UNIVERZA V LJUBLJANI

FAKULTETA ZA MATEMATIKO IN FIZIKO

Kvantna prepletenost

Podiplomski seminar

Avtor: Tilen Huljev Čadež

Mentor: prof. dr. Anton Ramšak

Ljubljana, Maj 2009

Povzetek

Predmet seminarja je kvantna prepletenost, ena od osnovnih količin v teoriji kvantne informatike in kvantnega računalništva. Na primeru kvantne teleportacije je prikazana uporabnost maksimalno prepletenih stanj. Stopnjo prepletenosti čistih stanj izračunamo z entropijo prepletenosti, medtem ko za mešana stanja izbira mere prepletenosti ni enolična. Predstavljene so splošne lastnosti, ki jih mora imeti mera prepletenosti, kot primer so podrobneje predstavljene tri mere prepletenosti dvodelnih (bipartitnih) stanj, in sicer cena prepletenosti, prepletenost destilacije in prepletenost formacije.

Kazalo

1 Uvod **3**
- 1.1 Zgodovina kvantne prepletenosti . . . 4
- 1.2 Zgled uporabe prepletenosti: Kvantna teleportacija . . . 5

2 Kvantna prepletenost **7**
- 2.1 Prepletenost čistih stanj . . . 7
- 2.2 Mešana stanja . . . 9
- 2.3 Kako do mer prepletenosti? . . . 10
- 2.4 Postulati za mere prepletenosti . . . 11
- 2.5 Pregled mer prepletenosti . . . 13
  - 2.5.1 Cena prepletenosti . . . 13
  - 2.5.2 Prepletenost destilacije . . . 14
  - 2.5.3 Prepletenost formacije . . . 14

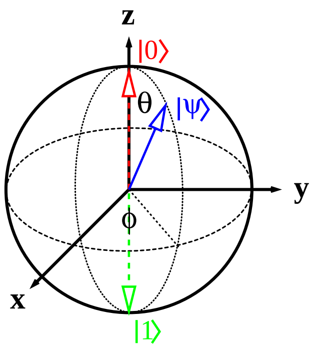
3 Zaključek **16**

1 Uvod

Najpreprostejši kvantni sistem je dvonivojski kvantni sistem oziroma *kvantni bit* (*kubit*) [1]. Stanje kubita je tipično definirano na mikroskopskem sistemu, kot je npr. jedrski spin, spin elektrona ali foton. S parom ortogonalnih stanj kubita lahko predstavimo dve logični stanji 0 in 1 (npr. horizontalna in vertikalna polarizacija fotona: $|0\rangle = |\leftrightarrow\rangle$, $|1\rangle = |\updownarrow\rangle$, ali pa projekcija spina elektrona: $|0\rangle = |\uparrow\rangle$, $|1\rangle = |\downarrow\rangle$). Splošno čisto stanje kubita je linearna kombinacija logičnih stanj

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

in ga geometrijsko predstavimo z enotskim vektorjem na *Blochovi sferi* (Slika 1). Ob projekcijski meritvi dobimo $|0\rangle$ z verjetnostjo $\cos^2(\Theta/2)$ in $|1\rangle$ z verjetnostjo $\sin^2(\Theta/2)$.



Slika 1: Kubit (1) na Blochovi sferi.

Splošno čisto stanje sistema n kubitov je oblike

$$|\Psi\rangle = \sum_{x=00...0}^{11...1} \alpha_x\,|x\rangle \tag{2}$$

kjer so α_x kompleksni koeficienti, za katera velja $\sum_x |\alpha_x|^2 = 1$ in $|x\rangle$ produkt n enodelčnih stanj. $|\Psi\rangle$ je torej enotski vektor v 2^n razsežnem Hilbertovem prostoru. V primeru dveh kubitov teče $|x\rangle$ po stanjih $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, zato tak sistem opišemo s superpozicijo teh štirih stanj

$$|\Psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle \tag{3}$$

Zamislimo si dva kubita, prvega v stanju $|\psi\rangle = \beta_0\,|0\rangle + \beta_1\,|1\rangle$ in drugega v stanju $|\phi\rangle = \gamma_0\,|0\rangle + \gamma_1\,|1\rangle$. Skupno stanje obeh je direkten (tenzorski) produkt posameznih stanj,

$$|\Psi\rangle = |\psi\rangle \otimes |\phi\rangle = \beta_0\gamma_0\,|00\rangle + \beta_0\gamma_1\,|01\rangle + \beta_1\gamma_0\,|10\rangle + \beta_1\gamma_1\,|11\rangle \tag{4}$$

Stanje dveh kubitov, enačba (3), je posebne oblike enačbe (4) samo v primeru, ko velja

$$\alpha_{00}\alpha_{11} = \alpha_{01}\alpha_{10}. \tag{5}$$

Enakost (5) ni izpolnjena za vsa stanja oblike (3), kar pomeni, da splošno čisto stanje dveh kubitov ni produkt dveh eno-kubitnih stanj. Podobno velja tudi za sistem n kubitov. Stanjem, ki jih ne moremo opisati s produktom enodelčnih stanj, pravimo *prepletena stanja*. Njihova značilnost je, da posamezen podsistem nima določenega čistega stanja, medtem ko ga cel sistem ima.

1.1 Zgodovina kvantne prepletenosti

V prvih desetletjih prejšnjega stoletja se je razvila kvantna mehanika, teorija, ki je uspešno pojasnila številna (takrat) odprta vprašanja v fiziki, kot je npr. stabilnost atoma. V kvantni mehaniki valovna funkcija opisuje stanje sistema, njen časovni razvoj pa podaja Schrödingerjeva enačba. Realne opazljivke so podane z operatorji, ki delujejo na valovno funkcijo, meritev pa je projekcija na lastne funkcije operatorja. Opazljivk, katerih pripadajoči operatorji med seboj ne komutirajo, ne moremo hkrati določiti.

