Pedagoška fakulteta v Mariboru
Oddelek za fiziko

Kvantni računalnik

Roman Bobnarič

Zadnjih sto let je računalnik temeljito spremenil svet. Vendar pa se bližamo mejam, ko tehnologija več ne bo mogla izboljšati računalniških sposobnosti. Zato bom v seminarju predstavil obetajoče raziskave na področju kvantnega računalništva. Predstavil bom najbolj obetavne tehnologije. Vendar pa nove tehnologije prinašajo tudi nove načine delovanja računalnikov. Zato bom predstavil Shorov algoritem, ki je eden pomembnejših algoritmov, na katerih temeljijo postopki računanja na kvantnih računalnikih.

Mentor: doc.dr. Aleksander Zidanšek

1. Uvod

Računalniki so v zadnjem stoletju korenito spremenili svet in naš pogled nanj. Prvi računalnik je bil težek več ton in je bil primeren le za nekaj osnovnih operacij. Med njim in današnjim računalnikom, ki ga srečamo že skoraj povsod, je ogromna razlika - kot da bi bilo med njima milijon let evolucije. A razvoj je ves čas tekel le v eni smeri, saj današnji najboljši računalniki delujejo še vedno na popolnoma enak način, kot so delovali prvi, kajti razvoj računalnikov je šel le v eni smeri- smeri pomanjševanja. Žal prav kmalu to več ne bo zadostovalo. Zato so se fiziki in elektroniki usmerili v svet najmanjših dimenzij - v svet kvantne mehanike, da bi poiskali rešitev tega problema. In zdi se, da upanje in vse vloženo delo niso šli v nič. Plodovi dolgotrajnega dela in teorijskih razglabljanj so že obrodili prve sadove: prve delujoče kvantne računalnike, ki pa so še vedno v fazi raziskovanja in izboljševanja osnovnih principov.
Do prvih pravih računalnikov, ki bodo sposobni opravljati opravila podobna opravilom današnjih računalnikov, bo verjetno minilo še kar nekaj časa. Vendar pa je kljub temu to zelo obetajoče področje prihodnje tehnologije.

2. Od začetkov do danes

Od izdelave prvih računskih strojev (ne računalnikov) je minilo že več stoletij. Prve prave računalnike pa srečamo šele ob začetku 20. stoletja. Lahko bi rekli, da je bila njihova uporabnost sorazmerna njihovi velikosti. Toda prav kmalu so znanstveniki razvili tehnologijo polprevodniških elementov. Ti so delovali enako kot pred njimi vakuumski elementi, vendar so bili veliko manjši, vzdržljivejši, cenejši in predvsem hitrejši. Ampak kmalu to ni bilo več dovolj in začela se je proizvodnja integriranih vezij. Najprej so bila ta vezja dokaj velika in je npr. tipičen procesor vseboval nekaj 100.000 tranzistorjev. Danes velja za merilo kvalitete tudi površinska gostota tranzistorjev v integriranih vezjih. Nato so tehniko izdelave vezij izpopolnili do te mere, da vsebuje tipičen procesor okoli 7 do 8 milijonov tranzistorjev. Taka je danes večina procesorjev. Tipične velikosti tranzistorja so okoli 1 μm, povezave na vezjih pa merijo le okoli 0,5 μm. Compaq trenutno prehaja na tehnologijo v kateri izdelujejo 0,18 μm debele povezave. Poleg zmanjšanja velikosti se tudi procesi vršijo do 100-krat hitreje, saj so se delovne frekvence povzpele z nekdanjih 5-20 MHz na sedanjih 500-700 MHz.
Ko preučimo stanje v današnji tehnologiji, lahko rečemo, da smo ob izboljšavah zmožni povečati gostoto integriranih vezij še do 100-krat. Če pa pogledamo še 10-krat večjo pomanjšavo, širino litografskega vezja predstavlja nekaj 10 atomov. Tu pa se končajo meje klasičnega poznavanja delovanja elektronskih elementov. Zato moramo poseči po naslednjem primernem orodju za opis: kvantni mehaniki. Prav to so storili teoretični fiziki pred nekaj desetletji.
Kaj se zgodi z informacijami, ko jih vnesemo v kvantni svet? Kako daleč lahko pomanjšamo elektronska vezja, da bodo še delovala? Ali je možno govoriti o informacijah v kvantnem svetu?
Taka in podobna vprašanja so vzpodbudila fizike različnih smeri, da so se osredotočili v pripravo in izdelavo takrat še sanjskih strojev. Tako je bil leta 1997 izdelan 2-bitni kvantni računalnik pod okriljem IBM [1], naslednje leto (1998) pa 3-bitni kvantni računalnik v laboratoriju v Los Alamosu. Leta 1999 je v Münchnu deloval že računalnik na 5 bitih [2].

