Fenomen kvantne superpozicije

in pomen le tega za kvantno računalništvo

seminarska naloga pri predmetu optične in nanotehnologije

Dunja Rosina

v Ljubljani, januar 2010

Kazalo

Uvod

Pričujoča seminarska naloga naj bi bralcu približno razložila vlogo kvantne mehanike v prihodnosti računalništva, predvsem pa kako kvantno računalništvo uporablja fenomen superpozicije, ki je eden izmed zakonov kvantne mehanike. Gre za zelo zapleteno snov, morda bi bilo bolje reči "nepredstavljivo" kot zapleteno, saj je še znani fizik Richard Feynman, ki ga bom velikokrat omenila v seminarski nalogi menda dejal:

"Mislim, da lahko z gotovostjo zatrdim, da kvantne mehanike ne razume nihče!"

Namen te seminarske naloge ni zelo dobro poznavanje kvantne mehanike, prav tako za računalničarja poglabljanje v kvantno mehaniko ni tako bistveno. Vendar je dobro, da spoznamo vsaj delček zgodovine ter osnove kvantne mehanike, ki jih moramo "razumeti" (recimo temu raje "vedeti zakaj gre"), preden se lotimo poglavja o kvantnem računalništvu.

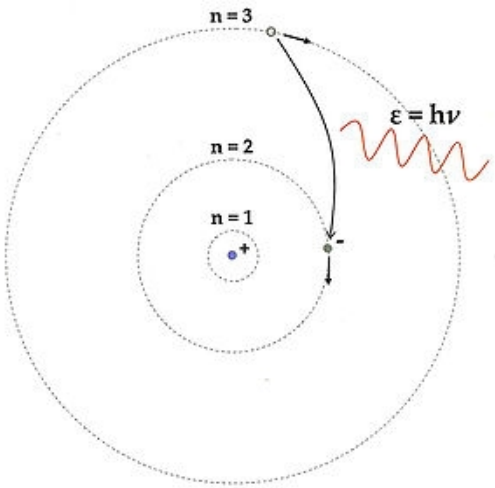
Kvantna mehanika

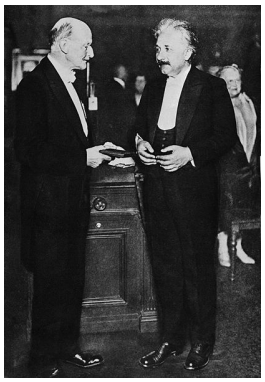
“Ali res verjameš, da luna obstaja samo, ko jo pogledaš?” - Einstein Abrahamu Paisu.

Ob študiranju kvantne mehanike izvemo, da lahko en delec potuje po več poteh hkrati, da je možno tudi zelo hitro računanje s kvantnimi delci in govori se tudi o možni teleportaciji – s tem, ko izmerimo en delec, vemo stanje drugega delca, ki je povezan s prvim, a lahko zelo oddaljen. V nekem smislu govorimo o prenosu na daljavo. Ta in vse ostale ideje se nam, vajenim otipljivega sveta, ki ga lahko enostavno izmerimo z rokami, očmi in tehtnicami zdijo izredno nenavadni, če že ne popolnoma nemogoči. Še celo Einstein in nekateri drugi znani fiziki so bili v prejšnjem stoletju zelo nenaklonjeni tej novi teoriji. Temu navkljub so poskusi, ki so danes (nekje od 70. let prejšnjega stoletja dalje) mogoči, pokazali da se kvantna mehanika ne moti.

Zgodovina kvantne mehanike

V klasični fiziki se je vedno predvidevalo, da količine kot je energija ustrezajo zveznim porazdeljenim funkcijam. A že leta 1900 je **Max Planck** pri preučevanju elektromagnetnega sevanja vročih teles ugotovil, da temu ni tako. **Niels Bohr** je leta 1913 objavil svojo teorijo modela atoma, ki je prva približno pojasnila kaj atom je, ponudila razlago zakaj pride do absorpcije in oddaje svetlobe od atomov le pri določenih valovnih dolžinah. Čeprav je imela veliko pomanjkljivosti je na čuden način teoretično prepletala klasično in kvantno fiziko. V zgodnjih 30tih letih prejšnjega stoletja se je tako izkazalo, da je čas za novo teorijo.





Slika 1: zgoraj: Max Planck in Albert Einstein leta 1929, levo: Rutherford–Bohrov model atomavodika , Vir: http://en.wikipedia.org/wiki/Max_Planck in http://en.wikipedia.org/wiki/Bohr_model

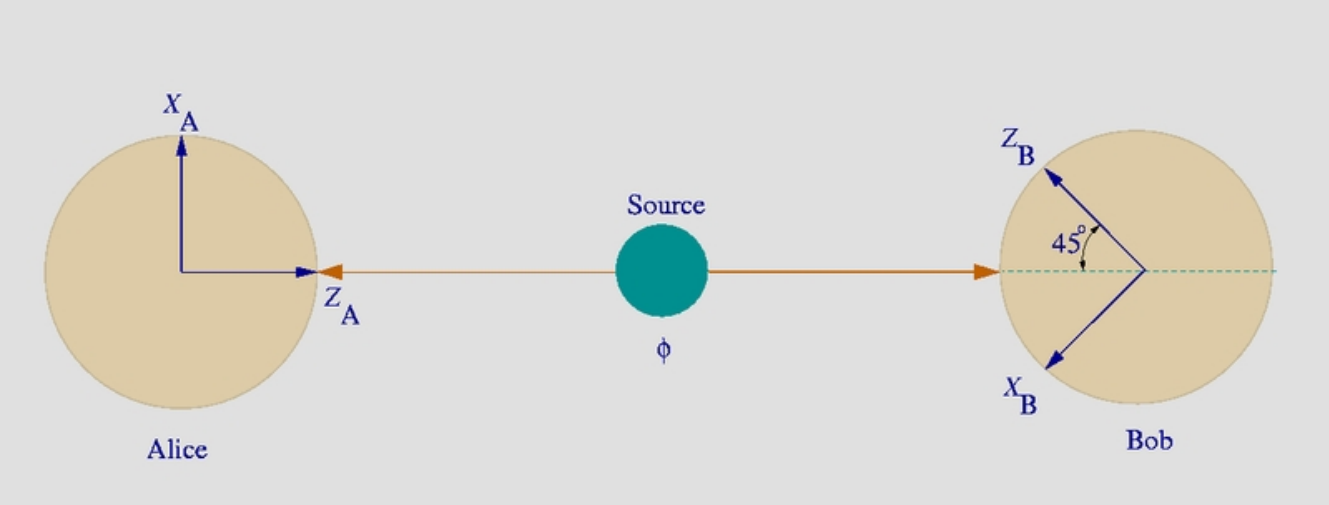
Nova teorija, imenovana kvantna mehanika, je bila strašno uspešna. Združila je koncept valov in delcev, lastnosti vse snovi. Kvantna mehanika se ukvarja z mikroskopskim svetom, atomi in svetlobno

hitrostjo. Vendar velja tudi v makroskopskem svetu, kar pa ne pomeni, da lahko zavržemo klasične (npr. Newtonove) zakone, saj le-ti dajejo dovolj dobre rezultate.