S takim pogledom na svet se niso vsi strinjali. Zaradi lastnosti nekaterih posebnih kvantnih stanj[1] so Einstein, Podolsky in Rosen [2] leta 1935 zaključili, da iz popolnega opisa fizikalne realnosti z valovno funkcijo sledi, da imata nekomutirajoči opazljivki simultano realnost. Pri tem so fizikalno realnost definirali z besedami [2]: *Če lahko, brez da bi kakorkoli zmotili sistem, napovemo z gotovostjo (tj. verjetnostjo enako 1) vrednost fizikalne količine, potem obstaja element fizikalne realnosti, ki ustreza tej fizikalni količini.* Ta posebna stanja imajo lastnost, da z meritvijo enega dela podsistema v trenutku izvemo tudi stanje drugega dela podsistema, čeprav sta oba lahko poljubno prostorsko ločena. Če drugi podsistem gledamo kot sistem zase, lahko dobimo informacijo o nekomutirajočih opazljivkah tega sistema, brez da bi ga zmotili. To je t. i. lokalni realizem. Einstein, Podolsky in Rosen so tako zaključili, da opis stanja z valovno funkcijo ni popoln.

Skoraj trideset let kasneje je J. S. Bell pokazal [3], da statistične korelacije nekaterih kvantnih stanj ne moremo opisati z lokalno realistično teorijo. Omejitve take teorije so podane z Bellovimi neenačbami. Stanja, ki kršijo le te, pa so prepletena stanja. Na Bellove neenačbe danes lahko gledamo kot na poskus kvantifikacije kvantnih korelacij med kvantnimi stanji.

Danes se na kvantno prepletenost gleda kot na dobrino, uporabno v hitro razvijajočih se področjih kvantne informatike, kvantne kriptografije in kvantnega računalništva [4, 5]. Kot primer njene uporabnosti bom predstavil kvantno teleportacijo [6].

[1] Danes znanih kot maksimalno prepletena, EPR (Einstein-Podolsky-Rosen), Bellova, singletna stanja.

1.2 Zgled uporabe prepletenosti: Kvantna teleportacija

Naj oseba, imenujmo jo Ana, poseduje kvantni bit v njej neznanem stanju $|\Phi_1\rangle$. Recimo, da Ana želi to stanje posredovati drugi osebi, ki naj bo Bob. Trivialna možnost je, da Ana pošlje kvantni bit Bobu. V primeru, da Ana ne ve, kje se Bob nahaja ali pa direkten prenos ni mogoč, se Ana lahko posluži kvantne teleportacije. V tem procesu nastopajo trije kubiti, od katerih je prvi v neznanem stanju

$$|\Phi_1\rangle = \alpha\,|0_1\rangle + \beta\,|1_1\rangle, \tag{6}$$

druga dva pa sta pripravljena v maksimalno prepletenem stanju

$$|\Psi_{23}^-\rangle = \frac{1}{\sqrt{2}}(|0_2\rangle|1_3\rangle - |1_2\rangle|0_3\rangle). \tag{7}$$

Števili 2 in 3 označujeta delca v singletu. Eden od delcev v EPR paru je pred teleportacijo v Anini (delec 2) in drugi v Bobovi (delec 3) lasti. V tem trenutku ima Ana dva delca (1 in 2), Bob pa tretjega. Celotni sistem teh treh delcev je v produktnem stanju

$$|\Psi_{123}\rangle = |\Phi_1\rangle|\Psi_{23}^-\rangle = \frac{\alpha}{\sqrt{2}}(|0_1\rangle|0_2\rangle|1_3\rangle - |0_1\rangle|1_2\rangle|0_3\rangle) + \frac{\beta}{\sqrt{2}}(|1_1\rangle|0_2\rangle|1_3\rangle - |1_1\rangle|1_2\rangle|0_3\rangle) \tag{8}$$

vendar EPR par zaenkrat ne vsebuje nobene informacije o stanju prvega delca. Da poveže EPR par s prvim delcem, Ana opravi meritev svojih dveh delcev v Bellovi bazi

$$\begin{aligned} |\Psi_{12}^\pm\rangle &= \frac{1}{\sqrt{2}}(|0_1\rangle|1_2\rangle \pm |1_1\rangle|0_2\rangle), \\ |\Phi_{12}^\pm\rangle &= \frac{1}{\sqrt{2}}(|0_1\rangle|0_2\rangle \pm |1_1\rangle|1_2\rangle). \end{aligned} \tag{9}$$

Enačba (8) se lahko prepiše v obliko

$$\begin{aligned} |\Psi_{123}\rangle &= \frac{1}{2}\Big[|\Psi_{12}^-\rangle\,(-\alpha\,|0_3\rangle - \beta\,|1_3\rangle) + |\Psi_{12}^+\rangle\,(-\alpha\,|0_3\rangle + \beta\,|1_3\rangle) \\ &+ |\Phi_{12}^-\rangle\,(\alpha\,|1_3\rangle + \beta\,|0_3\rangle) + |\Phi_{12}^+\rangle\,(\alpha\,|1_3\rangle - \beta\,|0_3\rangle)\Big]. \end{aligned} \tag{10}$$

Ne glede na začetno stanje $|\Phi_1\rangle$ je rezultat Anine meritve eno od Bellovih stanj (9), in sicer je verjetnost za katerokoli od teh stanj enaka 1/4. Po meritvi se tudi delec 3 v Bobovi lasti projicira v eno od čistih stanj v enačbi (10), glede na izid Anine meritve. Ko Ana s klasičnim signalom sporoči Bobu rezultat meritve, mora Bob opraviti unitarno transformacijo na svojem delcu kot je prikazano v tabeli (1). V vsakem primeru ima po končani teleportaciji Bob delec v stanju, ki je kopija prvotnega stanja (6), Ani pa ostaneta delca 1 in 2, ki sta maksimalno prepletena, brez sledu o prvotnem stanju. Če bi Bob želel uganiti Anin rezultat meritve, preden bi ga prejel prek klasične informacije, bi njegov delec končal v maksimalno mešanem stanju. Klasična komunikacija od Ane do Boba je za teleportacijo nujna in zagotavlja upoštevanje posebne teorije relativnosti. Za uspešno teleportacijo bi lahko uporabili katerikoli maksimalno prepleten par, teleportacija pa se lahko posploši tudi na sisteme, ki imajo več kot 2 ortogonalni stanji [6].

