

KVANTNO PROGRAMIRANJE

ZA PROGRAMERE, INŽENJERE I FIZIČARE



```
qpe = QuantumCircuit(4, 2)
qpe.h(0)
qpe.cx(1, 2)
result = execute(qpe, backend)
```

Vladimir Randelović

KVANTNO PROGRAMIRANJE

Vladimir Randelović

Sadržaj

1	Uvod	26
1.1	Šta su kvantni računari.....	26
1.2	Analogija između klasičnog i kvantnog računara	27
1.2.1	Klasično kolo	27
1.2.2	Kvantno kolo	28
1.2.3	Kvantna moć	30
1.3	Da li će kvantni računari zameniti standardne PC računare	32
1.3.1	Kvantni računari nisu univerzalna zamena.....	32
1.3.2	Koegzistencija kvantnih i klasičnih računara	32
1.3.3	Tehnička ograničenja kvantnih računara.....	33
1.3.4	Zaključak	33
1.4	Kako se programiraju kvantni računari.....	33
1.4.1	Izvršavanje kvantnog algoritma unutar kvantnog kola	36
1.4.2	Kvantni računari na internetu i kladu	37
1.4.3	Zaključak	37
1.5	Računska složenost.....	37
1.5.1	Notacija velikog O	38
1.5.2	Klase složenosti u klasičnom računarstvu.....	38
1.5.2.1	Klasa P: Problemi rešivi u polinomijalnom vremenu	38
1.5.2.2	Klasa NP: Nedeterminističko polinomijalno vreme.....	38
1.5.2.3	NP-potpuni problemi (NP-Complete)	39
1.5.2.4	NP-teški problemi (NP-Hard)	40
1.5.2.5	PSPACE (polinomijalna memorija)	40
1.5.3	Klase složenosti u kvantnom računarstvu	41
1.5.3.1	BQP (Bounded-error Quantum Polynomial time).....	41
1.5.4	Zaključak	41
1.6	Superiornost kvantnih računara	42
1.6.1	Klasični i kvantni model računanja	42

1.6.2	Univerzalnost kvantnih računara	42
1.6.2.1	Klasična kontrola toka u kvantnim algoritmima	43
1.6.3	Kvantna supremacija.....	44
1.6.4	Algoritamska nadmoć: Šorov i drugi algoritmi	45
1.6.5	Kvantne simulacije — prirodna nadmoć.....	45
1.6.6	Kvantni računari u ekonomiji i poslovnom odlučivanju	46
1.6.7	Ograničenja kvantnih računara danas	46
1.6.8	Perspektive i zaključak.....	47
1.7	Kvantna i post-kvantna kriptografija	47
1.8	Strategija čitanja knjige	48
1.8.1	Brza strategija: Samo programiranje.....	49
1.8.2	Programerska strategija: Razumevanje kvantnih algoritama	50
1.8.3	Akadska strategija: Sistematsko razumevanje.....	51
1.8.4	Poslovna strategija: Strateško razumevanje	52
1.8.5	Filozofska strategija: Ontologija i interpretacije	53
1.9	Citiranje knjige.....	54
2	Kratka istorija kvantne fizike	55
2.1	Kvantni eksperimenti.....	55
2.2	Kvantna čudnost	56
2.3	Solvejeva konferencija	56
2.4	Kopenhaška interpretacija.....	57
2.5	Fon Nojmanova matematička formulacija	58
2.6	Ajnštajnov pogled.....	58
2.7	Šredingerova mačka	59
2.8	Bomova interpretacija – pilotski talasi	60
2.9	Everetova interpretacija – višestruki svetovi	61
2.10	Dejvid Dojč i susret sa Everetom	63
2.11	Šta je dovelo do kvantnih kompjutera	63
2.12	Prvi kvantni algoritam.....	65
2.13	Šorov algoritam	65
2.14	Realni kvantni kompjuteri.....	66

2.15	Kvantne klad platforme	67
3	Matematičke osnove kvantnog računarstva	68
3.1	Kompleksni brojevi	68
3.1.1	Definicija	68
3.1.2	Geometrijska interpretacija	69
3.1.3	Sabiranje i množenje	69
3.1.4	Konjugovano kompleksni broj	70
3.1.5	Modul kompleksnog broja	70
3.1.6	Eksponecijalna forma	70
3.1.7	Primena u kvantnom računarstvu	71
3.2	Vektori	71
3.2.1	Definicija vektora	71
3.2.2	Dimenzionalnost	72
3.2.3	Sabiranje i množenje skalarom	72
3.2.4	Normirani vektori (jedinčni vektori)	72
3.2.5	Unutrašnji (skalarni) proizvod	72
3.2.6	Baza vektorskog prostora	73
3.3	Kompleksni vektori	73
3.3.1	Šta je kompleksni vektor?	73
3.3.2	Zbir vektora i množenje skalarom	74
3.3.3	Konjugovani vektor i unutrašnji proizvod	74
3.3.4	Norma vektora	75
3.3.5	Ortogonalnost vektora	75
3.3.6	Hilbertov prostor	76
3.3.6.1	Osobine Hilbertovog prostora	76
3.3.6.2	Zašto je Hilbertov prostor važan u kvantnoj mehanici?	78
3.4	Matrice	78
3.4.1	Transponovane matrice	79
3.4.1.1	Osobine transponovanja	80
3.4.2	Ermitski operatori	80
3.4.2.1	Definicija ermitskih operatora	80

Sadržaj

3.4.2.2	Primer ermitske matrice	81
3.4.2.3	Osobine ermitskih operatora	81
3.4.2.4	Fizičko značenje	81
3.4.2.5	Zaključak	82
3.4.3	Normalni operatori	82
3.4.3.1	Definicija i osnovna svojstva	82
3.4.3.2	Spektralna teorema za normalne operatore	83
3.4.3.3	Veza sa kvantnim merenjem	83
3.4.3.4	Normalni operatori koji nisu ermitski	83
3.4.3.5	Zaključak	84
3.4.4	Unitarni operatori	84
3.4.4.1	Definicija	84
3.4.4.2	Primer unitarne matrice	84
3.4.4.3	Fizičko značenje	85
3.4.4.4	Osobine unitarnih operatora	85
3.4.4.5	Važnost u kvantnim algoritmima	85
3.4.5	Paulijeve matrice	86
3.4.5.1	Definicija	86
3.4.5.2	Osobine Paulijevih matrica	86
3.4.6	Razlika između ermitske i klasične adjungovane matrice	88
3.4.6.1	Ermitska adjungovana matrica	88
3.4.6.2	Klasična adjungovana matrica	89
3.4.7	Inverzne matrice	90
3.4.7.1	Inverzna matrica i adjungovana matrica	91
3.4.7.2	Linearne transformacije i inverzne matrice	91
3.5	Dirakova bra-ket notacija	92
3.5.1	Osnovni pojmovi	93
3.5.2	Primeri	93
3.5.3	Spoljni proizvod	94
3.5.4	Matrice u bra-ket notaciji	94
3.6	Unutrašnji proizvod vektora	94

3.6.1	Definicija.....	95
3.6.2	Osobine unutrašnjeg proizvoda	95
3.6.3	Fizička interpretacija	95
3.6.4	Norma i ugao između vektora	96
3.7	Spoljašnji proizvod vektora	96
3.7.1	Definicija.....	96
3.7.2	Primer.....	97
3.7.3	Projekcioni operatori	97
3.7.4	Fizička interpretacija	97
3.8	Tenzorski proizvod.....	98
3.8.1	Tenzorski proizvod vektora	98
3.8.2	Kronekerovo pravilo	99
3.8.3	Osobine tenzorskog proizvoda.....	99
3.8.4	Fizički značaj.....	99
3.9	Sopstveni vektori i sopstvene vrednosti	100
3.9.1	Definicija.....	100
3.9.2	Karakteristična jednačina	101
3.9.3	Uloga u kvantnoj mehanici	101
3.9.4	Ortogonalnost i normalizacija	101
4	Kvantni svet.....	102
4.1	Šta je čudno u kvantnom svetu	102
4.1.1	Interferencija i klasični pristup	103
4.1.1.1	Amplitude verovatnoće i kompleksni brojevi	105
4.1.1.2	Hajgensov princip	105
4.1.2	Eksperiment sa dva proreza	106
4.1.2.1	Double slit eksperiment sa laserskim zrakom.....	107
4.1.2.2	Double slit eksperiment sa pojedinačnim fotonima	107
4.1.3	Kvantni tester bombe	109
4.2	Ontologija kvantnog sveta.....	112
4.2.1	Teorija kolapsa talasne funkcije	113
4.2.2	Pilotski talasi (Bomova mehanika)	115

4.2.3	Everetova interpretacija više svetova.....	116
4.2.3.1	Problem održanja energije	119
4.2.3.2	Problem verovatnoće	119
4.2.3.3	Popularnost Everetove interpretacije	121
4.2.4	Zaključak	122
4.3	Osnovni kvantni koncepti	122
4.3.1	Kubit	122
4.3.1.1	Fizičke realizacije kubita	123
4.3.2	Kvantna stanja	124
4.3.2.1	Primer: Spin elektrona	125
4.3.3	Superpozicija i interferencija	126
4.3.3.1	Ulazak u interferenciju i izlazak iz interferencije.....	128
4.3.3.2	Superpozicija: više mogućnosti odjednom.....	131
4.3.4	Kvantni paralelizam i Everetova interpretacija	131
4.3.4.1	Kvantni paralelizam: "sve vrednosti odjednom"	132
4.3.4.2	Everetova interpretacija: svi svetovi postoje	133
4.3.4.3	Interpretacija i praksa.....	135
4.3.5	Entanglovanje	135
4.3.5.1	Suština entanglovanja.....	136
4.3.5.2	Merenje jednog — određuje drugo.....	136
4.3.5.3	Everetova interpretacija entanglovanja	137
4.3.6	Problem merenja	138
4.3.6.1	Matematika idealnog merenja	140
4.3.7	Nemogućnost kloniranja kvantnih informacija	140
4.3.7.1	Nemogućnost kloniranja punog kvantnog stanja	141
4.3.7.2	Posledice teoreme o nemogućnosti kloniranja.....	142
4.3.8	Hajzenbergov princip neodređenosti.....	142
4.3.8.1	Suština principa	143
4.3.8.2	Šta neodređenost nije	143
4.3.8.3	Talasna osnova.....	143
4.3.8.4	Kvantna intuicija	146

4.3.9	Bornovo pravilo i verovatnoća	146
4.3.10	Šredingerova jednačina	148
4.3.10.1	Kvantno stanje Ψ	148
4.3.10.2	Evolucija kvantnog sistema	148
4.3.10.3	Opservable i proces merenja	150
4.3.10.4	Šredingerova jednačina i kvantno programiranje	151
5	Kvantna kola	153
5.1	Klasična logička kola	154
5.1.1	NOT kolo	154
5.1.2	AND kolo	156
5.1.3	OR kolo	158
5.1.4	XOR kolo	160
5.1.5	Univerzalna logička kola	161
5.1.5.1	NAND kolo	162
5.1.5.2	Realizacija logičkih kola pomoću NAND kola	162
5.1.5.3	Univerzalnost u kvantnom svetu	163
5.1.6	Klasična logička kola nisu reverzibilna	163
5.1.6.1	Značaj reverzibilnosti u kvantnom svetu	164
5.1.6.2	Fizički aspekt reverzibilnosti i Landauerov princip	165
5.2	Kubit	166
5.2.1	Prednosti kubita	167
5.2.2	Matematičko predstavljanje kubita	167
5.2.2.1	Kompleksna amplituda	168
5.2.3	Blohova sfera	168
5.2.3.1	Klasična stanja	169
5.2.3.2	Stanja u superpoziciji	170
5.3	Globalna i relativna faza	172
5.4	Q-sfera	173
5.4.1	Primer čitanja Q-sfere	174
5.5	Kvantni gejtovi	175
5.5.1	Paulijeva grupa gejtova	176

5.5.1.1	Pauli X-gejt.....	177
5.5.1.2	Pauli Y-gejt.....	177
5.5.1.3	Pauli Z-gejt.....	178
5.5.2	Adamarov gejt (H-gejt)	178
5.5.3	S-gejt.....	180
5.5.4	T-gejt	180
5.5.5	CNOT-gejt	181
5.5.5.1	CNOT i entanglovanje 2 kubita	182
5.5.5.2	CNOT liči na merenje.....	182
5.5.6	Univerzalni kvantni gejtovi.....	183
5.5.6.1	Klifordova grupa gejtova	183
5.5.6.2	H-gejt i T-gejt	183
5.5.6.3	Definisanje kvantne univerzalnosti.....	184
5.5.6.4	Standardni univerzalni skup: {H, T, CNOT}.....	184
5.5.6.5	Uloga Tofoli-gejta.....	185
5.6	Kvantna logička kola	187
5.6.1	Kvantno kolo za negaciju kubita: X-gejt	187
5.6.2	Kvantno XOR kolo.....	188
5.6.3	Kvantno AND logičko kolo.....	191
5.6.4	Kvantno OR logičko kolo.....	193
6	Osnovni mehanizmi kvantnih kola	195
6.1	Superpozicija.....	195
6.1.1	Transformacija Z-gejta u X-gejt.....	200
6.1.2	Nejednaka superpozicija	201
6.1.2.1	Primena X-gejta u slučaju nejednake superpozicije.....	202
6.1.3	Generisanje prave slučajnosti	203
6.1.4	Više kubita – više slučajnosti	204
6.2	Entanglovanje	204
6.2.1	Definicija entanglovanja iz ugla programera	204
6.2.1.1	Entanglovanje nasuprot klasične korelacije	205
6.2.2	Kvantno kolo za kreiranje entanglovanja	205

