

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta jaderná a fyzikálně inženýrská

Purifikační protokoly a kvantový chaos

Purification and quantum chaos

Výzkumný úkol

Bc. Martin Malachov

Školitel: Prof. Ing. Igor Jex, DrSc.

Praha, 1.9.2014

Poděkování

Rád bych poděkoval prof. Igoru Jexovi za vedení práce a poskytnutí studijního zázemí. Především mu děkuji za zorganizování setkání s maďarskými kolegy, které mi pomohlo proniknout do problematiky. Dík tak patří i těmto lidem, vedeným dr. Tamášem Kisseem.

Prohlášení

Prohlašuji, že jsem svůj výzkumný úkol vypracoval samostatně a použil jsem pouze podklady uvedené v přiloženém seznamu.

Nemám závažný důvod proti použití tohoto školního díla ve smyslu § 60 Zákona č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne

.....
podpis

Obsah

1	Úvod	3
2	Teoretická část	5
2.1	Chaos v klasické fyzice	5
2.2	Základy kvantové fyziky	6
2.3	Kvantová informace	9
2.4	Problematika chaosu v kvantové teorii	11
2.5	Purifikace	13
2.6	Teorie funkcí jedné komplexní proměnné	15
3	Praktická část	19
3.1	Základní vlastnosti daného nelineárního operátoru	19
3.2	Pevné body purifikačního protokolu	21
3.3	Stavy s krátkou periodou	26
3.4	Speciální skupiny stavů	27
3.5	Juliovy a Fatouovy množiny speciálních případů	30
4	Závěr	33
	Literatura	35

Abstrakt

Kvantové provázání je zajímavý kvantově-fyzikální jev, který je příčinou mnoha neintuitivních efektů neznámých v makrosvětě. Známým příkladem důsledků kvantového provázání je kvantová teleportace, kdy je změřením jedné částice automaticky zjištěn stav částice s ní provázané. Purifikace je proces, kdy dochází k cílenému zvýšení provázanosti systému. Jedním z cílů této práce je shrnout základní informace o purifikaci.

Kvantová fyzika jako teorie lineárních operátorů, zdá se, ve své podstatě neumožňuje chaotické chování. Dva blízké stavy zůstanou díky unitaritě časového vývoje blízké v každém okamžiku. Nelineární chování lze nicméně do kvantového světa zavést jednoduše - měřením systému. Purifikační protokol typicky slouží jako zdroj nelinearity, a tudíž i chaotického chování. Tuto situaci je důležité řešit např. kvůli citlivosti časového vývoje stavu na počátečních podmínkách.

Tato práce se zabývá shrnutím základních poznatků z kvantové fyziky a matematické teorie chaosu. Dále rozebírá konkrétní purifikační protokol, diskutuje chování dvoučásticového systému podrobeného iteracím příslušného nelineárního operátoru, tj. především nalézá stavy se speciálním chováním.

Klíčová slova: chaos, kvantový chaos, kvantové provázání, qubit, Juliova množina

Abstract

Quantum entanglement is a source of many non-intuitive effects not known in the macroworld. A known example is quantum teleportation in which by measuring the state of one particle we ascertain automatically the state of another particle entangled with it. The purification is a process in which the entanglement is intentionally enhanced. This work aims at an overview of basic facts about purification. A purification protocol serves as a source of nonlinearities, and therefore of a chaotic behaviour. We discuss a specific purification protocol related to a two-particle system subject to iterations of corresponding non-linear operator, looking for states with a particular behaviour.

Key words: chaos, quantum chaos, quantum entanglement, qubit, Julia set

Kapitola 1

Úvod

Svět bez špagátu je jen chaos.

— *Rudolph Smuntz*

Na samém počátku 19. století přišel Henri Poincaré s pojmem *chaos*. Jeho práce[1] změnila svět, který si do té doby neuvědomoval, popř. nebyl schopen poradit si se složitými jevy. Typicky systém tří těles představoval úlohu, která nemá analytické řešení a vzhledem k dané době nepřipadaly v úvahu numerické simulace. Ty ovšem nejsou jednoduchou záležitostí ani v dnešní době. Jednou z charakteristik chaosu (přesná definice viz 2.1.2) je, že při sebemenší změně počátečních podmínek se řešení rozchází exponenciálně v čase. Proto i v éře supermoderních výpočetních systémů, které jsou tak jako tak limitovány konečným počtem desetinných míst, nelze určit řešení takové úlohy přesně pro dalekou budoucnost.

V úloze tří těles pak mohou např. nastat okamžiky, kdy dvacáté desetinné místo rozhodne o tom, zda se bude soustava pohybovat v uzavřené oblasti, či bude jedno z těles odmrštěno do nekonečna. Při chaotickém chování typicky dochází k následujícím případům: Vybraná počáteční podmínka implikuje, že ve fázovém prostoru je trajektorie pohybu periodická (v krajním případě jediný bod). Pak existují trajektorie neperiodické, ale obsažené v konečné oblasti. A na konec existují trajektorie, které s časem běží do nekonečna. Pro periodické trajektorie se lze rovněž věnovat otázce poruchového počtu. Periodické trajektorie lze rozdělit do 4 disjunktních skupin, více viz [2, str. 86]. Tyto skupiny jsou do určité míry analogem eliptických, parabolických a hyperbolických cyklů v teorii funkcí komplexní proměnné, více viz [3, str. 45].

V kvantové fyzice je dobře známým faktem, že ve fázovém prostoru nemůžeme najít klasicky trajektorie, ale jen oblaka pravděpodobnosti¹. Už jen tento primitivní fakt dost komplikuje hledání chaosu v kvantové teorii. Zároveň je ale z principu korespondence nutno požadovat, aby existoval kvantový systém, který by se v makroměřítku choval klasicky chaoticky. Chaos tedy i v kvantové fyzice

¹Komplikace nastávají díky relacím neurčitosti 2.2, které neumožňují zároveň libovolně přesně určit polohu a hybnost částice. Díky tomu ani není možné znát přesné počáteční podmínky např. pro úlohu tří těles.

musí být obsažen, aplikace principu korespondence mezi klasickými chaotickými a kvantovými systémy je jeden z problémů studovaný v rámci tzv. *kvantového chaosu*.

Na druhou stranu ovšem víme, že pokud jsou si dvě vlnové funkce velmi blízké, pak z unitarity časového vývoje tyto vlnové funkce zůstanou blízké ve všech časech. Kam se tedy poděl chaos? Je-li časový vývoj systému unitární, nemůže k chotickému chování dojít. V takovém případě se jedná o kvantovou fyziku tak, jak je předkládána v základních kurzech. Částice sice může být zároveň všude, mít zároveň oba spiny, rozhodně se ale v čase bude chovat relativně slušně (rozplývání vlnových balíků,...). Nejsilnějším a přitom vlastně nejsnazší dostupným prostředkem, který je k dispozici k vyvolání chaosu v kvantové fyzice, je měření.

Měření je velmi netriviální proces, kterým se do systému dostávají nelineární jevy. Jednak se samotným měřením může odebrat/přidat energie, impuls atp., ale především některá měření můžeme popsat jako působení nelineárních operátorů na systém. Na aplikaci speciálních měřících procesů jsou postaveny takzvané purifikační protokoly. Tato schémata využívají právě nelinearit k tomu, aby stav upravila podle představ experimentátora.

Konkrétně mají za cíl zvýšit provázanost stavu. Kvantové provázání je termín označující určitou korelaci mezi podsystémy většího systému. Maximálně provázané dvoučásticové stavy se nazývají *Bellovy stavy*, [4, str. 25]. Jsou to:

$$\begin{aligned} |\Phi^+\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, |\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \\ |\Psi^+\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}, |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \end{aligned}$$

Zřejmě pro stavy $|\Phi^\pm\rangle$ platí, že první částice je stejná, jako druhá. Změřením jedné z nich zkolabuje vlnová funkce druhé do stejné hodnoty. Podobně pro stavy $|\Psi^\pm\rangle$ - např. má-li jeden foton polarizaci vertikální, má druhý horizontální. To je nesmírně silná vlastnost, která se v roce 1935 stala cílem Einsteinových myšlenkových experimentů. Problematika kvantového provázání se stala populární jako EPR paradox (Einstein - Podolsky - Rosen). Původní práce [5] se zabývala hybností - mějme dvě částice, které spolu komunikují (provází se jako výše) a pak se oddělí a již spolu neinteragují. Přesným určením hybnosti jedné z nich nelze přesně určit její polohu. Ale druhá částice se v okamžiku měření v úplně jiném místě "dozví" svou hybnost. Tato situace je vzhledem k teorii relativity a šíření této informace okamžitě, nikoliv rychlostí světla, paradoxní. Je ale základem pro kvantovou teleportaci. Změřením jednoho fotonu lze okamžitě určit stav druhého fotonu, který už mezitím ovšem může být v jiné galaxii. Detailnější popis viz [4].

Kapitola 2

Teoretická část

2.1 Chaos v klasické fyzice

Slovo **chaos** pochází z řecké mytologie a člověk si pod ním obvykle představí náhodné, nepředvídatelné chování. Ve fyzice se ovšem chaos řídí fyzikálními zákony, a je tedy (obvykle) deterministický. Například vývoj počasí je určen zdánlivě jednoduchými diferenciálními rovnicemi. Ty nejsme schopni analyticky vyřešit, ale lze je řešit numericky. Stačí znát tlak, teplotu, vlhkost vzduchu a některé další parametry v každém místě na Zemi. Proč tedy neumíme předpovědět počasí přesně na dlouhou dobu dopředu? Jde ve své podstatě jen o naši neschopnost určit všechny nezbytné podmínky k určení výsledku?

Odpověď není úplně snadné, záleží na tom - a to je nejdříve třeba říci - co ve fyzikálním smyslu je chaos a co ne. V historii došlo k několika pokusům definovat chaos [2, 6], tyto definice se mohou trochu lišit, základní rys mají ovšem společný. Je jím *citlivost k počátečním podmínkám*. Dvě blízké počáteční podmínky mohou v čase způsobit exponenciální rozchod řešení. Tato vlastnost je známa jako "efekt motýlích křídel", protože i pouhé motýlí mávnutí křídel může být tím, co vyvolá hurikán na opačné straně Země.

Definujme nyní matematicky, co bude znamenat chaotické chování v této práci.

Definice 2.1.1 (Dynamický systém). *Bud' X úplný metrický prostor, T těleso. Dynamickým systémem rozumíme dvojici $(\{S_t\}, X)$, kde $\{S_t\}$ je množina spojitých zobrazení prostoru X do sebe s následujícími vlastnostmi:*

1. $\forall t, u \in T : S_{t+u} = S_t \circ S_u,$

2. S_0 je identita.

Definice 2.1.2 (Chaotický dynamický systém dle Devaneyho). *Bud' (ρ, X) úplný metrický prostor s metrikou ρ , f funkce. Dynamický systém (f, X) je chaotický, pokud jsou splněny následující podmínky:*

1. Množina periodických bodů f (tj. $\{x \in X \mid \exists n \in \mathbb{N}_0 : f^{\circ n}(x) = x\}$) je hustá v X .
2. Funkce f má tranzitivní vlastnost, tj. pro libovolné dvě otevřené množiny U, V v X existuje $n \in \mathbb{N}$ takové, že $f^{\circ n}(U) \cap V \neq \emptyset$.

Poznámka 2.1.1. V původní Devaneyho definici byl ještě třetí bod:

3. funkce f je citlivá na počáteční podmínky. Tzn. existuje ε takové, že pro každé $x \in X$ a každé jeho okolí U existuje $y \in U$ a $n \in \mathbb{N}$ tak, že $\rho(f^{\circ n}(x), f^{\circ n}(y)) > \varepsilon$.

Až později bylo dokázáno, že tento bod plyne z předchozích dvou. Ale právě tento bod je důležitý, protože charakterizuje chaos.

V klasické teorii chaosu se lze setkat s rozlišováním měkkého (soft) a tvrdého (hard) chaosu [2, str. 116]. Ilustrujme tyto pojmy na poruchách integrabilních systémů - rozlišují se jednoduše řečeno podle struktury fázového prostoru. Pro integrabilní systém je pohyb ve fázovém prostoru možný pouze na tzv. invariantním toru (s kanonickými souřadnicemi akce-úhel). Malým narušením se tato varieta změní - v dostatečně hrubém měřítku jeví jako torus, nicméně při bližším pohledu je struktura narušena. Pro tvrdý chaos (silná porucha v hamiltoniánu) je struktura původního toru zcela roztržena.