3. Kvantna informacija

Poraba energije v današnjih računalnikih je namenjena predvsem za delovanje vseh naprav in za vzdrževanje informacijskega stanja v pomnilniku in procesorju. Pri tem vemo, da imamo lahko le digitalno obliko informacij, saj na analognih količinah ne moremo izvajati matematičnih operacij. Vzrok tega je dejstvo, da je analognih količin toliko kot realnih števil, torej neskončno. Veliko lažje je krmiliti neko stanje, ko lastnost je (logično stanje 1) ali je ni (logično stanje 0).
Obe stanji lahko izmerimo kot napetost; prvo kot stanje brez določene referenčne napetosti, drugo ob referenčni napetosti. Vsako od teh osnovnih stanj je osnovna informacija imenovana **bit**.
Sedaj pa se vprašajmo: Kaj bi lahko bil bit v kvantnem svetu?
Tukaj imamo za definicijo osnovnega stanja več možnosti in prav vse so odvisne od načinov merjenja in pisanja na »medij«. Medij je v tem primeru podlaga, na kateri se vrši postopek računanja, npr. kristal soli NaCl, molekule etanola,… Ne glede na zapis osnovnega dela informacije (bita), pa imamo tukaj novo ime za ta pojem - **QUBIT** (= »quantum bit«, angl.), torej kvantni bit.
Zelo zanimivo in tudi uporabno pa je dejstvo, da je lahko qubit tudi superpozicija obeh logičnih stanj (0 in 1), ki jih predstavimo z valovnima funkcijama Ψ_0 in Ψ_1. Tako imamo:

$$\Psi = \Psi_0 + \Psi_1 \quad . \tag{1}$$

Kot vidimo, govorimo pri kvantnih računalnikih o valovnih funkcijah, ki so edine primerne za opis stanj. Tako imamo za zaporedje *n* qubitov zapis:

$$\Psi = \sum_{x=000\ldots0}^{111\ldots1} c_k \left| x \right\rangle \ , \ c_k \in C \ , \ \left\{ 1 < k < 2^n \right\} . \tag{2}$$

Zaradi samega značaja informacij pa so v kvantnem računalniku potrebni popolnoma drugačni načini računanja. Običajni algoritmi več ne delujejo zaradi drugačnega načina delovanja logičnih vrat, ki ne računajo le z logičnimi 1 in 0. Zato je bilo potrebno poiskati nove algoritme.
Eden prvih takih algoritmov je bil Shorov algoritem, ki je namenjen iskanju dveh množiteljev nekega števila (npr. *40301 = 211· 191*), torej faktorizaciji. Zelo uporaben je na področju varovanja podatkov oz. kodiranja. Ena danes najpogosteje uporabljanih metod kodiranja je metoda javnega ključa. Ključ je produkt dveh števil. Eno je javno objavljeno (na www straneh ali pa ga prejme skupina uporabnikov), drugo pa ima pošiljatelj sporočil in drugih informacij.
Shorov algoritem deluje podobno kot Fourierova analiza na valovanjih, vendar pa Shorov algoritem deluje na valovnih enačbah stanj [3]. Njegova prednost je v hitrosti. Leta 1994 je 1600 računalnikov 8 mesecev faktoriziralo 129 mestno število. Shorov algoritem bi na kvantnem računalniku za to isto delo potreboval kvečjemu nekaj ur [4].
Drugi zelo pomemben je Groverjev algoritem. Uporablja se za iskanje funkcije z *n* neznankami in določenim rezultatom enačb. V klasični matematiki se taka funkcija išče v *n* korakih. Ta algoritem pa omogoča isto delo v $\sqrt{n}$ korakih. Danes ga uporabljamo tudi v klasičnih programih kot podprogram [4].
Matematiki in logiki še naprej vztrajno iščejo nove možnosti in načine računanja. Tako so razvili že nekaj različnih algoritmov, ki bodo polno uporabnost pokazali šele v kvantnih računalnikih. Vendar pa so kot idejno vodilo in pomožna orodja že sedaj vključeni v številne programe.

