $\cosh\xi_i$ resp. $\sinh\xi_i$. Porovnáním s (4.28) je vidět, že matice $\mathbf{G_D}$ reprezentuje soubor jednomódových stlačovacích prvků. Tedy i symplektická matice tohoto souboru bude diagonální $\mathbf{S}_p = \mathrm{diag}(\mathrm{e}^{\xi_1}, \ldots, \mathrm{e}^{\xi_n}, \mathrm{e}^{-\xi_1}, \ldots, \mathrm{e}^{-\xi_n})$.

Braunsteinův rozklad tak umožňuje pro libovolnou optickou soustavu vytvořit náhradní schéma, v němž se nejprve transformuje n–módový systém pomocí souboru pasivních prvků, pak každý jednotlivý mód nezávisle na sobě stlačit a nakonec tyto módy opět transformovat na souboru pasivních prvků. Tento rozklad je zřejmě vhodný pro zefektivnění příslušné transformace.



Obrázek 4.8: Schematické znázornění Braunsteinova rozkladu.

Kapitola 5

Sdílení tajemství

5.1 Sdílení klasického tajemství

Předpokládejme, že máme informaci o kombinaci otvírající trezor (kód), která je ve tvaru posloupnosti 101 001 111 011, a chceme ji předat dvěma dalším lidem, Alici a Bobovi. Nebylo by ovšem vhodné předávat ji v tomto tvaru každému z nich, protože si nejsme jisti, zda můžeme oběma věřit. Informaci proto „schováme“. Alici předáme posloupnost 011 010 101 001 a Bobovi 001 100 101 101. Dekódování se pak provede tak, že Alice a Bob poskytnou posloupnost, jež obdrželi, a podle pravdivostní tabulky

A	B	$A \circ B$
1	1	1
1	0	0
0	1	0
0	0	1

Tabulka 5.1

jsou kombinaci schopni získat. Skutečně se můžeme přesvědčit, že tomu tak je:

A	011 010 101 001
B	001 100 101 101
kód	101 001 111 011

Tabulka 5.2

Tento příklad ilustruje obecný přístup k problematice sdílení tajemství, které zavedl Shamir [10]. Jistá informace, neboli *tajemství (secret)*, jež chceme skrýt, je zakódována do většího počtu jiných informací, neboli *shares*, jež jsou předány *hráčům* (v našem příkladu Alice a Bob). Tito hráči pak mohou vzájemnou spoluprací tajemství dekódovat podle jistého *klíče* (v příkladu pravdivostní tabulka), když každý poskytne informaci, jež má k dispozici.

Skupina hráčů, která je toho schopna dosáhnout, se nazývá *autorizovaná skupina* (společně Alice a Bob) a skupina hráčů, jež toho není schopna vzájemnou spoluprací dosáhnout, se nazývá *neautorizovaná skupina* (jen Alice nebo jen Bob).

Problém, v němž je k zakódování tajemství použito n hráčů, z nichž minimálně k je schopno provést dekódování, se nazývá *prahové schéma (k,n)* (náš příklad je prahové schéma (2,2)).

Ve výše uvedeném příkladu je tajemství ve tvaru posloupnosti nul a jedniček. Ta se dá realizovat např. tím, že tuto informaci napíšeme na papír, nebo elektronicky, kdy „není signál“ znamená nulu a „je signál“ znamená jedničku. Tato tzv. klasická informace není jediný možný způsob realizace tajemství.

5.2 Sdílení kvantového tajemství

Další možností je využít kvantové mechaniky. Informacemi jsou pak kvantové stavy. Tato informace se nazývá *qubit*, pokud je to stav Hilbertova prostoru dimenze 2, *qutrit*, pokud je to stav Hilbertova prostoru dimenze 3, obecně *qudit*, pokud je to stav Hilbertova prostoru dimenze d.

Qubit je tak možno zapsat jako

$$|\psi\rangle_2 = \alpha|0\rangle + \beta|1\rangle, \tag{5.1}$$

přičemž $|\alpha|^2 + |\beta|^2 = 1$, qutrit jako

$$|\psi\rangle_3 = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle, \tag{5.2}$$

kde, $|\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1$, a qudit

$$|\psi\rangle_d = \sum_{n=0}^{d-1} \alpha_n |n\rangle, \tag{5.3}$$

kde $\sum_{n=0}^{d-1} |\alpha_n|^2 = 1$.

Na qubitu demonstrujme rozdíl mezi klasickou a kvantovou informací. Ty se liší tím, že

- kdyby $|\psi\rangle_2$ byla klasická, bylo by $\alpha = 0$ a $\beta = 1$ nebo $\alpha = 1$ a $\beta = 0$, u kvantové informace jsou koeficienty α a β obecně komplexní a libovolné takové, aby byla splněna normovací podmínka $|\alpha|^2 + |\beta|^2 = 1$, existuje jich tedy nekonečně mnoho,
- u kvantové informace může dojít k provázání (neboli entanglementu), což u klasické informace nelze.

Uveďme příklad. Uvažujme o stavu $\alpha|0\rangle+\beta|1\rangle+\gamma|2\rangle$ jakožto o kvantovém tajemství (qutrit), které je zakódováno transformací V takovou, že

$$\begin{aligned} V : \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \longrightarrow\ & \alpha(|000\rangle + |111\rangle + |222\rangle)+ \\ & \beta(|012\rangle + |120\rangle + |201\rangle)+ \\ & \gamma(|021\rangle + |102\rangle + |210\rangle), \end{aligned}$$

neboli první hráč (Alice), jež měl(a) na počátku stav $|0\rangle$, obdrží po transformaci provázaný stav $|000\rangle + |111\rangle + |222\rangle$, druhý hráč (Bob), jež měl na počátku stav $|1\rangle$, obdrží po transformaci provázaný stav $|012\rangle + |120\rangle + |201\rangle$ a třetí hráč (Carol), jež měl(a) na počátku stav $|2\rangle$, obdrží po transformaci provázaný stav $|021\rangle + |102\rangle + |210\rangle$. Každý z těchto hráčů má jistou informaci o tajemství, ale samostatně ji rozluštit nedokáže. Avšak spoluprací libovolných dvou hráčů toho dosáhnout lze. Dá se ukázat [16], že kvantověmechanickou transformací lze např. ze stavů Alice a Boba dostat stav

$$(\alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle) \otimes (|00\rangle + |12\rangle + |21\rangle),$$

tedy povedlo se *odprovázat* tuto dvojici tak, že Alice nyní vlastní hledané kvantové tajemství.

Podobně jako u klasického tajemství, i zde lze zavést *prahové schéma ((k,n))*, tedy při dané n–tici hráčů je schopna tajemství dekódovat minimálně k–tice z nich. V našem příkladu se jedná o prahové schéma ((2,3)).

Teorém o neklonování (No Cloning Theorem)

Podle tohoto teorému [3] nelze libovolný stav $|\psi\rangle$ „nakopírovat“ a vytvořit tak stav $|\psi\rangle \otimes |\psi\rangle$, tj. neexistuje unitární operátor $\hat{U}$ takový, že $\hat{U}\left(|\psi\rangle \otimes |0\rangle\right) = |\psi\rangle \otimes |\psi\rangle$.