Zajímavým tvrzením z oblasti měkkého chaosu je tzv. KAM teorém (Kolmogorov - Arnold - Moser). Ten říká, že při malé odchylce se struktura invariantních torů do určité míry zachovává, tj. že existují "ostrůvky stability" určitých počátečních podmínek, kde se pohyb odehrává téměř jako v nenarušeném případě.

Nejznámějším příkladem chaotického systému je *problém tří těles*. Tento problém, který nemá analytické řešení, podrobně prostudoval již Henri Poincaré ([1]) a právě díky němu celá teorie chaosu vznikla. Podrobně se tomuto problému věnuje mnoho literatury, např. [2]. Pokud je jedno těleso výrazně malé (a tedy je lze brát jako poruchu úlohy dvou těles), existují trajektorie blízké Keplerovým orbitám. Pro velké poruchy (podobně hmotná tělesa) existuje velmi málo stabilních trajektorií (uzavřených v omezené oblasti fázového prostoru), sebemenší odchylka od nich obvykle vede k vymrštění jednoho z těles do nekonečna.

Dalšími známými příklady chaotického chování kromě problému tří těles a počasí jsou: Brownův pohyb, mechanika sluneční soustavy, turbulence v proudění kapalin, vývoj v ekonomii, populaci... Každopádně co se týče otázky determinismu chaosu - pokud bychom znali přesně počáteční podmínky, je možno určit přesně vývoj systému. Bohužel sebemenší neznámá odchylka díky vlastnosti 2.1.1 naruší systém nepředvídatelným způsobem.

2.2 Základy kvantové fyziky

Hilbert space is a big space.

— Carlton Caves

Kvantová fyzika se od klasické liší v mnohém. Nutné je především se oprostít od slova "jistota" a do slovníku zařadit slovo "pravděpodobnost". Tato kapitola čerpá především z [7], detailnější informace lze najít právě tam.

Každému fyzikálnímu systému je přiřazen abstraktní Hilbertův prostor, tzv. stavový prostor $\mathcal{H}$. Konkrétní stav Ψ systému je určen jednorozměrným paprskem v $\mathcal{H}$, který obvykle reprezentujeme libovolným jednotkovým vektorem ψ v tomto paprsku, tyto vektory označíme v tzv. braketovém formalismu $|\psi\rangle$. Prvky duálního prostoru $\mathcal{H}^*$ označujeme $\langle\varphi|$, skalární součin dvou vektorů φ, ψ značíme $\langle\varphi|\psi\rangle$. Kvadrát velikosti skalárního součinu dvou vektorů $|\langle\varphi|\psi\rangle|^2$ má význam pravděpodobnosti přechodu, tj. pravděpodobnosti, že $|\varphi\rangle$ při měření přejde na stav $|\psi\rangle$. Díky existenci skalárního součinu můžeme hledat ortonormální bázi $\mathcal{H}$, označíme ji $\{|\phi_i\rangle\}_{i=1}^n$, kde n je dimenze $\mathcal{H}$ (může být i nekonečná, ale v této práci tomu tak nebude). Libovolný stav $|\psi\rangle$, lze vyjádřit rovností:

$$|\psi\rangle = \sum_i \langle\psi|\phi_i\rangle |\phi_i\rangle \stackrel{\text{ozn.}}{=} \sum_i c_i |\phi_i\rangle \quad (2.1)$$

Tato rovnost říká, že pravděpodobnosti přechodu $|\psi\rangle$ na $|\phi_i\rangle$ jsou $p_i = |c_i|^2$. Koeficienty c_i se nazývají Fourierovy a platí pro ně $\sum_i c_i^2 = 1$.

Ačkoliv stavový prostor je analogií fázovému prostoru klasické mechaniky, neexistuje v něm nic jako fázové trajektorie. Na místo toho si můžeme představit, že stavový vektor (= vlnová funkce) vytváří "oblak pravděpodobnosti" ve fázovém prostoru, který určuje nalezení částice v daném místě s danou hybností.

Pozorovatelná v klasickém světě je ve světě kvantovém reprezentována samosdruženým operátorem $A = A^+$ na $\mathcal{H}$, každému samosdruženému operátoru jednoznačně odpovídá tzv. rozklad jednotky $\{E_t^A\}_{t \in \mathbb{R}}$, tj. množina projektorů s vlastností $\langle\psi|A\varphi\rangle = \int t d\langle\psi|E_t^A\varphi\rangle$. Možnými výsledky měření jsou body ze spektra A . Díky samosdruženosti lze (dle očekávání) naměřit pouze reálné hodnoty. Pravděpodobnost naměření hodnoty v $(a, b) \subset \mathbb{R}$ pozorovatelné A na stavu $|\psi\rangle$ je rovna $p = \int_a^b 1 d\langle\psi|E_t^A\varphi\rangle$. Střední hodnota veličiny A na stavu $|\psi\rangle$ je rovna $\langle A \rangle_\psi = \langle\psi|A\psi\rangle$.

Důležitým a překvapivým vztahem kvantové fyziky jsou *relace neurčitosti*. Ty korelují vztah mezi směřodatnými odchylkami dvou pozorovatelných A_1, A_2 měřených na stavu $|\psi\rangle$:

$$(\Delta A_1)_\psi (\Delta A_2)_\psi \geq \frac{1}{2} \langle\psi| i[A_1, A_2] \psi\rangle \quad (2.2)$$

Tyto relace nedovolují, aby dvě nekomutující veličiny byly zároveň přesně změřeny. Známým případem jsou Heisenbergovy relace, což jsou relace neurčitosti pro operátory polohy a hybnosti, kdy 2.2 přechází na

$$(\Delta Q)_\psi (\Delta P)_\psi \geq \frac{\hbar}{2} \quad (2.3)$$

Důsledkem relací neurčitosti je to, že v kvantové fyzice nelze kopírovat stavy. Pokud by to bylo možné, mohli bychom neustálým kopírováním a měřením obejít relace neurčitosti. Nic ovšem nebrání tomu, aby např. v Stern-Gerlachově aparátu vyráběly stále stejné stavy.

Stavům, které byly dosud posány, se říká *čisté*, jelikož se dají vyjádřit jako vektor z $\mathcal{H}$. Může se ovšem stát, že o systému budeme vědět pouze pravděpodobnosti, že se nachází v tom kterém stavu. Takový případ, kdy stav je vlastně statistickým souborem čistých stavů, nazýváme *smíšený stav* a k jeho popisu se zavádí *matice hustoty*. Pro konečněrozměrný systém má tvar $\rho = \sum_i p_i |\phi_i\rangle \langle \phi_i|$, platí samozřejmě, že $\text{Tr}(\rho) = 1$. Pravděpodobnost, že na systému ve stavu ρ naměříme hodnotu A v intervalu (a, b) je rovna $p = \text{Tr}(E_{(a,b)}^A \rho)$, je-li výsledek kladný, po měření je systém popsán stavem $\rho' = \frac{E_{(a,b)}^A \rho E_{(a,b)}^A}{\text{Tr}(E_{(a,b)}^A \rho)}$, kde $E_{(a,b)}^A = E_b^A - E_a^A$.

Střední hodnota veličiny A je určena vztahem $\langle A \rangle_\rho = \text{Tr}(A\rho)$.

Je-li $\mathcal{H}_1$ s bazí $\{|\phi_i^1\rangle\}_{i=1}^n$ stavovým prostorem jednoho systému a $\mathcal{H}_2$ s bazí $\{|\phi_j^2\rangle\}_{j=1}^m$ stavovým prostorem druhého systému, pak společný systém je tenzorový součin $\mathcal{H}_1 \otimes \mathcal{H}_2$. Báze tohoto systému je např. $\{|\phi_i^1\rangle \otimes |\phi_j^2\rangle\}_{i,j}$.

Příkladem kvantového systému může být foton. Jeho polarizace může být vertikální, nebo horizontální. Stav fotonu z hlediska polarizace je tedy popsán vektorem z prostoru $\mathcal{H} = \mathbb{C}^2$. Označíme-li bazické vektory $|\uparrow\rangle, |\rightarrow\rangle$, pak je libovolný čistý stav popsán

$$|\psi\rangle = \alpha |\uparrow\rangle + \beta |\rightarrow\rangle, \quad (2.4)$$

kde koeficienty splňují normalizační podmínku

$$|\alpha|^2 + |\beta|^2 = 1 \quad (2.5)$$

Smíšeným stavem je např. foton nepolarizovaného světla. Ten je rovnocennou kombinací bazických vektorů, má tedy matici hustoty

$$\rho = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}.$$

Buďte nyní dva dva světelné svazky, jeden s vertikální, druhý s horizontální polarizací. Pokud z prvního svazku odebereme dva fotony, určitě na obou naměříme $\uparrow\uparrow$, vezmeme-li dva fotony z druhého svazku, určitě na nich naměříme $\rightarrow\rightarrow$. Pokud ovšem necháme oba svazky spojit a z výsledného svazku odebereme dva fotony, můžeme na nich se stejnými pravděpodobnostmi naměřit $\uparrow\uparrow, \uparrow\rightarrow, \rightarrow\uparrow, \rightarrow\rightarrow$, dostali jsme tedy stav $|\psi\rangle = \frac{1}{2}(|\uparrow\uparrow\rangle + |\uparrow\rightarrow\rangle + |\rightarrow\uparrow\rangle + |\rightarrow\rightarrow\rangle)$. Pokud na tento stav uplatníme speciální operátor (konkrétně $H \otimes H$, kde H je popsáno v 2.12), dostaneme stav $|\psi_1\rangle = |\uparrow\uparrow\rangle$. Pokud na tento stav uplatníme ještě další operátor (konkrétně $X \otimes X$ dle 2.11), dostaneme $|\psi_2\rangle = |\rightarrow\rightarrow\rangle$. Vyrobením a smícháním stavů $|\psi_1\rangle, |\psi_2\rangle$ získáme stav

$$|\Phi^+\rangle = \frac{|\uparrow\uparrow\rangle + |\rightarrow\rightarrow\rangle}{\sqrt{2}}, \quad (2.6)$$

analogicky lze vyrobit stavy

$$|\Phi^-\rangle = \frac{|\uparrow\uparrow\rangle - |\rightarrow\rightarrow\rangle}{\sqrt{2}}, \quad (2.7)$$

$$|\Psi^+\rangle = \frac{|\uparrow\rightarrow\rangle + |\rightarrow\uparrow\rangle}{\sqrt{2}}, \quad (2.8)$$

$$|\Psi^-\rangle = \frac{|\uparrow\rightarrow\rangle - |\rightarrow\uparrow\rangle}{\sqrt{2}}. \quad (2.9)$$

Stavy 2.6 - 2.9 nazýváme *Bellovy stavy*, nebo EPR páry. Mají speciální vlastnost, a to, že oba fotony jsou *provázané*. Matematicky to znamená, že stav nelze vyjádřit jako tenzorový součin dvou podstavů. V praxi to znamená, že takové fotony nejsou na sobě nezávislé, ale jeden zároveň nese informaci o druhém. Mějme stav 2.6 a změřme první z fotonů. Pokud dostaneme výsledek $\uparrow$, je jisté, že měřením druhého fotonu bychom dostali též $\uparrow$. Změřením prvního fotonu v podstatě dojde ke kolapsu vlnové funkce druhého fotonu $\frac{|\uparrow\rangle + |\rightarrow\rangle}{2} \xrightarrow{\text{měření}} \begin{cases} |\uparrow\rangle \\ |\rightarrow\rangle \end{cases}$. Kvantové provázání je demonstrací jisté nelokálnosti kvantové teorie, neboť změříme-li jeden z provázaných fotonů, dojde ke kolapsu vlnové funkce druhého fotonu okamžitě nezávisle na jeho poloze (tj. informace o změření jednoho fotonu dává informaci o druhém fotonu okamžitě, toho se využívá v kvantové teleportaci, [4]). Tento okamžitý přenos informace se zdál nejprve paradoxní, neboť porušuje kauzalitu v teorii relativity, kde se každá informace přenáší maximálně rychlostí světla. Einstein, Podolsky a Rosen tímto paradoxem chtěli kdysi vyvrátit konzistenci kvantové teorie a podpořit teorii skrytých proměnných. Nicméně později bylo dokázáno, že teorie skrytých proměnných nemůže platit, že skutečně EPR paradox je příkladem silné statistické provázanosti kvantových systémů (silnější než v případě teorie skrytých proměnných). Zasloužil se o to John Bell. Vztahy, které odvodil, se proto po něm jmenují *Bellovy nerovnosti*.

