Fakultata za matematiko in fiziko

Univerza v Ljubljani

Kvantna logična vrata

Seminar 4. letnika 2008/09

Andrej Petek

Mentor: dr. Anton Ramšak

Ljubljana, December 2008

Povzetek

Razvoj kvantnih računalnikov se je šele začel, vendar pa je matematični koncept računanja s kvantnimi računalniki že zelo razvit. Osnovne operacije kvantnega računanja predstavljajo kvantna logična vrta, oz. kar kvantna vrata. Seminar se prične s predstavitvijo nekaterih klasičnih logičnih vrat in kvantnega bita, kot pojasnlo glavnih razlik med klasičnimi in kvantnimi računalniki. Nato so predstavljena nekatera pomembnejša kvantna vrata in kako se iz njih sestavi kvantna vezja. Na koncu so predstavljeni problemi pri izdelavi kvantnih računalnikov/vrat in nekatere možne rešitve.

Kazalo

Uvod

Računalništvo je mlada znanstvena veda, začela se je leta 1936, ko je angleški matematik Alan Turing objavil svoj članek, v katerem je predstavil teoretični model računanja s strojem, t. i. Turingovim strojem. Turing je pokazal, da obstaja univerzalni Turingov stroj, ki je sposben simulirati vse ostale Turingove stroje, t. j. opraviti njihove računske operacije. Kmalu za tem so začeli izdelovati računalnike iz elektronskih komponent, preboj pa se je zgodil leta 1947 z izumom tranzistorja. Moč računalnikov od takrat narašča izredno hitro, kar je znano kot Mooreov zakon, ki pravi, da se moč računalnikov podvoji na približno vsaki dve leti. Moč računalnikov se lahko naprimer meri s številom tranzistorjev na prostorninsko enoto vezja. Vendar ima manjašanje elektronskih komponent svoje omejitve, ne le zaradi tehnične zahtevnosti miniaturizacije, ampak ker se na majhnih skalah začnejo pojavljati kvantni efekti. Tako se pojavi potreba po računalnikih, ki delujejo na principih kvantne mehanike: kvantnih računalnikih [1, 2, 3].

Klasična logična vrata

Računanje na ravni klasičnega računalnika poteka po pravilih Booleove algebre, ki pozna le dve diskretni vrednosti: logično 0 in logično 1. Najamanjša enota informacije, ki zavzame eno izmed teh dveh vrednosti, se imenuje bit. V računalniku se to izraža kot 2 pasova dovoljenih električnih napetosti. Pomemben je matematični dokaz, ki pravi, da lahko katerokoli n-bitno Booleanovo funkcijo f(b1, b2, …, bn) izrazimo s kombinacijo operacij NOT, AND ter OR (NE, IN, ALI). Te tri operacije tako predstavljajo univerzalni set logičnih operacij [1]. Elektronska vezja, ki opravljajo logične operacije imenujemo logična vrata.

Vrata NOT imajo poleg izhoda le en vhod, na izhodu pa se pojavi ravno obratna vrednost vhoda, torej pri vrednosti vhodnega bit 0 je rezultat operacije izhodni bit 1 in obratno. Vrata AND in OR imata dva vhoda. Na izhodu AND vrat se pojavi vrednost 1, če sta oba vhodna bita enaka 1, sicer 0, izhod vrat OR pa je enak 1, če je vsaj eden oh vhodnih bitov enak 1. Delovanje logičnih vrat lahko bolj pregledno predstavimo s tabelami [1]:

a_1	a_2	a_1 AND a_2
0	0	0
0	1	0
1	0	0
1	1	1

a_1	a_2	a_1 OR a_2
0	0	0
0	1	1
1	0	1
1	1	1

a_1	NOT a_1
0	1
1	0

Univerzalni set vrat pa lahko še naperj zreduciramo na ena sama vrata, vrata NAND. Vrata NAND vrnejo vrednost 0, če sta oba vhodna bita enaka 1, sicer pa 1, torej kot da bi najprej uporabili vrata AND, nato pa še NOT.

a_1	a_2	a_1 NAND a_2
0	0	1
0	1	1
1	0	1
1	1	0

Preprosto je pokazati, da lahko z NAND vrati nadomestimo vsa tri prej našteta vrata (a in b sta oznaki za vhodna bita):

a OR b = (a NAND a) NAND (b NAND b)

a AND b = (a NAND b) NAND (a NAND b)

NOT a = a NAND a [1, 4].

