Σχολή : Θετικών Επιστημών και Τεχνολογίας

Μεταπτυχιακό Πρόγραμμα Σπουδών :

Προχωρημένες Σπουδές στη Φυσική MSc

Διπλωματική Εργασία

Κβαντικοί Υπολογιστές

Θεωρητική Μελέτη-Δυνατότητες Πραγματοποίησης

Ζαρμπούτης Δημήτριος

Επιβλέπων καθηγητής: Ζούπας Ανδρέας

Μάιος 2018

Κβαντικοί Υπολογιστές

Θεωρητική Μελέτη-Δυνατότητες Πραγματοποίησης

Quantum Computers

Theoretical Consideration - Possibilities of Realization

Ζαρμπούτης Δημήτριος

Zarmpoutis Dimitrios

Επιτροπή Επίβλεψης Διπλωματικής Εργασίας

Επιβλέπων Καθηγητής:

Ζούπας Ανδρέας

Τμήμα Φυσικής, ΕΑΠ

Συν-Επιβλέπων Καθηγητής:

Περιβολαρόπουλος Λέανδρος

Τμήμα Φυσικής, ΕΑΠ

Μάιος 2018

Θα ήθελα να ευχαριστήσω ιδιαίτερα τον επιβλέποντα καθηγητή μου κύριο Ζούπα Ανδρέα για την άψογη συνεργασία μας.

Η εργασία μου αυτή είναι αφιερωμένη στην οικογένειά μου, στη γυναίκα μου Μπέτυ και στα παιδιά μου Σταμάτη, Νίκο και Νεφέλη.

Περίληψη

Η κβαντική μηχανική είναι γνωστό ότι από τα μέσα του 20^{ου} αιώνα που θεμελιώθηκε, έφερε επανάσταση στην επιστήμη της Φυσικής αλλά και στην κοινή λογική. Σίγουρα οι βασικές αρχές της, παρόλο που είναι σχετικά απλές από μαθηματικής άποψης, είναι φαινομενικά τουλάχιστον, ξένες ως προς τον συνηθισμένο τρόπο σκέψης. Αυτό είχε σαν αποτέλεσμα να πολεμηθεί από πολλούς ακόμα και ειδικούς. Στην πορεία οι μεγάλες επιτυχίες της την κατέστησαν από τα ισχυρότερα εργαλεία της επιστήμης, παρόλα αυτά υπάρχουν ακόμα εννοιολογικές διαμάχες γύρω απ' αυτήν. Δύο πολλά υποσχόμενα πεδία έρευνας σήμερα, είναι η κβαντική υπολογιστική και η κβαντική πληροφορία τα οποία παρουσιάζουν ενδιαφέρον γιατί εκτός από τις πιθανές πρακτικές εφαρμογές που προσδοκούνται απ' αυτά, κινούνται στα όρια των πιο παράξενων προβλέψεων της κβαντικής μηχανικής όπως οι καταστάσεις διεμπλοκής, τις οποίες ανέδειξαν πολλοί μεγάλοι Φυσικοί με πρώτο τον Albert Einstein, με τις οποίες ακόμα και σήμερα οι άνθρωποι δεν έχουν συμφιλιωθεί.

Η πορεία της μελέτης των πεδίων αυτών είναι ένα μεγάλο στοίχημα, αφού η βαθύτερη κατανόηση τους ίσως οδηγήσει στη βαθύτερη κατανόηση της «μυστηριώδους» κβαντικής μηχανικής και άρα της Φύσης, την οποία φαίνεται να περιγράφει με τόση επιτυχία με τα μέχρι τώρα δεδομένα. Ο σκοπός αυτής της εργασίας λοιπόν είναι να απαντήσει σε ερωτήματα όπως «ποιες είναι οι θεμελιώδεις αρχές της κβαντικής υπολογιστικής και της κβαντικής πληροφορίας;», «πώς αυτές οι αρχές έχουν αναπτυχτεί έως τώρα;», «ποια η συνεισφορά των αρχών αυτών στη βαθύτερη κατανόηση της κβαντικής μηχανικής;», «πού και πώς μπορούν αυτές οι ιδέες να χρησιμοποιηθούν;».

Λέξεις – Κλειδιά

Κβαντικός Υπολογιστής, Κβαντική Πληροφορία, Κβαντικές Πύλες, Κβαντικοί Αλγόριθμοι, Κβαντική Κρυπτογραφία.

Abstract

Quantum mechanics, since the beginning of the 20th century, where its fundamental principles were progressively formulated, has traversed a long trajectory in time, full of successes in theoretical explanations of inexplicable at the time phenomena and later of many practical applications. Today, our life is full of machines whose existence is due to quantum mechanics. Nevertheless there is another point of view in this story. That great theory, from the very beginning included a mystery regarding to its fundamental principles, which seemed to be incomprehensible and unreasonable. It is remarkable that some of the founders of quantum mechanics like Albert Einstein didn't like at all the way things had evolved and tried hard to prove that something was wrong. It is also remarkable that in all these years, although quantum mechanics has proven to be a very precise theory, it has only been a little progress on its deeper understanding. People are still feeling uncomfortable when they try to understand that theory.

Quantum Information and Quantum Computation are today two popular fields of research, for two reasons. The first is that maybe they can lead to many remarkable applications. The second, and rather more important for a physicist, is than they touch exactly that mystery of the deeper understanding of quantum mechanics. Thus, deeper understanding of Quantum Information and Quantum Computation means also deeper understanding, at last, of quantum mechanics and of Nature in general. In that sense, this essay tries to answer questions like "What are the fundamental principles of Quantum Information and Quantum Computation?", "How much have these principles evolved until today?", "What is the contribution of these principles to the deeper understanding of quantum mechanics?", "Where and how these new ideas could be used?".

Keywords

Quantum Computation, Quantum Information, Qubit, Quantum algorithms, Deutsh's algorithm, EPR states.

Περιεχόμενα

Κατάλογος Σχημάτων

1. Γενική θεώρηση-Ιστορική αναδρομή

Κβαντική υπολογιστική (quantum computation) και κβαντική πληροφορία (quantum information), είναι η μελέτη των επιτευγμάτων σε θέματα σχετικά με την πληροφορία που θα μπορούσαν να πραγματοποιηθούν χρησιμοποιώντας κβαντικά συστήματα. Για να γίνουν κατανοητά αυτά τα πεδία καθώς και το ερώτημα γιατί δεν είχε συλληφθεί αυτή η ιδέα νωρίτερα, θα πρέπει να γίνει μια σύντομη αναδρομή σε καθένα απ' τα πεδία που συνεισφέρουν στην οικοδόμηση της κβαντικής υπολογιστικής και της κβαντικής πληροφορίας που είναι η κβαντική μηχανική και η επιστήμη των υπολογιστών.

1.1 Ιστορική αναδρομή και βασικές αρχές της Κβαντικής Φυσικής

Η ιστορία της κβαντικής μηχανικής ξεκινά στις αρχές του 20^{ου} αιώνα όταν η ως τότε γνωστή Φυσική (η οποία σήμερα ονομάζεται Κλασική Φυσική), αδυνατούσε να εξηγήσει ορισμένα φαινόμενα σχετικά με το άτομο. Αυτή η αδυναμία αποδείχθηκε τόσο σοβαρή ώστε τελικά απαιτήθηκε μια ριζική αναθεώρηση της θεωρίας. Έτσι σταδιακά προέκυψε μια καινούργια θεωρία, η κβαντική μηχανική, η οποία από τότε έγινε αναπόσπαστο κομμάτι της επιστήμης και έχει εφαρμοστεί με τεράστια επιτυχία σχεδόν σε όλα τα πεδία όπως για παράδειγμα την κατασκευή του ατόμου, την πυρηνική σύντηξη στο εσωτερικό των αστέρων, την υπεραγωγιμότητα, την κατασκευή του DNA και τη Φυσική στοιχειωδών σωματιδίων. Οι αρχές της κβαντικής μηχανικής είναι σχετικά απλές αλλά ακόμα και οι ειδικοί βρίσκουν ότι αντιβαίνουν στην κοινή λογική. Μάλιστα οι πρώτοι που ασχολήθηκαν με την κβαντική υπολογιστική και την κβαντική πληροφορία, ίσως να παρακινήθηκαν απ' την επιθυμία της καλύτερης κατανόησης της κβαντικής μηχανικής. Ο πιο διάσημος επικριτής της κβαντικής μηχανικής ήταν ο Albert Einstein, ο οποίος έως το τέλος της ζωής του προσπαθούσε να αποδείξει τη μη ορθότητα της θεωρίας αυτής που μάλιστα ο ίδιος αρχικά συνέβαλε τα μέγιστα στην ανάπτυξή της. Από τότε γενιές φυσικών αγωνίζονται να βρουν πεδία στα οποία θα μπορέσουν να ερμηνεύσουν την κβαντική μηχανική με τέτοιο τρόπο ώστε οι προβλέψεις της να γίνουν πιο εύγευστες ως προς την κοινή λογική. Δύο τέτοια πεδία (συγγενικά μεταξύ τους), είναι η κβαντική υπολογιστική

και η κβαντική πληροφορία, των οποίων η ανάπτυξη μεταξύ άλλων φιλοδοξεί να οξύνει τη διαίσθηση μας σε σχέση με την κβαντική μηχανική και έτσι να κάνει τις προβλέψεις της περισσότερο οικείες στον ανθρώπινο νου.

Ας κάνουμε τώρα μια σύντομη επισκόπηση της κβαντικής μηχανικής διατυπώνοντας παράλληλα και τις βασικές αρχές της οι οποίες είναι απαραίτητες για την κατανόηση αυτής της εργασίας. Η ιστορία αρχίζει μπορεί να πει κανείς, στις αρχές του $20^{ου}$ αιώνα όταν παρατηρήθηκαν ορισμένα νέα για την εποχή φαινόμενα όπως η ακτινοβολία μέλανος σώματος (1900), το φωτοηλεκτρικό φαινόμενο (1905), τα ατομικά φάσματα καθώς και η ίδια η ατομική σταθερότητα (1911-13) και το φαινόμενο Compton (1921) στα οποία διαπιστώθηκε η αδυναμία της Κλασικής Φυσικής να τα ερμηνεύσει. Και όπου γινόταν προσπάθεια για κάτι τέτοιο, πολλές φορές κατέληγε σε παράλογες ερμηνείες με βάση την κοινή εμπειρία. Οι κορυφαίοι φυσικοί της εποχής (Planck, Einstein, Bohr), όπως ήταν φυσιολογικό προσπάθησαν να διορθώσουν τα πράγματα με τροποποιητικές προτάσεις πάνω στην κλασική θεωρία οι οποίες όμως αποδεικνύονταν ανίσχυρες να θεραπεύσουν την αδυναμία της. Έτσι φτάσαμε στο 1923 όταν διατυπώθηκε απ' τον De Broglie η επαναστατική *αρχή του κυματοσωματοδυϊκού δυϊσμού* και σιγά-σιγά αποδείχθηκε ότι αυτές οι προηγούμενες διορθωτικές τροποποιήσεις δεν ήταν τίποτα άλλο από προσεγγίσεις αυτής της γενικότερης αρχής σύμφωνα με την οποία :

Όλες οι οντότητες της φύσης έχουν διπλή υφή, σωματιδιακή και κυματική. Έτσι ότι ως τότε θεωρούνταν αποκλειστικά κύμα όπως το φως, με βάση αυτήν την αρχή θεωρείται ότι έχει και σωματιδιακές ιδιότητες και ότι θεωρούνταν αποκλειστικά ως σωματίδιο όπως το ηλεκτρόνιο θεωρείται ότι έχει και κυματικές ιδιότητες. Οι σχέσεις που συνδέουν αυτές τις φαινομενικά ασυμβίβαστες όψεις της φύσης είναι οι :

$$E = \hbar\omega \text{ **και** } p = \hbar k \qquad \textbf{(1-1)}$$

Όπου E, p η ενέργεια και η ορμή αντίστοιχα, είναι τα σωματιδιακά χαρακτηριστικά και ω και k αντίστοιχα η συχνότητα και ο κυματαριθμός, τα κυματικά χαρακτηριστικά των διαφόρων οντοτήτων.

Εφόσον λοιπόν διατυπώθηκε η άποψη ότι τα σωματίδια έχουν και κυματικές ιδιότητες, ήταν απαραίτητη και μια κυματική εξίσωση και αυτή ήταν η *εξίσωση Schrodinger* :

$$i\hbar\frac{\partial\psi}{\partial t} = -\frac{\hbar^2}{2m}\frac{\partial^2\psi}{\partial x^2} + V(x)\psi \qquad \textbf{(1-2)}$$

που είναι μια γραμμική μερική διαφορική εξίσωση ως προς τη συνάρτηση ψ(x,t) που ονομάστηκε κυματοσυνάστηση και περιγράφει με τον καλύτερο δυνατό τρόπο την κατάσταση ενός σωματιδίου μάζας m που βρίσκεται σε δυναμικό V(x).

Προκειμένου να εξηγηθεί το εύλογο ερώτημα πώς είναι δυνατόν ένα σωματίδιο να είναι ταυτόχρονα και κύμα, ο Max Born το 1926 διατύπωσε τη *στατιστική ερμηνεία* της κυματοσυνάρτησης, σύμφωνα με την οποία η ποσότητα $|\psi|^2$ μας δίνει την πυκνότητα πιθανότητας να βρεθεί το σωματίδιο σε κάποια περιοχή του χώρου. Έτσι σύμφωνα με αυτή την ερμηνεία, η μέγιστη πληροφορία που μπορούμε να έχουμε για ένα κβαντικό σύστημα είναι οι πιθανότητες που προκύπτουν από την κυματοσυνάρτηση ψ την οποία βρίσκουμε λύνοντας την εξίσωση Schrodinger.

Μια συνέπεια του κυματοσωματιδιακού δυϊσμού είναι η περίφημη *αρχή της αβεβαιότητας ή απροσδιοριστίας του Heisenberg* σύμφωνα με την οποία :

Δεν μπορούμε να γνωρίζουμε ταυτόχρονα κάποια φυσικά μεγέθη που αφορούν ένα σώμα όπως τη θέση του x και την ορμή του p. Συγκεκριμένα όσο καλύτερα ξέρουμε τη θέση (μικρή αβεβαιότητα Δx), τόσο λιγότερο καλά ξέρουμε την ορμή p (μεγάλη αβεβαιότητα Δp). Αυτή η αρχή μαθηματικά εκφράζεται απ' τη σχέση :

$$\Delta x \cdot \Delta p \geq \hbar/2 \qquad \textbf{(1-3)}$$

Μια άλλη μορφή της αρχής της αβεβαιότητας που θα μας φανεί χρήσιμη παρακάτω είναι η :

$$\Delta E \cdot \tau \geq \hbar/2 \qquad \textbf{(1-4)}$$

όπου ΔΕ η αβεβαιότητα στην ενέργεια και τ ο χρόνος εξέλιξης του συστήματος, ο χρόνος δηλαδή που απαιτείται για μια αισθητή μεταβολή σε κάποιες παραμέτρους του συστήματος.

Η μαθηματική περιγραφή των φυσικών μεγεθών στην κβαντική φυσική γίνεται αντιστοιχώντας κάθε φυσικό μέγεθος Α με έναν ερμιτιανό τελεστή $\hat{A}$ [1]. Λύνοντας την εξίσωση ιδιοτιμών :

[1] Ερμιτιανός λέγεται ένας τελεστής για τον οποίο ισχύει $\langle \varphi, \hat{A}\psi \rangle = \langle \hat{A}\varphi, \psi \rangle$. Η Ερμιτιανότητα εξασφαλίζει μεταξύ άλλων ότι η μέση τιμή και οι ιδιοτιμές του τελεστή είναι πραγματικές.

$$\hat{A}\psi = \alpha\psi \quad \textbf{(1-5)}$$

προκύπτουν οι ιδιοσυναρτήσεις ψ_i και οι ιδιοτιμές α_i του τελεστή $\hat{A}$ που αντιστοιχεί στο φυσικό μέγεθος Α. Οι ιδιοτιμές α_i είναι τα μόνα δυνατά αποτελέσματα μιας μέτρησης του μεγέθους Α. Αν η κατάσταση του συστήματος είναι μια ιδιοσυνάρτηση ψ_i, τότε το αποτέλεσμα της μέτρησης θα είναι η αντίστοιχη ιδιοτιμή α_i με πιθανότητα 100% και η κατάσταση του συστήματος θα εξακολουθήσει να είναι η ψ_i. Αν όμως η κατάσταση του συστήματος είναι γραμμικός συνδυασμός κάποιων ιδιοσυναρτήσεων δηλαδή η :

$$\psi = \sum_i c_i \psi_i \quad \textbf{(1-6)}$$

τότε λέμε ότι η κατάσταση ψ είναι κατάσταση επαλληλίας και το αποτέλεσμα της μέτρησης θα είναι μια απ' τις ιδιοτιμές α_i με πιθανότητα $|c_i|^2$. Να σημειωθεί ότι η συνάρτηση ψ είναι σίγουρα λύση της εξίσωσης Schrodinger αν είναι λύσεις οι συναρτήσεις ψ_i, λόγω της γραμμικότητας της εξίσωσης αυτής. Σε αυτήν την περίπτωση η κατάσταση του συστήματος αλλάζει και μεταπίπτει στην κατάσταση ψ_i η ιδιοτιμή της οποίας είναι η α_i που μετρήθηκε. Άρα αν ακολουθήσει νέα μέτρηση αυτή θα δώσει αποτέλεσμα πάλι α_i με πιθανότητα 100% αυτή τη φορά.

1.2 Ιστορική αναδρομή της επιστήμης των υπολογιστών

Ας στρέψουμε τώρα την προσοχή μας από την κβαντική μηχανική σε ένα άλλο τομέα που γεννήθηκε και αναπτύχτηκε ραγδαία τον 20^{ο} αιώνα, την επιστήμη των υπολογιστών. Τα πρώτα βήματα της επιστήμης αυτής χάνονται στα βάθη της ιστορίας. Για παράδειγμα επιγραφές σε σφηνοειδή γραφή δείχνουν ότι από την εποχή του Hammurabi γύρω στα 1750 π.Χ. , οι Βαβυλώνιοι είχαν αναπτύξει πολύ εκλεπτυσμένες ιδέες στους αλγόριθμους[2] και είναι πιθανό μερικές απ' αυτές τις ιδέες να ήταν ακόμη παλαιότερες. Η σύγχρονη εξέλιξη της επιστήμης των υπολογιστών, κυρίως οφείλεται στο σπουδαίο μαθηματικό Alan Turing ο οποίος παρουσίασε τις ιδέες του σε μια δημοσίευση σταθμό του 1936. Ο Turing παρουσίασε με λεπτομέρειες σε αφηρημένη μορφή αυτό που σήμερα ονομάζουμε

[2] Αλγόριθμος ονομάζεται μια σειρά από πεπερασμένες αυστηρά καθορισμένες ενέργειες που στοχεύουν στην επίλυση ενός προβλήματος σε πεπερασμένο χρόνο.

υπολογιστή και ήταν ένα πρότυπο για μέθοδο υπολογιστικής που σήμερα είναι γνωστό σαν μηχανή Turing προς τιμήν του. Ο Turing έδειξε ότι υπάρχει μια *«παγκόσμια μηχανή Turing»* η οποία μπορεί να προσομοιώσει κάθε άλλη μηχανή Turing. Επίσης ισχυρίστηκε ότι αν ένας αλγόριθμος μπορεί να «τρέξει» σε μια υπολογιστική μηχανή, τότε υπάρχει ένας ισοδύναμος αλγόριθμος για την «παγκόσμια μηχανή Turing» που μπορεί να επιτύχει το ίδιο αποτέλεσμα με τον προηγούμενο. Αυτός ο ισχυρισμός που είναι γνωστός ως θέση των Church-Turing, υποδηλώνει την ισοδυναμία μεταξύ ενός αλγορίθμου που μπορεί να πραγματοποιηθεί με μια φυσική διάταξη και μιας πιο αυστηρής μαθηματικής αντιμετώπισης της «παγκόσμιας μηχανής Turing». Η ευρεία αποδοχή αυτής της πρότασης οδήγησε στην ανάπτυξη της πολύ πλούσιας θεωρίας της «Επιστήμης των Υπολογιστών». Όχι πολύ αργότερα από τη δημοσίευση του Turing, κατασκευάστηκαν οι πρώτοι υπολογιστές. Αρχικά ο John von Newmann ανέπτυξε ένα απλό θεωρητικό μοντέλο για το πώς θα μπορούσε να κατασκευαστεί ένας υπολογιστής για να είναι τόσο αποτελεσματικός όσο η «παγκόσμια μηχανή του Turing». Η ανάπτυξη του hardware απογειώθηκε το 1947 όταν οι John Bardeen, Walter Bratain και Will Shockley κατασκεύασαν το transistor. Από τότε το computer hardware αναπτύχθηκε με τέτοιους ρυθμούς που έκαναν τον Gordon Moore το 1965 να διατυπώσει μια πρόταση η οποία σήμερα είναι γνωστή σαν νόμος του Moore σύμφωνα με την οποία :

«Η ισχύς των υπολογιστών θα διπλασιάζεται για σταθερό κόστος κάθε δύο χρόνια περίπου».

Και το καταπληκτικό ήταν ότι ο νόμος αυτός επαληθευόταν κατά προσέγγιση από το 1960 και μετά. Βέβαια οι ειδικοί πιστεύουν ότι αυτή η καταπληκτική αύξηση θα σταματήσει τις πρώτες δεκαετίες του 21^{ου} αιώνα που διανύουμε. Εν τω μεταξύ λόγω του όλο και μειούμενου μεγέθους των μερών του υπολογιστή, έχουν αρχίσει να γίνονται σημαντικά τα κβαντικά φαινόμενα και αλληλεπιδράσεις οι οποίες πρέπει να ληφθούν υπ’ όψιν και έτσι πρέπει να αλλάξουν και οι μέθοδοι κατασκευής. Μια πιθανή λύση σε αυτό το πρόβλημα που πιθανόν να προκαλέσει μη περεταίρω επαλήθευση του νόμου του Moore, θα μπορούσε να είναι η μετάβαση σε μια διαφορετική λογική στην κατασκευή των υπολογιστών. Μια τέτοια διέξοδος θα μπορούσε να είναι η θεωρία που είναι το αντικείμενο αυτής της εργασίας δηλαδή η κβαντική υπολογιστική, η οποία βασίζεται στην ιδέα της χρησιμοποίησης των ιδιαίτερων ιδιοτήτων ενός κβαντικού συστήματος για την κατασκευή των υπολογιστών. Λόγω της ικανότητας ενός κβαντικού συστήματος να

βρίσκεται σε κατάσταση υπέρθεσης δηλαδή κατά μια έννοια σε πολλές καταστάσεις ταυτόχρονα, έχει γίνει η υπόθεση ότι οι κβαντικοί υπολογιστές προσφέρουν ένα θεμελιώδες πλεονέκτημα στην ταχύτητα έναντι των κλασικών. Αυτό το πλεονέκτημα είναι τόσο σημαντικό ώστε πολλοί ερευνητές υποστηρίζουν ότι όση πρόοδος και να επιτευχθεί στο μέλλον στους κλασικούς υπολογιστές, θα είναι αδύνατο να καλύψουν τη διαφορά στην ισχύ τους από ένα κβαντικό υπολογιστή.

Ας αναλύσουμε τώρα λίγο περισσότερο τι εννοούμε με τον όρο «αποτελεσματική» και «μη αποτελεσματική» λειτουργία του κβαντικού και του κλασικού υπολογιστή. Πολλά από τα στοιχεία που θα χρησιμοποιηθούν για να απαντηθεί αυτό, είχαν διατυπωθεί πριν προκύψει η ιδέα για τους κβαντικούς υπολογιστές. Βασική έννοια σε αυτό το θέμα είναι το ποιοι θεωρούνται αποτελεσματικοί και ποιοι μη αποτελεσματικοί αλγόριθμοι. Έτσι αποτελεσματικός αλγόριθμος θεωρείται αυτός που οι θέσεις μνήμης που απαιτούνται για να τρέξει (και άρα ο χρόνος που απαιτείται), αυξάνονται γραμμικά (πολυωνυμικά) με το μέγεθος του προβλήματος που καλείται να λύσει. Αντίθετα μη αποτελεσματικός είναι αυτός ο αλγόριθμος που ο χρόνος που απαιτείται, αυξάνεται με συνάρτηση πιο απότομη από την πολυωνυμική πχ εκθετικά. Αυτό που παρατηρήθηκε στα τέλη της δεκαετίας του 60 και στις αρχές της δεκαετίας του 70, ήταν ότι το μοντέλο της μηχανής Turing ήταν τουλάχιστον ισάξιο και σε αποτελεσματικότητα όσο κάθε άλλο μοντέλο υπολογιστικής. Δηλαδή ένα πρόβλημα το οποίο θα μπορούσε να λυθεί αποτελεσματικά με ένα μοντέλο υπολογιστικής, θα μπορούσε επίσης να λυθεί αποτελεσματικά χρησιμοποιώντας το μοντέλο της μηχανής Turing δηλαδή θα μπορούσε να χρησιμοποιηθεί η μηχανή Turing να προσομοιώσει το άλλο μοντέλο υπολογιστικής. Αυτή η παρατήρηση διατυπώθηκε σαν μια ενισχυμένη έκδοση της θέσης Church-Turing :

«Κάθε αλγοριθμική διαδικασία μπορεί να προσομοιωθεί αποτελεσματικά χρησιμοποιώντας τη μηχανή Turing».

Αυτή η ενίσχυση είναι πολύ σημαντική διότι αναζητώντας αν ένα υπολογιστικό εγχείρημα μπορεί να πραγματοποιηθεί, μπορούμε να περιοριστούμε στη μελέτη του μοντέλου της μηχανής Turing. Μια δοκιμασία για την ενισχυμένη έκδοση της θέσης Church-Turing ήρθε από το πεδίο της αναλογικής, κλασικής υπολογιστικής. Στα χρόνια μετά τη διατύπωση της πρότασης, πολλές διαφορετικές ομάδες ερευνητών παρατήρησαν ότι ορισμένοι τύποι αναλογικών υπολογιστών μπορούν να επιλύσουν αποτελεσματικά, προβλήματα τα οποία θεωρούνταν ότι δεν μπορούσαν να λυθούν αποτελεσματικά σε μια

μηχανή Turing. Έτσι με πρώτη ματιά φαινόταν να παραβιάζεται η ενισχυμένη έκδοση της θέσης Church-Turing. Όμως τελικά δεν ήταν έτσι διότι όταν έγιναν ρεαλιστικοί υπολογισμοί και για το θόρυβο[3] που θα υπήρχε σε κάθε περίπτωση, αυτή η υπεροχή εξαφανιζόταν σε όλες τις περιπτώσεις. Αυτό το μάθημα ότι για να εκτιμηθεί η υπολογιστική αξία μιας διάταξης πρέπει να γίνουν εκτιμήσεις και για το θόρυβο, ήταν μια από τις πρώτες μεγάλες προκλήσεις που ήρθαν αντιμέτωπες οι θεωρίες της κβαντικής υπολογιστικής και της κβαντικής πληροφορίας. Την πρόκληση αυτή φαίνεται να την αντιμετώπισαν με επιτυχία με την ανάπτυξη δύο θεωριών, των «μεθόδων διόρθωσης κβαντικών λαθών» (quantum error-correcting codes) και «κβαντική υπολογιστική ανεκτική στα σφάλματα» (fault-tolerant quantum computation). Έτσι αντίθετα με την αναλογική υπολογιστική, η αντίστοιχη κβαντική μπορεί να λειτουργήσει με μια ορισμένη ποσότητα θορύβου διατηρώντας τα πλεονεκτήματά της.

Η πρώτη μεγάλη πρόκληση της ενισχυμένης εκδοχής της θέσης Church-Turing, προέκυψε στα μέσα της δεκαετίας του 70 όταν οι Robert Solovay και Volker Strassen έδειξαν ότι είναι δυνατό να διαπιστώσουν αν ένας ακέραιος αριθμός είναι πρώτος ή σύνθετος χρησιμοποιώντας ένα αλγόριθμο τυχαιοποίησης (randomize algorithm). Το σημαντικό σε αυτόν τον αλγόριθμο ήταν ότι η εξέταση για το αν ο αριθμός είναι πρώτος, χρησιμοποιούσε την τυχαιοποίηση σαν θεμελιώδες μέρος του. Δηλαδή ο αλγόριθμος δεν καθόριζε με βεβαιότητα αν ένας δεδομένος ακέραιος είναι πρώτος, αλλά καθόριζε ότι ο αριθμός είναι πιθανόν πρώτος. Επαναλαμβάνοντας όμως τον αλγόριθμο μερικές φορές, γινόταν δυνατό να προσδιοριστεί σχεδόν με βεβαιότητα αν ο αριθμός τελικά ήταν πρώτος. Η μέθοδος αυτή θεωρήθηκε εξαιρετικής σημασίας διότι την εποχή που προτάθηκε, δεν υπήρχε καμία αιτιοκρατική (ντετερμινιστική) μέθοδος για να διαπιστωθεί αν ένας αριθμός είναι πρώτος και ούτε μέχρι σήμερα υπάρχει. Έτσι φάνηκε ότι υπολογιστές με δυνατότητα να λειτουργούν με αλγόριθμους τυχαιοποίησης, ήταν ικανοί να αντιμετωπίσουν αποτελεσματικά προβλήματα που δεν ήταν ικανή να αντιμετωπίσει μια συμβατική μηχανή Turing. Αυτή η πρόκληση αντιμετωπίστηκε με τη διατύπωση αρχικά και τον έλεγχο αργότερα μιας λίγο τροποποιημένης μορφής της ενισχυμένης εκδοχής της θέσης Church-Turing η οποία είναι η εξής :

[3] Στην επιστήμη της πληροφορικής *θόρυβος* ονομάζεται η ανεπιθύμητη παραμόρφωση σε σύνολα δεδομένων, είτε συστηματικές είτε εντελώς τυχαίου χαρακτήρα. Εφόσον κατά κανόνα τα δεδομένα εκφράζονται ως αλληλουχίες αριθμών, ο θόρυβος δεν είναι παρά αριθμητικές τιμές οι οποίες προσθαφαιρούνται στα δεδομένα.

«Κάθε αλγοριθμική διαδικασία μπορεί να προσομοιωθεί αποτελεσματικά χρησιμοποιώντας μια πιθανολογική (probabilistic) μηχανή Turing».

