Kvantna računala

Esad Jakupović

Za kvantna računala govorilo se da su „sveti gral računalstva“ jer će čudesno zadovoljiti sve naše potrebe za računalima – što je unatoč prvom „komercijalno dobavljivom stroju“ još daleko od stvarne upotrebe

Posljednjih godina mnogo se pisalo o „prvom komercijalno dostupnom kvantnom računalu“ Orion tvrtke D-Wave Systems iz grada Burnabyja u Kanadi. Mnogi su ga spominjali kao graničnik koji će dovesti do razvoja pravih kvantnih računala. Unatoč takvom publicitetu stručnjaci tvrtke D-Wave na njemu zasad mogu rješavati samo sudoku i slične zagonetke, što znatno brže može obaviti već i najslabije računalo na našem stolu.

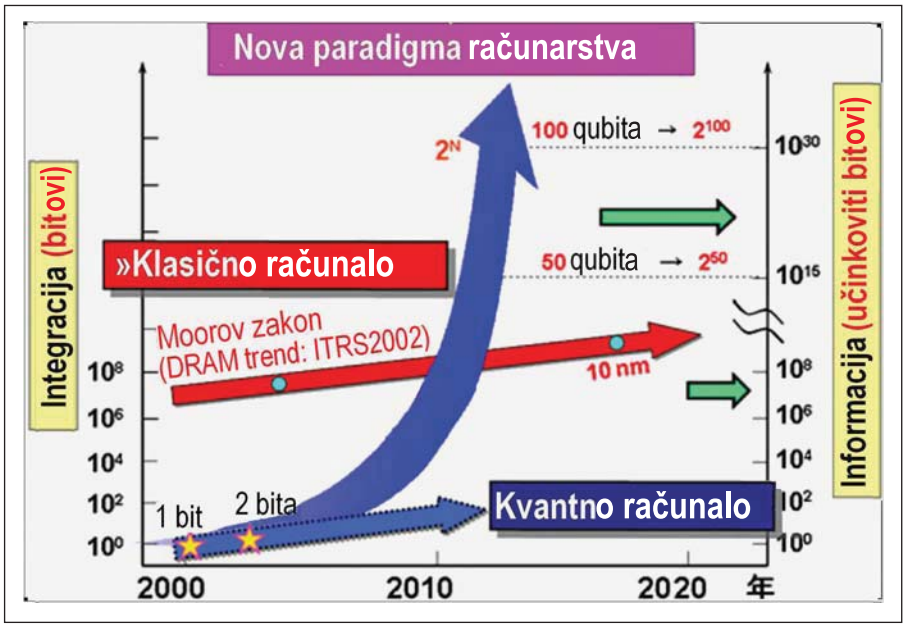
Protuslovna mišljenja

Kvantna računala prvi su put teoretski spomenuta osamdesetih godina prošlog stoljeća. U osnovi njihova djelovanja također su jedinice (1) i nule (0), kao kod običnih računala, ali ih u ovom slučaju predstavljaju elektroni koji preskaču između normalnoga (O) i pobuđenoga (1) energetskog stanja. Svaki od tih kvantnih bitova (q-bitova ili qubitova) zapravo može „visjeti u nekakvom zaboravljenom kraju“ te se istodobno ponašati kao 1 i kao 0. Zahvaljujući tom svojstvu qubitovi mogu istodobno iskušati sve mogućnosti i tako riješiti čak i krajnje kompleksne probleme, poput izvođenja simulacija kvantnih stanja koja postoje u prirodi. Upotrebu više qubitova već su prije pokušavale tvrtke kao što su IBM i NEC, ali ne s velikim uspjehom jer nisu mogle upotrijebiti više od tek nekoliko qubitova. U tvrtki D-Wave problem su riješili upotrebom rijetke kovine, niobija, ohlađene na jedva pettisućiti dio stupnja iznad apsolutne nule.

