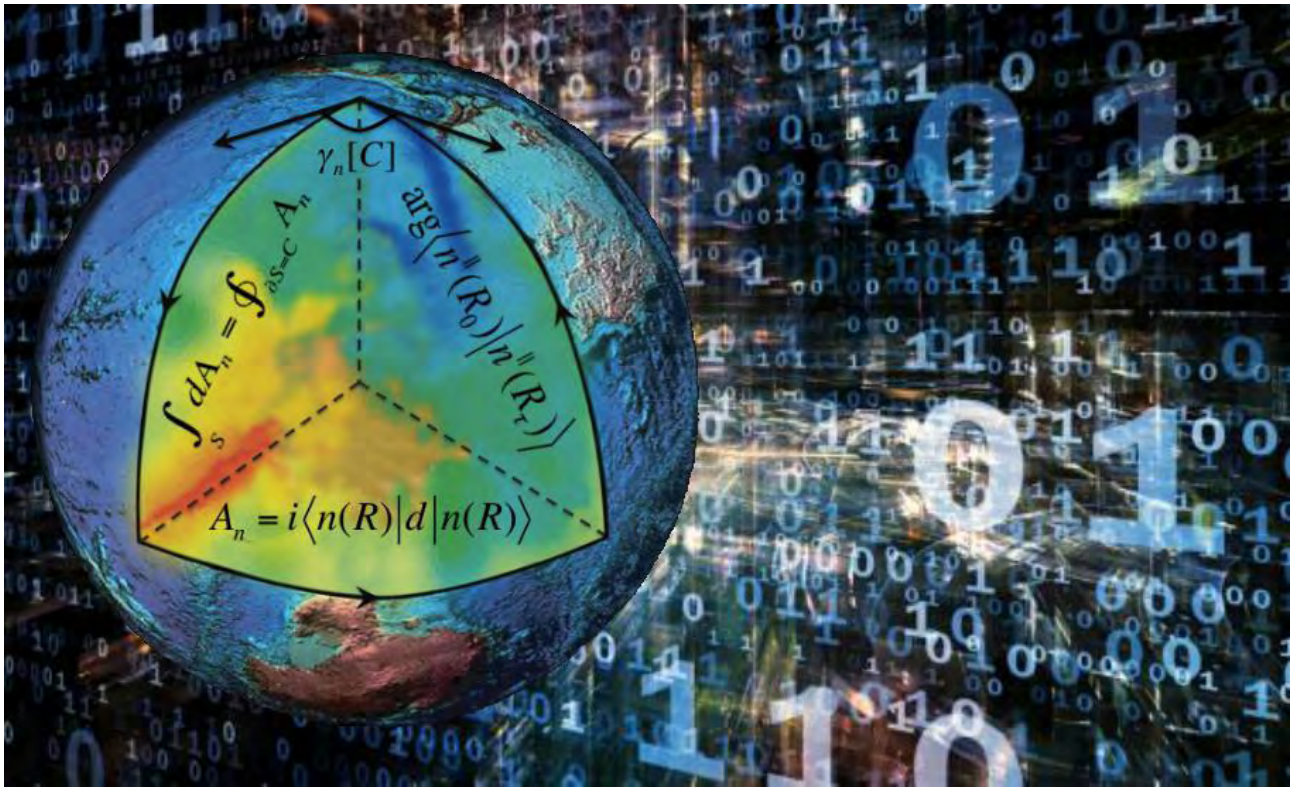
Πανεπιστήμιο Θεσσαλίας

Πολυτεχνική Σχολή

Τμήμα Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Διπλωματική Εργασία

«Μελέτη αρχών κβαντικών πυλών»



Μεταξάς Ηλίας

Βόλος, Ιούλιος 2015

Πανεπιστήμιο Θεσσαλίας

Πολυτεχνική Σχολή

Τμήμα Ηλεκτρολόγων Μηχανικών & Μηχανικών Υπολογιστών

Διπλωματική Εργασία

«Μελέτη αρχών κβαντικών πυλών»

«Study of quantum gates principles»

Μεταξάς Ηλίας

Επιβλέπων καθηγητής: Δρ. Σταμούλης Γεώργιος

Συνεπιβλέπων καθηγητής: Δρ. Βαβουγυιός Διονύσιος

Εγκρίθηκε από τη διμελή εξεταστική επιτροπή την .....

(Υπογραφή)	*(Υπογραφή)*
.....	.....
Σταμούλης Γεώργιος Καθηγητής Παν. Θεσσαλίας	Βαβουγυιός Διονύσιος Καθηγητής Παν. Θεσσαλίας

Διπλωματική εργασία για την απόκτηση του Διπλώματος του Μηχανικού Ηλεκτρονικών Υπολογιστών, Τηλεπικοινωνιών & Δικτύων του Πανεπιστημίου Θεσσαλίας, στα πλαίσια του Προγράμματος Προπτυχιακών Σπουδών του τμήματος Ηλεκτρολόγων Μηχανικών & Μηχανικών Η/Υ του Πανεπιστημίου Θεσσαλίας.

.....

Μεταξάς Ηλίας

Διπλωματούχος Μηχανικός Ηλεκτρονικών Υπολογιστών, Τηλεπικοινωνιών & Δικτύων του Πανεπιστημίου Θεσσαλίας

Στην Οικογένειά μου, για τα ανεξάντλητα αποθέματα αγάπης και υπομονής.

Στην Καλλιόπη μου, για το κάλλος και τη μεγαλοσύνη της καρδιάς της.

Ευχαριστίες

Με την περάτωση της παρούσας εργασίας, θα ήθελα να ευχαριστήσω θερμά τους επιβλέποντες καθηγητές της διπλωματικής εργασίας κ. Σταμούλη Γεώργιο και κ. Βαβουγυιό Διονύσιο για την εμπιστοσύνη που μου έδειξαν, καθώς και την ευκαιρία που μου έδωσαν να ασχοληθώ με ένα πολύ ενδιαφέρον θέμα. Κλείνοντας, νιώθω την ανάγκη να ευχαριστήσω από καρδιάς την οικογένειά μου, για την αμέριστη υποστήριξη και υπομονή τους καθ' όλη τη διάρκεια των σπουδών μου.

Πίνακας Περιεχομένων

ΠΡΟΛΟΓΟΣ ***9***

ΚΕΦΑΛΑΙΟ 1 ..... ***10***

1.ΚΒΑΝΤΙΚΗ ΘΕΩΡΙΑ 10

1.1 Εισαγωγή στην κβαντική θεωρία 10

1.2 Βασικές αρχές της κβαντικής θεωρίας 11

1.3 Τα Qubits 12

1.4 Κβαντικός καταχωρητής 19

1.5 Κβαντική διεμπλοκή 24

1.6 Κβαντικές πύλες 25

ΚΕΦΑΛΑΙΟ 2 ..... ***27***

2.ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ 27

2.1 Εισαγωγή στους κβαντικούς υπολογιστές 27

2.2 Πλεονεκτήματα και εφαρμογές των κβαντικών υπολογιστών 28

2.3 Προβλήματα στην υλοποίηση κβαντικών υπολογιστών 28

2.4 Κβαντική διόρθωση σφαλμάτων 29

2.5 Τεχνολογίες κατασκευής κβαντικών υπολογιστών 32

2.6 Η προοπτική και το μέλλον των κβαντικών υπολογιστών 37

ΚΕΦΑΛΑΙΟ 3 ..... ***39***

3.ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΜΟΙ & ΑΛΓΟΡΙΘΜΟΙ 39

3.1 Το κυκλωματικό μοντέλο των κβαντικών υπολογισμών 39

3.2 Κβαντικοί υπολογισμοί 40

3.3 Ο κβαντικός επεξεργαστής 41

3.4 Ο κβαντικός αλγόριθμος του Deutsch 42

3.5 Ο αλγόριθμος του Grover 43

3.6 Ο αλγόριθμος του Shor 44

ΚΕΦΑΛΑΙΟ 4 ..... ***45***

4.ΚΒΑΝΤΙΚΕΣ ΛΟΓΙΚΕΣ ΠΥΛΕΣ 45

4.1 Προκαταρκτικές έννοιες 45

4.2 Κβαντικές και λογικές πύλες 47

4.3 Κβαντικές πύλες που δρουν σε ένα qubit 47

4.4 Κβαντική πύλη εναλλαγής qubit 56

4.5 Κβαντικές πύλες που δρουν σε δύο qubits 57

ΚΕΦΑΛΑΙΟ 5 ..... ***70***

5.ΚΒΑΝΤΙΚΑ ΚΥΚΛΩΜΑΤΑ 70

Εισαγωγή και απεικόνιση κυκλωμάτων 70

ΠΡΟΛΟΓΟΣ

Σκοπός της παρούσης εργασίας είναι η μελέτη των αρχών που διέπουν τη δομή των κβαντικών πυλών, καθώς και η παρουσίαση κάποιων θεμελιωδών εννοιών και ορισμών που θα συμβάλουν στην καλύτερη κατανόηση της λειτουργίας τους.

Συγκεκριμένα, στο πρώτο κεφάλαιο επιχειρείται μια εισαγωγική παρουσίαση της κβαντικής θεωρίας και της σύνδεσής της με τον κόσμο των κβαντικών υπολογιστών. Εξηγούνται λεπτομερώς ορισμένες στοιχειώδεις δομές των κβαντικών υπολογιστών, όπως τα qubits και ο κβαντικός καταχωρητής.

Στο επόμενα δύο κεφάλαια γίνεται μια σύντομα αναφορά στην τεχνολογία των κβαντικών υπολογιστών, εκεί όπου παρουσιάζεται ιστορικά η πορεία προς τους κβαντικούς υπολογιστές, η λειτουργία τους και οι τελευταίες εξελίξεις όσον αφορά τις ερευνητικές προσπάθειες υλοποίησής τους. Επίσης, περιγράφονται στοιχειωδώς, βασικοί κβαντικοί αλγόριθμοι.

Στο τέταρτο κεφάλαιο παρουσιάζονται αναλυτικά οι κβαντικές πύλες. Εξηγείται η λειτουργία τους, η εφαρμογή της δράσης τους πάνω στα qubits καθώς και τα αποτελέσματα αυτών των δράσεων. Επιπλέον, γίνεται επεξήγηση της απεικόνισης της κάθε κβαντικής πύλης.

Στο πέμπτο κεφάλαιο, γίνεται εισαγωγή στα ολοκληρωμένα κβαντικά κυκλώματα, δομικά στοιχεία των οποίων αποτελούν οι κβαντικές πύλες που αναφέρονται στο προηγούμενο κεφάλαιο, αλλά και της ένταξης αυτών σε απεικόνιση ενός κβαντικού κυκλώματος.

ΚΕΦΑΛΑΙΟ 1

1. ΚΒΑΝΤΙΚΗ ΘΕΩΡΙΑ

1.1 Εισαγωγή στην κβαντική θεωρία

Η κβαντική θεωρία γεννήθηκε από την παρατήρηση ότι η συμπεριφορά του φωτός σε ορισμένα πειράματα θα μπορούσε να εξηγηθεί μόνο εάν θεωρηθεί ότι το φως αποτελείται από σωματίδια που μπορούν και συμπεριφέρονται σαν κύματα. Τα σωματίδια αυτά ονομάστηκαν φωτόνια. Το 1900 ο Max Planck εισήγαγε την ιδέα των "κβάντων" φωτός με σκοπό να εξηγήσει το φάσμα της ηλεκτρομαγνητικής ακτινοβολίας που εκπέμπει ένα μέλαν σώμα. Έτσι λοιπόν, ο Planck θεωρείται ο θεμελιωτής της κβαντικής θεωρίας, δηλ. της θεωρίας που εξηγεί τη φύση και τη συμπεριφορά κύματος και ύλης στο ατομικό και υποατομικό επίπεδο. Ο Planck είχε επιδιώξει να ανακαλύψει την αιτία, που η εκπεμπόμενη ακτινοβολία ενός σώματος αλλάζει χρώμα από το κόκκινο στο πορτοκαλί και τελικά στο μπλε, καθώς αυξάνεται η θερμοκρασία του. Διαπίστωσε ότι, μόνο εάν υποτεθεί ότι η ενέργεια ενός ηλεκτρομαγνητικού κύματος είναι ακέραιο πολλαπλάσιο μιας βασικής ποσότητας (κβάντο ενέργειας), θα μπορούσε να εξηγηθεί η συμπεριφορά της ακτινοβολίας του μέλανος σώματος.

Ο Planck, λοιπόν, θεώρησε πως η εκπομπή και η απορρόφηση της ηλεκτρομαγνητικής ακτινοβολίας γίνεται με διακριτές βασικές μονάδες ενέργειας. Αυτά τα ποσά ή αδιαίρετα πακέτα ενέργειας, τα ονόμασε "κβάντα". Η ενέργεια (E) κάθε κβάντου συνδέεται με τη συχνότητα του κύματος, με την παρακάτω απλή σχέση:

$$\mathbf{E} = \hbar \cdot \mathbf{f} \ (1),$$

όπου $\hbar$ είναι η σταθερά του Planck ($\hbar$=6,626 × 10^{-34} J·s)

Η εισαγωγή αυτής της εξίσωσης, εξήγησε το φαινόμενο του μέλανος σώματος με ακρίβεια. Ο Planck διαπίστωσε ότι σε ορισμένα ιδιαίτερα επίπεδα

θερμοκρασίας (ακριβή πολλαπλάσια μιας βασικής ελάχιστης αξίας), η ενέργεια από ένα φωσφορίζον σώμα θα καταλάβει διαφορετικές περιοχές του φάσματος των χρωμάτων. Αυτές οι υποθέσεις του Planck αποτέλεσαν τη βάση για την ανάπτυξη της κβαντικής θεωρίας.

Η σημερινή μορφή της κβαντικής θεωρίας προήλθε από τη συμβολή πολλών επιστημόνων, κυρίως στο πρώτο μισό του εικοστού αιώνα. Το 1923 ήταν η σειρά του Louis de Broglie, κύρια συνεισφορά του οποίου ήταν η αρχή του κυματοσωματιδιακού δυϊσμού της ύλης. Σύμφωνα με την αρχή αυτή, κάθε υλικό σωματίδιο είναι ταυτόχρονα και ένα κύμα με συχνότητα $f = E/\hbar$ και μήκος κύματος $\lambda = \hbar/p$, όπου E και p η ενέργεια και η ορμή του σωματιδίου αντίστοιχα. Οι Schrödinger και Heisenberg δημιούργησαν ένα γενικό μαθηματικό φορμαλισμό για την κβαντική θεωρία πάνω στον οποίο στηρίχθηκαν όλα τα εντυπωσιακά ποσοτικά αποτελέσματά της: ο Schrödinger την κυματομηχανική και ο Heisenberg τη μηχανική Μητρών (Matrix Mechanics).

Η κβαντική θεωρία κατάφερε να εξηγήσει πολλά φαινόμενα που δεν μπορούσαν να εξηγηθούν με την κλασική φυσική. Εκτός από την ακτινοβολία του μέλανος σώματος, εξηγήθηκε το φωτοηλεκτρικό φαινόμενο, η δομή των ατόμων που οδήγησε στην εξήγηση των χημικών αντιδράσεων, η αρχή λειτουργίας του laser, η αγωγιμότητα των ημιαγωγών, η υπεραγωγιμότητα και πολλά άλλα.

1.2 Βασικές αρχές της κβαντικής θεωρίας

Οι βασικές αρχές που διέπουν την κβαντική θεωρία είναι τέσσερις:

1. Η κβαντική κατάσταση ενός κλειστού κβαντικού συστήματος (π.χ. στοιχειώδες σωμάτιο όπως το ηλεκτρόνιο) περιγράφεται από ένα διάνυσμα μέσα σε διανυσματικό χώρο H στο σύνολο των μιγαδικών αριθμών C. Στο χώρο αυτό, που ονομάζεται χώρος Hilbert, ορίζεται το εσωτερικό γινόμενο μεταξύ δύο διανυσμάτων $|\psi\rangle$, $|\chi\rangle$ ως συνάρτηση από το $H \times H \to C$: $\langle \chi \mid \psi \rangle = \langle \chi \mid {}^t\psi \rangle$, όπου το t δηλώνει «ερμιτιανό ανάστροφο».

2. Σε κάθε φυσικό μέγεθος αντιστοιχεί και ένας γραμμικός μετασχηματισμός στο χώρο Hilbert, που συμβολίζεται συνήθως με κεφαλαίο γράμμα και «καπέλο» (π.χ. Â). Ο γραμμικός τελεστής που αντιστοιχεί σε φυσικά μεγέθη πρέπει να είναι ερμιτιανός τελεστής, δηλαδή να ισχύει $\hat{A}^t=\hat{A}$. Ο λόγος γι' αυτό είναι ότι μόνο οι ερμιτιανοί τελεστές έχουν πραγματικές ιδιοτιμές, κάτι που είναι απαραίτητη προϋπόθεση για ένα φυσικό μέγεθος.

3. Το αποτέλεσμα μίας μοναδικής μέτρησης ενός φυσικού μεγέθους A σε ένα κβαντικό σύστημα που βρίσκεται σε μία κατάσταση $|\psi\rangle$ μπορεί να είναι μόνο μία από τις ιδιοτιμές του αντίστοιχου γραμμικού τελεστή A του φυσικού μεγέθους. Αμέσως μετά τη μέτρηση το κβαντικό σύστημα καταρρέει σε μία νέα κατάσταση η οποία είναι το αντίστοιχο ιδιοδιάνυσμα του γραμμικού τελεστή. Για να βρούμε τις ιδιοτιμές και τα ιδιοδιανύσματα του A λύνουμε την εξίσωση:

$$A|\psi\rangle = \lambda|\psi\rangle,$$

όπου λ οι ιδιοτιμές και $|\psi\rangle$ το αντίστοιχο ιδιοδιάνυσμα.

4. Η πιθανότητα να ληφθεί μία από τις ιδιοτιμές λ_i ενός τελεστή ως αποτέλεσμα μίας μοναδικής μέτρησης πάνω σε κβαντικό σύστημα που βρίσκεται σε μία γενική κατάσταση $|\psi\rangle$ δίνεται από το τετράγωνο του μέτρου της προβολής της $|\psi\rangle$ πάνω στο αντίστοιχο ιδιοδιάνυσμα $|e_i\rangle$ του τελεστή:

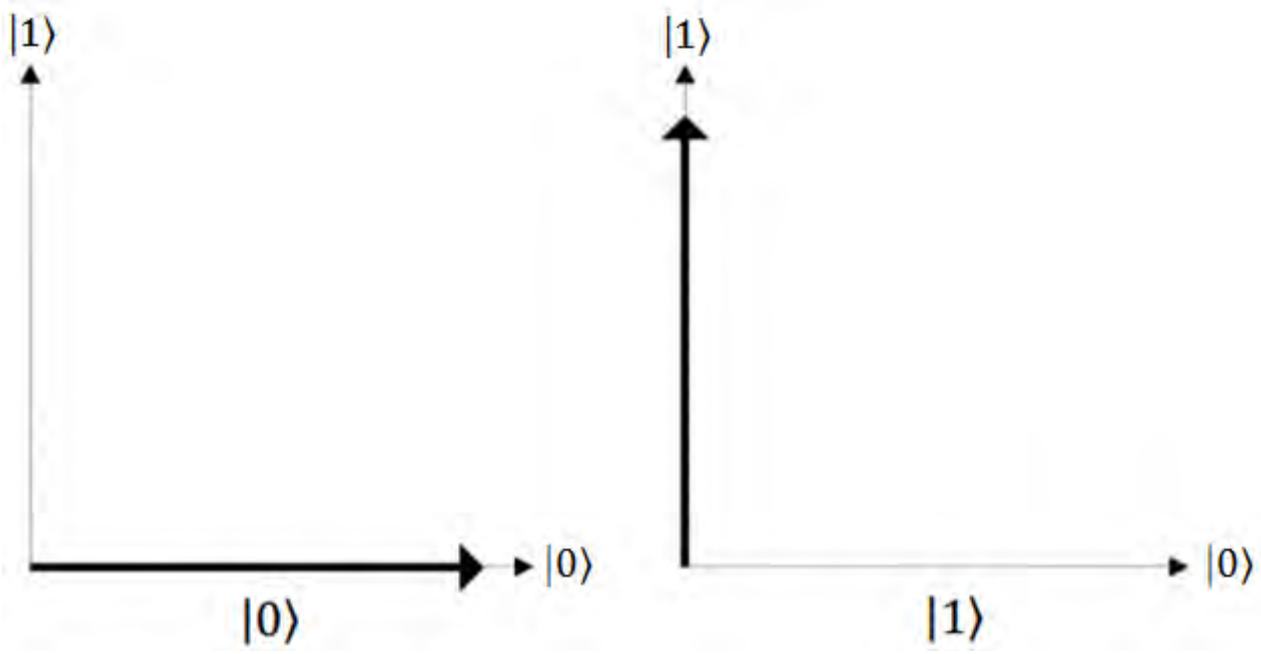
$$P(\lambda_i) = |\langle e_i|\psi\rangle|^2$$

1.3 Τα Qubits

Τα διακριτά στοιχεία πληροφορίας στα ψηφιακά συστήματα παριστάνονται από φυσικές ποσότητες που ονομάζονται σήματα. Τα σήματα σε όλους τους σύγχρονους ψηφιακούς υπολογιστές έχουν μόνο δύο διακριτές τιμές και γι΄αυτό τα ονομάζουμε δυαδικά. Εξαιτίας του υλικού οι υπολογιστές απεικονίζουν τα πάντα με δυαδικά ψηφία, τα γνωστά bits. Ένα bit πληροφορίας μπορεί να πάρει μόνο δύο τιμές, «0» και «1». Στους κβαντικούς υπολογιστές, μονάδα

πληροφορίας είναι το κβαντικό bit (quantum bit) ή αλλιώς qubit. Το qubit είναι ένα κβαντικό σύστημα δύο καταστάσεων. Οι δύο βασικές καταστάσεις του qubit συμβολίζονται με |0⟩ και |1⟩.