Αυτή όμως η τροποποίηση που έγινε αποκλειστικά για να δώσει εξήγηση στο συγκεκριμένο πρόβλημα, προκαλεί φυσιολογικά και το ερώτημα κατά πόσο στο μέλλον θα μπορούσε να βρεθεί κάποια άλλη υπολογιστική μέθοδος η οποία θα μπορούσε να λύσει προβλήματα στα οποία δεν μπορούσε να δώσει λύση η μέθοδος Turing. Και αμέσως έπεται το ερώτημα κατά πόσο θα μπορούσε να βρεθεί κάποια υπολογιστική μέθοδος η οποία να εγγυάται την αποτελεσματική προσομοίωση κάθε άλλης υπολογιστικής μεθόδου. Παρακινούμενος απ' αυτήν την ερώτηση ο David Deutsch αναρωτήθηκε κατά πόσο οι νόμοι της Φυσικής θα μπορούσαν να χρησιμοποιηθούν στην εξαγωγή μιας ακόμα ισχυρότερης έκδοσης της θέσης των Church-Turing. Έτσι αντί να υιοθετήσει μια εξ επί τούτου υπόθεση, ο Deutsch αναζήτησε στις φυσικές θεωρίες μια θεμελίωση της θέσης Church-Turing και έτσι τότε αυτή θα ήταν τόσο ασφαλής όσο η ισχύς αυτής της φυσικής θεωρίας. Συγκεκριμένα ο Deutsch προσπάθησε να ορίσει μια υπολογιστική διαδικασία η οποία να είναι ικανή να προσομοιώσει αποτελεσματικά ένα οποιοδήποτε φυσικό σύστημα. Και επειδή οι νόμοι της φύσης είναι θεμελιωδώς κβαντικοί, ο Deutsch οδηγήθηκε φυσιολογικά να εξετάσει υπολογιστικές διαδικασίες οι οποίες να βασίζονται στις αρχές της κβαντικής μηχανικής. Αυτές οι διαδικασίες είναι τα κβαντικά ανάλογα των μηχανών που είχε προτείνει περίπου 50 χρόνια πριν ο Turing και οδήγησαν στην μοντέρνα εκδοχή των κβαντικών υπολογιστών. Μέχρι σήμερα δεν έχει ξεκαθαρίσει κατά πόσο οι ιδέες αυτές του Deutsch για τον «παγκόσμιο κβαντικό υπολογιστή» είναι επαρκείς για να προσομοιώσουν αποτελεσματικά ένα οποιοδήποτε φυσικό σύστημα. Το αν θα γίνει αποδεκτή ή θα απορριφθεί αυτή η υπόθεση, είναι ένα από τα μεγάλα ανοικτά θέματα στο πεδίο της κβαντικής υπολογιστικής και της κβαντικής πληροφορίας. Είναι πιθανόν για παράδειγμα, ότι χρησιμοποιώντας κάποιες αρχές της κβαντικής θεωρίας πεδίου ή της θεωρίας των χορδών ή ακόμα και της κβαντικής θεωρίας της βαρύτητας να οδηγηθούμε πέρα από τον παγκόσμιο κβαντικό υπολογιστή του Deutsch και να αποκτήσουμε μια ακόμα ισχυρότερη υπολογιστική μέθοδο. Αυτό που ενεργοποίησε η θεωρία του Deutsch ήταν μια πρόκληση για την πρόταση των Church-Turing. Ο Deutsch αναρωτήθηκε κατά πόσο είναι δυνατόν για ένα κβαντικό υπολογιστή, να λύσει αποτελεσματικά υπολογιστικά προβλήματα τα οποία δεν μπορεί να λύσει ένας κλασικός υπολογιστής ακόμα και μια πιθανολογική μηχανή Turing. Έτσι επινόησε ένα παράδειγμα το οποίο έδειξε ότι πράγματι

οι κβαντικοί υπολογιστές έχουν μεγαλύτερη ισχύ από τους κλασικούς (αλγόριθμος του Deutsch, ενότητα 5.3). Αυτό το αξιοσημείωτο πρώτο βήμα βελτιώθηκε την επόμενη δεκαετία από πολλούς ερευνητές με αποκορύφωμα τον Peter Shor το 1994 που ισχυρίστηκε ότι δύο πολύ σημαντικά μαθηματικά προβλήματα, το πρόβλημα της εύρεσης των πρώτων διαιρετών ενός ακεραίου και το πρόβλημα του διακριτού λογαρίθμου, θα μπορούσαν να λυθούν αποτελεσματικά σε ένα κβαντικό υπολογιστή. Αυτό προκάλεσε μεγάλο ενδιαφέρον, διότι αυτά τα δύο προβλήματα θεωρούνταν και ακόμα θεωρούνται ότι δεν έχουν αξιόπιστη λύση σε ένα κλασικό υπολογιστή. Η εργασία του Shor ήταν μια ισχυρή ένδειξη ότι οι κβαντικοί υπολογιστές είναι πιο ισχυροί από τις μηχανές Turing ακόμα και από τις πιθανοκρατικές μηχανές Turing. Άλλη μια ένδειξη για την ισχύ των κβαντικών υπολογιστών, ήρθε το 1995 όταν ο Lov Grover παρουσίασε έναν αλγόριθμο με βάση τον οποίο ένα άλλο σημαντικό πρόβλημα, το να βρεθεί ο σωστός αριθμός από μια μεγάλη βάση δεδομένων, μπορούσε να λυθεί πολύ πιο γρήγορα από έναν κλασικό υπολογιστή (παράγραφος 5.5.3). Την ίδια εποχή περίπου που παρουσιάστηκαν οι αλγόριθμοι του Shor και Grover, πολλοί ερευνητές επεξεργάζονταν μια ιδέα του Richard Feynman που είχε διατυπώσει το 1982. Ο Feynman είχε επισημάνει ότι υπάρχουν θεμελιώδεις δυσκολίες στην προσομοίωση κβαντικών συστημάτων από κλασικούς υπολογιστές και πρότεινε ότι αν κατασκευάζονταν υπολογιστές με βάση τις αρχές της κβαντικής μηχανικής, τότε μόνο θα μπορούσαμε να αποφύγουμε αυτές τις δυσκολίες. Έτσι στη δεκαετία του 90 διάφορες ομάδες από ερευνητές άρχισαν να προσπαθούν να κάνουν πράξη αυτή την ιδέα και έδειξαν ότι είναι πράγματι δυνατό να χρησιμοποιηθούν οι κβαντικοί υπολογιστές για την αποτελεσματική προσομοίωση συστημάτων που δεν έχουν αποτελεσματική προσομοίωση σε κλασικούς υπολογιστές. Είναι πιθανό ότι μια από τις βασικότερες εφαρμογές των κβαντικών υπολογιστών στο μέλλον, θα είναι να επιτυγχάνουν προσομοιώσεις κβαντικών συστημάτων τα οποία είναι πολύ δύσκολο να προσομοιωθούν από κλασικούς υπολογιστές κάτι το οποίο θα είχε βαθιές επιστημονικές και τεχνολογικές εφαρμογές. Στο ερώτημα τώρα τι άλλα προβλήματα μπορούν να λύσουν οι κβαντικοί υπολογιστές πιο γρήγορα και αποτελεσματικά από τους κλασικούς, η απάντηση είναι ότι, αυτό είναι άγνωστο. Μια απαισιόδοξη εξήγηση θα μπορούσε να είναι ότι αυτό συμβαίνει διότι απλά δεν υπάρχουν. Η εφεύρεση καινούργιων καλών κβαντικών αλγορίθμων φαίνεται να είναι δύσκολη υπόθεση. Υπάρχει όμως και άλλη μια οπτική γωνία. Αυτή είναι ότι οι αλγόριθμοι που θα χρησιμοποιηθούν σε κβαντικούς υπολογιστές είναι δύσκολο να εφευρεθούν διότι οι σχεδιαστές τους έρχονται αντιμέτωποι με δύο

μεγάλα προβλήματα που δεν αντιμετωπίζουν οι συνάδερφοι τους που ασχολούνται με τους κλασικούς αλγορίθμους. Πρώτον, η ανθρώπινη διαίσθηση είναι προσαρμοσμένη σε ένα κλασικό κόσμο. Έτσι αν κάποιος χρησιμοποιεί τη διαίσθηση σαν εργαλείο κατά την κατασκευή αλγορίθμων, τότε οι ιδέες που θα προκύπτουν θα είναι κλασικές. Άρα για να κατασκευάσει κανείς καλούς κβαντικούς αλγόριθμους θα πρέπει πρώτα να «απενεργοποιήσει» την κλασική του διαίσθηση τουλάχιστον στο κομμάτι της διαδικασίας της κατασκευής που χρησιμοποιεί κβαντικά φαινόμενα για την επίτευξη του στόχου. Δεύτερον για να αξίζει τον κόπο, δεν είναι αρκετό να κατασκευαστεί ένας αλγόριθμος που να είναι απλώς κβαντικός, αλλά θα πρέπει να είναι πολύ καλύτερος από κάθε υπάρχον αντίστοιχο κλασικό, αλλιώς δεν θα έχει μεγάλο ενδιαφέρον για να εφαρμοστεί. Ίσως το πιο συναρπαστικό γεγονός στη μελέτη των κβαντικών υπολογιστών, είναι το πόσα λίγα ξέρουμε για τις απαντήσεις αυτών των ερωτημάτων και η μεγάλη πρόκληση για το μέλλον είναι να κατανοήσουμε αυτά τα ερωτήματα καλύτερα.

2. Qubits

Όπως είναι γνωστό, η θεμελιώδης μονάδα ενός κλασικού υπολογιστή είναι το bit. Το αντίστοιχο του bit σε ένα κβαντικό υπολογιστή είναι το quantum bit ή απλά qubit. Σε αυτό το κεφάλαιο θα αναφερθούν οι βασικές ιδιότητες ενός qubit αλλά και μιας ομάδας από περισσότερα και θα γίνει σύγκριση με τις αντίστοιχες κλασικές περιπτώσεις.

2.1 Το Qubit

Κατ' αρχήν πρέπει να τονιστεί ότι το qubit θα εξεταστεί σαν ένα μαθηματικό αντικείμενο με ανάλογες ιδιότητες τέτοιου τύπου. Έτσι μπορεί κάποιος να αναρωτηθεί κατά πόσο ένα qubit είναι μια πραγματική και πραγματοποιήσιμη φυσική οντότητα όπως είναι και το κλασικό bit και όπως απαιτείται για τη δημιουργία ενός πραγματικού κβαντικού υπολογιστή. Η απάντηση είναι ότι όντως τα qubit είναι πραγματικές φυσικές οντότητες όπως θα φανεί και στη συνέχεια, η αυστηρή όμως μαθηματική περιγραφή τους, μας δίνει την ελευθερία για μια γενική θεωρία της κβαντικής υπολογιστικής και πληροφορίας η οποία δεν εξαρτάται από το ποιο ακριβώς σύστημα κάθε φορά παίζει το ρόλο του qubit.

Τι είναι επομένως το qubit; Είναι ένα σύστημα το οποίο όπως και το κλασικό ανάλογο του (το bit), μπορεί να βρεθεί σε δύο καταστάσεις που ονομάζονται 0 και 1. Απαιτείται επομένως μια ιδιότητα ενός κβαντικού συστήματος η οποία να μπορεί να πάρει μόνο δύο τιμές όπως η προβολή του spin του ηλεκτρονίου για το όποιο ο κβαντικός αριθμός του spin είναι $s = 1/2$ και ο κβαντικός αριθμός της προβολής του spin στον άξονα z είναι $m_s = \pm 1/2$. Αν χρησιμοποιήσουμε το φορμαλισμό του Paul Dirac, οι καταστάσεις του συστήματος περιγράφονται από ένα αφηρημένο διάνυσμα κατάστασης $|\psi\rangle$ ενός διανυσματικού χώρου Hilbert που στην περίπτωση του spin είναι δύο διαστάσεων, με διανύσματα βάσης τα $|m_s = 1/2\rangle$ και $|m_s = -1/2\rangle$ τα οποία στην αναπαράσταση θέσης είναι οι γνωστές κυματοσυναρτήσεις. Στο qubit οι καταστάσεις αυτές συνήθως συμβολίζονται αντίστοιχα $|0\rangle$ και $|1\rangle$. Η μεγάλη διαφορά σε σχέση με το κλασικό bit είναι ότι ενώ αυτό μπορεί να βρεθεί μόνο σε μια απ' τις δύο καταστάσεις 0 ή 1, το qubit μπορεί

να βρεθεί και σε οποιαδήποτε κατάσταση επαλληλίας της μορφής $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ όπου τα α και β είναι μιγαδικοί αριθμοί. Για καλύτερη κατανόηση, θα μπορούσαμε να θεωρήσουμε ότι η κατάσταση $|\psi\rangle$ του qubit είναι ένα διάνυσμα σε ένα μιγαδικό διανυσματικό χώρο δύο διαστάσεων. Τότε τα διανύσματα $|0\rangle$ και $|1\rangle$ θα ήταν τα ορθοκανονικά διανύσματα βάσης. Άλλη μια θεμελιώδης διαφορά ανάμεσα σε ένα bit και ένα qubit είναι η εξής : μπορούμε εύκολα να εξετάσουμε ένα bit και να προσδιορίσουμε αν αυτό βρίσκεται στην κατάσταση 0 ή 1. Αυτό εξάλλου το κάνουν συνεχώς οι κλασικοί υπολογιστές όταν πχ επαναφέρουν τα περιεχόμενα της μνήμης τους. Με το qubit όμως τα πράγματα δεν είναι τόσο απλά. Κι αυτό γιατί δεν μπορούμε να το εξετάσουμε και να προσδιορίσουμε την κβαντική κατάσταση του, δηλαδή τους αριθμούς α και β. Αντίθετα όπως είναι γνωστό από ένα απ' τα αξιώματα της κβαντικής μηχανικής, μπορούμε να αποκτήσουμε περιορισμένη μόνο πληροφορία από την κβαντική κατάσταση αφού αν μετρήσουμε το qubit θα βρούμε είτε το αποτέλεσμα 0 με πιθανότητα $|\alpha|^2$ είτε το αποτέλεσμα 1 με πιθανότητα $|\beta|^2$, φυσικά με $|\alpha|^2+|\beta|^2=1$. Επίσης η μέτρηση καταστρέφει την κβαντική κατάσταση που βρισκόταν το qubit πριν απ' αυτήν και αυτό μεταπίπτει σε μια ιδιοκατάσταση με ιδιοτιμή αυτή που μετρήθηκε. Δηλαδή όχι μόνο δε βρίσκουμε σε ποια κατάσταση ήταν το qubit αλλά καταστρέφουμε και αυτήν την κατάσταση. Υπάρχει λοιπόν μια διαφορά ανάμεσα στη μη μετρημένη κατάσταση ενός qubit και στην πληροφορία που μπορούμε να αποκομίσουμε γι' αυτήν από την μέτρησή της, η οποία περιπλέκει την κατάσταση. Στα περισσότερα μοντέλα απεικόνισης της φύσης, υπάρχει μια αντιστοιχία ανάμεσα στοιχεία της απεικόνισης και στα μέρη του πραγματικού κόσμου. Άρα εδώ που δεν υπάρχει αυτό, είναι δύσκολο να διαισθανθεί κάποιος τη συμπεριφορά των κβαντικών συστημάτων. Έτσι θα πρέπει να αναζητηθεί μια έμμεση αντιστοιχία ανάμεσα στην κβαντική κατάσταση των qubits και στα αποτελέσματα των μετρήσεων. Να μετασχηματιστούν δηλαδή κατάλληλα αυτές τις καταστάσεις, ώστε τα αποτελέσματα των μετρήσεων να εξαρτώνται από τις διαφορετικές ιδιότητες τους. Τότε μόνο οι κβαντικές καταστάσεις θα έχουν πραγματικές και πειραματικά επαληθεύσιμες συνέπειες οι οποίες είναι προφανώς θεμελιώδεις για την κβαντική υπολογιστική.

Θα πρέπει σε αυτό το σημείο να τονιστεί η σημασία της βάσης στην οποία θα μετρηθεί μια κβαντική κατάσταση $|\psi\rangle$. Αυτό θα γίνει σαφές με το παράδειγμα που ακολουθεί :

Έστω ένα qubit το οποίο βρίσκεται στην κατάσταση :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \textbf{(2-1)}$$

δηλαδή η κατάσταση $|\psi\rangle$ έχει εκφραστεί ως γραμμικός συνδυασμός των διανυσμάτων βάσης $|0\rangle$ και $|1\rangle$. Όπως προαναφέρθηκε, μέτρηση αυτής της κατάστασης θα δώσει αποτέλεσμα 0 με πιθανότητα $|\alpha|^2$ ή 1 με πιθανότητα $|\beta|^2$. Πρέπει να τονιστεί όμως ότι για να ισχύει αυτό θα πρέπει η μέτρηση να γίνει με τρόπο που μπορεί να ανιχνεύσει τις καταστάσεις 0 και 1 ή όπως λέμε πρέπει η μέτρηση να γίνει στη «διεύθυνση» των βασικών διανυσμάτων $|0\rangle$ και $|1\rangle$. Αυτό είναι όμως μια από τις (θεωρητικά τουλάχιστον) πολλές επιλογές. Δηλαδή θα μπορούσε, όπως επιλέχθηκε η βάση $\{|0\rangle, |1\rangle\}$, να επιλεγεί μια άλλη βάση του δισδιάστατου διανυσματικού χώρου των καταστάσεων. Θα μπορούσε πχ να επιλεγεί η βάση $\{|+\rangle, |-\rangle\}$, όπου :

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \; |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \textbf{(2-2)}$$

Τότε η κατάσταση $|\psi\rangle$ θα μπορούσε να γραφεί ως γραμμικός συνδυασμός των διανυσμάτων $|+\rangle$ και $|-\rangle$. Πράγματι προσθέτοντας και αφαιρώντας τις σχέσεις (2.2) έχουμε :

$$|+\rangle + |-\rangle = \sqrt{2}|0\rangle, \quad |+\rangle - |-\rangle = \sqrt{2}|1\rangle \quad \textbf{(2-3)}$$

Έτσι έχουμε :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle \quad \textbf{(2-4)}$$

Έτσι από τη σχέση (2-4) προκύπτει ότι αν κάνουμε μέτρηση στη διεύθυνση των διανυσμάτων $|+\rangle$ και $|-\rangle$, θα προκύψει το αποτέλεσμα + με πιθανότητα $\frac{|\alpha+\beta|^2}{2}$ ή – με πιθανότητα $\frac{|\alpha-\beta|^2}{2}$. Για να γίνει πιο ξεκάθαρο το θέμα, ας υποθέσουμε ότι η κατάσταση $|\psi\rangle$ είναι ιδιοκατάσταση στη βάση $\{|0\rangle, |1\rangle\}$, πχ έστω ότι στη σχέση (2-1) είναι α=1 και β=0 οπότε η κατάσταση είναι η $|\psi\rangle = |0\rangle$. Τότε η μέτρηση προφανώς στη «διεύθυνση»

των διανυσμάτων $|0\rangle$ και $|1\rangle$, θα έδινε αποτέλεσμα 0 με πιθανότητα 100%. Η σχέση (2-4) για α=1 και β=0 γίνεται :

$$|\psi\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle \quad \textbf{(2-5)}$$

δηλαδή η κατάσταση $|\psi\rangle$ που είναι ιδιοκατάσταση στη βάση $\{|0\rangle,|1\rangle\}$, είναι κατάσταση επαλληλίας στη βάση $\{|+\rangle,|-\rangle\}$! Αυτό σημαίνει ότι η μέτρηση στη «διεύθυνση» των διανυσμάτων $|+\rangle$ και $|-\rangle$ θα έδινε αποτέλεσμα + με πιθανότητα $\left|\frac{1}{\sqrt{2}}\right|^2 = 50\%$ ή αποτέλεσμα – με πιθανότητα $\left|\frac{1}{\sqrt{2}}\right|^2 = 50\%$.

Παρόλη την ιδιομορφία τους, τα qubits είναι πραγματικά φυσικά συστήματα και η ύπαρξη και συμπεριφορά τους έχει διαπιστωθεί από διάφορα πειράματα (με πιο διάσημο ίσως αυτό των Stern-Gerlach) και έτσι αρκετά φυσικά συστήματα μπορούν να χρησιμοποιηθούν σαν qubits. Για παράδειγμα qubit θα μπορούσε να θεωρηθεί ένα φωτόνιο λόγω των δύο διαφορετικών καταστάσεων πόλωσης του. Επίσης qubit θα μπορούσε να θεωρηθεί ένα ηλεκτρόνιο λόγω των δύο διαφορετικών προσανατολισμών του spin του. Τέλος qubit θα μπορούσε να θεωρηθεί ένα άτομο ή ένα ιόν, το οποίο μπορεί να βρεθεί στη θεμελιώδη του κατάσταση ή απορροφώντας το κατάλληλο ποσό ενέργειας στην πρώτη διεγερμένη ή το πιο ενδιαφέρον σε μια επαλληλία αυτών των καταστάσεων.

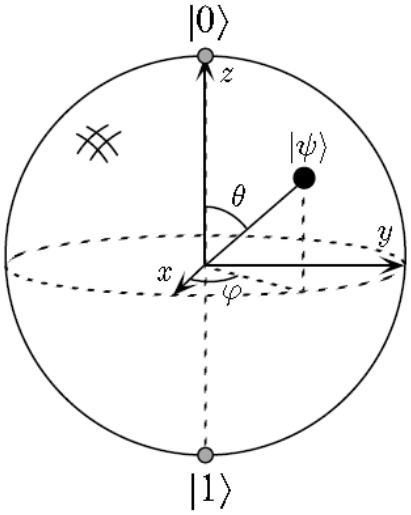
Όπως έγινε κατανοητό μέχρι τώρα, υπάρχει μια δυσκολία στην κατανόηση της φύσης της κατάστασης ενός qubit ειδικά αν αυτή είναι επαλληλία βασικών καταστάσεων. Έτσι έχει επινοηθεί μια πολύ χρήσιμη εικόνα η οποία είναι γεωμετρική αναπαράσταση και βοηθά προς αυτή την κατεύθυνση. Επειδή είναι $|\alpha|^2+|\beta|^2=1$, η σχέση $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ μπορεί να γραφεί στη μορφή :

$$|\boldsymbol{\psi}\rangle = \boldsymbol{e^{i\gamma}}\left(\boldsymbol{\cos\frac{\theta}{2}}|\mathbf{0}\rangle + \boldsymbol{e^{i\varphi}}\,\boldsymbol{\sin\frac{\theta}{2}}|\mathbf{1}\rangle\right) \quad \textbf{(2-6)}$$

όπου θ, φ και γ είναι πραγματικοί αριθμοί. Τον όρο όμως $e^{i\gamma}$ μπορούμε να τον αγνοήσουμε διότι δεν έχει παρατηρήσιμες συνέπειες και έτσι μπορούμε να γράψουμε τη σχέση στην απλούστερη μορφή (Nielsen & Chuang σελ. 15) :

$$|\boldsymbol{\psi}\rangle = \boldsymbol{\cos\frac{\theta}{2}}|\mathbf{0}\rangle + \boldsymbol{e^{i\varphi}}\,\boldsymbol{\sin\frac{\theta}{2}}|\mathbf{1}\rangle \quad \textbf{(2-7)}$$

Έτσι τώρα είναι φανερό ότι οι αριθμοί θ και φ ορίζουν ένα σημείο πάνω στην επιφάνεια μιας τρισδιάστατης σφαίρας και άρα η κατάσταση $|\psi\rangle$ μπορεί να θεωρηθεί σαν ένα διάνυσμα με αρχή το κέντρο της σφαίρας και τέλος ένα σημείο της σφαίρας αυτής όπως φαίνεται στο Σχήμα 2-1.



Σχήμα 2-1 : η αναπαράσταση ενός qubit μέσω της σφαίρας Bloch (Nielsen & Chuang σελ.15)

Η σφαίρα αυτή ονομάζεται σφαίρα Bloch και μας παρέχει μια πολύ χρήσιμη πολλές φορές εικονογράφηση της κατάστασης ενός απλού qubit. Πολλοί τελεστές οι οποίοι δρουν πάνω σε ένα απλό qubit περιγράφονται και κατανοούνται πολύ ικανοποιητικά με τη βοήθεια της σφαίρας Bloch. Πρέπει όμως να αναφερθεί ότι αυτό το διαισθητικό πλεονέκτημα που προσφέρει η σφαίρα Bloch είναι σχετικά περιορισμένο αφού δεν υπάρχει απλή γενίκευση της στην περίπτωση των δύο ή περισσοτέρων qubits.

Ένα καίριο ερώτημα είναι το πόση πληροφορία περιέχεται στα qubits. Είναι εντυπωσιακό ότι αφού υπάρχουν άπειρα σημεία στην επιφάνεια της σφαίρας Bloch, στα qubits περιέχεται τεράστιο ποσό πληροφορίας. Όμως αυτό το πλεονέκτημα μετριάζεται απ' το γεγονός ότι όπως προαναφέρθηκε και είναι γνωστό από τη βασική κβαντική μηχανική, αυτή η πληροφορία χάνεται κατά τη μέτρηση. Να θυμηθούμε ότι κατά τη μέτρηση ενός qubit θα βρούμε είτε 0 είτε 1, ενώ η κατάσταση του qubit απομακρύνεται απ' την επαλληλία και μεταπίπτει σε εκείνη τη βασική κατάσταση η οποία είναι συνεπής με το αποτέλεσμα της μέτρησης. Το γιατί γίνεται αυτό κανείς δεν γνωρίζει. Αυτό είναι εξάλλου ένα απ' τα αξιώματα της κβαντικής μηχανικής. Έτσι τελικά απ' το τεράστιο ποσό

πληροφορίας που περιέχεται σε ένα qubit, κάποιος μπορεί να επωφεληθεί μόνο ένα μικρό ποσό μέσω της μέτρησης. Άρα θα μπορούσε να αναρωτηθεί κανείς «Τι χρησιμεύει η τεράστια πληροφορία των qubits αφού δεν μπορούμε να την αξιοποιήσουμε;». Το μέλλον θα δείξει κατά πόσο μπορεί να ξεπεραστεί αυτή η δυσκολία όμως υπάρχει η άποψη ότι παρόλο που δεν μπορούμε να διαβάσουμε όλη την πληροφορία, αυτή εξακολουθεί να υπάρχει μέσα στα qubits κρυμμένη. Έστω και έτσι, οι διάφοροι υπολογισμοί μπορούν να γίνουν με πολύ μεγάλες ταχύτητες και τα αποτελέσματα αυτών μπορούμε να τα πάρουμε μετρώντας τελικά μόνο την κατάσταση ενός ή έστω λίγων qubits.

2.2 Σύστημα πολλών qubits

Πάμε τώρα στην περίπτωση που έχουμε περισσότερα qubits όπου εκεί φαίνεται και η (πιθανή) δύναμη της κβαντικής υπολογιστικής. Ας πάρουμε κατ' αρχήν την περίπτωση των δύο qubits. Αν ήταν κλασικά bits θα μπορούσαμε να έχουμε τέσσερεις διαφορετικές καταστάσεις τις 00, 01, 10, 11. Έτσι για το σύστημα των δύο qubits σε αντιστοιχία με την περίπτωση του ενός qubit, θα έχουμε τέσσερεις βασικές καταστάσεις τις $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ και έτσι η κατάσταση του συστήματος θα είναι γενικά η :

$$|\boldsymbol{\psi}\rangle=\alpha_{00}|\mathbf{00}\rangle + \alpha_{01}|\mathbf{01}\rangle + \alpha_{10}|\mathbf{10}\rangle + \alpha_{11}|\mathbf{11}\rangle \quad \textbf{(2-8)}$$

δηλαδή επαλληλία των τεσσάρων βασικών καταστάσεων όπου οι συντελεστές α_{ij} (i,j=0,1) είναι μιγαδικοί αριθμοί οι οποίοι συχνά ονομάζονται και πλάτη των αντίστοιχων βασικών καταστάσεων. Όπως και στην περίπτωση του ενός qubit, η μέτρηση θα έχει ως αποτέλεσμα ένα από τα 00, 01, 10, 11 με πιθανότητα $|\alpha_{ij}|^2$ και στη συνέχεια η κατάσταση του συστήματος να μεταπίπτει στην $|ij\rangle$. Βεβαίως πρέπει να ισχύει και η σχέση κανονικοποίησης $\sum|\alpha_{ij}|^2 = 1$. Αν τώρα μετρηθεί η κατάσταση μόνο του ενός απ' τα δύο qubits έστω του πρώτου, τότε ή το αποτέλεσμα θα είναι 0 με πιθανότητα $|\alpha_{00}|^2+|\alpha_{01}|^2$ ή θα είναι 1 με πιθανότητα $|\alpha_{10}|^2+|\alpha_{11}|^2$. Αν το αποτέλεσμα της μέτρησης είναι 0 τότε η κατάσταση του συστήματος θα μεταπέσει στην κατάσταση :

$$|\boldsymbol{\psi}'\rangle = \frac{\boldsymbol{\alpha_{00}}|\mathbf{00}\rangle+\boldsymbol{\alpha_{01}}|\mathbf{01}\rangle}{\sqrt{|\boldsymbol{\alpha_{00}}|^2+|\boldsymbol{\alpha_{01}}|^2}} \quad \textbf{(2-9)}$$

όπου προφανώς ο παρονομαστής εισήχθη για λόγους κανονικοποίησης. Το αποτέλεσμα αυτό προέκυψε, αφού θα «επιβιώσουν» μόνο οι βασικές καταστάσεις οι οποίες δίνουν αποτέλεσμα μέτρησης του πρώτου qubit το 0.

Μια πολύ σπουδαία κατάσταση αυτού του τύπου είναι η περίφημη κατάσταση Bell ή ζεύγος EPR που είναι η :

$$|\psi\rangle = \frac{|00\rangle+|01\rangle}{\sqrt{2}} \quad \textbf{(2-10)}$$

Αυτή η φαινομενικά «αθώα» κατάσταση είναι υπεύθυνη για πολλές διενέξεις στην κβαντική μηχανική, για πολλές εντυπωσιακές και μη αναμενόμενες συνέπειες όπως η τηλεμεταφορά και για τις μεγάλες προσδοκίες για εντυπωσιακά αποτελέσματα στην κβαντική πληροφορία και υπολογιστική. Η ιδιότητα κλειδί της κατάστασης Bell είναι ότι η μέτρηση του ενός απ' τα δύο qubits καθορίζει το αποτέλεσμα της μέτρησης στο άλλο. Πράγματι, αν κάποιος μετρήσει την κατάσταση του πρώτου qubit ή θα μετρήσει 0 με πιθανότητα 50% και η κατάσταση θα μεταπέσει στην $|00\rangle$ ή θα μετρήσει 1 με πιθανότητα πάλι 50% και η κατάσταση θα μεταπέσει στην $|11\rangle$. Έτσι τελικά αν γίνει μέτρηση και στο δεύτερο qubit, το αποτέλεσμα θα είναι 0 στην πρώτη περίπτωση και 1 στη δεύτερη. Δηλαδή η μέτρηση στο δεύτερο qubit θα δώσει σίγουρα το ίδιο αποτέλεσμα με αυτό της πρώτης. Έτσι τα αποτελέσματα είναι συσχετισμένα. Παρόμοιες συσχετίσεις μπορούν να προκύψουν αν πρώτα επηρεάσουμε την κατάσταση του ενός απ' τα δύο qubits και μετά κάνουμε τις μετρήσεις. Αυτού του τύπου οι συσχετισμοί, ήταν το αντικείμενο μεγάλου ενδιαφέροντος από τότε που έγινε μια διάσημη δημοσίευση από τους Einstein, Podolsky και Rosen (EPR), στην οποία φάνηκαν για πρώτη φορά οι περίεργες ιδιότητες της κατάστασης Bell. Το πνεύμα αυτής της δημοσίευσης πήρε και βελτίωσε εξαιρετικά ο John Bell, ο οποίος απέδειξε μια εξαιρετικής σημασίας πρόταση ότι :

«Οι συσχετίσεις στις μετρήσεις σε μια κατάσταση Bell είναι ισχυρότερες από αυτές που θα μπορούσαν να υπάρξουν μεταξύ κλασικών συστημάτων».

Αυτή η πρόταση ήταν ο πρώτος υπαινιγμός ότι η θεωρία της πληροφορίας που θα μπορούσε να αναπτυχθεί στηριζόμενη στην κβαντική μηχανική μπορεί να οδηγήσει πιο μακριά απ' όσο θα μπορούσε να οδηγήσει η κλασική μέθοδος.

Αν γενικεύσουμε τώρα στην περίπτωση των n qubits, η βασική κατάσταση αυτού του συστήματος θα είναι της μορφής $|x_1 x_2 \ldots\ldots x_n\rangle$ και έτσι η κβαντική κατάσταση ενός

τέτοιου συστήματος θα καθοριζόταν από 2^n πλάτη. Να θυμηθούμε ότι για δύο qubits είδαμε ότι χρειάζονταν $4=2^2$ πλάτη. Άρα αν n=500 τότε ο αριθμός των πλατών θα ήταν μεγαλύτερος από τον εκτιμώμενο αριθμό ατόμων που υπάρχουν σε όλο το σύμπαν! Προφανώς θα ήταν αδύνατο να αποθηκευτεί ένα τέτοιο ποσό πληροφορίας σε έναν κλασικό υπολογιστή όσο εξελιγμένος και αν ήταν. Συμπεραίνουμε επομένως ότι η φύση μπορεί να διαχειρίζεται τεράστιες ποσότητες δεδομένων ακόμα και για ένα σύστημα που περιέχει μόνο μερικές εκατοντάδες ατόμων. Το στοίχημα για το μέλλον λοιπόν είναι αν αυτό το τεράστιο δυναμικό υπολογιστικής ισχύος θα μπορούσε να καταστεί εκμεταλλεύσιμο.

3. Κβαντικές Πύλες

Οι μεταβολές που συμβαίνουν σε μια κβαντική κατάσταση μπορούν να περιγραφούν χρησιμοποιώντας τη γλώσσα της κβαντικής υπολογιστικής (quantum computation). Όπως ένας κλασικός υπολογιστής οικοδομείται από ένα ηλεκτρικό κύκλωμα το οποίο αποτελείται από καλώδια και λογικές πύλες, έτσι και ένας κβαντικός υπολογιστής θα οικοδομείται από ένα κβαντικό κύκλωμα το οποίο θα αποτελείται από καλώδια και μερικές βασικές κβαντικές πύλες οι οποίες θα μεταφέρουν και θα επεξεργάζονται την κβαντική πληροφορία. Σε αυτή την παράγραφο θα περιγράψουμε μερικές απλές κβαντικές πύλες που δρουν σε ένα και μια που δρα σε δύο qubits.

3.1 Απλές Κβαντικές Πύλες

Όπως αναφέρθηκε, οι κλασικοί υπολογιστές αποτελούνται από καλώδια και λογικές πύλες. Τα καλώδια χρησιμοποιούνται για να μεταφέρουν την πληροφορία στα διάφορα μέρη του κυκλώματος ενώ οι λογικές πύλες διαχειρίζονται την πληροφορία μετατρέποντας την από μια μορφή σε άλλη. Ας ξεκινήσουμε από τις λογικές πύλες που δρουν σε ένα μόνο κλασικό bit. Η μόνη μη τετριμμένη πύλη αυτής της κατηγορίας είναι η πύλη NOT η δράση της οποίας περιγράφεται από τον πίνακα αληθείας της που είναι :

$$0 \rightarrow 1 \ , \ 1 \rightarrow 0$$

Δηλαδή η δράση αυτής της πύλης αντιστρέφει την κατάσταση του bit. Το ερώτημα είναι αν υπάρχει μια ανάλογη κβαντική πύλη με την κλασική πύλη NOT. Προφανώς η πρώτη σκέψη θα ήταν αυτή η πύλη να έκανε τις αλλαγές $|0\rangle \rightarrow |1\rangle$ και $|1\rangle \rightarrow |0\rangle$. Όμως η κβαντική κατάσταση ενός qubit δεν μπορεί να είναι μόνο η $|0\rangle$ ή η $|1\rangle$ αλλά και κάθε κατάσταση επαλληλίας τους $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ άρα δεν μπορεί να υπάρχει πλήρης αντιστοιχία με την κλασική περίπτωση. Η κβαντική πύλη NOT τελικά ορίστηκε έτσι ώστε όταν δρα σε μια κβαντική κατάσταση, να εναλλάσσει τους ρόλους των $|0\rangle$ και $|1\rangle$ δηλαδή να έχει τη δράση :

$$\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle \rightarrow \alpha|\mathbf{1}\rangle + \beta|\mathbf{0}\rangle \quad \textbf{(3-1)}$$

Ένας βολικός τρόπος να αναπαραστήσει κανείς μια κβαντική πύλη όπως θα φανεί και στη συνέχεια, είναι η αναπαράσταση με τετραγωνικό πίνακα (μήτρα) κατάλληλης κάθε φορά διάστασης. Κατ' αρχήν ξεκινάμε απ' το συμβολισμό της κβαντικής κατάστασης με τη μορφή πίνακα. Έτσι η κατάσταση $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ αντιστοιχίζεται με τον πίνακα $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$. Αν ο πίνακας που αντιστοιχεί στην κβαντική πύλη NOT συμβολιστεί με X, τότε πρέπει να ισχύει η σχέση :

$$X\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\beta\\ \alpha\end{pmatrix} \quad \textbf{(3-2)}$$

Ο πίνακας που ικανοποιεί αυτή τη σχέση εύκολα βρίσκεται ότι είναι ο :

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

Απ' αυτήν την περίπτωση γίνεται κατανοητό ότι οι κβαντικές πύλες που δρουν σε ένα μόνο qubit αναπαρίστανται από τετραγωνικούς πίνακες διάστασης 2x2. Αντιστρέφοντας τώρα το ερώτημα, ποιοι πίνακες 2x2 μπορούν να αναπαραστήσουν κβαντικές πύλες που δρουν σε ένα qubit; Ο μόνος περιορισμός που υπάρχει, είναι ότι πρέπει να ισχύει ότι $|\alpha|^2+|\beta|^2=1$ για την αρχική κατάσταση $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ καθώς και $|\alpha'|^2+|\beta'|^2=1$ για την τελική κατάσταση $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ που προκύπτει από τη δράση της υποτιθέμενης πύλης. Τελικά αποδεικνύεται ότι η μόνη συνθήκη στην οποία πρέπει να υπακούει ένας πίνακας U για να αναπαριστά μια κβαντική πύλη που δρα σε ένα qubit, είναι αυτός να είναι μοναδιαίος (unitary) δηλαδή να ισχύει $U^+U=I$ όπου U^+ είναι ο ανάστοφος (adjoint) του U και I είναι ο 2x2 πίνακας μονάδα. Πράγματι είναι πολύ εύκολο να διαπιστώσει κανείς για τον πίνακα X που αναπαριστά την πύλη NOT ότι ισχύει $X^+X=I$. Αυτός ο περιορισμός να είναι ο U μοναδιαίος είναι ο μοναδικός, δηλαδή κάθε μοναδιαίος τετραγωνικός πίνακας αναπαριστά κάποια κβαντική πύλη. Μια πολύ ενδιαφέρουσα διαφορά με την κλασική περίπτωση είναι ότι ενώ η μοναδική κλασική πύλη που δρα σε ένα bit είναι η πύλη NOT, στην κβαντική περίπτωση υπάρχουν αρκετές μη τετριμμένες ανάλογες πύλες. Οι δύο πιο σημαντικές απ' αυτές είναι :

- η πύλη Z της οποίας η αναπαράσταση με πίνακα είναι η :

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

άρα αφήνει την κατάσταση $|0\rangle$ ανεπηρέαστη και αντιστρέφει το πρόσημο της $|1\rangle$ δηλαδή την κάνει $-|1\rangle$.