2.3 Kvantová informace

Kvantová teorie našla uplatnění i v analogii ke klasické informatice. Kvantová informatika slibuje podstatně rychlejší řešení některých problémů, v současnosti jde o velmi rozvíjenou oblast fyziky, současný stav poznání je ale shrnut snad v jediné obsáhlejší knize - [4]. Z té především čerpá tato kapitola.

Základním pojmem teorie informace je bit. Jde o nejmenší jednotku informace, nabývá právě dvou možných hodnot. Představuje např. dvojice ano/ne, +/-, zapnuto/vypnuto nejběžnější ovšem je reprezentace dvojkovou soustavou, tj. hodnotami 1/0. V teorii informace a výpočetních systémů se každá informace charakterizuje konečným počtem bitů, tj. charakterizuje se konečným počtem otázek ano/ne, zapisuje se ve dvojkové soustavě.

Kvantovým analogem klasického bitu je kvantový bit, zvaný zkráceně **qubit**. Ten rovněž jako klasický bit nabývá dvou stavů 1, 0. Navíc ale nabývá rovněž všech superpozic těchto stavů. Qubit má tedy tvar 2.4 spolu s podmínkou 3.3. Odteď ovšem budeme bazické vektory značit pro analogii ke klasickému bitu $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Tato báze je význačná z toho důvodu, že je ortonormální a hodnoty z měření čistých stavů $|0\rangle, |1\rangle$ označíme 0, 1, tedy analogicky ke klasickému bitu. Báze systému dvou qubitů má tvar.

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad (2.10)$$

Qubit může být realizován např. atomem se dvěma možnými hladinami excitace, fotonem se dvěma polarizacemi, spinem v elektronu...

Definovat lze i tzv. *qudit*, což je vícerozměrná analogie qubitů. Reprezentován může být např. atomem s více hladinami excitace. Místo dvojkové soustavy u quditu vystupují soustavy $\mathbb{Z} \bmod n$.

V kvantovém výpočetním systému jsou kvantové bity (v analogii ke klasické informaci) přenášeny kvantovým analogem spojů a zpracovávány kvantovými logickými *branami*. Jejich úkolem je stejně jako v klasickém případě měnit na základě vstupu vloženou informaci. Např. klasická NOT brána mění bit 1 na 0 a opačně 0 na 1. Kvantově analogická NOT brána funguje následovně: $\alpha|1\rangle + \beta|0\rangle \rightarrow \alpha|0\rangle + \beta|1\rangle$. Tato operace je skutečně lineární a má spávné vlastnosti, v maticovém zápisu má jako operátor tvar

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \quad (2.11)$$

Důležitou jednoqubitovou branou je Hadamardova brána

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (2.12)$$

která mění bazické qubity na Bellovy stavy. Zajímavá je následující vlastnost:

Věta 2.3.1. *Postačující podmínkou pro to, aby matice $\in \mathbb{C}^{2,2}$ představovala platnou jednoqubitovou kvantovou bránu, je unitarita.*

Z vícequbitových bran jmenujme např. CNOT (controlled-not) bránu

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad (2.13)$$

která první qubit bere jako kontrolní a podle jeho hodnoty nemění, nebo mění hodnotu qubitů druhého. Dvouqubitové stavy jsou významné díky vlastnosti:

Věta 2.3.2. *Dvouqubitové stavy jsou univerzální, tj. s jejich pomocí lze simulovat jakýkoliv systém. Množina $\{CNOT, \text{jednoqubitové brány}\}$ je univerzální, tj. používáním výhradně jejích prvků lze vytvořit libovolnou logickou bránu.*

Podstatnou vadou kvantových výpočtů je, že nelze jako v klasickém případě kopírovat qubity.

Necht' Alice má jeden z Bellových stavů, např. 2.6. Alice si nechá jednu částici z páru a druhou pošle Bobovi. Pokud by chtěla vědět, v jakém stavu je Bobova částice, stačí jí k tomu změřit svou částici. Toto je princip kvantové teleportace. Namísto toho, aby Bob změřil svoji částici a klasickou cestou poslal výsledky svých měření, dostane se k Alici informace okamžitě.

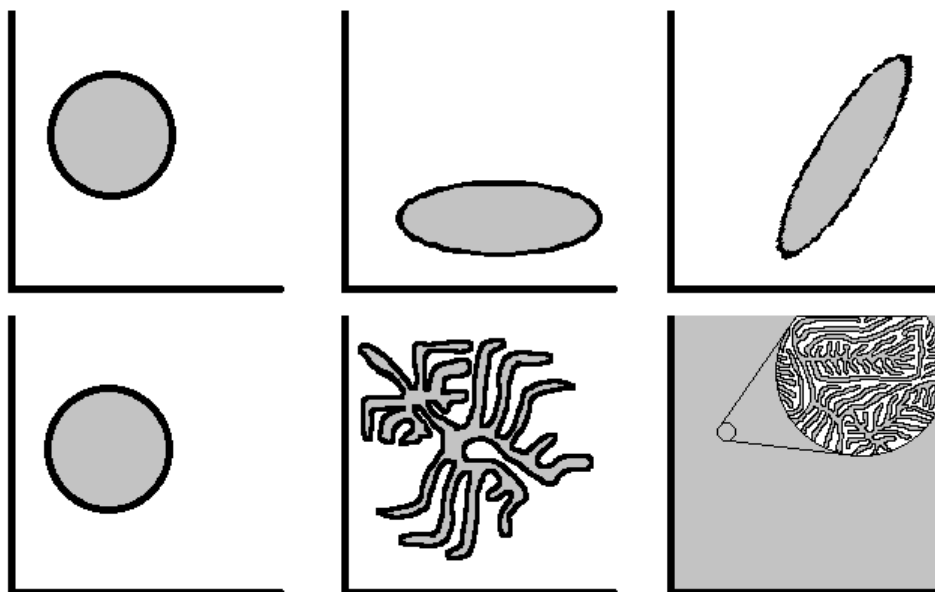
Bellovy stavy umožňují přenášet neznámý stav (nikoliv kopírovat): Pokud by Alice chtěla Bobovi poslat jí zcela neznámý qubit $|\psi\rangle$, ale směla by mu poskytnout pouze klasickou informaci, bez Bellových stavů by si neporadila. Pokud ovšem zkombinuje neznámý qubit se svou EPR částicí, výsledek měření obou částic pošle Bobovi a ten na základě Aliciných výsledků provede určité operace na své EPR částici, dostane přesně stav $|\psi\rangle$. Podrobný rozpis algoritmu je v [4, str. 26-28]. Provázané stavy umožňují i další "triky", které mohou mít ohromné uplatnění v praxi. Jde např. o šifrování v kvantové kryptografii, superhusté kódování, atp.

Kvantová fyzika může mít uplatnění ve výpočetních systémech i tím, že zmenší zdroje potřebné k výpočtům. Příkladem je hledání prvočíselného rozkladu čísla. To je úloha v klasickém případě s exponenciální složitostí. V kvantovém případě vágně řečeno vydělíme dané číslo všemi čísly najednou a pak už jen měříme výsledky. Úloha se tak stává jen polynomicky náročnou.

2.4 Problematika chaosu v kvantové teorii

Jak již bylo řečeno v kapitole 2.1, fázové trajektorie se mohou v klasické mechanice exponenciálně rozcházet i pro nepatrný rozdíl počátečních podmínek. Blízko sebe trajektorie zůstávají pouze pro integrabilní systémy. Chaotické systémy jsou charakteristické tím, že zvolená malá kulička bodů ve fázovém prostoru se v čase rozvíjí velmi neuspořádaně a tvoří rozmanité obrazce. Samozřejmě zůstává v platnosti Liouvilleův teorém. Znázorněna je situace na obrázku 2.1. Prvním problémem, který ovšem v kvantové fyzice vyvstává, je, že neexistuje nic jako trajektorie ve fázovém prostoru. Heisenbergovy relace 2.3 říkají, že čím přesněji známe polohu, tím méně známe hybnost a naopak. Z tohoto hlediska tedy chaos v kvantové fyzice hledat nelze.

Dalším problémem je, že kvantová fyzika definovaná v sekci 2.2 je lineární teorie. Veškeré pozorovatelné jsou samosdružené lineární operátory. Pokud tedy máme dva blízké stavy, a necháme je vyvíjet v čase, zůstanou blízké v každém okamžiku. Neexistuje zde nic jako citlivost na počáteční podmínky. Tedy zde neexistuje v mikroměřítku nic, co chápeme jako chaos v klasickém světě.



Obrázek 2.1: Vývoj množiny bodů ve fázovém prostoru -
nahore integrabilní systém, dole chaotický.

Dalším argumentem nepříznivým pro chaos v kvantové fyzice je ten, že v klasickém smyslu chaos impikuje neperiodičnost charakteristických proměnných. V kvantové fyzice jsou základem hladiny energie, které v důsledku umožňují pouze pohyb s přesně definovanými frekvencemi. V časovém vývoji tedy existuje mechanismus, který potlačuje chaotické chování. Mohli bychom vyslovit myšlenku, že pro velké objekty, jako třeba planety a asteroidy, bude toto potlačování velmi pomalé, ale pro Hyperion (Saturnův měsíc s chaotickým obíháním mateřské planety) by to mělo být jen několik desetiletí. To je v rozporu s pozorováním.

Naproti "principu potlačování chaosu" ovšem působí dekoherence. Tímto slovem je označen efekt, kdy (i obrovský) kvantový systém citlivě reaguje na nekontrolovatelné vnější vlivy. Např. i svazek slunečních fotonů, který se od Hyperionu musel odrazit, abychom jej mohli pozorovat, ovlivnil jeho chování. Zato objekt typu atom je možno mnohem lépe izolovat, proto u něj chaos nepozorujeme.

Shrňme dosud, co jsme zjistili o vztahu chaos - kvantová teorie: V kvantové fyzice jako takové není místo pro exponenciální citlivost k počátečním podmínkám, a tedy chaos. V klasickém světě existují dynamické systémy s chaotickým chováním. Musíme proto vyžadovat dle principu korespondence existenci kvantových systémů, jejichž klasická limita dá chtěný chaotický systém. Studium této problematiky se obvykle zachycuje právě slovním spojením *kvantový chaos*. Konkrétně v kvantové chaologii jde tedy o studování vztahů mezi klasickým chaosem a kvantovou fyzikou, tj. aplikace principu korespondence, aplikace poruchové teorie s

velkými poruchami, statistické zpracování např. teorie náhodných Hamiltoniánů atd. Jedním ze způsobů, jak se v kvantové teorii uplatní chaos, je v otevřených systémech, kdy do chování studovaného systému zasahuje jeho okolí.

V této práci budeme chaosem myslet zejména chaotickou dynamiku vývoje jednoqubitového, nebo dvouqubitového systému. Tím myslíme vývoj především koeficientů lineární kombinace bazických vektorů, když je qubit podroben působení nějakých operátorů. Všechny brány z předchozí sekce jsou lineární, zdá se, že tedy není co studovat. Odpověď na otázku, kde tedy v takovém systému je chaos, je však překvapivě jednoduchá. Stačí qubit změřit. Měření představuje netriviální a především nelineární proces. A právě nelinearita může v dynamice qubitů vyvolat chaotické chování ve smyslu 2.1.2. Myšlenka, že měřením lze cíleně ovlivnit stav systému je poměrně mladá, nicméně posledních letech je intenzivně rozvíjena [8–11].

Experimentálně není možné vyrobit přesně čistý stav, např. Bellův. Jsme schopni vyrobit stavy blízké, ale ne plně provázané. Proto je typickou vlastností, kterou se snažíme měřením ovlivnit, právě provázanost. Mechanismus, který se snaží aplikovat nelineární procesy (prostřednictvím měření) na systém s cílem záměrně zvýšit provázanost systému, se nazývá *purifikační protokol*. Jejím cílem je zvýšit (purifikovat) provázanost stavu, aby jej bylo možné použít např. v kvantové teleportaci.