Τα διανύσματα κατάστασης μπορούν να αναπαρασταθούν σε ένα σύστημα δύο αξόνων (Σχήμα 1), όπου ο οριζόντιος είναι το |0⟩ και ο κάθετος είναι το |1⟩. Το |0⟩ αντιπροσωπεύεται σε αυτό το σύστημα με γραμμή που εφάπτεται στον οριζόντιο άξονα και το |1⟩ με γραμμή που εφάπτεται στον κάθετο άξονα.



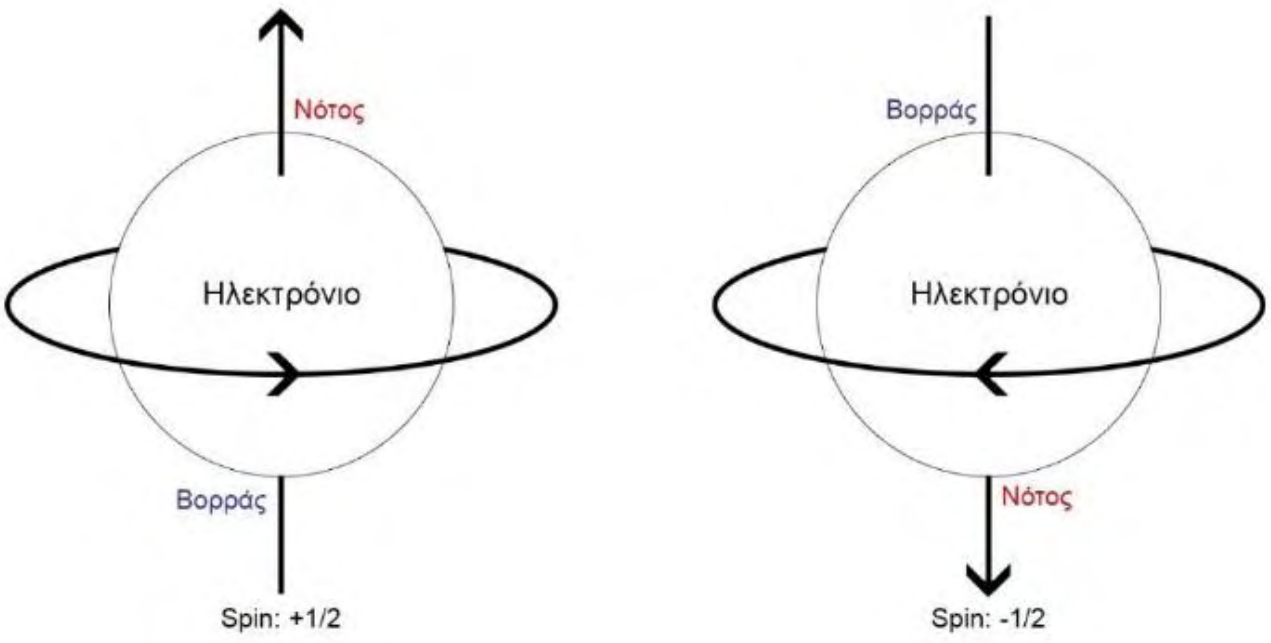
Σχ.1 Γραφικές απεικονίσεις των διανυσμάτων κατάστασης 0 και 1

Στην κβαντομηχανική ένα σωμάτιο μπορεί να βρίσκεται οπουδήποτε, ακόμη και σε πολλά σημεία στο χώρο ταυτόχρονα. Από τη στιγμή όμως που θα μετρήσουμε ένα φυσικό μέγεθος (δηλαδή μια ιδιοτιμή ενός τελεστή) εντοπίζουμε το σωμάτιο, επηρεάζουμε δηλαδή την κίνησή του και η περαιτέρω χρονική εξέλιξη αρχίζει από τη στιγμή της μέτρησης. Αυτό εξηγεί και το γεγονός ότι το qubit μπορεί να είναι συγχρόνως 0 και 1 σε αντίθεση με το κλασικό bit.

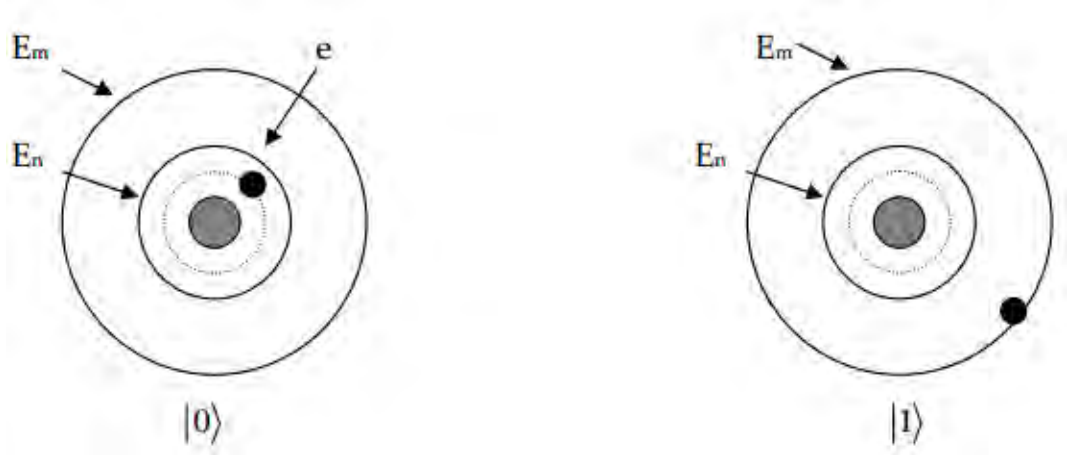
Υπάρχουν αρκετά κβαντικά συστήματα δύο διακριτών καταστάσεων τα οποία μπορούν να χρησιμοποιηθούν ως qubits. Για παράδειγμα η κατάσταση του spin ενός σωματιδίου με spin ½ μπορεί να θεωρηθεί ως qubit, όπου η κατάσταση

spin +1/2 αντιστοιχεί στην βασική κατάσταση |1⟩ και η κατάσταση spin -1/2 στην βασική κατάσταση |0⟩ (Σχήμα 2):

$$|+1/2\rangle \rightarrow |1\rangle \text{ και } |-1/2\rangle \rightarrow |0\rangle$$



Σχ.2 Τα δύο διαφορετικά spin ενός ηλεκτρονίου.

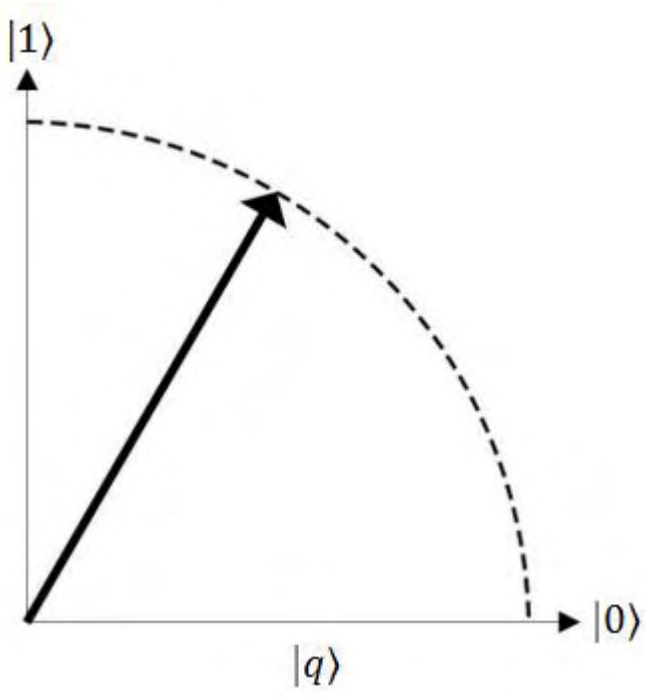


Σχ.3 Αναπαράσταση ενός qubit από δύο διακριτά ενεργειακά επίπεδα Em και En σε ένα άτομο.

Η διεύθυνση πόλωσης ενός φωτονίου μπορεί να αναπαραστήσει ένα qubit, όπου η οριζόντια πόλωση αντιστοιχεί στην κατάσταση |0⟩ και η κάθετη στην κατάσταση |1⟩. Ένα qubit μπορεί να αναπαρασταθεί και από δύο διακριτά

ενεργειακά επίπεδα, Em και En, σε ένα άτομο, όπως φαίνεται και στο Σχήμα 3. Η παρουσία ενός ηλεκτρονίου με ενέργεια ίση με Em αντιστοιχεί στην κατάσταση $|1\rangle$ και η παρουσία ενός ηλεκτρονίου με ενέργεια ίση με En αντιστοιχεί στην κατάσταση $|0\rangle$.

Η αρχική κατάσταση ενός qubit είναι πάντα μία από τις δύο λογικές καταστάσεις. Χρησιμοποιώντας κατάλληλες διαδικασίες (πύλες Hadamard), όπως θα δούμε και παρακάτω, μπορούμε να μεταβούμε σε ένα γραμμικό συνδυασμό (υπέρθεση) των λογικών καταστάσεων. Οι υπερθέσεις αυτές εκφράζονται σαν αθροίσματα της μορφής $a|0\rangle + b|1\rangle$, όπου a, b είναι μιγαδικοί αριθμοί που αναπαριστούν πλάτη πιθανότητας της αντίστοιχης λογικής κατάστασης. Η ύπαρξη τέτοιων καταστάσεων είναι από τις βασικές αρχές της κβαντικής θεωρίας και ονομάζεται αρχή της υπέρθεσης, για την αναπαράσταση της οποίας το διάνυσμα κατάστασης απεικονίζεται με διεύθυνση ανάμεσα στους δύο άξονες (Σχήμα 4).



Σχ. 4 Το διάνυσμα κατάστασης της υπέρθεσης $|q\rangle$

Όπως αναφέρθηκε στο τρίτο σχήμα που παρουσιάστηκε, το qubit μπορεί να βρεθεί σε οποιαδήποτε υπέρθεση των δύο βασικών καταστάσεων:

$$|q\rangle = \alpha|0\rangle + b|1\rangle, \text{ (1)}$$

όπου η προβολή του διανύσματος της κατάστασης της υπέρθεσης στον άξονα $|0\rangle$ έχει μήκος α και στον άξονα $|1\rangle$ έχει μήκος b. Όταν γίνει παρατήρηση για να βρεθεί η τιμή μιας κατάστασης που βρίσκεται σε υπέρθεση δύο άλλων βασικών καταστάσεων, όπως είναι η $|q\rangle$, υπάρχει αβεβαιότητα για την τιμή που θα παρατηρηθεί. Εδώ βρίσκεται και η μεγάλη διαφορά ανάμεσα στους κλασσικούς και στους κβαντικούς υπολογιστές. Ενώ στους κλασσικούς υπολογιστές η τιμή της βασικής μονάδας της πληροφορίας παρατηρείται με ακρίβεια, είτε 0 είτε 1, στους κβαντικούς υπολογιστές δε συμβαίνει αυτό. Στους τελευταίους, λόγω της υπέρθεσης, το σύστημα-μονάδα πληροφορίας βρίσκεται στις δύο καταστάσεις $|0\rangle$ και $|1\rangle$ ταυτόχρονα και η τιμή που θα ανιχνευθεί εξαρτάται από κάποιες πιθανότητες.

Η πιθανότητα το qubit να βρίσκεται στην κατάσταση $|0\rangle$ είναι $|a|^2$ ενώ η πιθανότητα να βρίσκεται στην κατάσταση $|1\rangle$ είναι $|b|^2$. Η συνολική λοιπόν πιθανότητα το σύστημα να βρίσκεται είτε στην κατάσταση $|1\rangle$ είτε στην κατάσταση $|0\rangle$ είναι 1. Παρόλα αυτά, η μέτρηση για την εύρεση της τιμής της κατάστασης είναι καταστροφική για την υπέρθεση, γιατί μετά από αυτή το σύστημα μπορεί να βρίσκεται μόνο σε μία από τις δύο βασικές καταστάσεις.
Σύμφωνα με τα παραπάνω και σε συνδυασμό με την θεωρία πιθανοτήτων, αφού οι δύο πιθανότητες είναι $|a|^2$ και $|b|^2$ και αυτά είναι τα μοναδικά αποτελέσματα που μπορεί να προκύψουν, έχουμε την εξίσωση: $|a|^2 + |b|^2 = 1$. (2)

Συνεπώς, το διάνυσμα κατάστασης κινείται πάνω σε έναν κύκλο ακτίνας μήκους 1, όπου κάθε διαφορετική διεύθυνση αντιστοιχεί σε διαφορετικές πιθανότητες και πλάτη πιθανοτήτων.

Προκειμένου να αποσαφηνίσουμε την έννοια των qubits, είναι χρήσιμο να εξετάσουμε τα είδη φυσικών συστημάτων που θα μπορούσαν να αποτελούν το κβαντικό υλισμικό. Στον Πίνακα 1 παρουσιάζονται κάποια από τα πιο σημαντικά συστήματα που έχουν εξεταστεί σε αυτό το πλαίσιο. Σε όλες τις περιπτώσεις έχουμε ένα μεμονωμένο κβαντικό σύστημα με δύο σαφώς διακρίσιμες

καταστάσεις. Προκειμένου να είναι το σύστημα χρησιμοποιήσιμο, απαιτούμε η επιλεγμένη ιδιότητα να είναι εύκολα μετρήσιμη, και οι δύο καταστάσεις να είναι ορθογώνιες μεταξύ τους, δηλαδή $\langle 0|1\rangle = 0$.

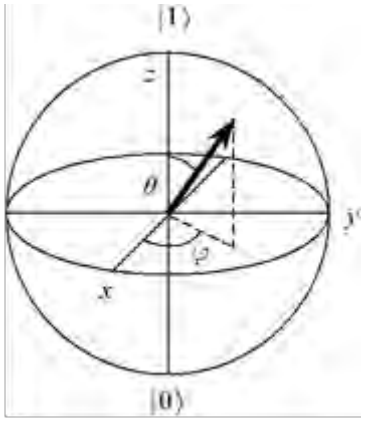
Κβαντικό σύστημα	Φυσική ιδιότητα	$\|0\rangle$	$\|1\rangle$
Φωτόνιο	Γραμμική πόλωση	Οριζόντια	Κατακόρυφη
Φωτόνιο	Κυκλική πόλωση	Αριστερή	Δεξιά
Πυρήνας	Σπιν	Πάνω	Κάτω
Ηλεκτρόνιο	Σπιν	Πάνω	Κάτω
Διασταθμικό άτομο	Κατάσταση διέγερσης	Θεμελιώδης	Διεγερμένη
Επαφή Josephson	Ηλεκτρικό φορτίο	*N* ζεύγη Cooper	*N* + 1 ζεύγη Cooper
Υπεραγώγιμος βρόχος	Μαγνητική ροή	Πάνω	Κάτω

Πίνακας 1: Μερικές φυσικές πραγματώσεις qubits

Από τη συνθήκη κανονικοποίησης της Εξ.2, αντιλαμβανόμαστε ότι μπορούμε να αναπαραστήσουμε την κατάσταση ενός μεμονωμένου qubit με τη μορφή διανύσματος που ονομάζεται διάνυσμα Bloch. Το διάνυσμα Bloch διαγράφει μια σφαίρα μοναδιαίας ακτίνας που ονομάζεται σφαίρα Bloch (Σχήμα 5). Τα σημεία της σφαίρας Bloch ορίζονται από τις πολικές τους γωνίες (θ,φ), όπου θ και φ είναι πραγματικοί αριθμοί και $0 \leq \theta \leq \pi$ και $0 \leq \varphi \leq 2\pi$. Η γωνία θ καθορίζει τις τιμές των πλατών πιθανότητας και τις πιθανότητες εμφάνισης της κάθε βασικής κατάστασης. Η γωνία φ ονομάζεται γωνία φάσης. Ο βόρειος πόλος (θ=0) και ο νότιος πόλος (θ=π) της σφαίρας ορίζονται έτσι ώστε να αντιπροσωπεύουν τις καθαρές καταστάσεις $|1\rangle$ και $|0\rangle$, αντίστοιχα. Όλες οι άλλες τιμές της θ αντιστοιχούν σε καταστάσεις υπέρθεσης του τύπου της Εξ.1

Η αντιστοίχιση ανάμεσα στους συντελεστές πλάτους και στις πολικές γωνίες μπορεί να γίνει ρητή αν θέσουμε

$$\alpha = \sin(\theta/2)$$
$$b = e^{i\varphi}\cos(\theta/2)$$



Σχ.5 Η αναπαράσταση qubits μέσω της σφαίρας Bloch. Οι καταστάσεις των qubits αντιστοιχούν σε σημεία της επιφάνειας της σφαίρας· η κατάσταση $|0\rangle$ *βρίσκεται στο νότιο πόλο, η κατάσταση* $|1\rangle$ *στο βόρειο πόλο, και οι καταστάσεις υπέρθεσης σε όλα τα άλλα σημεία.*

Μια σημαντική παρατήρηση αφορά το γεγονός ότι σε μία μόνο μέτρηση δεν μπορεί κάποιος να ξεχωρίσει δύο qubits τα οποία διαφέρουν μόνο κατά τη γωνία φάσης. Αυτό συμβαίνει γιατί οι πιθανότητες εμφάνισης μιας βασικής κατάστασης και τα πλάτη αυτών, τα οποία είναι τα μετρήσιμα μεγέθη, δεν περιέχουν τη γωνία φάσης φ. Παρόλα αυτά, η γωνία φάσης παίζει πολύ σημαντικό ρόλο.

Ένας άλλος χρήσιμος τρόπος για να αναπαραστήσουμε την κατάσταση ενός μεμονωμένου qubit που διέπεται από την κυματοσυνάρτηση της Εξ.1 είναι μέσω ενός διανύσματος στήλης της μορφής πινάκων και έχουμε την αντιστοίχιση:

$$|0\rangle \leftrightarrow \begin{bmatrix}1\\0\end{bmatrix}$$

$$|1\rangle \leftrightarrow \begin{bmatrix}0\\1\end{bmatrix}$$

$$\alpha|0\rangle + b|1\rangle \leftrightarrow \begin{bmatrix}a\\b\end{bmatrix}$$

Αυτή η αναπαράσταση μέσω διανυσμάτων στήλης μας επιτρέπει να αναπαριστούμε τις πράξεις που εκτελούνται στα qubits μέσω πινάκων 2×2, πράγμα που απλοποιεί την τυπική πραγμάτευση.

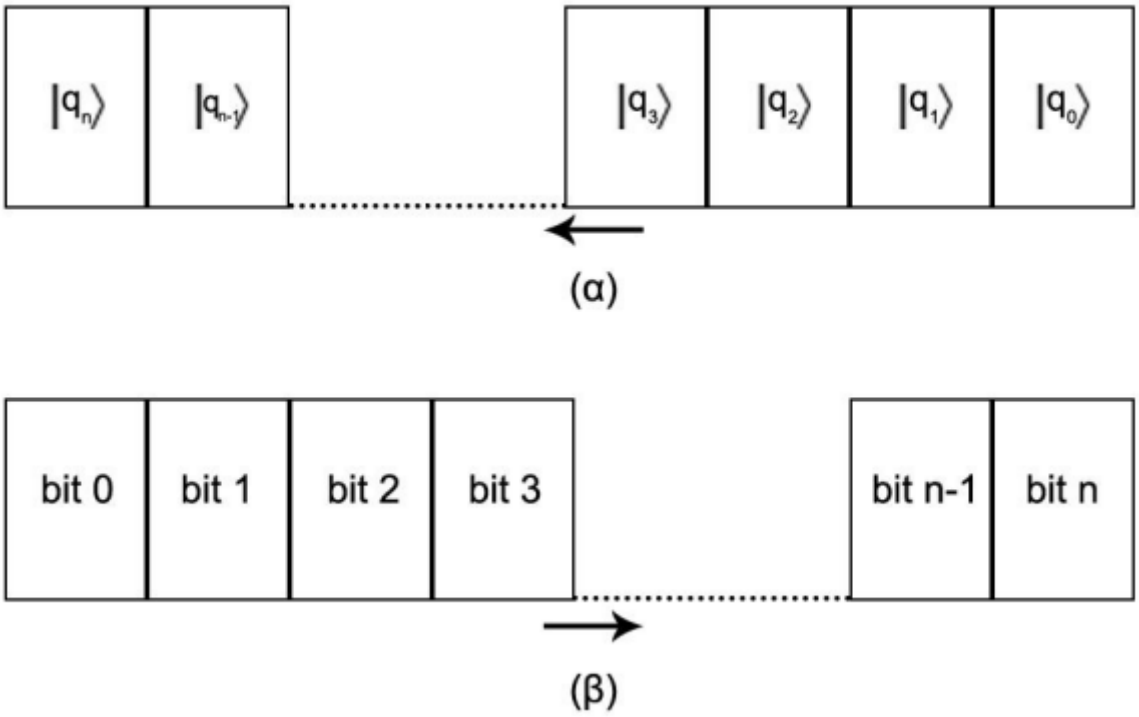
Γενικά τα qubits είναι εξαιρετικά ευαίσθητα. Τυχαίες αλληλεπιδράσεις με το περιβάλλον τους, υποβαθμίζουν τις υπερθέσεις εξαιρετικά γρήγορα, μετατρέποντάς τις σε τυχαία διατεταγμένα συνηθισμένα bits. Το κβαντικό bit

μπορεί να φαίνεται ότι περιέχει άπειρη ποσότητα πληροφορίας, αφού περιγράφεται με 2 συνεχείς βαθμούς ελευθερίας, όμως αυτή δεν εξάγεται, αφού με τυχόν μέτρηση η υπέρθεση καταρρέει και αυτή η πληροφορία χάνεται. Η πληροφορία αυτή δεν μπορεί καν να αντιγραφεί (θεώρημα μη κλωνοποίησης). Αυτό δηλαδή σημαίνει ότι μία άγνωστη κβαντική κατάσταση δεν μπορεί να αντιγραφεί σε μία άλλη. Απαγορεύεται η αναπαραγωγή μίας κατάστασης υπέρθεσης. Παρακάτω θα εξηγηθεί αυτό το γεγονός με το φαινόμενο της διεμπλοκής (entanglement).

