UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO
ODDELEK ZA FIZIKO

Jernej Mravlje

Pomen prepletenosti kvantnih stanj za teorijo in aplikacijo

Seminar

Mentor: Anton Ramšak

Ljubljana, 2005

Povzetek

Einstein se nikdar ni mogel sprijazniti z dejstvom, da nekatera kvantna stanja niso lokalne narave. Nelokalnost in (navidezno) kontradikcijo v napovedih kvantne teorije je izpostavil v znamenitem Einstein-Podolsky-Rosen-ovem paradoksu in nadomestno rešitev iskal v teorijah s skritimi spremenljivkami. Bell je združil omejitve, ki veljajo za poljubno teorijo s skritimi spremenljivkami v Bellovo neenakost. Eksperiment je potrdil kršitev Bellove neenakosti, ki se ujema z napovedmi kvantne teorije, in s tem ovrgel teorije s skritimi spremenljivkami. Kvantna stanja, ki kršijo Bellovo neenakost, imenujemo *prepletena*.

V seminarju je kvantna prepletenost predstavljena predvsem s teoretskega stališča, kljub temu pa je pojasnjen tudi njen aplikativni pomen v kvantni informatiki – v procesih kot so kvantna kriptografija in kvantna teleportacija.

Kazalo

1 Uvod **3**

2 Formalizem **4**
- 2.1 Aksiomi kvantne mehanike 4
- 2.2 Gostotna matrika, čista in mešana stanja 5
- 2.3 Vpliv razdelitve sistema na podsisteme 6

3 Bellova neenakost in nelokalnost kvantnih sistemov **7**
- 3.1 Lokalni realizem in skrite spremenljivke 7
- 3.2 Bellova neenakost 7
- 3.3 Kršitev Bellove neenakosti 8

4 Uporaba prepletenosti **9**
- 4.1 Gosta komunikacija 9
- 4.2 Kvantni prenos (klasičnega) ključa 10
- 4.3 Kvantna teleportacija 10

5 Vzpostavljanje prepletenosti med kvantnimi biti **11**

6 Kvantifikacija prepletenosti; konkurenca **12**

7 Zaključek **13**

1 Uvod

Z manjšanjem velikosti elektronskih elementov v računalniških vezjih se bližamo nanometerskim dimenzijam, pri katerih postanejo pomemembni kvantni efekti kot so diskretna narava elektronskih stanj in tuneliranje. Po eni strani kvantni efekti pomenijo omejitev možne miniaturizacije (in s tem zmogljivosti) klasičnih računalnikov, po drugi strani pa lahko uporaba kvantnih pojavov omogoči razvoj računalnikov novih vrst. Prvi predlogi [1, 2, 3], da bi lahko zmogljivosti računalnika, ki bi izkoriščal lastnosti kvantno mehanskih stanj kot je npr. koherentna superpozicija, resno presegle zmogljivosti klasičnih računalnikov, so dali zagon področju kvantne informatike. Algoritem se na klasičnemu računalniku izvaja kot zaporedje operacij, ki nizu vhodnih bitov (npr. 01101) priredi niz izhodnih bitov; algoritem, ki ga izvaja kvantni računalnik, pa je unitarna transformacija, ki začetno valovno funkcijo prevede v končno ($\psi' = U\psi$). Navadno se v kvantni informatiki govori o sistemih, katerih osnovni gradnik je dvonivojski kvantni sistem (npr. spin elektrona ali polarizacija fotona):

$$\psi = a\left|1\right\rangle + b\left|0\right\rangle,$$

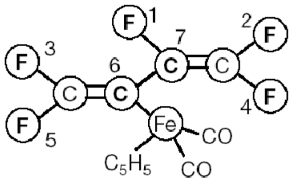
kjer smo stanji označili z 0 in 1. Tak dvonivojski sistem bomo imenovali kvantni bit ali kar na kratko – *kubit*. Vhodna valovna funcija je potem koherentna superpozicija stanj kubitov, npr.

$$\psi = a_1\left|000\right\rangle + a_2\left|001\right\rangle + a_3\left|010\right\rangle + ... + a_8\left|111\right\rangle.$$

Pomemben mejnik na področju kvantnega računalništva je postavil Shor [4]. Izdelal je namreč algoritem, ki lahko faktorizira naravna števila v času, ki narašča polinomsko s številom vhodnih (klasičnih) bitov, medtem ko pri klasičnem izračunu to število narašča eksponentno s številom vhodnih bitov[1].

Primer pohitritve glede na klasični izračun je predstavil tudi Grover [5]. Pokazal je, da je kvantni algoritem iskanja v neurejenem seznamu N elementov uspešen že po reda $\sqrt{N}$ operacijah (v primerjavi s klasičnim, ko moramo v povprečju preiskati polovico seznama, se pravi napraviti $N/2$ operacij, da najdemo iskani element). Shorov algoritem so preiskusili tudi eksperimentalno. Skupina z raziskovalnega oddelka IBM je leta 2001 razstavila število 15 na prafaktorje v sistemu s sedmimi kubiti (Slika 1), na katerih je izvajala operacijo z metodo NMR [6]. Na tem mestu je potrebno poudariti velik pomen, ki ga ima faktorizacija števil za metodo šifriranja z javnim ključem.

