Εθνικο Μετσοβιο Πολυτεχνειο
Σχολη Ηλεκτρολογων Μηχανικων και Μηχανικων Υπολογιστων
Τομεας Τεχνολογιας Πληροφορικης και Υπολογιστων

Τίτλος Διπλωματικής

Διπλωματικη Εργασια

της

ΗΛΙΑΝΑΣ Θ. ΜΠΕΤΣΟΥ

Επιβλέπων: Επιβλέπων
Τίτλος

Αθήνα, Ιούνιος 2019

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών

Τίτλος Διπλωματικής

Διπλωματικη Εργασια

της

ΗΛΙΑΝΑΣ Θ. ΜΠΕΤΣΟΥ

Επιβλέπων: Επιβλέπων
Τίτλος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την Ημερομηνία Παρουσίασης.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Επιβλέπων	1ος Εξεταστής	2ος Εξεταστής
Τίτλος	Τίτλος	Τίτλος

Αθήνα, Ιούνιος 2019

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών

Υπεύθυνη Δήλωση

Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας, και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Μηχανικών Πληροφορικής Τ.Ε. του ΤΕΙ Πελοποννήσου.

(Υπογραφή)

.....
Ηλιάνα Μπέτσου

Περίληψη

Λέξεις Κλειδιά

Abstract

Keywords

Αφιέρωση

Ευχαριστίες

Θα ήθελα καταρχήν να ευχαριστήσω τον καθηγητή κ. ..... για την επίβλεψη αυτής της διπλωματικής εργασίας και για την ευκαιρία που μου έδωσε να την εκπονήσω στο εργαστήριο Συστημάτων Βάσεων Γνώσεων και Δεδομένων. Επίσης ευχαριστώ ιδιαίτερα τον Δρ. ..... για την καθοδήγησή του και την εξαιρετική συνεργασία που είχαμε. Τέλος θα ήθελα να ευχαριστήσω τους γονείς μου για την καθοδήγηση και την ηθική συμπαράσταση που μου προσέφεραν όλα αυτά τα χρόνια.

Περιεχόμενα

Κεφάλαιο 1

Introduction and Overview

1.1 History

1.2 Future Directions

Κεφάλαιο 2

Fundamentals

2.1 Overview

2.2 Quantum Computation

2.2.1 Qubits

2.2.2 Quantum Circuits

2.3 The Dirac notation nad Hilbert spaces

2.4 Quantum Circuits

2.4.1 The quantum Circuit model

2.4.2 Quantum Gates

2.4.3 Universal Quantum Gates

Κεφάλαιο 3

Introduction to Computer Science

3.1 Overview

3.2 Turing Machines

3.3 Computanional Complexity

3.4 Problems in classes P and NP

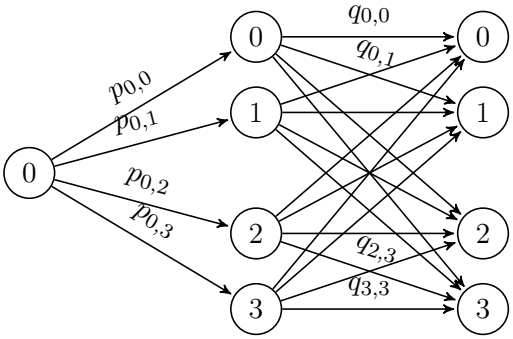
Κεφάλαιο 4

Quantum Algorithms

4.1 Probabilistic Versus Quantum Algorithms

Οι πιθανοτικοί αλγόριθμοι έχουν ευρεία χρήση στη θεωρητική πληροφορική καθώς χρησιμοποιούνται στη λύση πολλών διαφορετικών προβλημάτων. Σε αυτό το κεφάλαιο θα δούμε πως είναι δυνατό οι κβαντικοί αλγόριθμοι να αποτελέσουν μια γενίκευση των πιθανοτικών αλγορίθμων.

Θα ξεκινήσουμε με ένα απλό παράδειγμα ενός κλασσικού πιθανοτικού αλγόριθμου. Το παρακάτω σχήμα απεικονίζει τα πρώτα δύο βήματα ενός τέτοιου υπολογισμού σε έναν καταχωρητή ο οποίος μπορεί να βρίσκεται σε μια από τις τέσσερις καταστάσεις.

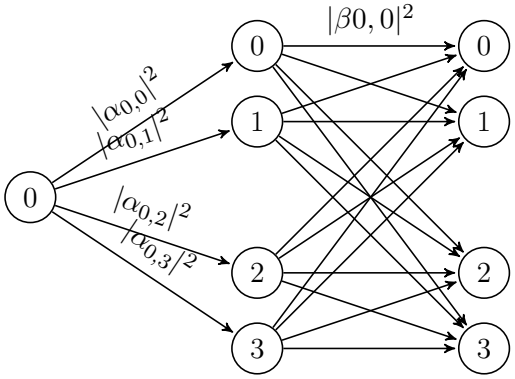


Αρχικοποιούμε τον καταχωρητή στο 0. Μετά το πρώτο βήμα, ο καταχωρητής είναι στην κατάσταση j με πιθανότητα $p_{0,j}$. Υποθέτουμε ότι θέλουμε να βρούμε τη συνολική πιθανότητα ότι ο υπολογισμός τερματίζει στην κατάσταση 3 μετά το δεύτερο βήμα. Αυτός ο υπολογισμός γίνεται σε δύο στάδια. Στο πρώτο υπολογίζουμε την πιθανότητα που σχετίζεται με τα διαφορετικά υπολογιστικά μονοπάτια τα οποία τερματίζουν στην κατάσταση 3 και στο δεύτερο προσθέτωντας τις πιθανότητες όλων αυτών των διαφορετικών μονοπατιών. Μπορούμε να μεταβούμε από την κατάσταση 0 στην κατάσταση j και στη συνέχεια από την κατάσταση j στην κατάσταση 3 με ένα από τα τέσσερα $j\epsilon 0, 1, 2, 3$. Όπως είναι ήδη γνωστό η πιθανότητα που σχετίζεται με καθένα από τα μονοπάτια βρίσκεται εάν πολλαπλασιάσουμε την πιθανότητα $p_{0,j}$ της μετάβασης από την 0 στην j με την πιθανότητα $q_{j,3}$ της μετάβασης από τη j στην 3. Η συνολική πιθανότητα να τερματίσουμε στην 3 δίνεται αν προσθέσουμε τις τέσσερις πιθανότητες που προκύπτουν. Όμως οι πιθανότητες αυτές που προκύπτουν είναι τα τετράγωνα

των χβαντικών πιθανοτικών πλατών. Δηλαδή $p_{0,j} = |\alpha_{0,j}|^2$ και $q_{j,k} = |\beta_{j,k}|^2$. Άρα το τελικό αποτέλεσμα που προκύπτει είναι [9]:

$$prob = \sum_j p_{0,j} q_{j,3}$$

Και εδώ έχουμε το προηγούμενο σχήμα με χρήση χβαντικών πλατών.



Αν μετρήσουμε την κατάσταση αμέσως μετά το πρώτο βήμα του υπολογισμού, η πιθανότητα να προκύψει το αποτέλεσμα 2 είναι:

$$prob = |\alpha_{0,2}|^2 = p_{0,2}$$

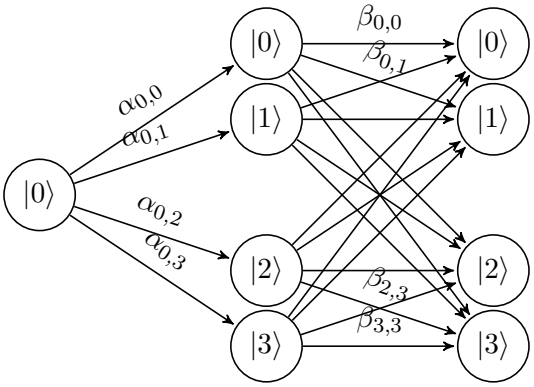
Και τελικά η συνολική πιθανότητα να μετρήσουμε το αποτέλεσμα 3 μετά το δεύτερο βήμα είναι:

$$\begin{aligned} prob_3 &= \sum_j |\alpha_{0,j}|^2 |\beta_{j,3}|^2 \\ &= \sum_j |\alpha_{0,j}\beta_{j,3}|^2 \end{aligned}$$

Παρότι στο συγκεκριμένο παράδειγμα κάναμε τις μετρήσεις αμέσως μετά από κάθε βήμα, σε ένα χβαντικό αλγόριθμο αυτό δεν είναι εφικτό. Αυτό σημαίνει ότι τα χβαντικά πλάτη θα μπορούσαν να επηρεάσουν το τελικό αποτέλεσμα. Δηλαδή αν μετρήσουμε τη συνολική πιθαντότητα να φτάσουμε στην τελική κατάσταση 3, μετά το δεύτερο βήμα, το αποτέλεσμα είναι διαφορετικό από ότι πριν γιατί δεν γνωρίζουμε τη διαδρομή που ακολούθησε ο αλγόριθμος μέχρι να φτάσει εκεί. Σε αυτή τη περίπτωση λοιπόν, αντί να προσθέσουμε τις πιθανότητες, προσθέτουμε τα πλάτη των πιθανοτήτων. Άρα η πιθανότητα να φτάσουμε στο αποτέλεσμα 3 μετά το δεύτερο βήμα προκύπτει από το τετράγωνο του συνολικού πλάτους της πιθαντότητας αυτής.

$$prob_3 = |\sum_j \alpha_{0,j}\beta_{j,3}|^2$$

Και λίγο πιο παραστατικά:



Όπως μπορούμε να δούμε, οι κλασσικοί πιθανοτικοί αλγόριθμοι μπορούν να προσομοιαστούν από τους κβανιτκούς αλγορίθμους. Είναι εφικτή όμως η αντίστροφη διαδικασία· Η αντικατάσταση μιας κβαντικής πύλης με μια πιθανοτική κλασσική πύλη μπορεί να δώσει τελείως διαφορετικά αποτελέσματα, άρα δεν είναι μια εφικτή λύση. Ωστόσο σε κάποιες συγκεκριμένες περιπτώσεις όπως τα κβαντικά κυκλώματα που χρησιμοποιούν μόνο πύλες $CNOT, H, X, Y, Z, T$, μπορούν να προσομοιαστούν σε έναν κλασσικό υπολογιστή. Μπορούμε να συμπεράνουμε ότι είναι πολύ πιθανό οι κβαντικοί αλγόριθμοι να επιλύουν πολύ πιο γρήγορα τα όποια προβλημάτα σε σχέση με τους κλασσικούς πιθανοτικούς αλγορίθμους.

4.2 Quantum Parallelism

Ο κβαντικός παραλληλισμός (*parallelism*) αποτελεί βασικό στοιχείο για πολλούς αλγόριθμους. Πολύ γενικά θα μπορούσαμε να πούμε ότι επιτρέπει σε έναν κβαντικό υπολογιστή να "άξιολογήσει" μια συνάρτηση $f(x)$ για πολλές διαφορετικές τιμές του x ταυτόχρονα.

Έστω ότι έχουμε μια συνάρτηση $f(x) : 0,1 \to 0,1$. Μπορούμε να υπολογίσουμε τη συνάρτηση αυτή θεωρώντας έναν κβαντικό υπολογιστή με δύο *qubits* που ξεκινάει με την κατάσταση $|x, y\rangle$. Με μια ακολουθία λογικών πυλών μπορούμε να το μετασχηματίσουμε στην κατάσταση $|x, y \oplus f(x)\rangle$. Ο πρώτος καταχωρητής ονομάζεται *data register* και ο δέυτερος *target register*. Ονομάζομε τον μετασχηματισμό $U_f = |x, y\rangle \to |x, y \oplus f(x)\rangle$.

Έστω ένα κύκλωμα που εφαρμόζει την U_f σε μια είσοδο αλλά όχι σε υπολογιστική βάση. Τότε ο *data register* είναι προετοιμασμένος για την υπέρθεση $(|0\rangle + |1\rangle)/\sqrt{2}$ το οποίο μπορούμε να το δημιουργήσουμε με μια πύλη $Hadamard$. Και εφαρμόζοντας την U_f έχουμε [11]:

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}}.$$

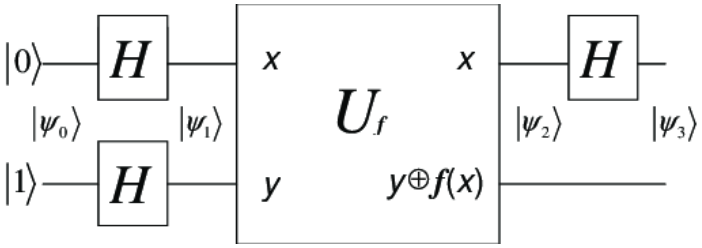
Και εδώ είναι το σημαντικότερο σημείο, γιατί οι διαφορετικοί όροι περιέχουν πληροφορίες τόσο για την $f(0)$ αλλά και για την $f(1)$ σχεδόν ταυτόχρονα. Αντίθετα με τον κλασσικό παραλληλισμό, όπου πολλαπλά κυκλώματα προσπαθούσαν να υπολογίσουν την $f(x)$ ταυτόχρονα, εδώ ένα και μόνο κύκλωμα υπολογίζει πολλαπλές τιμές χρησιμοποιώντας τη δυνατότητα των κβαντικών υπλογιστών να είναι σε υπερθέσεις διαφορετικών καταστάσεων.

Η παραπάνω διαδικασία/παράδειγμα θα μπορούσε να γενικευτεί σε συναρτήσεις με έναν τυχαίο αριθμό $bits$ χρησιμοποιώντας τη γενική διαδικασία $Hadamard\,Transform$ ή $Walsh-Hadamard\,Transform$. Η συγκεκριμένη διαδικασία είναι επί της ουσίας n πύλες $Hadamard$ που δρουν παράλληλα σε n $qubits$.

Παρότι ο κβαντικός παραλληλισμός μας δίνει τη δυνατότητα να ελέγξουμε όλες τις πιθανές τιμές της f ταυτόχρονα, δεν μπορεί να χρησιμοποιηθεί απευθείας. Στο παράδειγμα μας η μέτρηση της κατάστασης θα επέστρεφε είτε $|0, f(0)\rangle$ είτε $|1, f(1)\rangle$ μόνο. Στη γενική περίπτωση η μέτρηση της κατάστασης $\sum_x |x, f(x)\rangle$ θα έδινε μόνο $f(x)$ για μια μοναδική τιμή x, κάτι που θα μπορούσε να κάνει και ένας κλασσικός υπολογιστής. Ένας κβαντικός υπολογισμός, απαιτεί περισσότερα από έναν κβαντικό παραλληλισμό καθώς χρειάζεται την δυνατότητα να αντλεί πληροφορίες για παραπάνω από μια τιμή της $f(x)$ από την υπέρθεση της κατάστασης $\sum_x |x, f(x)\rangle$.

