ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΜΟΙ

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΚΩΝΣΤΑΝΤΙΝΟΣ Σ. ΡΑΜΠΑΛΑΚΟΣ

Πανεπιστήμιο Κρήτης
Τμήμα Μαθηματικών, 2004

Αυτή η μεταπτυχιακή εργασία κατατέθηκε στο Τμημα Μαθηματικων του Πανεπιστημίου Κρήτης τον Νοεμβριο του 2004. Επιβλέπων καθηγητής ήταν ο κ.Μιχαλης Κολουτζάκης, τον οποίο θα ήθελα να ευχαριστήσω για την βοήθεια και την συμπαράσταση του καθ'ολη την διάρκεια της εργασίας . Την επιτροπή αποτέλεσαν οι : Α.Φειδάς, Θ.Μήτσης και Μ.Κολουτζάκης.

Περιεχόμενα

1 Εισαγωγή. **5**

2 Χώροι καταστάσεων. **9**

2.1 *Qubits.* 10
2.2 Πολλαπλά *qubits.* 11
2.3 Κβαντικές πύλες. 12
2.4 Μετρήσεις στον χώρο καταστάσεων. 15
2.5 Ο μετασχηματισμός *Hadamard.* 16
2.6 Ο αλγόριθμος του *Deutch.* 17
2.7 Το θεώρημα "μη αναπαραγωγής". 18
2.8 *Quantum teleportation.* 18

3 Ο αλγόριθμος αναζήτησης του *Grover*. **21**

3.1 Ο Αλγόριθμος του *Grover* είναι βέλτιστος. 25

4 Ο Αλγόριθμος του *P.Shor*. **31**

4.1 Μετασχηματισμός *Fourier* σε αβελιανές ομάδες. 31
4.1.1 Η ομάδα Χαρακτήρων. 31
4.1.2 Η *group* άλγεβρα $\mathbb{C}G$ ως χώρος *Hilbert*. 32
4.2 Διακριτός Μετασχηματισμός *Fourier* στο $\mathbb{Z}_n$. 35
4.3 *Quantum Fourier Transform* (*Q.F.T.*). 38
4.4 Ο αλγόριθμος του *P.Shor*. 41
4.4.1 Υπολογισμός της περιόδου της f_x. 41
4.4.2 Συνεχή Κλάσματα. 47
4.4.3 Από τον υπολογισμό της περιόδου μιας περιοδικής συνάρτησης, στην ανάλυση ενος ακεραίου σε πρώτους παράγοντες. . . 51

Κεφάλαιο 1

Εισαγωγή.

Στις αρχές της δεκαετίας του 80, ο *Richard Feynman* δημοσίευσε μια εργασία στην οποία αποδείκνυε ότι υπάρχουν φαινόμενα στον χώρο της κβαντικής μηχανικής τα οποία δεν μπορούν να εξομοιωθούν πλήρως σε ένα κλασσικό υπολογιστικό σύστημα. Το αποτέλεσμα αυτό προέκυψε εν τέλει φυσιολογικά, αν αναλογιστούμε το γεγονός ότι τα αντικείμενα που υπεισέρχονται στην μελέτη της κβαντικής μηχανικής λειτουργούν πολλές φορές πέρα από την προσδοκόμενη συμπεριφορά τους (με βάση την διαίσθησή μας, η οποία και αυτή με την σειρά της ακολουθεί την λογική της κλασσικής μηχανικής). Είναι πια κοινή αντίληψη ότι η κβαντική θεωρία είναι καθολική˙ οι νόμοι της ερμηνεύουν την λειτουργία του σύμπαντος, με την κλασσική μηχανική να περιορίζεται στην ερμηνεία των τοπικών συμπεριφορών των κβαντικών φαινομένων. Το γεγονός αυτό, γέννησε νέα ερωτήματα στην θεωρία της υπολογισιμότητας: Μήπως η εξομοίωση των κβαντικών φαινομένων μπορεί να πραγματοποιηθεί σε υπολογιστικά συστήματα τα οποία θα βασίζουν την λειτουργία τους στους νόμους της κβαντικής μηχανικής; Αυτά τα υπολογιστικά συστήματα (τα οποία και θα αποκαλούμε στο εξής κβαντικούς υπολογιστές), μήπως με την σειρά τους θα μπορούσαν να εξομοιώσουν την λειτουργία των κλασσικών υπολογιστών και, ακόμα περισσότερο, μήπως θα ήταν πολύ πιο ισχυρά από αυτούς;

Η κατασκευή κβαντικών υπολογιστών ή τουλάχιστον αλγορίθμων οι οποίοι θα πραγματοποιούνταν με την χρήση ενός κβαντικού υπολογιστή, αποδείχθηκε τελικά δύσκολη υπόθεση στα χρόνια που ακολούθησαν μετά την δημοσίευση του *Feynman*. Η εξέλιξη της θεωρίας της κβαντικής υπολογισιμότητας υπήρξε εξαιρετικά αργή μέχρι το 1994, οπότε και ο *Peter Shor* δημοσίευσε μια εργασία η οποία έμελλε να δώσει σημαντική ώθηση στην εν λόγω θεωρία˙ Στην εργασία αυτή, ο *Shor* περιέγραψε έναν κβαντικό αλγόριθμο πολυωνυμικής πολυπλοκότητας για την παραγοντοποίηση ακεραίων αριθμών, δίνοντας "λύση" σε ένα πρόβλημα το οποίο θεωρούταν από τους περισσότερους μαθηματικούς αδύνατο να λυθεί αποτελεσματικά με χρήση κλασσικών μεθόδων. Η εργασία αυτή προκάλεσε το ενδιαφέρον της μαθηματικής κοινότητας και έδωσε έναν αυτόνομο χαρακτήρα στην θεωρία της κβαντικής υπολογισιμότητας. Λίγα χρόνια νωρίτερα, είχε ήδη αποδειχθεί ότι οποιοσδήποτε κλασσικός αλγόριθμος θα μπορούσε να λειτουργήσει σε έναν

κβαντικό υπολογιστή, σε αντίστοιχο χρόνο. Ο $Shor$ λοιπόν απέδειξε ότι, αν είχαμε την δυνατότητα να κατασκευάσουμε έναν κβαντικό υπολογιστικό σύστημα, αυτό θα μπορούσε να ήταν γνήσια ισχυρότερο από οποιοδήποτε κλασσικό υπολογιστή, με δεδομένο ότι δεν γνωρίζουμε αν υπάρχει κλασικός πολυωνυμικός αλγόριθμος για την παραγοντοποίηση. Το γεγονός αυτό έχει από μόνο του τεράστιο ενδιαφέρον, προκαλώντας έτσι έντονη δραστηριότητα προς την κατεύθυνση της δημιουργίας ενός κβαντικού υπολογιστή, με τα πρώτα αποτελέσματα να έχουν κάνει ήδη την εμφάνιση τους έστω και σε εμβρυακό στάδιο (έχει κατασκευαστεί ο πρώτος $3-bit$ υπολογιστής, που λειτουργεί κάνοντας χρήση του κβαντικού περιβάλλοντος).

Η ισχύς ενός κβαντικού υπολογιστικού συστήματος έγκειται κύριως στο γεγονός ότι μπορεί να πραγματοποιήσει "παράλληλους" υπολογισμούς, χωρίς αυτό να προκαλεί εκθετική αύξηση του απαιτούμενου χώρου (όπως συμβαίνει στην κλασσική περίπτωση). Έτσι, στην ίδια χωρική ποσότητα, ο κβαντικός υπολογιστής πραγματοποιεί το ίδιο μέγεθος υπολογισμών σε εκθετικά λιγότερο χρόνο από τον αντίστοιχο ενός κλασσικού υπολογιστή. Τούτο οφείλεται στο γεγονός ότι ο χώρος καταστάσεων ενός κβαντικου συστήματος είναι ριζικά διαφορετικός από την κλασσική περίπτωση. Ένας συμβατικός υπολογιστής λειτουργεί σε έναν n-διάστατο χώρο ο οποίος αποτελείται από τις πεπερασμένες ακολουθίες από 0 και 1, τα $n-bits$. Το κβαντικό του ανάλογο είναι ένα σύστημα από $n-qubits$ το οποίο περιγράφεται σαν ένα μοναδιαίο διάνυσμα σε έναν διανυσματικό χώρο διάστασης 2^n. Το φαινόμενο της υπέρθεσης καταστάσεων σε έναν τέτοιο χώρο (το οποίο θα περιγράψουμε αναλυτικά στο Κεφάλαιο 2) προκαλεί την εκθετική αύξηση στο πλήθος των υπολογισμών που μπορούν να πραγματοποιηθούν σε δεδομένο χρόνο.

Παρ'όλο όμως που ένα κβαντικό σύστημα μπορεί να πραγματοποιήσει πολλούς υπολογισμούς ταυτόχρονα, η πρόσβαση στα αποτελέσματα αυτών των υπολογισμών δέχεται αυστηρούς περιορισμούς, οι οποίοι πηγάζουν από τα θεμελιώδη αξιώματα της κβαντικής μηχανικής. Για να τα διαχειριστεί κάποιος, θα πρέπει να επέμβει στην κατάσταση του κβαντικού συστήματος μέσω της παρατήρησης, γεγονός το οποίο με την σειρά του προκαλεί την προβολή αυτής της κατάστασης σε κάποιο από τα διανύσματα βάσης του χώρου καταστάσεων μέσω της κατανομής πιθανότητας μιας διακριτής τυχαίας μεταβλητής. Οι τιμές αυτής της μεταβλητής αντιστοιχούν στα αποτελέσματα των υπολογισμών που πραγματοποιούνται από έναν κβαντικό υπολογιστή. Όχι μόνο λοιπόν δεν μπορούμε να δούμε παρά ένα αποτέλεσμα κάθε φορά, αλλά και αυτό το αποτέλεσμα δεν μπορούμε καν να το προβλέψουμε πλήρως. Στο κεφάλαιο 2 περιγράφουμε αναλυτικά την διαδικασία παρατήρησης της κατάστασης ενός κβαντικού συστήματος, καθώς και ορισμένους πολύ βασικούς $unitary$ τελεστές που χρησιμοποιούνται σαν βήματα για τους περισσότερους κβαντικούς αλγορίθμους.

Τα τελευταία χρόνια, έχουν ανακαλυφθεί ορισμένες τεχνικές διαχείρισης του προβλήματος της μέτρησης οι οποίες χρησιμοποιούν μεθόδους εώς τώρα άγνωστες στην θεωρία της κλασσικής υπολογισιμότητας. Στο κεφάλαιο 3 περιγράφουμε αναλυτικά τον αλγόριθμο αναζήτησης του $Grover$, στον οποίο η κβαντική κατάσταση μετασχηματίζεται κατάλληλα έτσι ώστε να αυξηθεί η πιθανότητα εμφάνισης του αποτελέσματος που επιθυμούμε να πάρουμε ύστερα από μια μέτρηση (μια παρατήρηση δηλαδή του χώρου καταστάσεων του συστήματος). Αποδεικνύουμε

παράλληλα ότι ο αλγόριθμος του *Grover* είναι βέλτιστος ανάμεσα στούς αλγορίθμους αναζήτησης ενός στοιχείου μιας βάσης δεδομένων. Στο κεφάλαιο 4 περιγράφεται ο αλγόριθμος παραγοντοποίησης ακεραίων του *P.Shor*, ο οποίος χρησιμοποιεί ένα κβαντικό ανάλογο του διακριτού μετασχηματισμού *Fourier* για να εξάγει την περίοδο μιάς συνάρτησης με πιθανότητα σχεδόν ίση με 1. Η τελευταία αυτή τεχνική χρησιμοποιείται και στούς περισσότερους κβαντικούς αλγορίθμους που έχουν ανακαλυφθεί μέχρι σήμερα.

Κεφάλαιο 2

Χώροι καταστάσεων.

