OSVJEŽIMO ZNANJE
Uređuje: Nenad Bolf

N. Bolf *
Fakultet kemijskog inženjerstva i tehnologije
Sveučilišta u Zagrebu
Zavod za mjerenja i automatsko vođenje procesa
Savska cesta 16/5a, 10 000 Zagreb

Kvantna računala – tehnologija 21. stoljeća

Ne trebamo samo snažnija računala nego i drugačija – a to bi mogla biti kvantna računala. Jedan od najpoznatijih svjetskih fizičara druge polovice 20. stoljeća Richard Feynman znao je govoriti da su digitalna ili klasična računala (kakva danas i poznajemo) loša u procjeni prirodnih procesa. A računati s prirodom moguće je ako je računalo temeljeno na kvantnoj mehanici. Takva računala primjenjuju radikalno drukčije algoritme. Nitko još zapravo ne zna sve buduće primjene kvantnih računala, ali stručnjaci su uvjereni da će to biti jedna od najvažnijih tehnologija 21. stoljeća.

Ideja o kvantnom računalu pojavila se prije već više od 35 godina, no tek posljednjih nekoliko godina počeli su se odvijati značajni(ji) koraci u njihovu razvoju. *IBM*, *Google*, *NASA*, a odnedavno i *Microsoft* ne samo da investiraju milijune, već nalaze i načine kojima ta posebno izvedena računala mogu otvoriti i novo poglavlje u tehnološkom razvoju.

Što je kvantno računanje?

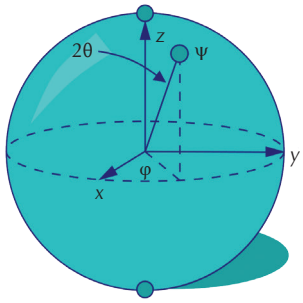
Kvantno računalo je bilo kakav uređaj za računanje koji izravno upotrebljava različite kvantnomehaničke fenomene, kao što su superpozicija i povezanost (spregnutost), kako bi obavile operacije nad podatcima. U klasičnom (ili konvencionalnom) računalu, količina podataka je mjerena bitovima – u kvantnom su računalu podatci mjereni **qubitovima** (engl. *quantum bit*). Osnovno načelo kvantnoga računanja jest to da se kvantna svojstva čestica mogu upotrebljavati za predstavljanje i strukturiranje podataka i da se kvantni mehanizmi mogu primijeniti za izvođenje operacija nad tim podacima.

U klasičnom računanju neizvjesnost je neprihvatljiva. Međutim, s kvantnim računalima to je prednost. Kvantna računala imaju inherentnu sposobnost učenja radeći s vjerojatnošću, dok istražuju višestruke odgovore kako bi došli do složenih odluka.

Kvantna računala briljiraju kod obrade velikog broja podataka. Dizajniraju se za rješavanje složenih zadataka čije bi rješavanje na klasičnim računalima potrajalo danima ili se uopće ne bi mogli riješiti.

Zanimljivo je da kvantna računala nisu univerzalno brža od klasičnih računala, ali brže obavljaju određene vrste izračuna. Svaka operacija možda neće biti brža, no broj operacija potrebnih za postizanje rezultata pomoću određenih algoritama je eksponencijalno manji.

Potencijal je, dakle, nevjerojatan – no usprkos desetljećima od početne ideje, ta grana znanosti još je u povojima. Ideja o kvantnom računalu seže u 1980., kada ga je matematičar Jurij Ivanovič Manin opisao u svojem radu "Izračunljivo i neizračunljivo". Svega godinu nakon, Richard Feynman predložio je izradu računala na temelju zakona kvantne mehanike.



Slika 1 – Blochova sfera je reprezentacija qubita, fundamentalnog gradivnog bloka kvantnih računala (izvor: Wikipedia, ref. 2)

Kako u osnovi funkcionira kvantno računalo

Svi smo navikli na binarna računala koja se temelje na tranzistorskim procesorima. Uključeno, isključeno, jedna, nula ... prilično predvidljivo. Međutim, priča se potpuno mijenja s kvantnim računalima. Tu su obrada i pohrana 1 i 0 klasičnih sustava ustupile mjesto qubitovima ili kvantnim bitovima kao temeljnim blokovima kvantne informacije. Moć qubita je u sposobnosti eksponencijalnog skaliranja, pri čemu 2-qubitni stroj provodi četiri izračuna istodobno, 3-qubitni osam izračuna istodobno, a 4-qubitni provodi 16 istodobnih izračuna.