Důkaz: Předpokládejme, že takový operátor existuje, tedy $\hat{U}^\dagger \hat{U} = \mathbf{1}$. Uvažujme o dvou neortogonálních stavech $|\psi\rangle$ a $|\phi\rangle$, tj. $\langle\psi|\phi\rangle \neq 0$. Pak

$$\begin{aligned}
\langle\psi|\phi\rangle &= \langle\psi|\phi\rangle\langle 0|0\rangle = \\
&= (|\psi\rangle \otimes |0\rangle)^\dagger (|\phi\rangle \otimes |0\rangle) = \\
&= (|\psi\rangle \otimes |0\rangle)^\dagger \hat{U}^\dagger \hat{U} (|\phi\rangle \otimes |0\rangle) = \\
&= \langle\psi|\phi\rangle\langle\psi|\phi\rangle.
\end{aligned}$$

Celkem máme

$$\langle\psi|\phi\rangle = \langle\psi|\phi\rangle^2,$$

což může nastat ve dvou případech: buď $\langle\psi|\phi\rangle = 0$, což je ve sporu s předpokladem $\langle\psi|\phi\rangle \neq 0$, nebo $\langle\psi|\phi\rangle = 1$, což znamená, že stavy $|\psi\rangle$ a $|\phi\rangle$ jsou totožné. To znamená, že neexistuje žádné kvantové zařízení, které je schopno vytvořit kopii dvou různých stavů.

Z teorému o neklonování plyne, že nemůže existovat prahové schéma $((k, n))$ pro $n \geq 2k$. Kdyby ano, znamenalo by to, že jistá k–tice hráčů může dekódovat tajemství $|\psi\rangle$ a totéž by mohla udělat jiná k–tice hráčů, jež má disjunktní průnik s první k–ticí. To by ale znamenalo, že ze stavu $|\psi\rangle$ by bylo možno dostat stav $|\psi\rangle \otimes |\psi\rangle$, což teorém o neklonování vylučuje.

V kvantové teorii informace bylo nejprve zkoumáno sdílení kvantových tajemství v diskrétních proměnných (např. [16], [11], [15]), později se ukázalo vhodné zabývat se i sdílení kvantových tajemství ve spojitých proměnných [9]. Rozdíl je v dimenzi Hilbertova prostoru - u diskrétních proměnných je konečná, u spojitých proměnných je nekonečná.

Zakódování kvantového stavu se realizuje jeho provázáním s tzv. pomocnými stavy užitím optické interferometrie.

Kapitola 6

Efektivní sdílení kvantových tajemství ve spojitých proměnných

V článku [4] byl nalezen extrakční protokol pro prahové schéma $((k, 2k-1))$. Jedno kvantové tajemství se provázalo se stlačenými vakuovanými stavy. Prvních k z nich byly stlačeny a–krát, zbylých k $\frac{1}{a}$–krát. Dále se ukázalo, že k odprovázání jednoho kvantového tajemství spoluprací k hráčů je postačující použití dvou stlačovacích prvků.

V této práci jsem se pokusil rozšířit výsledek z [4] a zjistit, zda je možné odprovázat více kvantových tajemství najednou, nalézt extrakční protokol a snížit počet stlačovačů potřebných k odprovázání tajemství na minimum.

Mějme l kvantových stavů $|\psi_1\rangle, \ldots, |\psi_l\rangle$ představujících kvantová tajemství, která chceme zakódovat. To provedeme tak, že je provážeme jednak navzájem a jednak současně s tzv. pomocnými stavy $|\varphi_1^{1/a}\rangle, \ldots, |\varphi_k^{1/a}\rangle, |\varphi_1^a\rangle, \ldots, |\varphi_k^a\rangle$ tím, že je necháme projít optickou soustavou skládající se s optických pasivních (děliče svazku, posouvače fáze) a aktivních (stlačovače) prvků. Tato soustava se též nazývá aktivní interferometr.

Souřadnicové reprezentace pomocných stavů jsou

$$\langle x|\varphi_i^{1/a}\rangle = \sqrt[4]{\frac{1}{a\pi}}\, e^{-\frac{x^2}{2a}} \qquad \text{a} \qquad \langle x|\varphi_i^a\rangle = \sqrt[4]{\frac{a}{\pi}}\, e^{-\frac{a}{2}x^2},$$

$i = 1, \ldots, k$, přičemž požadujeme, aby číslo a bylo dostatečně velké, tj. aby $a \to \infty$ (smysl tohoto požadavku bude zřejmý později). Jedná se o stlačené vakuové stavy, přičemž prvních k stavů jsou v souřadnicové reprezentaci velmi široké gaussovy křivky a druhých k stavů jsou naopak velmi úzké gaussovy křivky. Tyto stavy se volí jako pomocné jednak proto, že vakuum umíme prakticky nejlépe stlačit a jednak pro jejich jisté matematické vlastnosti, které budeme potřebovat také později.

Označme celkový počet stavů jako n, čili $n = l + 2k$. Počáteční stav před transformací je separabilním stavem

$$|\Phi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_l\rangle \otimes |\varphi_1^a\rangle \otimes \cdots \otimes |\varphi_k^a\rangle \otimes |\varphi_1^{1/a}\rangle \otimes \cdots \otimes |\varphi_k^{1/a}\rangle.$$

Vyjádřeme jej v souřadnicové bázi

$$\begin{aligned}|\Phi\rangle &= \int \mathrm{d}x_1 \ldots \mathrm{d}x_n (|x_n\rangle \otimes \cdots \otimes |x_1\rangle\langle x_1| \otimes \cdots \otimes \langle x_n|)|\psi_1\rangle \otimes \cdots \otimes |\varphi_k^{1/a}\rangle \\ &= \int \mathrm{d}x_1 \ldots \mathrm{d}x_n \prod_{i=1}^{l} \psi_i(x_i) \prod_{i=1}^{k} \varphi_i^{1/a}(x_{l+i}) \prod_{i=1}^{k} \varphi_i^a(x_{l+k+i}) |x_1\rangle \otimes \cdots \otimes |x_n\rangle\end{aligned}$$

Pro přehlednost přeznačme proměnné

$$\begin{aligned} x_i &= x_i && \text{pro } i = 1, \dots, l \\ y_i &= x_{l+i} && \text{pro } i = 1, \dots, k \\ z_i &= x_{l+k+i} && \text{pro } i = 1, \dots, k. \end{aligned}$$

a ještě označme $\mathbf{x} = (x_1, \dots, x_l, y_1, \dots, y_k, z_1, \dots, z_k)$. Při tomto označení máme

$$\begin{aligned} |\Phi\rangle &= \int \mathrm{d}^n\mathbf{x} \prod_{i=1}^{l} \psi_i(x_i) \prod_{i=1}^{k} \varphi_i^{1/a}(y_i) \prod_{i=1}^{k} \varphi_i^{a}(z_i) |x_1\rangle \otimes \cdots \otimes |z_k\rangle = \\ &= \int \mathrm{d}^n\mathbf{x} \prod_{i=1}^{l} \psi_i(x_i) \exp\left[-\frac{1}{2a} \sum_{i=1}^{k} y_i^2 - \frac{a}{2} \sum_{i=1}^{k} z_i^2 \right] |x_1\rangle \otimes \cdots \otimes |z_k\rangle \end{aligned} \tag{6.1}$$

Průchod stavu $|\Phi\rangle$ přes optickou soustavu, kterou můžeme reprezentovat operátorem $\hat{G}$, dá výsledný stav $\hat{G}|\Phi\rangle$. Nicméně, jak jsme viděli v předcházející kapitole, lze tyto transformace chápat jako symplektické transformace souřadnic a impulzů zastupované maticí $\mathbf{S}$. Uvažujme speciální typ těchto transformací, kdy se mění pouze souřadnice na souřadnice (prostřednictvím *regulární* matice $\mathbf{G} \in \mathbb{R}^{n \times n}$) a komplementárně pak impulzy na impulzy. V případě našeho stavu (6.1) tak bude

$$|\Phi\rangle_G \equiv \hat{G}|\Phi\rangle = \sqrt{|\det \mathbf{G}|} \int \mathrm{d}^n\mathbf{x} \prod_{i=1}^{l} \psi_i(x_i) \exp\left[-\frac{1}{2a} \sum_{i=1}^{k} y_i^2 - \frac{a}{2} \sum_{i=1}^{k} z_i^2 \right] |g_1(\mathbf{x})\rangle \otimes \cdots \otimes |g_n(\mathbf{x})\rangle, \tag{6.2}$$

přičemž g_i je i–tý řádek matice $\mathbf{G}$. V souřadnicové reprezentaci se stav $|\Phi\rangle$ transformuje tak, že se lineárně transformují souřadnicové proměnné prostřednictvím matice $\mathbf{G}$, tj bázový prvek $|x_1\rangle \otimes \cdots \otimes |z_k\rangle$ přechází na bázový prvek $|g_1(\mathbf{x})\rangle \otimes \cdots \otimes |g_n(\mathbf{x})\rangle$.