Ας θεωρήσουμε ένα κβαντικό σύστημα, δηλαδή ένα φυσικό σύστημα που αποτελείται από ένα ή περισσότερα "σωματίδια". Η κατάσταση ενός τέτοιου κβαντικού συστήματος σε δεδομένο χρόνο t μπορεί να αναπαρασταθεί σαν ένα μοναδιαίο διάνυσμα σε έναν χώρο $Hilbert$ $\mathbb{H}$, ο οποίος ονομάζεται χώρος καταστάσεων του συστήματος. Ο χώρος καταστάσεων H θεωρείται διαχωρίσιμος διανυσματικός χώρος πάνω από το $\mathbb{C}$ και για τους κβαντικούς αλγορίθμους αρκεί να θεωρήσουμε ότι ο $\mathbb{H}$ έχει πεπερασμένη διάσταση, είναι δηλαδή ισόμορφος με τον $\mathbb{C}^n$ για κάποιο $n \in \mathbb{N}$.

Θα χρησιμοποιήσουμε τον $Dirac$ συμβολισμό για τα στοιχεία του $\mathbb{H}$. Έτσι, κάθε $x \in \mathbb{H}$ θα συμβολίζεται ως $|x\rangle$. Στην κβαντική υπολογισιμότητα οι καταστάσεις της μορφής $\lambda|x\rangle$, $\lambda \in \mathbb{C}$, θα θεωρούνται ως ίδιες, για δεδομένο $|x\rangle$. Από την ανισότητα $Cauchy - Schwartz$, για κάθε $x \in \mathbb{H}$, η απεικόνιση $x^* : H \mapsto \mathbb{C}$ με $x^*(y) = \langle x, y\rangle$ για κάθε $y \in \mathbb{H}$, είναι φραγμένο γραμμικό συναρτησιοειδές, το οποίο και θα συμβολίζουμε με $\langle x|$. Εάν $|x\rangle, |y\rangle \in \mathbb{H}$, τότε $\langle x|y\rangle := \langle x|\big(|y\rangle\big)$ θα είναι το εσωτερικό τους γινόμενο και $|x\rangle\langle y|$ το εξωτερικό τους γινόμενο, δηλαδή η απεικόνιση που ορίζεται ως

$$|x\rangle\langle y| : \mathbb{H} \mapsto \{\alpha|x\rangle : \alpha \in \mathbb{C}\}$$

$$|x\rangle\langle y|\Big(|z\rangle\Big) = \langle y|z\rangle|x\rangle$$

για κάθε $|z\rangle \in \mathbb{H}$.

Για παράδειγμα, αν $\{|0\rangle, |1\rangle\}$ είναι η ορθοκανονική βάση του $\mathbb{C}^2$ τότε το εξωτερικό γινόμενο $|0\rangle\langle 1|$ μετασχηματίζει το διάνυσμα $|1\rangle$ στο $|0\rangle$ και αφήνει αναλλοίωτο το $|0\rangle$,

$$|0\rangle\langle 1||1\rangle = \langle 1|1\rangle|0\rangle = |0\rangle$$

και

$$|0\rangle\langle 1||0\rangle = \langle 1|0\rangle|0\rangle = |0\rangle$$

Ισοδύναμα, μπορούμε να γράψουμε το $|0\rangle\langle 1|$ στην μορφή πίνακα. Αν $|0\rangle = (1,0)^T$, $\langle 0| = (1,0)$, $|1\rangle = (0,1)^T$, $\langle 1| = (0,1)$ είναι οι αναπαραστάσεις των διανυσμάτων βάσης και των αντίστοιχων δυϊκών τους στοιχείων, τότε

$$|0\rangle\langle 1| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Αντίστοιχα, ο μετασχηματισμός που απεικονίζει το $|0\rangle$ στο $|1\rangle$ και αντίστροφα, δίνεται από τον τελεστή

$$\mathcal{X} = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Μετασχηματισμοί της παραπάνω απλής μορφής θα αποδειχθούν πολύ σημαντικοί στην συνέχεια.

2.1 *Qubits.*

Το απλούστερο κβαντικό σύστημα που εμφανίζεται στην κβαντική υπολογισιμότητα είναι το *qubit*. Ο χώρος καταστάσεων του είναι ο $\mathbb{C}^2$, με ορθοκανονική βάση τις καταστάσεις $\{|0\rangle := (1,0),\ |1\rangle := (0,1)\}$, η οποία θα αναφέρεται στο εξής ως υπολογιστική βάση του *qubit*. Βέβαια, οποιαδήποτε βάση του $\mathbb{C}^2$ μπορεί να χρησιμοποιηθεί ως υπολογιστική βάση για τους υπολογισμούς μας, με την προυπόθεση αυτή να μένει αμετάβλητη κατά την διάρκεια αυτών των υπολογισμών. Συμβατικά όμως, εκτός αν δηλώνεται διαφορετικά, όλες οι μετρήσεις (παρατηρήσεις) που πραγματοποιούμε στον χώρο καταστάσεων ενός *qubit* θα γίνονται ως προς την υπολογιστική βάση $\{|0\rangle, |1\rangle\}$.

Ένα *qubit* $|x\rangle$ είναι λοιπόν ένα διάνυσμα στην μοναδιαία μπάλα του $\mathbb{C}^2$, της μορφής $|x\rangle = \alpha|0\rangle + \beta|1\rangle$, $\alpha, \beta \in \mathbb{C}$. Εάν $\alpha = 0, \beta = 1$ ή $\alpha = 1, \beta = 0$, τότε $|x\rangle = |0\rangle$ ή $|x\rangle = |1\rangle$, οπότε το *qubit* ταυτίζεται σε αυτή την περίπτωση με τα "κλασικά *bits*" $0, 1$. Τα *qubits* θα θεωρούνται λοιπόν ως το κβαντικό ανάλογο των *bits*, των θεμελιωδών μονάδων της κλασσικής υπολογισιμότητας και ως τέτοια θα χρησιμοποιούνται στο εξής.

Εδώ όμως προκύπτει ήδη μια από τις θεμελιώδεις διαφορές μεταξύ κβαντικών και κλασσικών υπολογισμών. Ένα *qubit* δεν έχει μονάχα την δυϊκή υπόσταση $|0\rangle$ ή $|1\rangle$ διότι, εξ ορισμού, μπορεί να βρίσκεται σε οποιαδήποτε υπέρθεση των $|0\rangle, |1\rangle$ το διατηρεί στην μοναδιαία μπάλα του $\mathbb{C}^2$. Το σύνολο λοιπόν των *qubits* στον χώρο καταστάσεων είναι υπεραριθμήσιμο, κατά συνέπεια ένα *qubit* περιέχει απείρως μεγαλύτερη πληροφορία από τα κλασσικά *bits*.

Βεβαίως, για να μπορέσουμε να εκμεταλλευτούμε αυτή την ισχυρή ιδιότητα, θα πρέπει κατ' αρχήν να παρατηρήσουμε αυτό το *qubit* μέσα στον χώρο καταστάσεων του (στην κβαντική υπολογισιμότητα, οποιαδήποτε παρατήρηση ενός κβαντικού συστήματος ονομάζεται "μέτρηση"). Σε αυτό το σημείο προκύπτει όμως ένα, κατά τα φαινόμενα, ανυπέρβλητο εμπόδιο. Σύμφωνα με τις αρχές της κβαντικής μηχανικής, οποιαδήποτε παρατήρηση μιας κατάστασης του κβαντικού συστήματος προβάλει αυτόματα το διάνυσμα της στην ορθοκανονική βάση του χώρου καταστάσεων και έτσι το αποτέλεσμα μιας τέτοιας παρατήρησης θα είναι κάποιο

από τα διανύσματα βάσης. Αν παρατηρήσουμε λοιπόν ένα *qubit*, το μόνο που θα δούμε είναι τα *bits* 0,1, τα οποία αντιστοιχούν στα διανύσματα $|0\rangle, |1\rangle$ της υπολογιστικής βάσης του $\mathbb{C}^2$. Παίρνουμε έτσι την ίδια πληροφορία που θα παίρναμε και στην κλασσική περίπτωση. Στην παράγραφο 2.3 , όπου θα μελετήσουμε αναλυτικά την έννοια της μέτρησης, θα δούμε ότι η κατάσταση γίνεται ακόμα πιο πολύπλοκη· όχι μόνο παίρνουμε απλά την κλασσική πληροφορία $0, 1$, αλλά μιας και οι μετρήσεις είναι πιθανοθεωρητικές διαδικασίες (τυχαίες μεταβλητές), δεν γνωρίζουμε με βεβαιότητα ποια από τις δυο τιμές θα προκύψει ως αποτέλεσμα. Ο βασικός σκοπός λοιπόν ενός κβαντικού αλγορίθμου είναι το πως θα διαχειριστεί το κβαντικό περιβάλλον κατάλληλα, ώστε να εξάγει με μια μέτρηση στο τέλος των υπολογισμών το επιθυμητό αποτέλεσμα με όσο το δυνατόν μικρότερο σφάλμα (δες παρ. 2.4).

2.2 Πολλαπλά *qubits*.

Η ισχύς των κβαντικών υπολογισμών αρχίζει να φαίνεται καθαρά, εάν εισάγουμε την έννοια των $n - qubits$.

Ας θεωρήσουμε λοιπόν ένα κβαντικό σύστημα το οποίο αποτελείται από n το πλήθος *qubits*, κάθε ένα με την αντίστοιχη υπολογιστική βάση $\{|0\rangle, |1\rangle\}$. Τότε, ο χώρος καταστάσεων $\mathbb{H}^n$ του συστήματος είναι, σύμφωνα με τα αξιώματα της κβαντικής μηχανικής, το τανυστικό γινόμενο των χώρων καταστάσεων των *qubits* από τα οποία αποτελείται,

$$\mathbb{H}^n := \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes ... \otimes \mathbb{C}^2 = \mathbb{C}^{2^n}.$$

Ας ανακαλέσουμε κατ' αρχήν τον ορισμό του τανυστικού γινομένου δυο διανυσματικών χώρων $\mathbb{W}, \mathbb{V}$ πεπερασμένης διάστασης:

Ορισμός 2.2.1 *Εστω $\mathbb{W} = \mathbb{C}^m$, $\mathbb{V} = \mathbb{C}^n$, $m, n \in \mathbb{N}$. Τότε, ορίζεται φυσιολογικά η απεικόνιση $T : \mathbb{W} \times \mathbb{V} \mapsto \mathbb{C}^{mn}$, με τύπο*

$$T\Big(((x_1, x_2, ..., x_m), (y_1, y_2, ..., y_n))\Big) = (x_1y_1, x_1y_2, .., x_1y_n, .., x_my_1, x_my_2, .., x_my_n),$$

για κάθε $(x_1, x_2, ..., x_m) \in \mathbb{W}$ και $(y_1, y_2, ..., y_n) \in \mathbb{V}$.

Αν $w \in \mathbb{W}$, $v \in \mathbb{V}$, τότε το $T(w, v)$ θα λέγεται τανυστικό γινόμενο των w, v και συμβολικά θα γράφουμε $T(w, v) = w \otimes v$.

Το ζεύγος $(\mathbb{C}^{mn}, \otimes)$ ονομάζεται τανυστικό γινόμενο των $\mathbb{W}, \mathbb{V}$ (συμβολικά, $\mathbb{C}^{mn} := \mathbb{W} \otimes \mathbb{V}$) και αποτελείται από όλα τα πεπερασμένα τυπικά αθροίσματα της μορφής $\sum_{i,j\in\mathcal{I}} \alpha_{i,j} w_i \otimes v_j$, όπου $w_i \in \mathbb{W}$,$v_j \in \mathbb{V}$,$\alpha_{i,j} \in \mathbb{C}$, $\mathcal{I} \subset \mathbb{N}$.

Εύκολα ελέγχονται οι ακόλουθες στοιχειώδεις ιδιότητες του τανυστικού γινομένου: Για κάθε $w_1, w_2 \in \mathbb{W}$, $v_1, v_2 \in \mathbb{V}$, $\alpha \in \mathbb{C}$ ισχύει,

(i) $\alpha(w_1 \otimes v_1) = (\alpha w_1) \otimes v_1 = w_1 \otimes (\alpha v_1)$,

(ii) $(w_1 + w_2) \otimes v = w_1 \otimes v + w_2 \otimes v$,

(iii) $w \otimes (v_1 + v_2) = w_1 \otimes v_1 + w \otimes v_2$,

(iv) $\langle w_1 \otimes v_1 | w_2 \otimes v_2 \rangle = \langle w_1 | w_2 \rangle \langle v_1 | v_2 \rangle$.

