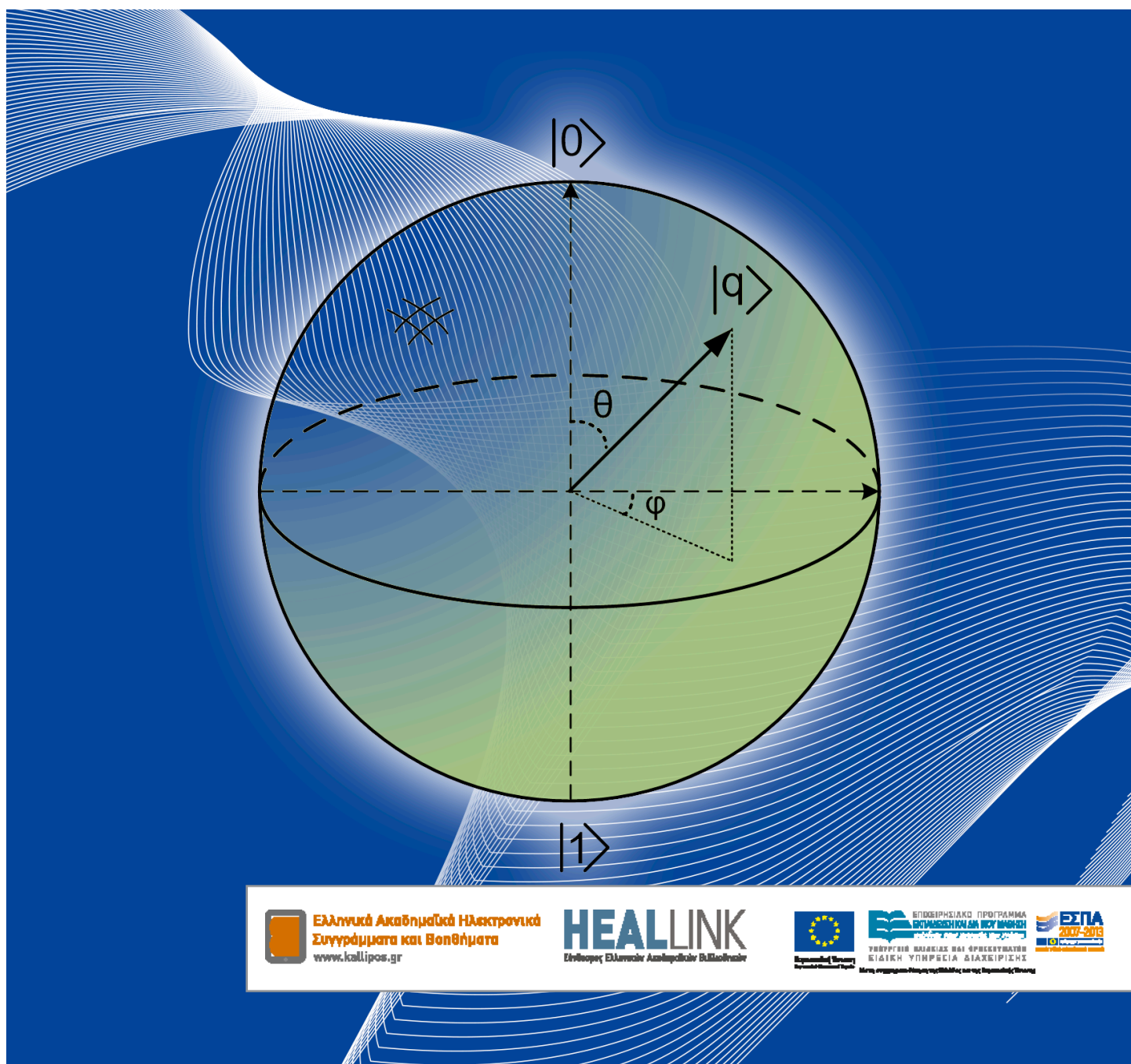


Κβαντική Υπολογιστική

ΙΩΑΝΝΗΣ ΚΑΡΑΦΥΛΛΙΔΗΣ

Καθηγητής

Τμήμα Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών, Δ.Π.Θ.



Ελληνικά Ακαδημαϊκά Ηλεκτρονικά
Συγγράμματα και Βοηθήματα
www.kallipos.gr

HEALLINK
Επίσημος Ελληνικός Ασπαστικός Διανομητής



ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΣΤΡΑΤΕΓΙΚΗ ΚΑΙ ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ
ΥΠΟΥΡΓΕΙΟ ΠΑΡΑΚΤΗΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης



ΙΩΑΝΝΗΣ ΚΑΡΑΦΥΛΛΙΔΗΣ
Καθηγητής
Τμήμα Ηλεκτρολόγων Μηχανικών
και Μηχανικών Υπολογιστών, Δ.Π.Θ.

Κβαντική Υπολογιστική



Ελληνικά Ακαδημαϊκά Ηλεκτρονικά
Συγγράμματα και Βοηθήματα
www.kallipos.gr

Κβαντική Υπολογιστική

Συγγραφή

Ιωάννης Καραφυλλίδης

Κριτικός αναγνώστης

Δημήτριος Σούντρης

Συντελεστές έκδοσης

ΓΛΩΣΣΙΚΗ ΕΠΙΜΕΛΕΙΑ: Ιωάννης Καραφυλλίδης

ΓΡΑΦΙΣΤΙΚΗ ΕΠΙΜΕΛΕΙΑ: Ιωάννης Καραφυλλίδης

ΤΕΧΝΙΚΗ ΕΠΕΞΕΡΓΑΣΙΑ: Σπυρίδων Παπαβασιλείου

ISBN: 978-960-603-002-4

Copyright © 2015, ΣΕΑΒ



Το παρόν έργο αδειοδοτείται υπό τους όρους της άδειας Creative Commons Αναφορά Δημιουργού - Μη Εμπορική Χρήση - Όχι Παράγωγα Έργα 3.0. Για να δείτε ένα αντίγραφο της άδειας αυτής επισκεφτείτε τον ιστότοπο <https://creativecommons.org/licenses/by-nc-nd/3.0/gr/>

ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ

Εθνικό Μετσόβιο Πολυτεχνείο

Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφου

www.kallipos.gr

Ο ξένος δεν έβαλε την χείρα εις την τσέπη. Αλλά μεταξύ του αντίχειρος, του λιχανού και του μέσου της δεξιάς ευρέθει κρατών μίαν αγγλικήν λίραν.

Αλέξανδρος Παπαδιαμάντης, «Ο Αμερικάνος»

*σου έδειχνα ένα πουλί
έλεγες – Είναι λουλούδι
σου έδειχνα ένα λουλούδι
όχι, έλεγες – Είναι πουλί*

Μίλτος Σαχτούρης

*Κι η ποίηση είναι σα ν' ανεβαίνεις μιά φανταστική σκάλα
για να κόψεις ένα ρόδο αληθινό.*

Τάσος Λειβαδίτης

Στην Ελισάβετ

Πίνακας περιεχομένων

Πίνακας περιεχομένων.....	5
Πρόλογος.....	8
Εισαγωγή	9
1. Στοιχεία κβαντικής μηχανικής	10
1.1 Κβαντικά συστήματα δύο καταστάσεων	10
1.2 Διανύσματα Bra και Ket, συμβολισμός Dirac	13
1.3 Αλλαγή κατάστασης, τελεστές.....	17
1.4 Το κβαντικό παιχνίδι	20
1.5 Η εξίσωση του Schrödinger	22
Βιβλιογραφία	24
Ασκήσεις	25
2. Αποθήκευση της κβαντικής πληροφορίας.....	28
2.1 Το κβαντικό bit (qubit).....	28
2.2 Η σφαίρα Bloch	29
2.3 Ο κβαντικός καταχωρητής.....	32
2.4 Μερική μέτρηση ενός κβαντικού καταχωρητή.....	38
2.5 Βασικά στοιχεία του χώρου Hilbert	40
Βιβλιογραφία	43
Ασκήσεις	43
3. Τελεστές και κβαντικές πύλες.....	46
3. 1 Οι κβαντικές πύλες ως τελεστές του χώρου Hilbert	46
3. 2 Κβαντικές πύλες που δρουν σε ένα qubit	47
3.2.1 Η κβαντική πύλη αδρανείας.....	47
3.2.2 Η Κβαντική πύλη μετατόπισης φάσης.....	48
3.2.3 Η κβαντική πύλη Hadamard	49
3. 3 Κβαντικές πύλες Pauli	51
3. 4 Κβαντικές πύλες που δρουν σε δύο qubits	52
3.4.1 Η κβαντική πύλη ελεγχόμενου OXI.....	52
3.4.2 Η κβαντική πύλη ελεγχόμενης μετατόπισης φάσης	54
3. 5 Κβαντικές πύλες που δρουν σε τρία qubits.....	55
3.5.1 Η κβαντική πύλη διπλά ελεγχόμενου OXI.....	55
3.5.2 Η κβαντική πύλη Fredkin	57
3. 6 Η αδυναμία αντιγραφής της κατάστασης ενός qubit.....	59
Βιβλιογραφία	62

Ασκήσεις	62
4. Η αρχή της κβαντικής υπολογιστικής - Κβαντικός αλγόριθμος του Deutsch	65
4.1 Το κυκλωματικό μοντέλο των κβαντικών υπολογισμών	65
4.2 Ένας αναλυτικός κβαντικός υπολογισμός.....	66
4.3 Η αρχή της κβαντικής υπολογιστικής.....	72
4.4 Η αρχή της κβαντικής υπολογιστικής και η εξίσωση του Schrödinger	76
4.5 Ο κβαντικός αλγόριθμος του Deutsch	77
Βιβλιογραφία	84
Ασκήσεις	84
5. Κβαντική Διερεύνηση - Κβαντικός αλγόριθμος του Grover	87
5.1 Διερεύνηση μη δομημένων βάσεων δεδομένων	87
5.2 Ο κβαντικός αλγόριθμος του Grover	87
5.3 Γεωμετρικές ερμηνείες του κβαντικού αλγορίθμου του Grover.....	92
5.4 Πρώτο παράδειγμα εφαρμογής του κβαντικού αλγορίθμου του Grover	98
5.5 Δεύτερο παράδειγμα εφαρμογής του κβαντικού αλγορίθμου του Grover	100
Βιβλιογραφία	105
Ασκήσεις	105
6. Η κβαντική διεμπλοκή και ο κβαντικός μετασχηματισμός Fourier	107
6.1 Η κβαντική διεμπλοκή.....	107
6.2 Ο τελεστής πυκνότητας.....	112
6.3 Εντροπία von Neumann και υπολογισμός της διεμπλοκής	115
6.4 Ο κβαντικός μετασχηματισμός Fourier	116
Βιβλιογραφία	123
Ασκήσεις	124
7. Ο κβαντικός αλγόριθμος του Shor	126
7.1 Το κρυπτογραφικό σύστημα RSA	126
7.2 Περιγραφή του κβαντικού αλγορίθμου του Shor.....	127
7.3 Τα βήματα του κβαντικού αλγορίθμου του Shor	129
7.4 Παράδειγμα και ερμηνεία του κβαντικού αλγορίθμου του Shor	131
Βιβλιογραφία	133
Ασκήσεις	133
8. Κβαντική τηλεμεταφορά	134
8.1 Η κβαντική τηλεμεταφορά.....	134
Βιβλιογραφία	138
Ασκήσεις	138

9. Ο Προσομοιωτής Κβαντικού Υπολογιστή QCS	139
9.1 Άδεια χρήσης του QCS.....	139
9.2 Δομή και εγκατάσταση του QCS.....	139
9.3 Χρήση του QCS.....	140
9.4 Σφάλματα χρήσης του QCS	146
Βιβλιογραφία	147
Απόδοση όρων	149

Πρόλογος

Το αντικείμενο του βιβλίου αυτού είναι η Κβαντική Υπολογιστική και η κβαντική επεξεργασία της πληροφορίας, το οποίο συντίθεται από την Κβαντική Μηχανική, την Επιστήμη και την Τεχνολογία των Υπολογιστών και την Επιστήμη της Πληροφορικής. Η διεπιστημονικότητα του αντικειμένου αποτελεί ίσως την κυριότερη δυσκολία που αντιμετωπίζουν όσοι επιθυμούν να ασχοληθούν με αυτό. Το βιβλίο φιλοδοξεί όχι μόνο να εισαγάγει μεθοδικά τους φοιτητές και τους ενδιαφερόμενους επιστήμονες και ερευνητές σε αυτό το ραγδαία αναπτυσσόμενο πεδίο, αλλά και να παρουσιάσει με αναλυτικό και κατανοητό τρόπο τις πιο σύνθετες και δύσκολες πλευρές της Κβαντικής Υπολογιστικής, όπως η κβαντική διεμπλοκή και η κβαντική τηλεμεταφορά.

Το βιβλίο διαμορφώθηκε έτσι ώστε να μπορεί να το διαβάσει και να το κατανοήσει άνετα ο αναγνώστης που δεν έχει καθόλου γνώσεις κβαντικής μηχανικής, γιατί όλα τα απαραίτητα στοιχεία της εμπεριέχονται σ' αυτό. Επίσης, το βιβλίο μπορεί να το διαβάσει άνετα και ο αναγνώστης που δεν έχει γνώσεις επιστήμης των υπολογιστών, τεχνολογίας των υπολογιστών ή πληροφορικής. Ο φοιτητής, ο επιστήμονας ή ο ερευνητής που θέλουν να ασχοληθούν με τους κβαντικούς υπολογιστές θα βρουν στο βιβλίο αυτό έναν οδηγό που θα τους εισάγει και θα τους οδηγήσει βήμα-βήμα στο αντικείμενο αυτό. Όταν τελειώσουν το βιβλίο, θα μπορούν άνετα να διαβάσουν και να καταλάβουν ερευνητικές επιστημονικές εργασίες με θέμα τους κβαντικούς υπολογιστές. Το βιβλίο συνοδεύεται από έναν προσομοιωτή κβαντικού υπολογιστή, τον QCS, που αναπτύχθηκε από τον συγγραφέα. Για να τρέξει ο QCS, είναι απαραίτητο το πακέτο λογισμικού Matlab. Ο προσομοιωτής αυτός παρέχει τις καταστάσεις των κβαντικών καταχωρητών και τις φάσεις των κβαντικών bits που τους αποτελούν, σε κάθε βήμα του κβαντικού υπολογισμού. Η χρήση του QCS θα βοηθήσει τον αναγνώστη να παρακολουθήσει τους περισσότερους από τους κβαντικούς υπολογισμούς που περιέχονται στο βιβλίο και θα του δώσει τη δυνατότητα να εκτελέσει δικούς του κβαντικούς υπολογισμούς. Οι οδηγίες χρήσης του QCS δίνονται στο τελευταίο κεφάλαιο του βιβλίου. Ο προσομοιωτής κβαντικού υπολογιστή QCS είναι διαθέσιμος στην ιστοσελίδα του κεφαλαίου 9 αυτού του βιβλίου, στον Ελληνικό Συσσωρευτή Ακαδημαϊκών Ηλεκτρονικών Βιβλίων (<http://repository.kallipos.gr>).

Το βιβλίο γράφτηκε έτσι ώστε η ύλη του να αποτελέσει ένα πλήρες εξαμηνιαίο μάθημα για προπτυχιακούς φοιτητές των τελευταίων εξαμήνων ή για μεταπτυχιακούς φοιτητές των Τμημάτων των Ελληνικών Α.Ε.Ι. που έχουν ως αντικείμενο την Επιστήμη των Υπολογιστών, την Τεχνολογία των Υπολογιστών, την Πληροφορική ή τις Θετικές Επιστήμες.

Ελπίζω το βιβλίο αυτό να σας βοηθήσει να καταλάβετε τι είναι και πώς λειτουργούν οι κβαντικοί υπολογιστές, ώστε να μπορέσετε να παρακολουθήσετε ή και να πάρετε μέρος σε μία από τις πιο μεγάλες επιστημονικές περιπέτειες του αιώνα μας.

Ξάνθη 2015

Ιωάννης Καραφυλλίδης
Καθηγητής Δ.Π.Θ.

Εισαγωγή

Ένα κβαντικό παιχνίδι:

Ο Captain Class, κυβερνήτης του διαστημοπλοίου “Classical”, αντιμετωπίζει μία πολύ δύσκολη κατάσταση. Βρίσκεται με το διαστημόπλοιο του πολύ μακριά από τη Γη, στην πιο απομακρυσμένη μεριά του γαλαξία. Ο κινητήρας έχει χαλάσει και κανείς από το πλήρωμα δεν μπορεί να τον επισκευάσει. Ταξιδεύει με τον βοηθητικό κινητήρα αλλά δεν μπορεί να αναπτύξει ταχύτητα και έτσι δεν θα προλάβει να εκτελέσει την αποστολή του.

Ξαφνικά εμφανίζεται ένα άγνωστο διαστημόπλοιο. Ο Captain Class διαβάζει το όνομα “Quantum” γραμμένο στην πλευρά του. Επικοινωνεί με το “Quantum” και ζητά βοήθεια. Ο κυβερνήτης του διαστημοπλοίου “Quantum” ονομάζεται Quant και είναι μια κβαντική οντότητα. Ο Quant προτείνει στον Captain Class να συναντηθούν και να παίξουν ένα παιχνίδι. Αν ο Captain Class κερδίσει, τότε ο Quant θα επισκευάσει τον κινητήρα χωρίς αντάλλαγμα. Αν όμως χάσει, τότε ο Quant θα μεταφέρει αυτόν και το πλήρωμά του στην κοντινότερη βάση και μετά θα φύγει παίρνοντας μαζί του το διαστημόπλοιο “Classical”.

Το παιχνίδι που προτείνει ο Quant είναι το εξής:

1. Ο Quant δίνει στον Captain Class ένα κέρμα. Το κέρμα αυτό έχει δύο εντελώς ίδιες όψεις, μόνο που στη μία όψη φαίνεται το γράμμα Η και στην άλλη το γράμμα Τ. Είναι αδύνατον να ξεχωρίσει κανείς τις όψεις με την αφή.

2. Ο Quant φεύγει από το δωμάτιο και ο Captain Class βάζει το κέρμα πάνω σε ένα τραπέζι με όποια από τις δύο όψεις θέλει προς τα επάνω. Γράφει το γράμμα που φαίνεται στην πάνω όψη σε ένα χαρτί, βάζει το χαρτί σε έναν φάκελο, τον σφραγίζει και τον βάζει στην άκρη του τραπεζιού. Στη συνέχεια καλύπτει το κέρμα με ένα κάλυμμα, που έχει ένα μικρό άνοιγμα από το οποίο αυτός και ο Quant μπορούν να βάλουν το χέρι τους και να δράσουν στο κέρμα. Το κάλυμμα είναι απολύτως αδιαφανές και κανείς δεν μπορεί να δει το κέρμα.

3. Ο Quant έρχεται στο δωμάτιο, βάζει το χέρι του μέσα στο κάλυμμα και δρα στο κέρμα.

4. Ο Captain Class βάζει το χέρι του μέσα στο κάλυμμα και δρα στο κέρμα.

5. Ο Quant βάζει για δεύτερη φορά το χέρι του μέσα στο κάλυμμα και δρα στο κέρμα.

6. Βγάζουν το κάλυμμα για να φανεί το κέρμα και ανοίγουν τον φάκελο.

7. Αν το κέρμα βρεθεί με την αρχική όψη προς τα επάνω, ο Quant κερδίζει, αλλιώς κερδίζει ο Captain Class.

Ο Captain Class αρνείται να παίξει το διαστημόπλοιο του σ’ αυτό το παιχνίδι. Ο Quant τότε του κάνει την εξής πρόταση: να παίξουν το παιχνίδι χίλιες φορές και, αν σε μία από αυτές χάσει ο Quant, τότε θα επισκευάσει τον κινητήρα, αν όμως κερδίσει και στις χίλιες, τότε ο Captain Class θα χάσει το διαστημόπλοιο του. Ο Captain Class θεωρεί εξαιρετικά απίθανο να κερδίσει ο Quant χίλιες φορές στη σειρά, και δέχεται να παίξει. Παίζουν το παιχνίδι χίλιες φορές και ο Quant κερδίζει σε όλες. Ο Captain Class χάνει το διαστημόπλοιο του.

Μετά την επιστροφή του στη Γη, ο Captain Class παρουσιάζεται στο δικαστήριο για να κριθεί για τις αποφάσεις που πήρε. Οι δικαστές αναγνωρίζουν ότι βρέθηκε σε δύσκολη κατάσταση και θεωρούν λογική την απόφασή του να παίξει το παιχνίδι. Επειδή όμως τελικά έχασε το διαστημόπλοιο “Classical”, τον υποβιβάζουν σε κυβερνήτη μεταγωγικού διαστημοπλοίου. Ο Captain Class αναλαμβάνει κυβερνήτης του μεταγωγικού διαστημοπλοίου “Boring”. Στις ατελείωτες και μονότονες ώρες των ταξιδιών του προσπαθεί να καταλάβει πώς έχασε από τον Quant.

Μήπως μπορείτε να το εξηγήσετε εσείς; (Η λύση στο κεφάλαιο 1.4 του βιβλίου)

1. Στοιχεία κβαντικής μηχανικής

Σύνοψη

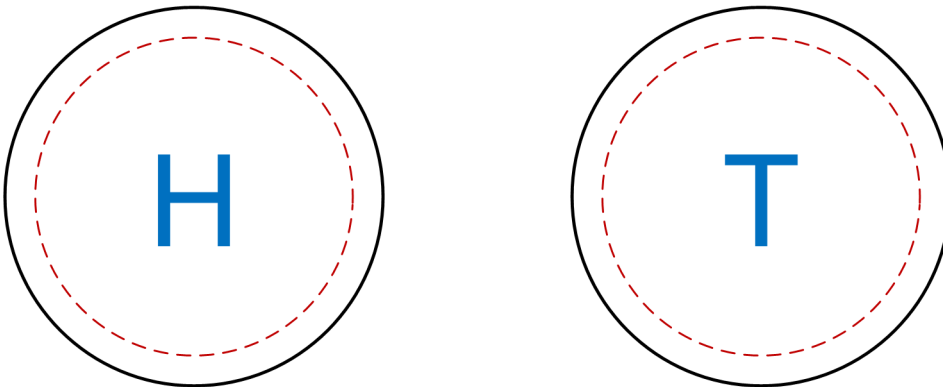
Στο κεφάλαιο αυτό, παρουσιάζονται τα κβαντικά συστήματα δύο καταστάσεων, οι βασικές τους καταστάσεις και η έννοια της υπέρθεσης καταστάσεων. Δίνονται ορισμοί και παραδείγματα του συμβολισμού Dirac, του εσωτερικού και του εξωτερικού γινομένου διανυσμάτων κατάστασης. Περιγράφονται οι τελεστές και η δράση τους στα διανύσματα κατάστασης. Η εξίσωση του Schrödinger παρουσιάζεται ως έκφραση της αρχής της διατήρησης της ενέργειας.

Προαπαιτούμενη γνώση

Γραμμική άλγεβρα και κυρίως ο πολλαπλασιασμός πινάκων.

1.1 Κβαντικά συστήματα δύο καταστάσεων

Ας πούμε ότι έχουμε ένα κέρμα πάνω σε ένα τραπέζι. Το κέρμα αυτό, όπως όλα τα κέρματα, έχει δύο όψεις. Οι δύο αυτές όψεις είναι εντελώς ίδιες, μόνο που στη μία φαίνεται το γράμμα «H» και στην άλλη όψη το γράμμα «T».

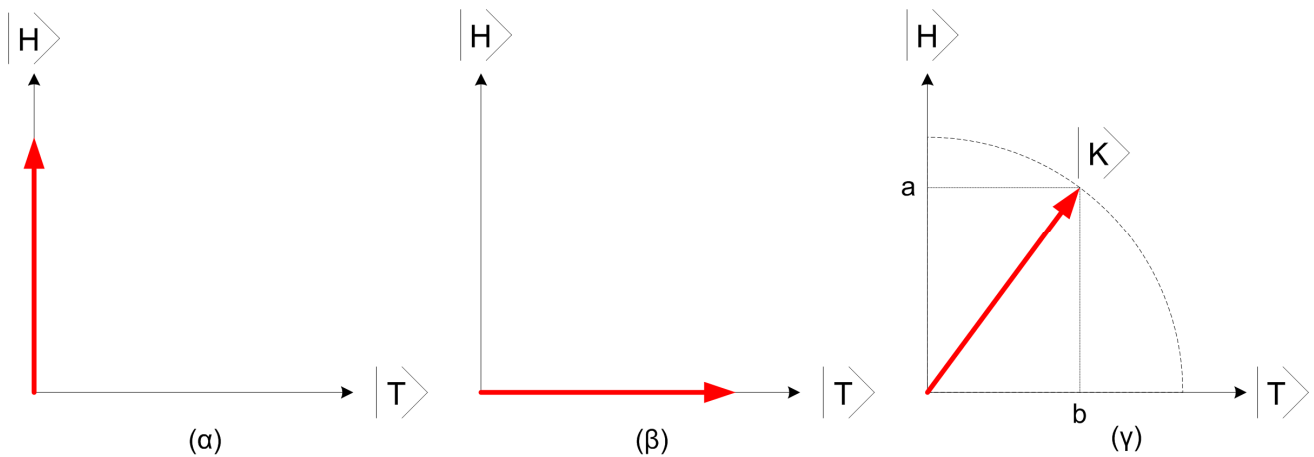


Σχήμα 1-1 Οι δύο όψεις του κέρματος.

Οι δύο όψεις του κέρματος φαίνονται στο Σχήμα 1-1. Δεν μας ενδιαφέρει καμία άλλη ιδιότητα του κέρματος, όπως το βάρος του, το χρώμα του ή σκληρότητά του. Μας ενδιαφέρει μόνο αν η πάνω όψη του είναι αυτή με το γράμμα H ή αυτή με το γράμμα T . Ένα συνηθισμένο κέρμα, όπως αυτά που χρησιμοποιούμε καθημερινά, το ονομάζουμε «κλασικό» κέρμα. Ένα κλασικό κέρμα μπορεί να βρεθεί ή με το γράμμα H ή με το γράμμα T στην πάνω όψη του και τότε λέμε ότι το κέρμα βρίσκεται στην κατάσταση «H» ή στην κατάσταση «T».

Ας υποθέσουμε τώρα ότι μπορούμε με κάποιον τρόπο να αντιληφθούμε και να χειριστούμε τα κβαντικά φαινόμενα. Τώρα μπορούμε να έχουμε στις τσέπες μας και «κβαντικά» κέρματα. Ας υποθέσουμε επίσης ότι για κάποιο λόγο δεν μπορούμε να δούμε αν τα κέρματα (κλασικά ή κβαντικά) βρίσκονται στην κατάσταση «H» ή στην κατάσταση «T». Για να αντιληφθούμε σε ποια κατάσταση βρίσκονται τα κέρματα, έχουμε στη διάθεσή μας μία συσκευή μέτρησης. Με τη συσκευή αυτή μετράμε το κέρμα και, αν διαβάσουμε στην οθόνη της συσκευής το γράμμα H , τότε ξέρουμε ότι το κέρμα βρίσκεται στην κατάσταση «H», αν διαβάσουμε το γράμμα T , τότε ξέρουμε ότι το κέρμα βρίσκεται στην κατάσταση «T».

Ένα κλασικό και ένα κβαντικό κέρμα πέφτουν πάνω στο τραπέζι. Δε μετράμε ακόμη τις καταστάσεις τους. Το κλασικό κέρμα μπορεί να βρεθεί ή στην κατάσταση «H» ή στην κατάσταση «T». Δεν μπορούμε όμως να πούμε το ίδιο και για το κβαντικό κέρμα. Η κατάσταση που βρίσκεται το κβαντικό κέρμα περιγράφεται από το «διάνυσμα κατάστασης».



Σχήμα 1-2 Το διάνυσμα κατάστασης του κβαντικού κέρματος. (α) Το διάνυσμα βρίσκεται πάνω στον άξονα $|H\rangle$ και το κβαντικό κέρμα βρίσκεται στην κατάσταση $|H\rangle$. (β) Το διάνυσμα βρίσκεται πάνω στον άξονα $|T\rangle$ και το κβαντικό κέρμα βρίσκεται στην κατάσταση $|T\rangle$. (γ) Η κατάσταση του κβαντικού κέρματος $|K\rangle$ είναι υπέρθεση των δύο καταστάσεων $|H\rangle$ και $|T\rangle$.

Το διάνυσμα κατάστασης του κβαντικού κέρματος υπάρχει σε έναν χώρο δύο διαστάσεων του οποίου οι δύο άξονες αντιστοιχούν στις καταστάσεις «H» και «T». Για να ξεχωρίζουμε τις καταστάσεις του κβαντικού κέρματος από αυτές του κλασικού, θα τις συμβολίζουμε από εδώ και πέρα με $|H\rangle$ και $|T\rangle$. Το Σχήμα 1-2 θα μας βοηθήσει να καταλάβουμε καλύτερα το διάνυσμα κατάστασης του κβαντικού κέρματος.

Στο Σχήμα 1-2 το διάνυσμα με την παχιά κόκκινη γραμμή είναι το διάνυσμα κατάστασης του κβαντικού κέρματος. Η αρχή του διανύσματος κατάστασης βρίσκεται πάντα στο σημείο της τομής των αξόνων $|H\rangle$ και $|T\rangle$. Όταν το διάνυσμα βρίσκεται πάνω στον άξονα $|H\rangle$, όπως στο Σχήμα 1-2(α), τότε το κβαντικό κέρμα βρίσκεται σίγουρα στην κατάσταση $|H\rangle$, δηλαδή η πάνω όψη του είναι αυτή με το γράμμα H. Όταν το διάνυσμα βρίσκεται πάνω στον άξονα $|T\rangle$, όπως στο Σχήμα 1-2(β), τότε το κβαντικό κέρμα βρίσκεται σίγουρα στην κατάσταση $|T\rangle$, δηλαδή η πάνω όψη του είναι αυτή με το γράμμα T.

Μέχρι εδώ δεν φαίνεται να υπάρχει καμία διαφορά ανάμεσα στο κλασικό και στο κβαντικό κέρμα. Όμως το κβαντικό κέρμα έχει μια ιδιότητα που δεν έχει το κλασικό. Το διάνυσμα της κατάστασής του, εκτός από τις διευθύνσεις των αξόνων $|H\rangle$ και $|T\rangle$, μπορεί να έχει οποιανδήποτε άλλη διεύθυνση, όπως φαίνεται στο Σχήμα 1-2(γ).

Τι συμβαίνει στην περίπτωση αυτή; Το κβαντικό κέρμα βρίσκεται ταυτόχρονα και στην κατάσταση $|H\rangle$ και στην κατάσταση $|T\rangle$. Μην προσπαθήσετε να φανταστείτε την κατάσταση αυτή του κβαντικού κέρματος γιατί δε θα μπορείτε. Φανταζόμαστε με τον εγκέφαλό μας ο οποίος είναι ένα κλασικό σύστημα και ένα κλασικό σύστημα είναι αδύνατον να προσομοιώσει (να φανταστεί στην περίπτωσή μας) ένα κβαντικό σύστημα.

Πρέπει εδώ να θυμηθούμε ότι δεν έχουμε μετρήσει ακόμη την κατάσταση του κέρματος. Το μόνο που ξέρουμε είναι η διεύθυνση του διανύσματος κατάστασης. Πώς το ξέρουμε αυτό; Όπως θα μάθουμε σε επόμενα κεφάλαια του βιβλίου, μπορούμε να βρούμε τη διεύθυνση του διανύσματος κάνοντας κάποιους υπολογισμούς. Πρέπει ακόμη να θυμόμαστε ότι η αρχή του διανύσματος κατάστασης βρίσκεται πάντα στο σημείο της τομής των αξόνων $|H\rangle$ και $|T\rangle$. Επίσης, το μήκος του διανύσματος είναι πάντα το ίδιο, όποια και αν είναι η διεύθυνσή του (Bell, 1987). Το πόσο είναι το μήκος αυτό θα το δούμε σε λίγο.

Ερχόμαστε πάλι στο Σχήμα 1-2(γ). Το διάνυσμα της κατάστασης του κβαντικού κέρματος δεν βρίσκεται ούτε πάνω στον άξονα $|H\rangle$ ούτε πάνω στον άξονα $|T\rangle$, αλλά σε μια ενδιάμεση διεύθυνση. Το κβαντικό κέρμα βρίσκεται και στην κατάσταση $|H\rangle$ και στην κατάσταση $|T\rangle$. Ας ονομάσουμε την κατάσταση αυτή $|K\rangle$. Η προβολή του διανύσματος της κατάστασης στον άξονα $|H\rangle$ έχει μήκος a και στον άξονα $|T\rangle$ έχει μήκος b . Η κατάσταση $|K\rangle$ δίνεται από την παρακάτω σχέση :

$$|K\rangle = a|H\rangle + b|T\rangle \quad (1.1)$$

Στη γλώσσα της κβαντικής μηχανικής λέμε ότι η κατάσταση $|K\rangle$ είναι υπέρθεση των δύο καταστάσεων $|H\rangle$ και $|T\rangle$.

Δεν έχουμε μετρήσει ακόμα την κατάσταση του κβαντικού κέρματος. Αυτό που μας ενδιαφέρει πάρα πολύ είναι να προβλέψουμε το αποτέλεσμα αυτής της μέτρησης. Όταν ξέρουμε ότι το κβαντικό κέρμα βρίσκεται στην κατάσταση $|H\rangle$, τότε μπορούμε να προβλέψουμε με απόλυτη βεβαιότητα πως, όταν μετρήσουμε θα βρούμε το κβαντικό κέρμα με το γράμμα H στην πάνω όψη. Το ίδιο και όταν ξέρουμε ότι το κβαντικό κέρμα βρίσκεται στην κατάσταση $|T\rangle$. Τότε όταν μετρήσουμε, σίγουρα θα βρούμε το κβαντικό κέρμα με το γράμμα T στην πάνω όψη.

Ποιο θα είναι το αποτέλεσμα της μέτρησης όταν το κβαντικό κέρμα βρίσκεται στην κατάσταση $|K\rangle$; Τα δυνατά αποτελέσματα στην περίπτωση αυτή είναι δύο: το κβαντικό κέρμα θα βρεθεί ή με το γράμμα H ή με το γράμμα T στην πάνω όψη. Αυτό είναι όλο; Δηλαδή όταν το κβαντικό κέρμα δεν βρίσκεται στις καταστάσεις $|H\rangle$ και $|T\rangle$, δεν μπορούμε να κάνουμε καμία πρόβλεψη για το αποτέλεσμα της μέτρησης; Όχι, αυτό που συμβαίνει είναι ότι δεν μπορούμε να προβλέψουμε με σιγουριά το αποτέλεσμα της μέτρησης. Ξέρουμε όμως την πιθανότητα για το κάθε ένα από τα δύο αποτελέσματα. Όταν το κβαντικό κέρμα βρίσκεται στην κατάσταση $|K\rangle$, η πιθανότητα να μετρήσουμε και να βρούμε το κβαντικό κέρμα με το γράμμα H στην πάνω όψη είναι ίση με $|a|^2$ και η πιθανότητα να μετρήσουμε και να βρούμε το κβαντικό κέρμα με το γράμμα T στην πάνω όψη είναι ίση με $|b|^2$. Τα a και b είναι οι προβολές του διανύσματος της κατάστασης στους άξονες $|H\rangle$ και $|T\rangle$ που φαίνονται στο Σχήμα 1-2(γ) και στη σχέση (1.1). Αυτή είναι όλη και όλη η πρόβλεψη για το αποτέλεσμα της μέτρησης που μπορούμε να κάνουμε. Όσο και με όποιον τρόπο και αν προσπαθήσουμε, δε θα μπορέσουμε να αντλήσουμε περισσότερη πληροφορία από το κβαντικό κέρμα, ώστε να κάνουμε μια καλύτερη πρόβλεψη για το αποτέλεσμα της μέτρησης της κατάστασής του.

Αφού λοιπόν η πιθανότητα να βρούμε το κβαντικό κέρμα με το γράμμα H στην πάνω όψη είναι ίση με $|a|^2$ και η πιθανότητα να βρούμε το κβαντικό κέρμα με το γράμμα T στην πάνω όψη είναι ίση με $|b|^2$ και αφού αυτά είναι τα μόνα δυνατά αποτελέσματα, τότε θα πρέπει το άθροισμα των δύο πιθανοτήτων να είναι ίσο τη μονάδα:

$$|a|^2 + |b|^2 = 1 \quad (1.2)$$

Δηλαδή το μήκος του διανύσματος κατάστασης είναι πάντα ίσο με τη μονάδα. Η αρχή του βρίσκεται πάντα στο σημείο τομής των αξόνων $|H\rangle$ και $|T\rangle$, και το τέλος του πάνω στην περιφέρεια του κύκλου που έχει ως κέντρο το σημείο τομής των αξόνων και ακτίνα ίση με τη μονάδα. Διαφορετικές διευθύνσεις του διανύσματος κατάστασης $|K\rangle$ αντιστοιχούν σε διαφορετικές τιμές για τα a και b και σε διαφορετικές πιθανότητες για το κάθε ένα από τα δύο δυνατά αποτελέσματα της μέτρησης της κατάστασης.

Παράδειγμα 1.1

Η κατάσταση ενός κβαντικού κέρματος δίνεται από τη σχέση:

$$|K\rangle = 0,500|H\rangle + 0,866|T\rangle$$

Η πιθανότητα να μετρήσουμε και να βρούμε το κέρμα με το γράμμα «H» στην πάνω όψη είναι $0,500^2 = 0,25$ δηλαδή 25%. Η πιθανότητα να μετρήσουμε και να βρούμε το κέρμα με το γράμμα «T» στην πάνω όψη είναι $0,866^2 = 0,75$ δηλαδή 75%. ♦

Μέχρι τώρα είδαμε πολύ σημαντικά πράγματα. Αξίζει να τα δούμε πάλι συνοπτικά χρησιμοποιώντας περισσότερο τη γλώσσα της κβαντικής μηχανικής. Πρέπει εδώ να πούμε ότι το κβαντικό κέρμα αντιπροσωπεύει τα κβαντικά συστήματα δύο καταστάσεων (Feynman, 1965).

- Η κατάσταση ενός κβαντικού συστήματος δύο καταστάσεων περιγράφεται από το διάνυσμα κατάστασης. Στην περίπτωση του κβαντικού κέρματος, το διάνυσμα κατάστασης φαίνεται στο Σχήμα 1-2. Από εδώ και πέρα οι όροι «κατάσταση» και «διάνυσμα κατάστασης» θα είναι ισοδύναμοι, θα σημαίνουν δηλαδή το ίδιο πράγμα.
- Οι δύο δυνατές καταστάσεις, στις οποίες μπορεί να βρεθεί μετά από μέτρηση ένα κβαντικό σύστημα δύο καταστάσεων, ονομάζονται βασικές καταστάσεις. Στην περίπτωση του κβαντικού κέρματος αυτές είναι οι $|H\rangle$ και $|T\rangle$.
- Το κβαντικό σύστημα μπορεί να βρεθεί και σε καταστάσεις που είναι υπερθέσεις των δύο βασικών καταστάσεων. Η υπέρθεση των δύο βασικών καταστάσεων περιγράφεται από τη σχέση (1.1).
- Οι αριθμοί a και b , με τους οποίους πολλαπλασιάζονται οι δύο βασικές καταστάσεις στη σχέση (1.1), ονομάζονται πλάτη πιθανότητας και είναι γενικά μιγαδικοί αριθμοί. Το Σχήμα 1-2 απεικονίζει την περίπτωση που οι a και b είναι θετικοί πραγματικοί αριθμοί. Στη γενική περίπτωση που τα πλάτη πιθανότητας είναι μιγαδικά τότε το διάνυσμα κατάστασης υπάρχει σε έναν χώρο που ονομάζεται χώρος Hilbert.
- Η μέτρηση της κατάστασης ενός κβαντικού συστήματος δύο καταστάσεων μπορεί να έχει μόνο δύο δυνατά αποτελέσματα που αντιστοιχούν στις δύο βασικές καταστάσεις. Η μέτρηση καταστρέφει την υπέρθεση και αναγκάζει το κβαντικό σύστημα να βρεθεί σε μία από τις δύο βασικές καταστάσεις. Αυτό ονομάζεται «καταστροφή της υπέρθεσης». Ο όρος αποδίδει το ίδιο φαινόμενο που αποδίδεται και με τον όρο «κατάρρευση της κυματοσυνάρτησης», που ίσως έχετε συναντήσει.
- Δεν μπορούμε να προβλέψουμε με βεβαιότητα το αποτέλεσμα της μέτρησης της κατάστασης ενός κβαντικού συστήματος που βρίσκεται σε υπέρθεση καταστάσεων. Το μόνο που μπορούμε να ξέρουμε, είναι οι πιθανότητες να μετρήσουμε μία από τις δύο βασικές καταστάσεις. Οι πιθανότητες δίνονται από το τετράγωνο των πλατών πιθανότητας. Στην περίπτωση του κβαντικού κέρματος οι πιθανότητες δίνονται από τα $|a|^2$ και $|b|^2$ τα οποία είναι μέσα στο σύμβολο της απόλυτης τιμής, γιατί γενικά είναι μιγαδικοί αριθμοί.
- Το μήκος του διανύσματος κατάστασης είναι πάντα ίσο με τη μονάδα. Αυτό ισχύει για όλα τα κβαντικά συστήματα και είναι έτσι, για να μπορεί το άθροισμα των πιθανοτήτων να είναι πάντα ίσο με τη μονάδα. Αυτό πρακτικά σημαίνει ότι έχουμε τη δυνατότητα να γνωρίζουμε όλες τις βασικές καταστάσεις ενός κβαντικού συστήματος.

1.2 Διανύσματα Bra και Ket, συμβολισμός Dirac

Bracket στα Αγγλικά είναι η αγκύλη. Αγκύλες είναι τα σύμβολα μέσα στα οποία περικλείουμε φράσεις ή τμήματα πληροφορίας. Ως αγκύλες χρησιμοποιούνται και τα σύμβολα $>$ και $<$. Ο P. A. M. Dirac, ένας από τους μεγάλους φυσικούς που συνέβαλαν στην ανάπτυξη της κβαντικής μηχανικής, συμβόλισε τα διανύσματα

κατάστασης των κβαντικών συστημάτων βάζοντάς τα σε μισές αγκύλες, δηλαδή σε: $\langle \quad |$ και $|\quad \rangle$. Το πρώτο σύμβολο το ονόμασε bra, από τα τρία πρώτα γράμματα της λέξης bracket και το δεύτερο ket, από τα τρία τελευταία γράμματα της ίδιας λέξης. Τα διανύσματα κατάστασης $|H\rangle$, $|T\rangle$ και $|K\rangle$ που είδαμε προηγουμένως είναι διανύσματα ket (Dirac, 1958).

Τα διανύσματα ket μπορούν να γραφούν ως πίνακες με μία στήλη. Οι πίνακες αυτοί ονομάζονται πίνακες κατάστασης. Στην περίπτωση των κβαντικών συστημάτων δύο καταστάσεων οι πίνακες αυτοί έχουν δύο στοιχεία. Παρακάτω θα γράψουμε το γνωστό μας διάνυσμα κατάστασης $|K\rangle$ ως πίνακα:

$$|K\rangle = a|H\rangle + b|T\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \quad (1.3)$$

Δηλαδή, τα δύο στοιχεία του πίνακα είναι τα μήκη της προβολής του $|K\rangle$ στους άξονες των $|H\rangle$ και $|T\rangle$. Πώς θα γράψουμε τα διανύσματα ket των βασικών καταστάσεων; Για το $|H\rangle$ θα γράψουμε:

$$|H\rangle = 1|H\rangle + 0|T\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (1.4)$$

Για το $|T\rangle$ θα γράψουμε:

$$|T\rangle = 0|H\rangle + 1|T\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (1.5)$$

Αυτά για τα διανύσματα ket των κβαντικών συστημάτων δύο καταστάσεων. Τι είναι όμως τα διανύσματα bra; Για να καταλάβουμε καλύτερα τη σχέση των διανυσμάτων bra και ket ας γράψουμε το γνωστό μας διάνυσμα κατάστασης $|K\rangle$ ως διάνυσμα bra:

$$\langle K| = a^* \langle H| + b^* \langle T| = [a^* \quad b^*] \quad (1.6)$$

όπου a^* και b^* είναι οι μιγαδικοί συζυγείς των a και b . Να θυμηθούμε εδώ ότι ο μιγαδικός συζυγής του αριθμού $(p + iq)$ είναι ο $(p - iq)$. Δηλαδή, ο πίνακας που αντιστοιχεί στο διάνυσμα $\langle K|$ προκύπτει από τον πίνακα που αντιστοιχεί στο διάνυσμα $|K\rangle$ με τη μετατροπή της στήλης σε γραμμή και με την αντικατάσταση των στοιχείων από τα μιγαδικά συζυγή τους. Με τον ίδιο τρόπο γράφουμε και τα διανύσματα bra των βασικών καταστάσεων:

$$\langle H| = 1\langle H| + 0\langle T| = [1 \quad 0] \quad (1.7)$$

$$\langle T| = 0\langle H| + 1\langle T| = [0 \quad 1] \quad (1.8)$$

Ας θεωρήσουμε τώρα μία άλλη κατάσταση του κβαντικού κέρματος την $|N\rangle$:

$$|N\rangle = c|H\rangle + d|T\rangle = \begin{bmatrix} c \\ d \end{bmatrix} \quad (1.9)$$

όπου, φυσικά:

$$|c|^2 + |d|^2 = 1 \quad (1.10)$$

Δηλαδή, όταν το κβαντικό κέρμα βρίσκεται στην κατάσταση αυτή, η πιθανότητα να μετρήσουμε και να βρούμε το κβαντικό κέρμα με το γράμμα H στην πάνω όψη είναι ίση με $|c|^2$ και η πιθανότητα να βρούμε το κβαντικό κέρμα με το γράμμα T στην πάνω όψη είναι ίση με $|d|^2$. Τώρα θα ορίσουμε δύο πολύ σημαντικά γινόμενα, το εσωτερικό και το εξωτερικό γινόμενο δύο διανυσμάτων κατάστασης (Shankar, 1994).

Το εσωτερικό γινόμενο των δύο καταστάσεων $|N\rangle$ και $|K\rangle$ γράφεται $\langle N|K\rangle$, δηλαδή είναι το γινόμενο του bra της πρώτης κατάστασης επί το ket της δεύτερης. Ας το δούμε και με μορφή πινάκων:

$$\langle N|K\rangle = [c^* \quad d^*] \begin{bmatrix} a \\ b \end{bmatrix} = (c^* a + d^* b) \quad (1.11)$$

Το εσωτερικό γινόμενο δύο καταστάσεων είναι ένας αριθμός. Παρακάτω θα υπολογίσουμε τα εσωτερικά γινόμενα των βασικών καταστάσεων του κβαντικού κέρματος. Πρώτα το $\langle H|T\rangle$:

$$\langle H|T\rangle = [1 \quad 0] \begin{bmatrix} 0 \\ 1 \end{bmatrix} = 0 \quad (1.12)$$

Το εσωτερικό γινόμενο $\langle H|H\rangle$ είναι:

$$\langle H|H\rangle [1 \quad 0] \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 1 \quad (1.13)$$

Με τον ίδιο τρόπο υπολογίζουμε και τα γινόμενα $\langle T|H\rangle$ και $\langle T|T\rangle$. Ας γράψουμε όλα τα αποτελέσματα μαζί:

$$\begin{aligned} \langle H|H\rangle &= 1 & \langle H|T\rangle &= 0 \\ \langle T|H\rangle &= 0 & \langle T|T\rangle &= 1 \end{aligned} \quad (1.14)$$

Όταν το εσωτερικό γινόμενο δύο καταστάσεων είναι μηδέν, τότε οι δύο καταστάσεις ονομάζονται ορθογώνιες. Όλες οι βασικές καταστάσεις είναι ορθογώνιες μεταξύ τους. Αυτό μπορούμε να το γράψουμε ως εξής (Schiff, 1983):

$$\langle j|k\rangle = \delta_{jk} \quad (1.15)$$

όπου τα j και k συμβολίζουν τις βασικές καταστάσεις ενός κβαντικού συστήματος. Στην περίπτωση του κβαντικού κέρματος τα j και k είναι τα H και T . Δηλαδή το εσωτερικό γινόμενο δύο βασικών καταστάσεων είναι ίσο με το μηδέν, εκτός από την περίπτωση του γινομένου bra επί ket της ίδιας βασικής κατάστασης, οπότε είναι ίσο με ένα.

Παράδειγμα 1.2

Δίνονται οι παρακάτω δύο καταστάσεις. (Θυμίζουμε εδώ και πάλι ότι οι έννοιες «κατάσταση» και «διάνυσμα κατάστασης» είναι ταυτόσημες):

$$|K\rangle = 0,500|H\rangle - 0,866|T\rangle$$

$$|N\rangle = 0,866|H\rangle + 0,500|T\rangle$$

Θα υπολογίσουμε πρώτα το εσωτερικό γινόμενο $\langle N|K\rangle$:

$$\langle N|K\rangle = [0,866 \quad 0,500] \begin{bmatrix} 0,500 \\ -0,866 \end{bmatrix} = (0,433 - 0,433) = 0$$

Δηλαδή οι δύο καταστάσεις είναι ορθογώνιες μεταξύ τους.

Στη συνέχεια θα υπολογίσουμε το εσωτερικό γινόμενο $\langle K|K\rangle$:

$$\langle K|K\rangle = [0,500 \quad -0,866] \begin{bmatrix} 0,500 \\ -0,866 \end{bmatrix} = (0,25 + 0,75) = 1 \quad \blacklozenge$$

Το εξωτερικό γινόμενο των δύο καταστάσεων $|N\rangle$ και $|K\rangle$ γράφεται $|N\rangle\langle K|$, δηλαδή είναι το γινόμενο του ket της πρώτης κατάστασης επί το bra της δεύτερης. Ας το δούμε και με μορφή πινάκων χρησιμοποιώντας τις καταστάσεις $|K\rangle$ και $|N\rangle$ που δίνονται από τις (1.3) και (1.9):

$$|N\rangle\langle K| = \begin{bmatrix} c \\ d \end{bmatrix} \begin{bmatrix} a^* & b^* \end{bmatrix} = \begin{bmatrix} ca^* & cb^* \\ da^* & db^* \end{bmatrix} \quad (1.16)$$

Δηλαδή το εξωτερικό γινόμενο δύο καταστάσεων είναι ένας πίνακας.

Παράδειγμα 1.3

Δίνονται οι παρακάτω δύο καταστάσεις:

$$|K\rangle = 0,500|H\rangle - 0,866|T\rangle$$

$$|N\rangle = 0,866|H\rangle + 0,500|T\rangle$$

Θα υπολογίσουμε το εξωτερικό γινόμενο $|N\rangle\langle K|$:

$$|N\rangle\langle K| = \begin{bmatrix} 0,866 \\ 0,500 \end{bmatrix} [0,500 \quad -0,866] = \begin{bmatrix} 0,433 & 0,750 \\ 0,250 & -0,433 \end{bmatrix} \quad \blacklozenge$$

Ας συνοψίσουμε:

- Οι καταστάσεις ενός κβαντικού συστήματος παριστάνονται με διανύσματα bra και ket.
- Το εσωτερικό γινόμενο δύο καταστάσεων είναι ένας αριθμός.
- Όταν το εσωτερικό γινόμενο δύο καταστάσεων είναι μηδέν, οι καταστάσεις αυτές είναι ορθογώνιες μεταξύ τους.
- Οι βασικές καταστάσεις ενός κβαντικού συστήματος είναι ορθογώνιες μεταξύ τους.
- Το εξωτερικό γινόμενο δύο καταστάσεων είναι ένας πίνακας.

1.3 Αλλαγή κατάστασης, τελεστές

Ας δούμε πρώτα πώς μπορούμε να αλλάξουμε την κατάσταση του κλασικού κέρματος. Όπως έχουμε πει, το κλασικό κέρμα μπορεί να βρεθεί σε δύο μόνο καταστάσεις: ή στην κατάσταση «H» ή στην κατάσταση «T». Ας γράψουμε αυτές τις καταστάσεις ως πίνακες:

$$\langle H \rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ και } \langle T \rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (1.17)$$

Δύο πράγματα μπορείτε να κάνετε σε ένα κλασικό κέρμα, ή να το αφήσετε όπως είναι ή να το στρέψετε, ώστε η πάνω όψη να πάει κάτω. Γενικά οι δράσεις που ασκούνται σε συστήματα περιγράφονται από μαθηματικά αντικείμενα που ονομάζονται τελεστές. Οι τελεστές στην κβαντική μηχανική μπορούν να παρασταθούν με πίνακες. Ας συμβολίσουμε τη δράση «δεν κάνω τίποτα», δηλαδή αφήνω το κέρμα όπως είναι, με \hat{I} . Το \hat{I} είναι ένας τελεστής. Από εδώ και εμπρός θα συμβολίζουμε τους τελεστές με κεφαλαίο γράμμα που επάνω του θα έχει το σύμβολο: $\hat{}$ και τους πίνακες με κεφαλαίο γράμμα. Δηλαδή ο τελεστής \hat{I} περιγράφεται από τον πίνακα [I] που γράφεται ως εξής:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (1.18)$$

Ας συμβολίσουμε τη δράση «στρέφω το κέρμα» με \hat{A} . Ο αντίστοιχος πίνακας [A] είναι:

$$A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (1.19)$$

Θεωρούμε ότι το κλασικό κέρμα βρίσκεται στην κατάσταση «T» και το στρέφουμε, ώστε να βρεθεί στην κατάσταση «H». Με τη μορφή των τελεστών αυτό γράφεται (Jordan, 1986):

$$\hat{A} \langle T \rangle = \langle H \rangle \quad (1.20)$$

και με μορφή πινάκων:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (1.21)$$

Αν το κέρμα βρίσκεται στην κατάσταση «T» και το αφήνουμε όπως είναι, γράφουμε:

$$\hat{I} \langle T \rangle = \langle T \rangle \quad (1.22)$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (1.23)$$

Με τον ίδιο τρόπο γράφουμε και τις περιπτώσεις που το κλασικό κέρμα βρίσκεται στην κατάσταση «H» και το στρέφουμε ή το αφήνουμε όπως είναι.

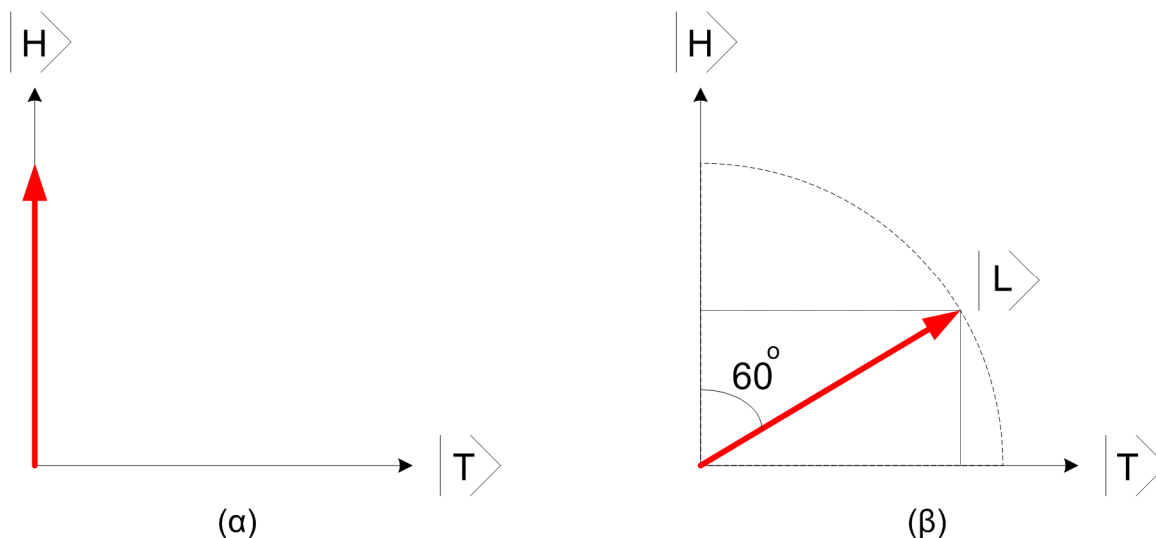
Ας δούμε τώρα και το κβαντικό κέρμα. Όπως και το κλασικό κέρμα μπορούμε να το αφήσουμε όπως είναι ή να το στρέψουμε. Μπορούμε όμως να δράσουμε στο κβαντικό κέρμα με τρόπους που δεν έχουν κλασικό αντίστοιχο, μπορούμε δηλαδή να πολλαπλασιάσουμε τον πίνακα της κατάστασής του και με άλλους πολλούς

πίνακες με 2×2 στοιχεία. Για παράδειγμα αν το κβαντικό κέρμα βρίσκεται στη βασική κατάσταση $|H\rangle$ μπορούμε να δράσουμε όπως παρακάτω:

$$\begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} \quad (1.24)$$

Δηλαδή η δράση μας είχε ως αποτέλεσμα τη μετάβαση του κβαντικού κέρματος από τη βασική κατάσταση $|H\rangle$ σε μία νέα κατάσταση $|L\rangle$ που είναι υπέρθεση των βασικών καταστάσεων και δίνεται από:

$$|L\rangle = \frac{1}{2}|H\rangle + \frac{\sqrt{3}}{2}|T\rangle \quad (1.25)$$



Σχήμα 1-3 Σχηματική παράσταση της δράσης που περιγράφεται από την σχέση (1.24). (α) Το διάνυσμα κατάστασης βρίσκεται πάνω στον άξονα $|H\rangle$ και το κβαντικό κέρμα βρίσκεται στην κατάσταση $|H\rangle$. (β) Η νέα κατάσταση $|L\rangle$

Το αποτέλεσμα της δράσης αυτής φαίνεται στο Σχήμα 1-3. Στο Σχήμα 1-3(α) φαίνεται ότι το κβαντικό κέρμα βρίσκεται στη βασική κατάσταση $|H\rangle$ και στο Σχήμα 1-3(β) φαίνεται η κατάσταση μετά τη δράση που περιγράφεται από την (1.24). Μπορούμε να πούμε ότι περιστρέψαμε το διάνυσμα κατάστασης του κβαντικού κέρματος 60° κατά τη φορά των δεικτών του ρολογιού.