[1] Učinkovitega klasičnega algoritma za faktorizacijo ni, zato je treba preizkusiti vsa števila. Ker je za število velikosti reda v splošnem 2^n potrebno preizkusiti reda 2^n celih števil, število operacij, ki jih je potrebno izvesti, eksponentno narašča z n. Kvantni algoritem izračun pohitri, saj je lahko vhodno stanje v tem primeru superpozicija vseh možnih stanj.



Slika 1: Kvantni računalnik, ki je razstavil število 15 na 3 in 5, je v resnici raztopina molekul, v kateri se spine jeder 7 fluorovih atomov (označenih na sliki), neodvisno obrača z metodami jedrske magnetne resonance. Kvantno računanje se v tem primeru izvaja na množici molekul hkrati [6].

Verjetno je jasno, da so nekateri podatki take narave, da si njihovi lastniki želijo ohraniti zaupnost na daljši rok. Zato je kljub temu, da sta omenjena algoritma (poleg simulacije kvantnih sistemov) edina, za katera so do danes pokazali prednost kvantnih računalnikov glede na klasične, in velikim oviram, ki se pojavljajo v izdelavi kvantnega 'hardvera' (predvsem dekoherenca), področje zanimivo in finančno podprto s strani predvsem vladnih organizacij različnih držav. Razvoj učinkovitega kvantnega računalnika v roku, recimo, 20-ih let bi omogočil dešifriranje precejšnjega deleža informacij (vsega, kar je šifrirano z algoritmom javnega ključa), ki naj bi do takrat ostale skrite.

Principa, ki ju izkorišča kvantni računalnik za svoje delovanje, sta koherentna superpozicija in kvantna prepletenost. V tem seminarju si bomo ogledali pojav kvantne prepletenosti v kvantnih stanjih in pomen prepletenosti v EPR paradoksu [7]. Poleg teoretične zanimivosti ima prepletenost tudi aplikativen pomen. Omogoča namreč kvantno kriptografijo [9], kvantno teleportacijo [8] in je pomembna za nekatere vrste kvantnega računanja [10, 11]. Predstavili bomo tudi tvorbo prepletenih parov kubitov v trdni snovi: primer tvorbe prepletenih parov si bomo podrobneje ogledali v sistemu dveh kvantnih pik.

2 Formalizem

2.1 Aksiomi kvantne mehanike

1. Stanje je popoln opis sistema [12, 13]. Predstavljeno je z *nitjo* v Hilbertovem prostoru. Stanjem, ki jih lahko predstavimo z nitjo, pravimo tudi *čista* stanja. Hilbertov prostor je vektorski prostor kompleksnih funkcij. Vektorje v Hilbertovem prostoru označimo v Diracovem zapisu s $|\psi\rangle$. Nit v Hilbertovem prostoru je množica takih vektorjev, ki se razlikujejo za poljubno kompleksno fazo. Brez izgube splošnosti lahko predpostavimo, da so stanja normirana $\langle\psi|\psi\rangle = 1$.

2. Opazljivke so predstavljene s Hermitskimi operatorji. Opazljivko lahko

v lastni bazi zapišemo z

$$A = \sum_n A_n |n\rangle \langle n| . \quad (1)$$

Rezultat meritve je v vsakem primeru ena lastnih vrednosti opazljivke. Če tudi stanje sistema razvijemo po lastnih funkcijah opazljivke $|\psi\rangle = \sum_n \psi_n |n\rangle$, izmerimo vrednost A_n z verjetnostjo $P_n = |\psi_n|^2$.

3. Razvoj stanja v času narekuje Shrödingerjeva enačba:

$$i\frac{d}{dt} |\psi(t)\rangle = H |\psi(t)\rangle . \quad (2)$$

Formalno lahko rešimo to enačbo z unitarnim operatorjem časovnega razvoja.

$$|\psi(t)\rangle = e^{-iHt} |\psi(0)\rangle = U |\psi(0)\rangle . \quad (3)$$

2.2 Gostotna matrika, čista in mešana stanja

Splošno stanje v kvantni mehaniki lahko ekvivalentno zapišemo tudi z gostotno matriko.

$$\rho = |\psi\rangle \langle\psi| . \quad (4)$$

Pričakovane vrednosti operatorjev so v tem primeru kar

$$\langle A\rangle = \mathrm{Tr}\rho A, \quad (5)$$

česar ni težko preveriti[2]. Dodatna prednost identifikacije stanja z gostotno matriko je, da ni potrebno vpeljati dodatno pojma niti: pri transformaciji $\psi \to e^{i\phi}\psi$ se namreč gostotna matrika ne spremeni. Na tem mestu je potrebno poudariti, da taka oblika gostotne matrike v splošnem velja le, kadar sistem ni sklopljen z okolico. Za sistem, ki je v termičnem ravnovesju z okolico, velja znan rezultat statistične mehanike [14] , da je gostotna matrika enaka

$$\rho = \sum_n e^{-\beta\epsilon_n} |\Psi_n\rangle \langle\Psi_n| ,$$

če so Ψ_n lastna stanja sistema z energijami ϵ_n. V primerih, ko je gostotna matrika vsota gostotnih matrik čistih stanj, pravimo, da je sistem v *mešanemu* stanju.

