

KVANTNO RAČUNANJE

Igor Belič, VPVŠ, Kotnikova 8, 1000 Ljubljana

Quantum computing

ABSTRACT

Where will new directions in computer technologies go is the main question of the original paper written by Tom Thompson and published by Byte. There is a particularly interesting section describing the potentials of quantum computing that requires the vacuum system in order to operate. If the quantum computing story ever comes true it will also be the moment of great vacuum technology expansion.

POVZETEK

Originalni članek Toma Thompsona daje nekaj odgovorov na vprašanje usmeritev računalniških tehnologij v prihodnosti. Posebej zanimiv je del članka, ki opisuje možnosti kvantnega računanja. Elementi, ki izvajajo kvantno računanje, lahko delujejo le v vakuumskem okolju. Če bodo principi kvantnega računanja kdaj postali resničnost, potem bo to tudi začetek velikega vzpona vakuumskih tehnologij.

1 Uvod

Iskanje novih tehnologij, ki bi omogočile izdelavo še hitrejših in zmogljivejših računalnikov, je kot zlata mrzlica. Zelo veliko ljudi se ukvarja s tem iskanjem, vendar, kot povesod drugje, so tudi tu le redki izbrani.

Vakuumske tehnologije so v zadnjih desetletjih izrinjene na rob uporabe v široki porabi. Navzoče so posredno, ker sodobnih mikroelektronskih vezij in še česa brez vakuumskih procesiranja ne bi bilo. Povzetek članka T. Thompsona, objavljenega v reviji Byte /1/, nakazuje možnost povratka vakuumskih tehnologij v samo osrednje v široki porabi uporabljenih elektronskih komponent in to ne v tako zelo oddaljeni prihodnosti.

2 Kvantni procesorji

Kakšno je stanje na področju procesorjev, uporabljenih v sodobnih računalnikih? Ali obstajajo principi, ki bi uspešno zamenjali digitalne principe delovanja? Morda s čim, še manjšim od dosedaj najbolj miniaturiziranih integriranih vezij - s posameznimi atomi, ioni, elektroni. Skozi leta so se fiziki v laboratorijskih okoljih ukvarjali z delom na atomarnem in subatomarnem nivoju. V današnjem času poskušajo izvesti računske operacije z izkoriščanjem fizikalnih lastnosti, ki veljajo za atomarni nivo. Delo na tem področju se precej razlikuje od običajne uporaba binarne logike in principov Booleove algebre. Odkrite so nove zakonitosti, ki se jih da uporabiti za izvajanje računskih operacij. Običajna fizikalna pravila, ki veljajo tudi za najbolj miniaturizirana CMOS logična vrata (logična vrata so osnovni sestavni elementi logičnih vezij za izvajanje operacij, kot so AND, OR, negirani AND in OR itd.), tu ne veljajo več. Namesto tega veljajo za subatomarne delce pravila kvantne mehanike.

Vsak delec lahko opišemo kot delec ali kot valovanje. Kadar subatomarni delec obravnavamo kot delec (korpuskularni opis), potem ta lahko zaseda le diskretna energijska stanja, ki jim rečemo energijski kvanti. Valovni opis govori o tem istem delcu v prostorsko-časovnem smislu. Ko se val, ki predstavlja elektron,

razširi v prostoru in času, postane lokacija elektrona negotova; veljajo zakoni verjetnosti.

Slika je podobna, ko vržemo kamen v bazen, napolnjen z mirujočo vodo. V trenutku, ko se kamen dotakne vodne gladine, se začne centrično razširjati valovi proti robu bazena in se od njega odbijejo. Čez določen čas je celotna gladina bazena v valovanju. Valovna predstavitev "kamna" je porazdeljena po celotni površini bazena. Elektron je zato v valovnem smislu povesod naenkrat.

Stanje nedoločenosti (fuzzy state) se nadaljuje toliko časa, dokler elektron ne interagira z nekim drugim delcem ali s fotonom. V trenutku interakcije je izdana lokacija elektrona, ki je v točki, kjer razširjajoči se val razpade v množico lokaliziranih valov (elektron in drugi delec).

Kot primer tega dogodka si predstavljajmo majhen prostor, v katerem je zaprt elektron. Prisotnost elektrona lahko predstavimo kot val. Valovna funkcija govori tudi o verjetnosti, da se delec nahaja zunaj s stenami omejenega prostora. Pod ustreznimi pogoji elektron pobegne iz omejenega prostora. Proces imenujemo tuneliranje.