Formulace problému

Našim cílem nyní bude odprovázat kvantové stavy $|\psi_1\rangle, \dots, |\psi_l\rangle$ z provázaného stavu $|\Phi\rangle_G$ prostřednictvím vhodné transformace aplikované na prvních $l + k$ stavů tak, aby k tomu bylo zapotřebí pokud možno co nejméně stlačovacích prvků.

Ukazuje se, že je výhodné trochu zaměnit formální přístup. Nezávislé proměnné $x_1, \dots, x_n$ nahradíme souborem vektorů $(\mathbf{f}_1, \dots, \mathbf{f}_n)$ tvořících standardní bázi[1] tak, že

$$\mathbf{f}_i(\bar{\mathbf{x}}) = x_i \qquad i = 1, \dots, n,$$

kde $\bar{\mathbf{x}} = (x_1, \dots, x_n)$. Důležitá je skutečnost, že tyto vektory jsou řádkové. Každý takový vektor zastupuje příslušný stav. Soubor $(\mathbf{f}_1, \dots, \mathbf{f}_n)$ generuje vektorový prostor $\mathbb{V}$ dimenze n. Napišme jej jako direktní součet tří podprostorů

$$\mathbb{V} = \mathbb{X} \oplus \mathbb{Y} \oplus \mathbb{Z},$$

přičemž prostor $\mathbb{X}$ je generován vektory $(\mathbf{f}_1, \dots, \mathbf{f}_l)$, které přísluší kvantovým tajemstvím, a má tak dimenzi l, prostor $\mathbb{Y}$ je generován vektory $(\mathbf{f}_{l+1}, \dots, \mathbf{f}_{l+k})$, které přísluší první k–tici

[1] Standardní báze je tvořena takovými vektory $(\mathbf{f}_1, \dots, \mathbf{f}_n)$, že $\mathbf{f}_i = (0, \dots, 0, 1, 0, \dots, 0)$, přičemž jednička je na i–tém místě.

pomocných stavů a prostor $\mathbb{Z}$ je generován vektory $(\mathbf{f}_{l+k+1}, \ldots, \mathbf{f}_n)$, které přísluší druhé k–tici pomocných stavů, oba mají dimenzi k.

Lineární transformace souřadnic reprezentovaná maticí $\mathbf{G}$ tak převádí soubor $(\mathbf{f}_1, \ldots \mathbf{f}_n)$ na nový soubor $(\mathbf{g}_1, \ldots, \mathbf{g}_n)$, přičemž

$$\mathbf{g}_i = \sum_{j=1}^{n} g_{ij}\mathbf{f}_j, \qquad \text{pro } i = 1, \ldots, n.$$

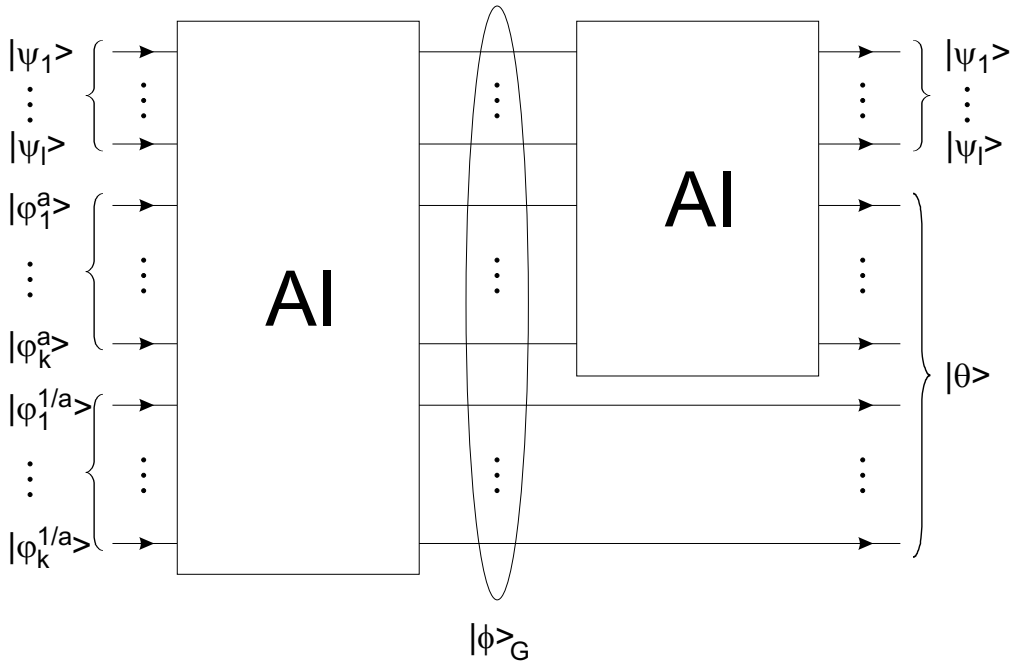
Maticový zápis této transformace je

$$\begin{pmatrix} \mathbf{g}_1 \\ \vdots \\ \mathbf{g}_n \end{pmatrix} = \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ \vdots & \ddots & \vdots \\ g_{n1} & \cdots & g_{nn} \end{pmatrix} \begin{pmatrix} \mathbf{f}_1 \\ \vdots \\ \mathbf{f}_n \end{pmatrix}.$$

Ale jelikož vektory $(\mathbf{f}_1, \ldots, \mathbf{f}_n)$ tvoří standardní bázi, je matice jimi tvořená jednotková a řádky matice $\mathbf{G}$ tak tvoří soubor transformovaných vektorů.

Odprovázání kvantových tajemství

Abychom odprovázali kvantové stavy $|\psi_1\rangle, \ldots, |\psi_l\rangle$, stačilo by pouze transformovat soubor $(\mathbf{g}_1, \ldots, \mathbf{g}_n)$ pomocí matice $\mathbf{G}^{-1}$, což by šlo, poněvadž jsme předpokládali, že $\mathbf{G}$ je regulární. Nicméně taková transformace by se vztahovala na celý soubor $(\mathbf{g}_1, \ldots, \mathbf{g}_n)$. My však chceme odprovázat kvantová tajemství prostřednictvím transformace prvních $(l+k)$ vektorů $(\mathbf{g}_1, \ldots, \mathbf{g}_{l+k})$, a to pomocí regulární matice $\mathbf{T} \in \mathbb{R}^{n\times n}$. Ta působí neidenticky na podprostor $\mathbb{X} \oplus \mathbb{Y}$ a identicky na podprostor $\mathbb{Z}$.



Obrázek 6.1: Schéma provázání $l + 2k$ stavů a následného odprovázání l tajemství (AI = aktivní interferometr).