[2]Vstavimo v izraz za pričakovano vrednost kompletnostno relacijo

$$\langle\psi| A |\psi\rangle = \sum_{n'} \langle\psi| A |n'\rangle \langle n'|\psi\rangle = \sum_{n'} \langle n'|\psi\rangle \langle\psi| A |n'\rangle .$$

2.3 Vpliv razdelitve sistema na podsisteme

V primeru, ko se omejimo na podsistem nekega sistema, ki je v čistem stanju, naletimo na naslednje zanimive posledice:

- Stanje je v splošnem mešano – *ni* predstavljeno z nitjo v Hilbertovem prostoru.
- Merjenja niso ortogonalne projekcije.
- Razvoj stanja po času ni unitaren.

Tu si bomo ogledali le prvo točko in sicer na najenostavnejšem primeru: na sistemu sestavljenem iz dveh kubitov, v katerem se izvaja meritve le na enem od kubitov iz para. Vzemimo, da je celotni sistem v stanju

$$|\psi\rangle_{AB} = a\,|0\rangle_A\,|0\rangle_B + b\,|1\rangle_A\,|1\rangle_B$$

V takem stanju sta kubita A in B *korelirana*. Če denimo izmerimo stanje kubita A dobimo z verjetnostjo $|a|^2$ končno stanje $|0\rangle_A\,|0\rangle_B$ in z verjetnostjo $|b|^2$ stanje $|1\rangle_A\,|1\rangle_B$. Če merimo pričakovano vrednost poljubne opazljivke M, ki deluje le v podprostoru A

$$\begin{aligned}\langle M\rangle &= \langle\psi|\,M_A\otimes 1_B\,|\psi\rangle\\ &= |a|^2{}_A\,\langle 0|\,M_a\,|0\rangle_A + |b|^2{}_A\,\langle 1|\,M_A\,|1\rangle_A\,,\end{aligned}$$

vidimo, da lahko izraz prepišemo v obliko

$$\begin{aligned}\langle M_A\rangle &= \mathrm{Tr}(M_A\rho_A)\\ \rho_A &= |a|^2\,|0\rangle_A\,{}_A\langle 0| + |b|^2\,|1\rangle_A\,{}_A\langle 1|\,.\end{aligned}$$

Ker velja rezultat za poljubno opazljivko M_A, je smiselno interpretirati ρ_A kot mešano stanje, torej nekoherentno mešanico čistih stanj. V primeru, ko je $|a| = |b|$, je gostotna matrika večkratnik identičnega operatorja $\rho_A = 1/2$. O stanju sistema takrat z lokalnimi meritvami ne moremo dobiti nobene informacije. Čista stanja celega sistema, za katera velja, da je reducirana gostotna matrika večkratnik identičnega operatorja (se pravi, da ne nosijo nobene lokalne informacije), imenujemo *maksimalno prepletena stanja*. Maksimalno prepletena stanja za sistem dveh kubitov so

$$\begin{aligned}\left|\phi^\pm\right\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} \pm |11\rangle_{AB}\right), \quad \text{in}\\ \left|\psi^\pm\right\rangle_{AB} &= \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} \pm |10\rangle_{AB}\right). \qquad (6)\end{aligned}$$

Ta stanja so medsebojno ortogonalna, ne tvorijo pa vektorskega podprostora: njihova linearna kombinacija v splošnem ni maksimalno prepleteno stanje. Z lokalnimi unitarnimi transformacijami je mogoče prehajati med stanji. Lokalna transformacija σ_1^A (σ_i so Paulijeve matrike, npr. $\sigma_1\,|1\rangle = |0\rangle\,, \sigma_1\,|0\rangle = |1\rangle$) pomeni prehod $\phi \leftrightarrow \psi$, medtem ko transformacija σ_3 pomeni zamenjavo stanj $+ \leftrightarrow -$.