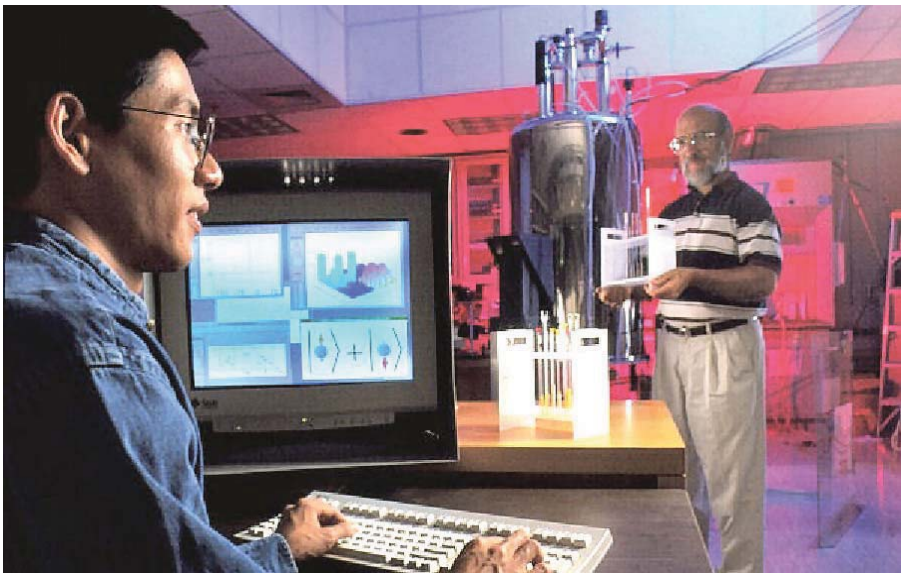
Rješenje tvrtke D-Wave neki danas hvale, drugi se na njegov račun šale, a treći samo sumnjaju da će dovesti do stvarnih procesora s više od tisuću qubitova. Najskeptičniji uopće ne vjeruju da će upotrebljiva kvantna računala ikada biti izgrađena. Među znanstvenicima koji su rješenje tvrtke D-Wave prihvatili optimistično, također je inženjer mehanike na MIT-u Seth Lloyd, koji kaže da je Orion „konkretno i potencijalno solidno dostignuće“. Neki su skeptičniji, poput fizičara Johna Martinsa s Kalifornijskog sveučilišta u Santa Barbari, koji naglašava da je „kvantno stanje u sustavu tvrtke D-Wave sasvim minimalno“ (qubitovi, naime, moraju djelovati u jedinstvenom zajedničkom kvantnom stanju, a postizanje skladnosti je problematično). Osnivač tvrtke D-Wave Geordie Rose obećava: „Izgradit ćemo kvantna računala i vidjeti ponašaju li se kako treba.“

Prva „kvantna“ zarada?

Orion upotrebljava procesor od 16 bitova, sastavljen od 16 malih prstena, po jednim za svaki qubit, koji su ohlađeni gotovo do apsolutne nule da bi elektroni mogli protjecati bez otpora. Osnivač tvrtke Geordie Rose najavljivao je povećanje broja qubitova sa 16 na 128, a poslije čak na 1 000 i više. Obećao je također skori početak komercijalne upotrebe i iznajmljivanja kvantnog računala tvrtke D-Wave. U prosincu 2008. objavljena je informacija o izgradnji 128-bitnog procesora WIRA i malo poslije također o izgradnji 128-bitnoga kvantnog računala. Objavljene



Kratka povijest računala: *razvoj od zupčanika, preko releja i ventila do integriranih veza omogućio je izgradnju čipova velikih samo dio mikrometra te doveo do logičkih vrata veličine pregršt atoma*



Prva upotreba kvantnog računala: *dr. Isaac Chuang iz IBM-a i Constantino Yannoni iz MIT-a za kvantne izračune upotrijebili su interakcije spinova jezgra unutar posebno oblikovane molekule*

su informacije o izgradnji golemoga supervodičkog „računala“ nazvanog Dragon, koje je stajalo 70 milijuna dolara. Nakon toga nije bilo nekih informacija, tako da se i ne zna je li tko prihvatio ponudu tvrtke D-Wave o upotrebi 128-bitnog računala. Ako jest, to bi bio prvi slučaj da je netko nešto zaradio s kvantnim računalom.