Pomembna lastnost logičnih operacij/vrat je reverzibilnost, t. j. ali lahko na podlagi izhodnih bitov izvemo kakšni so bili vhodni. Izmed prejšnjih vrat so reverzibilna le NOT vrata, ki so same sebi inverz. Reverzibilnega računanja ni možno izvesti le z dvobitnimi vrati, je pa to možno z univerzalnimi trobitnimi vrati, celo z enimi samimi, ki jih je predstavil Toffoli leta 1981 [1, 4]. Toffolijeva vrata oz. Controlled-Controlled-NOT (CC-NOT) vrata predstavlja spodnja tabela [1]:

T_3 = CC-NOT	$\langle 000 \rangle$	...					$\langle 110 \rangle$	$\langle 111 \rangle$
$\langle 000 \rangle$	1	0	0	0	0	0	0	0
$\langle 001 \rangle$	0	1	0	0	0	0	0	0
$\langle 010 \rangle$	0	0	1	0	0	0	0	0
$\langle 011 \rangle$	0	0	0	1	0	0	0	0
$\langle 100 \rangle$	0	0	0	0	1	0	0	0
$\langle 101 \rangle$	0	0	0	0	0	1	0	0
$\langle 110 \rangle$	0	0	0	0	0	0	0	1
$\langle 111 \rangle$	0	0	0	0	0	0	1	0

Delujejo tako, da se na tretjem (ciljnem) bitu izvede operacija NOT, če sta tako prvi kontrolni kot drugi kontrolni bit enaka 1, sicer so vse izhodne vrednosti enake vhodnim.

Kvantni bit

Klasični bit lahko zavzame vrednost 0 ali 1, realizira pa se kot električna napetost v vezju. Realizacija kvantnih računalnikov še ni znana, enoto informacije pa naj bi predstavljal delec ali kakšen drug dvonivojski kvantni sistem, imenovan kvantni bit (angleško quantum bit), oz. qbit. Namesto vrednosti 0 in 1 nastopata v Diracovi notaciji predstavljeni vrednosti oz. osnovnih stanji $|0\rangle$ in $|1\rangle$, ki opisujeta smer spina ali kakšno drugo kvantno lastnost delca $|\Psi\rangle$. $|\ \rangle$ imenujemo stanje ali ket. Kot matematični objekt pa predstavlja vektor v Hilbertovem prostoru. $|0\rangle$ in $|1\rangle$ tvorita ortonormirano bazo za 1 qbit v ustreznem Hilbertovem prostoru, možno pa si je izbrati tudi kakšno drugo bazo.

Lastnost, ki loči qbit od klasičnega bita, je da lahko qbit poleg vrednosti $|0\rangle$ in $|1\rangle$ predstavlja poljubno linearno kombinacijo (t. i. superpozicijo) osnovnih stanj

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

kjer sta α in β kompleksna koeficienta, imenovana amplitudi [1, 2, 5, 6]. Kvadrata njunih absolutnih vrednosti predstavljata verjetnost, da bo qbit pri meritvi zavzel bodisi vrednost $|1\rangle$ (z verjetnostjo $|\alpha|^2$) bodisi vrednost $|0\rangle$ (z verjetnostjo $|\beta|^2$). Pri tem velja

$$|\alpha|^2 + |\beta|^2 = 1,$$

kar pomeni, da bomo pri meritivi gotovo dobili eno izmed stanj $|0\rangle$ ali $|1\rangle$. Ta pogoj imenujemo normalizacija. Potrebno je še poudariti, da je meritev neobrnljiv (ireverzibilen) proces.