Αν $\mathcal{A} : \mathbb{W} \mapsto \mathbb{W}$, $\mathcal{B} : \mathbb{V} \mapsto \mathbb{V}$ είναι γραμμικοί τελεστές, τότε ορίζεται το τανυστικό τους γινόμενο,

$$\mathcal{A} \otimes \mathcal{B} : \mathbb{W} \otimes \mathbb{V} \mapsto \mathbb{W} \otimes \mathbb{V}$$
$$(\mathcal{A} \otimes \mathcal{B})(w \otimes v) = \mathcal{A}w \otimes \mathcal{B}v,$$

για κάθε $w \in \mathbb{W}$, $v \in \mathbb{V}$.

Εάν τώρα $\{w_i\}_{i=1}^m$, $\{v_j\}_{j=1}^n$ είναι ορθοκανονικές βάσεις για τους $\mathbb{W}$, $\mathbb{V}$ αντίστοιχα, τότε μπορούμε εύκολα να αποδείξουμε ότι το σύνολο $\{w_i \otimes v_j / i = 1, ..., m,\ j = 1, ..., n\}$ είναι ορθοκανονική βάση του τανυστικού τους γινομένου.

Για παράδειγμα, σε ένα κβαντικό σύστημα που αποτελείται από 2 $qubits$ κάθε ένα με την υπολογιστική βάση $\{|0\rangle, |1\rangle\}$, ο χώρος καταστάσεων είναι ο $\mathbb{C}^2 \otimes \mathbb{C}^2 := \mathbb{C}^4$, τετραδιάστατος διανυσματικός χώρος πάνω από το $\mathbb{C}$ με την ορθοκανονική βάση $\Big\{ |0\rangle \otimes |0\rangle,\ |0\rangle \otimes |1\rangle,\ |1\rangle \otimes |0\rangle,\ |1\rangle \otimes |1\rangle \Big\}$, την οποία θα γράφουμε συντομότερα ως $\{|00\rangle,\ |01\rangle,\ |10\rangle,\ |11\rangle\}$. Αντίστοιχα, η υπολογιστική βάση για ένα $3 - qubit$ κβαντικό σύστημα είναι η $\{|000\rangle,\ |001\rangle,\ |010\rangle,\ |011\rangle,\ |100\rangle, |101\rangle,\ |110\rangle,\ |111\rangle\}$. Παρατηρώντας λίγο τα διανύσματα αυτής της βάσης, βλέπουμε ότι περιέχουν όλους τους ακεραίους x με $0 \leq x < 2^3 - 1$ γραμμένους στην δυαδική τους αναπαράσταση. Γενικότερα λοιπόν, μπορούμε να γράψουμε την υπολογιστική βάση του χώρου καταστάσεων ενός $n - qubit$ στην ποιο απλή μορφή $\{|x\rangle : 0 \leq x < 2^n - 1,\ \textit{το } x \textit{ στην δυαδική του αναπαράσταση}\}$. Η διάσταση του $\mathbb{C}^{2^n}$ πάνω από το $\mathbb{C}$ είναι 2^n, έχουμε λοιπόν εκθετική αύξηση του χώρου καταστάσεων όσο αυξάνουμε το πλήθος των $qubits$ που περιέχει. Αυτή ακριβώς υποδεικνύει και μια πιθανή εκθετική αύξηση στην ταχύτητα των υπολογισμών κάνοντας χρήση του κβαντικού υπολογιστικού περιβάλλοντος , γεγονός που επιβεβαιώνεται τελικά μέσα από τους αλγορίθμους που θα περιγράψουμε στα επόμενα κεφάλαια.

Τα διανύσματα βάσης στον χώρο καταστάσεων ενός $n - qubit$ μπορούν να γραφούν λοιπόν στην μορφή τανυστικού γινομένου των διανυσμάτων βάσης των επι μέρους $qubit$ από τα οποία αποτελείται. Το επόμενο παράδειγμα αποδεικνύει ότι κάτι τέτοιο δεν ισχύει για μια τυχαία κατάσταση του $\mathbb{C}^{2^n}$· πράγματι, ας θεωρήσουμε το $2 - qubit$ $\frac{1}{\sqrt{2}}\big(|10\rangle + |01\rangle\big)$, και ας υποθέσουμε ότι αυτό μπορεί να γραφεί σαν το τανυστικό γινόμενο δύο $qubits$ $\alpha_1|0\rangle + \beta_1|1\rangle$, $\alpha_2|0\rangle + \beta_2|1\rangle$ με $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{C}$. Τότε,

$$\big(\alpha_1|0\rangle + \beta_1|1\rangle\big) \otimes \big(\alpha_2|0\rangle + \beta_2|1\rangle\big) = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle,$$

οπότε $\alpha_1\alpha_2 = \beta_1\beta_2 = 0$, το οποίο είναι άτοπο.

Καταστάσεις αυτής της μορφής, οι οποίες δεν συναντώνται στην κλασσική περίπτωση, θα τις ονομάζουμε μεικτές και σε αυτές ακριβώς οφείλεται η εκθετική αύξηση στον χώρο καταστάσεων των κβαντικών συστημάτων που μελετάμε.

2.3 Κβαντικές πύλες.

Ας δούμε τώρα πως μπορούμε να πραγματοποιήσουμε υπολογισμούς, χρησιμοποιώντας το μοντέλο της κβαντικής υπολογισιμότητας που έχουμε ορίσει εώς τώρα. Για

να πραγματοποιηθεί οποιοδήποτε είδος υπολογισμού στον χώρο καταστάσεων ενός $n-qubit$, θα πρέπει φυσικά να διαταράξουμε αυτόν τον χώρο, θα πρέπει δηλαδή να προκαλέσουμε την εξέλιξή του μεταξύ δύο χρονικών σημείων. Οποιαδήποτε εξέλιξη ενός απομονωμένου κβαντικού συστήματος $\mathbb{H}$ αναπαρίσταται από έναν $unitary$ τελεστή, δηλαδή έναν γραμμικό φραγμένο τελεστή $\mathbb{U} : \mathbb{H} \mapsto \mathbb{H}$ τέτοιο ώστε $\mathbb{U}\mathbb{U}^* = \mathbb{I}$, όπου $\mathbb{U}^*$ είναι ο συζυγής τελεστής του $\mathbb{U}$, ο τελεστής για τον οποίο ισχύει $\langle \mathbb{U}x|y\rangle = \langle x|\mathbb{U}^*y\rangle$ για κάθε $x, y \in \mathbb{H}$. Οι κβαντικοί υπολογισμοί είναι λοιπόν πεπερασμένες ακολουθίες $unitary$ τελεστών, οι οποίοι δρούν στον χώρο καταστάσεων ενός $n-qubit$ (του υπολογιστικού συστήματος) μέσω της σύνθεσης, έχουν δηλαδή την μορφή:

$$\mathcal{W}_1 \circ \mathcal{W}_2 \circ ... \circ \mathcal{W}_n : \mathbb{H} \longmapsto \mathbb{H}$$

για κάποιους $unitary$ τελεστές $\{\mathcal{W}_i\}_{i=1}^n : \mathbb{H} \longmapsto \mathbb{H}$. Κάθε $\mathbb{W}_i$ θα αντιστοιχεί σε χρόνο 1 και θα εφαρμόζεται στον χώρο καταστάσεων ενός $qubit$, ενός $2-qubit$ ή ενός $3-qubit$ (σε αντιστοιχία με τους κλασσικούς υπολογισμούς, μια τέτοια ακολουθία δεν μπορεί να εφαρμοστεί συνολικά σε ένα $n-qubit$).

Εύκολα βλέπουμε ότι οι $unitary$ τελεστές, τους οποίους θα ονομάζουμε στο εξής "κβαντικές πύλες", είναι ισομετρίες του $\mathbb{H}$:

$$\|\mathbb{U}(x)\|^2 = \langle \mathbb{U}x|\mathbb{U}x\rangle = \langle x|\mathbb{U}^*\mathbb{U}x\rangle = \langle x|x\rangle = \|x\|^2$$

για κάθε $x \in \mathbb{H}$. Αυτή τους η ιδιότητα είναι απολύτως απαραίτητη για την εξέλιξη του κβαντικού υπολογιστικού συστήματος, αφού με αυτό τον τρόπο απεικονίζονται "καταστάσεις" σε "καταστάσεις" (υπενθυμίζουμε εδώ ότι οι καταστάσεις του κβαντικού συστήματος δεν είναι παρά τα στοιχεία που βρίσκονται στην μοναδιαία σφαίρα του $\mathbb{H}$.).

Οι $unitary$ τελεστές είναι εξ ορισμού αντιστρέψιμοι στον $\mathbb{H}$. Έπεται λοιπόν ότι οι κβαντικές πύλες που μπορούν να χρησιμοποιηθούν σε έναν κβαντικό αλγόριθμο θα πρέπει να είναι αντιστρέψιμοι μετασχηματισμοί κάποιου κατάλληλου χώρου καταστάσεων, σε αντίθεση με την κλασική υπολογιστική θεωρία στην οποία υπάρχουν μη αντιστρέψιμες διαδικασίες. Ένα από τα βασικότερα ερωτήματα που τέθηκαν λοιπόν κατά την θεμελίωση της κβαντικής υπολογιστικής θεωρίας είναι το κατά πόσο ένας κβαντικός υπολογιστής θα μπορούσε να εξομοιώσει επαρκώς τους υπολογισμούς που μπορεί να πραγματοποιήσει ένας συμβατικός υπολογιστής. Η απάντηση σε αυτό το ερώτημα ήταν τελικά καταφατική και δώθηκε από τους $Bennet\ Fredkin$ και $Toffoli$, οι οποίοι απέδειξαν ότι οποιοσδήποτε κλασσικός υπολογισμός μπορεί να αντιστραφεί (και κατ' επέκταση να εξομοιωθεί από μια πεπερασμένη ακολουθία από κβαντικές πύλες).

Ας δούμε όμως ορισμένα απλά παραδείγματα κβαντικών πυλών τα οποία είναι καθοριστικής σημασίας για τους αλγορίθμους που θα περιγράψουμε στα επόμενα κεφάλαια. θα μας απασχολήσουν κατ'αρχήν $unitary$ τελεστές οι οποίοι δρούν στον $\mathbb{C}^2$, στον χώρο καταστάσεων ενός απλού $qubit$. Αν $\{|0\rangle, |1\rangle\}$ είναι η υπολογιστική βάση του $\mathbb{C}^2$, τότε ο απλούστερος τέτοιος τελεστής είναι ο ταυτοτικός τελεστής $\mathbb{I}$, ο οποίος αφήνει αναλλοίωτα τα στοιχεία της βάσης. Οι πίνακες $Pauli$

$$\mathcal{X} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \ \mathcal{Y} = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix} \ \mathcal{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

είναι *unitary* μετασχηματισμοί του $\mathbb{C}^2$. Για παράδειγμά,

$$\mathcal{Y}\mathcal{Y}^* = \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix} \begin{bmatrix} 0 & -\imath \\ \imath & 0 \end{bmatrix} = \mathbb{I},$$

οπότε μπορούν και αυτοί με την σειρά τους να χρησιμοποιηθούν ως κβαντικές πύλες.

