MEĐUOVISNOST RAZVOJA KLASIČNE I KVANTNE INFORMATIKE

Smrt Mooreovog zakona

Ilustracija: Larisa Orešković

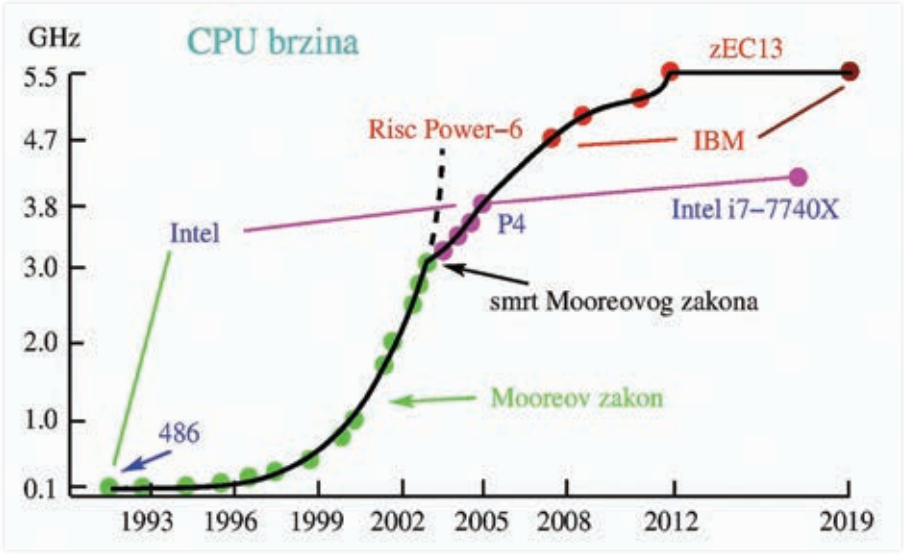
PIŠE: **MLADEN PAVIČIĆ**

The New York Times je 23. X. 2019. objavio članak *Google tvrdi da je napravio kvantni proboj koji može promijeniti računanje*. Nakon tjedan dana 30. X. 2019. objavio je i drugi: *Zašto je važna Googleova kvantno-suprematistična prekretnica*. Taj događaj je pokrenuo lavinu članaka i videa u svjetskim medijima pa i ovaj koji upravo čitate. Iz tih članaka, videa i komentara ubrzo je postalo jasno da nije najjednostavnije objasniti pa ni razumjeti da bi se objasnilo kako radi kvantno računalo, što je ono dosad izračunalo i što može izračunati. Tako se 6. XII. 2019. u *The New York Timesu* pojavio članak *Što je dovraga kvantno računalo* (*What on Earth Is a Quantum Computer*). U njemu su navedeni opisi kvantnog računala nekoliko vrhunskih eksperata jezikom koji svatko može razumjeti. Naprimjer Daniel Lidar priložio je haiku koji počinje ovako: *Kvantna računala // rješavaju neke probleme puno brže // ali su sklona šumu*. Na webu nalazimo deset najvažnijih neočekivanih budućih primjena kvantnih računala od kojih je prva: igranje. Ipak je dodano – možda. Probat ćemo to pojasniti malo bolje.

Svi mi manje-više poznajemo računala i internet pa pojedine detalje klasične informatike možemo lako dohvatiti pretraživačima. No, u ovom članku referirat ćemo se samo na detalje vezane uz fizikalna kvantna ograničenja daljnjeg razvoja klasične informatike ili na ona koje kvantna informatika može prevladati. Zatim ćemo govoriti o razvoju kvantne informatike u funkciji neminovnog socijalnog i ekonomskog razvoja te pokazati da se ta dva razvoja međusobno uvjetuju.

Već petnaest godina ne samo da nema eksponencijalnog ubrzanja klasičnog procesora (CPU), kako je predviđao takozvani Mooreov zakon nego više nema nikakvog ubrzanja (slika 1). Intel je 2004. godine postigao 3,8 Ghz i otad je oko 4 GHz maksimum koji si pojedinci ili manje tvrtke mogu priuštiti. Nešto brži IBM-ovi procesori namijenjeni su superračunalima, a njihove cijene se kreću od minimalno 100.000 dolara naviše. Godine 2012. proizveden je dosad najbrži procesor na svijetu - ne računajući *overclockinge* do 9 Ghz u svrhu rekorda - IBM zEC13 5,5 Ghz površine 597,24 mm^2 koji sadrži 2,75 milijarde tranzistora, 32 nm CMOS-a (*complementary metal–oxide–semiconductor*). CMOS su 0-1 logička vrata, a prijelaz od nabijenog

Eksponencijalni razvoj znanosti, tehnologije, administracije, političke i vojne kontrole bio je do 2004. omogućen povećanjem brzine CPU-a i minijaturizacijom elektroničkih i pogonskih elemenata



Slika 1: Smrt Mooreovog zakona – procesorske brzine.

stanja 1 (CMOS je esencijalno kondenzator) do ispražnjenog stanja 0 i obratno zahtijeva neko vrijeme koje se ne može izbjeći i uzrokuje prvo vremensko ograničenje.