Kadar obravnavamo naenkrat več (n) qbitov raste dimenzija Hilbertovega prostora kot 2^n. Pri dveh qbitih nastopajo 4 splošne amplitude, pri treh qbitih jih je že 8 itd., pri npr. n = 500 pa že več kot je trenutna ocena števila atomov v vesolju.

Poglejmo si splošen primer z dvema qbitoma [2]:

$$|\Psi\rangle = |q_1\ q_2\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle.$$

Kvadrati absolutnih vrednosti amplitud pred keti ponovno predstavljajo verjetnosti, da qbita najdemo v ustreznih stanjih, njihova vsota pa mora biti ponovno 1. Če npr. izmerimo vrednost prvega qbita bomo izmerili njegovo vrednost $|0\rangle$ z verjetnostjo $|\alpha_{00}|^2 + |\alpha_{01}|^2$, v tem primeru bo novo stanje enako

$$|\Psi'\rangle = |0\ q_2\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

Pri tem smo novo stanje renormaliziranli, tako da bo vsota kvadratov absolutnih vrednosti novih amplitud ponovno enaka 1.

Kvantna logična vrata

Realizacijo računskih operacij na qbitih predstavljajo kvantna logična vrata. Če stanje qbita $\alpha|0\rangle + \beta|1\rangle$ zapišemo kot vektor $(\alpha,\beta)^T$, lahko delovanje kvantnih logičnih vrat predstavimo v matrični obliki. V primeru enega qbita je matrika velikosti 2×2, v splošnem pa $2^n \times 2^n$ za n qbitov [2, 5].

Iz pogoja normalizacije stanj pred in po operaciji sledi, da mora biti matrika U, ki predstavlja kvantna vrata, unitarna, kar pomeni

$$U^\dagger U = UU^\dagger = I$$

oz.

$$U^\dagger = U^{-1}.$$

To pomeni, da so vse računske operacije kvantnih vrat reverzibilne, tako v matematičnem kot fizičnem smislu. Izkaže se, da je unitarnost tudi edini pogoj, torej vsaka unitarna matrika (prave velikosti) predstavlja kvantna logična vrata. Pri tem omenimo še matematično resnico, da je produkt unitarnih matrik ponovno unitarna matrika.

Klasično obstajajo le ena netrivialna enobitna vrata, namreč vrata NOT, kvantnih netrivialnih enoqbitnih vrat pa je neskončno, saj obstaja neskončno 2×2 unitarnih matrik. Poglejmo si nekaj primerov enoqbitnih kvantnih vrat:

Vse tri Paulijeve matrike predstavljajo kvantna vrata, med njimi pa so najbolj pomembna

$$\sigma_x = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

ki v primeru vhodnega bita vrednsoti $|0\rangle$ vrne $|1\rangle$ in obratno. Matrika X tako predstavlja kvantna NOT vrata. S pomočjo matrike si lahko pogledamo delovanje X vrat na supepozicijo osnovnih stanj

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}.$$

Vidimo, da v splošnem X vrata zamenjajo verjetnost, da bomo ob meritivi našli qbit v posameznem osnovnem stanju

$\alpha|0> + \beta|1> \rightarrow \beta|0> + \alpha|1>$.

Matrika

$$\sigma_z = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

osnovnega stanja |0> ne spreminja, pri osnovnem stanju |1> pa zamenja predznak amplitude

$\alpha|0> + \beta|1> \rightarrow \alpha|0> - \beta|1>$.

Matrika

$$\sigma_y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

prav tako zamenja verjetnosti, poleg tega pa še pomnoži amplitudi z i oz. -i

$\alpha|0> + \beta|1> \rightarrow -i\beta|0> + i\alpha|1>$.