6.2.2.1	Evolucija stanja	205
6.2.2.2	Rezultat	207
6.2.3	Belova stanja	208
6.2.4	Intuitivno razumevanje entanglovanja	208
6.3	Kvantna crna kutija	209
6.3.1	Mikrokontroler kao klasična crna kutija	209
6.3.2	Osnovna ideja kvantnog orakla	210
6.3.3	Kako funkcioniše kvantni orakl	210
6.3.3.1	Kvantni orakl kod Dojčovog algoritma	211
6.3.3.2	Konstantna funkcija	212
6.3.3.3	Balansirana funkcija	213
6.4	Fazni povratni efekat	217
6.4.1	Matematički pristup faznom povratnom efektu	218
6.4.2	Everetov pristup faznom povratnom efektu	220
6.4.3	Fazni povratni efekat kada ciljni kubit nije u superpoziciji	223
6.4.4	Ukratko o faznom povratnom efektu	223
7	Programiranje Qiskit bibliotekom	226
7.1	„Little-endian“ redosled kubita u Qiskitu	226
7.2	Prvi kvantni program	228
7.3	Biblioteka quantum_utils	230
7.3.1	Metode za analizu stanja	231
7.3.1.1	get_state	231
7.3.1.2	get_full_state	232
7.3.1.3	print_state	233
7.3.1.4	get_probabilities	233
7.3.1.5	print_probabilities	234
7.3.1.6	get_fidelity	235
7.3.2	Metode za vizualizaciju	235
7.3.2.1	show_bloch_sphere	235
7.3.2.2	show_qsphere	237
7.3.2.3	show_qc	238

7.3.2.4	show_measurement.....	239
7.4	Pisanje kvantnog programa	240
7.5	Pristup kvantnim računarima putem IBM-a	244
7.6	Generalna struktura kvantnog programa	247
8	Kvantni algoritmi	249
8.1	Dojčov algoritam	249
8.1.1	Šta rešava Dojčov algoritam?	250
8.1.2	Kako algoritam radi?	250
8.1.3	Implementacija u Qiskit-u	253
8.1.4	Opis programa	254
8.1.4.1	Dojčov algoritam sa konstantnom funkcijom.....	254
8.1.4.2	Dojčov algoritam sa balansiranom funkcijom.....	255
8.1.5	Zaključak	257
8.2	Kvantna Furijeova transformacija.....	258
8.2.1	Klasična Furijeova transformacija	258
8.2.1.1	Digitalizacija analognog signala	260
8.2.2	Diskretna Furijeova transformacija (DFT)	262
8.2.2.1	Matematička definicija DFT-a.....	262
8.2.2.2	Primer DFT-a	263
8.2.2.3	Zaključak	265
8.2.3	Kvantna Furijeova transformacija.....	265
8.2.3.1	Definicija QFT	266
8.2.3.2	Primer QFT(101)	267
8.2.4	Kvantno kolo za QFT?	268
8.2.5	Enkodovanje binarnog broja u fazu.....	274
8.3	Inverzna Furijeova transformacija	275
8.3.1	Matematička definicija	276
8.3.2	Primena QFT^{-1}	276
8.3.3	Kvantno kolo za QFT^{-1}	277
8.4	Kvantna estimacija faze (QPE – Quantum Phase Estimation)	279
8.4.1	Uslovi za primenu QPE algoritma?	279

8.4.2	Estimacija faze T-gejta.....	281
8.5	Šorov algoritam.....	284
8.5.1	RSA enkripcija.....	284
8.5.2	Kako se enkriptuje poruka.....	285
8.5.3	Orbite i period modularne funkcije.....	287
8.5.3.1	Period modularne funkcije.....	288
8.5.3.2	Orbite modularne funkcije i dejstvo operatora U	289
8.5.3.3	Orbita početnog stanja.....	289
8.5.3.4	Unitarni operator U za kretanje po orbiti.....	290
8.5.3.5	Različite orbite modularne funkcije.....	291
8.5.3.6	Analogija sa 3x3 matricom.....	292
8.5.4	Kvantno određivanje perioda Šorovim algoritmom.....	292
8.5.4.1	Određivanje broja kubita po registrima.....	294
8.5.4.2	Inicijalizacija registara.....	295
8.5.4.3	Modularna eksponencijacija.....	296
8.5.4.4	Inverzna Furijeova transformacija u Šorovom algoritmu.....	309
8.5.4.5	Merenje i određivanje perioda.....	311
8.5.5	Faktorizacija i dekripcija.....	322
8.5.5.1	Faktorizacija broja N na osnovu perioda.....	322
8.5.5.2	Izračunavanje privatnog ključa.....	325
8.5.5.3	Dekripcija poruke.....	326
8.5.6	Sažetak postupka dekripcije RSA poruke.....	327
8.6	Kvantna teleportacija.....	329
8.6.1	Protokol teleportacije.....	330
8.6.2	Zaključak.....	338
9	Kvantno kolo uradi-sam.....	340
9.1	Teorijski koncept kvantnog kola uradi-sam.....	340
9.1.1	Koncept: Kubit kao putanja fotona.....	340
9.1.2	Komponente našeg kvantnog kola.....	340
9.1.3	Matematički opis eksperimenta: Korak po korak.....	342
9.1.4	Ekvivalentan Qiskit program.....	345

Sadržaj

9.2	Praktična realizacija kvantnog kola	347
9.2.1	Realizacija optičkog dela kvantnog kola.....	347
9.2.1.1	Potrebne optičke komponente:	347
9.2.1.2	Postavljanje komponenti	347
9.2.2	Realizacija hardvera uz pomoć Arduina.....	350
9.2.3	Arduino program	352
9.2.3.1	Objašnjenje Arduino programa	353
9.3	Kvantnomehanička interpretacija eksperimenta	356
9.3.1	Superpozicija stanja	356
9.3.2	Uloga X-gejtova.....	357
9.3.3	Interferencija verovatnoća	357
9.3.4	Uloga pomerača faze (Z-gejt)	358
9.3.5	Merenje i „kolaps“ talasne funkcije	359
9.3.6	Zašto je ovo važno?	359
Dodatak 1 – Kvantna teleportacija.....		360
Dodatak 2 – Koherentna dužina lasera		362
Literatura.....		364
Indeks		373

1 Uvod

Ova knjiga je namenjena pre svega programerima, inženjerima i naučnicima koji su zainteresovani da upoznaju oblast kvantnih računara. Osnovna namera je prikaz kvantnog računarstva na intuitivan način kako bi se čitaoci pripremili za novu revoluciju koja trenutno obećava promene, možda čak i veće i značajnije od bilo koje tehnološke revolucije do sada. Ova knjiga trebalo bi da objasni zbog čega je najavljena revolucija toliko velika i na koji način nam kvantni svet pruža mogućnosti koje ne mogu ni da se zamisle iz ugla bilo koje klasične tehnologije.

Cilj knjige je:

1. **Prikaz i razumevanje kvantnog računarstva na intuitivan način.**

Dugi niz godina u kvantnoj fizici je važno pravilo „čuti i računaj“. Ovo pravilo obeshrabrivalo je mnoge naučnike i inženjere da razumeju suštinu kvantne fizike, a sva kvantna predviđanja i izračunavanja rađena su isključivo putem matematičkih formula. Ovo je sprečavalo mnoge istraživače da na intuitivan način pristupe kvantnom programiranju. Naravno da su koncepti kvantnog sveta i dalje misteriozni i da ne postoji potpuno slaganje među naučnicima o jedinstvenoj interpretaciji kvantnih fenomena, ali svejedno, ova knjiga objašnjava kvantni svet uz pomoć dijagrama i realnih kvantnih programa koji prezentuju kvantni paralelizam i omogućuju intuitivno, a ne samo matematičko, razumevanje kvantnog sveta.

2. **Upoznavanje samo sa neophodnim matematičkim alatom.**

Iako je akcenat knjige na intuitivnom razumevanju, svi kvantni algoritmi koriste matematičke alate kako bi modelovali kvantne procese pa ih je neophodno razumeti do određenog nivoa. U ovoj knjizi selektovana su samo važna poglavlja linearne algebre koja su neophodna za razumevanje i modelovanje ovih procesa. Matematički jezik verovatno je najjednostavniji način da se opišu stanja kvantnih kola, a istovremeno predstavlja i vid komunikacije koji dobro razumeju svi ljudi koji se bave ovom vrstom programiranja. Zbog toga je određen stepen matematike ipak neophodan.

1.1 Šta su kvantni računari

Najjednostavnije rečeno, kvantni računari su uređaji koji koriste kvantne efekte, pre svega superpozicije i entanglovanja, kako bi vršili različite proračune. Za razliku od klasičnih računara, koji koriste bitove kao osnovne jedinice informacija, kvantni računari koriste kvantne bitove ili kubite. I upravo u kubitima leži njihova moć.

Vrlo bukvalno možemo da kažemo da se čini da kubiti nisu sa ovog sveta pošto je njihovo ponašanje potpuno različito od svega na šta smo navikli. Ključ razumevanja kvantne prednosti upravo je u razumevanju načina na koji funkcionišu kubiti.

Na samom početku važno je shvatiti da je svet koji naša čula vide samo delić ukupne realnosti. Čula nas sprečavaju da vidimo širu sliku, ali nam zato to omogućavaju različiti kvantni eksperimenti.

Upravo zahvaljujući ovim eksperimentima uočeni su potpuno neverovatni fenomeni iz ugla gledanja na koji smo navikli. Na primer, u klasičnom svetu, potpuno je neshvatljivo da jedan elektron može da se nađe na dva mesta istovremeno ili da istovremeno ima dva spina (spin gore $\uparrow$ i spin dole $\downarrow$). Kada govorimo o postojanju jednog elektrona na dva mesta, onda ne mislimo da nam se čini da je elektron na dva različita mesta istovremeno, ili da, zbog nesavršenosti naše merne opreme, nismo u mogućnosti da tačno vidimo njegovu poziciju, već vrlo bukvalno mislimo da elektron može da postoji na više mesta ili u više stanja istovremeno. Možemo da zamislimo da, kada elektron uđe u superpoziciju spina gore i spina dole, da u stvari postoje dva elektrona (jedan sa spinom $\uparrow$ i drugi sa spinom $\downarrow$), pri čemu se ova dva elektrona nalaze u paralelnim svetovima, koji samo privremeno utiču jedan na drugi i kreiraju efekte interferencije koje možemo da detektujemo. Ovakvo stanje kvantnog objekta, kada se on nalazi u više stanja istovremeno, zove se **superpozicija**. Dodatni trik je u tome da, dok je kvantni objekat u superpoziciji, mi možemo da vidimo efekte superpozicije i da ih koristimo za različita izračunavanja, ali da u trenutku kada želimo da vidimo (da izmerimo) spin elektrona ($\uparrow$ ili $\downarrow$), onda uvek dobijemo jednu od ove dve moguće vrednosti – nikada obe istovremeno. Kvantni objekat koji može da bude u superpoziciji, na primer spina gore i spina dole, a koji se merenjem svodi na jednu od ove dve vrednosti, naziva se **kubit**.

Potpuno je jasno da ova ideja ne deluje logično i prihvatljivo. Ona će postati jasna tek tokom analize poglavlja 4 - Kvantni svet.

1.2 Analogija između klasičnog i kvantnog računara

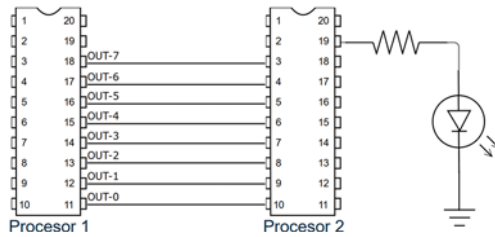
Osnovna prednost kvantnih računara ogleda se u mogućnosti da višestruka stanja (superpozicija) u kojima postoje kvantni objekti (npr. spin $\uparrow$ i $\downarrow$) budu iskorišćena za paralelno izračunavanje.

Kako bismo najbolje prikazali superiornost kvantnih računara, upoređićemo klasično (slika 1) i kvantno kolo (slika 2) sa sledećeg primera i pokušati da uočimo nadmoć superpozicije u kvantnom kolu u odnosu na klasičan mikroprocesorski sistem.