- η πύλη Hadamard :

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

Αυτή η πύλη μετατρέπει την κατάσταση $|0\rangle$ στην $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ δηλαδή στη μισή διαδρομή ανάμεσα στη $|0\rangle$ και στην $|1\rangle$ και την $|1\rangle$ στην $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ που είναι πάλι στη μέση της διαδρομής. Εύκολα μπορεί να δείξει κανείς ότι είναι $H^2=I$ δηλαδή η εφαρμογή δύο φορές της πύλης H σε ένα qubit, επαναφέρει το qubit στην αρχική του κατάσταση.

Παρακάτω φαίνεται η δράση των τριών πυλών που προαναφέρθηκαν σε μια κατάσταση επαλληλίας $\alpha|0\rangle+\beta|1\rangle$:

$$X(\alpha|\mathbf{0}\rangle+\beta|\mathbf{1}\rangle)=\beta|\mathbf{0}\rangle+\alpha|\mathbf{1}\rangle \quad \textbf{(3-3)}$$

$$Z(\alpha|\mathbf{0}\rangle+\beta|\mathbf{1}\rangle)=\alpha|\mathbf{0}\rangle-\beta|\mathbf{1}\rangle \quad \textbf{(3-4)}$$

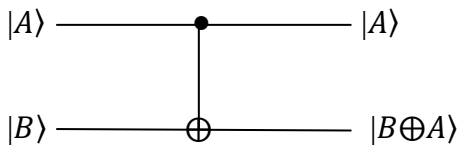
$$H(\alpha|\mathbf{0}\rangle+\beta|\mathbf{1}\rangle)=\boldsymbol{\alpha}\frac{|\mathbf{0}\rangle+|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}+\boldsymbol{\beta}\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}} \quad \textbf{(3-5)}$$

Αφού υπάρχουν άπειροι 2x2 μοναδιαίοι πίνακες, θα υπάρχουν πάρα πολλές πύλες που δρουν σε ένα qubit. Παρόλα αυτά αποδεικνύεται ότι οι ιδιότητες μιας πλήρους ομάδας από πύλες, μπορούν να κατανοηθούν μελετώντας τις ιδιότητες μιας ομάδας με πολύ λιγότερα μέλη που λέγεται «παγκόσμια» ομάδα (Nielsen & Chuang σελ. 20). Για να μπορέσουμε να κατασκευάσουμε μια τέτοια μικρή ομάδα θα πρέπει πρώτα να εισάγουμε μερικές κβαντικές πύλες που δρουν σε περισσότερα του ενός qubits.

3.2 Πύλες που δρουν σε πολλά qubits

Ας γενικεύσουμε τώρα από τις πύλες που δρουν σε ένα σε αυτές που δρουν σε περισσότερα qubits. Μερικές συνηθισμένες πύλες που δρουν σε δύο κλασικά bits είναι οι AND, OR, XOR (exclusive OR), NAND και NOR. Ένα σπουδαίο αποτέλεσμα της υπολογιστικής θεωρίας, είναι ότι κάθε συνάρτηση από bits μπορεί να συντεθεί χρησιμοποιώντας μόνο πύλες NAND άρα αυτή η πύλη είναι μια «παγκόσμια» πύλη. Αντίθετα αυτό δεν συμβαίνει με άλλες πύλες πχ με την XOR ή ακόμα και με τις XOR και NOT μαζί. Άρα αυτή η ομάδα δεν αποτελεί «παγκόσμια» ομάδα.

Η πιο σημαντική κβαντική πύλη που δρα σε δύο qubits είναι πύλη control-NOT ή απλά CNOT. Αυτή η πύλη έχει δύο qubits εισόδου τα οποία λέγονται το qubit ελέγχου και το qubit στόχος. Η κυκλωματική αναπαράσταση για μια τέτοια πύλη απεικονίζεται στο Σχήμα 3-1.



Σχήμα 3-1 : Κυκλωματική αναπαράσταση της πύλης CNOT

Η πάνω γραμμή αναπαριστά το qubit ελέγχου και η κάτω γραμμή το qubit στόχο. Η δράση της πύλης αυτής μπορεί να περιγραφεί ως εξής : αν η κατάσταση του qubit ελέγχου είναι η $|0\rangle$ τότε η κατάσταση του qubit στόχου παραμένει ως έχει, ενώ αν η κατάσταση του qubit ελέγχου είναι $|1\rangle$ τότε η κατάσταση του qubit στόχου αντιστρέφεται. Δηλαδή συνοπτικά έχουμε :

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle, |10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle$$

Άλλος ένας τρόπος να περιγράψουμε τη δράση της πύλης CNOT, είναι να τη θεωρήσουμε σαν γενίκευση της κλασικής πύλης XOR αφού η δράση της μπορεί να περιγραφεί συνοπτικά ως $|A, B\rangle \rightarrow |A, B \oplus A\rangle$ όπου $\oplus$ είναι το σύμβολο της πρόσθεσης modulo 2 που είναι ακριβώς η δράση της XOR πύλης. Άρα η κατάσταση των δύο qubit γίνεται $B \oplus A$ και το αποτέλεσμα καταχωρείται στο qubit στόχο.

Βεβαίως ένας άλλος τρόπος να περιγραφεί η δράση της CNOT είναι με αναπαράσταση πίνακα. Για να γίνει αυτό, πρέπει πρώτα να αναπαρασταθούν οι καταστάσεις των qubit με πίνακες στήλη. Έτσι αν γίνει η αντιστοίχηση :

$$|00\rangle \rightarrow \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, |01\rangle \rightarrow \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, |10\rangle \rightarrow \begin{pmatrix}0\\0\\0\\1\end{pmatrix}, |11\rangle \rightarrow \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$$

τότε η αναπαράσταση της πύλης CNOT είναι ο πίνακας :

$$U_{CNOT} = \begin{pmatrix}1 & 0 & 0 & 0\\0 & 1 & 0 & 0\\0 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{pmatrix}$$

Όπως και στην περίπτωση της πύλης που δρα σε ένα qubit, η απαίτηση να διατηρείται η πιθανότητα εκφράζεται με το γεγονός ότι ο U_{CNOT} πρέπει να είναι ένας μοναδιαίος πίνακας δηλαδή να ισχύει $U_{CNOT}^{+} U_{CNOT}=I$.

Είδαμε λοιπόν ότι για την κλασική πύλη NOT, υπάρχει η κβαντική πύλη CNOT η οποία εκτελεί την ίδια πράξη με την κλασική πύλη XOR. Μπορεί άραγε να γίνει αυτή η διαδικασία και με άλλες κλασικές πύλες όπως πχ η NAND ή η XOR, δηλαδή να ορίσουμε αντίστοιχες κβαντικές πύλες; Η απάντηση είναι ότι αυτό δεν είναι δυνατό. Και ο λόγος είναι ότι οι άλλες κλασικές πύλες είναι μη αναστρέψιμες. Αυτό σημαίνει ότι αν έχουμε πχ το αποτέλεσμα $B \oplus A$ από μια πύλη XOR, δεν είναι δυνατόν να προσδιορίσουμε ποια είναι τα A και B με μοναδικό τρόπο, υπάρχει δηλαδή μια απώλεια πληροφορίας λόγω της μη αντιστρεψιμότητας της δράσης της πύλης. Από την άλλη μεριά οι κβαντικές πύλες είναι όλες αντιστρέψιμες λόγω του ότι ο αντίστροφος ενός μοναδιαίου πίνακα είναι επίσης μοναδιαίος και έτσι μια κβαντική πύλη μπορεί να αντιστραφεί πάντα από μια άλλη κβαντική πύλη.

Φυσικά υπάρχουν και άλλες ενδιαφέρουσες πύλες που δρουν σε δύο qubits. Παρόλα αυτά η πύλη CNOT και οι απλές πύλες που δρουν σε ένα qubit αποτελούν τη βάση για όλες τις άλλες λόγω της παρακάτω πρότασης που δίνει σ' αυτές μια παγκοσμιότητα. Η σχετική πρόταση λέει ότι :

«Κάθε λογική πύλη που δρα σε πολλά qubits, μπορεί να συντεθεί από την πύλη CNOT και απλές πύλες, πύλες δηλαδή που δρουν σε ένα qubit».

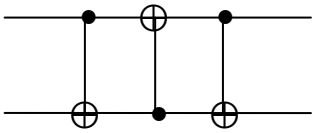
Αυτή η πρόταση είναι το κβαντικό ανάλογο της παγκοσμιότητας της πύλης NAND που αναφέρθηκε προηγουμένως.

4. Κβαντικά κυκλώματα

Σε αυτό το κεφάλαιο θα δούμε τα γενικά χαρακτηριστικά των κβαντικών κυκλωμάτων καθώς και μερικά απλά αλλά πολύ σημαντικά κβαντικά κυκλώματα.

4.1 Γενικά για τα κβαντικά κυκλώματα

Ένα απλό κβαντικό κύκλωμα το οποίο αποτελείται από τρεις κβαντικές πύλες είναι αυτό που φαίνεται στο Σχήμα 4-1.



Σχήμα 4-1 : Απλό κβαντικό κύκλωμα

Τα κυκλώματα αυτής της εργασίας διαβάζονται από τα αριστερά προς τα δεξιά. Κάθε γραμμή στο κύκλωμα αναπαριστά και ένα καλώδιο. Αυτό το καλώδιο δεν είναι απαραίτητα με την κυριολεκτική έννοια του όρου αλλά μπορεί να αντιστοιχεί στο πέρασμα του χρόνου ή ίσως σε ένα σωματίδιο όπως φωτόνιο το οποίο μετακινείται από ένα σημείο σε ένα άλλο. Το κύκλωμα που αναφέραμε σαν παράδειγμα στο Σχήμα 4-1, εκτελεί μια απλή αλλά χρήσιμη εργασία : ανταλλάσει την κατάσταση δύο qubits. Πράγματι η διαδοχή των κβαντικών πυλών του κυκλώματος έχει την παρακάτω διαδοχή στην κατάσταση στην αρχική βασική κατάσταση έστω $|a, b\rangle$:

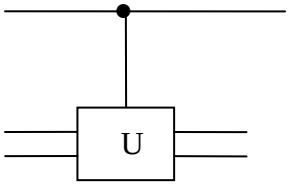
$$|a, b\rangle \rightarrow |a, a \oplus b\rangle \rightarrow |a \oplus (a \oplus b), a \oplus b\rangle = |b, a \oplus b\rangle \rightarrow |b, (a \oplus b) \oplus b\rangle = |b, a\rangle$$

όπου όλες οι προσθέσεις είναι modulo 2.

Υπάρχουν ορισμένες δυνατότητες στα κλασικά κυκλώματα οι οποίες δεν μπορούν να γίνουν στα αντίστοιχα κβαντικά. Κατ' αρχήν δεν επιτρέπονται βρόχοι (loops) δηλαδή διανύοντας το κύκλωμα ξεκινώντας από ένα σημείο να καταλήξουμε πάλι σε αυτό, άρα ένα κβαντικό κύκλωμα πρέπει να είναι άκυκλο. Δεύτερον ενώ σε ένα κλασικό κύκλωμα δύο ή περισσότερα καλώδια μπορούν να ενώνονται σε ένα και το αποτέλεσμα να είναι αυτό της πύλης OR (αυτή η διαδικασία στη γλώσσα της υπολογιστικής λέγεται FUNIN), αυτό δεν γίνεται στα κβαντικά κυκλώματα γιατί προφανώς αυτή η διαδικασία δεν είναι

αντιστρέψιμη. Τρίτο η αντίστροφη απ' την προηγούμενη διαδικασία η οποία λέγεται FUNOUT, δηλαδή η διακλάδωση ενός καλωδίου σε περισσότερα, το οποίο θα σήμαινε την παραγωγή δύο ή περισσοτέρων αντίγραφων ενός bit, επίσης επιτρέπεται στα κλασικά κυκλώματα αλλά όχι στα κβαντικά. Πράγματι αποδεικνύεται ότι η κβαντική μηχανική απαγορεύει την αντιγραφή ενός qubit όπως θα δούμε και λίγο παρακάτω (παράγραφος 4.2).

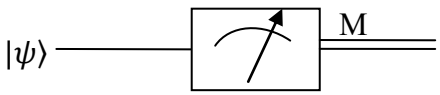
Ας δούμε τώρα μια άλλη κβαντική πύλη που δρα σε πολλά qubits η οποία είναι γενίκευση της πύλης CNOT. Αυτή η πύλη φαίνεται σχηματικά στο Σχήμα 4-2.



Σχήμα 4-2 : Γενικευμένη Πύλη CNOT (controlled U)

Έστω ότι ο U είναι ένας οποιοσδήποτε μοναδιαίος τελεστής ο οποίος δρα σε μια ομάδα από n qubits έτσι ώστε η U να μπορεί να θεωρηθεί μια κβαντική πύλη γι' αυτά τα n qubits. Τότε μπορεί να οριστεί μια πύλη η οποία λέγεται controlled-U η οποία έχει ένα qubit ελέγχου και n qubits στόχους τα οποία στο σχήμα είναι μέσα στο κουτί U και είναι αυτά στα οποία δρα η πύλη U. Η πύλη λειτουργεί ως εξής : αν το qubit ελέγχου είναι στην κατάσταση 0 τότε τίποτα δε συμβαίνει στα qubits στόχους. Αν όμως το qubit ελέγχου είναι στην κατάσταση 1 τότε η πύλη U δρα πάνω στα qubits στόχους. Είναι φανερό το γιατί η πύλη controlled-U θεωρείται γενίκευση της πύλης CNOT (controlled-NOT). Η CNOT είναι αυτής της μορφής με U=X.

Άλλη μια πολύ σημαντική διαδικασία στα κβαντικά κυκλώματα, είναι φυσικά αυτή της μέτρησης. Αυτή συμβολίζεται όπως φαίνεται στο Σχήμα 4-3.



Σχήμα 4-3 : Σχηματική αναπαράσταση της διαδικασίας της μέτρησης. Η διπλή γραμμή συμβολίζει κλασικό κανάλι επικοινωνίας.

Όπως είναι γνωστό από τη θεμελιώδη κβαντική μηχανική και έχει αναφερθεί και προηγουμένως, αυτή η διαδικασία μετατρέπει μια κατάσταση ενός απλού qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ σε μια κλασική κατάσταση ενός bit είτε 0 με πιθανότητα $|\alpha|^2$ είτε 1 με πιθανότητα $|\beta|^2$. Όπως θα δούμε και παρακάτω σε μερικές περιπτώσεις, τα κβαντικά κυκλώματα είναι χρήσιμα σαν μοντέλα για όλες τις κβαντικές διαδικασίες συμπεριλαμβανομένων, αλλά όχι μόνο, την υπολογιστική, την επικοινωνία ακόμα και τον κβαντικό θόρυβο.

4.2 Θεώρημα μη αντιγραφής

Η κλασική πύλη CNOT μπορεί να χρησιμοποιηθεί για μια πολύ σημαντική λειτουργία, την αντιγραφή ενός bit. Πράγματι αν σε αυτήν την πύλη το bit ελέγχου είναι σε μια άγνωστη κατάσταση x και το bit στόχος είναι στην κατάσταση 0, τότε μετά τη δράση της πύλης και τα δύο bit θα είναι στην άγνωστη κατάσταση x. Έστω τώρα ότι επιχειρούμε να αντιγράψουμε την κατάσταση ενός qubit η οποία είναι η $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ με τον ίδιο τρόπο χρησιμοποιώντας δηλαδή την κβαντική πύλη CNOT. Αν το qubit στόχος είναι στην κατάσταση 0 τότε η αρχική κατάσταση των δύο qubits μπορεί να γραφεί ως

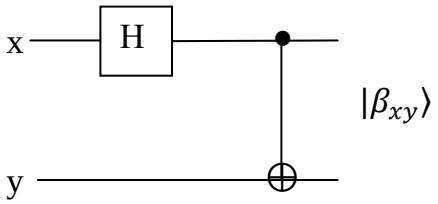
$$[\alpha|0\rangle + \beta|1\rangle]|0\rangle = \alpha|00\rangle + \beta|10\rangle$$

Η δράση της πύλης CNOT προκαλεί την αντιστροφή του δεύτερου qubit αν το πρώτο είναι στην κατάσταση 1. Άρα η τελική κατάσταση θα είναι η $\alpha|00\rangle + \beta|11\rangle$. Έχουμε πετύχει τότε την αντιγραφή της κατάστασης $|\psi\rangle$; Αν έχει γίνει αυτό, τότε η τελική κατάσταση πρέπει να είναι η $|\psi\rangle|\psi\rangle$. Αυτή η κατάσταση μπορεί να γραφεί γενικά στη μορφή $|\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \beta\alpha|10\rangle + \beta^2|11\rangle$. Άρα αν η αρχική κατάσταση είναι η $|\psi\rangle = |0\rangle$ ή η $|\psi\rangle = |1\rangle$ τότε πράγματι έχει αντιγραφεί η αρχική κατάσταση και αυτή είναι στην ουσία η κλασική περίπτωση. Αν όμως δεν ισχύει αυτό, τότε συγκρίνοντας με το αποτέλεσμα $\alpha|00\rangle + \beta|11\rangle$ βλέπουμε ότι καταλήγουμε σε διαφορετικό αποτέλεσμα εκτός αν αβ=0. Αυτό το αποτέλεσμα δεν είναι τυχαίο αλλά αποδεικνύεται γενικά ότι είναι αδύνατο να φτιαχτεί αντίγραφο μιας άγνωστης κβαντικής κατάστασης. Αυτή η πρόταση είναι γνωστή ως *θεώρημα μη κλωνοποίησης ή μη αντιγραφής* και είναι μια από τις θεμελιώδεις διαφορές μεταξύ των θεωριών της κβαντικής και κλασικής πληροφορίας.

Υπάρχει όμως και ένας βαθύτερος λόγος για τον οποίο θα έπρεπε να περιμένει κανείς να ισχύει το θεώρημα της μη κλωνοποίησης. Αυτός είναι ο εξής : λόγω της κβαντικής φύσης του qubit, η διαίσθηση μας λέει ότι σε ένα qubit η περισσότερη πληροφορία είναι κρυμμένη και όχι απ' ευθείας προσβάσιμη με τη μέτρηση. Έτσι αν γίνει η μέτρηση σε ένα απ' τα qubits που βρίσκονται στην κατάσταση $\alpha|00\rangle + \beta|11\rangle$ θα μετρήσουμε είτε 0 είτε 1 με πιθανότητες $|\alpha|^2$ ή $|\beta|^2$ αντίστοιχα. Άρα όταν μετρηθεί το ένα qubit, η κατάσταση του άλλου είναι απολύτως καθορισμένη και καμία επιπλέον πληροφορία για τα α και β δεν μπορεί να κερδηθεί. Με αυτή την έννοια η επιπλέον κρυμμένη πληροφορία που ήταν αποθηκευμένη στο σύστημα των δύο qubit αρχικά όταν αυτά ήταν στην κατάσταση $|\psi\rangle$ χάθηκε μετά την πρώτη μέτρηση και δεν μπορεί να ανακτηθεί. Αν όμως το qubit μπορούσε να αντιγραφεί, τότε το αντιγραμμένο qubit θα είχε αυτήν την κρυμμένη χαμένη πληροφορία. Άρα δεν θα ήταν λογικό να περιμένει κανείς ότι θα μπορούσαμε να κατασκευάζαμε αντίγραφα των qubits.

4.3 Καταστάσεις Bell

Ας περάσουμε τώρα σε ένα λίγο πολυπλοκότερο κύκλωμα που απεικονίζεται στο Σχήμα 4-4.



Σχήμα 4-4 : Κύκλωμα το οποίο «παράγει» καταστάσεις Bell

Όπως βλέπουμε, αυτό έχει μια πύλη Hadamard η οποία δρα στο πάνω qubit και ακολουθεί μια πύλη CNOT. Έστω ότι η αρχική κατάσταση των δύο qubit εισόδου είναι 0 και για τα δύο ή αλλιώς το σύστημα βρίσκεται στην κατάσταση $|00\rangle$. Τότε η πύλη Hadamard μετασχηματίζει το πρώτο qubit στην κατάσταση $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ άρα συνολικά η κατάσταση είναι η $\frac{|0\rangle+|1\rangle}{\sqrt{2}}|0\rangle$. Μετά δρα η πύλη CNOT και αν το qubit ελέγχου είναι στην κατάσταση 1 αλλάζει το qubit στόχο. Έτσι καταλήγουμε στην κατάσταση $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ η οποία έχει

καθιερωθεί να συμβολίζεται $|\beta_{00}\rangle$. Ομοίως βρίσκουμε σε ποια κατάσταση καταλήγει το σύστημα ανάλογα με την αρχική κατάσταση και έτσι προκύπτουν συνοπτικά τα παρακάτω αποτελέσματα :

$$|\mathbf{00}\rangle \rightarrow \frac{|\mathbf{00}\rangle+|\mathbf{11}\rangle}{\sqrt{\mathbf{2}}} = |\boldsymbol{\beta}_{\mathbf{00}}\rangle \quad \textbf{(4-1)}$$

$$|\mathbf{01}\rangle \rightarrow \frac{|\mathbf{01}\rangle+|\mathbf{10}\rangle}{\sqrt{\mathbf{2}}} = |\boldsymbol{\beta}_{\mathbf{01}}\rangle \quad \text{(4-2)}$$

$$|\mathbf{10}\rangle \rightarrow \frac{|\mathbf{00}\rangle-|\mathbf{11}\rangle}{\sqrt{\mathbf{2}}} = |\boldsymbol{\beta}_{\mathbf{10}}\rangle \quad \textbf{(4-3)}$$

$$|\mathbf{11}\rangle \rightarrow \frac{|\mathbf{01}\rangle-|\mathbf{10}\rangle}{\sqrt{\mathbf{2}}} = |\boldsymbol{\beta}_{\mathbf{11}}\rangle \quad \textbf{(4-4)}$$

Αυτές οι τέσσερεις καταστάσεις λέγονται καταστάσεις Bell ή μερικές φορές καταστάσεις EPR ή ζεύγη EPR λόγω των Bell και Einstein, Podolsky, Rosen οι οποίοι πρώτοι έδειξαν την παράξενη φύση καταστάσεων σαν αυτές όπως έχει αναφερθεί και προηγουμένως. Οι καταστάσεις Bell μπορούν να γραφούν και στη συμπυκνωμένη μορφή :

$$|\boldsymbol{\beta}_{\mathbf{xy}}\rangle = \frac{|\mathbf{0},\mathbf{y}\rangle+(-\mathbf{1})^{\mathbf{x}}|\mathbf{1},\bar{\mathbf{y}}\rangle}{\sqrt{\mathbf{2}}} \quad \textbf{(4-5)}$$

όπου $\bar{y}$ είναι η άλλη κατάσταση από αυτήν της y.

4.4 Κβαντική τηλεμεταφορά

Θα εφαρμόσουμε τώρα τις τεχνικές που αναπτύχθηκαν προηγουμένως σε κάτι μη τετριμμένο, που προκαλεί έκπληξη και είναι και διασκεδαστικό, την κβαντική τηλεμεταφορά! Η κβαντική τηλεμεταφορά είναι μια τεχνική χάρη στην οποία μπορεί να μεταφερθεί μια κβαντική κατάσταση από ένα τόπο σε έναν άλλο ακόμα και χωρίς να υπάρχει κβαντικό κανάλι επικοινωνίας να συνδέει τον αποστολέα με τον παραλήπτη. Ας δούμε τώρα πώς διατυπώνεται το πρόβλημα :

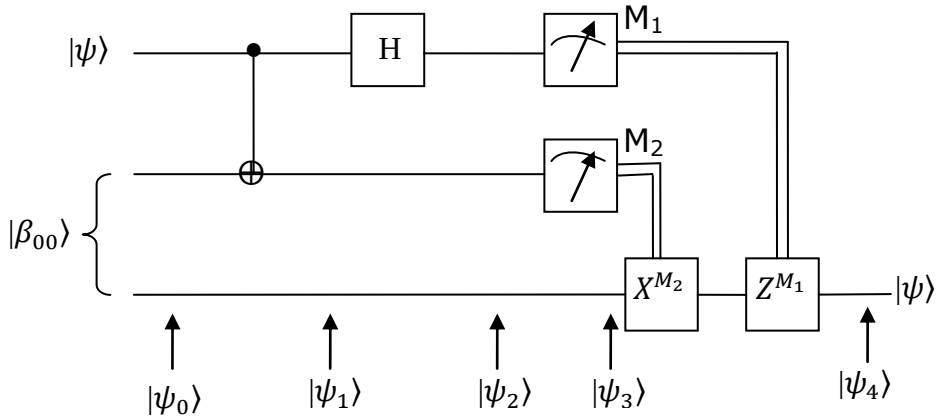
Η Alice και ο Bob έχουν γνωριστεί καιρό πριν αλλά τώρα ζουν σε μέρη που είναι πολύ μακριά. Όταν ήταν μαζί κατασκεύασαν ένα ζευγάρι καταστάσεων EPR και όταν χωρίστηκαν, ο καθένας πήρε από ένα qubit απ' αυτό το ζεύγος μαζί του. Μετά από πολλά χρόνια ο Bob κρύβεται και η αποστολή της Alice είναι να παραδώσει ένα qubit $|\psi\rangle$ στον

Bob. Η Alice δεν γνωρίζει την κατάσταση στην οποία βρίσκεται αυτό το qubit και επίσης μπορεί να στείλει στον Bob πληροφορία μόνο με τον κλασικό τρόπο.

Μπορεί η Alice να το κάνει; Διαισθητικά τα πράγματα φαίνονται άσχημα. Ενώ δεν ξέρει την κατάσταση $|\psi\rangle$, οι νόμοι της κβαντομηχανικής την εμποδίζουν να τη διαβάσει γιατί τότε θα την καταστρέψει και έχει μόνο ένα αντίγραφο του qubit αυτού στην κατοχή της. Έτσι κι αλλιώς βέβαια ακόμα και αν γνώριζε την κατάσταση $|\psi\rangle$, για να την περιγράψει ακριβώς θα χρειαζόταν άπειρο ποσό πληροφορίας αφού η $|\psi\rangle$ παίρνει τιμές από ένα συνεχές διάστημα. Έτσι θα χρειαζόταν άπειρο χρόνο για να την στείλει στον Bob μέσω ενός κλασικού καναλιού επικοινωνίας. Παρόλα αυτά όμως όπως θα δούμε η αποστολή αυτή είναι δυνατή.

Τα βήματα για τη λύση είναι τα συνοπτικά τα εξής : Η Alice αλληλεπιδρά με τον κατάλληλο τρόπο το qubit $|\psi\rangle$ που θέλει να στείλει, με το qubit του ζεύγους EPR που έχει στην κατοχή της και μετά μετρά τα δύο qubits που προκύπτουν απ' την αλληλεπίδραση. Στη συνέχεια στέλνει το αποτέλεσμα της μέτρησης στον Bob το οποίο είναι ένα απ' τα 00, 01, 10, 11. Ο Bob τώρα ανάλογα με το αποτέλεσμα που του στέλνει η Alice με το κλασικό κανάλι επικοινωνίας που έχουν στη διάθεση τους, εφαρμόζει την κατάλληλη αλληλεπίδραση με το δικό του qubit απ' το ζεύγος EPR. Και ως εκ θαύματος όταν το κάνει αυτό, μπορεί να ανακτήσει το qubit $|\psi\rangle$. Ας δούμε όλα αυτά αναλυτικά :

Το κβαντικό κύκλωμα της τηλεμεταφοράς είναι αυτό που φαίνεται στο Σχήμα 4-5.



Σχήμα 4-5 : Κβαντικό κύκλωμα τηλεμεταφοράς

Η κατάσταση που πρέπει να τηλεμεταφερθεί είναι η $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ όπου α και β είναι άγνωστα πλάτη. Η αρχική κατάσταση και των τριών qubits όπως φαίνεται και στο κύκλωμα στο Σχήμα 4-5είναι η :

$$|\boldsymbol{\psi_0}\rangle = |\boldsymbol{\psi}\rangle|\boldsymbol{\beta_{00}}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}[\boldsymbol{\alpha}|\mathbf{0}\rangle(|\mathbf{00}\rangle + |\mathbf{11}\rangle) + \boldsymbol{\beta}|\mathbf{1}\rangle(|\mathbf{00}\rangle + |\mathbf{11}\rangle)] \quad \textbf{(4-6)}$$

όπου χρησιμοποιήθηκε η σύμβαση ότι τα πρώτα δύο qubits από αριστερά ανήκουν στην Alice ενώ το τρίτο στον Bob. Όπως είπαμε και νωρίτερα, το δεύτερο qubit της Alice και το qubit του Bob αποτελούν ένα ζεύγος EPR. Κατ' αρχήν η Alice στέλνει τα qubits της σε μια πύλη CNOT οπότε προκύπτει η κατάσταση :

$$|\boldsymbol{\psi_1}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}[\boldsymbol{\alpha}|\mathbf{0}\rangle(|\mathbf{00}\rangle + |\mathbf{11}\rangle) + \boldsymbol{\beta}|\mathbf{1}\rangle(|\mathbf{10}\rangle + |\mathbf{01}\rangle)] \quad \textbf{(4-7)}$$

Μετά στέλνει το πρώτο qubit της σε μια πύλη Hadamard και έτσι προκύπτει η κατάσταση

$$|\boldsymbol{\psi_2}\rangle = \frac{\mathbf{1}}{\mathbf{2}}[\boldsymbol{\alpha}(|\mathbf{0}\rangle + |\mathbf{1}\rangle)(|\mathbf{00}\rangle + |\mathbf{11}\rangle) + \boldsymbol{\beta}(|\mathbf{0}\rangle - |\mathbf{1}\rangle)(|\mathbf{10}\rangle + |\mathbf{01}\rangle)] \quad \textbf{(4-8)}$$

Αυτή η κατάσταση μπορεί να ξαναγραφτεί αναδιατάσσοντας τους όρους στη μορφή :

$$|\boldsymbol{\psi_2}\rangle = \frac{\mathbf{1}}{\mathbf{2}}[|\mathbf{00}\rangle(\boldsymbol{\alpha}|\mathbf{0}\rangle + \boldsymbol{\beta}|\mathbf{1}\rangle) + |\mathbf{01}\rangle(\boldsymbol{\alpha}|\mathbf{1}\rangle + \boldsymbol{\beta}|\mathbf{0}\rangle) + |\mathbf{10}\rangle(\boldsymbol{\alpha}|\mathbf{0}\rangle - \boldsymbol{\beta}|\mathbf{1}\rangle) + |\mathbf{11}\rangle(\boldsymbol{\alpha}|\mathbf{1}\rangle - \boldsymbol{\beta}\mathbf{0}] \quad \textbf{(4-9)}$$

Αυτή η μορφή είναι βολική γιατί διαχωρίζονται τα qubits της Alice και του Bob και μπορεί να χωριστεί σε τέσσερεις όρους. Ο πρώτος όρος έχει τα qubits της Alice στην κατάσταση $|00\rangle$ και του Bob στην κατάσταση $\alpha|0\rangle + \beta|1\rangle$ που είναι η κατάσταση $|\psi\rangle$ που θέλαμε να τηλεμεταφέρουμε. Έτσι αν η Alice μετρήσει τα qubits της και τα βρει στην κατάσταση 00 τότε ο Bob θα έχει στο δικό του qubit την κατάσταση $|\psi\rangle$. Με παρόμοιο τρόπο ανάλογα με το αποτέλεσμα της μέτρησης της Alice, η κατάσταση στο qubit του Bob είναι η :

$$\mathbf{00} \rightarrow |\boldsymbol{\psi_3}(\mathbf{00})\rangle = [\boldsymbol{\alpha}|\mathbf{0}\rangle + \boldsymbol{\beta}|\mathbf{1}\rangle] \quad \textbf{(4-10)}$$

$$\mathbf{01} \rightarrow |\boldsymbol{\psi_3}(\mathbf{01})\rangle = [\boldsymbol{\alpha}|\mathbf{1}\rangle + \boldsymbol{\beta}|\mathbf{0}\rangle] \quad \textbf{(4-11)}$$

$$\mathbf{10} \rightarrow |\boldsymbol{\psi_3}(\mathbf{10})\rangle = [\boldsymbol{\alpha}|\mathbf{0}\rangle - \boldsymbol{\beta}|\mathbf{1}\rangle] \quad \textbf{(4-12)}$$

$$\mathbf{11} \rightarrow |\boldsymbol{\psi_3}(\mathbf{11})\rangle = [\boldsymbol{\alpha}|\mathbf{1}\rangle - \boldsymbol{\beta}|\mathbf{0}\rangle] \quad \textbf{(4-13)}$$

Φυσικά για είναι το qubit του Bob στην επιθυμητή κατάσταση, πρέπει να του πει η Alice το αποτέλεσμα της δικής της μέτρησης και αυτό μπορεί να γίνει μέσω κλασικών καναλιών

επικοινωνίας όπως φαίνεται απ' τις διπλές γραμμές στο Σχήμα 4-5. Όταν ο Bob πάρει αυτή την πληροφορία μπορεί να φτιάξει την κατάσταση του qubit του ώστε να είναι η επιθυμητή, δηλαδή η $|\psi\rangle$. Αυτό μπορεί να γίνει εφαρμόζοντας κάθε φορά την κατάλληλη πύλη (ή πύλες) εκτός βέβαια απ' την περίπτωση που το αποτέλεσμα της μέτρησης είναι 00 οπότε δεν χρειάζεται καμία παρέμβαση όπως είδαμε. Αν η μέτρηση είναι 01 τότε ο Bob πρέπει να δράσει πάνω στο qubit του την πύλη X. Αν η μέτρηση είναι 10 τότε ο Bob πρέπει να δράσει την πύλη Z. Και τέλος αν η μέτρηση είναι 11 τότε ο Bob πρέπει να δράσει πρώτα την πύλη X και μετά την πύλη Z όπως μπορεί να διαπιστωθεί πολύ εύκολα. Συνοπτικά θα μπορούσαμε να πούμε ότι σε κάθε περίπτωση ο Bob πρέπει στο qubit του να εφαρμόσει τη δράση $Z^{M_1}X^{M_2}$ όπου M_1, M_2 είναι τα αποτελέσματα των δύο μετρήσεων της Alice.

