VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ

FACULTY OF MECHANICAL ENGINEERING

ÚSTAV MATEMATIKY

INSTITUTE OF MATHEMATICS

KVANTOVÁ TEORIE HER DVOU HRÁČŮ

TWO PERSON QUANTUM GAME THEORY

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — Matěj Krajný

AUTHOR

VEDOUCÍ PRÁCE — doc. Mgr. Jaroslav Hrdina, Ph.D.

SUPERVISOR

BRNO 2022

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA STROJNÍHO INŽENÝRSTVÍ

Zadání bakalářské práce

Ústav:	Ústav matematiky
Student:	**Matěj Krajný**
Studijní program:	Matematické inženýrství
Studijní obor:	bez specializace
Vedoucí práce:	**doc. Mgr. Jaroslav Hrdina, Ph.D.**
Akademický rok:	2021/22

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma bakalářské práce:

Kvantová teorie her dvou hráčů

Stručná charakteristika problematiky úkolu:

Kvantové výpočty v některých algoritmech využívají entaglování kvantových stavů. Z matematického hlediska se jedná o nerozložitelné tenzory příslušného řádu. V kvantové verzi dvou hráčů jsou strategie unitární transformace a hra se odehrává na entaglovaném 2–qubitu. Míra entaglovanosti pak může popisovat vzájemnou důvěru hráčů.

Cíle bakalářské práce:

– Osvojení si základů kvantového počítání a teorie her dvou hráčů.
– Hledání rovnovážných stavů pro standardní hry dvou hráčů při různé míře entaglovanosti.
– Student si zvolí jednu z klasických her dvou hráčů, jako například vězňovo dilema, nebo hra pohlaví, a vytvoří její kvantovou verzi.
– Vypočte rovnovážný stav pro různé míry etaglovanosti a pokusí se kvantifikovat míru důvěry.

Seznam doporučené literatury:

DE LIMA MARQUEZINO, F. et al. A Primer on Quantum Computing, SpringerBriefs in Computer Science, 2019.

OWEN, G. Game Theory, Emerald Group Publishing Limited, Bingley: Emerald, 2013.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2021/22

V Brně, dne

L. S.

prof. RNDr. Josef Šlapal, CSc. ředitel ústavu	doc. Ing. Jaroslav Katolický, Ph.D. děkan fakulty

ABSTRAKT

Práce se věnuje zavedení matematické notace kvantových stavů, následně pak hlubšímu porozumění jejich reprezentace. V práci je uvedeno rozšíření klasické hry dvou hráčů Vězňova dilematu o kvantové strategie. Jsou pozorovány změny rovnovážného stavu hry oproti hře nekvantové.

KLÍČOVÁ SLOVA

kvantový bit, Blochova sféra, entanglement, vězňovo dilema

ABSTRACT

This thesis presents introductuion to mathematical notation of quantum states, furthermore foucuses on deeper understanding of their representation. We broaden a clasical game of two players Prisoners dilema by adding quantum strategies. And we observe changes of equilibrium in comparison to clasical game.

KEYWORDS

quantum bit, Bloch sphere, entanglement, prisoners dilema

Vysázeno pomocí balíčku `thesis` verze 4.07; `http://latex.feec.vutbr.cz`

KRAJNÝ, Matěj. *Kvantová teorie her dvou hráčů*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, Ústav matematiky, 2022, 49 s. Bakalářská práce. Vedoucí práce: doc. Mgr. Jaroslav Hrdina, Ph.D.

Prohlášení autora o původnosti díla

Jméno a příjmení autora:	Matěj Krajný
VUT ID autora:	209410
Typ práce:	Bakalářská práce
Akademický rok:	2021/22
Téma závěrečné práce:	Kvantová teorie her dvou hráčů

Prohlašuji, že svou závěrečnou práci jsem vypracoval samostatně pod vedením vedoucí/ho závěrečné práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené závěrečné práce dále prohlašuji, že v souvislosti s vytvořením této závěrečné práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora*

*Autor podepisuje pouze v tištěné verzi.

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu doc. Mgr.Jaroslav Hrdina Ph.D. za odborné vedení, mnohé konzultace, neutuchající trpělivost a podnětné návrhy k práci.

Obsah

Úvod

V dnešním světě se stále častěji začínají objevovat zmínky o kvantových počítačích. Už v roce 2019 Google publikoval své výsledky na téma kvantové nadřazenosti. Kdy je dána stejná výpočetní úloha kvantovému počítači a velice výkonému klasickému počítači. Google tvrdí, že algoritmus na jejich kvantovém počítači dokončil výsledky za 200 sekund, zatímco odhad trvání výpočtu stejné úlohy by nejrychlejšímu počítači na světě trval přes 10 000 let. Toto tvrzení bylo později zpochybněno firmou IBM, která tvrdí, že po optimalizaci klasického algoritmu, by výpočet trval pouze několik dní. S tím, jaký zájem mají kvantové počítače v prostoru technologických gigantů, je pouze logické očekávat jejich další rozvoj. Není proto od věci zaměřit se na pochopení základů kvantových algoritmů. Na první pohled patrným rozdílem klasického a kvantového algoritmu je jejich způsob práce s informacemi. Zatímco klasický počítač bere v potaz pouze diskrétní hodnoty 1 a 0 chceme-li pravda a nepravda. Kvantový počítač pracuje s celým spektrem hodnot mezi pravdou a nepravdou, a o konkrétním výstupu rozhoduje až finální pozorování. Toto se ve fyzických kvantových počítačích děje, za pomoci částic kvantové fyziky a jejich vlastnosti superpozice. Kdy částice jsou zdánlivě ve více stavech zároveň, a až pozorováním (měřením), dochází ke kolapsu do jednoho ze stavů. Tento fakt reprezentujeme za pomoci konstrukce kvantových bitů 'qubitů' jako prvků komplexních vektorových prostorů, jak uvidíme dále. Stavíme tedy paralely mezi světy: běžné výpočetní techniky, kvantové fyziky a kvantových počítačů.

1 Matematický formalismus

1.1 Zavedení qubitu

Abychom mohli mluvit o teorii her v kvantovém světě, musíme si nejprve stanovit jasný komunikační rámec. O hrách můžeme mluvit jako o algoritmech, a abychom mohli popisovat kvantové algoritmy, musíme nejprve poznat jejich doménu nad kterou pracují tedy data. V tradiční výpočetní technice využíváme k uchování informace takzvané bity. Binární jednotku informace uloženou ve formě 1 nebo 0, chcete-li pravda/nepravda. Ale ty pro popis kvantových stavů nestačí. A proto zavádíme takzvané qubity jako prvky $\mathbb{C}^2$ následovně:

$$\mathcal{Q} := \left\{ \vec{q} = \begin{pmatrix} q_1 \\ q_2 \end{pmatrix}, \;\; q_1, q_2 \in \mathbb{C} \;\; \|\vec{q}\| = 1 \right\},$$

kde $\|\vec{q}\|$ definujeme jako zobrazení z $\mathbb{C}^2$ do $\mathbb{R}$ s následujícím předpisem:

$$\|\cdot\| := \mathbb{C}^2 \to \mathbb{R} \;\; \forall \vec{q} \in \mathbb{C}^2 \;\; : \;\; \|\vec{q}\| = \sqrt{q_1\overline{q_1} + q_2\overline{q_2}},$$

kde $\overline{q}$ je číslo komplexně sdružené.

Tímto jsme si definovali qubit, což je základní informační jednotka, při popisu kvantových algoritmů. Obdobně jako v binární výpočetní technice, máme základní stavy 0 a 1, máme pro tyto stavy obdoby i na qubitech. Vyberme si tedy jednu z mnoha bází $\mathbb{C}^2$, jejíž vektory označíme $\vec{0}$ a $\vec{1}$, a nazvěme ji Kanonickou:

$$\vec{0} = \begin{pmatrix} 1 + 0 \cdot i \\ 0 + 0 \cdot i \end{pmatrix}, \quad \vec{1} = \begin{pmatrix} 0 + 0 \cdot i \\ 1 + 0 \cdot i \end{pmatrix}.$$

Libovolný 1-qubit pak můžeme sestrojit takto:

$$\vec{q} \in \{a \cdot \vec{0} + b \cdot \vec{1} \quad | \quad a, b \in \mathbb{C} \qquad \|a\|^2 + \|b\|^2 = 1\}.$$

Tato báze však není jediná se kterou budeme pracovat. Zmiňme zde proto aspoň některé další, přičemž k jejich podrobnému popisu se dostaneme později. Budeme je nazývat $\pm$ báze a její prvky jsou:

$$\vec{+} = \frac{\sqrt{2}}{2} \cdot \vec{0} + \frac{\sqrt{2}}{2} \cdot \vec{1}, \qquad \vec{-} = \frac{\sqrt{2}}{2} \cdot \vec{0} - \frac{\sqrt{2}}{2} \cdot \vec{1}$$

a $\pm i$ báze s prvky:

$$\vec{+i} = \frac{\sqrt{2}}{2} \cdot \vec{0} + \frac{\sqrt{2}}{2} i \cdot \vec{1}, \qquad \vec{-i} = \frac{\sqrt{2}}{2} \cdot \vec{0} - \frac{\sqrt{2}}{2} i \cdot \vec{1}$$

1.1.1 Diracova notace

Obvykle, pro popisování kvantových stavů používáme Diracova zápisu. Je to jen jiný způsob notace vektoru, který nám ale zápis zpřehlední, a výpočty opticky zjednoduší. Sloupcový vektor a nazýváme 'ket' a zapisujeme následovně:

$$\vec{q} = \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} = |q\rangle.$$

Řádkový vektor nazýváme 'bra' a značíme takto:

$$(p_1, p_2) = \langle p|.$$

Přičemž mějme † zobrazení, mezi prostory 'ket' vektorů a 'bra' vektorů. Takové že platí:

$$\langle p|^\dagger = |q\rangle \quad \Leftrightarrow \quad p_1 = \overline{q_1} \wedge p_2 = \overline{q_2}.$$

Jasně vidíme, že zobrazení výše je pouze transponování vektoru spolu s komplexní konjugací jeho složek. A to ukažme na příkladu:

$$|a\rangle = \vec{a} = \begin{pmatrix} -\frac{\sqrt{3}}{3} + \frac{\sqrt{3}}{3}i \\ 0 - \frac{\sqrt{3}}{3}i \end{pmatrix}, \quad \langle a| = \vec{a}^{\,\dagger} = \left(-\frac{\sqrt{3}}{3} - \frac{\sqrt{3}}{3}i, 0 + \frac{\sqrt{3}}{3}i \right).$$

*(*Pro snadné zapamatování, můžeme nad zápisem vektorů uvažovat jako nad psaním závorek neboli 'brackets'. Pokud bychom slovo rozdělili foneticky napůl, dostaneme bra a ket, a máme jasnou nápovědu jak který vektor nazvat.*)

1.1.2 Zavedení operací na qubitech

Pro jednoduchost uvádíme příklady na 1-qubitech, ale veškeré operace, lze jednoduše zobecnit na n-qubit.

Sčítání $\oplus$

Uvědomme si, že prostor qubitů netvoři vektorový prostor. Klasická operace sčítání na vektorech by proto na prostoru qubitů nedávala smysl, navíc nemáme k dispozici nulový vektor. A proto na qubitech nezavádíme sčítání, stejně jako na obvyklých vektorových prostorech po složkách, ale se změnou a to takovou, že vždy vynutíme, aby byl výsledek považován za qubit. Tedy po každém klasickém součtu ještě výsledek normalizujeme:

$$\vec{p} \oplus \vec{q} = \frac{\vec{p} + \vec{q}}{\|\vec{p} + \vec{q}\|},$$

kde + značíme tradiční součet po složkách. Důležité je poznamenat, že můžeme sčítat pouze bra vektory s bra vektory a očekávat výsledek opět jako bra vektor. Stejně pak s ket vektory.