Zanimivo branje je članek ob 100 letnici kvantne mehanike, ki je izšel v reviji Scientific American in je na voljo na spletnem naslovu: *http://www-f1.ijs.si/~ramsak/teaching/km1/100letkm.pdf*

EPR paradoks

Kot sem že omenila v uvodu, vsi le niso bili tako zadovoljni z novo teorijo. E**instein, Podolsky, in Rosen** (od tu tudi ime paradoksa – EPR) so leta 1935 predstavili miselni eksperiment, ki je postal znan kot EPR paradoks, kot argument proti kvantni mehaniki kot popolni fizikalni teoriji. Bodisi gre za napovedovanje prihodnosti (v nekem smislu že vnaprej vemo stanje delca B, ko zmerimo stanje njegovega povezanega delca A), bodisi pa manjkajo še neke skrite spremenljivke.



Slika2: Miselni eksperiment, ki je kasneje postal znan kot EPR paradoks; vir (source) na sredini pošlje delce k opazovalcem (Alice in Bob). K Alice elektrone in pozitrone k Bobu, ki opravi meritev "spina"
Vir: http://en.wikipedia.org/wiki/Epr_paradox

Einstein vseeno ni nikoli mogel sprejeti kvantne mehanike kot popolne fizikalne teorije, čeprav je bil na začetku nad njo navdušen. A ko je ugotovil, da ni mogoče napovedati, kdaj bo atom izseval foton in kam bo ta odšel in ko je **Max Born** (nemški fizik in Einsteinov dolgoletni dobri prijatelj) pojasnil absolutni kvadrat valovne funkcije iz Schrodingerjeve enačbe[1] kot verjetnostno gostoto, ga je navdušenje minilo. Pomisleke je imel že veliko let pred izdanim EPR paradoksom. Izmišljal si je poskuse, ki naj bi pokazali, da je mogoče obiti Heisenbergovo neenačbo. V kvantni mehaniki Heisenbergova neenačba pomeni, da je nemogoče istočasno s poljubno natančnostjo poznati določene pare fizikalnih lastnosti, kot sta na primer lega ali gibalna količina izbranega delca. Načelo natančno določa to nedoločenost in je eno od temeljev kvantne mehanike. Še posebno jasno je Einstein svoje pomisleke izražal v pismih, ki sta si jih izmenjevala s fizikom Nielsom Bohrom, ki jih je kasneje tudi

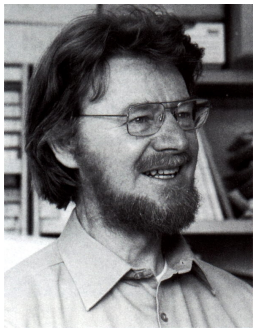
1 Schrodingerjeva enačba takorekoč nadomešča 2. Newtonov zakon v prostoru osnovnih delcev. Je osnovni zakon kvantne mehanike in nam omogoča, da pridemo do napovedi bodočega gibanja dinamičnega sistema na osnovi analitičnega in verjetnostnega računa. Lahko je časovno odvisna (prehajanja med stanji) ali pa neodvisna (stacionarna stanja))

izdal v obliki knjige. Z Bohrom sta bila prijatelja, a sta velikokrat zastopala različna stališča in pri kvantni mehaniki Einstein nikakor ni mogel Bohru dokazati, da se moti. Pravzaprav ravno obratno, Bohr je s svojim poskusom z uro, vzmetno tehtnico in vratci "premagal" Einsteina[2] (a prepričal ga ni) in pokazal, da se neenačbi ni mogoče izogniti.

Vrnimo se torej k EPR paradoksu. Leta 1931 je Einstein v ZDA sodeloval s Tolmanom in Borisom Podolskim, kjer so skupaj objavili članek na temo poskusa z dvema delcema, ki istočasno zapustita izvir. Ugotovili so, da gibanje delca ni negotovo le v prihodnosti temveč tudi v preteklosti in na podlagi tega ugotovili, da delca ne morejo izmeriti, ne da bi ga zmotili oziroma spremenili njegove gibalne količine. A menili so, da kvantna mehanika vseeno ni popolna.

Einstein si je izmislil poskus, kjer dva delca letita en proti drugemu, sodelujeta, nato odletita narazen. Potem izmerimo prvi delec in izvemo nekaj o drugemu. Vprašanje: kako na končno stanje drugega delca vpliva merjenje, če pa smo merili prvi delec, ki ne sodeluje več z drugim delcem? Merjenje v delu prostora A res ustvari tudi rezultat v delu prostora B. Vendar spoznanje, ki v poljubno kratkem času seže iz dela A v B ni prenašalec nobenega sporočila in posledično ne nasprotuje teoriji relativnosti (kjer sporočilo ne potuje hitreje od svetlobe). Po tej strani EPR ni spremenil pojmovanja kvantne mehanike. Razprave o EPR paradoksu pa še vedno trajajo.

29 let kasneje je fizik **John Bell** pokazal, da je mogoče eksperimentalno preveriti ali je naš svet lokalen in resničen. Njegov teorem je danes znan kot Bellove neenakosti (Bell's inequalities). Zelo v splošnem lahko povzamemo Bellov teorem: posledica podrobne napovedi kvantne mehanike je to, da lastnosti sistema ne obstajajo. Izrek ni odvisen od tega ali kvantna mehanika ponuja popoln opis realnosti ali ne.



Slika3: John S. Bell, Vir: http://phys.bspu.unibel.by/hist/physport/physlist.html

Še nekaj let kasneje, 1982 so na ameriških univerzah naredili več poskusov, ki so dokazali, da so predvidevanja kvantne mehanike pravilna, Einstein pa ni imel prav, ko je trdil, da je kvantna mehanika lokalna teorija. Merili so polarizacijo dveh fotonov, ki sta nastala po zaporednih prehodih atoma v različna stanja. Rezultati so se skladali z napovedjo kvantne mehanike.