Dva spomenuta stanja 0 i 1 definiraju informaciju koju dobivamo kad je jedno od njih određeno, proslijeđeno ili izmjereno. Naziv za tu informaciju je jedan bit. Sljedeće fizikalno ograničenje brzine CPU-a je temperatura i disipacija topline. Snaga koja se razvija u vodičima (koji čine trećinu mase CPU-a - ukupna duljina unutar CPU-a im je nekoliko kilometara) je proporcionalna kvadratu napona struje i ne može se proizvoljno smanjivati jer postoji naponski prag ispod kojeg CPU ne radi. Isto tako ne možemo CPU proizvoljno ohladiti jer ne radi ispod -55°C. Navedena fizikalna ograničenja brzine CPU-a potječu od kvantne strukture materijala.

Za godinu ili dvije udarit ćemo o kvantni zid minijaturizacije elektroničkih elemenata. Vodiči ne mogu biti tanji od monosloja debljine jednog atoma i logička vrata - tranzistori ne mogu biti manji od jednog atoma, a već i prije tih limita ne može se izbjeći nekontrolirani prijelaz ili curenje (*leakage*) elektrona iz jednog elementa u drugi (slika 2).

Eksponencijalni rast CPU brzine do 2004. i minijaturizacije elektronike do 2020. godine bio je spregnut s neregulirnim eksponencijalnim rastom ekonomije i tehnologije što je dovelo do uništavanja Zemlje i istrebljenja njenih bioloških vrsta. Problemi optimizacije proizvodnje, transporta, simuliranja mogućih rješenja tehnoloških, proizvodnih, ekonomskih, administrativnih, socijalnih i drugih zadataka, modeliranja novih tehničkih proizvoda, molekula, biološke dinamike, strukture materijala, generacije fizikalnih i kemijskih spojeva i drugih struktura su polinomijalno* ili eksponencijalno kompleksni što znači da s linearnim povećanjem broja parametara koji definiraju problem vrijeme potrebno za njegovo rješavanje polinomijalno ili eksponencijalno raste. Eksponencijalni razvoj znanosti, tehnologije, administracije, političke i vojne kontrole bio je do 2004. omogućen i podržan eksponencijalnim povećanjem brzine CPU-a i minijaturizacijom elektroničkih i pogonskih elemenata u tvornicama, vozilima, internetskoj i elektroenergetskoj mreži, laptopima, mobitelima itd.

Od 2004. godine kao palijativna zamjena za Mooreovo eksponencijalno ubrzanje uvodi se paralelizacija operacija: *clusteri*, *cloud*, superračunala, a na nivou individualnih procesora CPU s dvije, 4, 6, 8, ..., 18, ..., 28 jezgara (najavljen je Intel 5 GHz Core i7-8086 K *Anniversary Limited Edition*). No, linearna paralelizacija za linearno i eksponencijalno kompleksne probleme daje samo linearno ubrzanje, što znači da bismo za adekvatno brzo rješavanje eksponencijalno kompleksnih problema trebali eksponencijalno povećavati broj računalskih jedinica s pripadnim CPU-ovima unutar *clustera* i superračunala. A to se upravo i događa. Najmoćnije superračunalo na svijetu Tianhe-2 - s 80.000 CPU-ova koji sadrže 3,120,000 jezgri - konzumira električnu energiju snage 24 MW. Za usporedbu, to je točno snaga hidroelektrane Miljacka na Krki koja je prije jednog stoljeća bila najsnažnija hidroelektrana u Europi. Projekcije pokazuju da će do 2025. godine informacijska i komunika-

Promatrajmo razbijanje broja N koji je kreiran kao umnožak dva prosta broja. Prosti brojevi su oni koji nisu umnošci manjih brojeva - npr. 7 ili 13. Razbijanje čistom silom svodi se na sukcesivno dijeljenje broja N s **1, 2, 3, ...,** $\sqrt{N}$**-1**, tj., u $\sqrt{N}$ koraka. Na analognom računalu najefikasniji algoritam za takvo dijeljenje ima kompleksnost $\log N$, što daje vrijeme $O(\sqrt{N}\log N)$. To je prikazano na slici 3 za $N=2\cdot10^{153}$ do $N=14\cdot10^{153}$ gdje vidimo da vrijeme ne raste eksponencijalno. Na digitalnom računalu moramo pretvoriti N u digitalni oblik $N=2^n$, gdje je n broj bitova i onda je $\sqrt{N}\log N = n\,2^{n/2}$ pa vrijeme eksponencijalno raste kao funkcija od n, $O(n\,2^{n/2})$ što je prikazano na slici 4. Algoritam na digitalnom računalu ima eksponencijalnu kompleksnost.