Skalární součin $(\cdot,\cdot) \sim \langle\cdot|\cdot\rangle$

Pro vyjádření skalárního součinu, za pomoci Diracovy notace, potřebujeme nejprve odkázat na adjungované prostory. Konkrétně nás zajímají prostory všech lineárních zobrazení z $\mathbb{C}^2$ do $\mathbb{C}$. Tedy zobrazení z prostoru ket vektorů do komplexních čísel. Mějme lineární zobrazení $\langle f|$ z prostoru $\mathbb{C}^2$ do $\mathbb{C}$.

$$\langle f| : \mathbb{C}^2 \to \mathbb{C}.$$

Na prostoru $\mathbb{C}^2$ značíme obecný prvek $|q\rangle$ přičemž, ten získáváme lineární kombinací bázových prvků $\{|0\rangle, |1\rangle\}$ tohoto prostoru následovně:

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C} \quad \wedge \quad \|\alpha\|^2 + \|\beta\|^2 = 1.$$

Pak díky linearitě zobrazení $\langle f|$ platí:

$$\langle f|q\rangle = \langle f|0\rangle \cdot \alpha + \langle f|1\rangle \cdot \beta.$$

Vidíme, že pro jednoznačné určení libovolného zobrazení $\langle x|$ stačí určit hodnoty v bázových vektorech. Definujme nyní zobrazení $\langle 0|$, $\langle 1|$ pomocí báze prostoru ket vektorů indexované takto:

$$\langle j|i\rangle = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \quad | \quad i, j, \in \{0, 1\}$$

Je vidět, že tato zobrazení jsou lineárně nezávislá. Mějme libovolné zobrazení $\langle f|$ a vektor $|x\rangle$ pak platí:

$$\langle f|x\rangle = \langle f|(|0\rangle\langle 0| + |1\rangle\langle 1|)|x\rangle = \langle f|0\rangle\langle 0|x\rangle + \langle f|1\rangle\langle 1|x\rangle = f_1x_1 + f_2x_2,$$

kde $|0\rangle\langle 0|+|1\rangle\langle 1|$ je identické zobrazení. Dokonce z předchozího vztahu výše vyplývá, že zobrazení $\{\langle 0|, \langle 1|\}$ tvoří bázi prostoru, adjungovanému prostoru ket vektorů. Tento prostor, pak nazveme prostorem 'bra' vektorů. Přičemž každý bra vektor můžeme vyjádřit jako lineární kombinaci bázových bra vektorů:

$$\langle f| = f_1\langle 0| + f_2\langle 1|.$$

Na druhou stranu výpočet hodnoty komplexního skalárního součinu ve zvolené bázy můžeme zapsat takto:

$$(|p\rangle, |q\rangle) = \overline{\alpha} \cdot \gamma + \overline{\beta} \cdot \delta = \phi.$$

kde

$$|p\rangle = \alpha|0\rangle+\beta|1\rangle, \quad |q\rangle = \gamma|0\rangle+\delta|1\rangle, \quad \alpha, \beta, \gamma, \delta \in \mathbb{C}, \quad \|\alpha\|^2+\|\beta\|^2 = \|\gamma\|^2+\|\delta\|^2 = 1.$$

Celkově tedy vidíme, že ve zvolené bázi můžeme definovat komplexní skalární součin pomocí Diracovy notace jako:

$$(|p\rangle, |q\rangle) = |p\rangle^\dagger |q\rangle = \langle \overline{p} | q \rangle$$

Dále pak pro libovolný ket vektor $|q\rangle$ vidíme jasnou souvislost skalárního součinu a normy vektoru:

$$\langle q|q\rangle = (\overline{|q\rangle}, |q\rangle) = ||\vec{q}\,||^2,$$

což pokud $|q\rangle \in \mathcal{Q}$ považujeme za qubit musí splňovat podmínku normality:

$$\langle q|q\rangle = (\overline{|q\rangle}, |q\rangle) = ||\vec{q}\,||^2 = 1.$$

Pro úplnost ještě označme prostor 'bra' vektorů:

$$\mathcal{Q}^\dagger := \Big\{ \langle q| = \Big(q_1, q_2\Big), q_1, q_2 \in \mathbb{C} \quad q_1\overline{q_1} + q_2\overline{q_2} = 1 \Big\}.$$

Tenzorový součin

Rozebírání tříd tenzorů a detailní popis fungování jejich součinu, je mimo možnosti této bakalářské práce. Avšak poznamenejme zde, jak funguje tenzorový součin vektorů $ket \times ket \sim |q\rangle|p\rangle$, a $ket \times bra \sim |q\rangle\langle p|$. Zatímco se u skalárního součinu $bra \times ket$ dimenze redukuje na skalár, bude se při tenzorovém součinu dimenze navyšovat. A to například tak, že budeme li násobit ket vektor $|d\rangle$ dimenze 4 s ket vektorem $|b\rangle$ dimenze 2 dostaneme ket vektor $|h\rangle$ dimenze 8. Přičemž vektory zapíšeme takto:

$$|d\rangle = \begin{pmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{pmatrix} \quad , \quad |b\rangle = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix} \quad , \quad |h\rangle = \begin{pmatrix} h_0 \\ h_1 \\ h_2 \\ h_3 \\ h_4 \\ h_5 \\ h_6 \\ h_7 \end{pmatrix}$$

Chceme zjistit jak tenzorové násobení zpracovává jednotlivé souřadnice vektorů, vyjádřeme indexy i, j, k jako binární čísla:

$$i = \begin{matrix} 0 & 00 \\ 1 & 01 \\ 2 & 10 \\ 3 & 11 \end{matrix} \quad j = \begin{matrix} 0 & 0 \\ 1 & 1 \end{matrix} \quad k = \begin{matrix} & i \ |j \\ 0 & 00|0 \\ 1 & 00|1 \\ 2 & 01|0 \\ 3 & 01|1. \\ 4 & 10|0 \\ 5 & 10|1 \\ 6 & 11|0 \\ 7 & 11|1 \end{matrix}$$

Všimněme si, že indexy i,j jsou jakoby schovány v indexu k. Nyní tedy potřebujeme index k vyjádřit pomocí indexů i a j, a to provedeme následovně:

$$k = dim(|b\rangle) \cdot i + j.$$

Konečně definujeme součin $|d\rangle \times |b\rangle = |h\rangle$ tak, že pro h_k platí:

$$h_k = b_i \cdot d_j \longleftrightarrow k = dim(|b\rangle) \cdot i + j \quad | \quad i = 0,1,2,3 \quad j = 0,1 \quad k = 0,1,...,6,7$$

Všimněme si že tato operace není komutativní vůči výsledku samotnému, ale prohození pořadí násobení zachová typ výsledného vektoru. Také poznamenejme, že násobení $bra \times bra$ bude fungovat naprosto obdobně, tedy ho jen shrňme příkladem:

$$\langle \mathbf{u}| = \frac{5}{13}\langle 0| + \frac{12}{13}\langle 1| \qquad \langle \mathbf{v}| = \frac{1}{10}\langle 00| + \frac{5}{10}\langle 01| + \frac{5}{10}\langle 10| + \frac{7}{10}\langle 11|$$

$$\langle w| = \langle u| \times \langle v| = (\frac{5}{13}\langle 0| + \frac{12}{13}\langle 1|) \times (\frac{1}{10}\langle 00| + \frac{5}{10}\langle 01| + \frac{5}{10}\langle 10| + \frac{7}{10}\langle 11|) =$$

$$= \frac{1}{10}\frac{5}{13}\langle 0|\langle 00| + \frac{5}{10}\frac{5}{13}\langle 0|\langle 01| + \frac{5}{10}\frac{5}{13}\langle 0|\langle 10| + \frac{7}{10}\frac{5}{13}\langle 0|\langle 11| +$$

$$+\frac{1}{10}\frac{12}{13}\langle 1|\langle 00| + \frac{5}{10}\frac{12}{13}\langle 1|\langle 01| + \frac{5}{10}\frac{12}{13}\langle 1|\langle 10| + \frac{7}{10}\frac{12}{13}\langle 1|\langle 11| =$$

$$= \frac{5}{130}\langle 000| + \frac{25}{130}\langle 001| + \frac{25}{130}\langle 010| + \frac{35}{130}\langle 011| +$$

$$+\frac{12}{130}\langle 100| + \frac{60}{130}\langle 101| + \frac{60}{130}\langle 110| + \frac{84}{130}\langle 111|.$$

Zde poprvé vidíme plnou sílu způsobu značení kanonické báze pomocí binárního vyjádření indexu nenulového prvku. Totiž nad operací $\langle 10|\langle 1|$ nemusíme příliš přemýšlet a rovnou píšeme $\langle 101|$.

Poslední varianta, kterou jsme ještě neprozkoumali je násobení vektorů způsobem $ket \times bra$. Což díky tenzorovému součinu jde také, a vlastně intuitivně. Pokud jsme

totiž postupem *bra* $\times$ *ket* dimenze ztráceli, tak nyní je bude nabývat zpět. Dovolím si zde poměrně přímočaré zjednodušení, ale pro naše potřeby, bude vyhovující. Tedy součin vektorů $|q\rangle\langle p|$ kde $dim(\langle p|) = m$ a $dim(|q\rangle) = n$ nám dá matici řádu $m \times n$. Přičemž konkrétní postup násobení definujme následovně:

$$\langle p| = \begin{pmatrix} p_1 & p_2 & \cdots & p_{m-1} & p_m \end{pmatrix}, \qquad |q\rangle = \begin{pmatrix} q_1 \\ q_2 \\ \vdots \\ q_{n-1} \\ q_n \end{pmatrix},$$

$$|q\rangle\langle p| := \begin{pmatrix} p_1 \cdot q_1 & p_2 \cdot q_1 & \cdots & p_{m-1} \cdot q_1 & p_m \cdot q_1 \\ p_1 \cdot q_2 & p_2 \cdot q_2 & \cdots & p_{m-1} \cdot q_2 & p_m \cdot q_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ p_1 \cdot q_{n-1} & p_2 \cdot q_{n-1} & \cdots & p_{m-1} \cdot q_{n-1} & p_m \cdot q_{n-1} \\ p_1 \cdot q_n & p_2 \cdot q_n & \cdots & p_{m-1} \cdot q_n & p_m \cdot q_n \end{pmatrix}.$$

1.1.3 2-qubit a n-qubity

Až doposud jsme se věnovaly zavedení 1-qubitu. Pokud ale chceme qubity využít jako stavební kámen pro algoritmy, musíme být schopni ukládat větší množství informací než je ekvivalent jednoho bitu. Začněme tedy zavedením 2-qubitů *(čtěme "dva kjůbitů")*. Obecně jsou 2-qubity prvky vektorového prostoru $\mathbb{C}^4$, opět s omezením jejich velikosti na 1. Všechny 2-qubity tedy můžeme popsat jako tuto množinu:

$$|q_2\rangle \in \mathcal{Q}^2 := \{\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \mid \|\alpha\|^2 + \|\beta\|^2 + \|\gamma\|^2 + \|\delta\|^2 = 1\}.$$

Kde vektory $|00\rangle, |01\rangle, |10\rangle$ a $|11\rangle$ tvoří ortonormální bázi prostoru dimenze čtyři nad polem $\mathbb{C}$.

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

Všimněme si zde "binárního"způsobu označení vektorů kanonické báze. Neboli vektor mající na nultém místě (indexujeme od nuly) číslo 1 a na ostatních nuly, značíme binárně nula. Vektor mající na prvním místě číslo jedna, a všude jinde nuly, značíme binárně jedna a tak dále. Toto označení, nám přijde vhod, obzvláště s přihlédnutím k fungování tenzorového součinu.