3 Bellova neenakost in nelokalnost kvantnih sistemov

3.1 Lokalni realizem in skrite spremenljivke

Einstein ni verjel v nedeterminizem v kvantni mehaniki - znana je njegova izjava: 'Bog ne kocka'. Trdil je, da je stohastični značaj izida neke meritve posledica naše nepopolne vednosti o sistemu. Tako po njegovem mnenju npr. za elektronu v čistem stanju s spinom $+1/2$ glede na os z $|\psi_z\rangle = |\uparrow_z\rangle$ popoln opis v resnici vključuje še skrito spremenljivko: $|\psi_z\rangle \to |\psi_{z,\lambda}\rangle$. Če spin takega elektrona merimo glede na os $\hat{n}$, ki je nagnjena glede na os z za kot θ, je primer odvisnosti od skrite spremenljivke, s katerim se, po Einsteinovem mnenju, napovedi kvantne mehanike navidez ujemajo:

$$
\begin{aligned}
&|\uparrow_{\hat{n}}\rangle\,, \quad \text{za} \quad 0 \leq \lambda \leq \cos^2\frac{\theta}{2} \\
&|\downarrow_{\hat{n}}\rangle\,, \quad \text{za} \quad \cos^2\frac{\theta}{2} \leq \lambda \leq 1.
\end{aligned} \tag{7}
$$

Če bi poznali skrito spremenljivko λ, bi bil rezultat meritve determinističen. Ker pa λ ne poznamo, se bo izid merjenja ujemal z napovedjo kvantne mehanike. V primeru večdelnega sistema, katerega deli so prostorsko ločeni, Einstein trdi, da izvajanje meritev na enem podsistemu ne more vplivati na vrednost skritih spremenljivk drugega podsistema. Tak pogled imenujemo *lokalni realizem*. Z uvedbo skritih spremenljivk se je Einstein želel izogniti trenutnemu vplivu merjenja v enem podsistemu na podsistem, ki je daleč stran (Einstein-Podolsky-Rosen paradoks)[7]. Predpostavka o skritih spremenljivkah in lokalnosti ima pomembne posledice.

3.2 Bellova neenakost

Denimo, da so a, a', b in b' štiri opazljivke z izidom meritve ± 1, ki je določen z nam neznanimi vrednostmi skritih spremenljivk. V vsakem primeru velja $a + a' = 0$ in $a - a' = \pm 2$ ali pa $a - a' = 0$ in $a + a' = \pm 2$. Zato velja tudi

$$C = (a + a')b + (a - a')b' = \pm 2.$$

Sedaj izračunajmo pričakovano vrednost

$$|\langle C\rangle| \leq \langle |C| \rangle = 2. \tag{8}$$

Tu je potrebno posebej poudariti, da se je pričakovana vrednost v tem primeru računala kot integral C po neznanih skritih spremenljivkah pomožen z verjetnostno porazdelitveno funkcijo po teh spremenljivkah. Ker pa velja

$|C| = 2$ za *vsako* vrednost skritih spremenljivk, zveza (8) velja v splošnem. Prišli smo do posplošene Bellove neenakosti[3].

$$|\langle ab\rangle + \langle a'b\rangle + \langle ab'\rangle - \langle a'b'\rangle| \leq 2. \tag{9}$$

V nadaljevanju bomo videli, da korelacije med spini v kvantno mehanskem opisu kršijo neenakost (9), kar pomeni, da se kvantnih rezultatov z determinističnо teorijo skritih spremenljivk ne da reproducirati. To pomeni, da se lokalni realizem in kvantna mehanika medsebojno izključujeta.

3.3 Kršitev Bellove neenakosti

Oglejmo si korelacije spin-spin[4] na primeru dveh elektronov, ki sta v spinskem singletnemu stanju $|\psi\rangle = (|10\rangle_{AB} - |01\rangle_{AB})/\sqrt{2} = |\psi^-\rangle_{AB}$. Singletno stanje je sferično simetrično stanje s celim spinom enakim nič. Velja torej

$$(\vec{\sigma}^{(A)} + \vec{\sigma}^{(B)})\,|\psi^-\rangle = 0, \tag{10}$$

kar je preprosto preveriti tudi z ekplicitnim izračunom. Korelacije spin-spin

$$c_{\hat{n}\hat{m}} = {}_{AB}\langle\psi^-|\,(\vec{\sigma}^{(A)}\cdot\hat{n})(\vec{\sigma}^{(B)}\cdot\hat{m})\,|\psi^-\rangle_{AB}$$

se z uporabo zveze (10) ovrednoti kot pričakovana vrednost operatorja, ki deluje le v podprostoru A, se pravi

$$c_{\hat{n}\hat{m}} = -{}_{AB}\langle\psi^-|\,(\vec{\sigma}^{(A)}\cdot\hat{n})(\vec{\sigma}^{(A)}\cdot\hat{m})\,|\psi^-\rangle_{AB} = -\sum_{ij} n_i m_j \mathrm{Tr}(\rho_A \sigma_i^{(A)}\sigma_j^{(A)}) =$$

$$-\sum_{ij} n_i m_j \delta_{ij} = -\hat{n}\cdot\hat{m}. \tag{11}$$

Rezultat je preprost in plauzibilen. Če sta osi glede na kateri opazovalca v sistemih A in B merita spin medsebojno pravokotni $\hat{n}\cdot\hat{m} = 0$, korelacije med spinoma ni, za splošno orientacijo osi pa je enaka $c_{\hat{n}\hat{m}} = -\cos\theta$, kjer $\theta = \hat{n}\cdot\hat{m}$ kot med osema.