Rezultat Anine meritve	Bobova transformacija
$\vert\Psi_{12}^{-}\rangle$	I
$\vert\Psi_{12}^{+}\rangle$	σ_z
$\vert\Phi_{12}^{-}\rangle$	σ_x
$\vert\Phi_{12}^{+}\rangle$	σ_y

Tabela 1: Unitarne transformacije, ki jih mora opraviti Bob glede na rezultat Anine meritve.

Eksperimentalna kvantna teleportacija

Do sedaj so izvedli teleportacijo s fotoni in jedrskim spinom [7, 8, 9, 10, 11]. Pri teh poizkusih je bilo najtežje ustvariti in izmeriti EPR pare.

Pri teleportaciji fotonov se kot stanji $|0\rangle$ in $|1\rangle$ uporablja polarizacija fotonov. Prvo uspešno teleportacijo [7] so izvedli z začetnim EPR parom v singletnem stanju $|\psi_{23}^{-}\rangle$, ki so ga dobili s *parametrično konverzijo*, nelinearnim optičnim pojavom, pri katerem iz enega fotona nastaneta dva in z Bellovo meritvijo samo singletnega stanja $|\psi_{12}^{-}\rangle$. Le ta se je zgodila z verjetnostjo 1/4, v tem primeru pa je imel Bob že v lasti teleportirano stanje. Uspešnost teleportacije je bila dokazana s koincidenčnimi meritvami. Z uporabo nelinearnih optičnih pojavov je druga skupina [8] opravila teleportacijo z meritvijo vseh štirih Bellovih stanj, vendar tudi brez Bobove unitarne transformacije. Zaradi manjše verjetnosti za nelinearne pojave, je bila frekvenca uspešnih teleportacij manjša kot pri zgornji meritvi. Odmevna je bila teleportacija, ki je leta 2004 uspela skupini avstrijskih fizikov [9]. V realnih pogojih so teleportirali polariziran foton skozi 800 m dolg optični vodnik, ki je bil položen v kanalizacijskem sistemu pod reko Donavo. Vodnik je bil izpostavljen temperaturnim fluktuacijam in ostalim zunanjim dejavnikom. Ana je opravila dve izmed štirih Bellovih meritev ($|\Psi_{12}^{+}\rangle$ in $|\Psi_{12}^{-}\rangle$), kar je maksimum, ki se ga da doseči z uporabo linearne optike. Pri tem eksperimentu je bil prvič uporabljen klasični kanal in opravljena unitarna transformacija z Bobove strani, ki je bila izvedena z uporabo elektro-optičnega modulatorja. Meritev dveh Bellovih stanj je podvojila frekvenco teleportacij glede na prvo uspešno teleportacijo [7] in je znašala 0.04 s^{-1}. Poleg polarizacije fotonov kot osnovnih stanj kubita, lahko uporabimo tudi časovne bine (angl. time-bin), ki so pari časovno oziroma posledično krajevno zakasnjenih verjetnostnih amplitud. Tak kubit je superpozicija dveh časovnih binov. Teleportacijo te vrste so izvedli [10] pri telekomunikacijskih valovnih dolžinah $(1.3, 1.55\,\mu\text{m})$ skozi standardni telekomunikacijski optični vodnik dolžine 2 km.

Uspešno so teleportirali tudi jedrski spin, in sicer na molekuli tri-kloro-etilena (TCE) [11].

Pri tem eksperimentu so z jedrsko magnetno resonanco teleportirali začetno stanje ogljikovega (^{13}C) spina na atom vodika (H). Ker je teleportacija potekla le na razdalji desetink nanometra, je bila to bolj demonstracija metode, kot pa praktično uporabna vrsta teleportacije.

2 Kvantna prepletenost

2.1 Prepletenost čistih stanj

Kvantna prepletenost se uporablja v teoriji kvantne informatike in računalništva v številnih procesih (npr. teleportacija, gosto kodiranje, algoritmi...). Zato je koristno uvesti količino, ki za dano valovno funkcijo $|\psi\rangle$ ovrednoti stopnjo prepletenosti. Oglejmo si to na primeru teleportacije.

Naj si Ana in Bob delita stanje

$$|\Psi_{23}\rangle = \cos(\vartheta)|0_2 1_3\rangle - \sin(\vartheta)|1_2 0_3\rangle, \tag{11}$$

ki je produktno za $\vartheta = 0, \pi/2$, prepleteno sicer in singletno za $\vartheta = \pi/4$. Tridelčna valovna funkcija je pred Anino meritvijo

$$\begin{aligned} |\Psi_{123}\rangle &= \frac{1}{\sqrt{2}}\Big[|\Psi^-_{12}\rangle\,(-\beta\,\cos(\vartheta)\,|1_3\rangle - \alpha\,\sin(\vartheta)\,|0_3\rangle) + |\Psi^+_{12}\rangle\,(\beta\,\cos(\vartheta)\,|1_3\rangle - \alpha\,\sin(\vartheta)\,|0_3\rangle) \\ &+ |\Phi^-_{12}\rangle\,(\alpha\,\cos(\vartheta)\,|1_3\rangle + \beta\,\sin(\vartheta)\,|0_3\rangle) + |\Phi^+_{12}\rangle\,(\alpha\,\cos(\vartheta)\,|1_3\rangle - \beta\,\sin(\vartheta)\,|0_3\rangle)\Big] \end{aligned} \tag{12}$$