2 Základy kvantového počtu

2.1 Měření stavů

Prozatím jsme byli schopni klást qubity do paralely s bity v klasické informatice. Nyní se však budeme věnovat problému měření kvantových stavů. U tradičních bitů je měření, něco nad čím se příliš nepozastavujeme. Pokud hodnotu bitu zjistíme, ta zůstává stejná a jeho stav se nemění. Avšak zde máme první důvod qubity nazývat kvantovými bity. A to proto, že stav qubitu může být libovolný mezi $|0\rangle$ a $|1\rangle$. Takže mluvíme o hodnotě pravděpodobnosti, že qubit při měření zkolabuje do jednoho ze stavů, a my tuto hodnotu naměříme. Tuto dualitu můžeme nejlépe chápat jako paralelu s fyzikálním Youngovým pokusem. Tedy že chování elektronů se mění v závislosti na tom, jestli jsou a nebo nejsou při průchodu štěrbinami pozorování.
Označme kolaps obecného stavu $|q\rangle$ do stavu $|x\rangle$ jako $\mapsto$. Pak pravděpodobnost, že obecný kvantový stav reprezentovaný qubitem $|q\rangle$ při měření zkolabuje do stavu $|x\rangle$, určíme následovně:

$$P(|q\rangle \mapsto |x\rangle) = \|\langle x|q\rangle\|^2$$

Pokud si vezmeme libovolnou ortonormální bázi $\mathbb{C}^2$ prostoru qubitů:

$$\{|x_1\rangle, |x_2\rangle\}$$

oproti které budeme měřit stav $|q\rangle$, naměříme příslušné prvky báze s následujícími pravděpodobnostmi:

$$P(x_1) = P(|q\rangle \mapsto |x_1\rangle) = \|\langle x_1|q\rangle\|^2 \quad P(x_2) = P(|q\rangle \mapsto |x_2\rangle) = \|\langle x_2|q\rangle\|^2$$

$$\sum_{j=1}^{2} P(x_j) = 1$$

Uveďme příklad pro objasnění:

$$|a\rangle = \frac{1}{\sqrt{30}} \cdot \begin{pmatrix} 2+3i \\ -4+i \end{pmatrix} \sim |a\rangle = \frac{2+3i}{\sqrt{30}}|\mathbf{0}\rangle \; + \; \frac{-4+i}{\sqrt{30}}|\mathbf{1}\rangle.$$

Měření pro bázi $\{|\mathbf{0}\rangle, |\mathbf{1}\rangle\}$ pomocí zápisu vektorů po složkách:

$$\begin{aligned} P(|a\rangle \mapsto |\mathbf{0}\rangle) = \|\langle \mathbf{0}|a\rangle\|^2 &= \left\| (1,0)\frac{1}{\sqrt{30}} \begin{pmatrix} 2+3i \\ -4+i \end{pmatrix} \right\|^2 \\ &= \left\| \frac{2+3i}{\sqrt{30}} \right\|^2 = \frac{\|2+3i\|^2}{30} = \frac{13}{30} \\ P(|a\rangle \mapsto |\mathbf{1}\rangle) = \|\langle \mathbf{1}|a\rangle\|^2 &= \left\| (0,1)\frac{1}{\sqrt{30}} \begin{pmatrix} 2+3i \\ -4+i \end{pmatrix} \right\|^2 \\ &= \left\| \frac{-4+i}{\sqrt{30}} \right\|^2 = \frac{\|-4+i\|^2}{30} = \frac{17}{30}. \end{aligned}$$

Za pomoci Diracovy notace:

$$P(|a\rangle \mapsto |\mathbf{0}\rangle) = \left\| \langle \mathbf{0}| \left(\tfrac{2+3i}{\sqrt{30}}|\mathbf{0}\rangle \; + \; \tfrac{-4+i}{\sqrt{30}}|\mathbf{1}\rangle \right) \right\|^2 = \left\| \frac{2+3i}{\sqrt{30}} \langle \mathbf{0}|\mathbf{0}\rangle + \frac{-4+i}{\sqrt{30}} \langle \mathbf{0}|\mathbf{1}\rangle \right\|^2$$
$$= \left\| \frac{2+3i}{\sqrt{30}} \cdot 1 + \frac{-4+i}{\sqrt{30}} \cdot 0 \right\| = \left\| \frac{2+3i}{\sqrt{30}} \right\|^2 = \frac{\|2+3i\|^2}{30} = \frac{13}{30}$$
$$P(|a\rangle \mapsto |\mathbf{1}\rangle) = \left\| \langle \mathbf{1}| \left(\tfrac{2+3i}{\sqrt{30}}|\mathbf{0}\rangle \; + \; \tfrac{-4+i}{\sqrt{30}}|\mathbf{1}\rangle \right) \right\|^2 = \left\| \frac{2+3i}{\sqrt{30}} \langle \mathbf{1}|\mathbf{0}\rangle + \frac{-4+i}{\sqrt{30}} \langle \mathbf{1}|\mathbf{1}\rangle \right\|^2$$
$$= \left\| \frac{2+3i}{\sqrt{30}} \cdot 0 + \frac{-4+i}{\sqrt{30}} \cdot 1 \right\| = \left\| \frac{-4+i}{\sqrt{30}} \right\|^2 = \frac{\|-4+i\|^2}{30} = \frac{17}{30}.$$

Měření se za pomoci Diracovy notace, zdá být zdlouhavější. Ale to pouze proto, že je pro názornost postup rozepsáno krok po kroku. Pokud ale máme qubit zapsaný za pomoci báze kterou měříme, můžeme jednoduše využít její ortonormality. Tedy pokud bychom obecný qubit zapsali jako:

$$|q\rangle = \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle \quad , \|\alpha\|^2 + \|\beta\|^2 = 1.$$

Pak díky postupu výše vidíme, že:

$$P(|q\rangle \mapsto |\mathbf{0}\rangle) = \|\alpha\|^2 \qquad P(|q\rangle \mapsto |\mathbf{1}\rangle) = \|\beta\|^2.$$

Měření pro bazi $\{|+\rangle, |\text{-}\rangle\}$ pomocí zápisu vektorů po složkách:

$$P(|a\rangle \mapsto |+\rangle) = \|\langle +|a\rangle\|^2 = \left\| (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}) \frac{1}{\sqrt{30}} \begin{pmatrix} 2+3i \\ -4+i \end{pmatrix} \right\|^2 =$$
$$= \left\| \frac{(2+3i)+(-4+i)}{\sqrt{2 \cdot 30}} \right\|^2 = \frac{\|-2+4i\|^2}{60} = \frac{20}{60} = \frac{1}{3}$$
$$P(|a\rangle \mapsto |\text{-}\rangle) = \|\langle \text{-}|a\rangle\|^2 = \left\| (\frac{1}{\sqrt{2}}, \frac{-1}{\sqrt{2}}) \frac{1}{\sqrt{30}} \begin{pmatrix} 2+3i \\ -4+i \end{pmatrix} \right\|^2 =$$
$$= \left\| \frac{(2+3i)-(-4+i)}{\sqrt{2 \cdot 30}} \right\|^2 = \frac{\|6+2i\|^2}{60} = \frac{40}{60} = \frac{2}{3}$$

2.2 Blochovsky podobné vektory

Z toho jak jsme výše popsali měření qubitů, je patrné, že měření rozhodně není jednoznačné. Rovnou uveďme ilustrační příklad. Vektory $|0\rangle$ a $\frac{\sqrt{2}}{2}(1+i)|0\rangle$ rozhodně nejsou totožné, naměříme však pravděpodobnost vzájemného kolapsu 1:

$$\|\langle 0|\frac{\sqrt{2}}{2}(1+i)|0\rangle\|^2 = \|\frac{\sqrt{2}}{2}(1+i)\langle 0|0\rangle\|^2 = \|\frac{\sqrt{2}}{2}(1+i)\cdot 1\|^2 = \frac{\sqrt{2}}{2}(1+i)\frac{\sqrt{2}}{2}(1-i) = 1.$$

Uvažujme tedy nad tím, zda by mohlo měření kvantových stavů dělit prostor qubitů do tříd ekvivalence. Prostor, který je pak tvořen zástupci těchto tříd nazvěme Blochovou sférou, přičemž zástupce můžeme vyjádřit ve tvaru:

$$|\psi\rangle \;=\; \cos(\,\frac{\theta}{2}\,)\,|0\rangle \;+\; e^{i\phi}\sin(\,\frac{\theta}{2}\,)\,|1\rangle \quad \theta \in [0,\pi], \phi \in [0,2\pi].$$

Blochově sféře jako takové se budeme věnovat ještě o kapitolu později,nyní se však pokusme popsat důvod její existence. Začněme rovnou tvrzením, že vektory jsou na Blochově sféře rozeznatelné za pomoci vzájemného měření. Myšleno ve smyslu, že jediná dvojice vektorů u které naměřím pravděpodobnost kolapsu 1, je dvojice totožných vektorů. Avšak toto rozhodně neplatí pro celý prostor qubitů.

Uvažujme tedy množinu všech takových vektorů, které kolabují k pevně zvolenému vektoru $|q\rangle$ s pravděpodobností 1:

$$\mathcal{I}_q := \Big\{ |p\rangle \in \mathcal{Q} : \|\langle p|q\rangle\|^2 = 1 \Big\}.$$

Taková množina vždy obsahuje minimálně generující prvek $|q\rangle$, jak ale zjistíme záhy, není to prvek jediný. Dále definujme množinu Λ_q pro každý vektor $|q\rangle$ jako množinu všech vektorů, které jsou na něj kolmé, následovně:

$$\Lambda_q := \Big\{ |\lambda\rangle \in \mathcal{Q} : \|\langle \lambda|q\rangle\|^2 = 0 \Big\}.$$

Zaveďme označení, že vektory $|p\rangle$ a $|q\rangle$ jsou si Blochovsky podobné jestliže nejsou rozeznatelné za pomoci měření jejich skalárního součinu neboli:

$$\|\langle p|q\rangle\|^2 = 1$$

Což také znamená:

$$\mathcal{I}_p = \mathcal{I}_q$$

Nyní uveďme tvrzení, že vektory si jsou Blochovsky podobné mají-li stejné množiny Λ.

Lemma 1 (Parametrizace Λ_q)**.** *Pro každý qubity $|q\rangle = q_1|0\rangle + q_2|1\rangle$ můžeme sestrojit Λ_q s následující parametrizací:*

$$\Lambda_q = \begin{cases} \left\{ \begin{pmatrix} kt \\ t \end{pmatrix} = |\lambda\rangle, \quad \|k\|^2\|t\|^2 + \|t\|^2 = 1 \quad k = -\frac{q_2}{q_1}, t \in \mathbb{C} \right\} & q_1 \neq 0 \\ \left\{ \begin{pmatrix} t \\ 0 \end{pmatrix} = |\lambda\rangle, \quad t \in \mathbb{C} \;\wedge\; \|t\|^2 = 1 \right\} & q_1 = 0. \end{cases}$$

Důkaz. Zaměřme se na popis množin Λ pomocí zápisu:

$$\|\langle \lambda|q\rangle\|^2 = 0.$$

Je asi zřejmé, že pokud má být norma komplexního čísla rovna nule, musí oním komplexním číslem být právě nula. Zápis tedy můžeme zjednodušit na :

$$\langle \lambda | q \rangle = 0.$$

A nyní tento zápis rozepišme podrobně.

$$\begin{aligned}
\langle \lambda | q \rangle &= 0 \\
\begin{pmatrix} \lambda_1 & \lambda_2 \end{pmatrix} \begin{pmatrix} q_1 \\ q_2 \end{pmatrix} &= 0 \\
\lambda_1 q_1 + \lambda_2 q_2 &= 0 \\
&\text{Pokud } q_1 \neq 0 : \\
\lambda_1 q_1 = -\lambda_2 q_2 \Rightarrow \lambda_1 &= -\frac{q_2}{q_1} \lambda_2 \\
&\text{Pokud } q_1 = 0 : \\
\lambda_2 q_2 = 0 \Rightarrow \lambda_2 = 0 \ \wedge \ \lambda_1 \in \mathbb{C} \ &: \ \|\lambda_1\| = 1
\end{aligned}$$

Máme tedy parametrický předpis pro to, jak vypadá množina Λ_q s jedním komplexním parametrem. Tím je důkaz kompletní. □

Lemma 1. *Všechny vektory $|p\rangle$, pro které platí: $\Lambda_p = \Lambda_q$, můžeme vyjádřit za pomoci vektoru $|q\rangle = q_1|0\rangle + q_2|1\rangle$ následovně:*

$$|p\rangle = \begin{cases} \begin{pmatrix} l \\ sl \end{pmatrix}, & s = \frac{q_2}{q_1}, \quad l \in \mathbb{C} \quad \|s\|^2 \|l\|^2 + \|l\|^2 = 1 \quad q_1 \neq 0 \\ \begin{pmatrix} 0 \\ l \end{pmatrix}, & l \in \mathbb{C}, \quad \|l\|^2 = 1 \qquad\qquad\qquad\qquad\quad q_1 = 0 \end{cases}$$