1.2.1 Klasično kolo

Na slici 1 je prikazano klasično kolo koje se sastoji od dva procesora povezanih tako što je 8 izlaznih pinova procesora 1 spojeno sa 8 ulaznih pinova procesora 2. Pinovi procesora funkcionišu tako što prisustvo napona od 0 V označava binarni broj 0, dok napon od 5 V označava binarni broj 1. Ovih 8 pinova mogu da generišu

ukupno $2^8=256$ različitih brojeva, odnosno cele brojeve od 0 (bin: 0000 0000) do 255 (bin: 1111 1111). Zamislimo da sistem funkcioniše tako da procesor 2 predstavlja crnu kutiju koja proverava da li na svojim ulaznim pinovima postoji tajni broj kako bi upalio LED preko svog izlaznog pina. Možemo da zamislimo i da, umesto LED-a, procesor 2 otključava neku bravu, a da neko želi da je provali. Kako god, ako je broj koji aktivira LED, na primer 142, odnosno binarna vrednost 1000 1110, tada je procesoru 2 potrebno dovesti navedeni binarni broj na ulazne pinove kako bi se aktivirao izlazni pin i upalio LED. U suprotnom slučaju LED je ugašen.



Slika 1. Klasično kolo sa mikroprocesorima

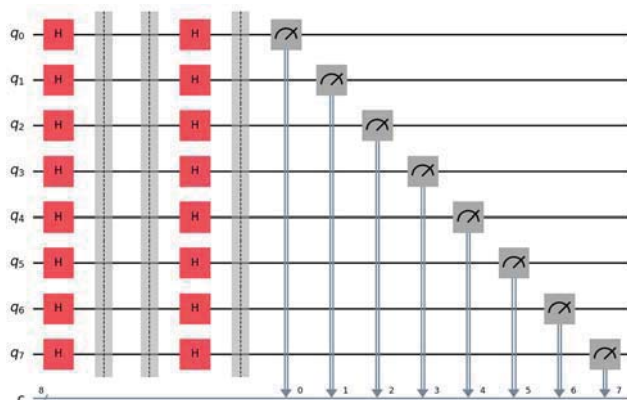
Zamislimo sada da ne znamo koji broj aktivira LED i da je potrebno da ga sami pronađemo. Pošto je procesor 2 za nas crna kutija i ne znamo tajni broj, neophodno je da redom menjamo sve moguće brojeve kako bismo videli koji od njih aktivira LED. Dakle, morali bismo da počnemo od broja 0 i da ih redom menjamo do 255. U našem primeru, menjali bismo brojeve od 0 do 142. Ako pretpostavimo da provera svakog broja traje $1\mu s$, da bismo otkrili broj 142, bilo bi nam potrebno $142\mu s$ (142 milionita dela sekunde). Ovo je, naravno, jako brzo i ne bismo imali problem sa hakovanjem ovakvog sistema. Na različitim primerima ovakvih sistema morali bismo da u proseku proveravamo $256/2=128$ brojeva, odnosno, u proseku bismo trošili $128\mu s$.

Međutim, šta ako je potrebno pronaći tajni broj u registru koji ima 300 bitova. Koliko nam je tada potrebno vremena? Očigledno, da nam je, u najgorem slučaju, potrebno $2^{300} \mu s$, odnosno $2^{300} \mu s = 2^{300} \times 10^{-6} s \approx 6,46 \times 10^{76}$ godina. Poređenja radi, starost univerzuma je oko $1,38 \times 10^{10}$ godina, što znači da je vreme potrebno za razbijanje ove šifre oko 10^{66} puta duže od starosti svemira. Kvantni paralelizam omogućava da se ovakvo izračunavanje obavi mnogo brže što ćemo videti u sledećem odeljku.

1.2.2 Kvantno kolo

Pogledajmo šta se dešava u slučaju kvantnog kola koje je prikazano na slici 2. Kvantno kolo takođe ima kvantni registar od 8 kubita. Na svaki od kubita primenjujemo kvantni H-gejt, poznat i kao Adamar gejt, po francuskom matematičaru Žaku Adamaru (Jacques Hadamard). Ovaj gejt dovodi kubite u stanje **superpozicije**, odnosno stanje koje podrazumeva da je kubit istovremeno i u stanju $|0\rangle$ i u stanju $|1\rangle$. Ovde je važno da razumemo da nije reč o tome da se ne zna u kom je stanju kubit, pa iz probabilističkih razloga kažemo da na njemu

možemo da sa određenom verovatnoćom izmerimo i 0 i 1, već je bukvalno reč o tome da se oba stanja istovremeno nalaze na kubit.



Slika 2. Kvantno kolo

Na primer, ako pod kubitom podrazumevamo elektron čiji spin označava stanje kubita, onda možemo da se dogovorimo da je stanje $|0\rangle$ reprezentovano spinom gore $|\uparrow\rangle$, dok je stanje $|1\rangle$ reprezentovano spinom dole $|\downarrow\rangle$. Kada ovakav kubit dovedemo u stanje superpozicije, primenom H-gejta, to bukvalno znači da taj elektron istovremeno ima i spin gore i spin dole. Bukvalno možemo da zamislimo da, umesto jednog elektrona koji ima ili spin gore $|0\rangle$ ili dole $|1\rangle$, sada imamo dva elektrona od kojih jedan ima spin gore, odnosno stanje $|0\rangle$, dok drugi ima spin dole, odnosno stanje $|1\rangle$. Kako dva elektrona, kada govorimo o samo jednom elektronu? Možemo, na primer, da zamislimo da se jedan elektron pretvara u dva elektrona koji se nalaze u različitim dimenzijama stvarnosti, odnosno, možemo reći u različitim „paralelnim univerzumima“. Kada god bi probali da izmerimo spin na elektronu, uvek bismo dobili ili spin gore ili spin dole, u zavisnosti od toga koji od ova dva „univerzuma“ se realizuje u našoj stvarnosti, ali, dok ne izmerimo spin, oba elektrona postoje u dve „paralelne stvarnosti“.

Ideju o paralelnim univerzumima koristićemo za sada samo kako bi čitaocu bilo jednostavnije da intuitivno razume dešavanja u kvantnom svetu. Ričard Fajnmen (Richard Feynman), jedan od najpoznatijih fizičara dvadesetog veka, kaže: „Mogu bezbedno da kažem da niko ne razume kvantnu fiziku“. Dakle, u ovom trenutku najbolje je koristiti ideju o paralelnim univerzumima kako bismo mogli da intuitivno razmišljamo o dešavanjima u kvantnom svetu. Međutim, kako je moguće da se jedan elektron pretvori u dva elektrona na različitim mestima, ili sa različitim spinovima, biće detaljnije analizirano u poglavlju 4.2 Ontologija kvantnog sveta.

Šta se dešava kada imamo situaciju sa 8 kubita q_0 - q_7 , koji su u stanju superpozicije? Mogli bismo da zamislimo da bukvalno postoji 256 paralelnih univerzuma i da, u svakom od njih postoji po jedna vrednost binarnog broja od 0000 000 pa do 1111 1111 (0 je spin gore, 1 je spin dole). Ovo je situacija koja se bukvalno i dešava u kvantnom kolu. Drugim rečima, dovođenjem registra od 8

kubita u superpoziciju, istovremeno smo stvorili 256 stanja. Unutar crne kutije (prostor u kvantnom kolu između dva vertikalna preseka), možemo da radimo različite operacije sa istovremenim vrednostima 0-255, pri čemu će se operacije odvijati u različitim paralelnim stvarnostima. Odnosno, koju god operaciju da primenimo u prostoru između dve vertikalne crte, ta operacija biće primenjena u svih 256 univerzuma u kojima postoje naših 8 kubita, pri čemu će, u svakom univerzumu, naš 8-kubitni registar biti u različitom stanju (stanja od 0-255). **Ova pojava predstavlja kvantni paralelizam i najvažniji je razlog superiornosti kvantnih računara!!!**

Posle drugog preseka (druge barijere na kvantnom kolu), ponovo primenjujemo H-gejtove, čime zatvaramo superpoziciju i vršimo sjedinjavanje paralelnih univerzuma u jedan univerzum. Sada smo spremni za merenje kubita koje će nam očitati jedan od brojeva od 0-255. Trik kod kvantnih računara je da, za vreme superpozicije (paralelizma), izvršimo paralelne operacije u različitim (paralelnim) univerzumima tako da na kraju, po povratku u jedan univerzum, budemo u stanju da očitamo određeni broj koji će predstavljati rezultat kvantnog izračunavanja.

Na ovaj način, mi bismo teorijski mogli da, u jednom ciklusu, pronađemo tajni kod sakriven u crnoj kutiji. U realnosti, ove operacije nisu jednostavne i zahtevaju puno analiza i različitih trikova, ali se cilj svodi na to da se u „paralelnim univerzumima“ izvrše različita izračunavanja na takav način da, po povratku u „naš“ univerzum, možemo da očitamo rezultate ovog izračunavanja.

1.2.3 Kvantna moć

Analogija između klasičnog i kvantnog računara predstavljena je sa ciljem intuitivnog razumevanja kubita. Za sada bi trebalo da se fokusiramo samo na intuitivno razumevanje, pri čemu treba imati u vidu da ćemo precizno znanje o principu rada kvantnog računara steći tek u narednim poglavljima.

Kod kvantnog računara, naš kvantni registar q_0 - q_7 možemo da postavimo u superpoziciju i da, umesto samo jednog broja, u jednom trenutku imamo istovremeno prisustvo svih mogućih brojeva, odnosno istovremeno prisustvo svih vrednosti od 0000 0000 do 1111 1111.

Da bismo shvatili koliko je velika moć kvantnih računara, moramo da se podsetimo da, na osnovu teorije informacija i Landauerovog zakona (5.1.6.2), svaka informacija ima materijalnu pozadinu, odnosno, materijalni nosač. Bilo da je to jednostavan mehanički prekidač koji može biti u stanju ON (stanje 1) ili OFF (stanje 0), ili da je u pitanju npr. elektronsko kolo poznato kao flip-flop memorija, koje ima mikro-dimenzije i nalazi se unutar memorijskog čipa, u oba slučaja ovi materijalni nosači čuvaju po jedan bit informacije (0 ili 1).

Klasičan 8-bitni registar iz našeg primera sastoji se iz 8 minijaturnih flip-flop memorijskih jedinica koje čuvaju 8 bitova. Čak i najmanje memorijske jedinice ugrađene u memorijske čipove visokog kapaciteta sastoje se iz velikog broja atoma i molekula. Ali, ako bismo zamislili da jednog dana ovladamo superiornom

tehnologijom koja će čuvati 1 bit klasične informacije u samo jednom atomu, to bi značilo da nam za jedan 8-bitni registar treba 8 atoma. Ovih 8 atoma u stanju su da čuvaju jedno 8-bitno stanje u jednom trenutku. Ali, ako bismo hteli da u istom trenutku baratamo sa svih 256 brojeva 8-bitnog registra, bilo bi nam potrebno $8 \times 256 = 2048$ bitova, odnosno atoma koji predstavljaju materijalne nosače ovih informacija. To je, naravno, mali broj atoma koji može da stane u jako malu zapreminu. Paralelno prisustvo svih vrednosti 8-bitnog registra važno je ako želimo da obavimo računicu koja je istovremena nad svim vrednostima jednog registra.

Međutim, analizirajmo sada kvantni računar koji ima npr. samo 300 kubita (očekuje se da bi ovaj broj logičkih kubita mogao da postane dostupan u bliskoj budućnosti). 300 kubita omogućava istovremeno prisustvo 2^{300} različitih 300-bitnih brojeva.

Ako bi jednu memorijsku lokaciju, kao što smo već rekli, predstavljao samo jedan atom, ovo bi značilo da nam je za reprezentaciju 2^{300} različitih stanja 300-bitnog registra potrebno $300 \cdot 2^{300}$ atoma. Čak i ako bismo jedan 300-bitni broj predstavili samo jednim atomom, za istovremeno enkodovanje 2^{300} različitih stanja ovog registra bilo bi potrebno 2^{300} atoma. Međutim, grube procene, bazirane na masi Zemlje i hemijskim elementima iz kojih je sastavljena, ukazuju na to da se na planeti Zemlji nalazi aproksimativno $1,33 \cdot 10^{50} \approx 2^{166}$ atoma, dok se u vidljivom Univerzuma nalazi oko $10^{80} \approx 2^{265}$ atoma.

Kako je onda moguće da jedan mali kvantni računar od 300 kubita, može da raspolaze sa 2^{300} kvantnih stanja u superpoziciji, svako od kojih doprinosi ukupnoj slici, odnosno ukupnom rezultatu algoritma. Postoji više interpretacija kvantne fizike koje pokušavaju da odgovore na pitanje šta se zaista događa u kvantnom svetu. Ove interpretacije obrađene su u poglavlju 4.2 Ontologija kvantnog sveta.