Ιδιαίτερα σημαντικός είναι και ο $\mathbb{C}_{not}$ τελεστής, ο οποίος δρα γραμμικά στον χώρο καταστάσεων ενός 2-*qubit* ως εξής:

$$|00\rangle \longmapsto |00\rangle$$
$$|01\rangle \longmapsto |01\rangle$$
$$|10\rangle \longmapsto |11\rangle$$
$$|11\rangle \longmapsto |10\rangle$$

Χρησιμοποιώντας δηλαδή το πρώτο *bit* σαν οδηγό, αλλάζει την τιμή του δεύτερου *bit*, αν το πρώτο *bit* είναι 1 και το αφήνει αναλλοίωτο, αν το πρώτο *bit* είναι 0. Έτσι λοιπόν, ο $\mathbb{C}_{not}$ τελεστής έχει την αναπαράσταση

$$\mathbb{C}_{not} := (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Τέλος, μπορεί να αποδειχθεί (*Ekert,Jozsa*) ότι οι *unitary* μετασχηματισμοί

$$\mathbb{U}_1 = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix},\ \mathbb{U}_2 = \begin{bmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{bmatrix},$$

$$\mathbb{U}_3 = \begin{bmatrix} e^{i\theta} & 0 \\ 0 & 1 \end{bmatrix},\ \mathbb{U}_4 = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

μαζί με τους αντίστοιχους αντιστρόφους τους $\mathbb{U}_5, \mathbb{U}_6, \mathbb{U}_7, \mathbb{U}_8$, αποτελούν ένα καθολικό σύνολο κβαντικών πυλών στον χώρο καταστάσεων ενός *qubit*, με την έννοια ότι αν το θ είναι άρρητο πολλαπλάσιο του π, το σύνολο $\{\mathbb{U}_1, \mathbb{U}_2, ...\mathbb{U}_8\}$ παράγει μια ομάδα με πράξη την σύνθεση, η οποία είναι πυκνή στο ομάδα $\mathbb{U}(2)$ των *unitary* μετασχηματισμών του $\mathbb{C}^2$. Έτσι, για κάθε $\epsilon > 0$ και για κάθε $\mathbb{U} \in \mathbb{U}(2)$, υπάρχει $\mathbb{U}_n$ της μορφής $\mathbb{U}_n = \mathbb{U}_{n_1}\mathbb{U}_{n_2}...\mathbb{U}_{n_k}$, $n_i \in \{1, 2, ..., 8\}$ $\forall i = 1, ..., k$, με μήκος $k \leq poly(\frac{1}{\epsilon})$ (όπου $poly(\frac{1}{\epsilon})$ κάποιο πολυώνυμο του $\frac{1}{\epsilon}$), τέτοιο ώστε $\|\mathbb{U} - \mathbb{U}_n\| \leq \epsilon$.

Οι *Ekert* και *Jozsa* απέδειξαν μαλιστα κάτι πολύ ισχυρότερο: Ένας *unitary* μετασχηματισμος ενός n διάστατου διανυσματικού χώρου $\mathbb{H}$ μπορεί να γραφεί ως σύνθεση $2n^2 - n$ το πλήθος βασικών *unitary* μετασχηματισμών, κάθε ένας από τους οποίους δρα στον αντίστοιχο διδιάστατο διανυσματικό χώρο ο οποίος παράγεται από ένα ζεύγος καταστάσεων της υπολογιστικής βάσης του $\mathbb{H}$. Έπεται λοιπόν ότι οι παραπάνω βασικοί *unitary* μετασχηματισμοί στον χώρο καταστάσεων ενός *qubit* είναι καθολικοί, για αυτό και θα χρησιμοποιούνται ως θεμέλιοι λίθοι για τους υπολογισμούς σε κβαντικό περιβάλλον.

2.4 Μετρήσεις στον χώρο καταστάσεων.

Για να μπορέσουμε να εκμεταλλευθούμε τα αποτελέσματα των υπολογισμών που πραγματοποιούμε, θα πρέπει να παρατηρήσουμε την κατάσταση του κβαντικού υπολογιστικού συστήματος μέσα στον κατάλληλο χώρο καταστάσεων. Οι παρατηρήσεις αυτές ονομάζονται μετρήσεις και η λειτουργία τους υπόκεινται σε ένα πιθανοθεωρητικό μοντέλο, κατά τα αξιώματα της κβαντικής μηχανικής.

Σύμφωνα με αυτό, μια κβαντική μετρήση $\mathbb{M}$ είναι ένα πεπερασμένο σύνολο $\{P_i\}_{i=1}^m$ προβολών οι οποίες δρούν στον χώρο καταστάσεων του υπό μέτρηση συστήματος, δίνοντας τα αποτελέσματα $1, ..., m$ με αντίστοιχες πιθανότητες $\mathbb{P}(\mathbb{M} = i) = \langle x|P_i x\rangle$, όπου $|x\rangle$ είναι η κατάσταση του κβαντικού συστήματος την στιγμή που πραγματοποιούμε την μέτρηση. Ο χώρος καταστάσεων $\mathbb{H}$ διαμερίζεται λοιπόν σαν καρτεσιανό γινόμενο των ορθογώνιων υποχώρων που αντιστοιχούν στίς παραπάνω προβολές $\mathbb{H} = \mathbb{H}_1 \times \mathbb{H}_2 \times, ... \times \mathbb{H}_m$, η μέτρηση επιλέγει τυχαία μια από αυτές τις προβολές $\{P_i\}_{i=1}^m$, απεικονίζοντας το $|x\rangle$ στο κανονικοποιημένο διάνυσμα $\frac{P_i|x\rangle}{\|P_i|x\rangle\|} \in \mathbb{H}_i$ και δίνοντας έτσι την τιμή i σαν αποτέλεσμα.

Μια χαρακτηριστική κλάση μετρήσεων που παρουσιάζουν μεγάλο ενδιαφέρον στην κβαντική υπολογισιμότητα, είναι οι " μετρήσεις ως προς την υπολογιστική βάση ". Αυτές οι μετρήσεις είναι προβολές ενός $n - qubit$ σε κάποιο από τα διανύσματα βάσης του χώρου καταστάσεών του. Άς υποθέσουμε λοιπόν ότι θέλουμε να μετρήσουμε ένα $n - qubit$ $|x\rangle$ μέσα στον χώρο καταστάσεων $\mathbb{C}^{2^n}$, με την υπολογιστική βάση $|0\rangle, |1\rangle, ..., |2^n - 1\rangle$. Θεωρούμε τίς προβολές $\{P_i = |i\rangle\langle i|,\ i = 1, ..., 2^n - 1\}$, όπου κάθε P_i προβάλει το διάνυσμα $|x\rangle = \sum_{i=1}^{2^n-1}\langle i|x\rangle|i\rangle$ στο υπόχωρο που παράγει το αντίστοιχο διάνυσμα βάσης $|i\rangle$. Πράγματι, έχουμε $P_i|x\rangle = (|i\rangle\langle i|)|x\rangle = \langle i|x\rangle|i\rangle$ για κάθε $|x\rangle \in \mathbb{C}^{2^n}$, $i = 1, ..., n$, οπότε μια τέτοια μέτρηση θα μας δώσει τις τιμές $0, 1, ..., 2^n - 1$ με αντίστοιχες πιθανότητες $\mathbb{P}(\mathbb{M} = i) = \langle x|P_i x\rangle = |\langle i|x\rangle|^2$.

Οι προβολές της παραπάνω μορφής ικανοποιούν την εξίσωση πληρότητας

$$\Big(\sum_i |i\rangle\langle i|\Big)|x\rangle = \sum_i \langle i|x\rangle|i\rangle = |x\rangle \text{ για κάθε } x \in \mathbb{C}^{2^n} \iff \sum_i |i\rangle\langle i| = \mathbb{I},$$

από την οποία έπεται ότι συνάρτηση κατανομής της μέτρησης $\mathbb{M}$ είναι καλά ορισμένη:

$$\sum_i \mathbb{P}(\mathbb{M} = i) = \sum_m \langle x|P_m x\rangle = \langle x|\sum_m P_m x\rangle = \langle x|x\rangle = 1.$$

(Η εξίσωση πληρότητας ισχύει και στην γενική περίπτωση της μέτρησης σε οποιοδήποτε χώρο καταστάσεων).

Ας δούμε τώρα το απλούστερο παράδειγμα μιας τέτοιας μέτρησης. Ας υποθέσουμε ότι έχουμε τον χώρο καταστάσεων ενός $qubit$ και έστω ότι το κβαντικό σύστημα λίγο πριν την μέτρηση βρίσκεται στην κατάσταση $|x\rangle = \alpha|0\rangle + \beta|1\rangle$, με $\alpha, \beta \in \mathbb{C}$ και $|\alpha|^2 + |\beta|^2 = 1$. Πραγματοποιώντας την μέτρηση $\{P_0 = |0\rangle\langle 0|,\ P_1 = |1\rangle\langle 1|\}$ ως προς την υπολογιστική βάση $\{|0\rangle, |1\rangle\}$, θα πάρουμε την τιμή 0 με πιθανότητα $\langle x|0\rangle = |\alpha|^2$ και την τιμή 1 με πιθανότητα $\langle x|1\rangle = |\beta|^2$, με την κατάσταση του συστήματος αμέσως μετά την μέτρηση να είναι $\frac{\alpha}{|\alpha|}|0\rangle$ και $\frac{\beta}{|\beta|}|1\rangle$ αντίσ-

τοιχα. Αν πραγματοποιούσαμε υπολογισμούς στον χώρο καταστάσεων με εφαρμογή κάποιας πεπερασμένης ακολουθίας *unitary* τελεστών και $|x\rangle$ ήταν η τελική κατάσταση του συστήματος, τότε δεν θα γνωρίζαμε με βεβαιότητα ποιο αποτέλεσμα θα παίρναμε! Βέβαια, μια δεύτερη μέτρηση στον χώρο του *qubit* ώς προς την ίδια υπολογιστική βάση θα μας έδινε προφανώς τα αποτελέσματα 0 ή 1 αντίστοιχα, με πιθανότητα 1, όμως η κατάσταση του κβαντικού συστήματος αμέσως μετά την πρώτη μέτρηση είναι διαφορετική από την τελική κατάσταση των υπολογισμών, οπότε η δεύτερη μέτρηση δεν θα μας έδινε απολύτως καμία πληροφορία!

Ας δούμε τώρα μια μέτρηση στον $\mathbb{C}^4$, τον χώρο καταστάσεων ενός $2-qubit$. Κάθε $2-qubit$ $|x\rangle$ μπορεί να γραφεί στην μορφή $|x\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ με $|a|^2+|b|^2+|c|^2+|d|^2 = 1$. Διαισθητικά, ένα $2-qubit$ είναι η συνύπαρξη 2 $qubits$ στο τανυστικό γινόμενο των αντίστοιχων χώρων καταστάσεων. Ας υποθέσουμε λοιπόν ότι πραγματοποιούμε μέτρηση του πρώτου $qubit$ ως προς την υπολογιστική βάση $|0\rangle, |1\rangle$. Χρησιμοποιώντας τις προβολές $\{P_0 = |0\rangle\langle 0| \otimes \mathbb{I},\ P_1 = |1\rangle\langle 1| \otimes \mathbb{I}\}$ όπου $\mathbb{I}$ ο ταυτοτικός τελεστής, παίρνουμε την τιμή 0 με πιθανότητα $\mathbb{P}(\mathbb{M} = 0) = \langle x|P_0 x\rangle$. Τώρα, από την γραμμικότητα της P_0, παίρνουμε

$$P_0|x\rangle = a\Big(|0\rangle\langle 0| \otimes \mathbb{I}\Big)|00\rangle + b\Big(|0\rangle\langle 0| \otimes \mathbb{I}\Big)|01\rangle + c\Big(|0\rangle\langle 0| \otimes \mathbb{I}\Big)|10\rangle$$

$$+d\Big(|0\rangle\langle 0| \otimes \mathbb{I}\Big)|11\rangle = a|00\rangle + b|01\rangle,$$

οπότε

$$\mathbb{P}(\mathbb{M} = 0) = \langle x|P_0 x\rangle = |a|^2 + |b|^2,$$

με την κατάσταση του συστήματος αμέσως μετά την μέτρηση να είναι $|x'\rangle = \frac{P_0|x\rangle}{\|P_0|x\rangle\|} = \frac{1}{\|P_0|x\rangle\|}\Big(|0\rangle \otimes (a|0\rangle + b|1\rangle)\Big)$.

Αντίστοιχα,

$$\mathbb{P}(\mathbb{M} = 1) = \langle x|P_1 x\rangle = |c|^2 + |d|^2,$$

με την μέτρηση να προβάλει το $|x\rangle$ στο διάνυσμα $|x'\rangle = \frac{1}{\|P_1|x\rangle\|}\Big(|1\rangle \otimes (c|0\rangle + d|1\rangle)\Big)$.

2.5 Ο μετασχηματισμός *Hadamard*.