Tukaj pa je tudi velika razlika med kvantno in klasično fiziko – klasična fizika namreč predpostavlja, da na velikih razdaljah telesi postaneta neodvisni eno od drugega in ne delujeta več eno na drugo. V kvantni mehaniki pa fotona, ki nastaneta skupaj, ostaneta povezana ne glede na razdaljo, če ju vmes ne zmotimo – ta fotona ustrezata delcema pri EPR paradoksu. Govorimo o "entanglement" oziroma prepletenem stanju. Izraz je skoval **Erwin Schrodinger** (v originalu Verschränkung). S tema fotonoma

2 prav z Einsteinovim načelom ekvivalentnosti

ni mogoče prenesti sporočila, lahko pa ju uporabimo za šifriranje. Ena izmed obetajočih “kvantnih” področij je tudi kvantno kodiranje, ki ga omogoča prepletenost. Vendar na tem mestu kriptografiji ne bomo posvečali večje pozornosti.

V spodnjih tabelah lahko vidimo pod a) v prvi vrstici naključno zaporedje bitov, ki jih Alice želi poslati, v drugi njen izbor polarizacije za vsak bit in v zadnji vrstici tabele polarizacija fotona, ki ga pošlje b) dejansko stanje polariziranega fotona, ki ga sprejme Bob, njegove nastavitve polarizacije c) Alice pokliče Boba ter mu pove katere nastavitve je uporabila, da lahko Bob zavrže bite, kjer nista uporabila istih. Če nekdo prisluškuje, bosta Bob in Alice prišla do nesoglasij, čeprav sta imela iste nastavitve.

a)

1	1	1	1	1	0	0	1
x	+	x	x	x	x	x	+
\	-	\	\	\	/	/	-

b)

\	-	\	\	\	/	/	-
+	+	x	+	x	x	+	x
0	1	1	1	1	0	0	0

c)

	1	1		1	0		
	+	x		x	x		
	+	x		x	x		
	1	1		1	0		

Superpozicija

"Do you know Hilbert? No? Then
what are you doing in his space?" -
šala študentov MIT

Princip superpozicije za vse linearne sisteme pravi, da če iz A sledi X in iz B sledi Y, potem iz A + B sledi X+ Y. V matematiki superpoziciji pravzaprav rečemo aditivnost in lahko zapišemo:

$$f(x+y)=f(x)+f(y)$$

Slovar slovenskega knjižnega jezika nam pove, da je superpozicija: *superpozícija -e ž (í) fiz. združevanje dveh ali več valovanj* – in res v fiziki najpogosteje srečamo izraz superpozicija ravno pri valovanju. Ko dve valovanji potujeta skozi isti del prostora in v istem času $s_1(x,t)$ in $s_2(x,t)$, obe valovanji skupaj tvorita novo valovanje, ki ima enako frekvenco in potuje v isti smeri. Pravimo, da je novo valovanje nastalo s superpozicijo obeh začetnih valovanj s_1 in s_2.

$$s(x,t)=s_1(x,t)+s_2(x,t)$$

Ne gre za nič drugega kot za interferenco – kot imenujemo ta pojav. Odmik v novem valovanju v izbrani točki in v izbranem trenutku je vsota odmikov v prvem valovanju in v drugem valovanju v tej točki (x) in v tem trenutku (t). Premike seštevamo kot vektorje. Valovanji se lahko oslabita ali pa ojačata.

Kvantna superpozicija

Kvantna superpozicija je eden izmed osnovnih zakonov kvantne mehanike. Rečemo, da definira nabor vseh stanj, ki jih lahko zavzame delec.

Za lažjo predstavo vzemimo optično prevaro imenovano Neckerjeva kocka (prvič jo je objavil L.A. Necker, po katerem je tudi poimenovana, leta 1832). Ko gledamo skico kocke, se nam enkrat "zdi", da je leva stranica v ospredju, drugič da je desna stranica v ospredju. Ko enkrat vidimo kocko v danem položaju, moramo rahlo pogledati vstran, da lahko z očmi preklopimo na drug "položaj" kocke. Tako lahko rečemo, da skica predstavlja pravzaprav kocko v obeh legah – odvisno pa je od opazovalca kako jo bo zagledal. V trenutku, ko vidimo desno stranico v ospredju, je ta slika edina prava. Nekako tako si lahko zelo približno predstavljamo kvantno superpozicijo.

V teoriji verjetnosti ima vsak mogoč dogodek ustrezno realno število med 0 in 1, ki opisuje verjetnost, da se bo dogodek res zgodil. Verjetnost dveh neodvisnih dogodkov (na primer dogodek A in dogodek B) je zmnožek obeh verjetnosti AxB. Podobno teorija verjetnosti obravnava tudi med sabo se izključujoče dogodke, idr.

Tako tudi v kvantni mehaniki obravnavamo dogodke, le s to razliko, da ne gre za verjetnosti (ki so

seveda očitno vedno nenegativna realna števila) ampak amplitude (kompleksna števila). Princip superpozicije pravi, da lahko svet opišemo tako, da vsaki možni situaciji pripišemo ustrezno kompleksno število in spremembe opišemo tako, da matematično obravnavamo ta števila, kot bi šlo za verjetnosti. Ker tu ne gre le za nenegativna realna števila, se lahko zgodi, da če imamo več možnosti kako bo dogodek potekal – da se sploh ne bo zgodil. Kar je navidez skregano z vsakdanjo logiko, a če pomislimo, da gre lahko za dogodek z negativno "verjetnostjo" in dogodek s pozitivno"verjetnostjo" si to lažje predstavljamo.

Princip superpozicije torej pravi: če je lahko svet v kakršnem koli stanju, razporedu delcev in če je lahko tudi v nekem drugem stanju, potem je lahko tudi v stanju, ki je superpozicija teh dveh stanj.

Vzemimo na primer stanji A in B. Če je lahko delec v A in B, potem je lahko tudi v stanju, ki je 2i/3 stanja A in 1/5 stanja B. Z |*> označimo, da gre za stanje (pozicijo) delca. To je tako imenovana Diracova notacija ali Bra-ket notacija, ki je standard za opisovanje kvantnih stanj v kvantni mehaniki. Je izredno razširjena med fiziki, v matematiki se je načeloma ne uporablja.