Kvantno računalo dizajnirano za implementaciju algoritama baziranih na Fourierovim transformacijama objasnit ćemo na pojednostavljenom modelu J. Summhammera [4] prikazanom na slici 5, koji analogno Shorovom algoritmu razbija brojeve - iako ne toliko velike - i implementira Fourierovu transformaciju. U medijima se često kvantno računalo objašnjava kao ono koje koristi kvantne bitove - qubite - koji se od klasičnih bitova razlikuju po tome što mogu poprimiti vrijednosti između **0 i 1**, npr. **0.3 ili 0.762** ili po tome što poprimaju vrijednosti **0** i **1** istodobno. Takva je interpretacija nije odgovarajuća što pokazuje slika 5. Foton pada na polupropusno zrcalo s gornje strane. Qubit je stanje tog fotona i njega označavamo sa **|0>**. Stanje fotona je oblik elektromagnetskog vala čiji je foton nositelj. Možemo uzeti da je to sinusoida. Da je foton došao s donje strane njegovo bismo stanje označili sa **|1>**, ali nije i to smo naznačili iscrtkanom linijom. Na polupropusnom zrcalu se val djelomično reflektira, a djelomično prolazi kroz njega u omjeru **1:1**. U principu se ne može saznati je li se sam foton reflektirao ili je prošao kroz njega. Takvo saznanje uništilo bi interferenciju i računanje. Nakon polupropusnog zrcala elektromagnetski valovi ili preciznije *Bornovi valovi vjerojatnosti* – sad ne govorimo o fotonu već isključivo o valovima – prolaze kroz dva optička elementa ε_0 i ε_1 koji uzrokuju pomake u fazama valova – istodobno. Nakon toga val s gornje strane dolazi do drugog polupropusnog zrcala pa ili se od njega reflektira ili prolazi kroza nj, a jednako tako i val s donje strane. Ti valovi interferiraju i ulaze u detektore D_0 i D_1. Kažemo da foton interferira sam sa sobom. Klik u detektoru znači detekciju fotona. Ako je interferencija (superpozicija) konstruktivna, vjerojatnost da će detektor detektirati foton je **1**, tj. **100 %**. To je na slici 5 prikazano za D_1. Ako je interferencija destruktivna, vjerojatnost da će detektor detektirati foton je **0**, tj. **0 %**. To je na slici 5 prikazano za D_0. Interferencija je određena faznim pomacima. Ako fazni pomaci nisu cjelobrojni višekratnici od **2π**, onda postoji određena vjerojatnost da će i D_0 i D_1 dati klik, ali ne istodobno. (više o interferenciji Pavičić, youTube-1 [5] od 12:00.)

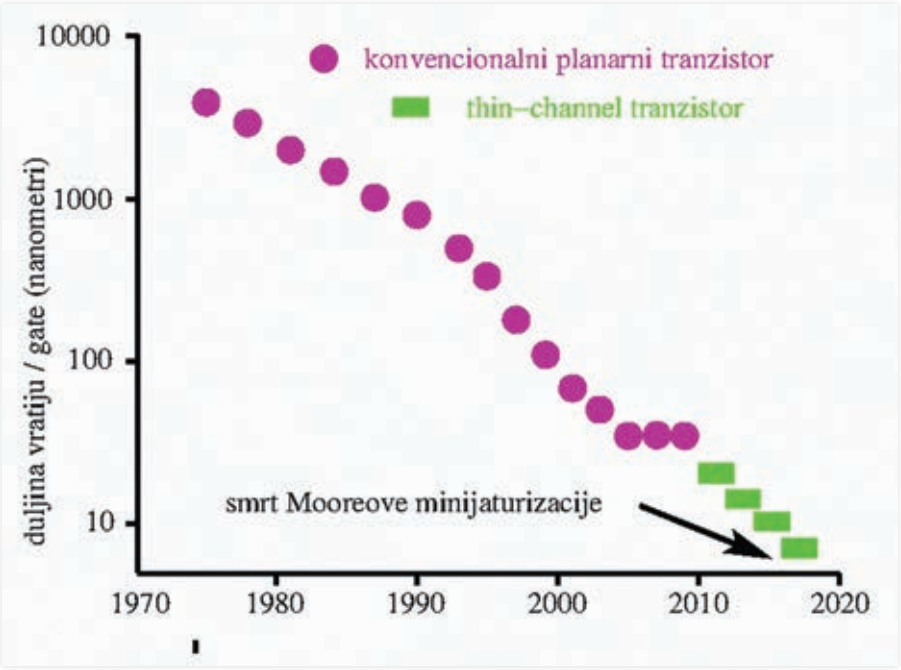
Računanje se izvodi na sljedeći način. Želimo odrediti je li n faktor broja N, tj. da li je $N = m\cdot n$. Za odabrani n, povećavamo fazni pomak φ u diskretnim koracima $2\pi/n$ tako da je $\varphi = 2\pi j/n$. Za svaki takav pomak šaljemo u naše računalo (Mach-Zehnderov interferometar - na slici 5) novi foton. Odabiremo $j=kN$, $k=1,2,3,...,n$. Kad obavimo sva n mjerenja za odabrani n suma klikova S_n u detektoru D_1 na slici 5 reći će nam je li n faktor broja N ili ne. Naime, ako je n faktor od N, tj. ako je $n=N/m$ onda ćemo imati $\cos\varphi = \cos 2\pi km = 1$ i $S_n = n$, tj. detektor D_1 će reagirati uvijek, a D_0 nikad. Ako n nije faktor od N onda ćemo imati $-1 < \cos\varphi < 1$ i $S_n \approx n/2$, tj. i D_0 i D_1 će reagirati podjednako. U toj je proceduri najveći n koji moramo provjeriti $\sqrt{N}$, a za svaki n moramo provjeriti n različitih faznih pomaka, kad n povećavamo od **1** do $\sqrt{N}$. Dakle, vrijeme koje maksimalno moramo utrošiti je $n^2 = N$, tj. kompleksnost je linearna.

cijska tehnologija trošiti 20 % električne energije. K tome, mnogi problemi su sekvencijalni i ne mogu se paralelizirati.