Analogija između različitih stanja memorije koju bismo čuvali u atomima i različitih stanja kubita nije u potpunosti ista. Ovde je prikazana ova vrsta analogije da bi se stekao intuitivni osećaj, iako razlika ima puno. Naime, atomi, ili druge memorijske jedinice, mogli bi da čuvaju vrednosti bitova kakve želimo. Međutim, registar kubita u superpoziciji uvek mora da ima sve vrednosti počev od 0000... pa do 1111... i mi ne možemo da biramo ove vrednosti.

Ono što je vrlo važno istaći je da, bez obzira na interpretaciju, matematički model koji predviđa rezultate kvantnih algoritama, radi nepogrešivo. „Čuti i računaj“ je ideja kojom se kaže da, ako nekome nije jasno kako u ontološkom smislu rade kvantni sistemi, onda to i nije mnogo važno – jedino što je važno je da znamo da primenimo matematički model kvantne fizike koji nam osigurava dobre rezultate. Međutim, cilj ove knjige je drugačiji. Cilj je, ne samo razumevanje matematičkog modela, već i intuitivno razumevanje koje omogućava sagledavanje algoritama i na logičkom nivou.

Ovde se već nazire neverovatna prednost kvantnih računara. Ono što se iz prethodnog primera moglo videti - da broj kvantnih stanja koje ima kvantni računar sa 300 kubita daleko nadmašuje ukupan broj atoma u vidljivom univerzumu - dovoljno govori o tome da kvantni svet otvara vrata nečem zaista velikom.

Za krajnjeg korisnika, kvantni računari će često biti "nevidljivi" — dostupni putem interneta ili kao deo kompleksnih informacionih sistema, bez potrebe da fizički poseduju kvantni računar kod kuće ili u kancelariji.

1.3.3 Tehnička ograničenja kvantnih računara

Trenutni kvantni računari su izuzetno osetljivi, zahtevaju ekstremno niske temperature, visoku stabilnost i kompletnu izolaciju od spoljašnjih uticaja. To ih čini nepraktičnim za svakodnevnu upotrebu izvan specijalizovanih laboratorija.

Takođe, kvantni računari su danas ograničeni brojem kubita, vremenom koherencije i greškama u proračunima, što dodatno potvrđuje da nisu blizu masovne komercijalne primene u širem smislu.

1.3.4 Zaključak

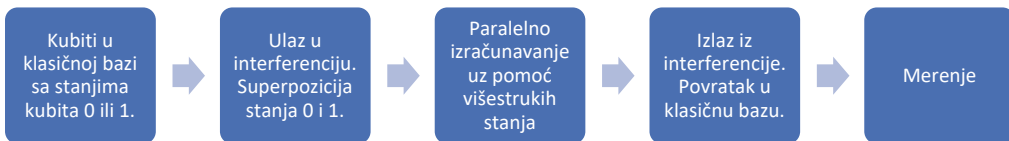
Kvantni računari neće zameniti standardne PC računare u skoroj budućnosti, niti postoji verovatnoća da će to ikada učiniti u potpunosti. Umesto toga, biće integrisani kao specijalizovani alati za rešavanje problema koje klasični računari ne mogu efikasno da obrade.

Svet budućnosti verovatno će kombinovati najbolje od oba sveta — stabilnost i univerzalnost klasičnih računara sa revolucionarnim mogućnostima kvantnog računanja.

1.4 Kako se programiraju kvantni računari

Programiranje kvantnih računara značajno se razlikuje od programiranja klasičnih računara. Dok smo kod standardnih računara navikli da pišemo kod u jezicima kao što su C, Python, Java, ili slično, kod kvantnih računara moramo razmišljati o dvojakoj strukturi programa.

Sa jedne strane, koristimo na primer Python i biblioteku Qiskit kako bismo, uz pomoć klasičnih alata na klasičnom računaru, dizajnirali kvantni program koji će se izvršavati unutar kvantnog računara. U suštini, Python program (program 1) koristimo da generišemo kvantno kolo sa slike 4. Najveći problem predstavlja upravo ovaj korak – dizajn kvantnog kola. Kada dizajniramo samo kvantno kolo, uglavnom vodimo računa da to kolo funkcioniše u sledećim koracima (slika 3) kako bismo mogli da što bolje iskoristimo prednosti kvantnog paralelizma.



Slika 3. Princip rada kvantnih programa

Kao što smo prethodno rekli, programiranje kvantnog računara odvija se u dva koraka:

1. Generisanje kvantnog kola klasičnim programskim jezicima

U ovom koraku koristi se klasičan programski jezik (npr. Python sa Qiskit bibliotekom) da bi programskim putem generisali kvantno kolo. Iako je program klasičan, unutar sebe on definiše kubite i kvantne gejtove koji, u principu, prate korake sa slike 3.

Python

```
import math
import quantum_utils as q
from qiskit import QuantumCircuit

# Definisanje kvantnog kola sa dva kubita i dva klasična bita
qc = QuantumCircuit(2, 2)
qc.reset([0, 1])
qc.barrier()
q.show_bloch_sphere(qc)

# Uvođenje u superpoziciju
qc.h(0)
qc.h(1)
qc.barrier()
q.show_bloch_sphere(qc)

# Izračunavanje u paralelnom režimu superpozicije
qc.z(1)
qc.t(0)
qc.barrier()
q.show_bloch_sphere(qc)

# Izlaz iz superpozicije i povratak u klasičnu bazu
qc.h(0)
qc.h(1)
qc.barrier()
q.show_bloch_sphere(qc)

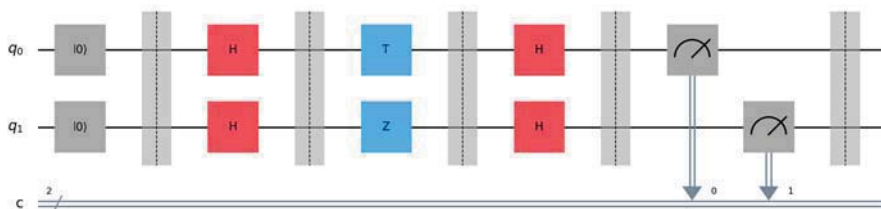
# Merenje
qc.measure(0, 0)
qc.measure(1, 1)
qc.barrier()
q.show_qc(qc)
q.show_measurement(qc)
```

Program 1. Python program za generisanje jednostavnog kvantnog kola

2. Kvantno kolo koje izvršava kvantni algoritam

Kvantni program izvršava se na kvantnom računaru postavljanjem određenog broja kubita i njihovom manipulacijom uz pomoć različitih kvantnih gejtova.

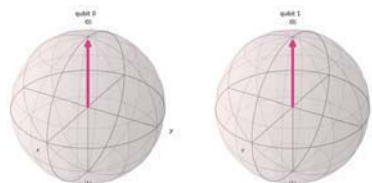
U svakom slučaju, da bi kvantni računar mogao da radi, prvi korak je da, na osnovu problema, dizajniramo kvantno kolo (eng. *quantum circuit*). Slika 4 daje primer jednostavnog kvantnog kola koje možemo da iskoristimo da steknemo uvid u njihovu tipičnu strukturu. Kvantno kolo predstavlja niz kvantnih operacija koje se primenjuju nad definisanim kubitima.



Slika 4. Primer kvantnog kola

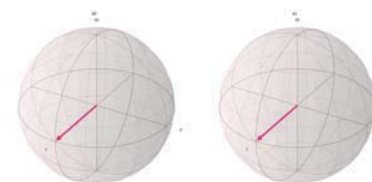
1. Inicijalizacija

Kvantno kolo sa slike otpočinje postavljanjem kubita u stanje $|0\rangle$ (generalno je moguća je bilo koja kombinacija $|0\rangle$ i $|1\rangle$).



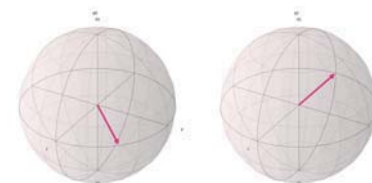
2. Ulaz u superpoziciju

Ovo je stanje u kojem kubiti imaju istovremeno stanja $|0\rangle$ i $|1\rangle$. Odnosno, trenutak kada npr. elektron istovremeno ima spin gore $\uparrow$ i spin dole $\downarrow$. Ovo je trenutak kada počinje kvantni paralelizam i kada počinju interferencioni efekti.



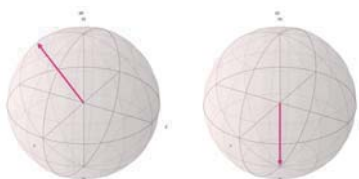
3. Kvantni paralelizam

Izvršavanje nekog od algoritama za izračunavanje za vreme dok se kubiti nalaze u superpoziciji. Drugim rečima, kvantni računari vrše izračunavanje koristeći višestruka stanja kvantnih objekata. Ova višestruka stanja, odnosno kvantni paralelizam, su ključ njihove nadmoći u odnosu na klasične računare. Najlakše je da zamislimo da ova paralelna stanja postoje u paralelnim svetovima samo za vreme dok su kubiti u superpoziciji.



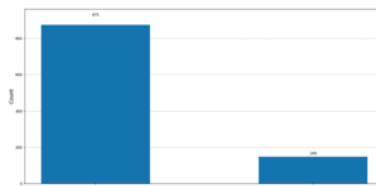
4. Izlaz iz superpozicije

Izlaskom iz superpozicije spajamo sve paralelne svetove u jedan (naš svet) i prelazimo iz superpozicionog u klasični režim rada, omogućavajući klasičnom svetu (našem univerzumu) da dobije uvid u ono što se prethodno dešavalo u kvantnom svetu (paralelnim univerzumima).



5. Merenje

Merenjem kubita nepovratno se prekida kvantni režim kola i iz kubita se dobijaju samo klasične vrednosti 0 ili 1.



1.4.1 Izvršavanje kvantnog algoritma unutar kvantnog kola

Kada je kvantno kolo definisano, ono se šalje kvantnom računaru, gde se stvarno izvršava, ili se šalje kvantnom simulatoru, koji simulira rad kvantnog računara. Kvantni algoritam je zapravo niz kvantnih operacija koje kolektivno koriste kvantne efekte poput superpozicije, interferencije i entanglovanja da bi rešile određene zadatke.

Primer poznatih kvantnih algoritama:

- Dojčov algoritam (prvi kvantni algoritam)
- Algoritam za Furijeovu transformaciju
- Algoritam za kvantnu estimaciju faze
- Šorov algoritam za faktORIZACIJU velikih brojeva
- Algoritmi za simulaciju kvantnih sistema u hemiji i fizici

U suštini, kvantno kolo koje definišemo u Python programu, predstavlja tehničku specifikaciju kvantnog algoritma. Nakon što se kolo, u formi klasičnog programa, pošalje na kvantni računar, kvantni algoritam se izvršava nad stvarnim kubitima unutar kvantnog računara.

Ako izvršavamo kvantno kolo na pravom kvantnom računaru, onda mu pristupamo preko interneta, tako što mu šaljemo Python program koji definiše kvantno kolo. Po slanju kvantnog programa kvantnom računaru, ostaje nam samo da sačekamo rezultate sa kvantnog računara, koje dobijamo putem interneta. Ukoliko koristimo simulator, tada simulaciju radimo na sopstvenom računaru uz pomoć Python-a i biblioteke Qiskit. Naravno, sopstvene računare možemo koristiti samo za probe algoritama i simulaciju malog broja kubita. Kod realnih potreba, koristimo veliki broj kubita i tada bi bilo neophodno pristupiti pravom kvantnom računaru preko interneta.

razvoja kvantnih računara, bezbednost široko korišćenih asimetričnih kriptografskih šema kao što su RSA i ECC biće ozbiljno ugrožena.

Upravo iz tog razloga, razmatra se pretnja poznata kao „Sačuvaj sada, dekriptuj kasnije“ (engl. Harvest now, decrypt later), u kojoj se, danas prikupljeni i sačuvani šifrovani podaci, mogu dekriptovati u budućnosti kada kvantni računari postanu dovoljno moćni. Zbog toga, prelazak na post-quantne algoritme već sada postaje strateški pravac i preporučena praksa u industriji.

Prvi i najpoznatiji protokol kvantne kriptografije, BB84, pokazuje kako se fundamentalna svojstva kvantnog merenja mogu iskoristiti za bezbednu razmenu ključeva, pri čemu svaki pokušaj prisluškivanja neminovno ostavlja detektabilan trag [13]. Takođe, kvantna razmena ključeva zasniva se na entanglovanim stanjima i Belovim nejednakostima, što je prvi put formalizovano u Ekertovom E91 protokolu [45].