Zelo pomembna so Hadamardova vrata

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

ki se uporabljajo k kvantnih algoritmih, kvantni teleportaciji,... [2, 5] Uporabnost Hadamardovih vrat izhaja iz lastnosti, da iz osnovnih stanj ustvarjajo superpozicije

$$|0> \rightarrow \frac{|0> + |1>}{\sqrt{2}}$$

$$|1> \rightarrow \frac{|0> - |1>}{\sqrt{2}} .$$

V splošnem pa delujejo sledeče

$$\alpha|0> + \beta|1> \rightarrow \frac{\alpha+\beta}{\sqrt{2}}|0> + \frac{\alpha-\beta}{\sqrt{2}}|1> .$$

Če dvakrat zapored uporabimo Hadamardova vrata dobimo nazaj začetni qbit, saj velja

$$H^2 = I\ .$$

Pomembna so tudi vrata faznega zamika [5]

$$P = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\rho} \end{bmatrix},$$

ki spremenijo fazo amplitude drugega qbita glede na amplitudo prvega

$$P \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ e^{i\rho}\beta \end{bmatrix}\ .$$

Z vrata so poseben primer P vrat, ko je ρ = π. Omenimo še posebna pirmera S (ρ = π /2) in T (ρ = π /4) vrat

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.$$

Splošna oblika enobitnih vrat pa je

$$U(\theta, \psi, \phi) = \begin{bmatrix} \cos\theta & e^{-i\psi}\sin\theta \\ e^{i(\phi-\psi)}\sin\theta & e^{i\phi}\cos\theta \end{bmatrix}.$$

Prvi uspeh pri iskanju univerzalnosti kvantnih logičnih vrat je uspel Davidu Deutschu z matriko (prazni prostori pomenijo 0) [1]

$$D(\alpha) = \begin{bmatrix} 1 & & & & & & & \\ & 1 & & & & & & \\ & & 1 & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ & & & & & & i\cos\alpha & \sin\alpha \\ & & & & & & \sin\alpha & i\cos\alpha \end{bmatrix},$$

ki deluje na tri qbite naenkrat. Če namreč pravilno nastavimo parameter α (kot

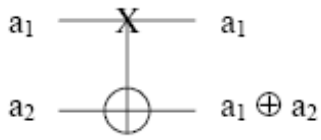
neracionalni večkratnik števila π) lahko z asimptotskim ponavljanjem teh D vrat poljubno natančno simuliramo katerakoli D vrata, z vsemi D vrati pa katerakoli kvantna vrata, ki delujejo na poljubno št. qbitov. Poseben primer Deutschevih vrat dobimo pri α = π /2, namreč Toffolijeva vrata, ki pa lahko opravijo vse operacije klasičnega računalnika.
Že čez nekaj let se je izkazalo, da za univerzalnost kvantnega (reverzibilnega) računanja zadostujejo le dvoqbitna vrata. Podobno kot Deutscheva so univerzalna tudi vrata [1]

$$\Gamma(\theta,\psi,\phi) = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \cos\theta & e^{-i\psi}\sin\theta \\ & & e^{i(\phi-\psi)}\sin\theta & e^{i\phi}\cos\theta \end{bmatrix},$$

Γ pa lahko sestavimo iz večih enoqbitnih in dvoqbitnih vrat XOR
(Exclusive OR, t. j. izključitveni ALI) oz. C-NOT (Controlled-NOT).

C-NOT vrata so ena najbolj pomembnih kvantnih vrat [1, 2, 4]. Opravijo NOT operacijo na drugem (ciljnem) qbitu, če je prvi (kontrolni) enak |1>

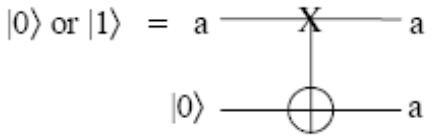
|00> → |00>
|01> → |01>
|10> → |11>
|11> → |10>.