Orion i Dragon nisu prvi slučaj nekakva uspjeha u vezi s kvantnim računalima. Godinu dana prije toga, u ožujku 2007., fizičar David Deutsch sa Sveučilišta u Oxfordu napisao je: „Skeptici prema kvantnim računalima tvrdili su da ih nikada neće biti moguće napraviti, tvrdili su također da to neće biti praktično – i pogriješili su.“ Deutsch tvrdi da ćemo „uskoro“ dočekati istinska kvantna računala, „koja će obična obilježja kvantne mehanike upotrebljavati za izvođenje zahtjevnih proračuna milijun put brže od najmoćnijih superračunala našeg doba“. Takvi će uređaji, kaže Deutsch, „preokrenuti kriptografiju i mnogobrojna druga područja te također revolucionirati industriju računala“. Oxfordski fizičar ne obazire se previše na skeptike koji upozoravaju da istraživači unatoč „blistavim prognozama“ zasad imaju samo napuhane kvantne sustave „koji su sposobni rješavati matematičke probleme kakve djeca uglavnom rješavaju napamet“.

Kvantni bit: *žuto-crna 3D struktura predstavlja qubit, kojeg proizvodi kvantna definicija stanja 0 i 1*

Schrödingerova mačka

Deutsch je još 1985. godine nacrtao prvi plan kvantnog računala, ali je također 2005. godine vjerovao da smo od bilo kakvih upotrebljivih kvantnih strojeva daleko najmanje 20 godina. U ljeto 2005. mu je Simon Benjamin, i sam istraživač na Oxfordu, iznio svoje zamisli o „stanju roja“ koje bi moglo riješiti glavne teškoće s kojima se suočava kvantna zajednica. Riječ je o drukčijem određivanju načina na koji kvantno računalo obrađuje informaciju, pri čemu se prvo pobrine za najnepouzdanije bitove proračuna. Time se omogućuje jednostavnije povećavanje sustava radi izvođenja sve većih proračuna. Benjaminova zamisao utjecala je na Deutscha da izgradi novu viziju, u kojoj je zahvaljujući novim argumentima svojih „najmanje 20 godina“ pretvorio u „najviše 10 godina“.

Očekivane prednosti kvantnih računala pred klasičnima već dugo oduševljavaju fizičare. Tradicionalna računala predstavljaju informacije kao bitove koji imaju u određenom trenutku vrijednost 1 ili 0. Bitovi se u stvarnome svijetu prikazuju kao električni naboji ili razine napona. Kvantni bitovi, odnosno qubitovi (koje možemo izgovarati prema engleskom izvorniku „kju-bitovi“ ili prema našem „kubitovi“) postoje u superpozicijskom stanju, istodobno kao „1“ i „0“. Tek ako tko pokuša mjeriti stanje qubitova, kvantni se bit ustali u jednom stanju. To je slično kao u slučaju Schrödingerove mačke u kutiji, koja je istodobno živa i mrtva sve dok netko ne otvori kutiju. Netko je tu prednost kvantnog računala – da sadržava obje vrijednosti – opisao kao „dobivanje dvaju proračuna za cijenu jednoga“.

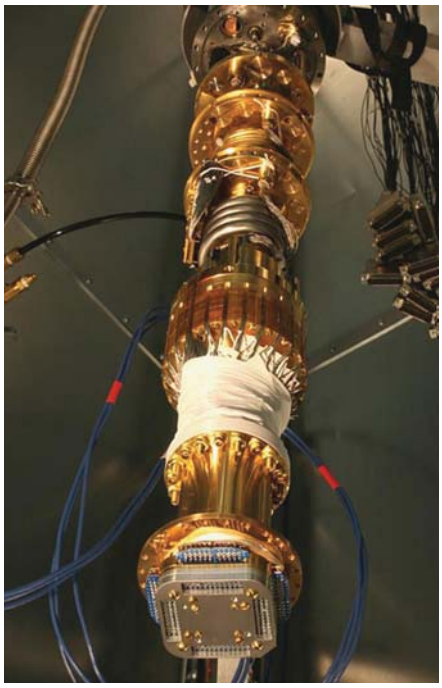
„Jednosmjerno izračunavanje“

Kvantno računalstvo među ostalim iskorištava fenomen „čvorova“, dakle povezivanja dvaju ili više qubitova, čime se povezuju i njihova svojstva. Qubitovima je moguće tako manipulirati da je jedan uvijek 0 ako je drugi 1, ili tako da su oba 1. Superpozicijom i povezivanjem kvantna računala mogu izvoditi proračune s mnogo više brojeva nego dosadašnja „klasična“ računala. Sa samo nekoliko stotina qubitova povezanih u čvorove moguće je istodobno predstaviti