Deset godina prije toga - 1994. - Peter W. Shor je našao algoritam za tada samo principijelno definirano kvantno računalo koji je eksponencijalno kompleksni problem faktoriziranja brojeva sveo na polinomijalno kompleksni problem. To je izazvalo veliki interes jer se glavni protokol za enkripciju lozinki i tekstova na internetu, dakle, u ICT-ju (*information and communications technology*), takozvani RSA protokol (*Rivest-Shamir-Adelman* iz 1977.), bazira na umnošku dvaju vrlo velikih prostih brojeva u jedan još veći. Razbiti takav veliki broj grubom silom je eksponencijalno kompleksan problem, tako da je sam Rivest 1978. procjenjivao kako bi za razbijanje 126-digitnog (RSA-419 bitnog) broja trebalo 40 kvadrilijuna godina.

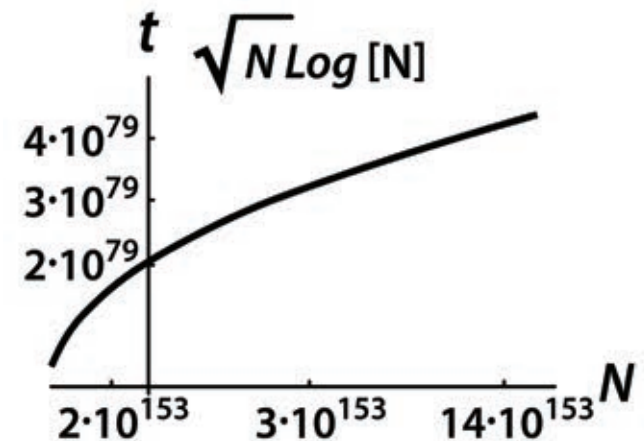
Za godinu ili dvije udarit ćemo o kvantni zid minijaturizacije elektroničkih elemenata; logička vrata - tranzistori ne mogu biti manji od jednog atoma.

Međutim, u međuvremenu su nađeni subeksponencijalno kompleksni algoritmi koji takve brojeve na *cloudu* razbijaju za nekoliko sati. I već je 2009. razbijen 617-digitni (RSA-2050 bitni) broj tako da se danas prelazi s enkripcije pomoću RSA-512 bita na onu pomoću RSA-1024 bita. To je bitno zbog toga što se klasična enkriptirana poruka od pošiljateljice Alice do primatelja Boba uvijek može na pola puta neopazivo hakirati i spremiti. S razvojem algoritama i tehnologije za nekoliko godina moći će se lako pročitati na *clusterima* ili *cloudu*. Pitanje je hoće li državne i privatne agencije prije moći pročitati dokumente građana ili građani njihove. Agencije su taj problem djelomično riješile zahtjevom da provideri spuste enkripciju za građane koji imaju svoj neovisni internet ili jednostavno zabrane slobodno enkriptiranje. Ali to ne rješava pitanje kriminala i hakiranja bankovnih lozinki. Štete od zloupotreba se procjenjuju na stotine milijuna dolara godišnje. S druge strane nije dokazano da polinomijalni algoritam za razbijanje brojeva ne postoji pa postoji vjerojatnost da bi ga neki hakerski genij mogao smisliti preko noći i od sljedećeg jutra mogao bi se na osobnom računalu razbiti bilo koji enkriptirani dokument ili lozinka. To bi dovelo do trenutnog kolapsa internetskih povjerljivih transakcija, npr. bankovnih i do nesagledive svjetske ekonomske krize.

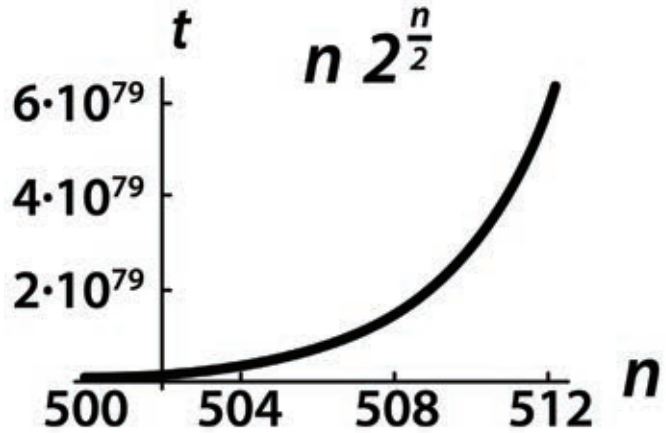


Slika 2: Smrt Mooreovog zakona – minijaturizacija elektronskih elemenata.