Kao odgovor na pretnju koju kvantni algoritmi, pre svega Šorov algoritam, predstavljaju za savremenu kriptografiju, zasnovanu na faktorizaciji i diskretnom logaritmu, Nacionalni institut za standarde i tehnologiju (NIST) je 2024. godine finalizovao prve zvanične post-quantne kriptografske standarde, uključujući ML-KEM za razmenu ključeva, ML-DSA i SLH-DSA za digitalne potpise (National Institute of Standards and Technology [NIST], 2024a, 2024b, 2024c) [69, 70, 71].

1.8 Strategija čitanja knjige

Predložene strategije čitanja omogućavaju selektivno čitanje knjige iz različitih uglova, u zavisnosti od interesovanja i ciljeva čitaoca. Iako je za sveobuhvatno razumevanje kvantnog programiranja preporučljivo čitanje knjige od početka do kraja, u praksi je često korisno fokusirati se samo na određene aspekte uz pomoć odgovarajućih strategija čitanja.

Sledeća slika daje grafički prikaz sadržaja po različitim strategijama čitanja.



Slika 5. Poređenje algoritma čitanja knjige

1.8.1 Brza strategija: Samo programiranje

Čitaoci koji bi želeli da brzo nauče samo praktično kvantno programiranje, bez velike analize kvantnih algoritama, matematike i filozofije kvantnog sveta, trebalo bi da krenu sa ovom strategijom. Po završetku, mogu preći na programersku strategiju.

Vreme čitanja: 6-8 nedelja

Ciljna grupa Inženjeri i programeri koji žele što pre da počnu sa praktičnim kvantnim programiranjem, bez ulaženja u teorijske osnove, fiziku ili filozofiju.

Karakteristike strategije čitanja:

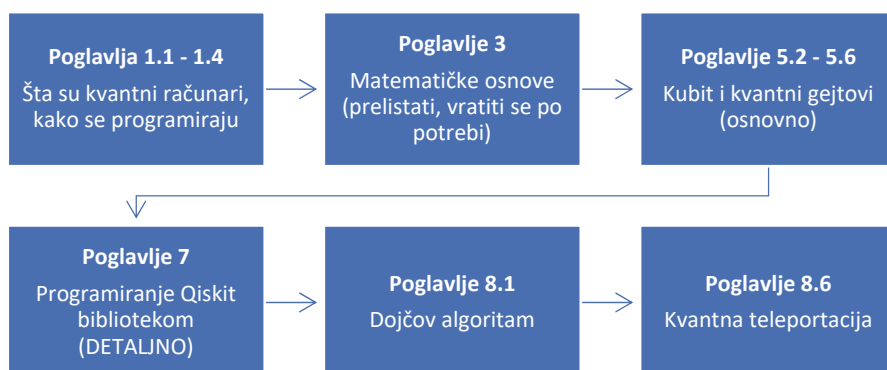
- Minimalna teorija, maksimalna praksa.
- Fokus na "kako" umesto "zašto".
- Direktan pristup programiranju.
- Preskakanje istorijskog i filozofskog konteksta.

Očekivano znanje nakon čitanja:

- Sposobnost pisanja osnovnih kvantnih programa u Qiskit-u.
- Razumevanje osnovnih kvantnih gejtova.
- Implementacija jednostavnijih kvantnih algoritama.

Nedostaci:

- Površno razumevanje teorijskih osnova bez dubljeg razumevanja načina na koji algoritmi funkcionišu.
- Teškoće pri samostalnoj modifikaciji složenijih algoritama.



Slika 6. Brza strategija čitanja knjige

1.8.2 Programerska strategija: Razumevanje kvantnih algoritama

Ova strategija pogodna je za ljude koji žele da steknu dublje razumevanje kvantnih algoritama bez velike analize filozofskih i istorijskih aspekata. Za još dublju analizu, pogodno je preći na Akademsku strategiju.

Vreme čitanja: 4-6 meseci

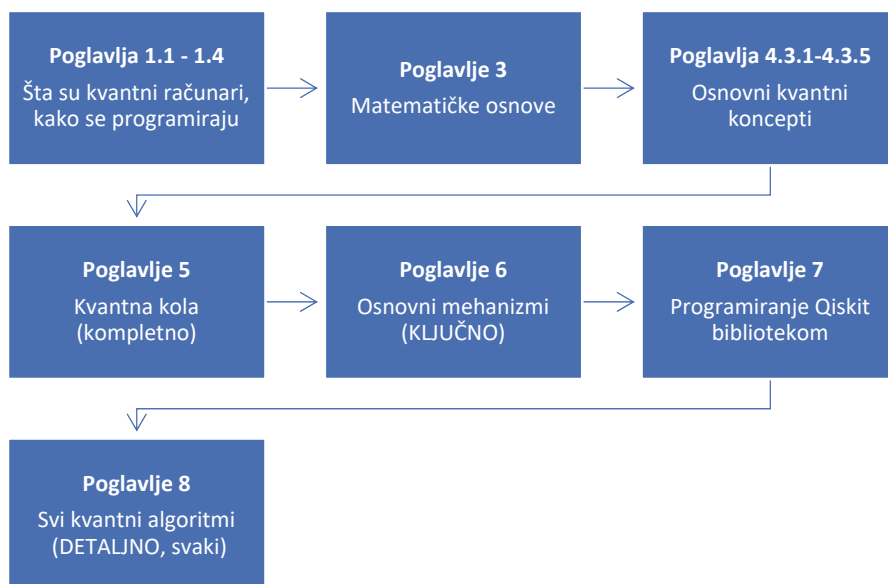
Ciljna grupa Inženjeri i programeri koji žele detaljno razumevanje svakog algoritma.

Karakteristike strategije čitanja:

- Detaljna analiza svakog kvantnog algoritma.
- Kombinacija teorije i prakse.
- Fokus i na „zašto“, a ne samo na „kako“ algoritmi rade.
- Kreativna primena znanja sa razumevanjem.

Očekivano znanje nakon čitanja:

- Sposobnost modifikacije i optimizacije kvantnih algoritama.
- Razumevanje konstrukcije algoritama i eksperimentisanje sa varijantama postojećih algoritama.



Slika 7. Programerska strategija čitanja knjige

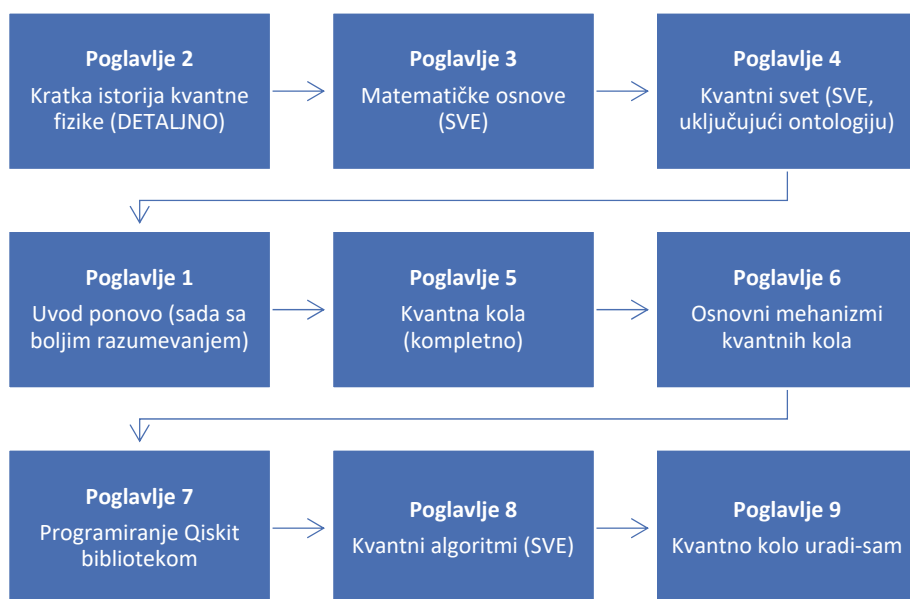
1.8.3 Akademska strategija: Sistematsko razumevanje

Uz pomoć akademske strategije čitanja, naučnici i studenti iz oblasti fizike i računarskih nauka mogu da steknu detaljan uvid u sve aspekte kvantnog programiranja koji su obrađeni u ovoj knjizi.

Vreme čitanja: 6 - 9 meseci

Ciljna grupa Studenti fizike, matematike, računarskih nauka koji žele duboko razumevanje kvantnog računarstva sa svim teorijskim osnovama.

- Karakteristike strategije čitanja:
- Sistematičan pristup.
 - Razumevanje matematike i fizike.
 - Potpuno čitanje knjige.
 - Uključuje sve istorijske i filozofske aspekte.
- Očekivano znanje nakon čitanja:
- Razumevanje osnova kvantnog računarstva.
 - Razumevanje predstavljenih kvantnih algoritama.
 - Sposobnost analize i konstrukcije algoritama.
 - Kritičko razumevanje ograničenja i mogućnosti.



Slika 8. Akademska strategija čitanja knjige

1.8.4 Poslovna strategija: Strateško razumevanje

Tehnički orijentisani poslovni ljudi koji se bave donošenjem odluka mogu da pronađu objašnjenja neophodna za razumevanje kvantnih tehnika, kao i da budu u stanju da razlikuju realistična od lažnih predviđanja vezanih za kvantne računare.

Vreme čitanja: 4 – 6 nedelja

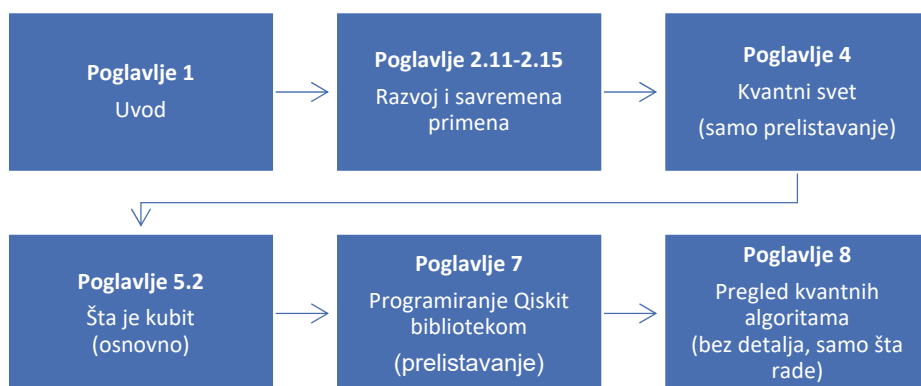
Ciljna grupa Menadžeri, donosioci odluka, investitori, konsultanti koji već imaju dovoljan nivo tehničkog znanja i koji žele da razumeju osnovne implikacije kvantnih računara u različitim poslovnim oblastima.

Karakteristike algoritma čitanja:

- Fokus na primenu i implikacije.
- Minimalno programiranje.
- Osnovno razumevanje mogućnosti i ograničenja.
- Strateška perspektiva.

Očekivano znanje nakon čitanja:

- Osnovno razumevanje gde i pod kojim uslovima kvantni računari mogu ponuditi prednost.
- Svesnost ograničenja kvantne tehnologije.
- Osnovno razumevanje bezbednosnih implikacija.
- Realistična očekivanja o kvantnim računarima.



Slika 9. Poslovna strategija čitanja knjige

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \quad T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

Pošto se kompleksna faza ne može generisati, skup $\{H, Tofoli\}$ nije univerzalan. Da bismo dobili univerzalan skup, možemo da dodamo još T-gejt koji sadrži kompleksnu fazu, što znači da bi skup $\{H, T, Tofoli\}$ bio univerzalni skup kvantnih kola.

5.6 Kvantna logička kola

U klasičnoj digitalnoj elektronici, logička kola poput NOT, AND i OR predstavljaju osnovne gradivne blokove za obradu informacija. Kvantna logička kola nastaju kao njihov pandan u kvantnom svetu, ali sa suštinskom razlikom: ona manipulišu kubitima, koji mogu biti u superpoziciji i međusobno entanglovani. Zbog toga, kvantna realizacija klasičnih logičkih operacija zahteva pažljivo korišćenje unitarnih gejtova i pomoćnih kubita, kako bi se očuvala reverzibilnost kvantne dinamike.

U ovom poglavlju analiziramo kako se klasične logičke operacije mogu implementirati u okviru kvantnih kola. Počecemo od najjednostavnijeg slučaja — negacije kubita (X-gejt). Zatim ćemo razmotriti kvantni analog XOR operacije i konstrukciju kvantnih AND i OR kola, uz objašnjenje kako se klasična logika realizuje u okviru fundamentalno reverzibilnog kvantnog formalizma.

5.6.1 Kvantno kolo za negaciju kubita: X-gejt

Kao što je već rečeno X-gejt vrši rotaciju oko X-ose na Blohovoju sferi. Najčešće se koristi da bi delovalo na kubite čije je stanje u računskoj bazi ($|0\rangle$ ili $|1\rangle$).