in je za singlet enaka enačbi (10). Ko Ana opravi meritev v Bellovi bazi (9) se Bobov kubit projicira v ustrezno stanje v enačbi (12). Izid Anine meritve je odvisen od začetnega stanja (6), saj so verjetnosti za posamezen izid $\mathrm{P}(|\varphi_{12}\rangle) = \langle\varphi_{12}|(\mathrm{T}r_3|\Psi_{123}\rangle\langle\Psi_{123}|)|\varphi_{12}\rangle$ in sicer $\mathrm{P}(|\Psi^{\pm}_{12}\rangle) = 1/2\,(|\alpha|^2\sin^2(\vartheta) + |\beta|^2\cos^2(\vartheta))$ ter $\mathrm{P}(|\Phi^{\pm}_{12}\rangle) = 1/2\,(|\beta|^2\sin^2(\vartheta) + |\alpha|^2\cos^2(\vartheta))$. Recimo[2], da Ana izmeri singlet $|\Psi^-_{12}\rangle$. Bobovo stanje je (do predznaka) v tem primeru

$$|\psi_k\rangle = \frac{\alpha\,\sin(\vartheta)\,|0_3\rangle + \beta\,\cos(\vartheta)\,|1_3\rangle}{\sqrt{|\alpha|^2\sin^2(\vartheta) + |\beta|^2\cos^2(\vartheta)}}.$$

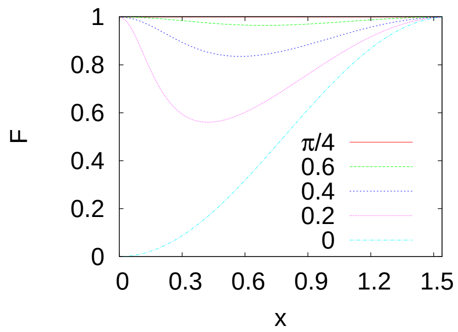
Če bi Bob želel transformirati stanje $|\psi_k\rangle$ v stanje oblike (6), bi moral za konstrukcijo unitarne transformacije poznati koeficienta v začetnem stanju, saj je le ta odvisna od teh koeficientov. Vendar pa je v primeru poznavanja koeficientov v začetnem stanju teleportacija nepotrebna, saj bi Bob ustrezno stanje lahko pripravil lokalno. Druga možnost je, da bi Bob po prejemu izida Anine meritve opravil ustrezno transformacijo iz tabele (1), ki je za singlet identiteta. V tem primeru je Bobovo končno stanje kar $|\psi_k\rangle$ in ni enako stanju

[2]Za ostale tri izide bi bila nadaljna obravnava podobna, zaključki pa enaki.

$|\phi_z\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \cos(x)|0\rangle + \sin(x)\,e^{i\phi}|1\rangle$, ki smo ga želeli teleportirati. Verjetnost, da je končno stanje izmerjeno kot začetno stanje nam podaja *zvestoba* (fidelity)

$$F = |\langle\psi_k|\phi_z\rangle|^2 = \frac{(\cos^2(x)\sin(\vartheta) + \sin^2(x)\cos(\vartheta))^2}{\cos^2(x)\sin^2(\vartheta) + \sin^2(x)\cos^2(\vartheta)}, \tag{13}$$

ki je za singlet enaka 1, sicer pa je odvisna od začetnega stanja in je splošno manjša od 1 (Slika 2).



Slika 2: Zvestoba kvantne teleportacije, enačba (13), v odvisnosti od izbranega začetnega stanja pri različnih vrednostih ϑ.

Kvantna teleportacija je uspešna samo v primeru, da si Ana in Bob na začetku delita singletno stanje. Če pa si delita stanje (11) teleportacija ni popolna in je odvisna od ϑ ter od samega stanja, ki ga želimo teleportirati.

Za čisto stanje para kuditov[3], tj. stanja, ki ga zapišemo v obliki

$$|\psi\rangle = \sum_{x=11}^{dd} \alpha_x\,|x\rangle$$

je količina E_P, ki meri prepletenost definirana [12] kot *entropija prepletenosti* (entropy of entanglement),

$$E_P(|\psi\rangle\langle\psi|) = S(\mathrm{Tr}_{A(B)}(|\psi\rangle\langle\psi|)) \tag{14}$$

in je $S(\sigma) = -\mathrm{T}r(\sigma\,\log_2\sigma)$ *von-Neumannova entropija* in σ podana z delno sledjo $|\psi\rangle\langle\psi|$ po podsistemu $A(B)$.

Kot zgled si oglejmo entropijo prepletenosti naslednjega stanja

$$|\psi_u\rangle = \cos(\vartheta)\,|01\rangle + e^{i\varphi}\,\sin(\vartheta)\,|10\rangle,$$

ki za $\varphi = \pi$ ustreza stanju (11). Razpišemo

$$|\psi_u\rangle\langle\psi_u| = \cos^2(\vartheta)\,|01\rangle\langle 01| + \sin^2(\vartheta)\,|10\rangle\langle 10| + 1/2\,\sin(2\vartheta)[e^{i\varphi}|10\rangle\langle 01| + e^{-i\varphi}|01\rangle\langle 10|]$$

[3] d-dimenzionalni kvantni sistem.

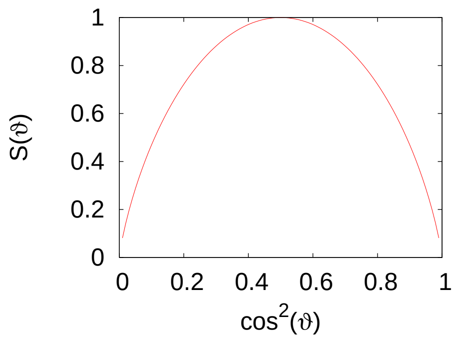
ter

$$\sigma = \mathrm{Tr}_A(|\psi_u\rangle\langle\psi_u|) = \cos^2(\vartheta)\,|1\rangle\langle 1| + \sin^2(\vartheta)\,|0\rangle\langle 0|$$

in izračunamo entropijo prepletenosti

$$E_P(|\psi_u\rangle\langle\psi_u|) = S(\vartheta) = -2\Big(\cos^2(\vartheta)\,\log_2[\cos(\vartheta)] + \sin^2(\vartheta)\,\log_2[\sin(\vartheta)]\Big).$$

Za primer $\vartheta = 0$ je stanje separabilno in entropija prepletenosti[4] $E_P = 0$, medtem ko je za primer $\vartheta = \pi/4$ stanje maksimalno prepleteno $E_P = 1$ (Slika 3).