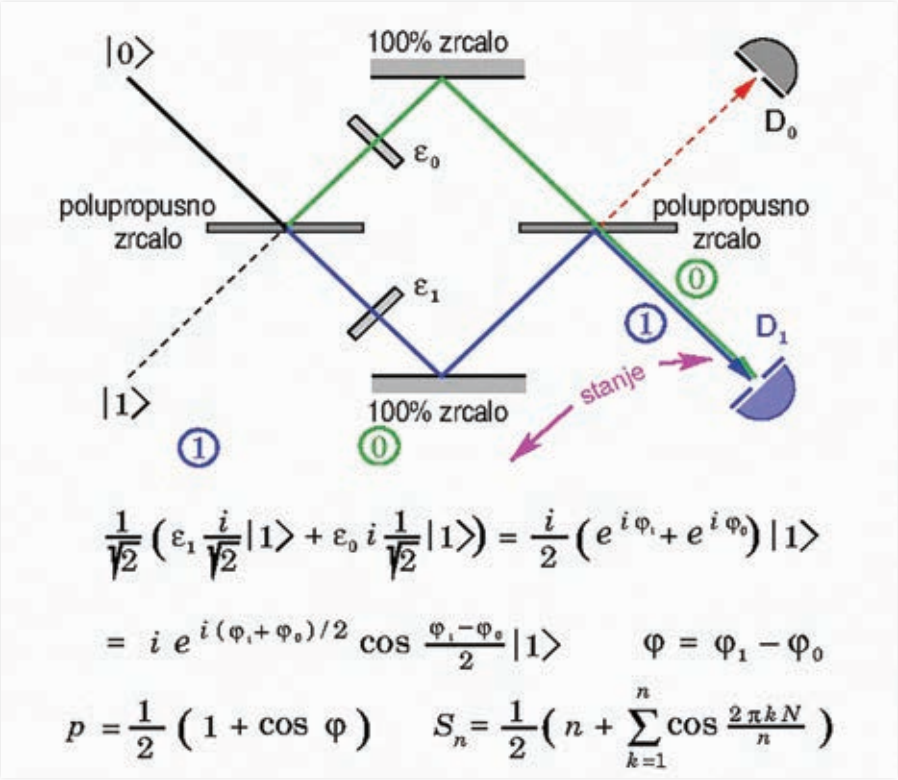
Godine 1984. taj su problem riješili Charles Bennett i Gilles Brassard dizajniranjem apsolutno neprobojne kvantne kriptografije – BB84 protokola. Ideja je kvantno jednostavna. Alice šalje Bobu jedan po jedan linearno polarizirani foton u dvije baze: pravocrtnoj (+) ili dijagonalnoj (x). Pojedinačni fotoni su polarizirani kao i svjetlost koja sadrži mnogo takvih fotona, naprimjer onih koji dolaze s ekrana vaših računala. I vaše sunčane naočale su najčešće polarizirane pa ako ih stavite pred ekran i zakrećete vidjet ćete da se slika u određenom položaju, recimo u (+), potpuno zatamnjuje dok je pod kutom od 45° (x) punog intenziteta. (Alternativno možete pogledati Pavičić, youTube-2 [1] od 1:50.) Alice nasumično odabire bazu i šalje foton Bobu. U pravocrtnoj bazi vertikalno polarizirani foton (|) znači poruku 1, a horizontalno polarizirani (-) poruku 0. U dijagonalnoj bazi desno zakrenuti (/) znači 1, a lijevo (\) znači 0. Bob također nasumično odabire bazu i mjeri fotone. Poslije Alice javlja Bobu klasičnim internetom koje



Slika 3: Faktorizacija brojeva na analognom računalu.



Slika 4: Faktorizacija brojeva na digitalnom računalu.



Slika 5: Pojednostavljeno kvantno računalo: Mach-Zehnderov interferometar.

je baze koristila za koji foton i Bob zadržava samo ona mjerenja koja odgovaraju podudarnim bazama o čemu povratno informira Alice također klasičnim internetom. No, hakerica Eve može pokušati ukrasti poruku. Ona ne može ukrasti dio fotona - kao što može skrenuti dio klasičnog snopa - jer je foton nedjeljiv već mora zamijeniti pojedine fotone svojima, ali to može učiniti samo nasumično, ne znajući koji je foton ispravno polariziran u bazi koju nije pogodila. Ako je uvijek u istoj bazi onda će pogriješiti u 25 % slučajeva. Nakon matematičke obrade mjerenja, što Alice i Bob obavljaju naknadno, Eve ostaje bez ijednog bita informacije. (Za detalje v. Pavičić, M., *Quantum Computation and Quantum Communication: Theory and Experiments, Springer*, New York (2006)[2], str. 69.) Protokol se može učiniti još sigurnijim ako Alice koristi spregnuti par fotona od kojih jedan drži u kvantnoj memoriji (npr. u optičkoj petlji), a drugi šalje Bobu koji ga također drži u kvantnoj memoriji. Taj je foton potpuno nepolariziran sve dok Alice ne izmjeri svoj foton i ne pošalje baze Bobu klasičnim internetom. (Pavičić, youTube-3[3] od 16:25.) Eve može također spremiti ukradeni foton, ali ne može izbjeći da ne pošalje Bobu u 50 % slučajeva pogrešan foton.