Denimo, da se Alica in Bob odločita izvesti vsak na svojem kubitu nekaj meritev opazljivk

$$a = \sigma_3^{(A)}, \quad a' = \sigma_1^{(A)}, \quad b = \frac{1}{\sqrt{2}}(\sigma_3^{(B)} + \sigma_1^{(B)}),$$

$$b' = \frac{1}{\sqrt{2}}(\sigma_1^{(B)} - \sigma_3^{(B)}).$$

[3] Ta oblika je v resnici znana kot Clauser-Horne-Shimony-Holt-ova (CHSH) neenakost [15]. Izvirna Bellova neenakost [16] je posebni primer CHSH neenakosti.

[4] V tem razdelku bomo zaradi lažje predstave govorili o spinu elektrona. Enaki rezultati veljajo za korelacije med stanji poljubnega dvonivojskega sistema.

Z uporabo izračuna (11) ni težko izračunati:

$$_{AB}\left\langle \psi^- \right| ab \left| \psi^- \right\rangle_{AB} = {}_{AB}\left\langle \psi^- \right| ab' \left| \psi^- \right\rangle_{AB} = {}_{AB}\left\langle \psi^- \right| a'b \left| \psi^- \right\rangle_{AB} = \frac{1}{\sqrt{2}},$$

in

$$_{AB}\left\langle \psi^- \right| a'b' \left| \psi^- \right\rangle_{AB} = -\frac{1}{\sqrt{2}},$$

se pravi, da je

$$_{AB}\left\langle \psi^- \right| ab \left| \psi^- \right\rangle_{AB} + {}_{AB}\left\langle \psi^- \right| ab' \left| \psi^- \right\rangle_{AB} + {}_{AB}\left\langle \psi^- \right| a'b \left| \psi^- \right\rangle_{AB} -$$

$$- {}_{AB}\left\langle \psi^- \right| a'b' \left| \psi^- \right\rangle_{AB} = \frac{4}{\sqrt{2}} > 2,$$

kar je kršitev Bellove neenakosti (9).

Ker Bellova neenakost velja za poljuben klasični sistem, ki je popolnoma določen z lokalnimi spremenljivkami, lahko zaključimo, da za nekatera kvantno-mehanska stanja načelo lokalnosti ne velja. Dva spina v singletu tvorita en sam objekt, čeprav sta prostorsko ločena. Za tista stanja, ki kršijo Bellovo neenakost, pravimo, da so *prepletena* (ang. entangled).

4 Uporaba prepletenosti

V prejšnjem razdelku smo pokazali, da za določena kvantna stanja lokalni opis ni dober. V tem razdelku bomo pokazali, kako se prepletenost kvantnih bitov uporabi v vlogi prenosnika klasične in kvantne informacije. Ogledali si bomo tudi, kako kvantna prepletenost omogoča varno izmenjavo skrivnega niza klasičnih bitov - ključa za šifriranje.

4.1 Gosta komunikacija

Denimo, da si Alica in Bob delita prepleten par kubitov $|\phi^+\rangle_{AB}$. Alica lahko na svojem kubitu – npr. s tem, da svoj spin postavi v primerno usmerjeno magnetno polje – izvede eno izmed štirih unitarnih transformacij (I, σ_1, σ_2, σ_3), ki transformirajo stanje $|\phi^+\rangle_{AB}$ v eno izmed štirih ortogonalnih stanj ($|\phi^+\rangle_{AB}$, $|\psi^+\rangle_{AB}$, $|\psi^-\rangle_{AB}$, $|\phi^-\rangle_{AB}$) . Če sedaj Alica pošlje svoj kubit Bobu, lahko Bob s projekcijo na ortogonalno bazo teh štirih kubitov določi katero štirih operacij je Alica izvedla in s tem izlušči dva bita klasične informacije. Zanimiva lastnost tovrstnega prenosa je, da je varen pred prisluškovanjem. Gostotna matrika prenesenega kubita je namreč enaka $\rho_A = 1_A/2$, kar pomeni da kubit sam po sebi ne nosi nobene informacije. Vsa informacija je kodirana v korelacijah med kubitoma.

4.2 Kvantni prenos (klasičnega) ključa

Prepletenost med kvantnimi biti omogoča varen prenos informacije. Denimo, da si Alica in Bob delita množico prepletenih kubitov. Potem se za vsak kubit Alica in Bob naključno odločita, da bosta izmerila σ_1 ali σ_3. Javno objavita, katero opazljivko sta merila, ne razkrijeta pa rezultatov, ki sta jih dobila. Za tiste primere, kjer sta merila isto opazljivko, sedaj vesta, da so rezultati njunih meritev popolnoma antikorelirani. Na tak način sta si Alica in Bob pridobila skupni naključni ključ.

V principu bi lahko prisluškovalka Eva prepletla svoje kubite s kubiti Alice in Boba že pred začetkom njune komunikacije. Pokaže se lahko, da se v tem primeru stanje spremeni tako, da ni več hkrati lastno stanje $\sigma_1^A\sigma_1^B$ in $\sigma_3^A\sigma_3^B$, kar lahko Alica in Bob izmerita. Ker lahko preverita poljubno mnogo prenešenih kubitov (s tem sicer zavržeta delež prenešene informacije), lahko z veliko statistično verjetnostjo ugotovita ali je Eva prisluškovala ali ne.