1.4 Κβαντικός καταχωρητής

Στο κλασσικό μοντέλο αρχιτεκτονικής των μοντέρνων υπολογιστών, η οποία ονομάζεται Von Neumman, οι καταχωρητές (registers) είναι διατάξεις στις οποίες αποθηκεύονται μικρές ποσότητες πληροφορίας με τη μορφή bits. Χρησιμοποιούνται κυρίως στην κεντρική μονάδα επεξεργασίας (CPU) και υπάρχουν διάφοροι τύποι, π.χ. για αποθήκευση εντολών ή για αποθήκευση δεδομένων. Βρίσκονται στην κορυφή της ιεραρχίας των μνημών, όντας οι ταχύτερα προσπελάσιμες μνήμης. Ένας καταχωρητής αποτελείται από ένα σύνολο bits για την αποθήκευση μικρών τμημάτων πληροφορίας.

Παρόμοια με τον καταχωρητή του ψηφιακού υπολογιστή, ο καταχωρητής ενός κβαντικού υπολογιστή αποτελείται από ένα σύστημα πολλών qubits, συνήθως τοποθετημένα σε σειρά, μετρώντας από δεξιά προς τα αριστερά, σε αντίθεση με τα bits του κλασσικού καταχωρητή (Σχήμα 6).



Σχήμα 6: (α) Ένας κβαντικός καταχωρητής, μετρώντας από δεξιά προς τα αριστερά
(β) Ένας κλασσικός καταχωρητής, μετρώντας από αριστερά προς τα δεξιά

Αρχικά, πρέπει να οριστεί η έννοια του τανυστικού γινομένου. Θα ορισθεί για πίνακες με μία στήλη και δύο γραμμές. Το τανυστικό γινόμενο δύο πινάκων, μιας στήλης και δύο γραμμών, $A = \begin{bmatrix} a \\ b \end{bmatrix}$ και $B = \begin{bmatrix} c \\ d \end{bmatrix}$, ορίζεται ακολούθως, ως:

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

Όπως διακρίνεται, το αποτέλεσμα του τανυστικού γινομένου των δύο πινάκων, είναι ένας νέος πίνακας με πλήθος στοιχείων ίσο με το άθροισμα των στοιχείων των δύο προηγούμενων πινάκων.

Προχωρώντας στον κόσμο των qubits, με τη βοήθεια του τανυστικού γινομένου μπορούμε να βρούμε τις βασικές καταστάσεις ενός κβαντικού καταχωρητή που αποτελείται από n qubits καθώς και τα πλάτη πιθανότητας της κάθε κατάστασης. Κατόπιν εξετάζεται η απλούστερη περίπτωση, στην οποία ο καταχωρητής αποτελείται από δύο qubits. Έστω αυτά είναι τα q_0 και q_1, καθένα με το εξής διάνυσμα κατάστασης:

$$|q_1\rangle = a|0\rangle + b|1\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \kappa\alpha\iota\ |q_0\rangle = c|0\rangle + d|1\rangle = \begin{bmatrix} c \\ d \end{bmatrix}$$

Ο καταχωρητής των δύο παραπάνω qubits περιγράφεται από τη σχέση, που περιγράφει το διάνυσμα κατάστασης του καταχωρητή:

$$|q_{reg}\rangle = |q_1\rangle \otimes |q_0\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot c \\ b \cdot d \end{bmatrix}$$

Αναλυτικότερα, έχουμε:

$$\begin{aligned} |q_{reg}\rangle = |q_1\rangle \otimes |q_0\rangle &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) = \\ &= (ac) \cdot |0\rangle \otimes |0\rangle + (ad) \cdot |0\rangle \otimes |1\rangle + (bc) \cdot |1\rangle \otimes |0\rangle + (bd) \cdot |1\rangle \otimes |1\rangle = \\ &= (ac) \cdot |00\rangle + (ad) \cdot |01\rangle + (bc) \cdot |10\rangle + (bd) \cdot |11\rangle \end{aligned}$$

Συμπερασματικά, ο κβαντικός καταχωρητής που αποτελείται από δύο qubits είναι ένα κβαντικό σύστημα τεσσάρων βασικών καταστάσεων, οι οποίες είναι η $|00\rangle$, η $|01\rangle$, η $|10\rangle$ και η $|11\rangle$. Καθεμιά τους βρίσκεται ως το τανυστικό γινόμενο των δύο βασικών καταστάσεων των qubits. Η αναπαράστασή τους σε πίνακα είναι:

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

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

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

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

Οι τέσσερεις αυτές βασικές καταστάσεις έχουν η καθεμιά ξεχωριστά πλάτη πιθανότητας, τα οποία είναι μιγαδικοί αριθμοί, αλλά και ξεχωριστές πιθανότητες εμφάνισης.

Βασική Κατάσταση	Πλάτος πιθανότητας	Πιθανότητα εμφάνισης
$\|00\rangle$	$a \cdot c$	$\|a \cdot c\|^2$
$\|01\rangle$	$a \cdot d$	$\|a \cdot d\|^2$
$\|10\rangle$	$b \cdot c$	$\|b \cdot c\|^2$
$\|11\rangle$	$b \cdot d$	$\|b \cdot d\|^2$

Πίνακας 2: Πλάτη πιθανότητας και πιθανότητες εμφάνισης των διαφορετικών βασικών καταστάσεων ενός καταχωρητή των 2 qubits.

Έτσι, ύστερα από μία μέτρηση για να βρεθεί η κατάσταση του καταχωρητή, η κάθε βασική κατάσταση έχει τη δική της πιθανότητα εμφάνισης και η υπέρθεση καταστρέφεται. Τέλος, βάσει της θεωρίας πιθανοτήτων, το άθροισμα των πιθανοτήτων εμφάνισης των τεσσάρων μοναδικών καταστάσεων που μπορεί να εμφανιστούν, ισούται με 1:

$$|a \cdot c|^2 + |a \cdot d|^2 + |b \cdot c|^2 + |b \cdot d|^2 = 1$$

Το διάνυσμα κατάστασης του κβαντικού καταχωρητή βρίσκεται σε ένα χώρο Hilbert τεσσάρων διαστάσεων και έχει μήκος 1. Φυσικά δεν μπορεί να αναπαρασταθεί με τη χρήση της σφαίρας Bloch αλλά με κανέναν άλλο τρόπο ο οποίος να είναι αντιληπτός και κατανοητός από τον ανθρώπινο εγκέφαλο.

Όσον αφορά το θέμα σύγκρισης το θέμα σύγκρισης της χωρητικότητας του κβαντικού καταχωρητή δύο qubits και του κλασσικού καταχωρητή των δύο bits, πρέπει να τονιστεί η μεγάλη διαφορά που παρουσιάζουν στη δυνατότητα αποθήκευσης πληροφοριών. Ενώ ο κλασσικός καταχωρητής των δύο bits μπορεί να αποθηκεύσει το πολύ ένα δυαδικό αριθμό (είτε τον 00, ή τον 01, ή τον 10, ή τον 11), το μέγιστο που ο κβαντικός καταχωρητής μπορεί να αποθηκεύσει είναι τέσσερεις δυαδικοί αριθμοί ταυτόχρονα, τον 00($|00\rangle$), τον 01($|01\rangle$), τον 10($|10\rangle$), τον 11($|11\rangle$). Το φαινόμενο αυτό ονομάζεται κβαντική παραλληλία

και αποτελεί ένα από τα σημαντικότερα φαινόμενα των κβαντικών υπολογιστών.

Ένας άλλος συμβολισμός που χρησιμοποιείται ευρύτατα είναι η αντικατάσταση της κατάστασης του καταχωρητή από δυαδική μορφή σε δεκαδική, κατά τα γνωστά πρότυπα. Ως εκ τούτου, προκύπτει η εξής αναλογία για την περίπτωση του καταχωρητή των δύο qubits:

Δυαδική μορφή		Δεκαδική μορφή
$\|00\rangle$	→	$\|0\rangle$
$\|01\rangle$	→	$\|1\rangle$
$\|10\rangle$	→	$\|2\rangle$
$\|11\rangle$	→	$\|3\rangle$

Πίνακας 3: Αναλογία μεταξύ της δυαδικής και δεκαδικής απεικόνισης του καταχωρητή των 2 qubits.

Τα πλάτη πιθανότητας μπορεί να γραφούν ως c_j, όπου j είναι η δεκαδική μορφή της αντίστοιχης κατάστασης. Συνεπώς, η εξίσωση του διανύσματος κατάστασης του κβαντικού καταχωρητή γίνεται:

$$\begin{aligned}\left|q_{reg}\right\rangle &= |q_1\rangle \otimes |q_0\rangle = (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= (ac)\cdot|00\rangle + (ad)\cdot|01\rangle + (bc)\cdot|10\rangle + (bd)\cdot|11\rangle \\ &= (ac)\cdot|0\rangle + (ad)\cdot|1\rangle + (bc)\cdot|2\rangle + (bd)\cdot|3\rangle \\ &= c_0|0\rangle + c_1|1\rangle + c_2|2\rangle + c_3|3\rangle \\ &= \sum_{i=0}^{3} c_i\,|i\rangle\end{aligned}$$

Από τα παραπάνω μπορούν να εξαχθούν γενικά συμπεράσματα για τις ιδιότητες ενός κβαντικού καταχωρητή n qubits. Πρωτίστως, ο κβαντικός αυτός καταχωρητής έχει 2^n βασικές καταστάσεις και μπορεί να αποθηκεύσει 2^n αριθμούς ταυτόχρονα. Ακόμα για το διάνυσμα κατάστασης, ισχύει:

$$|q_{reg}\rangle = |q_{n-1}\rangle \otimes \dots |q_3\rangle \otimes |q_2\rangle \otimes |q_1\rangle \otimes |q_0\rangle = \sum_{i=0}^{2^n-1} c_i,$$

όπου οι βασικές καταστάσεις του καταχωρητή είναι συνδυασμοί των βασικών καταστάσεων των qubits που τον αποτελούν, i είναι ένας δεκαδικός αριθμός που δηλώνει τη βασική κατάσταση του καταχωρητή όπως περιγράφηκε παραπάνω και c_i είναι το πλάτος πιθανότητας για την κάθε βασική κατάσταση του καταχωρητή. Το παραπάνω διάνυσμα κατάστασης του καταχωρητή βρίσκεται σε χώρο Hilbert 2^n διαστάσεων και έχει μήκος ίσο με τη μονάδα. Για τις πιθανότητες εμφάνισης των διαφόρων βασικών καταστάσεων ισχύει:

$$\sum_{i=0}^{2^n-1} |c_i|^2 = |c_0|^2 + |c_1|^2 + |c_2|^2 + \dots + |c_{2^n-1}|^2 = 1$$

1.5 Κβαντική διεμπλοκή (entanglement)

Κβαντική διεμπλοκή (entanglement), ονομάζεται το φαινόμενο κατά το οποίο η κατάσταση δύο ή περισσοτέρων κβαντικών bit δεν μπορεί να περιγραφεί σαν συνδυασμός των καταστάσεων του κάθε bit ξεχωριστά. Διεμπλοκή μπορεί να δημιουργηθεί από διάφορους κβαντικούς μετασχηματισμούς που διενεργούνται σε περισσότερα του ενός bit .

Όταν τα bit p και q είναι συμπλεγμένα ο προσδιορισμός της τιμής του ενός μας δίνει πληροφορία για την κατάσταση του άλλου. Όταν δύο κβαντικά bit δεν είναι συμπλεγμένα λέγονται ανεξάρτητα. Σε αυτή την περίπτωση η κατάσταση ενός καταχωρητή που τα περιέχει μπορεί να δοθεί αν πολλαπλασιάσουμε τους αντίστοιχους συντελεστές των δύο qubit. Μαθηματικά δηλαδή, λέμε ότι δύο συστήματα βρίσκονται σε κβαντική διεμπλοκή, όταν η κατάστασή τους δεν μπορεί να γραφεί σαν τανυστικό γινόμενο των βασικών τους καταστάσεων. Αυτή η μαθηματική πρόταση αναλύεται παρακάτω με ένα παράδειγμα:

Ας θεωρήσουμε ότι έχουμε δύο qubits, το $|q_{e0}\rangle$ και το $|q_{e1}\rangle$, τα οποία βρίσκονται στην κατάσταση $|q_e\rangle$ που δίνεται από:

$$|q_e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Η $|q_e\rangle$ δεν μπορεί, όπως φαίνεται εύκολα, να γραφεί σαν τανυστικό γινόμενο των καταστάσεων των δύο qubits, οπότε τα $|q_{e0}\rangle$ και $|q_{e1}\rangle$ βρίσκονται σε κβαντική διεμπλοκή. Αυτό σημαίνει πως 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 στην 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 το βρούμε στην 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. Αυτή η απόλυτη συσχέτιση ισχύει πάντα ανεξάρτητα με τον τρόπο που γίνεται η μέτρηση (π.χ. εάν τα qubits υλοποιούνται μέσω συστήματος σπιν ½, τότε ανεξάρτητα από τον άξονα μέτρησης του σπιν για τα δύο σωματίδια θα παίρνουμε πάντα συσχετισμένα αποτελέσματα). Η συσχέτιση ισχύει ανεξάρτητα και από την χωρική απόσταση των δύο qubits.

1.6 Κβαντικές πύλες

Οι κλασικοί υπολογιστές 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 αποτελούνται από τρανζίστορ.

Στους κβαντικούς υπολογιστές οι κβαντικές πύλες αντιπροσωπεύουν δράσεις που ασκούνται σε qubits ή σε κβαντικούς καταχωρητές. Οι δράσεις στα κβαντικά συστήματα αντιπροσωπεύονται από τελεστές οι οποίοι περιγράφονται από πίνακες. Μία άλλη σημαντική διαφορά είναι ότι η πληροφορία δε διέρχεται μέσα από τις κβαντικές πύλες. Η πληροφορία βρίσκεται αποθηκευμένη σε qubits ή σε κβαντικούς καταχωρητές και παραμένει εκεί.

Στους κβαντικούς υπολογιστές το κάθε qubit χαρακτηρίζεται από υπέρθεση της κατάστασης $|0\rangle$ και $|1\rangle$. Η κβαντική πύλη θα είναι ένα είδος κυκλώματος, το οποίο πραγματοποιεί πράξεις σε qubits για κάποιο χρονικό διάστημα, ενώ σε αντίθεση με τις κλασικές, είναι *πάντα* αντιστρεπτές άρα θα έχουν τον ίδιο αριθμό εισόδων και εξόδων. Παρακάτω αναφέρονται μόνο ονομαστικά οι βασικές κβαντικές πύλες ενώ στο επόμενο κεφάλαιο παρουσιάζεται η λειτουργία της κάθε πύλης αναλυτικά.

Κβαντικές πύλες

- Κβαντική πύλη αδράνειας
- Κβαντική πύλη μετατόπισης φάσης
- Κβαντική πύλη Hadamard
- Κβαντική πύλη ελεγχόμενης άρνησης (CNOT)
- Κβαντική πύλη ελεγχόμενης μετατόπισης φάσης
- Κβαντική πύλη διπλά ελεγχόμενης άρνησης (CCNOT)
- Κβαντική πύλη Fredkin

ΚΕΦΑΛΑΙΟ 2

2. ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ

2.1 Εισαγωγή στους κβαντικούς υπολογιστές

Η ιδέα για τη δημιουργία ενός υπολογιστή που θα βασίζεται στις αρχές της κβαντομηχανικής διατυπώθηκε στις αρχές της δεκαετίας του ’80, όταν οι φυσικοί Richard Feynman, David Deutsch και Paul Benioff διαπίστωσαν ότι οι κλασικοί υπολογιστές είχαν βασικούς περιορισμούς στο χρόνο και στη μνήμη για την εκπόνηση βασικών λειτουργιών. Κατανόησαν ότι η συνεχής συρρίκνωση των στοιχείων που συσκευάζονται επάνω στα τσιπ πυριτίου θα έφθανε σε ένα σημείο όπου τα μεμονωμένα στοιχεία δεν θα ήταν μεγαλύτερα από μερικά άτομα. Η συνεχής μείωση, με λιθογραφικές τεχνικές, των διαστάσεων θα μπορούσε να φτάσει στις διαστάσεις των ατόμων και οι υπολογιστές θα μπορούσαν να κατασκευαστούν από το ίδιο το άτομο με παρουσία κβαντικών κανόνων.

Ο Feynman ήταν ο πρώτος που προσπάθησε να δώσει λύση στο παραπάνω θέμα με την παραγωγή ενός προτύπου που έδειχνε πώς ένα κβαντικό σύστημα θα μπορούσε να χρησιμοποιηθεί για να κάνει υπολογισμούς. Σύμφωνα με το πρότυπό του, ένας φυσικός θα μπορούσε να πραγματοποιήσει πειράματα στην κβαντική φυσική μέσα από έναν κβαντικό υπολογιστή.

Πώς υλοποιείται ένας κβαντικός υπολογιστής; Στους κλασικούς υπολογιστές η πληροφορία κωδικοποιείται σε μία σειρά από bits τα οποία μέσω των λογικών πυλών μετασχηματίζονται για να παράγουν ένα τελικό αποτέλεσμα. Ομοίως, ένας κβαντικός υπολογιστής χειρίζεται τα qubits μέσω των κβαντικών πυλών που υλοποιούν μετασχηματισμούς σε ένα ή σε ζευγάρι qubits. Τοποθετώντας τις κβαντικές πύλες σε μία συγκεκριμένη σειρά ένας κβαντικός υπολογιστής μπορεί να υλοποιήσει περίπλοκους μετασχηματισμούς σε μία σειρά από qubits από μία αρχική κατάσταση στην τελική. Έπειτα τα qubits μπορούν να μετρηθούν στην τελική τους κατάσταση και από τις μετρήσεις αυτές να εξαχθεί ένα τελικό

υπολογιστικό αποτέλεσμα.

Τελικά η ομοιότητα στον υπολογισμό μεταξύ κλασικού και κβαντικού υπολογιστή θεωρητικά μπορεί να μας οδηγήσει στο συμπέρασμα ότι ένας κλασικός υπολογιστής μπορεί να προσομοιώσει ακριβώς έναν κβαντικό υπολογιστή. Όμως η προσομοίωση ενός κβαντικού υπολογιστή από έναν κλασικό είναι ένα *υπολογιστικά δύσκολο* πρόβλημα (δηλαδή ένα πρόβλημα πολυπλοκότητας NP) επειδή οι συσχετισμοί μεταξύ των κβαντικών κομματιών είναι ποιοτικά διαφορετικοί από τους συσχετισμούς μεταξύ των κλασικών κομματιών.

2.2 Πλεονεκτήματα και εφαρμογές των κβαντικών υπολογιστών

Τα πλεονεκτήματα των κβαντικών υπολογιστών σε σχέση με τους κλασικούς είναι τα εξής:

1. Μεγαλύτερη ταχύτητα
2. Τεράστια μνήμη
3. Δυνατότητα επίλυσης ορισμένων «*υπολογιστικά δύσκολων*» κλασικών προβλημάτων (προβλήματα NP) σε πολυωνυμικό χρόνο.

2.3 Προβλήματα στην υλοποίηση κβαντικών υπολογιστών

Ο πρώτος που επινόησε έναν κβαντικό υπολογιστικό αλγόριθμο ήταν ο Peter Shor, που μπόρεσε εκμεταλλευόμενος την κβαντική δύναμη να παραγοντοποιήσει πολύ μεγάλους αριθμούς σε κλάσματα δευτερολέπτου. Αν και έχει σημειωθεί σημαντική πρόοδος από τη σύλληψη της ιδέας του κβαντικού υπολογιστή μέχρι σήμερα, ωστόσο υπάρχουν πολλά εμπόδια στην υλοποίησή του. Το κυριότερο πρόβλημα στη δημιουργία κβαντικών υπολογιστών είναι η ύπαρξη σφαλμάτων και η αντιμετώπισή τους. Το πρόβλημα που προκύπτει στη διόρθωση σφάλματος είναι ποια λάθη χρειάζονται διόρθωση (στην επόμενη παράγραφο περιγράφονται κώδικες διόρθωσης σφαλμάτων). Η απάντηση είναι πρώτιστα εκείνα τα λάθη που

προκύπτουν ως άμεσο αποτέλεσμα αποσυσχετισμού (decoherence) ή από την τάση ενός κβαντικού υπολογιστή να αποσυντεθεί από μία δεδομένη κβαντική κατάσταση σε μία ασυνάρτητη κατάσταση καθώς αλληλεπιδρά με το περιβάλλον. Αυτές οι αλληλεπιδράσεις μεταξύ του περιβάλλοντος και των qubits είναι αναπόφευκτες και προκαλούν τη διακοπή των πληροφοριών που αποθηκεύονται στον κβαντικό υπολογιστή, και έτσι τα λάθη στον υπολογισμό.

2.4 Κβαντική διόρθωση σφαλμάτων

Η διόρθωση σφαλμάτων είναι απαραίτητη στην υλοποίηση των κβαντικών υπολογιστών γιατί τα κβαντικά συστήματα αλληλεπιδρούν με το περιβάλλον. Αυτή η αλληλεπίδραση, όπως ειπώθηκε, μπορεί να οδηγήσει σε κατάρρευση του συστήματος και η ύπαρξη μηχανισμών για τη διόρθωση των λαθών είναι απαραίτητη.