2.5 Purifikace

Je nutné rozlišit dva matoucí pojmy - purifikaci stavů a purifikaci provázanosti. Oproti purifikaci provázání, tj. úpravě stavu za účelem zvýšení provázanosti, lze purifikaci stavu matematicky definovat následovně:

Definice 2.5.1. *Bud' ρ_A stav kvantového systému A . Potom lze zavést systém B a definovat čistý stav $|\psi\rangle$ složeného systému $A \otimes B$ takový, že $\rho_A = \text{Tr}_B(|\psi\rangle\langle\psi|)$. Stav $|\psi\rangle$ je purifikací ρ_A .*

Poznámka 2.5.1. *Libovolný stav je purifikací změněn na čistý stav, ale většího systému. Systém B může být ryze virtuální, bez přímého fyzikálního významu. Purifikace může být provedena na libovolném stavu, důkaz viz [4][str. 109-111].*

V této práci se touto purifikací nebudeme zabývat, purifikaci provázání je důležité zkoumat pro využití v kvantové informatice. Purifikace provázanosti stavů je potřeba zejména z toho důvodu, že při přenášení stavu komunikačním kanálem dochází k dekoherenci stavu, stav je narušován všeobecným šumem. Ten roste s délkou kanálu. Z toho důvodu je potřeba po určitých úsecích stav opět vyčistit.

Prakticky purifikační protokoly spočívají v iterativní aplikaci nelineární operace na systém qubitů. Purifikačních protokolů již existuje mnoho a různé protokoly mohou být různě účinné na různé skupiny stavů. Příklady konkrétních

purifikačních protokolů a jejich využití lze nalézt např. v [12–14]. Purifikačnímu protokolu je třeba dodat soustavu qubitů rozdělenou na kontrolní a cílové. Na kontrolních qubitech se v jedné iteraci provede měření a podle výsledků se aplikují operace na cílových qubitech. Kontrolní qubity jsou již ”poškozené” měřením, proto se zahodí. S každou iterací tak dochází k (exponenciálnímu) zmenšování systému qubitů, k dosažení dobré provázanosti je tedy třeba velkého množství výchozích qubitů.

Experiment, tj. měření využívané v kvantové purifikaci, a teoretický protokol jsou dvě rozdílné věci. Realizace měření může být velmi komplikovaná. A i když teoreticky probíhají protokoly velmi dobře, praktický průběh vzhledem k nevyhnutelným nedokonalostem není tak úspěšný.

Nyní se věnujme konkrétnímu purifikačnímu protokolu, který bude rozebírán v této práci. Detailně je v obecném případě definován v [15], jeho aplikace v [16, 17]. Spočívá v používání logické brány XOR. To je brána, která se aplikuje na kontrolní a cílový qubit následovně: pokud kontrolní qubit nabývá hodnoty 0, cílový qubit zůstává nezměněn. V případě, že je na kontrolním qubitě naměřena hodnota 1, je na cílový qubit aplikována brána X z 2.11, tj. je prohozena báze. Kontrolní qubit je zahozen (pokud bychom nezahodili kontrolní qubit, šlo by o operaci CNOT v 2.13). Tuto operaci lze zapsat jako

$$\text{XOR } |i\rangle |j\rangle = |i\rangle |i \oplus j\rangle, \quad i, j \in \{0, 1\}, \quad (2.14)$$

kde $\oplus$ značí sčítání modulo dvěma. V článku [15] je tato brána zobecněna na systém více quditů, je označena GXOR a na dva qubity působí následovně:

$$\text{GXOR } |i\rangle |j\rangle = |i\rangle |i \ominus j\rangle, \quad i, j \in \{0, 1\}, \quad (2.15)$$

kde $\ominus$ značí odčítání modulo dvěma. Pro případ quditů jde v XOR/GXOR o sčítání/odčítání modulo d , kde d je dimenze quditu.

Konkrétní působení na cílový obecný qudit je detailně rozebráno v práci [15], zde pro stručnost zapíšeme výsledek. Je-li vstupní kontrolní i cílový stav stejný¹ (ozn. ρ), nejdůležitější částí operace je

$$\rho = \begin{pmatrix} \rho_{11} & \rho_{12} & \cdots & \rho_{1n} \\ \rho_{21} & \rho_{22} & \cdots & \rho_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{n1} & \rho_{n2} & \cdots & \rho_{nn} \end{pmatrix} \xrightarrow{\text{purifikace}} \rho \odot \rho = \begin{pmatrix} \rho_{11}^2 & \rho_{12}^2 & \cdots & \rho_{1n}^2 \\ \rho_{21}^2 & \rho_{22}^2 & \cdots & \rho_{2n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \rho_{n1}^2 & \rho_{n2}^2 & \cdots & \rho_{nn}^2 \end{pmatrix} \quad (2.16)$$

při označení Hadamardova součinu symbolem $\odot$. Toto ”umocnění” matice hustoty je nelineární operace a výsledkem je matice s nejednotkovou stopou, proto je nutno ji normalizovat. Operátor působící $\rho \rightarrow \frac{\rho \odot \rho}{\text{Tr}(\rho \odot \rho)}$ označíme S . Aplikaci S lze ještě doplnit působením dalšího již unitárního operátoru. Aplikace (takového

¹Tak tomu u purifikačních protokolů obvykle bývá.

tzv. local twirling operátoru, viz [15]) je dokonce nutná, aby purifikace konvergovala k žádanému čistému stavu. Lze použít různé operátory, každý bude dávat jiný výsledek co se týče chování protokolu. V této práci bude dodatečným operátorem $H \otimes H$, kde H je Hadamardova brána 2.12.

V tomto výzkumném úkolu budeme protokol aplikovat výhradně na dvouqubitové systémy, a to na čisté stavy tvaru (až na normalizaci)

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \quad (2.17)$$

které se změní na

$$|\psi'\rangle = a^2|00\rangle + b^2|01\rangle + c^2|10\rangle + d^2|11\rangle. \quad (2.18)$$

Celkově tedy jedna iterace protokolu působí takto: Kontrolním i cílovým systémem je stejná dvojice qubitů. Dle stavu kontrolního qubitů je cílový qubit upraven, což má za následek 2.17 $\rightarrow$ 2.18. Dále je tento stav upraven operátorem lokální operaci představované branou $H \otimes H$. Tím je vytvořena nová množina stavů (dvojic qubitů), která se rozdělí opět na kontrolní a cílové.

Článek [17] nalézá stavy $|00\rangle, \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ jakožto výsledky purifikačního protokolu aplikovaného na stavy $\frac{1}{N(z)}(|00\rangle + z|11\rangle)$. Protokol převádí první nalezený stav na druhý a naopak. V závislosti na počtu opakování protokolu se obecný stav přiblíží jednomu z těchto limitních případů. Dle parity tak lze rozložit počáteční stavy na konvergující po dané iteraci ke stavu $|00\rangle$ a na konvergující ke stavu $\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$. Hranice těchto dvou množin má tvar fraktálu a naznačuje chaotické chování systému podrobeného zmíněnému purifikačnímu protokolu.

2.6 Teorie funkcí jedné komplexní proměnné

Aplikace purifikačních protokolů je z matematického hlediska diskrétním a opakovaným působením jistého nelineárního operátoru. Pro účely klasické fyziky byl již na začátku minulého století vyvinut velmi silný nástroj pro studium chování iterovaných komplexních funkcí. Bohužel pro svoji komplikovanost je tato teorie dodnes rozpracována dobře pouze pro dimenzi 1, viz např. [3], pro více komplexních proměnných se situace výrazně komplikuje. Některé poznatky pro vícerozměrné případy lze nalézt např. v publikaci [18].

Pro jisté speciální případy stavů se bude působení purifikačního protokolu redukovat právě na řešení chování funkce jedné komplexní proměnné, proto je zde této teorii věnováno místo. Dobré je začít specifikací prostoru, na kterém bude funkce působit, vždy se vyžaduje tzv. *Riemannova plocha*. V této práci budeme automaticky vyžadovat jednoduchou souvislost, protože typicky půjde o složku jednotkového vektoru.

Teorém 2.6.1 (Uniformizační teorém). *Každá jednoduše souvislá Riemannova plocha je konformně izomorfní (tj. existuje homomorfismus variet holomorfní i s inverzem) jedné z následujících variet:*

1. tělesu komplexních čísel $\mathbb{C}$,
2. jednotkovém kruhu $\mathbb{D} = \{z = x + iy \in \mathbb{C} | x^2 + y^2 < 1\}$,
3. Riemannově sféře $\hat{\mathbb{C}} = \mathbb{C} \cup \infty$.

Poznámka 2.6.1. *Pro obecný případ bez jednoduché souvislosti platí tvrzení, že libovolná Riemannova plocha je konformně izomorfní faktorvarietě $S = \tilde{S}/\Gamma$, kde $\tilde{S}$ je již jednoduše souvislá Riemannova plocha a Γ je diskrétní grupa konformních automorfismů taková, že každý její nejednotkový element nemá pevný bod.*

V této práci bude Riemannovou varietou obvykle $\hat{\mathbb{C}}$. Co se týče funkcí, budeme uvažovat výhradně racionální lomené funkce, tj. funkce tvaru $f(z) = P(z)/Q(z)$, kde P, Q jsou polynomy.

Definice 2.6.1. *Stupněm funkce $f(z) = P(z)/Q(z)$ rozumíme maximum stupňů polynomů P, Q .*

Definice 2.6.2 (normální soubor funkcí). *Bud'te X, Y Riemannovy plochy, $\mathcal{A}$ množina spojitých zobrazení $X \rightarrow Y$. $\mathcal{A}$ je normální soubor funkcí, pokud z libovolné posloupnosti funkcí $f \in \mathcal{A}$ lze vybrat posloupnost lokálně uniformně konvergující ke spojitému zobrazení $X \rightarrow Y$.*

Poznámka 2.6.2. *Přechází a některé další věty lze zobecnit z Riemannových ploch na úplné metrické prostory.*

Poznámka 2.6.3 (k notaci). *n -tou iteraci funkce f budeme značit jednoduše $f^n(x) = f(f(\dots(f(x))\dots))$.*

Definice 2.6.3 (Fatouovy a Juliovy množiny). *Bud' $f : S \rightarrow S$ nekonstantní holomorfní zobrazení Riemannovy plochy S . Pro pevně zvolený bod z_0 nastává právě jedna ze dvou možností:*

1. *Existuje U okolí z_0 takové, že f^n/U tvoří normální soubor funkcí. Pak říkáme, že z_0 je normální/regulární bod, reps. že patří do Fatouovy množiny funkce f , ozn. $\mathcal{F}(f)$.*
2. *Pokud takové okolí U neexistuje, řekneme, že z_0 je z Juliovy množiny $\mathcal{J}(f)$.*

Juliova množina je kruciálním pojmem teorie funkce jedné komplexní proměnné (tj. nadále $\text{Dom}(f) = \hat{\mathbb{C}}$). Má mnoho zajímavých vlastností (např. soběpodobnost, pro kterou jsou tyto množiny známé). Podstatnější jsou ovšem následující vlastnosti:

Lemma 2.6.1. *Juliova množina je plně invariantní, tj. $f^n(\mathcal{J}(f)) = \mathcal{J}(f)$ pro $\forall n \in \mathbb{Z}$.*

Důsledek 2.6.1. *Jelikož $\mathcal{F}(f) \cup \mathcal{J}(f) = \mathbb{C}$, platí stejné tvrzení i pro $\mathcal{F}(f)$.*

Lemma 2.6.2. *Je-li f stupně alespoň 2, pak Juliova množina je neprázdná a uzavřená. Navíc nemá izolované body.*

Definice 2.6.4. *Orbita bodu z je posloupnost jeho dopředných obrazů, tj. $\{z, f(z), f^2(z), \dots\}$.*

Definice 2.6.5. *Vlastnost platí pro generický bod $x \in \mathcal{M}$, pokud platí pro všechny body spočetného průniku nějakého systému hustých podmnožin množiny $\mathcal{M}$.*

Věta 2.6.1. *Pro každé $z_0 \in \mathcal{J}(f)$ platí, že množina jeho vzorů je všude hustá v $\mathcal{J}(f)$, tj. $\{z | (\exists n \in \mathbb{N}_0)(f^n(z) = z_0)\} = \mathcal{J}(f)$.*

Věta 2.6.2. *Pro generické $z_0 \in \mathcal{J}(f)$ platí, že jeho orbita je všude hustá v $\mathcal{J}(f)$, tj. $\{z | (\exists n \in \mathbb{N}_0)(f^n(z_0) = z)\} = \mathcal{J}(f)$.*

Lemma 2.6.3. *Má-li Juliova množina vnitřní bod, pak $\mathcal{J}(f) = \hat{\mathbb{C}}$.*

Definice 2.6.6. *Pokud $\exists n \in \mathbb{N}$ takové, že $f^n(z) = z$ a $f^k(z) \neq z$ pro $\forall k \in \{1, \dots, n-1\}$, pak orbitu z nazveme periodickou, krátce též jen cyklus. Číslo n nazýváme délka periody. Číslo $\lambda = (f^n)'(z)$ nazýváme multiplikátorem cyklu.*

Definice 2.6.7. *Cyklus, jehož multiplikátor je*

1. $\lambda = 0$ nazveme *superpřitažlivým*,
2. $0 < |\lambda| < 1$ nazveme *přitažlivým*,
3. $|\lambda| = 1$ nazveme *neutrálním*,
4. $|\lambda| > 1$ nazveme *odpudivým*.