4.3 Deutsch's Algorithm

Ο κβαντικός αλγόριθμος του $Deutsch$ είναι ένας από τους πρώτους και πιο απλούς κβαντικούς αλγορίθους. Ο κβαντικός αλγόριθμος του $Deutsch$ συνδυάζει τον κβαντικό παραλληλισμό που είδαμε παραπάνω με κάποιες βασικά στοχεία της κβαντομηχανικής γνωστά ως "$interference$". Αρχικά θα χρησιμοποιήσουμε πάλι μια πύλη $Hadamard$ για να ετοιμάσουμε το πρώτο $qubit$ της υπέρθεσης $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, αλλά τώρα ετοιμάζουμε και ένα δέυτερο $qubit$, y σαν την υπέρθεση $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ χρησιμοποιώντας μια πύλη $Hadamard$ στην κατάσταση $|1\rangle$. Παρακάτω η διάταξη του αλγορίθμου:



Ας δούμε λίγο επιγραμματικά τον αλγόριθμο. Ο στόχος του αλγορίθμου δεν είναι να υπολογίσουμε όλες τις ξεχωριστές τιμές της $f(x)$, αλλά να ορίσουμε την τιμή της $f(0) \oplus f(1)$. Όπως είπαμε ξεκινάμε περίπου όπως στο παράδειγμα για τον κβαντικό παραλληλισμό. Αρχικά η κατάσταση του καταχωρητή είναι $|01\rangle$. Στη συνέχεια δρουν οι δύο πύλες $Hadamard$. Μετά ξεκινάει ο συνδυασμός κβαντικών πυλών U_f και ακολουθεί η πύλη στο πρώτο $qubit$. Μετράμε την κατάσταση του πρώτου $qubit$. Αν είναι στην κατάσταση $|0\rangle$, τότε η $f(x)$ είναι σταθερή [8] ενώ αν βρεθεί στην κατάσταση $|1\rangle$ η $f(x)$ είναι ισορροπημένη [3].

Πιο αναλυτικά, αρχικά δημιουργούμε την κβαντική εκδοχή του κυκλώματατος για την f, και έτσι μπορούμε να δώσουμε κβαντικά $qubits$ σαν είσοδο. Επίσης έχουμε ορίσει την U_f τέτοια ώστε αν θέσουμε το δεύτερο $qubit$ στην κατάσταση $|y\rangle = |0\rangle$, τότε το πρώτο $qubit$ που είναι στην κατάσταση $|x\rangle = |0\rangle$ θα δώσει $|0 \oplus f(0)\rangle = |f(0)\rangle$ στο δεύτερο $qubit$ και αν

έχουμε $|x\rangle = |1\rangle$ τότε το πρώτο *qubit* θα μας δώσει $|f(1)\rangle$. Βέβαια τα *qubits* εισόδου δεν είναι απαραίτητο να είναι σε μια μόνο κατάσταση, αλλά μπορεί να βρίσκονται σε μια υπέρθεση των $|0\rangle$ και $|1\rangle$. Κρατώντας το δεύτερο *qubit* στην κατάσταση $|y\rangle = |0\rangle$, θέτουμε το πρώτο *qubit* σαν την υπέρθεση των δυο καταστάσεων, άρα:

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

Επομένως η είσοδος που θα δώσουμε στην U_f είναι:

$$(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)|0\rangle \tag{4.1}$$

$$= \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|0\rangle \tag{4.2}$$

Η έξοδος της U_f είναι η εξής:

$$U_f(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle) = = \frac{1}{\sqrt{2}}U_f|00\rangle + \frac{1}{\sqrt{2}}U_f\rangle 10| = \tag{4.3}$$

$$= \frac{1}{\sqrt{2}}|0\rangle|0 \oplus f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|0 \oplus f(1)\rangle = \tag{4.4}$$

$$= \frac{1}{\sqrt{2}}|0\rangle|f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|0 \oplus f(1)\rangle \tag{4.5}$$

Αν μετρούσαμε τώρα την έξοδο σε υπολογιστική βάση, το αποτέλεσμα θα ήταν είτε $|0\rangle|f(0)\rangle$ είτε $|1\rangle|1 \oplus f(1)\rangle$. Μετά την μέτρηση, η κατάσταση της εξόδου θα είναι είτε $|f(0)\rangle$ είτε $|f(1)\rangle$. Όμως ο στόχος του αλγορίθμου δεν είναι να υπολογίσουμε όλες τις διαφορετικές τιμές της $f(x)$. Ο αλγόριθμος περιγράφει πως μπορούμε να χρησιμοποιήσουμε τους κβαντικούς μηχανισμούς ($interference$) για να βρουμε μια γενική πληροφορία για την f και πως μπορούμε να το κάνουμε αυτό πολύ πιο αποδοτικά σε σχέση με τον κλασσικό τρόπο. Αρχικά το πρώτο *bit* είναι στην κατάσταση $|0\rangle$ και το δεύτερο στην κατάσταση $\frac{|0\rangle - |1\rangle}{2}$. Πριν επιδράσει καμία πύλη, έχουμε ότι

$$|\psi_0\rangle = |0\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.6}$$

Αμέσως μετά την επίδραση της πρώτης πύλης $Hadamard$ στο πρώτο *qubit* η κατάσταση γίνεται:

$$|\psi_1\rangle = (\frac{1}{\sqrt{2}}|0\rangle) = \tag{4.7}$$

$$= \frac{1}{\sqrt{2}}|0\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) + \frac{1}{\sqrt{2}}|1\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.8}$$

Και στη συνέχεια επιδρά ο συνδυασμός πυλών U_f:

$$|\psi_2\rangle = \frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) + \frac{(-1)^{f(1)}}{\sqrt{2}}|1\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \tag{4.9}$$

$$= (\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \tag{4.10}$$

$$= (-1)^{f(0)}(\frac{|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.11}$$

Εδώ έχουμε μερικές διαφορετικές περιπτώσεις. Αν η f είναι σταθερή συνάρτηση, τότε έχουμε:

$$|\psi_2\rangle = (-1)^{f(0)}(\frac{|0\rangle + |1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.12}$$

Και άρα η η τελευταία πύλη $Hadamard$ στο πρώτο $qubit$ μας δίνει το εξής:

$$|\psi_3\rangle = (-1)^{f(0)}|0\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.13}$$

Αν όμως η f είναι ισορροπημένη, τότε έχουμε:

$$|\psi_2\rangle = (-1)^{f(0)}(\frac{|0\rangle - |1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.14}$$

και άρα η τελευταία πύλη μας δίνει:

$$|\psi_3\rangle = (-1)^{f(0)}|1\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.15}$$

Προσπαθώντας να γενικοποιήσουμε λίγο τον αλγόριθμο του Δευτσχη, αρχικά θα πρέπει να θυμόμαστε ότι η $U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$, μπορεί να αντιμετωπιστεί ως ένας $single-qubit$ $operator(\widehat{U_{f(x)}})$ του οποίου η επίδραση στο δεύτερο $qubit$ εξαρτάται από την κατάσταση του πρώτου $qubit$. Η κατάσταση $(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$ είναι μια ιδιοκατάσταση $(eigenstate)$ της $(\widehat{U_{f(x)}})$ με ιδιοτιμή την $(-1)^{f(x)}$. Κωδικοποιώντας αυτές τις ιδιοτιμές με βάση το $qubit$ ελέγχου, δηλαδή το πρώτο $qubit$ μπορούμε να προσδιορίσουμε το $f(0) \oplus f(1)$, προσδιορίζοντας τους σχετικούς συντελεστές φάσης ανάμεσα στα $|0\rangle$ και $|1\rangle$. Η διάκριση μεταξύ των $(\frac{|0\rangle+|1\rangle}{\sqrt{2}})$ και $(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$ γίνεται με την πύλη $Hadamard$ [9].

Κάτι άλλο που θα πρέπει να τονίσουμε είναι η δράση της πύλης $CNOT$. Όταν ο καταχωρητής αποτελείται από δυο $qubits$ οπως στην περίπτωση του αλγόριθμου του $Deutsch$, τότε η $CNOT$, δεν επηρεάζει την κατάσταση του πρώτου $qubit$, αλλα επιδρά στην κατάσταση του δεύτερου (εάν) το πρώτο βρίσκεται στην κατάσταση $|1\rangle$ [10].

Συνοψίζοντας ο αλγόριθμος του $Deutsch$ μας δίνει λύση στο εξής:

The Deutsch Problem
Input: Ένα μαύρο κουτί ($blackbox$) για τον υπολογισμό της άγνωστης συνάρτησης $f : 0, 1 \to 0, 1$
Problem: Προσδιόρισε την τιμή της $f(0) \oplus f(1)$ κάνοντας ερωτήματα ($queries$) στην f

4.4 Deutsch-Jozsa Algorithm

Ο αλγόριθμος που θα δούμε τώρα αποτελεί τη λύση σε ένα πρόβλημα που είναι γενίκευση του προβλήματος που είδαμε στον αλγόριθμο του *Deutsch*. Ο αλγόριθμος έχει ακριβώς την ίδια δομή και δέχεται μια άγνωστη συνάρτηση f που αυτή τη φορά είναι της μορφής:

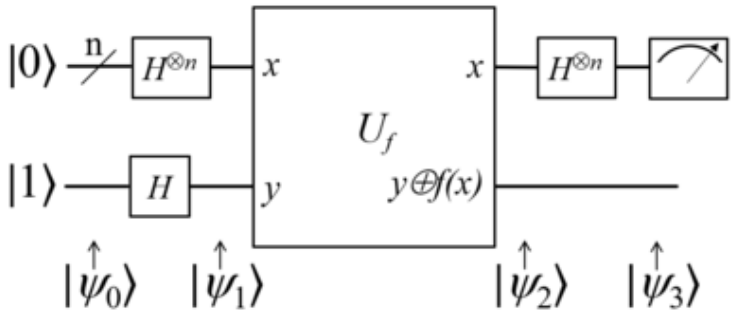
$$f : 0, 1^n \to 0, 1 \tag{4.16}$$

Επίσης η f, μπορεί να είναι είτε *constant* (σταθερή για κάθε x) είτε *balanced* (ισορροπημένη $f(x) = 0$ για τα μισά ακριβώς x, $f(x) = 1$ για τα υπόλοιπα x). Το ζητούμενο εδώ είναι να αποφασίσουμε αν τι είναι η f.

Ακολουθώντας την ίδια λογική που ακολουθήσαμε και στον προηγούμενο αλγόριθμο, θα ορίσουμε την κβαντική διαδικασία ως εξής:

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \otimes f(x)\rangle$$

Το κύκλωμα φαίνεται παρακάτω:



Σε σχέση με τον αλγόριθμο του *Deutsch*, εδώ αντί για μια απλή $1-qubit$ πύλη $Hadamard$, έχουμε n $1-qubit$ πύλες $Hadamard$ και συμβολίζεται ως $H^{\oplus n}$. Χρησιμοποιούμε το συμβολισμό $|0\rangle^{\otimes n}$ ή $|\mathbf{0}\rangle$ για την κατάσταση που είναι *tensor product* από n *qubits* το καθένα στην κατάσταση $|0\rangle$.

Ακολουθούμε λοιπόν την πορεία του κυκλώματος. Αρχική κατάσταση

$$|\psi_0\rangle = |0\rangle^{\oplus n}(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.17}$$

Υπολογίζοντας τη δράση ενός $n - qubit$ $Hadamard$ μετασχηματισμού στην κατάσταση $|0\rangle^{\oplus n}$

$$H^{\oplus n}|0\rangle^{\oplus 0} = (\frac{1}{\sqrt{2}})^n \underbrace{(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes ... \otimes (|0\rangle + |1\rangle)}_{n} \tag{4.18}$$

Και εξάγοντας, το *tensor product* μπορεί να γραφτεί σαν

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x\epsilon 0,1^n} |x\rangle \tag{4.19}$$

Αμέσως μετά την πρώτη $H^{\otimes n}$ ο αλγόριθμος είναι

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\epsilon 0,1^n} |n\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{4.20}$$

Η εγγραφή στον καταχωρητή είναι σε μια ισόβαρη υπέρθεση όλων των πιθανών $n-$ *bitstring* εισόδου. Τώρα δρα η U_f

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} U_f(\sum_{x\epsilon 0,1^n} |x\rangle (\frac{|0\rangle - |1\rangle}{\sqrt{2}})) = \tag{4.21}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x\epsilon 0,1^n} (-1)^{f(x)} |x\rangle (\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.22}$$

Η εγγραφή στον καταχωρητή είναι σε μια ισόβαρη υπέρθεση όλων των πιθανών $n-$ *bitstring* εισόδου. Τώρα δρα η U_f

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} U_f(\sum_{x\epsilon 0,1^n} |x\rangle (\frac{|0\rangle - |1\rangle}{\sqrt{2}})) = \tag{4.23}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{x\epsilon 0,1^n} (-1)^{f(x)} |x\rangle (\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.24}$$

Το $(-1)^{f(x)}$ είναι η μετατόπιση της φάσης, το οποίο έχει συνδεθεί με το πρώτο *qubit*.

Στη συνέχεια θα δούμε πως επιδρά η $n-ost$ πύλη $Hadamard$ στο $n-qubit$ βασικής κατάστασης $|x\rangle$.

$$H^{\otimes n}|x\rangle = H^{\otimes n}(|x_1\rangle|x_2\rangle...|x_n\rangle) = \tag{4.25}$$

$$= H|x_1\rangle H|x_2\rangle...H|x_n\rangle = \tag{4.26}$$

$$= \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_2}|1\rangle)...\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_n}|1\rangle) = \tag{4.27}$$

$$= \frac{1}{\sqrt{2}} \sum_{z_1 z_2 ... z_n \epsilon 0,1^n} (-1)^{x_1 z_1 + ... + x_n z_n} |z_1\rangle|z_2\rangle...|z_n\rangle \tag{4.28}$$

Το τελικό αποτέλεσμα μετά την επίδραση της $n-ostc$ πύλης $Hadamard$:

$$|\psi_3\rangle = (\frac{1}{\sqrt{2^n}} \sum_{x\epsilon 0,1^n} (-1)^{f(x)} \frac{1}{\sqrt{2^n}} \sum_{z\epsilon 0,1^n} (-1)^{xz} |z\rangle)(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \tag{4.29}$$

$$= \frac{1}{\sqrt{2^n}} \sum_{z\epsilon 0,1^n} (\sum_{x\epsilon 0,1^n} (-1)^{f(x)+xz}) |z\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{4.30}$$

Και στις δύο παραπάνω εκφράσεις, το $x.z$ ορίζει το εσωτερικό γινόμενο των $x, z, modulo2$. Στο τέλος του αλγορίθμου, η μέτρηση του πρώτου καταχωρητή είναι σε υπολογιστική βάση και για να το δούμε καλυτερα, θεωρούμε το τελικό πλάτος του $|z\rangle = |0\rangle^{\otimes n}$ στον πρώτο καταχωρητή κατάστασης $|\psi_3\rangle$, το οποίο είναι:

$$\frac{1}{2^n}\sum_{x\epsilon 0,1^n}(-1)^{f(x)} \tag{4.31}$$

Και τώρα έχουμε πάλι δύο περιπτώσεις.