Εκτός δηλαδή από τις δύο δράσεις «δεν κάνω τίποτα» και «στρέφω το κέρμα», που μπορούν να ασκηθούν και στο κλασικό και στο κβαντικό κέρμα, υπάρχουν και άλλες πολλές δράσεις που μπορούν να ασκηθούν μόνο στο κβαντικό κέρμα. Οι δράσεις αυτές έχουν ως αποτέλεσμα την περιστροφή του διανύσματος κατάστασης του κβαντικού κέρματος. Οι δράσεις αυτές (οι τελεστές αυτοί) περιγράφονται με πίνακες με 2×2 στοιχεία. Τα στοιχεία αυτά είναι γενικά μιγαδικά, οπότε η περιστροφή του διανύσματος γίνεται στον χώρο Hilbert και τότε δεν μπορούμε να την απεικονίσουμε με το Σχήμα 1-3 όπως κάναμε προηγουμένως (von Neumann, 1955). Αυτά όμως θα τα δούμε σε επόμενο κεφάλαιο.

Όλοι οι πίνακες με 2×2 στοιχεία μπορούν να παραστήσουν δράσεις που περιστρέφουν το διάνυσμα κατάστασης; Όχι. Το μήκος του διανύσματος κατάστασης πρέπει πάντα να είναι ίσο με τη μονάδα, άρα

αποκλείονται οι πίνακες που, όταν τους πολλαπλασιάζουμε με πίνακες καταστάσεων, μεταβάλλουν το μήκος του διανύσματος κατάστασης.

Υπάρχει ακόμη ένας περιορισμός. Η κβαντική μηχανική είναι συμμετρική ως προς τη φορά του χρόνου. Δηλαδή, αν δεν είμαστε αυστηροί, μπορούμε να πούμε ότι η συμπεριφορά ενός κβαντικού συστήματος δεν αλλάζει, αν αλλάξει η φορά ροής του χρόνου. Αυτό για το κβαντικό κέρμα σημαίνει ότι, αν με μία δράση αλλάζουμε την κατάσταση του από $|K\rangle$ σε $|L\rangle$, τότε πρέπει με την αντίστροφη δράση να μπορούμε να γυρίσουμε την κατάσταση από $|L\rangle$ πίσω στην $|K\rangle$. Δηλαδή, αν πολλαπλασιάζοντας με έναν πίνακα την κατάσταση $|K\rangle$ παίρνουμε την κατάσταση $|L\rangle$ τότε πολλαπλασιάζοντας την κατάσταση $|L\rangle$ με τον αντίστροφο αυτού του πίνακα πρέπει να πάρουμε την κατάσταση $|K\rangle$. Οι πίνακες που είναι κατάλληλοι για την περιστροφή διανυσμάτων κατάστασης ονομάζονται ορθομοναδιαίοι. Για τους πίνακες αυτούς ισχύει: $[A]^\dagger [A] = [A] [A]^\dagger = [I]$ και $[A]^\dagger = [A]^{-1}$ (Gasiowicz, 1974).

Παράδειγμα 1.4

Δίνεται η παρακάτω κατάσταση:

$$|L\rangle = \frac{1}{2}|H\rangle + \frac{\sqrt{3}}{2}|T\rangle$$

Δρούμε στην κατάσταση αυτή για να πάρουμε μία νέα κατάσταση. Η δράση μας περιγράφεται από τον πίνακα B:

$$B = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

Υπολογίζουμε τη νέα κατάσταση $|K\rangle$:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} = \begin{bmatrix} \frac{1+\sqrt{3}}{2\sqrt{2}} \\ \frac{1-\sqrt{3}}{2\sqrt{2}} \end{bmatrix}$$

οπότε:

$$|K\rangle = \frac{1+\sqrt{3}}{2\sqrt{2}}|H\rangle + \frac{1-\sqrt{3}}{2\sqrt{2}}|T\rangle$$

Ας δούμε αν το μήκος του διανύσματος $|K\rangle$ είναι ίσο με τη μονάδα:

$$\left| \frac{1+\sqrt{3}}{2\sqrt{2}} \right|^2 + \left| \frac{1-\sqrt{3}}{2\sqrt{2}} \right|^2 = \frac{1+3+2\sqrt{3}}{8} + \frac{1+3-2\sqrt{3}}{8} = 1 \spadesuit$$

Ας συνοψίσουμε:

- Σε ένα κλασικό σύστημα δύο καταστάσεων μπορούμε να ασκήσουμε δύο δράσεις. Δηλαδή, ή να το αφήσουμε όπως είναι ή να το αλλάξουμε κατάσταση, από αυτή που βρίσκεται στην άλλη.
- Σε ένα κβαντικό σύστημα δύο καταστάσεων (για να είμαστε πιο ακριβείς, πρέπει να πούμε δύο βασικών καταστάσεων) εκτός από τις προηγούμενες δύο δράσεις, μπορούμε να ασκήσουμε και άλλες δράσεις, μεταφέροντάς το από μία βασική κατάσταση σε οποιαδήποτε υπέρθεση βασικών καταστάσεων. Μπορούμε επίσης να το μεταφέρουμε και από μία υπέρθεση καταστάσεων σε μία άλλη υπέρθεση καταστάσεων όπως κάναμε στο παράδειγμα 1.4. Φυσικά μπορούμε να το μεταφέρουμε και από τη μία βασική κατάσταση στην άλλη.
- Οι δράσεις αυτές ονομάζονται τελεστές και περιγράφονται από τετραγωνικούς πίνακες που έχουν 2×2 στοιχεία. Τα στοιχεία αυτά είναι μιγαδικά.
- Οι δράσεις είναι περιστροφές του διανύσματος κατάστασης.

Θυμηθείτε ότι οι όροι «κατάσταση», «διάνυσμα κατάστασης» και «πίνακας κατάστασης» σημαίνουν το ίδιο πράγμα. Το ίδιο και οι όροι «δράση» και «τελεστής». Οι τελεστές περιγράφονται με πίνακες.

1.4 Το κβαντικό παιχνίδι

Έχουμε μάθει αρκετά πράγματα για τα κβαντικά συστήματα δύο καταστάσεων και μπορούμε να εξηγήσουμε πως κέρδισε ο Quant (Eisert, 1999). Ας δούμε το παιχνίδι βήμα προς βήμα:

1. Ο Captain Class βάζει το κέρμα στο τραπέζι με την πλευρά που έχει το γράμμα H προς τα επάνω. Η κατάσταση του κέρματος δίνεται από τον πίνακα:

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

Ο Captain Class γράφει το γράμμα H σε ένα χαρτί, βάζει το χαρτί σε ένα φάκελο, τον σφραγίζει, τον βάζει στην άκρη του τραπεζιού και καλύπτει το κέρμα.

2. Ο Quant έρχεται στο δωμάτιο και βάζει το χέρι του μέσα στο κάλυμμα για να δράσει στο κέρμα. Ο Quant είναι κβαντική οντότητα και με τη δράση του φέρνει το κέρμα σε υπέρθεση καταστάσεων. Επιλέγει να χρησιμοποιήσει τη δράση που περιγράφεται από τον πίνακα B που είδαμε στο παράδειγμα 1.4. Θα υπολογίσουμε τη νέα κατάσταση του κέρματος:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

3. Ο Captain Class βάζει το χέρι του μέσα στο κάλυμμα και δρα στο κέρμα. Ο Captain Class μπορεί να δράσει με δύο μόνο τρόπους. Μπορεί να αφήσει το κέρμα όπως είναι ή να το στρέψει. Οι δύο αυτές δράσεις περιγράφονται από τους πίνακες I και A που δίνονται από τις σχέσεις (1.18) και (1.19). Επιλέγει να στρέψει το κέρμα. Ας υπολογίσουμε τη νέα κατάσταση του κέρματος:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}$$

4. Ο Quant βάζει για δεύτερη φορά το χέρι του μέσα στο κάλυμμα, για να δράσει στο κέρμα. Επιλέγει και αυτή τη φορά να χρησιμοποιήσει τη δράση που περιγράφεται από τον πίνακα B . Θα υπολογίσουμε τη νέα κατάσταση του κέρματος:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

5. Βγάζουν το κάλυμμα, ανοίγουν το φάκελο και βρίσκουν το κέρμα με την αρχική όψη προς τα επάνω. Ο Captain Class χάνει.

Ας κάνουμε τώρα όλους τους υπολογισμούς μαζί:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad (1.26)$$

Στο δεξιό μέρος της εξίσωσης (1.26) βρίσκεται ο πίνακας της τελικής κατάστασης του κέρματος. Στο αριστερό μέρος της (1.26) αμέσως αριστερά από το ίσον βρίσκεται ο πίνακας της αρχικής κατάστασης του κέρματος. Ο πίνακας που περιγράφει την πρώτη δράση, δηλαδή τη δράση του Quant, τοποθετείται αμέσως αριστερά από τον πίνακα της αρχικής κατάστασης. Ο πίνακας που περιγράφει τη δεύτερη δράση, δηλαδή τη δράση του Captain Class, τοποθετείται αμέσως αριστερά από τον πίνακα της πρώτης δράσης. Τέλος, αριστερά από τον πίνακα της δεύτερης δράσης τοποθετείται ο πίνακας που περιγράφει την τρίτη δράση, δηλαδή την τελευταία δράση του Quant. Οι πίνακες που περιγράφουν δράσεις τοποθετούνται από τα δεξιά προς τα αριστερά σύμφωνα με τη χρονική σειρά που ασκήθηκαν οι δράσεις. Αυτό είναι πολύ σημαντικό.

Θα δούμε τώρα έναν άλλο γύρο του παιχνιδιού. Και αυτή τη φορά ο Captain Class τοποθετεί αρχικά το κέρμα στο τραπέζι με την πλευρά που έχει το γράμμα H προς τα επάνω. Όταν έρχεται όμως η σειρά του να δράσει, επιλέγει να αφήσει το κέρμα όπως είναι. Η δράση του αυτή περιγράφεται από τον πίνακα I . Ο Quant επιλέγει πάλι την ίδια δράση. Θα κάνουμε όλους τους υπολογισμούς μαζί:

$$\begin{aligned}
& \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \\
& = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}
\end{aligned} \tag{1.27}$$

Ο Quant πάλι κερδίζει. Το ίδιο θα συνέβαινε ακόμα και αν ο Captain Class τοποθετούσε το κέρμα με το γράμμα T στην πάνω όψη. Ο Quant πάντα κερδίζει επιλέγοντας την ίδια δράση άσχετα με το τι θα κάνει ο Captain Class.

- Στο παιχνίδι αυτό ο Captain Class αντιπροσωπεύει έναν κλασικό υπολογιστή και ο Quant έναν κβαντικό υπολογιστή.
- Οι σχέσεις (1.26) και (1.27) είναι οι πρώτοι μας κβαντικοί υπολογισμοί.
- Το παιχνίδι αυτό δείχνει μόνο ένα μέρος από τις δυνατότητες των κβαντικών υπολογιστών που προέρχεται από την υπέρθεση των βασικών καταστάσεων.
- Τα κβαντικά παιχνίδια είναι ένα πάρα πολύ σημαντικό ερευνητικό αντικείμενο της επιστήμης των κβαντικών υπολογιστών και έχει ως στόχο την ανάπτυξη μεθόδων για την προσομοίωση φυσικών φαινομένων, συστημάτων και διεργασιών με κβαντικούς υπολογιστές.

1.5 Η εξίσωση του Schrödinger

Οι μεταβολές της κατάστασης, στο χώρο και στο χρόνο, ενός κβαντικού συστήματος περιγράφονται από την εξίσωση του Schrödinger (Greiner, 1989). Η εξίσωση αυτή εκφράζει την αρχή της διατήρησης της ενέργειας. Η ολική ενέργεια ενός φυσικού συστήματος, E , είναι ίση με το άθροισμα της κινητικής του ενέργειας, E_{KIN} και της δυναμικής του ενέργειας $E_{\text{ΔΥΝ}}$:

$$E = E_{\text{KIN}} + E_{\text{ΔΥΝ}} \tag{1.28}$$

Η εξίσωση (1.28) γράφεται αναλυτικά ως εξής:

$$E = \frac{1}{2} m v^2 + V(x, t) \tag{1.29}$$

Στην παραπάνω εξίσωση, v είναι η ταχύτητα του συστήματος, m η μάζα του και $V(x, t)$ η δυναμική του ενέργεια, η οποία εξαρτάται από τον χώρο και τον χρόνο. Αν θυμηθούμε ότι η ορμή είναι: $p = m v$ και αντικαταστήσουμε, θα έχουμε:

$$E = \frac{p^2}{2m} + V(x, t) \tag{1.30}$$

Στην κβαντική μηχανική, οι ποσότητες που μπορούν να παρατηρηθούν και να μετρηθούν, όπως η ενέργεια και η ορμή, αντιπροσωπεύονται από τελεστές. Ο τελεστής που αντιπροσωπεύει την ολική ενέργεια είναι:

$$E \rightarrow i\hbar \frac{\partial}{\partial t} \quad (1.31)$$

Ο τελεστής που αντιπροσωπεύει την ορμή είναι:

$$p \rightarrow -i\hbar \frac{\partial}{\partial x} \quad (1.32)$$

Αν αντικαταστήσουμε τους τελεστές αυτούς στη θέση της ολικής ενέργειας και της ορμής στην εξίσωση (1.30) θα έχουμε (Weinberg, 1987):

$$i\hbar \frac{\partial}{\partial t} = -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} + V(x,t) \quad (1.33)$$

Η εξίσωση αυτή είναι μία εξίσωση τελεστών και για να αποκτήσει φυσικό νόημα, θα πρέπει οι τελεστές να δράσουν πάνω σε κάποια συνάρτηση (Morrison, 1990). Η συνάρτηση πάνω στην οποία δρουν οι τελεστές είναι η $\Psi(x,t)$, η οποία ονομάζεται συνάρτηση κύματος. Η εξίσωση (1.33) με τους τελεστές να δρουν πάνω στη συνάρτηση κύματος είναι:

$$i\hbar \frac{\partial}{\partial t} \Psi(x,t) = -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} \Psi(x,t) + V(x,t)\Psi(x,t) \quad (1.34)$$

Η (1.34) είναι η εξίσωση του Schrödinger σε μία διάσταση. Η εξίσωση αυτή σε τρεις διαστάσεις είναι (Hanabuss, 1997):

$$i\hbar \frac{\partial}{\partial t} \Psi(r,t) = -\frac{\hbar^2}{2m} \nabla^2 \Psi(r,t) + V(r,t)\Psi(r,t) \quad (1.35)$$

Η συνάρτηση κύματος είναι μία μιγαδική συνάρτηση και δεν αποδίδεται σε αυτή καμία φυσική έννοια. Όμως, το μέτρο αυτής της συνάρτησης είναι μία πραγματική συνάρτηση:

$$P(x,t) = |\Psi(x,t)|^2 \quad (1.36)$$

Η $P(x,t)$, είναι η πυκνότητα πιθανότητας από την οποία μπορούμε να υπολογίσουμε την πιθανότητα ένα κβαντικό σύστημα, το οποίο έχει ολική ενέργεια E , να βρίσκεται στην θέση x την χρονική στιγμή t . Μπορούμε να γράψουμε την εξίσωση του Schrödinger ως εξής:

$$i\hbar \frac{\partial}{\partial t} \Psi(x,t) = \left(-\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} + V(x,t) \right) \Psi(x,t) \quad (1.37)$$

Θα αντικαταστήσουμε τους τελεστές του δεξιού μέλους της εξίσωσης με έναν μόνο τελεστή:

$$H = \left(-\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} + V(x,t) \right) \quad (1.38)$$

Ο τελεστής H ονομάζεται τελεστής του Hamilton ή Hamiltonian και αντιπροσωπεύει την ενέργεια του κβαντικού συστήματος. Μετά από αυτό η εξίσωση του Schrödinger γίνεται (Merzbacher, 1970):

$$i\hbar \frac{\partial}{\partial t} \Psi(x,t) = H \Psi(x,t) \quad (1.39)$$

Αν το δυναμικό $V(x,t)$ δεν εξαρτάται από τον χρόνο, τότε και η συνάρτηση κύματος δεν εξαρτάται από τον χρόνο. Στην περίπτωση αυτή η εξίσωση του Schrödinger παίρνει τη μορφή:

$$E \Psi(x) = H \Psi(x) \quad (1.40)$$

Μπορούμε να μην γράφουμε πια τη μεταβλητή x και να έχουμε:

$$E \Psi = H \Psi \quad (1.41)$$

Η εξίσωση του Schrödinger στην μορφή της (1.41) μπορεί να γραφεί και με μορφή πινάκων:

$$E[\Psi] = [H][\Psi] \quad (1.42)$$

Η ενέργεια E είναι ένας πραγματικός αριθμός. Ο πίνακας $[\Psi]$, που αντιπροσωπεύει τη συνάρτηση κύματος, έχει μία στήλη και γραμμές όσες και οι βασικές καταστάσεις του κβαντικού συστήματος. Είναι δηλαδή ένα διάνυσμα και το όνομά του είναι διάνυσμα κατάστασης ή κατάσταση. Αν το κβαντικό σύστημα έχει n βασικές καταστάσεις, τότε ο $[\Psi]$ είναι ένας πίνακας με διαστάσεις $n \times 1$. Ο πίνακας $[H]$, που αντιπροσωπεύει τον τελεστή Hamilton, είναι ένας τετραγωνικός πίνακας διαστάσεων $n \times n$.

Οι ιδιοτιμές του πίνακα $[H]$ είναι n τον αριθμό, και είναι οι διακριτές ενεργειακές τιμές τις οποίες μπορεί να πάρει το κβαντικό σύστημα. Αφού η ενέργεια είναι κάτι που μπορούμε να το μετρήσουμε, κάτι πραγματικό δηλαδή, θα πρέπει και οι ιδιοτιμές του $[H]$ να είναι πραγματικοί αριθμοί. Υπάρχει ένα είδος πινάκων των οποίων οι ιδιοτιμές είναι πάντα πραγματικοί αριθμοί. Οι πίνακες αυτοί ονομάζονται Ερμιτιανοί και έχουν την εξής ιδιότητα:

$$[H] = [H]^\dagger \quad (1.43)$$

Στα επόμενα κεφάλαια, δεν θα χρησιμοποιούμε το $[]$ για να συμβολίζουμε πίνακες, οι οποίοι θα συμβολίζονται με ένα κεφαλαίο γράμμα. Οι τελεστές, θα συμβολίζονται και αυτοί με κεφαλαίο γράμμα. Αν κάπου υπάρχει πιθανότητα σύγχυσης τότε θα χρησιμοποιούμε το $[]$ για τους πίνακες και το $\hat{}$ για τους τελεστές.

Στα κβαντικά συστήματα δύο καταστάσεων που μελετήσαμε στο κεφάλαιο αυτό, οι καταστάσεις αντιπροσωπεύονταν από πίνακες με μία στήλη και δύο γραμμές, ενώ οι τελεστές από τετραγωνικούς πίνακες με 2×2 στοιχεία. Οι δράσεις των τελεστών σε καταστάσεις δεν είναι τίποτε άλλο παρά η εφαρμογή της εξίσωσης του Schrödinger (Perry, 2012). Αυτό θα γίνει πιο κατανοητό στα επόμενα κεφάλαια.

Βιβλιογραφία

- Bell J. S., *Speakable and unspeakable in quantum mechanics*, Cambridge University Press, 1987.
- Dirac P. A. M., *The principles of quantum mechanics*, Oxford University Press, 1958 (ανατύπωση 1999).
- Eisert J., Wilkens M. & Lewenstein M., Quantum Games and Quantum Strategies, *Physical Review Letters*, 83, pp. 3077–3080, 1999.
- Feynman R. P., Leighton R. B. & Sands M., *The Feynman lectures on Physics*, Vol. III, Addison-Wesley, 1965.
- Gasiorowicz S., *Quantum Physics*, John Willey and Sons, 1974

- Greiner W., *Quantum mechanics. An introduction*, Springer-Verlag, 1989.
- Hanabuss K., *An Introduction to quantum theory*, Oxford University Press, 1997.
- Jordan T. E., *Quantum mechanics in simple matrix form*, John Willey and Sons, 1986.
- Merzbacher E., *Quantum mechanics*, John Willey and Sons, 1970.
- Morrison M. A., *Understanding quantum Physics*, Prentice Hall, 1990.
- von Neumann J., *Mathematical foundations of quantum mechanics*, Princeton University Press, 1955 (ανατύπωση 1983).
- Perry R. T., *Quantum computing from the ground up*, World Scientific, 2012.
- Schiff L. I., *Quantum mechanics*, McGraw-Hill, 1968.
- Shankar R., *Principles of quantum mechanics*, Plenum Press, 1994.
- Weinberg S., *Towards the final laws of Physics*, The 1986 Dirac Memorial Lectures, p. 61, Cambridge University Press, 1987.

Ασκήσεις

Άσκηση 1.1

Ποια από τα παρακάτω διανύσματα είναι διανύσματα κατάστασης;
(Να κάνετε τις πράξεις με ακρίβεια δεύτερου δεκαδικού ψηφίου)

α. $|K\rangle = 0,7071|H\rangle + 0,7071|T\rangle$

β. $|K\rangle = 0,70|H\rangle + 0,30|T\rangle$

γ. $|K\rangle = -0,500|H\rangle + 0,866|T\rangle$

δ. $|K\rangle = 0,50|H\rangle - 0,50|T\rangle$

Άσκηση 1.2

Ποια από τα παρακάτω διανύσματα είναι διανύσματα κατάστασης;
(Να κάνετε τις πράξεις με ακρίβεια δεύτερου δεκαδικού ψηφίου)

α. $|K\rangle = (0,4472 + i 0,4472)|H\rangle + (0,5916 + i 0,5000)|T\rangle$

β. $|K\rangle = -0,500|H\rangle + i 0,866|T\rangle$

γ. $|K\rangle = \cos \theta |H\rangle + \sin \theta |T\rangle$

Άσκηση 1.3

Να υπολογίσετε το εσωτερικό γινόμενο $\langle N | K \rangle$ των καταστάσεων:

$$|K\rangle = \frac{\sqrt{2}}{2}|H\rangle - \frac{\sqrt{2}}{2}|T\rangle$$

$$|N\rangle = \frac{\sqrt{2}}{2}|H\rangle + \frac{\sqrt{2}}{2}|T\rangle$$

Άσκηση 1.4

Να υπολογίσετε το εσωτερικό γινόμενο $\langle N|K\rangle$ των καταστάσεων:

$$|K\rangle = -\frac{1}{2}|H\rangle + \frac{\sqrt{3}}{2}|T\rangle$$

$$|N\rangle = \frac{\sqrt{2}}{2}|H\rangle + \frac{\sqrt{2}}{2}|T\rangle$$

Άσκηση 1.5

Να αποδείξετε ότι το εσωτερικό γινόμενο $\langle K|K\rangle$ μίας κατάστασης $|K\rangle$ είναι ίσο με τη μονάδα.

Άσκηση 1.6

Να υπολογίσετε το εξωτερικό γινόμενο $|K\rangle\langle N|$ των καταστάσεων:

$$|K\rangle = \frac{1}{2}|H\rangle - \frac{\sqrt{3}}{2}|T\rangle$$

$$|N\rangle = \frac{\sqrt{2}}{2}|H\rangle + \frac{\sqrt{2}}{2}|T\rangle$$

Άσκηση 1.7

Θεωρούμε μία δράση που περιγράφεται από τον πίνακα H :

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}$$

Να βρείτε τις καταστάσεις που προκύπτουν ως αποτέλεσμα της δράσης αυτής στις βασικές καταστάσεις $|H\rangle$ και $|T\rangle$. Βεβαιωθείτε ότι το μήκος των νέων διανυσμάτων κατάστασης είναι ίσο με τη μονάδα.

Άσκηση 1.8

Θεωρούμε μία δράση που περιγράφεται από τον πίνακα P :

$$P = \begin{bmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$$

Να βρείτε την κατάσταση που προκύπτει ως αποτέλεσμα της δράσης αυτής στη κατάσταση:

$$|N\rangle = \frac{1}{\sqrt{2}}|H\rangle - \frac{1}{\sqrt{2}}|T\rangle$$

Βεβαιωθείτε ότι το μήκος του νέου διανύσματος κατάστασης είναι ίσο με τη μονάδα.

Άσκηση 1.9

Θεωρούμε δύο δράσεις που περιγράφονται από τους πίνακες H και P :

$$H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \quad P = \begin{bmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{bmatrix}$$

Δρούμε στη βασική κατάσταση $|T\rangle$ πρώτα με τη δράση που περιγράφεται από τον πίνακα P και στη συνέχεια με τη δράση που περιγράφεται από τον πίνακα H . Να βρείτε την κατάσταση που προκύπτει ως αποτέλεσμα των δράσεων αυτών. Βεβαιωθείτε ότι το μήκος των νέων διανυσμάτων κατάστασης είναι ίσο με τη μονάδα.

Άσκηση 1.10

Να κάνετε τους υπολογισμούς ενός γύρου του παιχνιδιού όπου ο Captain Class τοποθετεί αρχικά το κέρμα στο τραπέζι με την πλευρά που έχει το γράμμα «T» προς τα επάνω και, όταν έρχεται η σειρά του να δράσει, επιλέγει να αφήσει το κέρμα όπως είναι.

Άσκηση 1.11

Να κάνετε τους υπολογισμούς ενός γύρου του παιχνιδιού όπου ο Captain Class τοποθετεί αρχικά το κέρμα στο τραπέζι με την πλευρά που έχει το γράμμα «T» προς τα επάνω και, όταν έρχεται η σειρά του να δράσει, επιλέγει να στρέψει το κέρμα.

2. Αποθήκευση της κβαντικής πληροφορίας

Σύνοψη

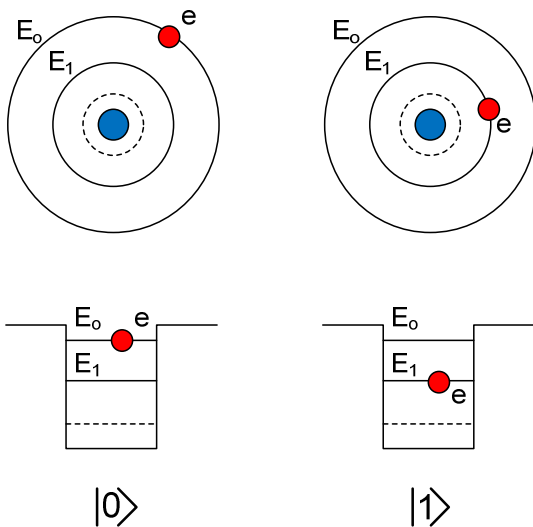
Στο κεφάλαιο αυτό θα περιγραφεί η μονάδα της κβαντικής πληροφορίας που είναι το κβαντικό bit (quantum bit). Θα περιγραφούν φυσικά συστήματα τα οποία μπορούν να χρησιμοποιηθούν ως κβαντικά bits. Θα δοθεί η μαθηματική περιγραφή του κβαντικού bit ως διανύσματος του χώρου Hilbert και η παράστασή του με χρήση της σφαίρας Bloch. Στη συνέχεια θα περιγραφεί ο τρόπος με τον οποίο πολλά κβαντικά bits μπορούν να αποτελέσουν έναν κβαντικό καταχωρητή, όπου αποθηκεύεται η κβαντική πληροφορία. Θα δοθεί η μαθηματική περιγραφή των κβαντικών καταχωρητών ως διανυσμάτων στον χώρο Hilbert.

Προαπαιτούμενη γνώση

Γραμμική άλγεβρα και το πρώτο κεφάλαιο του βιβλίου αυτού.

2.1 Το κβαντικό bit (qubit)

Στους κλασικούς υπολογιστές μονάδα πληροφορίας είναι το bit. Ένα bit πληροφορίας μπορεί να πάρει μόνο δύο τιμές την «0» και την «1». Στους κβαντικούς υπολογιστές μονάδα πληροφορίας είναι το κβαντικό bit (quantum bit) το οποίο για συντομία γράφεται ως qubit. Το qubit είναι ένα κβαντικό σύστημα δύο καταστάσεων, όπως το κβαντικό κέρμα που είδαμε στο προηγούμενο κεφάλαιο. Όπως θα θυμάστε, συμβολίσαμε τις δύο βασικές καταστάσεις του κβαντικού κέρματος με $|H\rangle$ και $|T\rangle$. Οι δύο βασικές καταστάσεις του qubit συμβολίζονται με $|0\rangle$ και $|1\rangle$



Σχήμα 2.1 Αναπαράσταση ενός qubit από δύο διακριτά ενεργειακά επίπεδα E_0 και E_1 σε ένα άτομο(επάνω) και σε μία κβαντική στιγμή (κάτω).

Υπάρχουν αρκετά κβαντικά συστήματα δύο καταστάσεων τα οποία μπορούν να χρησιμοποιηθούν ως qubits (Rieffel & Polak, 2014). Για παράδειγμα, η κατάσταση του spin ενός σωματιδίου με spin $1/2$, μπορεί να θεωρηθεί ως qubit, όπου η κατάσταση spin $+1/2$ αντιστοιχεί στην βασική κατάσταση $|0\rangle$ και η κατάσταση spin $-1/2$ στη βασική κατάσταση $|1\rangle$:

$$\left|+\frac{1}{2}\right\rangle \rightarrow |0\rangle \quad \text{και} \quad \left|-\frac{1}{2}\right\rangle \rightarrow |1\rangle \quad (2.1)$$

Επίσης, η διεύθυνση πόλωσης ενός φωτονίου μπορεί να αναπαραστήσει ένα qubit, όπου η οριζόντια πόλωση αντιστοιχεί στην κατάσταση $|0\rangle$ και η κάθετη στην $|1\rangle$. Όπως φαίνεται στο Σχήμα 2-1, ένα qubit μπορεί να αναπαρασταθεί και από δύο διακριτά ενεργειακά επίπεδα, E_0 και E_1 , σε ένα άτομο ή σε μία κβαντική στιγμή. Η παρουσία ενός ηλεκτρονίου με ενέργεια ίση με E_1 αντιστοιχεί στην κατάσταση $|1\rangle$ και η παρουσία ενός ηλεκτρονίου με ενέργεια ίση με E_0 αντιστοιχεί στην κατάσταση $|0\rangle$. Το qubit μπορεί ακόμα να παρασταθεί και από τον τρόπο ταλάντωσης δύο ιόντων που βρίσκονται μέσα σε μία παγίδα ιόντων. Η τεχνολογία κατασκευής των κβαντικών υπολογιστών θα καθορίσει ποιο φυσικό κβαντικό σύστημα δύο καταστάσεων θα επιλεγεί για να αναπαραστήσει το qubit (Williams & Clearwater, 2000). Εμείς θέλουμε να περιγράψουμε τα βασικά χαρακτηριστικά και τη λειτουργία των κβαντικών υπολογιστών ανεξάρτητα από την τεχνολογία κατασκευής, οπότε δε χρειάζεται να προσδιορίσουμε ποιο φυσικό κβαντικό σύστημα δύο καταστάσεων χρησιμοποιούμε ως qubit.

Όπως το κβαντικό κέρμα, το qubit μπορεί να βρεθεί σε οποιαδήποτε υπέρθεση των δύο βασικών καταστάσεων:

$$|q\rangle = a|0\rangle + b|1\rangle \quad \text{όπου} \quad |a|^2 + |b|^2 = 1 \quad (2.2)$$

Οι δύο βασικές καταστάσεις του qubit μπορούν να γραφούν ως πίνακες, όπως και οι βασικές καταστάσεις του κβαντικού κέρματος:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{και} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad (2.3)$$

Το ίδιο και η υπέρθεση καταστάσεων:

$$|q\rangle = a|0\rangle + b|1\rangle = a \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \quad (2.4)$$

Όπως και στο κβαντικό κέρμα, οι βασικές καταστάσεις ενός qubit είναι ορθογώνιες μεταξύ τους:

$$\begin{aligned} \langle 0|0\rangle &= 1 & \langle 0|1\rangle &= 0 \\ \langle 1|0\rangle &= 0 & \langle 1|1\rangle &= 1 \end{aligned} \quad (2.5)$$

Οι αριθμοί a και b των εξισώσεων (2.2) και (2.4), που όπως θα θυμάστε ονομάζονται πλάτη πιθανότητας, είναι μιγαδικοί αριθμοί και το διάνυσμα κατάστασης $|q\rangle$ του qubit είναι ένα διάνυσμα στον χώρο Hilbert που έχει δύο διαστάσεις. Στο κεφάλαιο 2.5 περιγράφονται τα κύρια χαρακτηριστικά του χώρου Hilbert.

2.2 Η σφαίρα Bloch

Στο προηγούμενο κεφάλαιο παραστήσαμε το διάνυσμα κατάστασης ενός κβαντικού συστήματος δύο καταστάσεων, όπως το qubit, με τα Σχήματα 1-2 και 1-3. Όμως, μία τέτοια αναπαράσταση είναι χρήσιμη μόνο όταν τα a και b είναι πραγματικοί αριθμοί. Όταν τα πλάτη πιθανότητας είναι, όπως συνήθως, μιγαδικοί αριθμοί, τότε χρειαζόμαστε έναν χώρο Hilbert δύο διαστάσεων ή έναν πραγματικό διανυσματικό χώρο τεσσάρων διαστάσεων για να αναπαραστήσουμε το διάνυσμα κατάστασης του qubit (Brooks, 1999).

Αφού λοιπόν τα πλάτη πιθανότητας a και b είναι μιγαδικοί αριθμοί, μπορούμε να γράψουμε την εξίσωση (2.2) με μια πιο γενική μορφή:

$$|q\rangle = e^{i\gamma} \cos \frac{\theta}{2} |0\rangle + e^{i\delta} \sin \frac{\theta}{2} |1\rangle \quad (2.6)$$

όπου, οι γωνίες γ και δ είναι πραγματικοί αριθμοί. Αφού θυμηθούμε ότι $|e^{i\omega}|^2 = 1$ για κάθε ω , έχουμε:

$$\left| e^{i\gamma} \cos \frac{\theta}{2} \right|^2 + \left| e^{i\delta} \sin \frac{\theta}{2} \right|^2 = \left| \cos \frac{\theta}{2} \right|^2 + \left| \sin \frac{\theta}{2} \right|^2 = 1 \quad (2.7)$$

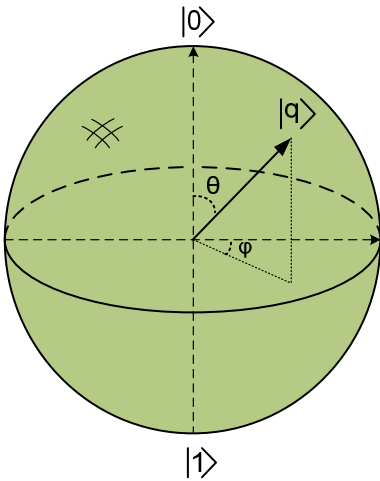
Η εξίσωση (2.6) μπορεί να γραφεί και ως εξής:

$$|q\rangle = e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + e^{i(\delta-\gamma)} \sin \frac{\theta}{2} |1\rangle \right) \quad (2.8)$$

Αν δεν λάβουμε υπόψη τον γενικό όρο φάσης $\exp(i\gamma)$, και ονομάσουμε φ τη διαφορά των γωνιών δ και γ , ($\varphi = \delta - \gamma$), η κατάσταση του qubit γράφεται:

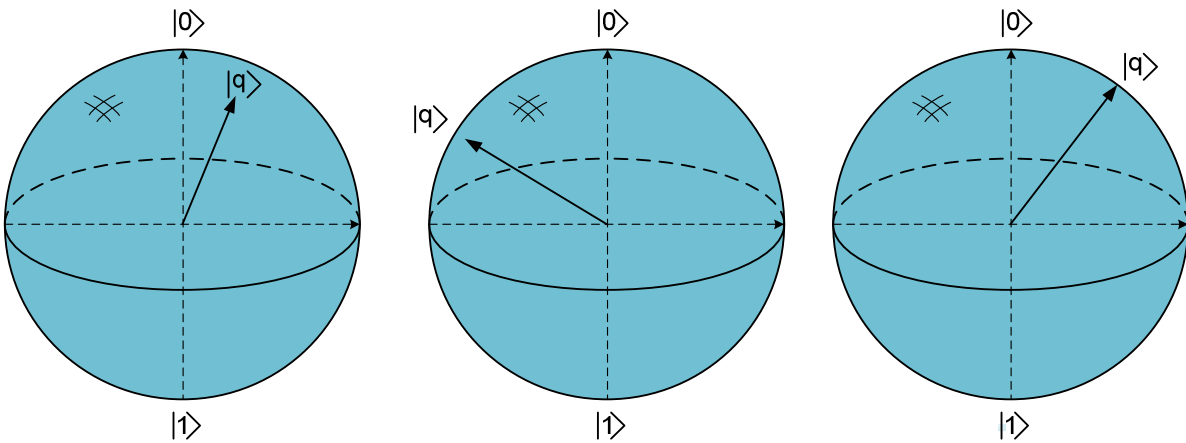
$$|q\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \quad (2.9)$$

Το διάνυσμα κατάστασης του qubit, όπως περιγράφεται από την εξίσωση (2.9) μπορεί να αναπαρασταθεί σε τρεις διαστάσεις με τη χρήση μίας σφαίρας που ονομάζεται σφαίρα Bloch.



Σχήμα 2-2 Το διάνυσμα $|q\rangle$ στη σφαίρα Bloch

Η σφαίρα Bloch έχει ακτίνα ίση με τη μονάδα και το διάνυσμα κατάστασης $|q\rangle$ του qubit, έχει την αρχή του στο κέντρο της σφαίρας και το τέλος του στο σημείο της επιφάνειας της σφαίρας που καθορίζεται από τις γωνίες θ και φ . Φυσικά, το μήκος του $|q\rangle$ είναι ίσο με τη μονάδα (D'Espagnat, 1999). Στο Σχήμα 2-2 φαίνονται τρία διαφορετικά διανύσματα κατάστασης. Όταν το qubit βρίσκεται στη βασική κατάσταση $|0\rangle$, το διάνυσμά του είναι κατακόρυφο με φορά προς τα επάνω και, όταν βρίσκεται στη βασική κατάσταση $|1\rangle$, το διάνυσμά του είναι κατακόρυφο με φορά προς τα κάτω. Προσέξτε ότι, ενώ οι καταστάσεις $|0\rangle$ και $|1\rangle$ είναι ορθογώνιες μεταξύ τους, στη σφαίρα Bloch εμφανίζονται στην ίδια γραμμή. Η σφαίρα Bloch απεικονίζει σχεδόν όλα τα χαρακτηριστικά του qubit (Keyl, 2002). Η γωνία θ καθορίζει τις τιμές των πλατών πιθανότητας. Η γωνία φ ονομάζεται γωνία φάσης. Στο Σχήμα 2-3 φαίνονται τρία διαφορετικά διανύσματα κατάστασης σε σφαίρες Bloch.



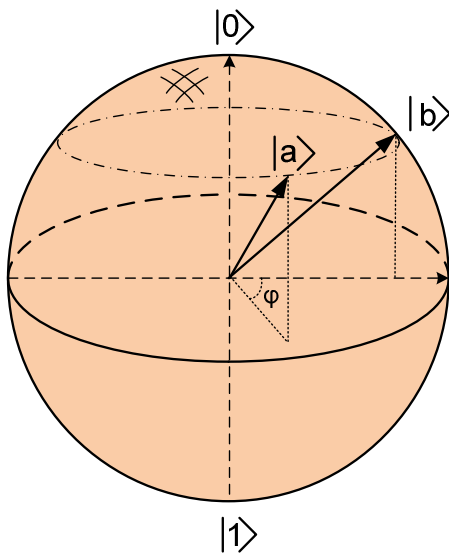
Σχήμα 2-3 Τρία διανύσματα κατάστασης σε σφαίρες Bloch.

Στο Σχήμα 2-4 φαίνονται δύο qubits, τα $|a\rangle$ και $|b\rangle$ τα οποία έχουν την ίδια γωνία θ , αλλά το πρώτο έχει γωνία φάσης φ και το δεύτερο μηδενική γωνία φάσης. Οι καταστάσεις τους δίνονται από:

$$|a\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle$$

(2.10)

$$|b\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} |1\rangle$$



Σχήμα 2-4 Δύο qubits $|a\rangle$ και $|b\rangle$ τα οποία έχουν την ίδια γωνία θ , αλλά το πρώτο έχει γωνία φάσης φ και το δεύτερο μηδενική γωνία φάσης.

Αν μετρήσουμε, η πιθανότητα να βρούμε το καθένα από τα δύο αυτά qubits στην κατάσταση $|0\rangle$ είναι ίση με $|\cos(\theta/2)|^2$ και η πιθανότητα να βρούμε το καθένα από τα δύο αυτά qubits στην κατάσταση $|1\rangle$ είναι

ίση με $|\sin(\theta/2)|^2$. Δηλαδή, είναι αδύνατο να ξεχωρίσουμε με μία μέτρηση δύο qubits που διαφέρουν μόνο κατά τη γωνία φάσης. Παρά το γεγονός ότι η γωνία φάσης δεν επηρεάζει το αποτέλεσμα της μέτρησης παίζει, όπως θα δούμε, σημαντικό ρόλο κατά την εκτέλεση των κβαντικών υπολογισμών, διότι προκαλεί αλληλεπίδραση μεταξύ των qubits.

Παράδειγμα 2.1

Δίνονται τα παρακάτω qubits. Μπορείτε να τα ξεχωρίσετε μετρώντας την κατάστασή τους;

$$|a\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

$$|b\rangle = \frac{1}{\sqrt{2}}|0\rangle + \left(\frac{\sqrt{3}}{2\sqrt{2}} + i\frac{1}{2\sqrt{2}}\right)|1\rangle$$

Η πιθανότητα να βρούμε τα qubits $|a\rangle$ και $|b\rangle$ στην κατάσταση $|0\rangle$ είναι και για τα δύο ίση με $|1/\sqrt{2}|^2 = 0.5$. Η πιθανότητα να βρούμε το $|a\rangle$ στην κατάσταση $|1\rangle$ είναι επίσης 0.5. Η πιθανότητα να βρούμε το $|b\rangle$ στην κατάσταση $|1\rangle$ είναι:

$$\left|\frac{\sqrt{3}}{2\sqrt{2}} + i\frac{1}{2\sqrt{2}}\right|^2 = \left(\sqrt{\left|\frac{\sqrt{3}}{2\sqrt{2}}\right|^2 + \left|\frac{1}{2\sqrt{2}}\right|^2}\right)^2 = \frac{3}{8} + \frac{1}{8} = 0.5$$

δηλαδή ίση με την πιθανότητα να βρούμε το $|a\rangle$ στην κατάσταση $|1\rangle$. Επομένως τα δύο qubits διαφέρουν μόνο κατά τη γωνία φάσης και δεν μπορούμε να τα ξεχωρίσουμε. ♦

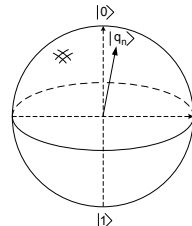
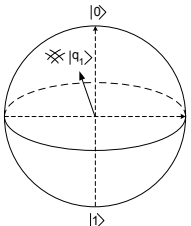
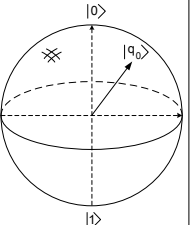
Ας συνοψίσουμε:

- Η μονάδα πληροφορίας στους κβαντικούς υπολογιστές είναι το qubit.
- Το qubit είναι ένα κβαντικό σύστημα δύο καταστάσεων. Οι βασικές του καταστάσεις συμβολίζονται με $|0\rangle$ και $|1\rangle$.
- Το qubit είναι ένα διάνυσμα στον χώρο Hilbert που έχει δύο διαστάσεις και απεικονίζεται ως διάνυσμα στη σφαίρα Bloch.
- Είναι αδύνατο να ξεχωρίσουμε δύο qubits που διαφέρουν μόνο κατά τη γωνία φάσης μετρώντας την κατάστασή τους.

2.3 Ο κβαντικός καταχωρητής

Στους κλασικούς υπολογιστές ένα σύνολο bits αποτελεί έναν καταχωρητή. Στους καταχωρητές αποθηκεύονται συνήθως οι τιμές κάποιων μεταβλητών. Αντίστοιχα, στους κβαντικούς υπολογιστές ένα σύνολο qubits (τα οποία είναι συνήθως διατεταγμένα σε σειρά) αποτελεί έναν κβαντικό καταχωρητή. Στο Σχήμα 2-5 φαίνονται σχηματικά ένας κλασικός και ένας κβαντικός καταχωρητής. Προσέξτε ότι η αρίθμηση των qubits γίνεται από τα δεξιά προς τα αριστερά (Lewin, 2001).

Σε έναν κβαντικό καταχωρητή μπορούμε να αποθηκεύσουμε πολύ περισσότερη πληροφορία από όση στον κλασικό καταχωρητή. Ας το δούμε αυτό αρχίζοντας από την απλούστερη περίπτωση του κβαντικού καταχωρητή που αποτελείται από δύο μόνο qubits, τα $|q_1\rangle$ και $|q_0\rangle$.

0		1		0
				

Σχήμα 2-5 Στο πάνω μέρος του σχήματος φαίνεται ένας κλασικός και στο κάτω ένας κβαντικός καταχωρητής.

Στην περίπτωση αυτή, η κατάσταση του κβαντικού καταχωρητή $|q_R\rangle$ δίνεται από το τανυστικό γινόμενο των καταστάσεων των qubits που τον αποτελούν και γράφεται ως εξής:

$$|q_R\rangle = |q_1\rangle \otimes |q_0\rangle = |q_1\rangle |q_0\rangle = |q_1 q_0\rangle \quad (2.11)$$

όπου το \otimes συμβολίζει το τανυστικό γινόμενο. Τα $|q_1\rangle \otimes |q_0\rangle$, $|q_1\rangle |q_0\rangle$ και $|q_1 q_0\rangle$ συμβολίζουν το ίδιο πράγμα. Τι είναι όμως το τανυστικό γινόμενο; Επειδή οι κβαντικοί υπολογιστές εκτελούν υπολογισμούς, μας ενδιαφέρει η έκφραση του τανυστικού γινομένου με μορφή πινάκων. Αν λοιπόν έχουμε δύο πίνακες με μία στήλη, τον A και τον B :

$$A = \begin{bmatrix} a \\ b \end{bmatrix} \quad B = \begin{bmatrix} c \\ d \end{bmatrix} \quad (2.12)$$

τότε, το τανυστικό γινόμενο των δύο αυτών πινάκων είναι ένας πίνακας με μία στήλη, ο C που δίνεται από:

$$C = A \otimes B = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot c \\ b \cdot d \end{bmatrix} \quad (2.13)$$

Δηλαδή, ο C έχει αριθμό στοιχείων ίσο με το άθροισμα του αριθμού των στοιχείων του A και του B . Το πρώτο του στοιχείο είναι το γινόμενο του πρώτου στοιχείου του A επί το πρώτο στοιχείο του B . Το δεύτερο στοιχείο του C είναι το γινόμενο του πρώτου στοιχείου του A επί το δεύτερο στοιχείο του B . Το τρίτο και τέταρτο στοιχείο του C είναι το γινόμενο του δεύτερου στοιχείου του A επί το πρώτο και το δεύτερο στοιχείο του B αντίστοιχα (Lloyd, 1993). Δηλαδή, αν οι καταστάσεις των δύο qubits δίνονται από:

$$|q_1\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \quad (2.14)$$

$$|q_0\rangle = c|0\rangle + d|1\rangle = \begin{bmatrix} c \\ d \end{bmatrix}$$

η κατάσταση του κβαντικού καταχωρητή δίνεται από:

$$\begin{aligned} |q_R\rangle &= |q_1\rangle \otimes |q_0\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= (a \cdot c)|0\rangle \otimes |0\rangle + (a \cdot d)|0\rangle \otimes |1\rangle + (b \cdot c)|1\rangle \otimes |0\rangle + (b \cdot d)|1\rangle \otimes |1\rangle \\ &= c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle \end{aligned} \quad (2.15)$$

Στην (2.15) αντικαταστήσαμε τα $a \cdot c$, $a \cdot d$, $b \cdot c$ και $b \cdot d$ με τα c_0 , c_1 , c_2 και c_3 αντίστοιχα. Δηλαδή, ο κβαντικός καταχωρητής που αποτελείται από δύο qubits είναι ένα σύστημα τεσσάρων βασικών καταστάσεων. Η κάθε μία από τις βασικές του καταστάσεις προκύπτει ως τανυστικό γινόμενο των βασικών καταστάσεων των qubits. Οι βασικές καταστάσεις σε μορφή πινάκων δίνονται από:

$$|0\rangle \otimes |0\rangle = |0\rangle|0\rangle = |00\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$|0\rangle \otimes |1\rangle = |0\rangle|1\rangle = |01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$|1\rangle \otimes |0\rangle = |1\rangle|0\rangle = |10\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

$$|1\rangle \otimes |1\rangle = |1\rangle|1\rangle = |11\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

(2.16)

και είναι ορθογώνιες μεταξύ τους. Ας γράψουμε τη (2.15) με πίνακες λαμβάνοντας υπόψη τη (2.16):

$$|q_R\rangle = |q_1\rangle \otimes |q_0\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot c \\ b \cdot d \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} \quad (2.17)$$

$$= c_0 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + c_1 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + c_3 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = c_0 |00\rangle + c_1 |01\rangle + c_2 |10\rangle + c_3 |11\rangle$$

Στις (2.15) και (2.17) τα c_0, c_1, c_2 και c_3 είναι τα πλάτη πιθανότητας των αντίστοιχων βασικών καταστάσεων και είναι μιγαδικοί αριθμοί. Αν ο κβαντικός καταχωρητής των δύο qubits βρίσκεται σε υπέρθεση των τεσσάρων βασικών καταστάσεων, μία μέτρηση της κατάστασης του θα δώσει μία από τις τέσσερις βασικές καταστάσεις με πιθανότητα ίση με το τετράγωνο του μέτρου των c_0, c_1, c_2 και c_3 . Δηλαδή, μία μέτρηση της κατάστασής του θα δώσει ως αποτέλεσμα το $|00\rangle$ με πιθανότητα ίση με $|c_0|^2$, το $|01\rangle$ με πιθανότητα ίση με $|c_1|^2$, το $|10\rangle$ με πιθανότητα ίση με $|c_2|^2$ και το $|11\rangle$ με πιθανότητα ίση με $|c_3|^2$. Αφού αυτά είναι τα μόνα δυνατά αποτελέσματα, το άθροισμα των τεσσάρων προηγούμενων πιθανοτήτων πρέπει να είναι ίσο με τη μονάδα:

$$|q_R\rangle = c_0 |00\rangle + c_1 |01\rangle + c_2 |10\rangle + c_3 |11\rangle, \quad |c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2 = 1 \quad (2.18)$$

Το διάνυσμα κατάστασης αυτού του κβαντικού καταχωρητή υπάρχει σε έναν χώρο Hilbert τεσσάρων διαστάσεων και το μήκος του είναι ίσο με τη μονάδα.

Σε έναν κλασικό καταχωρητή των δύο bits μπορούμε να αποθηκεύσουμε ή το δυαδικό αριθμό 00, ή τον 01, ή τον 10 ή τον 11. Όμως, σε έναν κβαντικό καταχωρητή των δύο qubits που βρίσκεται σε υπέρθεση βασικών καταστάσεων μπορούμε να αποθηκεύσουμε και το δυαδικό αριθμό 00 και τον 01 και τον 10 και τον 11, δηλαδή ο κβαντικός καταχωρητής των δύο qubits μπορεί να κρατήσει ταυτόχρονα τέσσερις αριθμούς (Nielsen & Chuang, 2000). Μπορούμε να γράψουμε τη (2.18) και με τον εξής τρόπο:

$$|q_R\rangle = c_0 |00\rangle + c_1 |01\rangle + c_2 |10\rangle + c_3 |11\rangle = c_0 |0\rangle + c_1 |1\rangle + c_2 |2\rangle + c_3 |3\rangle = \sum_{i=0}^3 c_i |i\rangle \quad (2.19)$$

όπου οι δυαδικοί αριθμοί που συμβολίζουν τις βασικές καταστάσεις αντικαταστάθηκαν με τους αντίστοιχους δεκαδικούς. Δεν είναι τίποτε άλλο παρά μια αλλαγή συμβολισμού.

Η δυνατότητα να κρατηθούν ταυτόχρονα και οι τέσσερις βασικές καταστάσεις, δηλαδή τέσσερις αριθμοί, από ένα κβαντικό καταχωρητή αποτελεί τη βάση της κβαντικής παραλληλίας. Υποθέστε ότι έχουμε μία συνάρτηση $F(x)$ με τη μεταβλητή x να παίρνει τις τιμές 0, 1, 2 και 3. Για να γίνει με έναν κλασικό υπολογιστή παράλληλος υπολογισμός των τιμών της $F(x)$, για $x = 0, 1, 2, 3$, χρειάζονται τέσσερις καταχωρητές των δύο bits και τέσσερις υπολογισμοί της τιμής της $F(x)$. Για να γίνει σειριακός υπολογισμός, ένας καταχωρητής των δύο bits φορτώνεται τέσσερις φορές με τους αριθμούς 0, 1, 2 και 3 και κάθε φορά εκτελείται υπολογισμός της τιμής της $F(x)$. Αντίθετα, σε έναν κβαντικό υπολογιστή χρειάζεται μόνο ένας κβαντικός καταχωρητής των δύο qubits και ένας μόνο υπολογισμός της συνάρτησης που μας δίνει και τις τέσσερις τιμές:

$$F(|q_R\rangle) = c_0 F(|00\rangle) + c_1 F(|01\rangle) + c_2 F(|10\rangle) + c_3 F(|11\rangle) = \sum_{i=0}^3 c_i F(|i\rangle) \quad (2.20)$$

Με τον ίδιο τρόπο μπορούμε να δούμε και τον κβαντικό καταχωρητή που αποτελείται από τρία qubits τα $|q_2\rangle$, $|q_1\rangle$ και $|q_0\rangle$:

$$|q_2\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$

$$|q_1\rangle = c|0\rangle + d|1\rangle = \begin{bmatrix} c \\ d \end{bmatrix} \quad (2.21)$$

$$|q_0\rangle = e|0\rangle + f|1\rangle = \begin{bmatrix} e \\ f \end{bmatrix}$$

Η κάθε μία από τις βασικές καταστάσεις του κβαντικού καταχωρητή προκύπτει ως τανυστικό γινόμενο των βασικών καταστάσεων των qubits. Το τανυστικό γινόμενο τριών πινάκων με μία στήλη είναι:

$$\begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} \otimes \begin{bmatrix} e \\ f \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \cdot e \\ c \cdot f \\ d \cdot e \\ d \cdot f \end{bmatrix} = \begin{bmatrix} a \cdot c \cdot e \\ a \cdot c \cdot f \\ a \cdot d \cdot e \\ a \cdot d \cdot f \\ b \cdot c \cdot e \\ b \cdot c \cdot f \\ b \cdot d \cdot e \\ b \cdot d \cdot f \end{bmatrix} \quad (2.22)$$

Θα υπολογίσουμε ως παράδειγμα τον πίνακα που αντιστοιχεί στη βασική κατάσταση $|1\rangle \otimes |0\rangle \otimes |1\rangle = |101\rangle$:

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad (2.23)$$

Όμοια υπολογίζονται και οι άλλοι πίνακες. Ας γράψουμε τώρα την κατάσταση του κβαντικού καταχωρητή με πίνακες, όπως κάναμε και με τη (2.17):

$$|q_R\rangle = |q_2\rangle \otimes |q_1\rangle \otimes |q_0\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} \otimes \begin{bmatrix} e \\ f \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \cdot e \\ c \cdot f \\ d \cdot e \\ d \cdot f \end{bmatrix} = \begin{bmatrix} a \cdot c \cdot e \\ a \cdot c \cdot f \\ a \cdot d \cdot e \\ a \cdot d \cdot f \\ b \cdot c \cdot e \\ b \cdot c \cdot f \\ b \cdot d \cdot e \\ b \cdot d \cdot f \end{bmatrix} = \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix}$$

$$= c_0 \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + c_1 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \dots + c_7 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = c_0 |000\rangle + c_1 |001\rangle + \dots + c_7 |111\rangle$$

(2.24)

Στη (2.24) αντικαταστήσαμε τα $a \cdot c \cdot e$, $a \cdot c \cdot f$, ..., $b \cdot d \cdot f$ με τα c_0, c_1, \dots, c_7 αντίστοιχα. Μπορούμε να γράψουμε τη (2.24) και με τον εξής τρόπο:

$$\begin{aligned} |q_R\rangle &= c_0 |000\rangle + c_1 |001\rangle + c_2 |010\rangle + c_3 |011\rangle + c_4 |100\rangle + c_5 |101\rangle + c_6 |110\rangle + c_7 |111\rangle \\ &= c_0 |0\rangle + c_1 |1\rangle + c_2 |2\rangle + c_3 |3\rangle + c_4 |4\rangle + c_5 |5\rangle + c_6 |6\rangle + c_7 |7\rangle = \sum_{i=0}^7 c_i |i\rangle \end{aligned}$$

(2.25)

Και εδώ το άθροισμα των πιθανοτήτων είναι ίσο με τη μονάδα:

$$|c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2 + |c_4|^2 + |c_5|^2 + |c_6|^2 + |c_7|^2 = 1$$

(2.26)

Το διάνυσμα κατάστασης του κβαντικού καταχωρητή που αποτελείται από τρία qubits υπάρχει σε έναν χώρο Hilbert οκτώ διαστάσεων και το μήκος του είναι ίσο με τη μονάδα. Ο κβαντικός αυτός καταχωρητής είναι ένα κβαντικό σύστημα με οκτώ βασικές καταστάσεις που είναι όλες ορθογώνιες μεταξύ τους. Όταν βρίσκεται σε υπέρθεση βασικών καταστάσεων, μπορεί να κρατήσει ταυτόχρονα οκτώ αριθμούς.