4. Metode računanja

Pri računanju moramo vedno imeti nek medij, na katerega zapisujemo in z njega beremo informacije. Zato se je najprej treba vprašati, katera sredstva sploh lahko uporabimo.
Na to vprašanje je fizikom v precejšnji meri že uspelo odgovoriti. Trenutno najbolj obetavne tehnologije [5], so prikazane v tabeli 1. V stolpcu **tehnologija** so navedene različne snovi, ki so sredstva računanja. Čas izvedbe ene operacije na danem sredstvu je $\mathbf{t_{elem.}}$ V času $\mathbf{T_{dekoh}}$ razpade koherentno stanje sistema. Število **M** pove, koliko operacij je mogoče izvesti, preden v sredstvu nastopi stanje dekoherence.

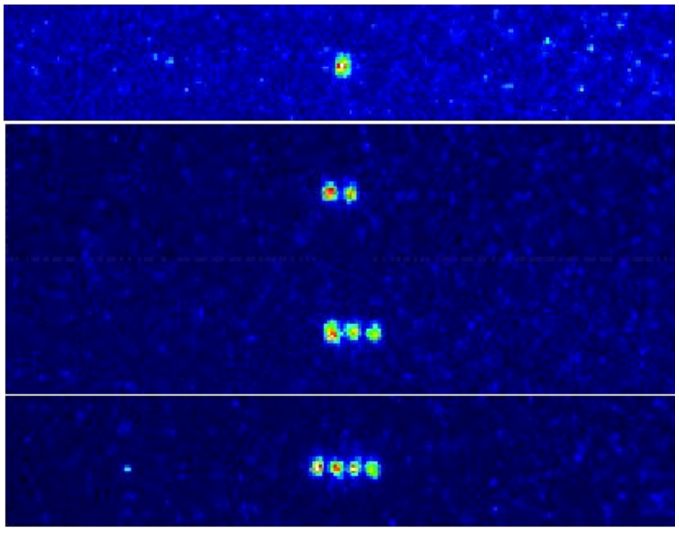
Tehnologija	$\mathbf{t_{elem}}$ **[s]**	$\mathbf{T_{dekoh}}$ **[s]**	**M**
Mösbauerjeva jedra	10^{-19}	10^{-10}	10^{9}
GaAs elektroni	10^{-13}	10^{-10}	10^{3}
Au elektroni	10^{-14}	10^{-8}	10^{6}
Ujeti ioni	10^{-14}	10^{-1}	10^{13}
Optične jame	10^{-14}	10^{-5}	10^{9}
Elektronski spin	10^{-7}	10^{-3}	10^{4}
Elektronske kvantne pike	10^{-6}	10^{-3}	10^{3}
Jedrski spin	10^{-3}	10^{4}	10^{7}
Superprevodni »otočki«	10^{-9}	10^{-3}	10^{6}

Tabela 1. Najbolj obetavne tehnologije za delovanje kvantega računalnika.

4.1 Računanje z ujetimi ioni

Najbolj perspektivna je metoda računanja z ujetimi ioni, ker je število operacij, ki jih je mogoče izvesti na mediju pred stanjem dekoherence, največje (glej tabelo 1).
Pri tej metodi so ioni ujeti v primerno oblikovanih molekulskih sitih. Ujamemo jih lahko z električnim in/ali magnetnim poljem, včasih pa se ujamejo že zaradi samih lastnosti sit oz. pasti. S primernimi pulzi laserskih žarkov in z zelo natančno fokusiranim žarkom spreminjamo stanje ionov v teh pomnilnih delovnih celicah. Z dovedeno energijo spremenimo aktivnost iona, ki se zaradi večje kinetične energije giblje v večjem območju prostora. Zato se gostota verjetnosti, da ga najdemo v pasti zmanjša.To stanje ustreza logičnemu stanju 0.

a.)
b.)
c.)
d.)