1. Η f είναι *constant*, άρα το πλάτος του $|0\rangle^{\otimes n}$ είναι είτε $+1$ είτε -1 και επομένως η μέτρηση του πρώτου καταχωρητή είναι σίγουρο οτι θα μας επιστρέψει όλα τα 0.

2. Η f είναι *balanced*, άρα οι θετικές και αρνητικές συνιστώσες των πλατών αναιρούνται και το συνολικό πλάτος είναι $|0\rangle^{\otimes n} = 0$. Άρα η μέτρηση στον πρώτο καταχωρητή είναι βέβαιο ότι θα μας επιστρέψει όλες τις μη μηδενικές τιμές.

Βλέπουμε επομένως ότι είναι πολύ εύκολο ανάλογα με τη μέτρηση του πρώτου καταχωρητή να κρίνουμε αν η f είναι *balanced* ή *constant*.

Ένας κλασσικός αλγόριθμος για να δώσει απάντηση στο πρόβλημα του $Deutsch - Josza$ χρειάζεται $2^{n-1}+1$ *queries* στην χειρότερη περίπτωση. Ένας πιθανοτικός κλασσικός αλγόριθμος θα μπορούσε να το λύσει με $\frac{1}{3}$ πιθανότητα λάθους χρησιμοποιώντας 2 μόνο *queries*. Η πιθανότητα λάθους μειώνεται στο $\frac{1}{2^n}$ με $n+1 queries$. Βλέπουμε ότι η διαφορά μεταξύ της πολυπλοκότητας ενός κλασσικού πιθανοτικού *query* και της πολυπλοκότητας ενός κβαντικού υπολογιστικού *query*, είναι σταθερή στην περίπτωση ενλος σταθερού *error* και μετατρέπεται σε γραμμική διαφορά στην περίπτωση ενός μικρού εκθετικού *error* [9].

Τελικά συνοψίζοντας τον αλγόριθμο [11]:

Algorithm: Deutsch-Josza
Inputs:Ενα $blackboxU_f$ το οποίο εφαρμόζει τον εξής μετασχηματισμό $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$ για κάθε $x\epsilon 0, ..., 2^n - 1$ και $f(X)\epsilon 0, 1$. Η $f(x)$ μπορεί να είναι είτε *constant* είτε *balanced* για όλες τις τιμές του x.
Outputs: 0 ανν η f είναι *constant*.
Procedure:

1. $|0\rangle^{\otimes n}|1\rangle$ initialize state
2. $\rightarrow \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle[\frac{|0\rangle-|1\rangle}{\sqrt{2}}]$ create superposition using Hadamard gates
3. $\rightarrow \sum_x(-1^f(x))|x\rangle[\frac{|0\rangle-|1\rangle}{\sqrt{2}}]$ calculate function f using U_f
4. $\longrightarrow \sum_z\sum_x \frac{(-1)^{xz+f(x)}|z\rangle}{\sqrt{2^n}}[\frac{|0\rangle-|1\rangle}{\sqrt{2}}]$ perform Hadamard Transform
5. $\rightarrow z$ measure to obtain final output z

4.5 Simon's Algorithm

Ο αλγόριθμος του *Simon* είναι λίγο διαφορετικός από τους αλγορίθμους που είδαμε μέχρι τώρα και λύνει ένα άλλο πρόβλημα. Η γενική ιδέα είναι η εξής:

Simon's Problem
Input: Ένα *blackbox* για τον υπολογισμό της άγνωστης συνάρτησης $f : 0, 1^n \to X$, όπου το X είναι ένα πεπερασμένο σύνολο.
Promise: Υπάρχει $strings = s_1 s_2 ... s_n$ τέτοιο ώστε $f(x) = f(y)$ ανν $x = y$ ή $x = y \oplus s$.
Problem: Βρίσκουμε το *strings* κάνοντας ερωτήματα στην f

Στον προηγούμενο αλγόριθμο, είδαμε σε έναν $n - qubit$ $Hadamard$ μετασχηματισμό ισχύει το εξής:

$$H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{z \epsilon 0,1^n} (-1)^{xz}|z\rangle \tag{4.32}$$

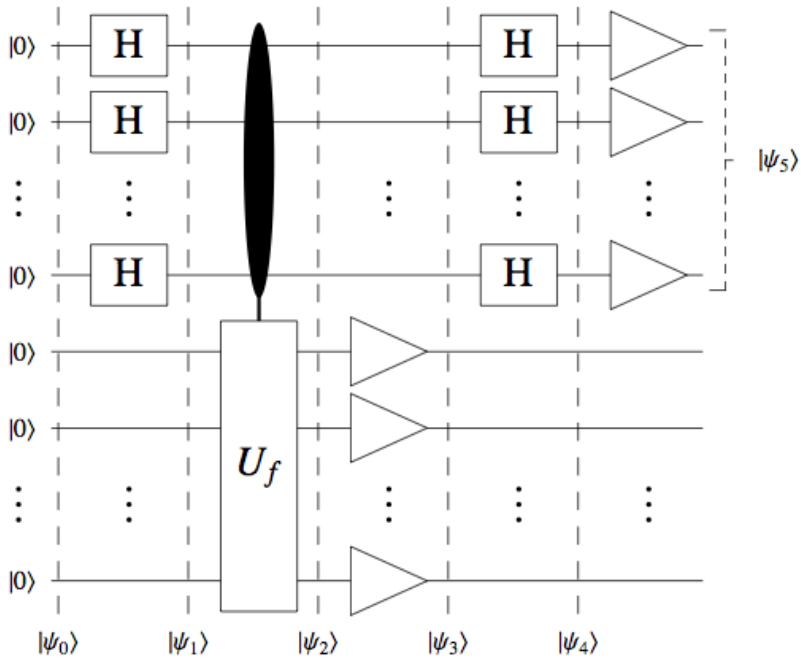
Αν όμως εφαρμόσουμε το $H^{\oplus n}$ σε μια υπέρθεση με δύο βασικές καταστάσεις όπως $|0\rangle + |s\rangle$ έχουμε

$$H^{\oplus n}|x\rangle(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|s\rangle) = \frac{1}{\sqrt{2^{n+1}}} \sum_{z \epsilon 0,1^n} |z\rangle + \frac{1}{\sqrt{2^{n+1}}} \sum_{z \epsilon 0,1^n} (-1)^{sz}|z\rangle = \tag{4.33}$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{z \epsilon 0,1^n} (1 + (-1)^{sz})|z\rangle \tag{4.34}$$

Άρα:

$$H^{\oplus n}(\frac{1}{\sqrt{2}}|x\rangle + \frac{1}{\sqrt{2}}|y\rangle) = \frac{1}{\sqrt{2^{n-1}}} \sum_{z \epsilon s \perp} |z\rangle \tag{4.35}$$



Το κύκλωμα του αλγορίθμου.

Τα βήματα του αλγορίθμου περιληπτικά και θεωρώντας ότι έχουμε το αντιστρέψιμο *black box* για την υλοποίηση της f

$$U_f : |x\rangle|b\rangle \rightarrow |x\rangle|b \otimes f(x)\rangle$$

Algorithm for Simon's Problem

1. Set a counter i = 1
2. Prepare $\frac{1}{\sqrt{2^n}} \sum_{x \epsilon 0,1^n} |x\rangle|0\rangle$
3. Apply U_f, to produce the state $\sum_{x \epsilon 0,1^n} |x\rangle|f(x)\rangle$
4. Measure the second register
5. Apply $H^{\otimes n}$ to the first register
6. Measure the first register and record the value w_i
7. If the dimension of the span of w_i equals n-1, then go to Step 8, otherwise increment i and got to Step 2
8. Solve the linear equation $W_s^T = 0^T$ and let s to be the unique non-zero solution
9. Output s

Επίσης ο αναμενόμενος αριθμός δειγμάτων από το $s\perp$ μέχρι να ολοκληρωθεί ο αλγόριθμος, είναι λιγότερα από $m + 1 = n$. Και οδηγούμαστε στο παρακάτω θεώρημα:

Θεώρημα 4.1. *Ο αλγόριθμος μας οδηγεί στην εύρεση των κρυμμένων strings στο πρόβλημα του Simon. Ο αναμενόμενος αριθμός των εκτιμήσεων της f μέχρι να ολοκληρωθεί ο αλγόριθμος είναι λιγότερο από n και ο αναμενόμενος αριθμός από άλλες στοιχειώδεις πύλες είναι στο $O(n^3)$*

Εάν θέλουμε να γενικεύσουμε το πρόβλημα του *Simon* μπορούμε να το δούμε έτσι:

Generalized Simon's Problem
Input:Ενα $blackboxU_f$ που υλοποιεί την $f : 0,1^n \rightarrow X$, όπου το X είναι κάποιο πεπερασμένο σύνολο.
Promise:$f(x) = f(y)$ ανν $x - y \epsilon S$ για κάποιο υποσύνολο $S \leq Z_2^n$
Problem: Η εύρεση μιας βάσης $s_1, ..., s_m$ για κάποιο S, όπου m η διάσταση του υποσυνόλου S

Ο αλγόριθμος που επιλύει το γενικευμένο πρόβλημα του *Simon* είναι περίπου ο ίδιος με το απλό πρόβλημα. Σημαντικό εδώ είναι ότι αν $S = 0, x_1, ..., x_{2^{m-1}}$ είναι ένα υποσύνολο διάστασης m του $Z_2^n = 0,1^n$ πάνω στο Z_2, τότε το σύνολο $0,1^n$ μπορεί να χωριστεί σε

δύο 2^{n-m} υποσύνολα της μορφής $y, y \oplus x_1, y \oplus x_2, ..., y \oplus x_{2^{m-1}}$, το οποίο αναφέρεται και ως $y + S$. Τότε στο 3ο βήμα μπορούμε να δούμε ότι έχουμε την κατάσταση

$$\sum_{x \epsilon 0,1^n} |x\rangle |f(x)\rangle = \frac{1}{\sqrt{2^{n-m}}} \sum_{y \epsilon I} |y + S\rangle |f(y)\rangle \tag{4.36}$$

όπου το I είναι το υποσύνολο του $0, 1^n$ το οποίο αντιπροσωπεύεται από κάθε ένα από τα 2^{n-m} υποσύνολα. Έτσι αφού μετρήσουμε τον δεύτερο καταχωρητή στο βήμα 4, ο πρώτος καταχωρητής είναι σε μια κατάσταση της μορφής $|y + S\rangle$ για ένα τυχαίο y. Στη συνέχεια μετά τον μετασχηματισμό $Hadamard$ στο βήμα 5, ο πρώτος καταχωρητής περιέχει μια ομοειδή υπέρθεση από στοιχεία του $S^{\perp}$, που σημαίνει ότι στο 6ο βήμα η μέτρηση στον πρώτο καταχωρητή μας επιστρέφει μια τιμή w_i σε ομοιόμορφη δειγματοληψία από ένα τυχαίο $S^{\perp}$. Το μόνο τμήμα που αλλάζει είναι τα τελευταία τρία στάδια του αλγορίθμου. Αν γνωρίζουμε τη διάσταση m του S, τότε ξέρουμε ότι το $S^{\perp}$ έχει διαστάσεις $n - m$ και μπορούμε να αντικαταστήσουμε τα τελευταία 3 βήματα του αλγορίθμου με τα εξής:

8. If the dimension of the span of w_i equals n - m, then go to Step 8, otherwise increment i and go to Step 2.

9. Solve the linear equation $W_S^T = 0^T$ and let $s_1, s_2, ..., s_m$ be generators of the solution space.

10. Output $s_1, s_2, ..., s_m$

Και έχουμε το εξής θεώρημα:

Θεώρημα 4.2. *Ο "νέος" αλγόριθμος λύνει το πρόβλημα του Simon με γνωστή τη διάσταση m του S. Ο αναμενόμενος αριθμός αξιολογήσεων της f στην εκτέλεση του αλγορίθμου είναι μικρότερη από $n - m + 1$ και $O(n^3)$ στοιχειώδεις διαδικασίες.*

Όταν δεν γνωρίζουμε το m, γνωρίζουμε ότι επαρκούν $m + 4$ δείγματα για τη δημιουργία του $S^{\perp}$ με πιθανότητα το λιγότερο $\frac{2}{3}$ [9].

4.6 Grover's Algorithm - Quantum Search Algorithms

Ο επόμενος αλγόριθμος που θα δούμε είναι πιο περίπλοκος και λύνει ένα καινούριο πρόβλημα. Είναι ο πρώτος κβαντικός αλγόριθμος αναζήτησης. Έστω ότι μας δίνεται ένα χάρτης με διάφορες πόλεις και θέλουμε να βρούμε τη συντομότερη διαδρομή που να περνάει από όλες τις πόλεις. Ένας απλός αλγόριθμος για αυτό, είναι να βρούμε όλες τις πιθανές διαδρομές και να κρατήσουμε τα μήκη τους ώστε να επιστρέψουμε τη συντομότερη διαδρομή. Σε έναν κλασσικό υπολογιστή εάν υπάρχουν N πιθανές διαδρομές, τότε θα μας πάρει $O(N)$ χρόνο για να βρούμε τη συντομότερη. Υπάρχει ωστόσο ένας κβαντικός αλγόριθμος αναζήτησης που μπορεί να επισπέυσει τη διαδικασία αυτή και να βρει τη συντομότερη διαδρομή σε $O(\sqrt{N})$ χρόνο. Αυτός ο αλγόριθμος είναι ο αλγόριθμος του *Grover* και μπορεί να χρησιμοποιηθεί σε πολλά κλασσικά προβλήματα αναζήτησης [11]. Ο *Lou Grover* [7] απέδειξε το 1966 ότι με

έναν κβαντικό υπολογιστή μπορούμε να βρούμε ένα στοιχείο μέσα σε μια μη δομημένη βάση δεδομένων σε $\sqrt{N}$ φορές. Όσο αυξάνει το μέγεθος της βάσης, τόσο περισσότερο αυξάνεται και η ταχύτητα. Επιπλέον ο ίδιος αλγόριθμος μπορεί να χρησιμοποιηθεί και για την εύρεση k αντικειμένων τα οποία να ικανοποιούν μια συγκεκριμένη συνθήκη μέσα στο σύνολο N με $\frac{\pi}{4}(\sqrt{\frac{N}{k}})$ δοκιμές [10] [12]. Ακόμα ο αλγόριθμος του *Grover* μπορεί να έχει πολύ περισσότερες εφαρμογές στο πεδίο των μαθηματικών από ότι έχουμε σκεφτεί μέχρι σήμερα [5] και οι *Nielsen Chuang* υποστηρίζουν ότι μπορεί να βοηθήσει στην πιο γρήγορη επίλυση ορισμένων $NP - complete$ προβλημάτων [11].