Υπάρχουν πολλά σχόλια που θα μπορούσε να κάνει κανείς σχετικά με την κβαντική τηλεμεταφορά. Ας αναφέρουμε εδώ μόνο δύο πολύ χαρακτηριστικά που με πρώτη ματιά φαίνονται παράδοξα. Το πρώτο είναι ότι αφού η κατάσταση $|\psi\rangle$ μοιάζει να μεταφέρεται ακαριαία από την Alice στο Bob, φαινομενικά παραβιάζεται η βασική αρχή της Ειδικής Θεωρίας της Σχετικότητας. Κι αυτό γιατί σύμφωνα με αυτήν, αν η πληροφορία μπορούσε να μεταδοθεί ταχύτερα απ' την ταχύτητα του φωτός τότε αυτή η πληροφορία θα μεταφερόταν πίσω στο χρόνο. Ευτυχώς αυτό δεν συμβαίνει, γιατί για να ολοκληρωθεί η τηλεμεταφορά, η Alice πρέπει να στείλει στον Bob τις μετρήσεις της χρησιμοποιώντας κλασικό κανάλι επικοινωνίας το οποίο δεν μπορεί φυσικά να γίνει ταχύτερα απ' το φως, οπότε το παράδοξο δεν υφίσταται.

Το δεύτερο φαινομενικό παράδοξο στην τηλεμεταφορά, είναι ότι φαίνεται η αρχική κατάσταση $|\psi\rangle$ τελικά να αντιγράφεται, αφού στο τέλος της διαδικασίας έχει ένα αντίτυπο η Alice και ένα ο Bob. Και αυτό παραβιάζει φυσικά το θεμελιώδες θεώρημα της μη κλωνοποίησης που αναφέρθηκε προηγουμένως. Όμως ούτε αυτό συμβαίνει διότι τελικά μόνο το qubit του Bob βρίσκεται στην κατάσταση $|\psi\rangle$ αφού το πρώτο qubit της Alice στο τέλος της διαδικασίας βρίσκεται σε μια απ' τις βασικές καταστάσεις $|0\rangle$ ή $|1\rangle$ λόγω της ιδιότητας της μέτρησης να καταστρέφει την αρχική κατάσταση.

Σίγουρα απ' την κβαντική τηλεμεταφορά έχουμε μάθει πολλά και συνεχίζουμε να μαθαίνουμε όλο και περισσότερα. Είναι κάτι πολύ περισσότερο από ένα εντυπωσιακό κόλπο με τις κβαντικές πύλες. Η κβαντική τηλεμεταφορά τονίζει την ικανότητα ανταλλαγής πληροφορίας μεταξύ διαφορετικών μερών μέσω της κβαντικής μηχανικής και

δείχνει ότι είναι δυνατόν με ένα χωρισμένο EPR ζεύγος μαζί με δύο κλασικά bits επικοινωνίας, να γίνει επικοινωνία (μεταφορά) τουλάχιστον ενός qubit. Οι θεωρίες της κβαντικής υπολογιστικής και της κβαντικής πληροφορίας έχουν αποκαλύψει πληθώρα τέτοιων μεθόδων πολλές απ' τις οποίες βασίζονται στην κβαντική τηλεμεταφορά. Η κβαντική τηλεμεταφορά μπορεί να χρησιμοποιηθεί για την κατασκευή κβαντικών πυλών που είναι ανθεκτικές στο θόρυβο. Επίσης η κβαντική τηλεμεταφορά είναι άρρηκτα συνδεδεμένη με τους κβαντικούς κώδικες διόρθωσης λαθών.

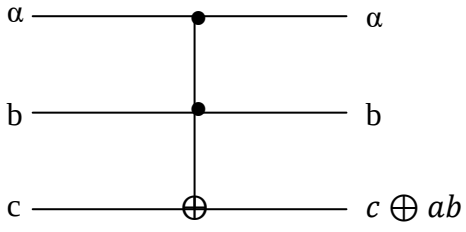
Βέβαια παρόλα αυτά, θα ήταν σωστότερο να λέγαμε ότι βρισκόμαστε ακόμα στην αρχή της κατανόησης της βαθύτερης αιτίας που είναι δυνατή η κβαντική τηλεμεταφορά και σίγουρα είναι ένα πεδίο που απαιτείται περαιτέρω διερεύνηση.

5. Κβαντικοί αλγόριθμοι

Θα εξετάσουμε τώρα, ποια κατηγορία υπολογισμών μπορεί να παρουσιαστεί χρησιμοποιώντας τα κβαντικά κυκλώματα. Και επίσης θα εξεταστεί, πώς μπορεί αυτή κατηγορία υπολογισμών να συγκριθεί με αυτούς που χρησιμοποιούν κλασικά λογικά κυκλώματα. Και θα γίνει προσπάθεια να απαντηθεί το κρίσιμο ερώτημα του αν και κατά πόσο υπάρχει κάποιο πεδίο στο οποίο ένας κβαντικός υπολογιστής μπορεί να λειτουργήσει καλύτερα από έναν κλασικό.

5.1 Κλασικοί Υπολογισμοί σε Κβαντικό Υπολογιστή

Θα εξετάσουμε τώρα αν είναι δυνατόν να πραγματοποιήσουμε έναν υπολογισμό που γίνεται από ένα κλασικό κύκλωμα με ένα αντίστοιχο κβαντικό. Η απάντηση είναι ότι αυτό είναι δυνατό και δεν θα πρέπει να μας εκπλήσσει. Κι αυτό διότι είναι πλέον γενική πεποίθηση ότι όλα τα φαινόμενα στη φύση συμπεριλαμβανομένων προφανώς και των λογικών κυκλωμάτων, εξηγούνται θεμελιωδώς από την κβαντική μηχανική. Βέβαια η μετάβαση από τα κλασικά κυκλώματα στα αντίστοιχα κβαντικά, δεν είναι και τόσο άμεση με απλή αντικατάσταση δηλαδή των κλασικών πυλών με κάποιες αντίστοιχες κβαντικές. Ο λόγος είναι ότι όπως έχει προαναφερθεί, μερικές κλασικές πύλες είναι μη αντιστρέψιμες όπως η NAND και αυτό δεν επιτρέπεται στα κβαντικά κυκλώματα. Αυτό όμως μπορεί να ξεπεραστεί αφού είναι γνωστό από την κλασική θεωρία υπολογιστών ότι κάθε κλασικό κύκλωμα μπορεί να αντικατασταθεί με ένα ισοδύναμο το οποίο να περιέχει μόνο αντιστρέψιμες πύλες κάνοντας χρήση μιας αντιστρέψιμης πύλης γνωστής σαν πύλη Toffoli. Η πύλη αυτή φαίνεται σχηματικά στο Σχήμα 5-1.



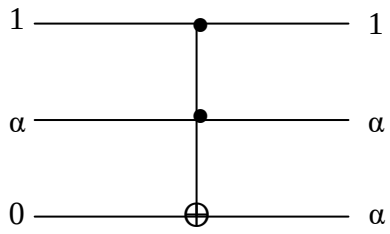
Σχήμα 5-1 : Πύλη Toffoli

Όπως φαίνεται απ' το σχήμα, η πύλη αυτή έχει τρία qubits εισόδου και άλλα τόσα εξόδου και τα δύο πάνω είναι qubits ελέγχου ενώ το κάτω είναι qubit στόχος. Τα δύο qubits ελέγχου μένουν ανεπηρέαστα από τη δράση της πύλης ενώ το τρίτο αλλάζει κατάσταση μόνο αν τα άλλα δύο είναι στην κατάσταση 1. Αυτό περιγράφεται συμπυκνωμένα με την πρόταση: αν τα δύο qubits ελέγχου είναι αρχικά στις καταστάσεις α και b και το qubit στόχος στην κατάσταση c, τότε μετά τη δράση της πύλης, τα qubits ελέγχου παραμένουν στις καταστάσεις α και b ενώ το qubit στόχος μεταβαίνει στην κατάσταση $c \oplus ab$. Μια σημαντική παρατήρηση είναι ότι η πύλη Toffoli έχει μια ιδιότητα που έχει και η πύλη CNOT και αυτή είναι ότι αν δράσει δύο διαδοχικές φορές επαναφέρει το σύστημα στην αρχική του κατάσταση. Πράγματι το σύστημα μεταβαίνει διαδοχικά στις καταστάσεις

$$(\alpha, b, c) \rightarrow (\alpha, b, c \oplus \alpha b) \rightarrow [a, b, (c \oplus \alpha b) \oplus \alpha b] = (\alpha, b, c)$$

Αυτό εκτός των άλλων αποδεικνύει ότι η πύλη αυτή, είναι αντιστρέψιμη αφού η αντίστροφη της είναι ο εαυτός της.

Η πύλη Toffoli μπορεί να χρησιμοποιηθεί σαν πύλη NAND αν το qubit στόχος αρχικά τεθεί στην κατάσταση 1 αφού τότε μετά τη δράση της πύλης, θα βρεθεί στην κατάσταση $1 \oplus \alpha b = -(\alpha b)$. Επίσης η πύλη αυτή μπορεί να χρησιμοποιηθεί και για FUNOUT αν αρχικά το ένα qubit ελέγχου τεθεί στην κατάσταση 1 και το qubit στόχος στην κατάσταση 0 όπως φαίνεται στο Σχήμα 5-2 :



Σχήμα 5-2: Η πύλη Toffoli μπορεί να χρησιμοποιηθεί για FUNOUT

Έτσι ξεπερνιούνται και οι δύο δυσκολίες που υπάρχουν στο να μετατραπεί ένα κλασικό κύκλωμα σε κβαντικό και έτσι τελικά ένα οποιοδήποτε κλασικό κύκλωμα μπορεί να προσομοιωθεί με ένα ισοδύναμο (αντιστρέψιμο) κβαντικό.

Άλλο ένα ερώτημα είναι τώρα, αν αυτή η μετατροπή ενός κλασικού κυκλώματος σε κβαντικό, μπορεί να γίνει ακόμα και στην περίπτωση που ο κλασικός υπολογιστής είναι μη ντετερμινιστικός δηλαδή αν έχει την ικανότητα να παράγει τυχαία bits τα οποία τα

χρησιμοποιεί στους υπολογισμούς. Επειδή η κβαντική μηχανική έχει άμεση σχέση με το «τυχαίο», είναι λογικό να υποθέσει κανείς ότι η απάντηση θα είναι θετική. Και πράγματι έτσι είναι. Αν πχ ένα qubit ετοιμαστεί στην κατάσταση $|0\rangle$ και επιδράσει σε αυτό μια πύλη Hadamard, τότε η κατάσταση του θα γίνει η $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ και εάν την μετρήσουμε τότε τα αποτελέσματα της μέτρησης θα είναι είτε $|0\rangle$ είτε $|1\rangle$ με ποσοστά 50% για το κάθε ενδεχόμενο οπότε η παραγωγή τυχαίων qubits γίνεται πολύ εύκολα.

Άρα ένας κβαντικό κύκλωμα μπορεί να αντικαταστήσει έναν κλασικό. Βέβαια αν αυτή ήταν η μοναδική ικανότητα των κβαντικών υπολογιστών μάλλον δεν θα άξιζε όλος αυτός ο κόπος για τη διερεύνηση τους. Υπάρχει όμως η πίστη η οποία στηρίζεται σε μερικά πρώτα ενθαρρυντικά αποτελέσματα που θα δούμε στη συνέχεια, ότι η κβαντική υπολογιστική μπορεί να προσφέρει δυνατότητες πολύ πέρα από τις κλασικές δηλαδή μπορεί να πραγματοποιήσει εργασίες που δεν θα ήταν δυνατόν να γίνουν σε κλασικούς υπολογιστές είτε λόγω της φύσης της εργασίας είτε λόγω της ταχύτητας που θα απαιτείτο. Παρακάτω θα μελετήσουμε τον αλγόριθμο Deutsch-Jozsa (ενότητα 5.4) σαν ένα πρώτο παράδειγμα κβαντικού αλγόριθμου ο οποίος μπορεί να επιλύσει ένα πρόβλημα γρηγορότερα από οποιονδήποτε κλασικό αλγόριθμο.

5.2 Κβαντικός Παραλληλισμός

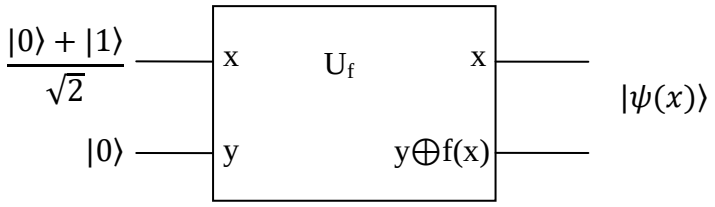
Ο κβαντικός παραλληλισμός είναι ένα χαρακτηριστικό αποκλειστικά των κβαντικών αλγορίθμων και η υφή του βρίσκεται στη ρίζα της κβαντικής μηχανικής. Σε αυτή τη δυνατότητα οφείλεται η δημιουργία πολλών κβαντικών αλγορίθμων όπως θα δούμε παρακάτω. Ένας απλός ορισμός του κβαντικού παραλληλισμού (με τον κίνδυνο της υπεραπλούστευσης), είναι ο παρακάτω :

Κβαντικός παραλληλισμός είναι η λειτουργία που επιτρέπει στους κβαντικούς υπολογιστές να υπολογίζουν τις τιμές μιας συνάρτησης f(x) για πολλές τιμές του x ταυτόχρονα!

Ας δούμε πώς λειτουργεί αυτό το φαινόμενο καθώς και τους περιορισμούς του.

Έστω f(x) μια συνάρτηση από το σύνολο {0,1} στο σύνολο {0,1}. Έστω επίσης ότι έχουμε ένα κβαντικό υπολογιστή με 2 qubits τα οποία είναι αρχικά στην τυχαία

κατάσταση $|x,y\rangle$. Τέλος έστω ότι υπάρχει μια κβαντική πύλη η οποία όταν δράσει στην κατάσταση $|x,y\rangle$ τη μετατρέπει στην κατάσταση $|x,y\oplus f(x)\rangle$. Ας ονομάσουμε αυτό το μετασχηματισμό (τελεστή) U_f , ο οποίος αποδεικνύεται ότι είναι μοναδιαίος. Αν είναι y=0 τότε προφανώς η τελική κατάσταση του δεύτερου qubit θα είναι η f(x). Η κβαντική πύλη U_f μπορεί να πραγματοποιηθεί διότι όπως είδαμε για ένα δεδομένο κλασικό κύκλωμα υπολογισμού μιας συνάρτησης f, υπάρχει ένα κβαντικό κύκλωμα παρόμοιας αποτελεσματικότητας το οποίο λειτουργεί με το μετασχηματισμό U_f. Για αυτήν την παράγραφο όμως μπορούμε να μην μπούμε σε λεπτομέρειες αλλά να θεωρήσουμε ότι είναι ένα μαύρο κουτί που κάνει αυτό το μετασχηματισμό. Ας θεωρήσουμε λοιπόν το κύκλωμα που απεικονίζεται στο Σχήμα 5-3.



Σχήμα 5-3: Κύκλωμα με το οποίο επιτυγχάνεται κβαντικός παραλληλισμός

Στο κύκλωμα αυτό όπως φαίνεται και απ' το σχήμα, το πάνω qubit δεν είναι σε μια βασική κατάσταση αλλά στην κατάσταση επαλληλίας $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ η οποία όπως έχει αναφερθεί μπορεί να δημιουργηθεί δρώντας μια πύλη Hadamard σε ένα qubit το οποίο βρίσκεται στην κατάσταση $|0\rangle$. Η τελική κατάσταση των δύο qubits μετά τη δράση της U_f είναι η

$$\frac{|\mathbf{0},\mathbf{f}(\mathbf{0})\rangle+|\mathbf{1},\mathbf{f}(\mathbf{1})\rangle}{\sqrt{\mathbf{2}}} \qquad \textbf{(5-1)}$$

Αυτή είναι μια αξιοπρόσεκτη κατάσταση διότι περιέχει πληροφορίες για δύο τιμές της συνάρτησης, την f(0) και την f(1). Δηλαδή είναι σαν να έχουμε υπολογίσει ταυτόχρονα τις δύο αυτές τιμές της συνάρτησης άρα έχει γίνει κβαντικός παραλληλισμός. Η διαφορά με την αντίστοιχη κλασική περίπτωση είναι ότι εκεί θα χρειάζονταν δύο κυκλώματα, το ένα να υπολογίσει την τιμή f(0) και το άλλο την f(1) ενώ στην κβαντική περίπτωση αυτές υπολογίστηκαν μόνο από ένα κύκλωμα εκμεταλλευόμενοι τη δυνατότητα ενός qubit να βρίσκεται σε καταστάσεις επαλληλίας.

Αυτή η διαδικασία μπορεί να γενικευτεί και στην περίπτωση που η συνάρτηση f είναι πολλών μεταβλητών έστω n. Τότε πρέπει να χρησιμοποιήσουμε ένα γενικότερο

μετασχηματισμό γνωστό ως μετασχηματισμό Hadamard ή Walsh-Hadamard. Αυτός ο μετασχηματισμός είναι απλά η δράση n πυλών Hadamard παράλληλα στα n qubits. Έτσι στο προηγούμενο κύκλωμα αντί για το πάνω qubit θα έχουμε n qubits και συνολικά στο κύκλωμα n+1. Στην περίπτωση που είναι n=2 μετά τη δράση των πυλών Hadamard αν αρχικά τα δύο qubits ήταν στην κατάσταση $|0\rangle$, η κατάσταση τους θα είναι η :

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)=\frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2} \quad \textbf{(5-2)}$$

Την παράλληλη δράση των δύο πυλών Hadamard θα συμβολίζουμε με $H^{\otimes 2}$. Στη γενική περίπτωση τώρα των n qubits που βρίσκονται αρχικά στην κατάσταση $|0\rangle$, μετά την παράλληλη δράση των πυλών Hadamard (που τώρα θα συμβολίζεται με $H^{\otimes n}$), αυτά θα είναι στην κατάσταση :

$$\frac{1}{\sqrt{2^n}}\sum_n |x\rangle \quad \textbf{(5-3)}$$

όπου x είναι η κάθε δυνατή τιμή συνδυασμού βασικών καταστάσεων των qubits. Για παράδειγμα στην περίπτωση που n=2, οι δυνατές τιμές του x είναι x=00, 01, 10, 11. Δηλαδή η δράση του μετασχηματισμού Hadamard προκαλεί μια ισοδύναμη υπέρθεση όλων των βασικών καταστάσεων. Και μάλιστα δημιουργεί υπέρθεση 2^n καταστάσεων χρησιμοποιώντας μόνο n πύλες. Έτσι συνοπτικά, η γενική περίπτωση της συνάρτησης n μεταβλητών μπορεί να διατυπωθεί ως εξής :

Έχουμε ένα κβαντικό υπολογιστή με n+1 qubits και τα ετοιμάζουμε αρχικά στην κατάσταση $|0\rangle^{\otimes n}|0\rangle$. Στη συνέχεια εφαρμόζουμε μετασχηματισμό Hadamard στα πρώτα n qubits και μετά επιδρούμε το μαύρο κουτί που πραγματοποιεί το μετασχηματισμό U_f. Έτσι η συνολική κατάσταση των n+1 qubits γίνεται η :

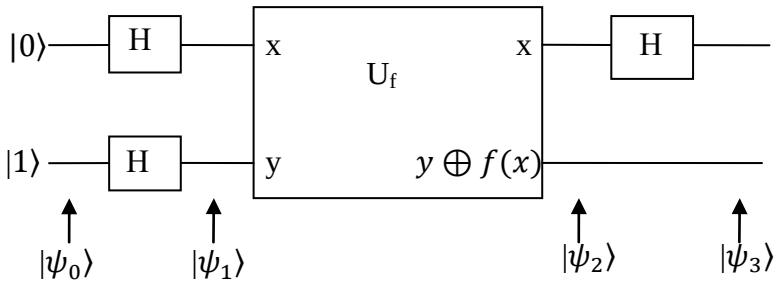
$$\frac{1}{2^n}\sum_x |x\rangle|f(x)\rangle$$

Κατά κάποια έννοια ο κβαντικός μετασχηματισμός προϋποθέτει να έχουν υπολογιστεί όλες οι δυνατές τιμές της συνάρτησης f(x) ταυτόχρονα. Παρόλα αυτά, αυτός δεν είναι άμεσα αξιοποιήσιμος. Κι αυτό διότι για παράδειγμα στην πιο απλή περίπτωση του ενός qubit, η μέτρηση της τελικής κατάστασης θα δώσει είτε το αποτέλεσμα $|0, f(0)\rangle$ είτε το $|1, f(1)\rangle$ δηλαδή μόνο τη μια τιμή της f(x). Και στη γενική περίπτωση η μέτρηση της κατάστασης $\sum_x |x, f(x)\rangle$ θα δώσει το αποτέλεσμα $|x, f(x)\rangle$ δηλαδή μόνο μια τιμή της συνάρτησης για ένα συγκεκριμένο x. Αυτό βέβαια θα μπορούσε να το κάνει εύκολα και

ένας κλασικός υπολογιστής. Άρα η κβαντική υπολογιστική απαιτεί κάτι περισσότερο από αυτή τη μορφή του κβαντικού παραλληλισμού για να θεωρείται πραγματικά χρήσιμη. Πρέπει κάπως να βρεθεί τρόπος να εξαχθούν πληροφορίες για περισσότερες από μια τιμές της συνάρτησης f(x) από καταστάσεις υπέρθεσης του τύπου $\sum_x |x, f(x)\rangle$. Στις επόμενες δύο παραγράφους θα δοθούν δύο παραδείγματα για το πώς μπορεί να γίνει αυτό.

5.3 Ο αλγόριθμος του Deutsch

Ένα κύκλωμα ελαφρά τροποποιημένο απ' αυτό της προηγούμενης παραγράφου, μας δείχνει πώς μπορούν τα κβαντικά κυκλώματα να ξεπεράσουν τα αντίστοιχα κλασικά. Αυτό το κύκλωμα φαίνεται στο Σχήμα 5-4 και πραγματοποιεί το λεγόμενο αλγόριθμο του Deutsch.



Σχήμα 5-4 : Κύκλωμα που περιγράφει τον αλγόριθμο του Deutsch

Για την ακρίβεια αυτό το κύκλωμα απεικονίζει μια απλοποιημένη και βελτιωμένη εκδοχή του πρωτότυπου αλγόριθμου του Deutsch. Ο αλγόριθμος αυτός συνδυάζει τον κβαντικό παραλληλισμό με μια ιδιότητα των κβαντικών συστημάτων γνωστής ως συμβολή (interference).

Πριν ξεκινήσουμε τον υπολογισμό των καταστάσεων που προκύπτουν στα διάφορα βήματα του αλγόριθμου, θα αποδείξουμε πρώτα τη σχέση :

$$\mathbf{U_f}|\mathbf{x}\rangle\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}} = (-\mathbf{1})^{\mathbf{f(x)}}|\mathbf{x}\rangle\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}} \text{ , όπου x =0 ή x=1} \qquad \textbf{(5-4)}$$

η οποία θα χρειαστεί στους υπολογισμούς αυτούς :

Κατ' αρχήν είναι $U_f|x\rangle|0\rangle = |x\rangle|0\oplus f(x)\rangle$ και $U_f|x\rangle|1\rangle = |x\rangle|1\oplus f(x)\rangle$. Είναι όμως f(x)=0 ή f(x)=1 οπότε έχουμε :

$$U_f|x\rangle|0\rangle = \begin{cases} |x\rangle|0\rangle, \alpha\nu\ f(x)=0 \\ |x\rangle|1\rangle, \alpha\nu\ f(x)=1 \end{cases} \text{ και}$$

$$U_f|x\rangle|1\rangle = \begin{cases} |x\rangle|1\rangle, \alpha\nu\ f(x)=0 \\ |x\rangle|0\rangle, \alpha\nu\ f(x)=1 \end{cases}.$$

άρα έχουμε : $U_f|x\rangle(|0\rangle-|1\rangle) = \begin{cases} |x\rangle(|0\rangle-|1\rangle), \alpha\nu\ f(x)=0 \\ -|x\rangle(|0\rangle-|1\rangle), \alpha\nu\ f(x)=1 \end{cases}$ και τελικά είναι :

$$U_f|x\rangle(|0\rangle-|1\rangle) = (-1)^{f(x)}|x\rangle(|0\rangle-|1\rangle)$$

η οποία προφανώς ισοδυναμεί με τη ζητούμενη.

Πάμε τώρα αναλυτικά στα βήματα του αλγόριθμου. Η αρχική κατάσταση όπως φαίνεται στο σχήμα είναι η $|\psi_0\rangle = |01\rangle$. Μετά την παράλληλη δράση των πυλών Hadamard η κατάσταση γίνεται η :

$$|\boldsymbol{\psi_1}\rangle = \left[\frac{|\mathbf{0}\rangle+|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}\right]\left[\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}\right] \quad \textbf{(5-5)}$$

Για την κατάσταση $|\psi_2\rangle$ έχουμε :

$$|\boldsymbol{\psi_2}\rangle = \boldsymbol{U_f}|\boldsymbol{\psi_1}\rangle = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\boldsymbol{U_f}[(|\mathbf{0}\rangle+|\mathbf{1}\rangle)\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}] = \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\boldsymbol{U_f}(|\mathbf{0}\rangle\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}) + \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\boldsymbol{U_f}(|\mathbf{1}\rangle\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}) =$$

$$\frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(-\mathbf{1})^{f(\mathbf{0})}|\mathbf{0}\rangle\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}} + \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}(-\mathbf{1})^{f(\mathbf{1})}|\mathbf{1}\rangle\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}} \quad \textbf{(5-6)}$$

Έτσι τελικά έχουμε :

$$|\boldsymbol{\psi_2}\rangle = \begin{cases} \pm\left[\frac{|\mathbf{0}\rangle+|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}\right]\left[\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}\right], \boldsymbol{\alpha\nu}\ \mathbf{f(0)=f(1)} \\ \pm\left[\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}\right]\left[\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}\right], \boldsymbol{\alpha\nu}\ \mathbf{f(0)\neq f(1)} \end{cases} \quad \textbf{(5-7)}$$

Το πρόσημο + στο πάνω σκέλος του άγκιστρου αντιστοιχεί στην περίπτωση που f(0)=f(1)=0 και το – στην περίπτωση που f(0)=f(1)=1, ενώ στο κάτω σκέλος του άγκιστρου το + αντιστοιχεί στην περίπτωση που f(0)=0 και f(1)=1 και το – αντιστοιχεί στην περίπτωση που f(0)=1 και f(1)=0.

Με τη δράση στη συνέχεια της πύλης Hadamard στο πάνω qubit, έχουμε για την κατάσταση $|\psi_3\rangle$:

$$|\boldsymbol{\psi_3}\rangle = \begin{cases} \pm|\mathbf{0}\rangle\left[\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}\right], \boldsymbol{\alpha\nu}\ \mathbf{f(0)=f(1)} \\ \pm|\mathbf{1}\rangle\left[\frac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}\right], \boldsymbol{\alpha\nu}\ \mathbf{f(0)\neq f(1)} \end{cases} \quad \textbf{(5-8)}$$

Επειδή η ποσότητα $f(0)\oplus f(1)$ είναι ίση με 0 αν $f(0)=f(1)$ και 1 αν $f(0)\neq f(1)$, μπορούμε να γράψουμε την προηγούμενη σχέση σε συμπυκνωμένη μορφή ως :

$$|\boldsymbol{\psi_3}\rangle = \pm|\mathbf{f(0)}\oplus\mathbf{f(1)}\rangle|[\tfrac{|\mathbf{0}\rangle-|\mathbf{1}\rangle}{\sqrt{\mathbf{2}}}] \quad \textbf{(5-9)}$$

Αυτό το αποτέλεσμα μας δείχνει ότι αρκεί να μετρήσουμε μόνο το πρώτο qubit ώστε να ξέρουμε την τιμή της ποσότητας $f(0)\oplus f(1)$. Ισοδύναμα μπορούμε να βρούμε αν η συνάρτηση είναι σταθερή (δηλαδή $f(0)=f(1)$) ή όχι. Συγκεκριμένα αν το πρώτο qubit μετρηθεί στην κατάσταση $|0\rangle$ τότε η f είναι σταθερή αλλιώς δεν είναι, δηλαδή είναι $f(0)\neq f(1)$ και τότε η συνάρτηση λέγεται ισοζυγισμένη.

Το ενδιαφέρον στον αλγόριθμο Deutsch είναι ότι καταφέρνει να υπολογίσει ένα «ολικό» (global) χαρακτηριστικό της συνάρτησης f (την ποσότητα $f(0)\oplus f(1)$), κάνοντας μόνο ένα «τρέξιμο» του κβαντικού υπολογιστή αντί για δύο που θα απαιτούσε ο αντίστοιχος κλασικός. Τώρα μπορούμε να εξηγήσουμε καλύτερα το λόγο που ο αλγόριθμος αυτός συνδυάζει τα δύο θεμελιώδη χαρακτηριστικά της κβαντικής μηχανικής τον κβαντικό παραλληλισμό και τη συμβολή.

Κατ' αρχήν για τον κβαντικό παραλληλισμό. Το πρώτο βήμα του αλγόριθμου είναι να φέρει την κατάσταση των qubits σε καταστάσεις επαλληλίας πριν δράσει σε αυτά η βασική πύλη U_f. Αυτό γίνεται ώστε η δράση αυτής της πύλης να γίνει παράλληλα για x=0 και για x=1 και μάλιστα σε ποσοστό 50% σε κάθε μια, όπως είδαμε ότι είναι η δράση των πυλών Hadamard.

Για το ρόλο της συμβολής τώρα, στον αλγόριθμο σε πρώτη φάση με τη δράση των πυλών Hadamard στο πρώτο βήμα, γίνεται διαχωρισμός των καταστάσεων ώστε αυτές στη συνέχεια να ακολουθήσουν παράλληλες διαφορετικές διαδρομές και στη συνέχεια με τη δράση πάλι της πύλης Hadamard στο πάνω qubit ξαναγίνεται συμβολή ώστε η έξοδος στο πρώτο qubit να είναι σε μια βασική κατάσταση ώστε να είναι εύκολα προσδιορίσιμη. Αυτή η πορεία μας φέρνει στο μυαλό το γνωστό πείραμα συμβολής ηλεκτρονίων ή φωτονίων στα οποία η αρχική δέσμη διαχωρίζεται σε δύο επιμέρους και στη συνέχεια αυτές πάλι ανασυντίθενται ώστε να δημιουργήσουν μια νέα δέσμη τα χαρακτηριστικά της οποίας εξαρτώνται από τη διαφορά φάσης των δύο αρχικών δεσμών λόγω της διαφορετικής διαδρομής που ακολούθησαν.

Ο αλγόριθμος του Deutsch αναδεικνύει και τη διαφορά ανάμεσα στον κβαντικό παραλληλισμό και στους κλασικούς αλγόριθμους τυχαιότητας (randomized algorithms). Κι αυτό διότι θα μπορούσε να υποστηρίξει κάποιος ότι μια κατάσταση της μορφής $|0\rangle|f(0)\rangle+|1\rangle|f(1)\rangle$ μπορεί να θεωρηθεί σαν η λειτουργία ενός πιθανοκρατικού κλασικού υπολογιστή ο οποίος υπολογίζει την τιμή f(0) με πιθανότητα 50% και την τιμή f(1) με πιθανότητα 50%. Η καίρια διαφορά όμως είναι ότι σε ένα κλασικό υπολογιστή αυτές οι δύο επιλογές είναι αλληλοαποκλειόμενες ενώ σε έναν κβαντικό είναι δυνατό να συμβάλλουν, ώστε να οδηγούν σε μια ολική ιδιότητα της συνάρτησης f χρησιμοποιώντας κάτι σαν την πύλη Hadamard ώστε να ανασυντεθούν οι διαφορετικές επιλογές όπως γίνεται στον αλγόριθμο του Deutsch.

5.4 Ο αλγόριθμος Deutsch-Jozsa

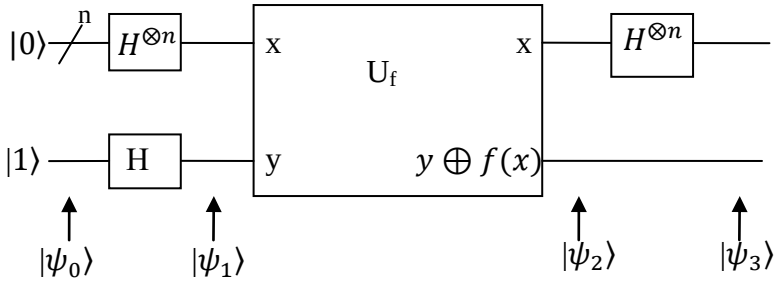
Ο αλγόριθμός Deutsch που αναλύθηκε στην προηγούμενη παράγραφο, αποτελεί μια ειδική περίπτωση ενός γενικότερου αλγόριθμου ο οποίος ονομάζεται αλγόριθμος Deutsch-Jozsa. Αυτός ο αλγόριθμος φιλοδοξεί να λύσει το παρακάτω πρόβλημα γνωστό και ως πρόβλημα του Deutsch το οποίο διατυπώνεται ως εξής :

Η Alice διαλέγει έναν αριθμό x από τους 0 έως 2^n-1 (2^n το πλήθος) και τον ταχυδρομεί στο φίλο της τον Bob ο οποίος βρίσκεται πολύ μακριά. Ο Bob μόλις λαμβάνει τον αριθμό x υπολογίζει την ποσότητα f(x) όπου f μια συνάρτηση με σύνολο τιμών το {0,1} η οποία είναι ή σταθερή δηλαδή f(x)=0 ή f(x)=1 για κάθε x ή ισοζυγισμένη . Ο όρος ισοζυγισμένη αναφέρθηκε και στην προηγούμενη παράγραφο για συνάρτηση με πεδίο ορισμού το {0,1}. Τώρα γενικεύοντας, ισοζυγισμένη ονομάζεται η συνάρτηση η οποία στην περίπτωση μας παίρνει τιμές f(x)=0 για ακριβώς τις μισές δυνατές τιμές του x και f(x)=1 για τις άλλες μισές. Μόλις ο Bob κάνει αυτόν τον υπολογισμό, ταχυδρομεί πίσω στην Alice το αποτέλεσμα. Ο σκοπός του προβλήματος είναι η Alice να μπορέσει να προσδιορίσει με βεβαιότητα αν η συνάρτηση f που χρησιμοποίησε ο Bob ήταν σταθερή ή ισοζυγισμένη.