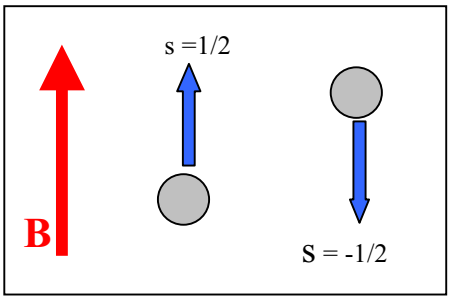


Slika 1: Meritev stanja sistema ionskih pasti v laboratoriju Los Alamos[6]: Stanje a je 0010; stanje b 0110; stanje c 0111 in stanje d 1111.

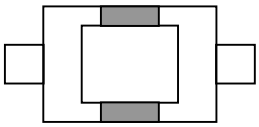
Na sliki 1 je prikazan primer štirih pasti, ki so v različnih logičnih konfiguracijah. Četrto stanje je na primer stanje 1111. Svetle točke so kalcijevi ioni v pasti. Za pasti se največkrat uporabljajo posebne polimerne snovi, ki se dajo dobro kontrolirati tako po obliki kot tudi po lokalnem naboju.

4.2 Računanje z elektronskim spinom

Tudi elektronski spin lahko uporabimo kot sredstvo računanja. Pri tem moramo paziti, da uporabljamo atome, ki imajo spinsko nevtralna jedra. Ker ima elektron lahko le natanko določen spin (±1/2), imamo podlago za binarni sistem zapisa informacij. Na primer, lahko se dogovorimo, da: s = +1/2 ustreza stanju |1> in s = - 1/2 ustreza |0>.
Spin elektronov spreminjamo z zunanjim magnetnim poljem, saj je smer spina elektrona določena z smerjo efektivnega magnetnega polja elektrona (glej sliko 2). Pri večjem številu atomov skupno stanje zapišemo kot vsoto posameznih stanj.
Dobimo stanja, ki niso čista |1> ali |0>, ker ni nujno, da posamezne spine merimo natanko pod pravim kotom glede na os rotacije. Rečemo torej lahko, da spin zavzame vsa stanja med –1/2 in +1/2.
Merilniki pri računanju z elektronskim spinom so »Superconducting Quantum Interference Device « naprave (SQUID). To so naprave sestavljene iz zaporedja posameznih SQIUD-ov (glej sliko 3). SQIUD je troslojni element sestavljen iz dveh superprevodnih in ene navadne plasti snovi. Navaden material v sredini je navadno izolator, ki je kot potencialna pregrada med obema valovanjema v superprevodnem materialu. V superprevodnem materialu so elektroni združeni v pare imenovane *Cooperjevi pari*. V primerih, ko se pretok skozi zanko spremeni, lahko *Cooperjevi pari* tunelirajo skozi izolatorsko pregrado.
Ena posebnih značilnosti tega elementa je zmožnost meriti večkratnik magnetnega pretoka $h/2e_0$. Ta količina pa je enaka Bohrovemu magnetonu ϕ_m . Če lahko izmerimo velikost ϕ_m, pa lahko izmerimo količine, ki so tudi 100-krat večje.
Metoda s SQUID-i in elektronskim spinom je zelo obetajoča, vendar pa ima tudi veliko pomanjkljivost: vsako zunanje magnetno polje lahko zmoti normalno delovanje registra in uniči informacijsko stanje.



Slika 2: Dogovor o določitvi logičnega stanja elektronskega spina.



Slika 3: SQUID. Osenčen del je izolator. Neosenčen del pa je superprevodni material.