V dalším ukážeme, že pokud se nám podaří nalézt takovou matici $\mathbf{T}$, že celková transformace reprezantovaná maticí $\mathbf{D} = \mathbf{TG}$, $\mathbf{D} \in \mathbb{R}^{n\times n}$, $\mathbf{D} = (d_{ij})_{i,j=1}^{n}$, takovou, že

$$\begin{aligned} d_{ij} &= \delta_{ij} && \text{pro } i = 1,\dots,l; j = 1,\dots,l+k \\ d_{ij} &= d_{i+k,j} && \text{pro } i = l+1,\dots,l+k; j = 1,\dots,l+k, \end{aligned}$$

přičemž zbývající prvky jsou libovolné, tak je možno odprovázat kvantová tajemství. V maticovém tvaru je pak

$$\mathbf{D} = \left(\begin{array}{ccc|ccc|ccc} 1 & \cdots & 0 & 0 & \cdots & 0 & c_{1,1} & \cdots & c_{1,k} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 & 0 & \cdots & 0 & c_{l,1} & \cdots & c_{l,k} \\ \hline a_{1,1} & \cdots & a_{1,l} & b_{1,1} & \cdots & b_{1,k} & c_{l+1,1} & \cdots & c_{l+1,k} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{k,1} & \cdots & a_{k,l} & b_{k,1} & \cdots & b_{k,k} & c_{l+k,1} & \cdots & c_{l+k,k} \\ \hline a_{1,1} & \cdots & a_{1,l} & b_{1,1} & \cdots & b_{1,k} & c_{l+k+1,1} & \cdots & c_{l+k+1,k} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{k,1} & \cdots & a_{k,l} & b_{k,1} & \cdots & b_{k,k} & c_{n,1} & \cdots & c_{n,k} \end{array}\right)$$

nebo pomocí submatic

$$\mathbf{D} = \left(\begin{array}{c|c|c} \mathbf{E} & \mathbf{0} & \mathbf{C}_1 \\ \hline \mathbf{A} & \mathbf{B} & \mathbf{C}_2 \\ \hline \mathbf{A} & \mathbf{B} & \mathbf{C}_3 \end{array}\right),$$

kde $\mathbf{E}$ je jednotková, $\mathbf{0}$ nulová matice a

$$\mathbf{A} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,l} \\ \vdots & \ddots & \vdots \\ a_{k,1} & \cdots & a_{k,l} \end{pmatrix} \qquad \mathbf{B} = \begin{pmatrix} b_{1,1} & \cdots & b_{1,k} \\ \vdots & \ddots & \vdots \\ b_{k,1} & \cdots & b_{k,k} \end{pmatrix}$$

$$\mathbf{C}_1 = \begin{pmatrix} c_{1,1} & \cdots & c_{1,k} \\ \vdots & \ddots & \vdots \\ c_{l,1} & \cdots & c_{l,k} \end{pmatrix} \qquad \mathbf{C}_2 = \begin{pmatrix} c_{l+1,1} & \cdots & c_{l+1,k} \\ \vdots & \ddots & \vdots \\ c_{l+k,1} & \cdots & c_{l+k,k} \end{pmatrix}$$

$$\mathbf{C}_3 = \begin{pmatrix} c_{l+k+1,1} & \cdots & c_{l+k+1,k} \\ \vdots & \ddots & \vdots \\ c_{n,1} & \cdots & c_{n,k} \end{pmatrix}.$$

Označme $\mathbf{d}_i = \tilde{\mathbf{a}}_i + \tilde{\mathbf{b}}_i + \tilde{\mathbf{c}}_i$ jako i–tý řádek matice $\mathbf{D}$ a $\tilde{\mathbf{a}}_i$, $\tilde{\mathbf{b}}_i$, $\tilde{\mathbf{c}}_i$ ortogonální projekci vektoru $\mathbf{d}_i$ po řadě na podprostory $\mathbb{X}$, $\mathbb{Y}$, $\mathbb{Z}$. Máme tedy

$$\begin{aligned} |\Phi\rangle_D = \int \mathrm{d}^n\mathbf{x} \prod_{i=1}^{l} \psi_i(x_i) \exp\left[-\frac{1}{2a}\sum_{i=1}^{k} y_i^2 - \frac{a}{2}\sum_{i=1}^{k} z_i^2\right] |x_1 + \tilde{\mathbf{c}}_1(\mathbf{x})\rangle \otimes \cdots \otimes |x_l + \tilde{\mathbf{c}}_l(\mathbf{x})\rangle \otimes \\ \otimes |\tilde{\mathbf{a}}_{l+1}(\mathbf{x}) + \tilde{\mathbf{b}}_{l+1}(\mathbf{x}) + \tilde{\mathbf{c}}_{l+1}(\mathbf{x})\rangle \otimes \cdots \otimes |\tilde{\mathbf{a}}_{l+k}(\mathbf{x}) + \tilde{\mathbf{b}}_{l+k}(\mathbf{x}) + \tilde{\mathbf{c}}_{l+k}(\mathbf{x})\rangle \otimes \\ \otimes |\tilde{\mathbf{a}}_{l+1}(\mathbf{x}) + \tilde{\mathbf{b}}_{l+1}(\mathbf{x}) + \tilde{\mathbf{c}}_{l+k+1}(\mathbf{x})\rangle \otimes \cdots \otimes |\tilde{\mathbf{a}}_{l+k}(\mathbf{x}) + \tilde{\mathbf{b}}_{l+k}(\mathbf{x}) + \tilde{\mathbf{c}}_{n}(\mathbf{x})\rangle \end{aligned}$$

Pro přehlednost ještě proveďme přeznačení

$$\begin{aligned}
\mathbf{a}_i &= \tilde{\mathbf{a}}_{l+i} \qquad \text{pro } i = 1, \dots, k \\
\mathbf{b}_i &= \tilde{\mathbf{b}}_{l+i} \qquad \text{pro } i = 1, \dots, k \\
\mathbf{c}_i &= \tilde{\mathbf{c}}_i \qquad \text{pro } i = 1, \dots, n.
\end{aligned}$$

Potom

$$\begin{aligned}
|\Phi\rangle_D = \int \mathrm{d}^n\mathbf{x} \prod_{i=1}^{l} \psi_i(x_i) \exp\left[-\frac{1}{2a}\sum_{i=1}^{k} y_i^2 - \frac{a}{2}\sum_{i=1}^{k} z_i^2\right] |x_1 + \mathbf{c}_1(\mathbf{x})\rangle \otimes \cdots \otimes |x_l + \mathbf{c}_l(\mathbf{x})\rangle \otimes \\
\otimes |\mathbf{a}_1(\mathbf{x}) + \mathbf{b}_1(\mathbf{x}) + \mathbf{c}_{l+1}(\mathbf{x})\rangle \otimes \cdots \otimes |\mathbf{a}_k(\mathbf{x}) + \mathbf{b}_k(\mathbf{x}) + \mathbf{c}_{l+k}(\mathbf{x})\rangle \otimes \\
\otimes |\mathbf{a}_1(\mathbf{x}) + \mathbf{b}_1(\mathbf{x}) + \mathbf{c}_{l+k+1}(\mathbf{x})\rangle \otimes \cdots \otimes |\mathbf{a}_k(\mathbf{x}) + \mathbf{b}_k(\mathbf{x}) + \mathbf{c}_n(\mathbf{x})\rangle.
\end{aligned}$$