Ας υποθέσουμε ότι θέλουμε να ψάξουμε σε μια μη δομημένη βάση N στοιχείων, όπου κάθε στοιχείο έχει αριθμηθεί από το 0 έως το $N-1$. Επιπλέον έχουμε ένα υποθετικό σύστημα το οποίο μπορεί να αναγνωρίσει εάν κάποιο στοιχείο είναι αυτό που θέλουμε ή όχι. Το σύστημα αυτό σε έναν κλασσικό υπολογιστή θα μπορούσε να είναι ένας καταχωρητής που έχουμε αποθηκεύσει το στοιχείο που ψάχνουμε και ένα κύκλωμα λογικών πυλών. Το κύκλωμα αυτό συγκρίνει κάθε νέο στοιχείο που έρχεται σαν είσοδος με το αποθηκευμένο στοιχείο. Το σύστημα αυτό το οποίο θεωρούμε ως ένα μάυρο κουτί, το ονομάζουμε *oracle* στη διεθνή βιβλιογραφία.

Πως όμως λύνεται το πρόβλημα μας σε έναν κλασσικό υπολογιστή. Έστω ότι έχουμε τη βάση που αναφέραμε προηγουμένως. Το στοιχείο που αντιστοιχεί στον αριθμό k, το συμβολίζουμε με x_k. Το *oracle* είναι μια συνάρτηση f που παίρνει τιμές 0 και 1. Για το στοιχείο x_i που ψάχνουμε λοιπόν έχουμε
$f(x) = \begin{cases} 1, & x = x \\ 0, & x \neq x_i \end{cases}$ Δηλαδή δίνουμε ένα στοιχείο στην *oracle* και μας επιστρέφεται 0 ή 1 ανάλογα με το αν είναι αυτό που ψάχνουμε ή όχι.

Ας δούμε τώρα την ίδια αναζήτηση σε έναν κβαντικό υπολογιστή. Μπορούμε να γράψουμε το πλήθος των στοιχείων και με τον εξής τρόπο:

$$N = 2^n, n = 1, 2, 3, ... \tag{4.37}$$

και εφόσον έχουμε λιγότερα στοιχεία, μπροούμε να προσθέσουμε μέχρι να φτάσουμε στον επιθυμητό αριθμό.

Και στη συνέχεια αντιστοιχίζουμε κάθε ένα από τα στοιχεία αυτά σε μία από τις βασικές καταστάσεις ενός κβαντικού καταχωρητή με *nqubits*. Έστω το στοιχείο με δεκαδική αναπαράσταση $|2\rangle$ και συμβολίζεται με $|x_2\rangle$ αντιστοιχεί στη βασική κατάσταση $|000...00010\rangle$ [11].

4.6.1 Oracle

Έστω ότι το κβαντικό *oracle* βρίσκεται στην κατάσταση $|xy\rangle$, τότε:

$$|xy\rangle = |x\rangle|y\rangle \xrightarrow{o} |x\rangle|f(x) \oplus y\rangle \tag{4.38}$$

Το $|y\rangle$ ονομάζεται *oracle qubit*. Αρχικά το *oracle qubit* είναι στην βασική κατάσταση $|1\rangle$ και αμέσως μετά επιδράσ ε αυτό μια κβαντική πύλη H. Και έχουμε:

$$|1\rangle \xrightarrow{\text{H}} \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{4.39}$$

Σε ένα τυχαίο στοιχείο x θα ισχύει:

$$|x\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \xrightarrow{\text{o}} |x\rangle|f(x) \oplus \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{4.40}$$

Εάν η κατάσταση $|x\rangle$ δεν αντιστοιχεί στο στοιχείο που ψάχνουμε, τότε η $f(x)$ παίρνει την τιμή 0 και η σχέση (4.40) γίνεται:

$$|x\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \xrightarrow{\text{o}} |x\rangle(|0\rangle \oplus \frac{|0\rangle - |1\rangle}{\sqrt{2}}) = |x\rangle(\frac{|0\rangle \oplus |0\rangle - |0\rangle \oplus |1\rangle}{\sqrt{2}}) = \tag{4.41}$$

$$= |x\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.42}$$

Έστω τώρα ότι η $|x\rangle$ αντιστοιχεί στο στοιχείο που ψάχνουμε, η $f(x)$ παίρνει την τιμή 1 και έχουμε:

$$|x\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \xrightarrow{\text{o}} |x\rangle(|1\rangle \oplus \frac{|0\rangle - |1\rangle}{\sqrt{2}}) = |x\rangle(\frac{|1\rangle \oplus |0\rangle - |1\rangle \oplus |1\rangle}{\sqrt{2}}) = \tag{4.43}$$

$$= -|x\rangle(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{4.44}$$

Δεδομένου ότι το *qubit* του κβανικού *oracle* δεν μεταβάλλεται σε καμία περίπτωση μπορούμε να το απαλείψουμε από τις δύο παραπάνω σχέσεις και άρα έχουμε:

$$|x\rangle \xrightarrow{\text{o}} \begin{cases} +|x\rangle, & |x\rangle not the selected element \\ -|x\rangle, & |x\rangle the selected element \end{cases}$$

Και πιο συνοπτικά μπορούμε να γράψουμε την παραπάνω σχέση ως εξής:

$$|x\rangle \xrightarrow{\text{o}} (-1)^{f(x)}|x\rangle$$

όπου η $f(x)$ παίρνει τιμές 0 ή 1, άρα $|x\rangle \xrightarrow{\text{o}} \begin{cases} (-1)^0|x\rangle = +|x\rangle, & f(x) = 0 \\ (-1)^1|x\rangle = -|x\rangle, & f(x) = 1 \end{cases}$

Συνοψίζοντας λοιπόν όλα τα παραπάνω βλέπουμε ότι το κβαντικό *oracle* δρα στις βασικές καταστάσεις $|x\rangle$. Αν η βασική κατάσταση αντιστοιχεί στο στοιχείο που ψάχνουμε τότε της αλλάζει το πρόσημο, αλλιώς την αφήνει όπως είναι.

4.6.2 Algorithm's Procedure

Ο αλγόριθμος ξεκινάει με τον υπολογιστή να βρίσκεται στην κατάσταση $|0\rangle^{\otimes n}$ και στη συνέχεια εφαρμόζεται ο μετασχηματισμός $Hadamard$ για να θέσει τον υπολογιστή σε μια υπέρθεση της μορφής:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x_i\rangle \tag{4.45}$$

Στη συνέχεια εφαρμόζονται επαναλαμβανόμενες υπορουτίνες που είνα γνωστές ως *Grover iteration* ή *Grover operator* και συμβολίζεται με G. Θα μπορούσαμε να αναλύσουμε την υπορουτίνα αυτή σε τέσσερα απλά προβλήματα

1. Εφαρμόζουμε το *oracle* O

2. Εφαρμόζουμε τον μετασχηματισμό $Hadamard$ της μορφής $H^{\oplus n}$

3. Κάνουμε μια μετατόπιση ($shift$) της φάσης όπου κάθε κατάσταση εκτός της $|0\rangle$ μετατοπίζεται κατά -1 $|x\rangle \rightarrow -(-1)^{\delta_{x0}}|x\rangle$

4. Εφαρμογή του μετασχηματισμού $Hadamard$ [11]

Ας πάμε πάλι στην αρχική κατάσταση. Μια μέτρηση του καταχωρητή θα μας έδινε ακριβώς τα ίδια αποτελέσματα με την κλασσική περίπτωση. Δηλαδή θα είχαμε το επιθυμητό $|x_i\rangle$ με πιθανότητα $\frac{1}{\sqrt{2}}$. Ο στόχος μας είναι να σχηματίσουμε την κατάσταση $|s\rangle$ με κατάλληλο τρόπο, ώστε να αυξήσουμε την πιθανότητα αυτή. Αυτό γίνεται με το να αυξηθεί ο συντελεστής του $|x_i\rangle$ όσο το δυνατόν πιο κοντά στη μονάδα και ταυτόχρονα να μειωθούν οι συντελεστές των υπολοίπων καταστάσεων. Όπως είπαμε η $|s\rangle$ είναι η υπέρθεση των N βασικών καταστάσεων με $N = 2^n$ και ψάχνουμε για το στοιχείο που αντιστοιχεί στην $|x_i\rangle$. Θα θέσουμε $b = 1$ όπου b είναι ο αριθμός επαναλήψεων των επόμενων βημάτων.

1. Εφαρμογή του τελεστή $\hat{O} = \hat{I} - 2|x_i\rangle\rangle x_i|$ στον κβαντικό καταχωρητή

2. Εφαρμογή του τελεστή $\hat{G} = 2|s\rangle\rangle s| - \hat{I}$ στον κβαντικό καταχωρητή.

Αν ο αριθμός b είναι μεγαλύτερος ή περίπου ίσος με $((\frac{\pi}{4})\sqrt{N}) - 0.5$ τότε μετράμε την κατάσταση του καταχωρητή και είναι σχεδόν βέβαιο ότι θα είναι η ζητούμενη. Αν όχι τότε ξαναγυρνάμε στο 1ο βήμα.

Στα παραπάνω βήματα, χρησιμοποιήσαμε το $\hat{I}$. Οι κβαντικές πύλες, επί της ουσίας είναι τελεστές του χώρου $Hilbert$ που δρουν σε $qubits$ και σε κβαντικούς καταχωρητές αλλάζοντας την κατάσταση τους. Από τη στιγμή λοιπόν που κάθε κβαντικό κύκλωμα είναι τελεστής του χώρου $Hilbert$, αυτόματα συμπεραίνουμε ότι και το *oracle* είναι τελεστής του χώρου $Hilbert$. Για το στοιχείο που ψάχνουμε, το *oracle* είναι

$$\hat{O} = \hat{I} - 2|x_i\rangle\rangle x_i|$$

όπου $\hat{I}$ είναι ο τελεστής που αντιστοιχεί στην πύλη αδράνειας και όταν δρα δεν αλλάζει καμία κατάσταση. Η μαθηματική αναπαράσταση του αλγορίθμου, θα μπορούσε να είναι η εξής:

Algorithm: Quantum Search
Inputs: (1) A black box oracle O which performs the transformation $O|x\rangle|q\rangle = |x\rangle|q \oplus f(x)\rangle$ where $f(x) = 0$ for all $0 \leq x \leq 2^n$ except x_0 for which $f(x_0) = 1$
(2) $n+1$ qubits in the state $|0\rangle$
Outputs: x_0
Runtime: $O(\sqrt{2^n})$ operations. Succeeds with probability $O(1)$
Procedure:

1. $|0\rangle^{\otimes n}|0\rangle$ initial state
2. $\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle[\frac{|0\rangle-|1\rangle}{\sqrt{2}}]$ apply $H^{\otimes n}$ to the first n qubits, and HX to the last *qubit*
3. $\rightarrow [(2|s\rangle\rangle s|-\hat{I})\hat{O}]^R \sum_{x=0}^{2^n-1} |x\rangle[\frac{|0\rangle-|1\rangle}{\sqrt{2}}] \approx |x_0\rangle[\frac{|0\rangle-|1\rangle}{\sqrt{2}}]$ apply the Grover iteration $R \approx \lceil \frac{\pi\sqrt{2^n}}{4}$ times.
4. $\rightarrow x_0$ measure the first n qubits

4.6.3 Example

Ας δούμε τώρα και ένα παράδειγμα του κβαντικού αλγορίθμου του *Grover*. Έστω ότι έχουμε μια μη δομημένη βάση δεδομένων με 4 στοιχεία και θέλουμε να βρούμε το στοιχείο που αντιστοιχεί στην βασική κατάσταση $|x_i\rangle = |01\rangle$. Αρχικά θα έχουμε έναν κβαντικό καταχωρητή με 2 *qubits* και θα ψάξουμε τον αριθμό που αντιστοιχεί στον αριθμό 1, με βάση την κατάσταση του. Θα εκτελέσουμε ένα ένα όλα τα βήματα που είδαμε παραπάνω:

Βήμα 1ο

Αρχίζουμε με τον κβαντικό καταχωρητή στην κατάσταση $|00\rangle$ και τον θέτουμε σε υπέρθεση βασικών καταστάσεων. Το πλάτος πιθανότητας για κάθε κατάσταση πρέπει να είναι το ίδιο όποτε χρησιμοποιούμε δύο κβαντικές πύλες H. Άρα θα έχουμε:

$$|s\rangle = H \otimes H|00\rangle = \begin{bmatrix} [\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & \frac{1}{2}] \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \Rightarrow$$

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

Άρα έχουμε φέρει τον καταχωρητή στη βασική μορφή υπέρθεσης που θέλουμε. Δεδομένου ότι ψάχνουμε την $|01\rangle$, θέλουμε να φέρουμε τον καταχωρητή σε τέτοια κατάσταση ώστε ο συντελεστής της $|01\rangle$ να είναι πολύ κοντά στη μονάδα.

Βήμα 2ο:

Τώρα δρα ο τελεστής $\hat{O} = \hat{I} - 2|x_i\rangle\rangle x_i|$ όπου έχουμε:

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

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

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

Άρα

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

Και όπως βλέπουμε το πρόσημο της ζητούμενης κατάστασης έχει αλλάξει.

Βήμα 3ο

Τώρα επιδρά ο τελεστής $\hat{G} = 2|s\rangle\rangle s| - \hat{I}$

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

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

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

Με τη δράση της $\hat{G}$ το αποτέλεσμα που παίρνουμε είναι:

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

Αν μετρήσουμε λοιπόν την κατάσταση του κβαντικού καταχωρητή, είναι βέβαιο ότι θα βρούμε την κατάσταση $|x_i\rangle = |01\rangle$, όπου ο αριθμός των επαναλήψεων είναι $(\frac{\pi}{4}\sqrt{N}) - 0.5 \cong 1$