Takvo što je moguće zbog toga što su kvantna računala u osnovi drugačija od današnjih standardnih računala. Kvantni bit ili qubit, može biti ili jedinica, ili nula ili oboje istodobno, što je poznato kao **kvantna superpozicija**. Upravo to svojstvo qubita uz niz drugih kvantnih učinaka omogućuje kvantnim računalima da određene operacije izvode znatno brže u odnosu na standardna računala.

Izrada takvog računala donijela je obilje problema, a praktični dokaz o funkcionalnosti i potencijalu stigao je 2013. Kanadska tvrtka **D-Wave** objavila je kako je prvi put u nekoj zadaći njihovo kvantno računalo od 439 qubita pobijedilo obično računalo. *D-Wave*ovo računalo konstruirano je tako da rješava zadatke optimizacije, odnosno da smanji broj rješenja složenih jednadžbi. Kvantno računalo bilo je 3600 puta brže.

* Prof. dr. sc. Nenad Bolf
e-pošta: bolf@fkit.hr

Testiranje je bilo kontroverzno jer su mnogi skeptici sumnjali u to da je *D-Wave*ov uradak istinsko kvantno računalo, no naknadni testovi pokazali su da uistinu primjenjuje kvantne efekte za svoj rad iako je ustanovljeno da je, od nekoliko stotina qubita, kvantno spregnuto manje od deset qubita.

U drugom dijelu 2015. ***NASA*** i ***Google*** objavili su kako je kvantno računalo ***D-Wave 2X*** s više od 1000 qubita brže od običnog računala za čak 100 milijuna puta. To je zvučalo znanstvenofantastično.

Obećavajući početni rezultati bili su dovoljni da se divovi IT industrije dignu na noge i počnu ulagati milijune u razvoj. ***Microsoft*** je odlučio istražiti i neke nove pristupe izradom tzv. topološkog qubita.

Dok *D-Wave* radi skupocjena kvantna računala koja su brza u određenim operacijama, ***IBM*** svojim pristupom radi na nečem što bi imalo praktičnije primjene.

Hoće li svijet u skorije vrijeme prijeći na kvantna računala?

Kvantna fizika toliko je zahtjevna da standardna računala nemaju dovoljno moći i memorije da se nose s tim proračunima. Manipulacijom tako goleme količine podataka kvantna računala bi mogla razviti gotovo neprobojne sigurnosne sustave, no to je tek jedna od mogućih primjena.

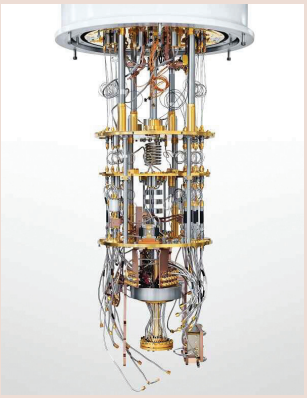
Svijet znanosti i tehnologija doživio bi pravi procvat zato što bi znanstvenici mogli provoditi virtualne pokuse. Kvantnim računalom bilo bi moguće raditi **modele kvantnih sustava**, moglo bi se pratiti **vladanje atoma i čestica** u neobičnim uvjetima, što je primjerice danas moguće tek u golemim akceleratorima čestica poput LHC-a. Nadalje, moglo bi se **modelirati i kemijske reakcije**, što bi omogućilo istraživanje i izvedbu novih materijala, ali i dovelo do drastičnog proboja u medicini – **izrada i testiranje lijekova** mogla bi se simulirati, računalni modeli bi mogli otkriti kako se javljaju neke bolesti i kako ih spriječiti. Izdvojimo još i razvoj superkatalizatora, sigurnost podataka, biomimikriju, financijske usluge, lanac opskrbe i logistiku itd.