Što mogu donijeti kvantna računala

Klasično računalo neke probleme ne uspijeva riješiti u razumnom roku. Kvantno računalo moglo bi ponuditi trikove kojima bismo rješavali sljedeće zadatke:

- pretraživati divovske banke podataka
- izvoditi simulacije sa subatomskim česticama
- izračunavati statistiku velikih populacija
- prepoznavati kompleksne obrasce i slike
- pripremati komplicirane sheme kodiranja kao što je RSA za potrebe sigurnih transakcija na internetu.



Kvantni proračuni, iako skromni: *kvantno računalo Orion tvrtke D-Wave*

znatno više brojeva nego što ima atoma u svemiru. Barem u teoriji, jer razvoj kvantnih računala tek počinje. U dosadašnjim modelima istraživači su među ostalim upotrebljavali energetske razine iona uhvaćenih u električnom polju, koji su tako služili kao kvantne jedinice ili nule. U drugim slučajevima qubitove su tražili u polarizaciji fotona. A u trećima su se koristili obrtanjem dijelova jezgra unutar molekule kloroforma ili obrtanjem elektrona u nanokristalima poznatima kao „kvantne točke".

Bez obzira na podrijetlo qubitova, uvijek se pojavljuje isti problem: proračun je veoma

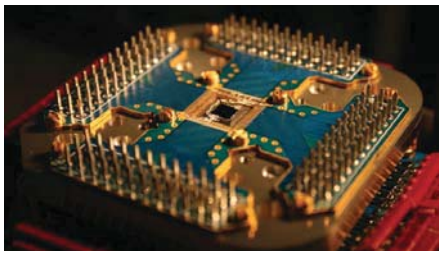
Kandidati za kvantna računala

Koji su fizički sustavi najbolji kandidati za kvantno računalo budućnosti?

IONSKE ZAMKE: Qubitovi se spremaju s pomoću različitih energetskih razina iona. Ioni prenose informacije među sobom vibracijama u elektromagnetnom polju, kojim se može upravljati u „ionskoj zamci". Istraživači uspijevaju stvoriti i povezati u čvorove istodobno po nekoliko qubitova s pomoću ionskih zamki, ali rad s tisućama iona u zamci može biti nemoguć. Neki istraživači predlažu za prijenos informacija među skupinama održavanje iona u mnogobrojnim odvijenim zamkama i pomicanje pojedinačnih iona između zamki.

KVANTNE TOČKE: Da bi spremali qubitove, istraživači upravljaju stanjem elektrona uhvaćenih u poluvodičkim nanokristalima, odnosno kvantnim točkama, manipuliranjem obrtanja (spina) elektrona ili poticanjem elektrona da napusti svoje normalno obrtanje u kristalu. Za to se koriste laserima ili usmjerivanjem električnih naboja u točke. Istraživači sada traže bolje postupke povezivanja dvaju ili više qubitova da bi ih prisilili na izvođenje proračuna i učinili ih stabilnijima. Ako u tome uspiju, bit će moguća upotreba mnogo više qubitova i također upotreba već postojećih postupaka proizvodnje poluvodiča.

POLUVODIČI: Poluvodički qubitovi utemeljeni su na kvantnim svojstvima poluvodiča materija koje na veoma niskim temperaturama nemaju električnog otpora. Izrađeni od dva poluvodiča s izolacijom između njih, takvi qubitovi mogu se kodirati s pomoću električnog naboja, smjera električnog toka i kvantnog svojstva nazvanog „faza". Time je omogućena upotreba postojećih tehnologija i kvantne se komponente mogu integrirati s običnim elektroničkim komponentama. Istraživači mogu pripremiti pojedinačne qubitove, ali ih još očekuje razvoj postupaka povezivanja velikog broja qubitova u čvorove i izvođenje jednostavnih algoritama s pomoću njih.