Γενικά, η κατάσταση ενός κβαντικού καταχωρητή που αποτελείται από n qubits δίνεται από:

$$|q_R\rangle = |q_{n-1}\rangle \otimes \dots \otimes |q_1\rangle \otimes |q_0\rangle = |q_{n-1} \dots q_1 q_0\rangle$$

(2.27)

Το διάνυσμα κατάστασής του υπάρχει σε ένα χώρο Hilbert με 2^n διαστάσεις και έχει 2^n βασικές καταστάσεις που είναι όλες ορθογώνιες μεταξύ τους. Αν θεωρήσουμε τη δεκαδική αναπαράσταση των καταστάσεων μπορούμε αυτό να το γράψουμε ως εξής:

$$\langle k | m \rangle = \delta_{km}, \quad k, m \in \{0, 1, 2, \dots, 2^n - 1\} \quad (2.28)$$

Όταν ο καταχωρητής αυτός τεθεί σε υπέρθεση κρατά ταυτόχρονα 2^n αριθμούς:

$$\begin{aligned} |q_R\rangle &= c_0 |0 \dots 000\rangle + c_1 |0 \dots 001\rangle + c_2 |0 \dots 010\rangle + \dots + c_{2^n - 1} |111 \dots 1\rangle \\ &= c_0 |0\rangle + c_1 |1\rangle + c_2 |2\rangle + \dots + c_{2^n - 1} |2^n - 1\rangle = \sum_{i=0}^{2^n - 1} c_i |i\rangle \end{aligned} \quad (2.29)$$

δηλαδή όλους τους αριθμούς από 0 έως $2^n - 1$.

Ένας κβαντικός καταχωρητής που αποτελείται από 2, 3, 4, ... n qubits μπορεί να κρατήσει ταυτόχρονα 4, 8, 16, ... 2^n αριθμούς.

Αν σε έναν κβαντικό καταχωρητή των n qubits που μπορεί να κρατήσει 2^n αριθμούς προστεθεί ένα ακόμη qubit, τότε ο κβαντικός καταχωρητής κρατά διπλάσιους αριθμούς, δηλαδή 2^{n+1} αριθμούς. Στην ιδιότητα αυτή των κβαντικών καταχωρητών βασίζεται η δυνατότητα των κβαντικών υπολογιστών να επεξεργάζονται ποσότητες δεδομένων τις οποίες είναι αδύνατον να επεξεργαστούν οι κλασικοί υπολογιστές, να ψάχνουν σε πολύ μεγάλες βάσεις δεδομένων και να αντιμετωπίζουν πολύπλοκα υπολογιστικά προβλήματα.

2.4 Μερική μέτρηση ενός κβαντικού καταχωρητή

Γνωρίζουμε ότι το αποτέλεσμα της μέτρησης ενός κβαντικού καταχωρητή θα είναι μία από τις βασικές του καταστάσεις. Τι γίνεται όμως αν αντί να μετρήσουμε όλα τα qubits ενός κβαντικού καταχωρητή μετρήσουμε κάποιο ή κάποια από αυτά; Αυτή η μέτρηση ονομάζεται μερική και θα δούμε πώς επηρεάζει την κατάσταση του κβαντικού καταχωρητή. Θα περιγράψουμε την μερική μέτρηση σε έναν καταχωρητή των δύο qubits. Η έννοια της μερικής μέτρησης εύκολα επεκτείνεται και σε καταχωρητές με περισσότερα qubits.

Έστω ότι έχουμε έναν κβαντικό καταχωρητή των δύο qubits ο οποίος βρίσκεται στην παρακάτω υπέρθεση βασικών καταστάσεων:

$$|q_R\rangle = c_0 |00\rangle + c_1 |01\rangle + c_2 |10\rangle + c_3 |11\rangle \quad (2.30)$$

και μετράμε μόνο το δεύτερο (αριστερό) qubit. Η πιθανότητα να μετρήσουμε την κατάσταση $|1\rangle$ είναι:

$$P(1) = |c_2|^2 + |c_3|^2 \quad (2.31)$$

και η πιθανότητα να μετρήσουμε την κατάσταση $|0\rangle$ είναι:

$$P(0) = |c_0|^2 + |c_1|^2 \quad (2.32)$$

Θέλουμε να δούμε ποια θα είναι η κατάσταση του κβαντικού καταχωρητή μετά την μέτρηση αυτού του qubit. Θα δούμε και τις δύο περιπτώσεις. Αν μετρήσουμε και βρούμε την κατάσταση $|1\rangle$, τότε η κατάσταση του κβαντικού καταχωρητή μετά τη μερική μέτρηση θα είναι:

$$|q_R\rangle = a |10\rangle + b |11\rangle = |1\rangle \otimes (a |0\rangle + b |1\rangle) \quad (2.33)$$

Τα νέα πλάτη πιθανότητας a και b πρέπει να εξαρτώνται από τα πλάτη πιθανότητας της κατάστασης πριν την μέτρηση και επίσης, το άθροισμα των μέτρων τους πρέπει να είναι ίσο με τη μονάδα. Για να ικανοποιηθούν και οι δύο αυτές απαιτήσεις, τα νέα πλάτη πιθανότητας είναι:

$$\alpha = \frac{c_2}{\sqrt{|c_2|^2 + |c_3|^2}} \quad b = \frac{c_3}{\sqrt{|c_2|^2 + |c_3|^2}} \quad (2.34)$$

Για το άθροισμα των μέτρων ισχύει:

$$|\alpha|^2 + |b|^2 = \frac{|c_2|^2}{|c_2|^2 + |c_3|^2} + \frac{|c_3|^2}{|c_2|^2 + |c_3|^2} = 1 \quad (2.35)$$

Δηλαδή η κατάσταση του κβαντικού καταχωρητή μετά τη μέτρηση του δεύτερου (αριστερού) qubit που έδωσε ως αποτέλεσμα $|1\rangle$ είναι:

$$|q_R\rangle = |1\rangle \otimes \left(\frac{c_2}{\sqrt{|c_2|^2 + |c_3|^2}} |0\rangle + \frac{c_3}{\sqrt{|c_2|^2 + |c_3|^2}} |1\rangle \right) = \frac{c_2}{\sqrt{|c_2|^2 + |c_3|^2}} |10\rangle + \frac{c_3}{\sqrt{|c_2|^2 + |c_3|^2}} |11\rangle \quad (2.36)$$

Όμοια, η κατάσταση του κβαντικού καταχωρητή μετά τη μέτρηση του δεύτερου (αριστερού) qubit που έδωσε ως αποτέλεσμα $|0\rangle$ είναι:

$$|q_R\rangle = |0\rangle \otimes \left(\frac{c_0}{\sqrt{|c_0|^2 + |c_1|^2}} |0\rangle + \frac{c_1}{\sqrt{|c_0|^2 + |c_1|^2}} |1\rangle \right) = \frac{c_0}{\sqrt{|c_0|^2 + |c_1|^2}} |00\rangle + \frac{c_1}{\sqrt{|c_0|^2 + |c_1|^2}} |01\rangle \quad (2.37)$$

Παράδειγμα 2.2

Έστω ότι έχουμε έναν κβαντικό καταχωρητή των δύο qubits ο οποίος βρίσκεται στην παρακάτω υπέρθεση βασικών καταστάσεων:

$$|q_R\rangle = \frac{3}{\sqrt{30}} |00\rangle + \frac{4}{\sqrt{30}} |01\rangle + \frac{1}{\sqrt{30}} |10\rangle + \frac{2}{\sqrt{30}} |11\rangle$$

και μετράμε μόνο το δεύτερο (αριστερό) qubit. Αν η μέτρηση δώσει ως αποτέλεσμα το $|1\rangle$, η κατάσταση του κβαντικού καταχωρητή μετά την μέτρηση θα είναι:

$$|q_R\rangle = |1\rangle \otimes \left(\frac{\frac{1}{\sqrt{30}}}{\sqrt{\frac{1}{30} + \frac{4}{30}}} |0\rangle + \frac{\frac{2}{\sqrt{30}}}{\sqrt{\frac{1}{30} + \frac{4}{30}}} |1\rangle \right) = \frac{1}{\sqrt{5}} |10\rangle + \frac{2}{\sqrt{5}} |11\rangle$$

Αν η μέτρηση δώσει ως αποτέλεσμα το $|0\rangle$, η κατάσταση του κβαντικού καταχωρητή μετά τη μέτρηση θα είναι:

$$|q_R\rangle = |0\rangle \otimes \left(\frac{\frac{3}{\sqrt{30}}}{\sqrt{\frac{9}{30} + \frac{16}{30}}} |0\rangle + \frac{\frac{4}{\sqrt{30}}}{\sqrt{\frac{9}{30} + \frac{16}{30}}} |1\rangle \right) = \frac{3}{5} |00\rangle + \frac{4}{5} |11\rangle \quad \blacklozenge$$

2.5 Βασικά στοιχεία του χώρου Hilbert

Η κατάσταση κάθε κβαντικού συστήματος αντιπροσωπεύεται από ένα διάνυσμα στον χώρο Hilbert. Ο χώρος Hilbert είναι ένας διανυσματικός χώρος πάνω στο πεδίο των μιγαδικών αριθμών. Δηλαδή, είναι ένας μιγαδικός διανυσματικός χώρος (complex vector space). Τα στοιχεία που αποτελούν τον χώρο αυτό είναι ένα σύνολο διανυσμάτων $\{|a\rangle, |b\rangle, |c\rangle, \dots\}$ τα οποία έχουν τις παρακάτω ιδιότητες (Riefel & Polak, 2014):

Για κάθε ζεύγος διανυσμάτων $|a\rangle$ και $|b\rangle$ υπάρχει ένα διάνυσμα $|c\rangle$ το οποίο ονομάζεται άθροισμα των $|a\rangle$ και $|b\rangle$:

$$|a\rangle + |b\rangle = |c\rangle \quad (2.38)$$

$$|a\rangle + |b\rangle = |b\rangle + |a\rangle \quad (2.39)$$

$$(|a\rangle + |b\rangle) + |c\rangle = |a\rangle + (|b\rangle + |c\rangle) \quad (2.40)$$

Υπάρχει το μηδενικό διάνυσμα $|0\rangle$ με ιδιότητα:

$$|a\rangle + |0\rangle = |a\rangle \quad (2.41)$$

Για κάθε διάνυσμα $|a\rangle$ του χώρου Hilbert υπάρχει το αντίστροφο $|-a\rangle$, και για τα δύο αυτά διανύσματα ισχύει:

$$|a\rangle + |-a\rangle = |0\rangle \quad (2.42)$$

Αν μ και ν είναι δύο τυχαίοι μιγαδικοί αριθμοί, τότε ισχύουν οι παρακάτω σχέσεις:

$$\mu(|a\rangle + |b\rangle) = \mu|a\rangle + \mu|b\rangle \quad (2.43)$$

$$(\mu + \nu)|a\rangle = \mu|a\rangle + \nu|a\rangle \quad (2.44)$$

$$\mu\nu|a\rangle = \mu(\nu|a\rangle) \quad (2.45)$$

$$1|a\rangle = |a\rangle \quad (2.46)$$

Στο χώρο Hilbert ορίζεται εσωτερικό γινόμενο το οποίο συμβολίζεται ως εξής:

$$(|a\rangle, |b\rangle) = \langle a|b\rangle \quad (2.47)$$

Το αποτέλεσμα του εσωτερικού γινομένου δύο διανυσμάτων στον χώρο Hilbert είναι ένας μιγαδικός αριθμός. Το εσωτερικό γινόμενο έχει τις εξής ιδιότητες:

$$(|a\rangle, \lambda |b\rangle) = \lambda (|a\rangle, |b\rangle), \text{ όπου } \lambda \text{ είναι ένας τυχαίος μιγαδικός αριθμός} \quad (2.48)$$

$$(\lambda |a\rangle, |b\rangle) = \lambda^* (|a\rangle, |b\rangle) \quad (2.49)$$

$$(|a\rangle, |b\rangle + |c\rangle) = (|a\rangle, |b\rangle) + (|a\rangle, |c\rangle) = \langle a|b\rangle + \langle a|c\rangle \quad (2.50)$$

$$(|a\rangle + |b\rangle, |c\rangle) = (|a\rangle, |c\rangle) + (|b\rangle, |c\rangle) = \langle a|c\rangle + \langle b|c\rangle \quad (2.51)$$

$$(|a\rangle, |b\rangle) = (|b\rangle, |a\rangle)^* \text{ ή } \langle a|b\rangle = \langle b|a\rangle^* \quad (2.52)$$

Το μέτρο ενός διανύσματος $|a\rangle$ ορίζεται ως:

$$\|a\| = \sqrt{\langle a|a\rangle}$$

Ένα σύνολο διανυσμάτων $\{|q_n\rangle\}$ στον χώρο Hilbert αποτελεί ένα ορθοκανονικό σύστημα αν:

$$\langle q_n | q_m \rangle = \delta_{nm} \quad (2.53)$$

Ένα ορθοκανονικό σύστημα διανυσμάτων στον χώρο Hilbert, $\{|q_n\rangle\}$, είναι πλήρες, όταν κάθε τυχαίο διάνυσμα του χώρου, $|\psi\rangle$, μπορεί να εκφραστεί ως άθροισμα των διανυσμάτων αυτών:

$$|\psi\rangle = \sum_n a_n |q_n\rangle \quad (2.54)$$

όπου a_n είναι μιγαδικοί αριθμοί.

Γενικά, αν a_n και a_m είναι μιγαδικοί αριθμοί, τότε ισχύει:

$$a_m = \langle q_m | \psi \rangle = \left\langle q_m \left| \sum_n a_n |q_n\rangle \right. \right\rangle = \sum_n a_n \langle q_m | q_n \rangle = \sum_n a_n \delta_{nm} = a_m \quad (2.55)$$

Επομένως η (2.54) μπορεί να γραφεί ως εξής:

$$|\psi\rangle = \sum_n |q_n\rangle \langle q_n | \psi \rangle \quad (2.56)$$

Ένα ορθοκανονικό σύστημα n διανυσμάτων $\{|q_n\rangle\}$, μπορεί να αποτελέσει τη βάση ενός χώρου Hilbert n διαστάσεων.

Για τους τελεστές στον χώρο Hilbert ισχύουν οι εξής ιδιότητες:

$$\hat{A}(a|\psi\rangle + b|\phi\rangle) = a\hat{A}|\psi\rangle + b\hat{A}|\phi\rangle \quad (2.57)$$

$$(\hat{A} + \hat{B})|\psi\rangle = \hat{A}|\psi\rangle + \hat{B}|\psi\rangle \quad (2.58)$$

$$(\hat{A} \cdot \hat{B})|\psi\rangle = \hat{A} \cdot (\hat{B}|\psi\rangle) \quad (2.59)$$

Γενικά ισχύει:

$$\hat{A} \cdot \hat{B} \neq \hat{B} \cdot \hat{A} \quad (2.60)$$

Υπάρχει ο τελεστής μονάδας $\hat{1}$ ο οποίος, όταν δρα σε ένα διάνυσμα το αφήνει αναλλοίωτο:

$$\hat{1}|\phi\rangle = |\phi\rangle \quad (2.61)$$

Υπάρχει ο μηδενικός τελεστής $\hat{0}$ για τον οποίο ισχύει:

$$\hat{0}|\phi\rangle = 0 \quad (2.62)$$

Αν στο διάνυσμα $|\psi\rangle$ δρα πρώτα ο τελεστής \hat{A} , μετά ο \hat{B} και μετά ο \hat{C} , η σειρά αναγραφής των τελεστών είναι:

$$\hat{C}\hat{B}\hat{A}|\psi\rangle \quad (2.63)$$

Αν η δράση ενός τελεστή \hat{A} στο διάνυσμα $|\psi\rangle$ έχει ως αποτέλεσμα τον πολλαπλασιασμό του διανύσματος με έναν αριθμό c :

$$\hat{A}|\psi\rangle = c|\psi\rangle \quad (2.64)$$

τότε το διάνυσμα ονομάζεται ιδιοδιάνυσμα και ο αριθμός c ιδιοτιμή του τελεστή \hat{A} . Γενικά ο αριθμός c είναι μιγαδικός. Αν ο τελεστής \hat{A} είναι Ερμιτιανός, τότε ο αριθμός c είναι πραγματικός.

Βιβλιογραφία

- Brooks M. (Ed.), *Quantum computing and communications*, Springer-Verlag, 1999.
- D' Espagnat B., *Conceptual foundations of quantum mechanics*, Perseus Books, 1999.
- Keyl M., Fundamentals of quantum information theory, *Physics Reports*, vol. 369, pp. 431-548, 2002.
- Lewin D. I., Searching for the elusive qubit, *IEEE Computers*, July/August issue, pp. 4-7, 2001.
- Lloyd S., Review of Quantum Computation, *Vistas in Astronomy*, vol. 37, pp. 291-295, 1993.
- Nielsen M. A. & Chuang I. L., *Quantum computation and quantum information*, Cambridge University Press, 2000.
- Rieffel E. G., & Polak W. H., *Quantum computing: a gentle introduction*, The MIT Press, 2014.
- Williams C. P. & Clearwater S. H., *Ultimate zero and one. Computing at the quantum frontier*, Copernicus, Springer-Verlag, 2000.

Ασκήσεις

Άσκηση 2.1

Δίνονται τα παρακάτω qubits. Μπορείτε να τα ξεχωρίσετε μετρώντας την κατάσταση τους;

$$|a\rangle = \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$$

$$|b\rangle = \frac{1}{\sqrt{2}}|0\rangle + i\frac{1}{\sqrt{2}}|1\rangle$$

Άσκηση 2.2

Δίνονται τα παρακάτω qubits. Μπορείτε να τα ξεχωρίσετε μετρώντας την κατάσταση τους;

$$|a\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$$

$$|b\rangle = \frac{\sqrt{3}}{2}|0\rangle - i\frac{1}{2}|1\rangle$$

Άσκηση 2.3

Δίνονται τα παρακάτω qubits. Μπορείτε να τα ξεχωρίσετε μετρώντας την κατάσταση τους;

$$|a\rangle = \left(\frac{\sqrt{2}}{4} + i\frac{\sqrt{2}}{4}\right)|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$$

$$|b\rangle = \frac{1}{2}|0\rangle + \left(\frac{\sqrt{6}}{4} + i\frac{\sqrt{6}}{4}\right)|1\rangle$$

Άσκηση 2.4

Να δείξετε ότι οι βασικές καταστάσεις ενός κβαντικού καταχωρητή που αποτελείται από δύο qubits είναι ορθογώνιες μεταξύ τους.

Άσκηση 2.5

Ποια από τα παρακάτω διανύσματα είναι διανύσματα κατάστασης ενός κβαντικού καταχωρητή που αποτελείται από δύο qubits;

$$\alpha. |q_R\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$$

$$\beta. |q_R\rangle = \frac{2}{\sqrt{2}}|00\rangle + \frac{3}{\sqrt{6}}|01\rangle - \frac{1}{2}|10\rangle - \frac{\sqrt{2}}{4}|11\rangle$$

$$\gamma. |q_R\rangle = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{2\sqrt{2}}|01\rangle - \frac{1}{2\sqrt{2}}|10\rangle - \frac{1}{2}|11\rangle$$

Άσκηση 2.6

Να υπολογίσετε τους πίνακες που αντιστοιχούν στις βασικές καταστάσεις $|100\rangle$, $|001\rangle$ και $|111\rangle$.

Άσκηση 2.7

Να ελέγξετε αν τα παρακάτω ζεύγη καταστάσεων είναι ορθογώνια μεταξύ τους.

$$\alpha. |100\rangle, |001\rangle$$

$$\beta. |001\rangle, |101\rangle$$

Άσκηση 2.8

Να γράψετε την κατάσταση ενός κβαντικού καταχωρητή που αποτελείται από 4 qubits ως υπέρθεση όλων των βασικών του καταστάσεων, δηλαδή με τη μορφή της εξίσωσης (2.27).

Άσκηση 2.9

Έστω ότι έχουμε έναν κβαντικό καταχωρητή των δύο qubits ο οποίος βρίσκεται στην παρακάτω υπέρθεση βασικών καταστάσεων:

$$|q_R\rangle = \frac{3}{\sqrt{30}}|00\rangle + \frac{4}{\sqrt{30}}|01\rangle + \frac{1}{\sqrt{30}}|10\rangle + \frac{2}{\sqrt{30}}|11\rangle$$

και μετράμε μόνο το πρώτο (δεξιό) qubit. Αν η μέτρηση δώσει ως αποτέλεσμα το $|1\rangle$, να βρείτε την κατάσταση του κβαντικού καταχωρητή μετά τη μέτρηση.

Άσκηση 2.10

Έστω ότι έχουμε έναν κβαντικό καταχωρητή των δύο qubits ο οποίος βρίσκεται στην παρακάτω υπέρθεση βασικών καταστάσεων:

$$|q_R\rangle = \frac{3}{\sqrt{54}}|00\rangle + \frac{2}{\sqrt{54}}|01\rangle + \frac{5}{\sqrt{54}}|10\rangle + \frac{4}{\sqrt{54}}|11\rangle$$

και μετράμε μόνο το δεύτερο (αριστερό) qubit. Αν η μέτρηση δώσει ως αποτέλεσμα το $|1\rangle$ να βρείτε την κατάσταση του κβαντικού καταχωρητή μετά τη μέτρηση.

3. Τελεστές και κβαντικές πύλες

Σύνοψη

Στο κεφάλαιο αυτό παρουσιάζονται οι κβαντικές πύλες ως τελεστές του χώρου Hilbert. Περιγράφονται οι κβαντικές πύλες που δρουν σε ένα qubit. Παρουσιάζονται επίσης οι κβαντικές πύλες που δρουν σε κβαντικούς καταχωρητές των δύο και των τριών qubits. Δίνεται η απόδειξη του θεωρήματος αδυναμίας αντιγραφής κβαντικής κατάστασης.

Προαπαιτούμενη γνώση

Γραμμική άλγεβρα, το πρώτο και το δεύτερο κεφάλαιο του βιβλίου αυτού.

3. 1 Οι κβαντικές πύλες ως τελεστές του χώρου Hilbert

Οι επεξεργαστές των κλασικών υπολογιστών αποτελούνται από αγωγούς και λογικές πύλες οι οποίες συγκροτούν κυκλώματα. Οι αγωγοί μεταφέρουν την πληροφορία με τη μορφή τάσης ή ρεύματος από πύλη σε πύλη. Οι λογικές πύλες επεξεργάζονται και μετατρέπουν την πληροφορία που έρχεται στην είσοδό τους, σύμφωνα με τον πίνακα αληθείας τους. Οι λογικές πύλες στους κλασικούς υπολογιστές είναι φυσικά συστήματα κατασκευασμένα από πυρίτιο και, σε όλους σχεδόν τους κλασικούς υπολογιστές, αποτελούνται από τρανζίστορες που ονομάζονται MOSFETs. Δηλαδή, οι πύλες των κλασικών υπολογιστών είναι φυσικά συστήματα και η πληροφορία διέρχεται από μέσα τους.

Αντίθετα, στους κβαντικούς υπολογιστές οι κβαντικές πύλες δεν είναι συνήθως φυσικά συστήματα, αλλά αντιπροσωπεύουν δράσεις που ασκούνται σε qubits ή σε κβαντικούς καταχωρητές. Οι δράσεις στα κβαντικά συστήματα αντιπροσωπεύονται από τελεστές του χώρου Hilbert που, όπως είδαμε, περιγράφονται από πίνακες (Kaye, Lafflamme & Mosca, 2007). Η δράση του Quant στο κβαντικό παιχνίδι που είδαμε στο πρώτο κεφάλαιο, είναι μία κβαντική πύλη και συγκεκριμένα η πύλη Hadamard, την οποία θα περιγράψουμε στο κεφάλαιο αυτό.

Μία άλλη σημαντική διαφορά είναι ότι η πληροφορία δεν διέρχεται μέσα από τις κβαντικές πύλες. Η πληροφορία βρίσκεται αποθηκευμένη σε qubits ή σε κβαντικούς καταχωρητές και παραμένει εκεί. Αυτό συμβαίνει σε όλες τις υλοποιήσεις στερεάς κατάστασης των κβαντικών κυκλωμάτων, όπως με παγίδες ιόντων ή με NMR. Τα qubits είναι σωματίδια που παραμένουν σταθερά στις θέσεις τους, όσο βέβαια τους το επιτρέπει η αρχή της απροσδιοριστίας. Όπως θα δούμε στο επόμενο κεφάλαιο, οι κβαντικές πύλες δρουν η μία μετά την άλλη στα qubits ή στους κβαντικούς καταχωρητές αλλάζοντας την κατάστασή τους. Οι κβαντικές πύλες είναι δηλαδή, δράσεις πάνω στα σωματίδια με μαγνητικά πεδία ή παλμούς laser. Θυμηθείτε ότι στο κβαντικό μας παιχνίδι το κβαντικό κέρμα που αντιπροσωπεύει το qubit ή τον κβαντικό καταχωρητή παραμένει στην ίδια θέση ενώ οι δύο παίκτες δρουν σε αυτό ο ένας μετά τον άλλο. Όπως θα δούμε, το παιχνίδι αυτό είναι ένας κβαντικός υπολογισμός, όπου το κβαντικό κέρμα αντιπροσωπεύει το qubit ή τον κβαντικό καταχωρητή και ο Quant τις κβαντικές πύλες.

Τώρα μπορούμε να ορίσουμε τις κβαντικές πύλες. Οι καταστάσεις των qubits και των κβαντικών καταχωρητών είναι διανύσματα στον χώρο Hilbert. Οι κβαντικές πύλες είναι τελεστές του χώρου Hilbert που δρουν σε qubits και σε κβαντικούς καταχωρητές αλλάζοντας την κατάστασή τους. Δηλαδή οι κβαντικές πύλες περιστρέφουν τα διανύσματα κατάστασής των qubits και των κβαντικών καταχωρητών χωρίς να αλλάζουν το μήκος τους, το οποίο είναι πάντα ίσο με τη μονάδα (Keyl 2002).

Όλοι οι τελεστές του χώρου Hilbert μπορούν να είναι κβαντικές πύλες; Όχι. Οι κβαντικές πύλες πρέπει να μην μεταβάλλουν το μήκος του διανύσματος κατάστασης και να μην μεταβάλουν τις τιμές των εσωτερικών γινομένων μεταξύ δύο διανυσμάτων κατάστασης. Για τον λόγο αυτό αντιπροσωπεύονται από ορθομοναδιαίους τελεστές και πίνακες. Έστω ότι έχουμε δύο διανύσματα κατάστασης, τα $|q_{R1}\rangle$ και $|q_{R2}\rangle$. Το εσωτερικό τους γινόμενο διατηρείται, όταν δρα σε αυτά ένας ορθομοναδιαίος τελεστής \hat{G} :

$$\langle q_{R2} | q_{R1} \rangle = \langle q_{R2} | \hat{G}^\dagger \hat{G} | q_{R1} \rangle = \langle q_{R2} | \hat{G}^{-1} \hat{G} | q_{R1} \rangle = \langle q_{R2} | q_{R1} \rangle \quad (3.1)$$

Παρακάτω θα περιγράψουμε τις κβαντικές πύλες και θα δούμε τα αποτελέσματα των δράσεών τους.

3.2 Κβαντικές πύλες που δρουν σε ένα qubit

Εδώ θα ασχοληθούμε με κβαντικές πύλες που δρουν σε ένα μόνο qubit. Οι πύλες αυτές περιστρέφουν το διάνυσμα κατάστασης ενός qubit μέσα στη σφαίρα Bloch, δηλαδή μεταβάλλουν τις γωνίες θ και φ . Υπάρχουν άπειρες τέτοιες περιστροφές και επομένως, υπάρχουν άπειρες κβαντικές πύλες που δρουν σε ένα qubit. Δηλαδή, κάθε ορθομοναδιαίος τελεστής μπορεί να θεωρηθεί ως μία κβαντική πύλη που δρα σε ένα qubit. Υπάρχουν λοιπόν άπειρες κβαντικές πύλες που δρουν σε ένα qubit, όμως δεν χρησιμοποιούνται όλες. Χρησιμοποιούνται κυρίως τρεις πύλες οι οποίες έχουν ονομαστεί και θα τις δούμε αμέσως παρακάτω.

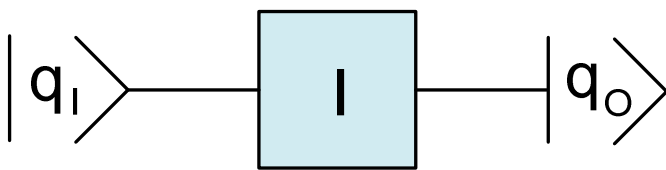
3.2.1 Η κβαντική πύλη αδρανείας

Η πύλη αδρανείας και συμβολίζεται με I και περιγράφεται από έναν τελεστή που ονομάζεται τελεστής αδρανείας. Ο πίνακας που αντιστοιχεί στον τελεστή της πύλης αυτής είναι:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (3.2)$$

Η κβαντική πύλη αδρανείας, αφήνει αμετάβλητη την κατάσταση του qubit:

$$I |q\rangle = |q\rangle \quad (3.3)$$



Σχήμα 3-1. Το σύμβολο της κβαντικής πύλης αδρανείας, I .

Στο Σχήμα 3-1 φαίνεται το σύμβολο της πύλης αδρανείας. Ο Πίνακας 3-1 δείχνει τη δράση της πύλης αυτής στις καταστάσεις ενός qubit:

$ q_i\rangle$	$ q_o\rangle$
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$ 1\rangle$
$ q\rangle$	$ q\rangle$

Πίνακας 3-1. Η δράση της κβαντικής πύλης αδρανείας στις καταστάσεις ενός qubit.

Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των qubits πριν τη δράση της πύλης και στη δεύτερη οι καταστάσεις μετά τη δράση της πύλης. Προσοχή στον συμβολισμό. Στο Σχήμα 3-1 η πληροφορία δεν διέρχεται μέσα από την πύλη, αλλά συμβολίζουμε με $|q_i\rangle$ την κατάσταση του qubit πριν τη δράση της πύλης και με $|q_o\rangle$ την κατάστασή του μετά τη δράση της πύλης.

3.2.2 Η Κβαντική πύλη μετατόπισης φάσης

Η κβαντική πύλη μετατόπισης φάσης περιγράφεται από έναν τελεστή που ονομάζεται Φ . Ο πίνακας που αντιστοιχεί στον τελεστή της πύλης αυτής είναι (Barenco, 1995):

$$\Phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \quad (3.4)$$

Ας δούμε τώρα το αποτέλεσμα της δράσης αυτής της πύλης σε ένα qubit. Έστω ένα qubit $|q_I\rangle$ του οποίου η κατάσταση δίνεται από:

$$|q_I\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \quad (3.5)$$

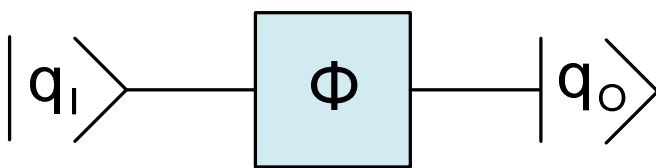
Η κβαντική πύλη μετατόπισης φάσης δρα σ' αυτό και αλλάζει την κατάστασή του σε $|q_O\rangle$. Ας υπολογίσουμε τη νέα αυτή κατάσταση:

$$|q_O\rangle = \Phi |q_I\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ e^{i\varphi} b \end{bmatrix} \quad (3.6)$$

Η νέα κατάσταση του qubit είναι:

$$|q_O\rangle = a|0\rangle + e^{i\varphi}b|1\rangle \quad (3.7)$$

Δηλαδή, η δράση της πύλης αυτής άλλαξε μόνο τη γωνία φάσης του qubit.



Σχήμα 3-2. Το σύμβολο της κβαντικής πύλης μετατόπισης φάσης, Φ .

Στο Σχήμα 3-2 φαίνεται το σύμβολο της πύλης Φ και στον Πίνακα 3-2 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των qubits πριν τη δράση της πύλης ($|q_I\rangle$) και στη δεύτερη οι καταστάσεις μετά τη δράση της πύλης ($|q_O\rangle$).

$ q_I\rangle$	$ q_O\rangle$
$ 0\rangle$	$ 0\rangle$
$ 1\rangle$	$e^{i\varphi} 1\rangle$
$a 0\rangle + b 1\rangle$	$a 0\rangle + e^{i\varphi}b 1\rangle$

Πίνακας 3-2. Η δράση της κβαντικής πύλης μετατόπισης φάσης στις καταστάσεις ενός qubit.

3.2.3 Η κβαντική πύλη Hadamard

Η κβαντική πύλη Hadamard περιγράφεται από έναν τελεστή που ονομάζεται H . Ο πίνακας που αντιστοιχεί στον τελεστή της πύλης αυτής είναι:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (3.8)$$

Ας δούμε το αποτέλεσμα της δράσης αυτής της πύλης σε ένα qubit που βρίσκεται στη βασική κατάσταση $|0\rangle$:

$$H|0\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (3.9)$$

Ας δούμε και το αποτέλεσμα της δράσης αυτής της πύλης σε ένα qubit που βρίσκεται στη βασική κατάσταση $|1\rangle$:

$$H|1\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (3.10)$$

Δηλαδή, όταν η πύλη Hadamard δρα σε qubits που βρίσκονται σε μία από τις δύο βασικές καταστάσεις, τα θέτει σε μία κατάσταση που είναι υπέρθεση των βασικών καταστάσεων. Όταν ένα qubit βρίσκεται είτε στην κατάσταση που δίνεται από την (3.9) είτε στην κατάσταση που δίνεται από την (3.10), η πιθανότητα να μετρήσουμε και να το βρούμε στην βασική κατάσταση $|0\rangle$ είναι ίση με την πιθανότητα να το βρούμε στην βασική κατάσταση $|1\rangle$. Φυσικά και οι δύο πιθανότητες είναι ίσες με 0,5.

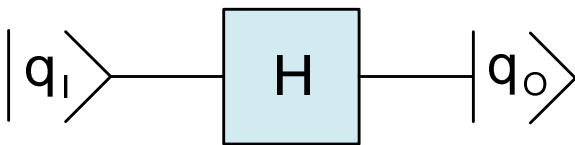
Ας δούμε τώρα τι αποτέλεσμα θα έχουμε αν η πύλη Hadamard δράσει σε ένα qubit που βρίσκεται στην υπέρθεση καταστάσεων που δίνεται από την (3.9):

$$H \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle \quad (3.11)$$

Ας δούμε τη δράση της πύλης και στο qubit που βρίσκεται στην υπέρθεση καταστάσεων που δίνεται από την (3.10):

$$H \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle \quad (3.12)$$

Δηλαδή η πύλη Hadamard επιστρέφει τα qubits στις βασικές τους καταστάσεις.



Σχήμα 3-3. Το σύμβολο της κβαντικής πύλης Hadamard, H .

$ q_i\rangle$	$ q_o\rangle$
$ 0\rangle$	$\frac{1}{\sqrt{2}} (0\rangle + 1\rangle)$
$ 1\rangle$	$\frac{1}{\sqrt{2}} (0\rangle - 1\rangle)$
$\frac{1}{\sqrt{2}} (0\rangle + 1\rangle)$	$ 0\rangle$
$\frac{1}{\sqrt{2}} (0\rangle - 1\rangle)$	$ 1\rangle$

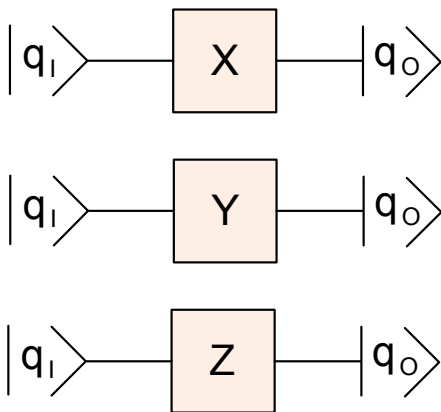
Πίνακας 3-3. Η δράση της κβαντικής Hadamard στις καταστάσεις ενός qubit.

Στο Σχήμα 3-3 φαίνεται το σύμβολο της πύλης H και στον Πίνακα 3-3 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των qubits πριν τη δράση της πύλης ($|q_i\rangle$) και στη δεύτερη οι καταστάσεις μετά τη δράση της πύλης ($|q_o\rangle$).

Η πύλη Hadamard είναι πολύ σημαντική διότι μπορεί να μεταφέρει τα qubits από τις βασικές τους καταστάσεις (οι οποίες γίνονται αντιληπτές από εμάς), σε υπέρθεση καταστάσεων, που είναι χαρακτηριστικό μόνο των κβαντικών συστημάτων. Επίσης, μεταφέρει τα qubits από υπέρθεση καταστάσεων στις βασικές τους καταστάσεις. Αναμένεται ότι οι πύλες Hadamard θα αποτελέσουν το κύριο στοιχείο για τη διασύνδεση κλασικών και κβαντικών υπολογιστών.

3. 3 Κβαντικές πύλες Pauli

Μία πολύ σημαντική ομάδα κβαντικών πυλών που δρουν σε ένα qubit είναι οι κβαντικές πύλες Pauli. Αυτές οι κβαντικές πύλες είναι σημαντικές διότι κάθε δυνατή κβαντική πύλη του ενός qubit μπορεί να συντεθεί από έναν γραμμικό συνδυασμό των πυλών Pauli και της πύλης αδρανείας (Cybenko, 2001). Δηλαδή, με τις πύλες αυτές μπορούμε να εκτελέσουμε όλες τις περιστροφές του διανύσματος κατάστασης ενός qubit στη σφαίρα Bloch.



Σχήμα 3-4. Τα σύμβολα των κβαντικών πυλών Pauli.

	$ q_1\rangle$	$ q_0\rangle$
X	$a 0\rangle + b 1\rangle$	$b 0\rangle + a 1\rangle$
Y	$a 0\rangle + b 1\rangle$	$-ib 0\rangle + ia 1\rangle$
Z	$a 0\rangle + b 1\rangle$	$a 0\rangle - b 1\rangle$

Πίνακας 3-4. Οι δράσεις των κβαντικών πυλών Pauli στις καταστάσεις ενός qubit.

Οι κβαντικές πύλες Pauli συμβολίζονται με τα γράμματα X, Y και Z. Τα σύμβολα των πυλών αυτών φαίνονται στο Σχήμα 3-4. Οι πύλες Pauli περιγράφονται αντίστοιχα από τους τελεστές X, Y και Z στους οποίους αντιστοιχούν οι παρακάτω πίνακες:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (3.13)$$

Η δράση της πύλης X σε ένα qubit είναι:

$$X|q_i\rangle = X(a|0\rangle + b|1\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix} = b|0\rangle + a|1\rangle = |q_o\rangle \quad (3.14)$$

Η δράση της πύλης Y σε ένα qubit είναι:

$$Y|q_i\rangle = Y(a|0\rangle + b|1\rangle) = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} -ib \\ ia \end{bmatrix} = -ib|0\rangle + ia|1\rangle = |q_o\rangle \quad (3.15)$$

Η δράση της πύλης Z σε ένα qubit είναι:

$$Z|q_i\rangle = Z(a|0\rangle + b|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ -b \end{bmatrix} = a|0\rangle - b|1\rangle = |q_o\rangle \quad (3.16)$$

Οι ιδιότητες των κβαντικών πυλών Pauli φαίνονται συνοπτικά στον Πίνακα 3-4.

3. 4 Κβαντικές πύλες που δρουν σε δύο qubits

Εδώ θα περιγραφούν δύο κβαντικές πύλες που δρουν σε δύο qubits, η κβαντική πύλη ελεγχόμενου ΟΧΙ και η κβαντική πύλη ελεγχόμενης μετατόπισης φάσης. Μπορεί επίσης να θεωρηθεί ότι οι πύλες αυτές δρουν σε κβαντικούς καταχωρητές των δύο qubits.

3.4.1 Η κβαντική πύλη ελεγχόμενου ΟΧΙ

Η πύλη ελεγχόμενου ΟΧΙ δρα σε δύο qubits. Ο Αγγλικός όρος για την πύλη αυτή είναι Controlled-NOT και ο τελεστής που την περιγράφει συμβολίζεται με $CNOT$, από το αρχικό της λέξης controlled και το NOT.

Όπως είπαμε, η πύλη αυτή δρα σε δύο qubits, το ένα ονομάζεται qubit ελέγχου και συμβολίζεται με c και το άλλο qubit στόχος και συμβολίζεται με t . Οι καταστάσεις των δύο qubits πριν τη δράση της πύλης είναι $|c_i\rangle$ και $|t_i\rangle$. Οι καταστάσεις των qubits μετά τη δράση της πύλης είναι $|c_o\rangle$ και $|t_o\rangle$. Η πύλη $CNOT$ αλλάζει την κατάσταση του qubit στόχου, όταν η κατάσταση του qubit ελέγχου είναι $|1\rangle$, ενώ αφήνει την κατάσταση του qubit στόχου αναλλοίωτη, όταν η κατάσταση του qubit ελέγχου είναι $|0\rangle$. Η κατάσταση του qubit ελέγχου $|c_i\rangle$ δεν μεταβάλλεται, δηλαδή ισχύει πάντα $|c_i\rangle = |c_o\rangle$. Η πύλη $CNOT$ περιγράφεται από τον παρακάτω πίνακα:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad (3.17)$$

Ας δούμε τη δράση της πύλης αυτής σε έναν κβαντικό καταχωρητή που αποτελείται από δύο qubits. Η γενική περιγραφή της δράσης της πύλης είναι:

$$CNOT |c_i t_i\rangle = |c_o t_o\rangle \quad (3.18)$$

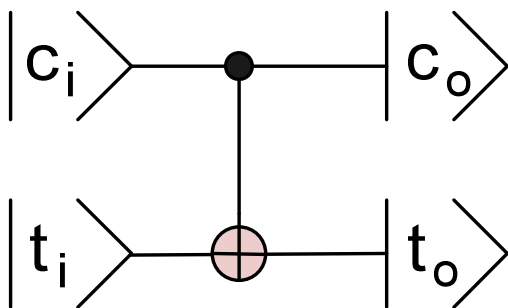
Έστω ότι η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|10\rangle$, τότε:

$$CNOT|10\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle \quad (3.19)$$

Δηλαδή, η κατάσταση του qubit στόχου άλλαξε από $|0\rangle$ σε $|1\rangle$ διότι η κατάσταση του qubit ελέγχου είναι $|1\rangle$. Ας δούμε και την περίπτωση $|01\rangle$:

$$CNOT|01\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle \quad (3.20)$$

Αφού η κατάσταση του qubit ελέγχου είναι $|0\rangle$, η κατάσταση του qubit στόχου δεν αλλάζει. Με τον ίδιο τρόπο μπορούμε να δούμε και τις υπόλοιπες δύο περιπτώσεις.



Σχήμα 3-5. Το σύμβολο της κβαντικής πύλης ελεγχόμενου ΟΧΙ, CNOT.

$ c_i t_i\rangle$	$ c_o t_o\rangle$
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$

Πίνακας 3-5. Η δράση της κβαντικής πύλης CNOT στα qubits ελέγχου και στόχου.

Στο Σχήμα 3-5 φαίνονται το σύμβολο της πύλης CNOT και στον Πίνακα 3-5 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των δύο qubits πριν τη δράση της πύλης ($|c_i t_i\rangle$) και στη δεύτερη οι καταστάσεις τους μετά τη δράση της πύλης ($|c_o t_o\rangle$).

Κάτι πολύ σημαντικό: η πύλη $CNOT$ η πύλη H και η πύλη Φ αποτελούν ένα γενικευμένο σύνολο κβαντικών πυλών. Δηλαδή, μπορούμε να εκτελέσουμε οποιοδήποτε κβαντικό υπολογισμό χρησιμοποιώντας μόνο αυτές τις πύλες.

3.4.2 Η κβαντική πύλη ελεγχόμενης μετατόπισης φάσης

Η πύλη αυτή δρα σε δύο qubits. Στη βιβλιογραφία ο τελεστής της πύλης αυτής συμβολίζεται με διάφορους τρόπους, αλλά οι πιο συνηθισμένοι είναι οι S , CP και $C\Phi$. Εδώ θα χρησιμοποιήσουμε το $C\Phi$. Όπως και στην πύλη $CNOT$ το ένα qubit ονομάζεται qubit ελέγχου και συμβολίζεται με c και το άλλο qubit στόχος και συμβολίζεται με t . Με $|c_i\rangle$ και $|t_i\rangle$ συμβολίζονται οι καταστάσεις των δύο qubits πριν τη δράση της πύλης, και με $|c_o\rangle$ και $|t_o\rangle$ οι καταστάσεις των qubits μετά τη δράση της πύλης. Η πύλη $C\Phi$ πολλαπλασιάζει την κατάσταση του qubit στόχου με τον παράγοντα φάσης $e^{i\phi}$ μόνο όταν και η κατάσταση του qubit ελέγχου και η κατάσταση του qubit στόχου είναι $|1\rangle$. Σε όλες τις άλλες περιπτώσεις δεν μεταβάλλει τις καταστάσεις των qubits. Η πύλη $C\Phi$ περιγράφεται από τον παρακάτω πίνακα:

$$C\Phi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{bmatrix} \quad (3.21)$$

Η γενική περιγραφή της δράσης της πύλης είναι:

$$C\Phi |c_i t_i\rangle = |c_o t_o\rangle \quad (3.22)$$

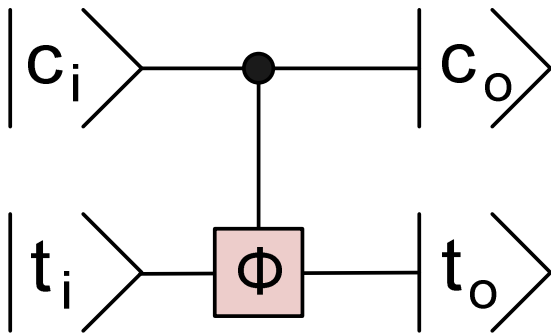
Ας δούμε τη δράση της πύλης στην κατάσταση ενός κβαντικού καταχωρητή που αποτελείται από δύο qubits. Έστω ότι η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|10\rangle$, τότε:

$$C\Phi |10\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle \quad (3.23)$$

Ας δούμε και την περίπτωση $|11\rangle$:

$$C\Phi |11\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ e^{i\phi} \end{bmatrix} = e^{i\phi} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = e^{i\phi} |11\rangle \quad (3.24)$$

Δηλαδή, αλλάζει η γωνία φάσης της κατάστασης $|11\rangle$. Με τον ίδιο τρόπο μπορούμε να υπολογίσουμε και τις άλλες δύο περιπτώσεις.



Σχήμα 3-6. Το σύμβολο της κβαντικής πύλης ελεγχόμενης μετατόπισης φάσης, $C\Phi$.

$ c_i t_i\rangle$	$ c_o t_o\rangle$
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 10\rangle$
$ 11\rangle$	$e^{i\varphi} 11\rangle$

Πίνακας 3-6. Η δράση της κβαντικής πύλης $C\Phi$ στα qubits ελέγχου και στόχου.

Στο Σχήμα 3-6 φαίνεται το σύμβολο της πύλης $C\Phi$ και στον Πίνακα 3-6 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των δύο qubits πριν τη δράση της πύλης ($|c_i t_i\rangle$) και στη δεύτερη οι καταστάσεις τους μετά τη δράση της πύλης ($|c_o t_o\rangle$).

3. 5 Κβαντικές πύλες που δρουν σε τρία qubits

Παρακάτω θα περιγραφούν δύο κβαντικές πύλες που δρουν σε τρία qubits, η κβαντική πύλη διπλά ελεγχόμενου OXI και η κβαντική πύλη Fredkin. Μπορεί επίσης να θεωρηθεί ότι οι πύλες αυτές δρουν σε κβαντικούς καταχωρητές των τριών qubits.

3.5.1 Η κβαντική πύλη διπλά ελεγχόμενου OXI

Ο Αγγλικός όρος για την πύλη αυτή είναι Controlled-Controlled-NOT και ο τελεστής που την περιγράφει συμβολίζεται με $CCNOT$. Η πύλη αυτή δρα σε τρία qubits. Τα δύο qubits ονομάζονται qubits ελέγχου, και συμβολίζονται με c_1 και c_2 και το άλλο qubit στόχος και συμβολίζεται με t . Οι καταστάσεις των τριών qubits πριν τη δράση της πύλης είναι $|c_{1i}\rangle$, $|c_{2i}\rangle$ και $|t_i\rangle$, ενώ οι καταστάσεις των qubits μετά τη δράση της πύλης είναι $|c_{1o}\rangle$, $|c_{2o}\rangle$ και $|t_o\rangle$. Η πύλη $CCNOT$ αλλάζει την κατάσταση του qubit στόχου, όταν και τα δύο qubits ελέγχου βρίσκονται στην κατάσταση $|1\rangle$, ενώ δεν αλλάζει την κατάσταση του qubit στόχου σε κάθε

άλλη περίπτωση. Οι καταστάσεις των qubits ελέγχου $|c_i\rangle$ και $|c_{2i}\rangle$ δεν μεταβάλλονται, δηλαδή ισχύει πάντα $|c_i\rangle = |c_{1o}\rangle$ και $|c_{2i}\rangle = |c_{2o}\rangle$.

Η πύλη $CCNOT$ περιγράφεται από τον παρακάτω πίνακα:

$$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad (3.25)$$

Η γενική περιγραφή της δράσης της πύλης είναι:

$$CCNOT |c_{2i} c_{1i} t_i\rangle = |c_{2o} c_{1o} t_o\rangle \quad (3.26)$$

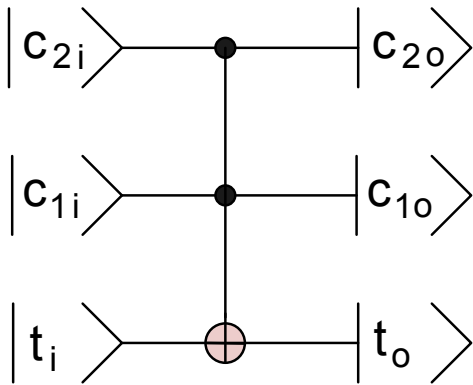
Ας δούμε τη δράση αυτής της πύλης σε έναν καταχωρητή που αποτελείται από τρία qubits. Έστω ότι η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|101\rangle$, τότε:

$$CCNOT |101\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |101\rangle \quad (3.27)$$

Ας δούμε και την περίπτωση που η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|111\rangle$:

$$CCNOT |111\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |110\rangle \quad (3.28)$$

Δηλαδή, η κατάσταση του qubit στόχου αλλάζει μόνο όταν και τα δύο qubits ελέγχου βρίσκονται στην κατάσταση $|1\rangle$. Με τον ίδιο τρόπο υπολογίζουμε και τις άλλες περιπτώσεις.



Σχήμα 3-7. Το σύμβολο και οι ιδιότητες της κβαντικής πύλης διπλά ελεγχόμενου OXI, CCNOT.

$ c_i t_{2i} t_{1i}\rangle$	$ c_o t_{2o} t_{1o}\rangle$
$ 000\rangle$	$ 000\rangle$
$ 001\rangle$	$ 001\rangle$
$ 010\rangle$	$ 010\rangle$
$ 011\rangle$	$ 011\rangle$
$ 100\rangle$	$ 100\rangle$
$ 101\rangle$	$ 110\rangle$
$ 110\rangle$	$ 101\rangle$
$ 111\rangle$	$ 111\rangle$

Πίνακας 3-7. Η δράση της κβαντικής πύλης CCNOT στα qubits ελέγχου και στόχου.

Στο Σχήμα 3-7 φαίνεται το σύμβολο της πύλης CCNOT και στον Πίνακα 3-7 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των τριών qubits πριν τη δράση της πύλης ($|c_{2i} c_{1i} t_i\rangle$) και στη δεύτερη οι καταστάσεις τους μετά τη δράση της πύλης ($|c_{2o} c_{1o} t_o\rangle$).

3.5.2 Η κβαντική πύλη Fredkin

Η κβαντική πύλη Fredkin δρα σε τρία qubits και ο τελεστής της συμβολίζεται με F . Το ένα qubit ονομάζεται qubit ελέγχου, και συμβολίζεται με c , και τα άλλα δύο qubits ονομάζονται qubits στόχοι και συμβολίζονται με t_1 και t_2 . Οι καταστάσεις των τριών qubits πριν τη δράση της πύλης είναι $|c_i\rangle$, $|t_{1i}\rangle$ και $|t_{2i}\rangle$, ενώ οι καταστάσεις των qubits μετά τη δράση της πύλης είναι $|c_o\rangle$, $|t_{1o}\rangle$ και $|t_{2o}\rangle$. Η πύλη F εναλλάσσει τις καταστάσεις των qubits στόχων, όταν το qubit ελέγχου βρίσκεται στην κατάσταση $|1\rangle$. Όταν το qubit ελέγχου

βρίσκεται στην κατάσταση $|0\rangle$, οι καταστάσεις των qubits στόχων δεν αλλάζουν. Η κατάσταση του qubit ελέγχου $|c_i\rangle$ δεν μεταβάλλεται, δηλαδή ισχύει πάντα $|c_i\rangle = |c_o\rangle$.

Η πύλη F περιγράφεται από τον παρακάτω πίνακα:

$$F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (3.29)$$

Η γενική περιγραφή της δράσης της πύλης είναι:

$$F |c_i t_{2i} t_{1i}\rangle = |c_o t_{2o} t_{1o}\rangle \quad (3.30)$$

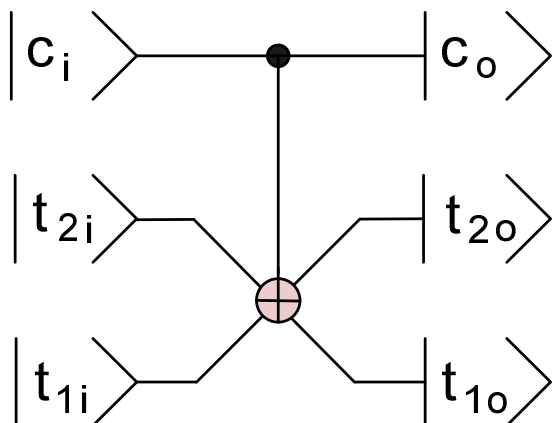
Ας δούμε τη δράση αυτής της πύλης F σε έναν καταχωρητή που αποτελείται από τρία qubits. Έστω ότι η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|001\rangle$, τότε:

$$F |001\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |001\rangle \quad (3.31)$$

Ας δούμε και την περίπτωση όπου η κατάσταση του κβαντικού καταχωρητή πριν τη δράση της πύλης είναι $|101\rangle$, τότε:

$$F |101\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |110\rangle \quad (3.32)$$

Δηλαδή οι καταστάσεις των qubits στόχων εναλλάχθηκαν διότι το qubit ελέγχου βρισκόταν στην κατάσταση $|1\rangle$. Με τον ίδιο τρόπο υπολογίζουμε και τις άλλες περιπτώσεις.



Σχήμα 3-8. Το σύμβολο και οι ιδιότητες της κβαντικής πύλης Fredkin, F .

$ c_i t_{2i} t_{1i}\rangle$	$ c_o t_{2o} t_{1o}\rangle$
$ 000\rangle$	$ 000\rangle$
$ 001\rangle$	$ 001\rangle$
$ 010\rangle$	$ 010\rangle$
$ 011\rangle$	$ 011\rangle$
$ 100\rangle$	$ 100\rangle$
$ 101\rangle$	$ 110\rangle$
$ 110\rangle$	$ 101\rangle$
$ 111\rangle$	$ 111\rangle$

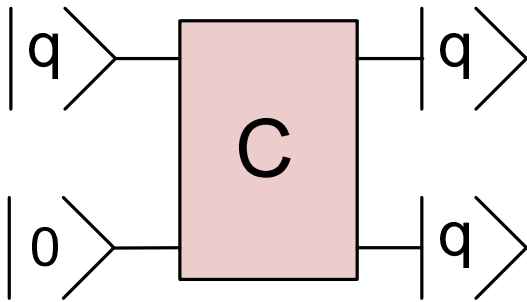
Πίνακας 3-8. Η δράση της κβαντικής πύλης Fredkin στα qubits ελέγχου και στόχου.

Στο Σχήμα 3-8 φαίνεται το σύμβολο της πύλης F και στον Πίνακα 3-8 οι ιδιότητές της. Στην πρώτη στήλη του πίνακα φαίνονται οι καταστάσεις των τριών qubits πριν τη δράση της πύλης ($|c_i t_{2i} t_{1i}\rangle$) και στη δεύτερη οι καταστάσεις τους μετά τη δράση της πύλης ($|c_o t_{2o} t_{1o}\rangle$).

3.6 Η αδυναμία αντιγραφής της κατάστασης ενός qubit

Εδώ θα αναφερθούμε σε μία πύλη που δεν υπάρχει. Η διακλάδωση (cloning) ενός bit σε δύο ανεξάρτητα bits, δηλαδή η αντιγραφή ενός bit, είναι πάρα πολύ εύκολη στους κλασικούς υπολογιστές. Κάτι τέτοιο όμως

είναι αδύνατον στους κβαντικούς υπολογιστές, δηλαδή δεν μπορούμε να αντιγράψουμε την άγνωστη κατάσταση ενός qubit (Hirvensalo, 2001). Ας δούμε καλύτερα αυτή την αδυναμία.



Σχήμα 3-9. Η κατάσταση του άγνωστου qubit $|q\rangle$ διακλαδίζεται (αντιγράφεται) με τη δράση της κβαντικής πύλης C . Μια τέτοια πύλη είναι αδύνατον να υπάρξει.

Στο Σχήμα 3-9 φαίνεται μία κβαντική πύλη που τον τελεστή της τον ονομάσαμε C . Η πύλη αυτή δρα σε δύο qubits. Το ένα βρίσκεται στην κατάσταση $|0\rangle$ και το άλλο σε μία άγνωστη κατάσταση $|q\rangle$. Η κβαντική αυτή πύλη αλλάζει την κατάσταση του qubit που βρίσκεται στην κατάσταση $|0\rangle$, ώστε να γίνει ίδια με την κατάσταση $|q\rangle$. Μετά τη δράση της πύλης και τα δύο qubits βρίσκονται στην ίδια κατάσταση, δηλαδή η κατάσταση του $|q\rangle$ αντιγράφηκε στο qubit που είχε αρχικά την κατάσταση $|0\rangle$. Έχει αποδειχθεί ότι μια τέτοια πύλη είναι αδύνατον να υπάρξει. Αυτή η απόδειξη είναι γνωστή ως το θεώρημα αδυναμίας διακλάδωσης (στα Αγγλικά no-cloning theorem). Παρακάτω θα διατυπώσουμε και θα αποδείξουμε το θεώρημα αυτό.

Θεώρημα της αδυναμίας διακλάδωσης: Δεν μπορεί να υπάρξει μια κβαντική πύλη C τέτοια ώστε:

$$C |q 0\rangle = |q q\rangle \quad (3.33)$$

όπου $|q\rangle$ είναι ένα qubit με άγνωστη κατάσταση.