Υπάρχουν δύο είδη λαθών που μπορεί να εισάγει το περιβάλλον στο σύστημα. Αυτά είναι:

- Δυαδική αντιστροφή
- Αποσυσχετισμός

2.4.1 Δυαδική αντιστροφή (Bit flip)

Αρχικά υποθέτουμε ότι το σύστημά μας αποτελείται από ένα qubit. Ένα σφάλμα που μπορεί να προκύψει είναι όμοιο με αυτό σε έναν κλασικό υπολογιστή, είναι το σφάλμα της δυαδικής αντιστροφής. Αυτό το λάθος μετατρέπει την αρχική κατάσταση π.χ. από $\alpha|0\rangle + \beta|1\rangle$ σε $\alpha|1\rangle + \beta|0\rangle$.

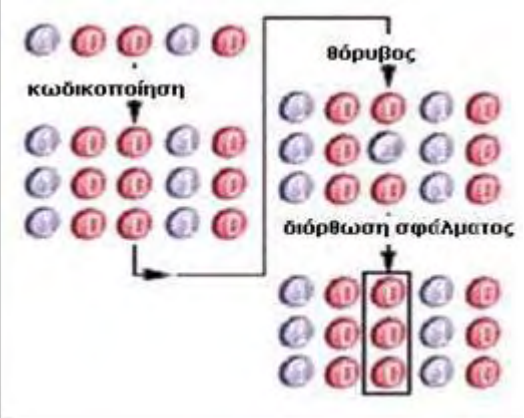
Μπορεί να διορθωθεί αυτό το λάθος χρησιμοποιώντας κλασικούς κώδικες διόρθωσης. Μπορούμε να εφαρμόσουμε έναν κλασικό κώδικα επανάληψης και να το αποφύγουμε. Είναι σημαντικό να τονίσουμε ότι η δυαδική αντιστροφή είναι μία αντιστρεπτή πράξη πάνω στα qubits και για αυτό το λόγο μπορεί εύκολα να διορθωθεί.

2.4.2 Αποσυσχετισμός

Ένα άλλο σφάλμα που ενδεχομένως να προκύψει σε έναν κβαντικό υπολογιστή είναι λόγω του φαινόμενου του αποσυσχετισμού (decoherence) των κβαντικών καταστάσεων. Σε αυτή την περίπτωση ανεπιθύμητες όσο και τυχαίες αλληλεπιδράσεις των κβαντικών καταχωρητών με το περιβάλλον οδηγούν στην κατάρρευση της κατάστασης του συστήματος. Αυτό ισοδυναμεί με «μέτρηση» του καταχωρητή η οποία είναι μία μη αντιστρεπτή διεργασία. Αν το σύστημα βρίσκεται σε μια αρχική κατάσταση και ένα δεύτερο qubit μετρηθεί, η κατάσταση του συστήματος καταρρέει και κατά συνέπεια χάνεται με μη αναστρέψιμο τρόπο η αποθηκεμένη πληροφορία. Η επίλυση αυτού του προβλήματος είναι εξαιρετικά δύσκολη και η επαναφορά του συστήματος μετά από τέτοια λάθη είναι σχεδόν αδύνατη.

2.4.3 Διόρθωση σφαλμάτων

Στους κλασικούς υπολογιστές για τον περιορισμό των σφαλμάτων, κωδικοποιείται κάθε bit ως μια τριπλέτα από όμοια bits. Αν κάποιος θόρυβος αντιστρέψει ένα bit, το σφάλμα μπορεί να αποκατασταθεί επιδιορθώνοντας το μεμονωμένο bit της τριπλέτας, όπως παρουσιάζεται στο Σχήμα 7.



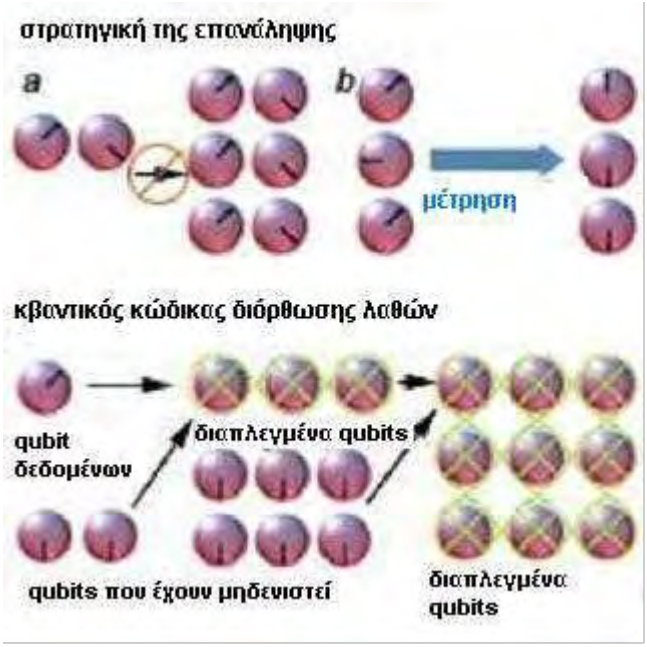
Σχ.7 Η διόρθωση στους κλασικούς υπολογιστές

Όσον αφορά τους κβαντικούς υπολογιστές, αρχικά φάνηκε ότι είναι αδύνατον να αναπτύξουμε κώδικες για την διόρθωση κβαντικών σφαλμάτων, διότι η κβαντομηχανική μας απαγορεύει να μάθουμε με βεβαιότητα την άγνωστη κατάσταση ενός κβαντικού αντικειμένου.

Ο κώδικας της απλής κλασικής τριπλέτας συνεπώς αποτυγχάνει διότι δεν μπορούμε να εξετάσουμε κάθε αντίγραφο ενός qubit χωρίς να καταστρέψουμε όλα τα αντίγραφα κατά την διαδικασία αυτή. Ακόμη χειρότερα, το να φτιάξουμε αντίγραφα στην αρχική κατάσταση δεν είναι απλό. Η κβαντομηχανική μας απαγορεύει να πάρουμε ένα άγνωστο qubit και να φτιάξουμε με αξιοπιστία ένα αντίγραφό του. Το αποτέλεσμα αυτό είναι γνωστό ως θεώρημα της αδυναμίας κλωνοποίησης.

Όμως στις αρχές 1990 ερευνητές της IBM υποστήριξαν ότι η κβαντική διόρθωση σφαλμάτων θα ήταν αναγκαία για τους κβαντικούς υπολογιστές, αλλά οι κλασικοί κώδικες δεν μπορούσαν να χρησιμοποιηθούν στον κβαντικό κόσμο. Απέδειξαν πως μπορούμε να κάνουμε κβαντική διόρθωση σφαλμάτων, χωρίς να μάθουμε ποτέ τις καταστάσεις των qubits.

Όπως και με τον κώδικα της τριπλέτας, κάθε τιμή παριστάνεται με ένα σύνολο από qubits. Τα qubits αυτά περνάνε μέσα από ένα κύκλωμα (το κβαντικό ανάλογο των λογικών πυλών) το οποίο βρίσκει με επιτυχία ένα σφάλμα στα qubits χωρίς να "διαβάσει" πραγματικά ποιες είναι οι ξεχωριστές καταστάσεις (σχηματικά φαίνεται η κβαντική διόρθωση στο Σχήμα 8).



Σχ.8 Κβαντική διόρθωση σφαλμάτων

Η προστασία των κβαντικών καταστάσεων από τον θόρυβο επιτεύχθηκε με τη χρήση ενός συνδυασμού ιδεών από την επιστήμη της πληροφορίας και από τη βασική κβαντομηχανική. Η κβαντική διόρθωση σφαλμάτων έχει δημιουργήσει επίσης πολλές ενδιαφέρουσες νέες ιδέες. Για παράδειγμα μερικά φυσικά συστήματα μπορεί να έχουν ένα τύπο φυσικής ανοχής στο θόρυβο. Αυτά τα συστήματα θα χρησιμοποιούν κβαντική διόρθωση σφαλμάτων, χωρίς την ανθρώπινη επέμβαση και θα μπορούν να επιδείξουν εξαιρετική αντίσταση στην καταστροφή της υπέρθεσης των καταστάσεων.

2.5 Τεχνολογίες κατασκευής κβαντικών υπολογιστών

Στην προσπάθειά τους να αναζητήσουν τον τρόπο κατασκευής ενός υπολογιστή που θα εκμεταλλευόταν τις αρχές της κβαντομηχανικής πολλοί ερευνητές ακολουθούν διάφορες ετερόκλητες τεχνολογίες, συμπεριλαμβανομένων των κβαντικών υπολογιστών στερεάς κατάστασης, όπως δηλαδή και οι κλασικοί, των παγίδων ιόντων (ion-traps), υπολογιστών κοιλότητας κβαντικής ηλεκτροδυναμικής (cavity QED) καθώς και του πυρηνικού μαγνητικού συντονισμού (NMR).

2.5.1 Μοριακοί υπολογιστές

Τελευταία έχει αναπτυχθεί ένα νέο είδος υπολογιστικής διαδικασίας, η οποία στηρίζεται στην κίνηση των μορίων. Ερευνητές στην IBM έχουν καταφέρει να επιδείξουν λογικές πύλες χρησιμοποιώντας μία στοιβάδα μορίων μονοξειδίου του άνθρακα για να μεταφέρει δεδομένα. Οι συσκευές που γίνονται κατ' αυτό τον τρόπο έχουν διαστάσεις στην κλίμακα των νανομέτρων (10^{-9}), μεγέθους αρκετές τάξεις μικρότερες από την τεχνολογία πυριτίου των σημερινών συμβατικών υπολογιστών.

Η πυκνότητα των συστατικών στα μικροτσίπ πυριτίου έχει αυξηθεί εκθετικά τα τελευταία σαράντα χρόνια. Οι ερευνητές της IBM έχουν υπερνικήσει αυτό το πρόβλημα, σε γενικές γραμμές, με τη χρησιμοποίηση ενός ζεύγους, χαμηλής θερμοκρασίας, ηλεκτρονικών μικροσκοπίων σάρωσης, για να διευθετήσουν ζεύγη μορίων μονοξειδίου του άνθρακα σε μια επιφάνεια του χαλκού. Μετακίνησαν ένα απλό μόριο μονοξειδίου του άνθρακα παράλληλα με ένα από αυτά τα ζεύγη, έτσι ώστε τα τρία μόρια σχημάτισαν ένα σχήμα σαν την κεφαλή ενός βέλους. Εντούτοις, ο σχηματισμός αυτός ήταν ασταθής επειδή αύξησε την ενέργεια του συστήματος.

Οι ερευνητές της IBM χρησιμοποίησαν την αρχή αυτή για να κάνουν την πύλη AND. Τοποθέτησαν τρεις σειρές ζευγών μορίων σε μια μορφή Y, με ένα απλό μόριο στο κεντρικό σημείο, όπου συναντώνται οι σειρές. Δύο σειρές ενέργησαν ως είσοδοι και η τρίτη ενεργεί ως έξοδος. Εάν υπάρχει ένας καταρράκτης και στις δύο σειρές, δηλαδή εάν υπάρχει ένα "1" και στις δύο εισόδους, μόρια θα πεταχτούν κατά μήκος των σειρών για να διαμορφώσουν την κεφαλή του βέλους με το απλό μόριο, που είναι ήδη στο σημείο όπου συναντώνται οι τρεις σειρές. Αυτή η κεφαλή έπειτα θα αποσυντεθεί, παράγοντας έναν καταρράκτη (δηλ. ένα σήμα) στην έξοδο. Οι ερευνητές χρησιμοποίησαν μια παρόμοια ρύθμιση που κάνει την πύλη OR.

Δυστυχώς οι μοριακές συσκευές καταρρακτών που έγιναν από τους

ερευνητές της IBM ήταν πολύ αργές και θα μπορούσαν μόνο να χρησιμοποιηθούν για να εκτελέσουν μια απλή λειτουργία. Για να επαναχρησιμοποιήσουν τις συσκευές αυτές οι ερευνητές έπρεπε να τοποθετήσουν τα μόρια πίσω στην αρχική θέση τους χρησιμοποιώντας ένα από τα ηλεκτρονικά μικροσκόπια σάρωσης. Για να είναι χρήσιμοι, οι μοριακοί υπολογιστές καταρρακτών θα χρειάζονταν έναν αυτόματο μηχανισμό που θα επαναρρύθμιζε μερικά από τα μόρια και θα άφηνε τα υπόλοιπα άθικτα για να ενεργήσουν ως καταχωρητές δεδομένων.

2.5.2 Παγίδες ιόντων

Μία νέα τεχνική για τη δημιουργία κβαντικών υπολογιστών είναι αυτή με τις παγίδες ιόντων. Ένας κβαντικός υπολογιστής, όπως έχουμε αναφέρει, λειτουργεί με κβαντικά bit (qubits), αντί των συνηθισμένων bit. Ένα qubit μπορεί να είναι όχι μόνο ο ή 1 αλλά και μία υπέρθεση των δύο τιμών, στην οποία οι δύο προηγούμενες τιμές συνδυάζονται σε μια ενιαία κατάσταση.

Μια σημαντική κατηγορία υπερθέσεων πολλών qubit είναι οι διαπλεγμένες καταστάσεις. Σε αυτό τις διαμορφώσεις, η κατάσταση του κάθε qubit διασυνδέεται με έναν λεπτό τρόπο με την κατάσταση του γειτονικού του. Πειράματα με τα ατομικά ιόντα περιλαμβάνουν τεράστιες ηλεκτρομαγνητικές παγίδες για να συγκρατηθούν τα ιόντα στη σειρά μέσα σε κενό. Αν και είναι καλό για τα πειράματα να γίνονται με έναν μικρό αριθμός ιόντων, είναι εντελώς αδύνατον για τα μεγάλης κλίμακας συστήματα όπως ένας κβαντικός υπολογιστής, αν θέλουμε να έχει σημαντική χρήση.

Τελευταία όμως ερευνητές έχουν δείξει μια ιοντική παγίδα μεγέθους 100 μικρών μέσα σε ένα τσιπ ημιαγωγών. Χρησιμοποίησαν το τσιπ για να παγιδέψουν ένα μόνο ιόν καδμίου και το μετακίνησαν προς διαφορετικές θέσεις στην παγίδα εφαρμόζοντας ηλεκτρικά σήματα στα ηλεκτρόδια. Η παγίδα φτιάχτηκε με τη βοήθεια της καθιερωμένης μεθόδου της λιθογραφίας. Μια ηλεκτρομαγνητική παγίδα είναι αυτή που κρατά τα ιόντα σε σειρά μέσα σε κενό, ενώ λέιζερ χειρίζονται τις καταστάσεις τους.

Σε γενικές γραμμές οι τεχνικές μπορούν να ενσωματώσουν μεγαλύτερους αριθμούς ιόντων. Ένα εμπόδιο όμως ήταν ότι η ποιότητα της πεπλεγμένης κατάστασης μειώθηκε καθώς αυξανόταν ο αριθμός των ιόντων. Για να μειώσουν αυτό το λάθος, οι ερευνητές θα μπορούσαν να ρυθμίσουν τις λεπτομέρειες των παλμών του λέιζερ, χρησιμοποιώντας διαφορετικές καταστάσεις ιόντων για την αναπαράσταση του 0 και του 1, ή να δουλέψουν με ένα διαφορετικό είδος ιόντων συνολικά.

Για να είναι χρήσιμος ένας κβαντικός υπολογιστής πρέπει όχι μόνο να μπορούμε να δημιουργούμε ειδικές καταστάσεις qubit αλλά και να τις χειριζόμαστε με τρόπο που να διατηρούνται τα κβαντικά χαρακτηριστικά τους. Δηλαδή κάποιος να μπορεί να εκτελέσει κβαντικούς αλγορίθμους στον υπολογιστή. Ένας γνωστός αλγόριθμος είναι ο κβαντικός αλγόριθμος του Grover σε ένα σύστημα δύο παγιδευμένων ιόντων καδμίου. Ο αλγόριθμος κάνει αναζήτηση μέσα σε μια βάση δεδομένων, όπου οι καταχωρήσεις έγιναν με έναν τυχαίο τρόπο. Η έρευνα ενός τυχαίου στοιχείου απαιτεί συνήθως την εξέταση κάθε καταχώρησης και άρα ο αντίστοιχος αλγόριθμος είναι τάξεως n, όπου n το μέγεθος της λίστας καταχωρήσεων. Ο κβαντικός αλγόριθμος αναζήτησης καταφέρνει το ίδιο σε αριθμό βημάτων που είναι τάξεως $n^{1/2}$.

2.5.3 Cavity QED

Μία τρίτη ερευνητική κατεύθυνση για την υλοποίηση κβαντικών υπολογιστών είναι αυτή με τη χρήση κοιλότητας κβαντικής ηλεκτροδυναμικής (cavity QED).

Πιο συγκεκριμένα, η κβαντική ηλεκτροδυναμική (QED) είναι μια κβαντική θεωρία του ηλεκτρομαγνητισμού που περιγράφει τις αλληλεπιδράσεις της ακτινοβολίας με την φορτισμένη ύλη. Η QED είναι μια σχετικιστική θεωρία από τις εξισώσεις της οποίας προκύπτουν οι εξισώσεις της ειδικής θεωρίας της σχετικότητας. Η κβαντική ηλεκτροδυναμική (που είναι βασικός κορμός των κβαντικών θεωριών

πεδίου), θεωρεί ότι η ανάπτυξη των ηλεκτρομαγνητικών δυνάμεων αποδίδεται στην εκπομπή και την απορρόφηση φωτονίων ως σωματιδίων ανταλλαγής, τα οποία αντιπροσωπεύουν διαταραχές των ηλεκτρομαγνητικών πεδίων. Κατά τρόπο ανάλογο και τα ηλεκτρόνια μπορούν να θεωρηθούν ως διαταραχές αντίστοιχων κβαντισμένων πεδίων.

Αυτά όμως τα φωτόνια είναι εικονικά (virtual) δηλαδή δεν μπορούν να φανερωθούν ή να ανιχνευθούν με κανένα τρόπο επειδή η ύπαρξή τους παραβιάζει την διατήρηση της ενέργειας και της ορμής. Η ανταλλαγή σωματιδίων είναι όμοια με τη "δύναμη" της αλληλεπίδρασης, επειδή τα αλληλεπιδρώντας σωματίδια αλλάζουν την ταχύτητα και την κατεύθυνση της κίνησης τους καθώς αυτά ελευθερώνουν ή απορροφούν την ενέργεια ενός φωτονίου.

Τα φωτόνια μπορούν επίσης να εκπεμφθούν σε μια ελεύθερη κατάσταση, οπότε μόνο σ' αυτή την περίπτωση μπορούν να παρατηρηθούν. Η αλληλεπίδραση των δύο φορτισμένων σωματιδίων συμβαίνει σε μια σειρά διαδικασιών αυξανόμενης πολυπλοκότητας. Στον απλούστερο τρόπο, μόνο ένα εικονικό φωτόνιο μπορεί να περιληφθεί. Σε μια διαδικασία δεύτερης τάξης, υπάρχουν δύο φωτόνια και ούτω καθ' εξής.

Οι διαδικασίες αντιστοιχούν σε όλους τους πιθανούς τρόπους στους οποίους μπορούν να αλληλεπιδράσουν τα σωματίδια κάνοντας ανταλλαγή εικονικών φωτονίων. Η κατασκευή των κβαντικών υπολογιστών με αυτή τη μέθοδο, συνίσταται στην παγίδευση ουδέτερων ατόμων και στην πόλωση φωτονίων, όπως περιγράφηκε παραπάνω. Η κβαντική πληροφορία αποθηκεύεται σε εσωτερικές καταστάσεις των ατόμων και είναι εύκολο να δημιουργηθούν αλληλεπιδράσεις με τα qubits.

2.5.4 Τεχνολογία NMR

Ο Πυρηνικός Μαγνητικός Συντονισμός (NMR) είναι ένα φαινόμενο που έχει χρησιμοποιηθεί για τη δημιουργία κβαντικών υπολογιστών. Η τεχνολογία NMR έχει χρησιμοποιηθεί παλιότερα σε ιατρικές εφαρμογές

και μία νέα προοπτική είναι και η χρήση της στους κβαντικούς υπολογιστές.

Η τεχνολογία αυτή έχει το πλεονέκτημα ότι μπορεί να χρησιμοποιηθεί σε θερμοκρασία δωματίου και έχει αποδειχθεί ότι είναι εύκολο να κατασκευαστεί με αυτή ένας κβαντικός υπολογιστής των 2 ή 3 qubits. Η βασική ιδέα είναι ότι ένας κβαντικός καταχωρητής είναι ένα μόριο που αποτελείται από δέκα άτομα. Κάθε qubit αναπαρίσταται με τον προσανατολισμό του σπιν του κάθε ατομικού πυρήνα στα άτομα του μορίου. Ο αριθμός των ατόμων ενός NMR κβαντικού υπολογιστή είναι ίσος με τον αριθμό των ατόμων σε κάθε μόριο.

Εκμεταλλευόμενοι τις ιδιότητες του φαινομένου ερευνητές κατάφεραν μέσω NMR πειραμάτων να αναπτύξουν θεμελιώδη εργαλεία που μπορούν να χρησιμοποιηθούν σε πολλούς μελλοντικούς τύπους κβαντικών υπολογιστών. Αυτή η τεχνολογία έχει αποδειχθεί ότι εύκολα μπορεί να σχεδιάσει 2 ή 3 qubits NMR κβαντικά συστήματα. Όμως τελευταία προσομοιώθηκε ένας υπολογιστής των 7-qubit με τη χρήση ενός νέου μορίου που αποτελείται από 7 πυρηνικά σπιν, όπου το κάθε ένα μπορεί να αλληλεπιδρά με το άλλο, ενώ οι αλληλεπιδράσεις αυτές μπορούν να ανιχνευτούν με όργανα NMR.