4.7 Summary of Quantum Algorithms

Σε αυτή την ενότητα, θα προσπαθήσουμε να κάνουμε μια μικρή περίληψη των κβαντικών αλγορίθμων που είδαμε μέχρι τώρα. Αρχικά είδαμε πως μπορούμε να χρησιμοποιήσουμε έναν πιθανοτικό αλγόριθμο σε έναν κβαντικό υπολογιστή. Το βασικότερο εδώ είναι ότι η συνολική πιθανότητα να μεταβούμε από μια κατάσταση σε μια άλλη, είναι ίση με τα τετράγωνα των κβαντικών πλατών για τις πιθανότητες αυτές. Για να βρούμε λοιπόν τη συνολική πιθανότητα, αντί να προσθέσουμε τις πιθανότητες για τα διαφορετικά μονοπάτια (για να φτάσουμε από μια κατάσταση σε μια άλλη), προσθέτουμε τα κβαντικά πλάτη. Στη συνέχεια είδαμε μερικά πράγματα για τον κβαντικό παραλληλισμό, που αποτελεί την βάση για αρκετούς κβαντικούς αλγορίθμους. Αυτό που μας επιτρέπει ο κβαντικός παραλληλισμός είναι να ελέγξουμε μια συνάρτηση $f(x)$ για πολλές διαφορετικές τιμές του x ταυτόχρονα. Αυτό επιτυγχάνεται με τη χρήση 2 *qubits* και μια ακολουθία λογικών πυλών. Στο τελικό στάδιο, έχουμε τις πληροφορίες για την $f(0)$ και την $f(1)$ ταυτόχρονα. Ο πρώτος κανονικός κβαντικός αλγόριθμος που υπήρξε, ήταν ο αλγόριθμος του *Deutsch*. Σε αντίθεση με τον κβαντικό παραλληλισμό, εδώ ο στόχος του αλγορίθμου είναι να ορίσουμε την τιμή της $f(0) \oplus f(1)$. Έχουμε περίπου την ίδια βάση με τον κβαντικό παραλληλισμό. Έχουμε πάλι 2 *qubits* όπου το πρώτο *qubit* είναι το *qubit* ελέγχου και η επίδραση των κβαντικών πυλών στο δεύτερο *qubit* εξαρτάται από το πρώτο. Στη συνέχεια, κωδικοποιώντας τις τιμές του δεύτερου *qubit* με βάση το πρώτο, προσδιορίζουμε την $f(0) \oplus f(1)$, προσδιορίζοντας τους συντελεστές φάσης μεταξύ των $|0\rangle$ και $|1\rangle$. Η γενίκευση του αλγορίθμου του *Deutsch*, ή μάλλον του προβλήματος του *Deutsch*, είναι το πρόβλημα του $Deutsch - Josza$. Πάλι έχουμε σαν είσοδο μια άγνωστη συνάρτηση f, όπου αυτή τη φορά θέλουμε να αποφασίσουμε τι είναι η f, δηλαδή αν είναι *constant* ή *balanced*. Εδώ έχουμε $nn - qubits$ πύλες $Hadamard$. Στο τέλος του αλγορίθμου η μέτρηση του πρώτου καταχωρητή γίνεται σε υπολογιστική βάση και εάν η f είναι *constant*, τότε το πλάτος της τελικής κατάσταση· θα είναι είτε +1 είτε -1 και άρα η μέτρηση του πρώτου καταχωρητή θα μας επιστρέψει σίγουρα όλα τα 0. Αν αντίστοιχα η f είναι *balanced* και οι συνιστώσες των πλατών αλληλοαναιρούνται, το συνολικό πλάτος θα είναι 0 και η τελική μέτρηση στον πρώτο καταχωρητή θα μας δώσει όλες τις μη μηδενικές τιμές. Επομένως ανάλογα με τη μέτρηση του καταχωρητή μπορούμε να αποφανθούμε για το τι είναι η f. Ο επόμενος αλγόριθμος είναι ο αλγόριθμος του *Simon*. Αυτός ο αλγόριθμος λύνει ένα αρκετά διαφορετικό πρόβλημα. Σε μια άγνωστη συνάρτηση $f : 0, 1^n \to X$, υπάρχει *string* s τέτοιο ώστε $f(x) = f(y)$ ανν $x = y$ ή $x = y \oplus s$. Ο αναμενόμενος αριθμός εκτιμήσεων της f είναι λιγότερος από n. Επίσης ο αλγόριθμος μπορεί να εφαρμοστεί είτε εάν γνωρίζουμε τη διάσταση m του υποσυνόλου στο οποίο κάνουμε την αναζήτηση, είτε όχι. Ο τελευταίος αλγόριθμος που είδαμε είναι ο αλγόριθμος του *Grover*. Είναι αρκετά πιο πολύπλοκος από τους προηγούμενους και είναι ο πρώτος κβαντικός αλγόριθμος αναζήτησης. Με λίγα λόγια ο συγκεκριμένος αλγόριθμος μας δίνει τη δυνατότητα να βρούμε ένα στοιχείο μέσα σε μια βάση N στοιχείων με $\sqrt{N}$

βήματα. Στον αλγόριθμο του *Grover* χρησιμοποιούμε μια συνάρτηση f που παίρνει τιμές 0 και 1 (κβαντικό *oracle*). Το *oracle* επιδρά στις βασικές κατάστασεις ενός τυχαίου σημείου x, δηλαδή στις καταστάσεις $|x\rangle$. Αν η βασική αυτή κατάσταση αντιστοιχεί στην κατάσταση του στοιχείου που ψάχνουμε, τότε της αλλάζει το πρόσημο, αλλιώς το αφήνει ως έχει.

Θα μπορούσαμε να πούμε ότι υπάρχουν τρεις κλάσεις κβαντικών αλγορίθμων. Η πρώτη είναι η κλάση των αλγορίθμων που βασίζονται στον μετασχηματισμό $Fourier$ (θα δούμε λεπτομέρειες στο επόμενο κεφάλαιο). Ένα τέτοιο παράδειγμα είναι ο αλγόριθμος του $Deutsch-Josza$. Η δεύτερη κλάση είναι η κάση των κβαντικών αλγορίθμων αναζήτησης, όπως ο αλγόριθμος του *Grover*. Και η τελευταία κλάση είναι οι κβαντικοί αλγόριθμοι προσομοίωσης (*quantum simulation*), όπου ένας κβαντικός υπολογιστής χρησιμοποιείται για να προσομοιώσει ένα κβαντικό σύστημα [11].

Κεφάλαιο 5

The quantum Fourier Transformation

5.1 FFT

Οι πράξεις μεταξύ πολυωνύμων μεγάλου μεγέθους χρησιμοποιούνται ευρέως. Η ολοκλήρωση τους ¨χειροκίνητα' είναι μια χρονοβόρα και δύσκολη διαδικασία. Η επίλυση σε αυτό έρχεται με τη χρήση του Γρήγορου Μετασχηματισμού [1] $Fourier$ (FFT).
Ο FFT, βασίζεται σε κάποιες βασικές αρχές και ιδιότητες [6]. Η κυριότερη είναι η ιδιότητα των πολυωνύμων να χαρακτηρίζονται με δύο διαφορετικές μορφές.
Το πολυώνυμο $A(x)$ μπορεί να χαρακτηριστεί με τους εξής δύο τρόπους:

- Μέσω των συντελεστών του $a_0, a_1, ..., a_d$
- Μέσω των τιμών του $A(x_0), A(x_1), ..., A(x_d)$

Πολύ συνοπτικά, ο FFT είναι ένας αλγόριθμος διαίρει-και-βασίλευε, που βασίζεται στις ιδιότητες των μιγαδικών ριζών της μονάδας. Χρησιμοποιεί τον διακριτό μετασχηματισμό $Fourier$ (DFT) και τον αντίστροφο DFT για να μετατρέπει τις δύο μορφές αναπαράστασης του πολυωνύμου. Από την αναπαράσταση του πολυωνύμου βαθμού d μέσω συντελεστών, προκύπτει ένα διάνυσμα με τους συντελεστές $\alpha = (\alpha_0, \alpha_1, ..., \alpha_d)$. Η απεικόνιση ενός πολυωνύμου βαθμού d σε μορφή τιμών μας δίνει ένα πακέτο από d ζευγάρια της μορφής $(x_0, y_0), (x_1, y_1), ..., (x_d, y_d)$ τέτοια ώστε κάθε x_k να είναι διακριτοί αριθμοί και κάθε $y_k = A(x_k)$ για κάθε $k = 0, 1, ..., d$.

Η κεντρική ιδέα πάνω στην οποία βασίστηκε ο FFT, είναι η δυνατότητα κάθε πολυωνύμου βαθμού d, να μπορεί να χαρακτηριστεί μοναδικά από την τιμή του σε κάθε $d+1$ σημείο του. Έστω λοιπόν ότι έχουμε ένα γινόμενο $C(x)$, δύο πολυωνύμων $A(x)$ και $B(x)$ βαθμού d το καθένα. Αυτό σημαίνει ότι το $C(x)$, θα έχει βαθμό $2d$. Με βάση λοιπόν την παραπάνω ιδιότητα, το $C(x)$, θα μπορεί να χαρακτηριστεί μοναδικά σε κάθε $2d+1$ σημείο του. Εάν λοιπόν το x είναι γνωστό, έστω z, ο πολλαπλασιασμός είναι μια διαδικασία γραμμικού χρόνου, καθώς το αποτέλεσμα θα προκύπτει εάν κάνουμε $A(z)$ φορές το $B(z)$. Ο πολλαπλασιασμός δύο πολυωνύμων $A(x)$ και $B(x)$ βαθμού d το καθένα, θέλει χρόνο $\theta(d^2)$, καθώς κάθε συντελεστής στο διάνυσμα α πρέπει να πολλαπλασιαστεί με κάθε συντελεστή στο διάνυσμα β. Το

διάνυσμα συντελεστών του γινομένου $C(x)$, $c = (c_0, c_1, ..., c_{2d}$ ονομάζεται *convolution* των διανυσμάτων α και β και γράφεται και ως $c = \alpha \otimes \beta$.

Όμως εδώ έχουμε να αντιμετωπίσουμε το πρόβλημα, ότι και τα πολυώνυμα εισόδου αλλά και το γινόμενο θέλουμε να είναι σε μορφή συντελεστών. Επομένως πρέπει να γίνουν δύο μετατροπές. Μια μετατροπή από την μορφή των συντελεστών στην μορφή των τιμών (*evaluation*) τα επιλεγμένα σημεία στα οποία θα κάνουμε τον πολλαπλασιασμός και στη συνέχεια μετατρέπουμε ξανά το τελικό πλέον αποτέλεσμα σε μορφή συντελεστών (*interpolation*). Η διαδικασία *evaluation* στο σημείο x_0, αποτελείται από τον υπολογισμό της τιμής $A(x_0)$. Χρησιμοποιώντας το σχήμα *Horner* βρίσκουμε την τιμή σε χρόνο $\theta(n)$, ως εξής:

$$A(x_0) = \alpha_0 + x_0(\alpha_1 + x_0(\alpha_2 + ... + x_0(\alpha_d)...))$$

Η αντίστροφη διαδικασία, δηλαδή η *interpolation* καθορίζει την τιμή του συντελεστή του πολυωνύμου, από την τιμή που αναπαρίσταται. Για κάθε ¨πακέτο' $(x_0, y_0), (x_1, y_1), ..., (x_d, y_d)$, όπου κάθε x_k είναι διακριτός αριθμός, υπάρχει ένα μοναδικό πολυώνυμο $A(x)$ βαθμού d για το οποίο ισχύει ότι $y_k = A(x_k)$, για κάθε $k = 0, 1, ..., d$. Χρησιμοποιώντας τη μέθοδο *Lagrange*, μπορούμε να κάνουμε την *interpolation* σε χρόνο $\theta(d^2)$.

Το αμέσως επόμενο ερώτημα που προκύπτει είναι το πως ακριβώς θα επιλεγούν τα σημεία με βαθμό $< n - 1$ του $A(x)$, στα οποία θα εφαρμόσουμε τους μετασχηματισμούς. Για να μειώσουμε τις πράξεις κατά το μέγιστο δυνατό, επιλέγουμε ζευγάρια θετικών-αρνητικών αριθμών, $\pm x_i, ..., \pm x_{\frac{n}{2}-1}$. Με πιο απλά λόγια, χωρίζουμε το πολυώνυμο $A(x)$, με αυτόν τον τρόπο:

$$A(x) = A_e(x^2) + xA_o(x^2)$$

, όπου A_e ο συντελεστής των άρτιων δυνάμεων και A_o ο συνεντελεστής των περιττών δυνάμεων. Ο υπολογισμός ενός ζευγαριού $\pm x_i$ γίνεται ακόμα πιο έυκολος καθώς ισχύει η εξής ιδιότητα:

$$A(x_i) = A_e(x_i^2) + x_i A_o(x_i^2) kai A(x_i) = A_e(-x_i^2) - x_i A_o(x_i^2)$$

Κάνοντας *evaluation* του $A(x)$ σε n θετικά αρνητικά σημεία $\pm x_0, ..., x_{\frac{n}{2}-1}$ μειώνει την διαδικασία στα $A_e(x)$ και $A_o(x)$ σε $\frac{n}{2}$ σημεία. Έτσι λοιπόν το αρχικό πρόβλημα μήκους n μειώνεται σε δύο υποπροβλήματα μήκους $\frac{n}{2}$ το καθένα και σε κάποιες σχετικά απλές πράξεις. Ο συνολικός χρόνος εκτέλεσης είναι $T(n) = 2T(\frac{n}{2}) + O(n)$, το οποίο ανάγεται σε $O(nlogn)$, που είναι ένας πολύ ικανοποιητικός χρόνος.

Η τεχνική αυτή με την επιλογή θετικών-αρνητικών ζευγαριών εφαρμόζεται στο πρώτο επίπεδο. Για να προχωρήσουμε στο επόμενο επίπεδο θέλουμε $\frac{n}{2}$ σημεία $x_0^2, ..., x_{\frac{n}{2}-1^2}$ να είναι τα ίδια θετικά-αρνητικά ζευγάρια. Δεδομένου όμως ότι τα σημεία αυτά είναι υψωμένα στο τετράγωνο, είναι αδύνατο χωρίς την χρήση μιγαδικών αριθμών. Στο τελευταίο επίπεδο της αναδρομής θα έχουμε μόνο ένα σημείο, το ± 1. Στο ακριβώς προηγούμενο επίπεδο της

αναδρομής θα έχουμε τις ρίζες του ± 1, δηλαδή $\pm i$. Συνεχίζουμε έτσι σε κάθε επίπεδο μέχρι που καταλήγουμε στην $n-ost$ ρίζα του συνόλου, η οποία είναι οι μιγαδικές ρίζες της εξίσωσης $z_n = 1$.

Μέχρι αυτό το σημείο έχουμε δει πως γίνεται η μετατροπή σε τιμές και ο πολλαπλασιασμός αυτών. Ο FFT, μετατρέπει από της μορφή συντελεστών στη μορφή τιμών σε $O(nlogn)$ όταν τα σημεία x_i είναι οι μιγαδικές n-οστές ρίζες του 1 $(1, \omega, \omega^2, ..., \omega^{n-1})$. Σχηματικά ισχύει το εξής:

$$\langle values \rangle = FFT(\langle coefficients \rangle, \omega).$$

Ωστόσο δεν μπορούμε να αγνοήσουμε τους συντελεστές, καθώς σε αυτή τη μορφή μας δίνονται όλα τα δεδομένα μας. Η τελευταία αυτή μετατροπή γίνεται με τη διαδικασία $intepolation$.

$$\langle coefficients \rangle = \frac{1}{n} FFT(\langle values \rangle, \omega^{-1}).$$

Για να αποκτήσουμε μια καλύτερη εικόνα της $interpolation$, πρέπει να δούμε λίγο πιο αναλυτικά τη σχέση ανάμεσα στις δυο διαφορετικές απεικονίσεις του $A(x)$. Και οι δύο μορφές αποτελούν διανύσματα n αριθμών και η κάθε απεικόνιση είναι ο γραμμικός μετασχηματισμός της άλλης.

$$\begin{bmatrix} A(x_0) \\ A(x_1) \\ \vdots \\ A(x_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ & & \vdots & & \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-1} \end{bmatrix} \cdot \begin{bmatrix} \alpha_0 \\ \alpha 1 \\ \vdots \\ \alpha_{n-1} \end{bmatrix}$$

Ο μεσαίος πίνακας ονομάζεται M και έχει κάποιες συγκεκριμένες ιδιότητες. Εάν τα $x_0, ...x_{n-1}$ είναι διακριτοί αριθμοί, τότε ο M είναι αντιστρέψιμος. Η ύπαρξη του M^{-1}, μας δίνει τη δυνατότητα να αντιστρέψουμε την εξίσωση μήτρας και να εκφράσουμε την μορφή των συντελεστών σε μορφή τιμών. Με λίγα λόγια όταν κάνουμε $evaluating$ πολλαπλασιάζουμε με τον M και όταν κάνουμε $interpolation$, πολλαπλασιάζουμε με τον M^{-1}.