Θα εξετάσουμε τώρα έναν από τους σημαντικότερους (για την κβαντική υπολογισιμότητα) διδιάστατους *unitary* τελεστές. Θεωρούμε την απεικόνιση $\mathcal{H} : \mathbb{C}^2 \mapsto \mathbb{C}^2$, με την δράση του $\mathcal{H}$ στα στοιχεία της βάσης $\{|0\rangle, |1\rangle\}$ να ορίζεται ως

$$\mathcal{H}(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$\mathcal{H}(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

και να επεκτείνεται γραμμικά σε κάθε κατάσταση του $\mathbb{C}^2$. Ο $\mathcal{H}$ ονομάζεται μετασχηματισμός $\mathbf{Walsh - Hadamard}$ και η δράση του γενικεύεται φυσιολογικά

στον χώρο καταστάσεων ενός $n-qubit$, απεικονίζοντας το $|0...0\rangle \in (\mathbb{C}^2)^N$ σε μια ομοιόμορφη υπέρθεση των 2^n διανυσμάτων βάσης του $(\mathbb{C}^2)^N$:

$$\mathcal{H}^n(|0\rangle) = (\mathcal{H}\otimes\mathcal{H}....\otimes\mathcal{H})(|0....0\rangle) = \mathcal{H}|0\rangle\otimes\mathcal{H}|0\rangle...\mathcal{H}|0\rangle =$$

$$= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes....\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle,$$

όπου οι ακέραιοι $x = 0, ..., 2^n-1$ στο τελευταίο άθροισμα έχουν την δυαδική τους μορφή.

Ο $Hadamard$ μετασχηματισμός χρησιμοποιείται στους περισσότερους κβαντικούς αλγορίθμους, ακριβώς λόγω της ιδιότητας του να δημιουργεί την ομοιόμορφη υπέρθεση των διανυσμάτων της υπολογιστικής βάσης των $n-qubits$. Ένα χαρακτηριστικό παράδειγμα είναι η χρήση του $\mathcal{H}$ στον αλγόριθμο του $Grover$ (δες κεφ. 3).

2.6 Ο αλγόριθμος του $Deutch$.

Ας δούμε τώρα ένα πολύ απλό παράδειγμα κβαντικού αλγορίθμου, ο οποίος είναι και ο πρώτος που δώθηκε ποτέ ώστε να λειτουργεί σε κβαντικό περιβάλλον. Θεωρούμε μια συνάρτηση $f : \{0,1\}^n \longmapsto \{0,1\}$, της οποίας δεν γνωρίζουμε την μορφή. Αν υποθέσουμε ότι η f είναι σταθερή ή $balanced$ (δηλαδή ακριβώς οι μισές τιμές του πεδίου ορισμού της δίνουν $f(x) = 1$), το ζητούμενο είναι να βρούμε ποια από τις δύο ιδιότητες έχει. Ο αλγόριθμος του $Deutch$ δίνει την απάντηση υπολογίζοντας την f μονάχα μια φορά πάνω από το πεδίο ορισμού της! Ας δούμε πως γίνεται αυτό:

Ξεκινάμε προετοιμάζοντας το βοηθητικό $qubit$ $|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) = \mathcal{H}|1\rangle$. Θα κάνουμε χρήση της βοηθητικής $unitary$ απεικόνισης:

$$\mathcal{U}_f : (\mathbb{C}^2)^n\otimes\mathbb{C}^2 \mapsto (\mathbb{C}^2)^n\otimes\mathbb{C}^2$$
$$|x,0\rangle \mapsto |x, 0\oplus f(x)\rangle$$
$$|x,1\rangle \mapsto |x, 1\oplus f(x)\rangle$$

όπου $\oplus$ η $mod2$ πρόσθεση στον $\mathbb{Z}_2$. Η αρχική κατάσταση του συστήματος είναι η $|0\rangle|b\rangle$ όπου $|0\rangle = |00...0\rangle \in \mathbb{C}^{2^n}$. Έχουμε,

$|0\rangle|b\rangle \overset{\mathcal{H}\otimes\mathbb{I}}{\longmapsto} \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|b\rangle \overset{\mathcal{U}_f}{\longmapsto} \frac{(-1)^{f(x)}}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|b\rangle \overset{\mathcal{H}\otimes\mathbb{I}}{\longmapsto}$

$$\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}\frac{(-1)^{f(y)\oplus(x.y)}}{2^n}|x\rangle|b\rangle,$$

όπου $\mathcal{H}$ είναι ο τελεστής $Hadamard$, και $x.y$ είναι το εσωτερικό γινόμενο των x, y εάν τα γράψουμε στην δυαδική τους μορφή. Αν πραγματοποιήσουμε τώρα μια μέτρηση του πρώτου $n-qubit$ ως προς την υπολογιστική βάση $|0\rangle, 1\rangle, ..., |2^n-1\rangle$, θα πάρουμε την τιμή 0 ($|y\rangle = |00...0\rangle$) με πιθανότητα,

$$\mathbb{P}(\mathbb{M}=0)=\left|\sum_{y=0}^{2^n-1}\frac{(-1)^{f(y)}}{2^n}\right|^2=\begin{cases}1, & f \quad \text{σταθερή},\\ 0, & f \quad \textit{balanced}.\end{cases}$$

Οπότε, εάν η συνάρτηση είναι σταθερή θα δούμε σίγουρα το 0 σαν τιμή της μέτρησης, ενώ αν είναι *balanced* θα δούμε σίγουρα μια τιμή διαφορετική του μηδενός.

2.7 Το θεώρημα "μη αναπαραγωγής".

Στην παράγραφο αυτή αποδεικνύουμε το θεώρημα "μη αναπαραγωγής" των *Dieks* , *Wooters* και *Zurek*. Σύμφωνα με αυτό το θεώρημα, δεν μπορεί να υπάρξει κβαντικός αλγόριθμος ο οποίος να δέχεται σαν είσοδο ένα τυχαίο *qubit* $|x\rangle$ και να μας δίνει ένα ακριβές του αντίγραφο, διατηρώντας το $|x\rangle$ αναλλοίωτο. Η απόδειξη του θεωρήματος είναι μια απλή εφαρμογή της γραμμικότητας των *unitary* μετασχηματισμών.

Ας υποθέσουμε λοιπόν ότι υπάρχει ένας τέτοιος αλγόριθμος. Τότε, υπάρχει *unitary* τελεστής $\mathcal{U}$ ο οποίος να δρα ως

$$\mathcal{U}(|x0\rangle)=|xx\rangle$$

για κάθε κατάσταση $|x\rangle\in\mathbb{H}$, όπου $\mathbb{H}$ ο χώρος καταστάσεων του συστήματος. Έστω τώρα $|x_1\rangle$,$|x_2\rangle\in\mathbb{H}$ δυο τυχαίες καταστάσεις στο σύστημα. Τότε,

$$\mathcal{U}(|x_1,0\rangle)=|x_1x_1\rangle$$

και

$$\mathcal{U}(|x_2,0\rangle)=|x_2x_2\rangle.$$

Παίρνοντας εσωτερικά γινόμενα κατά μέλη, έχουμε

$$\langle x_1,0|\mathcal{U}|\mathcal{U}|x_2,0\rangle=\langle x_1x_1|x_2x_2\rangle\Longleftrightarrow\langle x_1,0|\mathcal{U}^*\mathcal{U}|x_2,0\rangle=\langle x_1|x_2\rangle\langle x_1|x_2\rangle\Longleftrightarrow$$

$$\Longleftrightarrow\langle x_10|x_20\rangle=\langle x_1|x_2\rangle^2\Longleftrightarrow\langle x_1|x_2\rangle\langle 0|0\rangle=\langle x_1|x_2\rangle^2\Longleftrightarrow\langle x_1|x_2\rangle=\langle x_1|x_2\rangle^2$$

$$\Longleftrightarrow\langle x_1|x_2\rangle=0\ \text{ή}\ 1\Longleftrightarrow|x_1\rangle=|x_2\rangle\ \text{είτε}\ |x_1\perp|x_2\rangle.$$

Κατά συνέπεια, εάν με κάποιο τρόπο μπορούσαμε να "αντιγράψουμε" μια άγνωστη κατάσταση $|x\rangle$, τότε οποιαδήποτε κατάσταση $|y\rangle$ η οποία δεν είναι κάθετη ή ταυτόσημη με το $|x\rangle$ δεν θα μπορούσε να αντιγραφεί.

2.8 *Quantum teleportation*.

Έχουμε ήδη δείξει ότι είναι αδύνατο να κατασκευάσουμε με κβαντικές μεθόδους το ακριβές αντίγραφο ενός άγνωστου σε μας *qubit*. Παρ' όλο όμως που ένα *qubit* δεν μπορεί να αντιγραφεί, αυτό που μπορούμε να πετύχουμε είναι να μεταφέρουμε, φαινομενικά (όπως θα δούμε στην συνέχεια) σε μηδενικό χρόνο, ένα *qubit* από μια δεδομένη (αρχική) θέση σε μια άλλη. Αυτό δεν σημαίνει ότι αναπαράγουμε

το αρχικό *qubit*. Κάτι τέτοιο θα ερχόταν σε πλήρη αντίθεση με όσα είπαμε μέχρι τώρα. Αντίθετα, μετά το τέλος της διαδικασίας (η οποία έχει ονομαστεί, αρκετά γλαφυρά, "χβαντική τηλεμεταφορά"), το αρχικό *qubit* καταστρέφεται και εμφανίζεται σαν ακριβές αντίγραφο στην τελική θέση. Έτσι, το αποτέλεσμα δεν έρχεται σε αντίθεση με τους θεωρητικούς περιορισμούς που έχουμε θέσει. Η χβαντική τηλεμεταφορά, τονίζει τις πρωτόγνωρες ιδιότητες τις οποίες εμφανίζουν οι μεικτές καταστάσεις σε ένα χβαντικό σύστημα. Ας την δούμε αναλυτικότερα:

Ας υποθέσουμε ότι υπάρχουν δυο παρατηρητές $\mathcal{A}, \mathcal{B}$ στις θέσεις $\mathbb{A}$ και $\mathbb{B}$ αντίστοιχα. Θέτουμε $|\psi\rangle$ το *qubit* το οποίο θα μεταφερθεί από την θέση $\mathbb{A}$ στην θέση $\mathbb{B}$. Πριν ξεκινήσει η διαδικασία μεταφοράς, οι δύο παρατηρητές προετοιμάζουν ένα κοινό $2-qubit$ και συγκεκριμένα το $|k\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Η μεικτή κατάσταση $|k\rangle$ προετοιμάζεται πολύ εύκολα, με την χρήση των *unitary* τελεστών $\mathbb{H}, \mathbb{C}_{not}, \mathbb{I}$:

$$|00\rangle \xrightarrow{\mathbb{H}\otimes\mathbb{I}} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)|0\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle + |10\rangle\big) \xrightarrow{\mathbb{C}_{not}} |k\rangle$$

Ο παρατηρητής $\mathcal{A}$ κατέχει λοιπόν το άγνωστο σε αυτόν *qubit* $|\psi\rangle$ (ας υποθέσουμε ότι $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ για κάποια $\alpha, \beta \in \mathbb{C}$) και το ένα από τα δύο *qubits* του $|k\rangle$. Το δεύτερο *qubit* είναι στην διάθεση του παρατηρητή $\mathcal{B}$. Η αρχική κατάσταση του συστήματος, είναι το $3-qubit$

$$|\psi_0\rangle = |\psi\rangle \otimes |k\rangle = \frac{1}{\sqrt{2}}\Big(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\Big),$$

όπου τα δύο πρώτα *qubits* "ανήκουν" στον παρατηρητή $\mathcal{A}$ και το τρίτο στον παρατηρητή $\mathcal{B}$. Στο πρώτο βήμα, ο $\mathcal{A}$ εφαρμόζει τον τελεστή $\mathbb{C}_{not}$ στα δικά του *qubits* και έτσι το σύστημα μεταβαίνει στην κατάσταση $|\psi_1\rangle$:

$$|\psi_1\rangle = \mathbb{C}_{not} \otimes \mathbb{I}\,(|\psi_0\rangle) = \frac{1}{\sqrt{2}}\Big(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\Big).$$