Sedaj lahko zapišemo:

$$|\psi> = \frac{2}{3} i\,|A> + \frac{1}{5}|B>$$

Pomembni sta relativna velikost komponent in kot, ki ga oklepata med seboj na kompleksni ravnini. Stanji, ki sta večkratnika drug drugemu sta torej enaki v opisu situacije.

$$|\psi> \approx \alpha\,|\psi>$$

Če se stanje A spremeni v stanje A1 in B v stanje B1, potem se bo v istem času tudi superpozicija spremenila v seštevek stanj A1 in B1 z istimi koeficienti kot sta se spremenili stanji A in B.

Kvantna superpozicija je dolgo časa zaradi svoje "nelogičnosti" begala priznane fizike. Na tem mestu lahko omenimo znani miselni poskus imenovan "Schrödingerjeva mačka" po avstrijskem fiziku s polnim imenom Erwin Rudolf Josef Alexander Schrödinger. Poskus, ki se glasi takole je predstavil leta 1935:

> V zapečateni škatli naj sedi mačka. S škatlo je povezana naprava, ki vsebuje radioaktivna atomska jedra in posodo s strupenim plinom. Na napravo mačka ne more vplivati. Preskus je pripravljen, ko je natančno 50% možnosti, da v eni uri razpade jedro. Če jedro razpade, bo oddalo delec, ki sproži napravo in ta odpre posodo, tako da plin mačko ubije. Če jedro ne razpade, mačka preživi. Kvantno-mehansko gledano neopazovani delec predstavlja superpozicijo (obstaja sočasno) »razpadlega« in »nerazpadlega jedra«. Ko opazovalec odpre posodo, vidi le »razpadlo jedro/mrtvo mačko« ali »nerazpadlo jedro/živo mačko«. Vprašanje se glasi: kdaj sistem preneha obstajati kot mešanica obeh stanj in postane eno ali drugo?

S tem je Erwin poskušal prikazati paradoks oziroma problem, ki ga je videl v kvantni mehaniki

(Kopenhagenska interpretacija)[3]

Miselni eksperiment je bil prvotno mišljen kot odgovor oziroma debata o EPR paradoksu. Seveda Erwin ni mislil dobesedno; mačko je izbral ravno zato, ker je želel pripeljati primerjavo do absurda. Vprašanje, ki ga postavlja pa je seveda: KDAJ se kvantni sistem nahaja v enem izmed in ne več v skupku dveh stanj? Bolj fizikalno se lahko vprašamo: kdaj pravo kvantno stanje ni več linearna kombinacija stanj? Če mačka preživi, se zagotovo ne bo spomnila, da je bila vmes mrtva in živa, ampak se spomni le, da je živa.

Slika4: Miselni eksperiment je postal strašno priljubljen v pop kulturi, Vir: http://www.thinkgeek.com/tshirts-apparel/womens/6f59/zoom/

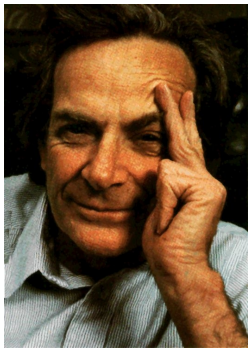
Prve ideje o kvantnem računalniku

Leta 1959 je **Richard Feynman** (priznan ameriški fizik, dobitnik Nobelove nagrade leta 1965)[4] v govoru[5], ki ga je imel po zborovanju ameriških fizikov po svoje napovedal prihodnost. Morda bi celo lahko rekli, da je s tem govorom označil začetek nove dobe nanotehnologije. Kot nanotehnologijo razumemo znanost, ki se ukvarja z manipulacijo snovi na nivoju nanometra. Poudaril je, da pravzaprav ne ustvarja nove fizike, le predlaga kako bi se to, kar že vemo (če so zakoni res taki, kot predpostavljamo) dalo narediti. Izjavil je, da bo podaril 1000 dolarjev nagrade tistemu, ki bo prvi naredil zelo majhen elektromotor in tistemu, ki bo celotno vsebino (informacije, ki jih knjiga nosi) neke knjige uspel spraviti na 4x10^-5 velikost. Obe nagradi je podelil, prvo že naslednje leto, drugo pa 26 let kasneje.

3 Poznamo več interpretacij, a po tej interpretaciji z merjenjem določene opazljivke sistema vedno zmotimo valovno funkcijo, tako da ta zavzame eno od tako imenovanih lastnih stanj te opazljivke. Verjetnost za posamezno lastno stanje določa stanje valovne funkcije, tik preden smo jo zmotili. Za zgled si oglejmo delec, ki se giblje v praznem prostoru. Če izmerimo lego delca, bomo dobili neko naključno vrednost x. V splošnem njene natančne vrednosti ne moremo napovedati vnaprej, je pa verjetneje, da bomo izmerili vrednost blizu središča valovnega paketa, kjer je amplituda verjetnostne gostote večja. V trenutku, ko meritev izvedemo, pa se valovna funkcija »sesede« v lastno stanje, ki je ostro nakopičeno okoli izmerjene vrednosti x.

4 BBC dokumentarec http://video.google.com/videoplay?docid=877738137850228685 2#

5 Prepis govora si lahko prebere bralec na http://www.zyvex.com/nanotech/feynman.html



Slika5: Richard Feynman; Vir: http://phys.bspu.unibel.by/hist/physport/physlist.html

Kaj se je torej do današnjega dne dogajalo s Feynmanovo vizijo nanotehnologije? V zgodovino računalništva, izum tranzistorja, prve osebne računalnike itd. se tukaj ne bomo spuščali. Zanimiv za nas pa je nov tip polprevodnika – t.i. "kvantna pika". To je odkril Louis E. Brus, profesor kemije, ko je bil zaposlen pri Bell labs. Izdelajo jo lahko, ko formirajo vrata iz kovine na površju kvantne jame.

Kaj pa je kvantna jama? To je potencialna jama, ki zadržuje delce, ki so se originalno premikali prosto v vse smeri, da se lahko gibljejo le v dveh smereh – torej le na ravnini. Izdelajo jih (v polprevodnikih) tako, da uporabijo material, kot je galijev arzenid (1,43 eV @ 300K) med dvema plastema drugega materiala, ki ima večji "band gap", kot je aluminijev arzenid (2,16 eV @ 300K).

S tem omogočijo elektronom, da lahko pridejo v piko s kvantnim tuneliranjem[6]. Kot rezultat imajo kvantne pike lastnosti, ki so nekje med navadnimi polprevodniki in diskretnimi molekulami.