Důkaz. Předpokládejme tedy $\Lambda_q = \Lambda_p$ a vyjádřeme všechny vektory $|p\rangle$, které by takovou Λ_p generovali, v závislosti na vektoru $|q\rangle$.

$$\begin{aligned}
&\text{Pokud } q_1 \neq 0 : \\
&\langle \lambda | p \rangle = 0 \\
\begin{pmatrix} -\frac{q_2}{q_1} t & t \end{pmatrix} &\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = 0 \\
-\frac{q_2}{q_1} t p_1 + t p_2 = 0 \qquad & t \neq 0 \\
-\frac{q_2}{q_1} p_1 + p_2 = 0 \Rightarrow p_2 &= \frac{q_2}{q_1} p_1
\end{aligned}$$

Pro ostatní případy pak:

$$\begin{aligned}
&\text{Pokud } q_1 = 0: \\
&\qquad \langle\lambda|p\rangle = 0 \\
&\begin{pmatrix} t & 0 \end{pmatrix}\begin{pmatrix} p_1 \\ p_2 \end{pmatrix} = 0 \\
&\qquad tp_1 + 0p_2 = 0 \Rightarrow tp_1 = 0 \Rightarrow p_1 = 0
\end{aligned}$$

Čímž je lemma dokázáno. □

Věta 1 (Dvojitá kolmost)**.** *Vektory $|p\rangle$ a $|q\rangle$ mají totožné množiny Λ, právě tehdy když, mají totožné množiny $\mathfrak{I}$.*

$$\Lambda_p = \Lambda_q \quad \Longleftrightarrow \quad \mathfrak{I}_p = \mathfrak{I}_q.$$

Důkaz. Za předpokladu $\Lambda_p = \Lambda_q$, máme z lemma výše parametrický vztah mezi $|p\rangle$ a $|q\rangle$. Rozveďme tedy detailněji jejich vzájemné měření $|\langle p|q\rangle|^2$.

$$\begin{aligned}
&q_1 = 0, \qquad p_1 = 0: \\
&\|\langle p|q\rangle\|^2 = \langle p|q\rangle\langle q|p\rangle = \begin{pmatrix} 0 & \overline{p_2} \end{pmatrix}\begin{pmatrix} 0 \\ q_2 \end{pmatrix}\begin{pmatrix} 0 & \overline{q_2} \end{pmatrix}\begin{pmatrix} 0 \\ p_2 \end{pmatrix} = \overline{p_2}q_2p_2\overline{q_2} = \overline{p_2}p_2 \cdot \overline{q_2}q_2 = 1 \\
&q_1 \neq 0, \qquad p_2 = \frac{q_2}{q_1}p_1 \Rightarrow \overline{p_2} = \overline{\frac{q_2}{q_1}p_1} = \frac{\overline{q_2}}{\overline{q_1}}\overline{p_1}: \\
&|\langle p|q\rangle|^2 = \langle p|q\rangle\overline{\langle p|q\rangle} = \langle p|q\rangle\langle q|p\rangle \\
&\qquad = \begin{pmatrix} \overline{p_1} & \frac{\overline{q_2}}{\overline{q_1}}\overline{p_1} \end{pmatrix}\begin{pmatrix} q_1 \\ q_2 \end{pmatrix}\begin{pmatrix} \overline{q_1} & \overline{q_2} \end{pmatrix}\begin{pmatrix} p_1 \\ \frac{q_2}{q_1}p_1 \end{pmatrix} = \Big(\overline{p_1}q_1 + \frac{q_2\overline{q_2}}{\overline{q_1}}\overline{p_1}\Big)\Big(\overline{q_1}p_1 + \frac{q_2\overline{q_2}}{q_1}p_1\Big) \\
&\qquad = \|p_1\|^2\|q_1\|^2 + 2\|q_2\|^2\|p_1\|^2 + \frac{\|q_2\|^4}{\|q_1\|^2}\|p_1\|^2 \\
&\qquad = \frac{\|p_1\|^2}{\|q_1\|^2}\Big(\|q_1\|^4 + 2\|q_1\|^2\|q_2\|^2 + \|q_2\|^4\Big) \\
&\qquad = \frac{\|p_1\|^2}{\|q_1\|^2}\Big(\|q_1\|^2 + \|q_2\|^2\Big)^2 = \frac{\|p_1\|^2}{\|q_1\|^2}
\end{aligned}$$

Nyní ukažme, že výraz $\frac{\|p_1\|^2}{\|q_1\|^2}$ je roven jedné. K tomu využijeme vztah odvozený výše

$p_2 = \frac{q_2}{q_1} p_1$ a fakt, že vektory $|p\rangle$ $|q\rangle$ reprezentují qubity, a jsou tedy normované.

$$
\begin{aligned}
1 - \|p_1\|^2 = \|p_2\|^2 &= \left\| \frac{q_2}{q_1} p_1 \right\|^2 \\
1 - \|p_1\|^2 &= \frac{\|q_2\|^2}{\|q_1\|^2} \|p_1\|^2 \\
1 &= \frac{\|q_2\|^2 \|p_1\|^2}{\|q_1\|^2} + \|p_1\|^2 = \|q_2\|^2 \frac{\|p_1\|^2}{\|q_1\|^2} + \|p_1\|^2 \\
1 &= (1 - \|q_1\|^2) \frac{\|p_1\|^2}{\|q_1\|^2} + \|p_1\|^2 = \frac{\|p_1\|^2}{\|q_1\|^2} \frac{-\|q_1\|^2 \|p_1\|^2}{\|q_1\|^2} + \|p_1\|^2 \\
1 &= \frac{\|p_1\|^2}{\|q_1\|^2} - \|p_1\|^2 + \|p_1\|^2 = \frac{\|p_1\|^2}{\|q_1\|^2}
\end{aligned}
$$

A tím je věta dokázána. □

Povšimněme si, že díky parametrizaci $p_2 = \frac{q_2}{q1} p_1$, kterou můžeme přepsat na $\frac{p_2}{p_1} = \frac{q_2}{q_1}$, máme jasně definovaný deskriptor třídy ekvivalence, ve smyslu měření skalárním součinem. A to právě onen poměr $\frac{q_2}{q_1}$ který jasně definuje tyto množiny, až na výjimku kdy $q_1 = 0$. Pro tento případ tedy zaveďme arbitrární značení ∞. Tedy máme jednoduchý způsob, jak určit, zda jsou si vektory Blochovsky podobné.

Věta 1 (Zaplněnost Blochovské sféry)**.** *Všechny možné třídy ekvivalence mají na Blochově sféře svého zástupce, a žádné jiné prvky, krom těchto zástupců Blochova sféra neobsahuje.*

Důkaz. Z vět a důkazů výše vidíme, že každou třídu ekvivalence můžeme dobře definovat pomocí koeficientu $\frac{q_2}{q_1} = \alpha \in \mathbb{C} \cup \infty$. Který pokud upravíme, jak je dobrým zvykem, tak aby komplexní člen nebyl ve jmenovateli dostaneme výraz:

$$\alpha = \frac{q_2}{q_1} = \frac{q_2 \overline{q_1}}{\|q_1\|^2} = \frac{q_2 \overline{q_1}}{\|q_1\|^2} \frac{\|q_2 \overline{q_1}\|^2}{\|q_2 \overline{q_1}\|^2} = \frac{q_2 \overline{q_1}}{\|q_2 \overline{q_1}\|^2} \frac{\|q_2 \overline{q_1}\|^2}{\|q_1\|^2}.$$

Vidíme, že beze změny hodnoty koeficientu jsme ho z poměru dvou komplexních čísel transformovat do tvaru součinu jednoho normalizovaného komplexního čísla a jednoho kladného reálného koeficientu. Nyní uveďme konvenci zápisu obecného kvantového stavu reprezentovaného na Blochově sféře:

$$|\psi\rangle \;=\; \cos(\,\frac{\theta}{2}\,)\,|0\rangle \;+\; e^{i\phi} \sin(\,\frac{\theta}{2}\,)\,|1\rangle \quad \theta \in [0, \pi], \phi \in [0, 2\pi].$$

a vytvořme pro něj koeficient Blochovsky podobných vektorů. Po úpravách dostaneme:

$$
\begin{aligned}
\frac{\psi_2}{\psi_1} &= \frac{e^{i\phi} \sin(\,\frac{\theta}{2}\,)}{\cos(\,\frac{\theta}{2}\,)} \\
&= \frac{(\cos\phi + i \sin\phi) \sin\frac{\theta}{2}}{\cos\frac{\theta}{2}} \\
&= (\cos\phi + i \sin\phi) \tan\frac{\theta}{2}
\end{aligned}
$$

Našli jsme tedy kompatibilní tvar koeficientu. Díky tomu, že funkce tangens zobrazuje interval $\langle 0; \frac{\pi}{2} \rangle$ na interval $\langle 0; \infty \rangle$, máme pokrytý celý rozsah reálného parametru výše. Máme tedy jasně ukázanou platnost toho, že pro každý prvek Blochovy sféry existuje právě jedna množina $\mathcal{I}_\psi$, a opačně. Pro úplnost poukažme ještě na následující výjimky. Kdy $q_1 = 0$ pak $\alpha = \infty$ a množinu Blochovsky podobných vektorů nám na Blochově sféře zastupuje vektor $|1\rangle$. Podobně v případě kdy $q_2 = 0$ pak $\alpha = 0$ a vektor jež na Blochově sféře zastupuje množinu Blochovsky podobných vektorů je $|0\rangle$. □

Koncem této kapitoly se sluší podotknout, že byť tomuto faktu nebývá často věnována pozornost. Je důležité při návrhu kvantových algoritmů dbát na to aby výstupní stavy, kterými chceme reprezentovat různé výsledky, nebyli Blochovsky podobné.

2.3 Vizuální reprezentace Blochovy sféry

Už několikrát jsme narazili na to jaký objekt qubity tvoří a jak ho znázornit. Vzhledem k tomu, že nemáme mimo jiné nulový prvek nemohou qubity tvořit kompletní vektorový prostor, jsou pouze podmnožinou prostoru $\mathbb{C}^{2^n}$ (kde n je rozměr qubitu). Proto přicházíme se zápisem jednotlivých kvantových stavů ve formátu:

$$|\psi\rangle \;=\; \cos(\,\frac{\theta}{2}\,)\,|0\rangle \;+\; e^{i\phi}\sin(\,\frac{\theta}{2}\,)\,|1\rangle$$

Kde $\phi \in [0, 2\pi]$ popisuje relativní fázi kvantového stavu a $\theta \in [0, \pi]$ určuje pravděpodobnost naměření kanonických stavů$|0\rangle, |1\rangle$. Tedy :

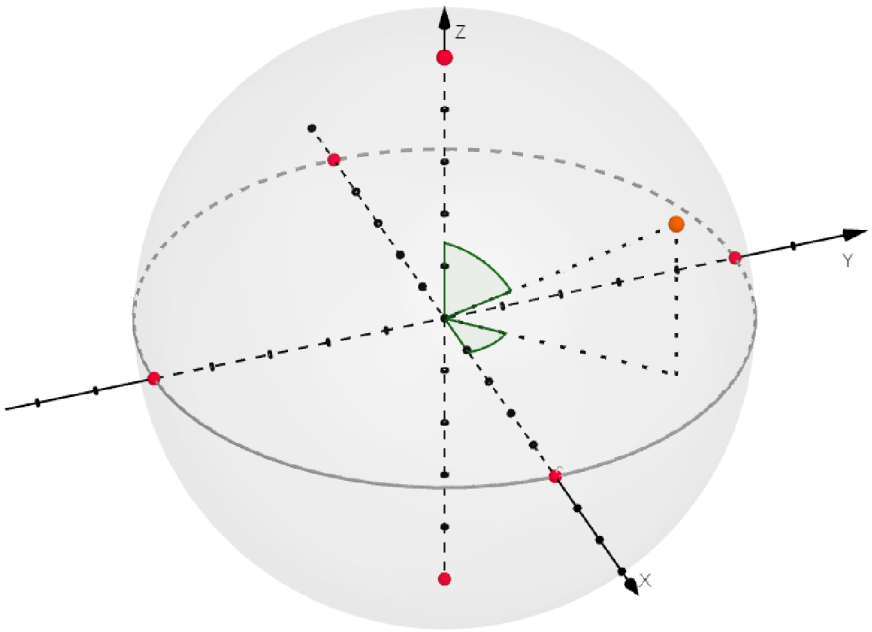
$$P(|\psi\rangle \mapsto |0\rangle = \cos(\,\frac{\theta}{2}\,)^2 \quad P(|\psi\rangle \mapsto |1\rangle = \sin(\,\frac{\theta}{2}\,)^2$$