Αν οι δύο φίλοι προσπαθούσαν να λύσουν το πρόβλημα με τον κλασικό τρόπο, για να προσδιορίσει η Alice με βεβαιότητα τη μορφή της συνάρτησης θα έπρεπε στην καλύτερη

περίπτωση να ανταλλάξουν 2 μηνύματα και στη χειρότερη $\frac{2^n}{2}+1$. Δηλαδή η Alice να στείλει στον Bob από 2 έως $\frac{2^n}{2}+1$ αριθμούς x και να λάβει ισάριθμες απαντήσεις. Κι αυτό γιατί, αν μεν οι δύο πρώτες απαντήσεις του Bob είχαν διαφορετικό αποτέλεσμα τότε η f θα ήταν ισοζυγισμένη, αν όμως η Alice είχε εξαντλήσει τους μισούς αριθμούς x (δηλαδή $\frac{2^n}{2}$) και η απάντηση ερχόταν όλο η ίδια πχ το 0, τότε θα έπρεπε να περιμένει να γίνει άλλη μια ανταλλαγή μηνυμάτων και αν η απάντηση ήταν πάλι 0 τότε η συνάρτηση θα ήταν σταθερή αλλιώς θα ήταν ισοζυγισμένη. Αν όμως οι δύο φίλοι μπορούσαν να ανταλλάσουν qubits, τότε θα χρειαζόταν μόνο μια επικοινωνία (μια αποστολή και μια απάντηση)! Ας δούμε πώς ακριβώς γίνεται αυτό :

Κατ' αναλογία με τον αλγόριθμο του Deutsch, η Alice πρέπει να διαθέτει n qubits για να καταχωρήσει εκεί τον αριθμό που επέλεξε και ένα qubit για να καταχωρηθεί εκεί η απάντηση του Bob. Το κύκλωμα του αλγόριθμου φαίνεται στο Σχήμα 5-5.



Σχήμα 5-5 : Κύκλωμα που περιγράφει τον αλγόριθμο Deutsch-Jozsa

Συνοπτικά η διαδικασία είναι η εξής :

πρώτα η Alice καταχωρεί τον αριθμό x που επέλεξε στα πάνω n qubits και το τελευταίο κάτω το ετοιμάζει στην κατάσταση $|1\rangle$. Η καταχώρηση γίνεται αντιστοιχώντας κάθε έναν απ' τους 2^n πιθανούς αριθμούς x σε ένα απ' τα 2^n βασικά διανύσματα του συστήματος των n qubits. Δηλαδή αν n=2 τότε οι δυνατές τιμές του x είναι x=0,1,2,3 (2^2=4 το πλήθος). Σε αυτή την περίπτωση τα βασικά διανύσματα του συστήματος των 2 qubits είναι τα $|00\rangle$, $|01\rangle, |10\rangle$ και $|11\rangle$. Έτσι η αντιστοιχία είναι η : $0 \to 00,\ 1 \to 01,\ 2 \to 10,\ 3 \to 11$ δηλαδή στην ουσία ο αριθμός x μετατρέπεται στο δυαδικό σύστημα. Στη συνέχεια η Alice

μετατρέπει όλα τα qubits σε κατάσταση επαλληλίας χρησιμοποιώντας φυσικά πύλες Hadamard. Μετά τα στέλνει όλα αυτά στον Bob ο οποίος εφαρμόζει τον μετασχηματισμό U_f δηλαδή στην ουσία υπολογίζει το f(x) χρησιμοποιώντας κβαντικό παραλληλισμό και αποθηκεύει το αποτέλεσμα στο τελευταίο qubit. Στη συνέχεια ο Bob τα ξαναστέλνει αυτά πίσω στην Alice η οποία τα μετατρέπει πάλι σε κατάσταση επαλληλίας χρησιμοποιώντας πύλες Hadamard στα n qubits που είχε αποθηκεύσει τον αριθμό x και στη συνέχεια πραγματοποιεί μέτρηση σε αυτά απ' την οποία διαπιστώνει αν τελικά η f είναι σταθερή ή ισοζυγισμένη.

Ας τα δούμε όλα αυτά βήμα-βήμα :

Έστω ότι η Alice διαλέγει τον αριθμό 0 (00…0). Τότε θα ετοιμάσει όλα τα πάνω n qubits στην κατάσταση $|0\rangle$. Αυτή είναι και η περίπτωση που έχει σχεδιαστεί στο Σχήμα 5-5. Σε αυτήν την περίπτωση η αρχική κατάσταση θα είναι η $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$.

Μετά την επίδραση των πυλών Hadamard στα πρώτα n qubits στηριζόμενοι στην εξίσωση (5-3) έχουμε την κατάσταση $\sum_x \frac{|x\rangle}{\sqrt{2^n}}$ όπου x είναι η κάθε δυνατή τιμή συνδυασμού βασικών καταστάσεων των qubits, ενώ με τη δράση της πύλης Hadamard στο τελευταίο qubit που βρίσκεται αρχικά στην κατάσταση $|1\rangle$ προκύπτει γι' αυτό η κατάσταση $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ κατά τα γνωστά. Έτσι η κατάσταση $|\psi_1\rangle$ είναι η :

$$|\psi_1\rangle = \sum_x \frac{|x\rangle}{\sqrt{2^n}} [\frac{|0\rangle - |1\rangle}{\sqrt{2}}] \qquad \textbf{(5-10)}$$

Στη συνέχεια το σύστημα πηγαίνει στον Bob ο οποίος δρα με την πύλη U_f :

$$|x, y\rangle \rightarrow |x, x \oplus f(x)\rangle$$

και έτσι χρησιμοποιώντας τη σχέση (5-4) έχουμε :

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} [\frac{|0\rangle - |1\rangle}{\sqrt{2}}] \qquad \textbf{(5-11)}$$

Το σύστημα τώρα επιστρέφει στην Alice η οποία δρα στα πρώτα n qubits πάλι πύλες Hadamard. Για να απεικονίσουμε το αποτέλεσμα της δράσης αυτής σε σχέση, γράφουμε

πρώτα τη δράση της πύλης Hadamard για τις δύο βασικές καταστάσεις ενός qubit που είναι οι γνωστές :

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ και } H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad \textbf{(5-12)}$$

και παρατηρούμε ότι μπορούν να γραφούν στη συμπαγή μορφή :

$$H|x\rangle = \frac{\sum_z (-1)^{xz}|z\rangle}{\sqrt{2}} \quad \textbf{(5-13)}$$

Αυτή η μορφή είναι βολική γιατί μπορεί εύκολα να γενικευτεί στην περίπτωση παράλληλης δράσης πυλών Hadamard σε n qubits :

$$H^{\otimes n}|x_1, x_2, ..., x_n\rangle = \frac{\sum_{z_1, z_2, ..., z_n} (-1)^{x_1 z_1 + x_2 z_2 + ... + x_n z_n}|z_1, z_2, ..., z_n\rangle}{\sqrt{2^n}} \quad \textbf{(5-14)}$$

και αν ορίσουμε $x \cdot z = x_1 z_1 + x_2 z_2 + ... + x_n z_n$ ένα είδος εσωτερικού γινομένου όπου $x=(x_1,x_2,\ldots,x_n)$ και $z=(z_1,z_2,\ldots,z_n)$, η σχέση θα πάρει την πολύ απλούστερη και βολικότερη μορφή :

$$H^{\otimes n}|x\rangle = \frac{\sum_z (-1)^{x \cdot z}|z\rangle}{\sqrt{2^n}} \quad \textbf{(5-15)}$$

Με βάση αυτή τη σχέση η κατάσταση $|\psi_3\rangle$ θα είναι η :

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)}|z\rangle}{2^n} [\frac{|0\rangle - |1\rangle}{\sqrt{2}}] \quad \textbf{(5-16)}$$

Στη συνέχεια η Alice μετρά τα πρώτα n qubits. Από τη μορφή της κατάστασης $|\psi_3\rangle$ παρατηρούμε ότι το πλάτος πιθανότητας να μετρηθούν όλα τα n qubits στην κατάσταση $|0\rangle$ είναι $\sum_x \frac{(-1)^{f(x)}}{2^n}$. Άρα αν η f(x) είναι σταθερή με τιμή f(x)=0 το πλάτος πιθανότητας θα είναι 1, ενώ αν η f(x) είναι σταθερή με τιμή f(x)=1 το πλάτος πιθανότητας θα είναι -1. Άρα και στις δύο περιπτώσεις η μέτρηση θα οδηγήσει με βεβαιότητα σε αυτό το αποτέλεσμα δηλαδή όλα τα qubits να είναι στην κατάσταση $|0\rangle$. Αν τώρα η f(x) είναι ισοζυγισμένη, τότε αφού οι τιμές του x για τις οποίες είναι f(x)=0 είναι ίσες με αυτές για τις οποίες είναι f(x)=1, το άθροισμα στον αριθμητή του πλάτους πιθανότητας θα έχει

ίσους όρους 1 και -1 και άρα θα είναι 0. Δηλαδή θα αποκλείεται το ενδεχόμενο η μέτρηση να δώσει όλα τα n qubits στην κατάσταση $|0\rangle$. Έτσι αν η Alice μετρήσει όλα τα n qubits στην κατάσταση $|0\rangle$ αυτό θα σημαίνει ότι η συνάρτηση f(x) είναι σταθερή αλλιώς είναι ισοζυγισμένη.

Δείξαμε λοιπόν ότι ένας κβαντικός υπολογιστής μπορεί να λύσει το πρόβλημα του Deutsch κάνοντας μόνο έναν υπολογισμό της συνάρτησης f σε αντίθεση με έναν κλασικό ο οποίος θα απαιτούσε έως και $\frac{2^n}{2}+1$ υπολογισμούς. Αυτό όμως που εκ πρώτης όψεως φαίνεται εντυπωσιακό έχει και ορισμένες αδυναμίες. Κατ' αρχήν αυτό το πρόβλημα δεν μπορεί να χαρακτηριστεί ιδιαίτερα σημαντικό αφού έως σήμερα δεν υπάρχουν γνωστές εφαρμογές όπου θα μπορούσε να χρησιμοποιηθεί. Δεύτερον στην ουσία δεν μπορεί να γίνει σύγκριση της λύσης του με αυτή ενός κλασικού υπολογιστή αφού η μέθοδος που χρησιμοποιείται σε αυτόν είναι τελείως διαφορετική. Τρίτον, αν ο κλασικός υπολογιστής ήταν πιθανοκρατικός, τότε αν ο Bob υπολόγιζε το f(x) για μερικές τυχαίες τιμές του x θα μπορούσε η Alice γρήγορα να προσδιορίσει αν η f ήταν σταθερή ή ισοζυγισμένη. Παρόλα αυτά ο αλγόριθμος Deutsch-Jozsa κάθε άλλο παρά ασήμαντος μπορεί να χαρακτηριστεί αφού θα μπορούσε να είναι η βάση για άλλους κβαντικούς αλγόριθμους και επίσης να βοηθήσει στην βαθύτερη κατανόηση των θεμελιωδών αρχών που κρύβονται στην κβαντική υπολογιστική.

5.5 Είδη κβαντικών αλγορίθμων

Οι κβαντικοί αλγόριθμοι οι οποίοι μπορούν δυνητικά να έχουν πλεονεκτήματα σε σχέση με τους αντίστοιχους γνωστούς κλασικούς, μπορούν να χωριστούν γενικά σε τρείς κατηγορίες. Αυτές είναι : οι αλγόριθμοι που βασίζονται στο μετασχηματισμό Fourier, οι αλγόριθμοι κβαντικής αναζήτησης και οι αλγόριθμοι προσομοίωσης. Ας δούμε τα γενικά χαρακτηριστικά της κάθε κατηγορίας και μερικά παραδείγματα.

5.5.1 **Αλγόριθμοι που βασίζονται στο μετασχηματισμό Fourier**

Ο διακριτός μετασχηματισμός Fourier συνήθως ορίζεται ως ένας μετασχηματισμός μιας ομάδας των N μιγαδικών αριθμών $x_0, x_1,\ldots,x_{N-1}$ σε μια ομάδα από άλλους N μιγαδικούς αριθμούς τους $y_0, y_1,\ldots,y_{N-1}$ με βάση τη σχέση :

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} x_j \qquad \textbf{(5-17)}$$

Όπως είναι γνωστό ο μετασχηματισμός Fourier χρησιμοποιείται σε πάμπολλες εφαρμογές της επιστήμης διότι το μετασχηματισμένο πρόβλημα είναι πολλές φορές πιο εύκολο να λυθεί από το αρχικό.

Ο μετασχηματισμός Fourier είναι τόσο χρήσιμος που έχουν αναπτυχθεί διάφορες θεωρίες γενίκευσης της μορφής του που ορίζεται απ' την παραπάνω σχέση. Αυτές οι θεωρίες βασίζονται σε ορισμένες αρχές από τη θεωρία πεπερασμένων ομάδων. Μια τέτοια περίπτωση είναι και ο μετασχηματισμός Hadamard που χρησιμοποιείται στον αλγόριθμο Deutsch-Jozsa όπως είδαμε. Όπως θα δούμε και άλλοι σημαντικοί κβαντικοί αλγόριθμοι επίσης χρησιμοποιούν κάποια μορφή του μετασχηματισμού Fourier. Δύο τέτοια παραδείγματα είναι οι δύο θεωρούμενοι πιο σημαντικοί αλγόριθμοι απ' αυτούς που υπάρχουν σήμερα, οι γνωστοί ως αλγόριθμοι του Shor για τα προβλήματα της παραγοντοποίησης και του διακριτού λογαρίθμου. Η εξίσωση (5-17) στη μορφή που είναι γραμμένη δεν θυμίζει και πολύ τον κβαντικό της χαρακτήρα. Γι' αυτό ας υποθέσουμε ότι ορίζουμε ένα γραμμικό μετασχηματισμό U πάνω σε n qubits του οποίου η δράση στις βασικές καταστάσεις $|j\rangle$ με $0 \le j \le 2^n - 1$, περιγράφεται απ' την εξίσωση :

$$|j\rangle \to \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle \qquad \textbf{(5-18)}$$

Αποδεικνύεται ότι αυτός ο μετασχηματισμός είναι μοναδιαίος άρα μπορεί να πραγματοποιηθεί από ένα κβαντικό κύκλωμα. Η δράση του μετασχηματισμού αυτού σε μια κατάσταση υπέρθεσης είναι :

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \to \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} [\sum_{j=0}^{2^n-1} e^{2\pi ijk/2^n} x_j] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle \qquad \textbf{(5-19)}$$

όπου :

$$y_k = \frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} e^{2\pi ijk/2^n} x_j \qquad \textbf{(5-20)}$$

Παρατηρούμε ότι η (5-19) αντιστοιχεί σε ένα διανυσματικό συμβολισμό της σχέσης (5-17) του μετασχηματισμού Fourier για $N=2^n$.

Όσον αφορά την ταχύτητα που μπορεί να πραγματοποιηθεί ο μετασχηματισμός Fourier, κλασικά απαιτούνται περίπου $N\log(N)=n2^n$ βήματα για να μετασχηματιστούν $N=2^n$ αριθμοί ενώ σε έναν κβαντικό υπολογιστή ο μετασχηματισμός μπορεί να πραγματοποιηθεί με περίπου $\log^2(N)=n^2$ βήματα, δηλαδή μια εκθετική οικονομία! Το αποτέλεσμα αυτό φαίνεται να δείχνει ότι οι κβαντικοί υπολογιστές μπορούν να μετασχηματίσουν πολύ γρήγορα 2^n μιγαδικούς αριθμούς κάτι που θα ήταν εξαιρετικά χρήσιμο σε ένα μεγάλο εύρος εφαρμογών. Βέβαια δεν είναι ακριβώς έτσι τα πράγματα. Ο μετασχηματισμός Fourier βρίσκεται στην πληροφορία που κρύβεται στα πλάτη της κβαντικής κατάστασης και αυτή η πληροφορία όπως έχει αναφερθεί αρκετές φορές δεν είναι άμεσα προσβάσιμη από τη μέτρηση αφού αυτή θα οδηγήσει κάθε qubit είτε στην κατάσταση $|0\rangle$ είτε στην κατάσταση $|1\rangle$ κάτι που μας εμποδίζει να μάθουμε απ' ευθείας το αποτέλεσμα y_k του μετασχηματισμού. Άρα λοιπόν απαιτείται περισσότερη ευφυΐα προκειμένου να τιθασεύσουμε την ισχύ αυτού του μετασχηματισμού. Ευτυχώς έχει καταστεί δυνατό να χρησιμοποιηθεί ο κβαντικός μετασχηματισμός Fourier για την αποτελεσματική λύση διαφόρων προβλημάτων τα οποία θεωρούνται ότι δεν έχουν τέτοια λύση σε κλασικούς υπολογιστές όπως το πρόβλημα του Deutsch και οι αλγόριθμοι του Shor για παραγοντοποίηση και το πρόβλημα του διακριτού λογαρίθμου.

5.5.2 **Αλγόριθμοι κβαντικής έρευνας**

Αυτή είναι μια τελείως διαφορετική κατηγορία κβαντικών αλγορίθμων της οποίας οι βασικές αρχές ανακαλύφθηκαν απ' τον Grover. Οι αλγόριθμοι κβαντικής έρευνας φιλοδοξούν να λύσουν το ακόλουθο πρόβλημα :

Από μια βάση δεδομένων N στοιχείων χωρίς προγενέστερη γνώση για το περιεχόμενο τους, θέλουμε να εντοπίσουμε ένα στοιχείο το οποίο έχει μια συγκεκριμένη ιδιότητα.

Κλασικά αυτό το πρόβλημα απαιτεί έως και N προσπάθειες (βήματα), ενώ χρησιμοποιώντας κβαντικό αλγόριθμο απαιτούνται περίπου $\sqrt{N}$ βήματα. Η μείωση των

βημάτων άρα δεν είναι το ίδιο εντυπωσιακή με αυτήν που επιτυγχάνεται με τους αλγορίθμους Fourier. Παρόλα αυτά οι αλγόριθμοι κβαντικής έρευνας θεωρούνται εξαιρετικού ενδιαφέροντος διότι θα μπορούσαν να χρησιμοποιηθούν σε πολύ μεγαλύτερο εύρος εφαρμογών από τους μετασχηματισμούς Fourier. Ο πιο σημαντικός αντιπρόσωπος αυτής της κατηγορίας είναι ο κβαντικός αλγόριθμος του Grover ο οποίος περιγράφεται παρακάτω.

5.5.3 **Κβαντικός Αλγόριθμος του Grover**

Ας δούμε ένα πρόβλημα της κατηγορίας που προσπαθεί να λύσει αυτός ο αλγόριθμος :

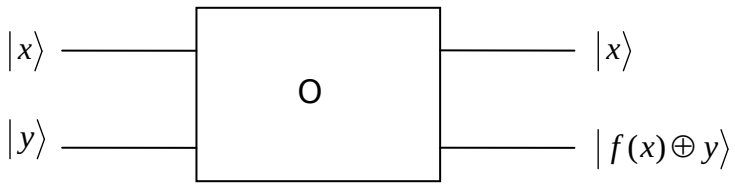
Έστω ότι έχουμε ένα τηλεφωνικό κατάλογο ο οποίος ως γνωστό έχει τους αριθμούς με βάση την αλφαβητική σειρά των ονομάτων. Είναι δομημένος δηλαδή με βάση τα ονόματα οπότε μπορεί κάποιος να βρει εύκολα τον αριθμό αν γνωρίζει το όνομα. Αν όμως κάποιος γνωρίζει τον αριθμό και ψάχνει να βρει το όνομα στο οποίο αντιστοιχεί, τότε αυτό είναι πάρα πολύ δύσκολο. Αυτό το πρόβλημα καλείται να λύσει ο κβαντικός αλγόριθμος του Grover και μάλιστα πιο γρήγορα από έναν κλασικό αλγόριθμο.

Για να λύσει αυτό το πρόβλημα ο κλασικός υπολογιστής, θα έπρεπε να έχει έναν καταχωρητή με δύο bit όπου στο ένα θα είχε καταχωρηθεί ο γνωστός αριθμός και στο άλλο θα εισάγονταν κάθε φορά ένας αριθμός από τον κατάλογο με το αντίστοιχο όνομα και εάν οι αριθμοί ήταν ίσοι, τότε θα σταματούσε η αναζήτηση ενώ αν δεν ήταν, θα προχωρούσε στον επόμενο αριθμό του καταλόγου μέχρι να βρει το ζητούμενο. Άρα αν οι αριθμοί του καταλόγου ήταν N, τότε το επιθυμητό αποτέλεσμα της διαδικασίας θα ερχόταν στην καλύτερη περίπτωση μετά από 1 προσπάθεια και στη χειρότερη μετά από N. Ο μέσος όρος δηλαδή N/2 προσπάθειες. Όπως αναφέρθηκε ο κβαντικός αλγόριθμος του Grover υπόσχεται ότι η διαδικασία μπορεί να γίνει με μόνο $\sqrt{N}$ προσπάθειες. Αυτό σημαίνει ότι αν ο κατάλογος περιέχει 1000000 αριθμούς, ο κλασικός υπολογιστής θα πρέπει να κάνει 500000 κατά μέσο όρο προσπάθειες ενώ ο κβαντικός με τον αλγόριθμο του Grover μόνο 1000!

Ας περιγράψουμε τώρα τον αλγόριθμο :

Έστω ότι η βάση δεδομένων που θέλουμε να μελετήσουμε έχει N στοιχεία τα οποία αριθμούμε από 0 έως N-1. Έστω ακόμα ότι υπάρχει η δυνατότητα ο υπολογιστής που θα τρέξει τον αλγόριθμο, να αναγνωρίζει αν ένας αριθμός είναι αυτός που ψάχνουμε ή όχι. Σε

αυτή τη φάση δεν μας ενδιαφέρει πώς γίνεται αυτό, αλλά θεωρούμε ότι στον υπολογιστή υπάρχει ένα μαύρο κουτί στο οποίο αν εισαχθεί ένα στοιχείο της βάσης δεδομένων, αυτό μπορεί να ελέγξει αν αυτό είναι το ζητούμενο στοιχείο. Αυτό το κουτί στη βιβλιογραφία ονομάζεται «oracle» του οποίου η μετάφραση στα Ελληνικά είναι «μάντης». Η λέξη αυτή όμως δεν αντιπροσωπεύει σχεδόν καθόλου αυτό που κάνει το μαύρο κουτί, άρα θα χρησιμοποιείται ο Αγγλικός όρος. Η λειτουργία του oracle μπορεί να περιγραφεί σαν μια συνάρτηση f(x) με πεδίο ορισμού τα στοιχεία x (N το πλήθος) της βάσης δεδομένων και σύνολο τιμών το {0,1}. Συγκεκριμένα αν στο oracle εισαχθεί η τιμή που ψάχνουμε έστω η x_i, τότε είναι $f(x)=f(x_i)=1$. Για κάθε άλλο $x\neq x_i$ θα είναι $f(x)=0$. Για να εισαχθούν οι N αριθμοί σε ένα κβαντικό καταχωρητή, αυτός θα πρέπει να περιέχει n qubits όπου $N=2^n$, n=1,2,3,…δηλαδή για να αποθηκευτούν 8 αριθμοί (N=8) απαιτούνται n=3 qubits ($2^3=8$). Πράγματι για παράδειγμα για ένα σύστημα τριών qubits, οι βασικές καταστάσεις είναι οι $|000\rangle,|001\rangle,|010\rangle,|011\rangle,|100\rangle,|101\rangle,|110\rangle,|111\rangle$ που είναι 8 το πλήθος. Δηλαδή μπορούμε να αντιστοιχήσουμε κάθε στοιχείο της βάσης δεδομένων με μια βασική κατάσταση των qubits όπως έγινε και στον αλγόριθμο Deutsch-Jozsa . Το κβαντικό oracle έστω O σχηματικά φαίνεται στο Σχήμα 5-6.



Σχήμα 5-6 : Λειτουργία του κβαντικού oracle

Στο σχήμα οι πάνω γραμμές δεν αντιπροσωπεύουν 1 αλλά n qubits, τα οποία όπως αναφέρθηκε έχουν $N=2^n$ βασικές καταστάσεις σε κάθε μια από τις οποίες αντιστοιχίζεται ένα στοιχείο της βάσης δεδομένων. Το qubit που βρίσκεται στην κάτω σειρά δηλαδή το $|y\rangle$, λέγεται qubit του oracle. Η δράση του oracle μπορεί να περιγραφεί με την αντιστοιχία :

$$|x\rangle|y\rangle \xrightarrow{O} |x\rangle|f(x)\oplus y\rangle$$

Ας δούμε τώρα τη λειτουργία του αλγόριθμου στο πρόβλημα μας. Αρχικά θέτουμε τα πάνω n qubits στη βασική κατάσταση $|x\rangle$ που όπως είπαμε αντιστοιχεί σε ένα στοιχείο της

βάσης δεδομένων και το qubit του oracle στη βασική κατάσταση $|1\rangle$.Στο τελευταίο δρούμε μια κβαντική πύλη Hadamard. Τότε το qubit του oracle μεταβαίνει στην κατάσταση $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ και άρα η συνολική κατάσταση είναι η $|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Αν τώρα δράσει σε αυτά το oracle θα έχουμε :

$$|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}\xrightarrow{O}|x\rangle\left|f(x)\oplus\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\rangle=|x\rangle\frac{|f(x)\oplus 0\rangle-|f(x)\oplus 1\rangle}{\sqrt{2}} \quad \textbf{(5-21)}$$

Αν τώρα το x είναι το στοιχείο που αναζητούμε, τότε θα είναι f(x)=1 άρα θα έχουμε :

$$|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}\xrightarrow{O}|x\rangle\frac{|1\oplus 0\rangle-|1\oplus 1\rangle}{\sqrt{2}}=|x\rangle\frac{|1\rangle-|0\rangle}{\sqrt{2}}=-|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \quad \textbf{(5-22)}$$

Αν δε, το x δεν είναι το στοιχείο που αναζητούμε, τότε θα είναι f(x)=0 και άρα θα έχουμε:

$$|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}\xrightarrow{O}|x\rangle\frac{|0\oplus 0\rangle-|0\oplus 1\rangle}{\sqrt{2}}=|x\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}} \quad \textbf{(5-23)}$$

Δηλαδή παρατηρούμε ότι και στις δύο περιπτώσεις το qubit του oracle μένει στην κατάσταση που ήταν, ενώ τα qubits που ήταν στην κατάσταση $|x\rangle$ αντιστρέφονται αν το x είναι το στοιχείο που ψάχνουμε ενώ αλλιώς μένουν και αυτά απαράλλαχτα. Όλη αυτή η διαδικασία μπορεί να περιγραφεί με την πιο συμπαγή αντιστοιχία :

$$|x\rangle\xrightarrow{O}(-1)^{f(x)}|x\rangle \quad \textbf{(5-24)}$$

όπου το qubit του oracle έχει παραληφθεί αφού η κατάστασή του δεν αλλάζει σε καμία περίπτωση.

Μπορεί εύκολα να δειχτεί ότι η δράση του oracle μπορεί να περιγραφεί από τον τελεστή $\hat{O}=\hat{I}-2|x_i\rangle\langle x_i|$, όπου x_i είναι το στοιχείο της βάσης που αντιστοιχεί στον αριθμό που αναζητούμε και $\hat{I}$ είναι ο τελεστής που αντιστοιχεί στην κβαντική πύλη αδράνειας η δράση της οποίας αφήνει ένα qubit στην κατάσταση που ήταν. Πράγματι αν δράσουμε τον τελεστή $\hat{O}$ πάνω στην τυχαία κατάσταση $|x_j\rangle$ θα έχουμε:

$$\hat{O}|x_j\rangle=\hat{I}|x_j\rangle-2|x_i\rangle\langle x_i||x_j\rangle=|x_j\rangle-2\delta_{ij}|x_i\rangle \quad \textbf{(5-25)}$$

αφού $\langle x_i || x_j \rangle = \delta_{ij}$ λόγω κανονικοποίησης. Αν τώρα το x_j είναι το στοιχείο που ψάχνουμε δηλαδή i=j θα είναι $\delta_{ij}=1$ και άρα η σχέση (5-25) δίνει $\hat{O}|x_j\rangle = -|x_j\rangle$ ενώ αν i≠j τότε $\delta_{ij}=0$ και άρα απ' την ίδια σχέση έχουμε $\hat{O}|x_j\rangle = |x_j\rangle$.

Έστω τώρα ότι θέτουμε τα n πάνω qubits όχι σε μια βασική τους κατάσταση $|x\rangle$ αλλά σε μια επαλληλία βασικών καταστάσεων δηλαδή σε μια κατάσταση της μορφής :

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |x_j\rangle \qquad \textbf{(5-26)}$$

Αυτή η κατάσταση μπορεί να δημιουργηθεί θέτοντας τα n qubits αρχικά όλα στην κατάσταση $|0\rangle$ και στη συνέχεια δρώντας σε όλα παράλληλα από μια πύλη Hadamard δηλαδή $|s\rangle = H^{\otimes n}|0\rangle$. Ορίζεται τότε ένας τελεστής ο $\hat{G}$,κατ' αναλογία με τον $\hat{O}$, σύμφωνα με τη σχέση :

$$\hat{G} = 2|s\rangle\langle s| - \hat{I} \qquad \textbf{(5-27)}$$

Ο αλγόριθμος του Grover απαιτεί τη διαδοχική δράση στην κατάσταση $|s\rangle$ των τελεστών $\hat{O}$ και $\hat{G}$. Ας δούμε τα αποτελέσματα αυτών των δράσεων. Είναι :

$$|s'\rangle = \hat{O}|s\rangle = \frac{1}{\sqrt{N}} \hat{O} \sum_{j=0}^{N-1} |x_j\rangle = \frac{1}{\sqrt{N}} \hat{O}(|x_0\rangle + |x_1\rangle + ... + |x_i\rangle + ... |x_{N-1}\rangle)$$

$$= \frac{1}{\sqrt{N}} (|x_0\rangle + |x_1\rangle + ... - |x_i\rangle + ... |x_{N-1}\rangle) = \sum_{j=0}^{N-1} a_j |x_j\rangle \text{ με } a_j = \frac{1}{\sqrt{N}} \text{ για j≠i}$$

και $a_j = -\frac{1}{\sqrt{N}}$ για j=i.

Δηλαδή η δράση του τελεστή $\hat{O}$ προκαλεί την αλλαγή του πρόσημου του πλάτους μόνο της κατάστασης $|x_i\rangle$ που αντιστοιχεί στο στοιχείο που αναζητούμε.

Για τη δράση του τελεστή $\hat{G}$ στην κατάσταση $|s'\rangle$ έχουμε :

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

Είναι τώρα :

$$\langle s|s'\rangle = \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1} a_j \langle x_k|x_j\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} a_j$$

αφού $\langle x_k|x_j\rangle = \delta_{kj}$. Αν τώρα θέσουμε $\langle\alpha\rangle = \frac{1}{\mathrm{N}}\sum_{j=0}^{N-1} a_j$ τη μέση τιμή των πλατών πιθανότητας, τότε έχουμε $\langle s|s'\rangle = \sqrt{N}\langle\alpha\rangle$ άρα έχουμε :

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

Άρα παρατηρούμε ότι η δράση του τελεστή $\hat{G}$ προκαλεί μια σύνθετη κατάσταση στην οποία οι βασικές καταστάσεις $|x_j\rangle$ έχουν πλάτη πιθανότητας $2\langle a\rangle - a_j$. Είδαμε όμως ότι στην κατάσταση $|s'\rangle$ όλα τα πλάτη είναι $a_j = \frac{1}{\sqrt{\mathrm{N}}}$ (αν j≠i) εκτός από ένα που είναι $-\frac{1}{\sqrt{\mathrm{N}}}$ (αν i=j) άρα η μέση τιμή τους είναι περίπου $\langle a\rangle \simeq \frac{1}{\sqrt{N}}$. Έτσι για τις βασικές καταστάσεις $|x_j\rangle$ με j≠i το πλάτος είναι περίπου :

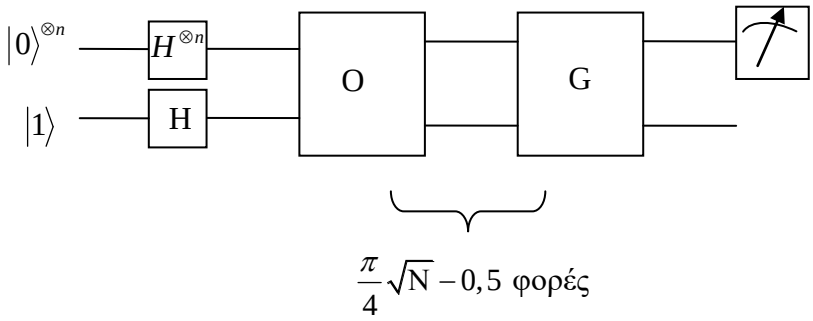
$$2\langle a\rangle - a_j = \frac{2}{\sqrt{\mathrm{N}}} - \frac{1}{\sqrt{\mathrm{N}}} \simeq \frac{1}{\sqrt{\mathrm{N}}}$$

δηλαδή σχεδόν (λίγο μικρότερο) όσο ήταν αρχικά, ενώ για τη βασική κατάσταση $|x_i\rangle$ που αντιστοιχεί στο στοιχείο που ψάχνουμε, είναι :

$$2\langle a\rangle - a_j = \frac{2}{\sqrt{\mathrm{N}}} + \frac{1}{\sqrt{\mathrm{N}}} \simeq \frac{3}{\sqrt{\mathrm{N}}}$$

δηλαδή τριπλάσιο από ότι ήταν. Δηλαδή με τη δράση $|s''\rangle = \hat{G}\hat{O}|s\rangle$ φτάσαμε σε μια κατάσταση η μέτρηση της οποίας έχει εννεαπλάσια πιθανότητα να έχει σαν αποτέλεσμα το ζητούμενο αριθμό σε σχέση με κάποιον άλλο. Βέβαια αυτό δεν είναι αρκετό. Όμως με την ίδια λογική αν επαναληφθεί αυτή η διαδικασία, η πιθανότητα να μετρηθεί ο ζητούμενος αριθμός θα είναι ακόμα μεγαλύτερη. Αποδεικνύεται (Nielsen & Chuang σελ 254) ότι αν η διαδικασία επαναληφθεί περίπου $\frac{\pi}{4}\sqrt{\mathrm{N}} - 0{,}5$ φορές, τότε μια μέτρηση στα n πρώτα qubits της διάταξης θα δώσει σχεδόν με βεβαιότητα το επιθυμητό αποτέλεσμα.

Το κύκλωμα του αλγόριθμου Grover φαίνεται σχηματικά στο Σχήμα 5-7.