Dakle, Shorov algoritam može se uzeti kao stimulans usvajanja i implementira-

Googleovo posljednje i njegova prethodna kvantna računala kao i IBM-ova - uključujući najavljeno IBM-ovo 50-qubitno supravodljivo računalo su sigurno proboj u tehnologiji kvantnog računalstva i znak da ulazimo u njegovu proizvodnu fazu.

nja BB84 protokola u svjetskom internetu. Istina je da još nisu na zadovoljavajući način dizajnirani kvantni repetitori, ali su postignute udaljenosti više od 300 km kroz optička vlakna i još veće preko Micius satelita, tako da je kvantni internet moguć u urbanim sredinama ili preko satelita. Agencija DARPA (*Defense Advanced Research Project Agency*) Ministarstva obrane SAD-a te sveučilišta Harvard i Boston implementirali su 2003. godine u Bostonu kvantnu mrežu dugu 29 km. *Senetas ID Quantique* (IDQ) je 2007. osigurala švicarsku federalnu izbornu mrežu kvantnom enkripcijom. Od 2004. do 2008. unutar projekta SECOQC (SE*cure COmmunication based on Quantum Cryptography*) implementirana je kvantna mreža sa šest čvorova u Beču. U Tokiju je 2010. postavljena još veća kvantna mreža suradnjom međunarodnih tvrtki - NICT, NEC, Mitsubishi, NTT, Toshiba, IDQ, All Vienna, itd.- koje se bave kvantnom tehnologijom.

Razumijevanje Shorovog kao i svih postojećih kvantnih algoritama u našem neposrednom kontekstu - koji svi moramo razumjeti - zahtijeva prizivanje nekoliko činjenica o klasičnom nasuprot kvantnom računanju. Prvo, pod klasičnim računanjem podrazumijeva se računanje na digitalnom računalu iako postoje i analogna. Neki problem može biti eksponencijalno kompleksan na digitalnom računalu iako je polinomijalno ili linearno kompleksan na analognom. Izlazni napon koji je proporcionalan omjeru ulaznog napona i odabranog otpora na analognom računalu daje rezultat u jednom koraku, dok je prebacivanje vrijednosti napona i otpora u digitalnu formu eksponencijalno kompleksna operacija s obzirom na rast iznosa vrijednosti napona i otpora. Nažalost, raspon vrijednosti napona i otpora je relativno mali i to je jedan od razloga zašto koristimo digitalna, a ne analogna računala. Drugo, svi postojeći kvantni algoritmi (Deutsch, Deutsch-Joysa, Bernstein-Vazirani, Shor, Grover - za pretraživanje baza podataka, Abrams-Lloyd i Zalka - za nalaženje svojstvenih vrijednosti i vektora) baziraju se na kvantnoj Fourierovoj transformaciji, a dat ćemo i primjer koji karakterizira takve algoritme (vidi okvir).

Jasno, složenost Shorovog i ostalih kvantnih algoritama, dakle, postojećeg kvantnog softvera je puno veća od algoritma implementiranog na Mach-Zehnderovom interferometru u našem primjeru – ali princip je jednak. Računanje se zasniva na superpoziciji stanja qubita i na povratnoj petlji koja inicira novu ako prethodna nije dala traženi rezultat. Međutim, takvo ponavljanje je polinomijalno kompleksno. Osim toga, ponavljanje rješava nestabilnost stanja pri računanju i korekcije grešaka tijekom računanja.

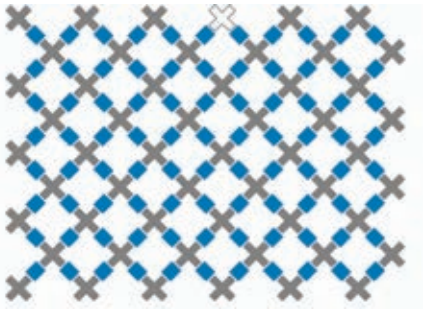
Kvantni hardver zasnovan na superpoziciji stanja moguće je ostvariti na različitim fizikalnim principima i sustavima - nuklearnoj magnetskoj rezonanciji, čvrstom stanju (silicijskim nuklearnim spinovima), kvantnim točkama (*quantum dots*), ionima u stupici i supravodljivosti (minijaturne supravodljive petlje). (Pavičić, M., *Companion to Quantum Computation and Communication*, Wiley-V-CH, Weinheim (2013)[6], Ch. 2.) Posljednjih dvadesetak godina eksperimenti na svim tim sustavima izvođeni su paralelno jer se tražio sustav koji će najbolje riješiti problem dekoherencije, tj. nesta-

bilnosti stanja qubita tijekom računanja. Hardveri zasnovani na dva posljednja kandidata bili su posljednjih godina preferirani. Tvrtke IBM, Google, D-Wave, Intel i Rigetti dosad su se sve odlučile za supravodljivost.

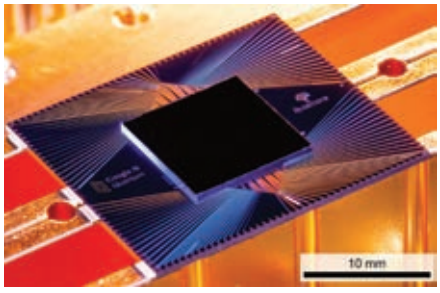
Potkraj 2019. godine 24. X. Google je objavio članak *Quantum supremacy using a programmable superconducting processor, Nature*, Vol. 574, 505 (2019) [7] u kojemu je predstavio svoj kvantni procesor Sycamore zasnovan na 53 supravodljiva qubita (slike 6 i 7) što odgovara računalnom prostoru stanja dimenzije 253. Tu se vidi da povećanje broja qubita za 1 daje dvostruko povećanje prostora stanja. Zadatak koji je izvršen na *Sycamoreu* ohlađenom na ispod 20 mK bilo je ponavljanje uzorka zadanog kvantnog kruga milijun puta unutar 200 sekundi. Trajanje simulacije tog zadatka na klasičnom superračunalu u članku je procijenjeno na 10.000 godina i to je uzeto kao osnova za tvrdnju o kvantnoj premoći (*quantum supremacy*) što je izazvalo veliku pozornost u medijima. IBM je nakon toga izjavio kako bi njihovom klasičnom superračunalu Summit za tu simulaciju trebalo dva i pol dana [8]. No, bez obzira na te procjene ovo Googleovo posljednje i njegova prethodna kvantna računala kao i IBM-ova - uključujući najavljeno IBM-ovo 50-qubitno supravodljivo računalo su sigurno proboj u tehnologiji kvantnog računalstva i znak da ulazimo u njegovu proizvodnu fazu.

Paralelno s tim tehnološkim probojem publiciran je *open source report* (*Quantum Computing Progress and Prospects* (2019), *The National Academies Press, Washington*)[9] u kojemu su prezentirani ključni rezultati o kvantnom softveru, dizajnu mogućeg hardvera te izdvojena i diskutirana dva spomenuta kandidata - ionski i supravodljivi - za buduću implementaciju. Sve je prezentirano detaljno sa svim relevantnim referencama, ali s apsolutno minimalnom količinom najjednostavnijih formula. U prvom poglavlju dana je samo jedna slika koja prikazuje svjetsku prodaju poluvodiča. Ona pokazuje eksponencijalni rast pod kutom od 40° u logaritamskom prikazu do 1995. godine i nagli pad na oko 15° nakon toga, što vodi k novom kvantnom pristupu računanju.

Drugo poglavlje daje pregled osnova kvantno-informatičkog formalizma i njegovu postojeću eksperimentalnu implementaciju. Treće poglavlje prezentira kvantne algoritme i korekciju grešaka. Četvrto obrađuje implikacije kvantnog računalstva na kriptografiju. Predviđa se da će današnja RSA kriptografija kroz



Slika 6: Shema Googleovog Sycamore procesora – iz [6].



Slika 7: Fotografija Googleovog Sycamore procesora – iz [6].

petnaest godina kolabirati pa bi prijelaz na kvantnu kriptografiju trebao početi za nekoliko godina. Već sad je pravilo 50 godina (vladini dokumenti drže se tajnima 50 godina) neodrživo.

Peto poglavlje prezentira bitne hardverske, a šesto softverske komponente kvantnog računala. Posljednje sedmo poglavlje diskutira izvedivost i vremenski okvir moguće implementacije kvantnog računanja sa sljedećim ključnim točkama:

1. **Ne može se očekivati da bi se kvantno računalo koje bi moglo razbiti RSA 2048 enkripciju moglo sagraditi u sljedećem desetljeću.**
2. **Ako se kvantna računala u bliskoj budućnosti ne pokažu komercijalno isplativima, za sprečavanje degradacije istraživanja i razvoja kvantnog računanja bi bila ključna državna potpora.**
3. **Za komercijalnu primjenu urgentno je potrebno istraživanje u području stabilnosti qubita u realnim uvjetima.**
4. **Vremenski okvir za pojedine faze razvoja se još ne može odrediti.**
5. **Postoji potreba unificirane konvencije prikazivanja rezultata - prikazane su realizirane implementacije, ulaganja po zemljama, te nacionalne i internacionalne inicijative.**
6. **do 10. Moguće primjene.**

U dodacima su detaljnije prezentirana ionska, supravodljiva, fotonska, atomna, poluvodička i topološka kvantna računala te globalna ulaganja u istraživanje i razvoj.

Kod nas je postignut značajan doprinos u razvoju jedne teorijske komponente kvantnog hardvera koja se pokazala esencijalnom za konstrukciju kvantnog računala tzv. kontekstualnosti. (M. Howard et al., *Contextuality supplies the 'magic' for quantum computation, Nature*, Vol. 510, 351 - 2014) [10].

Naša grupa u okviru Istraživačke jedinice za fotoniku i kvantnu optiku Centra izvrsnosti za napredne materijale i senzore - CEMS-Fotonika [11] dala je većinu svjetskog doprinosa u području kontekstualnih skupova. To su skupovi čiji elementi ne mogu imati pridijeljene određene vrijednosti 0 i 1, kao npr. klasična logička vrata - CMOS, tj. tranzistor u klasičnom računalu - već su isključivo kvantni.

Najznačajniji proboji s prethodno nepoznatim rezultatima dani su u Pavičić (2019)[12], Pavičić et al. (2019 [13] i Pavičić et al. (2018) [14]. ■

* Polinomijalno kompleksna funkcija je funkcija koja se mijenja s potencijama parametara (npr., kvadratom ili kubom).