Díky vyjádření všech měřením rozeznatelných qubitů za pomoci dvou parametrů, můžeme množinu pozorovatelných kvantových stavů vyjádřit jako dvouparametrickou plochu v trojrozměrném prostoru. Jak už název napovídá Blochova sféra je sféra:

$$\mathcal{B} := \{(x, y, z)^T \in \mathbb{R}^3 \quad | \quad x^2 + y^2 + z^2 = 1\}$$

na niž můžeme každému reprezentantu třídy ekvivalence prostoru qubitu přiřadit právě jeden bod. A to následovně:

$$\vec{r} = \begin{pmatrix} \sin(\theta)\cos(\phi) \\ \sin(\theta)\sin(\phi) \\ \cos(\theta) \end{pmatrix}$$



Obr. 2.1: Vizualizace Blochovy sféry, v programu GeoGebra

Naše známé vektory pak zobrazujeme takto:

$$|0\rangle: \quad \theta = 0 \quad \phi = \text{libovolné} \quad \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \qquad |1\rangle: \quad \theta = \pi \quad \phi = \text{libovolné} \quad \begin{pmatrix} 0 \\ 0 \\ -1 \end{pmatrix}$$

$$|+\rangle: \quad \theta = \frac{\pi}{2} \quad \phi = 0 \quad \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \qquad |-\rangle: \quad \theta = \frac{\pi}{2} \quad \phi = \pi \quad \begin{pmatrix} -1 \\ 0 \\ 0 \end{pmatrix}$$

$$|+i\rangle: \quad \theta = \frac{\pi}{2} \quad \phi = \frac{\pi}{2} \quad \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \qquad |-i\rangle: \quad \theta = \frac{\pi}{2} \quad \phi = \frac{3\pi}{2} \quad \begin{pmatrix} 0 \\ -1 \\ 0 \end{pmatrix}$$

Na Blochově sféře je pak dobře viditelné kolabování qubitu při měření. Protože ho zde reprezentujeme jednoduchým pootočením. Což nám dává možnost vizuálně reprezentovat i fenomén superpozice. Tedy kdy stav leží mezi dvěma stavy a kolabuje do jednoho z nich až při měření. Přičemž toto vidíme právě na úhlech, které spolu vektory na Blochově sféře svírají.

Všimněme si, že existence Blochovy sféry je odůvodněna pouze způsobem zavedení měření qubitů. Což nám tedy vysvětluje proč je Blochova sféra v literatuře používána jako množina všech pozorovatelných kvantových stavů. Jestliže existují i

jiné kvantové stavy než ty na Blochově sféře, stejně při měření splynou s některým, který na ni je. Jsou tedy pozorováním neodlišitelné.

2.4 Logické brány

Pokud jsme se zatím věnovali způsobu zápisu kvantových stavů z důvodu abychom na nim mohli stavět algoritmy, je na místě se nyní zaměřit na hlavní hybatele oněch algoritmů. Obdobně chceme-li klasické bity využít k výpočtu, musíme je nechat projít systémem logických bran, tak i my používáme kvantové logické brány. Tyto brány jsou obyčejnými zobrazeními z prostoru qubitů zpět do prostoru qubitů. Tedy přirozeně, tak jako chápeme qubity jako vektory, můžeme tyto brány chápat jako matice transformací. Ovšem máme zde pár omezení pro to aby nám jejich transformace dávaly smysl. Tedy hlavně to, že matice musí být unitární.

Unitární matice

Unitární maticí rozumíme jakoukoli čtvercovou matici, nad komplexními čísly, pro kterou platí:

$$U \times U^{\dagger} = \mathbb{1},$$

kde $\mathbb{1}$ je maticí identity, přesněji:

$$\mathbb{1} := [l]_{ij} \quad l_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} \quad i, j = 1, \cdots, n \quad | \quad n = dim(\mathbb{1}).$$

Značením † v horním indexu matice transformace pak rozumíme matici Hermitovsky sdruženou. Což je matice transponovaná a komplexně sdružená k matici výchozí. Neboli:

$$A = \begin{pmatrix} a_{00} & \cdots & a_{0n} \\ \vdots & \ddots & \vdots \\ a_{n0} & \cdots & a_{nn} \end{pmatrix}, \; A^{\dagger} = \overline{A^T} = \overline{\begin{pmatrix} a_{00} & \cdots & a_{n0} \\ \vdots & \ddots & \vdots \\ a_{0n} & \cdots & a_{nn} \end{pmatrix}} = \begin{pmatrix} \overline{a_{00}} & \cdots & \overline{a_{n0}} \\ \vdots & \ddots & \vdots \\ \overline{a_{0n}} & \cdots & \overline{a_{nn}} \end{pmatrix}.$$

Tato vlastnost nám zaručí, že při transformacích neopustíme prostor qubitů. Obecně je pak můžeme říci, že každá unitární matice, je i maticí ortonormální. Ukažme, že definice unitární matice:

$$A \times A^{\dagger} = \mathbb{1} \quad | \quad \mathbb{1} := \sum_{i \in I} |i\rangle\langle i|, \tag{2.1}$$

přímo implikuje následující vlastnosti:

a) Pro všechny řádky matice platí, že jejich eukleidovská norma je rovná 1.
b) Všechny řádky jsou, brány jako vektory, na sebe kolmé.

Toto odvoďme přímo roznásobením matic:

$$A = \sum_{i\in I}\sum_{j\in I} a_{ij}|i\rangle\langle j| \qquad A^\dagger = \sum_{s\in I}\sum_{t\in I} \overline{a}_{st}|t\rangle\langle s|.$$

$$\begin{aligned}
A \times A^\dagger = \mathbb{1} &= \Big(\sum_{i\in I}\sum_{j\in I} a_{ij}|i\rangle\langle j|\Big) \times \Big(\sum_{s\in I}\sum_{t\in I} \overline{a}_{st}|t\rangle\langle s|\Big) && (2.2)\\
&= \sum_{i\in I}\sum_{j\in I}\Big[a_{ij}|i\rangle\langle j| \sum_{s\in I}\sum_{t\in I} \overline{a}_{st}|t\rangle\langle s|\Big] && (2.3)\\
&= \sum_{i\in I}\sum_{j\in I}\sum_{s\in I}\sum_{t\in I} a_{ij}|i\rangle\langle j|\overline{a}_{st}|t\rangle\langle s| && (2.4)\\
&= \sum_{i\in I}\sum_{j\in I}\sum_{s\in I}\sum_{t\in I} a_{ij}\overline{a}_{st}|i\rangle\langle j|t\rangle\langle s| && (2.5)\\
&= \sum_{i\in I}\sum_{j\in I}\sum_{s\in I}\sum_{t\in I} a_{ij}\overline{a}_{sj}|i\rangle\langle j|j\rangle\langle s| && (2.6)\\
&= \sum_{i\in I}\sum_{j\in I}\sum_{s\in I} a_{ij}\overline{a}_{sj}|i\rangle\langle s| && (2.7)
\end{aligned}$$

(2.2) $\mapsto$ (2.3) $\mapsto$ (2.4) : Distributivita maticového součinu.
(2.4) $\mapsto$ (2.5) : Komutativita násobení skalárem.
(2.5) $\mapsto$ (2.6) : Mějme ortonormální bázi, indexovanou množinou indexů I pak : $\forall j, s \in I : \langle j|s\rangle = 0 \leftrightarrow j \neq s$ Tedy vyřazujeme všechny takové sčítance, které jsou nulové, a nahrazujeme index s značením j.
(2.6) $\mapsto$ (2.7) : Využijeme vlastnosti normality báze, a veškeré $\langle j|j\rangle$ nahradíme 1, kterou pak můžeme při násobení zanedbat. Následně také odebereme přebytečné sčítání přes, již sečtený index.

$$\begin{aligned}
\mathbb{1} = \sum_{i\in I}|i\rangle\langle i| &= \sum_{i\in I}\sum_{j\in I}\sum_{s\in I} a_{ij}\overline{a}_{sj}|i\rangle\langle s|\\
&\to \forall i, s \in I \wedge i = s : \sum_{s\in I}\sum_{j\in I} a_{sj}\overline{a}_{sj}|s\rangle\langle s| = \sum_{i\in I}|i\rangle\langle i|\\
&\Rightarrow \forall s \in I : \sum_{j\in I} a_{sj}\overline{a}_{sj} = \langle a_{s:}|a_{s:}\rangle = \|a_{s:}\|^2 = 1 && a)\\
&\Rightarrow \forall i, s \in I \wedge i \neq s : \sum_{j\in I} a_{ij}\overline{a}_{sj} = \sum_{j\in I}\overline{a}_{sj}a_{ij} = \langle a_{s:}|a_{i:}\rangle = 0 && b)
\end{aligned}$$

Přičemž, pro dokázání výroků a) a b) pro sloupce místo řádků provedeme stejný důkazový postup, jen s obraceným pořadím násobení. Což můžeme protože:

$$\begin{aligned}
A \times A^\dagger &= \mathbb{1}\\
A \times A^\dagger \times A &= A\\
A^{-1} \times A \times A^\dagger \times A &= A^{-1} \times A = \mathbb{1}\\
\Rightarrow A \times A^\dagger &= A^\dagger \times A = \mathbb{1}.
\end{aligned}$$

2.4.1 Brány na 1-qubitech

Nyní tedy už můžeme uvést základní brány, tedy takové transformace jež mají smysl na jednom qubitu. Bránu NOT zapíšeme jako:

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|.$$

A používáme takto:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \sim \sigma_x|0\rangle = \Big(|0\rangle\langle 1| + |1\rangle\langle 0|\Big)|0\rangle = |0\rangle\langle 1|0\rangle + |1\rangle\langle 0|0\rangle = |1\rangle$$

Pokud se pak podíváme na reprezentaci qubitů za pomoci Blochovy sféry, všimneme si, že při aplikaci σ_x dochází k rotaci okolo X-ové osy o π. Můžeme tedy uvést další brány, které budou provádět obdobné rotace.

$$\sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|.$$

Je rotací okolo z o π, nebo také přehození fáze, tedy přechod od $|+\rangle$ k $|-\rangle$ a zpět.

$$\begin{aligned} \sigma_z|+\rangle &= (|0\rangle\langle 0| - |1\rangle\langle 1|)\frac{\sqrt{2}}{2}(|0\rangle + |1\rangle) \\ &= \frac{\sqrt{2}}{2}\Big[|0\rangle\langle 0|0\rangle - |1\rangle\langle 1|0\rangle + |0\rangle\langle 0|1\rangle - |1\rangle\langle 1|1\rangle\Big] \\ &= \frac{\sqrt{2}}{2}\Big[|0\rangle 1 - |1\rangle 0 + |0\rangle 0 - |1\rangle 1\Big] \\ &= |-\rangle \end{aligned}$$

Rotaci okolo osy y, pak můžeme vyjádřit obdobně:

$$\sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = i\sigma_x\sigma_y.$$

Opět rotujeme o π na Blochově sféře, měníme jak hodnotu bitu, tak i fáze a přecházíme od $|+i\rangle$ k $|-i\rangle$ a zpět. Speciální pozornost si pak zaslouží brána zvaná Hadamardova, tato brána nám totiž slouží nejen k přechodu mezi bázemi $\{|0\rangle, |1\rangle\}$ a $\{|+\rangle, |-\rangle\}$, ale také nám pomáhá tvořit reprezentaci takzvaného entaglmentu, jak uvidíme později.

$$H = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{\sqrt{2}}{2}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\Big).$$

Brány na 2-qubitech

Typickým příkladem logické prány pro 2 bity je brána OR, tuto bránu však, nepovažujeme za bránu aplikovatelnou pro kvantové výpočty. Jednak nejde zapsat za pomoci matice, která by splňovala naše kritéria výše, a také protože při její aplikaci dochází ke ztrátě informace, chceme li dimenze. Proto používáme bránu CNOT, jež se dá slovy popsat jako kontrolovatelný exkluzivní OR, přičemž první z qubitů je bitem kontrolním, a druhý pak nese logický výsledek brány. CNOT pak zapisujeme takto:

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$

Působení CNOT brány, značené pomocí $\oplus$, pak můžeme vyjádřit i pomocí pravdivostní tabulky:

input		output	
x	y	x	x $\oplus$ y
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

2.4.2 Entaglment

Entaglment, už z překladu znamená provázanost, nebo zamotanost. A je to přesně ta vlastnost, která dělá kvantovou logiku zajímavou ke studiu. Obecně říkáme, že 2-qubit $|\psi\rangle_{A\,B}$ reprezentuje entaglované stavy A a B , jestliže nemůže vzniknout součinem dvou qubitů:

$$\nexists |\phi\rangle_A, |\theta\rangle_B \in \mathcal{Q} : |\phi\rangle_A \times |\theta\rangle_B = |\psi\rangle_{A\,B}.$$

Bellovy stavy

Bellovými stavy rozumíme čtyři 2-qubity, které jsou maximálně entaglované, a tvoří vlastní bázi prostoru $\mathbb{C}^4$.

$$\begin{aligned} |\psi^{00}\rangle &:= \tfrac{\sqrt{2}}{2}(|00\rangle + |11\rangle) \quad |\psi^{01}\rangle := \tfrac{\sqrt{2}}{2}(|01\rangle + |10\rangle) \\ |\psi^{10}\rangle &:= \tfrac{\sqrt{2}}{2}(|00\rangle - |11\rangle) \quad |\psi^{11}\rangle := \tfrac{\sqrt{2}}{2}(|01\rangle - |10\rangle) \end{aligned}$$

Obecný Bellův stav pak můžeme zapsat takto:

$$|\psi^{i\,j}\rangle = \left(\mathbb{1} \bigotimes \sigma_x^i \sigma_z^j\right)|\psi^{00}\rangle$$

Ukažme nyní využití Hadamardovy brány ke konstrukci Bellových stavů:

$$\begin{array}{cccc}
|i\,j\rangle_{A\,B} & & (H_A \bigotimes \mathbb{1}_B)|i\,j\rangle_{A\,B} & |\psi^{i\,j}\rangle \\
|0\,0\rangle & & \frac{\sqrt{2}}{2}(|0\,0\rangle + |1\,0\rangle) & \frac{\sqrt{2}}{2}(|0\,0\rangle + |1\,1\rangle) = |\psi^{0\,0}\rangle \\
|0\,1\rangle & \xrightarrow{H_A \bigotimes \mathbb{1}_B} & \frac{\sqrt{2}}{2}(|0\,1\rangle + |1\,1\rangle) & \xrightarrow{CNOT_{A\,B}} \frac{\sqrt{2}}{2}(|0\,1\rangle + |1\,0\rangle) = |\psi^{0\,1}\rangle \\
|1\,0\rangle & & \frac{\sqrt{2}}{2}(|0\,0\rangle - |1\,0\rangle) & \frac{\sqrt{2}}{2}(|0\,0\rangle - |1\,1\rangle) = |\psi^{1\,0}\rangle \\
|1\,1\rangle & & \frac{\sqrt{2}}{2}(|0\,0\rangle - |1\,0\rangle) & \frac{\sqrt{2}}{2}(|0\,1\rangle - |1\,0\rangle) = |\psi^{1\,1}\rangle
\end{array}$$

Přičemž operaci $\bigotimes$ chápeme jako tenzorové násobení matic následovně:

$$H = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$H \bigotimes \mathbb{1} = \begin{pmatrix} H \cdot 1 & H \cdot 0 \\ H \cdot 0 & H \cdot 1 \end{pmatrix} = \frac{\sqrt{2}}{2}\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

nebo v Diracově notaci:

$$\begin{aligned}
H_A \bigotimes \mathbb{1}_B &= \frac{\sqrt{2}}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|)_A \bigotimes (|0\rangle\langle 0| + |1\rangle\langle 1|)_B \\
&= \frac{\sqrt{2}}{2}(|0\rangle_A|0\rangle_B\langle 0|_A\langle 0|_B + |0\rangle_A|0\rangle_B\langle 1|_A\langle 0|_B + \\
&\quad + |1\rangle_A|0\rangle_B\langle 0|_A\langle 0|_B - |1\rangle_A|0\rangle_B\langle 1|_A\langle 0|_B + \\
&\quad + |0\rangle_A|1\rangle_B\langle 0|_A\langle 1|_B + |0\rangle_A|1\rangle_B\langle 1|_A\langle 1|_B + \\
&\quad + |1\rangle_A|1\rangle_B\langle 0|_A\langle 1|_B - |1\rangle_A|1\rangle_B\langle 1|_A\langle 1|_B) \\
&= \frac{\sqrt{2}}{2}(|00\rangle\langle 00| + |00\rangle\langle 10| + |10\rangle\langle 00| - |10\rangle\langle 10| + \\
&\quad + |01\rangle\langle 01| + |01\rangle\langle 11| + |11\rangle\langle 01| - |11\rangle\langle 11|)_{AB}.
\end{aligned}$$

3 Kvantové hry

3.1 Hry

V matematice nechápeme hry v tradičním slova smyslu dětských her. Hra je z matematického pohledu pevně stanovený systém pravidel a hodnocení stavů. Aktivní členy hry nazveme hráče, a jim umožníme konat pouze konkrétní akce neboli tahy. Soubor takových tahů provedených za sebou pak nazveme strategií. V rámci systému hodnocení stavu hry jsme pak u některých her schopni hledat optimální strategii.

Vězňovo dilema

Vězňovo dilema je jednoduchá hra pro dva hráče. Každý hráč má k dispozici pouze jeden možný tah. Tedy pro provedení obou dvou tahů hra končí. Název je zvolen podle analogie této hry vykreslované v podobě příběhu dvou podezřelých zločinců Adama a Barbory. Policie však nemá přímé důkazy, a proto potřebuje aspoň jednoho přimět k výpovědi. Zločinci tak dostávají na výběr zradit toho druhého,a nebo nevypovídat.V případě, kdy Adam zradí Barboru ale ta se rozhodne nevypovídat odchází Adam bez trestu do ochrany svědků, a Barbora dostává pět let vězení. S tím, že jednostranná zrada funguje symetricky, zradí-li tedy Barbora Adama i ona má možnost odejít bez trestu, a nechat Adama pět let ve vězení. Když se rozhodnou oba zradit odejdou každý s tříletým trestem, s přihlédnutím k tomu že spolupracovali s policií. Nakonec pokud nezradí ani jeden dostanou oba trest v rozsahu jednoho roku za kladení odporu při zatýkání. [1] Pokud bychom si zapsali tyto výstupy do tabulky dostaneme:

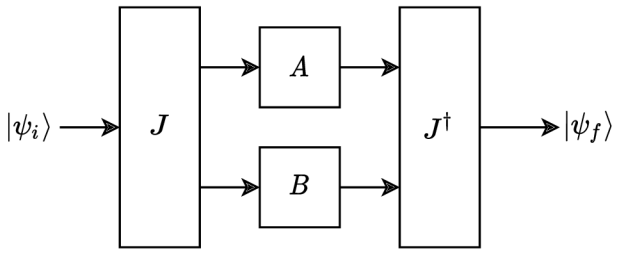
Adam\ Barbora	Zradí	Nezradí
Zradí	(3,3)	(0,5)
Nezradí	(5,0)	(1,1)

Vidíme tedy, že pokud hráč nemá informace o tom, jak hraje protihráč nutně je logickou úvahou veden zvolit zradu. Má totiž při zradě celkem šanci na trojnásobné prodloužení trestu nebo prominutí. V případě mlčení pak pětinásobnou nebo běžnou délku trestu. Vidíme tedy, že motivací zavést to hry kvantování, je snaha zohlednit ve hře sociální hladinu vztahu mezi hráči. Což dosahujeme za pomoci entaglmentu.

[1] Chtěl bych pouze krátce podotknout, že tato práce se nezabývá morálkou takového právního systému, ani neklade důraz na realističnost ilustračního příběhu.

3.2 Kvantové vězňovo dilema

V tradičním vězňovu dilematu musíme provést několik změn, abychom ho mohli nazývat kvantovým. Předně je třeba zavést proces entaglování, což je hlavní faktor definující rozdíly, mezi klasickou a kvantovou hrou. Ten provádíme za pomoci operátoru J, kterým na začátku transformujeme stav hráčů. Přičemž stav hráčů reprezentujeme 2-qubitem. Následně, necháme každého z hráčů, zahrát svoji strategii, za pomoci logické brány, kterou značíme A respektive B. Konečně qubity odentaglujeme, pomocí Hermitovsky sdruženého operátoru $J^\dagger$, a měříme výsledek. Proces hry můžeme vyjádřit i diagramem:



Tedy při zápisu celého procesu hry do tenzorových operací, dostaneme formuli, pro finální stav hry:

$$|\psi_f\rangle = J^\dagger(A \otimes B)J|\psi_i\rangle.$$

Kde $|\psi_i\rangle$ označuje počáteční stav a $|\psi_f\rangle$ stav finální ve formátu 2-qubitu. Nyní detailněji zaveďme operátor J, tak abychom mohli regulovat míru entaglovanosti.

$$J = \exp\{i\frac{\gamma}{2}\sigma_x \otimes \sigma_x\} \qquad \gamma \in [0, \frac{\pi}{2}]$$

Přičemž význam matice v exponentu chápeme, v případě čtvercové matice, jako zobecnění exponenciální funkce. A při použití Maclaurinova polynomu můžeme funkci přepsat do tvaru:

$$\exp\{X\} = \sum_{k=0}^{\infty} \frac{1}{k!} X^k.$$

Díky tomuto poznatku pak můžeme lépe pracovat s operátorem J jako s maticí.

$$J = \exp\{i\frac{\gamma}{2}\sigma_x \otimes \sigma_x\} = \sum_{k=0}^{\infty} \frac{1}{k!}\left(i\frac{\gamma}{2}\begin{pmatrix}0&1\\1&0\end{pmatrix}\otimes\begin{pmatrix}0&1\\1&0\end{pmatrix}\right)^k = \sum_{k=0}^{\infty}\frac{1}{k!}\left(i\frac{\gamma}{2}\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}\right)^k$$

$$= \sum_{\substack{k=0\\ k-\text{sudé}}}^{\infty} \frac{1}{k!}\left(\frac{i\gamma}{2}\right)^k \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix} + \sum_{\substack{k=0\\ k-\text{liché}}}^{\infty} \frac{1}{k!}\left(\frac{i\gamma}{2}\right)^k \begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$$

$$= \sum_{k=0}^{\infty} \frac{1}{2k!}\left(\frac{i\gamma}{2}\right)^{2k} \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix} + \sum_{k=0}^{\infty} \frac{1}{(2k+1)!}\left(\frac{i\gamma}{2}\right)^{(2k+1)} \begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$$

$$= \cos\frac{\gamma}{2}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix} + i\sin\frac{\gamma}{2}\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}.$$

Kdy pro $\gamma = \frac{\pi}{2}$ dostáváme maximální entaglovanost. A tedy tvar operátoru J:

$$J = \frac{\sqrt{2}}{2}\begin{pmatrix}1&0&0&i\\0&1&i&0\\0&i&1&0\\i&0&0&1\end{pmatrix}.$$

Naopak nulovou entaglovanost máme při $\gamma = 0$, kdy operátor J nabývá tvaru:

$$J = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

Což je jasné, protože je to tvar matice identity. Jak už jsme komentovali výše, v kapitole logických bran, abychom lineární transformaci mohli za logickou bránu považovat, musí být unitární. Tedy všechny možné strategie pro Adama či Barboru můžeme obecně zapsat jako:

$$U(\theta,\alpha,\beta) = \begin{pmatrix}e^{i\alpha}\cos\frac{\theta}{2} & e^{i\beta}\sin\frac{\theta}{2}\\ e^{-i\beta}\sin\frac{\theta}{2} & e^{-i\alpha}\cos\frac{\theta}{2}\end{pmatrix} \qquad \theta\in[0,\pi]\ ,\ \alpha,\beta\in[-\pi,\pi].$$

Jako příklad vlivu parametru θ uvažujme všechny strategie $U(\theta, 0, 0)$. Ukažme, že popisují určitou kombinaci mezi přehozením bitu, a identickým zobrazením. Kdy míru pravděpodobnosti, zda dojde nebo nedojde ke změně stavu, určuje právě θ:

$$\begin{aligned}
\begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} |0\rangle &= \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle = |q\rangle \\
\|\langle 0|q\rangle\|^2 &= \|\langle 0|(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle)\|^2 \\
&= \|\langle 0|\cos\frac{\theta}{2}|0\rangle\|^2 = \|\cos\frac{\theta}{2}\|^2 = \cos^2\frac{\theta}{2} \\
\|\langle 1|q\rangle\|^2 &= \|\langle 0|(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle)\|^2 \\
&= \|\langle 1|\sin\frac{\theta}{2}|0\rangle\|^2 = \|\sin\frac{\theta}{2}\|^2 = \sin^2\frac{\theta}{2}.
\end{aligned}$$

Z příkladu výše vidíme, že k přehození bitu dojde s pravděpodobností $\sin^2\frac{\theta}{2}$ a komplementárně pak s pravděpodobností $\cos^2\frac{\theta}{2}$ ke změně nedojde.