Βέβαια το φαινόμενο έχει κάποιες δυσκολίες όπως το γεγονός ότι είναι δύσκολο να διαχωριστούν τα qubits σε ένα μόριο από τις χημικές τους ιδιότητες στην περίπτωση μεγάλων μορίων. Επίσης είναι δύσκολο να αποσαφηνιστεί με ακρίβεια η αρχική κατάσταση. Είναι λοιπόν δύσκολο έως αδύνατο η τεχνολογία αυτή να χρησιμοποιηθεί σε υπολογιστές με περισσότερα από 12 qubits.

2.6 Η προοπτική και το μέλλον των κβαντικών υπολογιστών

Οι κβαντικοί υπολογιστές δεν είναι κατάλληλοι για όλες τις υπολογιστικές διεργασίες. Παραδείγματος χάριν δεν μπορούν να επιταχύνουν την επεξεργασία κειμένου ή την πλοήγηση στο διαδίκτυο. Το πιθανότερο είναι να

χρησιμοποιηθούν υβρίδια κλασικών και κβαντικών υπολογιστών στο μέλλον. Η βασική μελλοντική τους εφαρμογή θα είναι η χρήση τους για την προστασία απόρρητων και προσωπικών δεδομένων γιατί θα είναι αδύνατο να μπορούν να εισέρχονται σε e-mails και τραπεζικούς λογαριασμούς χρηστών του διαδικτύου, λόγω της ασφάλειας που θα παρέχουν. Επίσης, η αναζήτηση πληροφορίας στο διαδίκτυο θα διεξάγεται πολύ πιο γρήγορα, εφόσον υπάρχει κβαντικός αλγόριθμος αναζήτησης δεδομένων σε λίστα ο οποίος είναι μικρότερης τάξεως από τον αντίστοιχο κλασικό. Τέλος, μία άλλη εφαρμογή που έχει χρήση και στην καθημερινή ζωή, είναι η βελτίωση στη χρήση GPS δηλαδή συστημάτων που χρησιμοποιούνται σε αυτοκίνητα για να ανιχνεύεται μία θέση προς αναζήτηση. Αυτά τα συστήματα βασίζονται σε ρολόγια που λειτουργούν με βάση τις αρχές της κβαντομηχανικής. Οι κβαντικοί υπολογιστές θα μπορούν να βελτιώσουν αυτές τις ρυθμίσεις και η αναζήτηση με τα μηχανήματα να δίνει καλύτερα και πιο έγκυρα αποτελέσματα.

Όπως αναφέρθηκε, υπάρχουν διάφορες τεχνολογίες για την υλοποίηση κβαντικών υπολογιστών. Μέχρι στιγμής ο πρώτος κβαντικός υπολογιστής 2 qubits παρουσιάστηκε το 1998 από την IBM, η οποία το 1999 παρουσίασε κβαντικό υπολογιστή τριών qubits με δυνατότητα κβαντικής διόρθωσης σφαλμάτων ενώ από την ίδια εταιρεία το 2000 παρουσιάστηκε κβαντικός υπολογιστής των πέντε qubits. Ο τελευταίος υπολογιστής που έχει κατασκευαστεί είναι 7 qubits από τους Vandersypen, Steffen, Breyta, Yannoni, Sherwood, και Chuang το 2001.

ΚΕΦΑΛΑΙΟ 3

3. ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΜΟΙ ΚΑΙ ΚΒΑΝΤΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ

3.1 Το κυκλωματικό μοντέλο των κβαντικών υπολογιστών

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. Στους κβαντικούς υπολογιστές η πληροφορία βρίσκεται αποθηκευμένη σε qubits ή σε κβαντικούς καταχωρητές και παραμένει εκεί. Οι κβαντικές πύλες δεν είναι φυσικά συστήματα, αλλά αντιπροσωπεύουν μετασχηματισμούς (εφαρμογή γραμμικών τελεστών) που ασκούνται σε μεμονωμένα qubits ή σε κβαντικούς καταχωρητές (ομάδες από qubits).

Οι κβαντικοί υπολογισμοί είναι δράσεις τελεστών που έχουν σαν αποτέλεσμα την περιστροφή διανυσμάτων στο χώρο Hilbert. Τα διανύσματα αυτά παριστάνουν τις κβαντικές καταστάσεις των κβαντικών καταχωρητών. 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.

Σύμφωνα με αυτό, 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.

3.2 Κβαντικοί υπολογισμοί

Όλοι οι κβαντικοί υπολογισμοί που βασίζονται στο κυκλωματικό μοντέλο εκτελούνται με την παρακάτω διαδικασία όπως παρουσιάζεται και στο Σχήμα 9:

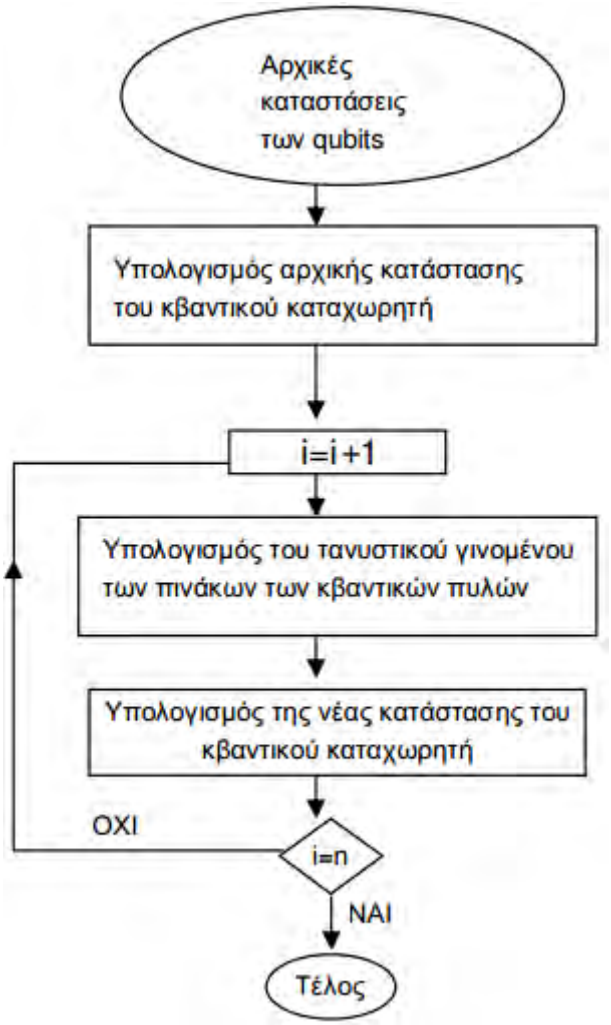
1. Δίνεται η αρχική κατάσταση των qubits που αποτελούν τον κβαντικό καταχωρητή. Υπολογίζεται το τανυστικό γινόμενο των πινάκων των καταστάσεων των qubits. Ο πίνακας που προκύπτει είναι η αρχική κατάσταση του κβαντικού καταχωρητή.

2. Υπολογίζεται το τανυστικό γινόμενο των πινάκων που περιγράφουν τις κβαντικές πύλες που δρουν στο επόμενο βήμα του κβαντικού υπολογισμού.

3. Ο πίνακας που προκύπτει από το τανυστικό γινόμενο των πινάκων των κβαντικών πυλών πολαπλασιάζεται με τον πίνακα της νέας κατάστασης του κβαντικού καταχωρητή.

4. Τα 2 και 3 επαναλαμβάνονται τόσες φορές όσα και τα βήματα του κβαντικού υπολογισμού.

5. Η τελική κατάσταση του κβαντικού καταχωρητή είναι το αποτέλεσμα του κβαντικού υπολογισμού.



Σχ.9 Διάγραμμα εκτέλεσης των κβαντικών υπολογισμών. Με i συμβολίζεται ο αριθμός του βήματος και με n ο συνολικός αριθμός βημάτων του κβαντικού υπολογισμού.

3.3 Ο κβαντικός επεξεργαστής

Μέχρι σήμερα δεν υπάρχει ένας προγραμματιζόμενος κβαντικός επεξεργαστής που να μπορεί να εκτελεί υπολογιστικά καθήκοντα. Για κάθε κβαντικό υπολογισμό συντίθεται και ένας κβαντικός επεξεργαστής, ο οποίος αποτελείται από έναν ή περισσότερους κβαντικούς καταχωρητές και από ένα σύνολο κβαντικών πυλών. Στους κβαντικούς υπολογιστές δεν υπάρχει σαφής διάκριση ανάμεσα στο υλικό και το λογισμικό όπως στους κλασικούς υπολογιστές. Σήμερα γίνεται έρευνα για να βρεθεί προγραμματιζόμενη αρχιτεκτονική για τους κβαντικούς υπολογιστές χωρίς ενθαρρυντικά αποτελέσματα.

3.4 Ο κβαντικός αλγόριθμος του Deutsch

Ο πρώτος κβαντικός αλγόριθμος, δηλαδή ένας αλγόριθμος που να μπορεί να τρέξει σε έναν κβαντικό υπολογιστή, αναπτύχθηκε από τον Deutsch. Στον αλγόριθμο αυτό χρησιμοποιείται η κβαντική παραλληλία, δηλαδή η υπέρθεση των βασικών καταστάσεων των qubits και για πρώτη φορά ένας κβαντικός υπολογιστής μπορεί να εκτελέσει υπολογισμούς που είναι αδύνατο 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}→{0,1}

Δηλαδή η μεταβλητή *x* και η συνάρτηση f(x) μπορούν να πάρουν μόνο τις τιμές 0 ή 1.

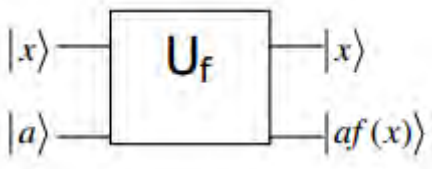
Για κάθε τέτοια συνάρτηση υπάρχουν δύο περιπτώσεις:

α) f(0)=f(1), οπότε η συνάρτηση ονομάζεται σταθερή

β) f(0)≠f(1), οπότε η συνάρτηση ονομάζεται ισορροπημένη.

Αν για παράδειγμα δοθεί μία συνάρτηση f(x) και θέλουμε να δούμε αν είναι σταθερή ή ισορροπημένη, κάνουμε τα εξής:

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 ισορροπημένη. Δεν είναι δυνατό να αποφασιστεί τι είναι η συνάρτηση με έναν μόνο υπολογισμό. Αυτό όμως είναι δυνατόν αν χρησιμοποιήσουμε έναν κβαντικό υπολογιστή, σύμφωνα με τον αλγόριθμο του Deutsch.

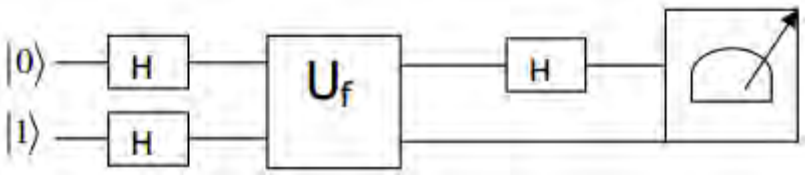


Σχ. 10 Κβαντικό κύκλωμα που υπολογίζει το άθροισμα με βάση το 2

Το κβαντικό αυτό κύκλωμα υπολογίζει το άθροισμα με βάση το 2 του πρώτου qubit με τη συνάρτηση f(x), όπου x το δεύτερο qubit .

Το Σχήμα 10 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 το ορθογώνιο $\mathbf{U_f}$. Για κάθε διαφορετική συνάρτηση f(x) χρειάζεται ένας διαφορετικός συνδυασμός κβαντικών πυλών. Ο συνδυασμός των κβαντικών πυλών $\mathbf{U_f}$ δρα στα δύο qubits και αφήνει το δεύτερο αμετάβλητο, ενώ φέρνει το πρώτο στην κατάσταση που αντιστοιχεί με το άθροισμα με βάση το 2 του πρώτου qubit $|a\rangle$ με τη συνάρτηση f(x), όπου x είναι το δεύτερο qubit.

Ο αλγόριθμος του Deutsch είναι και αυτός ένας κβαντικός υπολογισμός και περιγράφεται από το παρακάτω κύκλωμα στο Σχήμα 11. Η αρχική κατάσταση του πρώτου qubit είναι $|1\rangle$ και του δεύτερου $|0\rangle$. Στο πρώτο βήμα του αλγορίθμου του Deutsch, η κατάσταση του κβαντικού καταχωρητή είναι $01\rangle$. Στο δεύτερο βήμα δρουν δύο κβαντικές πύλες **H**. Στο τρίτο βήμα δρα ο συνδυασμός κβαντικών πυλών $\mathbf{U_f}$ 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 είναι ισορροπημένη.



Σχ.11 Ο αλγόριθμος του Deutsch είναι κβαντικός υπολογισμός και περιγράφεται από το κύκλωμα

3.5 Ο αλγόριθμος του Grover

Ο αλγόριθμος του Grover ερευνά μία δομημένη βάση δεδομένων που περιέχει N στοιχεία. Κάθε στοιχείο της βάσης έχει αριθμηθεί από ο έως N-1. Το σύστημα που διαθέτουμε μπορεί να αναγνωρίσει αν κάποιο στοιχείο είναι αυτό που αναζητάμε ή όχι. Σε έναν κλασικό υπολογιστή το σύστημα αυτό είναι ένας

καταχωρητής όπου έχουμε αποθηκεύσει τον αριθμό που ψάχνουμε να βρούμε και ένα κύκλωμα λογικών πυλών. Το κύκλωμα συγκρίνει κάθε αριθμό στην είσοδό του με τον αποθηκευμένο αριθμό. Το σύστημα αυτό ονομάζεται *oracle*.

Ο Grover επινόησε έναν κβαντικό αλγόριθμο ο οποίος μπορεί να ψάξει μία αταξινόμητη βάση δεδομένων και να την ταξινομήσει πολύ γρηγορότερα από ότι θα έκανε ένας κλασικός υπολογιστής. Κανονικά μία βάση δεδομένων με n στοιχεία θα έπαιρνε $N/2$ αριθμό αναζητήσεων για να βρεθεί το στοιχείο που αναζητείται, αλλά σε έναν κβαντικό υπολογιστή ο αριθμός αναζητήσεων είναι της τάξεως $N^{1/2}$.

Μία άλλη εφαρμογή του αλγορίθμου είναι στον τομέα των κρυπτογραφημένων στοιχείων. Υποθέτουμε ότι έχουμε μία εικονική βάση δεδομένων που είναι τόσο μεγάλη που δεν θα ταίριαζε στις μνήμες των κλασικών υπολογιστών. Αυτό επιτρέπει στους κβαντικούς υπολογιστές να χρησιμοποιήσουν ένα ευρέως γνωστό σύστημα για την προστασία των δεδομένων. Αυτό είναι το σύστημα DES (Data Encryption Standard). Το σύστημα αυτό στηρίζεται σε έναν αριθμό 56 bits. Μία εξαντλητική αναζήτηση με τα συμβατικά μέσα θα απαιτούσε 2^{55} αναζητήσεις πριν βρεθεί το σωστό κλειδί. Ο αλγόριθμος του Grover θα μπορούσε να βρει το κλειδί μόνο μετά από 185 αναζητήσεις.

3.6 Ο αλγόριθμος του Shor

Το 1994 ο Peter Shor απέδειξε ότι με τη χρήση κβαντικών υπολογιστών, μπορεί εύκολα και γρήγορα να αναλυθούν σε γινόμενο δύο πρώτων αριθμών, μεγάλοι ακέραιοι αριθμοί. Με έναν κβαντικό υπολογιστή απαιτείται πολυωνυμική αύξηση του χρόνου υπολογισμού για γραμμική αύξηση του μεγέθους n, δηλαδή του πλήθους των ψηφίων του αριθμού που έχει δύο πρώτους παράγοντες. Οι γρηγορότεροι κλασικοί αλγόριθμοι για το ίδιο πρόβλημα είναι υπερ-πολυωνυμικοί σε συνάρτηση με τον αριθμό ψηφίων n. Η μέθοδος που πρότεινε ο Shor είναι γνωστή ως «κβαντικός αλγόριθμος του Shor».

ΚΕΦΑΛΑΙΟ 4

4. ΚΒΑΝΤΙΚΕΣ ΛΟΓΙΚΕΣ ΠΥΛΕΣ

4.1 Προκαταρκτικές έννοιες

Ένας κλασσικός υπολογιστής αποτελείται από μνήμη και από έναν επεξεργαστή. Ο επεξεργαστής εκτελεί πάνω στα bits πληροφορίας που είναι αποθηκευμένα στη μνήμη πράξεις σύμφωνα με κάποιο πρόγραμμα, και δίνει ως έξοδο τα αποτελέσματα με τη μορφή ενός συνόλου bits. Οι πράξεις επεξεργασίας εκτελούνται από εκατομμύρια μεμονωμένες δυαδικές λογικές πύλες, όπως είναι οι πύλες NOT (ΟΧΙ) ή NAND (ΟΧΙ-ΚΑΙ), οι οποίες εκτελούν πράξεις σε ένα ή δύο bit κάθε φορά. Παραδείγματος χάριν, η πύλη NOT δρα σε ένα bit κάθε φορά, ενώ η πύλη NAND δρα σε δύο bits. Οι πίνακες αληθείας για αυτές τις κλασσικές πράξεις παρουσιάζονται στους Πίνακες 4 και 5. Για να εκτελέσει το πρόγραμμα την απαιτούμενη εργασία, καθορίζει με ποιον τρόπο συνδέονται μεταξύ τους οι δυαδικές πύλες σε ένα λογικό κύκλωμα.

Bit εισόδου	Bit εξόδου
0	1
1	0

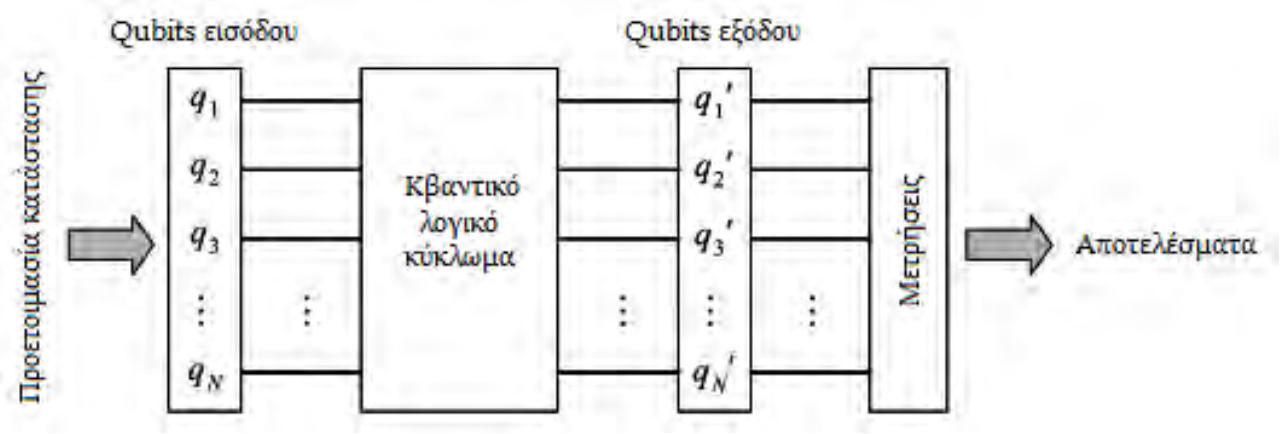
Πίνακας 4: Πίνακας αληθείας για την κλασσική μονοδύφια πύλη NOT

Bits εισόδου	Bit εξόδου
0 0	1
1 0	1
0 1	1
1 1	0

Πίνακας 5: Πίνακας αληθείας για την κλασσική διδύφια πύλη NAND

Η βασική ιδέα ενός κβαντικού υπολογιστή είναι εν πολλοίς ίδια. Οι πληροφορίες αποθηκεύονται σε έναν καταχωρητή qubits και οι εργασίες

επεξεργασίας εκτελούνται από κβαντικές λογικές πύλες. Οι κβαντικές αυτές πύλες συνδέονται μεταξύ τους σε ένα κβαντικό κύκλωμα προκειμένου να εκτελεστούν καθορισμένες εργασίες επεξεργασίας. Στο Σχήμα 12 απεικονίζεται ένα σχηματικό δομικό διάγραμμα κβαντικού υπολογιστή. Το πρώτο τμήμα του υπολογιστή είναι ένας καταχωρητής N qubits $\{q_1, q_2, q_3, \dots, q_N\}$, τα οποία έχουν ρυθμιστεί προηγουμένως στις απαιτούμενες αρχικές καταστάσεις. Αυτά τα qubits εισόδου εισάγονται στο κβαντικό λογικό κύκλωμα το οποίο στη συνέχεια εκτελεί τις εργασίες επεξεργασίας σύμφωνα με το πρόγραμμα του κβαντικού υπολογιστή. Η έξοδος του κβαντικού λογικού κυκλώματος είναι ένα νέο σύνολο qubits $\{q'_1, q'_2, q'_3, \dots, q'_N\}$. Τα τελικά αποτελέσματα της υπολογιστικής εργασίας λαμβάνονται με μετρήσεις πάνω σε αυτά τα qubits εξόδου, από τις οποίες προκύπτει ένα σύνολο N κλασσικών bit.