*Cyklus, pro nějž $\lambda = 1$ a zároveň funkce f^n není identita (tzn. $\lambda = e^{i\varphi}$, $\varphi \in \mathbb{R} \setminus \mathbb{Q}$), nazveme *parabolický*.*

Poznámka 2.6.4. *Tyto termíny jsou zavedeny intuitivně: Při malé poruše od přitažlivého cyklu se k němu s iteracemi narušená orbita přibližuje. Při sebemenší poruše odpudivého cyklu dochází k oddalování narušené a nenarušené orbity. Neutrální orbita nemá ani jednu tuto vlastnost. Narušená a nenarušená orbita se vyvíjejí blízko sebe, nedochází ani k limitnímu přibližování ani oddalování orbit.*

Definice 2.6.8. *K přitažlivému cyklu existuje neprázdná otevřená množina bodů, jejichž orbita se v limitě blíží k nějakému bodu cyklu. Tuto množinu nazýváme oblast přitažlivosti, Ω . Každému bodu $z \in \mathcal{F}(f)$ lze přiřadit jednu komponentu souvislosti Ω_z nějaké oblasti přitažlivosti, že $z \in \Omega_z$. Tuto komponentu nazýváme přímá oblast přitažlivosti.*

Teorém 2.6.2. *Každý přitažlivý cyklus je obsažen ve Fatouově množině, každý odpudivý a parabolický cyklus je obsažen v Juliově množině. Oblast přitažlivosti libovolného přitažlivého cyklu Ω je celá obsažena ve $\mathcal{F}(f)$, ale její hranice $\partial\Omega$ již je částí $\mathcal{J}(f)$. Dokonce topologická hranice oblasti přitažlivosti pro libovolný cyklus je rovna celé $\mathcal{J}(f)$.*

Věta 2.6.3. *Pro racionální lomenou funkci stupně $d \geq 2$ existuje nejvýše $2d - 2$ cyklů, které jsou přitažlivé, nebo parabolické. Cyklů, které nejsou odpudivé, je konečný počet.*

Dle [3][str. 82] lze při studování chování Fatouovy množiny využít tzv. kritické body:

Definice 2.6.9. *Bod, v kterém vymizí derivace funkce, tj. $f'(z) = 0$, nazveme kritický.*

Věta 2.6.4. *Bud' f racionální lomená funkce stupně ≥ 2 , potom každá přímá oblast přitažlivosti obsahuje alespoň jeden kritický bod.*

Tento aparát dává k dispozici snadnou metodu, jak rozhodnout o dynamice zadaného systému. Jde-li o funkci jedné proměnné, nalezením kritických bodů lze určit atraktivní cykly, ty jsou dle 2.6.3 nejvýše dva pro funkci stupně 2. Hranice oblastí přitažlivosti je dle 2.6.2 Juliova množina, ta je neprázdná pro funkci stupně alespoň 2, 2.6.2. Takto ji ale nelze dobře určit. Pokud nalezneme parabolický či odpudivý cyklus, ten je částí Juliovy množiny 2.6.2, pokud takové cykly nenalezneme, je třeba najít alespoň nějaké body Juliovy množiny. Celá Juliova množina se díky 2.6.1 dá v dobrém přiblížení rychle nalézt iterováním inverzní funkce v těchto bodech (jeden bod má obvykle více vzorů).

Kapitola 3

Praktická část

3.1 Základní vlastnosti daného nelineárního operátoru

V 2.5 byl definován operátor S , který je hlavní částí purifikačního protokolu [15]. Uvažujme jeho iterativní působení na stav ρ . Díky normalizování stavu v každém kroku a vlastnosti $x^2 \leq x$ pro $x \leq 1$ dojde k tomu, že menší diagonální prvky matice vymizí, zatímco největší prvek půjde k 1. Tím je dosaženo čistého stavu. Výjimkou je případ matice se všemi diagonálními prvky rovnými, ta je pevným bodem operátoru S . Při sebemenší odchylce však již stav konverguje k nějakému čistému.

Situace se komplikuje po uplatnění další operace. V této práci jde o

$$H_2 = H \otimes H = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \quad (3.1)$$

a tento operátor se aplikuje hned po S . Jedna iterace purifikačního protokolu je tedy $U = H_2 \circ S$ a působí na čistý stav následovně:

$$U \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = k \begin{pmatrix} a^2 + b^2 + c^2 + d^2 \\ a^2 - b^2 + c^2 - d^2 \\ a^2 + b^2 - c^2 - d^2 \\ a^2 - b^2 - c^2 + d^2 \end{pmatrix}, \quad (3.2)$$

kde vektor na levé straně splňuje normalizační podmínku

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1 \quad (3.3)$$

a k je normalizační konstanta. Druhá iterace purifikačního protokolu již dává

$$U^2 \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = k \begin{pmatrix} a^4 + b^4 + c^4 + d^4 \\ 2(a^2b^2 + c^2d^2) \\ 2(a^2c^2 + b^2d^2) \\ 2(a^2d^2 + b^2c^2) \end{pmatrix}. \quad (3.4)$$

S každou další iterací se výsledný vektor výrazně komplikuje (složky vektoru po třetí iteraci mají 23 členů osmého řádu atd.).

Nadále budeme značit

$$\vec{v} \stackrel{\text{ozn.}}{=} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \quad (3.5)$$

$\vec{x}' = U\vec{x}$. Dle [7] je zvykem stav kvantového systému reprezentovat jednotkovým vektorem z daného paprsku. To jednak znamená, že stav $|\psi\rangle$ určuje stejný stav, jako $e^{i\varphi}|\psi\rangle$. Navíc se ale lze oprostít i od normalizace, jelikož normalizační faktor (není-li nekonečný či nulový) je jen číslo, na fyzikální stav nemá vliv. Proto nebudeme v dalším textu vyžadovat splnění normalizační podmínky 3.3 a ani nás nebude zajímat normalizační konstanta k výsledného vektoru. Naopak výhodné bude zvolit reprezentační vektor stavu $\vec{v}$ tak, že jedna z jeho složek je rovna 1. Toho lze vždy dosáhnout, neboť nulový vektor není předmětem fyzikálního zájmu. Při takto zvolené "normalizaci" je ovšem třeba mít na paměti, že působení obecného operátoru A na libovolný vektor $|\psi\rangle$ generující stav Ψ dá nějaký vektor ze stavu $A\Psi$. Speciálně pro $A^n\Psi = \Psi$ jde o úlohu hledání vlastních vektorů a čísel operátoru A^n .

Funkce zobrazující $a \rightarrow a^2 + b^2 + c^2 + d^2, b \rightarrow \dots$ budou předmětem zkoumání této práce. I po "normalizaci", tj. zvolení jedné ze složek a, b, c, d rovné jedné, zůstává působení operátoru U ekvivalentní vektorové komplexní funkci 3 proměnných. Tato oblast není stále dostatečně dobře prozkoumána z hlediska dynamiky (problematicke se věnuje např. [18] proto se v dalším textu nevěnujeme obecným případům).

Jde-li o samotý operátor S , účinkuje jako kvadrát složek vektoru. To ovšem znamená, že

$$S \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = S \begin{pmatrix} -a \\ b \\ c \\ d \end{pmatrix} = S \begin{pmatrix} a \\ -b \\ c \\ d \end{pmatrix} = S \begin{pmatrix} -a \\ -b \\ c \\ d \end{pmatrix} = \dots \quad (3.6)$$

V důsledku lze u každého nalezeného řešení libovolně násobit jednotlivé složky konstantou -1 a výsledné vektory budou opět hledanými řešeními. Z prostorových důvodů nebudeme explicitně vypisovat takováto řešení.

3.2 Pevné body purifikačního protokolu

První důležitou charakteristikou jsou pevné body, tj. nalezneme nyní vektory splňující

$$U\vec{v} = \vec{v}. \quad (3.7)$$

Tato rovnice tedy znamená, že hledáme řešení rovnic

$$k \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a^2 + b^2 + c^2 + d^2 \\ a^2 - b^2 + c^2 - d^2 \\ a^2 + b^2 - c^2 - d^2 \\ a^2 - b^2 - c^2 + d^2 \end{pmatrix}. \quad (3.8)$$

Tuto soustavu lze rozdělit na dva případy - buď $a = 0$, což dává

$$k \begin{pmatrix} 0 \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} b^2 + c^2 + d^2 \\ b^2 + c^2 - d^2 \\ b^2 - c^2 - d^2 \\ b^2 - c^2 + d^2 \end{pmatrix} \quad (3.9)$$

(tento případ je vhodné dále normalizovat), nebo lze provést "normalizaci" na $a = 1$, přičemž dostáváme soustavu

$$k \begin{pmatrix} 1 \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 + b^2 + c^2 + d^2 \\ 1 - b^2 + c^2 - d^2 \\ 1 + b^2 - c^2 - d^2 \\ 1 - b^2 - c^2 + d^2 \end{pmatrix}. \quad (3.10)$$

Na tomto místě je vhodné připomenout, že jelikož nejde o lineární rovnice, je třeba dbát maximální opatrnosti při úpravě rovnic. Předně nelze jen tak bezmyšlenkovitě rovnice sčítat a dosazovat jednu do druhé. Je třeba dodržovat logické implikace a jakékoliv řešení zpětně kontrolovat. Rovněž je vhodné připomenout, že řešení s $k = 0, k = \infty$ nebereme v úvahu, proto je možné číslem k dělit.

Řešit přímo 3.10 či 3.9 "ručně" je prakticky nemožné. Zjednodušíme tedy řešení následujícími speciálními situacemi:

- $a = d = 1, b = c$

Nenulové řešení upravené soustavy 3.10

$$k \begin{pmatrix} 1 \\ b \\ b \\ 1 \end{pmatrix} = \begin{pmatrix} 2 + 2b^2 \\ 0 \\ 0 \\ 2 - 2b^2 \end{pmatrix} \quad (3.11)$$

existuje jediné, a to $b=0$, tedy

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \quad (3.12)$$

- $a = 1, b = c = d$

Už od pohledu na výsledek v 3.10 je vidět, že první složka vektoru je výjimečná. V ní se všechny mocniny sčítají, zatímco u ostatních složek se různým způsobem odečítají. Odečítání je ovšem tak vhodné, že, jsou-li poslední tři složky $\vec{v}$ stejné, jsou stejné i poslední tři složky $U\vec{v}$. Tudíž můžeme očekávat, že nalezneme nějaké řešení. Po zjednodušení dostáváme soustavu rovnic

$$k \begin{pmatrix} 1 \\ b \end{pmatrix} = \begin{pmatrix} 1 + 3b^2 \\ 1 - b^2 \end{pmatrix} \sim \begin{pmatrix} 1 \\ \frac{1-b^2}{1+3b^2} \end{pmatrix}. \quad (3.13)$$

Po eliminaci k docházíme k tomu, že řešením jsou kořeny rovnice

$$3b^3 + b^2 + b - 1 = 0. \quad (3.14)$$

Řešení této rovnice lze nalézt explicitně, snadno např. na [19]. Jde o tři kořeny, v numerickém přiblížení vypadají následovně:

$$\left. \begin{aligned} b_1 &= 0.46939642457, \\ b_2 &= -0.40136 - 0.74097i, \\ b_3 &= -0.40136 + 0.74097i. \end{aligned} \right\} \quad (3.15)$$

Přesvědčme se, že řešení pro b_1 skutečně je pevným bodem S .

$$\begin{aligned} H_2 S \vec{v} &= H_2 S \begin{pmatrix} 1 \\ 0.46939642457 \\ 0.46939642457 \\ 0.46939642457 \end{pmatrix} = H_2 \begin{pmatrix} 1 \\ 0.2203330034 \\ 0.2203330034 \\ 0.2203330034 \end{pmatrix} = \\ &= \begin{pmatrix} 1.660990102 \\ 0.7796669966 \\ 0.7796669966 \\ 0.7796669966 \end{pmatrix} \doteq 1.661 \vec{v} \end{aligned} \quad (3.16)$$

Analogicky se lze přesvědčit o tom, že i b_2, b_3 určují pevné body.