Budu li kvantna računala radila onako kako su teorijski zamišljena, do traženog podatka u gomili podataka doći će se za tren. Time su postavljeni i novi temelji za razvoj naprednih algoritama za neuronske mreže. Razvoj umjetne inteligencije bio bi još intenzivniji od onoga što se zbiva danas.

No do toga će proći još neko vrijeme. Izrada kvantnog računala velike snage i za opću uporabu težak je zadatak za koji još nema jasnog rješenja. Međutim, optimizam brojnih tvrtki iz IT svijeta govori kako se u skorijoj budućnosti mogu očekivati još značajniji proboji.

Kvantna revolucija pred vratima

Pojam "kvantne nadmoći" (*quantum supremacy*) opisuje kvantna računala koja bi mogla početi obavljati razne zadaće ne samo brže od klasičnih, nego bi se mogla uhvatiti u koštac s problemima koji su klasičnim računalima nedostižni. Tu, primjerice, spada rastavljanje velikih brojeva na faktore, što bi dovelo do probijanja gotovo svake enkripcije. Najjačim klasičnim superračunalima za takvu bi zadaću trebale tisuće godina, a smatra se da bi kvantno računalo moglo takve probleme rješavati u nekoliko minuta.



[Rigetti Computing, fotografirao Justin Fantl]

Slika 2 – Kvantni računalni čipovi u kriogenom okruženju

Iz *Googlea* su ranije ove godine predložili tzv. *Nevenov zakon*, prema kojem snaga kvantnih računala raste dvostruko eksponencijalno, umjesto eksponencijalno shodno Mooreovom zakonu.

Prema još uvijek neslužbenim informacijama u Googleovim je laboratorijima nastalo kvantno računalo moćnije od svih postojećih klasičnih sustava.

Navodno je *Google* već izradio znanstveni rad (nakratko objavljen u rujnu 2019. na stranicama NASA-e, pa uklonjen) u kojem se tvrdi da njihovo kvantno računalo može učiniti nešto neviđeno: izvesti kalkulaciju u **3 minute i 20 sekundi**, za koju bi najnaprednijem superračunalu današnjice, *Summitu*, trebalo otprilike – **deset tisuća godina!**

"To dramatično ubrzanje naspram svih poznatih klasičnih algoritama daje eksperimentalnu potvrdu kvantne nadmoći na jednom računalnom zadatku te navještava dolazak dugoočekivane promjene računalne paradigme", kažu autori te napominju da je njihovo postignuće prvo takve vrste.

Ipak, napominje se da je njihov kvantni sustav visoko specijaliziran za izvođenje samo te, jedne jedine, zadaće. Primjena kvantnih računala za rješavanje svakodnevnih "teških" matematičkih problema još će čekati dulje vrijeme.

S druge strane, IBM je nedavno objavio da će klijentima svoje usluge *IBM Q Network* sredinom listopada 2019. dati na raspolaganje kvantno računalo od 53 kubita – najveće komercijalno dostupno kvantno računalo do sada.

Izvor: www.bug.hr (21. rujna 2019.)

Literatura i daljnje informacije

1. https://www.edn.com/design/systems-design/4462206/The-basics-of-quantum-computing-A-tutorial.
2. https://www.dwavesys.com/tutorials/background-reading-series/quantum-computing-primer.
3. https://hr.wikipedia.org/wiki/Kvantno_ra%C4%8Dunalo.
4. https://www.tportal.hr/tehno/clanak/sto-su-to-kvantna-racunala-i-zasto-ce-promijeniti-svijet-20161201 (19. 1. 2017.).
5. https://cloudblogs.microsoft.com/quantum/author/microsoft-quantum-team/.
6. http://ideje.hr/radi-kvantno-racunalo-zasto-toliko-mahnito-brze-hint-lukavo/.
7. https://www.bug.hr/tehnologije/nevenov-zakon--adaptacija-mooreovog-zakona-ali-za-kvantna-racunala-10602.
8. http://mmrc.amss.cas.cn/tlb/201702/W020170224608150244118.pdf.