Slika 3: Entropija prepletenosti stanja $|\psi_u\rangle$.

2.2 Mešana stanja

Čisto stanje $|\psi\rangle$ lahko zapišemo z gostotno matriko

$$\rho = |\psi\rangle\langle\psi|.$$

Poleg čistih stanj obstajajo tudi *mešana stanja*, ki so linearna kombinacija gostotnih matrik čistih stanj

$$\rho = \sum_i p_i\,|\psi_i\rangle\langle\psi_i|. \tag{15}$$

Množica parov $\{p_i, |\psi_i\rangle\}$, ki nastopajo v enačbi (15), je dekompozicija gostotne matrike ρ na čista stanja $|\psi_i\rangle$, ki se v mešanem stanju pojavijo z verjetnostjo p_i ($\sum_i p_i = 1$). Za mešano stanje obstaja neskončno dekompozicij gostotne matrike.

Za sistem v termičnem ravnovesju z okolico velja $p_i \propto \exp(-\beta\varepsilon_i)$, kjer je ε_i energija lastnega stanja $|\psi_i\rangle$ in $\beta^{-1} = k_B T$.

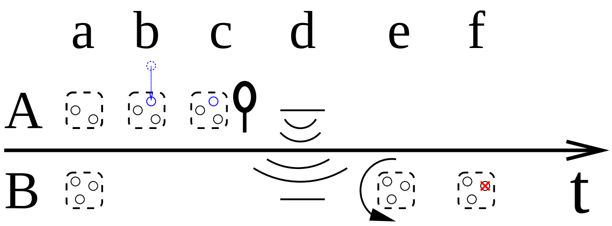
[4] Pri definiciji enačbe (14) velja dogovor $0\log_2[0] := 0$.

2.3 Kako do mer prepletenosti?

Podobno kot je merilo prepletenosti čistih stanj entropija prepletenosti (14), bi radi poiskali mero tudi za mešana stanja[5]. Separabilno mešano stanje zapišemo v obliki

$$\rho = \sum_i p_i \, \rho_A^i \otimes \rho_B^i \tag{16}$$

kjer je p_i verjetnostna porazdelitev. Stanje oblike (16) lahko ustvarita Ana in Bob lokalno, s tem da se s klasično komunikacijo dogovorita za izbrano porazdelitev in lokalno ustvarita pripadajoča stanja $\rho^i_{A/B}$. Take vrste operacij spadajo pod t. i. lokalne operacije in klasično komunikacijo - LOKK (Slika 4).



Slika 4: Lokalne operacije in klasična komunikacija: Imamo kvantni sistem, ki je sestavljen iz dveh prostorsko (poljubno) oddaljenih podsistemov A in B (a). V posamezen podsistem lahko dodamo delce (b) in na njem opravljamo meritve (c). S klasično komunikacijo lahko usklajujemo delovanje na podsistema oz. si sporočamo rezultate meritev (d). Glede na dobljene podatke lahko opravljamo lokalne unitarne transformacije (e) in/ali pa zavržemo del podsistema (f).

Z LOKK lahko ustvarimo le separabilna stanja, zato z njimi ne moremo ustvariti prepletenega stanja iz začetno neprepletenega. Velja pa tudi močnejša trditev [12, 13]. Recimo, da znamo z LOKK iz nekega stanja ρ narediti stanje σ. Potem vse kar lahko naredimo s stanjem σ in LOKK, lahko naredimo tudi z ρ in LOKK. Uporabnost kvantnih stanj se z LOKK ne poveča in lahko rečemo, da je stanje ρ vsaj toliko prepleteno kot stanje σ. Direktna posledica te lastnosti LOKK je, da se stopnja prepletenosti mešanega stanja ne spremeni[6] pri lokalni unitarni transformaciji U.

Naravno vprašanje, ki se pojavi pri obravnavi prepletenosti je ali obstajajo maksimalno prepletena stanja? Odgovor je pritrdilen vsaj v primeru dvodelnih (bipartitnih) sistemov sestavljenih iz dveh d-dimenzionalnih podsistemov (kuditov). Izkaže se, da je vsako stanje,

[5]Entropije prepletenosti v tem primeru ne moremo uporabiti zaradi neskončnega števila dekompozicij na čista stanja.

[6]Vsaka lokalna unitarna transformacija (LUT) ima inverz, ki je tudi LUT. Če je torej $U\rho = \sigma$ potem $E(\rho) \geq E(\sigma)$, hkrati pa velja tudi $U^{-1}\sigma = \rho$ in $E(\sigma) \geq E(\rho)$, torej $\rightarrow E(\rho) = E(\sigma)$, kjer $E(\rho)$ označuje mero prepletenosti stanja ρ.

ki je unitarno ekvivalentno[7] stanju

$$|\psi_d^+\rangle = \frac{1}{\sqrt{d}}\left(|0,0\rangle + |1,1\rangle + \cdots + |d-1,d-1\rangle\right)$$

maksimalno prepleteno, saj lahko iz tega stanja z LOKK ustvarimo poljubno čisto ali mešano bipartitno stanje dveh kuditov.