Ας προσπαθήσουμε να εξηγήσουμε λίγο μαθηματικά τον FFT. Με όρους γραμμικής άλγεβρας, ο γρήγορος μετασχηματισμός $Fourier$, έναν αυθαίρετο $vector$, διαστάσεως n (ο οποίος αποτελείται από τους συντελεστές του πολυωνύμου) με έναν πίνακα $n \times n$ της παρακάτω μορφής:

$$M_n(\omega) = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(n-1)} \\ & & \vdots & & \\ 1 & \omega^j & \omega^2 j & \dots & \omega^{(n-1)j} \\ & & \vdots & & \\ 1 & \omega^{(n-1)} & \omega^{2(n-1)} & \dots & \omega^{(n-1)(n-1)} \end{bmatrix}$$, όπου η πρώτη σειρά προκύπτει για $\omega^0 = 1$, η δεύτερη για ω, η τρίτη για ω^2 μέχρι την τελευταία που προκύπτει

για $\omega(n-1)$. Το ω είναι η n-οστή μιγαδική ρίζα του 1 και το n είναι μια δύναμη του 2. Βλέπουμε ότι ο συγκεκριμένος πίνακας είναι πολύ απλό να περιγραφεί καθώς σε κάθε (j,k) θέση βρίσκεται το ω^{jk}. Αυτό που μπορούμε να παρατηρήσουμε σε αυτό το στάδιο είναι ότι οι στήλες του M είναι ορθογώνιες μεταξύ τους. Αν πάρουμε το αποτέλεσμα από δύο τυχαίες στήλες του M, έστω j και k τότε προκύπτει το εξής:

$$1 + \omega^{j-k} + \omega^{2(j-k)} + ... + \omega^{(n-1)(j-k)}$$

, το οποίο είναι γεωμετρική σειρά με πρώτο όρο το 1 και τελευταίο το $\omega^{(n-1)(j-k)}$. Επομένως μετατρέπεται στο $(1-\omega^{n(j-k)})/(1-\omega^{(j-k)})$, το οποίο είναι 0 για κάθε τιμή εκτός από $j=k$, όπου σε αυτή την περίπτωση όλοι οι όροι είναι 1 και το τελικό σύνολο n. Οι στήλες αυτές θα μπορούσαν να θεωρηθούν ως η βάση ενός εναλλακτικού συστήματος συντεταγμένων, το οποίο συχνά αποκαλείται βάση $Fourier$. Ο πολλαπλασιασμός ενός διανύσματος με τον M, οδηγεί στην περιστροφή του κλασσικού συστήματος συντεταγμένων στο σύστημα βάσης $Fourier$. Ο αντίστροφος M, προκαλεί την αντίστροφη περιστροφή. Με λίγα λόγια ισχύει ότι: $M_n(\omega^{-1}) = \frac{1}{n}M_n(\omega^{-1})$. Όμως το ω^{-1} είναι και η n-οστή ρίζα της μονάδας και έτσι κάνοντας $interpolation$ επί της ουσίας κάνουμε FFT, μόνο που αντί για ω έχουμε ω^{-1}. Κοιτάζοντας λοιπόν συνολικά μέχρι εδώ βλέπουμε ότι και από γεωμετρικής άποψης, ο πολλαπλασιασμός μεγάλων πολυωνύμων είναι αρκετά πιο εύκολος στην βάση $Fourier$, από ότι στην κλασσική βάση. Αρχικά περιστρέφουμε τα διανύσματα σε βάση $Fourier$ ($evaluation$), στη συνέχεια κάνουμε την πράξη που θέλουμε (στην προκειμένη περίπτωση πολλαπλασιασμό) και τέλος περιστρέφουμε τα διανύσματα ξανά αντίστροφα ($interpolation$). Τα αρχικά διανύσματα είναι η απεικόνιση σε μορφή συντελεστών, όταν περιστρέφονται μετατρέπονται σε μορφή τιμών και μετά την αντίστροφη περιστροφή επανέρχονται σε μορφή συντελεστών. Η γρήγπρη εναλλαγή μεταξύ των δύο αυτών καταστάσεων είναι ο γρήγορος μετασχηματισμός $Fourier$.

Αυτό είναι το συνολικό υπόβαθρο του FFT. Ωστόσο το πιο ενδιαφέρον κομμάτι του είναι η υπορουτίνα που κάνει αυτή την εναλλαγή που είδαμε πιο πάνω. Ο FFT παίρνει σαν είσοδο ένα διάνυσμα $\alpha = (\alpha_0, ..., \alpha_{n-1})$ και έναν μιγαδικό αριθμό ω, του οποίου οι δυνάμεις αποτελούν τις μιγαδικές nοστές ρίζες της μονάδας. Πολλαπλασιάζει το διάνυσμα με τον πίνακα $M_n(\omega)$ διάστασης $n \times n$, ο οποίος έχει σαν είσοδο σε κάθε j,k σημείο του το αντίστοιχο ω^{jk}. Ο διαχωρισμός που αναλύσαμε παραπάνω σε ζεύγη θετικών αρνητικών είναι πολύ βοηθητικός σε αυτό ακριβώς το σημείο καθώς οι στήλες του M_n χωρίζονται σε αρνητικούς και θετικούς. Στο επόμενο βήμα απλοποιούμε τα στοιχεία στο κάτω μισό του πίνακα χρησιμοποιώντας τα $\omega^{n/2} = -1$ και $\omega^n = 1$. Το πάνω αριστερά κομμάτι του πίνακα όπως και το κάτω αριστερά με διάσταση $n/2 \times n/2$ είναι το $M_{n/2}(\omega^2)$. Επίσης ο πάνω δεξιά και ο κάτω δεξιά υποπίνακας είναι σχεδόν ίδιοι με τους προηγούμενους, μόνο που οι jοστές σειρές τους είναι πολλαπλασιασμένες με το ω^j και $-\omega^j$, αντίστοιχα. Έτσι λοιπόν το τελικό αποτέλεσμα είναι ακι το ζητούμενο διάνυσμα μας.

Συνοπτικά ο FFT έχει ώς εξής:

Fast Fourier Transform

1: $functionFFT(\alpha, \omega)$
2: $Input:$ $An\ array\ \alpha = (\alpha_0, ...\alpha_{n-1}),\ for\ n\ a\ power\ of\ 2$
3: $A\ primitive\ nth\ root\ of\ unity,\ \omega$
4: $Output:$ $M_n(\omega)\alpha$
5:
6: **if** $\omega = 1$ **then return** α
7: $(s_0, s_1, ..., s_{\frac{n}{2}-1} = FFT((\alpha_0, \alpha_2, ..., \alpha_{n-2}, \omega^2$
8: **for** $j = 0 \to \frac{n}{2} - 1$ **do**
9: $\quad r_j = s_j + \omega^j s'_j$
10: $\quad r_{j+\frac{n}{2}} = s_j - \omega^j s'_j$
return $(r_0, r_1, ..., r_{n-1}$

5.1.1 Υλοποίηση FFT

Παραπάνω πήραμε μια γενική ιδέα του αλγορίθμου. Όπως είδαμε ο FFT μπορεί να χωριστεί σε δύο βασικά βήματα. Αρχικά θέλουμε να φέρουμε τα δύο πολυώνυμα $A(x)$ και $B(x)$ στην κατάλληλη μορφή συντελεστών ($coefficients$) εφαρμόζοντας τον FFT, στη συνέχεια να τα πολλαπλασιάσουμε ανά στοιχείο και τέλος να μετατρέψουμε το τελικό διάνυσμα που έχουμε βρει στη σωστή μορφή με χρήση του $inverseFFT(iFFT)$, όπου θα αποτελεί τους συντελεστές του πολυωνύμου του γινομένου $C(x)$. Το πρώτο βήμα ονομάζεται $evaluation$ και το δεύτερο $intepolation$. Για το $evaluation$ θα χρειαστούμε ένα πολύ βασικό στοιχείο, τον αριθμό των σημείων τα οποία θα κάνουμε $evaluate$. Ο αριθμός αυτός προκύπτει από τις $n+1$ μιγαδικές ρίζες της μονάδας, όπου n ο βαθμός του πολυωνύμου του γινομένου $C(x)$. Οι μιγαδικές αυτές ρίζες προκύπτουν ως εξής: $\omega^n = 1$, $e^{\frac{2i\pi k}{n}}, k = 0, .., n-1$, όπου ξέρουμε ότι: $e^i u = cos(u) + isin(u)$ με το u να είναι μια γωνία στο καρτεσιανό σύστημα συντεταγμένων.

Παράδειγμα 5.1.1. Ας δούμε και ένα απλό παράδειγμα βήμα βήμα για το πως δουλεύει ο αλγόριθμος.

Έστω ότι έχουμε τα δύο πολυώνυμα $A(x) = 4x^2 + 4$ και $B(x) = 3x + 2$. Ο βαθμός του γινομένου $C(x)$ θα είναι 3, άρα $n = 4$. Οι 4 μιγαδικές ρίζες της μονάδας είναι $\omega^4 = 1 \to \omega = 1, i, -1, -i$.
Για το πολυώνυμο A:
Οι συντελεστές είναι (4,0,4,0), άρα για ο μετασχηματισμός για τις ζυγές θέσεις θα είναι $Even_A : (4, 4) \mapsto (8, 0)$ και για τις μονές θέσεις θα είναι: $Odd_A : (0, 0) \mapsto (0, 0)$.
Άρα ο μετασχηματισμός $Fourier$ του πολυωνύμου A θα είναι: (8, 0, 8, 0) το οποίο προκύπτει από τον υπολογισμό του συντελεστή περιστροφής, $X_{0,2} = E_0 \pm O_0$ και $X_{1,3} = E_1 \mp jO_1$ ($Twiddle\ Factor\ Calculation$).

Κάνουμε το ίδιο και στο δεύτερο πολυώνυμο, όπου το διάνυσμα συντελεστών είναι: (2,3,0,0). Ο μετασχηματισμός στις ζυγές και στις μονές θέσεις θα είναι: $Even_B : (2, 0) \mapsto (2, 2)$ και $Odd_B : (3, 0) \mapsto (3, 3)$.

Άρα ο μετασχηματισμός $Fourier$ του πολυωνύμου B θα είναι: $(5, 2-3\imath, -1, 2+3\imath)$.
Βρίσκουμε το μετασχηματισμό $Fourier$ του πολυωνύμου $C(x)$, πολλαπλασιάζοντας τους συντελεστές των A και B. Οι συντελεστές του C είναι: (40, 0, -8, 0). Όπως είπαμε και παραπάνω, πρέπει να εφαρμόσουμε τον αντίστροφο μετασχηματισμό ($iFFT$), για να ¨επαναφέρουμε' τους συντελεστές στην αρχική μορφή. Μια από τις πιο εντυπωσιακές ιδιότητες του FFT είναι ότι μπορεί να χρησιμοποιηθεί και προς τις δύο κατευθύνσεις με μερικές ελάχιστες διαφοροποιήσεις. Αυτή τη στιγμή έχουμε το αποτέλεσμα του *interpolation* και μπορούμε να εφαρμόσουμε τον FFT σε αυτό ακριβώς το διάνυσμα. Οι μόνες δύο διαφορές είναι οι εξής:

1. Αντί για το ω που χρησιμοποιήσαμε για να πάρουμε το *interpolated* διάνυσμα, στην αντίστροφη διαδικασία θα χρησιμοποιήσουμε στη θέση του το $\frac{1}{\omega}$
2. Το αποτέλεσμα θα είναι n φορές το διάνυσμα των συντελεστών, οπότε θα πρέπει να κάνουμε μια διαίρεση με το n.

Ο ψευδοκώδικας για τον αλγόριθμο του FFT είναι:

Fast Fourier Transform

```
FFT(a):
n = length(a); //a is the coefficients' vector
if n = 1 then return a
w = e^(2*pi*i/n); //the nth root of the universe
o = 1;
//Even and Odd coefficients
Even_A = [A0, ..., An - 2];
Odd_A = [A1, ..., An - 1];
x0 = FFT(Even_A);
x1 = FFT(Odd_A);
for k = 0 → n/2 - 1 do
    x[k] = x0[k] + o * x1[k];
    x[k + (n/2)] = x0[k] - o * x1[k];
    o = o*w;
return x
```

5.2 Κβαντική Διεμπλοκή

Η κβαντική διεμπλοκή έχει τις ρίζες της σε ένα άρθρο των A. Einstein, B. Podolsky και N. Rosen [4]. Ο σκοπός του άρθρου ήταν να αποδείξουν ότι η κβαντική μηχανική δεν είναι μια πλήρης φυσική θεωρία, αλλά ότι από την κβαντική περιγραφή της φύσης λείπουν κάποιες παράμετροι. Αργότερα οι παράμετροι αυτές ονομάστηκαν ¨κρυμμένες μεταβλητές¨. Σαν μοντέλο για την απόδειξη τους, χρησιμοποίησαν ένα θεωρητικό πείραμα στο οποίο δύο κβαντικλα συστήματα, αφού αλληλεπιδράσουν μεταξύ τους απομακρύνονται το ένα από το άλλο. Τα δύο αυτά κβαντικά συστήματα παραμένουν διασυνδεδεμένα το ένα με το άλλο με έναν

άγνωστο μη κλασσικό τρόπο. Αυτό έχει σαν αποτέλεσμα η μέτρηση μιας φυσικής ποσότητας του ενός, καθορίζει το αποτέλεσμα της μέτρησης της ίδιας φυσικής ποσότητας του άλλου. Το θεωρητικό αυτό πείραμα ονομάστηκε ¨παράδοξο EPR¨, από τα αρχικά των τριών ερευνητών. Η κβαντική διεμπλοκή είναι ίσως η πιο αινιγματική πλευρά της κβαντικής μηχανικής και δεν έχει κλασικό ανάλογο. Κάθε χρόνο πολλές δεκάδες άρθρα δημοσιεύονται σε επιστημονικά περιοδικά και περιγράφουν επιστημονικές εργασίες που έχουν ως στόχο την κατανόηση, το χειρισμό και τον υπολογισμό της κβαντικής διεμπλοκής. Για τους κβαντικούς υπολογιστές η κβαντική διεμπλοκή είναι ένας φυσικός πόρος, όπως η ενέργεια, τον οποίο μπορούμε να χρησιμοποιήσουμε για να εκτελέσουμε κβαντικούς υπολογισμούς και να αναπτύξουμε κβαντικούς αλγορίθμους [11]. Αυτό που έχει δηλαδή σημασία, δεν είναι να κατανοήσουμε τη φύση της κβαντικής διεμπλοκής (πράγμα που είναι ίσως αδύνατο), αλλά να μάθουμε να την παράγουμε και να τη χρησιμοποιούμε.