Απόδειξη: Υποθέτουμε ότι υπάρχει μία τέτοια κβαντική πύλη. Αυτή η κβαντική πύλη αντιπροσωπεύεται από τον ορθομοναδιαίο τελεστή \hat{C} . Βάζουμε την πύλη να δράσει σε δύο qubits το $|q\rangle$ και το $|b\rangle$ που είναι ορθογώνια μεταξύ τους και να τα αντιγράψει:

$$\hat{C} |q 0\rangle = |q q\rangle \quad (3.34)$$

$$\hat{C} |b 0\rangle = |b b\rangle$$

Θεωρούμε ένα άλλο qubit, το $|c\rangle$, η κατάσταση του οποίου είναι η υπέρθεση των καταστάσεων των δύο ορθογώνιων qubits $|q\rangle$ και $|b\rangle$:

Θεωρούμε τη γραμμική υπέρθεση των δύο qubits:

$$|c\rangle = \frac{1}{\sqrt{2}}(|q\rangle + |b\rangle) \quad (3.35)$$

Δρούμε τώρα με την κβαντική πύλη C στο qubit $|c\rangle$ αντιγράφοντας την κατάσταση του:

$$\begin{aligned} \hat{C}|c0\rangle &= \frac{1}{\sqrt{2}} \hat{C}(|q\rangle + |b\rangle)|0\rangle = \frac{1}{\sqrt{2}} \hat{C}(|q0\rangle + |b0\rangle) = \frac{1}{\sqrt{2}} \left(\hat{C}|q0\rangle + \hat{C}|b0\rangle \right) \\ &= \frac{1}{\sqrt{2}} (|qq\rangle + |bb\rangle) \end{aligned} \quad (3.36)$$

Αλλά πρέπει να ισχύει και:

$$\hat{C}|c0\rangle = |cc\rangle = |c\rangle|c\rangle = \frac{1}{\sqrt{2}}(|q\rangle + |b\rangle) \frac{1}{\sqrt{2}}(|q\rangle + |b\rangle) = \frac{1}{2}(|qq\rangle + |qb\rangle + |bq\rangle + |bb\rangle) \quad (3.37)$$

Οι εξισώσεις (3.36) και (3.37) έχουν τα αριστερά τους μέλη ίσα μεταξύ τους, όμως τα δεξιά τους μέλη είναι διαφορετικά, επομένως η κβαντική πύλη C δεν είναι δυνατόν να υπάρχει. ♦

Η αδυναμία διακλάδωσης, δηλαδή η αδυναμία αντιγραφής των qubits αποτελεί τη βάση της κβαντικής κρυπτογραφίας. Ας υποθέσουμε ότι η Αλίκη θέλει να στείλει στον Βασίλη ένα μήνυμα και το κωδικοποιεί σε qubits. Η Εύα θέλει να υποκλέψει το μήνυμα. Ακόμα και αν το μήνυμα βρεθεί στα χέρια της, δεν μπορεί να το αντιγράψει και να το αποκωδικοποιήσει. Αν το κρατήσει, τότε, για να το διαβάσει πρέπει να καταστρέψει την υπέρθεση των καταστάσεων των qubits. Δεν μπορεί δηλαδή να το διαβάσει και μετά να το στείλει στον Βασίλη. Ο Βασίλης δεν θα λάβει το μήνυμα και θα είναι σίγουρος ότι έχει υποκλαπεί και ότι η Εύα γνωρίζει το περιεχόμενό του, οπότε θα αλλάξει την τακτική ή τη στρατηγική του.

Ας συνοψίσουμε:

- Οι καταστάσεις των qubits και των κβαντικών καταχωρητών είναι διανύσματα στον χώρο Hilbert. Οι κβαντικές πύλες είναι ορθομοναδιαίοι τελεστές του χώρου Hilbert που δρουν σε qubits και σε κβαντικούς καταχωρητές αλλάζοντας την κατάσταση τους. Δηλαδή, οι κβαντικές πύλες περιστρέφουν τα διανύσματα κατάστασης των qubits και των κβαντικών καταχωρητών χωρίς να αλλάζουν το μήκος τους, το οποίο είναι πάντα ίσο με τη μονάδα.
- Οι κβαντικές πύλες που δρουν σε ένα qubit είναι η πύλη αδρανείας, I , η πύλη μετατόπισης φάσης, Φ και η πύλη Hadamard, H .
- Με τις κβαντικές πύλες Pauli μπορούμε να εκτελέσουμε όλες τις περιστροφές του διανύσματος κατάστασης ενός qubit στη σφαίρα Bloch.
- Οι κβαντικές πύλες που δρουν σε δύο qubits είναι η πύλη ελεγχόμενου ΟΧΙ, $CNOT$ και η πύλη ελεγχόμενης μετατόπισης φάσης, $C\Phi$.
- Οι κβαντικές πύλες που δρουν σε τρία qubits είναι η πύλη διπλά ελεγχόμενου ΟΧΙ, $CCNOT$ και η πύλη Fredkin, F .
- Η πύλη $CNOT$ η πύλη H και η πύλη Φ αποτελούν ένα γενικευμένο σύνολο κβαντικών πυλών. Δηλαδή μπορούμε να εκτελέσουμε οποιοδήποτε κβαντικό υπολογισμό χρησιμοποιώντας μόνο αυτές τις πύλες.
- Δεν μπορούμε να αντιγράψουμε την άγνωστη κατάσταση ενός qubit.

Βιβλιογραφία

- Barenco A., Bennett Ch. H., Cleve, R. et al., Elementary Gates for Quantum Computation, *Physical Review A*, vol. 52, pp. 3457-3467, 1995.
- Cybenko G., Reducing Quantum Computations to Elementary Unitary Operations, *IEEE Computers*, March/April issue, pp. 27-32, 2001.
- Hirvensalo M., *Quantum computing*, Springer-Verlag, 2001.
- Kaye P., Laflamme R., & Mosca M., *An introduction to quantum computing*, Oxford University Press, 2007.
- Keyl M, Fundamentals of Quantum Information Theory, *Physics Reports*, vol. 369, pp. 431-548, 2002.

Ασκήσεις

Άσκηση 3.1

Μία κβαντική πύλη που δρα σε ένα qubit, αλλά χρησιμοποιείται ελάχιστα είναι η πύλη \sqrt{NOT} . Η πύλη συμβολίζεται με $U_{\sqrt{NOT}}$ και περιγράφεται από τον πίνακα:

$$U_{\sqrt{NOT}} = \begin{bmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{bmatrix}$$

Να δείξετε ότι ο πίνακας αυτός είναι ορθομοναδιαίος.

Άσκηση 3.2

Να εφαρμόσετε την κβαντική πύλη $U_{\sqrt{NOT}}$ δύο φορές σε ένα qubit που βρίσκεται:

- Στη βασική κατάσταση $|0\rangle$
- Στη βασική κατάσταση $|1\rangle$

Άσκηση 3.3

Οι πίνακες:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

ονομάζονται πίνακες Pauli και είναι πολύ χρήσιμοι, γιατί μπορούμε με αυτούς να συνθέσουμε κβαντικές πύλες. (Να τους συγκρίνετε με τις κβαντικές πύλες Pauli). Να γράψετε την κβαντική πύλη H ως συνάρτηση των πινάκων Pauli πολλαπλασιασμένη επί έναν πραγματικό αριθμό.

Άσκηση 3.4

Υποθέστε ότι οι πίνακες Pauli περιγράφουν κβαντικές πύλες. Να υπολογίσετε τις δράσεις τους στις βασικές καταστάσεις του qubit. Δηλαδή να υπολογίσετε τα:

α. $\sigma_x |0\rangle$, β. $\sigma_x |1\rangle$

γ. $\sigma_y |0\rangle$, δ. $\sigma_y |1\rangle$

ε. $\sigma_z |0\rangle$, στ. $\sigma_z |1\rangle$

Άσκηση 3.5

Να υπολογίσετε τη δράση της κβαντικής πύλης $CNOT$ στις παρακάτω βασικές καταστάσεις:

α. $|00\rangle$

β. $|11\rangle$

Άσκηση 3.6

Να υπολογίσετε τη δράση της κβαντικής πύλης $C\Phi$ στη βασική κατάσταση $|01\rangle$:

Άσκηση 3.7

Να υπολογίσετε τη δράση της κβαντικής πύλης $CCNOT$ στις παρακάτω βασικές καταστάσεις:

α. $|011\rangle$

β. $|110\rangle$

Άσκηση 3.8

Να υπολογίσετε τη δράση της κβαντικής πύλης F στις παρακάτω βασικές καταστάσεις:

α. $|000\rangle$

β. $|110\rangle$

Άσκηση 3.9

Να υπολογίσετε τη δράση της κβαντικής πύλης H στο παρακάτω qubit που βρίσκεται σε υπέρθεση βασικών καταστάσεων:

$$|q\rangle = a |0\rangle + b |1\rangle$$

Άσκηση 3.10

Να υπολογίσετε τη δράση της κβαντικής πύλης $CNOT$ στο παρακάτω qubit που βρίσκεται σε υπέρθεση βασικών καταστάσεων:

$$|q\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

Άσκηση 3.11

Να υπολογίσετε τη δράση της κβαντικής πύλης $C\Phi$ στο παρακάτω qubit που βρίσκεται σε υπέρθεση βασικών καταστάσεων:

$$|q\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle$$

Άσκηση 3.12

Να υπολογίσετε τη δράση της κβαντικής πύλης $CCNOT$ στο παρακάτω qubit που βρίσκεται σε υπέρθεση βασικών καταστάσεων:

$$|q\rangle = c_0|000\rangle + c_1|001\rangle + c_2|010\rangle + c_3|011\rangle + c_4|100\rangle + c_5|101\rangle + c_6|110\rangle + c_7|111\rangle$$

Άσκηση 3.13

Να υπολογίσετε τη δράση της κβαντικής πύλης F στο παρακάτω qubit που βρίσκεται σε υπέρθεση βασικών καταστάσεων:

$$|q\rangle = c_0|000\rangle + c_1|001\rangle + c_2|010\rangle + c_3|011\rangle + c_4|100\rangle + c_5|101\rangle + c_6|110\rangle + c_7|111\rangle$$

4. Η αρχή της κβαντικής υπολογιστικής - Κβαντικός αλγόριθμος του Deutsch

Σύνοψη

Στο κεφάλαιο αυτό περιγράφεται το κυκλωματικό μοντέλο των κβαντικών υπολογισμών και δίνεται ένα αναλυτικό παράδειγμα κβαντικού υπολογισμού. Παρουσιάζεται η αρχή της κβαντικής υπολογιστικής και δίνεται το διάγραμμα ροής της. Δίνεται η εξίσωση του Schrödinger στη μορφή στην οποία βασίζεται η αρχή της κβαντικής υπολογιστικής. Περιγράφεται ο κβαντικός αλγόριθμος του Deutsch και δίνεται ένα παράδειγμα εφαρμογής του.

Προαπαιτούμενη γνώση

Γραμμική άλγεβρα, το πρώτο, δεύτερο και τρίτο κεφάλαιο αυτού του βιβλίου.

4.1 Το κυκλωματικό μοντέλο των κβαντικών υπολογισμών

Όπως είχαμε πει στην αρχή του 3^{ου} κεφαλαίου, οι κλασικοί υπολογιστές αποτελούνται από αγωγούς και λογικές πύλες, οι οποίες συγκροτούν κυκλώματα και επεξεργαστές. Οι αγωγοί μεταφέρουν την πληροφορία από πύλη σε πύλη όπου γίνεται η επεξεργασία της. Οι πύλες των κλασικών υπολογιστών είναι φυσικά συστήματα και η πληροφορία διέρχεται μέσα από αυτές. Μάθαμε στο ίδιο κεφάλαιο ότι στους κβαντικούς υπολογιστές η πληροφορία βρίσκεται αποθηκευμένη σε qubits ή σε κβαντικούς καταχωρητές και παραμένει εκεί. Οι κβαντικές πύλες συνήθως δεν είναι φυσικά συστήματα, αλλά αντιπροσωπεύουν δράσεις που ασκούνται σε qubits ή σε κβαντικούς καταχωρητές.

Οι κβαντικοί υπολογισμοί είναι δράσεις τελεστών που έχουν ως αποτέλεσμα την περιστροφή διανυσμάτων στο χώρο Hilbert. Είναι αδύνατο να σχηματίσουμε κάποια εικόνα για αυτούς στο μυαλό μας. Έχουν γίνει αρκετές προσπάθειες, για να αναπαρασταθούν οι κβαντικοί υπολογισμοί με κάποιο μοντέλο. Το πιο επιτυχημένο μοντέλο, που σήμερα χρησιμοποιείται σχεδόν αποκλειστικά, είναι το κυκλωματικό μοντέλο των κβαντικών υπολογισμών. Κάθε κβαντικός υπολογισμός, απλός ή πολύπλοκος, μπορεί να αναπαρασταθεί με ένα κύκλωμα. Τα κυκλώματα που αναπαριστούν κβαντικούς υπολογισμούς ονομάζονται κβαντικά κυκλώματα και αποτελούνται από qubits, κβαντικούς καταχωρητές και κβαντικές πύλες. Στα κβαντικά κυκλώματα δεν υπάρχει ροή πληροφορίας από πύλη σε πύλη, αλλά διαδοχικές δράσεις κβαντικών πυλών σε κβαντικούς καταχωρητές στους οποίους βρίσκεται αποθηκευμένη η πληροφορία. Τα κβαντικά κυκλώματα αναπαριστούν τη χρονική σειρά και τον τρόπο με τον οποίο δρουν οι κβαντικές πύλες στους κβαντικούς καταχωρητές (Nielsen & Chuang, 2000).

Ας αρχίσουμε την παρουσίαση και την περιγραφή του κυκλωματικού μοντέλου των κβαντικών υπολογισμών με ένα παράδειγμα. Στο παράδειγμα αυτό θα αναπαραστήσουμε με ένα κβαντικό κύκλωμα ένα γνωστό μας κβαντικό υπολογισμό, το παιχνίδι του Quant με τον Captain Class. Θα κάνουμε όμως μία μικρή αλλαγή στο συμβολισμό των καταστάσεων του κβαντικού κέρματος. Η κατάσταση στην οποία το κβαντικό κέρμα βρίσκεται με το γράμμα H στην πάνω όψη συμβολίζεται με $|0\rangle$ και η κατάσταση με το γράμμα T στην πάνω όψη συμβολίζεται με $|1\rangle$, δηλαδή το κβαντικό κέρμα είναι ένα qubit. Ο κβαντικός υπολογισμός αποτελείται από τα παρακάτω βήματα:

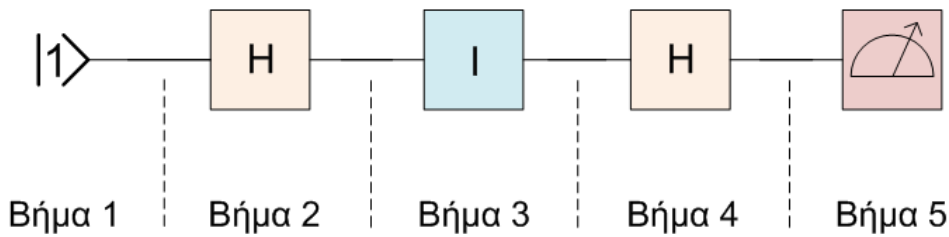
Βήμα 1^ο: Ο Captain Class τοποθετεί το κέρμα με το γράμμα T στην πάνω όψη.

Βήμα 2^ο: Ο Quant δρα στο κέρμα με την κβαντική πύλη Hadamard (H).

Βήμα 3^ο: Ο Captain Class δρα στο κέρμα με την κβαντική πύλη αδρανείας (I), δηλαδή δεν αλλάζει την κατάστασή του.

Βήμα 4^ο: Ο Quant δρα για δεύτερη φορά στο κέρμα με την κβαντική πύλη Hadamard (H).

Βήμα 5^ο: Βγάζουν το κάλυμμα για να φανεί το κέρμα, μετρούν δηλαδή την κατάσταση του. Φυσικά, το κέρμα βρίσκεται στην κατάσταση που βρισκόταν στην αρχή του παιχνιδιού.



Σχήμα 4-1. Το κυκλωματικό μοντέλο του κβαντικού υπολογισμού του παιχνιδιού του Quant με τον Captain Class.

Το κβαντικό κύκλωμα που αναπαριστά αυτόν τον κβαντικό υπολογισμό φαίνεται στο Σχήμα 4-1. Το ορθογώνιο με το ημικύκλιο και το βέλος στο 5^ο βήμα δεν είναι κβαντική πύλη, αλλά συμβολίζει τη μέτρηση της κατάστασης του qubit, δηλαδή του κέρματος. Δεν είναι απαραίτητο να σημειώνουμε τη μέτρηση σε ένα κβαντικό κύκλωμα, διότι κάθε κβαντικός υπολογισμός τελειώνει με μέτρηση της κατάστασης του qubit ή του κβαντικού καταχωρητή.

Πρέπει εδώ να τονίσουμε για ακόμη μία φορά ότι στα κβαντικά κυκλώματα η πληροφορία, που είναι αποθηκευμένη στα qubits ή στους κβαντικούς καταχωρητές, δε μεταφέρεται από πύλη σε πύλη. Η πληροφορία μένει στα qubits ή στους κβαντικούς καταχωρητές όπου δρουν οι κβαντικές πύλες. Το κέρμα δηλαδή μένει σκεπασμένο πάνω στο τραπέζι και δρουν σ' αυτό διαδοχικά οι δύο παίκτες. Το κβαντικό κύκλωμα αναπαριστά τη χρονική σειρά με την οποία δρουν οι κβαντικές πύλες. Από εδώ και εμπρός θα χρησιμοποιούμε το κυκλωματικό μοντέλο για να αναπαραστήσουμε κβαντικούς υπολογισμούς. Στα κβαντικά κυκλώματα δεν πρέπει να υπάρχουν διακλαδώσεις, αφού δεν μπορούμε να αντιγράψουμε την κατάσταση ενός qubit. Επίσης, δεν πρέπει να υπάρχουν βρόχοι ανάδρασης (Milburn, 1998).

4.2 Ένας αναλυτικός κβαντικός υπολογισμός

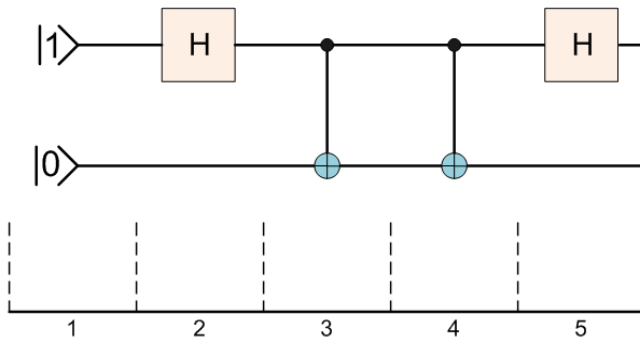
Στο πάνω μέρος του Σχήματος 4-2 φαίνεται ένα κβαντικό κύκλωμα που αναπαριστά έναν κβαντικό υπολογισμό. Θα κάνουμε τον υπολογισμό αυτό βήμα προς βήμα:

Βήμα 1^ο: Ο κβαντικός καταχωρητής του κυκλώματος αποτελείται από δύο qubits και η κατάστασή του είναι η $|10\rangle$. Ο πίνακας που αντιστοιχεί στην κατάσταση αυτή είναι το ταυυστικό γινόμενο των πινάκων που αντιστοιχούν στις καταστάσεις των δύο qubits:

$$|10\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 0|00\rangle + 0|01\rangle + 1|10\rangle + 0|11\rangle \quad (4.1)$$

Αν μετρήσουμε την κατάσταση του κβαντικού καταχωρητή στο βήμα αυτό, θα βρούμε με πιθανότητα ίση με τη μονάδα (δηλαδή σίγουρα) την κατάσταση $|10\rangle$.

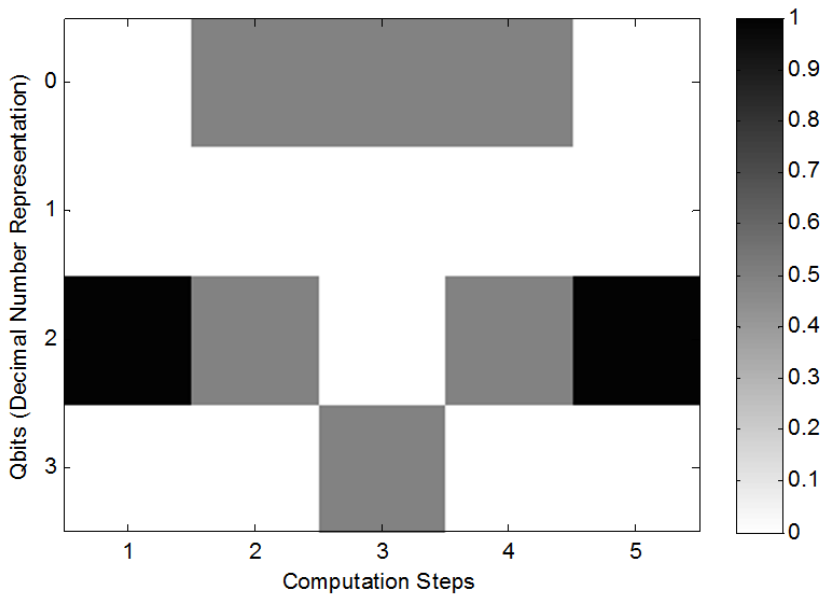
Στο μέσον του Σχήματος 4-2 φαίνεται ένας πίνακας του οποίου οι στήλες αντιστοιχούν στα βήματα του κβαντικού υπολογισμού και οι γραμμές στις βασικές καταστάσεις του κβαντικού καταχωρητή. Οι βασικές καταστάσεις αναγράφονται και ως δεκαδικοί αριθμοί. Στον πίνακα αυτό αναγράφονται οι πιθανότητες να μετρήσουμε τις βασικές καταστάσεις του κβαντικού καταχωρητή σε κάθε βήμα του κβαντικού υπολογισμού. Φυσικά, το άθροισμα των πιθανοτήτων σε κάθε στήλη του πίνακα πρέπει να είναι ίσο με τη μονάδα.



Βήματα υπολογισμού

0 $ 00\rangle$	0	0,5	0,5	0,5	0
1 $ 01\rangle$	0	0	0	0	0
2 $ 10\rangle$	1	0,5	0	0,5	1
3 $ 11\rangle$	0	0	0,5	0	0
	1	2	3	4	5

Βήματα υπολογισμού



Σχήμα 4-2. Στο πάνω μέρος φαίνεται το κβαντικό κύκλωμα. Στο μέσον δίνεται ο πίνακας με τις πιθανότητες να μετρηθούν οι καταστάσεις σε κάθε βήμα του κβαντικού υπολογισμού. Στο κάτω μέρος φαίνεται το αποτέλεσμα της προσομοίωσης του κβαντικού υπολογισμού από τον Προσομοιωτή Κβαντικού Υπολογιστή QCS.

Στο πρώτο βήμα η πιθανότητα να μετρήσουμε την $|10\rangle$ είναι ένα, ενώ η πιθανότητα να μετρήσουμε τις άλλες τρεις είναι μηδέν.

Βήμα 2^ο: Στο βήμα αυτό στο δεύτερο qubit δρα η πύλη Hadamard (H) και στο πρώτο qubit δεν δρα καμία πύλη. Αυτό είναι ισοδύναμο με τη δράση της πύλης αδρανείας I . Συνήθως, όταν σε κάποιο βήμα δεν δρα καμία πύλη σε κάποιο qubit, δεν βάζουμε στο κβαντικό κύκλωμα την πύλη αδρανείας, αλλά μία συνεχόμενη γραμμή όπως στο Σχήμα 4-2. Είναι πολύ σημαντικό όμως να θυμόμαστε ότι η συνεχής αυτή γραμμή αντιστοιχεί σε μία πύλη αδρανείας, γιατί στους κβαντικούς υπολογιστές το «δεν κάνω τίποτα» είναι και αυτό μία δράση. Αυτό θα το δούμε αμέσως παρακάτω.

Η συνολική δράση των κβαντικών πυλών σε ένα βήμα του κβαντικού υπολογισμού εκφράζεται από το τανυστικό γινόμενο των πινάκων που περιγράφουν τις πύλες αυτές. Στο 2^ο κεφάλαιο είδαμε πώς υπολογίζουμε το τανυστικό γινόμενο πινάκων με μία μόνο στήλη. Πριν προχωρήσουμε ας δούμε πώς υπολογίζουμε το τανυστικό γινόμενο δύο πινάκων που έχουν περισσότερες από μία στήλες και γραμμές. Αν έχουμε δύο πίνακες τον A και τον B :

$$A = \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} \quad B = \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \quad (4.2)$$

τότε, το τανυστικό τους γινόμενο δίνεται από:

$$\begin{aligned} A \otimes B &= \begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} \otimes \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} = \begin{bmatrix} a_{1,1} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} & a_{1,2} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \\ a_{2,1} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} & a_{2,2} \begin{bmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{bmatrix} \end{bmatrix} \\ &= \begin{bmatrix} a_{1,1} b_{1,1} & a_{1,1} b_{1,2} & a_{1,2} b_{1,1} & a_{1,2} b_{1,2} \\ a_{1,1} b_{2,1} & a_{1,1} b_{2,2} & a_{1,2} b_{2,1} & a_{1,2} b_{2,2} \\ a_{2,1} b_{1,1} & a_{2,1} b_{1,2} & a_{2,2} b_{1,1} & a_{2,2} b_{1,2} \\ a_{2,1} b_{2,1} & a_{2,1} b_{2,2} & a_{2,2} b_{2,1} & a_{2,2} b_{2,2} \end{bmatrix} \quad (4.3) \end{aligned}$$

Στο δεύτερο βήμα του κβαντικού υπολογισμού δρουν οι πύλες I και H . Η συνολική τους δράση δίνεται από το τανυστικό τους γινόμενο. Για να υπολογίσουμε το τανυστικό γινόμενο γράφουμε στην πιο δεξιά θέση την πύλη που δρα στο πρώτο qubit και στην πιο αριστερή αυτήν που δρα στο τελευταίο:

$$H \otimes I = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \quad (4.4)$$

Εδώ φαίνεται ότι το «δεν κάνω τίποτα», δηλαδή η δράση της πύλης αδρανείας, συμβάλλει στο τανυστικό γινόμενο. Θα υπολογίσουμε τώρα την κατάσταση του κβαντικού καταχωρητή στο τέλος του 2^{ου} βήματος, δηλαδή μετά τη δράση των πυλών:

$$H \otimes I |10\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} \quad (4.5)$$

$$= \frac{1}{\sqrt{2}} |00\rangle + 0 |01\rangle - \frac{1}{\sqrt{2}} |10\rangle + 0 |11\rangle = \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |10\rangle$$

Αφού θυμηθούμε ότι η πιθανότητα δίνεται από το τετράγωνο του μέτρου του πλάτους πιθανότητας, διαπιστώνουμε από την (4.5) ότι στο τέλος του 2^{ου} βήματος η πιθανότητα να βρεθεί ο κβαντικός καταχωρητής στην κατάσταση $|00\rangle$ είναι 0,5 και η πιθανότητα να βρεθεί στην κατάσταση $|10\rangle$ είναι 0,5. Οι πιθανότητες αυτές αναγράφονται στη δεύτερη στήλη του πίνακα που βρίσκεται στο μέσον του Σχήματος 4-2.

Βήμα 3^ο: Στο βήμα αυτό δρα στον κβαντικό καταχωρητή μόνο η κβαντική πύλη ελεγχόμενου όχι (*CNOT*). Για να υπολογίσουμε την κατάσταση του κβαντικού καταχωρητή στο τέλος του τρίτου βήματος, δηλαδή μετά τη δράση της *CNOT*, πολλαπλασιάζουμε τον πίνακα που περιγράφει την πύλη επί τον πίνακα της κατάστασης του κβαντικού καταχωρητή που υπολογίστηκε στο αμέσως προηγούμενο βήμα:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \quad (4.6)$$

$$= \frac{1}{\sqrt{2}} |00\rangle + 0 |01\rangle + 0 |10\rangle - \frac{1}{\sqrt{2}} |11\rangle = \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |11\rangle$$

Στο τέλος του 3^{ου} βήματος η πιθανότητα να βρεθεί ο κβαντικός καταχωρητής στην κατάσταση $|00\rangle$ είναι 0,5 και η πιθανότητα να βρεθεί στην κατάσταση $|11\rangle$ είναι 0,5. Οι πιθανότητες αυτές αναγράφονται στην τρίτη στήλη του πίνακα του Σχήματος 4-2.

Βήμα 4^ο: Όπως και στο 3^ο βήμα, στο βήμα αυτό δρα στον κβαντικό καταχωρητή μόνο η κβαντική πύλη ελεγχόμενου όχι (*CNOT*). Για να υπολογίσουμε την κατάσταση του κβαντικού καταχωρητή στο τέλος του τετάρτου βήματος, πολλαπλασιάζουμε τον πίνακα που περιγράφει την πύλη επί τον πίνακα της κατάστασης του κβαντικού καταχωρητή που υπολογίστηκε στο αμέσως προηγούμενο βήμα:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} \quad (4.7)$$

$$= \frac{1}{\sqrt{2}} |00\rangle + 0 |01\rangle - \frac{1}{\sqrt{2}} |10\rangle + 0 |11\rangle = \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |10\rangle$$

Στο τέλος του 4^{ου} βήματος η πιθανότητα να βρεθεί ο κβαντικός καταχωρητής στην κατάσταση $|00\rangle$ είναι 0,5 και η πιθανότητα να βρεθεί στην κατάσταση $|10\rangle$ είναι 0,5. Οι πιθανότητες αυτές αναγράφονται στην τέταρτη στήλη του πίνακα του Σχήματος 4-2.

Βήμα 5^ο: Στο βήμα αυτό, που είναι και το τελευταίο, στο δεύτερο qubit δρα η πύλη Hadamard (H) και στο πρώτο qubit δεν δρα καμία πύλη, δηλαδή δρα η πύλη αδρανεΐας. Η συνολική δράση των κβαντικών πυλών στο βήμα αυτό, εκφράζεται από το τανυστικό γινόμενο των πινάκων που περιγράφουν τις πύλες. Για να υπολογίσουμε την κατάσταση του κβαντικού καταχωρητή στο τέλος του πέμπτου βήματος, πολλαπλασιάζουμε τον πίνακα που προκύπτει από το τανυστικό γινόμενο των πινάκων των πυλών (το έχουμε ήδη υπολογίσει στην (4.4)) επί τον πίνακα της κατάστασης του κβαντικού καταχωρητή που υπολογίστηκε στο αμέσως προηγούμενο βήμα:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle \quad (4.8)$$

Στο τέλος του 5ου βήματος η πιθανότητα να βρεθεί ο κβαντικός καταχωρητής στην κατάσταση $|10\rangle$ είναι ένα. Αυτό αναγράφεται στην πέμπτη στήλη του πίνακα του Σχήματος 4-2.

Όταν ο κβαντικός καταχωρητής αποτελείται από πολλά qubits και ο κβαντικός υπολογισμός περιλαμβάνει αρκετά βήματα, τότε είναι σχεδόν αδύνατο να κάνουμε τους υπολογισμούς με το χέρι. Ο συγγραφέας του βιβλίου αυτού έχει αναπτύξει έναν προσομοιωτή κβαντικού υπολογιστή που τον ονόμασε *QCS*, από τα αρχικά των λέξεων Quantum Computer Simulator (Karafyllidis, 2005). Ο προσομοιωτής αναπτύχθηκε για ερευνητικούς σκοπούς και χρησιμοποιήθηκε σε αρκετές ερευνητικές εργασίες, όμως μία σχετικά απλή μορφή του προσομοιωτή *QCS* μπορεί να χρησιμοποιηθεί και ως διδακτικό εργαλείο.

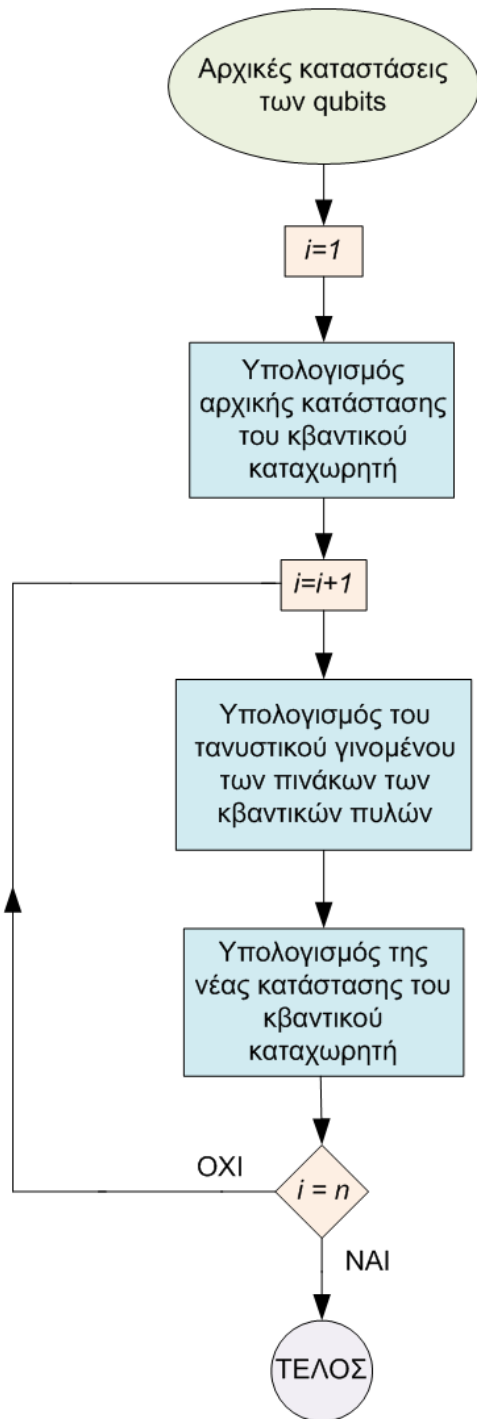
Μία απλή και εύχρηστη μορφή του προσομοιωτή *QCS* συνοδεύει αυτό το βιβλίο. Ο προσομοιωτής κβαντικού υπολογιστή *QCS* είναι διαθέσιμος στην ιστοσελίδα του κεφαλαίου 9 αυτού του βιβλίου, στον Ελληνικό Συσσωρευτή Ακαδημαϊκών Ηλεκτρονικών Βιβλίων (<http://repository.kallipos.gr>).

Στο 9^ο κεφάλαιο περιγράφεται ο *QCS* και δίνονται αναλυτικές οδηγίες για τη χρήση του, για να μπορέσει ο αναγνώστης να επαναλάβει τους κβαντικούς υπολογισμούς που περιγράφονται στο βιβλίο αυτό και να κάνει, εφόσον το θέλει, και δικούς του κβαντικούς υπολογισμούς. Η δομή και η λειτουργία του *QCS* περιγράφονται και στο: (Karafyllidis, 2005).

Στο κάτω μέρος του Σχήματος 4-2 δίνεται το αποτέλεσμα της προσομοίωσης του κβαντικού υπολογισμού με τον οποίο ασχοληθήκαμε. Η προσομοίωση έγινε με τον προσομοιωτή *QCS*. Πρόκειται για μία γραφική παράσταση του πίνακα του Σχήματος 4-2. Στον άξονα των x της γραφικής αυτής παράστασης δίνονται τα βήματα του υπολογισμού (Computation Steps). Στον άξονα των y δίνονται οι βασικές καταστάσεις των qubits που συμμετέχουν στον κβαντικό υπολογισμό, δηλαδή οι βασικές καταστάσεις του κβαντικού καταχωρητή (Karafyllidis, 2003). Οι βασικές καταστάσεις δίνονται σε δεκαδική μορφή (Decimal Number Representation). Οι πιθανότητες να βρεθεί ο κβαντικός καταχωρητής σε μία από τις βασικές καταστάσεις δίνονται εδώ όχι με αριθμούς, όπως στον πίνακα του Σχήματος 4-2, αλλά με τόνους του γκρι, όπου ο αριθμός 1 αντιστοιχεί στο μαύρο και ο αριθμός 0 στο άσπρο. Όλοι οι ενδιάμεσοι αριθμοί παριστάνονται με τόνους του γκρι. Για να διευκολυνθεί ο αναγνώστης, στο δεξιό μέρος του Σχήματος 4-2, όπου φαίνεται η προσομοίωση του κβαντικού υπολογισμού, υπάρχει μία στήλη όπου φαίνεται η αντιστοιχία των αριθμών που βρίσκονται μεταξύ του 0 και του 1 με τους τόνους του γκρι. Με τον τρόπο αυτό μπορούμε να έχουμε άμεση εποπτεία του κβαντικού υπολογισμού.

4.3 Η αρχή της κβαντικής υπολογιστικής

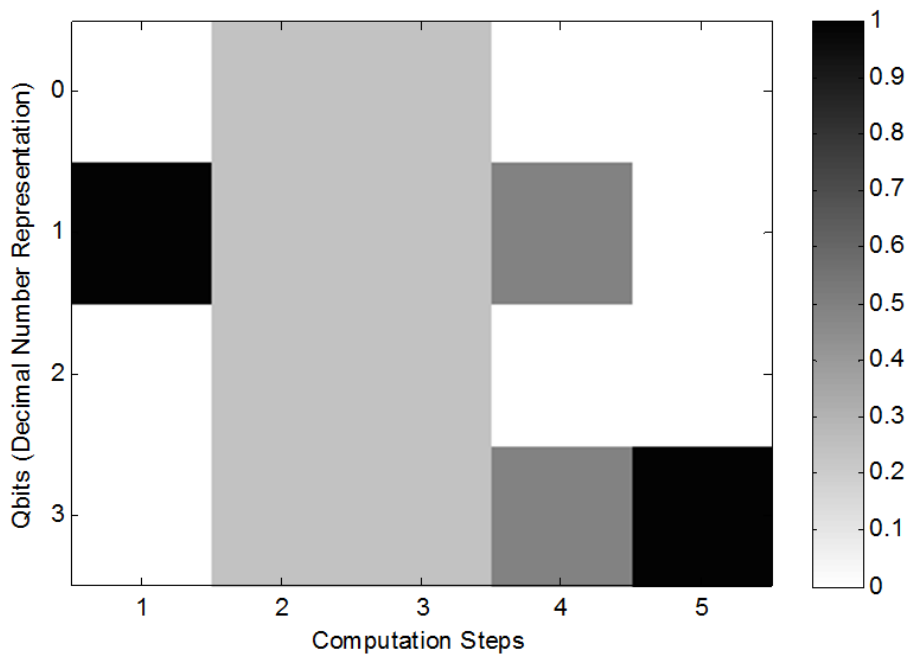
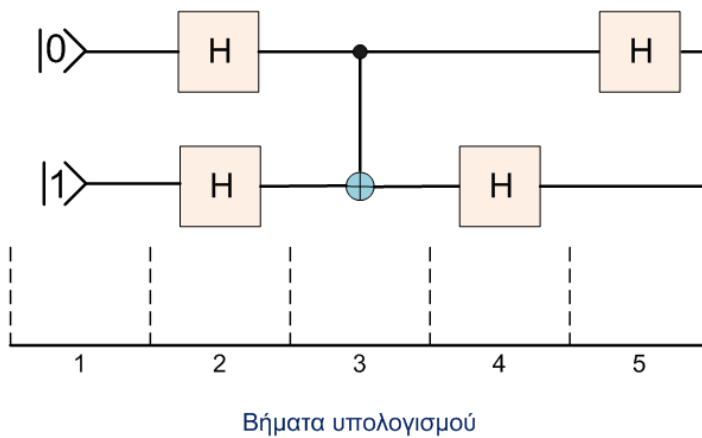
Όλοι σχεδόν οι κβαντικοί υπολογισμοί περιγράφονται από το κυκλωματικό μοντέλο και εκτελούνται με την ίδια διαδικασία που περιγράψαμε προηγουμένως. Στο Σχήμα 4-3 φαίνεται ένα διάγραμμα που περιγράφει τη διαδικασία αυτή η οποία αποτελεί και την αρχή της κβαντικής υπολογιστικής (Karafyllidis, 2003b). Συνοπτικά η διαδικασία είναι η εξής:



Σχήμα 4-3. Η αρχή της κβαντικής υπολογιστικής ως διάγραμμα ροής για την εκτέλεση των κβαντικών υπολογισμών. Με i συμβολίζεται ο αριθμός του βήματος και με n ο συνολικός αριθμός βημάτων του κβαντικού υπολογισμού.

1. Δίνεται η αρχική κατάσταση των qubits που αποτελούν τον κβαντικό καταχωρητή. Υπολογίζουμε το τανυστικό γινόμενο των πινάκων των καταστάσεων των qubits. Ο πίνακας που προκύπτει είναι η αρχική κατάσταση του κβαντικού καταχωρητή.
2. Υπολογίζουμε το τανυστικό γινόμενο των πινάκων που περιγράφουν τις κβαντικές πύλες οι οποίες δρουν στο επόμενο βήμα του κβαντικού υπολογισμού.
3. Πολλαπλασιάζουμε τον πίνακα που προκύπτει από το τανυστικό γινόμενο των πινάκων των κβαντικών πυλών με τον πίνακα της κατάστασης του κβαντικού καταχωρητή. Το αποτέλεσμα είναι ο πίνακας της νέας κατάστασης του κβαντικού καταχωρητή.
4. Επαναλαμβάνουμε τα 2 και 3 τόσες φορές όσα και τα βήματα του κβαντικού υπολογισμού.
5. Η τελική κατάσταση του κβαντικού καταχωρητή είναι το αποτέλεσμα του κβαντικού υπολογισμού.

Παρακάτω θα εκτελέσουμε έναν κβαντικό υπολογισμό ακολουθώντας τη διαδικασία που μόλις περιγράψαμε. Το κβαντικό κύκλωμα του κβαντικού υπολογισμού φαίνεται στο Σχήμα 4-4.



Σχήμα 4-4. Επάνω φαίνεται το κβαντικό κύκλωμα και κάτω το αποτέλεσμα της προσομοίωσης του κβαντικού υπολογισμού από τον Προσομοιωτή Κβαντικού Υπολογιστή QCS.

Η αρχική κατάσταση του κβαντικού καταχωρητή είναι $|01\rangle$ και η κατάστασή του στο πρώτο βήμα του κβαντικού υπολογισμού ($i=1$) δίνεται από:

$$|01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad (4.9)$$

Στο δεύτερο βήμα ($i=2$) υπολογίζουμε το τανυστικό γινόμενο των πινάκων των πυλών:

$$H \otimes H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix} \quad (4.10)$$

και τη νέα κατάσταση του κβαντικού καταχωρητή:

$$H \otimes H |01\rangle = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle \quad (4.11)$$

Στο τέλος του 2^{ου} βήματος όλες οι βασικές καταστάσεις έχουν την ίδια πιθανότητα, η οποία είναι ίση με 0,25. Ο αριθμός των βημάτων είναι πέντε ($n=5$) και αφού $i < n$, αυξάνουμε τον αριθμό βήματος κατά ένα ($i=3$) και επαναλαμβάνουμε.

Στο 3^ο βήμα δρα στον κβαντικό καταχωρητή μόνο η κβαντική πύλη *CNOT* και η νέα κατάσταση του κβαντικού καταχωρητή είναι:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix} = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \quad (4.12)$$

Όπως και στο τέλος του 2^{ου} βήματος, όλες οι βασικές καταστάσεις έχουν την ίδια πιθανότητα που είναι ίση με 0,25. Προσοχή όμως, σε κάποιες καταστάσεις τα πρόσημα (δηλαδή οι φάσεις) έχουν αλλάξει. Πάλι $i < n$, οπότε αυξάνουμε τον αριθμό βήματος κατά ένα ($i=4$) και επαναλαμβάνουμε.

Στο 4^ο βήμα δρουν στον κβαντικό καταχωρητή οι κβαντικές πύλες H και I . Υπολογίζουμε το τανυστικό γινόμενο των πινάκων των πυλών:

$$I \otimes H = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \quad (4.13)$$

και τη νέα κατάσταση του κβαντικού καταχωρητή:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle \quad (4.14)$$

Στο τέλος του 4^{ου} βήματος η πιθανότητα να βρεθεί ο κβαντικός καταχωρητής στην κατάσταση $|01\rangle$ είναι 0,5 και η πιθανότητα να βρεθεί στην κατάσταση $|11\rangle$ είναι 0,5. Αφού $i < n$, αυξάνουμε τον αριθμό βήματος κατά ένα ($i=5$) και επαναλαμβάνουμε.

Στο 5^ο βήμα δρουν στον κβαντικό καταχωρητή οι κβαντικές πύλες I και H , των οποίων το τανυστικό γινόμενο δίνεται από την (4.4). Υπολογίζουμε τη νέα κατάσταση του κβαντικού καταχωρητή:

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 0 \\ \frac{1}{\sqrt{2}} \\ 0 \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle \quad (4.15)$$

Στο τέλος του 5^{ου} βήματος ο κβαντικός καταχωρητής βρίσκεται σίγουρα στην κατάσταση $|11\rangle$. Τώρα έχουμε $i=n$, δηλαδή ο κβαντικός υπολογισμός έφτασε στο τέλος του. Στο κάτω μέρος του Σχήματος 4-4 φαίνεται όλος ο κβαντικός υπολογισμός ως αποτέλεσμα της προσομοίωσής του από τον Προσομοιωτή Κβαντικού Υπολογιστή QCS. Φαίνεται με μία ματιά ότι ο κβαντικός καταχωρητής βρισκόταν αρχικά στη βασική κατάσταση $|01\rangle$ και στο τέλος του κβαντικού υπολογισμού βρέθηκε στη βασική κατάσταση $|11\rangle$.

4.4 Η αρχή της κβαντικής υπολογιστικής και η εξίσωση του Schrödinger

Η αρχή της κβαντικής υπολογιστικής περιγράφει τη μεταβολή της κατάστασης των qubits και των κβαντικών καταχωρητών κατά τη διάρκεια των κβαντικών υπολογισμών, οι οποίοι αναπαριστώνται ως κβαντικά κυκλώματα (Beth & Leuchs, 2005). Στα κβαντικά κυκλώματα ο "άξονας των x" είναι ο χρόνος, δηλαδή τα κβαντικά κυκλώματα περιγράφουν τη χρονική αλληλουχία της δράσης των κβαντικών πυλών στα qubits και στους κβαντικούς καταχωρητές. Η αρχή της κβαντικής υπολογιστικής περιγράφεται από την εξίσωση του Schrödinger, όπως θα δούμε αμέσως παρακάτω.

Στο πρώτο κεφάλαιο του βιβλίου αυτού είχαμε γράψει την εξίσωση του Schrödinger στην μορφή της (1.39), η οποία επαναλαμβάνεται εδώ:

$$i\hbar \frac{\partial}{\partial t} \Psi(x,t) = H \Psi(x,t) \quad (4.16)$$

Η συνάρτηση κύματος $\Psi(x,t)$ περιγράφει την κατάσταση του κβαντικού συστήματος. Στο συμβολισμό του Dirac η συνάρτηση κύματος αντιστοιχεί στο διάνυσμα κατάστασης $|\Psi(x,t)\rangle$. Όπως είπαμε, οι κβαντικοί υπολογισμοί περιγράφουν τη χρονική μεταβολή της κατάστασης των qubits ή των κβαντικών καταχωρητών και για τον λόγο αυτό δεν θα λάβουμε υπόψη τη χωρική μεταβλητή "x" του διανύσματος κατάστασης, το οποίο θα γράψουμε ως: $|\Psi(t)\rangle$. Μετά από αυτό η (4.16) γίνεται:

$$i\hbar \frac{\partial}{\partial t} |\Psi(t)\rangle = H |\Psi(t)\rangle \quad (4.17)$$

Ας θυμηθούμε ότι:

$$\frac{\partial}{\partial t} e^{at} = a e^{at} \quad (4.18)$$

Θεωρούμε ότι ο κβαντικός υπολογισμός αρχίζει την χρονική στιγμή $t=0$, δηλαδή θεωρούμε ότι η αρχική κατάσταση των qubits ή των κβαντικών καταχωρητών είναι η $|\Psi(0)\rangle$. Με αυτή την αρχική συνθήκη η λύση της εξίσωσης του Schrödinger (4.17) είναι (Brylinski & Chen, 2002):

$$|\Psi(t)\rangle = e^{\frac{-iHt}{\hbar}} |\Psi(0)\rangle \quad (4.19)$$

Αντικαθιστούμε τον εκθετικό όρο που περιλαμβάνει τον τελεστή H με έναν νέο τελεστή, τον U ως εξής:

$$U(t) = e^{\frac{-iHt}{\hbar}} \quad (4.20)$$

Θα αναφέρουμε χωρίς απόδειξη ότι όταν δύο τελεστές συνδέονται με την εκθετική μορφή της (4.20) και ο τελεστής στον εκθέτη (ο H δηλαδή) είναι ερμιτιανός, τότε ο τελεστής U είναι ορθομοναδιαίος. Μετά από αυτό η (4.19) γράφεται:

$$|\Psi(t)\rangle = U(t) |\Psi(0)\rangle \quad (4.21)$$

Δηλαδή η δράση του ορθομοναδιαίου τελεστή U έχει ως αποτέλεσμα την περιστροφή στον χώρο Hilbert του διανύσματος των qubits ή των κβαντικών καταχωρητών, από την αρχική κατάσταση $|\Psi(0)\rangle$ στην τελική κατάσταση $|\Psi(t)\rangle$. Κατ' αναλογία με τους κλασικούς υπολογισμούς μπορούμε να πούμε ότι η $|\Psi(0)\rangle$ αντιστοιχεί με τα δεδομένα, ο τελεστής U με το κβαντικό κύκλωμα και η $|\Psi(t)\rangle$ με το αποτέλεσμα του κβαντικού υπολογισμού. Η διάρκεια του κβαντικού υπολογισμού είναι ίση με t . Η (4.21) μπορεί να αναλυθεί σε χρονικά βήματα:

$$|\Psi(n+1)\rangle = U(n+1) |\Psi(n)\rangle \quad (4.22)$$

Η $|\Psi(n)\rangle$ είναι η κατάσταση του κβαντικού καταχωρητή στο τέλος του χρονικού βήματος n του κβαντικού υπολογισμού. $U(n+1)$ είναι το τανυστικό γινόμενο των κβαντικών πυλών που δρουν στο $n+1$ χρονικό βήμα του κβαντικού υπολογισμού. Η $|\Psi(n+1)\rangle$ είναι η νέα κατάσταση του κβαντικού καταχωρητή στο τέλος του χρονικού βήματος $n+1$ του κβαντικού υπολογισμού. Η (4.22) αναπαριστά το διάγραμμα ροής του Σχήματος 4-3.

Η εξίσωση (4.22) που προήλθε από τη λύση της εξίσωσης του Schrödinger αποτελεί τη μαθηματική έκφραση της αρχής της κβαντικής υπολογιστικής.

4.5 Ο κβαντικός αλγόριθμος του Deutsch

Ο πρώτος κβαντικός αλγόριθμος, δηλαδή ένας αλγόριθμος που να μπορεί να τρέξει μόνο σε έναν κβαντικό υπολογιστή, αναπτύχθηκε από τον Deutsch (Deutsch, 1985). Στον αλγόριθμο αυτό χρησιμοποιείται η κβαντική παραλληλία, δηλαδή η υπέρθεση των βασικών καταστάσεων των qubits και φαίνεται για πρώτη φορά ότι ο κβαντικός υπολογιστής μπορεί να εκτελέσει υπολογισμούς που είναι αδύνατον να εκτελεστούν από έναν κλασικό υπολογιστή.

Το πρόβλημα που έθεσε ο Deutsch είναι το εξής: Δίνεται μία συνάρτηση $f(x)$ τέτοια ώστε:

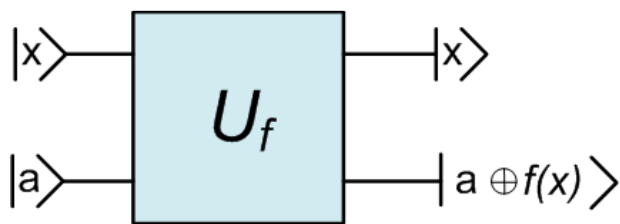
$$f(x) : \{0,1\} \rightarrow \{0,1\} \quad (4.23)$$

Δηλαδή η μεταβλητή x και η συνάρτηση $f(x)$ μπορούν να πάρουν μόνο τις τιμές 0 ή 1 . Για κάθε τέτοια συνάρτηση υπάρχουν δύο περιπτώσεις:

- α) $f(0) = f(1)$, οπότε η συνάρτηση ονομάζεται σταθερή, ή
- β) $f(0) \neq f(1)$, οπότε η συνάρτηση ονομάζεται ισορροπημένη.

Αν δοθεί λοιπόν μία τέτοια συνάρτηση, με έναν μόνο υπολογισμό της $f(x)$ να βρεθεί αν η συνάρτηση είναι σταθερή ή ισορροπημένη.

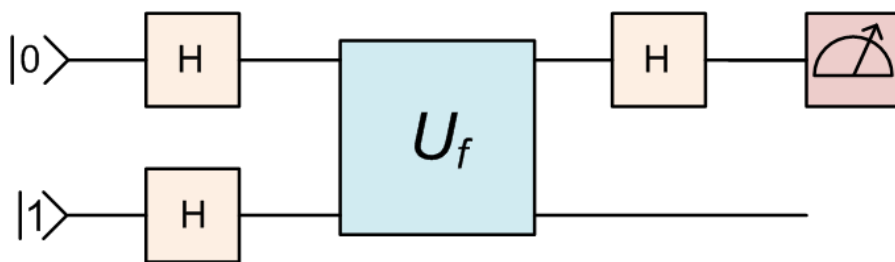
Αν χρησιμοποιήσουμε έναν κλασικό υπολογιστή θα πρέπει να υπολογίσουμε την τιμή $f(0)$, στη συνέχεια να υπολογίσουμε την τιμή $f(1)$ και να συγκρίνουμε τα αποτελέσματα. Αν είναι ίδια, τότε η συνάρτηση είναι σταθερή, αν είναι διαφορετικά, η συνάρτηση είναι ισορροπημένη. Δεν είναι δηλαδή δυνατόν να βρούμε τι είναι η συνάρτηση με έναν μόνο υπολογισμό. Αυτό όμως είναι δυνατό, αν χρησιμοποιήσουμε έναν κβαντικό υπολογιστή.



Σχήμα 4-5. Το κβαντικό αυτό κύκλωμα υπολογίζει το άθροισμα με βάση το 2 (mod2) του πρώτου qubit με την συνάρτηση $f(x)$, όπου x είναι το δεύτερο qubit.

Πριν περιγράψουμε τον αλγόριθμο του Deutsch, ας δούμε το κβαντικό κύκλωμα του Σχήματος 4-5. Το κύκλωμα αυτό αποτελείται από έναν κβαντικό καταχωρητή των δύο qubits, όπου το πρώτο είναι το $|a\rangle$ και το δεύτερο το $|x\rangle$, και από ένα συνδυασμό κβαντικών πυλών, που παριστάνεται από τον τελεστή (ορθογώνιο στο Σχήμα 4-5) U_f . Για κάθε διαφορετική συνάρτηση $f(x)$ χρειάζεται και ένας διαφορετικός συνδυασμός κβαντικών πυλών. Ο συνδυασμός των κβαντικών πυλών U_f δρα στα δύο qubits και αφήνει το δεύτερο αμετάβλητο, ενώ φέρνει το πρώτο στην κατάσταση που αντιστοιχεί με το άθροισμα με βάση το 2 (mod2) του πρώτου qubit $|a\rangle$ με τη συνάρτηση $f(x)$, όπου x είναι το δεύτερο qubit. Δηλαδή, υπολογίζεται η $f(x)$ και το άθροισμα της με το $|a\rangle \text{ mod } 2$. Το σύμβολο \oplus σημαίνει πρόσθεση με βάση το 2 (mod 2), δηλαδή $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$ και $1 \oplus 1 = 0$. Το κβαντικό κύκλωμα του Σχήματος 4-5 δίνεται από την:

$$U_f |x\rangle|a\rangle = |x\rangle|a \oplus f(x)\rangle \tag{4.24}$$



Σχήμα 4-6. Το κβαντικό κύκλωμα του αλγορίθμου του Deutsch.

Ο αλγόριθμος του Deutsch είναι και αυτός ένας κβαντικός υπολογισμός και περιγράφεται από το κβαντικό κύκλωμα του Σχήματος 4-6. Η αρχική κατάσταση του πρώτου qubit είναι $|1\rangle$ και του δεύτερου $|0\rangle$. Στο πρώτο βήμα του αλγορίθμου (δηλαδή του κβαντικού υπολογισμού) του Deutsch η κατάσταση του κβαντικού καταχωρητή είναι $|01\rangle$. Στο δεύτερο βήμα δρουν δύο κβαντικές πύλες H . Στο τρίτο δρα ο συνδυασμός κβαντικών πυλών U_f που περιγράψαμε προηγουμένως και στο τέταρτο δρα η κβαντική πύλη H στο δεύτερο qubit. Στο τέλος του τέταρτου βήματος μετράται η κατάσταση του δεύτερου qubit. Αν το qubit αυτό βρεθεί στην κατάσταση $|0\rangle$, τότε η συνάρτηση $f(x)$ είναι σταθερή και αν βρεθεί στην κατάσταση $|1\rangle$, τότε η $f(x)$ είναι ισοροπημένη. Ας δούμε πώς γίνεται αυτό.

Στο πρώτο βήμα η κατάσταση του κβαντικού καταχωρητή, που θα την ονομάσουμε $|q_1\rangle$ είναι $|01\rangle$. Γνωρίζουμε ότι η κατάσταση αυτή περιγράφεται από τον πίνακα:

$$|q_1\rangle = |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad (4.25)$$

Στο δεύτερο βήμα δρουν δύο κβαντικές πύλες H . Το ταυστικό γινόμενο των δύο πυλών δίνεται από την (4.10) και η νέα κατάσταση του κβαντικού καταχωρητή, η $|q_2\rangle$, είναι:

$$|q_2\rangle = H \otimes H |q_1\rangle = H \otimes H |01\rangle = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} \quad (4.26)$$

$$= \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle = \frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle)$$

Θυμηθείτε ότι $|pq\rangle = |p\rangle|q\rangle$.