4.3 Računanje z jedrskimi spini

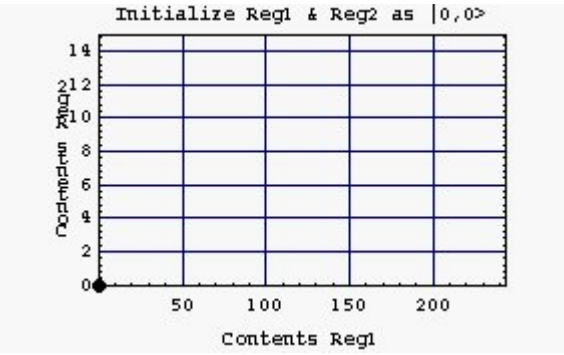
Če kot sredstvo uporabimo elektronski spin, mora biti jedro magnetno nevtralno. Če pa imajo jedra končen magnetni moment, ga, podobno kot prej elektronski spin, uporabimo za zapis digitalnih informacij.
Le način, kako vplivamo na jedrski spin je drugačen od metode, s katero spreminjamo spin elektrona. Uporabljamo namreč jedrsko magnetno resonanco (NMR). Osnova NMR je, da stanje jedrskega spina spremenimo z elektromagnetnim pulzom. Spremembi sledimo z NMR spektrometrom. Merilna sonda spektrometra je tuljavica, ki je ovita okoli vzorca. Sprememba magnetnega pretoka v tuljavici pa inducira napetost, ki jo merimo.

5. Shorov faktorizacijski algoritem

Eno največjih odkritij v razvoju primerne računalniške logike za kvantne računalnike je objavil Peter W. Shor [3]. Odkril je algoritem za faktorizacijo celih števil, ki teče eksponentno hitreje od katerega koli klasičnega algoritma. Ta algoritem ima za vhodne in izhodne informacije klasične informacije, pospešitev pa nastane zaradi izkoriščanja kvantnih efektov na vmesnih stopnjah.
Prva stvar, ki nam pade na pamet, ko hočemo faktorizirati neko število N, je, da bi ga postopno delili z vsemi števili. Vendar že po krajšem premisleku postopek skrajšamo na števila, manjša od $\sqrt{N}$. Danes kvantni računalnik simuliramo na klasičnih računalnikih, vendar so preračuni veliko počasnejši, kot bi bili na realnem kvantnem računalniku.
Namesto tega pa je Shor prevedel faktorizacijo števila N na drug problem - iskanje periode določene periodične funkcije in potem na tem problemu uporabil kvantne tehnike. Ker je ta algoritem nekakšna osnova ostalih kvantnih algoritmov, ima tudi poseben pomen. Zato ga bomo podrobneje razložili na primeru faktorizacije števila 15.
Sam proces poteka v korakih in zanje tudi ustrezno pripravi potrebne instrumente. Kvantni računalnik opremimo z dvema registroma, X in Y, in njune izhodiščne vrednosti postavimo na logične vrednosti 0 (*Booleova ničla*). Prvi register (X) je namenjen zapisu spremenljivke x, v drugem registru (Y) pa hranimo vrednosti funkcije $\Psi(x)$.
Faktorizacijo izvedemo po naslednjih korakih:

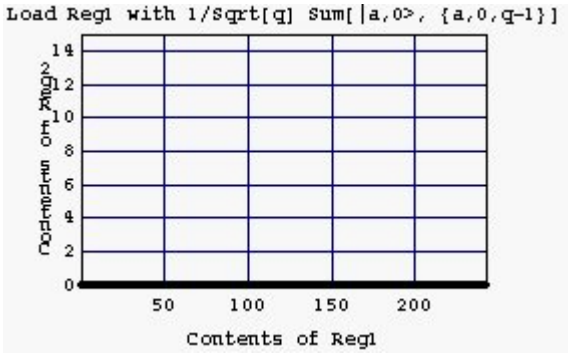
- Naključno izberemo število x, ki je tuje številu n=15. Program je v tem primeru izbral število x=7. Nato pa izberemo še število q, ki se nahaja v okolici n^2, q=243.

- Oba registra postavimo v izhodiščno stanje - ju spraznimo: $|x,y\rangle = |0,0\rangle$ ali $\Psi = 0$ (glej sliko 4).



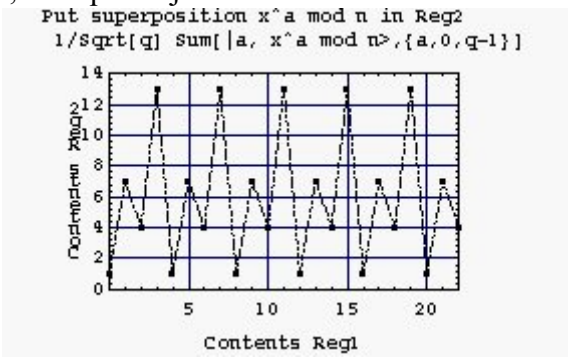
Slika 4: Postavitev ničle.

