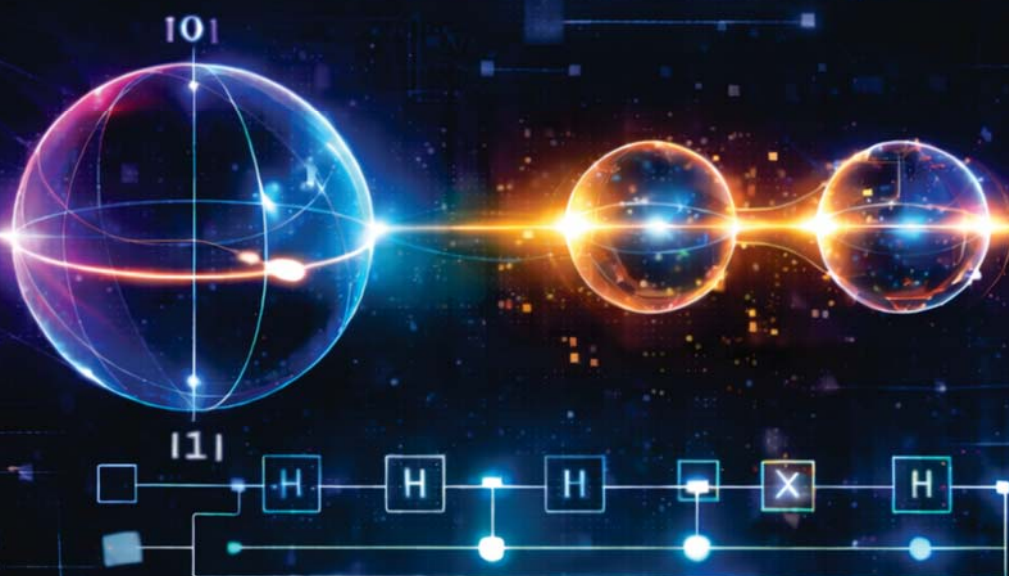


KVANTNO PROGRAMIRANJE

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

Sadržaj

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



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