[1]

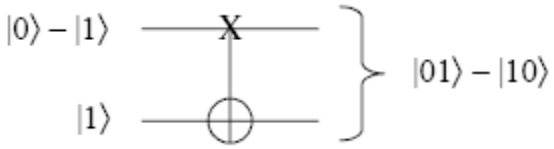
Križec (ali pa pika) predstavlja preverjanje, ali je qbit v stanju |1>, krogec pa predstavlja operacijo NOT.

Tako v primeru, da sta oba vhodna qbita v enem izmed osnovnih stanj, bo vrednost drugega izhodnega qbita ustrezala operaciji klasičnih vrat XOR (1 če je točno eden od vhodov enak 1, sicer 0).
Poseben primer uporabe C-NOT vrat je kopiranje qbita, če je prvi qbit v enem izmed osnovnih stanj in drugi qbit enak |0>. V tem primeru sta ob izhodna qbita enaka prvemu vhodnemu.



[1]

Superozicije pa pretvarja v prepeltena stanja, t. i. EPR (Einstein, Podolsky, Rosen) pare [1, 2, 4].

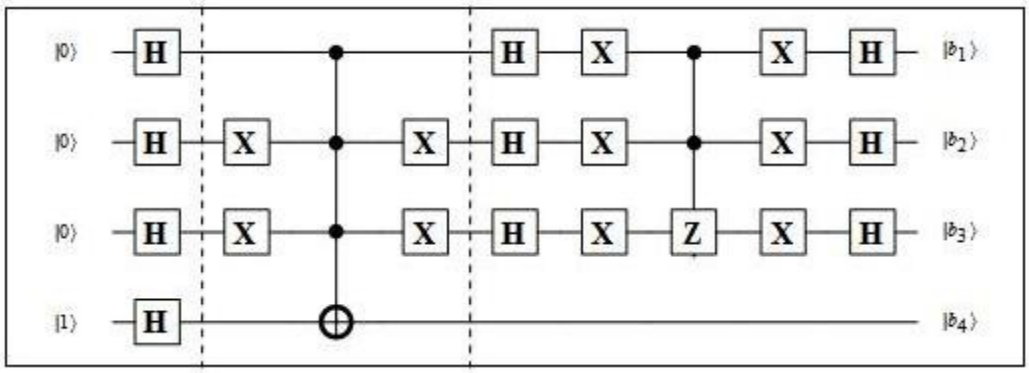


Superpozicijskih stanj se ne da kopirati, kar nam zagotavlja t. i. no cloning theorem [1, 2]. Matrična oblika C-NOT vrat je sledeča:

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Kvantna vezja

Shema kvantnih vezij se razlikuje od shem klasičnih vezij, razlika pa je v tem, da črte ne predstavljajo žic, ampak potek časa. Kvantna vrata na shemi ne prikazujejo fizičnega obstoja vezja, ampak operacijo na izbranem qbitu, torej delovanje na kvantni sistem, ki ga predstavlja. Tako v kvantnih vezjih niso možne povratne zanke. Shema se bere od leve proti desni. Če se na qbitu opravi meritev, se naprej prenese navadni bit (predstavlja informacijo o rezultatu meritve), kar se prikaže z dvojno črto [2, 5].



Primer vezja, ki izvaja Groverjev kvantni algoritem, ki poišče element v neurejeni tabeli hitreje od klasičnih algoritmov. Del vezja, omejen s prekinjenima črtama, se ponovi večkrat, odvisno od velikosti tabele [7].