V šestdesetih in sedemdesetih letih sta Rolf Landauer in Charles H. Bennet iz centra IBM Thomas J. Watson raziskovala in odkrila osnovne fizikalne zakonitosti računanja, ki so kasneje postali temeljni principi kvantnega računanja. Bennet je pokazal, da je možno zgraditi molekularni računalnik, ki deluje na temelju Turingovega stroja.

Okoli leta 1980 je Paul Benioff iz Argonne National Laboratory ugotovil, da se računanje lahko izvaja na sistemih, ki popolnoma sledijo zakonom kvantne mehanike. David Deutsch z Univerze v Oxfordu je leta 1985 dognal, da taki sistemi lahko izvajajo celo kvantno paralelno računanje. Ko so bili sistemi kvantnega računanja še v teoretskih povojih, je že kazalo, da bodo taki računalniki precej zmogljivejši, kot so sedanji.

Leta 1993 je Seth Lloyd iz Los Alamos National Laboratory pokazal, da veliko kvantnih sistemov, vključno s preprostimi kristalom soli, lahko deluje kot kvantni računalnik. Istega leta je Peter W. Shor iz AT&T Bell Laboratory demonstriral, da kvantni računalnik lahko izvaja praktično delo hitreje kot katerikoli znani digitalni računalnik. Vsa ta odkritja so sprožila renesanso raziskav kvantnega računanja, kjer številne skupine poskušajo zgraditi prototipne elemente kvantnih računalniških sistemov.

Teoretične ideje, kako narediti osnovna kvantna "vrata", se razlikujejo glede na to, v kateri raziskovalni skupini so nastale. Kljub temu sta dve skupini naredili pomembne korake pri laboratorijskih poskusnih izvedbah. Skupina, ki deluje pod vodstvom Davida J. Winelanda v National Institute of Standards (NIST), je zgradila XOR (eXclusive OR) vrata z uporabo ionov, ujetih v pasti. Druga skupina pod vodstvom Jeffa H. Kimbleja iz Cal Techa uporablja optično kavitacijo v past ujetega atoma za izvedbo kvantnih faznih vrat (Quantum Phase Gate QPG). Izhod QPG vrat spremeni

fazni kot polarizacije vhodnega laserskega žarka. Taka logična vrata lahko izvajajo več različnih logičnih funkcij.

Konstrukcija osnovnih gradbenih elementov ni lahka naloga. Vrata NIST so izvedena v vakuumskem sistemu s štirimi elektrodami (slika 1).

Čeprav je skupina NIST zgradila logična vrata, ki izvajajo logično funkcijo, kot klasična elektronska vrata, je treba posebej poudariti, da kvantna logika ne deluje nujno tako. Kot je bilo že prej omenjeno, kvantno računanje uporablja neke vrste paralelno računanje zaradi verjetnostne narave vedenja delcev in tudi vrata NIST izkazujejo take lastnosti.

"Prostor stanj sistema kvantnega računanja je bistveno večji kot pri klasičnem digitalnem računalniku, zato ker kvantni sistem lahko realizira eksponentno mnogo stanj naenkrat," je dejal Kimble. Zaradi tega se kvantni biti imenujejo qu-biti, da jih tako razlikujemo od klasičnih bitov.

"3-bitni register shrani v enem trenutku le eno število, medtem ko 3 qu-bitni vseh osem možnih števil naenkrat, vse dokler jih ne odčitamo," pravi Chris Monroe, ki je ravno tako član skupine NIST.

Kvantni paralelizem teoretično omogoča izvajanje zahtevnih operacij precej hitreje. Faktoriranje velikih števil navadno zahteva od računalnika ogromno število operacij, ki naraščajo eksponentno z velikostjo števila, ki se faktorira. Kvantni računalnik se loti naloge tako, da izračuna potence manjših števil z različnimi potencami naenkrat.

Kvantni računalnik ne izvaja nujno digitalnega računanja. Richard Feynman predlaga, da kvantne računalnike uporabljamo za simulacijo kvantnomehanskih sistemov, torej kot analogne računalnike. To idejo uporablja Seth Lloyd, ki deluje na MIT. Želi simulirati časovni razvoj 40 delcev, ki sestavljajo snov v jedru

eksplozivno zvezde. Izvedba takih izračunov s klasičnim digitalnim računalnikom zahteva delo z matrikami reda $2^{40} \times 2^{40}$, kar dovolj natančno opiše bistvene kvantne lastnosti delcev.

Uporabiti bi morali 10^{24} digitalnih operacij za izračun rezultata. TFLOPS (Tera Floating Point Operations per Second) računalniški sistem bi porabil za to delo trilijon sekund ali 31 709 let. Z uporabo laserjev za kontrolo oziroma programiranje delovanja 40 ionov v ionski pasti bi kvantni računalnik porabil le sto kvantnih interakcij. Tak kvantni analogni računalnik bi izkoriščal kvantne lastnosti uporabljenih delcev (spin) za izračun kvantnih učinkov simulacije.

