



## Kada i kako započeti učiti o kvantnom računarstvu?

Mladen Viher<sup>1</sup>

Zadnjih godina mnogo toga je napisano o kvantnom računarstvu, od popularnih članaka do teorijskih radova. Međutim, čini nam se kako još uvijek nedostaje tekst koji bi darovitim i zainteresiranim srednjoškolcima ukazao na mogućnost prema samoobrazovanju u ovom području. Smatramo kako im nastavni sadržaji matematike i fizike u četvrtom razredu gimnazije pružaju dobre temelje za razumijevanje koncepta kvantnog računarstva, primjenjiv u jednostavnim primjerima i komplementaran s klasičnim računarstvom za kojeg su mnogi od njih već razvili interes. Potrebna znanja matematike su linearna algebra do razine matricnog računa, kompleksni brojevi u eksponencijalnom obliku i osnove teorije vjerojatnosti. Ovaj članak nema ambiciju pružiti uvod u kvantno računarstvo, već zainteresirati, ohrabriti i uputiti čitatelja na tečajeve koji će mu to pružiti, a primjereni su razini završnih razreda gimnazije. U ovom članku željeli bismo uputiti na mogućnosti korištenja emulatora kvantnih računala za stjecanje osnovnih znanja iz kvantnog računarstva. Projekte kvantnih emulatora sponzoriraju velike informatičke tvrtke i sveučilišta upravo radi promicanja što ranijeg zanimanja za kvantno računarstvo kako bi u budućnosti osigurali dovoljan broj stručnjaka nužan za održavanje zamaha u razvoju ove tehnologije.

Kvantno računarstvo je područje računarstva koje koristi principe kvantne fizike za obradu informacija. Umjesto klasičnih bitova, koji isključivo mogu imati vrijednosti 0 ili 1, kvantna računala koriste kvantne bitove, kubite, koji mogu *istovremeno biti u stanju 0 i 1* zbog kvantne pojave; superpozicije. Ova značajka, zajedno s kvantnom spregnutošću i kvantnim tuneliranjem, omogućava kvantnim računalima paralelno procesiranje tamo gdje klasična računala sekvencijalno koriste grananja i petlje.

Interes za kvantno računarstvo naglo se povećao sredinom devedesetih godina prošlog stoljeća nakon što je američki matematičar Peter Shor objavio algoritam za brzu faktORIZACIJU velikih brojeva na kojoj se temelji suvremena asimetrična kriptografija. Shorov algoritam koristi brzu Fourierovu transformaciju pri čemu se vrlo velik broj iteracija može istovremeno izvesti u tzv. supergustom kodiranju (engl. *superdense coding*) na kvantnom računalu. Unatoč tome što još uvijek nemamo uporabljivo kvantno računalno, postalo je izvjesno kako je asimetrična kriptografija ugrožena. O njoj danas ovisi razmjena ključeva u zaštićenoj komunikaciji, financijske transakcije kao i potvrda autentifikacije na internetu. Potaknut ovom spoznajom, američki Nacionalni institut za standarde (NIST) inicirao je još prije osam godina međunarodni natječaj za novi enkripcijski algoritam koji može odoljeti kvantnom računalu. Rezultat ovog natječaja su nedavno postavljeni novi standardi tzv. post-kvantne kriptografije (PQC) za enkripciju i digitalni potpis.

Kvantno računalno je, po svom značaju, u središtu kvantnih tehnologija [1]. Međutim bilo bi nepošteno tvrditi da je ono i njihovo ishodište jer su kvantni senzori, uređaji izuzetno velike osjetljivosti, postojali desetljećima ranije. Većina suvremenih autora slaže se oko podjele kvantnih tehnologija na tri glavna područja: kvantno računarstvo, kvantne

<sup>1</sup> Autor je docent na studijskim programima Vojno inženjerstvo i Vojno vođenje i upravljanje na Hrvatskom vojnom učilištu, Zagreb; e-pošta: mladen.viher@suradnik.unizg.hr

telekomunikacije i kvantne senzore [2]. Ponekad se kvantna kriptografija izdvaja kao zasebno područje, zbog svojeg izuzetnog značaja, no možemo ju promatrati unutar područja kvantnih telekomunikacija pa čak i kvantnog računarstva. Unutar svakog od ovih područja nailazimo na tehnološke subspecijalizacije.

Tako kvantno računarstvo obuhvaća skup tehnologija koje pružaju teorijsku podlogu, izradu računalnih komponenti, softvera i njihovo integriranje u primjenjivo kvantno računalno. U vrijeme pisanja ovog teksta naponi istraživača usmjereni su u stvaranje kvantnog računala sa što većim brojem kubita i u produženje razdoblja njihova koherentnog rada, tijekom kojeg je moguće iskoristiti stanje kvantne superpozicije. Unutar kvantnog računarstva razvijaju se tehnologije: kvantnih točki (*quantum dots*), kvantnog čipa, kvantne memorije, kvantnog računala i kvantnih simulacija, odnosno programiranja.

Kvantne telekomunikacije, uključimo li u njih i kvantnu kriptografiju, su već djelomično primijenjene tehnologije. Elektronički i fotonički sklopovi temeljeni na kvantnim pojavama omogućavaju znatno brže, pouzdanije i sigurnije telekomunikacije. Kod prijenosa signala na velike udaljenosti radi ostvarenja kvantnih informacijskih mreža, uključujući kvantni internet, te signale je nužno pojačati i zadržati im koherentnost. Za to se razvijaju kvantne inačice mrežnih ponavljača i prespojnika. Kvantna kriptologija također je na samoj granici praktične primjene. Postavljeni su novi standardi za post-quantnu kriptografiju koji mogu odoljeti kvantnom računalu; FIPS 203/CRYSTALS-Kyber, FIPS 204/CRYSTALS'Dilithium i FIPS 205/SLH-DSA. Prvi je kriptografski standard koji će zamijeniti postojeći AES, a druga dva su algoritmi za digitalni potpis. Kvantna distribucija ključeva jedno je od najaktivnijih područja istraživanja kvantnih tehnologija. Ona omogućava dostavljanje kriptografskih ključeva javnim kanalima (npr. internetom) bez potrebe da se dvije strane fizički sastanu (npr. zamislite da prilikom svakog plaćanja putem interneta morate otići u banku po ključ, čemu onda zaštićena komunikacija?). Koristeći teorem nemogućnosti kvantnog kloniranja može se jamčiti da ključ nije tijekom puta bio presretnut i pročitao od treće strane. Jedna od usputnih tehnologija je i kvantno generiranje slučajnih brojeva (QRNG), primjenjiva u generiranju ključeva. Na kraju, kvantna računala moći će se uspješno koristiti u kriptanalizi koja često koristi "iscrpljivanje" mogućih kombinacija ključeva. Isto to su radile "Bombe" i "Collosusi" još u doba Alana Turinga, a mogućnosti kvantnih računala su pri tome neusporedivo veće.

Kvantni senzori su već danas zreli i većinom primijenjene tehnologije. Vrlo precizna mjerenja električnih i magnetskih polja koriste se u istraživanjima i visokim tehnologijama, na primjer: metoda ionskih klopki, Ramanova atomska interferencija, dušikove šupljine, atomizirane pare i supervodička kvantna interferencijska naprava (SQUID). Kvantni senzori koriste se u mjeriteljstvu i etaloniziranju (npr. kvantni satovi) omogućavajući za nekoliko redova veličina preciznija mjerenja u odnosu na klasične metode. Od novijih kvantnih senzora možemo navesti kvantni fotoakustički senzor, kvantne širokopojasne radio antene, kvantni radar i kvantni inercijski senzor. Ovaj kratak pregled kvantnih tehnologija naveli smo kao ilustraciju koliko je veliko područje u kojem se budući stručnjaci mogu razviti.

Kvantno računarstvo, kao i klasično računarstvo, bavi se hardverom i softverom. Bavljenje hardverom zahtijevat će primjenjiva znanja iz kvantne fizike koja se stječu tek na visokom učilištu. Unatoč tome, željeli bismo uputiti motivirane maturante na velike mogućnosti samoedukacije o kvantnim računalima kroz tečajeve Coursere ([www.coursera.org](http://www.coursera.org)), Khan Academy ([www.khanacademy.org](http://www.khanacademy.org)), Microsofta ([www.edx.org](http://www.edx.org)), IBM-a ([skillbuild.org](http://skillbuild.org)), CERN-a ([quantum.cern](http://quantum.cern)), Stanforda ([online.stanford.edu](http://online.stanford.edu)) i MIT-a ([www.classcentral.com](http://www.classcentral.com)). Nabrojanjem ovih nekoliko tečajeva mogućnosti samoedukacije nisu ni izbliza iscrpljene. To su samo neki od najboljih općenitih tečajeva o kvantnom računarstvu, a na specijalizirane tečajeve za kvantno programiranje uputit ćemo kasnije u

nastavku teksta. Također bismo skrenuli pozornost na, zasad, jedinstven udžbenik opće fizike za početne godine fakulteta (što znači i za motivirane srednjoškolce) koji već od prve stranice priprema studenta za koncepte kvantne fizike. Radi se o *A Radically Modern Approach to Introductory Physics* autora Davida J. Raymonda sa Sveučilišta u Novom Meksiku [3] koji započinje s valovima kako bi studenta što prije uveo u valno-čestičnu dvojnost. U njegovom pristupu se klasična mehanika, optika i toplina javljaju tek kasnije, kao pojave velikog mnoštva čestica. Udžbenik je besplatan, adresa s koje ga možete preuzeti je u popisu literature, a jedini veći nedostatak mu je amaterski prijelom i oprema.

Tablica 1. Subspecijalizacije u klasičnom i kvantnom računarstvu

| subspecijalizacija računalnih znanosti | klasično računarstvo                                                                                                     | kvantno računarstvo                                                                                                                                |
|----------------------------------------|--------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| teorijska razina                       | temeljna i primijenjena istraživanja u računarstvu uz primjenu matematike i teorijske fizike                             | razvoj matematičke i fizikalne osnove za primjenu u kvantnom računarstvu, npr. Shorov algoritam                                                    |
| fizička razina                         | konkretno ostvarenje poluvodičkih logičkih sklopova                                                                      | primijenjena kvantna fizika i kemija te napredni materijali za izradu kvantnih elemenata i čipova                                                  |
| osnovne logičke operacije              | programiranje procesora na razini mikroinstrukcija (npr. x86, ARM, RISC. . . ) i integracija u složenije logičke krugove | razvoj, izrada i programiranje kvantnog sklopovlja na najnižoj razini radi integracije u složenije sustave kvantnih računala i kvantnih mreža      |
| niža razina programiranja              | izravno programsko upravljanje integriranim krugovima, asemblersko programiranje (FASM, Watcom, NASM, VASM. . . )        | asemblersko programiranje kvantnih čipova (Quill, QASM, Blackbird. . . )                                                                           |
| visoka razina programiranja            | programiranje aplikacija uz pomoć viših programskih jezika; Python, C++ , Java, C#, . . .                                | programiranje u višem programskom jeziku prilagođenom kvantnim računalima: Q#, LispyQuant, Silq, Quipper, Qiskit, Cirq. . .                        |
| razina aplikacijskog programiranja     | rad s naprednim aplikacijama; npr. AutoCAD, CATIA, ArcGIS, LTSpice. . .                                                  | rad u namjenskoj aplikaciji (npr. za kvantnu kriptografiju, optimizaciju, strojno učenje) koja u radu koristi kvantno računalo i/ili kvantnu mrežu |

Složit ćemo se s primjedbom da kvantne tehnologije, a time i kvantno računarstvo, zahitjevaju solidna znanja iz matematike i fizike koja se stječu tek na prvim godinama visokog obrazovanja [4]. Međutim, smatramo da se unutar subspecijalizacija kvantnog raču-

narstva mogu naći “sporedna vrata” za motiviranog srednjoškolca, posebno za onog koji je već stručan u programiranju. U tablici 1 naveli smo subspecijalizacije unutar računalnih znanosti, usporedno za klasično i kvantno računarstvo. Teorijske osnove kvantnog računarstva i kvantno sklopovlje svakako zahtijevaju dobro poznavanje kvantne fizike i više matematike. Međutim, programiranje na razini viših programskih jezika prilagođenih kvantnim računalima, poput: Q#, LispyQuanta, Silqa, Quippera, Qiskita ili Cirqa odličan su ulaz u tehnologije kvantnog programiranja, a time i u načela rada kvantnog računala čak i bez detaljnog poznavanja kako njihov hardver radi. Slično je i u klasičnom računarstvu u kojem već i srednjoškolac-programer može stvarati složene C++ aplikacije bez da u detalje poznaje kako se ponašaju elektroni pri prijelazu slojeva poluvodiča u čipovima. O oba slučaja to je već netko za njih napravio na nižim razinama programiranja.

Cijeli dosadašnji pregled kvantnih tehnologija i kvantnog računarstva unutar njih proveli smo kako bi ukazali na visoku razinu programiranja kao mogućnost da se kroz nju motivirani srednjoškolci uvedu u kvantno računarstvo. U tome veliku pomoć pružaju softverske tvrtke koje značajno ulažu u razvoj kvantnih tehnologija. Riječ je o vodećim tvrtkama koje moraju razmišljati unaprijed, nije dovoljno samo razviti tehnologije, već taj razvoj mora biti dugoročno održiv, a najvažnija komponenta te održivosti su upravo kvalificirani stručnjaci.

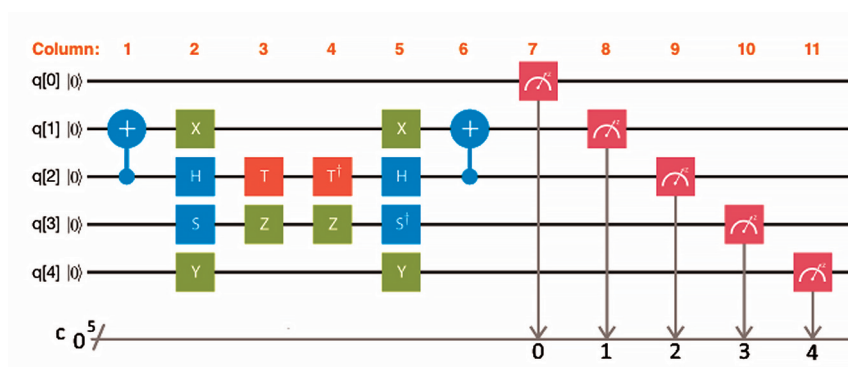
U tablici 2 dan je prikaz softverskih razvojnih sučelja za programske jezike visoke razine namijenjene za kvantna računala. Najbolju korisničku podršku, u vidu literature, popratnih tečajeva i dodataka imaju stranice velikih softverskih tvrtki: IBM (learning.quantum.ibm.com), Google (quantumai.google) i Microsoft (www.edx.org/learn/quantum-computing) tako da je bilo koja od njih dobar prvi izbor. Prethodno znanje programiranja je potrebno, a iskustvo s Pythonom je velika prednost. Polaznik tečaja će, već nakon prvih nekoliko cjelina, brzo razumjeti koncept kvantnog računarstva i moći će prepoznati razlike u odnosu na klasično računarstvo. Svi početni tečajevi kreću od neke inačice “Hello World!” programa koji se izvodi na emulatoru kvantnog računala. Emulacija je daleko sporija u odnosu na izvedbu programa na pravom kvantnom računalu, zbog toga IBM i Google nude mogućnost izvedbe programa na njihovim kvantnim računalima s tim što treba platiti za zakup vremena na kvantnom računalu. Za tom opcijom možemo posegnuti tek ukoliko imamo neki složeniji i potencijalno primjenjiv algoritam npr. u okviru nekog projekta ili znanstvenog rada.

Tablica 2. Softverska razvojna sučelja za programiranje kvantnih računala

| softversko razvojno sučelje | mrežna stranica                                                                                        |
|-----------------------------|--------------------------------------------------------------------------------------------------------|
| IBM Qiskit                  | <a href="http://www.ibm.com/quantum/qiskit">www.ibm.com/quantum/qiskit</a>                             |
| Google Cirq                 | <a href="http://quantumai.google/cirq">quantumai.google/cirq</a>                                       |
| Microsoft Azure QDK         | <a href="http://learn.microsoft.com/en-us/azure/quantum/">learn.microsoft.com/en-us/azure/quantum/</a> |
| ETH ProjectQ                | <a href="http://github.com/ProjectQ-Framework/ProjectQ">github.com/ProjectQ-Framework/ProjectQ</a>     |
| D-Wave Ocean                | <a href="http://github.com/dwavesystems/dwave-ocean-sdk">github.com/dwavesystems/dwave-ocean-sdk</a>   |
| Quantum Ket                 | <a href="http://github.com/quantum-ket/ket">github.com/quantum-ket/ket</a>                             |
| Quibo                       | <a href="http://qibo.science">qibo.science</a>                                                         |
| Xanadu Penny Lane           | <a href="http://www.xanadu.ai/products/pennylane/">www.xanadu.ai/products/pennylane/</a>               |
| Xanadu Strawberry Fields    | <a href="http://strawberryfields.ai">strawberryfields.ai</a>                                           |

Tečajeve za rad sa softverskim sučeljima za kvantna računala nude sve navedene softverske tvrtke. U obilju izbora dobrih tečajeva uputili bismo na one najbolje među njima. Na prvom mjestu bismo istaknuli IBM-ov Qiskit (learning.quantum.ibm.com) koji je

jako dobro podržan pratećim nastavnim materijalom i softverskim razvojnim okvirom. Temе kreću od osnova kvantnog računarstva i kvantnih logičkih krugova koji su izvedeni kako bi omogućili rad s kubitima. Već nakon nekoliko tema polaznik je u stanju analizirati kvantni logički krug i samostalno izvoditi njegove nadogradnje (slika 1).



Slika 1. Primjer jednog kvantnog logičkog sklopa, na lijevoj strani dijagrama je njegova konstrukcija, a simboli aparata sa skalom na desnoj strani predstavljaju mjerenja kad kvantne funkcije kolabriraju u rezultat, napravljeno u sklopu jedne od prvih lekcija u Qiskitu.

Qiskit nije namijenjen samo za stjecanje osnovnih znanja o kvantnim računalima jer pruža i mogućnost rada sa složenim kvantnim aplikacijama koje se odnose na realne probleme iz matematike, računarstva i prirodnih znanosti koje su primjerene razini visokog školovanja i inženjerskoj praksi, tako da je zanimljiv i dalje tijekom fakulteta i profesije. Cirq je Googleov programski okvir za razvoj kvantnih algoritama za rad s kvantnim računalima i simulatorima ([quantumai.google](https://quantumai.google)). Cirq je nešto tehnički zahtjevniji u odnosu na Qiskit, no uz dobro poznavanje Python-a tečaj se može lako slijediti (slika 2).

```
import cirq

# Pick a qubit.
qubit = cirq.GridQubit(0, 0)

# Create a circuit
circuit = cirq.Circuit(
    cirq.X(qubit)**0.5, # Square root of NOT.
    cirq.measure(qubit, key='m') # Measurement.
)
print("Circuit:")
print(circuit)

# Simulate the circuit several times.
simulator = cirq.Simulator()
result = simulator.run(circuit, repetitions=20)
print("Results:")
print(result)
```

Slika 2. Primjer jednostavnog koda u Cirqu sadrži sve osnovne komponente kvantnog programiranja; uvoz biblioteka, definiranje klase kubita, konstruiranje konkretnog kubita, višestruko mjerenje i ispis najvjerojatnijeg rezultata.

Autori ovog tečaja su više pažnje obratili na šum u kvantnim krugovima pa ponavljanje mjerenja i vjerojatnost dolaze više do izražaja. Azure Quantum je platforma koja kombinira pristup Microsoftovim kvantnim računalima i programskim alatima poput Q# jezika. U odnosu na Qiskit i Cirq, Azure je najsloženiji, ali i najnapredniji tečaj. Za sva tri tečaja zajedničko je što nude obilje edukativnog materijala i održavaju forum korisnika.

Suvremeni tehnološki razvoj, koji uključuje sve veći broj kvantnih tehnologija, vjerojatno će dovesti do potrebe da se u srednjoškolskoj nastavi fizike poveća udio tema o kvantnoj fizici. Također, kod nas još uvijek ne postoji prototip kvantnog računala što ne bi smjelo odvratiti interes od kvantnog programiranja jer postoji mogućnost izvođenja programa na emulatoru kvantnog računala. U svakom slučaju darovitim učenicima može se preporučiti financijski pristupačna i metodološki-stručno provjerena literatura [5] i u tekstu navedeni tečajevi o kvantnom računarstvu. Ono nije tehnološki hir i sigurno će biti tehnologija u punoj primjeni već za petnaestak godina. Nadamo se kako će ovaj pregled kvantnih tehnologija i kvantnog računarstva, s upućivanjem na samoedukaciju, biti koristan do uvođenja ovih tehnologija u kurikulum fizike i informatike.

## Literatura

---

- [1] S. GUNASHEKAR, C. D'ANGELO, I. FLANAGAN, D. MOTSI-OMOJIJADE, M. VIRDEE, C. FEIJAO, *Using Quantum Computers and Simulators in the Life Sciences*, RAND, 2022., dostupno na [https://www.rand.org/pubs/research\\_reports/RRA1899-1.html](https://www.rand.org/pubs/research_reports/RRA1899-1.html)
- [2] R. MÜLLER, F. GREINERT, *Quantum Technologies For Engineers*, De Gruyter, Berlin, 2024.
- [3] D. J. RAYMOND, *A Radically Modern Approach to Introductory Physics*, Physics Department, New Mexico Tech, 2001., dostupno na <http://kestrel.nmt.edu/~raymond/books/radphys/radphys.xhtml>
- [4] L. JEAGER, *The Second Quantum Revolution – From Entanglement to Quantum Computing and Other Super-Technologies*, Springer Nature, 2018.
- [5] *Simply Quantum Physics*, Dorling Kindersley Ltd., London 2022.