Ale jelikož

$$\begin{aligned}
\mathbf{a}_i(\mathbf{x}) &= \sum_{j=1}^{l} a_{ij} x_j \qquad \text{pro } i = 1, \dots, k \\
\mathbf{b}_i(\mathbf{x}) &= \sum_{j=1}^{k} b_{ij} y_j \qquad \text{pro } i = 1, \dots, k \\
\mathbf{c}_i(\mathbf{x}) &= \sum_{j=1}^{k} c_{ij} z_j \qquad \text{pro } i = 1, \dots, n,
\end{aligned}$$

tak

$$\begin{aligned}
|\Phi\rangle_D = \int \mathrm{d}^n\mathbf{x} \prod_{i=1}^{l} \psi_i(x_i) \exp\left[-\frac{1}{2a}\sum_{i=1}^{k} y_i^2 - \frac{a}{2}\sum_{i=1}^{k} z_i^2\right] \left| x_1 + \sum_{j=1}^{k} c_{1j} z_j \right\rangle \otimes \cdots \otimes \left| x_l + \sum_{j=1}^{k} c_{lj} z_j \right\rangle \otimes \\
\otimes \left| \sum_{j=1}^{l} a_{1j} x_j + \sum_{j=1}^{k} b_{1j} y_j + \sum_{j=1}^{k} c_{l+1,j} z_j \right\rangle \otimes \cdots \otimes \left| \sum_{j=1}^{l} a_{kj} x_j + \sum_{j=1}^{k} b_{kj} y_j + \sum_{j=1}^{k} c_{l+k,j} z_j \right\rangle \otimes \\
\otimes \left| \sum_{j=1}^{l} a_{1j} x_j + \sum_{j=1}^{k} b_{1j} y_j + \sum_{j=1}^{k} c_{l+k+1j} z_j \right\rangle \otimes \cdots \otimes \left| \sum_{j=1}^{l} a_{kj} x_j + \sum_{j=1}^{k} b_{kj} y_j + \sum_{j=1}^{k} c_{nj} z_j \right\rangle.
\end{aligned}$$

Nyní provedeme substituci ve dvou krocích:
<u>1. krok</u>: První má tvar $x_i \to x_i - \sum_{j=1}^{k} c_{ij} z_j$, $i = 1, \dots, l$. Po této transformaci je

$$\begin{aligned}
|\Phi\rangle_D = \int \mathrm{d}^n\mathbf{x} \prod_{i=1}^{l} \psi_i(x_i - \sum_{j=1}^{k} c_{ij} z_j) \exp\left[-\frac{1}{2a}\sum_{i=1}^{k} y_i^2 - \frac{a}{2}\sum_{i=1}^{k} z_i^2\right] |x_1\rangle \otimes \cdots \otimes |x_l\rangle \otimes \\
\otimes \left| \sum_{j=1}^{l} a_{1j} x_j + \sum_{j=1}^{k} b_{1j} y_j + \sum_{j=1}^{k} c'_{l+1,j} z_j \right\rangle \otimes \cdots \otimes \left| \sum_{j=1}^{l} a_{kj} x_j + \sum_{j=1}^{k} b_{kj} y_j + \sum_{j=1}^{k} c'_{l+k,j} z_j \right\rangle \otimes \\
\otimes \left| \sum_{j=1}^{l} a_{1j} x_j + \sum_{j=1}^{k} b_{1j} y_j + \sum_{j=1}^{k} c'_{l+k+1j} z_j \right\rangle \otimes \cdots \otimes \left| \sum_{j=1}^{l} a_{kj} x_j + \sum_{j=1}^{k} b_{kj} y_j + \sum_{j=1}^{k} c'_{nj} z_j \right\rangle,
\end{aligned}$$

přičemž $c'_{l+i,j} = c_{l+i,j} - \sum_{m=1}^{l} a_{im}c_{mj}$ pro $i = 1, \dots, k$ a $c'_{l+k+i,j} = c_{l+k+i,j} - \sum_{m=1}^{l} a_{im}c_{mj}$ pro $i = 1, \dots, k$. Poněvadž $a \to \infty$, tak platí relace

$$\prod_{i=1}^{l} \psi_i(x_i - \sum_{j=1}^{k} c_{ij}z_j) \exp\left[-\frac{a}{2}\sum_{i=1}^{k} z_i^2\right] \approx \prod_{i=1}^{l} \psi_i(x_i) \exp\left[-\frac{a}{2}\sum_{i=1}^{k} z_i^2\right]$$

pro všechny hodnoty $\sum_{j=1}^{k} c_{ij}z_j$, pro něž $\exp\left[-\frac{a}{2}\sum_{i=1}^{k} z_i^2\right]$ je nezanedbatelné. Celkem máme

$$\begin{aligned}
|\Phi\rangle_D \approx \int \mathrm{d}^n\mathbf{x} \prod_{i=1}^{l} \psi_i(x_i) \exp\left[-\frac{1}{2a}\sum_{i=1}^{k} y_i^2 - \frac{a}{2}\sum_{i=1}^{k} z_i^2\right] |x_1\rangle \otimes \cdots \otimes |x_l\rangle \otimes \\
\otimes \left|\sum_{j=1}^{l} a_{1j}x_j + \sum_{j=1}^{k} b_{1j}y_j + \sum_{j=1}^{k} c'_{l+1,j}z_j\right\rangle \otimes \cdots \otimes \left|\sum_{j=1}^{l} a_{kj}x_j + \sum_{j=1}^{k} b_{kj}y_j + \sum_{j=1}^{k} c'_{l+k,j}z_j\right\rangle \otimes \\
\otimes \left|\sum_{j=1}^{l} a_{1j}x_j + \sum_{j=1}^{k} b_{1j}y_j + \sum_{j=1}^{k} c'_{l+k+1j}z_j\right\rangle \otimes \cdots \otimes \left|\sum_{j=1}^{l} a_{kj}x_j + \sum_{j=1}^{k} b_{kj}y_j + \sum_{j=1}^{k} c'_{nj}z_j\right\rangle .
\end{aligned}$$

<u>2. krok</u>: Další substitucí se budeme snažit odstranit proměnné $x_1, \dots, x_l$ z bázových ket vektorů v pořadí $l+1, \dots, n$. Jako vhodná se ukazuje substituce $y_r \to y_r - \sum_{m=1}^{k}\sum_{j=1}^{l} b^{rm}a_{mj}x_j$, kde koeficienty b^{km} jsou takové, že $\sum_{j=1}^{k} b_{ij}b^{jp} = \delta_{ip}$. Ukažme dosazením, že tomu tak je:

$$\begin{aligned}
\sum_{j=1}^{l} a_{ij}x_j + \sum_{p=1}^{k} b_{ip}\left(y_p - \sum_{m=1}^{k}\sum_{j=1}^{l} b^{pm}a_{mj}x_j\right) &= \sum_{j=1}^{l} a_{ij}x_j + \sum_{j=1}^{k} b_{ij}y_j - \sum_{p=1}^{k}\sum_{m=1}^{k}\sum_{j=1}^{l} b_{ip}b^{pm}a_{mj}x_j = \\
&= \sum_{j=1}^{l} a_{ij}x_j + \sum_{j=1}^{k} b_{ij}y_j - \sum_{m=1}^{k}\sum_{j=1}^{l} \delta_{im}a_{mj}x_j = \sum_{j=1}^{l} a_{ij}x_j + \sum_{j=1}^{k} b_{ij}y_j - \sum_{j=1}^{l} a_{ij}x_j = \\
&= \sum_{j=1}^{k} b_{ij}y_j
\end{aligned}$$