Στο τρίτο βήμα δρα στον κβαντικό καταχωρητή ο συνδυασμός κβαντικών πυλών U_f . Αν λάβουμε υπόψη την (4.24), η νέα κατάσταση του κβαντικού καταχωρητή, $|q_3\rangle$, είναι:

$$\begin{aligned}
|q_3\rangle &= U_f |q_2\rangle = U_f \frac{1}{2} (|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle) = \\
&= \frac{1}{2} (U_f |0\rangle|0\rangle - U_f |0\rangle|1\rangle + U_f |1\rangle|0\rangle - U_f |1\rangle|1\rangle) \\
&= \frac{1}{2} (|0\rangle|0 \oplus f(0)\rangle - |0\rangle|1 \oplus f(0)\rangle + |1\rangle|0 \oplus f(1)\rangle - |1\rangle|1 \oplus f(1)\rangle)
\end{aligned} \tag{4.27}$$

Πρέπει εδώ να δούμε και τις τέσσερις δυνατές περιπτώσεις τιμών της $f(x)$.

Περίπτωση 1^η: $f(0)=0$ και $f(1)=0$, τότε η (4.27) γίνεται:

$$|q_3\rangle = \frac{1}{2} (|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle) \tag{4.28 α}$$

Περίπτωση 2^η: $f(0)=1$ και $f(1)=1$, τότε η (4.27) γίνεται:

$$\begin{aligned}
|q_3\rangle &= \frac{1}{2} (|0\rangle|1\rangle - |0\rangle|0\rangle + |1\rangle|1\rangle - |1\rangle|0\rangle) \\
&= \frac{1}{2} (-|0\rangle|0\rangle + |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle)
\end{aligned} \tag{4.28 β}$$

Περίπτωση 3^η: $f(0)=0$ και $f(1)=1$, τότε η (4.27) γίνεται

$$\begin{aligned}
|q_3\rangle &= \frac{1}{2} (|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|1\rangle - |1\rangle|0\rangle) \\
&= \frac{1}{2} (|0\rangle|0\rangle - |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle)
\end{aligned} \tag{4.28 γ}$$

Περίπτωση 4^η: $f(0)=1$ και $f(1)=0$, τότε η (4.27) γίνεται

$$\begin{aligned}
|q_3\rangle &= \frac{1}{2} (|0\rangle|1\rangle - |0\rangle|0\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle) \\
&= \frac{1}{2} (-|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle)
\end{aligned} \tag{4.28 δ}$$

Οι δύο πρώτες περιπτώσεις αντιστοιχούν σε σταθερή συνάρτηση και οι δύο τελευταίες σε ισορροπημένη. Προσέξτε ότι στις (4.28) αλλάζουν μόνο τα πρόσημα (δηλαδή οι φάσεις) των τεσσάρων βασικών καταστάσεων των οποίων η υπέρθεση δίνει την κατάσταση $|q_3\rangle$.

Στο τέταρτο βήμα δρουν οι κβαντικές πύλες I και H . Το ταυνοστικό τους γινόμενο δίνεται από την (4.4). Θα υπολογίσουμε την τελική κατάσταση του κβαντικού καταχωρητή $|q_4\rangle$ για την πρώτη από τις προηγούμενες περιπτώσεις, δηλαδή την (4.28 α):

$$\begin{aligned}
|q_4\rangle &= H \otimes I |q_3\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \\ -\frac{1}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|01\rangle \\
&= \frac{1}{\sqrt{2}}|0\rangle|0\rangle - \frac{1}{\sqrt{2}}|0\rangle|1\rangle = |0\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)
\end{aligned}
\tag{4.29}$$

Δηλαδή, στην περίπτωση που $f(0) = 0$ και $f(1) = 0$ το πρώτο qubit βρίσκεται σε υπέρθεση βασικών καταστάσεων, ενώ το δεύτερο στη βασική κατάσταση $|0\rangle$. Με τον ίδιο τρόπο υπολογίζουμε την $|q_4\rangle$ και για τις άλλες τρεις περιπτώσεις. Όλα τα αποτελέσματα φαίνονται στον Πίνακα 4-1.

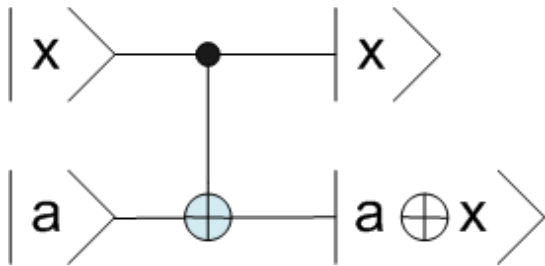
Η συνάρτηση $f(x)$ είναι:	Περίπτωση	Τελική κατάσταση $ q_4\rangle$
Σταθερή	$f(0)=0$ και $f(1)=0$	$ 0\rangle \left(\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right)$
	$f(0)=1$ και $f(1)=1$	$ 0\rangle \left(\frac{ 1\rangle - 0\rangle}{\sqrt{2}} \right)$
Ισορροπημένη	$f(0)=0$ και $f(1)=1$	$ 1\rangle \left(\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right)$
	$f(0)=1$ και $f(1)=0$	$ 1\rangle \left(\frac{ 1\rangle - 0\rangle}{\sqrt{2}} \right)$

Πίνακας 4-1 Αποτελέσματα του κβαντικού αλγορίθμου του Deutsch για όλες τις περιπτώσεις της συνάρτησης $f(x)$.

Όπως φαίνεται από τον πίνακα, όταν η συνάρτηση $f(x)$ είναι σταθερή, τότε το δεύτερο qubit βρίσκεται πάντα στην κατάσταση $|0\rangle$. Όταν όμως είναι ισορροπημένη, το δεύτερο qubit βρίσκεται πάντα στην κατάσταση $|1\rangle$. Δεν χρειάζεται να μετρήσουμε την κατάσταση του πρώτου qubit, η οποία δεν μας ενδιαφέρει, αλλά μόνο του δεύτερου, όπως φαίνεται στο Σχήμα 4-6. Με τον αλγόριθμο του Deutsch, χρησιμοποιώντας δηλαδή την κβαντική παραλληλία, μπορούμε να βρούμε τι είναι η $f(x)$ με ένα μόνο υπολογισμό της τιμής της. Αυτό είναι αδύνατον να επιτευχθεί με τη χρήση κλασικών υπολογιστών.

Παράδειγμα 4.1

Όπως προκύπτει από τον Πίνακα 3-5, όταν η κβαντική πύλη *CNOT* δρα σε έναν κβαντικό καταχωρητή που αποτελείται από δύο qubits, δεν επηρεάζει την κατάσταση του δεύτερου, αλλά μεταβάλλει την κατάσταση του πρώτου, αν το δεύτερο βρίσκεται στην κατάσταση $|1\rangle$. Με λίγη προσοχή μπορούμε να δούμε ότι μετά τη δράση της *CNOT*, το πρώτο qubit είναι το άθροισμα με βάση το 2 των αρχικών καταστάσεων των δύο qubits. Χρησιμοποιώντας το συμβολισμό του Σχήματος 4-5, η *CNOT* γίνεται:



Αν θεωρήσουμε ότι ο συνδυασμός των κβαντικών πυλών U_f περιλαμβάνει μόνο τη *CNOT*, τότε η συνάρτηση $f(x)$ είναι η: $f(x) = x$, δηλαδή μία ισοροπημένη συνάρτηση. Για τη συνάρτηση αυτή $f(0) = 0$ και $f(1) = 1$, οπότε έχουμε την περίπτωση της (4.28 γ), δηλαδή την τρίτη γραμμή του πίνακα. Οπότε, μετά την εκτέλεση του αλγορίθμου, το πρώτο qubit θα βρεθεί στην κατάσταση $|1\rangle$ και ο κβαντικός καταχωρητής στην κατάσταση:

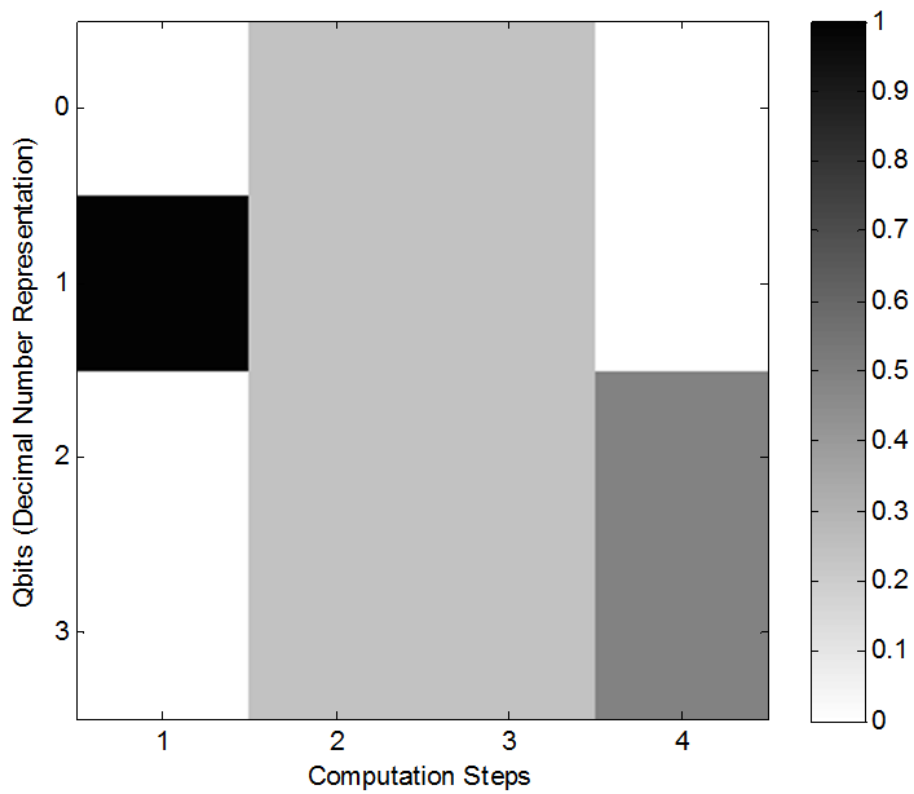
$$|q_4\rangle = |1\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = \frac{1}{\sqrt{2}} |1\rangle |0\rangle - \frac{1}{\sqrt{2}} |1\rangle |1\rangle = \frac{1}{\sqrt{2}} |10\rangle - \frac{1}{\sqrt{2}} |11\rangle$$

Ας δούμε αν είναι έτσι.

Τα τρία πρώτα βήματα του αλγορίθμου του Deutsch με την *CNOT* στη θέση της U_f ταυτίζονται με τα τρία πρώτα βήματα του κβαντικού υπολογισμού του Σχήματος 4-4. Μετά το τέλος του τρίτου βήματος η κατάσταση του κβαντικού καταχωρητή δίνεται από την (4.12) που ταυτίζεται με την (4.28 γ). Στο τέταρτο βήμα του αλγορίθμου δρουν οι I και H , που το ταυστικό τους γινόμενο δίνεται από την (4.4). Στο τέλος του τετάρτου βήματος η κατάσταση του κβαντικού καταχωρητή θα είναι:

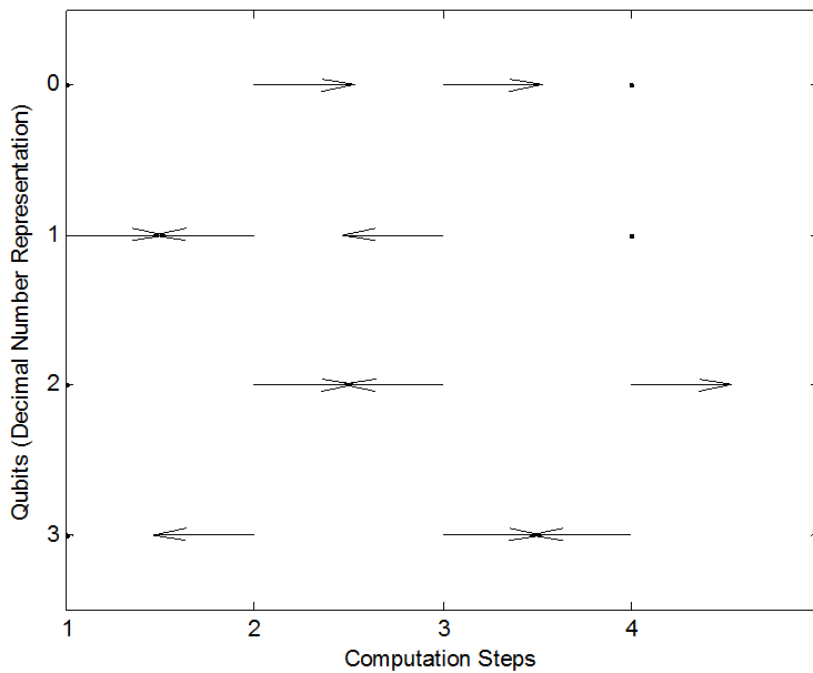
$$|q_4\rangle = H \otimes I |q_3\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{2} \\ -\frac{1}{2} \\ -\frac{1}{2} \\ \frac{1}{2} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} |10\rangle - \frac{1}{\sqrt{2}} |11\rangle$$

Ας δούμε και την εκτέλεση του αλγορίθμου αυτού του από τον *QCS*:



Ο υπολογισμός ξεκινά από την κατάσταση $|01\rangle$ που αντιστοιχεί στον δεκαδικό 1. Ο υπολογισμός τελειώνει με πιθανότητα 0.5 να μετρηθεί κάθε μια από τις καταστάσεις $|10\rangle$ και $|11\rangle$ που αντιστοιχούν στους δεκαδικούς 2 και 3.

Οι γωνίες των φάσεων των καταστάσεων κατά την εξέλιξη του κβαντικού υπολογισμού δίνονται στην παρακάτω έξοδο του QCS:



Τα οριζόντια, στραμμένα προς τα δεξιά, βέλη αντιστοιχούν σε μηδενική γωνία φάσης. Στο τρίτο βήμα οι καταστάσεις 0 και 3 (δεκαδικό) έχουν φάση μηδέν. Τα βέλη είναι σε γωνία μηδέν και τα πρόσημα των πλατών πιθανότητας των δύο αυτών καταστάσεων είναι "+". Στο ίδιο βήμα, οι καταστάσεις 1 και 2 (δεκαδικό) έχουν φάση ίση με " π ". Τα βέλη είναι σε γωνία " π " και τα πρόσημα των πλατών πιθανότητας των δύο αυτών καταστάσεων είναι "-". ♦

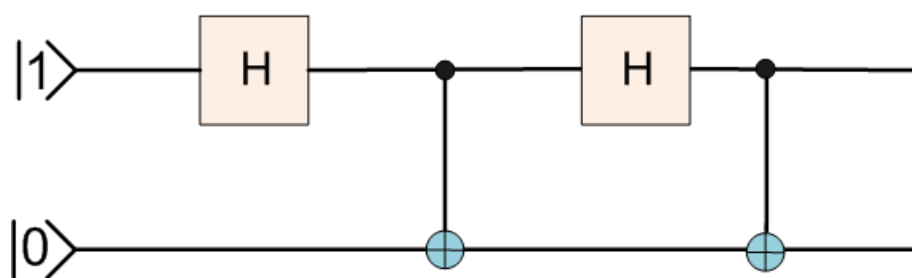
Βιβλιογραφία

- Beth T., & Leuchs G., *Quantum information processing*, Wiley-VCH, 2005.
- Brylinski R. K., & Chen C., *Mathematics of quantum computation*, Chapman & Hall / CRC, 2002.
- Deutsch D., Quantum theory, the Church-Turing Principle and the Universal Quantum Computer, *Proceedings of the Royal Society London A*, vol. 400, pp. 97-117, 1985.
- Karafyllidis G. I., Visualization of the Quantum Fourier Transform using a Quantum Computer Simulator, *Quantum Information Processing*, vol. 2, pp. 271-288, 2003.
- Karafyllidis G. I., Cellular Quantum Computer Architecture, *Physics Letters A*, vol 320, pp. 35-38, 2003 b.
- Karafyllidis G. I. "Quantum Computer Simulator based on the Circuit Model of Quantum Computation, *IEEE Transactions on Circuits and Systems I*, vol. 52, pp. 1590-1596, 2005.
- Milburn G. J., *The Feynman processor*, Perseus Books, 1998.
- Nielsen M. A., & Chuang I. L., *Quantum computation and quantum information*, Cambridge University Press, 2000.

Ασκήσεις

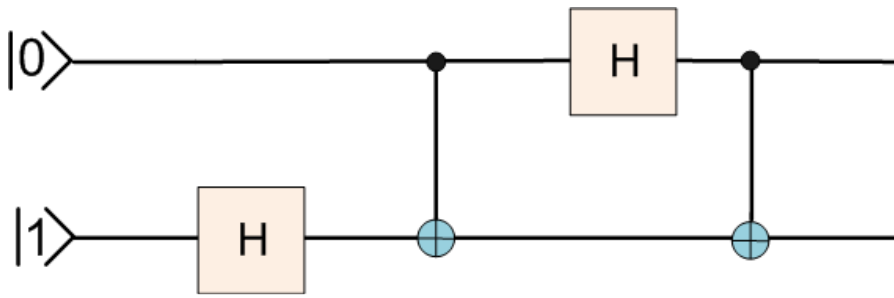
Άσκηση 4.1

Να κάνετε τον παρακάτω κβαντικό υπολογισμό:



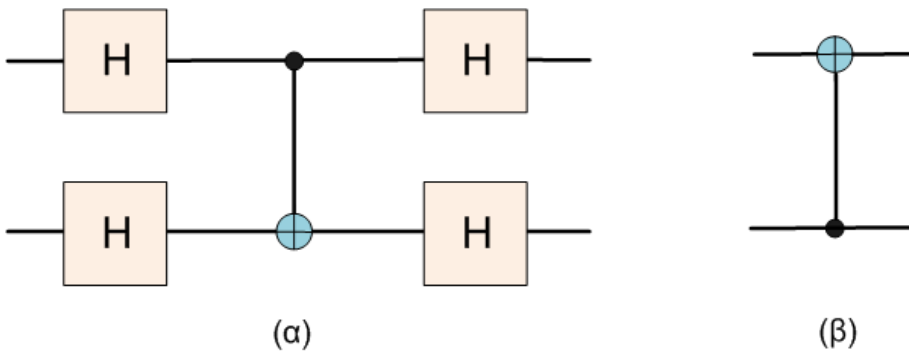
Άσκηση 4.2

Να κάνετε τον παρακάτω κβαντικό υπολογισμό:



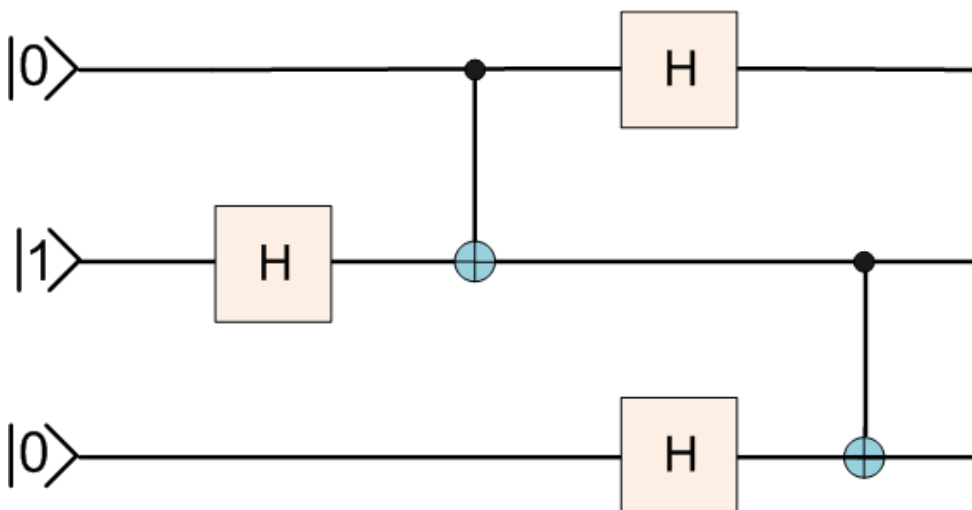
Άσκηση 4.3

Να αποδείξετε ότι οι κβαντικοί υπολογισμοί (α) και (β) είναι ισοδύναμοι. Δηλαδή όταν οι αντίστοιχες κβαντικές πύλες δρουν στον ίδιο κβαντικό καταχωρητή, μεταβάλλουν την κατάσταση του με τον ίδιο τρόπο.



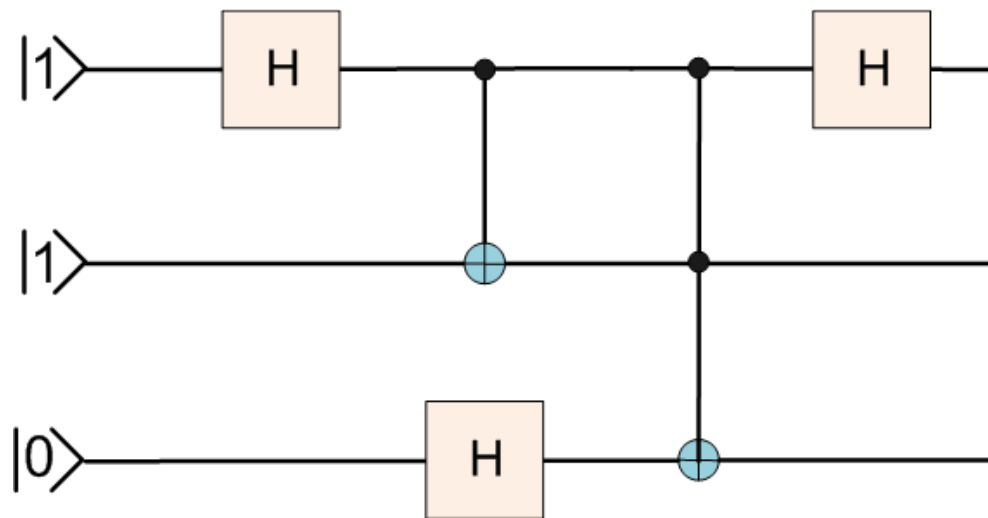
Άσκηση 4.4

Να κάνετε τον παρακάτω κβαντικό υπολογισμό:



Άσκηση 4.5

Να κάνετε τον παρακάτω κβαντικό υπολογισμό:



5. Κβαντική Διερεύνηση - Κβαντικός αλγόριθμος του Grover

Σύνοψη

Στο κεφάλαιο αυτό παρουσιάζεται ο αλγόριθμος του Grover για τη διερεύνηση μη δομημένων βάσεων δεδομένων. Περιγράφονται οι τελεστές και το κβαντικό κύκλωμα του κβαντικού αλγορίθμου του Grover. Δίνονται δύο ερμηνείες του κβαντικού αυτού αλγορίθμου και δύο παραδείγματα εφαρμογής του.

Προαπαιτούμενη γνώση

Γραμμική άλγεβρα, το πρώτο, δεύτερο και τρίτο κεφάλαιο αυτού του βιβλίου.

5.1 Διερεύνηση μη δομημένων βάσεων δεδομένων

Όπως γνωρίζουμε, ένας έντυπος τηλεφωνικός κατάλογος περιέχει ένα μεγάλο αριθμό ονομάτων, σε καθ' ένα από τα οποία αντιστοιχεί ένας αριθμός τηλεφώνου. Στους τηλεφωνικούς καταλόγους τα ονόματα είναι ταξινομημένα κατά αλφαβητική σειρά και είναι πολύ εύκολο για έναν άνθρωπο ή για έναν κλασικό υπολογιστή να βρει τον αριθμό τηλεφώνου που αντιστοιχεί σε κάποιο όνομα. Οι τηλεφωνικοί κατάλογοι είναι δηλαδή δομημένες βάσεις δεδομένων όσον αφορά στα ονόματα.

Ας δούμε τώρα το αντίστροφο πρόβλημα. Μας δίνουν έναν έντυπο τηλεφωνικό κατάλογο που περιέχει N ονόματα ταξινομημένα σε αλφαβητική σειρά, σε καθένα από τα οποία αντιστοιχεί ένας αριθμός τηλεφώνου. Μας δίνουν επίσης έναν αριθμό τηλεφώνου. Εμείς πρέπει να βρούμε στον κατάλογο το όνομα στο οποίο αντιστοιχεί ο αριθμός αυτός. Το πρόβλημα αυτό είναι δύσκολο, διότι οι αριθμοί στον τηλεφωνικό κατάλογο ακολουθούν τη σειρά των ονομάτων, δηλαδή ο τηλεφωνικός κατάλογος είναι μια μη δομημένη βάση δεδομένων όσον αφορά στους αριθμούς τηλεφώνων.

Ο μόνος τρόπος να ερευνηθεί ένας άνθρωπος ή ένας κλασικός υπολογιστής μία μη δομημένη βάση δεδομένων για να βρει ένα στοιχείο της είναι να προσπαθεί συνεχώς στην τύχη μέχρι να το βρει. Αν η μη δομημένη βάση δεδομένων περιέχει N στοιχεία και είμαστε τυχεροί, θα βρούμε το στοιχείο που ψάχνουμε την πρώτη φορά και αν είμαστε άτυχοι θα το βρούμε μετά από N προσπάθειες. Γενικά μπορούμε να πούμε ότι για να βρούμε ένα στοιχείο σε μία μη δομημένη βάση δεδομένων με N στοιχεία, πρέπει να την ερευνήσουμε $N/2$ φορές.

Όμως, ο Lov Grover με ένα άρθρο του με τίτλο «Η κβαντική μηχανική μπορεί να μας βοηθήσει να βρούμε μια βελόνα στ' άχυρα» απέδειξε ότι αν χρησιμοποιήσουμε έναν κβαντικό υπολογιστή μπορούμε να βρούμε ένα στοιχείο σε μία μη δομημένη βάση δεδομένων αν την ερευνήσουμε μόνο \sqrt{N} φορές περίπου (Grover 1997). Αυτή είναι μία σημαντική βελτίωση, διότι για να βρει ένας κλασικός υπολογιστής ένα στοιχείο σε μια μη δομημένη βάση δεδομένων που περιέχει 1.000.000 στοιχεία, πρέπει να την ερευνήσει κατά μέσο όρο 500.000 φορές, ενώ ένας κβαντικός υπολογιστής πρέπει να την ερευνήσει μόνο 1.000 φορές. Η μέθοδος με την οποία ένας κβαντικός υπολογιστής ερευνά μία μη δομημένη βάση δεδομένων ονομάζεται κβαντικός αλγόριθμος του Grover και αποτελεί το αντικείμενο του κεφαλαίου αυτού.

5.2 Ο κβαντικός αλγόριθμος του Grover

Υποθέστε ότι θέλουμε να ερευνήσουμε μία μη δομημένη βάση δεδομένων που περιέχει N στοιχεία. Κάθε στοιχείο της βάσης έχει αριθμηθεί με έναν αριθμό από το 0 έως το $N-1$. Υποθέστε επίσης ότι έχουμε στη διάθεσή μας ένα σύστημα το οποίο μπορεί να αναγνωρίσει αν κάποιο στοιχείο είναι αυτό που ζητάμε ή όχι. Υποθέστε δηλαδή ότι ερευνάτε εσείς μία μη δομημένη βάση δεδομένων και συγκεκριμένα έναν τηλεφωνικό κατάλογο. Έχετε έναν βοηθό ο οποίος ερευνά τον τηλεφωνικό κατάλογο, βρίσκει αριθμούς και σας τους δείχνει. Εσείς βλέπετε τον αριθμό και λέτε αν είναι αυτός που ψάχνετε ή όχι. Αυτό ακριβώς κάνει και το σύστημα. Του παρουσιάζετε έναν αριθμό, αυτό επεξεργάζεται τον αριθμό και σας λέει αν είναι αυτός που ψάχνετε ή όχι. Το σύστημα αυτό σε έναν κλασικό υπολογιστή μπορεί να είναι ένας καταχωρητής όπου έχουμε αποθηκεύσει τον αριθμό που ψάχνουμε να βρούμε και ένα κύκλωμα λογικών πυλών, που συγκρίνει κάθε αριθμό που έρχεται στην είσοδο με τον αποθηκευμένο αριθμό. Το σύστημα αυτό, που το θεωρούμε ως ένα μαύρο κουτί, ονομάζεται

στη διεθνή βιβλιογραφία *oracle*. Η λέξη αυτή μπορεί να αποδοθεί ως *μάντης* ή ως *κάποιος που ξέρει πολλά*. Νομίζω ότι είναι καλύτερο να χρησιμοποιήσουμε τον όρο *oracle*.

Ας περιγράψουμε τώρα το πρόβλημα της έρευνας μίας μη δομημένης βάσης δεδομένων από έναν κλασικό υπολογιστή με έναν απλό μαθηματικό τρόπο (Grover 1996). Θεωρούμε ότι έχουμε N στοιχεία τα οποία αποτελούν τη βάση και ότι έχουμε αντιστοιχίσει σε κάθε στοιχείο έναν αριθμό από 0 έως $N-1$. Το στοιχείο που αντιστοιχεί στον αριθμό k συμβολίζεται με x_k . Το oracle είναι μία συνάρτηση $f(\cdot)$ η οποία παίρνει μόνο τις τιμές 0 και 1 . Αν το στοιχείο που ψάχνουμε είναι το x_i , τότε:

$$f(x) = \begin{cases} 1 & \text{αν } x = x_i \\ 0 & \text{αν } x \neq x_i \end{cases} \quad (5.1)$$

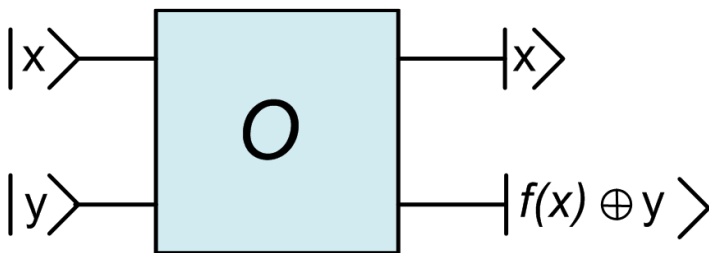
Δηλαδή, παρουσιάζουμε ένα στοιχείο στο oracle και αν είναι αυτό που ψάχνουμε τότε το oracle αποκρίνεται με 1 , αν όχι με 0 .

Ας δούμε τώρα το πρόβλημα της έρευνας μίας μη δομημένης βάσης δεδομένων με έναν κβαντικό υπολογιστή. Θεωρούμε ότι η βάση περιέχει N στοιχεία και χωρίς περιορισμό της γενικότητας μπορούμε να πούμε ότι:

$$N = 2^n - 1, \quad n = 1, 2, 3, \dots \quad (5.2)$$

Δηλαδή θέλουμε το πλήθος των στοιχείων της βάσης να μπορεί να γραφεί όπως στην (5.2). Αν έχουμε λιγότερα στοιχεία, μπορούμε να προσθέσουμε εμείς όσα χρειάζεται για να φτάσουμε στον επιθυμητό αριθμό (Kwiat, 2000).

Αντιστοιχίζουμε κάθε ένα από τα στοιχεία με μία από τις βασικές καταστάσεις ενός κβαντικού καταχωρητή που περιλαμβάνει n qubits. Δηλαδή, το στοιχείο που αντιστοιχεί στη βασική κατάσταση $|00\dots 0101\rangle$ που στη δεκαδική αναπαράσταση είναι η $|5\rangle$ συμβολίζεται με $|x_5\rangle$. Το κβαντικό oracle, δηλαδή το σύστημα που διακρίνει αν ένα στοιχείο είναι αυτό που ψάχνουμε ή όχι, είναι το κβαντικό κύκλωμα που συμβολίζεται με O και φαίνεται στο Σχήμα 5-1.



Σχήμα 5-1. Το κβαντικό oracle.

Δεν χρειάζεται να γνωρίζουμε τις κβαντικές πύλες από τις οποίες αποτελείται το κβαντικό oracle. Αυτό που χρειάζεται να γνωρίζουμε είναι η δράση του στον κβαντικό καταχωρητή. Αν δηλαδή το κβαντικό oracle δράσει στον κβαντικό καταχωρητή που βρίσκεται στην κατάσταση $|xy\rangle$ τότε:

$$|xy\rangle = |x\rangle |y\rangle \xrightarrow{O} |x\rangle |f(x) \oplus y\rangle \quad (5.3)$$

όπου, με \oplus συμβολίζεται η πρόσθεση με βάση το 2 (mod2) (θυμηθείτε ότι $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$ και $1 \oplus 1 = 0$). Το qubit $|y\rangle$ ονομάζεται qubit του oracle. Όπως και στο κλασικό oracle, η $f(x)$ παίρνει τιμή $|1\rangle$ αν το x είναι το στοιχείο που ψάχνουμε, αλλιώς παίρνει τιμή $|0\rangle$.

Ας δούμε καλύτερα τη δράση του κβαντικού oracle στη διαδικασία της έρευνας μίας μη δομημένης βάσης δεδομένων. Το qubit του oracle τίθεται στη βασική κατάσταση $|1\rangle$ και στη συνέχεια δρα σ' αυτό μία κβαντική πύλη H . Μέχρι τώρα περιγράφαμε τα κβαντικά κυκλώματα με πίνακες που αντιπροσωπεύουν καταστάσεις των καταχωρητών και κβαντικές πύλες. Εδώ όμως δεν θα μπορέσουμε να χρησιμοποιήσουμε τον ίδιο τρόπο, γιατί οι πίνακες είναι μεγάλοι για να χωρέσουν στις σελίδες του βιβλίου. Αντί για τους πίνακες θα χρησιμοποιούμε τα διανύσματα bra και ket και τα σύμβολα των κβαντικών πυλών. Για παράδειγμα, η δράση της H στο $|1\rangle$ γράφεται:

$$|1\rangle \xrightarrow{H} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (5.4)$$

Το $|x\rangle$ συμβολίζει μία βασική κατάσταση του κβαντικού καταχωρητή, κάθε βασική κατάσταση του οποίου αντιστοιχεί σε ένα στοιχείο της μη δομημένης βάσης δεδομένων. Δηλαδή η $|x\rangle$ αντιστοιχεί στο τυχαίο στοιχείο της βάσης. Το κβαντικό oracle δρα στο qubit του, που βρίσκεται στην κατάσταση που δίνεται από την (5.4), και στην $|x\rangle$. Το αποτέλεσμα της δράσης του δίνεται από:

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{o} |x\rangle \left| f(x) \oplus \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\rangle \quad (5.5)$$

Η $|x\rangle$ μπορεί να αντιστοιχεί στο στοιχείο που ψάχνουμε, μπορεί και να μην αντιστοιχεί. Ας δούμε πρώτα την περίπτωση που δεν αντιστοιχεί. Τότε η $f(x)$ παίρνει τιμή $|0\rangle$ και η (5.5) γίνεται:

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{o} |x\rangle \left(|0\rangle \oplus \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |x\rangle \left(\frac{|0\rangle \oplus |0\rangle - |0\rangle \oplus |1\rangle}{\sqrt{2}} \right) = |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (5.6)$$

Ας δούμε τώρα την περίπτωση που η $|x\rangle$ αντιστοιχεί στο στοιχείο που ψάχνουμε. Τότε η $f(x)$ παίρνει τιμή $|1\rangle$ και η (5.5) γίνεται:

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{o} |x\rangle \left(|1\rangle \oplus \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) = |x\rangle \left(\frac{|1\rangle \oplus |0\rangle - |1\rangle \oplus |1\rangle}{\sqrt{2}} \right) = |x\rangle \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}} \right) = -|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \quad (5.7)$$

Από της (5.6) και (5.7) έχουμε:

$$|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \xrightarrow{o} \begin{cases} |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \text{αν η } |x\rangle \text{ δεν αντιστοιχεί στο στοιχείο που ψάχνουμε} \\ -|x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) & \text{αν η } |x\rangle \text{ αντιστοιχεί στο στοιχείο που ψάχνουμε} \end{cases} \quad (5.8)$$

Δεδομένου ότι το qubit του κβαντικού oracle σε καμία περίπτωση δεν μεταβάλλεται, μπορούμε να το απαλείψουμε από την (5.8) και να τη γράψουμε ως εξής:

$$|x\rangle \xrightarrow{O} \begin{cases} |x\rangle & \text{αν η } |x\rangle \text{ δεν αντιστοιχεί στο στοιχείο που ψάχνουμε} \\ -|x\rangle & \text{αν η } |x\rangle \text{ αντιστοιχεί στο στοιχείο που ψάχνουμε} \end{cases} \quad (5.9)$$

Η (5.9) μπορεί να γραφεί και πιο συνοπτικά:

$$|x\rangle \xrightarrow{O} (-1)^{f(x)} |x\rangle \quad (5.10)$$

με την $f(x)$ να παίρνει τιμές 0 ή 1. Μην σας προβληματίζει το γεγονός ότι η $f(x)$ βρίσκεται στον εκθέτη. Αν $f(x) = 0$ τότε:

$$|x\rangle \xrightarrow{O} (-1)^0 |x\rangle = |x\rangle \quad (5.11)$$

και αν $f(x) = 1$ τότε:

$$|x\rangle \xrightarrow{O} (-1)^1 |x\rangle = -|x\rangle \quad (5.12)$$

Τι κάνει λοιπόν το κβαντικό oracle; Το κβαντικό oracle δρα στις βασικές καταστάσεις $|x\rangle$ που αντιστοιχούν σε στοιχεία της μη δομημένης βάσης δεδομένων. Αν η βασική κατάσταση δεν αντιστοιχεί στο στοιχείο που ψάχνουμε, την αφήνει όπως ήταν, αν όμως αντιστοιχεί, τότε τη «σημαδεύει» αλλάζοντας το πρόσημο της.

Όπως γνωρίζουμε, οι κβαντικές πύλες είναι τελεστές του χώρου Hilbert που δρουν σε qubits και σε κβαντικούς καταχωρητές, αλλάζοντας την κατάστασή τους. Κάθε κβαντικό κύκλωμα, το οποίο όπως ξέρουμε αποτελείται από κβαντικές πύλες, είναι και αυτό ένας τελεστής του χώρου Hilbert. Φυσικά, και το κβαντικό oracle είναι τελεστής του χώρου Hilbert. Αν το στοιχείο που ψάχνουμε αντιστοιχεί στη βασική κατάσταση $|x_i\rangle$, ο τελεστής του κβαντικού oracle είναι:

$$\hat{O} = \hat{I} - 2 |x_i\rangle\langle x_i| \quad (5.13)$$

όπου \hat{I} είναι ο τελεστής που αντιστοιχεί στην πύλη αδρανείας, και όταν δρα δεν αλλάζει την κατάσταση του qubit ή του κβαντικού καταχωρητή. Ας δούμε τώρα το αποτέλεσμα της δράσης του τελεστή \hat{O} σε μία βασική κατάσταση $|x_k\rangle$ η οποία δεν είναι αυτή που ψάχνουμε:

$$\hat{O} |x_k\rangle = \left(\hat{I} - 2 |x_i\rangle\langle x_i| \right) |x_k\rangle = \hat{I} |x_k\rangle - 2 |x_i\rangle\langle x_i | x_k\rangle = |x_k\rangle - 2 |x_i\rangle\langle x_i | x_k\rangle \quad (5.14)$$

Οι $|x_i\rangle$ και $|x_k\rangle$ είναι διαφορετικές βασικές καταστάσεις του κβαντικού καταχωρητή, και επομένως, όπως είδαμε στο δεύτερο κεφάλαιο, είναι ορθογώνιες μεταξύ τους: $\langle x_i | x_k\rangle = 0$. Η (5.14) γίνεται:

$$\hat{O} |x_k\rangle = |x_k\rangle - 2 |x_i\rangle\langle x_i | x_k\rangle = |x_k\rangle \quad (5.15)$$

Δηλαδή, ο τελεστής του κβαντικού oracle άφησε αναλλοίωτη την κατάσταση $|x_k\rangle$. Ας δούμε τώρα το αποτέλεσμα της δράσης του τελεστή \hat{O} στη βασική κατάσταση που ψάχνουμε, την $|x_i\rangle$:

$$\hat{O} |x_i\rangle = \left(\hat{I} - 2 |x_i\rangle\langle x_i| \right) |x_i\rangle = \hat{I} |x_i\rangle - 2 |x_i\rangle\langle x_i|x_i\rangle = |x_i\rangle - 2 |x_i\rangle = -|x_i\rangle \quad (5.16)$$

Δηλαδή, ο τελεστής του κβαντικού oracle άλλαξε το πρόσημο της κατάστασης που ψάχνουμε.

Όπως είχαμε αναφέρει παραπάνω, για να ερευνήσουμε μία μη δομημένη βάση δεδομένων που περιέχει N στοιχεία με έναν κβαντικό υπολογιστή, αντιστοιχίζουμε κάθε ένα από τα στοιχεία με μία από τις βασικές καταστάσεις ενός κβαντικού καταχωρητή. Ο καταχωρητής περιλαμβάνει n qubits. Τα N και n σχετίζονται με την (5.2). Για να το πετύχουμε αυτό, θέτουμε τον κβαντικό καταχωρητή σε μία κατάσταση $|s\rangle$ η οποία είναι μία υπέρθεση όλων των βασικών καταστάσεων. Σ' αυτή την υπέρθεση όλες οι καταστάσεις έχουν το ίδιο πλάτος πιθανότητας:

$$|s\rangle = \frac{1}{\sqrt{N}}|0\rangle + \frac{1}{\sqrt{N}}|1\rangle + \frac{1}{\sqrt{N}}|2\rangle + \dots + \frac{1}{\sqrt{N}}|(N-1)\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |x_i\rangle \quad (5.17)$$

Η (5.17) είναι η (2.29) στην οποία θέσαμε $c_i = (1/\sqrt{N})$ για κάθε i . Κατ' αναλογία με τον τελεστή \hat{O} ο Grover όρισε έναν ακόμη τελεστή, τον \hat{G} που δίνεται από (Grover, 1998):

$$\hat{G} = -\left(\hat{I} - 2 |s\rangle\langle s| \right) = 2 |s\rangle\langle s| - \hat{I} \quad (5.18)$$

Ο αλγόριθμος του Grover είναι μία διαδοχική εφαρμογή των τελεστών \hat{O} και \hat{G} στον κβαντικό καταχωρητή για $\left((\pi/4)\sqrt{N} \right) - 0,5$ περίπου φορές. Τα βήματα του αλγορίθμου του Grover είναι:

Βήμα 1°

Θέστε έναν κβαντικό καταχωρητή που περιλαμβάνει n qubits σε υπέρθεση βασικών καταστάσεων. Το πλάτος πιθανότητας να είναι ίδιο για κάθε βασική κατάσταση. Για να το πετύχετε αυτό, ξεκινάτε με τον κβαντικό καταχωρητή στην κατάσταση όπου όλα τα qubits είναι $|0\rangle$, δηλαδή στην κατάσταση $|000\dots 000\rangle$. Στη συνέχεια δράστε στο κάθε qubit με μία κβαντική πύλη Hadamard (H). Η κατάσταση του κβαντικού καταχωρητή είναι:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |x_j\rangle \quad (5.19)$$

Η $|s\rangle$ είναι η υπέρθεση των N βασικών καταστάσεων, όπου $N = 2^n - 1$. Αντιστοιχίστε κάθε βασική κατάσταση με ένα στοιχείο της μη δομημένης βάσης δεδομένων. Έστω ότι ψάχνετε για το στοιχείο που αντιστοιχεί στην $|x_i\rangle$.

Θέστε $b=1$, όπου b είναι ο αριθμός των επαναλήψεων εκτέλεσης των βημάτων που ακολουθούν.

Βήμα 2°

Δράστε στον κβαντικό καταχωρητή με τον τελεστή $\hat{O} = \hat{I} - 2 |x_i\rangle\langle x_i|$

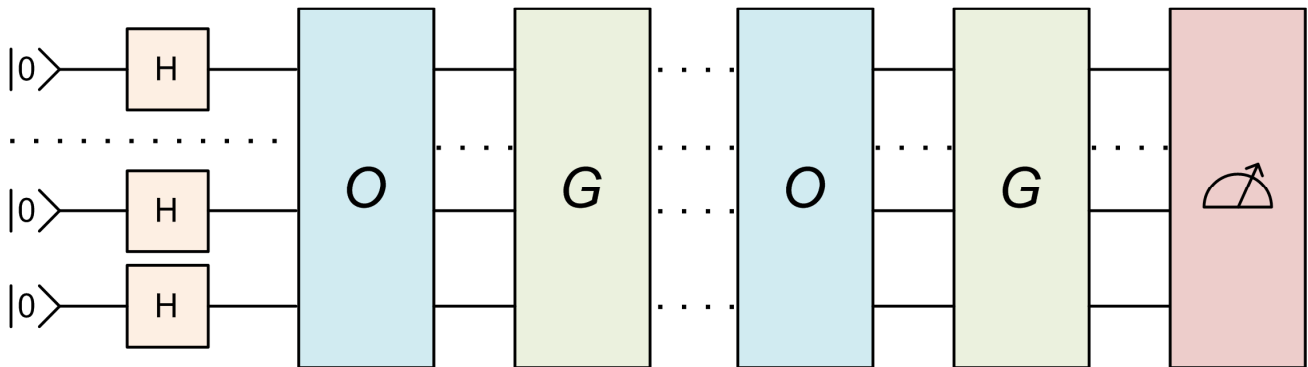
Βήμα 3°

Δράστε στον κβαντικό καταχωρητή με τον τελεστή $\hat{G} = 2 |s\rangle\langle s| - \hat{I}$

Είναι ο αριθμός επαναλήψεων b μεγαλύτερος από ή περίπου ίσος με $\left(\frac{\pi}{4}\sqrt{N}\right) - 0,5$; Αν ΝΑΙ προχωρήστε στο 4° Βήμα, αν ΟΧΙ αυξήστε το b κατά ένα ($b = b + 1$) και πηγαίετε στο 2° Βήμα.

Βήμα 4°

Μετρήστε την κατάσταση του κβαντικού καταχωρητή. Είναι πρακτικώς βέβαιο ότι θα βρίσκεται στην κατάσταση $|x_i\rangle$ που αντιστοιχεί στο στοιχείο που ψάχνετε.



Σχήμα 5-2. Το κβαντικό κύκλωμα του αλγορίθμου του Grover.

Το κβαντικό κύκλωμα που περιγράφει τον αλγόριθμο του Grover φαίνεται στο Σχήμα 5-2 (Jones, 1998).

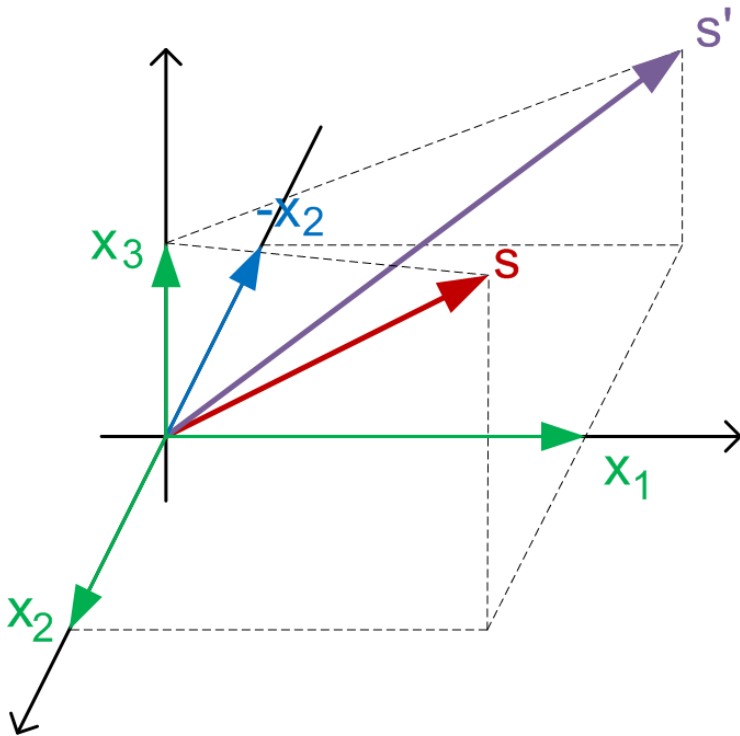
Αν διαβάζετε για πρώτη φορά αυτές τις γραμμές, είναι σχεδόν βέβαιο ότι δεν θα έχετε καταλάβει πώς λειτουργεί ο αλγόριθμος του Grover. Αυτό είναι φυσικό, διότι ο αλγόριθμος αυτός είναι πιο δυσνόητος κβαντικός αλγόριθμος. Για να γίνει κατανοητός αλγόριθμος του Grover, έχουν αναπτυχθεί δύο σχηματικές ή γεωμετρικές ερμηνείες τις οποίες θα δούμε αμέσως παρακάτω.

5.3 Γεωμετρικές ερμηνείες του κβαντικού αλγορίθμου του Grover

Πριν δώσουμε την πρώτη γεωμετρική ερμηνεία του κβαντικού αλγορίθμου του Grover, θα ήταν καλό να θυμηθούμε κάτι από τη διανυσματική ανάλυση.

Στο Σχήμα 5-3 φαίνονται διανύσματα στον Καρτεσιανό χώρο. Το διάνυσμα \vec{s} είναι το άθροισμα τριών διανυσμάτων:

$$\vec{s} = \vec{x}_1 + \vec{x}_2 + \vec{x}_3 \tag{5.20}$$



Σχήμα 5-3. Διανύσματα στον Καρτεσιανό χώρο. Το \vec{s}' είναι κατοπτρικό του \vec{s} .

Αν αλλάξουμε το πρόσημο ενός από τα διανύσματα \vec{x} , ας πούμε του \vec{x}_2 , τότε το νέο άθροισμα των τριών διανυσμάτων γίνεται:

$$\vec{s}' = \vec{x}_1 - \vec{x}_2 + \vec{x}_3 \quad (5.21)$$

Προσέξτε ότι το διάνυσμα \vec{s}' είναι κατοπτρικό του \vec{s} ως προς το επίπεδο που ορίζεται από τα άλλα δύο διανύσματα \vec{x}_1 και \vec{x}_3 , δηλαδή ως προς το επίπεδο που είναι κάθετο στο \vec{x}_2 . Αυτό θα μας χρειαστεί παρακάτω.

Ας έρθουμε τώρα στην πρώτη γεωμετρική ερμηνεία του κβαντικού αλγορίθμου του Grover. Στο Σχήμα 5-4(α) φαίνεται μία σχηματική παράσταση του χώρου Hilbert όπου φαίνονται τα διανύσματα (καταστάσεις) $|s\rangle$ και $|x_i\rangle$. Όπως γνωρίζουμε, η κατάσταση $|s\rangle$ είναι η υπέρθεση των N βασικών καταστάσεων του κβαντικού καταχωρητή και δίνεται από την (5.19), ενώ η $|x_i\rangle$ αντιστοιχεί το στοιχείο της μη δομημένης βάσης δεδομένων το οποίο ψάχνουμε.

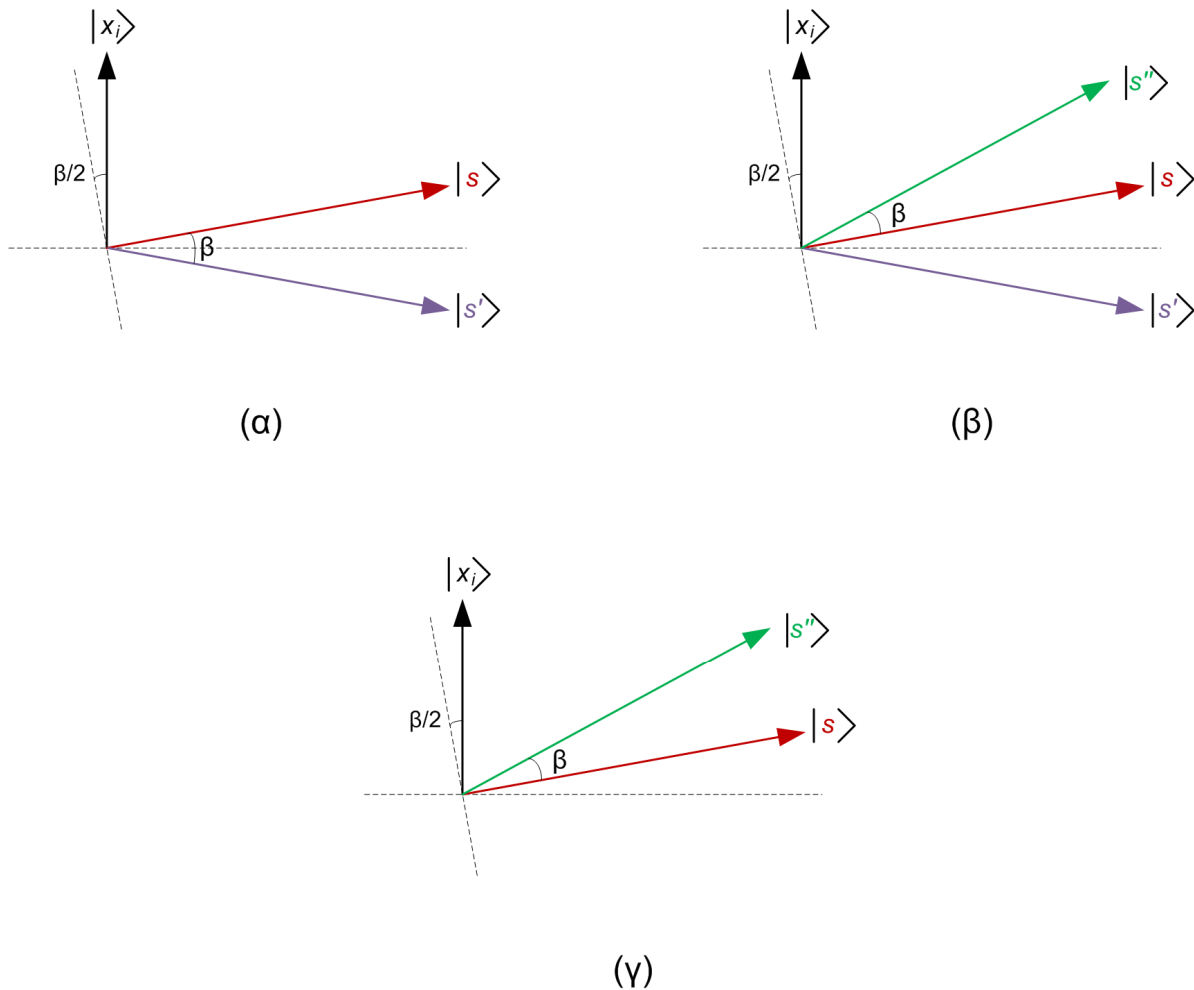
Σύμφωνα με τον κβαντικό αλγόριθμο του Grover πρώτα δρα ο τελεστής $\hat{O} = \hat{I} - 2|x_i\rangle\langle x_i|$ στην κατάσταση $|s\rangle$. Όπως προκύπτει από τις (5.15) και (5.16), η δράση του τελεστή αυτού έχει ως αποτέλεσμα την αλλαγή του προσήμου μόνο της κατάστασης $|x_i\rangle$:

$$|s'\rangle = \hat{O}|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} \hat{O}|x_i\rangle = \frac{1}{\sqrt{N}} (|x_0\rangle + |x_1\rangle + |x_2\rangle + \dots - |x_i\rangle + \dots + |x_{N-1}\rangle) \quad (5.22)$$

Όπως είδαμε στο Σχήμα 5.3, αυτή η αλλαγή του προσήμου σημαίνει ότι η κατάσταση $|s'\rangle$ είναι κατοπτρική της $|s\rangle$ ως προς το υπερεπίπεδο το κάθετο στην $|x_i\rangle$. Η διακεκομμένη γραμμή μεταξύ των $|s\rangle$ και $|s'\rangle$, στο σχήμα 5-4(α), είναι η παράσταση της τομής του υπερεπιπέδου αυτού με το επίπεδο του χαρτιού.

Στη συνέχεια δρα στην $|s'\rangle$ ο τελεστής $\hat{G} = 2|s\rangle\langle s| - \hat{I}$:

$$|s''\rangle = \hat{G}|s'\rangle \quad (5.23)$$



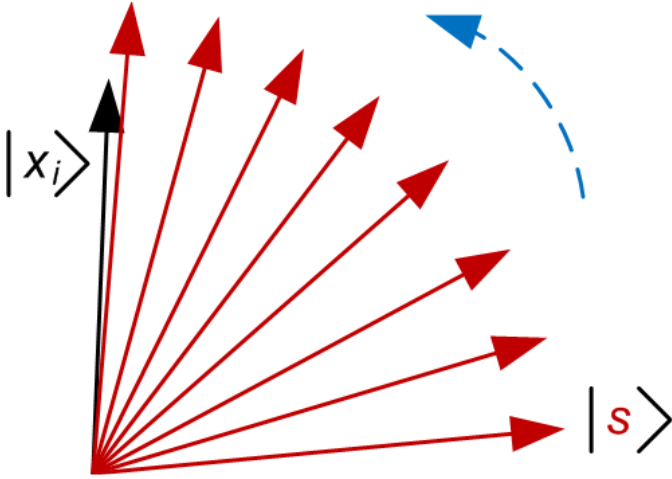
Σχήμα 5-4. (α) Η δράση του τελεστή \hat{O} περιστρέφει την $|s\rangle$ και τη φέρνει στην $|s'\rangle$. (β) Η δράση του τελεστή \hat{G} περιστρέφει την $|s'\rangle$ και τη φέρνει στην $|s''\rangle$. (γ) Η δράση των τελεστών $\hat{G} \hat{O}$ περιστρέφει την κατάσταση του κβαντικού καταχωρητή $|s\rangle$ κατά γωνία β προς την κατάσταση $|x_i\rangle$.

Όπως φαίνεται από την (5.18), αυτός ο τελεστής έχει τη μορφή του \hat{O} , αλλά με αντίθετο πρόσημο. Δηλαδή, η $|s''\rangle$ είναι κατοπτρική της $|s'\rangle$ όχι ως το επίπεδο το κάθετο στην $|s\rangle$, αλλά ως το υπερεπίπεδο που περιέχει την $|s\rangle$ και είναι κάθετο στο επίπεδο του χαρτιού (Σχήμα 5-4(β)).

Μπορούμε να πούμε ότι:

$$|s''\rangle = \hat{G} \hat{O} |s\rangle \quad (5.24)$$

δηλαδή ότι μία επανάληψη του κβαντικού αλγορίθμου του Grover περιστρέφει την κατάσταση $|s\rangle$ κατά γωνία β προς την κατάσταση $|x_i\rangle$. Αυτό φαίνεται στο Σχήμα 5-4(γ).