- Register *X* postavimo v superpozicijo vseh *q* Booleovih stanj, *Y* pa ostane na nič. Dobimo stanje, ki je predstavljeno kot pas vseh *x*, katerih *y* vrednost je *y=0*. Imamo torej stanje $\Psi = \frac{1}{\sqrt{q}} \sum_x |x,0\rangle$, ki je prikazano na sliki 5.



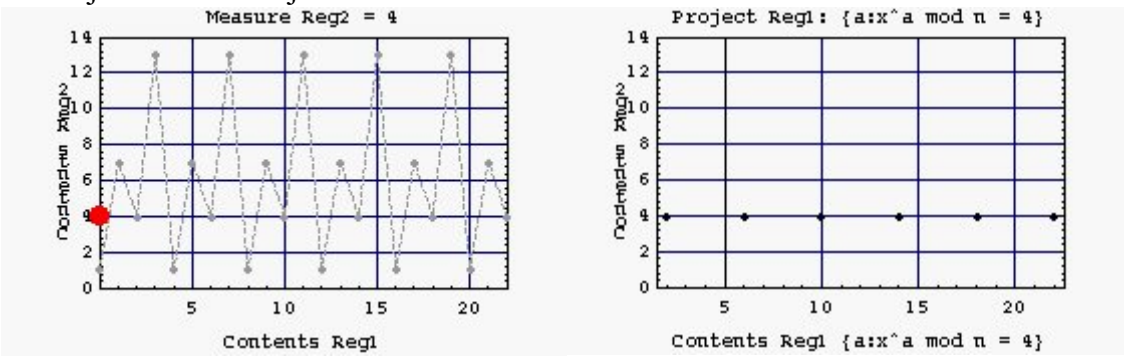
Slika 5: Inicializacija

- Izračunamo ustrezne vrednosti funkcije $f = x^a \bmod n$ in jih vnesemo v register Y. Izhodno stanje je zato $\frac{1}{\sqrt{q}} \sum_x |x, f(x)\rangle$ in je prikazano na sliki 6. Vlogo spremenljivke pa prevzame *a*, da ne bi prišlo do pomote, ker uporabljamo *x* kot izbrani element..



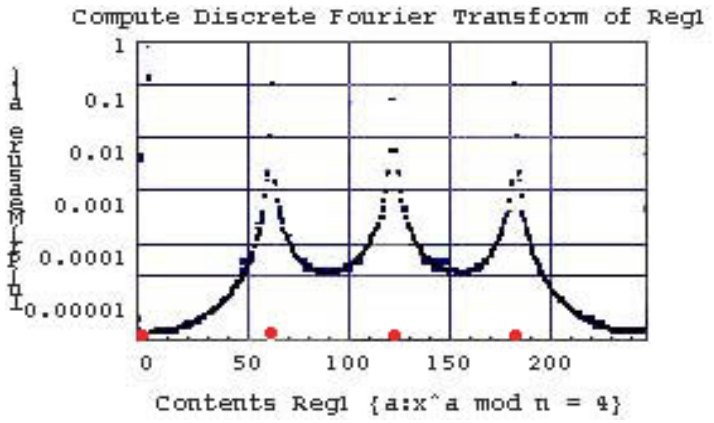
Slika 6: Periodična funkcija

- Izberemo točko *k* (y vrednost v funkciji) izračunane periodične funkcije in poiščemo rešitve enačbe $x^a \bmod n=k$. Vrednost *k* izberemo, ker ne moremo izmeriti celotnega sistema in bi ga s poskušanjem razbili. Glej sliko 7.



Slika 7: Izberemo vrednost *k* in dobimo stanje na desni.

- Dobiti moramo vrednost periode *r*, ki je v desnem grafu na sliki 7. Lahko bi jo dobili z direktnim merjenjem. Vendar pa imamo kvantni sistem, ki ga ne moremo meriti hkrati na več mestih. Z eno meritvijo namreč vplivamo na rezultat druge meritve. Zato na teh izmerjenih vrednostih opravimo Fourierovo transformacijo in dobimo stanje: $\psi = \frac{1}{q}\sum_{x,k} \exp\left[\frac{2\pi i k x}{q}\right] |k, f(x)\rangle$. Graf na sliki 8 prikazuje točke, ki jih dobimo po večjem številu ponavljanj.