Celkem je

$$\begin{aligned}
|\Phi\rangle_D \approx \int \mathrm{d}^n\mathbf{x} \prod_{i=1}^{l} \psi_i(x_i) \exp\left[-\frac{1}{2a}\sum_{i=1}^{k}\left(y_i - \sum_{m=1}^{k}\sum_{j=1}^{l} b^{im}a_{mj}x_j\right)^2 - \frac{a}{2}\sum_{i=1}^{k} z_i^2\right] |x_1\rangle \otimes \cdots \otimes |x_l\rangle \otimes \\
\otimes \left|\sum_{j=1}^{l} a_{1j}x_j + \sum_{j=1}^{k} b_{1j}y_j + \sum_{j=1}^{k} c'_{l+1,j}z_j\right\rangle \otimes \cdots \otimes \left|\sum_{j=1}^{l} a_{kj}x_j + \sum_{j=1}^{k} b_{kj}y_j + \sum_{j=1}^{k} c'_{l+k,j}z_j\right\rangle \otimes \\
\otimes \left|\sum_{j=1}^{l} a_{1j}x_j + \sum_{j=1}^{k} b_{1j}y_j + \sum_{j=1}^{k} c'_{l+k+1j}z_j\right\rangle \otimes \cdots \otimes \left|\sum_{j=1}^{l} a_{kj}x_j + \sum_{j=1}^{k} b_{kj}y_j + \sum_{j=1}^{k} c'_{nj}z_j\right\rangle
\end{aligned}$$

Podobně jako v předchozí substituci platí relace

$$\prod_{i=1}^{l} \psi_i(x_i) \exp\left[-\frac{1}{2a}\sum_{i=1}^{k}\left(y_i - \sum_{m=1}^{k}\sum_{j=1}^{l} b^{im}a_{mj}x_j\right)^2\right] \approx \prod_{i=1}^{l} \psi_i(x_i) \exp\left[-\frac{1}{2a}\sum_{i=1}^{k} y_i^2\right]$$

pro všechny hodnoty $x_1, \ldots, x_l$, pro něž je $\prod_{i=1}^{l} \psi_i(x_i)$ nezanedbatelná. Dospěli jsme tak k vyjádření

$$
\begin{aligned}
|\Phi\rangle_D \approx \int \mathrm{d}^n\mathbf{x} \prod_{i=1}^{l} \psi_i(x_i) \exp\left[-\frac{1}{2a}\sum_{i=1}^{k} y_i^2 - \frac{a}{2}\sum_{i=1}^{k} z_i^2\right] |x_1\rangle \otimes \cdots \otimes |x_l\rangle \otimes \\
\otimes \left|\sum_{j=1}^{k} b_{1j} y_j + \sum_{j=1}^{k} c'_{l+1,j} z_j\right\rangle \otimes \cdots \otimes \left|\sum_{j=1}^{k} b_{kj} y_j + \sum_{j=1}^{k} c'_{l+k,j} z_j\right\rangle \otimes \\
\otimes \left|\sum_{j=1}^{k} b_{1j} y_j + \sum_{j=1}^{k} c'_{l+k+1j} z_j\right\rangle \otimes \cdots \otimes \left|\sum_{j=1}^{k} b_{kj} y_j + \sum_{j=1}^{k} c'_{nj} z_j\right\rangle .
\end{aligned}
$$

To však znamená, že

$$|\Phi\rangle_D \approx |\psi_1\rangle \otimes \cdots \otimes |\psi_l\rangle \otimes |\theta\rangle,$$

kde $|\theta\rangle$ je provázaný stav

$$
\begin{aligned}
|\theta\rangle = \int \mathrm{d}^k\mathbf{y}\, \mathrm{d}^k\mathbf{z} \exp\left[-\frac{1}{2a}\sum_{i=1}^{k} y_i^2 - \frac{a}{2}\sum_{i=1}^{k} z_i^2\right] \\
\left|\sum_{j=1}^{k} b_{1j} y_j + \sum_{j=1}^{k} c'_{l+1,j} z_j\right\rangle \otimes \cdots \otimes \left|\sum_{j=1}^{k} b_{kj} y_j + \sum_{j=1}^{k} c'_{l+k,j} z_j\right\rangle \otimes \\
\otimes \left|\sum_{j=1}^{k} b_{1j} y_j + \sum_{j=1}^{k} c'_{l+k+1j} z_j\right\rangle \otimes \cdots \otimes \left|\sum_{j=1}^{k} b_{kj} y_j + \sum_{j=1}^{k} c'_{nj} z_j\right\rangle .
\end{aligned}
$$

Budeme se proto snažit nalézt takovou matici $\mathbf{T}$, aby

1) $\mathbf{D} = \mathbf{TG}$,

2) při rozkladu $\mathbf{T} = \mathbf{U}\mathbf{T}_D\mathbf{V}$, $\mathbf{U}$ a $\mathbf{V}$ unitární matice, obsahovala diagonální matice $\mathbf{T}_D$ co nejméně diagonálních prvků různých od jedničky.

Matice $\mathbf{U}$ a $\mathbf{V}$ zastupují soubor pasivních optických prvků a každý diagonální prvek matice $\mathbf{T}_D$ představuje jeden jednomódový stlačovací optický element. Tedy celkový počet nejednotkových diagonálních prvků matice $\mathbf{T}_D$ je roven celkovému počtu stlačovačů potřebných k odprovázání kvantových tajemství.

Řádky matice $\mathbf{D}$ tvoří soubor vektorů $(\mathbf{d}_1, \ldots, \mathbf{d}_n)$, z nějž lze vyextrahovat kvantová tajemství. Označme $\mathbf{d}_i^\perp$ ortogonální projekci vektoru $\mathbf{d}_i$ na podprostor $\mathbb{X} \oplus \mathbb{Y}$ pro $i = 1, \ldots, n$, tzn. že $\mathbf{d}_i^\perp = \mathbf{a}_i + \mathbf{b}_i$. Je zřejmé, že soubor $(\mathbf{d}_1^\perp, \ldots, \mathbf{d}_n^\perp)$ je takový, že

a) $\mathbf{d}_i^\perp = \mathbf{f}_i^\perp$, kde $\mathbf{f}_i^\perp$ je ortogonální projekce $\mathbf{f}_i$ na $\mathbb{X} \oplus \mathbb{Y}$ pro $i = 1, \ldots, l$

b) podprostory generované soubory $(\mathbf{d}_{l+1}^\perp, \ldots, \mathbf{d}_{l+k}^\perp)$ a $(\mathbf{d}_{l+k+1}^\perp, \ldots, \mathbf{d}_n^\perp)$ jsou totožné.

Řešení

Předpokládejme, že jsme takovou matici $\mathbf{T} = (t_{ij})_{i,j=1,\ldots,n}$ již našli. Označme ještě $\mathbf{g}_i^\perp$ ortogonální projekci $\mathbf{g}_i$ na $\mathbb{X} \oplus \mathbb{Y}$. Matice $\mathbf{T}$ lineárně transformuje soubor $(\mathbf{g}_1^\perp, \ldots, \mathbf{g}_{l+k}^\perp)$ a zbývající

vektory identicky, tj.

$$\mathbf{d}_i^\perp = \sum_{j=1}^{l+k} t_{ij}\mathbf{g}_j^\perp \qquad \text{pro } i = 1, \dots, l+k \tag{6.3}$$

$$\mathbf{g}_i = \mathbf{d}_i \qquad \text{pro } i = l+k+1, \dots, n \tag{6.4}$$

Jak se ukáže, podmínka a) umožní získat vektory $(\mathbf{t}_1, \dots, \mathbf{t}_l)$ a podmínka b) zase vektory $(\mathbf{t}_{l+1}, \dots, \mathbf{t}_{l+k})$, kde $\mathbf{t}_i$ je i–tý řádek matice $\mathbf{T}$.