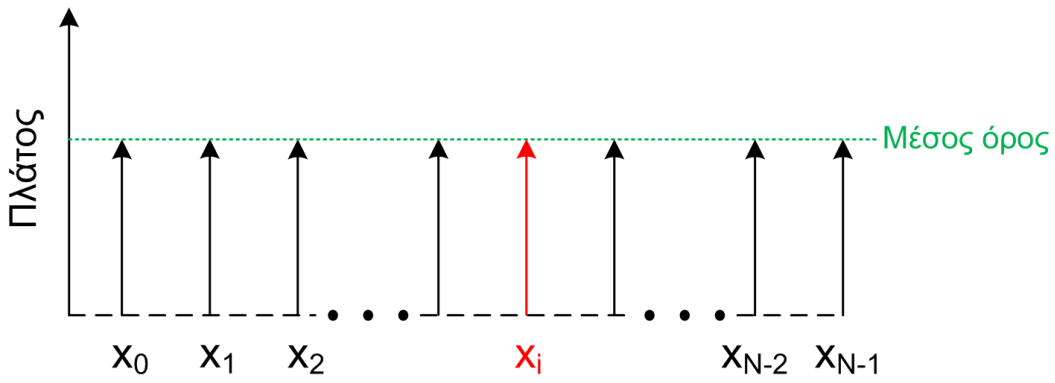


Σχήμα 5-5. Κάθε επανάληψη του κβαντικού αλγορίθμου του Grover περιστρέφει την κατάσταση του κβαντικού καταχωρητή $|s\rangle$ κατά γωνία β προς την κατάσταση $|x_i\rangle$.

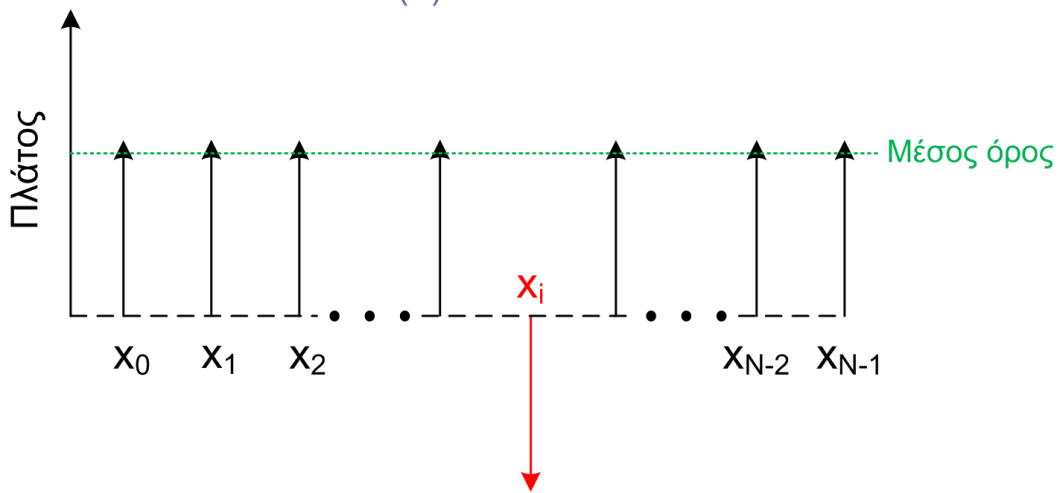
Όπως φαίνεται στο Σχήμα 5-5, κάθε επανάληψη του κβαντικού αλγορίθμου του Grover περιστρέφει την κατάσταση του κβαντικού καταχωρητή κατά γωνία β προς την κατάσταση $|x_i\rangle$. Η γωνία β είναι ίση με το μισό της γωνίας που σχηματίζεται από την $|x_i\rangle$ και το υπερεπίπεδο το κάθετο στην $|s\rangle$. Είναι εύκολο να υπολογιστεί ότι μετά από $\left(\frac{\pi}{4}\sqrt{N}\right) - 0,5$ επαναλήψεις, η κατάσταση του κβαντικού καταχωρητή θα συμπέσει ή θα βρεθεί πάρα πολύ κοντά στην κατάσταση $|x_i\rangle$ που αντιστοιχεί με το στοιχείο που ψάχνουμε. Τότε μία μέτρηση της κατάστασης του κβαντικού καταχωρητή είναι βέβαιο ή πρακτικά βέβαιο ότι θα δώσει την $|x_i\rangle$.

Μία άλλη ερμηνεία του κβαντικού αλγορίθμου του Grover, που είναι περισσότερο σχηματική παρά γεωμετρική, φαίνεται στο Σχήμα 5-6. Στο Σχήμα 5-6(α) φαίνονται τα πλάτη πιθανότητας όλων των βασικών καταστάσεων του κβαντικού καταχωρητή, όταν αυτός βρίσκεται στην υπέρθεση βασικών καταστάσεων που δίνεται από την (5.19). Όλα τα πλάτη πιθανότητας είναι ίσα με $(1/\sqrt{N})$ και ο μέσος όρος τους είναι και αυτός $(1/\sqrt{N})$. Τονίζεται και πάλι ότι η περιγραφή είναι σχηματική, διότι τα πλάτη πιθανότητας είναι γενικά μιγαδικοί αριθμοί.

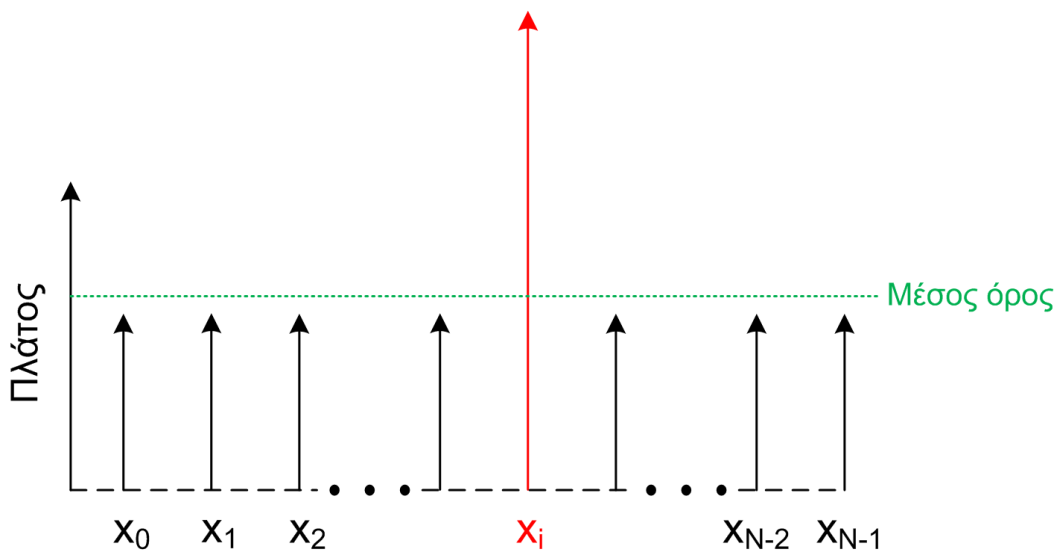
Σύμφωνα με τον κβαντικό αλγόριθμο του Grover πρώτα δρα ο τελεστής $\hat{O} = \hat{I} - 2|x_i\rangle\langle x_i|$ στην κατάσταση $|s\rangle$. Γνωρίζουμε από την (5.22) ότι $|s'\rangle = \hat{O}|s\rangle$. Όπως φαίνεται και από την (5.22), η δράση του τελεστή αυτού έχει ως αποτέλεσμα την αλλαγή του προσήμου μόνο της κατάστασης $|x_i\rangle$. Στο Σχήμα 5-6(β) φαίνονται τα πλάτη πιθανότητας όλων των βασικών καταστάσεων του κβαντικού καταχωρητή, όταν αυτός βρίσκεται, στην κατάσταση $|s'\rangle$.



(α)



(β)



(γ)

Σχήμα 5-6. (α) Τα πλάτη πιθανότητας των βασικών καταστάσεων πριν τη δράση των τελεστών \hat{G} και \hat{O} . (β) Τα πλάτη πιθανότητας μετά τη δράση του τελεστή \hat{O} . (γ) Τα πλάτη πιθανότητας μετά τη δράση του τελεστή \hat{G} .

Θεωρούμε μία γενική κατάσταση $|\psi\rangle$ η οποία εκφράζεται ως άθροισμα των βασικών καταστάσεων του κβαντικού καταχωρητή με διαφορετικά πλάτη πιθανότητας που δίνονται από τα a_j :

$$|\psi\rangle = \sum_{j=0}^{N-1} a_j |x_j\rangle \quad (5.25)$$

Το εσωτερικό γινόμενο της $|\psi\rangle$ με την $|s\rangle$ είναι:

$$\langle s|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{j=0}^{N-1} a_j \langle x_k|x_j\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} a_j = \frac{N}{\sqrt{N}} \frac{1}{N} \sum_{j=0}^{N-1} a_j = \sqrt{N} \langle a\rangle \quad (5.26)$$

όπου

$$\langle a\rangle = \frac{1}{N} \sum_{j=0}^{N-1} a_j \quad (5.27)$$

είναι ο μέσος όρος των πλατών πιθανότητας. Θυμηθείτε ότι $\langle x_j|x_k\rangle = \delta_{jk}$. Ας δούμε τώρα τη δράση του τελεστή \hat{G} στην κατάσταση $|s'\rangle$ που δίνεται από την (5.22):

$$\hat{G}|s'\rangle = \left(2|s\rangle\langle s| - \hat{I} \right) |s'\rangle = 2|s\rangle\langle s|s'\rangle - |s'\rangle \quad (5.28)$$

Αν λάβουμε υπόψη την (5.27) με τη $|s'\rangle$ στη θέση της $|\psi\rangle$, η (5.28) γίνεται:

$$\hat{G}|s'\rangle = 2|s\rangle\langle s|s'\rangle - |s'\rangle = 2\sqrt{N} \langle a\rangle |s\rangle - |s'\rangle \quad (5.29)$$

Αν αντικαταστήσουμε την $|s\rangle$ με την (5.19) και γράψουμε την $|s'\rangle$ με τον γενικό τρόπο της (5.25) (δηλαδή όπως στην (5.22) αλλά με a_j στη θέση των πλατών) έχουμε:

$$\hat{G}|s'\rangle = 2\sqrt{N} \langle a\rangle |s\rangle - |s'\rangle = 2\sqrt{N} \langle a\rangle \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |x_j\rangle - \sum_{j=0}^{N-1} a_j |x_j\rangle = \sum_{j=0}^{N-1} (2\langle a\rangle - a_j) |x_j\rangle \quad (5.30)$$

Δηλαδή, με τη δράση του τελεστή \hat{G} στην κατάσταση $|s'\rangle$ κάθε βασική κατάσταση $|x_j\rangle$ έχει πλάτος πιθανότητας $(2\langle a\rangle - a_j)$.

Στην (5.30) όλα τα πλάτη a_j είναι ίσα μεταξύ τους και ίσα με τον μέσο όρο, εκτός από το πλάτος της $|x_i\rangle$ που είναι ίσο με το αρνητικό του μέσου όρου:

$$a_j = \frac{1}{\sqrt{N}} = \langle a\rangle \quad j \neq i \quad (5.31)$$

$$a_j = -\frac{1}{\sqrt{N}} = -\langle a\rangle \quad j = i$$

Ας γράψουμε τώρα την (5.30) αναλυτικά:

$$\begin{aligned}
|s''\rangle &= \hat{G}|s'\rangle = \sum_{j=0}^{N-1} (2\langle a| - a_j)|x_j\rangle = (2\langle a| - a_0)|x_0\rangle + (2\langle a| - a_1)|x_1\rangle + \dots + (2\langle a| - a_i)|x_i\rangle \\
&+ \dots + (2\langle a| - a_{N-1})|x_{N-1}\rangle \\
&= \langle a|x_0\rangle + \langle a|x_1\rangle + \dots + 3\langle a|x_i\rangle + \dots + \langle a|x_{N-1}\rangle
\end{aligned} \tag{5.32}$$

Δηλαδή, με τη δράση του τελεστή \hat{G} έμειναν αναλλοίωτα και ίσα με $\langle a|$ τα πλάτη πιθανότητας όλων των βασικών καταστάσεων, εκτός από το πλάτος πιθανότητας της $|x_i\rangle$ που έγινε θετικό και ίσο με $3\langle a|$. Αυτό φαίνεται στο Σχήμα 5-6(γ). Με κάθε επανάληψη του κβαντικού αλγορίθμου του Grover, το πλάτος της $|x_i\rangle$ αυξάνεται, ενώ τα πλάτη των άλλων βασικών καταστάσεων μειώνονται. Μετά από $\left(\frac{\pi}{4}\sqrt{N}\right) - 0,5$ επαναλήψεις γίνεται 1 ή πρακτικά ίσο με 1, ενώ τα πλάτη των υπολοίπων βασικών καταστάσεων γίνονται 0 ή πρακτικά ίσα με 0. Αν μετρήσουμε τότε την κατάσταση του κβαντικού καταχωρητή, είναι βέβαιο ή πρακτικά βέβαιο ότι η μέτρηση θα δώσει τη βασική κατάσταση $|x_i\rangle$ που αντιστοιχεί με το στοιχείο της βάσης δεδομένων που ψάχνουμε. Αυτή η διαδικασία ονομάζεται ενίσχυση του πλάτους πιθανότητας.

(Για να είμαστε απόλυτα ακριβείς πρέπει εδώ να σημειώσουμε ότι το $\langle a|$ στην (5.32) είναι λίγο μικρότερο από $(1/\sqrt{N})$, διότι το άθροισμα των τετράγωνων των πλατών πιθανότητας πρέπει να είναι ίσο με τη μονάδα.)

5.4 Πρώτο παράδειγμα εφαρμογής του κβαντικού αλγορίθμου του Grover

Δίνεται μία μη δομημένη βάση δεδομένων με 4 στοιχεία. Να εφαρμόσετε τον κβαντικό αλγόριθμο του Grover για να βρείτε το στοιχείο που αντιστοιχεί στη βασική κατάσταση $|x_i\rangle = |01\rangle$.

Αρχίζουμε με έναν κβαντικό καταχωρητή με 2 qubits. Ψάχνουμε για το στοιχείο που αντιστοιχεί με τον αριθμό 1, δηλαδή με την κατάσταση $|x_i\rangle = |01\rangle$. Εκτελούμε ένα προς ένα τα βήματα του αλγορίθμου:

Βήμα 1°

Αρχίζουμε με τον κβαντικό καταχωρητή στην κατάσταση $|00\rangle$ και τον θέτουμε σε υπέρθεση βασικών καταστάσεων. Το πλάτος πιθανότητας πρέπει να είναι ίδιο για κάθε βασική κατάσταση. Για να το πετύχουμε αυτό χρησιμοποιούμε δύο κβαντικές πύλες H . Έχουμε ήδη υπολογίσει το $H \otimes H$, οπότε:

$$|s\rangle = H \otimes H |00\rangle = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \Rightarrow \quad (5.33)$$

$$|s\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Δηλαδή ο κβαντικός καταχωρητής βρίσκεται στην κατάσταση που δίνεται από την (5.19). Ψάχνουμε να βρούμε την $|01\rangle$, δηλαδή θέλουμε να φέρουμε τον κβαντικό καταχωρητή σε τέτοια κατάσταση ώστε η μέτρησή του να δώσει την $|01\rangle$ με πολύ μεγάλη πιθανότητα.

Βήμα 2°

Δρούμε στον κβαντικό καταχωρητή με τον τελεστή $\hat{O} = \hat{I} - 2|x_i\rangle\langle x_i|$ ο οποίος σε μορφή πίνακα δίνεται από:

$$\hat{O} = \hat{I} - 2|x_i\rangle\langle x_i| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} - 2 \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} - 2 \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \Rightarrow$$

$$\hat{O} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (5.34)$$

Οπότε:

$$|s'\rangle = \hat{O}|s\rangle = \frac{1}{2} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle + |11\rangle) \quad (5.35)$$

Δηλαδή η δράση του τελεστή άλλαξε το πρόσημο της $|01\rangle$

Βήμα 3°

Δρούμε στον κβαντικό καταχωρητή με τον τελεστή $\hat{G} = 2|s\rangle\langle s| - \hat{I}$ ο οποίος σε μορφή πινάκα δίνεται από:

$$\hat{G} = 2|s\rangle\langle s| - \hat{I} = 2 \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \frac{1}{2} [1 \ 1 \ 1 \ 1] - \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \Rightarrow$$

$$\hat{G} = \frac{1}{2} \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$

(5.36)

Η δράση του \hat{G} έχει ως αποτέλεσμα:

$$|s''\rangle = \hat{G}|s'\rangle = \frac{1}{4} \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 0 \\ 4 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle$$

(5.37)

Μετά από μία επανάληψη του αλγορίθμου αν μετρήσουμε την κατάσταση του κβαντικού καταχωρητή είναι βέβαιο ότι θα βρούμε την κατάσταση $|x_i\rangle = |01\rangle$. Ο αριθμός επαναλήψεων είναι: $((\pi/4)\sqrt{N}) - 0,5 \cong 1$

5.5 Δεύτερο παράδειγμα εφαρμογής του κβαντικού αλγορίθμου του Grover

Δίνεται μία μη δομημένη βάση δεδομένων με 8 στοιχεία. Να εφαρμόσετε τον κβαντικό αλγόριθμο του Grover για να βρείτε το στοιχείο που αντιστοιχεί στη βασική κατάσταση $|x_i\rangle = |101\rangle$.

Αρχίζουμε με έναν κβαντικό καταχωρητή με 3 qubits. Ψάχνουμε για το στοιχείο που αντιστοιχεί με τον αριθμό 5, δηλαδή με την κατάσταση $|x_i\rangle = |101\rangle$. Εκτελούμε ένα προς ένα τα βήματα του αλγορίθμου:

Βήμα 1°

Αρχίζουμε με τον κβαντικό καταχωρητή στην κατάσταση $|000\rangle$ και τον θέτουμε σε υπέρθεση βασικών καταστάσεων. Το πλάτος πιθανότητας πρέπει να είναι ίδιο για κάθε βασική κατάσταση. Για να το πετύχουμε αυτό χρησιμοποιούμε τρεις κβαντικές πύλες H . Έχουμε ήδη υπολογίσει το $H \otimes H$, οπότε:

$$|s\rangle = H \otimes H \otimes H |000\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} \otimes \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \end{bmatrix} |000\rangle =$$

$$= \begin{bmatrix} \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} \\ \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} \\ \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} \\ \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} \\ \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} \\ \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} \\ \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} \\ \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & \frac{1}{2\sqrt{2}} & -\frac{1}{2\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} =$$

$$\begin{aligned}
& \frac{1}{2\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{8}} (|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \\
& \hspace{20em} (5.38)
\end{aligned}$$

Δηλαδή ο κβαντικός καταχωρητής βρίσκεται στην κατάσταση που δίνεται από την (5.19). Ψάχνουμε να βρούμε την $|101\rangle$, δηλαδή θέλουμε να φέρουμε τον κβαντικό καταχωρητή σε τέτοια κατάσταση ώστε η μέτρησή του να δώσει την $|101\rangle$ με πολύ μεγάλη πιθανότητα.

Βήμα 2°

Δρούμε στον κβαντικό καταχωρητή με τον τελεστή $\hat{O} = \hat{I} - 2|x_i\rangle\langle x_i|$ ο οποίος σε μορφή πίνακα δίνεται από:

$$\begin{aligned}
\hat{O} = \hat{I} - 2|x_i\rangle\langle x_i| &= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} - 2 \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} [0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 0 \ 0] = \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} - 2 \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \\
& \hspace{20em} (5.39)
\end{aligned}$$

Οπότε:

$$|s'\rangle = \hat{O}|s\rangle = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{8}} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} \Rightarrow$$

$$|s'\rangle = \hat{O}|s\rangle = \frac{1}{\sqrt{8}} (|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle - |101\rangle + |110\rangle + |111\rangle) \quad (5.40)$$

Δηλαδή η δράση του τελεστή άλλαξε το πρόσημο της $|101\rangle$

Βήμα 3°

Δρούμε στον κβαντικό καταχωρητή με τον τελεστή $\hat{G} = 2|s\rangle\langle s| - \hat{I}$ ο οποίος σε μορφή πίνακα δίνεται από:

$$\hat{G} = 2 \frac{1}{\sqrt{8}} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \frac{1}{\sqrt{8}} [1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1] - \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} =$$

$$= \frac{1}{4} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} - \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} =$$

$$= \frac{1}{4} \begin{bmatrix} -3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -3 \end{bmatrix} \quad (5.41)$$

Η δράση του \hat{G} έχει ως αποτέλεσμα:

$$|s''\rangle = \hat{G}|s'\rangle = \frac{1}{4\sqrt{8}} \begin{bmatrix} -3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -3 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{4\sqrt{8}} \begin{bmatrix} 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 10 \\ 2 \\ 2 \end{bmatrix} \Rightarrow$$

$$|s''\rangle = \frac{1}{\sqrt{32}}|000\rangle + \frac{1}{\sqrt{32}}|001\rangle + \frac{1}{\sqrt{32}}|010\rangle + \frac{1}{\sqrt{32}}|011\rangle + \frac{1}{\sqrt{32}}|100\rangle + \frac{5}{\sqrt{32}}|101\rangle + \frac{1}{\sqrt{32}}|110\rangle + \frac{1}{\sqrt{32}}|111\rangle \quad (5.42)$$

Μετά από μία επανάληψη του αλγορίθμου, αν μετρήσουμε την κατάσταση του κβαντικού καταχωρητή, η πιθανότητα να βρούμε την κατάσταση $|x_i\rangle = |101\rangle$ είναι ίση με:

$$\left| \frac{5}{\sqrt{32}} \right|^2 = \frac{25}{32} = 0.78125 \cong 78\% \quad (5.43)$$

ενώ η πιθανότητα να βρούμε μία άλλη, π.χ. την $|100\rangle$ είναι:

$$\left| \frac{1}{\sqrt{32}} \right|^2 = \frac{1}{32} = 0.03125 \cong 3\% \quad (5.44)$$

Φυσικά, το άθροισμα των πιθανοτήτων είναι ίσο με τη μονάδα:

$$7 \cdot \left| \frac{1}{\sqrt{32}} \right|^2 + \left| \frac{5}{\sqrt{32}} \right|^2 = \frac{7}{32} + \frac{25}{32} = 1 \quad (5.45)$$

Ο αριθμός επαναλήψεων πρέπει να είναι ίσος ή μεγαλύτερος από $\left(\left(\pi/4\right)\sqrt{N}\right)-0,5 \cong 2$. Δηλαδή χρειάζεται άλλη μία επανάληψη του αλγορίθμου. Στο τέλος της επόμενης επανάληψης, η πιθανότητα να μετρήσουμε την $|101\rangle$ θα είναι πρακτικά ίση με τη μονάδα. Η συνέχεια αφήνεται σε εσάς. Οι τελεστές \hat{O} και \hat{G} έχουν ήδη υπολογιστεί.

Βιβλιογραφία

- Grover L. K., A fast quantum mechanical algorithm for database search, *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, pp. 212-219, 1996.
- Grover L. K., Quantum mechanics helps in searching for a needle in a haystack, *Physical Review Letters*, vol. 79, pp. 325-328, 1997.
- Grover L. K., Quantum computers can search rapidly by using almost any transformation, *Physical Review Letters*, vol. 80, pp. 4329-4332, 1998.
- Jones J. A., Mosca M., & Hansen R. H., Implementation of a quantum search algorithm on a quantum computer, *Nature*, vol. 393, pp. 344-346, 1998.
- Kwiat P. G., Mitchell J. R., Schwindt P. D. D., & White A. G., Grover's search algorithm: An optical approach, *Journal of Modern Optics*, vol. 47, pp. 257-266, 2000.

Ασκήσεις

Άσκηση 5.1

Δίνεται μία μη δομημένη βάση δεδομένων με 4 στοιχεία. Να εφαρμόσετε τον κβαντικό αλγόριθμο του Grover για να βρείτε το στοιχείο που αντιστοιχεί στη βασική κατάσταση $|x_i\rangle = |00\rangle$.

Άσκηση 5.2

Δίνεται μία μη δομημένη βάση δεδομένων με 4 στοιχεία. Να εφαρμόσετε τον κβαντικό αλγόριθμο του Grover για να βρείτε το στοιχείο που αντιστοιχεί στη βασική κατάσταση $|x_i\rangle = |10\rangle$.

Άσκηση 5.3

Δίνεται μία μη δομημένη βάση δεδομένων με 4 στοιχεία. Να εφαρμόσετε τον κβαντικό αλγόριθμο του Grover για να βρείτε το στοιχείο που αντιστοιχεί στη βασική κατάσταση $|x_i\rangle = |11\rangle$.

Άσκηση 5.4

Δίνεται μία μη δομημένη βάση δεδομένων με 8 στοιχεία. Να εφαρμόσετε τον κβαντικό αλγόριθμο του Grover για να βρείτε το στοιχείο που αντιστοιχεί στη βασική κατάσταση $|x_i\rangle = |000\rangle$.

Άσκηση 5.5

Δίνεται μία μη δομημένη βάση δεδομένων με 8 στοιχεία. Να εφαρμόσετε τον κβαντικό αλγόριθμο του Grover για να βρείτε το στοιχείο που αντιστοιχεί στη βασική κατάσταση $|x_i\rangle = |010\rangle$.

Άσκηση 5.6

Δίνεται μία μη δομημένη βάση δεδομένων με 8 στοιχεία. Να εφαρμόσετε τον κβαντικό αλγόριθμο του Grover για να βρείτε το στοιχείο που αντιστοιχεί στη βασική κατάσταση $|x_i\rangle = |111\rangle$.

6. Η κβαντική διεμπλοκή και ο κβαντικός μετασχηματισμός Fourier

Σύνοψη

Η κβαντική διεμπλοκή και ο κβαντικός μετασχηματισμός Fourier δεν σχετίζονται άμεσα μεταξύ τους, αποτελούν όμως τη βάση πολλών κβαντικών υπολογισμών. Αποτελούν τη βάση και του σπουδαιότερου κβαντικού αλγορίθμου, του κβαντικού αλγορίθμου του Shor, τον οποίο θα περιγράψουμε στο επόμενο κεφάλαιο.

Προαπαιτούμενη γνώση

Γραμμική άλγεβρα, το πρώτο, δεύτερο, τρίτο και τέταρτο κεφάλαιο του βιβλίου αυτού.

6.1 Η κβαντική διεμπλοκή

Η κβαντική διεμπλοκή έχει τις ρίζες της σε ένα άρθρο των Albert Einstein, Boris Podolsky και Nathan Rosen που δημοσιεύτηκε το 1935 (Einstein, Podolsky & Rosen, 1935). Σ' αυτό είχαν ως στόχο να αποδείξουν ότι η κβαντική μηχανική δεν είναι μία πλήρης φυσική θεωρία, αλλά ότι από την κβαντική περιγραφή της φύσης λείπουν κάποιες παράμετροι, οι οποίες αργότερα ονομάστηκαν «κρυμμένες μεταβλητές» (Bohm, 1952). Ως μοντέλο για την απόδειξή τους οι Einstein, Podolsky και Rosen χρησιμοποίησαν ένα θεωρητικό πείραμα στο οποίο δύο κβαντικά συστήματα, αφού αλληλεπιδράσουν μεταξύ τους απομακρύνονται το ένα από το άλλο. Τα δύο αυτά κβαντικά συστήματα παραμένουν διασυνδεδεμένα το ένα με το άλλο με έναν άγνωστο μη κλασικό τρόπο. Αυτό έχει ως αποτέλεσμα η μέτρηση μίας φυσικής ποσότητας του ενός να καθορίζει το αποτέλεσμα της μέτρησης της ίδιας φυσικής ποσότητας του άλλου. Το θεωρητικό πείραμα που περιγράφεται στο άρθρο αυτό είναι γνωστό ως «EPR» από τα αρχικά των επιθέτων των τριών ερευνητών ή ως «παράδοξο EPR». Το παράδοξο EPR προκάλεσε συζητήσεις, διαμάχες και πολλές προσπάθειες για να αποδειχθεί ότι η κβαντική μηχανική είναι μια πλήρης φυσική θεωρία και ότι δεν υπάρχουν κρυμμένες μεταβλητές. Η διαμάχη συνεχίστηκε ώσπου με άρθρο του, που δημοσιεύτηκε το 1964, ο John Bell απέδειξε με τη χρήση ανισοτήτων (που είναι πλέον γνωστές ως «ανισότητες Bell») ότι δεν υπάρχουν κρυμμένες μεταβλητές και ότι η κβαντική μηχανική είναι μία πλήρης φυσική θεωρία (Bell, 1964). Η ανισότητες Bell αποδείχτηκαν αργότερα και πειραματικά (Aspect, Dalibard & Roger, 1982).

Ο Erwin Schrödinger σε άρθρο του που δημοσιεύτηκε το 1935, για να περιγράψει την άγνωστη μη κλασική διασύνδεση μεταξύ δύο κβαντικών συστημάτων τα οποία, αφού αλληλεπιδράσουν, απομακρύνονται το ένα από το άλλο, χρησιμοποίησε το Γερμανικό όρο «verschränkung» που έχει την έννοια «σταυρώνω (τα χέρια)» (Schrödinger, 1935). Ο όρος αποδόθηκε στα Αγγλικά ως «entanglement» και στα Ελληνικά μπορεί να αποδοθεί ως «διαπλοκή» ή «διεμπλοκή». Στο βιβλίο αυτό ο όρος «entanglement» θα αποδίδεται ως «διεμπλοκή».

Η κβαντική διεμπλοκή είναι ίσως η πιο αινιγματική πλευρά της κβαντικής μηχανικής και δεν έχει κλασικό ανάλογο. Κάθε χρόνο πολλές δεκάδες άρθρα δημοσιεύονται σε επιστημονικά περιοδικά και περιγράφουν επιστημονικές εργασίες που έχουν ως στόχο την κατανόηση, το χειρισμό και τον υπολογισμό της κβαντικής διεμπλοκής.

Για τους κβαντικούς υπολογιστές η κβαντική διεμπλοκή είναι ένας φυσικός πόρος, όπως η ενέργεια, τον οποίο μπορούμε να χρησιμοποιήσουμε για να εκτελέσουμε κβαντικούς υπολογισμούς και να αναπτύξουμε κβαντικούς αλγορίθμους (Niesen & Chuang, 2004). Αυτό που έχει δηλαδή σημασία, δεν είναι να κατανοήσουμε τη φύση της κβαντικής διεμπλοκής (πράγμα που είναι ίσως αδύνατο), αλλά να μάθουμε να την παράγουμε και να τη χρησιμοποιούμε. Ας ορίσουμε λοιπόν την κβαντική διεμπλοκή με έναν απλό, αλλά χρήσιμο για εμάς τρόπο:

Ορισμός: Δύο κβαντικά συστήματα βρίσκονται σε κβαντική διεμπλοκή, όταν η κατάσταση τους δεν μπορεί να γραφεί ως τανυστικό γινόμενο των βασικών τους καταστάσεων.

Ας θεωρήσουμε ότι τα δύο κβαντικά συστήματα είναι qubits και ας δούμε τι σημαίνει αυτός ο ορισμός.

Θεωρούμε δύο qubits το $|q_{s,0}\rangle$ και το $|q_{s,1}\rangle$ που βρίσκονται στην κατάσταση $|q_s\rangle$ η οποία δίνεται από:

$$|q_s\rangle = \frac{1}{\sqrt{2}} (|10\rangle + |11\rangle) \quad (6.1)$$

Η $|q_s\rangle$ μπορεί να γραφεί:

$$|q_s\rangle = \frac{1}{\sqrt{2}} (|10\rangle + |11\rangle) = |1\rangle \otimes \left[\frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right] \quad (6.2)$$

Δηλαδή, οι καταστάσεις των $|q_{s0}\rangle$ και $|q_{s1}\rangle$ είναι:

$$|q_{s1}\rangle = |1\rangle \quad (6.3)$$

$$|q_{s0}\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

και η $|q_s\rangle$ γράφεται:

$$|q_s\rangle = |q_{s1}\rangle \otimes |q_{s0}\rangle$$

Δηλαδή, η $|q_s\rangle$ μπορεί να γραφεί ως τανυστικό γινόμενο των καταστάσεων των δύο qubits, οπότε τα $|q_{s0}\rangle$ και $|q_{s1}\rangle$ δεν βρίσκονται σε κβαντική διεμπλοκή αλλά σε υπέρθεση καταστάσεων.

Θεωρούμε άλλα δύο qubits το $|q_{e0}\rangle$ και το $|q_{e1}\rangle$ τα οποία βρίσκονται στην κατάσταση $|q_e\rangle$ που δίνεται από:

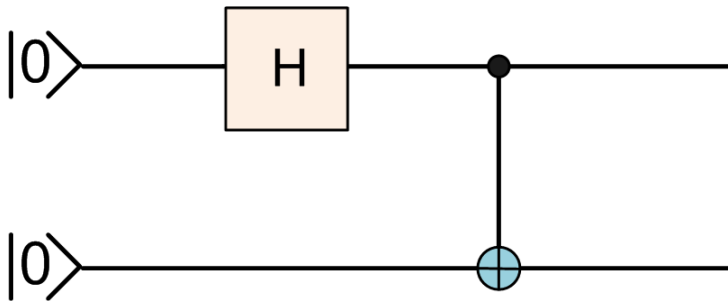
$$|q_e\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \quad (6.4)$$

Η $|q_e\rangle$ δεν μπορεί να γραφεί ως τανυστικό γινόμενο των καταστάσεων των δύο qubits, οπότε τα $|q_{e0}\rangle$ και $|q_{e1}\rangle$ βρίσκονται σε κβαντική διεμπλοκή. Η διαφορά μεταξύ της υπέρθεσης και της διεμπλοκής είναι η εξής:

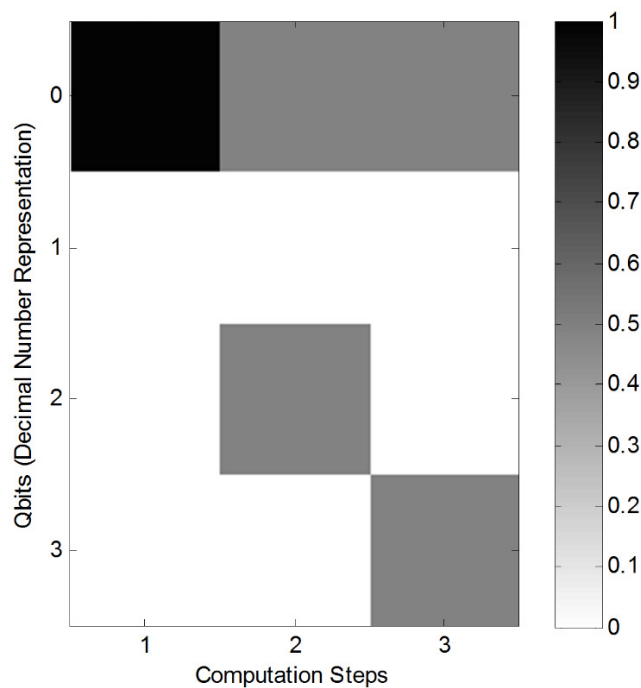
Αν μετρήσουμε την κατάσταση του qubit $|q_{s1}\rangle$ της κατάστασης $|q_s\rangle$, θα βρούμε σίγουρα ότι βρίσκεται στην κατάσταση $|1\rangle$. Μετά τη μέτρηση αυτή, το qubit $|q_{s0}\rangle$ μπορεί να βρίσκεται στην κατάσταση $|0\rangle$ ή $|1\rangle$ με πιθανότητα 0,5 για την κάθε μία περίπτωση. Δηλαδή, η μέτρηση της κατάστασης του ενός qubit δεν καθορίζει την κατάσταση του άλλου.

Αν μετρήσουμε την κατάσταση του qubit $|q_{e1}\rangle$ της κατάστασης $|q_e\rangle$, θα βρούμε με πιθανότητα 0,5 ότι βρίσκεται στην κατάσταση $|0\rangle$ και με πιθανότητα 0,5 ότι βρίσκεται στην κατάσταση $|1\rangle$. Αν το βρούμε την κατάσταση $|0\rangle$, τότε, αν μετρήσουμε την κατάσταση του qubit $|q_{e0}\rangle$, θα βρούμε σίγουρα ότι βρίσκεται και αυτό στην κατάσταση $|0\rangle$. Αν βρούμε την κατάσταση $|1\rangle$, τότε, αν μετρήσουμε την κατάσταση του qubit $|q_{e0}\rangle$, θα βρούμε σίγουρα ότι βρίσκεται και αυτό στην κατάσταση $|1\rangle$. Δηλαδή, αφού τα δύο qubits βρίσκονται σε διεμπλοκή, η μέτρηση της κατάστασης του ενός qubit καθορίζει την κατάσταση του άλλου.

Δώσαμε και εξηγήσαμε τον ορισμό της κβαντικής διεμπλοκής. Ας δούμε τώρα πώς μπορούμε να φέρουμε δύο qubits σε διεμπλοκή, δηλαδή πώς να παράγουμε κβαντική διεμπλοκή (Heiss, 2002). Για να το πετύχουμε αυτό χρειαζόμαστε δύο μόνο κβαντικές πύλες, την H και την $CNOT$. Το κβαντικό κύκλωμα για την παραγωγή διεμπλοκής φαίνεται στο Σχήμα 6-1(α).



(α)



(β)

Σχήμα 6-1. (α) Το κβαντικό κύκλωμα για την κβαντική διεμπλοκή δύο qubits. (β) Η προσομοίωση της διεμπλοκής από τον προσομοιωτή QCS.

Ας κάνουμε τον κβαντικό υπολογισμό που περιγράφεται από το κβαντικό κύκλωμα του Σχήματος 6-1:

$$\begin{aligned}
CNOT(H \otimes I)|00\rangle &= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ \frac{1}{\sqrt{2}} \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)
\end{aligned} \tag{6.5}$$

Η προσομοίωση του κβαντικού υπολογισμού με τον προσομοιωτή QCS φαίνεται στο Σχήμα 6-1(β). Μπορούμε να φέρουμε δύο qubits σε τέσσερις διαφορετικές καταστάσεις κβαντικής διεμπλοκής, μία για κάθε έναν από τους τέσσερις δυνατούς συνδυασμούς των αρχικών τους καταστάσεων:

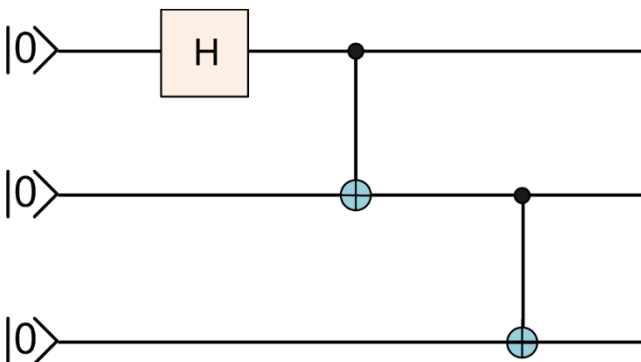
$$\begin{aligned}
|00\rangle &\xrightarrow{E} \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) \\
|01\rangle &\xrightarrow{E} \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) \\
|10\rangle &\xrightarrow{E} \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle) \\
|11\rangle &\xrightarrow{E} \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)
\end{aligned} \tag{6.6}$$

Το βέλος με το E συμβολίζει τη δράση του κυκλώματος του Σχήματος 6-1(α) που φέρνει δύο qubits σε κβαντική διεμπλοκή. Οι τέσσερις καταστάσεις κβαντικής διεμπλοκής της (6.6) ονομάζονται «καταστάσεις Bell» ή «ζεύγη EPR».

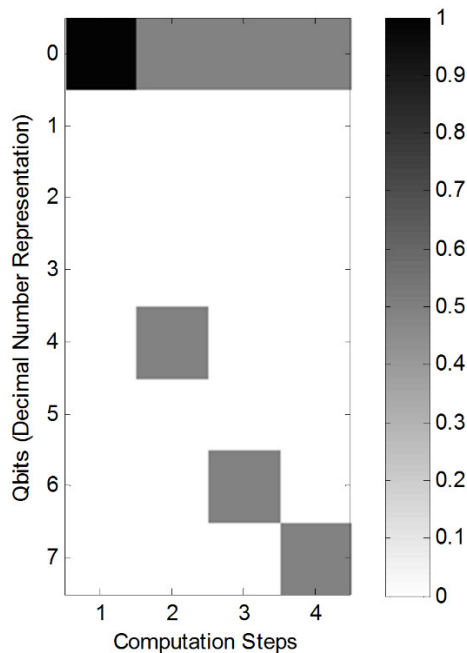
Μπορούμε να φέρουμε σε κατάσταση κβαντικής διεμπλοκής περισσότερες καταστάσεις των qubits με τη χρήση κβαντικών πυλών H και $CNOT$. Στο Σχήμα 6-2(α) φαίνεται ένα κβαντικό κύκλωμα που φέρνει σε κατάσταση κβαντικής διεμπλοκής τρία qubits. Ο κβαντικός υπολογισμός που περιγράφεται από αυτό το κύκλωμα είναι:

$$(I \otimes CNOT)(CNOT \otimes I)(H \otimes I \otimes I)|000\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \quad (6.7)$$

Η προσομοίωση του κβαντικού υπολογισμού με τον προσομοιωτή QCS φαίνεται στο Σχήμα 6-2(β) (Karafyllidis, 2004). Μπορούμε να φέρουμε τρία qubits σε οκτώ διαφορετικές καταστάσεις κβαντικής διεμπλοκής, μία για κάθε έναν από τους οκτώ δυνατούς συνδυασμούς των αρχικών τους καταστάσεων. Οι καταστάσεις κβαντικής διεμπλοκής τριών qubits είναι γνωστές και ως «καταστάσεις GHZ» από τα αρχικά των ονομάτων των ερευνητών Greenberger, Horne και Zeilinger. Στο Σχήμα 6-3 φαίνεται το κβαντικό κύκλωμα με το οποίο μπορούμε να φέρουμε σε κατάσταση κβαντικής διεμπλοκής περισσότερα από τρία qubits.

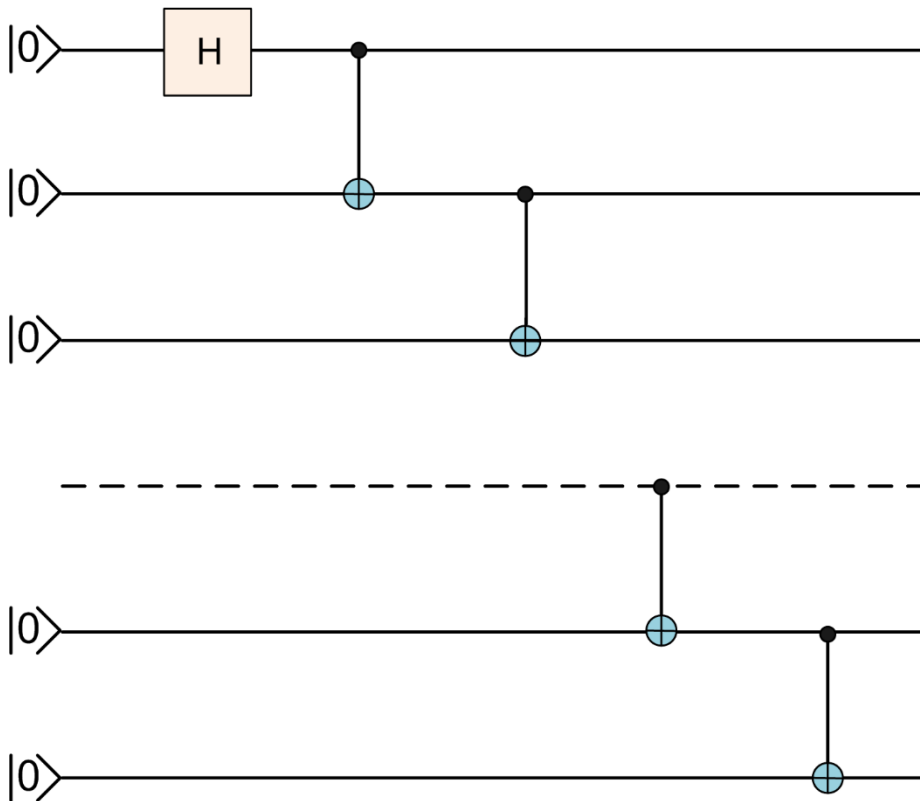


(α)



(β)

Σχήμα 6-2. (α) Το κβαντικό κύκλωμα για την κβαντική διεμπλοκή τριών qubits. (β) Η προσομοίωση της διεμπλοκής από τον προσομοιωτή QCS .



Σχήμα 6-3. Το κβαντικό κύκλωμα για την κβαντική διεμπλοκή οποιουδήποτε αριθμού qubits.

Ορίσαμε την κβαντική διεμπλοκή και μάθαμε πώς να φέρνουμε qubits σε κατάσταση κβαντικής διεμπλοκής. Τη χρήση της κβαντικής διεμπλοκής θα τη δούμε στο επόμενο κεφάλαιο, όπου θα περιγράψουμε τον κβαντικό αλγόριθμο του Shor.

6.2 Ο τελεστής πυκνότητας

Όπως ξέρουμε, η κατάσταση ενός qubit, ενός κβαντικού καταχωρητή και γενικά ενός κβαντικού συστήματος περιγράφεται από το διάνυσμα κατάστασης. Μπορούμε όμως να περιγράψουμε την κατάσταση ενός κβαντικού συστήματος και με έναν άλλο τρόπο: χρησιμοποιώντας τον τελεστή πυκνότητας, που συμβολίζεται με: ρ . Στην Κβαντική Υπολογιστική ο τελεστής πυκνότητας χρησιμοποιείται για τον υπολογισμό της διεμπλοκής μεταξύ των qubits και μεταξύ των κβαντικών καταχωρητών (Niesen & Chuang, 2004).

Ο τελεστής πυκνότητας χρησιμοποιείται επίσης και για την περιγραφή συστημάτων των οποίων η κατάσταση δεν είναι πλήρως γνωστή, καθώς και για την περιγραφή μικτών συστημάτων για τα οποία είναι στατιστικά γνωστές όλες ή κάποιες από τις πιθανότητες να βρίσκεται το σύστημα σε μία κατάσταση, η οποία ανήκει σε ένα σύνολο πιθανών καταστάσεων του συστήματος. Ας υποθέσουμε για παράδειγμα ότι ένα qubit μπορεί να βρίσκεται σε μία από τις παρακάτω καταστάσεις:

$$\begin{aligned}
 |q_1\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\
 |q_2\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle
 \end{aligned}
 \tag{6.8}$$

Δεν γνωρίζουμε σε ποια από τις δύο καταστάσεις βρίσκεται, αλλά γνωρίζουμε τις πιθανότητες που έχει να βρίσκεται σε κάθε μία από αυτές. Γνωρίζουμε ότι βρίσκεται στην κατάσταση $|q_1\rangle$ με πιθανότητα $p_1=2/3$, και στην κατάσταση $|q_2\rangle$ με πιθανότητα $p_2=1/3$. Δηλαδή αυτό το qubit βρίσκεται σε μία μικτή (mixed) κατάσταση που αποτελείται από το σύνολο καθαρών (pure) καταστάσεων $\{|q_1\rangle, |q_2\rangle\}$. Η μικτή αυτή κατάσταση, είναι ένα στατιστικό μίγμα των καθαρών (pure) καταστάσεων $|q_1\rangle$ και $|q_2\rangle$, και περιγράφεται πλήρως από τον τελεστή πυκνότητας, ρ , που ορίζεται ως:

$$\rho = p_1 |q_1\rangle\langle q_1| + p_2 |q_2\rangle\langle q_2| = \sum_{i=1}^2 p_i |q_i\rangle\langle q_i| \quad (6.9)$$

Γενικά, ένα κβαντικό σύστημα που έχει πιθανότητες p_1, p_2, \dots, p_n να βρίσκεται σε μία από τις καθαρές καταστάσεις $|q_1\rangle, |q_2\rangle, \dots, |q_n\rangle$, βρίσκεται σε μία μικτή κατάσταση που περιγράφεται από τον τελεστή πυκνότητας:

$$\rho = \sum_{i=1}^n p_i |q_i\rangle\langle q_i| \quad (6.10)$$

Μπορούμε να ορίσουμε τον τελεστή πυκνότητας και για τις περιπτώσεις όπου ένα qubit ή ένας κβαντικός καταχωρητής βρίσκεται σε μία καθαρή κατάσταση. Μπορούμε τότε να πούμε ότι όλες οι πιθανότητες της (6.10) είναι μηδέν εκτός από εκείνη που πολλαπλασιάζει την καθαρή κατάσταση $|q\rangle$, στην οποία βρίσκεται το qubit ή ο κβαντικός καταχωρητής. Η πιθανότητα αυτή είναι ίση με 1. Τότε ο τελεστής πυκνότητας, ρ , γίνεται:

$$\rho = |q\rangle\langle q| \quad (6.11)$$

Ο τελεστής πυκνότητας περιγράφεται από έναν πίνακα, ο οποίος ονομάζεται πίνακας πυκνότητας. Για παράδειγμα, ο πίνακας πυκνότητας του τελεστή της (6.9) είναι:

$$\begin{aligned} \rho = p_1 |q_1\rangle\langle q_1| + p_2 |q_2\rangle\langle q_2| &= \frac{2}{3} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} + \frac{1}{3} \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \\ &= \begin{bmatrix} 2/6 & 2/6 \\ 2/6 & 2/6 \end{bmatrix} + \begin{bmatrix} 1/6 & -1/6 \\ -1/6 & 1/6 \end{bmatrix} = \begin{bmatrix} 3/6 & 1/6 \\ 1/6 & 3/6 \end{bmatrix} \end{aligned} \quad (6.12)$$

Αν ένα qubit βρίσκεται στην καθαρή κατάσταση:

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle \quad (6.13)$$

Ο πίνακας πυκνότητας για το qubit αυτό δίνεται από:

$$\rho = |q\rangle\langle q| = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \begin{bmatrix} \alpha^* & \beta^* \end{bmatrix} = \begin{bmatrix} |\alpha|^2 & \alpha\beta^* \\ \beta\alpha^* & |\beta|^2 \end{bmatrix} \quad (6.14)$$

Παρακάτω περιγράφονται χωρίς απόδειξη οι πιο σημαντικές ιδιότητες του τελεστή και του πίνακα πυκνότητας (Niesen & Chuang, 2004):

- Ο τελεστής πυκνότητας είναι Ερμιτιανός: $\rho = \rho^\dagger$
- Το ίχνος ενός πίνακα πυκνότητας είναι πάντα ίσο με 1: $Tr(\rho) = 1$
- Αν η κατάσταση είναι μικτή τότε: $Tr(\rho^2) < 1$
- Αν η κατάσταση είναι καθαρή τότε: $Tr(\rho^2) = 1$
- Για κάθε ιδιοτιμή, λ , του πίνακα πυκνότητας ισχύει: $0 \leq \lambda \leq 1$

Ο τελεστής πυκνότητας χρησιμοποιείται και για την περιγραφή κβαντικών υποσυστημάτων που είναι μέρη ενός κβαντικού συστήματος. Μπορεί δηλαδή να περιγράψει την κατάσταση ενός qubit που είναι μέρος ενός κβαντικού καταχωρητή των δύο qubits. Έστω ένα κβαντικό σύστημα που αποτελείται από δύο υποσυστήματα, το A και το B, για το οποίο είναι γνωστός ο τελεστής πυκνότητας του συστήματος ρ^{AB} . Μπορούμε να υπολογίσουμε τον τελεστή πυκνότητας του υποσυστήματος A, τον ρ^A , ως εξής:

$$\rho^A = Tr_B(\rho^{AB}) \quad (6.15)$$

όπου Tr_B είναι το μερικό ίχνος στο υποσύστημα B και δίνεται από:

$$Tr_B(\rho^{AB}) = Tr_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2| Tr(|b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2| \langle b_2|b_1\rangle \quad (6.16)$$

Στην (6.16) οι $|a_1\rangle$ και $|a_2\rangle$ είναι οι βασικές καταστάσεις του υποσυστήματος A και οι $|b_1\rangle$ και $|b_2\rangle$ είναι οι βασικές καταστάσεις του υποσυστήματος B. Με όμοιο τρόπο μπορούμε να υπολογίσουμε τον τελεστή πυκνότητας του υποσυστήματος B. Το παρακάτω παράδειγμα θα αποσαφηνίσει τη χρήση του μερικού ίχνους.

Παράδειγμα 6.1

Ένας κβαντικός καταχωρητής των δύο qubits βρίσκεται στην κατάσταση:

$$|q_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Ο πίνακας πυκνότητας του qubit A δίνεται από:

$$\begin{aligned} \rho^A &= Tr_B(\rho^{AB}) = Tr_B\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)\right) = \\ &= \frac{1}{2}Tr_B(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) = \\ &= \frac{1}{2}(Tr_B(|00\rangle\langle 00|) + Tr_B(|00\rangle\langle 11|) + Tr_B(|11\rangle\langle 00|) + Tr_B(|11\rangle\langle 11|)) = \\ &= \frac{1}{2}((|0\rangle\langle 0| \langle 0|0\rangle) + (|0\rangle\langle 1| \langle 1|0\rangle) + (|1\rangle\langle 0| \langle 0|1\rangle) + (|1\rangle\langle 1| \langle 1|1\rangle)) \end{aligned}$$

Λαμβάνοντας υπόψη ότι οι βασικές καταστάσεις είναι ορθογώνιες έχουμε:

$$\rho^A = \frac{1}{2} (|0\rangle\langle 0| + |1\rangle\langle 1|)$$

Ο αντίστοιχος πίνακας πυκνότητας είναι:

$$\rho^A = \frac{1}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Δηλαδή, ενώ τα δύο qubits του κβαντικού καταχωρητή βρίσκονται σε κατάσταση διεμπλοκής το qubit A βρίσκεται σε μία μικτή κατάσταση, διότι $Tr((\rho_A)^2) < 1$. ♦

6.3 Εντροπία von Neumann και υπολογισμός της διεμπλοκής

Έχουμε ήδη μάθει πώς μπορούμε να φέρουμε σε κατάσταση διεμπλοκής δύο ή περισσότερα qubits. Η παραγωγή, διαχείριση και ο υπολογισμός της διεμπλοκής αποτελούν μεγάλες προκλήσεις για την Κβαντική Υπολογιστική. Για τον λόγο αυτό έχουν αναπτυχθεί θεωρητικά εργαλεία που μας βοηθούν να βρούμε αν δύο qubits ή δύο κβαντικοί καταχωρητές βρίσκονται σε κατάσταση διεμπλοκής ή όχι και να υπολογίσουμε την «ποσότητα» της διεμπλοκής τους.

Το σημαντικότερο θεωρητικό εργαλείο για τον υπολογισμό της διεμπλοκής είναι η εντροπία von Neumann. Για κάθε κβαντικό σύστημα που αποτελείται από υποσυστήματα, η διεμπλοκή του συστήματος προσδιορίζεται από την εντροπία von Neumann. Η μονάδα «μέτρησης» της διεμπλοκής είναι το entangled bit το οποίο για συντομία αναφέρεται ως *ebit*. Όπως θα δούμε αμέσως παρακάτω η ποσότητα της διεμπλοκής είναι ένας πραγματικός αριθμός. Δηλαδή η ποσότητα της διεμπλοκής μπορεί να είναι ίση με έναν μη ακέραιο αριθμό ebits (Brylinski & Goong, 2002).

Στους κβαντικούς υπολογισμούς οι κβαντικοί καταχωρητές βρίσκονται (σχεδόν πάντα) σε καθαρές καταστάσεις, στις οποίες τα qubits τους βρίσκονται σε υπέρθεση ή διεμπλοκή.

Θεωρούμε ένα κβαντικό σύστημα (έναν κβαντικό καταχωρητή) που αποτελείται από δύο υποσυστήματα, τα A και B. Τα υποσυστήματα αυτά μπορεί να είναι qubits ή δύο μικρότεροι κβαντικοί καταχωρητές. Ο κβαντικός καταχωρητής βρίσκεται στην καθαρή κατάσταση διεμπλοκής $|\psi\rangle$ η οποία δεν μπορεί να γραφεί ως ταυστικό γινόμενο των καταστάσεων των δύο υποσυστημάτων:

$$|\psi\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle \quad (6.17)$$

Η διεμπλοκή μίας καθαρής κατάστασης $|\psi\rangle$ μετριέται από την εντροπία της διεμπλοκής, E, που δίνεται από:

$$E(\psi) = S(\rho_A) = S(\rho_B) \quad (6.18)$$

Όπου $S(\rho)$ είναι η εντροπία von Neumann. Δηλαδή η ποσότητα της διεμπλοκής του συστήματος είναι ίση με την εντροπία von Neumann οποιουδήποτε από τα δύο υποσυστήματα.

$$S(\rho_A) = -Tr(\rho_A \log_2 \rho_A) \quad (6.19)$$

$$S(\rho_B) = -Tr(\rho_B \log_2 \rho_B)$$

όπου ρ_A και ρ_B είναι οι πίνακες πυκνότητας των υποσυστημάτων, που υπολογίζονται με τη χρήση του μερικού ίχνους:

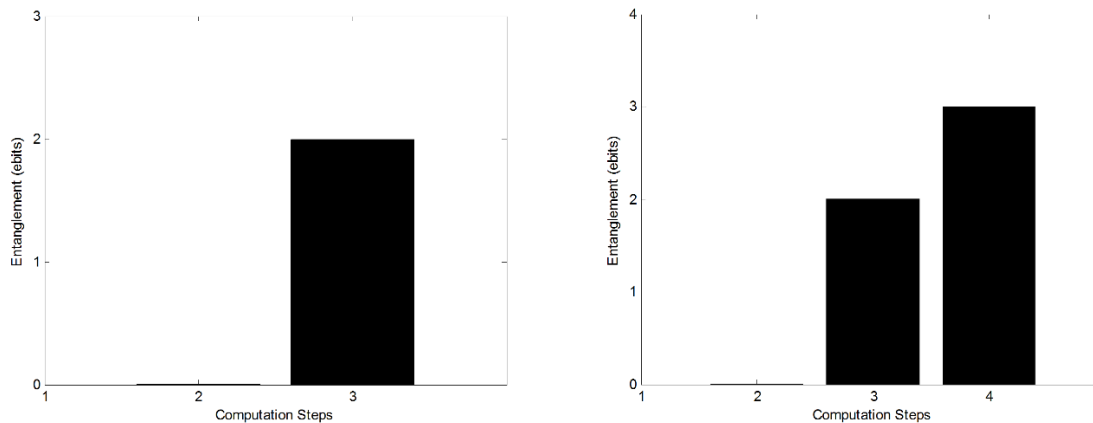
$$\rho_A = Tr_B (|\psi\rangle\langle\psi|) \tag{6.20}$$

$$\rho_B = Tr_A (|\psi\rangle\langle\psi|)$$

Η εντροπία von Neumann μπορεί εύκολα να υπολογιστεί από τις ιδιοτιμές $\{\lambda_i\}$ του πίνακα πυκνότητας ως εξής:

$$S(\rho) = -Tr (\rho \log_2 \rho) = \sum_i -\lambda_i \log_2 \lambda_i \tag{6.21}$$

Όπως είπαμε, η διεμπλοκή E μετριέται σε ebits και όπως φαίνεται από την παραπάνω εξίσωση, μπορεί να είναι και μη ακέραιος αριθμός.