Vrnimo se k Feymanu, ki je leta 1981 (nekateri viri navajajo 1982) šel še dlje v svojih napovedih in predstavil idejo o shranjevanju enega bita informacije z uporabo kvantnih stanj enega atoma, elektrona ali fotona. Za atom naj bi lahko uporabili dva najnižja nivoja energije za 0 ali 1, pri elektronu spinska kvantna števila[7] (1, -1), foton pa v dveh polariziranih stanjih (V in H)[8].

Kvantna informacija

Kot smo že omenili, je bila ideja Feymana, da bi namesto bitov uporabili kvantna stanja enega atoma, elektrona ali fotona. Vse skupaj zgleda kot implementacijama že znanega o računalniškem pomnjenju, saj je v "navadnem" računalniku bit predstavljen z eno pomnilno celico (ali preklopom, če gre za preklopno vezje). A tukaj pride do izraza superpozicija. Nova lastnost kvantne informacije izhaja ravno iz zmožnosti kvantnega sistema, da ni le v stanju 0 ali 1, temveč tudi v superpoziciji le-teh, kot to zahteva kvantna mehanika. To je bil velik skok v razmišljanju o sami informaciji, saj se je po 50 letih

6 Za kaj pa gre pri kvantnem tuneliranju? Če proizvedemo strukturo iz dveh elektronov in izolacijsko pregrado med njima, pričakujemo, da se bosta elektrona lahko tunelirala čez pregrado.

7 Posamezen elektron ima lahko bodisi spinsko kvantno število +1 (angl. spin-up), označeno kot ↑, bodisi spinsko kvantno število −1 (angl. spin-down), označeno kot ↓,

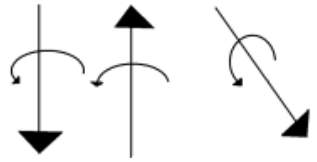
8 Predpostavljamo vertikalno polariziran foton, ki se bliža polaroidni merilni napravi. Če je polaroid v poziciji V (vertikalno), bo foton prešel čez neovirano, če pa bo v poziciji H (horizontalno) bo zagotovo absorbiran in ne bo prišel čez. Glej EPR paradoks

računalništva zdelo, da je pojem informacije nespremenljiv. Skupaj s tem prinaša kvantno računalništvo tudi nove algoritme (Shorov, kvantni model Turingovega stroja, Groverjev, …).

Qubit

Bitu informacije shranjenemu v kvantnem računalniku rečemo qubit oziroma quantum bit, kvantni bit. Čeprav lahko qubitu pripišemo tudi vrednosti 0 in 1, se vseeno od bita zelo razlikuje. Za opis klasičnega bita potrebujemo le eno binarno vrednost, medtem ko za opis enega realnega števila potrebujemo v načelu neskončno bitov, qubit pa opišemo pravzaprav z dvema realnima številoma. Ključna razlika med nam zelo dobro poznanim bitom in qubitom je v tem, da je vrednost bita vedno ali 0 ali 1 (seveda tukaj ne govorimo v smislu signala, ki lahko oslabi) medtem ko je vrednost qubita lahko poljubna linearna kombinacija 0 in 1 s kompleksnimi koeficienti. Seveda tako kot zakoni klasične fizike, tudi zakoni elektrotehnike ne veljajo za qubit, ki je del kvantne mehanike.

Qubit ima namesto dveh logičnih stanj dva vektorja $\alpha|0>ter\,\beta|1>$.



Slika6: Spinska predstavitev qubita, z leve proti desni |0>, |1> a |0> +b|1>

Druga pomembna razlika med klasičnimi biti in qubiti pa je ta, da qubiti lahko tvorijo prepletena stanja (že omenjen entanglement). A kako zgleda dejanska predstavitev qubita? Če je klasični bit predstavljen z napetostjo na kondenzatorju (recimo), kako lahko predstavimo qubit? Za to potrebujemo kvantni sistem, ki ima dve dobro ločeni stanji, ki nam pomenita stanji qubita |0> in |1>. Ker želimo s qubiti računati ter nemoteno delati, mora biti gibanje kvantnega sistema popolnoma urejeno in nadzorovano, motnje (kot vemo že iz klasičnega računalništva na primeru presluhov, odbojev) namreč zelo hitro onemogočijo pravilno delovanje in rezultat naših izračunov je napačen. Proces, ko neurejeno gibanje delcev v okolici pokvari proces računanja, imenujemo dekoherenca. Dekoherenca (s prepletenostjo ali brez) je fenomen kvantne teorije, ko se izgubi koherenca in s tem izgubimo interferenco.

Izpolniti moramo najmanj dva pogoja:

1. qubiti morajo biti dobro ločeni od okolice
2. znati moramo dobro nadzorovati medsebojno delovanje med qubiti.

Ta pogoja sta si pogosto nasprotujoča, torej nobene sklopitve z okolico, a hkrati močna sklopitev med sabo v kvantnem računalniku.

Pogosta in popularna je predstavitev qubitov s fotoni. Ti lahko zasedejo dve osnovni, med seboj pravokotni polarizaciji. Ti dve različni polarizaciji nam predstavljata stanji |0> in |1>, npr. stanje |0>

pomeni navpično polarizacijo, stanje |1> pa vodoravno. Foton kot kvantni delec se lahko nahaja v poljubni superpoziciji obeh polarizacij. Dobra lastnost fotonov je, da so vplivi okolice zelo šibki, a to hkrati tudi pomeni, da je fotone težko sklopiti med seboj.

Spinski model

Vsak vektor največkrat predstavlja neskončno stanj, vsota le-teh pa določi stanje. Qubit je lahko vezan na "spinski" model, ki ustreza gibanju kvantnega delca. Spin je lastna vrtilna količina kvantnega delca, velikost spina podajamo s spinskim kvantnim številom (večkratnik Planckove konstante)[9].