Σχήμα 12: Σχηματικό δομικό διάγραμμα των μηχανισμών ενός κβαντικού υπολογιστή. Τα qubits $\{q_1, q_2, q_3, \dots, q_N\}$ από τον καταχωρητή εισόδου ρυθμίζονται στις σωστές αρχικές καταστάσεις και εισάγονται στο κβαντικό λογικό κύκλωμα, το οποίο εκτελεί τις εργασίες επεξεργασίας και δίνει σαν έξοδο ένα νέο σύνολο qubits $\{q'_1, q'_2, q'_3, \dots, q'_N\}$. Στον καταχωρητή εξόδου εκτελούνται μετρήσεις, και κατόπιν εξάγονται τα αποτελέσματα.

4.2 Κβαντικές και λογικές πύλες

Σε προηγούμενο κεφάλαιο έγινε απλή αναφορά στις κβαντικές και στις λογικές πύλες. Χρήζει επισήμανσης ότι ενώ όλες οι κβαντικές πύλες είναι αντιστρέψιμες, δεν ισχύει το ίδιο για τις λογικές. 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 κατάστασης των qubits και των κβαντικών καταχωρητών χωρίς να αλλάζουν το μήκος τους , το οποίο είναι πάντα ίσο με τη μονάδα. Οι δράσεις αυτές αφορούν τελεστές-πίνακες οι οποίοι εφαρμόζονται πάνω στα διανύσματα κατάστασης και πραγματοποιούν πράξεις, επί παραδείγματι μεταβάλλουν τα πλάτη πιθανότητας των βασικών καταστάσεων. Εφαρμόζονται πράξεις πάνω στα qubits και αυτές είναι πάντα αντιστρεπτές. Αυτό σημαίνει ότι έχουν τον ίδιο αριθμό εισόδων και εξόδων. Οι κβαντικές πύλες έχουν δύο ιδιότητες: να μη μεταβάλλουν το μήκος διανύσματος κατάστασης και να τηρούν τη χρονική συμμετρία των κβαντικών συστημάτων.

Κάθε κβαντική πύλη που δρα σε n qubits περιγράφεται από έναν ορθομοναδιαίο πίνακα U διαστάσεων $2^n * 2^n$. Το αποτέλεσμα της δράσης μιας πύλης σε qubit υπολογίζεται με τον πολλαπλασιασμό του πίνακα της πύλης με τον πίνακα του διανύσματος κατάστασης. Ένα άλλο βασικό χαρακτηριστικό των κβαντικών πυλών είναι το γεγονός ότι η πληροφορία, τα qubits εν προκειμένω, δεν περνούν μέσα από την πύλη όπως στους κλασσικούς υπολογιστές, αλλά εφαρμόζονται πάνω στα qubits ή στους καταχωρητές.

4.3 Κβαντικές πύλες που δρουν σε ένα qubit (*μονοκβαντοδυφιακές*)

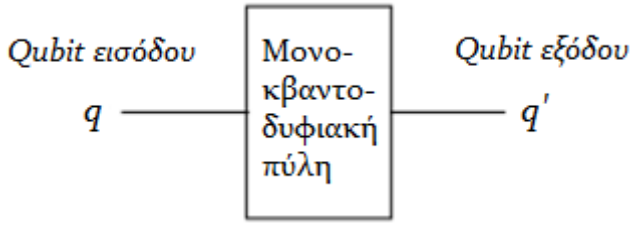
Οι πύλες που δρουν σε ένα qubit περιστρέφουν το διάνυσμα κατάστασης ενός qubit. Αυτό επιτυγχάνεται με τη μεταβολή των γωνιών φ και θ μέσω των πράξεων που εκτελούν οι πύλες πάνω στα qubits. Γενικότερα, οι περιστροφές που είναι δυνατόν να συμβούν είναι άπειρες και για το λόγο αυτό υπάρχουν άπειρες κβαντικές πύλες που δρουν σε ένα qubit. Επομένως, επειδή η κάθε τέτοια κβαντική πύλη περιγράφεται από έναν ορθομοναδιαίο πίνακα, κάθε

τέτοιος πίνακας μπορεί να είναι μία κβαντική πύλη. Παρόλα αυτά, υπάρχει μια γενική περίπτωση πίνακα-τελεστή που δρα σε ένα qubit. Αυτός είναι ο πίνακας *U*, ο οποίος είναι ένας πίνακας 2x2 και είναι ο εξής:

$$U = e^{i\alpha}\begin{bmatrix} e^{-i\frac{\beta}{2}} & 0 \\ 0 & e^{i\frac{\beta}{2}} \end{bmatrix}\begin{bmatrix} \cos\frac{\gamma}{2} & -sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & cos\frac{\gamma}{2} \end{bmatrix}\begin{bmatrix} e^{-i\frac{\delta}{2}} & 0 \\ 0 & e^{i\frac{\delta}{2}} \end{bmatrix} =$$

$$= \begin{bmatrix} cos\frac{\gamma}{2}\cdot e^{i\left(-\frac{\beta+\delta}{2}+\alpha\right)} & -sin\frac{\gamma}{2}\cdot e^{i\left(-\frac{\beta+\delta}{2}+\alpha\right)} \\ sin\frac{\gamma}{2}\cdot e^{i\left(\frac{\beta+\delta}{2}+\alpha\right)} & cos\frac{\gamma}{2}\cdot e^{i\left(\frac{\beta+\delta}{2}+\alpha\right)} \end{bmatrix}, \text{όπου } \alpha,\beta,\gamma,\delta \in \mathbb{R}$$

Η λειτουργία μιας μονοκβαντοδυφιακής πύλης απεικονίζεται διαγραμματικά στο Σχήμα 13.



Σχήμα 13: Σχηματικό διάγραμμα μιας μονοκβαντοδυφιακής πύλης. Η πύλη μετασχηματίζει ένα qubit εισόδου q σε ένα qubit εξόδου q′.

Η πύλη δέχεται ως είσοδο ένα μεμονωμένο qubit q και αποδίδει ως έξοδο ένα άλλο qubit q'. Εάν συμβολίσουμε τις κυματοσυναρτήσεις των q και q' με $|\psi\rangle$ και $|\psi'\rangle$, αντίστοιχα, όπου

$$|\psi\rangle = c_0|0\rangle + c_1|1\rangle,$$

και

$$|\psi'\rangle = c_0'|0\rangle + c_1'|1\rangle,$$

βλέπουμε ότι το αποτέλεσμα της πύλης είναι ότι μεταβάλλει τους συντελεστές πλάτους του qubit με καθορισμένο τρόπο. Χρησιμοποιώντας το συμβολισμό του διανύσματος στήλης, μπορούμε να περιγράψουμε την πύλη μέσω μιας 2x2 μήτρας M ως εξής:

$$\begin{bmatrix} c_0' \\ c_1' \end{bmatrix} = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix},$$

όπου

$$c_0' = M_{11}c_0 + M_{12}c_1$$
$$c_1' = M_{21}c_0 + M_{22}c_1$$

Όπως προκύπτει, η μόνη απαίτηση για τη μήτρα πύλης M είναι ότι θα πρέπει να είναι μοναδιαία:

$$MM^{\dagger} = I,$$

όπου $M^{\dagger}$ είναι η ερμιτιανή συζυγής μήτρα της M, και I είναι η ταυτοτική μήτρα. Η συνθήκη αυτή μπορεί να γραφεί αναλυτικά ως εξής:

$$\begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix} \begin{bmatrix} M_{11}^* & M_{21}^* \\ M_{12}^* & M_{22}^* \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Από την απαίτηση της μοναδιακότητας έπεται ότι όλες οι κβαντικές πύλες θα πρέπει να είναι *αντιστρεπτές*.

Οι βασικές μονοκβαντοδυφιακές πύλες

Μονάδα	I	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Hadamard	H	$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli X	X	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli Y	Y	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli Z	Z	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Φάση R_θ	R_θ	$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$

Ως πρώτη παρατήρηση στον παραπάνω πίνακα, οι τρεις πύλες *X, Y* και *Z* και οι αντίστοιχες μήτρες, δεν είναι παρά οι γνωστές *μήτρες του Pauli* σ_x, σ_y και σ_z που είναι ταυτόχρονα ερμιτιανές και μοναδιαίες λόγω της γνωστής τους ιδιότητας να είναι $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = 1$. Ερμιτιανή και μοναδιαία είναι επίσης και η πύλη Hadamard, αφού ισχύει και γι' αυτήν ότι $H^2 = 1$. Μεταξύ άλλων αυτό συνεπάγεται ότι η διπλή δράση αυτών των πυλών επαναφέρει το qubit στην αρχική του κατάσταση.

4.3.1 Κβαντική πύλη αδράνειας

Η κβαντική πύλη αδράνειας συμβολίζεται με *I* και αφήνει αμετάβλητη την κατάσταση του qubit στο οποίο εφαρμόζεται, όπως αποκαλύπτει άλλωστε και το όνομά της.

Ο συμβολισμός της πύλης αδράνειας είναι:

$$I\,|q\rangle = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} |q\rangle = |q\rangle$$

Με τη βοήθεια πίνακα για την αναπαράσταση των ιδιοτήτων της πύλης, έχουμε:

Πίνακας αληθείας της πύλης αδράνειας

$\|q_{πριν}\rangle$	→	$\|q_{μετά}\rangle$
$\|\mathbf{0}\rangle$		$\|0\rangle$
$\|\mathbf{1}\rangle$		$\|1\rangle$

4.3.2 Κβαντική πύλη Pauli-X (πύλη NOT)

Η κβαντική πύλη Pauli-X είναι η αντίστοιχη της πύλης NOT των κλασσικών υπολογιστών και αναπαρίσταται με το σύμβολο «*X*». Εναλλάσσει μεταξύ τους τους συντελεστές πλάτους, που σημαίνει ότι η πύλη αυτή αντιστρέφει την κατάσταση του qubit μετατρέποντας το 0 σε 1 και το 1 σε 0. Ουσιαστικά, πρόκειται για μια περιστροφή του διανύσματος κατάστασης γύρω από τον άξονα x κατά 180 μοίρες, ή π ακτίνια.

$$X\,|q\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \end{bmatrix} = \begin{bmatrix} c_1 \\ c_0 \end{bmatrix}$$

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

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

Υπό μορφή πίνακα οι ιδιότητες είναι:

Πίνακας αληθείας της πύλης NOT

$\|q_{πριν}\rangle$	→	$\|q_{μετά}\rangle$
$\|\mathbf{0}\rangle$		$\|1\rangle$
$\|\mathbf{1}\rangle$		$\|0\rangle$

4.3.3 Κβαντική πύλη Pauli-Y

Η κβαντική πύλη Pauli-Y αντιστοιχεί σε περιστροφή του διανύσματος κατάστασης του qubit γύρω από τον άξονα y κατά 180 μοίρες, ή π ακτίνια. Συμβολίζεται με «Y» και μετατρέπει το διάνυσμα $|0\rangle$ σε $i|1\rangle$ και την $|1\rangle$ σε $-i|0\rangle$. Ο πίνακας είναι:

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Οι επιδράσεις της πύλης με μαθηματικό συμβολισμό είναι:

$$Y|0\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ i \end{bmatrix} = 0|0\rangle + i|1\rangle = i|1\rangle$$

$$Y|1\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} -i \\ 0 \end{bmatrix} = -i|0\rangle + 0|1\rangle = -i|0\rangle$$

Οι ιδιότητες της παραπάνω πύλης, υπό μορφή πίνακα, είναι:

Πίνακας αληθείας της πύλης Pauli-Y

$\|q_{πριν}\rangle$	→	$\|q_{μετά}\rangle$
$\|\mathbf{0}\rangle$		$i\|1\rangle$
$\|\mathbf{1}\rangle$		$-i\|0\rangle$

4.3.4 Κβαντική πύλη Pauli-Z

Η κβαντική πύλη Pauli-Z συμβολίζεται με «*Z*» και αντιστοιχεί σε περιστροφή του διανύσματος κατάστασης του qubit γύρω από τον άξονα z κατά 180 μοίρες, ή π ακτίνια. Ουσιαστικά, αφήνει αμετάβλητη την κατάσταση $|0\rangle$ και μετατρέπει την κατάσταση $|1\rangle$ και την $-|1\rangle$. Ο πίνακας που αντιπροσωπεύει αυτήν την πύλη είναι:

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Οι επιδράσεις της πύλης είναι:

$$Z|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = 1|0\rangle + 0|1\rangle = |0\rangle$$

$$Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = 0|0\rangle + (-1)|1\rangle = -1|1\rangle$$

Ο πίνακας μετατροπών της συγκεκριμένης πύλης είναι ο εξής:

Πίνακας αληθείας της πύλης Pauli-Z

$\|q_{πριν}\rangle$	→	$\|q_{μετά}\rangle$
$\|\mathbf{0}\rangle$		$\|0\rangle$
$\|\mathbf{1}\rangle$		$-1\|1\rangle$

4.3.5 Κβαντική πύλη Hadamard

Η πύλη Hadamard εφαρμόζεται πάνω σε ένα qubit και αποτελεί βασικό και κρίσιμο εργαλείο για τη σχεδίαση κβαντικών κυκλωμάτων. Αυτό οφείλεται στο γεγονός ότι η πύλη έχει ως είσοδό της ένα qubit που δε βρίσκεται σε κατάσταση υπέρθεσης και το μετατρέπει έτσι ώστε να βρίσκεται σε μια τέτοια κατάσταση. Καθώς οι κβαντικοί υπολογιστές βασίζονται στην υπέρθεση των qubits για τις περισσότερες πράξεις που θα εκτελέσουν, μπορεί κανείς να καταλάβει τη μεγάλη σημασία που αποκτά. Συμβολίζεται με «*H*». Ο πίνακας της πύλης είναι:

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

Η επίδραση της πύλης Hadamard σε qubits που βρίσκονται στις βασικές καταστάσεις είναι:

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

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

Συνεπώς, η πιθανότητα να λάβει κάποιος, κατόπιν μιας μέτρησης, μια από τις δύο βασικές καταστάσεις, είναι ίδια και έχει τιμή ίση με $\left|\frac{1}{\sqrt{2}}\right|^2 = 0{,}5$. Επίσης, με εφαρμογή της πύλης Hadamard σε qubits που βρίσκονται σε υπέρθεση, δηλαδή τα $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ και $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, αυτά επανέρχονται στη βασική αρχική κατάσταση ως εξής:

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

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

Συνοπτικά, οι δράσεις της πύλης Hadamard και στις δύο περιπτώσεις φαίνονται στον παρακάτω πίνακα:

Πίνακας αληθείας της πύλης Hadamard

$\|q_{πριν}\rangle$	→	$\|q_{μετά}\rangle$
$\|0\rangle$		$\frac{1}{\sqrt{2}}\|0\rangle + \frac{1}{\sqrt{2}}\|1\rangle$
$\|1\rangle$		$\frac{1}{\sqrt{2}}\|0\rangle - \frac{1}{\sqrt{2}}\|1\rangle$
$\frac{1}{\sqrt{2}}\|0\rangle + \frac{1}{\sqrt{2}}\|1\rangle$		$\|0\rangle$
$\frac{1}{\sqrt{2}}\|0\rangle - \frac{1}{\sqrt{2}}\|1\rangle$		$\|1\rangle$

4.3.6 Κβαντική πύλη μετατόπισης φάσης

Η κβαντική πύλη μετατόπισης φάσης συμβολίζεται με R_θ και αποτελεί μια οικογένεια πυλών οι οποίες περιστρέφουν το διάνυσμα κατά θ μοίρες σε έναν νοητό οριζόντιο κύκλο. Ο πίνακας που αντιπροσωπεύει την πύλη μετατόπισης φάσης είναι:

$$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

Εξετάζοντας το αποτέλεσμα της δράσης της παραπάνω πύλης σε qubits που βρίσκονται σε μία από τις βασικές καταστάσεις, προκύπτουν τα εξής:

$$R_\theta|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

$$R_\theta|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ e^{i\theta} \end{bmatrix} = e^{i\theta}|1\rangle$$

Όπως φαίνεται από τις παραπάνω εξισώσεις, η πύλη μετατόπισης φάσης δεν αλλάζει την κατάσταση ενός qubit που βρίσκεται στη βασική κατάσταση $|0\rangle$, αλλά αλλάζει ένα qubit που βρίσκεται στη βασική

κατάσταση $|1\rangle$ σε $e^{i\theta}|1\rangle$. Η πιθανότητα να μετρηθεί η κατάσταση $|1\rangle$ παραμένει αμετάβλητη και το μόνο που αλλάζει είναι η γωνία φάσης του διανύσματος. Στη γενικότερη περίπτωση ενός qubit με πλάτη πιθανότητας α και b, έχουμε:

$$R_\theta|q\rangle = R_\theta(a|0\rangle + b|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \cdot e^{i\theta} \end{bmatrix} = a|0\rangle + b \cdot e^{i\theta}|1\rangle$$

Όπως και στην περίπτωση του qubit με κατάσταση $|1\rangle$, έτσι και σε αυτή αλλάζει μόνο η γωνία φάσης του διανύσματος του qubit, χωρίς να επηρεάζονται τα πλάτη πιθανότητας του qubit.

Οι δράσεις της πύλης αυτής συνοψίζονται στον παρακάτω πίνακα:

Πίνακας αληθείας της πύλης μετατόπισης φάσης

$\|q_{πριν}\rangle$	→	$\|q_{μετά}\rangle$
$\|\mathbf{0}\rangle$		$\|0\rangle$
$\|\mathbf{1}\rangle$		$e^{i\theta}\|1\rangle$
$\boldsymbol{a}\|\mathbf{0}\rangle + \boldsymbol{b}\|\mathbf{1}\rangle$		$a\|0\rangle + b \cdot e^{i\theta}\|1\rangle$

4.4 Κβαντική πύλη εναλλαγής qubit

Η κβαντική πύλη εναλλαγής qubit είναι μια κβαντική πύλη που εφαρμόζεται και δρα σε δύο qubits. Μετά την εφαρμογή της πύλης αυτής, τα δύο qubits που έχουν δεχθεί τη δράση της, έχουν εναλλάξει τις καταστάσεις που βρίσκονταν πριν. Συμβολίζεται με SWAP και ο πίνακας της είναι:

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

Αντίθετα με τις πύλες που δρουν σε ένα qubit, ο πίνακας μιας πύλης που δρα σε δύο qubits είναι ένας πίνακας 4x4, διότι ο διανυσματικός πίνακας δύο qubits αποτελείται από μία στήλη τεσσάρων στοιχείων. Έτσι, η εφαρμογή της

συγκεκριμένης πύλης σε δύο qubits q_1 και q_0 είναι:

$$q_1 = a|0\rangle + b|1\rangle$$
$$q_0 = c|0\rangle + d|1\rangle$$

$$|q_1 q_0\rangle = |q_1\rangle \otimes |q_0\rangle = \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot c \\ b \cdot d \end{bmatrix}$$

$$SWAP(|q_1 q_0\rangle) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot c \\ b \cdot d \end{bmatrix} = \begin{bmatrix} a \cdot c \\ b \cdot c \\ a \cdot d \\ b \cdot d \end{bmatrix} = \begin{bmatrix} c \\ d \end{bmatrix} \otimes \begin{bmatrix} a \\ b \end{bmatrix} = |q_0 q_1\rangle$$

Η δράση της κβαντικής πύλης εναλλαγής qubit εμφανίζεται παρακάτω:

Πίνακας αληθείας της πύλης εναλλαγής qubits

$\|q_{πριν}\rangle$	→	$\|q_{μετά}\rangle$
$\|q_1 q_0\rangle$		$\|q_0 q_1\rangle$
$\|q_0 q_1\rangle$		$\|q_1 q_0\rangle$

4.5 Κβαντικές πύλες που δρουν σε δύο qubits (*δικβαντοδυφιακές*)

4.5.1 Ελεγχόμενες κβαντικές πύλες

Ο όρος «ελεγχόμενες κβαντικές πύλες» αναφέρεται σε κβαντικές πύλες οι οποίες δρουν σε δύο (πύλη ελεγχόμενου ΟΧΙ) ή και περισσότερα qubits (πύλες Toffoli και Fredkin). Στο ένα qubit θα εφαρμοστεί πιθανώς ο μετασχηματισμός που ορίζει η πύλη, ενώ το άλλο (ή άλλα) καθορίζουν αν θα εφαρμοστεί τελικά αυτός ο μετασχηματισμός στην κατάσταση του qubit. Ουσιαστικά, τα qubits ελέγχου (control qubits) ορίζουν αν το qubit-στόχος θα υποστεί μετασχηματισμό ή όχι, καθώς αυτό θα περάσει από την πύλη.

Από τη θεωρία πινάκων της γραμμικής άλγεβρας, χρησιμοποιούμε έναν πιο εύχρηστο συμβολισμό για την περιγραφή της πύλης *U*, η οποία πλέον γράφεται

ως εξής:

$$U = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$$

Αυτό το κάνουμε επίσης, επειδή θα μελετηθούν ελεγχόμενες κβαντικές πύλες που δρουν σε δύο και τρία qubits και πρέπει να προσδιοριστούν μαθηματικά, σε μορφή πινάκων, τα διανύσματα κατάστασής τους.