Lemma. *Δύο κβαντικά συστήματα βρίσκονται σε κβαντική διεμπλοκή, όταν η κατάσταση τους δεν μπορεί να γραφεί ως τανυστικό γινόμενο των βασικών τους καταστάσεων.*

Για να κατανοήσουμε καλύτερα τον παραπάνω ορισμό, θεωρούμε ότι τα δύο κβαντικά συστήματα είναι αυτά τα δύο $qubits$, $|q_{s0}\rangle, |q_{s1}\rangle$, που βρίσκονται στην κατάσταση $|q_s\rangle$, η οποία είναι η εξής:

$$|q_s\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$$

Όμως μπορούμε να γράψουμε την $|q_s\rangle$, μπορεί να γραφεί ως εξής:

$$|q_s\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle) = |1\rangle \otimes [\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)]$$

Αυτό σημαίνει ότι οι καταστάσεις των $|q_{s0}\rangle$ και $|q_{s1}\rangle$ είναι:

$$|q_{s1}\rangle = |1\rangle, |q_{s0} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

και τελικά

$$|q_s\rangle = |q_{s1}\rangle \otimes |q_{s0}\rangle$$

Πρακτικά η παραπάνω σχέση μας λέει ότι η $|q_s\rangle$ μπορεί να γραφεί ως τανυστικό γινόμενο των καταστάσεων των δύο $qubits$, δηλαδή τα $qubits$ δε βρίσκονται σε κβαντική διεμπλοκή αλλά σε υπέρθεση καταστάσεων.

Ας θεωρήσουμε τώρα δύο άλλα $qubits$ το $|q_{e0}\rangle$ και $|q_{e1}\rangle$. Αυτά τα δύο νέα $qubits$, βρίσκονται στην κατάσταση $|q_e\rangle$, η οποία είναι:

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

Σε αυτή την περίπτωση όμως, η $|q_e\rangle$ δεν μπορεί να γραφεί σαν τανυστικό γινόμεντο των καταστάσεων των δυο $qubits$, άρα αυτά βρίσκονται σε κβαντική διεμπλοκή.

5.2.1 Κβαντική Διεμπλοκή και Υπέρθεση

Είδαμε λοιπόν ότι ανάμεσα στην κβαντική διεμπλοκή και την υπέρθεση υπάρχουν κάποιες βασικές διαφορές. Εάν μετρήσουμε την κατάσταση του $qubit|q_{s1}\rangle$ της κατάστασης $|q_s\rangle$, θα δούμε σίγουρα ότι βρίσκεται στην κατάσταση $|1\rangle$. Το $|q_{s0}\rangle$, μετά από αυτή τη μέτρηση, μπορεί να βρίσκεται είτε στην κατάσταση $|0\rangle$ είτε στην κατάσταση $|1\rangle$ με πιθανότητα 0.5, για την κάθε περίπτωση. Που σημαίνει ότι η μέτρηση του ενός δεν καθορίζει την κατάσταση του άλλου. Αυτό έρχεται σε αντίθεση με τα αποτελέσματα του θεωρητικού πειράματος που οδήγησε στο ¨παράδοξο EPR˙, άρα δεν μιλάμε για κβαντική διεμπλοκή.

Αν όμως μετρήσουμε την κατάσταση του $|q_{e1}$ της κατάστασης $|q_e\rangle$, θα βρούμε ότι βρίσκεται στην κατάσταση $|0\rangle$ με πιθανότητα 0.5 και στην κατάσταση $|1\rangle$ με πιθανότητα πάλι 0.5. Αν το βρούμε στην κατάσταση $|0\rangle$ και μετρήσουμε το $|q_{e0}\rangle$, θα το βρούμε σίγουρα στην κατάσταση $|0\rangle$. Αντίστοιχα αν το $|q_{e1}\rangle$, είναι στην κατάσταση $|1\rangle$, τότε και το $|q_{e0}\rangle$, θα είναι στην κατάσταση $|1\rangle$. Αυτό σημαίνει, ότι η μέτρηση του ενός $qubit$ καθορίζει το άλλο, άρα βρίσκονται σε κβαντική διεμπλοκή.

5.3 Quantum Fourier Transformation

Όπως έχουμε αναφέρει και παραπάνω η μεγαλύτερη δύναμη των κβαντικών υπολογιστών, είναι η δυνατότητα να επιτελέσουν πράξεις και να επιλύσουν προβλήματα που δεν είναι δυνατό με τους κλασσικούς υπολογιστές. Για παράδειγμα η παραγοντοποίηση σε πρώτους αριθμούς ενός $n-bit$ ακεραίου χρησιμοποιώντας τον καλύτερο δυνατό κλασσικό αλγόριθμο, θα χρειαζόταν $exp(\Theta(n^{1/3}log^{2/3}n))$. Αυτό επί της ουσίας είναι εκθετικά το μέγεθος του ακεραίου τον οποίο θέλουμε να παραγωγίσουμε. Γι΄ αυτόν ακριβώς τον λόγο, το πρόβλημα της παραγοντοποίησης θεωρείται άλυτο στους κλασσικούς υπολογιστές. Αντίστοιχα, ένας κβαντικός υπολογιστής, έχει τη δυνατότητα να λύσει το ίδιο πρόβλημα σε $O(n^2lognlog(logn))$, που σημαίνει ότι ένας κβαντικός υπολογιστής μπορεί να λύσει εκθετικά πιο γρήγορα το συγκεκριμένο πρόβλημα. Αυτό μπορεί από μόνο του να είναι εντυπωσιακό, ωστόσο σίγουρα δημιουργούνται τα ερωτήματα του πόσα άλλα προβλήματα μπορεί να λυθούν με τη χρήση κβαντικών υπολογιστών. Εδώ θα εξετάσουμε τον κβαντικό μετασχηματισμό $Fourier$ ($QuantumFourierTransformation$), ο οποίος αποτελεί τη βάση για πολλούς κβαντικούς αλγορίθμους.

Στον γρήγορο μετασχηματισμό $Fourier$ [6] παίρνουμε σαν είσοδο ένα μιγαδικό διάνυσμα M-διάστασης, α και σαν έξοδο επιστρέφει ένα μιγαδικό διάνυσμα M-διάστασης, β. Έχουμε δηλαδή το εξής:

$$\begin{bmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \vdots \\ \beta_{M-1} \end{bmatrix} = \frac{1}{\sqrt{M}} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{M-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(M-1)} \\ & & \vdots & & \\ 1 & \omega^j & \omega^2 j & \dots & \omega^{(M-1)j} \\ & & \vdots & & \\ 1 & \omega^{(M-1)} & \omega^2(M-1) & \dots & \omega^{(M-1)(M-1)} \end{bmatrix} \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_{M-1} \end{bmatrix}$$

,όπου το ω είναι η Μοστή μιγαδική ρίζα της μονάδας. Οι κλασσικές μέθοδοι θα χρειαζόταν χρόνο $O(M^2)$, ενώ ο γρήγορος μετασχηματισμός $Fourier(FFT)$, μπορεί να κάνει ακριβώς το ίδιο σε χρόνο $O(MlogM)$. Παρά την μεγάλη αύξηση στην ταχύτητα που προκαλεί ο FFT, ο χβαντικός μετασχηματισμός $Fourier$, (QFT), καταφέρνει να μειώσει και άλλο τον χρόνο εκτέλεσης εκθετικά φτάνοντας τον σε $O(log^2 M)$.

Ο χβαντικός μετασχηματισμός $Fourier$ είναι ο ίδιος μετασχηματισμός με λίγο διαφορετικές συμβάσεις. Επί της ουσίας είναι ένας ορθομοναδιαίος συντελεστής του χώρου $Hilbert$ [12]. Είναι ένας μετασχηματισμός που αποτελεί τη βάση για πολλούς χβαντικούς αλγορίθμους. Συνοπτικά μετασχηματίζει μια συνάρτηση από το πεδίο ορισμού του χρόνου $(timedomain)$, στο πεδίο ορισμού της συχνότητας $(frequencydomain)$, δηλαδή συναρτήσεις με περίοδο r σε συναρτήσεις που οι μη μηδενικές τιμές τους είναι μόνο τα πολλαπλάσια της συχνότητας $\frac{1}{r}$ [5].

Το αμέσως επόμενο ερώτημα που προκύπτει αφορά το πως είναι εφικτό ο QFT να έχει χρόνο μικρότερο από M που είναι το μήκος της εισόδου. Για να είναι εφικτό, κωδικοποιούμε την είσοδο σε μια υπέρθεση μεγέθους $m = logM$ $qubits$. Η υπέρθεση αυτή αποτελείται από 2^m τιμές πλάτους. Θα μπορούσαμε να γράψουμε την υπέρθεση με τον εξής τρόπο: $|\alpha\rangle = \sum_{j=0}^{M-1} \alpha_j |j\rangle$, όπου το α_i είναι το εύρος της δυαδικής συμβολοσειράς $m - bit$ που αντιστοιχεί στο i με τον φυσικό τρόπο. Αυτό μας οδηγεί σε ένα βασικό σημείο: το $|j\rangle$ είναι επί της ουσίας ένας διαφορετικός τρόπος γραφής ενός διανύσματος, όπου ο δείκτης κάθε καταχώρησης γράφεται στο ειδικό σύμβολο της αγκύλης. Ξεκινώντας από την υπέρθεση $|\alpha\rangle$, ο QFT τρέχει σε $m = logM$ βήματα. Σε κάθε βήμα, η υπέρθεση εξελίσσεται έτσι ώστε να κωδικοποιεί τα ενδιάμεσα στάδια το ίδιο με τον κλασσικό FFT. Αυτό μπορεί να επιτευχθεί με m χβαντικές διεργασίες σε κάθε στάδιο. Επομένως, μετά από m τέτοια στάδια και $m^2 = log^2 M$ βασικές διεργασίες, καταλήγουμε στην υπέρθεση $|\beta\rangle$ που ανταποκρίνεται στο επιθυμητό αποτέλεσμα του QFT.

Πέραν αυτού όμως, ο QFT έχει μια βασική διαφορά στο αποτέλεσμα εξόδου του σε σχέση με τον FFT. Ο κλασσικός FFT, επιστρέφει σαν αποτέλεσμα τους M μιγαδικούς αριθμούς $\beta_0, \beta_1, ..., \beta_{M-1}$. Αντίθετα ο QFT, επιστρέφει την υπέρθεση $\sum_{j=0}^{M-1} \beta |j\rangle$. Τα δεδομένα αυτά όμως δεν είναι προσβάσιμα σε εμάς. Έτσι λοιπόν ο μόνος τρόπος για να αξιοποιήσουμε το αποτέλεσμα, είναι μετρώντας το. Η μέτρηση της κατάστασης του συστήματος αποδίδει μόνο $m = logM$ κλασσικά $bits$. Πιο συγκεκριμένα, η έξοδος είναι ο δείκτης j με πιθανότητα $|\beta_j|^2$. Ο QFT μπορεί να εφαρμοστεί για αυθαίρετες τιμές του M και μπορούμε να τον συνοψίσουμε ως εξής:

Input: A superposition of $m = logM$ qubits , $|\alpha\rangle = \sum_{j=0}^{M-1} \alpha_j |j\rangle$

Method: Using $O(m^2) = O(log^2 M)$ quantum operations perform the quantum FFT to obtain the superposition $|\beta\rangle = \sum j = 0^{M-1} \beta_j |j\rangle$.
Output: A random m-bit number j, from the probability distribution $Pr[j] = |\beta_j|^2$.

Ο κβαντικός μεταασχηματισμός *Fourier* ορίζεται σε μια ορθοκανονική βάση $|0\rangle, ..., |N\rangle$ ως εξής [11]:

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle$$

και άρα γράφεται:

$$\sum_{j=0}^{N-1} x_j |j\rangle \to \sum_{k=0}^{N-1} y_k |k\rangle$$

όπου τα πλάτη y_k είναι τα αντίστοιχα πλάτη x_j του διακριτού μετασχηματισμού *Fourier*. Ο μετασχηματισμός αυτός είναι *unitary* και έτσι μπορεί να αποτελέσει τη βάση για έναν κβαντικό υπολογιστή. Μπορεί να αποδειχθεί ως εξής: Έστω $N = 2^n$, όπου n κάποιος ακέραιος και η βάση $|0\rangle, ..., |2^n\rangle$ είναι η υπολογιστική βάση για έναν κβαντικό υπολογιστή *nqubit*. Για την κατάσταση $|j\rangle$, χρησιμοποιούμε τη δυαδική αναπαράσταση $j = j_1 j_2 ... j_n = j_1 2^{n-1} + j_2 n^{n-2} + ... + j_n 2^0$. Επίσης η έκφραση $0._{j_1 j_{l=1} ... j_n}$ θα αναπαριστά το δυαδικό κλάσμα $\frac{j_1}{2} + \frac{j_{l+1}}{4} + ... + \frac{j_m}{2^{m-l+1}}$. Από τη γραμμική άλγεβρα, μπορούμε να γράψουμε τον κβαντικό μετασχηματισμό *Fourier* με τον εξής τρόπο:

$$|j_1, ..., j_n\rangle \to \frac{(|0\rangle + e^{2\pi i 0._{j_1 j_n}} |1\rangle)(|0\rangle + e^{2\pi i 0._{j_1 j_n}} |1\rangle) ... (|0\rangle + e^{2\pi i 0._{j_1 j_2 ... j_n}} |1\rangle)}{2^{\frac{n}{2}}}$$

Η παραπάνω αναπαράσταση είναι τόσο χρήσιμη που θα μπορούσε να χρησιμοποιηθεί και σαν τον ορισμό του QFT. Οι παραπάνω δύο σχέσεις μπορούν να γραφούν και έτσι:

$$|j\rangle \to \frac{1}{2^{\frac{n}{2}}} \sum_{k=0}^{2^n - 1} e^{\frac{2\pi i j k}{2^n}} |k\rangle \tag{5.1}$$

$$= \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^{1} ... \sum_{k_n=0}^{1} e^{2\pi i j (\sum_{l=1}^{n} k_l 2^{-l})} |k_1 ... k_n\rangle \tag{5.2}$$

$$= \frac{1}{2^{\frac{n}{2}}} \sum_{k_1=0}^{1} ... \sum_{k_n=0}^{1} \bigotimes e^{2\pi i j k_l 2^{-l}} |k_l\rangle \tag{5.3}$$

$$= \frac{1}{2^{\frac{n}{2}}} \bigotimes [\sum_{k_n=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle] \tag{5.4}$$

$$= \frac{1}{2^{\frac{n}{2}}} \bigotimes [|0\rangle e^{2\pi i j 2^{-l}} |1\rangle] \tag{5.5}$$

$$= \frac{(|0\rangle + e^{2\pi i 0._{j_n}} |1\rangle)(|0\rangle + e^{2\pi i 0._{j_{n-1} j_n}} |1\rangle)(|0\rangle + e^{2\pi i 0._{j_1 j_2 ... j_n}} |1\rangle)}{2^{\frac{n}{2}}} \tag{5.6}$$

Και βλέπουμε ότι όντως ο QFT είναι $unitary$.