Qubit lahko postavimo v formalne okvire, tako da lahko z njim računamo in sicer je qubit bit, ki ga dosežemo z dvema nivojema v kvantnem sistemu, povedano drugače: qubit je vektor stanja v dvonivojskem kvantno-mehanskem sistemu, kar je formalno ekvivalentno dvorazsežnemu vektorskemu prostoru nad kompleksnimi števili (to pa je Hilbertov prostor). Posledično lahko rečemo da je qubit tudi H2, dvodimenzionalni Hilbertov prostor. Fizikalna stanja v kvantnem svetu je namreč mogoče zelo natančno opisati z (enotnimi) vektorji v Hilbertovem prostoru, kjer predstavljajo hermitski operatorji fizikalne količine, lastne vrednosti operatorjev pa vse možne izide, ki jih lahko merjenja dajo. John von Neuman je prvi opazil, da sta dva navidezno zelo različna pristopa h kvantni mehaniki, Schroedingerjev valovni in Heisenbergov matrični, dejansko le dva različna modela istih (izomorfnih) operatorjev v Hilbertovem prostoru, matematično sta posledično ekvivalentna. Kaj pa je sploh Hilbertov prostor? Hilbertov prostor H (poimenovan po nemškem matematiku Davidu Hilbertu) je poln vektorski prostor s skalarnim produktom, v katerem lahko merimo dolžine in kote. Skalarni produkt inducira normo na H, ki inducira metriko na H, v kateri je H poln.

Imamo vektorski prostor V nad poljem K kompleksnih števil. Za $x, y \in V\ \alpha = (x, y);\ \alpha \in K$. Skalarni produkt v prostoru V je preslikava: $(.|.): V\ x\ V \rightarrow K$ ki se predstavlja z naslednjimi lastnostmi:

- $H_1: (x, x) \geqslant 0, (x, x) = 0 \Leftrightarrow x = 0;$
- $H_2: (x|x) = 0, \check{c}e\ je\ x = 0;$
- $H_3: (\alpha x|y) = \alpha(x|y),\ velja\ za\ vsak\ \alpha \in K\ ter\ za\ vsak\ x, y \in V$
- $H_4: (x_1 + x_2|y) = (x_1|y) + (x_2|y)\ velja\ za\ vsak\ x_{1,} x_{2,} y \in V$
- $H_5: (x|y) = \overline{(x, y)}\ velja\ za\ vsak\ x, y \in V$

Posledici gornjih petih lastnosti sta:

- $(x|\alpha y) = \overline{\alpha}(x|y)$
- $(x|y + z) = (x|y) + (x|z)$

S tem smo opredelili skalarnost. Prostor, v katerem velja zgoraj zapisani skalarni produkt je unitaren. V prostoru v katerem je definiran ta skalarni produkt, postavimo normo:

9 Planckova konstanta je poimenovana po nemškem fiziku Maxu Plancku. Je osnovna fizikalna konstanta, ki opisuje velikosti kvantov. Navadno jo označujemo s črko h. Njena vrednost je: $h = 6{,}62606896(33)\ x10^{-34}\ Js$

$$||x|| = \sqrt{((x|x))}$$

Na njeni osnovi pridemo do normiranega prostora H = () z unitarnimi značilnostmi. H je torej unitarni prostor, za katerega veljajo značilnosti:

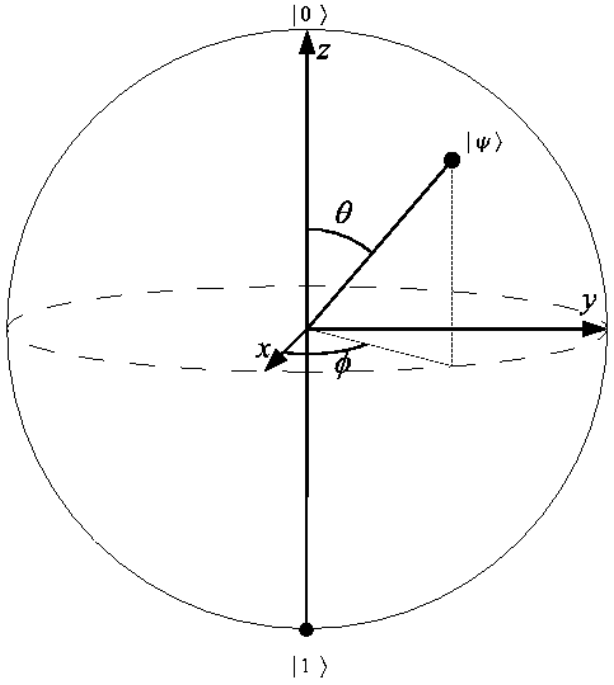
- $||x+y|| = ||x|| + ||y||$
- $||(x|y)|| \leq \sqrt{((x|x))}\sqrt{((y|y))}$
- $||x+y||^2 + ||x-y||^2 = 2(||x||^2 + ||y||^2)$

Blochova sfera

Prostor stanja posameznega qubita lahko ponazorimo z Blochovo sfero. Če komponente qubita uporabimo kot kartezične koordinate, nam padejo vsa možna fizikalna stanja v sfero z radijem, ki je enak enoti (polmer ima 1), ki jo imenujemo Blochova sfera. Vsa stanja, ki so na površju sfere imenujemo čista stanja (pure states). V kvantni mehaniki rečemo, da je Blochova sfera geometrijska predstavitev čistih stanj v dvo-nivojskem kvantnem sistemu. Poimenovana je po švicarskem fiziku Felixu Blochu, v Švici rojenega fizika, ki je večino svojega življenja preživel v ZDA in med drugo svetovno vojno delal v Los Alamosu z drugimi priznanimi fiziki takratnega časa.

Geometrijsko gledano je Blochova sfera dejansko sfera in lahko čista stanja nazorno podamo. Posplošeno se lahko Blochova sfera nanaša tudi na analogni prostor n-nivojskega kvantnega sistema.

Kot sem že zapisala, je kvantna mehanika formulirana v Hilbertovem prostoru. Prostor čistih stanj je podan z enodimenzionalnim podprostorom Hilbertovega prostora. Prostor enodimenzionalnih podprostorov v kateremkoli vektorskem prostoru je projeciran prostor.