Pitajte autora: https://www2.irb.hr/korisnici/mpavicic/
Saznajte više na str. 81

Upoznajte autora:

Mladen Pavičić je teorijski fizičar, bavi se kvantnim računalstvom, kvantnom kriptografijom, kvantnom optikom i kvantnim algebarskim strukturama. Autor je više od sto znanstvenih članaka s međunarodnom recenzijom - više od 60 u renomiranim međunarodnim časopisima te dviju knjiga. On je Humboldt i Senior Fulbright fellow. Bio je profesor na Građevinskom fakultetu u Zagrebu, a sad je znanstveni savjetnik u CEMS-u Instituta Ruđer Bošković. Bio je imenovani profesor na *University of Maryland Baltimore County*, USA i gostujući profesor na sveučilištima u Njemačkoj (*Universität zu Köln, Technische Universität Berlin, Humboldt Universität Berlin*), Austriji (*Atominstitut Technische Universität Wien, Erwin Schrödinger Institut Wien*), SAD-u (*Harvard University, Cambridge*) i Francuskoj (*L'université de Reims*). Bio je voditelj 4 projekta pri Ministarstvu znanosti i obrazovanja i suradnik na projektu Hrvatske zaklade za znanost. Voditelj je nekoliko međunarodnih suradnji.

Saznajte više...

Naši autori su pripremili popis kvalitetnih izvora za podrobnije upoznavanje s pojedinim temama

Članak na str. 10 Mladen Pavičić SMRT MOOREOVOG ZAKONA

[1] Pavičić, M., Predavanja iz fizike – optika 2, https://www.youtube.com/watch?v=NYammAar4a0#t=1m50s

[2] Pavičić, M., Quantum Computation and Quantum Communication: Theory and Experiments, Springer, New York (2006)

[3] Pavičić, M., Predavanja iz fizike – optika 3, https://www.youtube.com/watch?v=6PNjKTjFOXA#t=16m25s

[4] Summhammer, J., Physical Review A, 56, 4324 (1997).

[5] Pavičić, M., Predavanja iz fizike – optika 1, https://www.youtube.com/watch?v=n5DvPnJ_Hxs#t=12m0s

[6] Pavičić, M., Companion to Quantum Computation and Communication, Wiley-VCH, Weinheim (2013)

[7] Arute, F., et al. and John M. Martinis, Quantum supremacy using a programmable superconducting processor, Nature, Vol. 574, 505 (2019)

[8] https://www.nbcnews.com/mach/science/google-claims-quantum-computing-breakthrough-ibm-pushes-back-ncna1070461

[9] Quantum Computing Progress and Prospects (2019), The National Academies Press, Washington

[10] M. Howard et al., Contextuality supplies the 'magic' for quantum computation, Nature, Vol. 510, 351 (2014)

[11] Centar izvrsnosti za napredne materijale i senzore (CEMS-Fotonika) http://cems.irb.hr/hr/ Istraživačka jedinica za fotoniku i kvantnu optiku Centra izvrsnosti za napredne materijale i senzore (CEMS-Fotonika) http://cems.irb.hr/hr/research-units/photonics-and-quantum-optics/

[12] Pavičić, M., Hypergraph contextuality, Entropy, Vol. 21(11), 1107 (2019)

[13] Pavičić, M., M. Waegell, N. D. Megill & P. K. Aravind, Automated generation of Kochen-Specker sets, Scientific Reports, Vol. 9, 6765 (2019)

[14] Pavičić, M. and N. D. Megill, Vector Generation of Quantum Contextual Sets in Even Dimensional Hilbert Spaces, Entropy, Vol. 20(12), 928 (2018)

Ilustracija:
LARISA OREŠKOVIĆ

smartInfoTrend
Informatika za gospodarstvo znanja

NAKLADNIŠTVO:

TELEDOM d.o.o. za telekomunikacijski i informatički konzalting

Žajina 61/1, 10 000 Zagreb
OIB: 03544854623
Raiffeisenbank Austria d.d.
IBAN: HR5124840081103024067
Tel: +385 01/3040588; Faks: +385 01/3040593
e-pošta: infotrend@teledom.hr
smartInfoTrend online: www.infotrend.hr

Direktor:
Leo Petrov

Izvršni direktor:
Boris Blumenschein

REDAKCIJA:

Glavni urednik:
Branko Kosec
e-pošta: redakcije@trend.hr

Dopisnik iz BiH:
Haris Hamidović

Dopisnik iz Srbije:
Nikola Marković

Jezična obrada:
Lidija Orešković

Marketing i oglašavanje:
redakcije@trend.hr, 01 3040 588

Grafičko oblikovanje:
Larisa Orešković
art&design studio

Izrada i održavanje web-portala:
Novena d.o.o. Zagreb

Tisak:
AKD d.o.o. Zagreb

online: www.infotrend.hr

U OVOM BROJU

smart infoTrend

Broj 213 2019/Q4 CIJENA: 32 kn, 4,5 €, 5 KM

KVANTNO RAČUNALSTVO

korak do proizvodne faze

IT INDUSTRIJA
Stanje po županijama

SRCE
Projekti u potrazi za kadrovima

DEEP LEARNING
i razvoj umjetne inteligencije

VJEŠTINE ZA BUDUĆNOST
i promašeni obrazovni sustav

DIGITALNI MARKETING
Inovativni pristup kampanji

VIRTUALNA PRAVDA
AI u pravnom sektoru

ISSN 1330-0393
9 771330 039008 12019