- $a = 0 = d$

V tomto případě přechází soustava 3.9 na

$$k \begin{pmatrix} 0 \\ b \\ c \\ 0 \end{pmatrix} = \begin{pmatrix} b^2 + c^2 \\ b^2 + c^2 \\ b^2 - c^2 \\ b^2 - c^2 \end{pmatrix}, \quad (3.17)$$

která má jediné řešení, a to nezajímavý nulový vektor.

- $a = 0 \neq d$

V tomto případě lze soustavu 3.9 přepsat na:

$$k \begin{pmatrix} 0 \\ b \\ c \\ 1 \end{pmatrix} = \begin{pmatrix} b^2 + c^2 + 1 \\ b^2 + c^2 - 1 \\ b^2 - c^2 - 1 \\ b^2 - c^2 + 1 \end{pmatrix}. \quad (3.18)$$

Platí-li pro b, c první a poslední rovnice, pak platí, že

$$k = 2,$$

navíc z druhé a třetí rovnice plyne

$$kb = -kc - 2.$$

Potom se ovšem soustava redukuje na:

$$\begin{aligned} b + c &= -1 \\ 2b &= -b^2 + c^2 - 1 \\ 2c &= -c^2 + b^2 - 1 \end{aligned} \quad (3.19)$$

a tuto soustavu lze snadno vyřešit dosazením první rovnice např. do druhé (díky symetrii proměnných). Dostáváme rovnici

$$b^2 + b + 1 = 0, \quad (3.20)$$

jejím vyřešením dostáváme tedy výsledky

$$\begin{aligned} b_1 &= \frac{-1+i\sqrt{3}}{2}, & c_1 &= \frac{-1-i\sqrt{3}}{2} \\ b_2 &= \frac{-1-i\sqrt{3}}{2}, & c_2 &= \frac{-1+i\sqrt{3}}{2} \end{aligned} \quad (3.21)$$

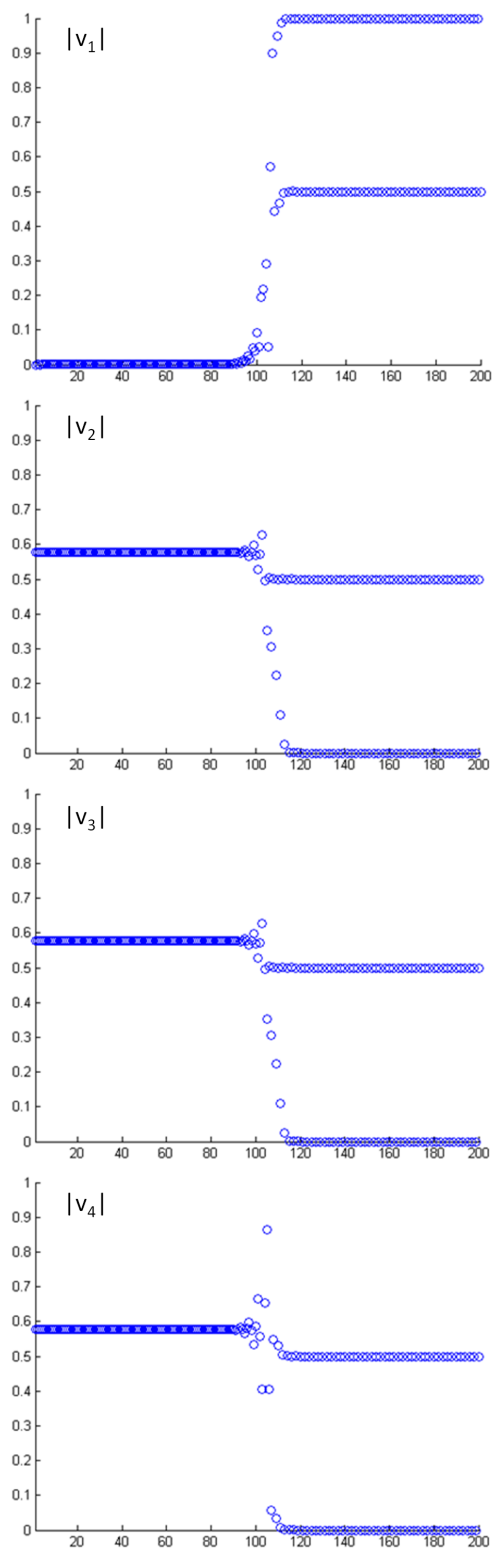
Snadno se lze přesvědčit, že vektory

$$\begin{pmatrix} 0 \\ \frac{-1+i\sqrt{3}}{2} \\ \frac{-1-i\sqrt{3}}{2} \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ \frac{-1-i\sqrt{3}}{2} \\ \frac{-1+i\sqrt{3}}{2} \\ 1 \end{pmatrix} \quad (3.22)$$

skutečně jsou pevnými body operátoru U . Zároveň ale nejsou přitažlivé, viz obr. 3.1. Chyba způsobená pouze zaokrouhlováním v prostředí MATLAB (řádu cca 10^{-15}) způsobí konvergenci stavu od tohoto pevného bodu ke stabilnímu řešení.

- ...

Lze hledat řešení s dalšími speciálními podmínkami, např. $a = 1 \neq d, b = c$. Tato řešení jsou ovšem už také složitá, proto budou zahrnuta v následujícím.



Obrázek 3.1: Popořadě vývoj složek prvního z vektorů 3.22 při opakování purifikačního protokolu. Labilita řešení způsobí přechod k 3.32. Vyneseny: na ose x počet iterací, na ose y absolutní hodnota složky.

Nyní přistoupíme k **obecnému řešení**. Rovnice 3.10, 3.9 byly vyřešeny prostřednictvím webových stránek [19]. Druhá soustava nemá nenulové řešení. Zato první soustava má 13 řešení, u kterých lze poskytnout přesný analytický tvar, ten je ale velmi komplikovaný. Konkrétní hodnoty lze přesně určené najít na webových stránkách http://www.wolframalpha.com/input/?i=a%3D1%2Bb%5E2%2Bc%5E2%2Bd%5E2%2Ca*b%3D1-b%5E2%2Bc%5E2-d%5E2%2Ca*c%3D1%2Bb%5E2-c%5E2-d%5E2%2Ca*d%3D1-b%5E2-c%5E2%2Bd%5E2 , numerické přiblížení výsledků je:

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0.543689 \\ 0.543689 \\ 0.295598 \end{pmatrix}, \begin{pmatrix} 1 \\ 0.469396 \\ 0.469396 \\ 0.469396 \end{pmatrix}, \quad (3.23)$$

$$\left\{ \begin{pmatrix} 1 \\ -0.771845 + 1.11514i \\ 0.543689 \\ -0.419643 + 0.606291i \end{pmatrix}, \begin{pmatrix} 1 \\ -0.771845 - 1.11514i \\ 0.543689 \\ -0.419643 - 0.606291i \end{pmatrix}, \begin{pmatrix} 1 \\ 0.543689 \\ -0.771845 + 1.11514i \\ -0.419643 + 0.606291i \end{pmatrix}, \begin{pmatrix} 1 \\ 0.543689 \\ -0.771845 - 1.11514i \\ -0.419643 - 0.606291i \end{pmatrix} \right\} \quad (3.24)$$

$$\begin{pmatrix} 1 \\ -0.771845 - 1.11514i \\ -0.771845 + 1.11514i \\ 1.83929 \end{pmatrix}, \begin{pmatrix} 1 \\ -0.771845 + 1.11514i \\ -0.771845 - 1.11514i \\ 1.83929 \end{pmatrix}, \quad (3.25)$$

$$\begin{pmatrix} 1 \\ -0.771845 + 1.11514i \\ -0.771845 + 1.11514i \\ -0.647799 - 1.72143i \end{pmatrix}, \begin{pmatrix} 1 \\ -0.771845 - 1.11514i \\ -0.771845 - 1.11514i \\ -0.647799 + 1.72143i \end{pmatrix}, \quad (3.26)$$

$$\begin{pmatrix} 1 \\ -0.401365 + 0.740971i \\ -0.401365 + 0.740971i \\ -0.401365 + 0.740971i \end{pmatrix}, \begin{pmatrix} 1 \\ -0.401365 - 0.740971i \\ -0.401365 - 0.740971i \\ -0.401365 - 0.740971i \end{pmatrix}. \quad (3.27)$$

Je zřejmé, že kromě již nalezených řešení v 3.23 a 3.27, bychom velkou část řešení našli řešením rovnic 3.10 s podmínkou $a = 1 \neq d, b = c$. Tato úloha je však též obtížná a neposkytla by řešení 3.24.

Pevnými body operátoru U jsou stavy určené vektory
3.22 a 3.23 - 3.27.

3.3 Stav s krátkou periodou

Hledání stavů s periodou délky 2, tj. pevných bodů operátoru U^2 , vyžaduje dle 3.4 řešit soustavu

$$k \begin{pmatrix} 1 \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 + b^4 + c^4 + d^4 \\ 2(b^2 + c^2 d^2) \\ 2(c^2 + b^2 d^2) \\ 2(d^2 + b^2 c^2) \end{pmatrix}, \quad (3.28)$$

respektive soustavu

$$k \begin{pmatrix} 0 \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} b^4 + c^4 + d^4 \\ 2c^2 d^2 \\ 2b^2 d^2 \\ 2b^2 c^2 \end{pmatrix}. \quad (3.29)$$

Řešení soustavy 3.29 lze rozdělit na případy

- $d = 0$

Potom soustava nemá nenulové řešení.

- $d \neq 0$

Potom soustava přechází na

$$k \begin{pmatrix} 0 \\ b \\ c \\ 1 \end{pmatrix} = \begin{pmatrix} b^4 + c^4 + 1 \\ 2c^2 \\ 2b^2 \\ 2b^2 c^2 \end{pmatrix}. \quad (3.30)$$

Tato soustava rovnic má samozřejmě za řešení vektory 3.22, žádná další řešení neexistují.

Řešení soustavy 3.28 je příliš složité, nalezneme tedy jen zjednodušené případy:

- $a = d$

Dostáváme soustavu

$$k \begin{pmatrix} 1 \\ b \\ c \\ 1 \end{pmatrix} = \begin{pmatrix} 2 + b^4 + c^4 \\ 2(b^2 + c^2) \\ 2(b^2 + c^2) \\ 2(1 + b^2 c^2) \end{pmatrix}, \quad (3.31)$$

z níž zjevně (díky nenulovosti k) plyne $b = c$. Kromě již získaného pevného bodu 3.12, jsou nyní pevné body (tj. periody délky 2) ještě důležitý 2-cyklus

$$\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \rightarrow \dots \quad (3.32)$$

a stavy dané numericky (analytické řešení opět viz [19]):

$$\begin{pmatrix} 1 \\ 0.54369 \\ 0.54369 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ -0.77184 \pm 1.11514i \\ -0.77184 \pm 1.11514i \\ 1 \end{pmatrix} \quad (3.33)$$

- $a = 1, d = 0$

V tomto případě ze soustavy

$$k \begin{pmatrix} 1 \\ b \\ c \\ 0 \end{pmatrix} = \begin{pmatrix} 1 + b^4 + c^4 \\ 2b^2 \\ 2c^2 \\ 2b^2c^2 \end{pmatrix} \quad (3.34)$$

plynou dvě řešení, která jsou součástí jednoho 2-cyklu:

$$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \rightarrow \dots \quad (3.35)$$

Ze soustav rovnic pro cyklus délky 3 byly nalezeny vzhledem ke složitosti úlohy pouze řešení odpovídající pevným bodům.