1. Definicija gejta:

Kvantni NOT ili X-gejt je analog klasične negacije. Njegova matrica je Pauli-X:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Imajući u vidu da se stanja iz računске baze predstavljaju kao vektori $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ i $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, dejstvo X gejta na osnovna stanja iz računске baze može se zapisati kao:

$$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

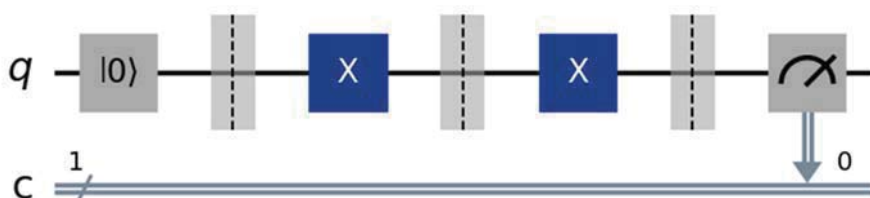
$$X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

2. Dvostruka negacija

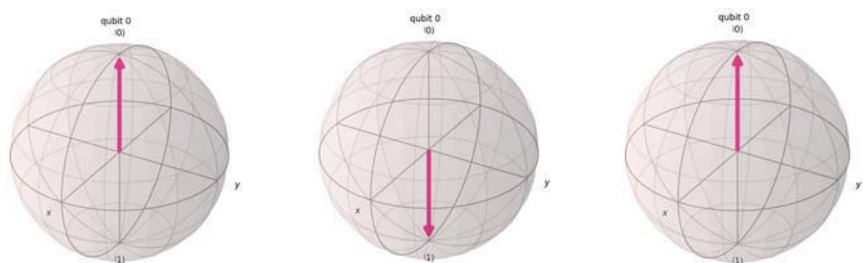
Ako isti kubit prođe kroz dva uzastopna X-gejta dešava se sledeće:

$$X^2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Drugim rečima, dvostruka primena X-gejta je u stvari matrica identiteta, odnosno, posle druge primene X-gejta, kubit se vraća u početno stanje. Ovaj postupak može se videti na realnom kvantnom kolu (slika 59).



Slika 59. Kvantno kolo sa dva X-gejta.



Početno stanje kubita
 $|0\rangle$.

Stanje kubita posle prvog
X-gejta je $|1\rangle$.

Stanje kubita posle
drugog X-gejta je $|0\rangle$.

5.6.2 Kvantno XOR kolo

Ovo kvantno kolo koristi dva kubita za ulaz i jedan klasičan bit za izlaz kako bi emuliralo ponašanje klasičnog XOR logičkog kola (slika 60). U suštini koristimo samo CX-gejt (CNOT-gejt), odnosno kontrolisani X-gejt (5.5.5), koji invertuje target kubit kada je kontrolni kubit u stanju $|1\rangle$.

1. Inicijalizacija ulaza

Kolo počinje sa dva kubita, q_0 i q_1 , koji su oba inicijalno u stanju $|0\rangle$.

- o Prvi ulaz je na kubit q_0 . Pošto su kubiti postavljeni u stanje $|0\rangle$, ako bismo želeli da q_0 bude jednak $|1\rangle$, potrebno je da na kubit q_0 dodamo X-gejt (NOT), čime se njegovo stanje menja iz $|0\rangle$ u $|1\rangle$.

- o Drugi ulaz je na kubit q_1 . Slično, ako želimo da q_1 umesto stanja $|0\rangle$ ima stanje $|1\rangle$, dodajemo jedan X-gejt.

Nakon ovog koraka, početno stanje sistema $|q_0, q_1\rangle$ tačno odgovara klasičnim ulaznim vrednostima (npr. za ulaze 1 i 0, stanje je $|10\rangle$).

2. XOR logika pomoću CNOT gejta

Centralni deo kola je CNOT (Controlled-NOT) gejt, gde je:

- o q_0 kontrolni kubit.
- o q_1 ciljani kubit.

CNOT gejt primenjuje X operaciju (NOT) na ciljani kubit (q_1) ako i samo ako je kontrolni kubit (q_0) u stanju $|1\rangle$. U nastavku je data analiza rada CNOT gejta:

- o Početno stanje $|00\rangle$: q_0 je $|0\rangle$. CNOT po definiciji ne radi ništa pošto je q_0 u stanju $|0\rangle$. Stanje ostaje $|00\rangle$.
- o Početno stanje $|01\rangle$: q_0 je $|0\rangle$. CNOT ne radi ništa. Stanje ostaje $|01\rangle$.
- o Početno stanje $|10\rangle$: q_0 je $|1\rangle$. CNOT se aktivira i primenjuje X-gejt na q_1 , menjajući ga iz $|0\rangle$ u $|1\rangle$. Finalno stanje je $|11\rangle$.
- o Početno stanje $|11\rangle$: q_0 je $|1\rangle$. CNOT se aktivira i primenjuje X-gejt na q_1 , menjajući ga iz $|1\rangle$ u $|0\rangle$. Finalno stanje je $|10\rangle$.

3. Merenje Rezultata

Na kraju, vršimo merenje samo drugog kubita (q_1) i rezultat smeštamo u klasični bit. Ako pogledamo stanje q_1 nakon primene CNOT gejta, vidimo da ono tačno odgovara XOR tablici istinitosti:

q_0	q_1	q_1 nakon CNOT	XOR rezultat
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	0

Sledeća slika prikazuje XOR kvantno kolo i stanja kubita u zavisnosti od različitih početnih vrednosti. Kao što se sa šeme kola može videti, kolo je reverzibilno, odnosno 2 ulazne vrednosti prevode se na dve izlazne vrednosti, na takav način da za svaku izlaznu vrednost možemo da odredimo inverznu funkciju i jednoznačno izračunamo ulazne vrednosti.

$0 \oplus 0 = 0$	Presek 1	Presek 2
Pesek: 1 2		
$1 \oplus 0 = 1$		
$0 \oplus 1 = 1$		
$1 \oplus 1 = 0$		

Slika 60. XOR kolo i stanja kubita za različite ulazne vrednosti

5.6.3 Kvantno AND logičko kolo

Ovo kvantno kolo koristi tri kubita za implementaciju AND logičkog kola. Dva kubita služe kao ulaz, dok treći služi kao izlaz.

1. Inicijalizacija ulaza i Izlaza

Kolo počinje sa tri kubita, q_0 , q_1 i q_2 , koji su svi inicijalno u stanju $|0\rangle$.

- o Ako bismo želeli da kubit q_0 ili q_1 imaju stanje $|1\rangle$, primenjujemo X-gejt (NOT), čime se njegovo stanje menja iz $|0\rangle$ u $|1\rangle$.
- o Kubit q_2 se ostavlja u stanju $|0\rangle$ i služi kao **radni (ancilla) kubit** na kojem se akumulira rezultat operacije.

2. AND logika pomoću Tofoli (CCX) gejta.

Tofoli gejt (CCX-gejt) u suštini je kontrolisani NOT gejt kod kojeg su kubiti q_0 i q_1 kontrolni kubiti, dok je kubit q_2 ciljni kubit. Kontrolni kubiti implementiraju klasičnu AND logiku tako da samo ako su oba kubita u stanju $|1\rangle$, Tofoli gejt primenjuje X (NOT) operaciju nad ciljnim kubitom. Drugim rečima, ciljni kubit q_2 biće invertovan samo ako su oba kubita q_0 i q_1 u stanju $|1\rangle$, dok u bilo kom drugom slučaju q_2 ostaje nepromenjen.

Ovo ponašanje direktno implementira AND logiku:

- o Početno stanje $|000\rangle$: Pošto oba kontrolna kubita nisu $|1\rangle$, Tofoli ne radi ništa. Stanje ostaje $|000\rangle$.
- o Početno stanje $|010\rangle$: Kontrolni kubiti nisu u stanju $|11\rangle$. Tofoli ne radi ništa. Stanje ostaje $|010\rangle$.
- o Početno stanje $|100\rangle$: Kontrolni kubiti nisu u stanju $|11\rangle$. Tofoli ne radi ništa. Stanje ostaje $|100\rangle$.
- o Početno stanje $|110\rangle$: Oba kontrolna kubita su $|1\rangle$. Tofoli se aktivira i primenjuje X na q_2 , menjajući ga iz $|0\rangle$ u $|1\rangle$. Finalno stanje je $|111\rangle$.

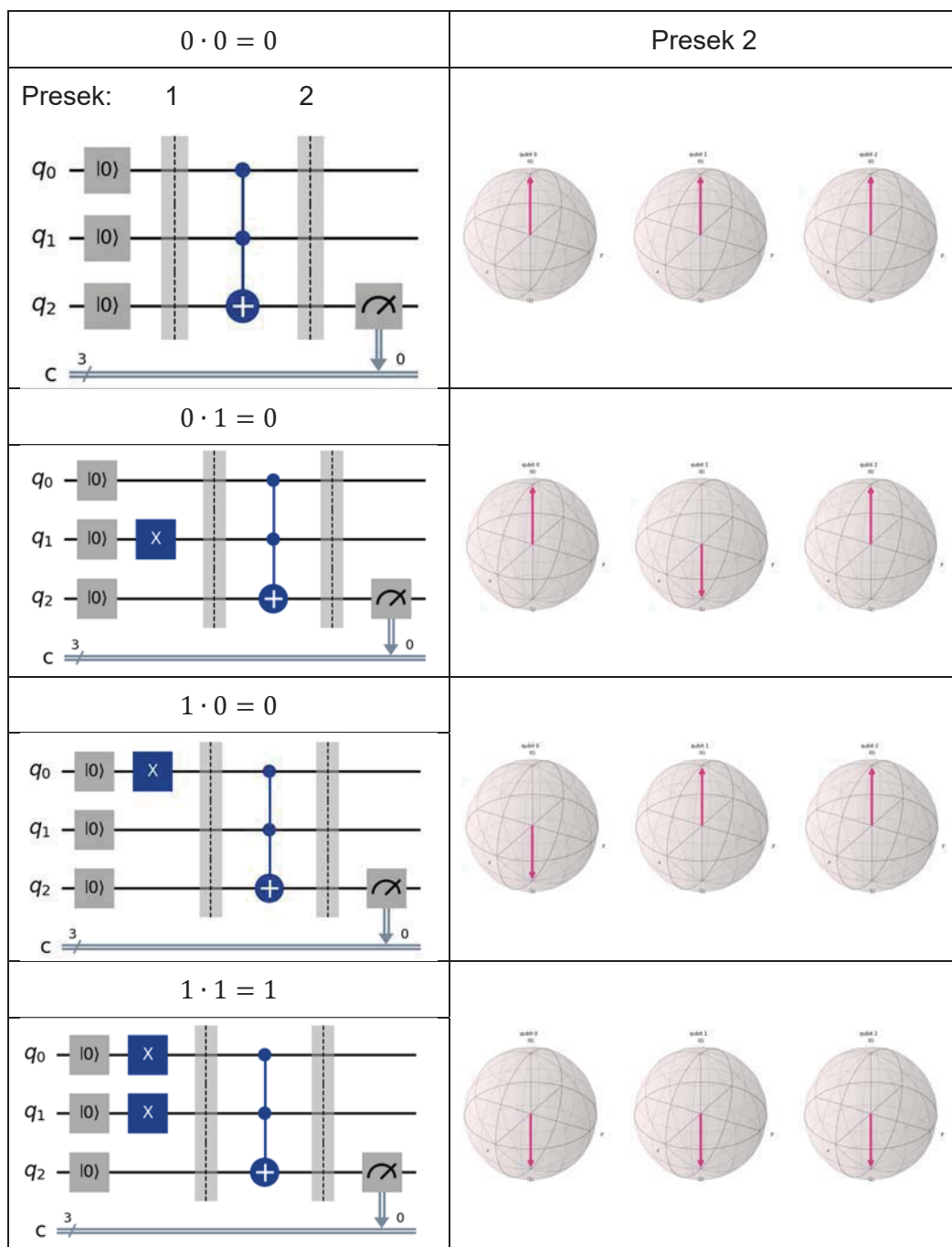
3. Merenje Rezultata

Na kraju, vršimo merenje samo trećeg kubita (q_2), jer on nosi rezultat AND operacije. Ako pogledamo stanje q_2 nakon primene Tofoli gejta, vidimo da ono tačno odgovara AND tablici istinitosti:

q_0	q_1	q_2 nakon CCX	AND rezultat
0	0	0	0
0	1	0	0
1	0	0	0
1	1	1	1

Tabela 4. Logika kvantnog AND kola

Slika 61 prikazuje AND kvantno kolo i stanja kubita u zavisnosti od različitih početnih vrednosti. I ovo kolo, kao i sva ostala kola, mora da bude reverzibilno.



Slika 61. AND kolo i stanja kubita za različite ulazne vrednosti

5.6.4 Kvantno OR logičko kolo

Da bismo napravili kvantno OR kolo, primenićemo matematičku logiku sa dva CNOT gejt i jednim Tofoli (CCX) gejtom. Kolo počinje sa tri kubita, q_0 , q_1 i q_2 , koji su svi inicijalno u stanju $|0\rangle$.