Slika 8: Fourierov spekter.

- Končno dobimo natančno vrednost s tem, ko klasično izmerimo vrhove v Fourierovem spektru. S preračunom pa nato dobimo tudi periodo *r*. Eden od vrhov je namreč osnovni, ostali pa so podobno kot v glasbi, večkratniki (v akustiki večkratniki osnovne frekvence). Ne vemo pa, kateri vrh je pravi. Zato moramo izračunati osnovni vrh z okrajšavo ulomka:

  $$\frac{\mathbf{a'}}{\mathbf{q}} = \frac{\mathbf{ë}}{\mathbf{r}}$$

  kjer je a' izbrano število Fourierovega spektra : $a' = \{0, 61, 121, 180, 240\}$ (glej sliko 8)

  q je število stanjanj registra : $q = 243$

  ë ≈ celo število

- Izvedemo še dva enostavna računa:
  $D(x^{r/2}-1, n)$ in $D(x^{r/2}+1, n)$. Funkcija D tukaj pomeni največji skupni delitelj. V našem primeru, ko smo faktorizirali število 15, smo imeli: x=7 (naključno izbran na začetku), n=15 (faktoriziranec). Iz računa 13^a mod 15 smo dobili periodo r=4.
  Za konec ostane le še $D(7^2-1,15)=3$ in $D(7^2+1,15)=5$. Dobili smo faktorja 3 in 5.

Vendar pa se lahko zgodi tudi, da algoritem odpove, ker je del njegove zasnove tudi naključna izbira.
Vsak od omenjenih korakov pred končno meritvijo stanja je unitaren in ga lahko predstvimo z unitarnimi transformacijami. Vsak korak pa lahko ekonomično izvedemo preko eno- ali dvo-qubitnih kvantnih operacij.

6. Problem dekoherence in napak

V klasičnih računalnikih so informacije predstavljene kot digitalno zaporedje vrednosti električne napetosti. Pri tem vemo, da se napetost zaradi upornosti sistema vodnikov nekoliko manjša. Zato včasih napetost pade celo toliko, da neka logična vrata več ne »vedo«, kaj signal predstavlja (0 ali 1). V tem primeru se statistično verjetno lahko zgodi, da logična vrata beležijo napačno vrednost. V začetku razvoja klasičnih računalnikov je bil to še dokaj velik problem. Vendar pa so kmalu našli algoritme, s katerimi so te napake odpravili ali se jim izognili. Tako imamo danes zelo malo težav s tem in nikoli ne dobimo primera *2+2=5*.
Večje število napak pa se danes pojavlja pri hranjenju in prenosu podatkov, vendar so tudi te zelo redke. Zaradi velikega števila pisanja in brisanja na pomnilne elemente le-ti izgubijo svoje dobre lastnosti ali se pokvarijo in se pri branju pojavijo napačne informacije. Ob tem pa se lahko pojavijo še napake čisto slučajnega izvora (npr. zaradi indukcije in influence se lahko medsebojno motijo). Danes informacije večinoma hranimo na medijih, ki izkoriščajo magnetne lastnosti snovi. Zaradi večkratnega pisanja in brisanja se pomnilni elementi segrevajo in lahko izgubijo pomnilne lastnosti. Pri tem niso redki primeri, ko bralno-pisalna glava mehansko poškoduje površino medija.
Tudi v kvantnem računalniku imamo vse te izvore napak. Poleg tega pa se pojavi še nov izvor napak. Kot vemo v kvantnih računalnikih uporabljamo za računanje zelo občutljive kvantne sisteme (kristal, tekočina, ioni,…). Pri tem je običajno zelo pomembna temperatura. Zaradi zvečanja termične energije se poruši kvazistabilno stanje sistema.
V kristalu zaradi povečanja termične energije atomi začnejo nihati okoli ravnovesne lege. S tem onemogočijo natančno meritev stanja oz. uničijo informacijo, ki smo jo pred tem shranili v kristal. V drugem mediju, npr. kapljici tekočine, lahko zvečana termična energija povzroči nastanek mikrotokov. Čeprav tu računamo na jedrskem spinu, pa je to zelo težko narediti, če moramo molekule slediti in jih dobesedno loviti. Naslednji negativen vpliv so tresljaji iz okolice. Zato je treba računalniški sistem tudi mehansko izolirati od okolice, vendar to več ne predstavlja tako velikih težav.
Vse te različne oblike motenj imenujemo s skupnim imenom **dekoherenca**. Zato moramo za uspešno računanje kvantni sistem dovolj dolgo vzdrževati v koherentnem, to je kvazistacionarnem stanju. Kako dolgo moramo vzdrževati koherentno stanje, je odvisno od medija v sistemu. Za oceno časa glej tabelo 1. Celoten proces dekoherence razumemo lažje, če vzamemo statistično povprečje vseh elementov in opišemo pojav z realno funkcijo ρ_{ij}. Funkcija ρ_{ij} opisuje stanja obeh registrov (*X* in *Y*) in jo lahko v tipičnem primeru, ko ima sistem **S** delcev in je z okolico v termičnem ravnovesju, zapišemo:

$$\rho_{ij}(t) = \rho_{ij}(0) \cdot e^{-S\frac{t}{\tau_{dekoh}}} \quad , \tag{4}$$

kjer τ_{dekoh} opisuje vezavo enega qubita na okolico. Močneje kot je delec povezan z okolico, krajši je čas dekoherence τ_{dekoh} - sistem je kratkoživ. Zato nam ostane manj časa, da lahko opravimo operacije na mediju.

7. Zaključek

Področje kvantnega računalništva se zelo hitro širi in pri tem že prehaja iz teoretičnih osnov v eksperimentalno fazo. Osnovni eksperimenti in primitivni računalniki že potrjujejo predvidevanja, ki so jih postavili teoretiki. Ne moremo pa še reči, ali bo kvantni računalnik sploh kdaj deloval kot celota, saj bo pred tem treba premagati še veliko tehničnih težav.
Vendar smo se tudi v preteklosti že srečali s podobnimi težavami, ki smo jih uspešno rešili. Zakaj jih ne bi tudi tokrat? Glede na dosedanji razvoj je prihodnost zelo obetavna.
Verjetno bomo lahko že okoli leta 2020 delali s prvimi kompleksnimi kvantnimi računalniki.

Literatura

1. Lov K. Grover: »Quantum computing«, The sciences, **39**, 24-30 (1999).
2. Steffen J. Glaser: »Realization of a 5-bit NMR Quantum Computer Using a New Molecular Architecture«, Technische Universität Műnchen,(1999): {http://ociialf.org.chemie.tu-muenchen.de/glaser/qcomp.html}.
3. Peter W. Shor: »Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer«, SIAM J. Computing, 26, 1484-1509 (1997).
4. Charles H. Bennet: »Quantum Information and Computation«, Physics today, **48**, 24-30 (1995).
5. Seth Lloyd: »Quantum-Mechanical Computers«, Scientific American, **273**, 44-50 (1995).
6. Richard J. Hughes: »Quantum Computation«, povzetek iz "Feynman and Computation ", A. J. G. Hey (ed), Perseus, Reading, (1999): http://p23.lanl.gov/Quantum/papers.html .
7. Adriano Barenco: »Quantum Physics and Computation«, Clarendon Laboratory, University of Oxford : {http://www.openqubit.org/top_papers.shtml} .
8. Christian Paquin: »Computing in the quantum world«, Universite de Montreal {http://www.iro.umontreal.ca/~paquin/Qu/quantum.html}.
9. Neil Gershenfeld in Isaac L.Chuang: »Quantum Computing with Molecules«, Scientific American, **279**: {http://www.sciam.com/1998/0698issue/0698gershenfeld.html} .
10. Arno Bohm, »Quantum Mechanics-Foundations and Aplications«, (Springer Verlag, Köln, 1993).
11. R. J. Hughes: »The Los Alamos Trapped Ion Quantum Computer Experiment« {http://lib-www.lanl.gov/la-pubs/00412906.pdf} (vir nekaterih slik).
12. Richard J. Hughes: »Decoherence Bounds on Quantum Computation with Trapped Ions«, Physical Review Letters, **77,** (1996).