Σχήμα 5-7 : Κύκλωμα του αλγόριθμου Grover

Παράδειγμα εφαρμογής αλγόριθμου Grover

Για την καλύτερη κατανόηση του αλγορίθμου Grover θα εφαρμόσουμε τα βήματά του, σε μια συγκεκριμένη περίπτωση που η βάση δεδομένων έχει N=8 στοιχεία. Τότε χρειαζόμαστε κβαντικό καταχωρητή με n=3 qubits αφού 2^3=8. Πράγματι, όπως έχει προαναφερθεί το σύστημα των 3 qubits έχει 8 βασικές καταστάσεις τις $|000\rangle$, $|001\rangle$, $|010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle$. Αντιστοιχίζουμε κάθε μια απ' αυτές σε ένα στοιχείο της βάσης δεδομένων και έστω ότι αυτό που αναζητούμε είναι αυτό που αντιστοιχεί στη βασική κατάσταση $|100\rangle$. Τα βήματα που πρέπει να γίνουν είναι με βάση τη γενική περιγραφή που προηγήθηκε, τα εξής :

Θέτουμε τα 3 qubits στην βασική κατάσταση $|000\rangle$ και δρούμε σε κάθε ένα απ' αυτά μια κβαντική πύλη Hadamard. Έτσι η κατάσταση τους γίνεται η επαλληλία με ίσα βάρη όλων των βασικών καταστάσεων δηλαδή η :

$$|s\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle) \quad \textbf{(5-28)}$$

Στη συνέχεια με τα qubits στην κατάσταση $|s\rangle$ εφαρμόζουμε τον τελεστή $\hat{O} = \hat{I} - 2|100\rangle\langle 100|$ (το oracle) και έχουμε την κατάσταση :

$$|s'\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle - |100\rangle + |101\rangle + |110\rangle + |111\rangle) \quad \textbf{(5-29)}$$

Μετά δρούμε στην κατάσταση $|s'\rangle$ τον τελεστή $\hat{G} = 2|s\rangle\langle s| - \hat{I}$ και καταλήγουμε στην κατάσταση:

$$|s''\rangle = \frac{1}{\sqrt{32}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |101\rangle + |110\rangle + |111\rangle) + \frac{5}{\sqrt{32}}|100\rangle \quad \textbf{(5-30)}$$

Να παρατηρήσουμε ότι αυτό είναι το ακριβές αποτέλεσμα και όχι το προσεγγιστικό που εξάχθηκε στη γενική περιγραφή. Η διαδικασία για την εξαγωγή του παραπάνω αποτελέσματος είναι σχετικά εύκολη αλλά απαιτεί αρκετές πράξεις κατά τις οποίες πρώτα υπολογίζονται οι πίνακες που αντιστοιχούν στους τελεστές $\hat{O}$ και $\hat{G}$ (Καραφυλλίδης Ι. σελ. 104) οι οποίοι είναι οι :

$$\hat{O} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \text{ και } \hat{G} = \frac{1}{4}\begin{pmatrix} -3 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -3 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -3 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -3 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & -3 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & -3 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & -3 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & -3 \end{pmatrix}$$

Παρατηρούμε λοιπόν ότι αν γίνει τώρα μέτρηση των 3 qubits αυτή θα δώσει το επιθυμητό αποτέλεσμα $|100\rangle$ με πιθανότητα :

$$\left|\frac{5}{\sqrt{32}}\right|^2 \simeq 0,78125 \text{ ή } 78\%$$

ενώ η πιθανότητα για κάθε ένα από τα άλλα αποτελέσματα είναι :

$$\left|\frac{1}{\sqrt{32}}\right|^2 \simeq 0,03125 \text{ ή } 3\%$$

Είναι φανερό ότι πλησιάσαμε το στόχο μας. Σύμφωνα με τα προηγούμενα, για να μετρήσουμε σχεδόν με βεβαιότητα το επιθυμητό, θα πρέπει να επαναλάβουμε τη διαδικασία περίπου $\frac{\pi}{4}\sqrt{N} - 0,5$ φορές που για N=8 δίνει περίπου 2 φορές.

Πράγματι αν επαναλάβουμε τη διαδικασία άλλη μια φορά τότε θα καταλήξουμε στην κατάσταση $|s'''\rangle = \hat{G}\hat{O}|s''\rangle$ η οποία μετά από ανάλογες πράξεις προκύπτει ότι είναι η :

$$|s'''\rangle = -\frac{1}{4\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle + |101\rangle + |110\rangle + |111\rangle) + \frac{11}{4\sqrt{8}}|100\rangle \qquad \textbf{(5-31)}$$

Αν τώρα γίνει μέτρηση αυτή θα δώσει την κατάσταση $|100\rangle$ με πιθανότητα :

$$\left|\frac{11}{4\sqrt{8}}\right|^2 \simeq 0,94 \text{ ή } 94\%$$

ενώ η πιθανότητα για κάθε ένα από τα άλλα αποτελέσματα είναι :

$$\left|-\frac{1}{4\sqrt{8}}\right|^2 \simeq 0,0078 \text{ ή } 0,78\%$$

5.6 Κβαντική Προσομοίωση

Η επιχείρηση προσομοίωσης ενός κβαντικού συστήματος από ένα κβαντικό υπολογιστή είναι ένα εγχείρημα το οποίο είναι λογικά αναμενόμενο να έχει άριστα αποτελέσματα, κάτι το οποίο θεωρείται ότι είναι δύσκολο να γίνει έστω και σε μικρότερο βαθμό από έναν κλασικό υπολογιστή. Οι κλασικοί υπολογιστές έχουν δυσκολία να προσομοιώσουν κβαντικά συστήματα. Ο λόγος είναι ότι ο αριθμός των μιγαδικών αριθμών που απαιτείται για να γίνει αυτό, γενικά αυξάνεται εκθετικά με το μέγεθος του συστήματος σε αντίθεση με τη γραμμική αύξηση που υπάρχει στα κβαντικά συστήματα. Συγκεκριμένα για να αποθηκευτεί στη μνήμη μια κβαντική κατάσταση n διακριτών συνιστωσών, απαιτούνται c^n bits μνήμης κλασικού υπολογιστή όπου c είναι μια σταθερά που εξαρτάται από τις λεπτομέρειες του συστήματος που προσομοιώνεται και την επιθυμητή ακρίβεια της προσομοίωσης. Αντίθετα ένας κβαντικός υπολογιστής μπορεί να προσομοιώσει το σύστημα χρησιμοποιώντας kn qubits, όπου k είναι πάλι μια σταθερά που εξαρτάται από της λεπτομέρειες του συστήματος που προσομοιώνεται. Αυτό επιτρέπει σε ένα κβαντικό υπολογιστή να προσομοιώσει ένα κβαντικό σύστημα αποτελεσματικά κάτι που δε θεωρείται ότι μπορεί να γίνει από ένα κλασικό.

Υπάρχει όμως και μια αδυναμία σε όλο αυτό την οποία και έχουμε δει σε αρκετές περιπτώσεις. Αυτή είναι ότι ακόμα και αν ένα κβαντικό σύστημα μπορεί να προσομοιωθεί αποτελεσματικά από έναν κβαντικό υπολογιστή, αυτό δεν σημαίνει ότι μπορεί να εξαχθεί και η επιθυμητή πληροφορία από το σύστημα. Και αυτό γιατί όταν μετρούνται τα kn qubits της προσομοίωσης, αυτά θα μεταπέσουν σε μια βασική κατάσταση δίνοντας έτσι μόνο kn bits πληροφορίας. Δηλαδή τα c^n bits κρυμμένης πληροφορίας δεν είναι ,απ' ευθείας τουλάχιστον, προσβάσιμα. Άρα λοιπόν το κρίσιμο βήμα για να γίνουν οι κβαντικές προσομοιώσεις πραγματικά χρήσιμες, είναι η ανάπτυξη κατάλληλων μεθόδων ώστε οι επιθυμητές απαντήσεις να μπορούν να εξαχθούν. Το πρόβλημα του πώς μπορεί να λυθεί αυτό το ζήτημα, έχει μόνο κατά ένα μέρος κατανοηθεί πώς θα επιλυθεί.

Παρά αυτό το μειονέκτημα, η κβαντική προσομοίωση θεωρείται μια εφαρμογή η οποία αν επιτευχθεί, θα αποτελεί ένα σημαντικό πλεονέκτημα των κβαντικών υπολογιστών. Η προσομοίωση κβαντικών συστημάτων είναι ένα σημαντικό πρόβλημα σε πολλά πεδία της επιστήμης όπως η Κβαντική Χημεία όπου οι υπολογιστικοί περιορισμοί που επιβάλλονται από τους κλασικούς υπολογιστές κάνουν εξαιρετικά δύσκολη την προσομοίωση της συμπεριφοράς ακόμα και των μικρών μορίων πόσο μάλλον των μορίων τεράστιου μεγέθους τα οποία υπάρχουν σε πολλά βιολογικά συστήματα πχ το DNA. Έτσι αν αναπτυχθούν τρόποι για πιο γρήγορες και ακριβείς προσομοιώσεις τέτοιων συστημάτων, θα μπορούσαν να αναπτυχθούν τομείς άλλων πεδίων στα οποία τα κβαντικά φαινόμενα είναι σημαντικά.

Άλλη μια εφαρμογή των κβαντικών αλγορίθμων προσομοίωσης, είναι ότι μέσα απ' αυτούς, μπορεί να γίνει βαθύτερη θεώρηση των άλλων τύπων αλγορίθμων. Προσεγγίζοντας το πρόβλημα με αυτή τη λογική, γίνεται ευκολότερη η κατανόηση της λογικής του κβαντικού αλγορίθμου.

Τέλος η κβαντική προσομοίωση επιβεβαιώνει και μια ενδιαφέρουσα και αισιόδοξη εκδοχή του νόμου του Moore. Υπενθυμίζεται ότι αυτός ο νόμος λέει ότι η ισχύς ενός κλασικού υπολογιστή θα διπλασιάζεται κάθε περίπου δύο χρόνια για σταθερό κόστος. Ας υποθέσουμε τώρα ότι έχουμε προσομοιώσει ένα κβαντικό σύστημα σε ένα κλασικό υπολογιστή. Αν θέλουμε να προσθέσουμε ένα μόνο qubit στο σύστημα που προσομοιώνεται, τότε η μνήμη που απαιτείται το λιγότερο θα διπλασιαστεί, με παρόμοιο κόστος και στο χρόνο που απαιτείται για την προσομοίωση. Άρα για να ισχύει ο νόμος του Moore στους κβαντικούς υπολογιστές απαιτείται απλώς η προσθήκη ενός μόνο

επιπλέον qubit κάθε δύο χρόνια. Αυτή βέβαια η θεωρητική διατύπωση δεν μπορεί να θεωρηθεί και τόσο έγκυρη, δίνει όμως ένα κίνητρο ίσως στο να ασχοληθούμε με τους κβαντικούς υπολογιστές με την ελπίδα ότι μια μέρα θα είναι ικανοί να ξεπεράσουν τους πιο ισχυρούς κλασικούς τουλάχιστον σε ορισμένες εφαρμογές.

6. Πραγματοποίηση κβαντικών υπολογιστών-Μέθοδος Ιοντικού Κλωβού (Ion Trap method)

Σε αυτό το κεφάλαιο γίνεται μια προσπάθεια να περάσουμε από το θεωρητικό μέρος στο πρακτικό. Γιατί όλη η θεωρία που αναπτύχθηκε στα προηγούμενα κεφάλαια δεν έχει καμία αξία αν δεν μπορέσει να μετουσιωθεί με κάποιο τρόπο σε πράξη. Έχουν γίνει και γίνονται και σήμερα διάφορες προσπάθειες πραγματοποίησης qubits και κβαντικών κυκλωμάτων (δηλαδή απλών κβαντικών υπολογιστών) που βασίζονται σε διάφορες τεχνολογίες όπως η μέθοδος του ιοντικού κλωβού (ion trap method), οι υπολογιστές κοιλότητας κβαντικής ηλεκτροδυναμικής (cavity QED) και πυρηνικού μαγνητικού συντονισμού (NMR). Εδώ θα γίνει μια σχετικά αναλυτική παρουσίαση της μεθόδου ιοντικού κλωβού ή παγίδας ιόντων.

6.1 Αποσυμφώνηση (Decoherence)

Όπως έχει γίνει κατανοητό από τα προηγούμενα κεφάλαια, για να λειτουργήσουν σχεδόν όλοι οι κβαντικοί αλγόριθμοι απαιτείται σε κάποια φάση τους μερικά απ’ τα qubits του υπολογιστή να βρεθούν σε καταστάσεις διεμπλοκής. Αυτή η κατάσταση προφανώς θα πρέπει, αν υποθέσουμε ότι μπορεί να επιτευχθεί, να διατηρείται τουλάχιστον για όσο χρόνο διαρκεί η εκτέλεση του αλγόριθμου. Αυτό όμως δεν είναι καθόλου εύκολο. Και ο λόγος είναι ότι τα qubits τα οποία είναι κβαντικά συστήματα, αλληλεπιδρούν εκτός από μεταξύ τους που είναι το επιθυμητό και με το περιβάλλον τους το οποίο είναι πολύ μεγαλύτερο σύστημα. Αυτή η αλληλεπίδραση (ή σύμπλεξη) με το περιβάλλον, μπορεί πολύ εύκολα να έχει σαν αποτέλεσμα την απώλεια της συμφωνίας φάσης μεταξύ των qubits δηλαδή την λεγόμενη αποσυμφώνηση (decoherence). Έτσι η εκτέλεση του αλγορίθμου δεν μπορεί να προχωρήσει. Είναι τόσο μεγάλο αυτό το πρόβλημα που θεωρείται η κύρια δυσκολία στην πραγματοποίηση των κβαντικών υπολογιστών και όλες οι μέθοδοι που αναπτύσσονται αποσκοπούν στην καταπολέμησή του, η κάθε μια με το δικό της τρόπο. Από την επιτυχή ή όχι αντιμετώπιση αυτού του προβλήματος θα εξαρτηθεί κατά μεγάλο ποσοστό και η επιτυχία ή η αποτυχία του εγχειρήματος της δημιουργίας κβαντικών υπολογιστών.

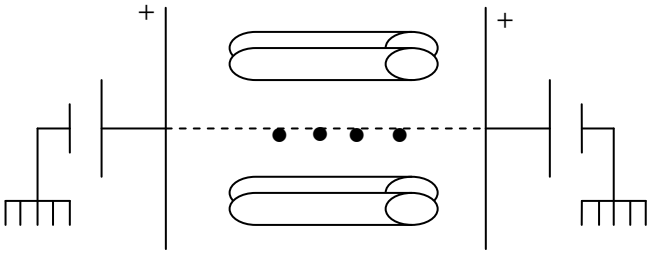
6.2 Μέθοδος Ιοντικού Κλωβού

6.2.1 **Η λογική της μεθόδου**

Η λογική αυτής της μεθόδου προκύπτει φυσιολογικά με απλές σκέψεις. Αφού δεν θέλουμε το σύστημα μας να αλληλεπιδρά με το περιβάλλον, λογικό είναι να θέλουμε το περιβάλλον αυτό να είναι όσο πιο «φτωχό» γίνεται. Δηλαδή θα θέλαμε το σύστημα μας να είναι στο κενό. Το απόλυτο κενό δεν υπάρχει βέβαια, αλλά θα θέλαμε να το προσεγγίσουμε όσο περισσότερο γίνεται, άρα η συσκευή μας καλό θα ήταν να τοποθετηθεί σε ένα θάλαμο κενού. Το δεύτερο ζήτημα που έχουμε να λύσουμε είναι το ποια σωματίδια θα παίζουν το ρόλο των qubits. Θα μπορούσαν ίσως να είναι ουδέτερα μόρια ή άτομα. Αν ήταν όμως έτσι, θα ήταν δύσκολο στο κενό να παραμένουν συνεχώς σε κάποιες καθορισμένες θέσεις αφού δεν θα υπήρχαν οι κατάλληλες δυνάμεις για να τα συγκρατούν. Έτσι θα ήταν πολύ βολικότερο να ήταν φορτισμένα ιόντα οπότε με τη χρήση κατάλληλων ηλεκτρικών πεδίων σε συνδυασμό με τις μεταξύ τους ηλεκτρικές αλληλεπιδράσεις, θα ήταν πολύ ευκολότερο να συγκρατηθούν σε καθορισμένες θέσεις. Αυτή είναι λοιπόν η βασική ιδέα της μεθόδου. Τα qubits να είναι μερικά ιόντα τα οποία βρίσκονται σε καθορισμένες θέσεις σε ένα θάλαμο κενού. Βέβαια υπάρχουν πολλά θέματα που πρέπει να αποσαφηνιστούν όπως το πώς ακριβώς θα είναι η διάταξη, πώς θα μπορούμε να επηρεάζουμε τα qubits (τα ιόντα) ώστε να αποκτούν την κατάσταση που επιθυμούμε, πώς θα αλλάζουμε αυτήν την κατάσταση (δηλαδή πώς θα πραγματοποιούνται οι κβαντικές πύλες που περιγράψαμε θεωρητικά στα προηγούμενα κεφάλαια) και κυρίως το πώς θα πετύχουμε την πολυπόθητη κβαντική σύμπλεξη (ή αλλιώς κβαντική διεμπλοκή). Αυτά όλα θα εξεταστούν στις επόμενες ενότητες του κεφαλαίου.

6.2.2 **Περιγραφή του κλωβού**

Είναι προφανές ότι η κατασκευή μιας διάταξης η οποία να ικανοποιεί τις απαιτήσεις που περιγράφηκαν στην προηγούμενη ενότητα δεν θα ήταν καθόλου εύκολο να πραγματοποιηθεί. Είναι όμως ευτύχημα ότι μια τέτοια διάταξη ήδη υπήρχε και είχε επινοηθεί από τον Paul για διαφορετικό σκοπό. Η διάταξη αυτή ονομάζεται *γραμμικός κλωβός του Paul* και μάλιστα λόγω αυτής της ανακάλυψης ο δημιουργός της τιμήθηκε με το βραβείο Nobel. Μια απλοποιημένη μορφή της διάταξης φαίνεται στο Σχήμα 6-1.



Σχήμα 6-1 : Σχηματική αναπαράσταση του κλωβού του Paul

Τα σωματίδια που θα παίξουν το ρόλο των qubits είναι προφανώς τα ίδια τα ιόντα. Τα πιο κατάλληλα ιόντα είναι του βηρυλλίου (Be^+), του ασβεστίου (Ca^+), του μαγνησίου (Mg^+) και του στροντίου (Sr^+). Επίσης μπορούν να χρησιμοποιηθούν και ιόντα άλλων στοιχείων αλλά τα πιο κατάλληλα θεωρούνται αυτά των αλκαλικών γαιών. Αυτό διότι οι διεγερμένες ενεργειακές τους στάθμες είναι τέτοιας ενέργειας ώστε μπορεί να γίνει εύκολα η διέγερση με τις διαθέσιμες δέσμες λέιζερ και επίσης διότι ανάμεσά τους υπάρχει και μια με μεγάλο χρόνο ζωής (της τάξης δευτερολέπτου) και άρα μπορεί να παίξει το ρόλο της κατάστασης $|1\rangle$ (η κατάσταση $|0\rangle$ θα είναι προφανώς η θεμελιώδη κατάσταση). Οι άλλες διεγερμένες ενεργειακές στάθμες δε που είναι κοντά σε αυτήν που έχει μεγάλο χρόνο ζωής, παρόλο που δε συμμετέχουν άμεσα στη διαδικασία, χρησιμεύουν καίρια σε άλλες διαδικασίες όπως η ψύξη των ιόντων στις πολύ χαμηλές θερμοκρασίες (περίπου 10^{-6} K) που απαιτούνται.

Η διάταξη τώρα όπως φαίνεται στο Σχήμα 6-1, αποτελείται από τέσσερα παράλληλα κυλινδρικά καλώδια τα οποία τροφοδοτούνται από μια πηγή ραδιοσυχνοτήτων συχνότητας μερικών MHz. Όλη η διάταξη βρίσκεται σε υψηλό κενό (πίεση περίπου 10^{-8} Pa). Η απλοποιημένη λογική της διάταξης είναι ότι τα ιόντα δέχονται δυνάμεις από το ηλεκτρικό πεδίο των κυλινδρικών καλωδίων αλλά λόγω της ταχύτατης αλλαγής της πολικότητας του πεδίου, τελικά δεν προλαβαίνουν να κινηθούν πάνω ή κάτω γιατί ως που να ξεκινήσουν να κινηθούν προς μια κατεύθυνση έχει αλλάξει η πολικότητα και δέχονται δύναμη προς την αντίθετη φορά. Έτσι εγκλωβίζονται στη διακεκομμένη γραμμή του σχήματος, που είναι ο άξονας συμμετρίας της διάταξης. Για να μην κινηθούν τώρα κατά μήκος της ευθείας λόγω της μεταξύ τους άπωσης, τοποθετούνται και δύο θετικά φορτισμένες πλάκες κάθετα στον άξονα συμμετρίας οπότε λόγω των μεταξύ τους απώσεων και των δυνάμεων από αυτές τις πλάκες, τα ιόντα τελικά σταθεροποιούνται. Τα

ιόντα μπορούν να επηρεάζονται από κατάλληλες δέσμες λέιζερ για να αλλάζουμε όπως θέλουμε την κατάστασή τους. Με τον ίδιο τρόπο σε συνδυασμό με κατάλληλο ανιχνευτή γίνεται και η ανάγνωση (μέτρηση) αυτής της κατάστασης.

Στην πραγματικότητα βέβαια η περιγραφή της λειτουργίας του κλωβού δεν είναι τόσο απλή. Για παράδειγμα οι κατακόρυφες πλάκες του σχήματος για λόγο που θα φανεί παρακάτω, θα πρέπει να τροφοδοτούνται όχι με σταθερή τάση αλλά με περιοδική τάση της μορφής $V(t)=V_o+V_1\cos\omega t$. Αυτό σημαίνει ότι για να περιγράψουμε την (κβαντική) συμπεριφορά των ιόντων, θα πρέπει να οδηγηθούμε στα σχετικά μαθηματικά τα οποία τελικά οδηγούν στη διαφορική εξίσωση (Τραχανάς Σ., σελ. 706) :

$$\ddot{x}(t)+(k_o+k_1\cos\omega t)x(t)=0 \qquad \textbf{(6-1)}$$

η οποία από άποψη μαθηματικής ανάλυσης είναι *εξίσωση Mathews*. Στην (6-1) αναζητούμε προφανώς δέσμιες λύσεις δηλαδή συναρτήσεις που δεν απειρίζονται όταν το $x\to\pm\infty$ αφού θέλουμε τα ιόντα εγκλωβισμένα.

Αυτή η εξίσωση μοιάζει πολύ με την :

$$\psi''(x)+(E-V_o\cos kx)\psi(x)=0 \qquad \textbf{(6-2)}$$

η οποία αναγνωρίζεται αμέσως ότι είναι η εξίσωση Schrodinger για την περίπτωση του χωρικά περιοδικού δυναμικού $V(x)=V_o\cos kx$ όπου E είναι μια σταθερά ανάλογη της ενέργειας. Αυτή η εξίσωση είναι σχετικά γνωστή από την κβαντική μηχανική και τη φυσική στερεάς κατάστασης και έχει λύσεις πεπερασμένες στο $\pm\infty$ μόνο για ορισμένες περιοχές (ζώνες) του E, τις γνωστές ενεργειακές ζώνες των ηλεκτρονίων σε ένα κρυσταλλικό στερεό μέσα στο οποίο το δυναμικό είναι περιοδικό.

Μπορεί να πει κανείς ότι η (6-1) είναι το χρονικό ανάλογο της (6-2). Άρα λοιπόν είναι λογικό να αναμένει κανείς το ότι για τις λύσεις της (6-1) που μας ενδιαφέρουν, η παράμετρος k_o θα πρέπει να βρίσκεται μέσα σε ορισμένες περιοχές αντίστοιχες των ενεργειακών ζωνών του στερεού. Έτσι σε γενικές γραμμές, καθορίζονται οι διάφορες τιμές των παραμέτρων της διάταξης.

Ένα πιθανό αναμενόμενο πρόβλημα στη λειτουργία του κλωβού, είναι ότι κατά τη διάρκεια της λειτουργίας του δημιουργούνται παράσιτα ηλεκτρικά πεδία πρώτον λόγω ενός φαινομένου που λέγεται *θόρυβος Johnson* που έχει να κάνει με τη θερμική κίνηση των ηλεκτρονίων και δεύτερον λόγω μικροανωμαλιών πάνω στα ηλεκτρόδια. Ο φόβος

είναι ότι λόγω αυτών των ηλεκτρικών πεδίων τα ιόντα θα θερμαίνονται και άρα θα κινούνται. Ευτυχώς όμως τα περισσότερα πειράματα δεν δείχνουν ότι αυτό το πρόβλημα μπορεί να ματαιώσει το εγχείρημα, αλλά είναι ελεγχόμενο.

6.2.3 **Δημιουργία κβαντικών πυλών στον ιοντικό κλωβό**

Ας δούμε τώρα πώς μπορεί να λειτουργήσει μια σειρά από εγκλωβισμένα ιόντα σαν κβαντικός υπολογιστής. Για να γίνει κατανοητή η παρακάτω ανάλυση, απαιτείται γνώση της θεωρίας των *κανονικών τρόπων ταλάντωσης* ενός συστήματος, τα κύρια σημεία της οποίας υπενθυμίζονται στο παράρτημα Α.

Ας δούμε κατ' αρχήν από τι θα καθορίζεται και πώς θα συμβολίζεται η κβαντική κατάσταση της αλυσίδας των ιόντων. Η κατάσταση τους θα καθορίζεται απ' την ξεχωριστή κατάσταση του κάθε ιόντος αν δηλαδή είναι 0 ή 1, θα πρέπει όμως να ληφθεί υπ' όψιν και η συλλογική κίνηση της αλυσίδας η οποία περιγράφεται απ' τους κανονικούς τρόπους ταλάντωσης και τα φωνόνια. Αυτή η συλλογική κίνηση καθορίζεται πλήρως απ' το πόσοι και ποιοι κανονικοί τρόποι ταλάντωσης είναι διεγερμένοι καθώς και από το πόσα φωνόνια από τον κάθε τρόπο υπάρχουν. Βέβαια όπως θα δούμε, θα μας χρειαστούν μόνο ο κοινός τρόπος ταλάντωσης (αυτός με τη μικρότερη συχνότητα) και σε αυτόν θα υπάρχουν είτε κανένα είτε ένα μόνο φωνόνιο. Με βάση αυτά η κατάσταση της αλυσίδας θα συμβολίζεται ως :

$$|\psi\rangle = |x_1, x_2, ..., x_N\rangle|\bar{n}\rangle = |x_1\rangle|x_2\rangle...|x_N\rangle|\bar{n}\rangle \qquad \textbf{(6-3)}$$

όπου x_i, i=1,2,…,N είναι οι καταστάσεις του κάθε ιόντος ξεχωριστά και $|\bar{n}\rangle$ η κατάσταση της συλλογικής κίνησης της αλυσίδας. Κανονικά η τελευταία θα έπρεπε να έχει το συμβολισμό :

$$|\bar{n}_1\rangle_{\omega_1}|\bar{n}_2\rangle_{\omega_2}...|\bar{n}_N\rangle_{\omega_N}$$

όπου ω_i, i=1,2,…,N είναι η συχνότητα του i τρόπου ταλάντωσης και n_i ο αριθμός των φωνονίων αυτού του τρόπου που είναι παρόντα. Όμως για τη λειτουργία του κλωβού όπως θα δούμε, απαιτείται μόνο ο κοινός τρόπος ταλάντωσης με συχνότητα ω_1 άρα η κατάσταση της αλυσίδας συμβολίζεται ως :

$$|\bar{n}_1\rangle_{\omega_1} \equiv |\bar{n}\rangle$$

Συνεπώς η κατάσταση $|\bar{n}\rangle$ σημαίνει ότι είναι διεγερμένος μόνο ο κοινός τρόπος ταλάντωσης και είναι παρόντα n φωνόνια.

Έστω τώρα ότι η αλυσίδα έχει μόνο δύο ιόντα. Τότε η κατάστασή της θα είναι η :

$$|\psi\rangle = |x_1\rangle|x_2\rangle|\bar{n}\rangle \quad \textbf{(6-4)}$$

για παράδειγμα αν $|\psi\rangle = |0\rangle|1\rangle|\bar{0}\rangle$ αυτό σημαίνει ότι το πρώτο ιόν είναι στην κατάσταση 0, το δεύτερο ιόν είναι στην κατάσταση 1 και είναι διεγερμένος μόνο ο κοινός τρόπος ταλάντωσης χωρίς κανένα φωνόνιο (zero point motion).

Ας δούμε σε αυτήν την περίπτωση των δύο ιόντων, τον τρόπο που πραγματοποιούνται οι κβαντικές πύλες. Και πρώτα οι πιο απλές που είναι αυτές που δρουν σε ένα μόνο qubit. Η περίπτωση αυτή είναι σχετικά απλή και οι πύλες πραγματοποιούνται με τη δράση στο σχετικό ιόν (που παίζει το ρόλο του qubit), μιας πολύ εστιασμένης δέσμης λέιζερ που πρέπει να έχει την κατάλληλη διάρκεια και συχνότητα ω_o που είναι αυτή που αντιστοιχεί στη μετάβαση $|0\rangle \to |1\rangle$. Η διεγερμένη κατάσταση $|1\rangle$ επειδή έχει μεγάλο χρόνο ζωής (περίπου 1sec), λόγω της αρχής της αβεβαιότητας της σχέσης (1-4), έχει πολύ μικρό φασματικό εύρος. Αυτό έχει σαν συνέπεια, η θεωρητική περιγραφή της διέγερσης $|0\rangle \to |1\rangle$ να μην περιγράφεται από τον κανόνα του Fermi όπως γίνεται σε ανάλογες περιπτώσεις αλλά από τη θεωρία των ταλαντώσεων Rabi[4]. Σύμφωνα με αυτή τη θεωρία, η δράση της δέσμης λέιζερ πάνω σε ένα ιόν θα φέρει αυτό σε μια κατάσταση της μορφής :

$$|\psi\rangle = c_o(t)|0\rangle + c_1(t)|1\rangle \quad \textbf{(6-5)}$$

και έτσι με κατάλληλη επιλογή του χρόνου δράσης t της ακτίνας, η επαλληλία που υπάρχει στην κατάσταση $|\psi\rangle$ μπορεί να έχει την επιθυμητή μορφή. Με βάση αυτά η επίδραση της δέσμης μπορεί να γίνει :

- Με τους λεγόμενους παλμούς π (διάρκειας T/2), οι οποίοι επιτυγχάνουν τις εξής μεταβάσεις στην κατάσταση του ιόντος :

  $$|0\rangle \to |1\rangle \text{ και } |1\rangle \to |0\rangle$$

  Αυτά αντιστοιχούν στην πύλη X.

[4] Για τη θεωρητική μελέτη των ταλαντώσεων Rabi βλέπε : (Τραχανάς Σ. σελ. 251)

- Με τους λεγόμενους παλμούς π/2 (διάρκειας T/4), οι οποίοι επιτυγχάνουν τις εξής μεταβάσεις στην κατάσταση του ιόντος :

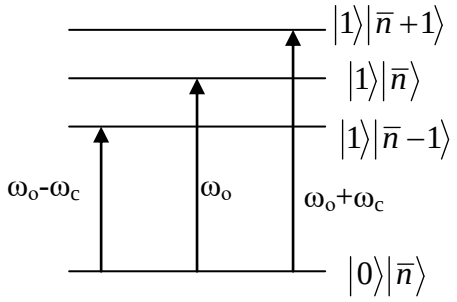
$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ και } |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

  Αυτά αντιστοιχούν στην πύλη Hadamard.

Με ανάλογο τρόπο δημιουργούνται και οι υπόλοιπες πύλες που δρουν σε ένα qubit.

Περνάμε τώρα στο πλαίσιο αυτού του μοντέλου, να δούμε πώς δημιουργείται η πιο δύσκολη αλλά και πιο σημαντική πύλη η CNOT η οποία δρα σε δύο qubits. Θεωρούμε ότι είναι η πιο σημαντική διότι το αποτέλεσμά της όπως είδαμε είναι οι καταστάσεις διεμπλοκής[5] οι οποίες είναι όλη η δύναμη της κβαντικής υπολογιστικής και πληροφορίας. Αφού σε αυτήν την περίπτωση πρέπει να έχουμε αλληλεπίδραση ανάμεσα στα ιόντα, είναι προφανές ότι θα παίξει καίριο ρόλο η συλλογική τους κίνηση, δηλαδή οι κανονικοί τρόποι ταλάντωσης και συγκεκριμένα ο κοινός τρόπος (common mode). Αν ω_c είναι η συχνότητα του κοινού τρόπου, τότε το φάσμα απορρόφησης ενός ιόντος στην περιοχή γύρω απ' τη συχνότητα ω_o της διέγερσης $|0\rangle \to |1\rangle$ είναι αυτό που φαίνεται στο Σχήμα 6-2. Να επισημάνουμε ότι η αριστερή μετάβαση του σχήματος συχνότητας ω_o-ω_c, δεν είναι δυνατή όταν $\bar{n} = 0$,διότι τότε δεν υπάρχει κανένα φωνόνιο να εκμεταλλευτούμε την ενέργεια του για να πετύχουμε τη διέγερση $|0\rangle \to |1\rangle$ με λιγότερη ενέργεια από $\hbar\omega_o$.

Η διαδικασία για να επιτύχουμε την κατάσταση διεμπλοκής, περιλαμβάνει τα παρακάτω βήματα :



Σχήμα 6-2 : Φάσμα απορρόφησης αλυσίδας ιόντων

[5] Καταστάσεις διεμπλοκής ή καταστάσεις σύμπλεξης ενός συστήματος δύο σωματιδίων, είναι αυτές οι καταστάσεις που η μέτρηση κάποιου φυσικού μεγέθους στο ένα καθορίζει το αποτέλεσμα της μέτρησης αυτού του μεγέθους στο άλλο σωματίδιο. Τέτοιες καταστάσεις είναι οι καταστάσεις Bell.

Αν δρούσαμε ένα παλμό π συχνότητας $\omega_o+\omega_c$ στην κατάσταση $|00\rangle|\bar{0}\rangle$, θα πετυχαίναμε τη μετάβαση :

$$|00\rangle|\bar{0}\rangle \rightarrow |01\rangle|\bar{1}\rangle$$

δηλαδή το πρώτο qubit δεν θα πάθαινε τίποτα, το δεύτερο qubit θα πάθαινε τη μετάβαση $|0\rangle \rightarrow |1\rangle$ και στην αλυσίδα των δύο ιόντων θα προστίθετω ένα φωνόνιο. Άρα αν δράσουμε ένα παλμό π/2 συχνότητας $\omega_o+\omega_c$ στην κατάσταση $|00\rangle|\bar{0}\rangle$, σύμφωνα με τα προηγούμενα, θα πετύχουμε τη μετάβαση :

$$|00\rangle|\bar{0}\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle|\bar{0}\rangle + |01\rangle|\bar{1}\rangle) \quad \textbf{(6-6)}$$

δηλαδή το πρώτο qubit δεν έπαθε τίποτα και έχουμε πετύχει κατάσταση διεμπλοκής αλλά όχι ανάμεσα στα δύο ιόντα που είναι το επιθυμητό, αλλά ανάμεσα στο δεύτερο ιόν και την αλυσίδα των ιόντων.

Δρούμε τώρα στο πρώτο ιόν ένα παλμό π συχνότητας $\omega_o-\omega_c$. Όπως προαναφέρθηκε, η κατάσταση $|00\rangle|\bar{0}\rangle$ δεν παθαίνει τίποτα ($\bar{n}=0$), ενώ η $|01\rangle|\bar{1}\rangle$ παθαίνει τη μετάβαση :

$$|01\rangle|\bar{1}\rangle \rightarrow |11\rangle|\bar{0}\rangle$$

άρα συνολικά έχουμε τη μετάβαση :

$$\frac{1}{\sqrt{2}}(|00\rangle|\bar{0}\rangle + |01\rangle|\bar{1}\rangle) \rightarrow \frac{1}{\sqrt{2}}(|00\rangle|\bar{0}\rangle + |11\rangle|\bar{0}\rangle) \quad \textbf{(6-7)}$$

η οποία είναι πράγματι μια κατάσταση διεμπλοκής ανάμεσα στα δύο ιόντα.