Στο δεύτερο βήμα, ο $\mathcal{A}$ εφαρμόζει τον τελεστή *Hadamard* $\mathbb{H}$ στο πρώτο *qubit* (δηλαδή τον τελεστή $\mathbb{H}\otimes\mathbb{I}\otimes\mathbb{I}$ στην $3-qubit$ κατάσταση $|\psi_1\rangle$), παίρνοντας

$$|\psi_2\rangle = \mathbb{H}\otimes\mathbb{I}\otimes\mathbb{I}\,(|\psi_1\rangle) = \frac{1}{2}\Big[\alpha\Big(|0\rangle + |1\rangle\Big)|00\rangle + \alpha\Big(|0\rangle + |1\rangle\Big)|11\rangle + \beta\Big(|0\rangle -$$
$$-|1\rangle\Big)|10\rangle + +\beta\Big(|0\rangle - |1\rangle\Big)|01\rangle\Big] = \frac{1}{2}\Big[|00\rangle\Big(\alpha|0\rangle + \beta|1\rangle\Big) + |01\rangle\Big(\alpha|1\rangle + \beta|0\rangle\Big) +$$
$$|10\rangle\Big(\alpha|0\rangle - \beta|1\rangle\Big) + + |11\rangle\Big(\alpha|1\rangle - \beta|0\rangle\Big)\Big].$$

Σε κάθε όρο του παραπάνω αθροίσματος, ο παρατηρητής $\mathcal{A}$ κατέχει τα δύο πρώτα *qubits*, ενώ ο $\mathcal{B}$ το τελευταίο (για παράδειγμα, στον όρο $|00\rangle\Big(\alpha|0\rangle + \beta|1\rangle\Big)$ το $2-qubit$ $|00\rangle$ ανήκει στον $\mathcal{A}$ και το *qubit* $\alpha|0\rangle + \beta|1\rangle$ ανήκει στον $\mathcal{B}$). Να παρατηρήσουμε εδώ ότι το αρχικό *qubit* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ το οποίο κατείχε ο $\mathcal{A}$, πέρασε στον $\mathcal{B}$, καθώς βρίσκεται στο τρίτο *qubit*, στον πρώτο όρο του παραπάνω

αθροίσματος στην τελική κατάσταση $|\psi_2\rangle$. Τώρα, ο $\mathcal{A}$ πραγματοποιεί μέτρηση των δύο πρώτων *qubits* ως προς την υπολογιστική βάση $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, παίρνοντας κάποιο από τα διανυσματα αυτής της βάσης με την ίδια πιθανότητα $\frac{1}{4}$. Ανάλογα με το αποτέλεσμα αυτής της μέτρησης, το *qubit* του $\mathcal{B}$ θα προβληθεί σε ένα από τα διανύσματα $\alpha|0\rangle + \beta|1\rangle$, $\alpha|1\rangle + \beta|0\rangle$, $\alpha|0\rangle - \beta|1\rangle$, και $\alpha|1\rangle - \beta|0\rangle$ αντίστοιχα. Ο $\mathcal{A}$ στέλνει λοιπόν το αποτέλεσμα της μέτρησης στον $\mathcal{B}$ με την μορφή των κλασσικών *bits* $00, 01, 10, 11$. Εάν ο $\mathcal{B}$ λάβει το 00, τότε γνωρίζει πως έχει στην διάθεσή του το αρχικό *qubit* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Εάν λάβει το 01, τότε έχει στην διάθεσή του το $\alpha|1\rangle + \beta|0\rangle$. Εφαρμόζωντας λοιπόν σε αυτό τον τελεστή $\mathcal{X}$ με $\mathcal{X}(|0\rangle) = |1\rangle$, $\mathcal{X}(|1\rangle) = |0\rangle$ παίρνει $\mathcal{X}\big(\alpha|1\rangle + \beta|0\rangle\big) = \alpha\mathcal{X}|1\rangle + \beta\mathcal{X}|0\rangle = \alpha|0\rangle + \beta|1\rangle = |\psi\rangle$. Ο παρακάτω πίνακας, δίνει τον κατάλληλο σε κάθε περίπτωση μετασχηματισμό:

Ψηφια	Αρχική Κατάσταση	Μετασχηματισμος	Τελική Κατάσταση
00	$\alpha\|0\rangle+\beta\|1\rangle$	$\mathbb{I}$	$\alpha\|0\rangle+\beta\|1\rangle$
01	$\alpha\|1\rangle+\beta\|0\rangle$	$\mathcal{X}$	$\alpha\|0\rangle+\beta\|1\rangle$
10	$\alpha\|0\rangle$-$\beta\|1\rangle$	$\mathcal{Z}$	$\alpha\|0\rangle+\beta\|1\rangle$
11	$\alpha\|1\rangle$-$\beta\|0\rangle$	$\mathcal{Z}\mathcal{X}$	$\alpha\|0\rangle+\beta\|1\rangle$

Ας παρατηρήσουμε εδώ ότι η παραπάνω διαδικασία δεν αντιγράφει το αρχικό *qubit* $|\psi\rangle$. Στην αρχή της διαδικασίας το $|\psi\rangle$ ήταν στην διάθεση του παρατηρητή $\mathcal{A}$, ενώ στο τέλος της βρίσκεται στην διάθεση μονάχα του παρατηρητή $\mathcal{B}$. Ουσιαστικά λοιπόν, το $|\psi\rangle$ καταστρέφεται κατά την διάρκεια της διαδικασίας που προηγήθηκε και επαναδημιουργείται στο τέλος της, στην θέση $\mathbb{B}$. Έτσι, η κβαντική τηλεμεταφορά δεν έρχεται σε αντίθεση με το θεώρημα μη αναπαραγωγής που αναφέραμε προηγουμένως.

Τέλος, κάποιος θα μπορούσε να ισχυριστεί ότι, από την στιγμή που η ανταλλαγή πληροφορίας γίνεται ουσιαστικά σε μηδενικό χρόνο, παραβιάζεται ένας από τους βασικότερους νόμους της κβαντικής φυσικής. Τίποτα δεν μπορεί να ταξιδέψει στον χωροχρόνο γρηγορότερα από την ταχύτητα του φωτός. Άν δούμε όμως τον παραπάνω αλγόριθμο λίγο πιο προσεκτικά, θα καταλάβουμε ότι δεν παραβιάζει τελικά αυτόν τον νόμο. Ο παρατηρητής $\mathcal{B}$ δεν μπορεί να δεχθεί την πληροφορία από τον παρατηρητή $\mathcal{A}$, χωρίς να χρησιμοποιήσει τα *bits* $00, 01, 10$ η 11 που ο $\mathcal{A}$ του στέλνει. Η αποστολή αυτών των *bits* όμως δεν μπορεί παρά να πραγματοποιηθεί με κλασσικές μεθόδους, οπότε η ταχύτητα διάδοσης της πληροφορίας περιορίζεται τελικά κάτω από την ταχύτητα του φωτός.

Κεφάλαιο 3

Ο αλγόριθμος αναζήτησης του *Grover*.

Ένας από τους πρώτους αλγορίθμους που κατασκευάστηκαν ώστε να κάνουν ουσιαστική χρήση του κβαντικού περιβάλλοντος είναι ο αλγόριθμος του *Grover*, ο οποίος αφορά στο πρόβλημα αναζήτησης μεταξύ N το πλήθος στοιχείων μιας βάσης δεδομένων. Ας διατυπώσουμε εδώ το πρόβλημα στην πιο απλή του μορφή:

Θεωρούμε το σύνολο

$$A = \{0, 1, ..., N-1\} \subset \mathbb{N}$$

και μια "υπολογίσιμη" απεικόνιση

$$p : A \mapsto \{0, 1\}$$

τέτοια ώστε

$$p(x) = \begin{cases} 1, & x = x_0 \\ 0, & x \neq x_0 \end{cases}$$

για κάποιο $x_0 \in A$. Το ζητούμενο είναι να βρούμε αυτό το στοιχείο μέσα στο σύνολο A.

Λειτουργώντας με κλασσικό τρόπο, θα μπορούσαμε να δοκιμάσουμε ένα προς ένα όλα τα στοιχεία του A σε τυχαία σειρά. Αυτή η απλοϊκή μέθοδος, είναι ταυτόχρονα ο καλύτερος κλασσικός αλγόριθμος αναζήτησης που μπορεί να υπάρξει για το πρόβλημα. Στην λιγότερο ευνοϊκή για μας περίπτωση, το τελευταίο στοιχείο που ελέγχουμε είναι και το ζητούμενο. Η πολυπλοκότητα λοιπόν του αλγορίθμου είναι της τάξεως $N = |A|$.

Ο αλγόριθμος αναζήτησης του *Grover*, κάνοντας χρήση του κβαντικού υπολογιστικού περιβάλλοντος, απαιτεί μονάχα $O(\sqrt{N})$ βήματα για την ολοκλήρωση του. Χωρίς βλάβη της γενικότητας, θα υποθέσουμε ότι $N = 2^n$ για κάποιο $n \in \mathbb{N}$. Έτσι, γράφοντας τα στοιχεία του A στην δυαδική τους αναπαράσταση, τα αντιστοιχίζουμε στα διανύσματα βάσης του χώρου $(\mathbb{C}^2)^n$, του χώρου καταστάσεων ενός $n-qubit$. Έτσι, γράφουμε ισοδύναμα το χώρο A στην μορφή

$$A = \{|x_1, x_2, ...x_n\rangle : x_i = 0 \text{ ή } 1 \text{ για κάθε } i = 1, ..., n\}$$

Ξεκινάμε από την κατάσταση $|0\rangle \in (\mathbb{C}^2)^n$ και εφαρμόζουμε τον μετασχηματισμό $Walsh - Hadamard$ όπως είδαμε προηγουμένως, παίρνοντας

$$\mathcal{H}(|0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

Έχουμε λοιπόν κατασκευάσει μια ομοιόμορφη (οι συντελεστές των $|x\rangle$ είναι όλοι ίσοι με $\frac{1}{\sqrt{2^n}}$) υπέρθεση των στοιχείων του συνόλου A. Σε αυτό το σημείο, μια μέτρηση στον χώρο καταστάσεων του $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$ θα είχε ακριβώς τα ίδια αποτελέσματα με την κλασσική περίπτωση. Η μέτρηση θα μας έδινε το επιθυμητό $|x_0\rangle$ με πιθανότητα $\frac{1}{2^n}$, σαν να επιλέγαμε με κλασσικό τρόπο ένα από τα 2^n το πλήθος στοιχεία του A στην τύχη. Η ιδέα εδώ είναι να καταφέρουμε να μετασχηματίσουμε την κατάσταση

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

κατάλληλα, έτσι ώστε να αυξήσουμε τον συντελεστή του $|x_0\rangle$ στο παραπάνω άθροισμα, ελλατώνοντας ταυτόχρονα τους συντελεστές των υπολοίπων καταστάσεων $|x_i\rangle, x_i \neq x_0$. Η επιθυμητή αύξηση θα μας οδηγήσει σε μια καινούρια κατάσταση της μορφής $\sum_{x=0}^{2^n-1} a_x|x\rangle$, τέτοια ώστε το $|a_{x_0}|^2$ να είναι πολύ κοντά στην μονάδα, παίρνοντας έτσι το στοιχείο $|x_0\rangle$ με μεγάλη πιθανότητα (χρησιμοποιώντας οποιαδήποτε μέτρηση ως προς την υπολογιστική βάση του $(\mathbb{C}^2)^N$). Για να απλουστεύσουμε την διαδικασία που θα ακολουθήσει, μεταβάλλουμε ελαφρά τον χώρο καταστάσεων στον οποίο δουλεύουμε προσθέτωντας σε αυτόν το $qubit$ $|0\rangle \in \mathbb{C}^2$. Έχουμε τώρα την κατάσταση

$$\sum_{x=0}^{2^n-1} |x, 0\rangle \in (\mathbb{C}^2)^n \otimes \mathbb{C}^2$$

και χρησιμοποιώντας την $unitary$ απεικόνιση

$$\mathcal{U} : (\mathbb{C}^2)^n \otimes \mathbb{C}^2 \mapsto (\mathbb{C}^2)^n \otimes \mathbb{C}^2$$

$$|x, 0\rangle \mapsto |x, 0 \otimes p(x)\rangle$$

$$|x, 1\rangle \mapsto |x, 1 \oplus p(x)\rangle$$

όπου $\oplus$ η $mod2$ πρόσθεση στον $\mathbb{Z}_2$, οδηγούμαστε στην

$$\mathcal{U}(\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, 0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \mathcal{U}(|x, 0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, p(x)\rangle$$

έχοντας έτσι ξανά μια ομοιόμορφη υπέρθεση των στοιχείων του A, αυτή την φορά όμως μαζί με την πληροφορία που δίνει η απεικόνιση p για κάθε στοιχείο του A. Είμαστε ήδη έτοιμοι για το σημαντικότερο μέρος του αλγορίθμου. Θα ακολουθήσουμε τα εξής βήματα:

(1) Αλλάζουμε το πρόσημο στον συντελεστή του $|x_0, p(x_0)\rangle$ στην υπέρθεση $\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x, p(x)\rangle$ και

(2) επιτυγχάνουμε μια αντιστροφή όλων των συντελεστών στους γραμμικούς παράγοντες της υπέρθεσης, γύρω από την μέση τιμή τους.