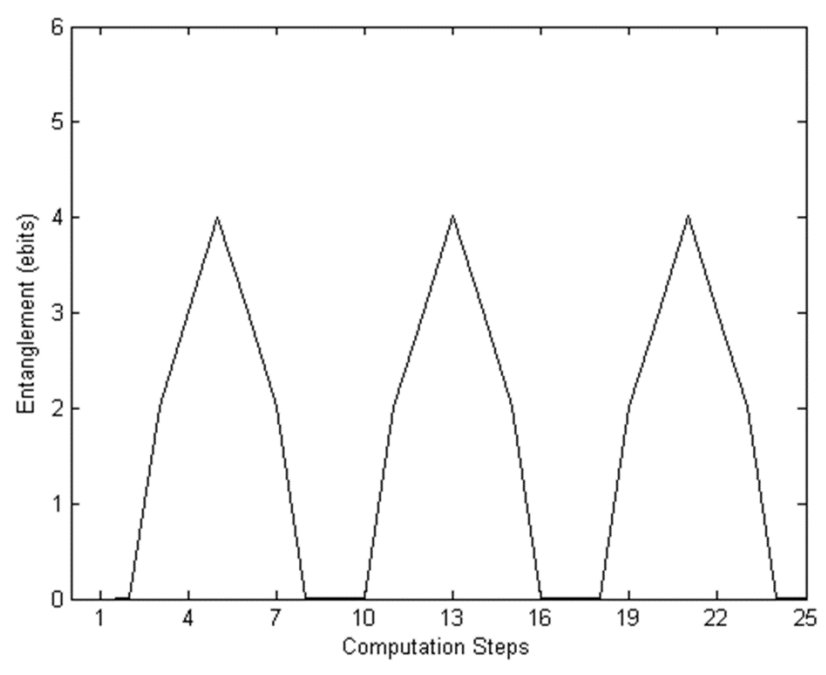
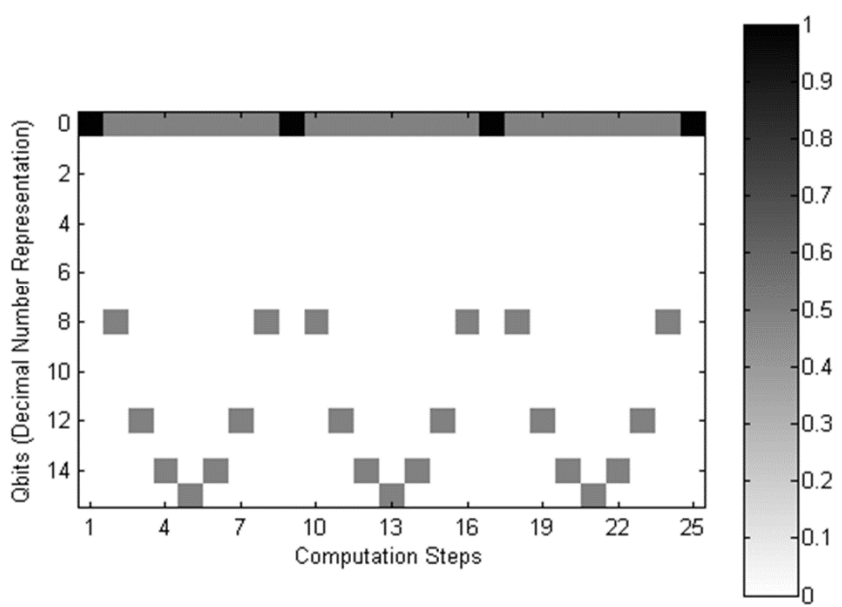
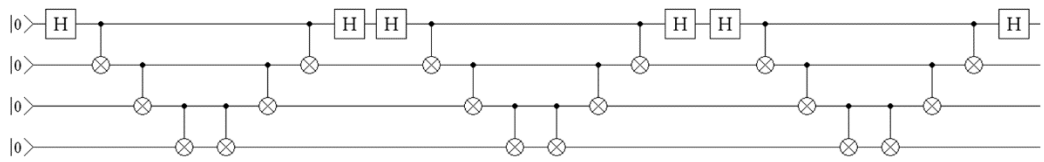
Σχήμα 6-4. Η μεταβολή της διεμπλοκής κατά τους κβαντικούς υπολογισμούς: αριστερά του Σχήματος 6-1 και δεξιά του Σχήματος 6-2.

Ο προσομοιωτής κβαντικού υπολογιστή QCS, υπολογίζει τη διεμπλοκή σε κάθε βήμα του κβαντικού υπολογισμού. Στα αριστερά και στα δεξιά του Σχήματος 6-4 φαίνεται η μεταβολή της διεμπλοκής κατά τους κβαντικούς υπολογισμούς των Σχημάτων 6-1 και 6-2 αντίστοιχα.

Στο πάνω τμήμα του Σχήματος 6-5 φαίνεται το κβαντικό κύκλωμα ενός κβαντικού υπολογισμού, στο μεσαίο η προσομοίωση του υπολογισμού και στο κάτω η μεταβολή της διεμπλοκής, όπως αυτά υπολογίστηκαν με χρήση του QCS.

6.4 Ο κβαντικός μετασχηματισμός Fourier

Ο κβαντικός μετασχηματισμός Fourier είναι ένας ορθομοναδιαίος τελεστής του χώρου Hilbert. Αποτελεί τη βάση για αρκετούς κβαντικούς αλγορίθμους, δρα σε κβαντικούς καταχωρητές μεταβάλλοντας τα πλάτη πιθανότητας και τις φάσεις των καταστάσεών τους, αποκαλύπτει την περιοδικότητα συναρτήσεων και προκαλεί αλληλεπιδράσεις μεταξύ qubits και μεταξύ κβαντικών καταχωρητών (Karafyllidis, 2003). Παρακάτω θα ορίσουμε τον κβαντικό μετασχηματισμό Fourier.



Σχήμα 6-5. Στο πάνω τμήμα του σχήματος φαίνεται το κβαντικό κύκλωμα ενός κβαντικού υπολογισμού, στο μεσαίο η προσομοίωση του υπολογισμού και στο κάτω η μεταβολή της διεμπλοκής, όπως αυτά υπολογίστηκαν με χρήση του QCS.

Θεωρούμε έναν κβαντικό καταχωρητή που αποτελείται από n qubits. Όπως γνωρίζουμε, οι βασικές καταστάσεις του στη δεκαδική αναπαράσταση είναι:

$$|0\rangle, |1\rangle, |2\rangle, \dots |a\rangle, \dots |N-2\rangle, |N-1\rangle \quad \text{όπου } N = 2^n - 1 \quad (6.22)$$

Ο κβαντικός μετασχηματισμός Fourier της τυχαίας βασικής κατάστασης $|a\rangle$ δίνεται από:

$$|a\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{c=0}^{N-1} e^{2\pi i \frac{ac}{N}} |c\rangle \quad (6.23)$$

όπου το (a, c) στον εκθέτη είναι ο πολλαπλασιασμός των δύο δεκαδικών αριθμών a και c . Εκτός από τις βασικές καταστάσεις, ο κβαντικός μετασχηματισμός Fourier μπορεί να δράσει και σε υπερθέσεις των βασικών καταστάσεων ενός κβαντικού καταχωρητή. Θεωρούμε την υπέρθεση βασικών καταστάσεων:

$$x_0|0\rangle + x_1|1\rangle + x_2|2\rangle + \dots + x_a|a\rangle + \dots + x_{N-1}|N-1\rangle = \sum_{a=0}^{N-1} x_a |a\rangle \quad (6.24)$$

Ο κβαντικός μετασχηματισμός Fourier της υπέρθεσης αυτής δίνεται από:

$$\sum_{a=0}^{N-1} x_a |a\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{c=0}^{N-1} \sum_{a=0}^{N-1} x_a e^{2\pi i \frac{ac}{N}} |c\rangle = \frac{1}{\sqrt{N}} \sum_{c=0}^{N-1} y_c |c\rangle \quad (6.25)$$

όπου το y_c , είναι ο κλασικός μετασχηματισμός Fourier του x_a και δίνεται από:

$$y_c = \sum_{a=0}^{N-1} e^{2\pi i \frac{ac}{N}} x_a \quad (6.26)$$

Για να καταλάβουμε καλύτερα τη δράση του κβαντικού μετασχηματισμού Fourier θα δούμε τρία παραδείγματα.

Παράδειγμα 6.2

Ποια είναι η δράση του κβαντικού μετασχηματισμού Fourier σε ένα qubit;

Ας υποθέσουμε ότι το qubit βρίσκεται στην κατάσταση $|0\rangle$. Τότε :

$$|0\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{c=0}^1 e^{2\pi i \frac{0c}{2}} |c\rangle = \frac{1}{\sqrt{2}} \sum_{c=0}^1 |c\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)$$

Αν το qubit βρίσκεται στην κατάσταση $|1\rangle$, τότε:

$$|1\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{c=0}^1 e^{2\pi i \frac{1c}{2}} |c\rangle = \frac{1}{\sqrt{2}} (|0\rangle + e^{\pi i} |1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Δηλαδή ο κβαντικός μετασχηματισμός Fourier δρα σε ένα qubit όπως η πύλη H . Για το λόγο αυτό η πύλη Hadamard αναφέρεται και ως «μετασχηματισμός Hadamard». ♦

Παράδειγμα 6.3

Στο παράδειγμα αυτό θα δούμε τη δράση του κβαντικού μετασχηματισμού Fourier σε έναν κβαντικό καταχωρητή που αποτελείται από δύο qubits και βρίσκεται στην κατάσταση $|10\rangle$ που αντιστοιχεί στο δεκαδικό $|2\rangle$:

$$|2\rangle \mapsto \frac{1}{\sqrt{4}} \sum_{c=0}^3 e^{2\pi i \frac{2c}{4}} |c\rangle = \frac{1}{2} (|0\rangle + e^{\pi i} |1\rangle + e^{2\pi i} |2\rangle + e^{3\pi i} |3\rangle) = \frac{1}{2} (|0\rangle - |1\rangle + |2\rangle - |3\rangle)$$

Αν ο κβαντικός καταχωρητής βρίσκεται στην κατάσταση $|01\rangle$, τότε:

$$|1\rangle \mapsto \frac{1}{\sqrt{4}} \sum_{c=0}^3 e^{2\pi i \frac{1c}{4}} |c\rangle = \frac{1}{2} \left(|0\rangle + e^{\frac{\pi i}{2}} |1\rangle + e^{\pi i} |2\rangle + e^{\frac{3\pi i}{2}} |3\rangle \right) = \frac{1}{2} (|0\rangle + i|1\rangle - |2\rangle - i|3\rangle) \blacklozenge$$

Παράδειγμα 6.4

Στο παράδειγμα αυτό θα δούμε τη δράση του κβαντικού μετασχηματισμού Fourier σε έναν κβαντικό καταχωρητή που αποτελείται από τρία qubits και βρίσκεται στην κατάσταση $|010\rangle$ που αντιστοιχεί στο δεκαδικό $|2\rangle$:

$$\begin{aligned} |2\rangle \mapsto \frac{1}{\sqrt{8}} \sum_{c=0}^7 e^{2\pi i \frac{2c}{8}} |c\rangle &= \frac{1}{\sqrt{8}} \left(|0\rangle + e^{\frac{\pi i}{2}} |1\rangle + e^{\pi i} |2\rangle + e^{\frac{3\pi i}{2}} |3\rangle + e^{2\pi i} |4\rangle + e^{\frac{5\pi i}{2}} |5\rangle + e^{3\pi i} |6\rangle + e^{\frac{7\pi i}{2}} |7\rangle \right) \\ &= \frac{1}{\sqrt{8}} (|0\rangle + i|1\rangle - |2\rangle - i|3\rangle + |4\rangle + i|5\rangle - |6\rangle - i|7\rangle) \end{aligned}$$

◆

Δηλαδή ο κβαντικός μετασχηματισμός Fourier μετασχηματίζει μία βασική κατάσταση ενός κβαντικού καταχωρητή σε υπέρθεση όλων των βασικών καταστάσεων, όπου όλες οι βασικές καταστάσεις έχουν το ίδιο πλάτος πιθανότητας αλλά διαφορετικές φάσεις.

Ο κβαντικός μετασχηματισμός Fourier είναι ένας ορθομοναδιαίος τελεστής που δρα στα διανύσματα καταστάσεως των qubits και των κβαντικών καταχωρητών. Η (6.23) μπορεί να γραφεί και ως εξής:

$$|a\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{c=0}^{N-1} \omega^{a \cdot c} |c\rangle \quad (6.27)$$

όπου :

$$\omega = e^{\frac{2\pi i}{N}} \quad (6.28)$$

Μετά από αυτό ο κβαντικός μετασχηματισμός Fourier των βασικών καταστάσεων ενός κβαντικού καταχωρητή γράφεται ως εξής:

$$|x_1\rangle \mapsto \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i \frac{x_1}{2}} |1\rangle \right) \quad (6.33)$$

Αν $|x_1\rangle = |0\rangle$, τότε :

$$|0\rangle \mapsto \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i \frac{0}{2}} |1\rangle \right) = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \quad (6.34)$$

Αν $|x_1\rangle = |1\rangle$, τότε :

$$|0\rangle \mapsto \frac{1}{\sqrt{2}} (|0\rangle + e^{\pi i} |1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \quad (6.35)$$

Αν ο κβαντικός καταχωρητής έχει δύο qubits, τα $|x_1 x_2\rangle$, τότε ο κβαντικός μετασχηματισμός Fourier μπορεί να γραφεί ως εξής:

$$|x_1 x_2\rangle \mapsto \frac{1}{2} \left(|0\rangle + e^{2\pi i \left[\frac{x_2}{2} \right]} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i \left[\frac{x_1 + x_2}{4} \right]} |1\rangle \right) \quad (6.36)$$

Θα εφαρμόσουμε την (6.36) στην περίπτωση που η κατάσταση του κβαντικού καταχωρητή είναι η $|01\rangle$ όπως στη δεύτερη περίπτωση του Παραδείγματος 6.3:

$$\begin{aligned} |01\rangle &\mapsto \frac{1}{2} \left(|0\rangle + e^{2\pi i \left[\frac{1}{2} \right]} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i \left[\frac{0+1}{4} \right]} |1\rangle \right) = \frac{1}{2} (|0\rangle + e^{\pi i} |1\rangle) \otimes (|0\rangle + e^{\pi i/2} |1\rangle) = \\ &= \frac{1}{2} (|00\rangle + e^{\pi i/2} |01\rangle + e^{\pi i} |10\rangle + e^{3\pi i/2} |11\rangle) = \frac{1}{2} (|00\rangle + i|01\rangle - |10\rangle - i|11\rangle) \end{aligned} \quad (6.37)$$

Θα χρησιμοποιήσουμε τον κλασματικό δυαδικό συμβολισμό:

$$[0.x_1 x_2 x_3 \dots x_m] = \sum_{k=1}^m \frac{x_k}{2^k} \quad (6.38)$$

Με τον συμβολισμό αυτό :

$$[0.x_2] = \frac{x_2}{2} \quad (\text{Προσοχή εδώ } m=1) \quad (6.39)$$

$$[0.x_1 x_2] = \frac{x_1}{2} + \frac{x_2}{2^2}$$

Χρησιμοποιώντας τον συμβολισμό αυτό η (6.36) γράφεται:

$$|x_1 x_2\rangle \mapsto \frac{1}{2} \left(|0\rangle + e^{2\pi i [0, x_2]} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i [0, x_1 x_2]} |1\rangle \right) \quad (6.40)$$

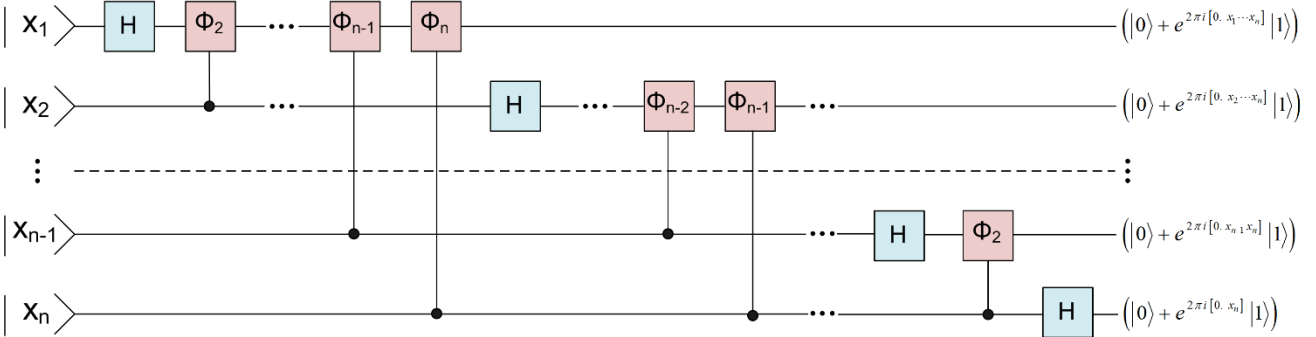
Ακολουθώντας αυτόν τον συμβολισμό, ο κβαντικός μετασχηματισμός Fourier για τη γενική περίπτωση ενός κβαντικού καταχωρητή με n qubits γράφεται:

$$|x_1 x_2 \dots x_j \dots x_n\rangle \mapsto \frac{1}{\sqrt{N}} \left(|0\rangle + e^{2\pi i [0, x_n]} |1\rangle \right) \otimes \left(|0\rangle + e^{2\pi i [0, x_{n-1} x_n]} |1\rangle \right) \otimes \dots \quad (6.41)$$

$$\dots \otimes \left(|0\rangle + e^{2\pi i [0, x_{n-j} x_{n-j+1} x_{n-j+2} \dots x_n]} |1\rangle \right) \otimes \dots \otimes \left(|0\rangle + e^{2\pi i [0, x_1 x_2 x_3 \dots x_n]} |1\rangle \right)$$

Από την (6.41) φαίνεται ότι το κβαντικό κύκλωμα του κβαντικού μετασχηματισμού Fourier θα περιλαμβάνει πύλες Hadamard που θα φέρνουν τα qubits σε υπερθέσεις των βασικών καταστάσεων και από πύλες ελεγχόμενης μετατόπισης φάσης που θα συνεισφέρουν τους εκθετικούς όρους. Το κβαντικό κύκλωμα του κβαντικού μετασχηματισμού Fourier φαίνεται στο Σχήμα 6-6. Στο κύκλωμα αυτό η ελεγχόμενη μετατόπιση φάσης, Φ_k , δίνεται από:

$$\Phi_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix} \quad (6.42)$$

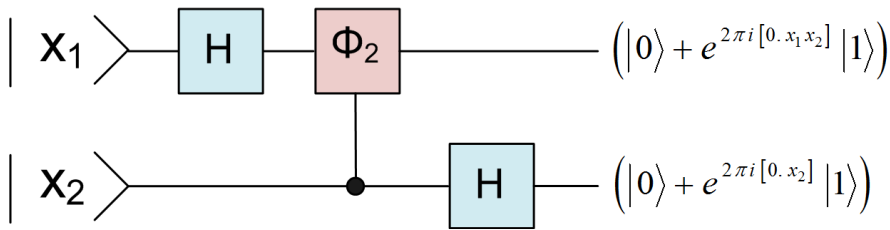


Σχήμα 6-6. Το κβαντικό κύκλωμα του κβαντικού μετασχηματισμού Fourier.

Το αποτέλεσμα του κβαντικού υπολογισμού του κβαντικού μετασχηματισμού Fourier είναι το ταυστικό γινόμενο των καταστάσεων στα δεξιά (στην «έξοδο») του κυκλώματος. Η σειρά των όρων του ταυστικού αυτού γινομένου θα πρέπει να τακτοποιηθεί για να υπάρχει αντιστοιχία με τις αρχικές καταστάσεις.

Παράδειγμα 6.5

Το κβαντικό κύκλωμα του κβαντικού μετασχηματισμού Fourier των καταστάσεων ενός κβαντικού καταχωρητή με δύο qubits $|x_1 x_2\rangle$ φαίνεται στο παρακάτω σχήμα:



Σχήμα 6-7. Το κβαντικό κύκλωμα του κβαντικού μετασχηματισμού Fourier για έναν κβαντικό καταχωρητή των δύο qubits.

Ο πίνακας του κβαντικού μετασχηματισμού Fourier είναι:

$$QFT = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^9 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{bmatrix}$$

◆

Βιβλιογραφία

- Aspect A., Dalibard J., & Roger G., Experimental test of Bell's inequalities using time-varying analyzers, *Physical Review Letters*, vol. 49, pp. 1804-1807, 1982.
- Bell J. S., On the Einstein-Podolsky-Rosen paradox, *Physics*, vol. 1, pp. 195-200, 1964.
- Bohm D. A suggested interpretation of the quantum theory in terms of "Hidden" variables, *Physical Review*, vol. 85, pp. 166-179, 1952.
- Brylinski R. K., & Goong Ch. (Eds), *Mathematics of quantum computation*, Chapman and Hall/CRC, 2002.
- Einstein A., Podolsky B., & Rosen N., Can quantum-mechanical description of physical reality be considered complete?, *Physical Review*, vol. 47, pp. 777-780, 1935.
- Heiss, D. (Ed.), *Fundamentals of quantum information*, Springer, 2002.
- Karafyllidis, I.G., Visualization of the quantum Fourier transform using a quantum computer simulator, *Quantum Information Processing*, vol. 2, pp. 271-288, 2003.
- Karafyllidis, I. G., Simulation of entanglement generation and variation in quantum computation, *Journal of Computational Physics*, vol. 200, pp. 383-397, 2004.
- Niesen M. A., & Chuang I. L., *Quantum computation and information*, Cambridge University Press, 2004.
- Schrödinger E., Probability relations between separated systems, *Proceedings of the Cambridge Philosophical Society*, vol. 31, pp. 555-563, 1935.

Ασκήσεις

Άσκηση 6.1

Να επιβεβαιώσετε την παραγωγή των καταστάσεων Bell:

$$|01\rangle \xrightarrow{E} \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$$

$$|10\rangle \xrightarrow{E} \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$$

$$|11\rangle \xrightarrow{E} \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$

εκτελώντας τους κβαντικούς υπολογισμούς και χρησιμοποιώντας τον προσομοιωτή QCS.

Άσκηση 6.2

Να δείξετε ότι η παρακάτω κατάσταση δεν είναι κατάσταση κβαντικής διεμπλοκής.

$$|q\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Άσκηση 6.3

Να δείξετε ότι η παρακάτω κατάσταση είναι κατάσταση κβαντικής διεμπλοκής.

$$|q\rangle = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

Άσκηση 6.4

Να χρησιμοποιήσετε τον προσομοιωτή QCS, για να παράγετε καταστάσεις GHZ, όταν οι αρχικές καταστάσεις των qubits είναι $|101\rangle$ και $|111\rangle$.

Άσκηση 6.5

Να χρησιμοποιήσετε τον προσομοιωτή QCS, για να παράγετε καταστάσεις κβαντικής διεμπλοκής τεσσάρων qubits, όταν οι αρχικές τους καταστάσεις είναι $|1010\rangle$ και $|0100\rangle$.

Άσκηση 6.6

Δίνεται η κατάσταση ενός qubit: $|q\rangle = e^{-i\phi} \sin \mathcal{G} |0\rangle + \cos \mathcal{G} |1\rangle$. Να βρείτε τον πίνακα πυκνότητας, να αποδείξετε ότι είναι Ερμιτιανός και να υπολογίσετε το ίχνος του.

Άσκηση 6.7

Δίνονται οι παρακάτω καταστάσεις δύο qubits:

$$|q_A\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

$$|q_B\rangle = \sqrt{\frac{2}{3}}|0\rangle + \frac{1}{\sqrt{3}}|1\rangle$$

Να βρείτε την κατάσταση: $|q_A q_B\rangle$, να υπολογίσετε τον πίνακα πυκνότητας και να βρείτε αν είναι μικτή ή καθαρή.

Άσκηση 6.8

Δίνονται οι παρακάτω καταστάσεις δύο qubits:

$$|q_A\rangle = |0\rangle$$

$$|q_B\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Οι δύο αυτές καταστάσεις αποτελούν μία μικτή κατάσταση με $p_1 = p_2 = 0,5$. Να υπολογίσετε την εντροπία von Neumann της μικτής κατάστασης.

Άσκηση 6.9

Να υπολογίσετε τη δράση του κβαντικού μετασχηματισμού Fourier σε έναν κβαντικό καταχωρητή που αποτελείται από δύο qubits και βρίσκεται στην κατάσταση $|11\rangle$.

Άσκηση 6.10

Να υπολογίσετε τη δράση του κβαντικού μετασχηματισμού Fourier σε έναν κβαντικό καταχωρητή που αποτελείται από τρία qubits και βρίσκεται στην κατάσταση $|011\rangle$.

Άσκηση 6.11

Να σχεδιάσετε το κβαντικό κύκλωμα του κβαντικού μετασχηματισμού Fourier των καταστάσεων ενός κβαντικού καταχωρητή με τρία qubits, να γράψετε τον πίνακα και βρείτε το αποτέλεσμα του κβαντικού υπολογισμού.

7. Ο κβαντικός αλγόριθμος του Shor

Σύνοψη

Ο κβαντικός αλγόριθμος του Shor μπορεί να χρησιμοποιηθεί για την εύρεση της περιόδου περιοδικών συναρτήσεων και για την ανάλυση ενός αριθμού σε γινόμενο πρώτων παραγόντων. Στο κεφάλαιο αυτό θα περιγραφεί ποιοτικά ο αλγόριθμος του Shor και θα δοθούν τα βήματά του. Στη συνέχεια θα περιγραφεί μαθηματικά ο κβαντικός αλγόριθμος. Θα δοθεί αναλυτικό παράδειγμα εφαρμογής του κβαντικού αλγορίθμου του Shor.

Προαπαιτούμενη γνώση

Γραμμική Άλγεβρα και το πρώτο, δεύτερο, τρίτο και έκτο κεφάλαιο του βιβλίου αυτού.

7.1 Το κρυπτογραφικό σύστημα RSA

Ένα από τα πιο επιτυχημένα κρυπτογραφικά συστήματα είναι το κρυπτογραφικό σύστημα RSA, που επινοήθηκε το 1978 από τους Ronald Rivest, Adi Shamir και Leonard Adelman και πήρε το όνομά του από τα αρχικά των επιθέτων τους. Το RSA είναι ένα κρυπτογραφικό σύστημα με δημόσιο κλειδί και θεωρείται ότι είναι αδύνατον να σπάσει με τη χρήση κλασικών υπολογιστών (Rivest, Shamir & Adelman, 1978). Σήμερα χρησιμοποιείται ευρύτατα κυρίως στις οικονομικές και τραπεζικές συναλλαγές.

Αν και η κρυπτογραφία δεν αποτελεί αντικείμενο του βιβλίου αυτού, θα κάνουμε μία πολύ σύντομη περιγραφή της βασικής δομής του κρυπτογραφικού συστήματος RSA, για να φανεί πώς μπορεί να σπάσει με τη χρήση ενός κβαντικού υπολογιστή και του αλγορίθμου του Shor τον οποίο θα περιγράψουμε αμέσως μετά. Η βασική δομή του RSA είναι η εξής:

- Επιλέγονται δύο ακέραιοι πρώτοι αριθμοί ο p και q και υπολογίζεται το γινόμενό τους $n = p \cdot q$.
- Επιλέγεται ένας τυχαίος αριθμός ο d , ο οποίος είναι πρώτος ως προς τους $(p-1)$ και $(q-1)$, δηλαδή ο μέγιστος κοινός διαιρέτης των d , $(p-1)$ και $(q-1)$ είναι το ένα.
- Υπολογίζεται ο αριθμός e από τη σχέση: $e \cdot d \mid_{\text{mod } (p-1)(q-1)} = 1$. Δηλαδή, ο e είναι ο αντίστροφος του d , $\text{mod } (p-1)(q-1)$.
- Το ζεύγος των αριθμών (e, n) είναι το δημόσιο κλειδί.
- Το ζεύγος των αριθμών (d, n) είναι το ιδιωτικό κλειδί.

Το δημόσιο κλειδί στέλνεται στον αποστολέα του μηνύματος (π.χ. στον πελάτη της τράπεζας που θέλει να κάνει μία συναλλαγή μέσω του διαδικτύου). Το ιδιωτικό κλειδί το κρατά ο παραλήπτης του μηνύματος (π.χ. η τράπεζα). Ο αποστολέας κωδικοποιεί το μήνυμα (π.χ. τα στοιχεία της συναλλαγής) με το δημόσιο κλειδί και στέλνει το μήνυμα στον παραλήπτη. Για να αποκωδικοποιηθεί το μήνυμα, χρειάζεται και το δημόσιο και το ιδιωτικό κλειδί. Το ιδιωτικό κλειδί δεν φεύγει ποτέ από τον παραλήπτη, οπότε δεν υπάρχει κίνδυνος υποκλοπής.

Μία καλή ερμηνεία του κρυπτογραφικού συστήματος RSA υπάρχει στο βιβλίο του S. Singh “*The Code Book*”, εκδόσεις Doubleday, 1999. Σύμφωνα με αυτή, ο παραλήπτης του μηνύματος (η τράπεζα) στέλνει στον αποστολέα (στον πελάτη) ένα κιβώτιο που κλειδώνει με ένα λουκέτο. Το λουκέτο είναι ανοιχτό και ο παραλήπτης κρατάει το κλειδί του. Ο αποστολέας παραλαμβάνει το κιβώτιο με το λουκέτο ανοιχτό, βάζει μέσα το μήνυμά του και κλειδώνει το λουκέτο. Τώρα δεν μπορεί κανείς, ούτε ο ίδιος ο αποστολέας, να το ανοίξει. Στη συνέχεια στέλνει το κλειδωμένο κιβώτιο στον παραλήπτη ο οποίος με το κλειδί ανοίγει το λουκέτο και βγάζει το μήνυμα από το κιβώτιο. Στο ερμηνευτικό αυτό μοντέλο το λουκέτο είναι το ζεύγος των αριθμών (e, n) , και το κλειδί του λουκέτου είναι το ζεύγος των αριθμών (d, n) .

Ας δούμε πώς μπορείτε να σπάσετε το σύστημα RSA, δηλαδή τι πρέπει να κάνετε, για να αποκρυπτογραφήσετε ένα μήνυμα που κρυπτογραφήθηκε με το σύστημα RSA. Μπορείτε πολύ εύκολα να βρείτε το δημόσιο κλειδί, δηλαδή το ζεύγος των αριθμών (e, n) . Αφού τώρα γνωρίζετε τον αριθμό n , δεν έχετε παρά να τον αναλύσετε σε γινόμενο δύο πρώτων αριθμών για να βρείτε τους αριθμούς p και q . Μόλις τους βρείτε, η αποκρυπτογράφηση γίνεται αμέσως, αφού η μέθοδος του συστήματος RSA είναι γνωστή.

Θα περιγράψουμε τον περισσότερο χρησιμοποιούμενο αλγόριθμο για την ανάλυση ενός αριθμού σε γινόμενο δύο πρώτων αριθμών. Αν δοθεί ένας ακέραιος αριθμός n , ο οποίος πρέπει να αναλυθεί σε γινόμενο δύο πρώτων αριθμών, τότε υπολογίζεται η περίοδος r της περιοδικής συνάρτησης $f_{n,a}(x) = a^x \pmod{n}$, όπου, $x = 0, 1, 2, 3, \dots$ και a είναι ένας τυχαίος ακέραιος που είναι πρώτος ως προς τον n . Ο πρώτος παράγοντας του n είναι ο μέγιστος κοινός διαιρέτης (ΜΚΔ) του n και του $(a^{r/2} - 1)$, και ο δεύτερος ο ΜΚΔ του n και του $(a^{r/2} + 1)$. Δηλαδή, το πρόβλημα της ανάλυσης ενός αριθμού σε γινόμενο δύο πρώτων αριθμών ανάγεται στο πρόβλημα της εύρεσης της περιόδου μιας περιοδικής συνάρτησης. Για να λυθεί αυτό πρόβλημα με έναν κλασικό υπολογιστή, απαιτείται εκθετική αύξηση του χρόνου υπολογισμού για γραμμική αύξηση του μεγέθους του n , δηλαδή του αριθμού των ψηφίων του (Lo, Popescu & Spiller, 1998).

Παράδειγμα 7.1

Να αναλυθεί ο αριθμός 15 σε γινόμενο δύο πρώτων αριθμών.

Επιλέγουμε τυχαία τον αριθμό $a = 2$, $\text{ΜΚΔ}(2, 15) = 1$. Οπότε:

$$f_{15,2}(0) = 2^0 \pmod{15} = 0, \quad f_{15,2}(1) = 2^1 \pmod{15} = 2, \quad f_{15,2}(2) = 2^2 \pmod{15} = 4, \quad f_{15,2}(3) = 2^3 \pmod{15} = 8,$$

$$f_{15,2}(4) = 2^4 \pmod{15} = 1, \quad f_{15,2}(5) = 2^5 \pmod{15} = 2, \quad f_{15,2}(6) = 2^6 \pmod{15} = 4, \quad f_{15,2}(7) = 2^7 \pmod{15} = 8, \dots$$

Η συνάρτηση έχει περίοδο $r = 4$, οπότε $\text{ΜΚΔ}\{(2^{4/2} - 1), n\} = 3$ και $\text{ΜΚΔ}\{(2^{4/2} + 1), n\} = 5$, δηλαδή $15 = 3 \times 5$. ♦

Ενώ είναι πολύ εύκολο να πολλαπλασιάσετε δύο πρώτους αριθμούς για να βρείτε το γινόμενό τους, είναι πάρα πολύ δύσκολο να αναλύσετε έναν αριθμό σε γινόμενο δύο πρώτων αριθμών και είναι πρακτικά αδύνατο αν ο αριθμός έχει πολλά ψηφία (Stolze & Suter, 2008).

Για να αποδείξουν ότι το κρυπτογραφικό τους σύστημα δεν μπορεί να σπάσει, οι Rivest, Shamir και Adelman ζήτησαν από όποιον νομίζει ότι μπορεί να αναλύσει σε γινόμενο δύο πρώτων αριθμών έναν ακέραιο με 129 ψηφία. Μετά από 17 χρόνια ο αριθμός αναλύθηκε από ένα δίκτυο 1.600 κλασικών υπολογιστών. Σύμφωνα με τον U. Vazirani: «ακόμη και αν κάθε σωματίδιο στο σύμπαν ήταν ένας κλασικός υπολογιστής ο οποίος θα λειτουργούσε για όλη τη μέχρι τώρα ζωή του σύμπαντος, δεν θα ήταν δυνατό να αναλυθεί σε γινόμενο δύο πρώτων αριθμών ένας ακέραιος αριθμός με 2.000 ψηφία».

Αυτό που χρειάζεται να θυμόμαστε είναι ότι το πρόβλημα της ανάλυσης ενός αριθμού σε γινόμενο δύο πρώτων αριθμών ανάγεται στο πρόβλημα εύρεσης της περιόδου μιας περιοδικής συνάρτησης και ότι το πρόβλημα αυτό είναι αδύνατο να λυθεί με τη χρήση κλασικών υπολογιστών, όταν ο αριθμός έχει πολλά ψηφία.

Όμως, το 1994 ο Peter Shor τα άλλαξε όλα αυτά αποδεικνύοντας ότι με τη χρήση κβαντικών υπολογιστών μπορεί εύκολα και γρήγορα να βρεθεί η περίοδος περιοδικών συναρτήσεων, δηλαδή να αναλυθούν σε γινόμενο δύο πρώτων αριθμών μεγάλοι ακέραιοι αριθμοί (Shor, 1994). Με έναν κβαντικό υπολογιστή απαιτείται πολυωνυμική αύξηση του χρόνου υπολογισμού για γραμμική αύξηση του μεγέθους του n , δηλαδή του αριθμού των ψηφίων του. Η μέθοδος που πρότεινε ο Shor είναι γνωστή ως «κβαντικός αλγόριθμος του Shor».

7.2 Περιγραφή του κβαντικού αλγορίθμου του Shor

Το πρόβλημα που λύνει ο κβαντικός αλγόριθμος του Shor είναι το εξής:

Αν δοθεί ένας ακέραιος αριθμός n , να βρεθεί η περίοδος της συνάρτησης $f_{n,a}(x) = a^x \pmod{n}$. Όπου a είναι ένας τυχαίος ακέραιος που είναι πρώτος ως προς τον n .

Θα δώσουμε πρώτα μία «ποιοτική» περιγραφή του αλγορίθμου και στη συνέχεια θα δώσουμε τα βήματα του και τη μαθηματική τους περιγραφή. Ο κβαντικός αλγόριθμος του Shor αρχίζει με δύο κβαντικούς καταχωρητές. Ο πρώτος ονομάζεται *Reg1* και ο δεύτερος *Reg2*. Οι δύο κβαντικοί καταχωρητές αποτελούν έναν

κβαντικό καταχωρητή που τον ονομάζουμε *Reg*. Αν η κατάσταση του *Reg1* είναι $|\psi_1\rangle$ και η κατάστασή του *Reg2* είναι $|\psi_2\rangle$, η κατάσταση του *Reg*, η $|\psi\rangle$, δίνεται από:

$$|\psi\rangle = |\psi_1\rangle |\psi_2\rangle = |\psi_1 \psi_2\rangle = |\psi_1, \psi_2\rangle \quad (7.1)$$

Προσέξτε ότι το κόμμα ανάμεσα στις καταστάσεις των *Reg1* και *Reg2* χρησιμοποιείται μόνο και μόνο για τη διευκόλυνση της ανάγνωσης και δε σημαίνει τίποτε. Οι καταστάσεις από εδώ και εμπρός θα δίνονται στη δεκαδική αναπαράσταση. Η αρχική κατάσταση του *Reg* είναι:

$$|\psi\rangle = |0, 0\rangle \quad (7.2)$$

Για να αναλύσουμε τον ακέραιο αριθμό n σε γινόμενο δύο πρώτων αριθμών, επιλέγουμε έναν ακέραιο αριθμό τον q , τέτοιο ώστε:

$$2n^2 \leq q \leq 3n^2 \quad (7.3)$$

Στη συνέχεια επιλέγουμε τυχαία έναν αριθμό, τον a , που είναι πρώτος ως προς τον n .

Φέρνουμε τον *Reg1* σε κατάσταση υπέρθεσης όλων των βασικών καταστάσεων από 0 έως $q-1$. Φυσικά έχουμε φροντίσει ο *Reg1* να αποτελείται από τον κατάλληλο αριθμό qubits. Δηλαδή, στον *Reg1* δημιουργούμε την υπέρθεση των ακεραίων αριθμών $x = 0, 1, 2, 3, \dots, q-1$, οι οποίοι θα χρησιμοποιηθούν ως οι ανεξάρτητες μεταβλητές της συνάρτησης $f_{n,a}(x) = a^x \pmod{n}$ της οποίας θέλουμε να βρούμε την περίοδο.

Στη συνέχεια με χρήση της κβαντικής παραλληλίας υπολογίζεται η τιμή της $f_{n,a}(x)$ για κάθε x και τα αποτελέσματα καταγράφονται στον *Reg2* ο οποίος κρατά πλέον την υπέρθεση όλων των τιμών της $f_{n,a}(x)$. Πρέπει εδώ να επισημάνουμε ότι μετά από αυτό, η κατάσταση του *Reg* δεν μπορεί να γραφεί ως ταυστικό γινόμενο των καταστάσεων των *Reg1* και *Reg2*. Δηλαδή, οι καταχωρητές βρίσκονται σε κβαντική διεμπλοκή, οπότε η μέτρηση της κατάστασης του ενός καθορίζει την κατάσταση του άλλου.

Κατόπιν γίνεται μέτρηση της κατάστασης του *Reg2*. Ο *Reg2* βρίσκεται σε υπέρθεση όλων των τιμών της $f_{n,a}(x)$, όμως το αποτέλεσμα της μέτρησης θα δώσει μόνο μία τιμή της συνάρτησης, ας πούμε την k . Δηλαδή, μετά τη μέτρηση ο *Reg2* βρίσκεται στην κατάσταση $|k\rangle$.

Θυμηθείτε ότι η μέτρηση της κατάστασης του *Reg2* καθορίζει την κατάσταση του *Reg1*, αφού οι δύο καταχωρητές βρίσκονται σε κβαντική διεμπλοκή. Τι σημαίνει αυτό; Σημαίνει, ότι αφού ο *Reg2* βρίσκεται στην κατάσταση $|k\rangle$, εξαιτίας της κβαντικής διεμπλοκής στον *Reg1* θα βρίσκονται πια μόνο οι αριθμοί x για τους οποίους ισχύει:

$$f_{n,a}(x) = a^x \pmod{n} = k \quad (7.4)$$

Δηλαδή, στον *Reg1* θα υπάρχουν ως υπέρθεση καταστάσεων οι αριθμοί $\{x, x+r, x+2r, x+3r, \dots\}$. Τα πλάτη πιθανότητας όλων των καταστάσεων είναι ίσα μεταξύ τους. Φυσικά, r είναι η ζητούμενη περίοδος της συνάρτησης.

Δεν τελειώσαμε όμως. Θα μπορούσαμε να βρούμε αμέσως την περίοδο r , αν ήταν δυνατόν να γίνουν δύο μετρήσεις οι οποίες θα δώσουν δύο διαδοχικούς αριθμούς που βρίσκονται ως υπέρθεση καταστάσεων στον *Reg1*, για παράδειγμα των $x+2r$ και $x+3r$. Όμως, είναι αδύνατον να πραγματοποιηθούν δύο τέτοιες μετρήσεις, γιατί η πρώτη μέτρηση θα έδινε μόνο έναν αριθμό και θα προκαλούσε καταστροφή της υπέρθεσης, καθιστώντας έτσι κάθε άλλη μέτρηση αδύνατη, αφού κάθε άλλη μέτρηση θα έδινε τον ίδιο αριθμό με την πρώτη μέτρηση.

Πώς μπορούμε να βρούμε την περίοδο r χωρίς να καταστρέψουμε την υπέρθεση στον *Reg1*; Χρησιμοποιώντας τον κβαντικό μετασχηματισμό Fourier.

Ο κβαντικός μετασχηματισμός Fourier δρα στον *Reg1*. Όπως και στην κλασική περίπτωση, ο κβαντικός μετασχηματισμός Fourier των περιεχομένων του *Reg1* θα έχει κορυφές στα ακέραια πολλαπλάσια της αντίστροφης περιόδου $1/r$. Αυτό συμβαίνει, γιατί ο κβαντικός μετασχηματισμός Fourier της υπέρθεσης

καταστάσεων που αντιστοιχούν στους αριθμούς $\{x, x+r, x+2r, x+3r, \dots\}$ έχει ως αποτέλεσμα μία νέα υπέρθεση καταστάσεων, στην οποία όμως τα πλάτη πιθανότητας των καταστάσεων δεν είναι πλέον ίσα. Τα πλάτη των καταστάσεων που αντιστοιχούν σε ακέραια πολλαπλάσια της αντίστροφης περιόδου $1/r$ είναι πολύ μεγαλύτερα από τα υπόλοιπα και, επομένως, μία μέτρηση της κατάστασης του *Reg1* είναι πρακτικά βέβαιο ότι θα δώσει αποτέλεσμα που θα είναι ακέραιο πολλαπλάσιο της αντίστροφης περιόδου. Τα βήματα του κβαντικού αλγορίθμου επαναλαμβάνονται αρκετές φορές (περίπου $\log(q)$ φορές), ώστε να ληφθούν αρκετά δείγματα ακεραίων πολλαπλασίων της αντίστροφης περιόδου, για να είναι δυνατός ο ακριβής υπολογισμός της.

7.3 Τα βήματα του κβαντικού αλγορίθμου του Shor

Έστω ότι θέλουμε να αναλύσουμε τον ακέραιο αριθμό n σε γινόμενο δύο πρώτων αριθμών. Για να το επιτύχουμε αυτό, θα υπολογίσουμε την περίοδο της συνάρτησης $f_{n,a}(x) = a^x \pmod n$.

Βήμα 1ο.

Επιλέγεται ένας ακέραιος αριθμός q τέτοιος ώστε $2n^2 \leq q \leq 3n^2$.

Βήμα 2ο.

Επιλέγεται τυχαία ένας ακέραιος αριθμός a που είναι πρώτος ως προς τον n .

Βήμα 3ο.

Ένας κβαντικός καταχωρητής, ο *Reg*, αποτελείται από δύο καταχωρητές, που ονομάζονται *Reg1* και *Reg2*, οι οποίοι βρίσκονται στην κατάσταση $|0\rangle$. Η κατάσταση του *Reg*, η $|\psi\rangle$, είναι:

$$|\psi\rangle = |0, 0\rangle \quad (7.5)$$

Βήμα 4ο.

Φέρνουμε τον *Reg1* σε κατάσταση υπέρθεσης όλων των βασικών καταστάσεων από 0 έως $q-1$. Δεν δρούμε στον *Reg2*. Μετά από αυτό, η κατάσταση του *Reg* δίνεται από:

$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x, 0\rangle \quad (7.6)$$

Βήμα 5ο.

Στη συνέχεια, με χρήση της κβαντικής παραλληλίας υπολογίζεται η τιμή της $f_{n,a}(x)$ για κάθε x και τα αποτελέσματα καταγράφονται στον *Reg2* ο οποίος κρατά πλέον την υπέρθεση όλων των τιμών της $f_{n,a}(x)$. Τώρα η κατάσταση του *Reg* δίνεται από:

$$|\psi\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x, a^x \pmod n\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x, f_{n,a}(x)\rangle \quad (7.7)$$

Οι καταχωρητές *Reg1* και *Reg2* βρίσκονται πλέον σε κβαντική διεμπλοκή.

Βήμα 6ο.

Μετράται η κατάσταση του $Reg2$. Ο $Reg2$ βρίσκεται σε υπέρθεση όλων των τιμών της $f_{n,a}(x)$, όμως το αποτέλεσμα της μέτρησης θα δώσει μόνο μία τιμή της συνάρτησης, ας πούμε την k . Δηλαδή, μετά τη μέτρηση ο $Reg2$ βρίσκεται στην κατάσταση $|k\rangle$. Η μέτρηση της κατάστασης του $Reg2$ καθορίζει την κατάσταση του $Reg1$. Δηλαδή, εξαιτίας της κβαντικής διεμπλοκής στον $Reg1$ θα βρίσκονται πια μόνο οι αριθμοί x για τους οποίους ισχύει: $f_{n,a}(x)=a^x \pmod n=k$. Οι αριθμοί αυτοί συμβολίζονται με x' και αποτελούν ένα σύνολο A που περιγράφεται ως εξής:

$$A = \{x' : a^{x'} \pmod n = k\} \quad (7.8)$$

Έστω ότι $\|A\|$ είναι ο αριθμός των στοιχείων του συνόλου A . Μετά τη μέτρηση η κατάσταση του Reg δίνεται από:

$$|\psi\rangle = \frac{1}{\sqrt{\|A\|}} \sum_{x' \in A} |x', k\rangle \quad (7.9)$$

Δηλαδή, αθροίζονται οι καταστάσεις που ανήκουν στο σύνολο A .

Βήμα 7ο.

Ο κβαντικός μετασχηματισμός Fourier δρα στον $Reg1$, ενώ το περιεχόμενο του $Reg2$ παραμένει αμετάβλητο. Ο κβαντικός μετασχηματισμός Fourier μετασχηματίζει κάθε κατάσταση $|x'\rangle$ σε μία υπέρθεση καταστάσεων που δίνεται από:

$$|x'\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i \frac{x'c}{q}} |c\rangle \quad (7.10)$$

Μετά την εφαρμογή του κβαντικού μετασχηματισμού Fourier η κατάσταση του Reg είναι:

$$|\psi\rangle = \frac{1}{\sqrt{\|A\|}} \sum_{x' \in A} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i \frac{x'c}{q}} |c, k\rangle \quad (7.11)$$

Βήμα 8ο.

Μετράται η κατάσταση του $Reg1$. Το αποτέλεσμα της μέτρησης δίνει μία μόνο τιμή, την c' , η οποία είναι κάποιο ακέραιο πολλαπλάσιο λ του q/r , όπου r είναι η περίοδος που πρέπει να προσδιοριστεί, δηλαδή:

$$c' = \lambda \frac{q}{r} \quad (7.12)$$

Βήμα 9ο.

Τα βήματα 3 έως και 8 επαναλαμβάνονται περίπου $\log(q)$ φορές. Η επανάληψη αυτή δίνει αρκετά δείγματα πολλαπλασίων του $1/r$, δηλαδή, δίνει τιμές $\lambda_1/r, \lambda_2/r, \lambda_3/r, \dots$ όπου λ_i είναι διάφοροι ακέραιοι, ώστε να είναι δυνατός ο υπολογισμός της r .

Αφού προσδιοριστεί η r , οι δύο πρώτοι αριθμοί που το γινόμενο τους δίνει τον n προσδιορίζονται υπολογίζοντας τον ΜΚΔ του n και του $(a^{r/2} - 1)$, και τον ΜΚΔ του n και του $(a^{r/2} + 1)$.

7.4 Παράδειγμα και ερμηνεία του κβαντικού αλγορίθμου του Shor

Οι κβαντικοί υπολογισμοί που γίνονται κατά την εκτέλεση του κβαντικού αλγορίθμου του Shor έχουν ως αποτέλεσμα όχι μόνο τη μεταβολή των πλατών πιθανότητας των καταστάσεων των *Reg1* και *Reg2*, αλλά και τη μεταβολή των φάσεών τους. Θα προσπαθήσουμε να ερμηνεύσουμε τον κβαντικό αλγόριθμο του Shor περιγράφοντας κυρίως τις μεταβολές των φάσεων και χρησιμοποιώντας ένα παράδειγμα. Αντί για τη συνάρτηση $f_{n,a}(x) = a^x \pmod{n}$ θα υπολογίσουμε την περίοδο μιας τριγωνομετρικής συνάρτησης που είναι πιο κατάλληλη ως παράδειγμα:

Να βρεθεί η περίοδος της συνάρτησης $f(x) = \cos(\pi x) + 1$. Όπου $x = 0, 1, 2, \dots, q-1$.

Στο 1ο βήμα επιλέγεται τυχαία ένας αριθμός q . Ο αριθμός αυτός πρέπει να είναι αρκετά μεγάλος, ώστε η $f(x)$ να κάνει τουλάχιστον δύο περιόδους. Για το συγκεκριμένο παράδειγμα επιλέγεται $q=8$.

Το 2ο βήμα δεν χρειάζεται για τη συνάρτηση του παραδείγματος.

Στο 3ο βήμα επιλέγεται το μέγεθος του κβαντικού καταχωρητή *Reg* που αποτελείται από δύο κβαντικούς καταχωρητές, τους *Reg1* και *Reg2*. Ο καταχωρητής *Reg1* θα κρατά τις τιμές του x , οπότε 3 qubits είναι αρκετά. Ο *Reg2* θα κρατά τις τιμές της συνάρτησης η οποία παίρνει μόνο τις τιμές 0 και 2, οπότε θα πρέπει να αποτελείται από 2 qubits.

Για παράδειγμα, αν το x πάρει την τιμή 5, τότε $f(x) = 0$, οπότε η κατάσταση του *Reg* είναι η: $|x, f(x)\rangle = |101, 00\rangle$ ή $|x, f(x)\rangle = |5, 0\rangle$ σε δεκαδική αναπαράσταση.

Στο 4ο βήμα ο *Reg1* οδηγείται σε κατάσταση υπέρθεσης όλων των βασικών καταστάσεων από 0 έως $q-1$. Καμία δράση στον *Reg2*. Μετά από αυτό η κατάσταση του *Reg* είναι:

$$|\psi\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^7 |x, 0\rangle = \frac{1}{\sqrt{8}} (|0, 0\rangle + |1, 0\rangle + |2, 0\rangle + \dots + |7, 0\rangle) \quad (7.13)$$

Στο 5ο βήμα με χρήση της κβαντικής παραλληλίας υπολογίζονται οι τιμές της $f(x) = \cos(\pi x) + 1$ για όλους τους ακέραιους x από 0 έως 7 και τα αποτελέσματα καταγράφονται στον *Reg2*, ο οποίος κρατά πλέον την υπέρθεση όλων των τιμών της $f(x)$. Οι *Reg1* και *Reg2* βρίσκονται πλέον σε κβαντική διεμπλοκή. Τώρα η κατάσταση του *Reg* δίνεται από:

$$|\psi\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^7 |x, f(x)\rangle = \frac{1}{\sqrt{8}} (|0, f(0)\rangle + |1, f(1)\rangle + |2, f(2)\rangle + \dots + |7, f(7)\rangle) \quad (7.14)$$

Στο 6ο βήμα μετράται η κατάσταση του *Reg2*. Έστω ότι η μέτρηση έδωσε την τιμή 2. Δηλαδή, μετά τη μέτρηση ο *Reg2* βρίσκεται στην κατάσταση $|2\rangle$. Η μέτρηση της κατάστασης του *Reg2* καθορίζει την κατάσταση του *Reg1*. Εξαιτίας της κβαντικής διεμπλοκής στον *Reg1* θα βρίσκονται πια μόνο οι αριθμοί x για τους οποίους ισχύει: $f(x) = 2$. Οι αριθμοί αυτοί συμβολίζονται με x' και αποτελούν ένα σύνολο:

$$A = \{0, 2, 4, 6\}.$$

Μετά από αυτό η κατάσταση του *Reg* είναι:

$$|\psi\rangle = \frac{1}{2} \sum_{x' \in A} |x', f(x')\rangle = \frac{1}{2} (|0, 2\rangle + |2, 2\rangle + |4, 2\rangle + |6, 2\rangle) \quad (7.15)$$

Στο 7ο βήμα ο κβαντικός μετασχηματισμός Fourier δρα στον *Reg1*, ενώ το περιεχόμενο του *Reg2* παραμένει αμετάβλητο. Μετά από αυτό η κατάσταση του *Reg* δίνεται από:

$$\begin{aligned}
 |\psi\rangle = \frac{1}{2} \sum_{x' \in A} \frac{1}{\sqrt{8}} \sum_{c=0}^7 e^{2\pi i \frac{x'c}{8}} |c, 2\rangle &= \frac{1}{\sqrt{32}} \{ |0, 2\rangle + |1, 2\rangle + \dots + |7, 2\rangle \} + \\
 &+ \frac{1}{\sqrt{32}} \{ |0, 2\rangle + e^{\pi i/2} |1, 2\rangle + \dots + e^{7\pi i/2} |7, 2\rangle \} + \\
 &+ \frac{1}{\sqrt{32}} \{ |0, 2\rangle + e^{\pi i} |1, 2\rangle + \dots + e^{7\pi i} |7, 2\rangle \} + \\
 &+ \frac{1}{\sqrt{32}} \{ |0, 2\rangle + e^{3\pi i/2} |1, 2\rangle + \dots + e^{21\pi i/2} |7, 2\rangle \}
 \end{aligned} \tag{7.16}$$

	$ 0, 2\rangle$	$ 1, 2\rangle$	$ 2, 2\rangle$	$ 3, 2\rangle$	$ 4, 2\rangle$	$ 5, 2\rangle$	$ 6, 2\rangle$	$ 7, 2\rangle$
$x' = 0$	0	0	0	0	0	0	0	0
$x' = 2$	0	$\pi/2$	π	$3\pi/2$	2π	$5\pi/2$	3π	$7\pi/2$
$x' = 4$	0	π	2π	3π	4π	5π	6π	7π
$x' = 6$	0	$3\pi/2$	3π	$9\pi/2$	6π	$15\pi/2$	9π	$21\pi/2$

Πίνακας 7-1 Οι φάσεις των πλατών πιθανότητας των καταστάσεων της (7.16)

	$ 0, 2\rangle$	$ 1, 2\rangle$	$ 2, 2\rangle$	$ 3, 2\rangle$	$ 4, 2\rangle$	$ 5, 2\rangle$	$ 6, 2\rangle$	$ 7, 2\rangle$
$x' = 0$	→	→	→	→	→	→	→	→
$x' = 2$	→	↑	←	↓	→	↑	←	↓
$x' = 4$	→	←	→	←	→	←	→	←
$x' = 6$	→	↓	←	↑	→	↓	←	↑

Πίνακας 7-2 Οι γωνίες των αντίστοιχων φάσεων του Πίνακα 7-1

Ας προσπαθήσουμε να ερμηνεύσουμε την (7.16). Στον Πίνακα 7-1 φαίνονται οι φάσεις των πλατών πιθανότητας των καταστάσεων που δίνονται από την (7.16). Αν δηλαδή το πλάτος πιθανότητας είναι $e^{i\theta}$, στον πίνακα φαίνεται η τιμή θ . Στον Πίνακα 7-2 φαίνονται οι γωνίες των αντίστοιχων φάσεων ως διανύσματα.