Αρχικά μελετάται η περίπτωση ενός καταχωρητή με δύο qubits. Έστω αυτά είναι τα $|q_1\rangle = a|0\rangle + b|1\rangle$ και $|q_0\rangle = c|0\rangle + d|1\rangle$. Όπως έχουμε ήδη αναφέρει, ο παραπάνω κβαντικός καταχωρητής είναι ο εξής:

$$|q_{reg\_2}\rangle = |q_1\rangle \otimes |q_0\rangle = \begin{bmatrix} a \cdot c \\ a \cdot d \\ b \cdot c \\ b \cdot d \end{bmatrix}$$

Έτσι, οι πιθανότητες εμφάνισης των τεσσάρων πιθανών καταστάσεων 00, 01, 10, 11 είναι $a \cdot c$, $a \cdot d$, $b \cdot c$ και $b \cdot d$ αντίστοιχα. Ακόμα, έστω $\alpha_{00} = a \cdot c$, $\alpha_{01} = a \cdot d$, $\alpha_{10} = b \cdot c$ και $\alpha_{11} = b \cdot c$, όπου ο δείκτης δείχνει την κατάσταση στην οποία βρίσκεται ο καταχωρητής. Το qubit $|q_1\rangle$ θεωρείται το qubit ελέγχου ενώ το $|q_0\rangle$ το qubit-στόχος. Όταν το $|q_1\rangle$ βρίσκεται στην κατάσταση $|0\rangle$, ο μετασχηματισμός της πύλης δε θα εφαρμοστεί στο $|q_0\rangle$. Αντίθετα, όταν το $|q_1\rangle$ βρίσκεται στην κατάσταση $|1\rangle$, τότε το $|q_0\rangle$ θα υποστεί το μετασχηματισμό που περιγράφει η κβαντική πύλη. Από αυτό προκύπτει ότι ο πίνακας μιας οποιασδήποτε κβαντικής πύλης U θα πρέπει να αφήνει ανεπηρέαστη την κατάσταση του καταχωρητή όταν αυτός είναι στις καταστάσεις $|00\rangle$ και $|01\rangle$ και να αλλάζει την κατάστασή του μόνο όταν συναντώνται οι καταστάσεις $|10\rangle$ και $|11\rangle$.

Τελικώς, ο πίνακας μιας οποιασδήποτε ελεγχόμενης κβαντικής πύλης είναι:

$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & x_{11} & x_{12} \\ 0 & 0 & x_{21} & x_{22} \end{bmatrix}$$

Μία, ακόμα πιο συμπαγής αναπαράσταση που μπορεί να χρησιμοποιηθεί για τον παραπάνω πίνακα αλλά και για πίνακες αλλά και για πίνακες ελεγχόμενων κβαντικών πυλών που επιδρούν σε τρία qubits, όπως αυτοί θα παρουσιαστούν παρακάτω, είναι η εξής:

$$CU = \begin{bmatrix} \boldsymbol{I_2} & \boldsymbol{0_2} \\ \boldsymbol{0_2} & \boldsymbol{U} \end{bmatrix},$$

όπου με $\boldsymbol{I_2}$ συμβολίζεται ο μοναδιαίος πίνακας 2x2 και με $\boldsymbol{0_2}$ ο μηδενικός πίνακας μεγέθους 2x2.

Αρκετά εύκολα μπορεί να αποδειχθεί ότι ο παραπάνω πίνακας επαληθεύει την απαίτηση μιας ελεγχόμενης κβαντικής πύλης να αφήνει ανεπηρέαστη την κατάσταση του κβαντικού καταχωρητή δύο qubits, αν το qubit ελέγχου είναι 0:

$$CU\left|q_{reg\_2}\right\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & x_{11} & x_{12} \\ 0 & 0 & x_{21} & x_{22} \end{bmatrix} \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} = \begin{bmatrix} a_{00} \\ a_{01} \\ x_{11}a_{10} + x_{12}a_{11} \\ x_{21}a_{10} + x_{22}a_{11} \end{bmatrix}$$

Παρόμοια μπορεί να γίνει ανάλυση για την αναπαράσταση οποιασδήποτε ελεγχόμενης κβαντικής πύλης που εφαρμόζεται σε καταχωρητή των τριών qubits, εκ των οποίων τα δύο χρησιμοποιούνται για έλεγχο. Χρησιμοποιούμε τα δύο προηγούμενα qubits που ορίστηκαν, δηλαδή τα $|q_1\rangle = a|0\rangle + b|1\rangle$ και $|q_0\rangle = c|0\rangle + d|1\rangle$, καθώς και ένα τρίτο qubit $|q_2\rangle = e|0\rangle + f|1\rangle$. Όπως και προηγουμένως, ο καταχωρητής των τριών αυτών qubits είναι ο εξής:

$$\left|q_{reg\_3}\right\rangle = |q_2\rangle \otimes |q_1\rangle \otimes |q_0\rangle = \begin{bmatrix} e \\ f \end{bmatrix} \otimes \begin{bmatrix} a \\ b \end{bmatrix} \otimes \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} e \cdot a \cdot c \\ e \cdot a \cdot d \\ e \cdot b \cdot c \\ e \cdot b \cdot d \\ f \cdot a \cdot c \\ f \cdot a \cdot d \\ f \cdot b \cdot c \\ f \cdot b \cdot d \end{bmatrix} = \begin{bmatrix} a_{000} \\ a_{001} \\ a_{010} \\ a_{011} \\ a_{100} \\ a_{101} \\ a_{110} \\ a_{111} \end{bmatrix}$$

Ο συμβολισμός που χρησιμοποιείται και εδώ είναι ίδιος με αυτόν που χρησιμοποιήθηκε παραπάνω. Κάθε στοιχείο *a* του διανύσματος, αντιπροσωπεύει την πιθανότητα εμφάνισης της κατάστασης που περιγράφεται στο δείκτη κατά τη διάρκεια μιας μέτρησης.

Με την ίδια φιλοσοφία, καταλήγουμε στο συμπέρασμα ότι ο πίνακας μιας γενικής κβαντικής πύλης που επηρεάζει τρία qubits και χρησιμοποιεί τα δύο από αυτά για έλεγχο, είναι:

$$CCU = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & x_{11} & x_{12} \\ 0 & 0 & 0 & 0 & 0 & 0 & x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} \boldsymbol{I_4} & \boldsymbol{0_4} \\ \boldsymbol{0_4} & CU \end{bmatrix}$$

Ο δεύτερος πίνακας αποτελεί μια απλουστευμένη αναπάρασταση του αρχικού 8x8 πίνακα. Όπου $\boldsymbol{I_4}$ είναι ο μοναδιαίος πίνακας μεγέθους 4x4 και *CU* ο πίνακας της γενικής ελεγχόμενης πύλης των 2 qubits με ένα qubit ελέγχου. Εφαρμόζοντας την πύλη *CCU* σε έναν καταχωρητή των τριών qubits, αποδεικνύεται ότι για να εφαρμοστεί ο μετασχηματισμός της πύλης στο qubit-στόχο, θα πρέπει και τα δύο qubits ελέγχου να είναι στην κατάσταση |1⟩:

$$CCU\left|q_{reg_3}\right\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & x_{11} & x_{12} \\ 0 & 0 & 0 & 0 & 0 & 0 & x_{21} & x_{22} \end{bmatrix} \begin{bmatrix} a_{000} \\ a_{001} \\ a_{010} \\ a_{011} \\ a_{100} \\ a_{101} \\ a_{110} \\ a_{111} \end{bmatrix} =$$

$$= \begin{bmatrix} a_{000} \\ a_{001} \\ a_{010} \\ a_{011} \\ a_{100} \\ a_{101} \\ x_{11}a_{110} + x_{12}a_{111} \\ x_{21}a_{110} + x_{22}a_{111} \end{bmatrix}$$

Ομοίως, συνεχίζοντας με την ίδια λογική, μπορεί να προκύψει ελεγχόμενη κβαντική πύλη η οποία δρα σε ένα qubit και να ελέγχεται από άλλα τρία. Αυτή μπορεί να εφαρμοστεί σε καταχωρητή τεσσάρων qubits και περιγράφεται από τον εξής πίνακα:

$$3CU = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_{11} & x_{12} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & x_{21} & x_{22} \end{bmatrix}$$

Η ονομασία $3CU$ του παραπάνω πίνακα αποτελεί συντομογραφία της ονομασίας *CCCU*, η οποία συμβαδίζει με τους προηγούμενους συμβολισμούς των τριών άλλων πινάκων. Επίσης, η μορφή του πίνακα μπορεί να συμπτυχθεί σε έναν πίνακα 4x4 ως εξής:

$$3CU = \begin{bmatrix} \boldsymbol{I_8} & \boldsymbol{0_8} \\ \boldsymbol{0_8} & CCU \end{bmatrix}$$

Λαμβάνοντας υπόψη τις προηγούμενες παρατηρήσεις για τις τρεις ελεγχόμενες κβαντικές πύλες, μπορεί να εξαχθεί ένας γενικός τρόπος αναπαράστασης πυλών αυτού του είδους. Έτσι, μια οποιαδήποτε τέτοια πύλη, η οποία εφαρμόζεται σε έναν καταχωρητή χωρητικότητας *n* qubits, χρησιμοποιεί τα *n-1* qubits για τον έλεγχο και το ένα qubit ως στόχο για την πιθανή εφαρμογή του μετασχηματισμού μιας οποιασδήποτε πύλης *U*. Γενικότερα, μπορούν να εφαρμοσθούν οι εξής κανόνες για μία ευκολότερη αναπαράσταση και κατανόηση της λειτουργίας της παραπάνω γενικής ελεγχόμενης πύλης:

1. Ο μετασχηματισμός της πύλης U εφαρμόζεται μόνο αν οι καταστάσεις των qubits ελέγχου είναι ταυτόχρονα $|1\rangle$. Σε οποιαδήποτε άλλη περίπτωση ο μετασχηματισμός δεν εφαρμόζεται και το qubit-στόχος μένει ανεπηρέαστο.
2. Για μία πιο συμπτυγμένη αναπαράσταση του συμβόλου της πύλης, μπορεί να χρησιμοποιηθεί ο συμβολισμός $(n-1)CU$, όπου n είναι ο αριθμός των qubits στα οποία εφαρμόζεται η ελεγχόμενη κβαντική πύλη.
3. Ο πίνακας της ελεγχόμενης κβαντικής πύλης είναι μεγέθους $2^n \times 2^n$.
4. Τα στοιχεία του πίνακα της πύλης U βρίσκονται στην κάτω δεξιά γωνία του παραπάνω πίνακα, δηλαδή στις θέσεις $(2^n-1, 2^n-1)$, $(2^n-1, 2^n)$, $(2^n, 2^n-1)$, $(2^n, 2^n)$.
5. Τα στοιχεία της διαγωνίου του πίνακα συμπληρώνονται με 1 έως και το στοιχείο στη θέση $(2^n-2, 2^n-2)$.
6. Όλα τα υπόλοιπα στοιχεία του πίνακα συμπληρώνονται με 0.

Οι παραπάνω κανόνες συνοψίζονται στον εξής πίνακα:

$$[(n-1)CU]_{n\times n} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x_{11} & x_{12} \\ 0 & 0 & 0 & \cdots & x_{21} & x_{22} \end{bmatrix}$$

Τα στοιχεία $x_{11}, x_{12}, x_{21}, x_{22}$ αποτελούν τον πίνακα της πύλης U.

Ακόμη, ο παραπάνω πίνακας μπορεί να γραφεί σαν πίνακας μεγέθους 4x4, για συντομία, ως εξής:

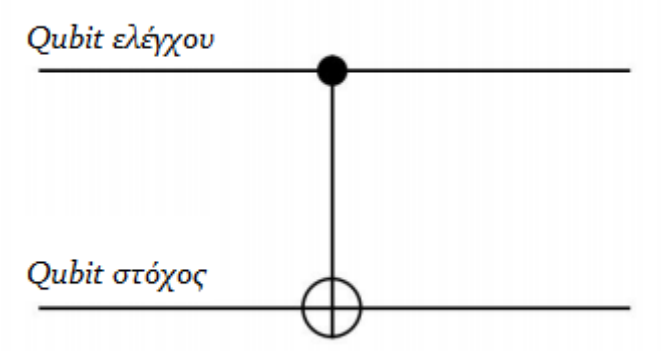
$$[(n-1)CU]_{4\times4} = \begin{bmatrix} \boldsymbol{I_{2^{n-1}}} & \boldsymbol{0_{2^{n-1}}} \\ \boldsymbol{0_{2^{n-1}}} & (n-2)CU \end{bmatrix}$$

Στον παραπάνω συμβολισμό, οι πίνακες $\boldsymbol{I_{2^{n-1}}}$ και $\boldsymbol{0_{2^{n-1}}}$ είναι ο μοναδιαίος και ο μηδενικός πίνακας αντίστοιχα, έκαστοι μεγέθους 2^{n-1}.

4.5.2 Ελεγχόμενες κβαντικές πύλες Pauli

Οι ελεγχόμενες κβαντικές πύλες Pauli είναι πύλες που εφαρμόζονται σε δύο qubits και χρησιμοποιούν το ένα qubit για έλεγχο και το δεύτερο qubit ως στόχο του μετασχηματισμού της εκάστοτε πύλης Pauli. Σύμφωνα με όλα τα παραπάνω που αναλύθηκαν στο προηγούμενο υποκεφάλαιο, αυτές, μαζί με τους πίνακες αληθείας τους, είναι οι εξής:

- Ελεγχόμενη πύλη Pauli-X ή *CX* ή πύλη ελεγχόμενου ΟΧΙ ή *CNOT*:

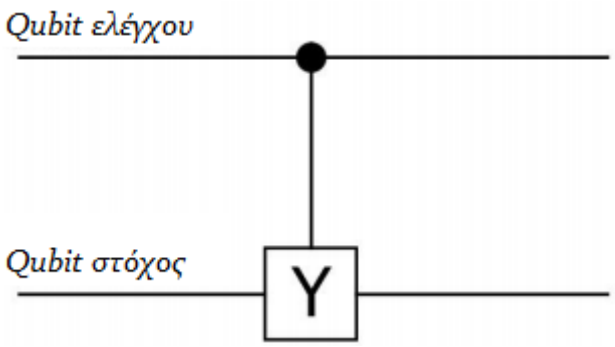


$$CX = CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} \boldsymbol{I_2} & \boldsymbol{0_2} \\ \boldsymbol{0_2} & NOT \end{bmatrix}$$

Πίνακας αληθείας της ελεγχόμενης πύλης NOT

$\|q_{πριν}\rangle$	→	$\|q_{μετά}\rangle$
$\|\mathbf{00}\rangle$		$\|00\rangle$
$\|\mathbf{01}\rangle$		$\|01\rangle$
$\|\mathbf{10}\rangle$		$\|11\rangle$
$\|\mathbf{11}\rangle$		$\|10\rangle$

- Ελεγχόμενη πύλη Pauli-Y ή *CY*:

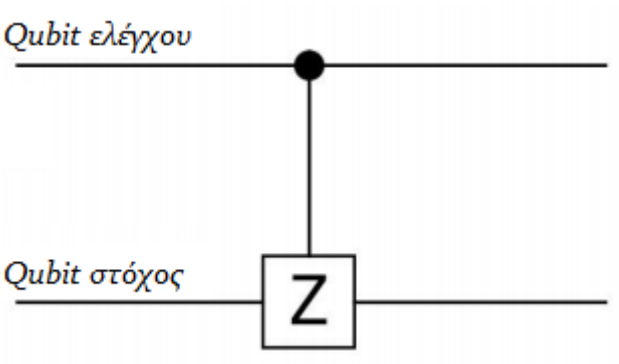


$$CY = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{bmatrix} = \begin{bmatrix} \boldsymbol{I_2} & \mathbf{0_2} \\ \mathbf{0_2} & Y \end{bmatrix}$$

Πίνακας αληθείας της ελεγχόμενης πύλης Pauli-Y

$\|q_{πριν}\rangle$	→	$\|q_{μετά}\rangle$
$\|\mathbf{00}\rangle$		$\|00\rangle$
$\|\mathbf{01}\rangle$		$\|01\rangle$
$\|\mathbf{10}\rangle$		$\|1\rangle \otimes i\|1\rangle$
$\|\mathbf{11}\rangle$		$\|1\rangle \otimes (-i)\|0\rangle$

- Ελεγχόμενη πύλη Pauli-Z ή *CZ*:



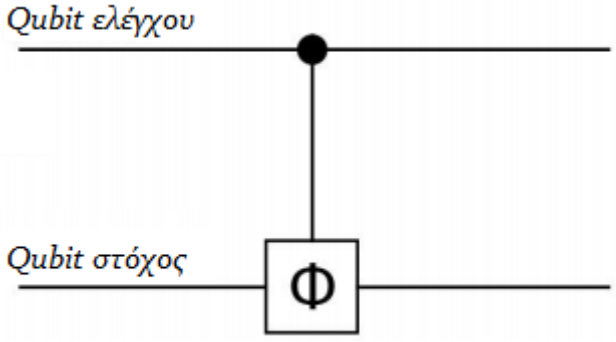
$$CY = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = \begin{bmatrix} \boldsymbol{I_2} & \boldsymbol{0_2} \\ \boldsymbol{0_2} & Z \end{bmatrix}$$

Πίνακας αληθείας της ελεγχόμενης πύλης Pauli-Z

$\|q_{πριν}\rangle$ →	$\|q_{μετά}\rangle$
$\|\mathbf{00}\rangle$	$\|00\rangle$
$\|\mathbf{01}\rangle$	$\|01\rangle$
$\|\mathbf{10}\rangle$	$\|10\rangle$
$\|\mathbf{11}\rangle$	$\|1\rangle \otimes (-1)\|1\rangle$

4.5.3 Κβαντική πύλη ελεγχόμενης μετατόπισης φάσης (CPh)

Η κβαντική πύλη ελεγχόμενης μετατόπισης φάσης εφαρμόζει την πύλη μετατόπισης φάσης στο qubit-στόχο, μόνο αν η κατάσταση του qubit ελέγχου είναι $|1\rangle$. Διαφορετικά, αφήνει την κατάσταση του καταχωρητή αμετάβλητη.



$$CR_\theta = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{bmatrix} = \begin{bmatrix} \boldsymbol{I_2} & \boldsymbol{0_2} \\ \boldsymbol{0_2} & R_\theta \end{bmatrix}$$

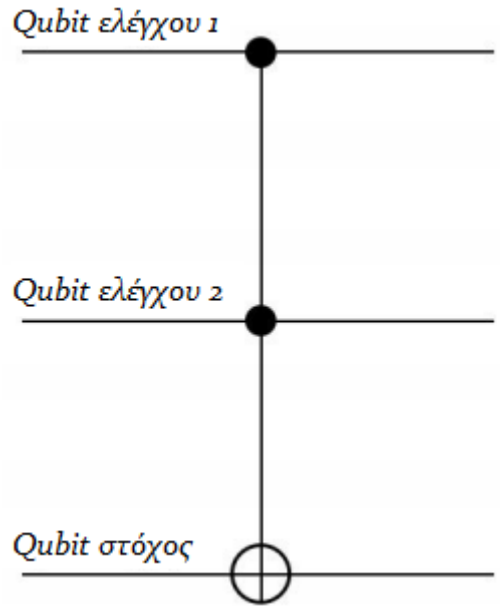
Πίνακας αληθείας της ελεγχόμενης πύλης μετατόπισης φάσης

$\lvert q_{\pi\rho\iota\nu}\rangle$	→	$\lvert q_{\mu\epsilon\tau\acute{\alpha}}\rangle$
$\lvert \mathbf{00}\rangle$		$\lvert 00\rangle$
$\lvert \mathbf{01}\rangle$		$\lvert 01\rangle$
$\lvert \mathbf{10}\rangle$		$\lvert 10\rangle$
$\lvert \mathbf{11}\rangle$		$\lvert 1\rangle \otimes (e^{i\theta})\lvert 1\rangle$

4.5.4 Κβαντική πύλη διπλά ελεγχόμενου ΌΧΙ (CCNOT - Toffoli)

Η κβαντική πύλη διπλά ελεγχόμενου ΌΧΙ, ή αλλιώς CCNOT, επινοήθηκε από τον ιταλό καθηγητή Tommaso Toffoli, προς τιμήν του οποίου αναφέρεται πολλές φορές και ως πύλη Toffoli. Είναι μια πύλη που εφαρμόζεται σε τρία qubits, χρησιμοποιώντας το πρώτο και το δεύτερο για έλεγχο ενώ το τρίτο αποτελεί το qubit-στόχο, στο οποίο εφαρμόζεται μια πύλη NOT. Αυτό σημαίνει ότι η πύλη NOT θα εφαρμοστεί στο qubit-στόχο μόνο όταν και τα δύο qubits ελέγχου βρίσκονται στην κατάσταση $|1\rangle$. Έχει ανάλογο στα κλασσικά υπολογιστικά συστήματα, η οποία λειτουργεί αντίστοιχα με bits. Η πύλη CCNOT σε μορφή πίνακα, καθώς και ο πίνακας αληθείας της, είναι:

$$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} \boldsymbol{I_4} & \boldsymbol{0_4} \\ \boldsymbol{0_4} & CNOT \end{bmatrix}$$



Πίνακας αληθείας της πύλης Toffoli

$\|q_{πριν}\rangle$	→	$\|q_{μετά}\rangle$
$\|000\rangle$		$\|000\rangle$
$\|001\rangle$		$\|001\rangle$
$\|010\rangle$		$\|010\rangle$
$\|011\rangle$		$\|011\rangle$
$\|100\rangle$		$\|100\rangle$
$\|101\rangle$		$\|101\rangle$
$\|110\rangle$		$\|111\rangle$
$\|111\rangle$		$\|110\rangle$

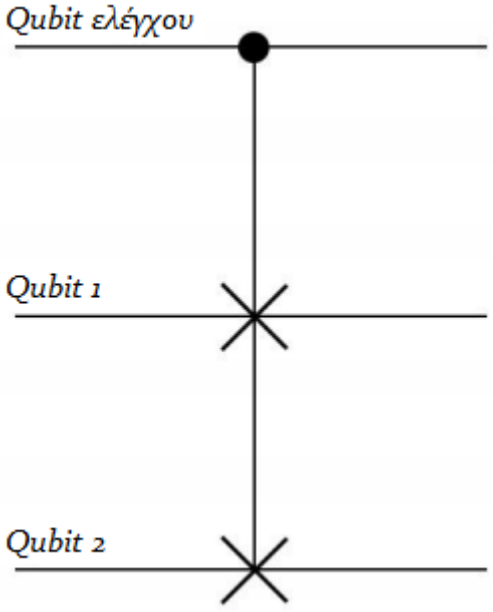
Παραδείγματα εφαρμογής της πύλης αυτής είναι τα εξής:

$$CCNOT|101\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |101\rangle$$

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

4.5.6 Κβαντική πύλη Fredkin

Η κβαντική πύλη Fredkin ονομάστηκε έτσι προς τιμήν του καθηγητή Edward Fredkin. Ουσιαστικά, πρόκειται για μία πύλη ελεγχόμενης εναλλαγής qubits. Αυτή εφαρμόζεται σε τρία qubits, εκ των οποίων το πρώτο είναι το qubit ελέγχου ενώ τα άλλα δύο είναι τα qubits-στόχοι που θα υποστούν το μετασχηματισμό της πύλης *SWAP*, γι' αυτό ονομάζεται και πύλη *CSWAP*. Αυτό σημαίνει ότι η εναλλαγή των δύο qubits-στόχων θα πραγματοποιηθεί μόνο όταν το πρώτο qubit-στόχος, θα είναι στην κατάσταση $|1\rangle$. Στη συνέχεια παρατίθεται η δράση της πύλης Fredkin σε μορφή πίνακα, μαζί με τον πίνακα αληθείας της πύλης.



$$CSWAP = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \boldsymbol{I_4} & \boldsymbol{0_4} \\ \boldsymbol{0_4} & SWAP \end{bmatrix}$$

Πίνακας αληθείας της πύλης Fredkin

$\|q_{\pi\rho\iota\nu}\rangle$	→	$\|q_{\mu\epsilon\tau\acute{\alpha}}\rangle$
$\|\mathbf{000}\rangle$		$\|000\rangle$
$\|\mathbf{001}\rangle$		$\|001\rangle$
$\|\mathbf{010}\rangle$		$\|010\rangle$
$\|\mathbf{011}\rangle$		$\|011\rangle$
$\|\mathbf{100}\rangle$		$\|100\rangle$
$\|\mathbf{101}\rangle$		$\|110\rangle$
$\|\mathbf{110}\rangle$		$\|101\rangle$
$\|\mathbf{111}\rangle$		$\|111\rangle$

Κάποια παραδείγματα εφαρμογής της πύλης αυτής σε κβαντικούς καταχωρητές είναι τα εξής:

$$CSWAP|101\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |110\rangle$$

$$CSWAP|111\rangle = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |111\rangle$$

ΚΕΦΑΛΑΙΟ 5

5. ΚΒΑΝΤΙΚΑ ΚΥΚΛΩΜΑΤΑ

Εισαγωγή και απεικόνιση κυκλωμάτων

Ένα κβαντικό κύκλωμα είναι ένας κβαντικός υπολογισμός που αποτελείται από μια σειρά κβαντικών πυλών οι οποίες εφαρμόζονται σε έναν κβαντικό καταχωρητή χωρητικότητας *n* qubits.