Αξιοσημείωτο είναι ότι η κατάσταση της αλυσίδας των ιόντων επανήλθε στην κατάσταση $|\bar{0}\rangle$, δηλαδή χρησιμοποιήθηκε σαν ενδιάμεσο σκαλοπάτι για τη δημιουργία της διεμπλοκής των ιόντων και τελικά επανήλθε στην αρχική της κατάσταση.

Παρά τις διάφορες δυσκολίες που παρουσιάστηκαν και παρουσιάζονται, αυτή η μέθοδος μπορεί να χαρακτηριστεί ελπιδοφόρα. Μάλιστα το 2007 επιτεύχθηκε με αυτήν, κατάσταση διεμπλοκής οκτώ ιόντων ενώ υπάρχει η προοπτική για περισσότερα.

6.3 Αποτελέσματα προσπαθειών έως σήμερα

Σε σχέση με τις προσπάθειες που έγιναν και εξακολουθούν να γίνονται πάνω στο θέμα, το βασικό συμπέρασμα είναι το εξής : μέχρι σήμερα δεν έχει καρποφορήσει το όνειρο που δεν είναι άλλο από τη δημιουργία ενός κβαντικού υπολογιστή όπως τον φανταζόμαστε. Ενός κβαντικού υπολογιστή δηλαδή, που να είναι σε θέση να λύνει πρακτικά προβλήματα πολύ ταχύτερα από τους υπάρχοντες κλασικούς ή που να λύνει προβλήματα που θεωρούνται άλυτα απ' αυτούς. Είναι σίγουρο όμως ότι έχει επιτευχθεί μεγάλη πρόοδος και το ότι υπάρχει η πεποίθηση επιτυχούς έκβασης αποδεικνύεται απ' το γεγονός ότι όλο και περισσότερες μεγάλες εταιρίες (και όχι μόνο εταιρίες αλλά και ερευνητικά ιδρύματα, κράτη και ιδιώτες), επενδύουν κάθε χρόνο μεγάλα ποσά στην έρευνα προς αυτήν την κατεύθυνση. Κατά καιρούς ανακοινώνονται και κάποια αποτελέσματα που δείχνουν την πρόοδο που έχει συντελεστεί και έχουν να κάνουν με την διεμπλοκή όλο και περισσότερων qubits με διάφορους τρόπους και με το χρόνο που συντηρείται αυτή η διεμπλοκή. Δεν θεωρήθηκε σκόπιμο να παρουσιαστούν αυτά σε αυτήν την εργασία, διότι όλα είναι ακόμα σε στάδιο που δεν είναι σίγουρο ότι θα οδηγήσουν κάπου. Το αν το όνειρο θα γίνει τελικά πραγματικότητα σίγουρα είναι κάτι που θα μας απασχολήσει τις επόμενες δεκαετίες.

7. Κβαντική Πληροφορία

Στο κεφάλαιο αυτό ας έρθουμε τώρα στην ιστορία ενός ακόμα κρίκου στην αλυσίδα της κατανόησης των κβαντικών υπολογιστών, της κβαντικής πληροφορίας. Γίνεται πρώτα μια ιστορική αναδρομή στη κλασική θεωρία της πληροφορίας, στη συνέχεια γίνεται μια επισκόπηση στην πορεία της κβαντικής πληροφορίας και τέλος δίνονται μερικά στοιχεία για την κλασική και κβαντική πληροφορία σε δίκτυο καναλιών επικοινωνίας.

7.1 Κλασική θεωρία της πληροφορίας

Την ίδια εποχή που συνέβαινε η επανάσταση στην επιστήμη των υπολογιστών, άλλη μια επανάσταση λάμβανε χώρα, αυτή στο χώρο της επικοινωνίας. Το 1948 ο Claude Shannon έκανε δύο σπουδαίες δημοσιεύσεις οι οποίες έβαλαν τα θεμέλια για τη σύγχρονη θεωρία της πληροφορίας και της επικοινωνίας. Ίσως το καθοριστικό βήμα που έκανε ο Shannon ήταν να ορίσει μαθηματικά την έννοια της πληροφορίας. Σε πολλές μαθηματικές επιστήμες υπάρχει αρκετή ευελιξία στην επιλογή των θεμελιωδών ορισμών. Έτσι και στην περίπτωση της πληροφορίας, διατυπώθηκαν διάφορες εκδοχές οι οποίες μάλιστα είχαν ευρεία αποδοχή. Η εκδοχή όμως του Shannon αποδείχθηκε μακράν η πιο αποδοτική σε κατανόηση αλλά και στο να οδηγήσει σε πλήθος βαθιά αποτελέσματα. Επίσης η θεωρία αυτή φάνηκε να δίνει εξήγηση στα περισσότερα (αν και όχι σε όλα) από τα προβλήματα επικοινωνίας του πραγματικού κόσμου. Ο Shannon ενδιαφέρθηκε κυρίως για δύο ερωτήματα κλειδιά που σχετίζονται με την επικοινωνία της πληροφορίας μέσω επικοινωνιακών καναλιών. Πρώτον, «ποιες πληροφορίες απαιτούνται για να γνωρίζουμε πόση πληροφορία μπορεί να μεταδοθεί μέσω ενός καναλιού;» Για παράδειγμα οι εταιρίες τηλεφωνίας θέλουν να ξέρουν πόση πληροφορία μπορεί να μεταδοθεί αξιόπιστα μέσω ενός δεδομένου τηλεφωνικού καλωδίου. Δεύτερον, «μπορεί η πληροφορία να μεταδοθεί με τέτοιο τρόπο, ώστε να είναι προστατευμένη από το θόρυβο που υπάρχει στο κανάλι επικοινωνίας;» Ο Shannon έδωσε απάντηση σε αυτά τα δύο ερωτήματα, αποδεικνύοντας τα δύο θεμελιώδη θεωρήματα της θεωρίας της πληροφορίας. Το πρώτο απ' αυτά λέγεται «προγραμματισμός σε κανάλι χωρίς θόρυβο» το οποίο ποσοτικοποιεί τις συνθήκες που απαιτούνται ώστε να αποθηκευτεί το προϊόν από μια πηγή πληροφορίας. Το δεύτερο θεώρημα λέγεται «προγραμματισμός σε κανάλι με θόρυβο» το οποίο ποσοτικοποιεί πόση

πληροφορία μπορεί να μεταφερθεί αξιόπιστα μέσω ενός καναλιού επικοινωνίας παρουσία θορύβου. Για να επιτευχθεί αξιόπιστη μεταφορά παρουσία θορύβου, ο Shannon έδειξε ότι «κώδικες διόρθωσης λαθών» θα μπορούσαν να χρησιμοποιηθούν για να προστατεύσουν την πληροφορία που αποστέλλεται. Το δεύτερο θεώρημα του Shannon δίνει ένα ανώτατο όριο στην προστασία που παρέχουν αυτοί οι «κώδικες διόρθωσης λαθών». Δυστυχώς το θεώρημα του Shannon δε δίνει κάποια ομάδα από ορισμένους «κώδικες διόρθωσης λαθών» μέσω των οποίων θα μπορούσε να επιτευχθεί αυτό το ανώτατο όριο. Από τον καιρό που ο Shannon δημοσίευσε τις εργασίες του μέχρι σήμερα, διάφοροι ερευνητές έχουν κατασκευάσει περισσότερες και καλύτερες ομάδες από τέτοιους κώδικες στην προσπάθεια τους να έρθουν πλησιέστερα στο όριο του δεύτερου θεωρήματος του Shannon. Σήμερα υπάρχει μια εκλεπτυσμένη θεωρία από «κώδικες διόρθωσης λαθών» η οποία προσφέρει τη δυνατότητα πολλών επιλογών στην αναζήτηση σχεδιασμού ενός αξιόπιστου τέτοιου κώδικα. Τέτοιοι κώδικες χρησιμοποιούνται σε διάφορες περιπτώσεις όπως σε cd players, computer modems και σε δορυφορικά συστήματα επικοινωνίας.

7.2 Κβαντική θεωρία της πληροφορίας

Η κβαντική θεωρία της πληροφορίας ακολούθησε με παρόμοια βήματα. Το 1995 ο Ben Schumacher διατύπωσε ένα θεώρημα ανάλογο με το πρώτο θεώρημα του Shannon και στη διαδικασία αυτή, όρισε το qubit ως μια χειροπιαστή φυσική πηγή πληροφορίας. Μέχρι σήμερα όμως, δεν έχει διατυπωθεί ακόμα ανάλογο θεώρημα με το δεύτερο θεώρημα του Shannon στη θεωρία της κβαντικής πληροφορίας. Εν τω μεταξύ σε αναλογία με την κλασική ομόλογη της, μια θεωρία κβαντικής διόρθωσης λαθών έχει αναπτυχθεί, η οποία επιτρέπει στους κβαντικούς υπολογιστές να εργάζονται αποτελεσματικά με την παρουσία θορύβου και επίσης επιτρέπουν αξιόπιστη επικοινωνία μέσω κβαντικών καναλιών με θόρυβο.

Οι κλασικές ιδέες στη διόρθωση λαθών στη μεταφορά της πληροφορίας, έχει αποδειχθεί ότι προσφέρουν πολύ σημαντική βοήθεια στην ανάπτυξη και κατανόηση της αντίστοιχης κβαντικής διόρθωσης. Το 1996 δύο ομάδες οι οποίες εργάζονταν ανεξάρτητα οι Robert Calderbank - Peter Shor και ο Andrew Stean, ανακάλυψαν μια σημαντική κλάση κβαντικών κωδίκων που είναι γνωστή ως CSS από τα αρχικά των ονομάτων τους. Αυτή η

δουλειά ήρθε να αθροιστεί με άλλους κώδικες που έχουν ανακαλυφθεί ανεξάρτητα από τους Robert Calderbank, Eric Rains, Peter Shor, Neil Sloane και από τον Daniel Gottensman. Έτσι οικοδομώντας πάνω στις βασικές αρχές της κλασικής θεωρίας κωδικοποίησης της πληροφορίας, αυτές οι ανακαλύψεις συνθέτουν ένα σύνολο αρχών που επιτρέπουν αρκετά καλή κατανόηση στην κβαντική διόρθωση λαθών της πληροφορίας και στις πρακτικές εφαρμογές της.

Η θεωρία της κβαντικής διόρθωσης λαθών αναπτύχθηκε για να προστατεύσει τις κβαντικές καταστάσεις από το θόρυβο. Άλλο ένα ερώτημα όμως είναι, τι γίνεται αν θέλουμε να μεταφέρουμε την κοινή κλασική πληροφορία χρησιμοποιώντας ένα κβαντικό κανάλι. Σε αυτό το πεδίο έχουν προκύψει μερικές εκπλήξεις. Το 1992 οι Charles Bennett και Stephen Wiesner εξήγησαν πως μπορούν να μεταφερθούν δύο κλασικά bit πληροφορίας ενώ μεταφέρεται μόνο ένα κβαντικό bit από τον αποστολέα στον παραλήπτη. Ακόμη πιο ενδιαφέροντα είναι τα αποτελέσματα στη συνδυασμένη κβαντική πληροφορία. Έστω ότι έχουμε ένα δίκτυο από δύο υπολογιστές οι οποίοι προσπαθούν να επιλύσουν ένα πρόβλημα. Πόση επικοινωνία απαιτείται μεταξύ τους; Πρόσφατα αποδείχθηκε ότι οι κβαντικοί υπολογιστές απαιτείται να έχουν εκθετικά λιγότερη επικοινωνία για να επιλύσουν συγκεκριμένα προβλήματα απ’ αυτήν που απαιτείται αν το δίκτυο αποτελείται από κλασικούς υπολογιστές. Δυστυχώς μέχρι σήμερα, τέτοιου είδους προβλήματα που επιχειρείται να λυθούν με αυτή τη μέθοδο, δεν είναι μεγάλης σπουδαιότητας και πρακτικής σημασίας και υποφέρουν από ανεπιθύμητους τεχνικούς περιορισμούς. Έτσι είναι μια μεγάλη πρόκληση για το μέλλον των κβαντικών υπολογιστών να βρεθούν πραγματικά σημαντικά προβλήματα στα οποία η συνδυασμένη κβαντική υπολογιστική να έχει σημαντικά πλεονεκτήματα σε σχέση με την αντίστοιχη κλασική.

7.3 Θεωρία της πληροφορίας σε δίκτυο καναλιών επικοινωνίας

Ας επιστρέψουμε τώρα στη θεωρία της πληροφορίας. Η μελέτη της θεωρίας αυτής ξεκινά με τη μελέτη ενός καναλιού επικοινωνίας. Στις εφαρμογές βέβαια συνήθως δεν έχουμε ένα μόνο κανάλι αλλά ένα δίκτυο από πολλά κανάλια. Το θέμα της θεωρίας πληροφορίας κλασικών δικτύων η οποία ασχολείται με τις ιδιότητες της μετάδοσης πληροφορίας μέσω

τέτοιων δικτύων, έχει αναπτυχθεί σε πολύ ικανοποιητικό βαθμό. Αντίθετα η αντίστοιχη θεωρία για τα κβαντικά δίκτυα ακόμα είναι σε εμβρυακό στάδιο. Ακόμα και για πολύ βασικά ερωτήματα πάνω στο θέμα είναι γνωστά ελάχιστα πράγματα. Έχουν γίνει βέβαια μερικά σημαντικά βήματα τα τελευταία χρόνια αλλά δεν υπάρχει ακόμα μια ενιαία θεωρία η οποία είναι απαραίτητη. Ένα χαρακτηριστικό παράδειγμα για τη χρησιμότητα μιας τέτοιας θεωρίας είναι το παρακάτω : Έστω ότι η Alice επιθυμεί να στείλει κβαντική πληροφορία στον Bob (η Alice και ο Bob είναι οι κλασικοί ήρωες στη βιβλιογραφία στα θέματα ανταλλαγής πληροφορίας όπως φάνηκε και σε πολλά άλλα σημεία αυτής της εργασίας), μέσω ενός θορυβώδους κβαντικού καναλιού. Αν αυτό το κανάλι έχει χωρητικότητα μηδέν για κβαντική πληροφορία, τότε είναι προφανώς αδύνατο να σταλεί στον Bob οποιαδήποτε πληροφορία. Έστω τώρα ότι υπάρχει και ένα δεύτερο παρόμοιο κβαντικό κανάλι μέσω του οποίου γίνεται προσπάθεια από την Alice να στείλει πληροφορία στον Bob ταυτόχρονα με το πρώτο. Διαισθητικά αλλά και αυστηρά μαθηματικά είναι φανερό ότι αν επρόκειτο για κλασικά κανάλια, τότε το σύστημα των δύο καναλιών επίσης θα είχε μηδέν χωρητικότητα άρα ο Bob δεν θα λάμβανε κανένα ποσό πληροφορίας. Το ίδιο θα συνέβαινε αν αντιστρέφαμε τη ροή πληροφορίας στο ένα απ' τα δύο κανάλια. Όταν όμως πρόκειται για κβαντικά κανάλια αποδεικνύεται ότι αν αντιστραφεί η φορά ροής πληροφορίας στο ένα κανάλι τότε υπάρχει πιθανότητα να έχουμε μεταφορά πληροφορίας! Τέτοιου είδους αποτελέσματα τα οποία είναι αντίθετα από τη διαίσθηση μας, δείχνουν την περίεργη φύση της κβαντικής πληροφορίας όπως άλλωστε συμβαίνει και γενικότερα με την κβαντική μηχανική.

8. Κβαντική Κρυπτογραφία

Ας αλλάξουμε τώρα πεδίο μελέτης και ας περάσουμε σε αυτό της κρυπτογραφίας. Γενικά κρυπτογραφία είναι το πρόβλημα της επικοινωνίας ανάμεσα σε δύο μέρη χωρίς η πληροφορία που ανταλλάσουν αυτά να είναι προσβάσιμη σε κάποιον άλλο. Το ποιο κοινό πρόβλημα που προσπαθεί να λύσει η κρυπτογραφία είναι η αποστολή μυστικών μηνυμάτων. Έστω ότι δύο άνθρωποι θέλουν να επικοινωνήσουν μυστικά. Πχ έστω ότι κάποιος θέλει να στείλει τον αριθμό της πιστωτικής του κάρτας σε κάποιον έμπορο για να αγοράσει κάτι και φυσικά δε θέλει αυτός ο αριθμός να πέσει στα χέρια κάποιου τρίτου. Αυτό μπορεί να γίνει χρησιμοποιώντας κάποιο πρωτόκολλο κρυπτογράφησης. Στα πρωτόκολλα κρυπτογράφησης υπάρχει μια σημαντική κατηγοριοποίηση. Με βάση αυτήν, η μια κατηγορία είναι αυτά με ιδιωτικό (κρυφό) κλειδί κρυπτογράφησης και η άλλη είναι αυτά με δημόσιο (φανερό) κλειδί. Παρακάτω αναλύονται οι επιδράσεις της κβαντομηχανικής στις δύο μεθόδους και θα δούμε ότι στην περίπτωση του ιδιωτικού κλειδιού η κβαντική μηχανική φαίνεται να δίνει μια ασφαλή λύση στα υπάρχοντα μειονεκτήματα της μεθόδου, ενώ αντίθετα στην περίπτωση του δημόσιου κλειδιού φαίνεται να καταστρέφει την πιο αξιόπιστη μέθοδο που υπάρχει σήμερα, τη μέθοδο RSA. Ότι δηλαδή σου δίνει με το ένα χέρι σου το παίρνει απ' το άλλο ή αντίστροφα, όπως το πάρει κανείς.

8.1 Κρυπτογράφηση με ιδιωτικό κλειδί

Στην περίπτωση του ιδιωτικού κλειδιού η Alice και ο Bob επιθυμούν να επικοινωνήσουν με τη βοήθεια ενός κλειδιού το οποίο γνωρίζουν μόνο αυτοί οι δύο. Η ακριβής μορφή του κλειδιού θα μπορούσε να είναι πχ ένας μεγάλος αριθμός με ψηφία 0 και 1. Η λογική είναι, η Alice με τη βοήθεια του κλειδιού να κωδικοποιήσει την πληροφορία που θέλει να στείλει στον Bob πχ προσθέτοντας με πρόσθεση modulo 2, qubit με qubit το αρχικό μήνυμα με το κλειδί, ώστε να μην μπορεί αυτή να είναι κατανοητή από ένα τρίτο. Στη συνέχεια η Alice στέλνει κωδικοποιημένη την πληροφορία και ο Bob αφού τη λάβει, θα πρέπει μετά με τη βοήθεια του ίδιου κλειδιού να αποκωδικοποιήσει την πληροφορία ξαναπροσθέτοντας το κωδικοποιημένο μήνυμα με το κλειδί αφού η διπλή πρόσθεση

modulo 2 ξαναδίνει το αρχικό αποτέλεσμα. Στο Σχήμα 8-1 φαίνεται ένα παράδειγμα μέσω του οποίου γίνεται κατανοητή αυτή η διαδικασία.

Alice									
Αρχικό Μήνυμα	1	0	0	1	1	1	0	1	0
	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Ιδιωτικό κλειδί	0	0	1	1	1	0	1	1	0
Κρυπτογραφημένο Μήνυμα	1	0	1	0	0	1	1	0	0

Bob									
Κρυπτογραφημένο Μήνυμα	1	0	1	0	0	1	1	0	0
	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕	⊕
Ιδιωτικό κλειδί	0	0	1	1	1	0	1	1	0
Αρχικό Μήνυμα	1	0	0	1	1	1	0	1	0

Σχήμα 8-1 : Παράδειγμα κωδικοποίησης με ιδιωτικό κλειδί

Αυτή η μέθοδος όμως παρουσιάζει διάφορα μειονεκτήματα, κυριότερο των οποίων είναι το πώς θα γίνει η αποστολή του κλειδιού. Έτσι πολλές φορές η αποστολή αυτή εγκυμονεί τους ίδιους κινδύνους με την αποστολή του ίδιου του μηνύματος, αφού ένας κακόβουλος τρίτος (η Eve συνήθως παίζει αυτό το ρόλο), μπορεί να υποκλέψει το κλειδί και στη συνέχεια να αποκωδικοποιήσει το μήνυμα. Μια από τις πρώτες διαπιστώσεις της μελέτης της κβαντικής πληροφορίας, ήταν ότι η αποστολή του κλειδιού θα μπορούσε να γίνει με τέτοιο τρόπο ώστε να είναι ασφαλής. Η διαδικασία η οποία είναι γνωστή ως κβαντική κρυπτογραφία στηρίζεται σε μια βασική αρχή (αξίωμα) της κβαντικής μηχανικής σύμφωνα με την οποία δεν είναι δυνατό να παρατηρήσει κανείς ένα κβαντικό σύστημα χωρίς να το διαταράξει. Έτσι αν κάποιος κατάσκοπος (η Eve), παρακολουθεί όταν η Alice και ο Bob προσπαθούν να μεταφέρουν ο ένας στον άλλον το κλειδί, η παρουσία του θα γίνει αντιληπτή λόγω της διαταραχής στο κανάλι επικοινωνίας μέσω του οποίου γίνεται η μεταφορά του κλειδιού. Βέβαια σε αυτό υπάρχει και μια ατέλεια. Η κβαντική κατάσταση

δεν καταστρέφεται μόνο σε μια περίπτωση : αν αυτή είναι μια βασική κατάσταση. Αυτή είναι σημαντική περίπτωση γιατί συνήθως ένα κβαντικό μήνυμα αποστέλλεται με τα qubits στις βασικές τους καταστάσεις. Άρα δεν είναι το θέμα και τόσο απλό και το πρόβλημα προσπαθούν να λύσουν τα διάφορα κβαντικά πρωτόκολλα κρυπτογράφησης, δύο απ' τα οποία θα αναλυθούν παρακάτω. Οι πρώτες ιδέες για κβαντική κρυπτογράφηση διατυπώθηκαν από τον Steven Wiesner στα τέλη της δεκαετίας του 60 αλλά δεν έγιναν δεκτές για δημοσίευση! Και έτσι φτάσαμε στο 1984 όταν οι Charles Bennett και Gilles Brassard βασιζόμενοι στη δουλειά του Weisner πρότειναν ένα πρωτόκολλο κρυπτογραφίας το οποίο χρησιμοποιούσε την κβαντική μηχανική για τη μεταφορά του κλειδιού μεταξύ της Alice και του Bob χωρίς –όπως ισχυρίζονταν-να υπάρχει πιθανότητα υποκλοπής το οποίο ονομάστηκε πρωτόκολλο BB84 απ' τα αρχικά των δημιουργών του **B**ennett και **B**rassard και το έτος που το πρότειναν 19**84**. Από τότε έχουν προταθεί και άλλα κβαντικά πρωτόκολλα κρυπτογραφίας όπως το πρωτόκολλο EPR. Η κβαντική κρυπτογραφία είναι πλέον ένα προϊόν που χρησιμοποιείται στην πράξη από τράπεζες, μεγάλους οργανισμούς αλλά και κράτη όπως για παράδειγμα τον Οκτώβρη του 2007 στις εκλογές της Ελβετίας, που χρησιμοποιήθηκε για την ασφαλή μεταφορά των αποτελεσμάτων από τα περιφερειακά εκλογικά τμήματα στην πρωτεύουσα!

8.1.1 **Το πρωτόκολλο BB84**

Η λογική του πρωτοκόλλου αυτού είναι η εξής :

Έστω ότι η Alice θέλει να στείλει στον Bob ένα μήνυμα που αποτελείται από μια ακολουθία N qubits. Τότε μέσω ενός κβαντικού καναλιού επικοινωνίας του στέλνει μια ακολουθία από 2N qubits, δηλαδή διπλάσια σε πλήθος από το μήνυμα για λόγο ο οποίος θα φανεί παρακάτω. Η ιδέα κλειδί του πρωτοκόλλου είναι ότι η Alice φροντίζει να έχει τη δυνατότητα να προετοιμάσει τα qubits που θα στείλει σε δύο διαφορετικές μετρητικές κατευθύνσεις δηλαδή σε μαθηματική ορολογία σε δύο διαφορετικές μετρητικές βάσεις του αντίστοιχου χώρου Hilbert. Και για κάθε qubit επιλέγει τυχαία ποια βάση (κατεύθυνση) θα χρησιμοποιήσει. Οι κατευθύνσεις αυτές δεν είναι ανάγκη να είναι κρυφές αλλά μπορεί να είναι και δημόσια γνωστές. Για να γίνουν περισσότερο κατανοητά όλα αυτά, αν τα qubits είναι γραμμικά πολωμένα φωτόνια (που έτσι είναι συνήθως στις περιπτώσεις που εφαρμόζεται η μέθοδος) και το κβαντικό κανάλι είναι μια οπτική ίνα, στη

μια βάση η μια βασική κατάσταση είναι η γραμμική πόλωση στον άξονα x έστω η $|x\rangle$ και η άλλη σε μια ορθογώνια κατάσταση στον άξονα y έστω η $|y\rangle$. Έτσι για να επανέλθουμε στο γνωστό συμβολισμό θα έχουμε την αντιστοιχία :

$$|0\rangle \rightarrow |x\rangle$$

$$|1\rangle \rightarrow |y\rangle$$

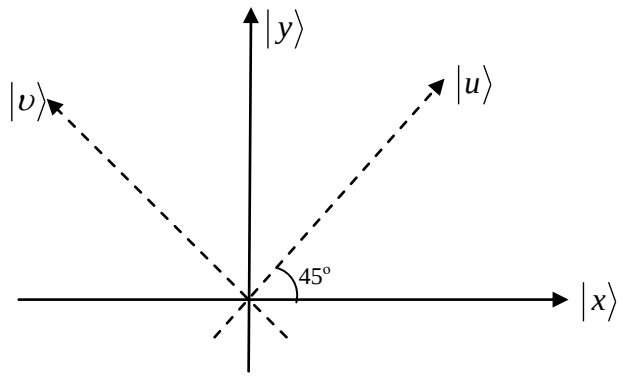
Για να μετρήσει κάποιος ένα qubit χρειάζεται μόνο ένα γραμμικό πολωτή πχ κατά τη διεύθυνση του άξονα x, οπότε αν ένα φωτόνιο διέλθει απ' αυτόν, σημαίνει ότι βρίσκεται στην κατάσταση $|x\rangle$ άρα στην $|0\rangle$, ενώ αν δε διέλθει, βρίσκεται στην κατάσταση $|y\rangle$ άρα στην $|1\rangle$.

Για τη δεύτερη τώρα μετρητική βάση που θα χρησιμοποιήσει η Alice, θα μπορούσε το ένα διάνυσμα της να είναι σε μια διεύθυνση που θα σχηματίζει γωνία 45^o με τον άξονα x, έστω τη u και το άλλο σε μια ορθογώνια διεύθυνση που θα σχηματίζει γωνία με τον x, 135^o (90^o +45^o), έστω τη υ. Εδώ έχουμε την αντιστοιχία :

$$|0\rangle \rightarrow |u\rangle$$

$$|1\rangle \rightarrow |\upsilon\rangle$$

Σχηματικά τα δύο ζευγάρια διευθύνσεων φαίνονται στο Σχήμα 8-2 .



Σχήμα 8-2 : Διανυσματική αναπαράσταση των δύο βάσεων του πρωτοκόλλου BB84

Όπως είναι φυσικό βέβαια, τα διανύσματα της μιας βάσης μπορούν να γραφτούν σαν γραμμικός συνδυασμός των διανυσμάτων της άλλης. Στη συγκεκριμένη περίπτωση έχουμε:

$$|u\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle),\ |\upsilon\rangle = \frac{1}{\sqrt{2}}(|x\rangle - |y\rangle) \quad \textbf{(8-1)}$$

και

$$|x\rangle = \frac{1}{\sqrt{2}}(|u\rangle + |\upsilon\rangle),\ |y\rangle = \frac{1}{\sqrt{2}}(|u\rangle - |\upsilon\rangle) \quad \textbf{(8-2)}$$

όπως μπορεί εύκολα να αποδειχθεί (Τραχανάς Σ. σελ 686). Έτσι μια κατάσταση η οποία είναι βασική στο ένα σύστημα, είναι κατάσταση επαλληλίας στο άλλο.

Για να μετρήσει κάποιος ένα qubit στη δεύτερη βάση, χρειάζεται τώρα ένα γραμμικό πολωτή κατά τη διεύθυνση του άξονα u, οπότε αν ένα φωτόνιο διέλθει, θα βρίσκεται στην κατάσταση $|u\rangle$ άρα στην $|0\rangle$,ενώ αν δε διέλθει βρίσκεται στην κατάσταση $|\upsilon\rangle$, άρα στην $|1\rangle$.

Πάμε τώρα στην άλλη άκρη της οπτικής ίνας όπου ο Bob λαμβάνει τα πολωμένα, με τον τρόπο που περιγράψαμε, φωτόνια που του έστειλε η Alice. Ο Bob πρέπει να διαθέτει δύο γραμμικούς πολωτές έναν για τη διεύθυνση x και έναν για τη διεύθυνση u. Με τη βοήθεια αυτών μετράει την κατάσταση τους, επιλέγοντας κι αυτός τυχαία τις διευθύνσεις (βάσεις) μέτρησης για κάθε ένα. Έτσι θα καταγράψει μια σειρά από 2N ψηφία 0 ή 1. Η διαδοχή δεν θα είναι προφανώς ίδια με αυτήν που έστειλε η Alice. Συγκεκριμένα για τα qubits που τυχαία στάλθηκαν και μετρήθηκαν στην ίδια βάση, θα υπάρχει συμφωνία Alice και Bob. Αυτά, αν το N είναι αρκετά μεγάλο, για στατιστικούς λόγους θα είναι N το πλήθος. Για τα υπόλοιπα N τώρα, αν η Alice τα έχει στείλει σε μια από τις βασικές καταστάσεις της βάσης xy και ο Bob τα μετρήσει στη βάση uu, αυτός θα τα βρει σε κατάσταση επαλληλίας και η μέτρηση θα δώσει κατά 50% το σωστό και κατά 50% το λάθος αποτέλεσμα λόγω των σχέσεων (8-1) και (8-2). Άρα είναι φανερό ότι για να διαβάσει ο Bob σωστά το μήνυμα, θα πρέπει να ξέρει ποια qubits μετρήθηκαν από τους δύο στην ίδια βάση. Αυτό όμως μπορεί να γίνει μέσω ενός κλασικού τρόπου επικοινωνίας ακόμα και το τηλέφωνο. Να υποδείξει δηλαδή η Alice στον Bob τις διευθύνσεις στις οποίες μέτρησε το κάθε φωτόνιο που έστειλε. Δεν έχει σημασία αν κάποιος υποκλέψει αυτήν την επικοινωνία διότι τότε θα ξέρει μόνο τη διεύθυνση αποστολής του κάθε φωτονίου και όχι την κατάσταση του (0 ή 1).

Μένει τώρα να εξηγήσουμε γιατί κάποιος (η Eve φυσικά), δεν μπορεί να παρεμβληθεί στη διαδικασία και να υποκλέψει το μήνυμα. Κατ' αρχήν δεν μπορεί να αντιγράψει το μήνυμα διότι όπως είδαμε υπάρχει το θεώρημα της μη αντιγραφής της κατάστασης ενός qubit. Άρα το μόνο που μπορεί να κάνει είναι να παρεμβληθεί στη γραμμή επικοινωνίας και να μετρήσει την κατάσταση των φωτονίων με τον ίδιο τυχαίο τρόπο και μετά να τα αφήσει να περάσουν προς τον Bob. Και πρέπει να το κάνει αυτό με όλα τα φωτόνια γιατί αλλιώς ο Bob θα διαπιστώσει το έλλειμμα. Τότε η Eve θα έχει μια σειρά από 2N το πλήθος 0 και 1. Απ' αυτά, όπως και στην περίπτωση του Bob, λόγω στατιστικής θα είναι σωστά τα N που τα μέτρησε στη σωστή βάση και μάλιστα η κατάστασή τους δεν θα επηρεαστεί απ' τη μέτρηση που έκανε διότι βρίσκονταν σε βασική κατάσταση. Τα υπόλοιπα N θα τα μετρήσει σε κατάσταση επαλληλίας και άρα θα τους αλλάξει την κατάσταση λόγω της μέτρησης, σε βασική κατάσταση στην άλλη όμως βάση. Αν για παράδειγμα η Alice στείλει ένα φωτόνιο στην κατάσταση 0 της βάσης xy δηλαδή τη $|x\rangle$ και η Eve το μετρήσει στη βάση uυ, για αυτήν το φωτόνιο θα είναι στην κατάσταση $\frac{1}{\sqrt{2}}(|u\rangle+|\upsilon\rangle)$ και άρα μετά τη μέτρηση αν μετρήσει 0, η κατάσταση θα γίνει $|u\rangle$. Άρα το φωτόνιο θα φτάσει στο Bob σε αυτήν την κατάσταση. Αν τώρα ο Bob διαλέξει να το μετρήσει στη βάση uυ, θα μετρήσει και αυτός σίγουρα 0 όπως έστειλε η Alice. Αυτό θα συμβεί σε N/2 περίπου φωτόνια. Αν όμως διαλέξει τη βάση xy που είχε διαλέξει και η Alice (στα άλλα N/2 φωτόνια), τότε για τον Bob η κατάσταση του φωτονίου θα είναι η $\frac{1}{\sqrt{2}}(|x\rangle+|y\rangle)$ και άρα έχει 50% να μετρήσει 0 όπως έστειλε η Alice (αυτό θα γίνει σε N/4 φωτόνια) και 50% να μετρήσει 1 αντίθετα με αυτό που έστειλε η Alice (στα άλλα N/4 φωτόνια). Δηλαδή αν παρεμβληθεί η Eve, θα υπάρχουν N/4 περίπου φωτόνια, που παρά το ότι ο Bob τα μέτρησε στην ίδια διεύθυνση που τα έστειλε η Alice, θα έχουν μετρηθεί διαφορετικά αποτελέσματα. Άρα αυτό που έχουν να κάνουν η Alice και ο Bob είναι να εκμεταλλευτούν αυτό το γεγονός και αφού επιλέξουν ένα τυχαίο δείγμα μήκους m ο καθένας απ' την αλυσίδα του, να συγκρίνουν ακόμα και δημόσια τα στοιχεία τους και αν διαπιστώσουν διαφορά σε περίπου m/4 απ' αυτά τότε πάει να πει ότι υπάρχει υποκλοπή, αλλιώς όχι. Για τους πολύ σχολαστικούς, υπάρχει και η πιθανότητα βέβαια να μην εντοπιστεί η υποκλοπή απ' αυτόν τον έλεγχο αφού για κάθε ψηφίο η πιθανότητα να είναι

σωστό είναι 75% και άρα μπορεί στα m ψηφία που θα διαλέξουμε να μην είναι αυτά που είναι λάθος. Η πιθανότητα όμως να είναι και τα m ψηφία σωστά αν πχ m=500 είναι :

$$(\frac{3}{4})^m = (\frac{3}{4})^{500} = 10^{-62}$$

μια εξωφρενικά μικρή πιθανότητα δηλαδή (Τραχανάς Σ. σελ 688).