Prvi u novom nizu: *16-bitni kvantni čip tvrtke D-Wave, namješten na posudi za uzorke, sastavljen je od 16 malih prstena*

teško izvoditi i, također, teško je održavati čvorove „na životu". Čvorovi se obično održavaju laserskim impulsima, koji također omogućuju manipuliranje njima. Ako su qubitovi gusto pakirani, teško je komunicirati s bilo kojim od njih, a da pritom ne ometamo susjedne qubitove. Ometanje na jednoj strani može pokvariti čvorove na drugoj strani te prisiliti qubit da izabere vrijednost (0 ili 1). Istraživači zasad mogu istodobno manipulirati s deset qubitova,

S pomoću Zero Clienta do veće dostupnosti i sigurnosti

Fujitsu je predstavio novi prijenosni uređaj Zero Client, s pomoću kojeg se proširio već postojeći koncept Zero Client. Prijenosni uređaj korisnicima uporabnikom infrastrukture Zero Client omogućuje siguran pristup virtualnim računalima preko bilo kojeg računala spojenog na mrežu. Novi prijenosni uređaj Zero Client MZ900 odgovara na sve veće potrebe mobilne prirode poslova, a u usporedbi s ostalim metodama udaljenog pristupa jamči visoku razinu sigurnosti, prilagodljivosti i dostupnosti. Prijenosni uređaj Zero Client MZ900 temelji se na memorijskoj USB kartici. Programska oprema (u stvarnosti uređaj koji omogućuje čitanje) ostvaruje osigurani pristup, nakon čega se korisnik može povezati sa svojim kućištem Zero Client. Veza je moguća s bilo kojeg računala na svijetu, a osjetljivi podaci su na šifriranom dijelu uređaja dostupni tek što se korisnik poveže i identificira.

S pomoću prijenosnog uređaja nastoji se smanjiti jedno od najvećih problema zaposlenika, koji su česti u praksi - nesigurnost zaraze s virusom ili trojanskim konjem tijekom povezivanja s matičnim uređajem. S pomoću prijenosnog uređaja Zero Client korporativne mreže su osigurane od nesigurnosti te vrste, jer matični uređaj ne može uređivati veze prijenosnog Zero Clienta i programske opreme za identifikaciju. Kako prijenosni Zero Client izvodi siguran pristup programskoj opremi za izvedbu postupka prijave na zaštićenoj particiji, omogućuje i zaštitu od zlonamjerne programske opreme sa gostujućih sustava koja može ostvariti vezu i unos podataka.

Koncept prijenosnog Zero Clienta tvrtkama donosi sve prednosti virtualizacije. Pored uštede na vremenu, zaposleni uživaju u većoj prilagodljivosti i proizvodnosti, a da pri tome ne moraju sobom nositi prijenosno računalo. Prijenosni Zero Client će biti dobavljiv do kraja studenoga 2010. ■

Svemir kao kvantno računalo

U filmovima kao što je „Matrica“ i znanstveno-fantastičnim romanima kakav je „Kultura“ autora Iana Banksa osobe se kreću kroz svemir virtualne stvarnosti u kojoj je sve iluzija. Stvarnost je, zapravo, samo informacija u računalnom svijetu koja zbunjuje njihova osjetila. Fizičari, naime, već dugo pokušavaju razviti „teoriju svega“, koja bi u osnovi stvarnost – prostor, vrijeme, gravitaciju i svojstva čestica kao što su elektroni i neutrini, dakle sve – opisala na jednostavan matematički način. Fizičari zasad imaju samo niz odvojenih teorija za različite dijelove stvarnosti, poput Einsteinove teorije relativnosti. Pa i sam se Einstein uzalud trudio naći jedinstvenu teoriju svega. Najnovija „teorija svega“, koja se imenuje „gravitacija (ili teorija) kvantne petlje“, proizlazi iz Einsteinove teorije relativnosti i ideje da je sve izgrađeno kao mreža odnosa zapetljanih u klupka. Pa i čestice su, zapravo, klupka. Još je neobičnija teorija da je svemir, zapravo, samo golema mreža informacija, samo divovsko računalo. Teorija kvantne petlje obećava jer može osigurati opise prostor-vremena i čestica koji odgovaraju stvarnosti. Može li osigurati i odgovore na sve ostalo, zasad nije poznato. Možda će ponuditi odgovore i na pitanja o životu i svemiru. Možda će konačan odgovor biti da je svemir samo divovsko kvantno računalo.