4.3 Kvantna teleportacija

Gosto kodiranje je bil primer uporabe kvantne informacije za ojačitev prenosa klasične informacije. Proces, ki je še bolj zanimiv, pa je verodostojen prepis kvantnega stanja s prenosom klasične informacije. Denimo, da si Alica in Bob delita prepleten par kubitov $|\phi^+\rangle_{AB}$. Alica naj ima še kubit v neznanem stanju $|\psi\rangle_C$. Nato Alica projicira par kubitov A in C na stanja $|\phi^\pm\rangle$ in $|\psi^\pm\rangle$ in pošlje rezultat meritve (dva bita klasične informacije) Bobu. Pokažimo, da lahko potem Bob rekonstruira stanje $|\psi\rangle$! Preuredimo stanje sistema pred meritvijo, ki jo izvede Alica:

$$|\psi\rangle_C\,|\phi^+\rangle_{AB} = (a\,|0\rangle_C + b\,|1\rangle_C)\frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) =$$

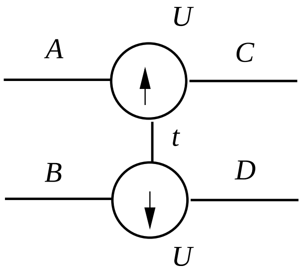
$$= \frac{1}{\sqrt{2}}(a\,|000\rangle_{CAB} + a\,|011\rangle_{CAB} + b\,|100\rangle_{CAB} + b\,|111\rangle_{CAB}) =$$

$$= \frac{1}{2}[a(|\phi^+\rangle_{CA} + |\phi^-\rangle_{CA}+)\,|0\rangle_B + a(|\psi^+\rangle_{CA} + |\psi^-\rangle_{CA}+)\,|1\rangle_B +$$
$$b(|\psi^+\rangle_{CA} - |\psi^-\rangle_{CA}+)\,|0\rangle_B + b(|\phi^+\rangle_{CA} - |\phi^-\rangle_{CA}+)\,|1\rangle_B] =$$
$$= \frac{1}{2}\,|\phi^+\rangle_{CA}\,(a\,|0\rangle_B + b\,|1\rangle_B) + |\psi^+\rangle_{CA}\,(a\,|1\rangle_B + b\,|0\rangle_B) +$$
$$+\,|\psi^-\rangle_{CA}\,(a\,|1\rangle_B - b\,|0\rangle_B) + |\phi^-\rangle_{CA}\,(a\,|0\rangle_B - b\,|1\rangle_B) =$$
$$\frac{1}{2}\left[|\phi^+\rangle_{CA}\,|\psi\rangle_B + |\psi^+\rangle_{CA}\,\sigma_1\,|\psi\rangle_B + |\psi^-\rangle_{CA}\,(-i\sigma_2)\,|\psi\rangle_B + |\phi^-\rangle_{CA}\,\sigma_3\,|\psi\rangle_B\right].$$

Rezultat Alicine meritve stanja para kubitov A in C je z verjetnostjo 1/4 vsako od možnih ortogonalnih maksimalno prepletenih stanj. Če sporoči rezultat meritve Bobu lahko Bob z uporabo unitarnih transformacij σ_i (velja $\sigma_i^2 = 1$) pripravi stanje ψ.

5 Vzpostavljanje prepletenosti med kvantnimi biti

Večina eksperimentov v kvantni informatiki je bila napravljena s fotoni. Kvantna kriptografija [8] in kvantna teleportacija [9] sta bili prikazani s prepletenimi fotonskimi pari. Za morebitne aplikacije na tehnološki ravni pa je za vzpostavljanje prepletenosti zanimiva predvsem trdna snov, saj tam industrija že pozna postopke, ki omogoča izgradnjo kompleksnih sistemov iz enostavnih sestavnih delov.



Slika 2: V sistemu dveh pik se elektrona sklopita v singlet zaradi izmenjalne interakcije $J \propto t^2/U$, kjer je U značilna vrednost Coulombskega odboja med elektronoma z nasprotnim spinov v isti kvantni piki, t pa obratni značilni čas tuneliranja elektronov med pikama. Z izmeničnim odpiranjem in zapiranjem parov kanalov A in B ter C in D se vzpostavi stalen vir prepletenih elektronov.