Ας ξεκαθαρίσουμε λίγο αυτά τα δύο βήματα. Κατ' αρχήν, θα δείξουμε πως μπορεί να επιτευχθεί η αλλαγή προσήμου στον συντελεστή του ζητούμενου *qubit* $|x_0, p(x_0)\rangle$:

Θεωρούμε το *qubit*

$$|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

και ορίζουμε την απεικόνιση

$$\mathcal{U}_p : (\mathbb{C}^2)^n \otimes \mathbb{C} \mapsto (\mathbb{C}^2)^n \otimes \mathbb{C}$$

$$|x, b\rangle \mapsto |x, b \oplus p(x)\rangle$$

όπου $\oplus$ είναι η $mod2$ πρόσθεση στον $\mathbb{Z}_2$. Τότε,

$$\mathcal{U}_p\Big((\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle) \otimes |b\rangle\Big) = \frac{1}{\sqrt{2^{n+1}}} \mathcal{U}_p\Big(\sum_{x=0}^{2^n-1} |x\rangle \otimes (|0\rangle - |1\rangle)\Big) =$$

$$= \frac{1}{\sqrt{2^{n+1}}} \mathcal{U}_p\Big(\sum_{x \neq x_0} |x, 0\rangle - \sum_{x \neq x_0} |x, 1\rangle + |x_0, 0\rangle - |x_0, 1\rangle\Big) =$$

$$= \frac{1}{\sqrt{2^{n+1}}} \Big(\mathcal{U}_p\Big(\sum_{x \neq x_0} |x, 0\rangle\Big) - \mathcal{U}_p\Big(\sum_{x \neq x_0} |x, 1\rangle\Big) + \mathcal{U}_p\Big(|x_0, 0\rangle\Big) - \mathcal{U}_p\Big(|x_0, 1\rangle\Big)\Big) =$$

$$= \frac{1}{\sqrt{2^{n+1}}} \Big(\sum_{x \neq x_0} |x, 0 \oplus 0\rangle - \sum_{x \neq x_0} |x, 1 \oplus 0\rangle + |x_0, 0 \oplus 1\rangle - |x_0, 1 \oplus 1\rangle\Big) =$$

$$= \frac{1}{\sqrt{2^{n+1}}} \Big(\sum_{x \neq x_0} |x, 0\rangle - \sum_{x \neq x_0} |x, 1\rangle + |x_0, 1\rangle - |x_0, 0\rangle\Big) =$$

$$= \frac{1}{\sqrt{2^{n+1}}} \Big(\sum_{x \neq x_0} |x, b\rangle - \big(|x_0, 0\rangle - |x_0, 1\rangle\big)\Big) = \frac{1}{\sqrt{2^{n+1}}} \Big(\sum_{x \neq x_0} |x, b\rangle - (|x_0, b\rangle)\Big) =$$

$$= \frac{1}{\sqrt{2^n}} \Big(\sum_{x=0}^{2^n-1} |x\rangle - |x_0\rangle\Big) \otimes b$$

Τελικά, αντιστρέψαμε το πρόσημο του $\frac{1}{\sqrt{2^n}}|x_0\rangle$ χωρίς να προκαλέσουμε μεταβολή στο $|b\rangle$. Ακριβώς γι' αυτό τον λόγο, το $|b\rangle \in (\mathbb{C}^2)^N$ είναι απλώς ένα βοηθητικό *qubit*, και έτσι η τελευταία διαδικασία μπορεί να λειτουργήσει πριν τον μετασχηματισμο $|x, 0\rangle \mapsto |x, p(x)\rangle$. Από εκεί και πέρα το $|b\rangle$ δεν είναι πλέον χρήσιμο.

Η διαδικασία του βήματος (1) ήταν λοιπόν μια απλή μεταβολή (στροφή) της φάσης του *qubit* $|x_0\rangle$ κατά τον παράγοντα π, αφήνοντας αναλλοίωτα όλα τα υπόλοιπα *qubits*. Ας δούμε τώρα το δεύτερο βήμα του αλγορίθμου στην γενική του μορφή:

Θεωρούμε μια οποιαδήποτε υπέρθεση καταστάσεων $\sum_{i=0}^{N-1}\alpha_i|x_i\rangle \in (\mathbb{C}^2)^N$, και συμβολίζουμε με $\overline{A}$ την μέση τιμή των συντελεστών των $|x_i\rangle$ σε αυτό το άθροισμα:

$$\overline{A} = \frac{1}{N}\sum_{i=1}^{N}\alpha_i$$

Ορίζουμε τώρα την απεικόνιση

$$T : (\mathbb{C}^2)^N \mapsto (\mathbb{C}^2)^N$$

$$T\left(\sum_{i=0}^{N-1}\alpha_i|x_i\rangle\right) = \sum_{i=0}^{N-1}(2\overline{A}-\alpha_i)|x_i\rangle$$

Ο πίνακας που αναπαριστά την T είναι ο $n \times n$ πίνακας

$$T = \begin{bmatrix} \frac{2}{N}-1 & \frac{2}{N} & \ldots.\frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \ldots.\frac{2}{N} \\ \vdots & \ddots & \vdots \\ \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{bmatrix}.$$

Πράγματι,

$$T\begin{bmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{bmatrix} = \begin{bmatrix} \frac{2}{N}-1 & \frac{2}{N} & \ldots.\frac{2}{N} \\ \frac{2}{N} & \frac{2}{N}-1 & \ldots.\frac{2}{N} \\ \vdots & \ddots & \vdots \\ \frac{2}{N} & \cdots & \frac{2}{N}-1 \end{bmatrix}\begin{bmatrix}\alpha_1\\ \alpha_2\\ \vdots\\ \alpha_n\end{bmatrix} = \begin{bmatrix} \alpha_1(\frac{2}{N}-1)+\alpha_2\frac{2}{N}+\ldots.+\alpha_n\frac{2}{N} \\ \alpha_1\frac{2}{N}+\alpha_2(\frac{2}{N}-1)+\ldots.+\alpha_n\frac{2}{N} \\ \vdots \\ \alpha_1\frac{2}{N}+\alpha_2\frac{2}{N}+\ldots.+\alpha_n(\frac{2}{N}-1) \end{bmatrix}$$

$$= \begin{bmatrix} 2\frac{\sum_{i=1}^{n}\alpha_i}{N}-\alpha_1 \\ 2\frac{\sum_{i=1}^{n}\alpha_i}{N}-\alpha_2 \\ \vdots \\ 2\frac{\sum_{i=1}^{n}\alpha_i}{N}-\alpha_n \end{bmatrix} = \begin{bmatrix} 2\overline{A}-\alpha_1 \\ 2\overline{A}-\alpha_2 \\ \vdots \\ 2\overline{A}-\alpha_n \end{bmatrix}$$

Έυκολα ελέγχουμε ότι $T = T^*$ και $T^2 = \mathbb{I}$, οπότε ο T είναι *unitary* τελεστής. Επίσης, $T = \mathcal{WRW}$, όπου $\mathcal{W}$ είναι ο πίνακας του $Walsh - Hadamard$ μετασχηματισμού και $\mathcal{R}$ είναι ο πίνακας

$$\mathcal{R} = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & -1 & 0 & \cdots & 0 \\ 0 & 0 & -1 & \cdots & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & 0 & \cdots & -1 \end{bmatrix}$$

Έτσι, ο T αναλύεται στους στοιχειώδεις μετασχηματισμούς $\mathcal{W}$,$\mathcal{R}$, οπότε είναι εύκολο να κατασκευαστεί σαν χβαντική πύλη. Για προφανείς λόγους, ο T ονομάζεται "αντιστροφή" γύρω απο την μέση τιμή των $\{\alpha_i,\}_{i=1}^n$.

Έχουμε λοιπόν στην περίπτωσή μας την υπέρθεση $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x,p(x)\rangle$ με μέση τιμή στους συντελεστές των $|x,p(x)\rangle$, $\overline{A}=\frac{1}{\sqrt{2^n}}$. Στο βήμα (1), αλλάζουμε το πρόσημο του συντελεστή του $|x_0,p(x_0)\rangle$ και έτσι ο νέος συντελεστής είναι αυτή την φορά $-\frac{1}{\sqrt{2^n}}$. Η νέα μέση τιμή, μετά το βήμα (1), είναι $\overline{A'}\simeq\frac{1}{\sqrt{2^n}}$. Κατά συνέπεια,

$$2\overline{A'}-\frac{1}{\sqrt{2^n}}\simeq\frac{1}{\sqrt{2^n}}$$

οπότε οι συντελεστές του $|x,p(x)\rangle$ που παρέμειναν αναλλοίωτοι από την αλλαγή φάσης του βήματος (1), στο βήμα (2) δεν επηρεάζονται σχεδόν καθόλου από την αντιστροφή τους γύρω από την μέση τιμή $\overline{A'}$. Ο συντελεστής όμως του $|x_0,p(x_0)\rangle$ υφίσταται σημαντική αύξηση:

$$\frac{1}{\sqrt{2^n}}|x_0,p(x_0)\rangle\overset{\text{βήμα 1}}{\longrightarrow}-\frac{1}{\sqrt{2^n}}|x,0\rangle\overset{\text{βήμα 2}}{\longrightarrow}\left(2\overline{A'}+\frac{1}{\sqrt{2^n}}\right)|x_0,p(x_0)\rangle$$

$$\simeq\frac{3}{\sqrt{2^n}}|x_0,p(x_0)\rangle.$$

Επαναλαμβάνοντας τα βήματα (1) και (2) $\frac{\pi}{4}\sqrt{2^n}$ φορές, και πραγματοποιώντας στο τέλος μέτρηση ως προς την υπολογιστική βάση του $(\mathbb{C}^2)^N$, θα πάρουμε την τιμή $|x_0,p(x_0)\rangle$ με πιθανότητα $\mathbb{P}\geq 1-\frac{1}{2^n}$. Ο αλγόριθμος *Grover* έχει λοιπόν πολυπλοκότητα της τάξης $\mathcal{O}(\sqrt{N})$.

3.1 Ο Αλγόριθμος του *Grover* είναι βέλτιστος.

Ας υποθέσουμε ότι υπάρχει ένας χβαντικός αλγόριθμος, ο οποίος μπορεί να "βρεί" ένα στοιχείο $|x\rangle$ μέσα στο σύνολο $\mathbb{A}=\{0,1,...,N-1\}\subset\mathbb{N}$. Θα αποδείξουμε ότι δεν μπορει να είναι ταχύτερος απο τον αλγόριθμο του *Grover*, δηλαδή η πολυπλοκότητά του δεν μπορεί να έχει τάξη μικρότερη απο $\mathbb{O}(\sqrt{N})$. Κατα συνέπεια, ο αλγόριθμος του *Grover* είναι βέλτιστος ανάμεσα στους αλγορίθμους αναζήτησης μιας βάσης δεδομένων με N στοιχεία.