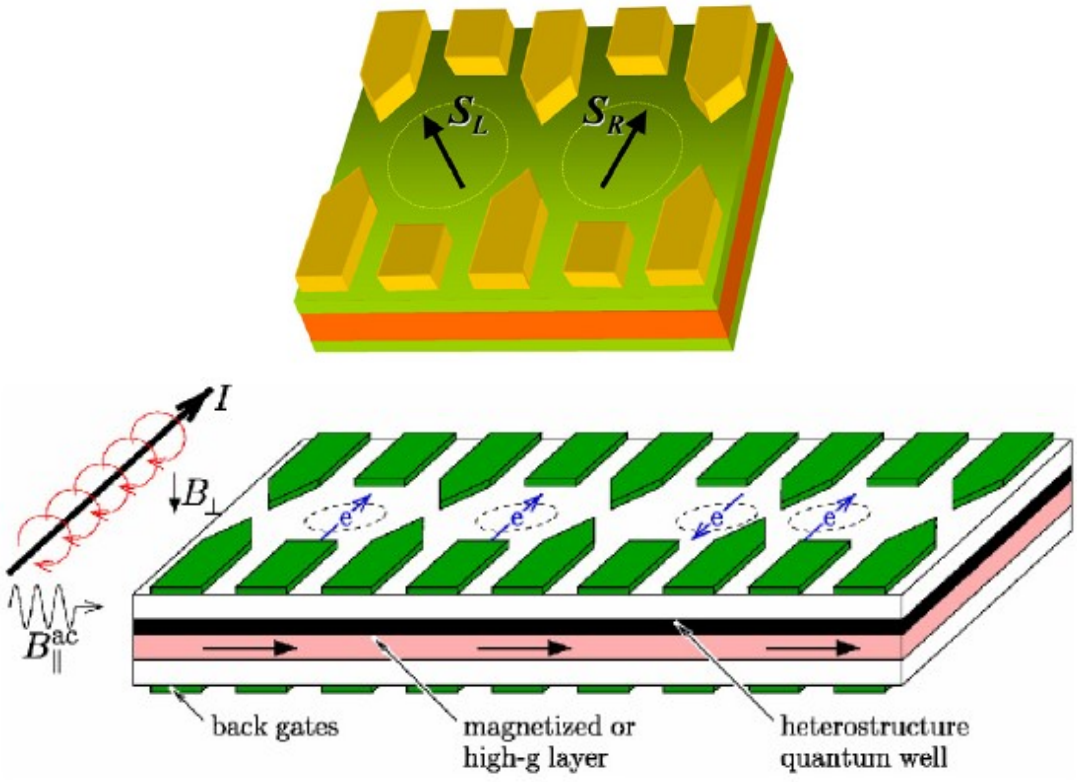
Realizacija

Izdelava kvantnega računalnika se je izkazala kot zelo težka naloga, saj je težko izpolniti vse DiVincenzove pogoje za uporabni kvantni računalnik [3]:

1. potreben je dovolj velik kvantni sistem (zadostno št. qbitov), ki se ohrani dovolj dolgo, da se izvede računanje
2. mora biti možno nastaviti stanje qbitov na |0> pred vsakim novim računanjem

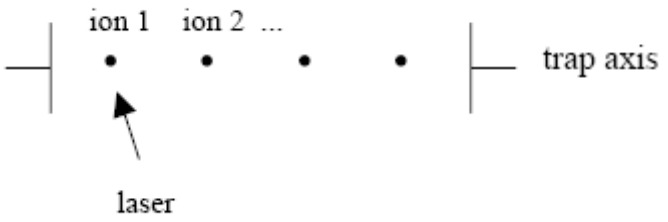
3. sistem mora biti zadostno izoliran, da vplivi okolice ne izničijo vpliva koherence qbitov
4. biti mora možno spreminjati stanja posameznih qbitov z zadovoljivo natančnostjo, kot tudi sprožiti interakcije med njimi. Čas delovanja vrat mora biti majhen v primerjavi s časom razvoja dekoherence, da bodo lahko metode popravljanja napak (error correction) učinkovite
5. možno mora biti izmeriti končna stanja qbitov po končanem računanju.