Predlogi za tvorbo prepletenih stanj se zanašajo predvsem na različne oblike interakcij elektronov v snovi. Eden predlogov je npr. superprevodnik v katerem so Cooperjevi pari spinski singleti [17, 18, 19, 20], ostali predlogi pa se zanašajo na Coulombsko interakcijo med elektroni. Ena od možnosti je tudi interakcija med elektroni v kvantnih pikah [21, 22, 23, 24, 25]. Oglejmo si predlog vzpostavljanja prepletenosti v sistemu dveh kvantnih pik (Slika 2) sklopljenih na štiri žice [25]. Z napetostjo kontrolirana vrata najprej spustijo par elektronov skozi žici A in B v kvantni piki. Coulombski odboj med elektroni kvantnih pikah povzroči izmenjalno interakcijo[5] J, ki zniža energijo singletnega para. Napetost na žicah lahko določimo tako, da se v piki prepusti le pare elektronov, ki so spinski singleti. Nato se skozi žici C in D elektrona odvede. Postopek se lahko periodično ponavlja, pri čimer je frekvenca produkcije (ocenjena na 6 GHz) omejena predvsem s hitrostjo preklopa vrat.

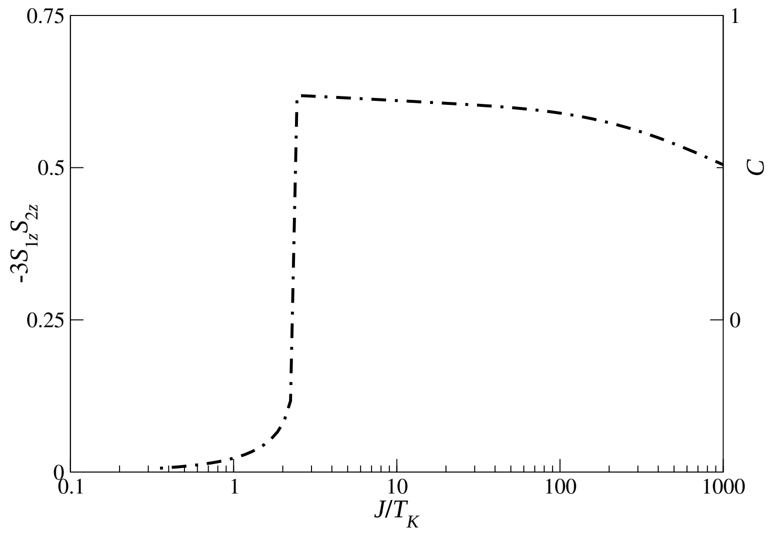
[5]Izmenjalna interakcija je interakcija, pri kateri si elektronski par zniža energijo s tem, da virtualno zamenja mesti (v prvem redu teorije motenj je popravek kar $J \propto t^2/U$, če je U odboj med elektronoma, t pa prekrivalni integral). Ker je vmesno stanje tako, da sta dva elektrona na istem mestu, so taki procesi možni le za elektrone z obratnim spinom – singlete.

6 Kvantifikacija prepletenosti; konkurenca

Hkrati s prepoznavanjem uporabnosti prepletenosti so se pojavile mere za količino prepletenosti v kvantnem stanju. V primeru para kubitov, kot je npr. sistem prikazan na sliki, je merilo za prepletenost sistema *konkurenca* [28, 29], ki se za spinske sisteme s krogelno simetrijo izrazi kar s pričakovano vrednostjo korelacije spin-spin

$$C = 2\text{Max}(0, 3\langle S_1^z S_2^z \rangle).$$

Preprost izraz je razumljiv. V primeru, ko je par elektronov združen v singlet ali pa nepovezan, je merilo za prepletenost kar verjetnost, da najdemo par elektronov v singletu. Za sistem predstavljen na Sliki 2 smo numerično izračunali [30] delež parov elektronov, ki so spinski singleti, v odvisnosti od razmerja med velikostjo izmenjalne interakcije J in Kondove energije [31]. Kondova energija je izmenjalna energija med elektroni na kvantnih pikah in elektroni v žicah. Poenostavljeno rečeno: energijsko ugodna so singletna stanja, ki se vzpostavijo ali med elektronoma na pikah ali pa med elektronom v kvantni piki in elektroni v kovinskem vodniku.



Slika 3: Vpliv tekmovanja med izmenjalno interakcijo J in Kondovim efektom na prepletenost elektronov v dvojni kvantni piki. Prikazana sta korelacija spin-spin in konkurenca C v odvisnosti od J/T_K. Ko izmenjalna interakcija preseže dvojno Kondovo energijo, sistem preide v antiferomagnetni režim z močno prepletenimi elektroni.

7 Zaključek

Ena izmed želja, ki sem jih imel ob pripravi tega seminarja, je odgovoriti na vprašanje, kakšna je pravzaprav vloga prepletenosti v kvantnem računalništvu. Sedaj, ko pisanje seminarja zaključujem, opažam, da na to vprašanje v resnici nisem odgovoril. Vzrok za to je, da vloga prepletenosti v kvantnem računalništvu še ni zares določena. Stanje najbrž najlepše osvetli stavek iz ene od biblij na področju kvantne informatike [32] '... *For reasons which nobody fully understands, entangled states play a crucial role in quantum computation* ...'.