Εκτός από τις βασικές καταστάσεις, ο κβαντικός μετασχηματισμός $Fourier$ μπορεί να δράσει και σε υπερθέσεις των βασικών καταστάσεων ενός κβαντικού καταχωρητή. Έστω η παρακάτω υπέρθεση βασικών καταστάσεων:

$$x_0|0\rangle + x_1|1\rangle + ... + x_a|a\rangle + ... + x_{N-1}|N-1\rangle = \sum_{a=0}^{N-1} x_a|a\rangle$$

Ο κβαντικός μετασχηματισμός της υπέρθεσης, δίνεται από το παρακάτω:

$$\sum_{a=0}^{N-1} x_a|a\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{c=0}^{N-1} \sum_{a=0}^{N-1} x_a e^{2\pi i \frac{ac}{N}}|c\rangle = \frac{1}{\sqrt{N}} \sum_{c=0}^{N-1} y_c|c\rangle$$

όπου το y_c είναι ο κλασσικός μετασχηματισμός $Fourier$ του x_a που δίνεται από:

$$y_c = \sum_{a=0}^{N-1} x_a e^{a\pi i \frac{ac}{N}}$$

Για να γίνει ακόμα πιο κατανοητός ο QFT, μπορούμε να δούμε τα τρία παρακάτω παραδείγματα.

Παράδειγμα 5.1. *Η επίδραση του QFT σε ένα qubit.*
Αρχικά υποθέτουμε ότι το qubit βρίσκεται στην κατάσταση $|0\rangle$. Άρα σύμφωνα με τα παραπάνω:

$$|0\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{c=0}^{1} e^{2\pi i \frac{0c}{2}}|c\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Αν όμως το qubit βρίσκεται στην κατάσταση $|1\rangle$, τότε:

$$|1\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{2\pi i \frac{1c}{2}} |c\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{\pi i}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{5.7}$$

Όπως βλέπουμε, ο κβαντικός μετασχηματισμός $Fourier$ δρα σε ένα bit όπως η πύλη H. Για τον λόγο αυτό, η πύλη H αναφέρεται και ως "μετασχηματισμός $Hadamard$".

Παράδειγμα 5.2. *Εδώ θα δούμε τον QFT σε έναν κβαντικό καταχωρητή που αποτελείται από δύο qubits και βρίσκεται στην κατάσταση $|10\rangle$ που αντιστοιχεί στο δεκαδικό $|2\rangle$.*

$$|2\rangle \mapsto \frac{1}{\sqrt{4}} \sum_{c=0}^{3} e^{2\pi i \frac{2c}{4}}|c\rangle = \frac{1}{2}(|0\rangle + e^{\pi i}|1\rangle + e^{3\pi i}|2\rangle + e^{3\pi i}|3\rangle) = \frac{1}{2}(|0\rangle - |1\rangle - |3\rangle) \tag{5.8}$$

Αν αντίστοιχα ο κβαντικός καταχωρητής βρίσκεται στην κατάσταση $|01\rangle$, τότε:

$$|1\rangle \mapsto \frac{1}{\sqrt{4}} \sum_{c=0}^{3} e^{2\pi i \frac{2c}{4}}|c\rangle = \frac{1}{2}(|0\rangle + e^{\frac{\pi i}{2}}|1\rangle + e^{\pi i}|2\rangle + e^{\frac{3\pi i}{2}}|3\rangle) = \frac{1}{2}(|0\rangle - i|1\rangle - |2\rangle_i|3\rangle) \tag{5.9}$$

Παράδειγμα 5.3. *Εδώ το ίδιο παράδειγμα σε έναν καταχωρητή με τρία qubits που βρίσκεται στην κατάσταση* $|010\rangle$ *δηλαδή* $|2\rangle$*, στο δεκαδικό.*

$$|2\rangle \mapsto \frac{1}{\sqrt{8}} \sum_{c=0}^{7} e^{2\pi i \frac{2c}{8}} |c\rangle \tag{5.10}$$

$$= \frac{1}{\sqrt{8}} (|0\rangle + e^{\frac{\pi i}{2}}|1\rangle + e^{\pi i}|2\rangle + e^{\frac{3\pi i}{2}}|3\rangle + e^{2\pi i}|4\rangle + e^{\frac{5\pi i}{2}}|5\rangle + e^{3\pi i}|6\rangle + e^{\frac{7\pi i}{2}}|7\rangle) \tag{5.11}$$

$$= \frac{1}{\sqrt{8}} (|0\rangle + i|1\rangle - |2\rangle - i|3\rangle + |4\rangle + i|5\rangle - |6\rangle - i|7\rangle) \tag{5.12}$$

Από όλα τα παραπάνω μπορούμε να δούμε ότι ο κβαντικός μετασχηματισμός $Fourier$ μετασχηματίζει μια βασική κατάσταση ενός κβαντικού καταχωρητή σε υπέρθεση όλων των βασικών καταστάσεων, όπου όλες οι βασικές καταστάσεις έχουν το ίδιο πλάτος πιθανότητας αλλά διαφορετικές φάσεις.

Ο QFT μας βοηθάει να βρίσκουμε με ευκολία την περίοδο μιας περιοδικής συνάρτησης. Σε έναν κβαντικό καταχωρητή μεγέθους $qbits$, που βρίσκεται σε υπέρθεση περιοδικών καταστάσεων περιόδου r, με τον QFT στον κβαντικό καταχωρητή θα μείνουν μόνο οι τιμές που είναι πολλαπλάσια του $\frac{q}{r}$. Αυτά τα πολλαπλάσια είναι ισοπίθανα άρα μια μέτρηση θα μας επιστρέψει ένα από αυτά. [6].

Προσπαθώντας να συνοψίσουμε κάπως όλα τα παραπάνω, ο κλασσικός γρήγορος μετασχηματισμός $Fourier(FFT)$ έχει πλυποκότητα $O(NlogN) = O(2^n n)$ με $N = 2^n$, είναι δηλαδή πολύ γρήγορος. Ωστόσο ο κβαντικός μετασχηματισμός $Fourier$ είναι ακόμα πιο γρήγορας με πολυπλοκότητα $O(log^2 N) - O(n^2)$ [2].

Η βασική τους διαφορά είναι ότι ο FFT επιστρέφει τη σωστή απάντηση, ενώ ο QFT υπολογίζει την υπέρθεση τως σωστής απάντησης.

$$|q\rangle = \sum_{i=0}^{2^n-1} c_i |c\rangle \tag{5.13}$$

με την μέτρηση του παραπάνω προκύπτει ένας αριθμός $n - bit$ με πιθανότητα $|c_i|^2$

5.3.1 Περιοδικότητα

Ο QFT, θα μπορούσαμε να πούμε ότι είναι ένας γρήγορος τρόπος για να πάρει κάποιος μια γενική ιδέα του FFT. Ανιχνέυουμε ένα από τα μεγαλύτερα στοιχεία του διανλύσματος της εξόδου, χωρίς όμως να μπορούμε να δούμε τίποτα για αυτό πέραν του δείκτη του.

Έστω ότι η είσοδος του QFT, $|\alpha\rangle = (\alpha_0, ..., \alpha_{M-1})$, τέτοια ώστε $\alpha_i = \alpha_j$ κάθε φορά που $i \equiv jmodk$, όπου k είναι ένας ακέραιος ο οποίος διαιρεί το M. Δηλαδή ο πίνακας α αποτελείται από M/k επαναλήψεις κάποιας ακολουθίας $(\alpha_0, ..., \alpha_{k-1})$, μήκους k. Ας υποθέσουμε ότι μόνο ένας από τους k αριθμούς είναι μη μηδενικός, ας πούμε ο α_j. Τότε λέμε ότι το $|\alpha\rangle$, είναι περιοδικό, με περίοδο k και μετατόπιση j. Αυτό σημαίνει ότι εάν το διάνυσμα εισόδου είναι περιοδικό, τότε μπορούμε να χρησιμοποιήσουμε τον κλασσικό FFT για να υπολογίσουμε την περίοδο του. Προκύπτει λοιπόν ο εξής ορισμός:

Υποθέτουμε ότι η είσοδος στον QFT είναι περιοδική με περίοδο k, για κάποια k που διαιρούν το M. Τότε η έξοδος θα είναι πολλαπλάσιο του $\frac{M}{k}$ και είναι δυνατό να είναι οποιοδήποτε από τα k πολλαπλάσια του $\frac{M}{k}$.

Αυτό που μπροούμε να δούμε εδώ, είναι πως με την πολλαπλή επανάληψη της δειγματοληψίας και στη συνέχεια επιλέγοντας τον μεγαλύτερο κοινό διαιρέτη όλων των δεικτών που επιστράφηκαν, έχουμε πολύ μεγάλη πιθανότητα να πάρουμε τον $\frac{M}{k}$ και έτσι να είναι εφικτό να βρούμε την περίοδο k της εισόδου.

Lemma. *Έστω ότι έχουμε s ανεξάρτητα δείγματα τα οποία έχουν σχεδιαστεί ομοιόμορφα από*

$$0, \frac{M}{k}, \frac{2M}{k}, ..., \frac{(k-1)M}{k}$$

Τότε με πιθανότητα τουλάχιστον $1-\frac{k}{2^s}$, ο μέγιστος κοινός διαιρέτης όλως αυτών των δειγμάτων είναι το $\frac{M}{k}$.

Ο μόνος τρόπος για να μην συμβεί αυτό, είναι όλα τα δείγματα να είναι πολλαπλάσια του $j \cdot \frac{M}{k}$, όπου το j είναι ακέραιος μεγαλύτερος του 1. Η πιθανότητα ένα τυχαίο δείγμα να είναι πολλαπλάσιο του $j \cdot \frac{M}{k}$ είναι το πολύ $\frac{1}{j} \leq \frac{1}{2}$ και η πιθανότητα να είναι όλα τα δείγματα πολλαπλάσια του $j \cdot \frac{M}{k}$ είναι το μέγιστο $\frac{1}{2^s}$. Όλα αυτά ισχύουν για συγκεκριμένο αριθμό j. Η πιθανότητα αυτό να συμβεί για μερικά j, όπου $j \leq k$ είναι το πολύ ίση με το άθροισμα όλων αυτών των πιθανοτήτων πάνω από τις διαφορετικές τιμές του j, που δεν είναι περισσότερες από $\frac{k}{2^s}$. Μπορούμε να μειώσουμε την πιθανότητα αποτυχίας επιλέγοντας το s έτσι ώστε να είναι κατάλληλο πολλαπλάσιο του $logM$.

Κεφάλαιο 6

The Shor's Code

6.1 Quantum error-correction

Κεφάλαιο 7

RSA Cryptosystem

Κεφάλαιο 8

Future Work/What's Happening Now

Κεφάλαιο 9

Summary

Παράρτημα Α΄

Παράδειγμα Παραρτήματος

Α΄.1 Πρώτη ενότητα

Α΄.2 Μελλοντικές Επεκτάσεις

Βιβλιογραφία

[1] Fast fourier transform, χ.χ.

[2] Dawar Anuj. Quantum computing (lectures - university of cambridge), 2007-2008.

[3] Michel Le Bellac. *A Short Introduction to Quantum Information and Quantum Computation*. Cambridge University Press, New York, NY, USA, 2006.

[4] John Stewart Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1(3):195–200, 1964.

[5] Cristian S. Calude και Gheorghe Păun. *Computing with Cells and Atoms: An Introduction to Quantum, DNA and Membrane Computing*. Taylor & Francis/Hemisphere, Bristol, PA, USA, 2001.

[6] Sanjoy Dasgupta, Christos H. Papadimitriou και Umesh V. Vazirani. *Algorithms*. McGraw-Hill, 2008.

[7] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack, 1997.

[8] S. P. Gudder. Ultimate zero and one: Computing at the quantum frontier. *Foundations of Physics*, 30(4):607–610, 2000.

[9] Phillip Kaye, Raymond Laflamme και Michele Mosca. *An Introduction to Quantum Computing*. Oxford University Press, Inc., New York, NY, USA, 2007.

[10] Mikio Nakahara και Tetsuo Ohmi. *Quantum Computing - From Linear Algebra to Physical Realizations*. 2008.

[11] Michael A. Nielsen και Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10τηη έκδοση, 2011.

[12] Riley T. Perry. *The Temple of Quantum Computing*. 2006.

Συντομογραφίες - Αρκτικόλεξα - - Ακρωνύμια

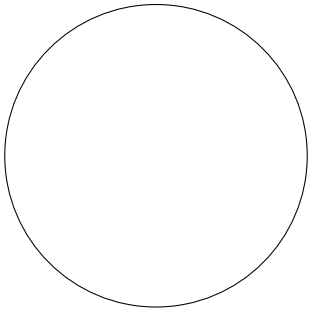
βλπ	βλέπε
κ.λπ.	και λοιπά
κ.ο.κ	και ούτω καθεξής
ΤΕΙ	Τεχνολογικό Εκπαιδευτικό Ίδρυμα
BPF	Band Pass Filter

Απόδοση ξενόγλωσσων όρων

Απόδοση	Ξενόγλωσσος όρος
αδερφός	sibling
αμεταβλητότητα	idempotency
ανάκτηση πληροφορίας	information retrieval
αντιμεταθετικότητα	commutativity
απόγονος	descedant
απορρόφηση	absorption
βάση δεδομένων	database
γνώρισμα	attribute
διαπροσωπεία	interface
διαφορά	difference
δικτυακός κατάλογος	portal catalog
δικτυωτή δομή	lattice
δομικές επερωτήσεις	structural queries
δομικές σχέσεις	structural relationships
δομικό σχήμα	schema
εγκυρότητα	validity
ένωση	union

ΤΕΙ ΠΕΛΟΠΟΝΝΗΣΟΥ - ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ - ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

Πρότυπο Σύστημα Ομότιμων Κόμβων Βασισμένο σε Σχήματα RDF



ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

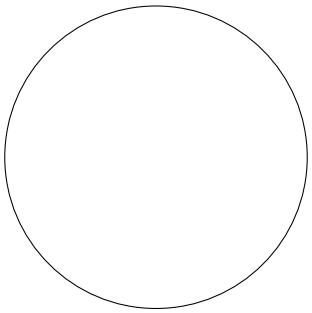
Κωνσταντίνος Δ. Δημητρίου

ΑΘΗΝΑ,
ΟΚΤΩΒΡΙΟΣ
2014

Θέση barcode

ΤΕΙ ΠΕΛΟΠΟΝΝΗΣΟΥ - ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ - ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

Πρότυπο Σύστημα Ομότιμων Κόμβων Βασισμένο σε Σχήματα RDF



ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κωνσταντίνος Δ. Δημητρίου

ΑΘΗΝΑ,
ΟΚΤΩΒΡΙΟΣ
2014

Θέση barcode

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Πρότυπο Σύστημα Ομότιμων Κόμβων Βασισμένο σε Σχήματα RDF

Κωνσταντίνος Δ. Δημητρίου

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2014

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Πρότυπο Σύστημα Ομότιμων Κόμβων Βασισμένο σε Σχήματα RDF

Κωνσταντίνος Δ. Δημητρίου

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2014