Ali je možno poiskati LOKK med splošnimi čistimi dvodelnimi stanji, tj. $|\psi\rangle \to |\varphi\rangle$? Iskanje odgovora nam da potrebne in zadostne pogoje za možnost takih manipulacij med čistimi stanji, poleg tega pa ponudi tudi protokole, s katerimi opravimo konverzijo. Ugotovimo, da obstajajo tudi pari stanj, ki jih med seboj ne moremo pretvoriti. Taki pari stanj so med seboj *neprimerljivi*, saj nobenemu ne moremo pripisati večje prepletenosti. Problemu neprimerljivosti parov čistih stanj se izognemo z omilitvijo zahteve po eksaktnem končnem stanju in se zadovoljimo s približnim končnim stanjem. Vendar pa je v tem primeru verjetnost za uspešno konverzijo odvisna od 'razlike' med eksaktnim in približnim končnim stanjem.

Do sedaj smo spoznali, da LOKK le delno uredijo čista prepletena stanja, medtem ko problem konverzije med mešanimi stanji sploh (še) ni rešen. Če želimo odgovoriti na vprašanje ali je neko (poljubno) stanje bolj prepleteno od drugega moramo nanj pogledati z drugega zornega kota. Primerjava je možna pri obravnavi LOKK transformacij med stanji v t. i. *asimptotskem režimu*. Namesto, da poizkušamo z LOKK transformirati $\rho \to \sigma$, se vprašamo ali je za naravni števili n, m možno poiskati LOKK transformacijo $\rho^{\otimes n} \to \sigma^{\otimes m}$, kjer je $\rho^{\otimes n}$ stanje, sestavljeno iz n enakih podsistemov ρ in podobno $\sigma^{\otimes m}$. Največje razmerje m/n, ki ga lahko dosežemo nam da informacijo o relativni prepletenosti med stanjema ρ in σ. Fizikalno se zadovoljimo s približnimi LOKK transformacijami $\rho^{\otimes n} \to \sigma_m$, ki v asimptotski limiti $n \to \infty$ pri fiksnem m/n postanejo poljubno natančne ($\sigma_m \to \sigma^{\otimes m}$). Takšna obravnava popolnoma uredi čista bipartitna stanja in vodi do mer kvantne prepletenosti.

2.4 Postulati za mere prepletenosti

V asimptotski limiti je manipulacija prepletenih čistih bipartitnih stanj z LOKK reverzibilna, iz česar sledi popolna urejenost takih stanj. Pri mešanih stanjih je situacija bolj kompleksna. Zato uporabimo aksiomatski pristop, s tem da definiramo funkcionale, ki vsebujejo lastnosti iz prejšnjega poglavja in z njimi pripišemo količino prepletenosti kvantnim stanjem. Na ta način so bile v zadnjih letih vpeljane številne mere kvantne prepletenosti, kot npr.[8] *prepletenost destilacije* (entanglement of distillation) [12, 14], *cena prepletenosti* (entanglement cost) [12, 15], *prepletenost formacije* (entanglement of formation) [12, 14, 16], *relativna entropija prepletenosti* (relative entropy of entanglement) [13]. Splošno si za mero

[7] Vsako stanje oblike $U|\psi_d^+\rangle$, kjer je U poljubna lokalna unitarna transformacija.

[8] Slovenskih imen za mere prepletenosti ni, zato sem imena prevedel, dodal pa sem originalna imena izrazov.

prepletenosti želimo, da izmeri kvantne korelacije, ki omogočajo izvedbo določenega kvantno informacijskega procesa. Zaradi različnih procesov so tudi lastnosti mer različne. Ne glede na vrsto procesa pa lahko mere prepletenosti vpeljemo s postulati [17]:

1. Mera kvantne prepletenosti je preslikava (funkcional), ki vsaki gostotni matriki ρ priredi pozitivno realno število
$$\rho \to E(\rho) \in \mathbb{R}^+$$
in je definirana za poljuben bipartitni sistem. Pogosto je v definicijo vključen normalizacijski faktor, tako da je prepletenost maksimalno prepletenega stanja dveh kuditov enaka $E(|\psi_d^+\rangle\langle\psi_d^+|) = \log_2(d)$.

2. $E(\rho) = 0$ za separabilna stanja ρ.

3. Mera prepletenosti se ne poveča pri LOKK.

4. Za čisto stanje $\rho = |\psi\rangle\langle\psi|$ se prepletenost reducira na entropijo prepletenosti (14).

Dodatne lastnosti nekaterih mer prepletenosti so:

- *Konveksnost*
To je lastnost mere kvantne prepletenosti
$$E(\sum_i p_i\, \rho_i) \leq \sum_i p_i\, E(\rho_i).$$
Ta lastnost je posledica izgube informacije v procesu, ko iz znanih stanj ρ_i, ki se pojavijo z verjetnostjo p_i, dobimo mešanico stanj oblike $\rho = \sum_i p_i\, \rho_i$.

- *Aditivnost*
Če velja $E(\rho^{\otimes n}) = nE(\rho)$ za vsako celo število n in stanje ρ potem je mera E aditivna. V nasprotnem primeru jo lahko redefiniramo v *regularizirani* oz. *asimptotski* obliki
$$E^\infty(\rho) := \lim_{n\to\infty} \frac{E(\rho^{\otimes n})}{n} \tag{17}$$
ki je avtomatsko aditivna. Močnejša je zahteva polne aditivnosti, kjer za poljubni stanji ρ in σ velja $E(\rho \otimes \sigma) = E(\rho) + E(\sigma)$.

- *Asimptotska zveznost*
Mera E je asimptotsko zvezna, če za vsako mešano stanje n parov kuditov ρ_n, za katero velja $\lim_{n\to\infty}\langle\psi^{\otimes n}|\rho_n|\psi^{\otimes n}\rangle = 1$ sledi
$$\frac{1}{n}|E(|\psi^{\otimes n}\rangle) - E(\rho_n)| \to 0$$
kjer je $|\psi\rangle$ poljubno čisto stanje para.