Ze všech možných strategií se budeme zabývat třemi, a to: $U(0,0,0)$, $U(\pi,0,0)$ a $U(\frac{\pi}{2},\frac{\pi}{2},0)$. Takže pokud bychom do hry vstupovali se stavem $|00\rangle$ reprezentovaným oboustrannou zradou, pak strategie $U(0,0,0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ je strategií zradit oponenta, strategie $U(\pi,0,0) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ je strategií nezradit oponenta, a strategie $U(\frac{\pi}{2},\frac{\pi}{2},0) = \frac{i\sqrt{2}}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, je strategií popisovanou jako *Eisertův zázračný tah*, který nám umožní naplno využít potenciálu entaglovanosti hráčů.

Chceme-li nějak výsledek hry kvantifikovat, musíme použít tabulku trestů, s níž jsme ilustrovali, klasické vězňovo dilema. Tabulku reprezentujme maticí s prvky $T_{i,j}$, například na pozici $T_{0,1}$ bude trest pro hráče, který zradil, a zároveň zrazen nebyl. Tedy z konkrétního případu výše:

$$T_{\text{Adam}} = \begin{pmatrix} 3 & 0 \\ 5 & 1 \end{pmatrix}, \qquad T_{\text{Barbora}} = \begin{pmatrix} 3 & 5 \\ 0 & 1 \end{pmatrix}.$$

Strategie u kvantových her budeme hodnotit podobně jako u těch klasických. Chceme určit hodnotu rizika, jaké kvůli vybrané strategii podstupujeme. Takže vezmeme pravděpodobnost každého výstupu, znásobíme ji s jemu příslušným trestem, a tyto hodnoty sečteme. Takže pokud při Adamově strategii A, a Bářině strategii B, máme

výstup $|\psi_f\rangle$, pak riziko pro Adama určíme následovně:

$$\begin{aligned}\text{Riziko} = T_{Adam[00]}\|\langle 00|\psi_f\rangle\|^2 + T_{Adam[01]}\|\langle 01|\psi_f\rangle\|^2 \\ + T_{Adam[10]}\|\langle 10|\psi_f\rangle\|^2 + T_{Adam[11]}\|\langle 11|\psi_f\rangle\|^2\end{aligned}$$

Vidíme tedy, že rizikovost Adamovi strategie, závisí nejen na strategii samotné, kterou si vybere, ale i na strategii Báry, která hru ovlivňuje stejně. Z toho pak vychází optimalizační postup za pomoci minimaxového kritéria. Kdy Adam si volí takovou strategii, která ho minimálně poškodí, v případě kdy Barbora zvolí strategii co mu uškodí maximálně. Adam tedy efektivně volí cestu nejmenšího zla, které na něm může být vykonáno.

Dále se tedy budeme věnovat výhodnosti hráčovi strategie v závislosti na strategii protihráče. Rozepišme si tedy všechny možné kombinace strategií, které hráčům poskytujeme, a vytvořme pro mě logickou bránu hry.

$$L = A \otimes B = \begin{pmatrix} A \cdot B_{[0,0]} & A \cdot B_{[0,1]} \\ A \cdot B_{[1,0]} & A \cdot B_{[1,1]} \end{pmatrix} = \begin{pmatrix} A_{[0,0]}B_{[0,0]} & A_{[0,1]}B_{[0,0]} & A_{[0,0]}B_{[0,1]} & A_{[0,1]}B_{[0,1]} \\ A_{[1,0]}B_{[0,0]} & A_{[1,1]}B_{[0,0]} & A_{[1,0]}B_{[0,1]} & A_{[1,1]}B_{[0,1]} \\ A_{[0,0]}B_{[1,0]} & A_{[0,1]}B_{[1,0]} & A_{[0,0]}B_{[1,1]} & A_{[0,1]}B_{[1,1]} \\ A_{[1,0]}B_{[1,0]} & A_{[1,1]}B_{[1,0]} & A_{[1,0]}B_{[1,1]} & A_{[1,1]}B_{[1,1]} \end{pmatrix}$$

1. Adam i Barbora zradí
2. Adam zradí Barboru, která kooperuje
3. Adam zradí Barboru, která hraje *miracle* strategii
4. Adam, který kooperuje, je zrazen Barborou
5. Adam i Barbora kooperují
6. Adam volí strategii kooperace a Barbora *miracle* strategii
7. Adam použije *miracle* strategii a je zrazen Barborou
8. Adam použije *miracle* strategii a Barbora kooperuje
9. Adam i Barbora použijí *miracle* strategii

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ a } B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ pak } L_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ a } B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ pak } L_2 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ a } B = \frac{i\sqrt{2}}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \text{ pak } L_3 = \frac{i\sqrt{2}}{2} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ a } B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ pak } L_4 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ a } B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ pak } L_5 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ a } B = \frac{i\sqrt{2}}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \text{ pak } L_6 = \frac{i\sqrt{2}}{2} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}$$

$$A = \frac{i\sqrt{2}}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ a } B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \text{ pak } L_7 = \frac{i\sqrt{2}}{2} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$A = \frac{i\sqrt{2}}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ a } B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \text{ pak } L_8 = \frac{i\sqrt{2}}{2} \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix}$$

$$A = \frac{i\sqrt{2}}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ a } B = \frac{i\sqrt{2}}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, pak \ L_9 = \frac{-1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Naším cílem je nyní pozorovat výsledky možných her v závislosti na parametru entaglovanosti γ. Proveďme tedy vyhodnocení her pro každý scénář 1-9, s ponecháním parametru γ jako neznámé, až k finálnímu stavu.$|\psi_{f_k}\rangle = J^\dagger L_k J|00\rangle \qquad k = 1, \ldots, 9$

$$|\psi_{f_1}\rangle = |00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad |\psi_{f_2}\rangle = |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|\psi_{f_3}\rangle = \tfrac{i\sqrt{2}}{2} \begin{pmatrix} \cos^2\frac{\gamma}{2} - \sin^2\frac{\gamma}{2} \\ 0 \\ 1 \\ -2i\cos\frac{\gamma}{2}\sin\frac{\gamma}{2} \end{pmatrix} \qquad |\psi_{f_4}\rangle = |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|\psi_{f_5}\rangle = |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \qquad |\psi_{f_6}\rangle = \tfrac{i\sqrt{2}}{2} \begin{pmatrix} 0 \\ \cos^2\frac{\gamma}{2} - \sin^2\frac{\gamma}{2} \\ -2i\cos\frac{\gamma}{2}\sin\frac{\gamma}{2} \\ 1 \end{pmatrix}$$

$$|\psi_{f_7}\rangle = \tfrac{i\sqrt{2}}{2} \begin{pmatrix} \cos^2\frac{\gamma}{2} - \sin^2\frac{\gamma}{2} \\ 1 \\ 0 \\ -2i\cos\frac{\gamma}{2}\sin\frac{\gamma}{2} \end{pmatrix} \qquad |\psi_{f_8}\rangle = \tfrac{i\sqrt{2}}{2} \begin{pmatrix} 0 \\ -2i\cos\frac{\gamma}{2}\sin\frac{\gamma}{2} \\ \cos^2\frac{\gamma}{2} - \sin^2\frac{\gamma}{2} \\ 1 \end{pmatrix}$$

$$|\psi_{f_9}\rangle = \tfrac{-1}{2} \begin{pmatrix} 1 \\ (\cos\frac{\gamma}{2} - i\sin\frac{\gamma}{2})^2 \\ (\cos\frac{\gamma}{2} - i\sin\frac{\gamma}{2})^2 \\ 1 \end{pmatrix}$$

Nyní proveďme zhodnocení jednotlivých her za pomoci výplatní funkce, chceme-li funkce trestu. Změřme tedy pravděpodobnosti, kolapsu finálních stavů k bázovým, a znásobme výsledky měření tresty z hráčovy tabulky postihů. Neboli:

$$riziko_k = T_{[00]}\|\langle 00|\psi_{f_k}\rangle\|^2 + T_{[01]}\|\langle 01|\psi_{f_k}\rangle\|^2 + T_{[10]}\|\langle 10|\psi_{f_k}\rangle\|^2 + T_{[11]}\|\langle 11|\psi_{f_k}\rangle\|^2,$$

kde $k = 1, \ldots, 9$ označuje index hry. Adamova rizika:

$$\begin{aligned}
\text{riziko}_1 &= 3\|\langle 00|00\rangle\|^2 + 0\|\langle 01|00\rangle\|^2 + 5\|\langle 10|00\rangle\|^2 + 1\|\langle 11|00\rangle\|^2 = 3 \\
\text{riziko}_2 &= 3\|\langle 00|01\rangle\|^2 + 0\|\langle 01|01\rangle\|^2 + 5\|\langle 10|01\rangle\|^2 + 1\|\langle 11|01\rangle\|^2 = 0 \\
\text{riziko}_3 &= \frac{1}{2}(3(\cos^2\frac{\gamma}{2} - \sin^2\frac{\gamma}{2})^2 + 5 + 4\cos^2\frac{\gamma}{2}\sin^2\frac{\gamma}{2}) \\
\text{riziko}_4 &= 3\|\langle 00|10\rangle\|^2 + 0\|\langle 01|10\rangle\|^2 + 5\|\langle 10|10\rangle\|^2 + 1\|\langle 11|10\rangle\|^2 = 5 \\
\text{riziko}_5 &= 3\|\langle 00|11\rangle\|^2 + 0\|\langle 01|1\rangle\|^2 + 5\|\langle 10|11\rangle\|^2 + 1\|\langle 11|11\rangle\|^2 = 1 \\
\text{riziko}_6 &= \frac{1}{2}(5 \cdot 4\cos^2\frac{\gamma}{2}\sin^2\frac{\gamma}{2} + 1) \\
\text{riziko}_7 &= \frac{1}{2}(3(\cos^2\frac{\gamma}{2} - \sin^2\frac{\gamma}{2})^2 + 4\cos^2\frac{\gamma}{2}\sin^2\frac{\gamma}{2}) \\
\text{riziko}_8 &= \frac{1}{2}(5(\cos^2\frac{\gamma}{2} - \sin^2\frac{\gamma}{2})^2 + 1) \\
\text{riziko}_9 &= \frac{1}{4}(3 + 5(\cos^2\frac{\gamma}{2} + \sin^2\frac{\gamma}{2})^2 + 1) = \frac{3+5+1}{4}
\end{aligned}$$

Rizika Barbory:

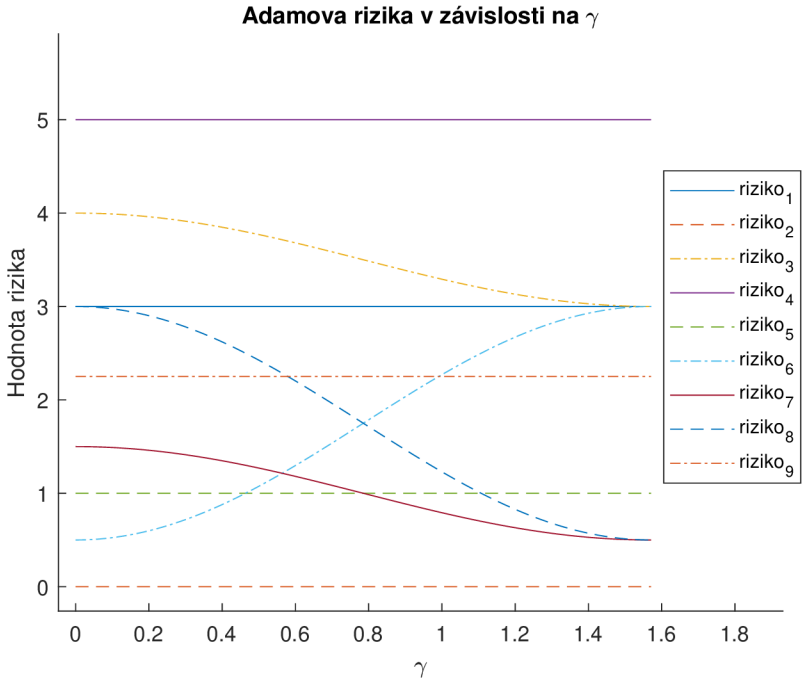
$$\begin{aligned}
\text{riziko}_1 &= 3\|\langle 00|00\rangle\|^2 + 5\|\langle 01|00\rangle\|^2 + 0\|\langle 10|00\rangle\|^2 + 1\|\langle 11|00\rangle\|^2 = 3 \\
\text{riziko}_2 &= 3\|\langle 00|01\rangle\|^2 + 5\|\langle 01|01\rangle\|^2 + 0\|\langle 10|01\rangle\|^2 + 1\|\langle 11|01\rangle\|^2 = 5 \\
\text{riziko}_3 &= \frac{1}{2}(3(\cos^2\frac{\gamma}{2} - \sin^2\frac{\gamma}{2})^2 + 4\cos^2\frac{\gamma}{2}\sin^2\frac{\gamma}{2}) \\
\text{riziko}_4 &= 3\|\langle 00|10\rangle\|^2 + 5\|\langle 01|10\rangle\|^2 + 0\|\langle 10|10\rangle\|^2 + 1\|\langle 11|10\rangle\|^2 = 0 \\
\text{riziko}_5 &= 3\|\langle 00|11\rangle\|^2 + 5\|\langle 01|11\rangle\|^2 + 0\|\langle 10|11\rangle\|^2 + 1\|\langle 11|11\rangle\|^2 = 1 \\
\text{riziko}_6 &= \frac{1}{2}(5(\cos^2\frac{\gamma}{2} - \sin^2\frac{\gamma}{2})^2 + 1) \\
\text{riziko}_7 &= \frac{1}{2}(3(\cos^2\frac{\gamma}{2} - \sin^2\frac{\gamma}{2})^2 + 5 + 4\cos^2\frac{\gamma}{2}\sin^2\frac{\gamma}{2}) \\
\text{riziko}_8 &= \frac{1}{2}(5 \cdot 4\cos^2\frac{\gamma}{2}\sin^2\frac{\gamma}{2} + 1) \\
\text{riziko}_9 &= \frac{1}{4}(3 + 5(\cos^2\frac{\gamma}{2} + \sin^2\frac{\gamma}{2})^2 + 1) = \frac{3+5+1}{4}
\end{aligned}$$

Následně uspořádejme rizika do tabulky, podle toho jakou strategii hráči zvolí.

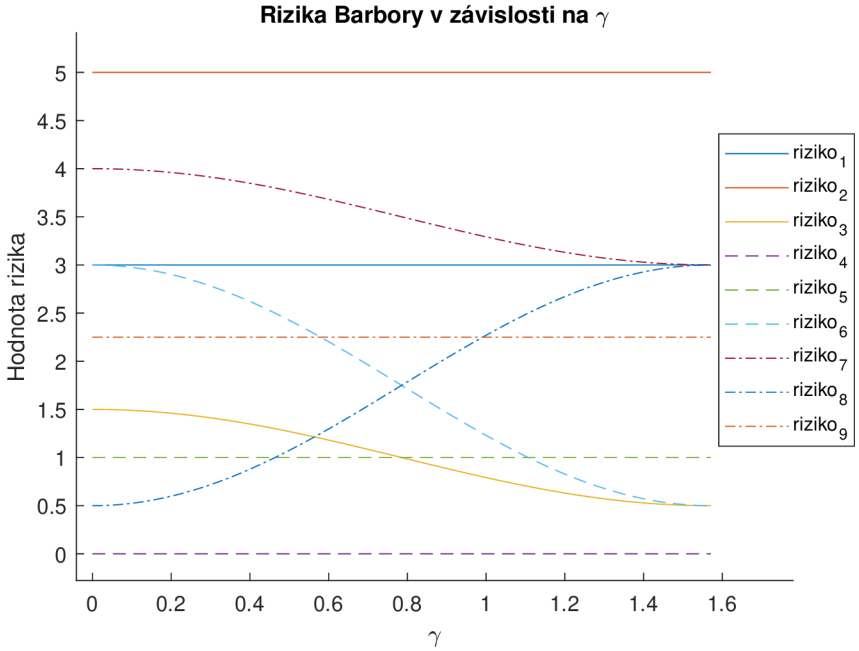
Adam\Barbora	Zradí	Nezradí	Miracle
Zradí	riziko_1	riziko_2	riziko_3
Nezradí	riziko_4	riziko_5	riziko_6
Miracle	riziko_7	riziko_8	riziko_9

Nyní použijeme minimax kritérium. Z Adamova pohledu minimax spočívá v minimalizaci rizika, kterým jej ohrožuje Barbora. Tedy z každého sloupce tabulky vybereme největší ohrožení, a z nich pak vybereme to nejmenší. Uvažujeme totiž způsobem, kdy hráči hrají proti sobě. Obdobnou analýzu rizik provedeme i z pohledu Barbory,

jen s rozdílem, že maxima vybíráme z řádků. Vzhledem k tomu, že jsou naše rizika závislá na parametru entaglmentu γ je snazší porovnávání provádět v grafech.



Obr. 3.1: Graf rizik hráče A, v závislosti na parametru entaglovanosti γ, vykresleno programem MATLAB.



Obr. 3.2: Graf rizik hráče B, v závislosti na parametru entaglovanosti γ, vykresleno programem MATLAB.

V grafech můžeme pozorovat změny rizikovosti jednotlivých strategií v závislosti na parametru entaglovanosti γ. Pokud budeme hledat nejlepší strategie hráčů, musíme začít volbou výběrového kritéria.

Nejprve zvolme algoritmus maxmin. Tedy pokud bychom chtěli vybrat strategii pro Adama, vezmeme strategie dle Barbořiny volby, které Adamovi nejvíce uškodí, a z nich vyberme ty, které uškodí nejméně.

$$\text{Adamova volba}_{maxmin} = min \begin{Bmatrix} max\{riziko_1, riziko_4 riziko_7\} \\ max\{riziko_2, riziko_5 riziko_8\} \\ max\{riziko_3, riziko_6 riziko_9\} \end{Bmatrix}.$$

Stejně pak postupujeme i při volbě Barbořiny strategie, jen s rozdílem že transponujeme tabulku rizik. Při výběru z grafů tak začneme předvýběrem maxima z všech strategií vykreslených stejným druhem čáry, kde hledáme nejhorší variantu jakou může protihráč uškodit. Z tohoto předvýběru katastrofických scénářů, pak vybereme minimum, abychom riziko co nejvíce snížili. Pro Adama tak dostáváme předvýběr jako riziko_4, $\text{riziko}_8 \to 5$ a riziko_3, ze kterého jasně vychází jako minimální $\text{riziko}_8 \to 5$. Tedy Adam by nejprve volil strategii 8, následně by by pak s narůstající γ přešel ke strategii 5. Neboli hrál by miracle, a chtěl by aby Barbora hrála kooperaci, a posléze by hrál kooperaci. Stejně tak Barbora dostane strategie mezi nimiž mění. Barboře však před změnou vychází strategie volit miracle a nechat Adama hrát kooperaci. Konečně pak po změně strategie i Barbora dojde ke strategii kooperace kooperace.

Nyní pozorujme, jak se změní vybrané strategie pokud změníme algoritmus výběru rizika. Tentokrát volíme algoritmus minmax, tedy přehodíme pořadí uspořádání. Přičemž myšlenka je taková, že si vybíráme minimálně škodlivé strategie, z nichž si pak protihráč volí takové aby maximalizoval náš postih. Adamovu úvahu nad riziky, pak můžeme zapsat následovně:

$$\text{Adamova volba}_{minmax} = max \begin{Bmatrix} min\{riziko_1, riziko_2 riziko_3\} \\ min\{riziko_4, riziko_5 riziko_6\} \\ min\{riziko_7, riziko_8 riziko_9\} \end{Bmatrix}.$$

Tady pak pro Adama vychází přechod dvou strategií, z rizika_7 k riziku_5 a to v bodě jejich průniku. Pro Barboru nám tímto postupem výběru vyjdou stejné křivky se stejnými průsečíky jako u Adama, jen s rozdílem, že přechází od rizika_3 k riziku_5. Znovu zde tedy vzniká konsensus až po přechodu u přechodných rizik.

Vidíme tedy, že pro vyhodnocení rizika můžeme provést několika způsoby, a vždy je třeba uvažovat nad tím, kterým směrem nás zvolený postup výběru vede.

Závěr

V práci se věnuji převážně pochopení problematiky kvantového počtu. Je do detailu rozebrána reprezentace qubitu, i to proč si vybíráme Blochovu sféru jako množinu pro reprezentaci všech kvantových stavů. Prezentuji zde své vlastní odvození toho, z jakého důvodu Blochovu sféru zavádíme, a dokazuji že je tvořena reprezentanty jednotlivých tříd ekvivalence. Cíle pochopení a ozřejmění jsou tedy naplněny. Dále jsou zde spočteny finální stavy pro vězňovo dilema v závislosti na parametru entaglovanosti. Což umožňuje sledovat strategie, ne jen z pohledu tabulek, ale i v jejich průběhu v závislosti na míře entaglovanosti hráčů. Je zde mnoho prostoru, pro zkoumání dalších možných strategii vězňova dilematu, i pro objasnění faktu, že pro každou kvantovou strategii existuje vhodná kvantová anti-strategie, která je vůči ní výherní. Toto jsou směry, kterými by se mohly vydávat další práce ve stejném tématickém okruhu. Navíc je zde postaven dobrý základ pro popis a tvorbu kvantových algoritmů. Vidím tedy potenciál navázat na základní popis logických bran pro qubity a věnovat se rozboru například Shorova algoritmu pro prvočíselný rozklad.

Literatura

[1] KOLMOGOROV, Andrej Nikolajevič a Sergej Vasil'jevič FOMIN. *Základy teorie funkcí a funkcionální analýzy: [určeno [též] pro posl. vys. škol techn. a universit].*[online] Praha: Státní nakladatelství technické literatury, 1975. Teoretická knižnice inženýra. Dostupné také z URL: <http://www.digitalniknihovna.cz/mzk/uuid/uuid:38ebe6e0-9fa2-11e4-94a8-005056827e51>.

[2] Elgazzar, A.S.: *Quantum prisoner's dilemma in a restricted one-parameter strategic space.* Applied Mathematics and Computation. 370, (2020) Dostupné také z URL: https://doi.org/10.1016/j.amc.2019.124927

[3] Flitney, A. P., Abbott D.: *An Introduction to quantum game theory*, Fluctuation and Noise Letters, Vol. 02, No. 04 R175– R187 (2002) Dostupné také z URL: https://doi.org/10.1142/S0219477502000981

[4] *Qiskit Introduction to Quantum Computing* Otevřený webový seminář zaměřený na základy kvantového počtu. Dostupný z URL: <https://qiskit.org/textbook-beta/summer-school/introduction-to-quantum-computing-and-quantum-hardware-2020/>.

[5] de Lima Marquezino Franklin, Portugal R., Lavor C.: A Primer on Quantum Computing. Springer Publishing Company (2019)

[6] Nielsen, M., Chuang, I.: *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge: Cambridge University Press (2010) Dostupné také z URL:10.1017/CBO9780511976667