Zadostiti vsem tem zahtevam hkrati je velik izziv za fizike in inžinirje, ki trenutno preizkušajo mnoge načine izdelave kvantnega računalnika, npr. uporaba dvospinskih stanj elektronov, ujetih v atomih, molekulah ali kvantnih pikah, ionov v harmonskem potencialu, jedrske magnetne resonance, superprevodnikov, kvantne elektrodinamike itd [3, 6]. Do sedaj so uspeli sestaviti le kvantne računalnike z manj kot destimi qbiti [3, 6].



Zgornji sliki prikazujeta elektrone s pripadajočimi spini, ujetimi v kvantne pike. To je zelo obetajoča metoda, saj omogoče razširitev na večje število qbitov [3].

Ena najbolj obetajočih možnosti izdelave kvantega računalnika je z ioni, ujetimi v enodimenzionalni harmonski potencial (trapped ion quantum computer), kar sta leta 1995 predlagala Cirac in Zoller [8]. Informacije o qbitih so shranjene v spinskih stanjih ujetih inov, z njimi pa se manipulira z laserskimi sunki, s katerimi lahko hkrati povzročijo spremembo spina in vibracijska vzbujanja. Računanje se opravi preko kvantiziranega gibanja ionov, ki so med seboj sklopljeni prek Coulombove električne sile [1, 6, 9]. S tako inosko pastjo so uspeli izvesti prva C-NOT vrata [3].



[1]

Kvantni bit naj bi ob meritvi zavzel vrednost bodisi |0> , bodisi |1>, kar se izraža kot stanje sistema, npr. osovno in prvo vzbujeno stanje delca. Vendar pa se lahko delec znajde tudi v kakšnem višjem vzbujenem stanju, ali pa pride do neželenega prehoda iz osnovnega v prvo vzbujeno stanje. Kot rešitev tega problema so razvili metode popravljanja napak [2, 4, 5] (error correction), vendar pa do njih ne sme priti prepogosto. Verjetnost za prehod je odvisna od temperature delca in razlike energij med stanjema, slednja pa je odvisna od velikosti sistema. Na nanometerski skali verjetnost za prehod pri sobni temperaturi ni zanemarljiva. To predstavlja še dodaten problem pri izgradnji kvantnih računalnikov.

Zaključek

Različni možni energijski nivoji delcev pa predstavljajo tudi priložnost. Namesto qbitov z dvema možnima stanjema predstavljajo kvantne bite z d možnimi vrednostmi – qdite. Prednost takega pristopa je, da je potrebnih manj delcev, npr. ionov v pasti harmonskega potenciala. Tudi pri univerzalnosti računanja s qditi zadostujejo dvoqditna vrata [1].

Prihodnost realizacije kvantnih računalnikov je še zelo nejasna, potrebnih bo še veliko poskusov in raziskav, preden bodo izdelani prvi uporabni kvantni računalniki.

Literatura

[1] Ashok Muthukrishnan, Rochester Center for Quantum Information (RCQI): Classical and Quantum Logic Gates: An Introduction to Quantum computing (Quantum Information Seminar, 1999)

[2] Michael A. Nielsen, Isaac L. Chuang: Quantum computation and Quantum Information, Cabridge University Press, 2000

[3] Veronica Cerletti, W A Coish, Oliver Gywat, Daniel Loss: Recepies for spin-based quantum computing, Nanotechnology **16** (2005) R27–R49

[4] David P. DiVincenzo: Quantum Gates and Circuits, IBM Research Division, Thomas J. Watson Research Center, Yorktown Heights, NY 10598 USA

[5] David McMahon: Quantum Computing Explained, John Wiley & Sons, Inc.

[6] www.wikipedia.org , December 2008

[7] http://demonstrations.wolfram.com/QuantumCircuitImplementingGroversSearchAlgorithm/, December 2008

[8] Cirac J. I. , Zoller P. Physical Review Letters 74 4091 (1995)

[9] Andrew M. Childs, Isaac L. Chuang: Universal quantum computation with two-level trapped ions, Physical Review A, Volume 63, December 2000