Slika7: Blochova sfera, Vir: http://www.quantiki.org/wiki/index.php/Bloch_sphere

Kvantni računalnik

I believe that at the end of the century the use of words and general educated opinion will have altered so much that one will be able to speak of machines thinking without expecting to be contradicted. - Alan Turing leta 1950 za revijo Mind

Richard Feynman je v začetku 80. let prejšnjega stoletja šel še dlje v svojih napovedih in predstavil idejo o shranjevanju enega bita informacije z uporabo kvantnih stanj enega atoma, elektrona ali fotona na konferenci na MIT. Vse skupaj naj bi se zgodilo zato, ker je pred tem eno leto sodeloval z Edwardom Fredklinom, ki je bil fizik in računalničar. Fredklin je predstavil idejo "obratnega" računalnika – v običajnem računalniku imamo strogo določen vhod in izhod na logičnih vratih, tega ne moremo zamenjati. Fredklinova nova vrata pa je možno obrniti, spodaj je primer najenostavnejših vrat, levo tabela za klasična vrata, desno pa tabela za Feymanova CNOT (contreolled NOT) vrata.

a	NOT a
0	1
1	0

a	b	a´	b´
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Iz tabele je razvidno, da lahko CNOT vrata ohranijo stanje, ali pa se obnašajo kot navaden negator. A vseeno, zakaj bi se s tem ukvarjali? Nadvse pomembno za kvantno računalništvo je dejstvo, da so zakoni kvantne mehanike lahko "obratni" v času. S tem je postalo jasno, kaj bo potrebno za kvantni računalnik – fizični sistem, kjer je informacija lahko shranjena v obliki qubitov in imeti mora mehanizme, s katerimi bi qubiti začeli medsebojno interakcijo in opravljali obratne logične operacije.

Zaradi superpozicije lahko predpostavimo, da smo naš računalnik zagnali tako, da je v superpoziciji vseh začetnih stanj, kar pomeni, da lahko vse izračunamo hkrati.

Leta 1985 je David Deutsch, fizik, ki predava na Oxfordski univerzi, prvi pokazal, da so kvantni računalniki (v teoriji) hitrejši in zmogljivejši od klasičnih. To naj bi bilo res zaradi tako imenovanega "kvantnega paralelizma". Najprej se zazdi, da je velika težava, ker bomo z meritvijo superpozicije izvedeli le stanje enega delca, kar ni dovolj. A omenili smo že "prepletanje" - izraz, ki ga je skoval Schrodinger.

Leta 1994 je **Peter Shor** (glej "kvantni algoritmi") prvi objavil uporaben algoritem za kvantni računalnik. To je bil naslednji veliki preboj v kvantnem računalništvu.

Leta 1999 je Charles Bennet (IBM) dejal, da so že tako daleč z raziskavami o kvantnem računalništvu, da bo kmalu dolgočasno. A dodal, da je seveda še nekaj malenkosti – kot na primer dejansko zgraditi tak računalnik …

Leta 2001 so Shorov algoritem preizkusili v podjetju IBM, kjer so na prafaktorje razstavili število 15 z NMR implementacijo kvantnega računalnika[10]. Rezultate so objavili v članku "Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance" v reviji Nature. Vendar so se kasneje pojavili dvomi, če je bila to res prava demonstracija kvantnega procesiranja, saj ni bilo moč opaziti prepletanja.

Če gre verjeti Wikipediji[11] , je trenutno v razvoju veliko vrst kvantnih računalnikov (prevajanje imen se mi ni zdelo smselno):

- Superconductor-based quantum computers (including SQUID-based quantum computers)
- Trapped ion quantum computer
- Optical lattices
- Topological quantum computer
- Quantum dot on surface (e.g. the Loss-DiVincenzo quantum computer)
- Nuclear magnetic resonance on molecules in solution (liquid NMR)
- Solid state NMR Kane quantum computers
- Electrons on helium quantum computers
- Cavity quantum electrodynamics (CQED)
- Molecular magnet
- Fullerene-based ESR quantum computer
- Optic-based quantum computers (Quantum optics)
- Diamond-based quantum computer
- Bose–Einstein condensate-based quantum computer
- Transistor-based quantum computer - string quantum computers with entrainment of positive holes using an electrostatic trap
- Spin-based quantum computer
- Adiabatic quantum computation
- Rare-earth-metal-ion-doped inorganic crystal based quantum computers

Kvantni algoritmi

Algoritem se na “navadnem” računalniku izvaja kot zaporedje operacij, ki nizu vhodnih bitov priredi niz izhodnih bitov; algoritem, ki ga izvaja kvantni računalnik, pa je unitarna transformacija, ki začetno valovno funkcijo prevede v končno ($\psi = U\psi$).

V računalništvu velikokrat probleme razvrstimo glede na časovno zahtevnost, ki ni nič drugega kot

10 Najbolj razširjena implementacija kvantnih računalnikov so NMR (Nuclear magnetic resonance), ki qubit predstavijo s spinom jedra v neki molekuli.

11 http://en.wikipedia.org/wiki/Quantum_computer#Developments

koliko korakov potrebujemo za njihovo rešitev. Seštevanje dveh števil, ki imata n števk, zahteva na primer n operacij. Najprej moramo sešteti enice, potem desetice, ...in tako naprej, vsega skupaj torej n osnovnih korakov. Na isti način lahko rečemo, da potrebujemo n^2 operacij za množenje, saj množimo vsako številko z vsako (za trimestno številko opravimo 9 operacij). V grobem lahko probleme razdelimo na tiste, pri katerih časovna zahtevnost raste z velikostjo problema n kot potenca n in na tiste, kjer zahtevnost narašča eksponentno z n, torej kot 2n. V prvo skupino spadata zgoraj omenjena seštevanje in množenje.

Problemi, ki imajo eksponentno zahtevnost, so izredno počasni, pravzaprav lahko rečemo, da so za človeka nerešljivi. Zakaj pravimo, da so "skoraj" nerešljivi – dober primer je razstavitev celega števila na prafaktorje ki ima zahtevnost 2n (število operacij za najboljši algoritem narašča malenkost počasneje kot eksponentno). Predpostavimo, da uspemo za n=1, torej za enomestna števila, oba problema rešiti na pamet brez uporabe pripomočkov v eni sekundi. Če sedaj upoštevamo zahtevnost obeh algoritmov, bomo za n=8 (torej osemmestna števila) potrebovali eno minuto za množenje in dve minuti za faktorizacijo. Za n=30 bomo za množenje potrebovali 15 minut, za faktorizacijo pa že 15 let! Kar je seveda preveč in tako lahko z lahkoto trdimo, da so določeni izračuni za človeka nerešljivi, še posebno ker vse skupaj eksponentno narašča.

Vsi torej vemo, da so nekateri problemi vsekakor bolj primerni za računalniško reševanje in s primernimi algoritmi tudi zelo trivialni. A faktorizacija velikih števil je tudi z uporabo računalnika praktično nemogoča. Več kot stomestnih števil tudi z računalniki ne gre razstavljati na praštevila! Smiselnost tega je seveda malo vprašljiva, dokler ne povežemo faktorizacije z metodo šifriranja z javnim ključem. Dejstvo, da je faktorizacija za klasične računalnike praktično nerešljiv problem, izkoriščajo razni kriptografski postopki.

Leta 1994 je Peter Shor, takrat zaposlen v laboratorijih AT&T Bell v ZDA (v laboratorijih iste družbe so približno 50 let prej naredili tudi prvi tranzistor), odkril kvantni algoritem za iskanje prafaktorjev danega števila, ki potrebuje le n^3 korakov, to je bistveno manj kot najboljši klasični algoritem. To pomeni, da bi bila faktorizacija več tisoč mestnih števil za kvantni računalnik mogoča. Algoritem je danes poznan kot Shorov algoritem in je sestavljen iz dveh delov:

1. Sprememba, ki jo lahko opravi tudi klasični računalnik in sicer problem iskanja prafaktorjev spremenimo v problem iskanja
2. Kvantni algoritem za iskanje

Shorov algoritem so preizkusili leta 2001 na IBMu in sicer so na praštevila razstavili 15 (5x3) z uporabo kvantnega računalnika s sedmimi qubiti. Narejenih je bilo veliko izboljšav Shorovega algoritma; med njimi lahko omenimo Davida McAnally-ja.

Zanimiv kvantni algoritem je odkril tudi Lov Grover (leta 1996), in sicer za iskanje danega elementa v podatkovni bazi, kot je na primer iskanje davčne številke državljana na podlagi imena in priimka. V najslabšem primeru klasično iskanje – če je državljanov n, zahteva to iskanje od nas n korakov. Seveda obstajajo zelo dobri algoritmi za iskanje tudi za "navadne računalnike", a s kvantnim računalnikom je mogoče to opraviti v približno $\sqrt{n}$ korakih. Zanimivo je, da bi bila ena izmed uporab takšnega kvantnega algoritma za iskanje ponovno povezana s kriptografijo.

Vzporedno z razvojem novih kvantnih algoritmov so se razvijale tudi nove tehnike algoritmov. Prav

tako je bilo veliko razvoja narejenega v smeri novih protokolov za kvantno komuniciranje. A vendarle moramo na koncu priznati, da poleg teh primerov uporabe ni veliko problemov, kjer bi bili kvantni računalniki hitrejši kot klasični. Razlogov je več. Prvič je pri kvantnih računalnikih treba rezultat dobiti na zelo nenavaden in človeškemu svetu tuj način, s superpozicijo in to otežuje razvijanje novih algoritmov. Drug razlog pa je, da seveda želimo razviti kvantne algoritme, ki so boljši kot vsi doslej znani klasični algoritmi, vendar je kvantno računalništvo razmeroma mlado področje. Klasični algoritmi so v teku razvoja že 50 in več let. Eno izmed glavnih še neodgovorjenih vprašanj kvantega računalništva tako ostaja, katere probleme sploh lahko rešimo s kvantnimi algoritmi hitreje kot z najboljšimi klasičnimi?

Superpozicija in kvantni računalnik, zaključek

Ni mi všeč in žal mi je, da sem imel karkoli opraviti z njo! - Erwin Schrödinger o naključnosti v kvantni mehaniki

Večinoma smo pomembnost fenomena superpozicije že spoznali skozi prejšnja poglavja seminarske naloge. Poskusimo nekako povzeti.

Qubit v koherentni superpoziciji opišemo z dvema realnima številoma, ki povesta, kolikšna je verjetnost, da najdemo qubit v stanju |0> oz. |1>, in kakšna je faza med obema stanjema. Kvantna teorija pravi, da lahko za qubit, ki je v koherentni superpoziciji, napovemo le verjetnost, da ga pri meritvi najdemo v stanju |0> oziroma |1>. Tako bi pri meritvi stanja qubita dobili včasih rezultat |1>, včasih |0>, četudi je ta vedno v natanko istem stanju. Izračunamo lahko le verjetnosti za oba izida, ne pa, ali bomo pri konkretni meritvi izmerili |1> ali |0>. To, da kvantna mehanika napoveduje naključnost kot osnovno lastnost naravnih pojavov, je zelo nenavadno. Iz običajnega sveta makroskopskih teles smo navajeni, da so stvari popolnoma predvidljive, če le poznamo začetne pogoje. V kvantnem svetu majhnih delcev je drugače.

Še bolj nenavadna lastnost kvantnih delcev kot superpozicija, o kateri smo že pisali (glej str.) je prepletenost (entanglement), ki smo jo že omenili pri poskusu s Schrodingerjevo mačko. Prepletenost je za razliko od interference popolnoma kvantni pojav. Je tudi odločilna zadeva za uspešno teleportacijo kvantnih stanj (na podlagi stanja enega delca ugotovimo stanje drugega delca ne glede na oddaljenost, če sta prepletena), torej neke vrste prenos na daljavo (seveda tukaj ne govorimo o znanstveni fantastiki in beam me up, Scotty), varno kriptografijo ali pa kvantno računanje. Predvsem je pomembno za kvantno računalništvo, da prepleteno stanje dveh qubitov tako vsebuje več informacije kot pa stanji obeh qubitov posebej – težava bi bila velika, če bi lahko pri meritvi kvantne superpozicije ugotovili le eno stanje enega izmed delcev. Zato je “entanglement” oziroma prepletenost prav tako izredno pomemben pojav za razvoj kvantnega računalništva.

Uporabljena literatura

HEY, T., WALTERS P. 2004. The new quantum universe, *Quantum jumps, Quantum engineering,* Cambridge University Press

STRNAD, J. 2005. Einstein E=mc2, *Einstein in kvantna mehanika, Poskus EPR*, Modrijan založba

VIRANT, J. 2007. Načrtovanje nanoračunalniških struktur, *Kvantnost v računalniških strukturah in sistemih, Zbirka teoretičnih podlag za QCA,*Založba Didakta

STRNAD, J. 1995. Fizika 1. del, *Nihanje in valovanje, valovanje v eni razsežnosti,* str. 152 – 158

WOLFRAM, S. 2002. A new kind of science, *Chapter 9, fundamental physics,* Wolfram media Inc.

GIANCOLI, D. C. 2009. Physics for scientists & engineerswith modern physics, fourth edition, *Quantum mechanics – chapter 38,* Pearson education Inc.

ŽNIDARIČ, M. 2005. Kvantni računalniki, Proteus, 2 / 68, str. 66 – 73.

Quantum superposition, Quantum computer, ... [online]. Dostopno na URL: http://en.wikipedia.org/

Quantiki portal [online]. Dostopno na URL: http://www.quantiki.org/