Četrti postulat se na prvi pogled zdi omejujoč, vendar pa je precej naraven. Entropija prepletenosti (14) namreč predstavlja razmerje reverzibilne pretvorbe med čistimi stanji v asimptotskem režimu [12], zato je primerna mera prepletenosti za čista stanja. Da pa se pokazati [18], da je vsak funkcional L, ki mešanemu stanju ρ priredi pozitivno realno število ($L(\rho) : \rho \to \mathbb{R}^+$) za čista stanja ekvivalenten entropiji prepletenosti natanko tedaj ko je L:

- normalizirana na singletno stanje
- aditivna na čistih stanjih
- nenaraščajoča pri LOKK med čistimi stanji
- asimptotsko zvezna na čistih stanjih

Zanimivo je, da je zadosten in nujen pogoj omejen le na lastnosti funkcije L za čista stanja.

Do sedaj smo navedli že nekaj pogojev, ki jih mora izpolniti vsaka mera kvantne prepletenosti. Izkaže pa se [18, 19], da lahko navzgor in navzdol omejimo vse možne mere prepletenosti. Natančneje, imejmo količino $L'(\rho)$, ki zadošča pogojem 1-3 in je asimptotsko zvezna na mešanih stanjih. Potem velja [18, 19]

$$E_C(\rho) \geq \underbrace{\lim_{n\to\infty} \frac{L'(\rho^{\otimes n})}{n}}_{L'^{\infty}(\rho)} \geq E_D(\rho) \tag{18}$$

kjer sta E_C cena prepletenosti in E_D prepletenost destilacije, ki jih bom predstavil v naslednjem poglavju.

Kot smo ugotovili, do sedaj ne obstaja enotna ureditev splošnih bipartitnih kvantnih stanj glede na kvantno prepletenost. Možna pot k enotni meri prepletenosti bipartitnih stanj je posplošitev operacij LOKK [20]. Zaenkrat pa se sprijaznimo z raznimi merami prepletenosti, kot posledica različnih procesov, ki jih opisujejo.

2.5 Pregled mer prepletenosti

2.5.1 Cena prepletenosti

Cena prepletenosti $E_C(\rho)$ meri minimalno možno razmerje $r = m/n$, da iz m singletov z LOKK ustvarimo n približnih stanj ρ, ki so v limiti $n \to \infty$ enaki stanjem ρ. Naj Λ označuje splošno LOKK operacijo in naj bo $P_+(K) = |\psi_K^+\rangle\langle\psi_K^+|$ gostotna matrika maksimalno prepletenega stanja v K dimezionalnem Hilbertovem prostoru. Potem je cena prepletenosti definirana

$$E_C(\rho) := \inf\{r; \lim_{n\to\infty} [\inf_{\Lambda} \mathrm{Tr}|\rho^{\otimes n} - \Lambda(P_+(2^{rn}))|] = 0\} \tag{19}$$

kjer je $\mathrm{T}r|\sigma - \rho|$ razdalja[9] med stanjema σ in ρ. Ta mera prepletenosti je pomembna saj pove 'število singletov' potrebno za pretvorbo v (poljubno) končno stanje $\rho^{\otimes n}$, v limiti $n \to \infty$. Kot pa je razvidno iz definicije (19), je zaradi minimizacije E_C težko izračunati za splošen ρ.

2.5.2 Prepletenost destilacije

Obraten proces kot v prejšnjem primeru je pridobivanje maksimalno prepletenih parov iz množice začetnih stanj $\rho^{\otimes n}$. Ta proces nam meri prepletenost destilacije[10] $E_D(\rho)$, ki je formalno definirana

$$E_D(\rho) := \sup\{r; \lim_{n\to\infty}[\inf_{\Lambda} \mathrm{T}r|\Lambda(\rho^{\otimes n}) - P_+(2^{rn})|] = 0\} \tag{20}$$

Prepletenost destilacije je pomembna mera, saj so singleti osnovna dobrina številnih kvantno-informacijskih procesov, kot je npr. kvantna teleportacija. V praksi ne moremo izolirati kvantnega sistema od okolice, zato tudi singlet s časom postane mešano stanje, kar je proces znan kot *dekoherenca*. Proti dekoherenci se Ana in Bob lahko 'borita' z destilacijo.

Kot nam pove neenakost (18) je $E_C(\rho) \geq E_D(\rho)$, enakost pa velja (postulat 4.) za čista stanja, saj sta v tem primeru obe prepletenosti enaki entropiji prepletenosti (14). Optimalno razmerje za pretvorbo stanja $|\psi_1\rangle$ v $|\psi_2\rangle$ lahko enostavno določimo, saj iz N enakih stanj $|\psi_1\rangle$ najprej destiliramo $\approx N\,E(|\psi_1\rangle\langle\psi_1|)$ singletov in iz njih ustvarimo $M \approx N\,E(|\psi_1\rangle\langle\psi_1|)/E(|\psi_2\rangle\langle\psi_2|)$ stanj $|\psi_2\rangle$. V limiti so aproksimacije točne in je optimalna vrednost pretvorbe $E(|\psi_1\rangle\langle\psi_1|)/E(|\psi_2\rangle\langle\psi_2|)$.

Tudi prepletenost destilacije je definirana prek ekstremizacije in jo je težko izračunati (razen za čista stanja). Navzgor jo omejimo z vsako drugo mero prepletenosti (18), medtem ko spodnje meje določajo eksplicitni protokoli, npr. [15].

2.5.3 Prepletenost formacije

Definicija prepletenosti formacije je naslednja [12, 14]: Imejmo gostotno matriko ρ bipartitnega kvantnega sistema in si zamislimo vse možne dekompozicije matrike ρ na ansambel čistih stanj $|\psi_i\rangle$ s pripadajočimi verjetnostmi p_i, tako da velja enačba (15). Potrebno je ponovno poudariti, da je takih dekompozicij za mešana stanja neskončno. Prepletenost formacije mešanega stanja ρ je definirana kot povprečna entropija prepletenosti (14) čistih stanj neke dekompozicije, minimizirana po vseh možnih dekompozicijah matrike ρ. Oziroma

$$E_F(\rho) := \inf\Big\{\sum_i p_i\,E(|\psi_i\rangle\langle\psi_i|); \rho = \sum_i p_i\,|\psi_i\rangle\langle\psi_i|\Big\} \tag{21}$$

[9] Izbira razdalje ni enolična [20, 21], uporablja se npr. norma sledi (trace norm distance) $\mathrm{T}r|\eta| = \mathrm{T}r\sqrt{\eta^\dagger\eta} = \sum_i \lambda_i$, kjer so λ_i koreni iz lastnih vrednosti matrike $\eta^\dagger\eta$.

[10] Če so začetna stanja čista, se proces imenuje koncentracija prepletenosti [12].

Prepletenost formacije je podobno kot cena prepletenosti definirana prek minimizacije. Pomembna razlika med njima je, da je E_C asimptotska količina, ki obravnava stanja $\rho^{\otimes n}$ v limiti $n \to \infty$. Da se pokazati [21], da je asimptotska verzija (17) prepletenosti formacije

$$E_F^\infty(\rho) := \lim_{n\to\infty} \frac{E_F(\rho^{\otimes n})}{n}$$

enaka ceni prepletenosti, torej

$$E_F^\infty(\rho) = E_C(\rho) \tag{22}$$

Izračun obeh asimptotskih količin je težak. Zaenkrat kaže, kar pa še ni bilo dokazano, da je prepletenost formacije aditivna, iz česar bi sledilo $E_F(\rho) = E_F^\infty(\rho)$. Ta rezultat bi, v primeru da bi bil dokazan, olajšal izračun cene prepletenosti $E_C(\rho)$. Poleg tega je E_F tesno povezana s klasično kapaciteto kvantnega kanala, ki je podana s Holevovo kapaciteto [22], da pa se pokazati, da je zahteva aditivnosti E_F ekvivalentna aditivnosti kapacitete klasične komunikacije skozi kvantne kanale [23].

Za bipartitne sisteme kubitov je možno prepletenost formacije izračunati analitično - najti dekompozicijo, ki minimizira povprečno entropijo prepletenosti v enačbi (21) - z uporabo Woottersove formule [24, 16]

$$C(\rho) = \max\,(0, 2\,\lambda_{max} - \sum_i \lambda_i) \tag{23}$$

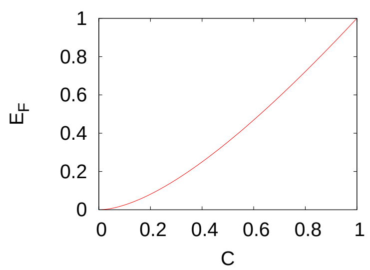
kjer je C konkurenca, ki je bijektivno povezana s prepletenostjo formacije (Slika 5) preko

$$E(\rho) = \mathcal{E}(C) \tag{24}$$

ter je funkcija $\mathcal{E}$ podana kot

$$\begin{aligned} \mathcal{E}(C) &= h\Big(\frac{1+\sqrt{1-C^2}}{2}\Big), \\ h(x) &= -x\,\log_2 x - (1-x)\,\log_2(1-x) \end{aligned} \tag{25}$$

in so λ_i kvadratni koreni lastnih vrednosti ne-Hermitske matrike $\rho\,\sigma_y \otimes \sigma_y\,\rho^*\,\sigma_y \otimes \sigma_y$.



Slika 5: Prepletenost formacije kot funkcija konkurence.

3 Zaključek

Kvantna prepletenost je lastnost mikroskopskih sistemov, ki je ne moremo opisati klasično. Je osnovna dobrina v teoriji kvantne informatike in kvantnega računalništva, kjer se uporablja v procesih kot je npr. kvantna teleportacija. Uporabnost različnih prepletenih stanj v teh procesih ni enaka, zato je pomembna vpeljava mere, ki ovrednoti stopnjo prepletenosti. Izbira mere ni enolična, v seminarju pa so predstavljene splošne lastnosti mer in tri pomembne mere kvantne prepletenosti dvodelnih kvantnih sistemov.

Literatura

[1] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).

[2] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).

[3] J. S. Bell, Physics **1**, 195 (1964).

[4] C. H. Bennett and D. P. DiVincenzo, Nature **404**, 247 (2000).

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[6] C. H. Bennett *et al.*, Phys. Rev. Lett. **70**, 1895 (1993).

[7] D. Bouwemeester *et al.*, Nature **390**, 575 (1997).

[8] Y.-H. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001).

[9] R. Ursin *et al.*, Nature **430**, 849 (2004).

[10] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, Nature **421**, 509 (2003).

[11] M. A. Nielsen, E. Knill, and R. Laflamme, Nature **396**, 52 (1998).

[12] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[13] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, Phys. Rev. Lett. **78**, 2275 (1997).

[14] C. H. Bennett *et al.*, Phys. Rev. Lett. **76**, 722 (1996).

[15] C. H. Bennett, D. P. DiVincenzo, J. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).

[16] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).

[17] M. B. Plenio and S. Virmani, Quantum Inf. Comput. **7**, 1 (2007), arXiv:quant-ph/0504163.

[18] M. J. Donald, M. Horodecki, and O. Rudolph, J. Math. Phys. **43**, 4252 (2002).

[19] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. Lett. **84**, 2014 (2000).

[20] K. Audenaert, M. B. Plenio, and J. Eisert, Phys. Rev. Lett. **90**, 027901 (2003).

[21] P. M. Hayden, M. Horodecki, and B. M. Terhal, J. Phys. A **34**, 6891 (2001).

[22] A. S. Holevo, IEEE Trans.Info.Theor. **44** (1998).

[23] A. A. Pomeransky, Phys. Rev. A **68**, 032317 (2003).

[24] S. Hill and W. K. Wootters, Phys. Rev. Lett. **78**, 5022 (1997).