Za izvedbo Shorovega algoritma stanja v resnici niso nujno prepletena, vse pa je odvisno od vrste kvantega računalnika. Obstajajo namreč predlogi za kvantni računalnik, ki so drugačne vrste [11]. V njem se operacije ne izvajajo z unitarnimi transformacijami stanja, pač pa z izvajanjem meritev na maksimalno prepletenem začetnem stanju. Postopek računanja je v tem 'enosmernem' kvantnem računalniku v nasprotju z 'običajnim' kvantnim računalnikom ireverzibilen. Vloga prepletenosti v kvantnem računalništvu je torej odvisna od konkretnega algoritma in njegove realizacije. Nasprotno pa je za procese, kot so kvantna kriptografija in kvantna teleportacija, prepletenost nujno potrebna in predstavlja *dobrino*, ki te postopke omogoča.

V seminarju smo izpostavili tudi pomen prepletenosti kot kontrasta klasični sliki. Kot smo pokazali, lokalni opis za lokalna stanja ni mogoč: par elektronov, ki je sklopljen v singlet, je *en* objekt četudi sta elektrona prostorsko ločena.

Pomembna točka, ki se je v seminarju nismo dotaknili je *dekoherenca*. To je proces, pri katerem se prepletenost iz nekega stanja prenese v njegovo okolico. Noben fizikalni sistem, razen celega vesolja, ni v resnici popolnoma izoliran od svoje okolice, zato okolica neprestano izvaja neke vrste meritve na sistemu in s tem ruši koherenco: prepletenost se iz sistema seli v prepletenost med sistemom in okolico. Dekoherenca je pomembna tako s teoretičnega – ključna je namreč za interpretacijo kvantne mehanike [33], kot z eksperimentalnega vidika, ravno dekoherenca je tista, ki onemogoča izdelavo kvantega računalnika v trdni snovi. Trdna snov je v resnici morje sklopljenih elektronov. V njej se prepletenost neprestano prenaša z enih skupkov elektronov na druge [34]. Kako se izogniti dekoherenci v trdni snovi, v resnici ni trenutno znano niti teoretikom niti eksperimentalnim fizikom.

Literatura

[1] R. Feynman, Int. J. Theoret. Phys. **21**, 467 (1982).

[2] P. Benioff, Phys. Rev. Lett. **48**, 1581 (1982).

[3] Deutsch, D. Proc. R. Soc. Lond. A 400, 97 (1985).

[4] P.W. Shor, Proc. 35th Annu. Symp. Foundations of Computer Science, 124, IEEE Computer Society Press, Los Alamitos, 1994.

[5] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997)

[6] L. Vandersypen *et al.*, Nature **414**, 883 (2001)

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

[8] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).

[9] J. Pan *et al.*, Nature **421**, (2003).

[10] N. Linden, Phys. Rev. Lett. **87**, 047901 (2001).

[11] P. Walther *et al.*, Nature **434**, 169 (2005).

[12] G. Auletta: *Foundations and Interpretation of Quantum Mechanics*, World Scientific Publishing Co., Singapore, 2000.

[13] J. Preskill: *Lecture Notes for Physics 229: Quantum Information and Computation* [http://theory.caltech.edu/p̃reskill/ph229].

[14] F. Schwabl: *Statistische Mechanik*, Springer, Berlin, 2000.

[15] J. F. Clauser *et al.*, Phys. Rev. Lett. **23**, 880 (1969).

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

[17] P. Recher, E.V. Sukhorukov in D. Loss, Phys. Rev. B **63**, 165314 (2001)

[18] P. Samuelsson, E.V. Sukhorukov in M. Büttiker, Phys. Rev. Lett, **91**, 157002 (2003).

[19] P. Recher in D. Loss, Phys. Rev. Lett. **91**, 267003 (2003).

[20] E. Prada in F. Sols, Eur. Phys. J. B **40**, 379 (2004).

[21] W.D. Oliver, F. Yamaguchi in Y. Yamamoto, Phys. Rev. Lett **88**, 037901 (2002).

[22] G. Leon *et al.* Europhys. Lett. **66**, 624 (2004).

[23] S. Yin *et al.* J. Phys.: Condens. Matter **17**, L183 (2005).

[24] D.S. Saraga in D. Loss, Phys. Rev. Lett. **90**, 166803 (2003).

[25] Xuedong Hu in S. Das Sarma, Phys. Rev B **69**, 115312(2005).

[26] C. H. Bennet *et al.* Phys. Rev. A **53**, 2046 (1996).

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

[28] L. Amico *et al.*, Phys. Rev A **69**, 022304(2005).

[29] T. Roscilde *et al.*, Phys. Rev. Lett **93**, 167203 (2004).

[30] J. Mravlje, A. Ramšak, T. Rejec, v pripravi.

[31] A. C. Hewson, *The Kondo Problem to Heavy Fermions* (Cambridge University Press, Cambridge, 1993).

[32] M. A. Nielsen in I. A. Chuang, *Quantum Information and Quantum Computation* (Cambridge University Press, Cambridge, 2001).

[33] M. Schlosshauer, Rev. Mod. Phys. **76**, 1267

[34] C.W.J. Beenakker, [cond-mat/0508488].