Čeprav kvantno računanje mnogo obeta, je še vedno veliko problemov in vprašanj, na katere zaenkrat še ni odgovora. Izjemen problem je, kako obdržati koherenten kvantni sistem. Kvantni računalniki morajo delovati pod dvema pogojevoma, ki sta zelo težko dosegljiva. Qu-bitovi morajo zelo močno interagirati med seboj, če želimo doseči postopek računanja. V interakciji ne sme sodelovati okolica opazovanih ionov (ohišje, elektrode). Obe zahtevi sta izredno težko dosegljivi, še posebej, če računanje poteka dlje časa. Termično nihanje okvira, ki je mehanska osnova sistema, lahko povzroči izgubo koherence sistema. Počasno in neizogibno spreminjanje delovne točke analogne opreme povzroča računске napake, ki jih digitalni računalniki ne poznajo.

Monroe priznava, da se še nihče ni resno lotil omenjenega problema. Celo navadna vrata XOR izgubijo koherenco po 10 do 20 interakcijah, verjetno zaradi nestabilnosti vzbujevalnega laserja. Bennet in ostali so raziskovali potencialne možnosti za popravljanje napak kvantnega računanja. Peter Shor je odkril obetajoč princip za popravljanje napak v kvantnem pomnilniku. Dokazal je, da uporaba devetih qu-bitov samodejno popravlja napake. Sistem je sicer zelo neefektiven, a deluje. Kaže, da bo potreben miselni preskok za rešitev omenjenega problema.

Čeprav opis in ideja sistema delujeta medlo, ne pozabimo, da je ideja kvantnega računanja še v svojih prvih korakih. Stanje je podobno kot takrat, ko so leta 1947 v Bellovih laboratorijih prvič izdelali transistor. Raziskovalci poskušajo preizkusiti nekaj desetletij staro teorijo v praksi. Vpeljava analogije klasičnih elektronskih vezij verjetno ni optimalna strategija. Kvantna fizika je bogata in neraziskano področje, kjer je razkorak med teoretičnimi dognanji in tehnološko izvedljivo rešitvijo izredno velik.

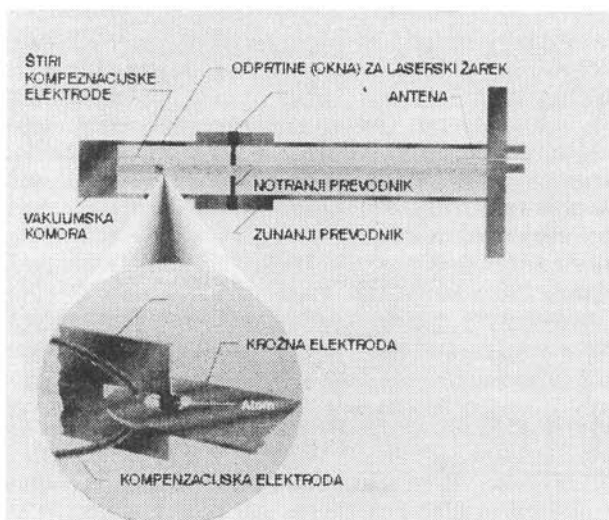
3 Diskusija

Morda diskusija na tem mestu niti ni smiselna, saj bralec lahko poseže po originalu in si tam ogleda tudi druge smeri razvoja računalniških tehnologij.

Osnovni namen pričujočega povzetka članka je bil nakazati smeri razvoja, ki so pomembne s strani vakuumske tehnologije. Ko bo prišel čas tehnološke zrelosti kvantnih računalnikov (če bo do tega tudi v resnici prišlo), bo to nedvomno izjemna priložnost za ponoven razcvet vakuumskih tehnologij.

4 Literatura

- /1/ T.Thompson, When Silicon Hits its Limits, What's Next?, Byte, Vol.21, N°4 (1996) 45-54.



Slika 1. Vrata XOR, ki jih je zgradila skupina NIST. Berilijev atom je ujet v magnetnem polju. Dva ultravijolična laserska žarka kontrolirata stanje atoma - njegovo nihanje in spin. Ti dve lastnosti sta uporabljeni za izdelavo 2-bitnega registra, ki deluje kot vrata XOR. Trenutno stanje atoma je merjeno s tretjim laserjem. Če atom kot odgovor na vzbujanje fluorescira, potem je to logično stanje 0. Če ne, potem je to stanje 1.