Z podmínky a) a požadavku (6.3) je jasné, že

$$\sum_{j=1}^{l+k} t_{ij}\mathbf{g}_j^\perp = \mathbf{f}_i^\perp \qquad \text{pro } i = 1, \dots, l,$$

neboli

$$\left(\begin{array}{ccc|ccc} (\mathbf{g}_1^\perp)^T & \cdots & (\mathbf{g}_{l+k}^\perp)^T & (\mathbf{f}_1^\perp)^T & \cdots & (\mathbf{f}_l^\perp)^T \end{array} \right) = \left(\begin{array}{ccc|ccc} & & & 1 & \cdots & 0 \\ & & & \vdots & \ddots & \vdots \\ (\mathbf{g}_1^\perp)^T & \cdots & (\mathbf{g}_{l+k}^\perp)^T & 0 & \cdots & 1 \\ & & & 0 & \cdots & 0 \\ & & & \vdots & \ddots & \vdots \\ & & & 0 & \cdots & 0 \end{array} \right).$$

Tím máme l soustav rovnic, které umožňují získat vektory $(\mathbf{t}_1, \dots, \mathbf{t}_l)$. Za zmínku stojí, že tyto vektory jsou již dány tvarem matice $\mathbf{G}$ a jsou tak pevně dané.

Podmínku b) lze splnit tak, že nalezneme podprostor $\mathcal{V}$, který je ortogonální ke $(\mathbf{g}_{l+k+1}, \dots, \mathbf{g}_n)$ a k tomuto podprostoru pak bude muset být ortogonální i soubor $(\mathbf{d}_{l+1}, \dots, \mathbf{d}_{l+k})$. Dimenze $\mathcal{V}$ je zřejmě l a označme jeho generátory $(\tilde{\mathbf{v}}_1, \dots, \tilde{\mathbf{v}}_l)$. Ty lze získat vyřešením soustavy

$$\left(\begin{array}{c|c} \mathbf{g}_{l+k+1} & 0 \\ \vdots & \vdots \\ \mathbf{g}_n & 0 \end{array} \right).$$

Pak zřejmě

$$0 = \tilde{\mathbf{v}}_m.\mathbf{d}_i^\perp = \tilde{\mathbf{v}}_m.\sum_{j=1}^{l+k} t_{ij}\mathbf{g}_j^\perp = \sum_{j=1}^{l+k} t_{ij}\tilde{\mathbf{v}}_m.\mathbf{g}_j^\perp$$

(pro všechna $i = l+1, \dots, l+k$ a $m = 1, \dots, l$) a při označení j–té složky vektoru $\tilde{\mathbf{w}}_m$ jako $\tilde{w}_{mj} \equiv \frac{\tilde{\mathbf{v}}_m.\mathbf{g}_j^\perp}{||\tilde{\mathbf{w}}_m||}$, kde $||\tilde{\mathbf{w}}_m|| = \sqrt{\sum_{i=1}^{l+k} \tilde{w}_{mi}^2}$ je norma vektoru $\tilde{\mathbf{w}}_m$, můžeme psát

$$0 = \sum_{j=1}^{l+k} t_{ij}\tilde{w}_{mj}. \tag{6.5}$$

Tzn. že soubory vektorů $(\mathbf{t}_{l+1}, \dots, \mathbf{t}_{l+k})$ a $(\tilde{\mathbf{w}}_1, \dots, \tilde{\mathbf{w}}_l)$ jsou vzájemně ortogonální. Nicméně nalezení vektorů $(\mathbf{t}_{l+1}, \dots, \mathbf{t}_{l+k})$ z rovnice (6.5) není pro dosažení našeho cíle podstatné.

Vektory $(\mathbf{t}_1, \dots, \mathbf{t}_l)$ jsou dány pevně a budeme dále předpokládat, že jsou navzájem ortogonální. Tento předpoklad je pro odprovázání kvantových tajemství zásadní. Co se týče vektorů $(\tilde{\mathbf{w}}_1, \dots, \tilde{\mathbf{w}}_l)$, ty jsou určeny vektory $(\tilde{\mathbf{v}}_1, \dots, \tilde{\mathbf{v}}_l)$, v jejichž volbě existuje určitý stupeň volnosti

- tvoří totiž bázi prostoru $\mathcal{V}$ a tato báze není jediná. Díky tomu v dalším nalezneme vektory $(\mathbf{v}_1, \ldots, \mathbf{v}_l)$ tak, aby vektory $(\mathbf{w}_1, \ldots, \mathbf{w}_l)$ jimi určené byly vzájemně ortogonální, tj.

$$\mathbf{w}_i.\mathbf{w}_j = \delta_{ij} \qquad \forall i, j = 1, \ldots, l. \tag{6.6}$$

Uvažujme tedy matici $\mathbf{M} = (m_{ij})_{i,j=1,\ldots,l}$ takovou, že

$$\mathbf{v}_i = \sum_{j=1}^{l} m_{ij} \tilde{\mathbf{v}}_j \qquad i = 1, \ldots, l,$$

čili $\mathbf{M}$ transformuje bázi $(\tilde{\mathbf{v}}_1, \ldots, \tilde{\mathbf{v}}_l)$ na novou bázi $(\mathbf{v}_1, \ldots, \mathbf{v}_l)$. S její pomocí nyní najdeme soubor $(\mathbf{w}_1, \ldots, \mathbf{w}_l)$, který musí splňovat (6.6), což pochopitelně omezuje možný výběr prvků matice $\mathbf{M}$, kterých je l^2, o celkový počet rovnic daných vztahem (6.6), kterých je $\frac{l(l-1)}{2}$. Tedy počet stupňů volnosti v prvcích matice $\mathbf{M}$ je $l^2 - \frac{l(l-1)}{2}$. Jak se ukáže, je ještě nutné požadovat, aby podprostory určené soubory $(\mathbf{t}_i, \mathbf{w}_i)$ a $(\mathbf{t}_j, \mathbf{w}_j)$ $\forall i, j = 1, \ldots, l$, $i \neq j$ byly ortogonální. To znamená, že $\mathbf{t}_i.\mathbf{t}_j = 0$, $\mathbf{t}_i.\mathbf{w}_j = 0$, $\mathbf{w}_i.\mathbf{t}_j = 0$ a $\mathbf{w}_i.\mathbf{w}_j = 0$. První rovnost je splněna z předpokladu, čtvrtá z předchozího výpočtu. Zbývá tak splnit rovnice $\mathbf{t}_i.\mathbf{w}_j = 0\ \forall i, j = 1, \ldots, l$, $i \neq j$, kterých je celkem $l(l-1)$ a jsou tak dalším omezením v možném výběru prvků matice $\mathbf{M}$. Celkový počet volných prvků matice $\mathbf{M}$ je tak $p(l) = l^2 - \frac{l(l-1)}{2} - l(l-1) = \frac{l(3-l)}{2}$. Odtud