***Život u „Matrici“**: teorija kvantne petlje možda će dovesti do objašnjenja da je svemir samo divovsko kvantno računalo*

što nije baš mnogo. Stanje roja može bitno poboljšati mogućnosti izračunavanja. Metodu su predložili 2001. godine istraživači Robert Raussendorf i Hans Briegel sa Sveučilišta u Münchenu. Prema njihovoj se ideji svi čvorovi podese na samom početku izračunavanja – postupak se naziva „jednosmjerno izračunavanje“.

Priprema je pola proračuna

Istraživači su na ideju došli po uzoru na optičku rešetku, u kojoj mreža lasera ulovi nenabijene elektrone u zamku na točkama presijecanja. S pomoću laserskih zraka qubitovi se mogu međusobno približavati, pri čemu je olakšano stvaranje višestrukih čvorova. U tom je slučaju znatno teže pomicanje pojedinačnih qubitova unutar niza, što ograničava upotrebu optičke rešetke u kvantnom računalstvu. U stanju roja se zato umjesto izvođenja višestrukih operacija tijekom određenog vremena na istoj skupini qubitova izvodi više proračuna na različitim skupinama (kolonama) qubitova. Na primjer, umjesto upotrebe pet operacija na istoj skupini kao kvantno računalo upotrijebi se rešetka s pet kolona sastavljenih od po četiri qubita, pri čemu svaka kolona znači jednu operaciju. Povezivanje u čvorove u nizu predstavlja vremenski redoslijed operacija, dok povezivanje u koloni prikazuje operacije među skupinama qubitova.

***Računalstvo za sva vremena:** umjetnikov simbolični prikaz kvantnog računala*

Izračunavanje u rešetki počinje mjerenjem stanja qubitova (0 ili 1) u prvoj koloni, podešavanjem sljedeće kolone i zatim mjerenja qubitova, pa tako sve do kraja, kada se dobije rezultat proračuna. Upotrebom stanja roja najteži dio problema „riješi se“ još prije nego što počne proračun, koji zatim ne traje dugo. Bilo kako bilo, mogući su također drugi postupci, koje razvijaju u Hewlett-Packardu, na Nacionalnom sveučilištu Singapura, na Sveučilištu u Beču te u još nekim ustanovama u svijetu. Pohod qubitova je počeo – mnogi vjeruju da će to biti također pohod kvantnih računala. Budući da ljudi lako izgube strpljenje kad je riječ o temi kvantnih računala, jer je teško razumiju, spomenimo da je poznati američki fizičar Richard Feynman (1918. - 1988.) jednom napisao: „Mislim da mogu sa sigurnošću tvrditi da kvantnu mehaniku ne razumije nitko.“

Lexmarkove boje za dokumente veličine A3

Lexmark predstavlja dva nova uređaja za tiskanje u boji dokumenata veličine A3. Aktualnoj ponudi laserskih pisača u boji pridružuje se i Lexmark C925de, a izbor višenamjenskih uređaja proširiti će model X925de. Nove uređaje odlikuje novo korisničko sučelje e-Task, koje donosi intuitivno upravljanje preko ekrana osjetljivog na dodir. Višenamjenski uređaj Lexmark X925de opremljen je 10,2-inčnim ekranom (26 cm), osjetljivim na dodir, na kojem korisnik može bez poteškoća pregledavati dokumente koje želi otisnuti. Tisak i kopiranje dokumenata dosiže brzine do 30 stranica u minuti, a automatsko dodavanje dokumenata omogućuje obostrano skeniranje dokumenata u boji. Pretinac pisača može prihvatiti do 100 listova papira. Kao jedini A3-pisač u svojem razredu, opremljen je s ekranom u boji osjetljivim na dodir e-Task dijagonale 10,9 cm.

www.lexmark.com
www.alterna-i.si