- Ako bismo želeli da q_0 ili q_1 postavimo u stanje $|1\rangle$, dovoljno je da primenimo X-gejt.
- Kubit q_2 se ostavlja u stanju $|0\rangle$ i služi kao izlazni kubit.

Nakon inicijalizacije, a pre CX i Tofoli gejtova, stanje sistema $|q_0 q_1 q_2\rangle$ tačno odgovara klasičnim ulaznim vrednostima (npr. za ulaze 1 i 0, stanje je $|100\rangle$).

Centralni deo kola koristi trik zasnovan na identitetu iz Bulove algebre:

$$A \vee B = (A \oplus B) \oplus (A \wedge B)$$

$$q_0 \vee q_1 = (q_0 \oplus q_1) \oplus (q_0 \wedge q_1)$$

Kolo implementira ovaj identitet u tri koraka, akumulirajući rezultat na izlaznom kubit q_2 :

1. Prvi CNOT: Primenjuje se CNOT sa q_0 kao kontrolom i q_2 kao metom. Ovo kolo upisuje stanje q_0 na q_2 . Ako je q_0 bio $|1\rangle$, q_2 postaje $|1\rangle$.
2. Drugi CNOT gejt: Odmah zatim, primenjuje se CNOT sa q_1 kao kontrolom i q_2 kao metom. Ovo efektivno izvršava operaciju XOR sa prethodnim stanjem. Stanje q_2 sada postaje q_0 XOR q_1 .
3. Tofoli gejt: Na kraju, primenjuje se Tofoli (CCX) gejt sa q_0 i q_1 kao kontrolama i q_2 kao metom. Ovaj gejt implementira q_0 AND q_1 i primenjuje XOR na trenutno stanje q_2 .

Nakon ova tri koraka, konačno stanje kubita q_2 je $(q_0 \text{ XOR } q_1) \text{ XOR } (q_0 \text{ AND } q_1)$, što je matematički ekvivalentno operaciji q_0 OR q_1 .

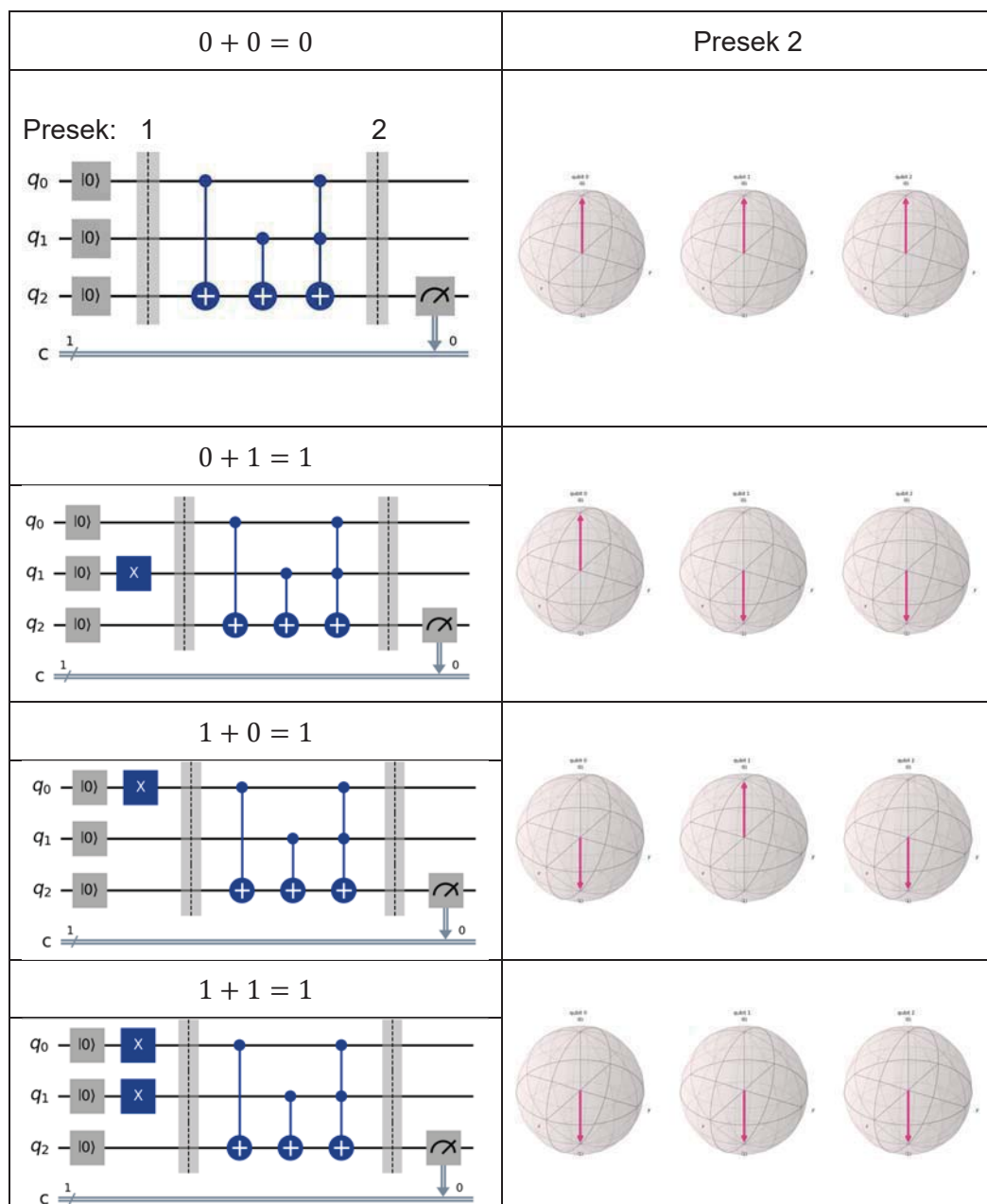
4. Merenje rezultata

Na kraju, vršimo merenje samo trećeg kubita (q_2), jer on nosi konačni rezultat OR operacije. Analizom stanja q_2 nakon sekvence gejtova, dobijamo tačnu OR tablicu istinitosti:

q_0	q_1	q_2 nakon gejtova	OR rezultat
0	0	0	0
0	1	1	1
1	0	1	1
1	1	1	1

Tabela 5. Tabela istinitosti kvantnog OR kola

Slika 62 prikazuje kvantno OR kolo i stanja kubita u zavisnosti od različitih početnih vrednosti.



Slika 62. OR kolo i stanja kubita za različite ulazne vrednosti

8 Kvantni algoritmi

Za razliku od klasičnih algoritama koji obrađuju informacije sekvencijalno, kvantni algoritmi koriste superpoziciju, interferenciju i kvantno entanglovanje kako bi istovremeno (paralelno) ispitivali veliki broj mogućih rešenja. Kod ove paralelnosti, nije reč samo o brzini, već i o kvalitativno drugačijem pristupu procesiranju informacija, koji omogućava rešavanje problema za koje klasični računari ponekad mogu da zahtevaju eksponencijalno više vremena.

Iako kvantni računari predstavljaju univerzalne računare [35], na kojima je u principu moguće izvršiti sve operacije kao i na klasičnom računaru, zbog specifičnosti njihove konstrukcije i cene, nema smisla koristiti ih za izvršavanje potpuno klasičnih algoritama. Zbog toga ne treba očekivati da se u ovom poglavlju obrađuju metode klasičnog procesiranja informacija, već isključivo algoritmi koji koriste kvantnu prednost u odnosu na klasične pristupe, odnosno algoritmi koji ostvaruju prednost kroz kvantni paralelizam i primenu principa superpozicije i entanglovanja.

U ovom poglavlju istražićemo najvažnije kvantne algoritme koji demonstriraju različite aspekte kvantne superiornosti. Počecemo od Dojčovog algoritma – najjednostavnijeg primera koji pokazuje kako kvantno računarstvo može smanjiti broj potrebnih koraka neophodnih za rešenje jednog problema. Zatim ćemo razmotriti kvantnu Furijeovu transformaciju i kvantnu estimaciju faze – fundamentalne alate koji omogućavaju analizu periodičkih struktura u kvantnim stanjima. Ovi koncepti spajaju se u Šorovom algoritmu, verovatno najpoznatijem kvantnom algoritmu koji može faktorizovati velike brojeve eksponencijalno brže od klasičnih metoda. Na kraju, analiziraćemo kvantnu teleportaciju – protokol koji demonstrira prenos kompletnog kvantnog stanja sa jedne fizičke lokacije na drugu.

U nastavku poglavlja biće prikazani neki od najznačajnijih kvantnih algoritama, uz naglasak na njihovo intuitivno razumevanje i praktičnu implementaciju u Qiskit okruženju. Prilikom oblikovanja pojedinih primera i načina prezentacije algoritama, delimično je korišćena inspiracija iz zvaničnih primera dostupnih u okviru Qiskit Textbook projekta [78]. Navedeni izvor sadrži znatno širi skup kvantnih algoritama, objašnjenja i ilustrativnih primera u odnosu na plan obuhvaćen ovom knjigom, te može poslužiti kao dodatni resurs čitaocima koji žele šire razumevanje kvantnih algoritama u kontekstu Qiskit platforme.

8.1 Dojčov algoritam

Pre analize ovog poglavlja, pogodno je pročitati poglavlje 6.3.3 Kako funkcioniše kvantni orakl, koje pruža uvod u funkcionisanje orakla, i poglavlje 6.4 Fazni povratni efekat, čije je razumevanje od suštinske važnosti za shvatanje Dojčovog algoritma.

Zamislamo funkciju koja prima jedan bit (0 ili 1) i vraća jedan bit. Postoje samo četiri moguće takve funkcije:

1. Konstantne funkcije (isti izlaz za oba ulaza):

$$f_1(0) = 0, f_1(1) = 0$$

$$f_2(0) = 1, f_2(1) = 1$$

2. Balansirane funkcije (različiti izlazi):

$$f_3(0) = 0, f_3(1) = 1$$

$$f_4(0) = 1, f_4(1) = 0$$

Podsetimo se samo da nad jednim bitom možemo da definišemo sledeće funkcije:

Naziv funkcije	Balansirana ili Konstantna	f(0)	f(1)	Objašnjenje	Formula
Konstantna nula	Konstantna	0	0	Uvek vraća 0	$f(x) = 0$
Konstantna jedinica	Konstantna	1	1	Uvek vraća 1	$f(x) = 1$
Identitet	Balansirana	0	1	Vraća isti bit	$f(x) = x$
Negacija	Balansirana	1	0	Invertuje bit	$f(x) = \neg x$

Tabela 10. Moguće funkcije nad jednim bitom

8.1.1 Šta rešava Dojčov algoritam?

Cilj algoritma je da utvrdi da li je data funkcija konstantna ili balansirana, koristeći što je moguće manje poziva funkciji.

1. Klasično rešenje

U klasičnom računarstvu moramo pozvati funkciju dva puta — izračunati $f(0)$ i $f(1)$, pa uporediti rezultate.

2. Kvantno rešenje

Dojčov algoritam rešava isti problem **samo jednim pozivom** funkcije. Ovo postiže koristeći kvantnu superpoziciju i interferenciju.

8.1.2 Kako algoritam radi?

Umesto da proveravamo vrednosti $f(0)$ i $f(1)$ posebno, kvantni algoritam ih istovremeno ispituje pomoću superpozicije. Kroz pametnu upotrebu interferencije, možemo zaključiti tip funkcije u oraklu bez sekvencijalne analize pojedinačnih vrednosti.

U suštini, funkcija koju želimo da ispitamo je funkcija nad jednim bitom (odnosno kubitom). Međutim, ne smemo da zaboravimo da u kvantnom računarstvu možemo da koristimo samo unitarne operatore (gejtove), čija je jedna od osnovnih osobina i reverzibilnost. Drugim rečima, bilo koja funkcija koju primenimo u oraklu, mora da bude reverzibilna. Ako pogledamo tabelu 10, možemo da primetimo da konstantne

- Ako je kubit bio u stanju $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ (balansirana funkcija), H-gejt ga pretvara u stanje $|1\rangle$.

Na kraju, samo izmerimo ulazni kubit:

- Ako izmerimo **0**, znamo sa 100% sigurnosti da je funkcija konstantna.
- Ako izmerimo **1**, znamo sa 100% sigurnosti da je funkcija balansirana.

Tako smo, sa samo jednim pozivom funkcije, otkrili njeno globalno svojstvo, što je u klasičnom svetu nemoguće.