Από τους Πίνακες 7-1 και 7-2 είναι φανερό ότι οι φάσεις των πλατών πιθανότητας των καταστάσεων $|1, 2\rangle, |2, 2\rangle, |3, 2\rangle, |5, 2\rangle, |6, 2\rangle$ και $|7, 2\rangle$ συμβάλλουν καταστροφικά, ενώ οι φάσεις των πλατών πιθανότητας των καταστάσεων $|0, 2\rangle$ και $|4, 2\rangle$ συμβάλλουν δημιουργικά. Έτσι, μετά τη δράση του κβαντικού μετασχηματισμού Fourier που προκαλεί τις παραπάνω καταστροφικές και δημιουργικές συμβολές, στον *Reg* υπάρχουν μόνο οι καταστάσεις $|0, 2\rangle$ και $|4, 2\rangle$. Επομένως η κατάσταση του *Reg* είναι:

$$|\psi\rangle = \frac{4}{\sqrt{32}} |0, 2\rangle + \frac{1}{\sqrt{32}} (1 + e^{2\pi i} + e^{4\pi i} + e^{6\pi i}) |4, 2\rangle = \frac{4}{\sqrt{32}} |0, 2\rangle + \frac{4}{\sqrt{32}} |4, 2\rangle \quad (7.17)$$

Στο 8ο βήμα μετράται η κατάσταση του *Reg1*. Το αποτέλεσμα της μέτρησης μπορεί να είναι 0 ή 4. Επαναλαμβάνοντας τα βήματα 3 έως και 8 τρεις φορές, είναι σχεδόν βέβαιο ότι θα μετρηθούν και οι δύο αυτές τιμές οι οποίες είναι πολλαπλάσια του $1/r$. Από την (7.12) έχουμε ότι:

$$c_1' = 0 = \lambda_1 \frac{8}{r} \Rightarrow \lambda_1 = 0 \quad (7.18)$$

και

$$c_2' = 4 = \lambda_2 \frac{8}{r} \Rightarrow r = 2 \lambda_2 \text{ οπότε για } \lambda_2 = 1 \text{ έχουμε } r = 2 \quad (7.19)$$

Με τον τρόπο αυτό υπολογίστηκε ότι η περίοδος της $f(x) = \cos(\pi x) + 1$ με $x = 0, 1, 2, \dots, q-1$, είναι ίση με 2.

Βιβλιογραφία

- Lo H. K., Popescu S., & Spiller T. (Eds), *Introduction to quantum computation and information*, World Scientific, 1998.
- Pittengen A. O., *An introduction to quantum computing algorithms*, Birkhäuser, 2000.
- Rivest R., Shamir A., & Adelman L., A method for obtaining digital signatures and public key cryptosystems, *Communications of the ACM*, vol. 21, pp. 120-126, 1978.
- Shor P., Algorithms for quantum computation: discrete logarithms and factoring, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pp. 124-134, 1994.
- Stolze J., & Suter D., *Quantum computing: A short course from theory to experiment*, Wiley-VCH, 2008.

Ασκήσεις

Άσκηση 7.1

Να χρησιμοποιήσετε τον κβαντικό αλγόριθμο του Shor για να βρείτε την περίοδο της συνάρτησης:

$$f(x) = \sin\left(\frac{\pi x}{2}\right) + 2 \quad \text{όπου} \quad x=0,1,2,3,\dots,q-1$$

Άσκηση 7.2

Να χρησιμοποιήσετε τον κβαντικό αλγόριθμο του Shor για να βρείτε την περίοδο της συνάρτησης:

$$f(x) = \cos\left(\frac{\pi x}{2}\right) - 1 \quad \text{όπου} \quad x=0,1,2,3,\dots,q-1$$

8. Κβαντική τηλεμεταφορά

Σύνοψη

Στο κεφάλαιο αυτό θα περιγραφεί η κβαντική τηλεμεταφορά και θα δοθεί το αντίστοιχο κβαντικό κύκλωμα. Θα εξηγηθεί γιατί η κβαντική τηλεμεταφορά δεν παραβιάζει το θεώρημα της αδυναμίας διακλάδωσης.

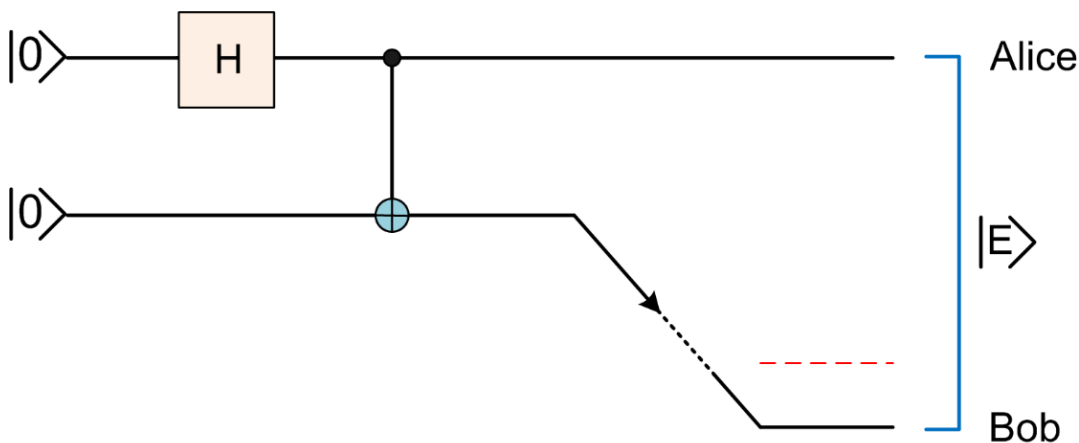
Προαπαιτούμενη γνώση

Τα τρία πρώτα κεφάλαια και το έκτο κεφάλαιο του βιβλίου αυτού.

8.1 Η κβαντική τηλεμεταφορά

Με την κβαντική τηλεμεταφορά μπορούμε να μεταφέρουμε την κατάσταση ενός ή περισσότερων qubits από τον αποστολέα στον παραλήπτη, οι οποίοι μπορούν να βρίσκονται σε οποιαδήποτε χωρική απόσταση μεταξύ τους. Η διαδικασία αυτή ονομάζεται τηλεμεταφορά γιατί δεν απαιτείται η ύπαρξη ενός κβαντικού καναλιού που να συνδέει τον αποστολέα με τον παραλήπτη (Niesen & Chuang, 2004). Όπως θα δούμε, η κβαντική διεμπλοκή αντικαθιστά το κβαντικό κανάλι. Θα πρέπει να τονιστεί από την αρχή ότι με τη διαδικασία αυτή δεν αντιγράφουμε, αλλά μεταφέρουμε την κατάσταση ενός qubit. Παρακάτω θα περιγράψουμε τη διαδικασία της κβαντικής τηλεμεταφοράς και το αντίστοιχο κβαντικό κύκλωμα.

Θεωρούμε δύο συστήματα ή δύο πρόσωπα, την Alice και τον Bob τα οποία θέλουν να επικοινωνήσουν χρησιμοποιώντας την κβαντική τηλεμεταφορά. Στην αρχή της διαδικασίας η Alice και ο Bob συναντώνται και χρησιμοποιώντας ένα κβαντικό κύκλωμα διεμπλοκής φέρνουν δύο qubits σε κατάσταση διεμπλοκής. Στη συνέχεια παίρνουν ο καθένας ένα από αυτά τα δύο qubits. Η Alice μένει στον τόπο της συνάντησης, ενώ ο Bob φεύγει και πηγαίνει σε έναν μακρινό τόπο. Ο τόπος που πηγαίνει ο Bob είναι τόσο μακρινός που το φως θέλει αρκετά λεπτά της ώρας για να διανύσει την απόσταση μεταξύ της Alice και του Bob. Η διαδικασία αυτή φαίνεται με τη μορφή κβαντικού κυκλώματος στο Σχήμα 8-1.



Σχήμα 8-1. Η αρχή της διαδικασίας της κβαντικής τηλεμεταφοράς.

Όπως φαίνεται στο Σχήμα 8-1, η Alice και ο Bob παίρνουν δύο qubits, που βρίσκονται και τα δύο στην κατάσταση $|0\rangle$ και τα φέρνουν σε κατάσταση διεμπλοκής, την $|E\rangle$, που δίνεται από:

$$|E\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad (8.1)$$

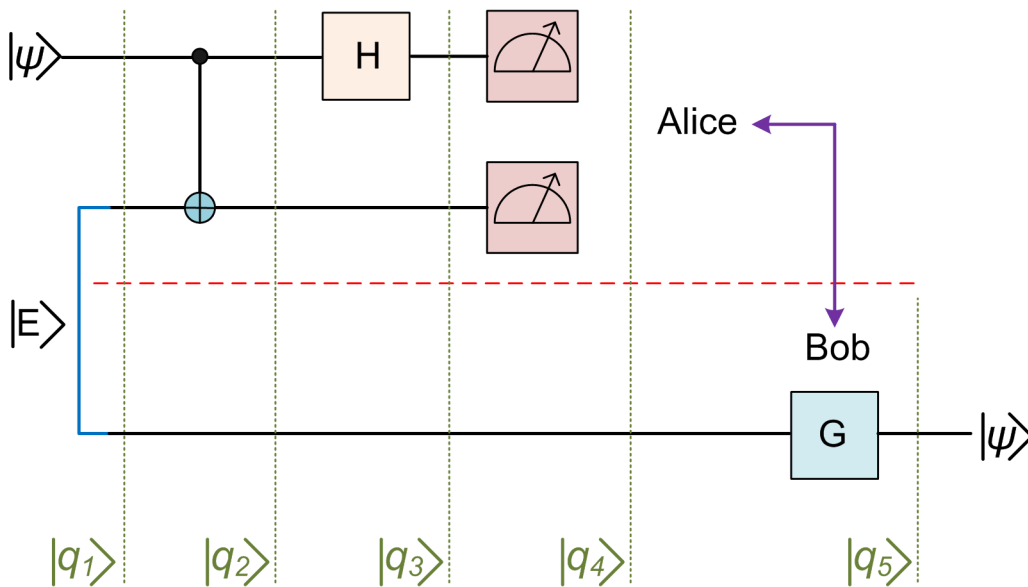
Για να ξεχωρίζουμε ποιο από τα δύο qubits είναι του Bob θα το συμβολίζουμε με τον δείκτη B. Με τον συμβολισμό αυτό η (8.1) γίνεται:

$$|E\rangle = \frac{|00_B\rangle + |11_B\rangle}{\sqrt{2}} \quad (8.2)$$

Μετά από αρκετό χρόνο, η Alice θέλει να στείλει στον Bob την κατάσταση ενός qubit, του $|\psi\rangle$, η οποία είναι άγνωστη σε αυτήν. Γενικά το qubit $|\psi\rangle$ θα βρίσκεται σε υπέρθεση των βασικών καταστάσεων:

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad (8.3)$$

Όπως είπαμε, η Alice δεν γνωρίζει τα πλάτη πιθανότητας a και b . Η Alice όμως μπορεί να τηλεμεταφέρει την άγνωστη κατάσταση του qubit αυτού, χρησιμοποιώντας το γεγονός ότι αυτή και ο Bob μοιράζονται ένα ζεύγος qubits τα οποία βρίσκονται σε κατάσταση διεμπλοκής. Η διαδικασία αυτής της κβαντικής τηλεμεταφοράς φαίνεται στο Σχήμα 8-2, με τη μορφή κβαντικού κυκλώματος.



Σχήμα 8-2. Το κβαντικό κύκλωμα της κβαντικής τηλεμεταφοράς.

Το qubit $|\psi\rangle$ και τα δύο qubits τα οποία βρίσκονται σε κατάσταση διεμπλοκής αποτελούν έναν κβαντικό καταχωρητή η κατάσταση του οποίου δίνεται από:

$$|q_1\rangle = |\psi\rangle|E\rangle = (a|0\rangle + b|1\rangle) \left(\frac{|00_B\rangle + |11_B\rangle}{\sqrt{2}} \right) = \frac{1}{\sqrt{2}} (a|0\rangle|00_B\rangle + a|0\rangle|11_B\rangle + b|1\rangle|00_B\rangle + b|1\rangle|11_B\rangle) \Rightarrow$$

$$|q_1\rangle = \frac{1}{\sqrt{2}} (a|000_B\rangle + a|011_B\rangle + b|100_B\rangle + b|111_B\rangle)$$

(8.4)

Στη συνέχεια η Alice δρα με μία κβαντική πύλη CNOT στα δύο qubits που βρίσκονται στο ίδιο τόπο με αυτήν, στο $|\psi\rangle$ και στο qubit το οποίο είναι σε κατάσταση διεμπλοκής με το qubit του Bob. Η νέα κατάσταση του κβαντικού καταχωρητή είναι:

$$\begin{aligned}
|q_2\rangle &= (CNOT \otimes I)|q_1\rangle = \frac{1}{\sqrt{2}} (CNOT \otimes I)(a|000_B\rangle + a|011_B\rangle + b|100_B\rangle + b|111_B\rangle) \Rightarrow \\
|q_2\rangle &= \frac{1}{\sqrt{2}}(a|000_B\rangle + a|011_B\rangle + b|110_B\rangle + b|101_B\rangle) \Rightarrow \\
|q_2\rangle &= \frac{1}{\sqrt{2}}(a|0\rangle(|00_B\rangle + |11_B\rangle) + b|1\rangle(|10_B\rangle + |01_B\rangle)) \tag{8.5}
\end{aligned}$$

Στο επόμενο βήμα, η Alice δρα με μία κβαντική πύλη H στο πάνω qubit. Η νέα κατάσταση του κβαντικού καταχωρητή είναι:

$$\begin{aligned}
|q_3\rangle &= (H \otimes I \otimes I)|q_2\rangle = \frac{1}{\sqrt{2}} (H \otimes I \otimes I)(a|0\rangle(|00_B\rangle + |11_B\rangle) + b|1\rangle(|10_B\rangle + |01_B\rangle)) \Rightarrow \\
|q_3\rangle &= \frac{1}{2}(a(|0\rangle + |1\rangle)(|00_B\rangle + |11_B\rangle) + b(|0\rangle - |1\rangle)(|10_B\rangle + |01_B\rangle)) \Rightarrow \tag{8.6}
\end{aligned}$$

$$|q_3\rangle = \frac{1}{2}(a(|000_B\rangle + |011_B\rangle + |100_B\rangle + |111_B\rangle) + b(|010_B\rangle + |001_B\rangle - |110_B\rangle - |101_B\rangle))$$

Ξεχωρίζουμε το qubit του Bob από τις καταστάσεις της (8.6) και έχουμε:

$$|q_3\rangle = \frac{1}{2}(|00\rangle a|0_B\rangle + |01\rangle a|1_B\rangle + |10\rangle a|0_B\rangle + |11\rangle a|1_B\rangle + |01\rangle b|0_B\rangle + |00\rangle b|1_B\rangle - |11\rangle b|0_B\rangle - |10\rangle b|1_B\rangle) \tag{8.7}$$

Βγάζουμε τους κοινούς παράγοντες που αντιστοιχούν στα δύο qubits που βρίσκονται στον τόπο της Alice και η (8.7) γίνεται:

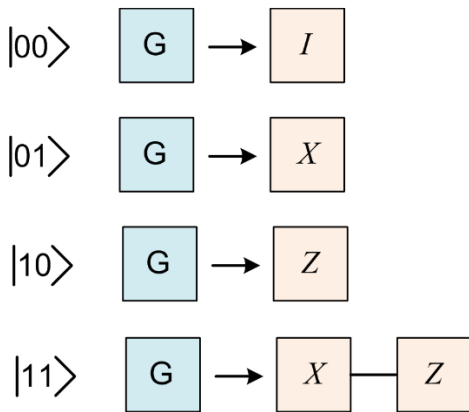
$$|q_3\rangle = \frac{1}{2}(|00\rangle(a|0_B\rangle + b|1_B\rangle) + |01\rangle(a|1_B\rangle + b|0_B\rangle) + |10\rangle(a|0_B\rangle - b|1_B\rangle) + |11\rangle(a|1_B\rangle - b|0_B\rangle)) \tag{8.8}$$

Κάθε ένας από τους τέσσερις όρους της (8.8) έχει μία από τις τέσσερις βασικές καταστάσεις των δύο qubits της Alice και το qubit του Bob σε τέσσερις διαφορετικές καταστάσεις υπέρθεσης, με πλάτη πιθανότητας a και b . Δηλαδή, με τον κβαντικό υπολογισμό που εκτέλεσε η Alice στα δύο δικά της qubits, μετέφερε τα άγνωστα πλάτη πιθανότητας στο qubit του Bob, εκμεταλλευόμενη τη διεμπλοκή.

Στη συνέχεια η Alice μετρά τα δύο δικά της qubits. Όπως γνωρίζουμε, η μέτρηση αυτή θα έχει ως αποτέλεσμα μία από τις τέσσερις βασικές καταστάσεις στις οποίες μπορούν να βρεθούν δύο qubits. Από την (8.8) προκύπτουν τα εξής:

- Αν η Alice μετρήσει $|00\rangle$, τότε το qubit του Bob βρίσκεται στην κατάσταση: $a|0\rangle + b|1\rangle$
- Αν η Alice μετρήσει $|01\rangle$, τότε το qubit του Bob βρίσκεται στην κατάσταση: $a|1\rangle + b|0\rangle$
- Αν η Alice μετρήσει $|10\rangle$, τότε το qubit του Bob βρίσκεται στην κατάσταση: $a|0\rangle - b|1\rangle$
- Αν η Alice μετρήσει $|11\rangle$, τότε το qubit του Bob βρίσκεται στην κατάσταση: $a|1\rangle - b|0\rangle$

Εκτός από την πρώτη περίπτωση, ο Bob θα πρέπει να χρησιμοποιήσει ένα δικό του κβαντικό κύκλωμα, το οποίο στο Σχήμα 8-2 συμβολίζεται με « G » για να φέρει το qubit του σε κατάσταση ίδια με την αρχική κατάσταση του $|\psi\rangle$. Για να επιλέξει το σωστό κβαντικό κύκλωμα ο Bob θα πρέπει να ξέρει τι μετρήσε η Alice. Μετά τη μέτρηση, η Alice επικοινωνεί με τον Bob μέσα από ένα κλασικό κανάλι και τον πληροφορεί για το αποτέλεσμα της μέτρησής της.



Σχήμα 8-3. Το κβαντικό κύκλωμα G που χρησιμοποιεί ο Bob ανάλογα με το αποτέλεσμα της μέτρησης της Alice.

Αν η Alice τον πληροφορήσει ότι μετρήσε $|00\rangle$, τότε ο Bob δεν χρειάζεται να κάνει τίποτε, θα χρησιμοποιήσει δηλαδή την πύλη αδρανείας I και η κατάσταση του qubit του θα είναι:

$$|q_5\rangle = I (a|0\rangle + b|1\rangle) = a|0\rangle + b|1\rangle = |\psi\rangle \quad (8.9)$$

Αν η Alice τον πληροφορήσει ότι μετρήσε $|01\rangle$, τότε ο Bob θα χρησιμοποιήσει την κβαντική πύλη X και η κατάσταση του qubit του θα είναι:

$$|q_5\rangle = X (a|1\rangle + b|0\rangle) = a|0\rangle + b|1\rangle = |\psi\rangle \quad (8.10)$$

Αν η Alice τον πληροφορήσει ότι μετρήσε $|10\rangle$, τότε ο Bob θα χρησιμοποιήσει την κβαντική πύλη Z και η κατάσταση του qubit του θα είναι:

$$|q_5\rangle = Z (a|0\rangle - b|1\rangle) = a|0\rangle + b|1\rangle = |\psi\rangle \quad (8.11)$$

Αν η Alice τον πληροφορήσει ότι μετρήσε $|11\rangle$, τότε ο Bob θα χρησιμοποιήσει πρώτα την κβαντική πύλη X και στη συνέχεια την κβαντική πύλη Z. Στο τέλος η κατάσταση του qubit του θα είναι:

$$|q_5\rangle = Z X (a|1\rangle - b|0\rangle) = Z (a|0\rangle - b|1\rangle) = a|0\rangle + b|1\rangle = |\psi\rangle \quad (8.12)$$

Το κβαντικό κύκλωμα « G » που χρησιμοποιεί ο Bob ανάλογα με το αποτέλεσμα της μέτρησης της Alice φαίνεται στο Σχήμα 8-3.

Είδαμε πως μπορεί να χρησιμοποιηθεί η διεμπλοκή για την κβαντική τηλεμεταφορά της κατάστασης ενός qubit από την Alice στον Bob. Θα πρέπει όμως να τονίσουμε τα εξής:

Κατά την κβαντική τηλεμεταφορά δεν μεταφέρεται το φυσικό σύστημα που υλοποιεί το άγνωστο qubit $|\psi\rangle$, αλλά η κατάσταση του (Bell, 1964). Αν για παράδειγμα χρησιμοποιηθεί το spin ενός ηλεκτρονίου ως qubit, τότε δεν μεταφέρεται το ηλεκτρόνιο. Το ηλεκτρόνιο παραμένει στον τόπο της Alice και μόνο η πληροφορία για την κατάστασή του μεταφέρεται στο ηλεκτρόνιο που υλοποιεί το qubit του Bob.

Η κβαντική τηλεμεταφορά δεν παραβαίνει το θεώρημα της αδυναμίας διακλάδωσης. Όπως προκύπτει από το Σχήμα 8-2, μετά τη μεταφορά η κατάσταση $|\psi\rangle$ δεν υπάρχει πια στον τόπο της Alice. Δηλαδή η Alice δεν μπορεί να έχει αντίγραφο της κατάστασης που μετέφερε στον Bob.

Μόλις η Alice μετρήσει τα δύο qubits της, το qubit του Bob μεταφέρεται σε μία από τις τέσσερις καταστάσεις ακαριαία, ανεξάρτητα από το πόσο μακριά βρίσκεται. Δηλαδή, αν η Alice μετρήσει $|00\rangle$ η κατάσταση του qubit του Bob γίνεται ακαριαία $|\psi\rangle$, ακόμη και αν το φως χρειάζεται αρκετά λεπτά της ώρας, για να διανύσει την απόσταση που χωρίζει την Alice από τον Bob. Πληροφορία ή ενέργεια δεν μπορεί να μεταφερθεί με ταχύτητα μεγαλύτερη από την ταχύτητα του φωτός. Αυτή είναι μία अपαραβάβητη αρχή. Η κβαντική τηλεμεταφορά δεν αντιβαίνει στην αρχή αυτή, διότι ο Bob πρέπει να πληροφορηθεί από την Alice το αποτέλεσμα της μέτρησής της, για να γνωρίζει σε ποια από τις τέσσερις δυνατές καταστάσεις έχει μεταφερθεί το qubit του. Την πληροφορία αυτή η Alice μπορεί να του τη δώσει μόνο χρησιμοποιώντας ένα κλασικό κανάλι (π.χ. ένα ηλεκτρομαγνητικό σήμα) στο οποίο η πληροφορία μεταφέρεται με ταχύτητα ίση ή μικρότερη από την ταχύτητα του φωτός (Aspect, Dalibard, & Roger, 1982).

Βιβλιογραφία

Aspect A., Dalibard J., & Roger G., Experimental test of Bell's inequalities using time-varying analyzers, *Physical Review Letters*, vol. 49, pp. 1804-1807, 1982.

Bell J. S., On the Einstein-Podolsky-Rosen paradox, *Physics*, vol. 1, pp. 195-200, 1964.

Niesen M. A., & Chuang I. L., *Quantum computation and information*, Cambridge University Press, 2004.

Ασκήσεις

Άσκηση 8.1

Να εκτελέσετε την κβαντική τηλεμεταφορά αν η Alice και Bob φέρουν σε διεμπλοκή δυο qubits, των οποίων η αρχική κατάσταση είναι: $|01\rangle$.

Άσκηση 8.2

Να εκτελέσετε την κβαντική τηλεμεταφορά αν η Alice και Bob φέρουν σε διεμπλοκή δύο qubits, των οποίων η αρχική κατάσταση είναι: $|11\rangle$.

9. Ο Προσομοιωτής Κβαντικού Υπολογιστή QCS

Σύνοψη

Στο κεφάλαιο αυτό δίνονται οι οδηγίες χρήσης του προσομοιωτή κβαντικού υπολογιστή QCS, ο οποίος έχει αναπτυχθεί από τον συγγραφέα και συνοδεύει το βιβλίο αυτό.

Προαπαιτούμενη γνώση

Τα τρία πρώτα κεφάλαια του βιβλίου αυτού.

9.1 Άδεια χρήσης του QCS

Ο συγγραφέας του βιβλίου αυτού ανέπτυξε για ερευνητικούς σκοπούς έναν προσομοιωτή κβαντικού υπολογιστή, ο οποίος ονομάστηκε QCS από τα αρχικά των λέξεων **Q**uantum **C**omputer **S**imulator (Karafyllidis, 2005). Ο προσομοιωτής QCS μπορεί να χρησιμοποιηθεί και ως διδακτικό εργαλείο. Το βιβλίο αυτό συνοδεύεται από την δεύτερη έκδοση του QCS.

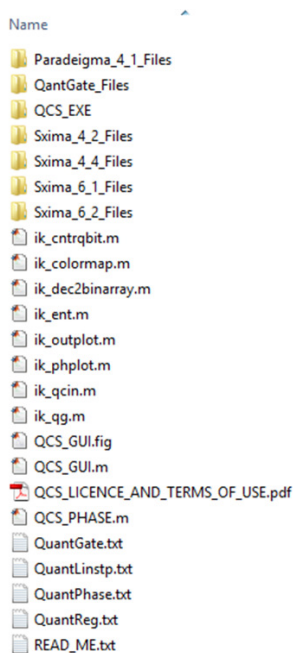
Μπορείτε να χρησιμοποιείτε ελεύθερα τον QCS για έρευνα ή διδασκαλία με την **απαραίτητη προϋπόθεση** να αναφέρετε σε κάθε παρουσίαση, κείμενο ή δημοσίευσή σας την παρακάτω βιβλιογραφική αναφορά:

I. G. Karafyllidis, “Quantum Computer Simulator based on the Circuit Model of Quantum Computation”, *IEEE Transactions on Circuits and Systems I*, vol. 52, pp. 1590-1596, 2005.

9.2 Δομή και εγκατάσταση του QCS

Ο προσομοιωτής κβαντικού υπολογιστή QCS είναι διαθέσιμος στην ιστοσελίδα του κεφαλαίου 9 αυτού του βιβλίου, στον Ελληνικό Συσσωρευτή Ακαδημαϊκών Ηλεκτρονικών Βιβλίων (<http://repository.kallipos.gr>) και μπορείτε να τον κατεβάσετε από εκεί.

Αφού κατεβάσετε και αποσυμπιέσετε το αρχείο «QCS_2.0.zip», θα δημιουργηθεί ένας φάκελος με όνομα «QCS_2.0». Τα περιεχόμενα του φακέλου αυτού φαίνονται στο Σχήμα 9-1.



Σχήμα 9-1. Τα αρχεία του QCS

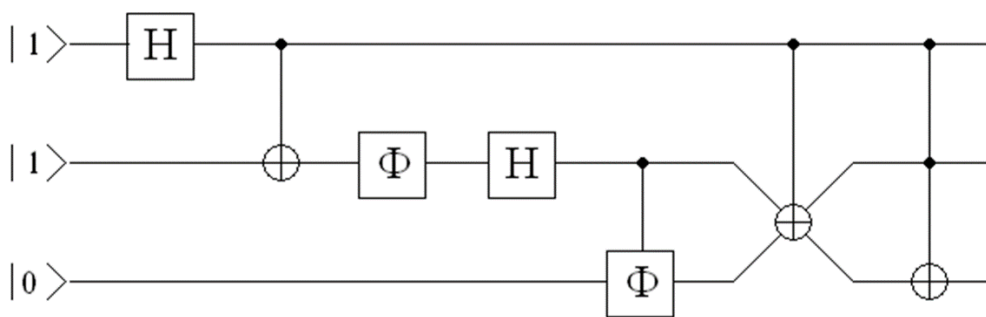
Για να τρέξετε τον προσομοιωτή QCS πρέπει να έχετε το πακέτο Matlab. Οι απαιτήσεις για τον υπολογιστή είναι αυτές του Matlab. Δηλαδή, αν τρέχει στον υπολογιστή σας το Matlab, θα τρέξει και ο προσομοιωτής QCS. Θα πρέπει να προσθέσετε στα paths του Matlab τη θέση όπου βρίσκεται ο QCS.

Μετά από τα παραπάνω ο QCS είναι έτοιμος για χρήση.

9.3 Χρήση του QCS

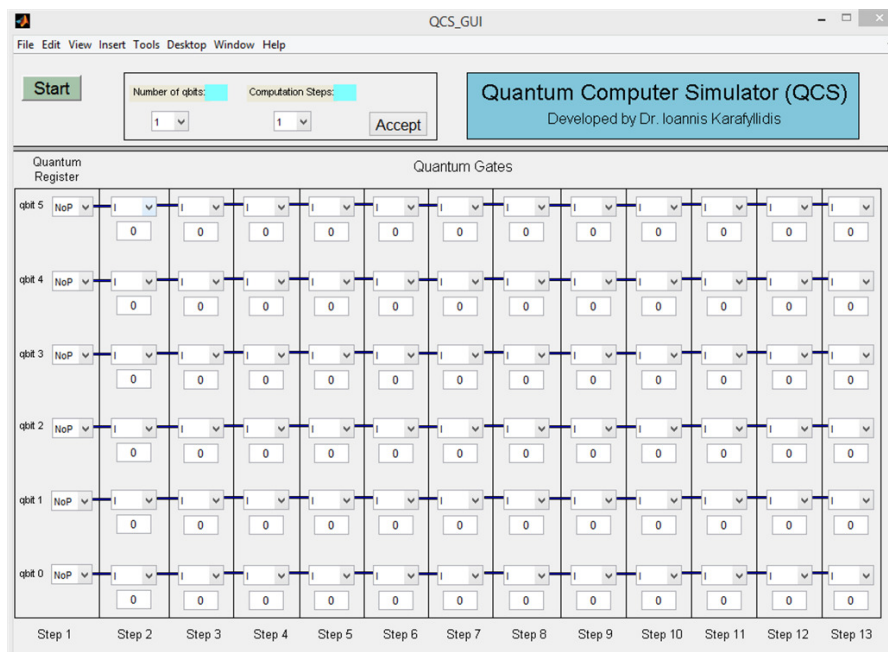
Τα δεδομένα του κβαντικού υπολογισμού που πρέπει να εισαχθούν στον προσομοιωτή QCS είναι:

- Ο αριθμός των qubits και ο αριθμός των βημάτων του κβαντικού υπολογισμού.
- Οι αρχικές καταστάσεις των qubits που αποτελούν τον κβαντικό καταχωρητή.
- Οι κβαντικές πύλες που δρουν σε κάθε βήμα του κβαντικού υπολογισμού.
- Οι γωνίες μετατόπισης φάσης, όπου χρησιμοποιούνται κβαντικές πύλες μετατόπισης φάσης και ελεγχόμενης μετατόπισης φάσης.



Σχήμα 9-2. Το κύκλωμα του κβαντικού υπολογισμού.

Τα δεδομένα του κβαντικού υπολογισμού εισάγονται από το γραφικό περιβάλλον του QCS. Παρακάτω θα περιγράψουμε την χρήση του QCS εκτελώντας παράλληλα ως παράδειγμα, τον κβαντικό υπολογισμό του Σχήματος 9-2. Στον υπολογισμό αυτό, οι μετατοπίσεις φάσεων είναι $64,32^\circ$ για την πύλη μετατόπισης φάσης και 136° για την πύλη ελεγχόμενης μετατόπισης φάσης. Τα βήματα είναι τα εξής:



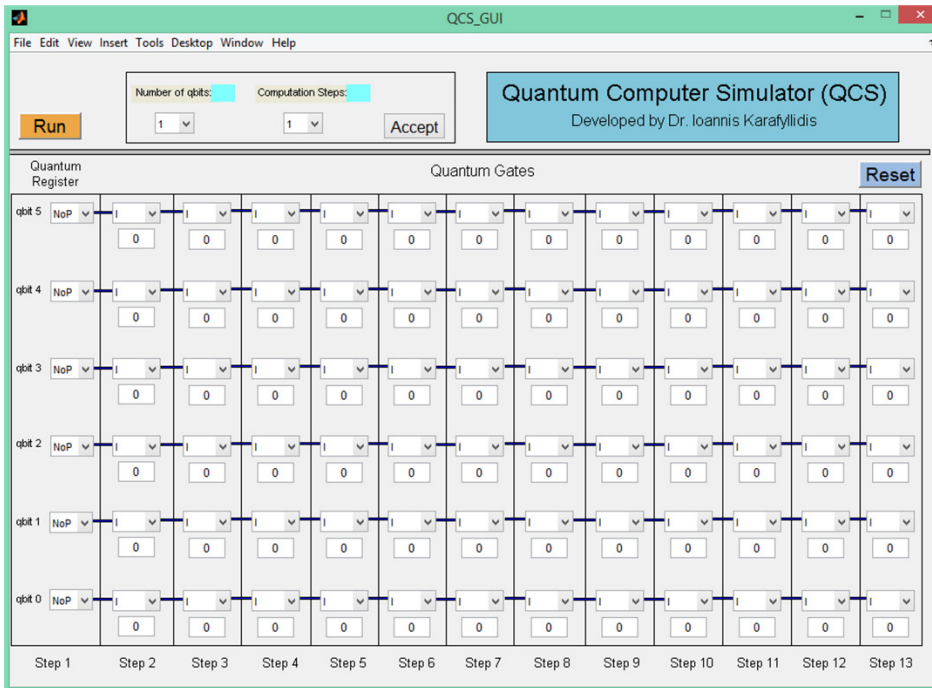
Σχήμα 9-3. Το γραφικό περιβάλλον του QCS για την εισαγωγή των δεδομένων του κβαντικού υπολογισμού.

1. Τρέξτε από το περιβάλλον του Matlab το αρχείο QCS_GUI.m

Μόλις το κάνετε αυτό θα εμφανιστεί η οθόνη του γραφικού περιβάλλοντος, η οποία φαίνεται στο Σχήμα 9-3. Η οθόνη είναι χωρισμένη σε στήλες. Κάθε στήλη αντιστοιχεί σε ένα βήμα του κβαντικού υπολογισμού. Η πρώτη στήλη είναι ο κβαντικός καταχωρητής και είναι το πρώτο βήμα (Step 1).

2. Πατήστε με το αριστερό πλήκτρο του ποντικιού το κουμπί «Start» που βρίσκεται πάνω αριστερά.

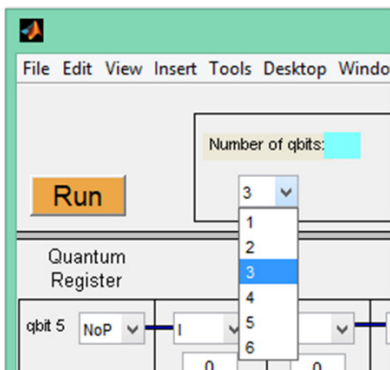
Μόλις το κάνετε αυτό η οθόνη του γραφικού περιβάλλοντος γίνεται όπως φαίνεται στο Σχήμα 9-4.



Σχήμα 9-4. Το γραφικό περιβάλλον του QCS μετά τη χρήση του «Start».

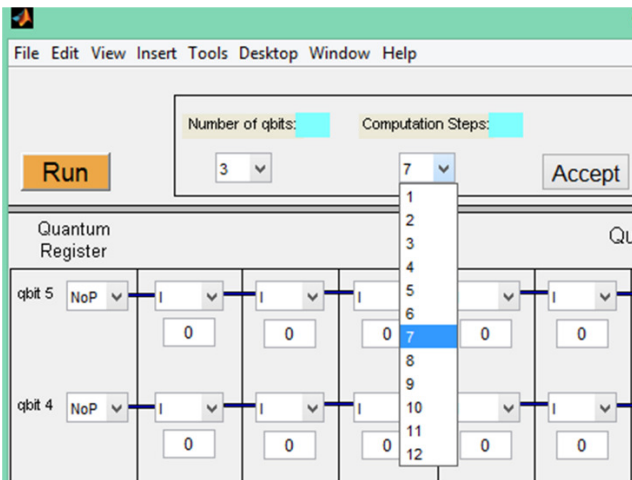
3. Επιλέξτε τον αριθμό των qubits και των βημάτων του κβαντικού υπολογισμού.

Επιλέξτε τον αριθμό των qubits (Number of qubits), που για το παράδειγμά μας είναι 3, όπως φαίνεται στο Σχήμα 9-5.



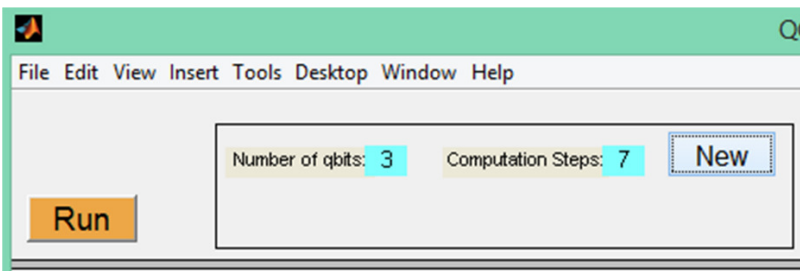
Σχήμα 9-5. Επιλογή του αριθμού των qubits.

Επιλέξτε τον αριθμό των βημάτων (Computation Steps) που για το παράδειγμά μας είναι 7, όπως φαίνεται στο Σχήμα 9-6. Εδώ δεν προσμετρούμε την αρχική κατάσταση των qubits ως υπολογιστικό βήμα.



Σχήμα 9-6. Επιλογή του αριθμού των βημάτων του κβαντικού υπολογισμού.

Μετά πατήστε το κουμπί «Accept». Μόλις το κάνετε αυτό εξαφανίζονται οι δύο κατάλογοι (drop-down menus), και οι αριθμοί που έχετε επιλέξει εμφανίζονται μέσα στα γαλάζια πλαίσια, όπως φαίνεται στο Σχήμα 9-7.

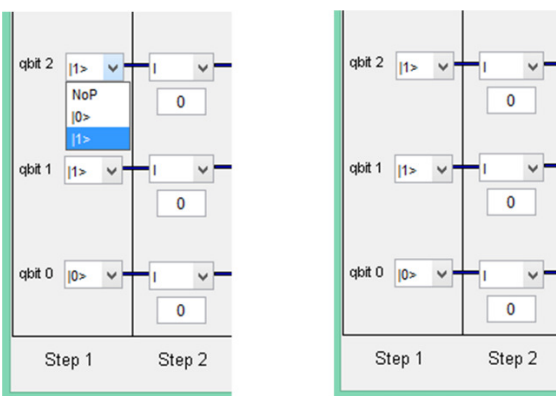


Σχήμα 9-7. Μετά την αποδοχή του αριθμού των qubits και των βημάτων του κβαντικού υπολογισμού.

Αν θέλετε να αλλάξετε τις επιλογές σας πατήστε το κουμπί «New», για να επαναλάβετε τη διαδικασία.

4. Επιλέξτε τις αρχικές καταστάσεις των qubits.

Να θυμάστε ότι αρχίζουμε από την κάτω αριστερή γωνία της οθόνης, διότι τα qubits αριθμούνται από κάτω προς τα επάνω. Για το παράδειγμα του Σχήματος 9-2, τα qubits είναι $|0\rangle$, $|1\rangle$ και $|1\rangle$, όπως φαίνεται στο Σχήμα 9-8.



Σχήμα 9-8. Οι αρχικές καταστάσεις των qubits.

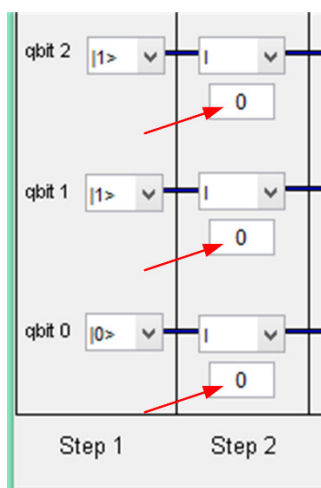
5. Επιλέξτε τις κβαντικές πύλες που δρουν σε κάθε βήμα του κβαντικού υπολογισμού.

Στην οθόνη του γραφικού περιβάλλοντος του QCS στις θέσεις των κβαντικών πυλών υπάρχουν κατάλογοι επιλογών (drop-down menus). Στους καταλόγους αυτούς οι κβαντικές πύλες εισάγονται χρησιμοποιώντας τα σύμβολα του Πίνακα 9-1.

Σύμβολο	Κβαντική πύλη
I	Πύλη αδρανείας (I)
H	Πύλη Hadamard (H)
Ph	Πύλη μετατόπισης φάσης (Φ)
CN	Qubit στόχος πύλης $CNOT$
CCN	Qubit στόχος πύλης $CCNOT$
Ft1	Πρώτο qubit στόχος πύλης F
CPh	Qubit στόχος πύλης $C\Phi$
Ft2	Δεύτερο qubit στόχος πύλης F
Cntr	Qubit ελέγχου

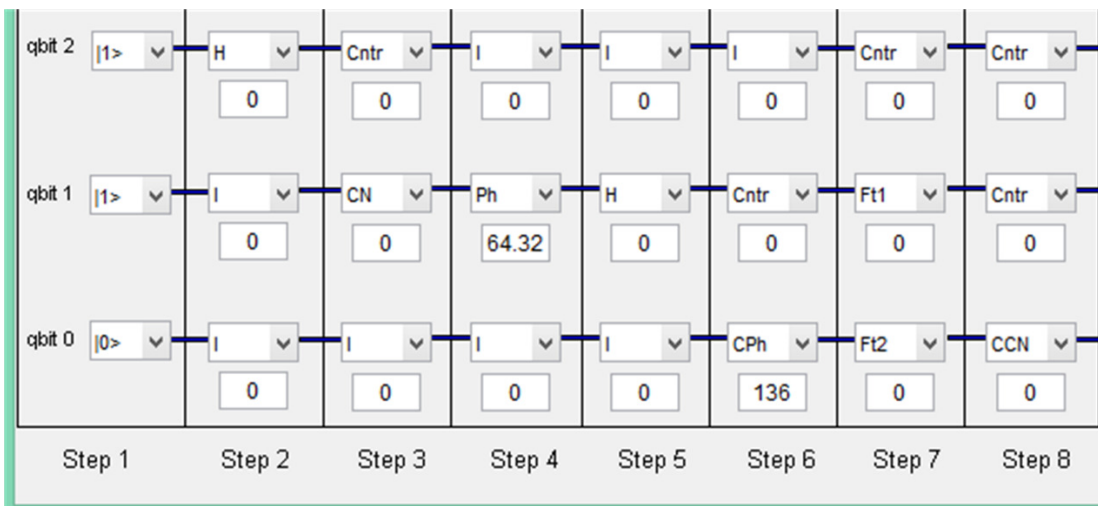
Πίνακας 9-1. Σύμβολα εισαγωγής των κβαντικών πυλών.

Εάν στο κβαντικό κύκλωμα περιλαμβάνονται και κβαντικές πύλες μετατόπισης φάσης ή ελεγχόμενης μετατόπισης φάσης, η γωνία της φάσης γράφεται στον χώρο κάτω από το σύμβολο της πύλης, ο οποίος επισημαίνεται με κόκκινο βέλος στο Σχήμα 9-9.



Σχήμα 9-9. Χώροι αναγραφής των γωνιών των φάσεων.

Εισάγουμε όλες τις κβαντικές πύλες για κάθε βήμα του κβαντικού υπολογισμού. Για το παράδειγμα του Σχήματος 9-2, μετά την εισαγωγή των κβαντικών πυλών και των γωνιών των φάσεων, η οθόνη του γραφικού περιβάλλοντος του QCS θα είναι όπως φαίνεται στο Σχήμα 9-10.



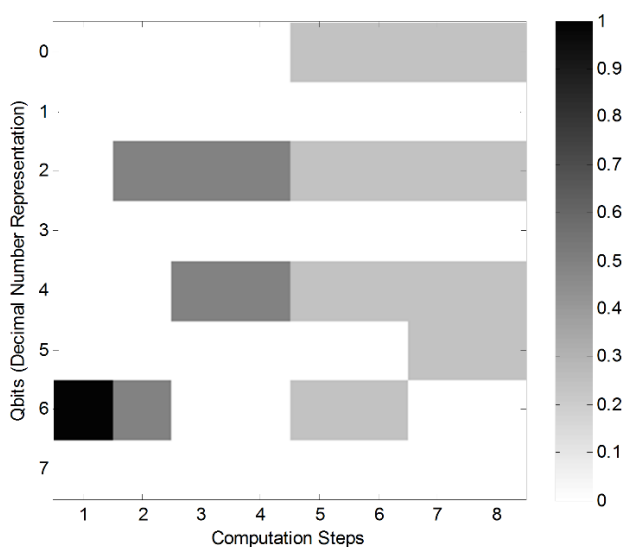
Σχήμα 9-10. Οι καταστάσεις των qubits και οι κβαντικές πύλες του παραδείγματος του Σχήματος 9-2.

6. Πατήστε το κουμπί «Run»

Μόλις πατήσετε το κουμπί «Run» γράφονται στον σκληρό δίσκο και στον φάκελο όπου βρίσκονται ο QCS τα τέσσερα αρχεία *QuantGate*, *QuantLinstp*, *QuantPhase* και *QuantReg*. Τα αρχεία αυτά περιέχουν όλα τα δεδομένα εισόδου για τον QCS. Αφού πατήσετε το «Run», η οθόνη παραμένει ίδια και θα πρέπει να την κλείσετε εσείς πατώντας στο «X» του παραθύρου.

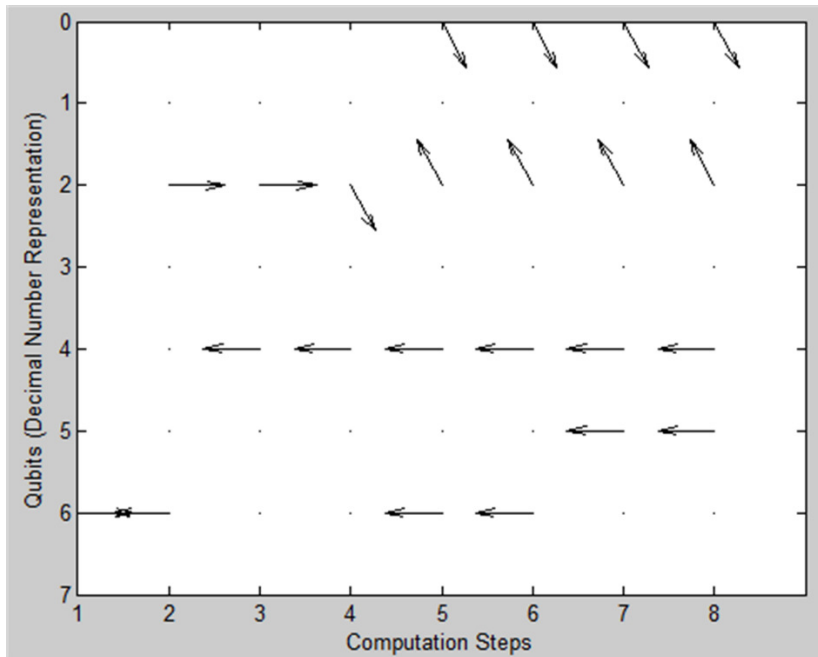
7. Εκτελέστε τον κβαντικό υπολογισμό.

Από το περιβάλλον του Matlab εκτελέστε το *QCS_PHASE.m*. Το **QCS_PHASE.m** είναι ο προσομοιωτής κβαντικού υπολογιστή QCS, ο οποίος εκτελεί τον κβαντικό υπολογισμό. Αν εμφανιστούν κάποια warnings αγνοήστε τα. Ο QCS παράγει τέσσερις εξόδους που εμφανίζονται ως εικόνες (Figures) του Matlab. Προσοχή: οι τέσσερις εικόνες εμφανίζονται η μία πάνω στην άλλη και θα πρέπει να τις μετακινήσετε με το ποντίκι για να τις δείτε όλες. Η πρώτη εικόνα δίνει την κατανομή των πιθανοτήτων των καταστάσεων του κβαντικού καταχωρητή σε κάθε βήμα του κβαντικού υπολογισμού. Η κατανομή αυτή για το παράδειγμά μας φαίνεται στο Σχήμα 9-11.



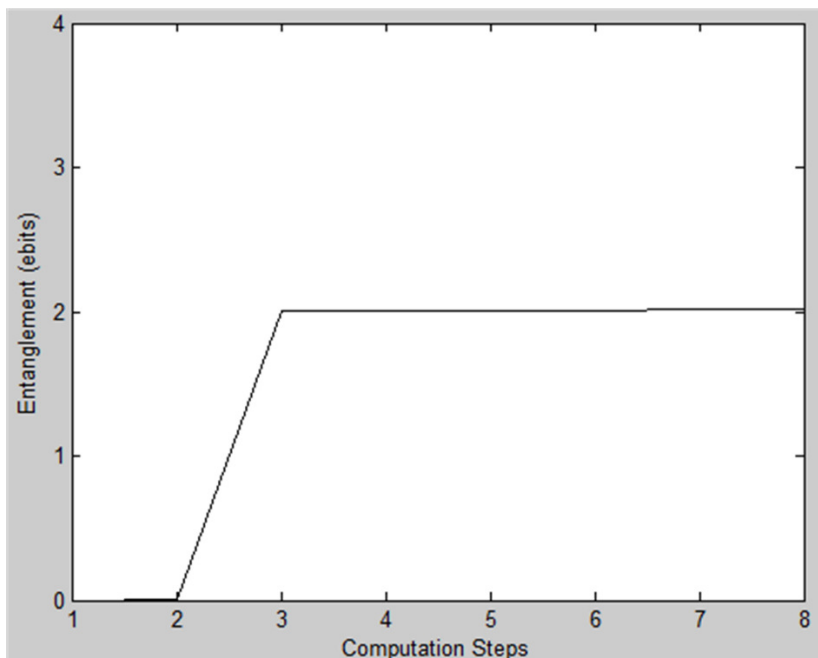
Σχήμα 9-11. Η κατανομή των πιθανοτήτων των καταστάσεων σε κάθε βήμα του κβαντικού υπολογισμού.

Η δεύτερη εικόνα δίνει τις γωνίες των φάσεων σε κάθε βήμα του κβαντικού υπολογισμού. Το οριζόντιο βέλος που δείχνει δεξιά αντιστοιχεί σε γωνία 0° . Οι γωνίες των φάσεων για το παράδειγμά μας φαίνονται στο Σχήμα 9-12.



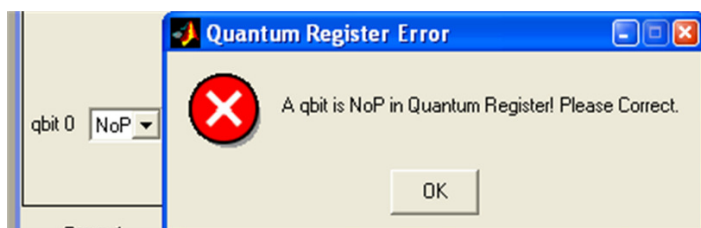
Σχήμα 9-12. Οι γωνίες των φάσεων.

Η τρίτη εικόνα δείχνει την κβαντική διεμπλοκή σε κάθε βήμα του κβαντικού υπολογισμού με γραμμικό διάγραμμα, ενώ η τέταρτη εικόνα δείχνει την κβαντική διεμπλοκή σε διάγραμμα bar. Για το παράδειγμά μας, οι εικόνες αυτές φαίνονται στα Σχήματα 9-13 και 9-14, αντίστοιχα.



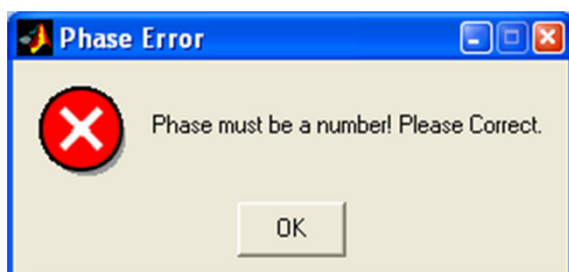
Σχήμα 9-13. Η μεταβολή της κβαντικής διεμπλοκής

Αν στην οθόνη του γραφικού περιβάλλοντος του QCS, πατώντας το κουμπί «Run», εμφανιστεί το μήνυμα σφάλματος, που φαίνεται στο Σχήμα 9-16, αυτό σημαίνει ότι δεν έχετε επιλέξει την αρχική κατάσταση ενός qubit στον κβαντικό καταχωρητή, ενώ από τη δήλωση του αριθμού των qubits, το qubit αυτό περιλαμβάνεται στον κβαντικό καταχωρητή. Θα πρέπει να επιλέξετε την αρχική κατάσταση που θέλετε.



Σχήμα 9-16. Σφάλμα στην δήλωση αρχικής κατάστασης qubit.

Αν πατώντας το κουμπί «Run» εμφανιστεί το μήνυμα σφάλματος του Σχήματος 9-17, αυτό σημαίνει ότι σε κάποια από τις θέσεις όπου πρέπει να βάλετε τη γωνία μετατόπισης φάσης έχετε βάλει κάποιον μη αριθμητικό χαρακτήρα. Η τιμή επανέρχεται στο 0 και πρέπει εσείς να βάλετε τη σωστή.



Σχήμα 9-17. Σφάλμα στην δήλωση φάσης.

Αν θέλετε να αρχίσετε από την αρχή, πατήστε το κουμπί «Reset» και θα εμφανιστεί μία καινούργια οθόνη.

Σε μελλοντικές εκδόσεις του Matlab, είναι ίσως πιθανό να υπάρξουν προβλήματα συμβατότητας στη χρήση του γραφικού περιβάλλοντος, που εκτελείται από το αρχείο «QCS_GUI.m». Για την περίπτωση αυτή, στον φάκελο «\QCS_EXE» υπάρχει μία εκτελέσιμη (exe) μορφή του γραφικού περιβάλλοντος, η «QCS.exe». Αντιγράψτε το αρχείο αυτό στον φάκελο όπου υπάρχει ο «QCS_PHASE.m» και χρησιμοποιήστε το «QCS.exe» αντί του «QCS_GUI.m».

Ο QCS έχει χρησιμοποιηθεί σε αρκετές ερευνητικές εργασίες, μερικές από τις οποίες αναφέρονται στη βιβλιογραφία του κεφαλαίου αυτού (Karafyllidis, 2003· Karafyllidis, 2003b· Karafyllidis, 2004· Karafyllidis, 2004b· Karafyllidis, 2012· Vlachos & Karafyllidis, 2009· Vlachos & Karafyllidis, 2009b).

Βιβλιογραφία

- Karafyllidis I. G., Cellular quantum computer architecture, *Physics Letters A*, vol 320, pp. 35-38, 2003.
- Karafyllidis I. G., Visualization of the quantum Fourier transform using a quantum computer simulator, *Quantum Information Processing*, vol. 2, pp. 271-288, 2003 b.
- Karafyllidis I. G., Simulation of entanglement generation and variation in quantum computation, *Journal of Computational Physics*, vol. 200, pp. 383-397, 2004.
- Karafyllidis I. G., Definition and evolution of quantum cellular automata with two qubits per cell, *Physical Review A*, vol. 70, pp. 044301-1 - 044301-4, 2004 b.
- Karafyllidis I. G., Quantum Computer Simulator based on the Circuit Model of Quantum Computation, *IEEE Transactions on Circuits and Systems I*, vol. 52, pp. 1590-1596, 2005.

6. Karafyllidis I. G., Quantum gate circuit model of signal integration in bacterial quorum sensing, *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 9, pp. 571-579, 2012.
- Vlachos P., & Karafyllidis I. G., Simulation of quantum key expansion using quantum cellular automata, *Computer Physics Communications*, vol. 180, pp. 251-255, 2009.
- Vlachos P., & Karafyllidis I. G., Quantum game simulator, using the circuit model of quantum computation, *Computer Physics Communications*, vol. 180, pp. 1990-1998, 2009 b.

Απόδοση όρων

Αδυναμία διακλάδωσης (no-cloning)

Αλληλεπίδραση (interaction)

Αναστρέψιμες πύλες (reversible gates)

Ανάστροφος πίνακας (transpose matrix)

Αντίστροφος πίνακας (inverse matrix)

Βασική κατάσταση (base state)

Γενικευμένο σύνολο πυλών (universal gate set)

Διάνυσμα κατάστασης (state vector)

Διάνυσμα bra (bra vector)

Διάνυσμα ket (ket vector)

Διακλάδωση (cloning)

Διεμπλοκή (entanglement)

Εξωτερικό γινόμενο (outer product)

Ερμιτιανός (Hermitian)

Ερμιτιανός τελεστής (Hermitian operator)

Εσωτερικό γινόμενο (inner product)

Ζεύγη EPR (EPR pairs)

Ιδιοάνυσμα (eigenvector)

Ιδιοτιμή (eigenvalue)

Ισορροπημένη συνάρτηση (balanced function)

Καθαρή κατάσταση (pure state)

Κατάσταση (state)

Καταστάσεις Bell (Bell states)

Καταστροφή της υπέρθεσης (superposition destruction)

Κατάρρευση της κυματοσυνάρτησης (wave function collapse)

Κβαντική μηχανική (quantum mechanics)

Κβαντική παραλληλία (quantum parallelism)

Κβαντική πληροφορία (quantum information)

Κβαντική πύλη (quantum gate)

Κβαντική στιγμή (quantum dot)

Κβαντικό (quantum)

Κβαντικό bit (quantum bit)

Κβαντικός καταχωρητής (quantum register)

Κβαντικό παιχνίδι (quantum game)

Κβαντικός υπολογιστής (quantum computer)

Κβαντικός υπολογισμός (quantum computation)

Κλασικό (classic)

Κλασικός υπολογιστής (classical computer)

Κρυμμένες μεταβλητές (hidden variables)

Λογισμικό (software)

Μέτρηση (measurement)

Μέτρο (norm)
Μηδενικός τελεστής (zero operator)
Μιγαδικός συζυγής (complex conjugate)
Μικτή κατάσταση (mixed state)
Μοναδιαίος πίνακας (unit matrix)

Ορθογώνιες καταστάσεις (orthogonal states)
Ορθοκανονικό σύστημα (orthonormal system)
Ορθομοναδιαίος πίνακας (unitary matrix)

Παγίδα ιόντων (ion trap)
Πιθανότητα (probability)
Πίνακας (matrix)
Πίνακας πυκνότητας (density matrix)
Πλάτος πιθανότητας (probability amplitude)
Πόρος (resource)
Πύλη αδρανείας (do-nothing gate)
Πύλη διπλά ελεγχόμενου ΟΧΙ (controlled-controlled-NOT gate)
Πύλη ελεγχόμενου ΟΧΙ (controlled-NOT gate)
Πύλη ελεγχόμενης μετατόπισης φάσης (controlled phase-shift gate)
Πύλη μετατόπισης φάσης (phase-shift gate)

Συσκευή μέτρησης (measuring device)

Τελεστής (operator)
Τελεστής αδρανείας (do-nothing operator)
Τελεστής μονάδας (unit operator)
Τελεστής πυκνότητας (density operator)
Τηλεμεταφορά (Teleportation)

Υλικό (hardware)
Υπερεπίπεδο (hyperplane)
Υπέρθωση καταστάσεων (state superposition)
Υπολογιστικό καθήκον (computation task)

Χαμιλτονιανή (Hamiltonian)