8.1.2 **Το πρωτόκολλο EPR**

Αυτό το πρωτόκολλο παρουσιάζει μεγάλο ενδιαφέρον εκτός από την πρακτική του πλευρά αλλά και γιατί αναδεικνύει σε όλο τους το μεγαλείο τις ιδιαίτερες ιδιότητες των καταστάσεων διεμπλοκής EPR. Η λογική του είναι πολύ απλή. Ένα τρίτο πρόσωπο που βρίσκεται σε κάποιο ενδιάμεσο σημείο της γραμμής επικοινωνίας, ετοιμάζει ζεύγη φωτονίων σε κατάσταση διεμπλοκής. Οι καταστάσεις διεμπλοκής των φωτονίων, είναι ανάλογες με αυτές των ηλεκτρονίων, μόνο που το κριτήριο δεν είναι το spin αν είναι πάνω ή κάτω, αλλά η διεύθυνση της γραμμικής τους πόλωσης αν είναι ο άξονας x ή ο άξονας y. Μια τέτοια κατάσταση διεμπλοκής είναι η λεγόμενη κατάσταση Aspect :

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|x\rangle|x\rangle + |y\rangle|y\rangle) \quad \textbf{(8-3)}$$

Αφού λοιπόν το τρίτο πρόσωπο ετοιμάσει τα ζεύγη, τα στέλνει προς τις δύο αντίθετες κατευθύνσεις στις άκρες του καναλιού επικοινωνίας που βρίσκονται η Alice και ο Bob. Έστω ότι η Alice βρίσκεται πλησιέστερα και λαμβάνει πρώτη τα φωτόνιά της. Τα μετράει λοιπόν με ένα γραμμικό πολωτή προσανατολισμένο κατά τον άξονα x και καταγράφει 0 αν διέλθουν και 1 αν δεν διέλθουν. Όμως λόγω της διεμπλοκής των καταστάσεων των φωτονίων, όταν ο Bob μετρήσει τα δικά του φωτόνια, αυτά λόγω της χαρακτηριστικής ιδιότητας αυτών των καταστάσεων, για κάθε φωτόνιο ενός ζεύγους θα μετρήσει ακριβώς το ίδιο αποτέλεσμα με την Alice. Πράγματι η Alice όταν μετρήσει λόγω της μορφής της επαλληλίας της κατάστασης $|\psi\rangle$, έχει 50% πιθανότητες να μετρήσει 0 και άλλες τόσες να μετρήσει 1. Η μέτρηση όμως αυτή έχει σαν αποτέλεσμα να αλλάξει η κατάσταση του ζεύγους και να μεταπέσει στην $|\psi'\rangle = |x\rangle|x\rangle$ αν η Alice μετρήσει 0 ή στην $|\psi''\rangle = |y\rangle|y\rangle$ αν η Alice μετρήσει 1. Έτσι αν η Alice μετρήσει 0 και ο Bob θα μετρήσει 0, ενώ αν η Alice μετρήσει 1 και ο Bob θα μετρήσει 1. Έτσι έχει γίνει η διανομή του κλειδιού.

Μένει τώρα να δούμε γιατί δεν μπορεί η Eve να υποκλέψει την επικοινωνία. Το δυνατό σημείο της μεθόδου σε αυτό το θέμα, είναι ότι κανένας δεν μπορεί να γνωρίζει την κατάσταση του κάθε φωτονίου ούτε καν αυτός που τα παρήγαγε. Κι αυτό γιατί αρχικά βρίσκονται σε κατάσταση επαλληλίας, δηλαδή ταυτόχρονα και στην κατάσταση $|x\rangle$ και στην κατάσταση $|y\rangle$. Και έτσι αν κάποιος προσπαθήσει να μετρήσει την κατάσταση τους, τότε λόγω της μέτρησης θα την αλλάξει και έτσι αυτό θα γίνει εύκολα αντιληπτό. Έτσι αυτό που πρέπει να κάνουν η Alice και ο Bob είναι να διαλέξουν ένα τυχαίο δείγμα από m ζεύγη φωτονίων και να μετρήσουν τις διευθύνσεις πόλωσης τους σε μια κοινή κατεύθυνση όχι την ίδια σε όλα αυτά τα ζεύγη. Αν δεν έχει παρεμβληθεί κάποιος, τότε θα πρέπει να έχουν απόλυτη ταύτιση στα αποτελέσματα τους λόγω της διεμπλοκής. Αν πάλι έχει γίνει παρεμβολή, τότε η διεμπλοκή θα έχει καταστραφεί και έτσι θα υπάρχει ταύτιση μόνο σε εκείνες τις περιπτώσεις που η Eve θα έχει διαλέξει την ίδια διεύθυνση μέτρησης με την Alice και τον Bob. Έτσι τελικά για να γίνει αυτός ο έλεγχος, θα πρέπει αυτός που θα δημιουργήσει και θα στείλει τα φωτόνια, να μη στείλει μόνο τα N του μήκους του μηνύματος (κλειδιού), αλλά και ακόμα m ώστε με τα m να γίνει ο έλεγχος παρεμβολής και στη συνέχεια αυτά να τα αγνοήσουν.

8.2 Κρυπτογράφηση με δημόσιο κλειδί

Στην περίπτωση τώρα του δημόσιου κλειδιού, η Alice και ο Bob δημοσιεύουν το κλειδί το οποίο είναι έτσι προσβάσιμο σε οποιονδήποτε. Η Alice με αυτό το κλειδί κωδικοποιεί το μήνυμα που θέλει να στείλει και η λογική της μεθόδου είναι ότι ένας κατάσκοπος παρόλο που γνωρίζει το κλειδί, δεν μπορεί να αποκωδικοποιήσει το μήνυμα. Για την ακρίβεια το «δεν μπορεί» δεν είναι η σωστή έκφραση. Η Alice πρέπει να έχει κωδικοποιήσει το μήνυμα με έξυπνο και μη τετριμμένο τρόπο ώστε να είναι εξαιρετικά δύσκολο (αν και όχι αδύνατο), να γίνει αποκωδικοποίηση από κάποιον που γνωρίζει μόνο το δημόσιο κλειδί. Έτσι οι κρυπτογραφήσεις που γίνονται με αυτόν τον τρόπο, λύνουν το πρόβλημα της ασφαλούς αποστολής του κλειδιού. Ένα παράδειγμα που συνηθίζεται να δίνεται για την κατανόηση αυτής μεθόδου κρυπτογράφησης, είναι ότι ο αποστολέας στέλνει ένα κουτί στον παραλήπτη με ένα λουκέτο ανοικτό, το κλειδί του οποίου έχει μόνο ο αποστολέας. Το λουκέτο είναι το δημόσιο κλειδί ενώ το κλειδί του λουκέτου είναι το ιδιωτικό. Ο

παραλήπτης βάζει μέσα στο κουτί ότι θέλει και στη συνέχεια κλείνει το λουκέτο το οποίο δεν μπορεί να ανοίξει ούτε ο ίδιος ούτε και κανένας άλλος εκτός από τον αποστολέα που κατέχει το (ιδιωτικό) κλειδί. Τελικά το κουτί ξαναφτάνει στον αποστολέα ο οποίος το ανοίγει. Παρόλα αυτά, η μέθοδος αυτή δεν έγινε ευρέως αποδεκτή μέχρι τα μέσα της δεκαετίας του 70 όταν προτάθηκε ανεξάρτητα από τους Whitfield Diffie και Martin Hellman και τον Ralph Merkle, προκαλώντας επανάσταση στο πεδίο της κρυπτογραφίας. Λίγο καιρό αργότερα οι Ronald Rivest, Adi Samir και Leonard Adleman ανέπτυξαν τη μέθοδο κρυπτογράφησης RSA η οποία μέχρι σήμερα είναι η πιο διαδεδομένη στην πράξη μέθοδος κρυπτογράφησης με δημόσιο κλειδί διότι θεωρείται ότι προσφέρει ισορροπία μεταξύ ασφάλειας και πρακτικής εφαρμογής. Το 1997 αποκαλύφθηκε ότι αυτές οι μέθοδοι είχαν εφευρεθεί από τη δεκαετία του 1970 από ερευνητές οι οποίοι εργάζονταν στη Βρετανική Υπηρεσία Πληροφοριών GCHQ. Όπως αναφέρθηκε, η λογική της μεθόδου με δημόσιο κλειδί είναι ότι είναι εξαιρετικά δύσκολο να γίνει αποκρυπτογράφηση του μηνύματος με γνώση μόνο του (δημόσιου) κλειδιού. Για παράδειγμα η αποκωδικοποίηση μηνύματος το οποίο έχει κωδικοποιηθεί με τη μέθοδο RSA, είναι ένα πρόβλημα που η λύση του ισοδυναμεί με τη λύση ενός άλλου διάσημου προβλήματος, αυτού της παραγοντοποίησης ενός αριθμού σε πρώτους παράγοντες. Έτσι η ασφάλεια της μεθόδου RSA βασίζεται στην πεποίθηση ότι η παραγοντοποίηση ενός πολύ μεγάλου αριθμού, είναι ένα πρόβλημα πολύ δύσκολο να λυθεί με κλασικούς υπολογιστές. Όμως ο αλγόριθμος του Shor για παραγοντοποίηση σε κβαντικούς υπολογιστές που προτάθηκε αργότερα όπως είδαμε, υπόσχεται ακριβώς τη γρήγορη λύση αυτού του προβλήματος και άρα θα μπορούσε να χρησιμοποιηθεί για να «σπάσει» την RSA! Ομοίως και άλλες μέθοδοι κρυπτογράφησης με δημόσιο κλειδί θα μπορούσαν να «σπάσουν» αν ήταν γνωστοί και άλλοι γρήγοροι αλγόριθμοι για τη λύση λογαριθμικών προβλημάτων. Είναι λοιπόν εντυπωσιακό το πώς η μια μεγάλη ανακάλυψη θα μπορούσε να χρησιμοποιηθεί για να ακυρώσει την άλλη!

9. Γενική Θεώρηση-Σύνοψη

Στην εργασία αυτή έγινε μια σύντομη μελέτη της ιστορίας και της παρούσας κατάστασης των εξελίξεων στο πεδίο της κβαντικής πληροφορίας και υπολογιστικής. Σε αυτό το κεφάλαιο θα γίνει μια γενική θεώρηση για το πώς οι επιστήμες οι οποίες εμπλέκονται σε αυτά τα πεδία έρευνας, δηλαδή η Φυσική και η υπολογιστική, βοήθησαν και θα μπορούσαν να βοηθήσουν στο μέλλον η μια την άλλη. Επίσης θα γίνει μια σύνοψη των κυριότερων σημείων της εργασίας αυτής.

9.1 Γενική θεώρηση

Η κβαντική υπολογιστική και η κβαντική θεωρία της πληροφορίας, μας έμαθαν και μας μαθαίνουν, πώς να σκεφτόμαστε με λογική Φυσικής κάνοντας υπολογιστική και αυτός ο τρόπος οδήγησε σε πολλές καινούργιες και συναρπαστικές δυνατότητες στα πεδία της πληροφορίας και επικοινωνίας. Οι επιστήμονες των υπολογιστών και οι θεωρητικοί της πληροφορίας έχουν πια εφοδιαστεί με ένα νέο και πλούσιο οπλοστάσιο για να κάνουν την έρευνα τους. Αυτό που έγινε κατανοητό τελικά, είναι ότι κάθε φυσική θεωρία και όχι μόνο η κβαντική μηχανική, θα μπορούσε να είναι το θεμέλιο για μια θεωρία μετάδοσης πληροφορίας και επικοινωνίας. Οι καρποί αυτού του τρόπου σκέψης ίσως μια μέρα να είναι, η πληροφορία και η επικοινωνία να φτάσει σε επίπεδα πολύ πιο προχωρημένα απ' τα σημερινά κάτι το οποίο θα επηρεάσει συνολικά την κοινωνία.

Το πεδίο της κβαντικής πληροφορίας και υπολογιστικής θα μπορούσε να λειτουργήσει και αντίστροφα. Δηλαδή θα μπορούσε και η Φυσική να ωφεληθεί από την πρόοδο στο πεδίο της κβαντικής πληροφορίας και υπολογιστικής. Υπάρχει η πεποίθηση ότι όπως έμαθαν οι ερευνητές της πληροφορικής να σκέφτονται με λογική Φυσικής κάνοντας υπολογιστική, έτσι θα μπορούσαν και οι συνάδελφοι τους Φυσικοί, να μάθουν να σκέφτονται με λογική υπολογιστικής ερευνώντας τη Φυσική. Έτσι ενώ η Φυσική παραδοσιακά στοχεύει στην κατανόηση θεμελιωδών εννοιών και συστημάτων, πολλές ενδιαφέρουσες πλευρές της Φύσης αναδύονται όταν τα υπό μελέτη συστήματα γίνονται μεγαλύτερα και πολυπλοκότερα. Η Χημεία και η Μηχανολογία ασχολούνται με τέτοια πολύπλοκα συστήματα σε κάποιο βαθμό, αλλά περισσότερο με τρόπο κάνοντας υποθέσεις για να

εξηγήσουν αυτά που θέλουν και όχι θεμελιώνοντας μια θεωρία. Με τη μελέτη της κβαντικής υπολογιστικής και πληροφορίας, είναι διαθέσιμο ένα νέο ισχυρό εργαλείο για να διαβούμε το χάσμα ανάμεσα στο μικρό και στο περισσότερο σύνθετο. Ήδη εφαρμόζοντας ιδέες απ' αυτά τα πεδία, έχουν αρχίσει να διαφαίνονται καινούργιες προοπτικές για τη Φυσική. Και είναι βάσιμη η ελπίδα, ότι αυτό θα συνεχιστεί στο μέλλον και θα αποδώσει τελικά σημαντικά καλύτερη κατανόηση της φύσης από τη Φυσική.

9.2 Σύνοψη

Παρακάτω ακολουθεί μια περίληψη των κυριοτέρων σημείων αυτής της εργασίας :

Η βασική ιδέα είναι, να χρησιμοποιηθεί η κβαντική μηχανική σαν βάση για την ανάπτυξη τεχνολογίας για υπολογιστική και πληροφορία. Το πλεονέκτημα που δίνει αυτή η ιδέα, είναι το ότι, ένα κβαντικό σύστημα (qubit) μπορεί να βρεθεί και σε κατάσταση επαλληλίας, δηλαδή κατά κάποιο τρόπο σε πολλές καταστάσεις ταυτόχρονα, άρα οι διάφοροι υπολογισμοί σε έναν υποθετικό κβαντικό υπολογιστή θα μπορούσαν να γίνουν με πολύ μεγαλύτερες ταχύτητες από έναν κλασικό, ο οποίος μπορεί να επεξεργάζεται μόνο μια κατάσταση κάθε φορά. Αν δε, έχουμε σύστημα από πολλά qubits, τότε υπάρχουν και οι καταστάσεις διεμπλοκής στις οποίες η μέτρηση ενός qubit καθορίζει το αποτέλεσμα των μετρήσεων στα άλλα κάτι που αυξάνει κατά πολύ τις προσδοκίες. Έτσι, αν πραγματοποιούταν η κατασκευή του, ένας κβαντικός υπολογιστής θα μπορούσε να λύσει προβλήματα που θεωρούνται άλυτα (ή θα απαιτούσαν πάρα πολύ χρόνο), από έναν κλασικό. Βέβαια όλα αυτά προφανώς, στην εφαρμογή τους έχουν μεγάλες δυσκολίες. Η πρώτη απ' αυτές, δημιουργεί η ίδια η φύση της κβαντικής μηχανικής και συγκεκριμένα η διαδικασία της μέτρησης, η οποία καταστρέφει την κατάσταση που υπήρχε πριν απ' αυτήν και έτσι χάνεται ένα σημαντικό μέρος της πληροφορίας. Για να μπορέσει να ξεπεραστεί αυτή η δυσκολία θα πρέπει να εφευρεθούν κατάλληλοι κβαντικοί αλγόριθμοι κάτι που έχει αποδειχθεί ιδιαίτερα δύσκολο. Παρόλα αυτά οι αλγόριθμοι Deutsch, Deutsch-Jozsa, Grover και Shor, έχουν δείξει καλά αποτελέσματα προς αυτήν την κατεύθυνση. Η δεύτερη δυσκολία, είναι η φυσική πραγματοποίηση των qubits και στη συνέχεια των κβαντικών πυλών και κβαντικών κυκλωμάτων. Έχουν χρησιμοποιηθεί διάφορες μέθοδοι γι' αυτό το σκοπό όπως οι παγίδες ιόντων (ion trap), η QED cavidy και η μέθοδος μαγνητικού

συντονισμού (NMR), οι οποίες έχουν ελπιδοφόρα αποτελέσματα. Άλλο ένα πεδίο στο οποίο η κβαντική πληροφορία θα μπορούσε να συνεισφέρει και το κάνει ήδη, είναι η κρυπτογραφία. Έχουν εφευρεθεί ήδη αξιόλογα πρωτόκολλα κβαντικής κρυπτογραφίας διανομής ιδιωτικού κλειδιού, όπως το πρωτόκολλο BB84 και το πρωτόκολλο EPR τα οποία ήδη έχουν διατεθεί στην αγορά και χρησιμοποιούνται. Μέχρι σήμερα δεν έχουμε κβαντικούς υπολογιστές οι οποίοι να λύνουν πρακτικά προβλήματα. Υπάρχουν όμως προσπάθειες στις οποίες έχει επιτευχθεί η δημιουργία και διεμπλοκή λίγων qubits και η συνέχιση με διαρκώς αυξανόμενο ρυθμό, αυτών των προσπαθειών, δείχνει την πίστη για την τελική θετική έκβαση του φιλόδοξου αυτού εγχειρήματος.

Βιβλιογραφία

Καραφυλλίδης Ι. (2015). *Κβαντική Υπολογιστική.* Αθήνα : Ελληνικά Ακαδημαϊκά Συγγράμματα και Βοηθήματα. Ανακτήθηκε από https://www.ebooks4greeks.gr/κβαντικη-υπολογιστικη

Τραχανάς Σ. (2009). *Κβαντομηχανική ΙΙ Θεμελιώδεις Αρχές και Μέθοδοι-Κβαντικοί Υπολογιστές.* Ηράκλειο: Πανεπιστημιακές Εκδόσεις Κρήτης.

Προύσαλης Κ.(2008). *Κβαντική Κρυπτογραφία & Κβαντική Κρυπτανάλυση* (Μεταπτυχιακή Διπλωματική Εργασία). Πανεπιστήμιο Αιγαίου, Σάμος.

Κερμεζής Ν. (2013). *Κβαντικοί Υπολογιστές* (Διπλωματική Εργασία). Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Θεσσαλονίκη.

Aitchison I J R, Hey A J G. (2003). *Gauge Theories in Particle Physics Volume 1.* London: Taylor & Francis.

Nielsen M. & Chuang I. (2010). *Quantum Computation and Quantum Information.* Cambridge : Cambridge University Press.

Deutsch D. (2017). *Lectures on Quantum Computation by David Deutsch.* Ανακτήθηκε Σεπτέμβριος 2017 , από http://www.quiprocone.org/Protected/DD_lectures.htm

Morin D. (2016). *Morin David notes*. Ανακτήθηκε Οκτώβρης 2016, από www.people.fas.harvard.edu/~djmorin/waves/normalmodes.pdf

Eli Biham, Michel Boyer, Gilles Brassard, Jeroen van de Graaf, and Tal Mor. *Security of Quantum Key Distribution against All Collective Attacks.* Technical Report quantph/9801022, Computing Research Repository, 1998.

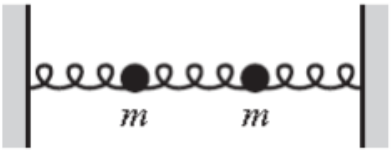
Bennett, Ch.H., G. Brassard and A. Ekert. *Quantum Cryptography*. Scientific Am. 267, 26-33 (int. ed.), 1992c.

G. Brassard. *Cryptography column Quantum cryptography: A*

bibliography. Sigact News, 24(3): 1620, 1993

Παράρτημα Α: Κανονικοί τρόποι ταλάντωσης-Φωνόνια

Έστω η διάταξη στο Σχήμα 0-1, όπου φαίνονται δύο σώματα ίδιας μάζας που συνδέονται με όμοια ελατήρια σταθεράς K.



Σχήμα 0-1 : Αλυσίδα δύο ατόμων που συνδέονται με όμοια ελατήρια.

Έστω q_1, q_2 οι μετατοπίσεις της αριστερής και της δεξιάς μάζας αντίστοιχα από τη θέση ισορροπίας τους. Τα q_1 και q_2 συνδέονται με τις θέσεις x_1 και x_2 των σωμάτων, με τις σχέσεις $q_i=x_i-x_{io}$, i=1,2 όπου x_{io} είναι οι θέσεις των σημείων ισορροπίας των δύο μαζών. Έτσι το πρώτο ελατήριο είναι παραμορφωμένο κατά q_1, το τρίτο κατά q_2 και το μεσαίο κατά q_2-q_1. Με βάση αυτά, η εφαρμογή του 2^{ου} νόμου του Newton για τις δύο μάζες δίνει:

$$m\ddot{q}_1 = -\mathrm{K}q_1 - \mathrm{K}(q_1 - q_2) = -2\mathrm{K}q_1 + \mathrm{K}q_2 \qquad \textbf{(0-1)}$$

$$m\ddot{q}_2 = -\mathrm{K}q_2 - \mathrm{K}(q_2 - q_1) = -2\mathrm{K}q_2 + \mathrm{K}q_1 \qquad \textbf{(0-2)}$$

Οι όροι $\mathrm{K}(q_1 - q_2)$ των εξισώσεων, που οφείλονται στη δύναμη που ασκεί το μεσαίο ελατήριο στις δύο μάζες, έχουν αντίθετο πρόσημο προφανώς λόγω δράσης-αντίδρασης. Για να βρούμε τη δυναμική ενέργεια V του συστήματος, βασιζόμαστε στις σχέσεις :

$$F_i = m\ddot{q}_i = -\frac{\partial V}{\partial q_i} \qquad \textbf{(0-3)}$$

όπου F_i η συνολική δύναμη που δέχεται το i σωμάτιο. Έτσι έχουμε τις σχέσεις :

$$\frac{\partial V}{\partial q_1} = 2\mathrm{K}q_1 - \mathrm{K}q_2 \qquad \textbf{(0-4)}$$

$$\frac{\partial V}{\partial q_2} = 2\mathrm{K}q_2 - \mathrm{K}q_1 \qquad \textbf{(0-5)}$$

Το σύστημα αυτών των εξισώσεων λύνεται εύκολα. Συγκεκριμένα η πρώτη δίνει :

$$V(q_1, q_2)=Kq_1^2-Kq_1q_2+f(q_2) \qquad \textbf{(0-6)}$$

ενώ η δεύτερη δίνει :

$$V(q_1, q_2)=Kq_2^2-Kq_1q_2+g(q_1) \quad \textbf{(0-7)}$$

Άρα αφού τα πρώτα μέλη είναι ίσα, θα είναι $f(q_2)= Kq_2^2$ και $g(q_1)= Kq_1^2$.

Έτσι τελικά έχουμε :

$$V(q_1, q_2)=Kq_1^2+Kq_2^2-Kq_1q_2 \quad \textbf{(0-8)}$$

που παρατηρούμε ότι υπάρχει και ο όρος αλληλεπίδρασης $-Kq_1q_2$.

Η κινητική ενέργεια του συστήματος είναι :

$$T=\frac{1}{2}m\dot{q}_1^2+\frac{1}{2}m\dot{q}_2^2 \quad \textbf{(0-9)}$$

και άρα η ολική ενέργεια είναι H=T+V.

Για να εξαλείψουμε τον όρο αλληλεπίδρασης στη δυναμική ενέργεια αλλά και για να λύσουμε το σύστημα, εισάγουμε τις μεταβλητές :

$$Q_1=\frac{q_1+q_2}{\sqrt{2}} \text{ και } Q_2=\frac{q_1-q_2}{\sqrt{2}} \quad \textbf{(0-10)}$$

οι οποίες λέγονται *κανονικές συντεταγμένες*. Προσθέτοντας και αφαιρώντας τις εξισώσεις (0-1) και (0-2), έχουμε :

$$m(\ddot{q}_1+\ddot{q}_2)=-K(q_1+q_2) \quad \textbf{(0-11)}$$

$$m(\ddot{q}_1-\ddot{q}_2)=-3K(q_1-q_2) \quad \textbf{(0-12)}$$

και με χρήση των (0-10), έχουμε :

$$m\ddot{Q}_1=-KQ_1 \quad \textbf{(0-13)}$$

$$m\ddot{Q}_2=-3KQ_2 \quad \textbf{(0-14)}$$

Η λύση τώρα αυτού του συστήματος προκύπτει πολύ εύκολα και είναι η :

$$Q_1(t)=A\cos(\omega_1 t)+B\sin(\omega_1 t) \quad \textbf{(0-15)}$$

$$Q_2(t)=C\cos(\omega_2 t)+D\sin(\omega_2 t) \quad \textbf{(0-16)}$$

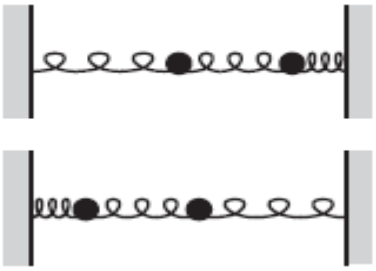
δηλαδή τα Q_1 και Q_2 ταλαντώνονται ανεξάρτητα με συχνότητες αντίστοιχα :

$$\omega_1=\left(\frac{K}{m}\right)^{1/2} \text{ και } \omega_2=\left(\frac{3K}{m}\right)^{1/2} \quad \textbf{(0-17)}$$

Οι δύο αυτές ταλαντώσεις ονομάζονται *κανονικοί τρόποι ταλάντωσης* και για να παρατηρηθούν, πρέπει οι αρχικές συνθήκες να είναι τέτοιες ώστε να διεγείρεται μόνο η μια κάθε φορά. Συγκεκριμένα, για αρχικές συνθήκες :

$q_1(0) = q_2(0) = \alpha$ και $\dot{q}_1(0) = \dot{q}_2(0) = 0$ δηλαδή $Q_2(0) = \dot{Q}_2(0) = \dot{Q}_1(0) = 0$ και $Q_1(0) = \sqrt{2}\alpha$, έχουμε $Q_1(t) = \sqrt{2}\alpha\cos(\omega_1 t)$ και $Q_2(t) = 0$.

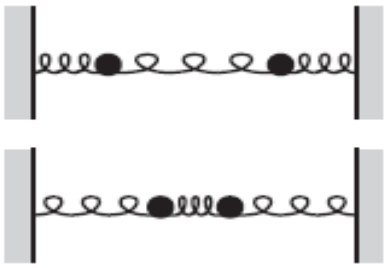
Αυτό σημαίνει ότι $q_1(t) = q_2(t) = \alpha\cos(\omega_1 t)$, δηλαδή οι δύο μάζες ταλαντώνονται ακριβώς με τον ίδιο τρόπο και ίδια φάση, με συχνότητα ω_1 (Σχήμα 0-2). Ο τρόπος αυτός ταλάντωσης ονομάζεται *κοινός τρόπος (common mode).*



Σχήμα 0-2: Κανονικός τρόπος ταλάντωσης με συχνότητα ω_1.

Για αρχικές συνθήκες $q_1(0) = \alpha, q_2(0) = -\alpha$ και $\dot{q}_1(0) = \dot{q}_2(0) = 0$ δηλαδή $Q_1(0) = \dot{Q}_2(0) = \dot{Q}_1(0) = 0$ και $Q_2(0) = \sqrt{2}\alpha$, έχουμε $Q_2(t) = \sqrt{2}\alpha\cos(\omega_2 t)$ και $Q_1(t) = 0$.

Αυτό σημαίνει ότι $q_1(t) = \alpha\cos(\omega_2 t)$ και $q_2(t) = -\alpha\cos(\omega_2 t)$ δηλαδή οι δύο μάζες ταλαντώνονται με διαφορά φάσης π rad (Σχήμα 0-3).



Σχήμα 0-3 : Κανονικός τρόπος ταλάντωσης με συχνότητα ω_2.

Για να υπολογίσουμε τώρα την κινητική, τη δυναμική και την ολική ενέργεια σε συνάρτηση με τα Q_1, Q_2, λύνουμε τις (0-10) ως προς q_1 και q_2 και έχουμε :

$$q_1 = \frac{Q_1 + Q_2}{\sqrt{2}} \text{ και } q_2 = \frac{Q_1 - Q_2}{\sqrt{2}} \quad \textbf{(0-18)}$$

Αντικαθιστώντας τις (0-18) στην (0-9), έχουμε με λίγες πράξεις :

$$\mathbf{T}=\frac{1}{2}m\dot{Q}_1^{\,2} + \frac{1}{2}m\dot{Q}_2^{\,2} \quad \textbf{(0-19)}$$

Από τις εξισώσεις (0-17) έχουμε $K=m\omega_1^{\,2}$ και $3K=m\omega_2^{\,2}$. Αντικαθιστώντας τις (0-18) στην (0-8) έχουμε :

$$V = \frac{K}{2}(Q_1^{\,2} + 3Q_2^{\,2}) = \frac{1}{2}KQ_1^{\,2} + \frac{1}{2}3KQ_2^{\,2}$$

ή τελικά :

$$V = \frac{1}{2}m\omega_1^{\,2}Q_1^{\,2} + \frac{1}{2}m\omega_2^{\,2}Q_2^{\,2} \quad \textbf{(0-20)}$$

Έτσι τελικά η ολική ενέργεια είναι :

$$\mathbf{H}=\frac{1}{2}m\dot{Q}_1^{\,2} + \frac{1}{2}m\dot{Q}_2^{\,2} + \frac{1}{2}m\omega_1^{\,2}Q_1^{\,2} + \frac{1}{2}m\omega_2^{\,2}Q_2^{\,2} \quad \textbf{(0-21)}$$

Δηλαδή όταν η ολική ενέργεια εκφραστεί σε σχέση με τις κανονικές συντεταγμένες, η έκφρασή της δεν περιέχει όρους αλληλεπίδρασης Q_1Q_2 άρα είναι σαν να έχουμε δύο ανεξάρτητους αρμονικούς (υποθετικούς) ταλαντωτές με συχνότητες ω_1 και ω_2.

Αν περάσουμε τώρα στην περίπτωση των N ατόμων, με την ίδια λογική που αναπτύχθηκε για N=2, σε συνάρτηση με τις πραγματικές μετατοπίσεις των μαζών q_i , η ενέργεια του συστήματος είναι :

$$\mathbf{H}=\sum_{i=1}^{N}\frac{1}{2}m\dot{q}_i^{\,2} + V(q_1, q_2, ..., q_N) \quad \textbf{(0-22)}$$

η οποία περιλαμβάνει και τους όρους αλληλεπίδρασης μεταξύ των q_i. Θεωρώντας τους μετασχηματισμούς :

$$Q_i = \sum_{s=1}^{N}\alpha_{is}q_i \quad \textbf{(0-23)}$$

οι οποίοι είναι ανάλογοι με τις σχέσεις (0-10) αλλά όχι τόσο απλές όσο αυτές, είναι δυνατόν να μετατρέψουμε τη σχέση (0-22), σαν άθροισμα ως προς τα Q_i χωρίς όρους αλληλεπίδρασης όπως η σχέση (0-21), δηλαδή στη μορφή :

$$\mathbf{H}=\sum_{i=1}^{N}(\frac{1}{2}m\dot{Q}_i^{\,2}+\frac{1}{2}m\omega_i^{\,2}Q_i^{\,2}) \qquad \textbf{(0-24)}$$

Οι Q_i είναι οι κανονικές συντεταγμένες και οι ω_i είναι οι συχνότητες των κανονικών τρόπων ταλάντωσης οι οποίες αποδεικνύεται ότι είναι (Morin D. , σχέση 63) :

$$\omega_i = 2\omega_o \sin[\frac{i\pi}{2(N+1)}] \qquad \textbf{(0-25)}$$

$$\text{με } \omega_o=(\frac{K}{m})^{1/2} \text{ και } i \text{ ακέραιος με } 1\le i\le N$$

Δηλαδή με βάση τις κανονικές συντεταγμένες, το σύστημα μπορεί να θεωρηθεί ότι αποτελείται από N ανεξάρτητους ταλαντωτές και ας μη συμβαίνει αυτό στην πραγματικότητα.

Αν τώρα θεωρήσουμε το σύστημα ότι είναι ένα στερεό σώμα, τότε επιβάλλεται να το θεωρήσουμε κβαντικό σύστημα. Είναι γνωστό τώρα από τη στοιχειώδη κβαντική μηχανική ότι η ενέργεια ενός αρμονικού ταλαντωτή συχνότητας ω_i, δίνεται απ' τη σχέση :

$$\varepsilon_i = (n_i+\frac{1}{2})\hbar\omega_i, n_i = 0,1,2.... \qquad \textbf{(0-26)}$$

που είναι κβαντισμένη, σε αντίθεση φυσικά με την αντίστοιχη κλασική περίπτωση. Η συνολική ενέργεια άρα των N ανεξάρτητων ταλαντωτών θα δίνεται απ' τη σχέση :

$$H=\sum_{i=1}^{N}(n_i+\frac{1}{2})\hbar\omega_i, n_i = 0,1,2... \qquad \textbf{(0-27)}$$

Άρα λοιπόν με βάση τα προηγούμενα, ξεχνάμε τους αρχικούς βαθμούς ελευθερίας $q_1,q_2,\ldots,q_N$ και τα πραγματικά N σωματίδια (άτομα) και επικεντρωνόμαστε στις κανονικές συντεταγμένες $Q_1,Q_2,\ldots,Q_N$ και θεωρούμε κάποια άλλα υποθετικά σωματίδια που ονομάζονται *κβάντα*, τα οποία ταλαντώνονται ανεξάρτητα με συχνότητες ω_i. Αυτή είναι η λογική της κβάντωσης ενός πεδίου (η σωματιδιακή φύση), που χρησιμοποιείται στις θεωρίες της Φυσικής Στοιχειωδών Σωματιδίων. Στην περίπτωση του στερεού, αυτά τα κβάντα του πεδίου, μια και πρόκειται για ηχητικό κύμα ονομάζονται *φωνόνια*, κατ' αναλογία με τα κβάντα του ηλεκτρομαγνητικού κύματος που ονομάζονται φυσικά, *φωτόνια*.

Υπεύθυνη Δήλωση Συγγραφέα:

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1986 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον.