

## Περιεχόμενα

Πρόλογος	ix
Ευρετήριο σχημάτων	xiii
Ευρετήριο πινάκων	xvii
Ευρετήριο προγραμμάτων (Python)	xix

<b>1 Εισαγωγή</b>	<b>1</b>
1.1 Στοιχεία Κβαντομηχανικής .....	1
1.1.1 Εξήγηση Φαινομένων .....	2
1.1.2 Η εξίσωση του Schrödinger .....	5
1.1.3 Αρχή Απροσδιοριστίας του Heisenberg.....	7
1.1.4 Το παράδοξο Einstein-Podolsky-Rosen (EPR) .....	9
1.1.5 Ανισότητες Bell .....	11
1.2 Η αυγή της Κβαντικής Υπολογιστικής .....	12
1.2.1 Από τον κλασικό στον κβαντικό υπολογιστή .....	12
1.2.2 Θεμελιώδεις Έννοιες Κβαντικής Υπολογιστικής .....	14
<b>2 Μαθηματικό Υπόβαθρο</b>	<b>21</b>
2.1 Βασικές έννοιες Θεωρίας Αριθμών .....	21
2.2 Βασικές έννοιες της Άλγεβρας .....	25
2.2.1 Πίνακες .....	25
2.2.2 Ορίζουσες .....	30
2.2.3 Ομάδες.....	31
2.2.4 Διανυσματικοί Χώροι .....	33
2.2.5 Διαγωνιοποίηση: Ιδιοτιμές -Ιδιοδιανύσματα .....	36
2.3 Πιθανότητες .....	41
2.4 Μιγαδικοί Αριθμοί.....	51
2.5 Σειρές Fourier .....	61
2.6 Ασκήσεις .....	69
<b>3 Python</b>	<b>73</b>
3.1 Μεταβλητές, τελεστές και τύποι δεδομένων .....	74
3.2 Δομές ελέγχου και επανάληψης.....	76
3.2.1 Δομές ελέγχου .....	76
3.2.2 Δομές επανάληψης .....	77
3.3 Ενσωματωμένοι τύποι δεδομένων .....	82
3.4 Συναρτήσεις .....	84
3.5 Μαθηματικά και γραφικές παραστάσεις .....	86
3.5.1 Η βιβλιοθήκη numpy.....	87

3.5.2	Η βιβλιοθήκη matplotlib .....	89
3.6	Python και Κβαντικός Προγραμματισμός .....	93
3.6.1	Qiskit .....	93
3.6.2	Circ .....	96
3.6.3	pyQuil .....	97
3.7	Ασκήσεις .....	98
<b>4</b>	<b>Εισαγωγή στην Κβαντική Υπολογιστική</b> .....	<b>101</b>
4.1	Qubits .....	103
4.2	bra και ket .....	105
4.3	Διάνυσμα κατάστασης (state vector) .....	107
4.4	Η σφαίρα Bloch .....	110
4.5	Ενδεικτικά λυμένες ασκήσεις .....	115
4.6	Ασκήσεις .....	116
<b>5</b>	<b>Καταχωρητές, Πύλες και Κυκλώματα</b> .....	<b>119</b>
5.1	Καταχωρητές .....	119
5.2	Κβαντικές Πύλες .....	125
5.2.1	Πύλη Hadamard .....	125
5.2.2	Πύλη Αδράνειας .....	128
5.2.3	Πύλες S και T .....	129
5.2.4	Πύλες Pauli .....	130
5.2.5	Πύλη αλλαγής φάσης .....	136
5.2.6	Πύλη CNOT (cX) .....	139
5.2.7	Πύλη ελεγχόμενης μετατόπισης φάσης .....	142
5.2.8	Πύλη CCNOT - Toffoli (ccX) .....	145
5.2.9	Πύλη Swap .....	146
5.2.10	Πύλη CSwap - Fredkin .....	149
5.2.11	Πύλη Αλλαγής φάσης .....	150
5.2.12	Δημιουργώντας μία πύλη .....	150
5.3	Κβαντικά Κυκλώματα .....	153
5.3.1	Επίλυση Κυκλωμάτων .....	153
5.3.2	Κβαντική διεμπλοκή - Bell states .....	155
5.3.3	Θεώρημα μη κλωνοποίησης - No cloning theorem .....	162
5.3.4	Επέκταση κβαντικής διεμπλοκής - GHZ state .....	163
5.3.5	Κβαντική τηλεμεταφορά - Quantum teleportation .....	165
5.3.6	Υλοποίηση πύλης Fredkin .....	171
5.3.7	Τυχαιότητα .....	174
5.4	Ενδεικτικά λυμένες ασκήσεις .....	176
5.5	Ασκήσεις .....	177
<b>6</b>	<b>Κβαντικοί Αλγόριθμοι</b> .....	<b>185</b>

6.1	Εισαγωγή .....	185
6.2	Ο αλγόριθμος Deutsch - Jozsa .....	186
6.2.1	Ο αλγόριθμος Deutsch .....	186
6.2.2	Ο αλγόριθμος των Deutsch-Jozsa .....	192
6.3	Ο αλγόριθμος Bernstein-Vazirani .....	195
6.3.1	Κλασσική προσέγγιση .....	196
6.3.2	Κβαντική προσέγγιση .....	197
6.3.3	Μελέτη περίπτωσης: Αναζήτηση συμβολοσειράς .....	202
6.4	Ο αλγόριθμος του Simon .....	203
6.4.1	Κλασσική προσέγγιση .....	204
6.4.2	Κβαντική προσέγγιση .....	206
6.5	Ο αλγόριθμος του Grover .....	211
6.5.1	Κλασσική προσέγγιση .....	212
6.5.2	Κβαντική προσέγγιση .....	212
6.5.3	Πύλη πολλαπλού ελεγχόμενου Not .....	216
6.5.4	Μία χρήσιμη τεχνική .....	216
6.5.5	Μαθηματική προσέγγιση .....	219
6.5.6	Παράδειγμα .....	226
6.6	Ασκήσεις .....	232
<b>7</b>	<b>Κβαντικά Παιχνίδια</b> .....	<b>235</b>
7.1	Εισαγωγή .....	235
7.2	Κβαντική ναυμαχία .....	238
7.3	Κβαντική τρίλιζα .....	242
7.4	Ένα παιχνίδι στρατηγικής .....	245
7.5	Το τετράγωνο των Mermin-Peres .....	249
7.6	Κβαντικών παιχνιδιών επίλογος .....	254
7.7	Ασκήσεις .....	257
<b>8</b>	<b>Κβαντική Υπολογιστική και Κρυπτογραφία</b> .....	<b>259</b>
8.1	Κρυπτογραφία .....	259
8.1.1	Λίγη Ιστορία .....	260
8.1.2	Συμμετρικά Κρυπτοσυστήματα .....	263
8.1.3	Ασύμμετρα Κρυπτοσυστήματα .....	267
8.2	Κβαντική Κρυπτογραφία .....	275
8.2.1	Διανομή Κβαντικού Κλειδιού .....	276
8.2.2	Οι απαρχές της Κβαντικής Κρυπτογραφίας .....	279
8.2.3	Πρωτόκολλο BB84 .....	280
8.2.4	Πρωτόκολλο B92 .....	286
8.2.5	Πρωτόκολλο E91 .....	288
8.2.6	Πρωτοκόλλων συνέχεια... ..	291
8.3	Ο Κβαντικός Μετασχηματισμός Fourier .....	291

8.4	Παραγοντοποίηση Ακεραίων.....	295
8.5	Διακριτοί Λογάριθμοι .....	296
8.6	Ο Αλγόριθμος του Shor .....	300
8.6.1	Περιγραφή του αλγόριθμου .....	301
8.6.2	Τα βήματα του αλγόριθμου του Shor .....	302
8.6.3	Ο Κβαντικός αλγόριθμος του Shor .....	302
8.6.4	Εφαρμογή του αλγόριθμου .....	307
8.6.5	Πραγματοποιείται η εκτέλεση του αλγορίθμου σε έναν κβαντικό υπολογιστή; .....	309
8.7	Επιθέσεις σε κβαντικά πρωτόκολλα .....	311
8.7.1	Απλές ατομικές επιθέσεις .....	312
8.7.2	Συμμετρικές ατομικές επιθέσεις .....	313
8.7.3	Επίθεση πλασματικής κατάστασης .....	316
8.7.4	Επίθεση Δούρειου Ίππου .....	318
8.7.5	PNS επιθέσεις .....	319
8.7.6	Πολεμώντας στην επίθεση .....	321
8.8	Μετά την Κβαντική Κρυπτογραφία τι; .....	322
8.9	Ασκήσεις .....	325
<b>9</b>	<b>Αξιολόγηση Κβαντικών Υπολογιστών</b> .....	<b>327</b>
9.1	Εισαγωγή .....	327
9.2	Αξιολόγηση Κβαντικών Υπολογιστών .....	328
9.2.1	Κβαντικός Όγκος.....	329
9.3	Μελέτες περιπτώσεων .....	331
9.3.1	Ο αλγόριθμος Bernstein-Vazirani .....	332
9.3.2	Ο αλγόριθμος Simon .....	340
9.4	Ο αλγόριθμος του Grover.....	343
9.5	Μετριάσιμος σφαλμάτων .....	346
9.6	Ασκήσεις .....	348
<b>10</b>	<b>Κβαντική Μηχανική Μάθηση</b> .....	<b>351</b>
10.1	Εισαγωγή .....	351
10.2	Παρούσα Κατάσταση.....	353
10.3	Κβαντικοί Αλγόριθμοι Μηχανικής Μάθησης.....	354
10.4	Προκλήσεις και μελλοντικές τάσεις .....	356
<b>11</b>	<b>Κβαντικό Διαδίκτυο</b> .....	<b>359</b>
11.1	Δυσκολίες αλλά και προοπτικές .....	360
	<b>Βιβλιογραφία</b> .....	<b>362</b>
	<b>Ευρετήριο όρων</b> .....	<b>369</b>