3.4 Speciální skupiny stavů

Zkoumejme nyní obecněji invariantní množiny stavů: $U(\mathcal{M}) \subset \mathcal{M}$. Vyjdeme ze skupin vektorů, jejichž jedna složka je nulová.

$$A = \left\{ \begin{pmatrix} 0 \\ b \\ c \\ d \end{pmatrix} \middle| b, c, d \in \mathbb{C} \right\}, B = \left\{ \begin{pmatrix} a \\ 0 \\ c \\ d \end{pmatrix} \middle| a, c, d \in \mathbb{C} \right\}, \dots \quad (3.36)$$

- skupina A

Hledáme množinu stavů $\mathcal{A}$ (podmnožinu A), uzavřenou na iterace. Z toho lze určit podmínky

$$\begin{pmatrix} 0 \\ b \\ c \\ d \end{pmatrix} \rightarrow \begin{pmatrix} b^2 + c^2 + d^2 \\ -b^2 + c^2 - d^2 \\ b^2 - c^2 - d^2 \\ -b^2 - c^2 + d^2 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 \\ c^2 \\ b^2 \\ d^2 \end{pmatrix} \rightarrow \begin{pmatrix} b^4 + c^4 + d^4 \\ 2b^4 \\ 2c^4 \\ 2d^4 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 \\ b^4 \\ c^4 \\ d^4 \end{pmatrix} \rightarrow \dots \quad (3.37)$$

To celkově implikuje podmínku, že

$$\mathcal{A} = \left\{ \begin{pmatrix} 0 \\ b \\ c \\ d \end{pmatrix} \middle| \forall k \in \mathbb{N} : b^{2^k} + c^{2^k} + d^{2^k} = 0 \right\}. \quad (3.38)$$

Je-li $d = 0$, podmínku nelze splnit. Pro $d \neq 0$ lze poslední složku normalizovat k jedné a k velkému překvapení existují dvě řešení splňující nekonečně mnoho podmínek v 3.38. Řešením jsou ale pouze pevné stavy 3.22. Určili jsme tímto, že nemohou existovat delší cykly v A, než 3.22. Navíc analogický postup pro $U^k A \in A$ výrazně omezuje existenci cyklů s delší periodou.

- skupina B

Analogickou úvahou lze dojít k množině

$$\mathcal{B} = \left\{ \begin{pmatrix} a \\ 0 \\ c \\ d \end{pmatrix} \middle| \forall k \in \mathbb{N} : (-1)^{k+1} a^{2^k} + c^{2^k} + (-1)^k d^{2^k} = 0 \right\}. \quad (3.39)$$

Nyní ovšem naopak neexistuje řešení pro $c \neq 0$. V opačném případě existuje jedno řešení, a to pouze 3.12.

- skupina C

Stejně jako v předchozím bodě

$$\mathcal{C} = \left\{ \begin{pmatrix} a \\ b \\ 0 \\ d \end{pmatrix} \middle| \forall k \in \mathbb{N} : (-1)^{k+1} a^{2^k} + b^{2^k} + (-1)^k d^{2^k} = 0 \right\}. \quad (3.40)$$

Opět existuje jediné řešení, tvaru 3.12.

- skupina D

Podmínka pro

$$\mathcal{D} = \left\{ \begin{pmatrix} a \\ b \\ 0 \\ d \end{pmatrix} \middle| \forall k \in \mathbb{N} : a^{2^k} + b^{2^k} + c^{2^k} = 0 \right\}. \quad (3.41)$$

jako v bodě A neumožňuje řešení s $a = 0$. V opačném případě lze volit $a = 1$ a každá iterace znamená

$$a \rightarrow a^2, b \rightarrow c^2, c \rightarrow b^2.$$

To s podmínkou

$$b^{2^k} + c^{2^k} = 1, \forall k \in \mathbb{N}$$

dává pouze dvě možná řešení - cyklus 3.35.

Nyní studujme zajímavé skupiny stavů inspirované soustavami 3.13 a 3.35.

$$\mathcal{E} = \left\{ \left(\begin{pmatrix} 1 \\ z \\ z \\ z \end{pmatrix} \right) \middle| z \in \mathbb{C} \right\}, \quad (3.42)$$

$$\mathcal{F}_1 = \left\{ \left(\begin{pmatrix} 1 \\ z \\ z \\ 1 \end{pmatrix} \right) \middle| z \in \mathbb{C} \right\}, \mathcal{F}_2 = \left\{ \left(\begin{pmatrix} 1 \\ z \\ 1 \\ z \end{pmatrix} \right) \middle| z \in \mathbb{C} \right\}, \mathcal{F}_3 = \left\{ \left(\begin{pmatrix} 1 \\ 1 \\ z \\ z \end{pmatrix} \right) \middle| z \in \mathbb{C} \right\}, \quad (3.43)$$

$$\mathcal{G}_1 = \left\{ \left(\begin{pmatrix} 1 \\ z \\ 0 \\ 0 \end{pmatrix} \right) \middle| z \in \mathbb{C} \right\}, \mathcal{G}_2 = \left\{ \left(\begin{pmatrix} 1 \\ 0 \\ z \\ 0 \end{pmatrix} \right) \middle| z \in \mathbb{C} \right\}, \mathcal{G}_3 = \left\{ \left(\begin{pmatrix} 1 \\ 0 \\ 0 \\ z \end{pmatrix} \right) \middle| z \in \mathbb{C} \right\}. \quad (3.44)$$

Bud'te $\begin{pmatrix} 1 \\ z \\ z \\ z \end{pmatrix} = \vec{u} \in \mathcal{E}$, $\begin{pmatrix} 1 \\ z \\ z \\ 1 \end{pmatrix} = \vec{v}_1 \in \mathcal{F}_1, \dots$, $\begin{pmatrix} 1 \\ z \\ 0 \\ 0 \end{pmatrix} = \vec{w}_1 \in \mathcal{G}_1, \dots$. Potom

$$U\vec{u} \rightarrow \begin{pmatrix} 1 \\ p \\ p \\ p \end{pmatrix}, \quad (3.45)$$

$$U^2\vec{v}_1 \rightarrow \begin{pmatrix} 1 \\ q \\ q \\ 1 \end{pmatrix}, U^2\vec{v}_2 \rightarrow \begin{pmatrix} 1 \\ q \\ 1 \\ q \end{pmatrix}, U^2\vec{v}_3 \rightarrow \begin{pmatrix} 1 \\ 1 \\ q \\ q \end{pmatrix}, \quad (3.46)$$

$$U^2\vec{w}_1 \rightarrow \begin{pmatrix} 1 \\ q \\ 0 \\ 0 \end{pmatrix}, U^2\vec{w}_2 \rightarrow \begin{pmatrix} 1 \\ 0 \\ q \\ 0 \end{pmatrix}, U^2\vec{w}_3 \rightarrow \begin{pmatrix} 1 \\ 0 \\ 0 \\ q \end{pmatrix}, \quad (3.47)$$

kde

$$p = \frac{1 - z^2}{1 + 3z^2} \text{ a } q = \frac{2z^2}{1 + z^4}. \quad (3.48)$$

Pro množiny $\mathcal{F}_i, \mathcal{G}_i$ tedy platí $U^2(\mathcal{F}_i) \subset \mathcal{F}_i, U^2(\mathcal{G}_i) \subset \mathcal{G}_i$ podléhají po každé sudé iteraci chování stejnému, jak případ rozebíraný v [17]. Mimoto platí:

$$U\mathcal{G}_i = \mathcal{F}_{i+1}, U\mathcal{F}_i = \mathcal{G}_{i-1}$$

Proto se budeme v posledním odstavci především věnovat studiu chování stavů v množině $\mathcal{E}$.

3.5 Juliovy a Fatouovy množiny speciálních případů

Shrňme zde výsledky pro $\mathcal{F}_i, \mathcal{G}_i$ jen stručně. Systém je charakterizován funkcí

$$g(z) = \frac{2z^2}{1+z^4} = f(f(z)), \text{ kde } f(z) = \frac{1-z^2}{1+z^2}. \quad (3.49)$$

Existuje jeden stabilní superpřitažlivý cyklus $\{0, 1\}$. Podle toho, zda stav dosáhne tohoto cyklu v sudém, či lichém počtu iterací f , rizpadá se $\mathcal{F}(f)$ na dvě disjunktní množiny. Jejich hranicí je $\mathcal{J}(f)$ s komplikovanou strukturou, viz [17].

Rozebereme nyní případ množiny $\mathcal{E}$. Stavů v ní podléhají chování určenému funkcí

$$f(z) = \frac{1-z^2}{1+3z^2}, \quad (3.50)$$

dynamickým systémem je tedy dvojice $(f, \hat{\mathbb{C}})$.

Pevné body funkce byly nalezeny již v 3.15 Jsou to:

$$\left. \begin{aligned} z_1 &= \frac{1}{9} \left(-1 - \sqrt[3]{\frac{256}{67+9\sqrt{57}}} + \sqrt[3]{2(67+9\sqrt{57})} \right) \doteq 0.469396424569995 \\ z_2 &\doteq -0.401364878951664 - 0.740971015312481i \\ z_3 &\doteq -0.401364878951664 + 0.740971015312481i \end{aligned} \right\} \quad (3.51)$$

Body z_1, z_2, z_3 jsou nestabilní, viz obr 3.1, proto jsou prvkem $\mathcal{J}(f)$. V předchozím odstavci jsme rovněž našli cyklus 3.32, jehož prvky jsou v $\mathcal{E}$.

Derivace f má tvar

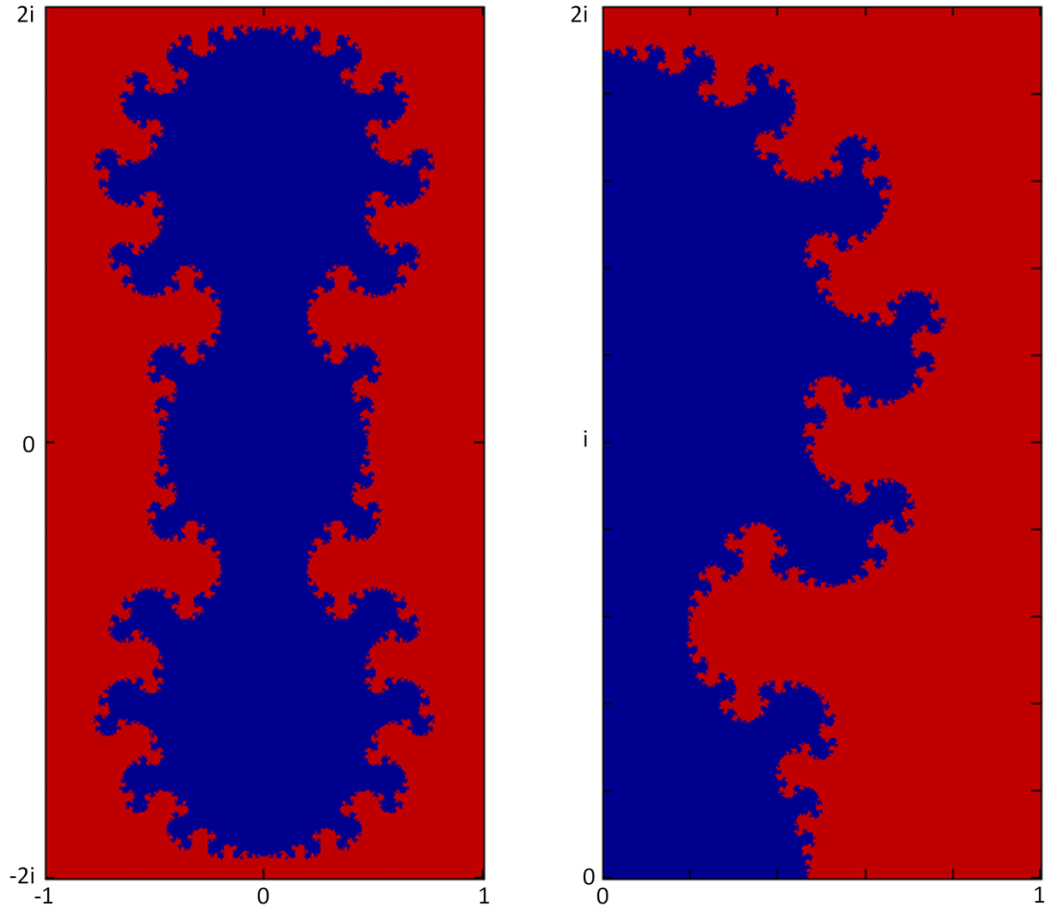
$$f'(z) = \frac{-8z}{(1+3z^2)^2}, \quad (3.52)$$

a proto jsou kritickými body:

$$z_{c_1} = 0, z_{c_2} = \infty. \quad (3.53)$$

Jelikož $z_{c_1} = 0$ je součástí cyklu 3.32, jde o cyklus superpřitažlivý. Druhý bod dává posloupnost bodů konvergující k stejnému cyklu, až na paritu iterací:

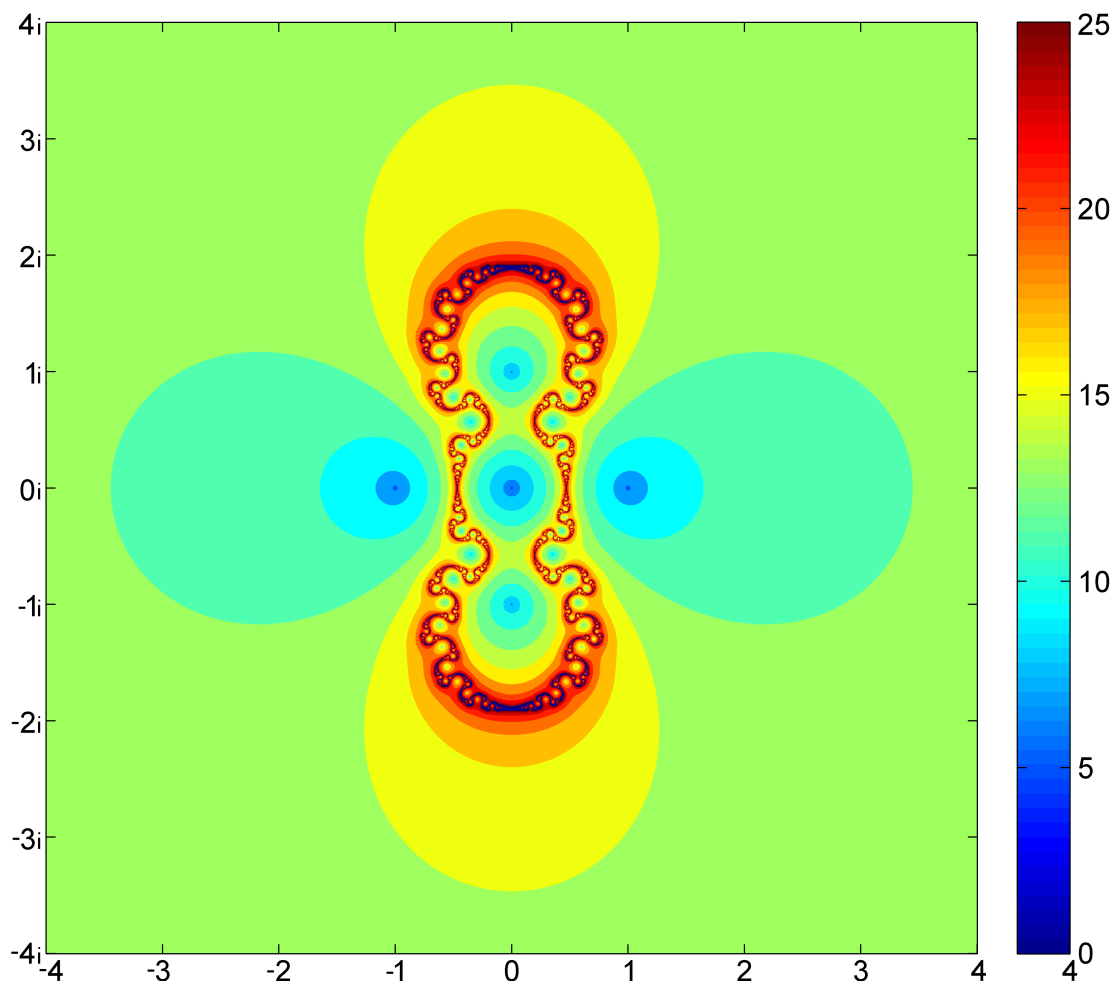
$$f^{2k}(z_{c_2}) \xrightarrow{k \rightarrow \infty} 1, f^{2k+1}(z_{c_2}) \xrightarrow{k \rightarrow \infty} 0.$$



Obrázek 3.2: Fatouova množina funkce 3.50 je rozdělena na dvě komponenty. Jejich hranice tvoří Juliovu množinu. Vlevo oblast $|\Re(z)| < 1, |\Im(z)| < 2$. Vpravo detail - $z \in \langle 0, 1 \rangle \times \langle 0, 2 \rangle i$

Juliova množina má tvar zachycený na obrázku 3.2. Fatouovu množinu lze podobně jako v [17] rozdělit na dva případy podle parity konvergence. V tomto případě situace vypadá následovně: Juliova množina je souvislá a rozděluje $\hat{\mathbb{C}}$ na dvě komponenty souvislosti. Jedna obsahuje ∞ , druhá obsahuje 0. Sjednocení obou komponent představuje oblast přitažlivosti jediného přitažlivého cyklu 3.32.

Komponenta souvislosti obsahující 0 odpovídá stavům, které se blíží k čistému stavu $|00\rangle$ v lichých iteracích operátoru U (3.2), v sudých se blíží kompletně separovanému $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)]$. V komponentě souvislosti obsahující ∞ je tomu naopak.



Obrázek 3.3: Rychlost konvergence bodů $z \in \langle -4, 4 \rangle \times \langle -4, 4 \rangle i$. Barevná škála představuje iteraci, po které bod již jistě dokonverguje.

Dále jsme se přesvědčili o rychlosti konvergence stavů k superpřitažlivému cyklu 3.32. Pro z bud' stanoveno, že po k -tém kroku *jistě dokonverguje* ke stavu $|00\rangle$, pokud dosáhne $z \rightarrow f^k(z) = z', |z'| < 0.0001$. Hodnoty k pro oblast blízko Juliovy množiny jsou zachyceny na obrázku 3.3. Z tohoto obrázku je patrné, že stavy, které jsou Juliově množině blíže, konvergují k přitažlivému cyklu pomaleji. Nicméně lze říci, že po 25 iteracích jsou již stavy dobře purifikované. Pro stavy vhodně vyrobené (již blízko $|00\rangle$) stačí k purifikaci pouze několik iterací.

Kapitola 4

Závěr

V první části práce byly shrnuty základní informace o chaosu a kvantové fyzice. Rozvinuta byla zejména témata kvantové informace a chaosu v kvantové fyzice. Podány byly podstatné definice a základní vlastnosti definovaných objektů.

Vysvětlen byl pojem purifikace jakožto prostředku k úpravě stavů za účelem zvýšení provázanosti. Kvantové provázání je totiž efektem kvantové fyziky, který lze použít ke kvantové teleportaci, superhustému kódování a kompresi dat, v kvantové kryptografii atd.

V posledním odstavci teoretické části byl vytvořen matematický aparát k zacházení s funkcemi jedné komplexní proměnné. Základním objektem této teorie je Juliova množina, jejíž vlastnosti jsou podrobně rozebrány. Celý aparát umožňuje (teoreticky snadno) zjistit chování funkce druhého stupně.

V praktické části byly prezentovány výsledky autorových výpočtů, rozpracováno bylo chování purifikačního problému daleko za rámec článku [17]. Nalezeny byly všechny pevné stavy operátoru 3.2, dále byly prostudovány cykly délky dva. Nalezeny byly zejména důležité cykly 3.22, 3.32, 3.35. Ty slouží jako výsledky purifikačního protokolu [15], resp. [16, 17].

Pevný bod 3.12 znamená, že stav $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$ je pevným bodem, a to dokonce přitažlivým. Blízké stavy se tedy protokolem vyčistí na stav Bellův stav 2.6. To ovšem není překvapivé, to přeci bylo cílem purifikačního protokolu.

Další cykly 3.32 jsou na tom stejně jako v článku [17]. Podle parity iterace se střídají separovaný stav $\frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)]$ a čistý stav $|00\rangle$.

V cyklu 3.35 se dle parity iterace střídají stavy: $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ a $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$. V každém případě se na první částici naměří hodnota 0. I tento cyklus je přitažlivý, ovšem jeho výsledky nejsou vhodné pro účely např. kvantové teleportace.

Poslední nalezené pevné body 3.22 a cykly 3.33 jsou ještě méně vhodné, ale naštěstí nejsou přitažlivé.

Pro speciální množinu stavů 3.42 jsme určili chování stavů v závislosti na výchozím a to díky teorii funkce komplexní proměnné aplikované na funkci 3.50.

Juliova množina je souvislá a rozděluje Fatouovu množinu na dvě komponenty souvislosti, vnější (obsahující kritický bod ∞) konverguje k superpřitažlivému cyklu 3.32, konkrétně ke stavu $|00\rangle$ v lichých iteracích. Prvky druhé komponenty souvislosti (obsahující druhý kritický bod 0) konvergují ke stejnému cyklu, ale ke stavu $|00\rangle$ v sudých iteracích. Rychlost konvergence stavu je obecně tím menší, čím blíže je stav Juliově množině.

Do budoucna je vhodné rozhodnout o existenci zbylých cyklů délky 2 a pokusit se najít cykly delší. K tomu mohou pomoci vlastnosti odvozené v kapitolách 3.3 a 3.4. Též je vhodné, aby bylo prozkoumáno působení purifikačního protokolu na smíšené stavy.

Dále je vhodné detailněji se věnovat vlastnostem Juliovy množiny funkce 3.50. Konkrétně by bylo vhodné dokázat její souvislost, kterou jsme v této práci "dokázali" obrázkem. To by se dalo uskutečnit např. při určování analogu Mandelbrotovy množiny skupiny funkcí

$$f_c(z) = \frac{1 - z^2}{1 + cz^2}.$$

Autor konstatuje, že neexistuje souhrnná práce věnující se purifikačním protokolům. Za nedostatečné považuje i množství publikací o kvantové informaci, kvantovém chaosu a teorii funkcí více komplexních proměnných (v porovnání s teorií funkcí jedné komplexní proměnné). Nemluvě o překladech do českého jazyka, v němž mnoho pojmů ani není zavedeno.

Autor doufá, že tato práce pomůže dalším studentům zorientovat se v problematice.

Literatura

- [1] Poincaré H., *Les Méthodes Nouvelles de la Mécanique Céleste*, (Gauthier-Villars, Paris) (1892)
- [2] Gutzwiller M. C. *Chaos in Classical and Quantum Mechanic*, (Springer-Verlag, New York) (1990)
- [3] Milnor J. W. *Dynamics in One Complex Variable*, 3. vydání (Princeton University Press) (2000)
- [4] Nielsen A. M., Chuang I. L. *Quantum Computation and Quantum Information*, (Cambridge University Press)(2000)
- [5] Einstein A., Podolsky B., Rosen N. *Phys. Rev.* **47**, 777 (1935)
- [6] Vymětal S. *Chaos in the conditional dynamics of purification protocols*, doktorská práce FJFI ČVUT, 2010
- [7] Blank J., Exner P., Havlíček M. *Lineární operátory v kvantové fyzice* (Karolinum) (1993)
- [8] Deutsch D. et al. *Phys. Rev. Lett.* **78**11 (2006)
- [9] Horodecki M., Horodecki P., Horodecki R. *Phys. Rev. Lett.* **78**(1997)
- [10] Bechmann-Pasquinucci H. et. al. *Phys. Lett. A* **242** (1998)
- [11] Hsieh J. Y., Li Ch. M., Chuu D. S. *Phys. Lett. A* **328** (2004)
- [12] Brun A. T., Caves C. M., Schack R. *Phys. Rev. A* **63**, 042309 (2001), arXiv:quant-ph/0010038
- [13] Kleinmann M., Kampermann H., Meyer T., Bruss D. *Phys. Rev. A* **73**, 062309 (2006)
- [14] Song W., Yang M., Cao Z. L. *Phys. Rev. A* **89** (2014)
- [15] Alber G., Delgado A., Gisin N., Jex I. *J. Phys. A: Math. Gen.* **34** (2001) str. 8821-8833

- [16] Kiss T., Jex I., Alber G., Vymětal S. *Phys. Rev. A* **74**, 040301 (2006)
- [17] Kiss T., Vymětal S., Tóth L.D., Gábris A., Jex I., Alber G.
Physical Review Letters **107**, 100501 (2011)
- [18] Fornæs J. E. *Dynamics in several complex variables*,
(Amer. Math. Soc.) (1994)
- [19] webová stránka <http://www.wolframalpha.com> založená na softwaru
Mathematica