l	$p(l)$
1	1
2	1
3	0

Tabulka 6.1

a pro $l > 3$ je $p(l) < 0$. Podprostory $(\mathbf{t}_1, \mathbf{w}_1), \ldots, (\mathbf{t}_l, \mathbf{w}_l)$ jsou navzájem ortogonální. V každém takovém podprostoru $(\mathbf{t}_i, \mathbf{w}_i)$ nalezneme vektor $\mathbf{w}_{i+l}$ tak, aby $\mathbf{w}_i.\mathbf{w}_{i+l} = 0$ pro každé $i = 1, \ldots, l$. To umožňuje vyjádřit $\mathbf{t}_i = \alpha_i \mathbf{w}_i + \beta_i \mathbf{w}_{i+l}$. Vektory $\mathbf{t}_{1+l}, \ldots, \mathbf{t}_{2l}$ dostaneme jako $\mathbf{t}_{i+l} = \gamma_i \mathbf{w}_{i+l}$ pro $i = 1, \ldots, l$, kde $\gamma_i = ||\mathbf{w}_{i+l}||$. Zbývající vektory $\mathbf{w}_{2l+1}, \ldots, \mathbf{w}_{2l+k}$ lze získat z $\mathbf{w}_1, \ldots, \mathbf{w}_{2l}$, jsou jejich ortogonálním doplňkem a jsou jednotkové. Zároveň můžeme položit $\mathbf{w}_{2l+i} = \mathbf{t}_{2l+i}$ pro $i = 1, \ldots, k$. V maticovém zápisu je

$$\mathbf{T} = \begin{pmatrix} \mathbf{t}_1 \\ \mathbf{t}_{1+l} \\ \mathbf{t}_2 \\ \mathbf{t}_{2+l} \\ \vdots \\ \mathbf{t}_l \\ \mathbf{t}_{2l} \\ \mathbf{t}_{2l+1} \\ \vdots \\ \mathbf{t}_{2l+k} \end{pmatrix} = \begin{pmatrix} \alpha_1 & \beta_1 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & \gamma_1 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & \alpha_2 & \beta_2 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \gamma_2 & \cdots & 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \alpha_l & \beta_l & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & \gamma_2 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} \mathbf{w}_1 \\ \mathbf{w}_{1+l} \\ \mathbf{w}_2 \\ \mathbf{w}_{2+l} \\ \vdots \\ \mathbf{w}_l \\ \mathbf{w}_{2l} \\ \mathbf{w}_{2l+1} \\ \vdots \\ \mathbf{w}_{2l+k} \end{pmatrix} \equiv \mathbf{XW}.$$

Nutný požadavek je proto, aby $l \leq k$, tj. počet kvantových tajemství musí být menší nebo roven polovině celkového počtu pomocných stavů. Matice $\mathbf{W}$ je ortogonální a matici $\mathbf{X}$ lze rozložit na $\mathbf{X} = \mathbf{UX}_D\mathbf{Y}$, kde $\mathbf{U}$, $\mathbf{Y}$ jsou ortogonální a $\mathbf{X}_D = \mathrm{diag}\,(\mathrm{u}_1, \mathrm{u}_{1+l}, \ldots, \mathrm{u}_l, \mathrm{u}_{2l}, 1, \ldots, 1)$. Celkem je $\mathbf{T} = \mathbf{UX}_D\mathbf{V}$, přičemž $\mathbf{V} = \mathbf{YW}$ je ortogonální. Jak již bylo řečeno, matice $\mathbf{U}$, $\mathbf{V}$ zastupují

soubor tvořený pasivními optickými prvky a počet nejednotkových prvků matice $\mathbf{X}_D$ odpovídá počtu jednomódových stlačovačů, kterých je tím pádem $2l$.

Poznámky:

- Z tabulky 6.1 vyplývá, že výběr bázových vektorů $\tilde{\mathbf{v}}_1, \ldots, \tilde{\mathbf{v}}_l$ prostoru $\mathcal{V}$ je libovolný v případě 1, 2 a 3 kvantových tajemství. V případě $l > 3$ je tyto vektory třeba vhodně vybrat tak, aby při případném hledání matice $\mathbf{M}$ byl počet volných parametrů $p(l)$ nezáporný. Toho lze dosáhnout vhodným výběrem $\tilde{\mathbf{v}}_1, \ldots, \tilde{\mathbf{v}}_l$, aby bylo splněno dostatečné množství ortogonálních relací $\tilde{\mathbf{w}}_i.\tilde{\mathbf{w}}_j = 0$, $\mathbf{t}_r.\tilde{\mathbf{w}}_s = 0$ některé $i, j, r, s = 1, \ldots, l$, $i \neq j$, $r \neq s$. Např. $p(4) = -2$, a tak tyto relace budou muset být alespoň 2.

- Pro odprovázání kvantových tajemství je nutné, aby $\mathbf{t}_1, \ldots, \mathbf{t}_l$ byly vzájemně ortogonální. Tyto vektory jsou určeny tvarem matice $\mathbf{G}$. Avšak výběr vektorů, které budeme transformovat maticí $\mathbf{T}$, je libovolný, musí jich být nejméně $l + k$. Můžeme se proto snažit vybrat vektory $(\mathbf{g}_{i_1}, \ldots, \mathbf{g}_{i_{l+k}}) \subset (\mathbf{g}_1, \ldots, \mathbf{g}_n)$ ve vhodném uspořádání tak, aby vektory $\mathbf{t}_{i_1}, \ldots, \mathbf{t}_{i_l}$ byly vzájemně ortogonální. Pokud se to podaří, je možno principiálně odprovázat kvantová tajemství.

Dodatky

Baker-Campbell-Hausdorffovy formule

$$e^{\hat{A}}\hat{B}e^{-\hat{A}} = \hat{B} + [\hat{A},\hat{B}] + \frac{1}{2!}[\hat{A},[\hat{A},\hat{B}]] + \cdots + \frac{1}{n!}[\hat{A},[\ldots,[\hat{A},[\hat{A},\hat{B}]\ldots] + \ldots \tag{6.7}$$

$$e^{\hat{A}}e^{\hat{B}} = e^{\hat{A}+\hat{B}+\frac{1}{2}[\hat{A},\hat{B}]+\frac{1}{12}[\hat{A},[\hat{A},\hat{B}]]+\frac{1}{12}[[\hat{A},\hat{B}],\hat{A}]+\ldots} \tag{6.8}$$

Kapitola 7

Závěr

Byl nalezen extrakční algoritmus pro odprovázání l kvantových tajemství pro prahové schéma $((l+k, l+2k))$. Při splnění jistých podmínek (viz. Poznámky v kapitole 6) je minimální počet stlačovací prvků potřebných k jejich extrakci $2l$. Proto musí být $k \geq l$.

Literatura

[1] L. D. Landau, E. M. Lifshitz: *Quantum Mechanics*, Butterworth-Heinemann, 2002

[2] M. O. Scully, M. S. Zubairy: *Quantum Optics*, Cambridge University Press, 1997

[3] W. K. Wooters, W. H. Zurek, Nature **299**, 802 (1982)

[4] T. Tyc, B. C. Sanders, Phys. Rev. A **65**, 042310

[5] L. Mandel, E. Wolf: *Optical Coherence and Quantum Optics*, Cambridge University Press, 1995

[6] D. Stoler, Phys. Rev. D **1**, 3217 (1970)

[7] R. J. Glauber, Phys. Rev. **131**, 2766 (1963)

[8] H. P. Yuen, Phys. Rev. A **6**, 2226 (1976)

[9] T. Tyc *et al.*, J. Phys. A: Math. Gen. **36** 7625 (2003)

[10] A. Shamir, Commun. ACM **22**, 612 (1979)

[11] A. D. Smith, e-print: quant-ph/0001087

[12] D. R. Truax, Phys. Rev. D **31**, 1988 (1984)

[13] S. L. Braunstein, e-print: quant-ph/9904002

[14] C. Schmid *et al.*, e-print: quant-ph/0502107

[15] M. Hillery, V. Bužek, A. Berthiaume, e-print: quant-ph/9806063

[16] R. Cleve, D. Gottesman, H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999)

[17] E. Schrödinger, Naturwissenschaft **14**, 664 (1926)