Αρχικά, για την καλύτερη κατανόηση και επεξήγηση των κβαντικών κυκλωμάτων και του συμβολισμού τους, θα πρέπει να γίνει μια σύντομη αναφορά στις αντιστρέψιμες κβαντικές πύλες και στα αντιστρέψιμα κβαντικά κυκλώματα.

Μια αντιστρέψιμη κβαντική πύλη μπορεί να περιγραφεί ως μία κβαντική πύλη της οποίας ο αριθμός των qubits που εξέρχονται από αυτήν είναι ίδιος με τον αριθμό των εισερχόμενων qubits. Επιπρόσθετα, εάν εφαρμοστεί η πύλη αντίστροφα σε κάποιο qubit που έχει υποστεί ήδη μετασχηματισμό, τότε θα ληφθεί η κατάσταση του αρχικού qubit. Ένα παράδειγμα μιας τέτοιας κβαντικής πύλης είναι η κβαντική πύλη Hadamard. Εφαρμόζοντας την πύλη αυτή σε ένα qubit με αρχική κατάσταση $|1\rangle$, αυτό μετασχηματίζεται ως εξής:

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

Συνεχίζοντας, αν η ίδια πύλη εφαρμοστεί στο παραπάνω qubit, τότε η έξοδος θα πρέπει να είναι το αρχικό qubit που βρίσκεται στην κατάσταση $|1\rangle$. Όντως, ο παραπάνω υποθετικός συλλογισμός επαληθεύεται καθώς:

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

Εξετάζοντας μία προς μία τις κβαντικές πύλες, διαπιστώνει κανείς ότι όλες οι προαναφερθείσες πύλες είναι αντιστρέψιμες.

Ακόμα ένα σημαντικό θεώρημα που αφορά τα κβαντικά κυκλώματα είναι το θεώρημα αδυναμίας διακλάδωσης (no-cloning theorem). Το θεώρημα αυτό παρουσιάστηκε από τους Wootters, Zurek και Dieks και αποτελεί θεμελιώδες θεώρημα της επιστήμης του κβαντικού υπολογισμού.

Πιο συγκεκριμένα, το θεώρημα αδυναμίας διακλάδωσης αναφέρει ότι είναι αδύνατον να αντιγράψουμε την κατάσταση ενός qubit σε ένα άλλο. Η απόδειξη του παραπάνω ισχυρισμού βασίζεται στην *εις άτοπον απαγωγή* και παρουσιάζεται παρακάτω:

Θεωρούμε ότι υπάρχει μια γενική πύλη *UC* που επιδρά σε δύο qubits. Ως εισόδους έχει ένα qubit σε κάποια άγνωστη κατάσταση q και ένα άλλο που βρίσκεται στην κατάσταση $|0\rangle$. Η δράση αυτής της πύλης είναι η αντιγραφή της κατάστασης του πρώτου qubit στο δεύτερο. Αυτό συνεπάγεται ότι η πύλη στην έξοδό της θα έχει δύο qubits με την ίδια κατάσταση q.

Έστω, λοιπόν, ότι η πύλη αυτή επιδρά σε δύο qubits, $|a\rangle$ και $|b\rangle$, που είναι ορθογώνια μεταξύ τους, ως εξής:

$$UC|a0\rangle = |aa\rangle \text{ και } UC|b0\rangle = |bb\rangle$$

Επιπλέον, υπάρχει άλλο ένα qubit, το οποίο αποτελεί υπέρθεση των δύο προηγουμένων:

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

Εφαρμόζοντας την πύλη *UC* στο παραπάνω qubit, έχουμε:

$$UC|c0\rangle = \frac{1}{\sqrt{2}}UC(|a\rangle + |b\rangle)|0\rangle = \frac{1}{\sqrt{2}}UC(|a0\rangle + |b0\rangle) = \frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle)$$

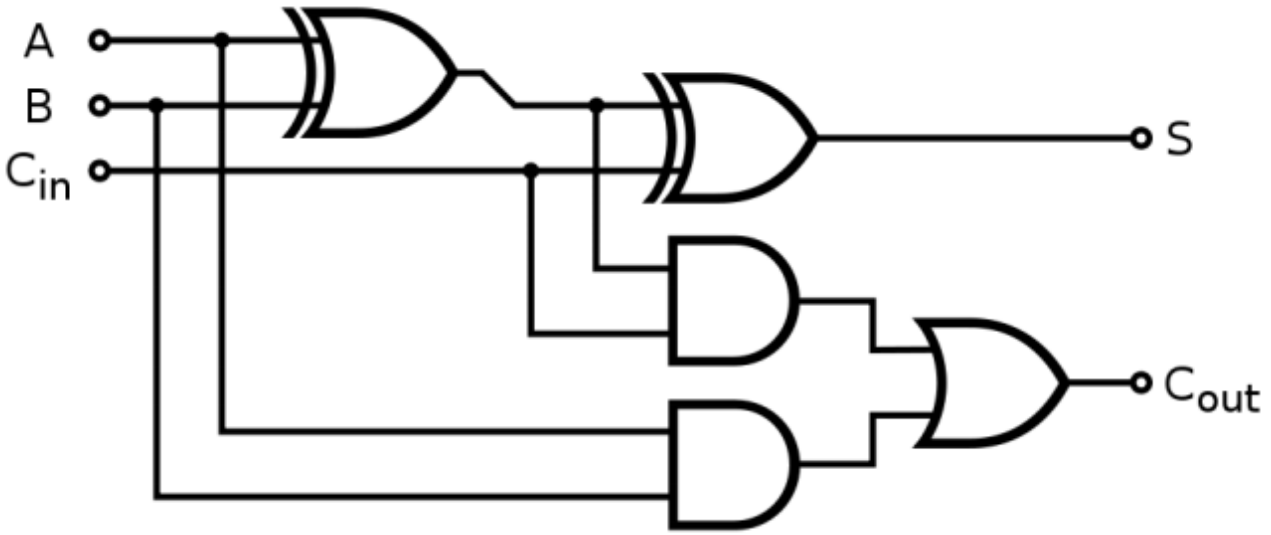
Συνεπώς, ενώ τα αριστερά μέλη των δύο παραπάνω εξισώσεων είναι ίδια, τα δεξιά τους μέλη είναι διαφορετικά και έτσι αυτή η πύλη δεν υφίσταται. Άρα, δεν

μπορεί να δημιουργηθεί κάποια πύλη η οποία να υλοποιεί την αντιγραφή της κατάστασης ενός qubit σε ένα άλλο.

Η σημασία του ανωτέρω θεωρήματος είναι εξαιρετικά σημαντική και αποτελεί τη βάση της κβαντικής κρυπτογραφίας. Η βάση του προηγούμενου ισχυρισμού είναι ότι δε δίνεται η δυνατότητα στον υποκλοπέα να αντιγράψει το μήνυμα για να το αποκρυπτογραφήσει. Ακόμη και αν κρατήσει το μήνυμα, θα πρέπει να καταστρέψει την υπέρθεση των qubits έτσι ώστε να μπορέσει να το διαβάσει. Επομένως, δε θα υπάρχει μήνυμα για να αποσταλεί στον τελικό παραλήπτη και ως εκ τούτου, αυτός θα αντιληφθεί ότι το μήνυμα υποκλάπηκε και θα αλλάξει τη στρατηγική επικοινωνίας με τον πομπό.

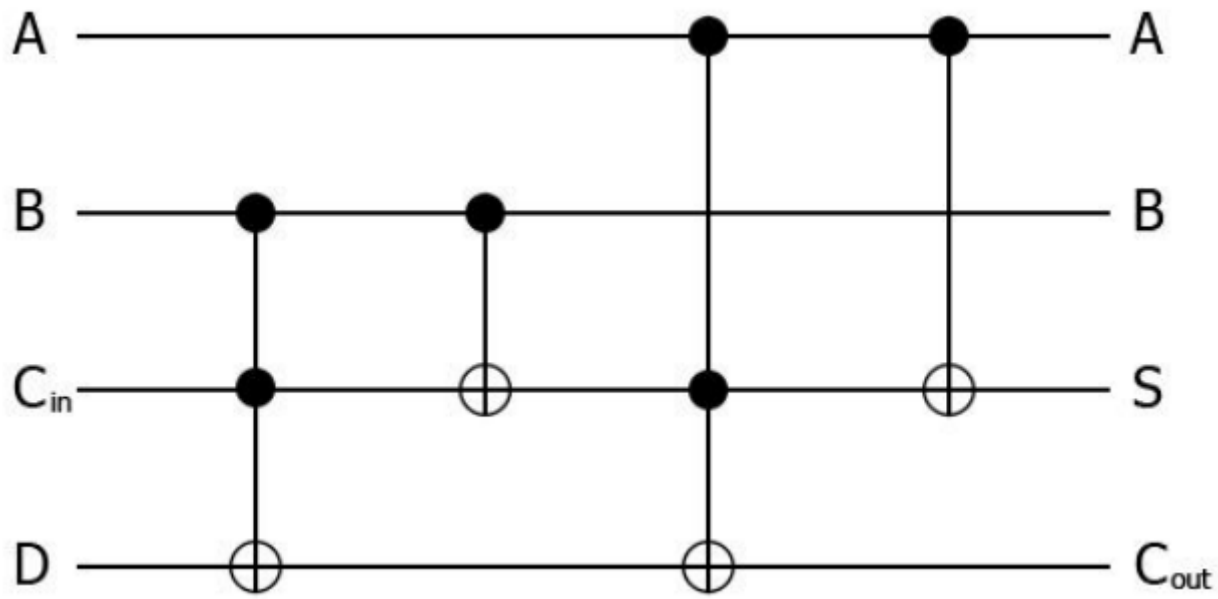
Ένα επιπλέον πρόβλημα που δημιουργείται από το θεώρημα αδυναμίας διακλάδωσης είναι το γεγονός ότι δεν επιτρέπει τις κλασσικές μεθόδους διόρθωσης λαθών. Το πρόβλημα προκύπτει όταν θα χρειαστεί κάποια αντιγραφή των καταστάσεων των qubits για να χρησιμοποιηθούν αργότερα για τη διόρθωση ενδεχόμενων σφαλμάτων. Αυτό το πρόβλημα λύθηκε το 1995 από τον Peter Shor, προτείνοντας έναν αλγόριθμο που παρακάμπτει το προηγούμενο θεώρημα.

Πλέον, μπορεί να γίνει αναφορά και παρουσίαση των κβαντικών λογικών κυκλωμάτων σε αντιστοιχία με αυτά των κλασσικών υπολογιστών. Όπως στα κλασσικά λογικά κυκλώματα, έτσι και στα κβαντικά, ο χρόνος και τα δεδομένα κινούνται από τα αριστερά προς τα δεξιά.



Σχήμα 14: Κύκλωμα ενός 1-bit πλήρους αθροιστή.

Παρακάτω παρατίθεται και το αντίστοιχο κβαντικό ανάλογο του προηγούμενου κυκλώματος.

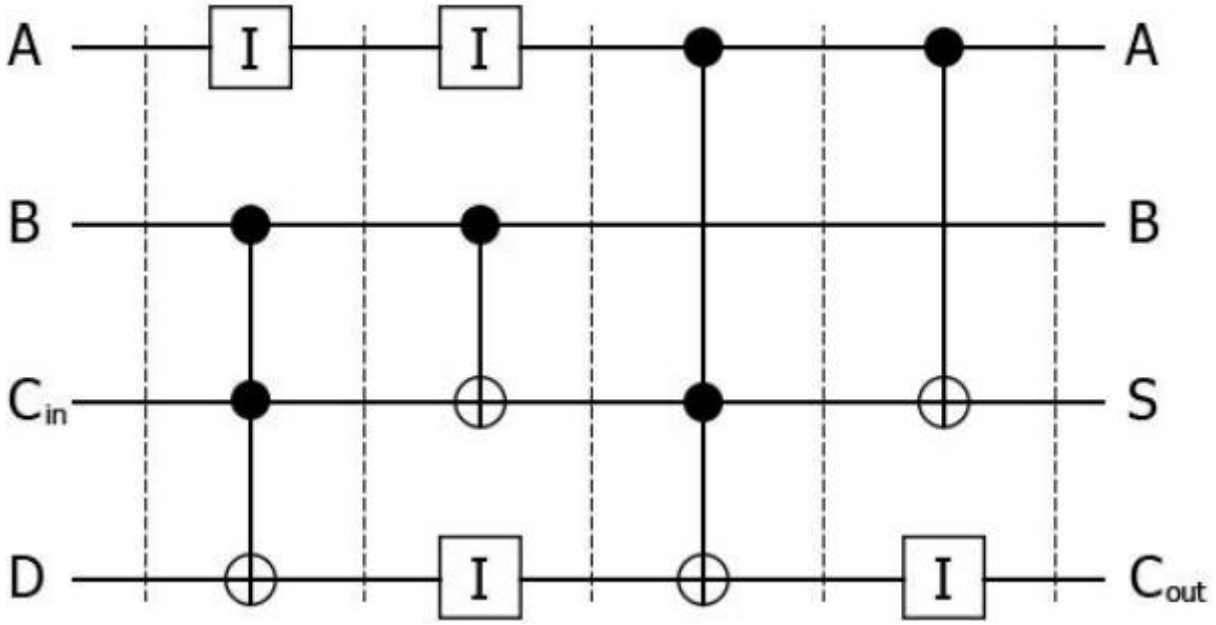


Πρώτη διαφορά που παρατηρείται είναι η ύπαρξη τεσσάρων qubits στην είσοδο και στην έξοδο. Εν αντιθέσει με το κλασσικό κύκλωμα, στο κβαντικό πρέπει να τηρηθεί η αντιστρεψιμότητα, για την επίτευξη της οποίας πρέπει τα qubits της εξόδου να είναι ισάριθμα των qubits της εισόδου. Για το λόγο αυτό, στην είσοδο προστίθεται ένα βοηθητικό qubit *D* (συνήθως με κατάσταση $|0\rangle$, έτσι ώστε να μην επηρεάζεται η έξοδος). Τελικώς, τα qubits που έχουν σημασία είναι τα *S* και

C_{out}, το άθροισμα και το κρατούμενο αντίστοιχα.

Ακόμα μία μεγάλη διαφορά είναι ο τρόπος εφαρμογής και λειτουργίας του εκάστοτε κυκλώματος. Στο κλασσικό κύκλωμα, τα bits εισόδου εισέρχονται στο κύκλωμα ως ηλεκτρικοί παλμοί, και μέσω κάποιων συνδέσεων-αγωγών μεταφέρονται από πύλη σε πύλη. Σε αντίθεση, στο κβαντικό κύκλωμα οι πύλες εφαρμόζονται με τη σειρά πάνω σε έναν κβαντικό καταχωρητή που έχει αποθηκευμένα τα qubits. Έτσι, στο τέλος της εφαρμογής του κυκλώματος, υπάρχει ο ίδιος καταχωρητής με διαφορετικές καταστάσεις των qubits. Επίσης, ενώ η σειρά των bits στο κλασσικό κύκλωμα είναι από πάνω προς τα κάτω, στο κβαντικό είναι από κάτω προς τα πάνω.

Μια επιπρόσθετη παρατήρηση αφορά τον τρόπο που παρουσιάζεται ο χρόνος στις κυκλωματικές απεικονίσεις. Στην περίπτωση του κλασσικού κυκλώματος, δεν μπορεί να εξαχθεί κάποιο σαφές συμπέρασμα για τον απαιτούμενο χρόνο επεξεργασίας των δεδομένων εισόδου και ανάκτησης των δεδομένων εξόδου. Αντίθετα, στο κβαντικό κύκλωμα υπάρχει διαμερισμός χρονικών διαστημάτων (βήματα), εντός των οποίων έχουμε δράση κάποιας κβαντικής πύλης σε κάθε qubit του κβαντικού καταχωρητή. Η περίπτωση που δεν υφίσταται κάποια αλλαγή σε ένα qubit σε ένα χρονικό διάστημα, είναι σαν να εφαρμόζεται η κβαντική πύλη αδράνειας. Έτσι, μπορεί να προκύψει μια νέα απεικόνιση για το κβαντικό κύκλωμα, η οποία δύναται να χρησιμοποιηθεί αρκετές φορές.



Ως φυσικό επακόλουθο, υπάρχουν μεγάλες διαφορές και στην απεικόνιση των πινάκων αληθείας των δύο κυκλωμάτων. Πιο συγκεκριμένα, η διαφορά έγκειται στη σειρά με την οποία παρουσιάζονται και είναι ταξινομημένα τα qubits στις στήλες του πίνακα.

Πίνακας αληθείας του κλασικού κυκλώματος του πλήρους αθροιστή

Είσοδος			Έξοδος	
A	B	C_{in}	S	C_{out}
0	0	0	0	0
0	1	0	1	0
1	0	0	1	0
1	1	0	0	1
0	0	1	1	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	1

Πίνακας αληθείας του κβαντικού κυκλώματος του πλήρους αθροιστή

Είσοδος				Έξοδος			
D	C_{in}	B	A	C_{out}	S	B	A
0	0	0	0	0	0	0	0
0	0	0	1	0	1	0	1
0	0	1	0	0	1	1	0
0	0	1	1	1	0	1	1
0	1	0	0	0	1	0	0
0	1	0	1	1	0	0	1
0	1	1	0	1	0	1	0
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	0
1	0	0	1	1	1	0	1
1	0	1	0	1	1	1	0
1	0	1	1	0	0	1	1
1	1	0	0	1	1	0	0
1	1	0	1	0	0	0	1
1	1	1	0	0	0	1	0
1	1	1	1	0	1	1	1

Βιβλιογραφία

1. Aaronson Scott (2013), Quantum Computing since Democritus, Cambridge University Press
2. Mark Fox (2006), Quantum Optics, An Introduction, Oxford University Press
3. Τραχανάς Στέφανος (2012), Στοιχειώδης Κβαντική Φυσική, Πανεπιστημιακές Εκδόσεις Κρήτης
4. Τραχανάς Στέφανος (2008), Κβαντομηχανική ΙΙ, Πανεπιστημιακές Εκδόσεις Κρήτης
5. Καραφυλλίδης Ιωάννης (2005), Κβαντικοί Υπολογιστές, Κλειδάριθμος.
6. Αντωνιάδης Ιωάννης, Σημειώσεις Μαθήματος Κβαντικών Υπολογιστών και Κβαντικής Κρυπτογραφίας, Τμήμα Πληροφορικής ΑΠΘ
7. Κροντήρης Ιωάννης (2000), Κβαντική Θεωρία της Πληροφορίας, Διδακτορική Διατριβή, Πανεπιστήμιο Ηρακλείου.
8. Bub Jeffrey (2010), Quantum Entanglement and Information, http://plato.stanford.edu/entries/qt-entangle/
9. Mermin N. David (2007), Quantum Computer Science: An Introduction, 1st Edition, Cambridge University Press.
10. Michael A. Nielsen (2011), Quantum Computation and Quantum Information: 10th Anniversary Edition, Cambridge University Press
11. Colin P. Williams (2011), Explorations in Quantum Computing, 2nd Edition, Springer