8.1.3 Implementacija u Qiskit-u

Demonstriraćemo algoritam na dve funkcije:

- Konstantna: $f(x) = 0$
- Balansirana: $f(x) = x$

Python

```
from qiskit import QuantumCircuit
import quantum_utils as q

# =====
# DEFINICIJA ORAKL FUNKCIJA (Uf:  $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ )
# =====
def balanced_oracle(qc):
    #  $f(x) = x \Rightarrow y \oplus x$  (CNOT: kontrola x=q0, cilj y=q1)
    qc.cx(0, 1)
    return qc

def constant_oracle(qc):
    #  $f(x) = 1$ 
    qc.id(1)
    return qc

# -----
# KORAK 1: INICIJALIZACIJA
# -----
qc = QuantumCircuit(2, 1)
qc.barrier()
qc.show_bloch_sphere(qc) # početno stanje oba kubita:  $|00\rangle$ 

# -----
# KORAK 2: PRIPREMA POMOĆNOG KUBITA q1 U  $|1\rangle$ 
# Napomena: u ket redosledu  $|q1\ q0\rangle$ , posle X na q1 fizičko stanje je  $|10\rangle$ 
# -----
qc.x(1)
qc.barrier()
q.show_bloch_sphere(qc)

# -----
# KORAK 3: H-GEJT NA OBA KUBITA (priprema  $|+\rangle$  i  $|-\rangle$ )
# q0:  $|0\rangle \rightarrow |+\rangle$ 
# q1:  $|1\rangle \rightarrow |-\rangle$ 
# -----
qc.h(0)
```

```

qc.h(1)
qc.barrier()
q.show_bloch_sphere(qc)

# -----
# KORAK 4: PRIMENA ORACLE-A
# -----
# qc = constant_oracle(qc)      # f(x)=1
qc = balanced_oracle(qc)      # f(x)=x
qc.barrier()
q.show_bloch_sphere(qc)

# -----
# KORAK 5: FINALNI H-GEJT
# -----
qc.h(0)
qc.h(1)
qc.barrier()
q.show_bloch_sphere(qc)

# -----
# KORAK 6: MERENJE PRVOG KUBITA
# -----
qc.measure(0, 0)
q.show_qc(qc)
q.show_measurement(qc)

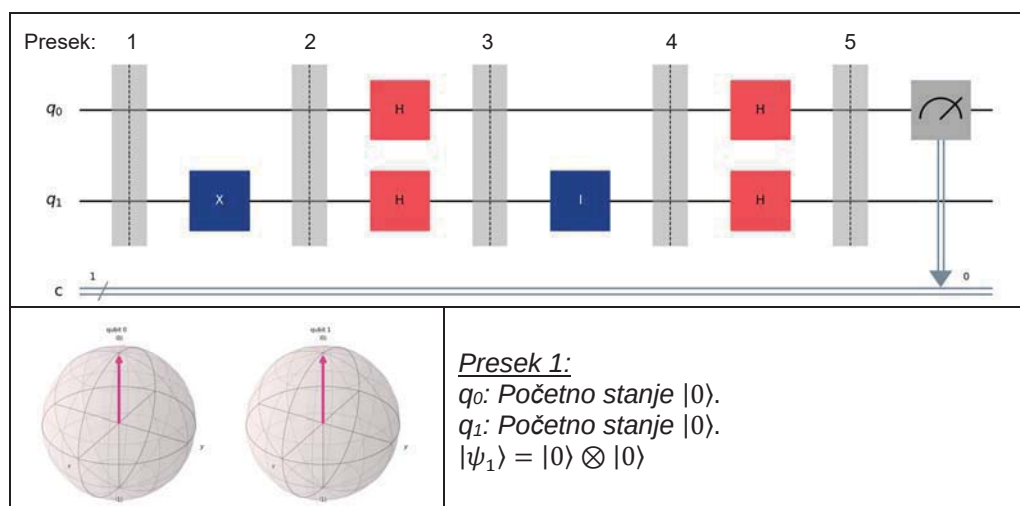
```

8.1.4 Opis programa

Sada ćemo obraditi svaki korak Dojčovog algoritma, i u slučaju konstantne, i u slučaju balansirane funkcije.

8.1.4.1 Dojčov algoritam sa konstantnom funkcijom

Dojčov algoritam sa konstantnom funkcijom u oraklu, ili ne primenjuje bilo koji gejt, ili primenjuje gejt identiteta – gejt koji ne menja kubit.



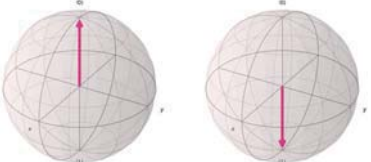
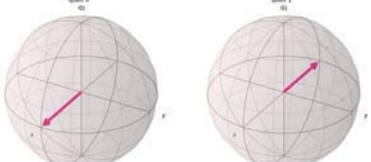
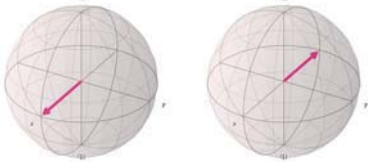
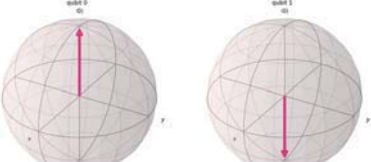
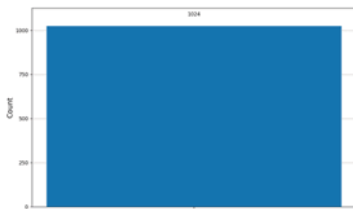
	<u>Presek 2:</u> Posle primene X-gejta, drugi kubit prelazi u stanje $1\rangle$. q_0: Zadržava stanje $0\rangle$. q_1: Prelazi u stanje $X 0\rangle = 1\rangle$ $\psi_2\rangle = 0\rangle \otimes X 0\rangle = 0\rangle \otimes 1\rangle$
	<u>Presek 3:</u> Primena H-gejta postavlja kubite u stanje superpozicije. q_0: $H 0\rangle = +\rangle$ q_1: $H 1\rangle = -\rangle$ $\psi_3\rangle = H 0\rangle \otimes H 1\rangle$ $= (\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)) \otimes (\frac{1}{\sqrt{2}}(0\rangle - 1\rangle))$ $= \frac{1}{2} [(0\rangle + 1\rangle) \otimes (0\rangle - 1\rangle)] = +\rangle \otimes -\rangle$
	<u>Presek 4:</u> Na ovom preseku vidimo dejstvo orakla kod konstantne funkcije $f(x)=1$. Kakvu god vrednost imao q_0, vrednost q_1 neće biti promenjena. Primena gejta identiteta na q_1 nema efekta ni na q_0 ni na q_1. q_0: $+\rangle = +\rangle$ q_1: $I -\rangle = -\rangle$ $\psi_4\rangle = +\rangle \otimes -\rangle$
	<u>Presek 5:</u> q_0: Posle prolaska kroz H-gejt, kubit se vraća na početno stanje $0\rangle$. q_1: Posle prolaska kroz H-gejt, kubit se vraća na početno stanje $1\rangle$. $\psi_5\rangle = H +\rangle \otimes H -\rangle = 0\rangle \otimes 1\rangle$
	<u>Merenje:</u> Pošto svih 1024 merenja daje rezultat 0, zaključujemo da je funkcija konstantna.

Tabela 11. Opis Dojčovog algoritma sa konstantnom funkcijom

8.1.4.2 Dojčov algoritam sa balansiranom funkcijom

Dojčov algoritam sa balansiranom funkcijom u oraklu može se realizovati ili CZ-gejtom u slučaju da q_1 postavimo u stanje $|1\rangle$, ili CX-gejtom, u slučaju da q_1 postavimo u stanje $|-\rangle$. U poglavlju 6.4.3 obratili smo slučaj faznog povratnog

efekta kada je q_1 u stanju $|1\rangle$, a u nastavku teksta obradićemo slučaj kada je q_1 u stanju $|-\rangle$. Razlika u primeni gejtja i stanja kubita q_1 javlja se zbog toga što je neophodno da q_1 bude u stanju koje predstavlja sopstveno stanje operatora kojim delujemo na q_1 . Drugim rečima, jedno od sopstvenih stanja Z-gejtja je stanje $|1\rangle$, dok je jedno od sopstvenih stanja X-gejtja, stanje $|-\rangle$.

Presek: 1 2 3 4 5	
	Presek 1: q_0: Početno stanje $0\rangle$. q_1: Početno stanje $0\rangle$. $\psi_1\rangle = 0\rangle \otimes 0\rangle$
	Presek 2: Posle primene X-gejtja, drugi kubit prelazi u stanje $1\rangle$. q_0: Zadržava stanje $0\rangle$. q_1: Prelazi u stanje $X 0\rangle = 1\rangle$ $\psi_2\rangle = 0\rangle \otimes X 0\rangle = 0\rangle \otimes 1\rangle$
	Presek 3: Primena H-gejtja postavlja kubite u stanje superpozicije. q_0: $H 0\rangle = +\rangle$ q_1: $H 1\rangle = -\rangle$ $\psi_3\rangle = H 0\rangle \otimes H 1\rangle$ $= (\frac{1}{\sqrt{2}}(0\rangle + 1\rangle)) \otimes (\frac{1}{\sqrt{2}}(0\rangle - 1\rangle))$ $= \frac{1}{2} [(0\rangle + 1\rangle) \otimes (0\rangle - 1\rangle)] = +\rangle \otimes -\rangle$
	Presek 4: Ovde vidimo dejstvo orakla, odnosno CX-gejtja. • U grani univerzuma gde je kontrolni kubit u stanju $0\rangle$, CX gejt ne radi ništa, i imamo: $0\rangle -\rangle \rightarrow 0\rangle -\rangle$

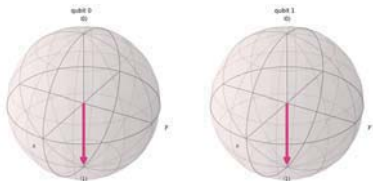
	U grani univerzuma gde je kontrolni kubit u stanju $1\rangle$, tada se na ciljni kubit primenjuje X-gejt koji menja $0\rangle \leftrightarrow 1\rangle$: $X -\rangle = X\left(\frac{ 0\rangle - 1\rangle}{\sqrt{2}}\right) = \frac{ 1\rangle - 0\rangle}{\sqrt{2}} = -\frac{ 0\rangle - 1\rangle}{\sqrt{2}} = - -\rangle$ Dakle, fizički gledano, sadržaj drugog kubita se ne menja (ostaje u stanju $-\rangle$), ali se pojavljuje fazni faktor -1, što znači: $ \psi_4\rangle = \frac{1}{\sqrt{2}}(0\rangle -\rangle - 1\rangle -\rangle) = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle) \otimes -\rangle$ Drugim rečima, fazni faktor $(-1)^{f(x)}$ prenosi informaciju o funkciji $f(x)$ na kontrolni kubit (q_0), dok ciljni kubit (q_1) ostaje u stanju $-\rangle$. Ovaj proces se može izraziti opštom formulom: $ x\rangle -\rangle \xrightarrow{U_f} (-1)^{f(x)} x\rangle -\rangle$
	Presek 5: Posle prolaska kroz H-gejt, dobijamo stanje: $q_0: H -\rangle = 1\rangle.$ $q_1: H -\rangle = 1\rangle.$ $\psi_5\rangle = H -\rangle \otimes H -\rangle = 1\rangle \otimes 1\rangle$ Iako su oba kubita u stanju $1\rangle$, samo stanje prvog kubita (q_0) nosi informaciju o tipu funkcije. Stanje drugog kubita je posledica konstrukcije orakla i ne učestvuje u donošenju zaključka.
	Merenje: Pošto svih 1024 merenja daje rezultat $q_0=1$, zaključujemo da je funkcija balansirana.

Tabela 12. Opis Dojčovog algoritma sa balansiranom funkcijom

8.1.5 Zaključak

U istorijskom smislu, Dojčov algoritam predstavlja prvi kvantni algoritam koji demonstrira kvantnu prednost — ne u smislu vremenske brzine izvršavanja, već u smislu broja poziva funkciji. Dok klasični algoritam mora da proveri oba moguća ulaza kako bi sa sigurnošću odredio da li je funkcija konstantna ili balansirana, kvantni algoritam koristi superpoziciju, interferenciju i merenje da isti problem reši uz samo jedan poziv oraklu.



Ova knjiga predstavlja sveobuhvatan uvod u kvantno programiranje namenjen inženjerima, programerima, fizičarima i svima koji žele da razumeju kako funkcioniše kvantno računarstvo — ne samo na nivou matematičkog formalizma i programskog koda, već i na nivou dubljeg fizičkog i ontološkog razumevanja.

Od osnovnih pojmova kvantne mehanike i linearne algebre, preko logike kvantnih kola i ključnih mehanizama kvantnog sveta — superpozicije, entanglovanja i interferencije — pa do Qiskit programiranja i najvažnijih kvantnih algoritama, čitalac se postepeno uvodi u način razmišljanja koji stoji iza nove računarske paradigme. Knjiga ne prikazuje kvantno programiranje samo kao skup formula i procedura, već kao oblast koja se može razumeti intuitivno, kroz dublje sagledavanje prirode kvantnog sveta.



www.PsiMosaic.com