Έστω $\mathbb{O}_x:=\mathbb{I}-2|x\rangle\langle x|$ ο τελεστής ο οποίος αλλάζει το πρόσημο στον συντελεστη του ζητούμενου στοιχείου $|x\rangle$:

$$\mathbb{O}_x(|x\rangle)=-|x\rangle$$
$$\mathbb{O}_x(|y\rangle)=|y\rangle,\quad\forall y\neq x.$$

Θεωρούμε ότι το σύστημα βρίσκεται σε μια αρχική κατάσταση $|\psi\rangle$. Η γενική μορφή του αλγορίθμου, στο κ-στο βήμα, θα είναι

$$|\psi_k^x\rangle=\mathbb{U}_k\,\mathbb{O}_x\,\mathbb{U}_{k-1}\,\mathbb{O}_x...\mathbb{U}_1\,\mathbb{O}_x\,|\psi\rangle$$

όπου $\mathbb{U}_1, ..., \mathbb{U}_k$ οι *unitary* τελεστές που χρησιμοποιεί ο αλγόριθμος. Θέτουμε επίσης

$$|\psi_k\rangle = \mathbb{U}_k\, \mathbb{U}_{k-1}, ..., \mathbb{U}_1 |\psi\rangle$$

και $|\psi_0\rangle = |\psi\rangle$.

Στο κ-στο βήμα, θα έχουμε

$$\mathbb{U}_k\, \mathbb{O}_x\, \mathbb{U}_{k-1}\, \mathbb{O}_x ... \mathbb{U}_1\, \mathbb{O}_x |\psi\rangle = \sqrt{1-\epsilon}|x\rangle + \sqrt{\epsilon}|g\rangle$$

για κάποιο $\epsilon \geq 0$, όπου $|x\rangle$ η κατάσταση που αναζητάμε, και $|g\rangle$ ένας γραμμικός συνδυασμός των υπόλοιπων καταστάσεων. Ένας επιτυχημένος αλγόριθμος θα μας δώσει λοιπόν

$$\sqrt{1-\epsilon}|x\rangle + \sqrt{\epsilon}|g\rangle \approx |x\rangle,$$

οπότε στο κ-στο βήμα το $\epsilon \geq 0$ θα είναι πολύ μικρό. ($\sqrt{1-\epsilon} \approx 1$)

Να παρατηρήσουμε εδώ ότι οι $|\psi_k^x\rangle$, $|\psi_k\rangle$, διαφέρουν κατά τον τελεστή $\mathbb{O}_x$, ο οποίος διαχωρίζει το $|x\rangle$ από τις υπόλοιπες καταστάσεις (αλλάζοντας του το πρόσημο).

Οι *unitary* τελεστές $\mathbb{U}_k$, $\mathbb{O}_x$ είναι αυτομορφισμοί του $\mathbb{C}^N$, οπότε $|\psi_k\rangle$, $|\psi_k^x\rangle \in \mathbb{C}^N$ για κάθε $k \in \mathbb{N}$. Ορίζουμε λοιπόν την ευκλείδια απόσταση μεταξύ των δύο αυτών καταστάσεων $|\psi_k\rangle$, $|\psi_k^x\rangle$ μετά από k δράσεις *unitary* τελεστών:

$$\mathbb{D}_k := \sum_x \||\psi_k^x\rangle - |\psi_k\rangle\|^2$$

Θα αποδείξουμε επαγωγικά, ότι $\mathbb{D}_k \leq 4k^2$:

Για k=1, έχουμε

$$\mathbb{D}_1 = \sum_x \||\psi_1^x\rangle - |\psi_1\rangle\|^2 = \sum_x \|\mathbb{U}_1\, \mathbb{O}_x |\psi_1\rangle - \mathbb{U}_1 |\psi_1\rangle\|^2 = \sum_x \|\mathbb{U}_1 (\mathbb{O}_x |\psi\rangle - |\psi\rangle)\|^2$$

Ο τελεστής U_1 είναι *unitary*, οπότε είναι ισομετρία στον $\mathbb{C}^N$. Έχουμε λοιπόν,

$$\mathbb{D}_1 = \sum_x \|\mathbb{U}_1 (\mathbb{O}_x |\psi\rangle - |\psi\rangle)\|^2 = \sum_x \|\mathbb{O}_x |\psi\rangle - |\psi\rangle\|^2 = \sum_x \|(\mathbb{O}_x - \mathbb{I})|\psi\rangle\|^2$$

Τώρα, $\mathbb{O}_x - \mathbb{I} = -2|x\rangle\langle x|$, οπότε

$$\sum_x \|(\mathbb{O}_x - \mathbb{I})|\psi\rangle\|^2 = \sum_x \|(-2|x\rangle\langle x|)|\psi\rangle\|^2 = 4\sum_x \|\langle x|\psi\rangle|x\rangle\|^2 = 4\sum_x |\langle x|\psi\rangle|^2 =$$

$= 4$, διότι $\sum_x |\langle x|\psi\rangle|^2 = 1$.

Έστω τώρα ότι $\mathbb{D}_k \leq 4k^2$. Τότε, μετά από $k+1$ δράσεις, θα έχουμε

$$\mathbb{D}_{k+1} = \sum_x \||\psi_{k+1}^x\rangle - |\psi_{k+1}\rangle\|^2$$

$$= \sum_x \|\mathbb{U}_{k+1}\mathbb{O}_x|\psi_k^x\rangle - \mathbb{U}_{k+1}|\psi_k\rangle\|^2 = \sum_x \|\mathbb{U}_{k+1}(\mathbb{O}_x|\psi_k^x\rangle - |\psi_k\rangle)\|^2$$

$$= \sum_x \|\mathbb{O}_x|\psi_k^x\rangle - |\psi_k\rangle\|^2 = \sum_x \|\mathbb{O}_x|\psi_k^x\rangle - \mathbb{O}_x|\psi_k\rangle + \mathbb{O}_x|\psi_k\rangle - |\psi_k\rangle\|^2 =$$

$$= \sum_x \|\mathbb{O}_x(|\psi_k^x\rangle - |\psi_k\rangle) + (\mathbb{O}_x - \mathbb{I})|\psi_k\rangle\|^2.$$

Χρησιμοποιώντας την στοιχειώδη ταυτότητα $\|x+y\|^2 \leq \|x\|^2 + 2\|x\|\|y\| + \|y\|^2$ και το γεγονός ότι ο $\mathbb{O}_x$ είναι ισομετρία στον $\mathbb{C}^N$, έχουμε

$$\mathbb{D}_{k+1} \leq \sum_x \big[\|\mathbb{O}_x(|\psi_k^x\rangle - |\psi_k\rangle)\|^2 + 2\|\mathbb{O}_x(|\psi_k^x\rangle - |\psi_k\rangle\|.\|(\mathbb{O}_x - \mathbb{I})|\psi_k\rangle\| +$$

$$\|(\mathbb{O}_x - \mathbb{I})|\psi_k\rangle\|^2\big] = \sum_x \|\psi_k^x\rangle - |\psi_k\rangle)\|^2 + 2\sum_x \|\psi_k^x\rangle - |\psi_k\rangle\|.\|(\mathbb{O}_x - \mathbb{I})|\psi_k\rangle\| +$$

$$+ \sum_x \|(\mathbb{O}_x - \mathbb{I})|\psi_k\rangle\|^2.$$

Τώρα, $\mathbb{O}_x - \mathbb{I} = -2|x\rangle\langle x|$, οπότε

$$\sum_x \||\psi_k^x\rangle - |\psi_k\rangle\|^2 = \mathbb{D}_k \tag{3.1}$$

$$2\sum_x \|\psi_k^x\rangle - |\psi_k\rangle\|.\|(\mathbb{O}_x - \mathbb{I})|\psi_k\rangle\| = 4\sum_x \|\psi_k^x\rangle - |\psi_k\rangle\|.\|\langle x|\psi_k\rangle|x\rangle\| \tag{3.2}$$

$$\sum_x \|(\mathbb{O}_x - \mathbb{I})|\psi_k\rangle\|^2 = \sum_x \|(-2|x\rangle\langle x|)|\psi_k\rangle\|^2 = \sum_x \|\langle x|\psi_k\rangle|x\rangle\|^2 =$$

$$= 4\sum_x |\langle x|\psi_k\rangle|^2 = 4\|\psi_k\|^2 = 4 \tag{3.3}$$

Από τις σχέσεις (3.1), (3.2), (3.3) η τελευταία ανισότητα γίνεται

$$\mathbb{D}_{k+1} \leq \mathbb{D}_k + 4\sum_x \||\psi_k^x\rangle - |\psi_k\rangle\|.\|\langle x|\psi_k\rangle|x\rangle\| + 4$$

Χρησιμοποιώντας την ανισότητα $Cauchy - Schwartz$, έχουμε

$$4\sum_x \||\psi_k^x\rangle - |\psi_k\rangle\|.\|\langle x|\psi_k\rangle|x\rangle\| \leq \big(\sum_x \||\psi_k^x\rangle - |\psi_k\rangle\|^2\big)^{\frac{1}{2}}.\big(\sum_x \|\langle x|\psi_k\rangle|x\rangle\|^2\big)^{\frac{1}{2}}$$

$$\Longleftrightarrow \mathbb{D}_{k+1} \leq \mathbb{D}_k + 4\sqrt{\mathbb{D}_k} + 4$$

Από την επαγωγική υπόθεση, $\mathbb{D}_k \leq 4k^2$, παίρνοντας τελικά,

$$\mathbb{D}_{k+1} \leq 4k^2 + 8k + 4 = 4(k+1)^2.$$

Έχουμε αποδείξει λοιπόν ότι $\mathbb{D}_k \leq \mathbb{O}(4k^2)$. Στο δεύτερο μέρος της απόδειξης, θα δείξουμε ότι η ποσότητα $\mathbb{D}_k$ είναι περίπου ίση προς το μέγεθος N της βάσης δεδομένων $\mathbb{A} = \{0, 1, ..., N-1\}$.

Ένας αλγόριθμος αναζήτησης θα πρέπει να προσεγγίζει την κατάσταση $|\psi_k^x\rangle$ στην $|x\rangle$ ολοένα και περισσότερο όσο αυξάνεται ο αριθμός των βημάτων. Έτσι, έπειτα από k βήματα, εάν κάνουμε μέτρηση του $|\psi_k^x\rangle$ ως προς την υπολογιστική βάση $|0\rangle, |1\rangle, ..., |N-1\rangle$ περιμένουμε να πάρουμε σαν αποτέλεσμα το $|x\rangle$ με μεγάλη πιθανότητα. Το λιγότερο που μπορούμε να ζητήσουμε είναι αυτή η πιθανότητα να είναι $\geq \frac{1}{2}$. Υποθέτουμε λοιπόν, ότι μετά από k βήματα, θα έχουμε $|\langle x|\psi_k^x\rangle|^2 \geq \frac{1}{2}$.

Ας εκτιμήσουμε τώρα την απόσταση $\||\psi_k^x\rangle - |x\rangle\|$. Έχουμε,

$$\||\psi_k^x\rangle - |x\rangle\|^2 = \langle \psi_k^x - x|\psi_k^x - x\rangle = \langle \psi_k^x|\psi_k^x - x\rangle - \langle x|\psi_k^x - x\rangle =$$

$$\langle \psi_k^x|\psi_k^x\rangle - \langle \psi_k^x|x\rangle - \langle x|\psi_k^x\rangle + \langle x|x\rangle = \langle \psi_k^x|\psi_k^x\rangle - 2Re\langle x|\psi_k^x\rangle + \langle x|x\rangle = 2 - 2Re\langle x|\psi_k^x\rangle,$$

διότι $\||x\rangle\| = \||\psi_k^x\rangle\| = 1$.

Τώρα, $\langle x|\psi_k^x\rangle = |\langle x|\psi_k^x\rangle|e^{i\theta}$ για κάποιο θ και $|\langle x|\psi_k^x\rangle| \geq \frac{1}{\sqrt{2}}$, οπότε

$$\||\psi_k^x\rangle - |x\rangle\|^2 = 2 - 2Re(|\langle x|\psi_k^x\rangle|e^{i\theta}) \leq 2 - \frac{2}{\sqrt{2}}Re(e^{i\theta}) \leq 2 + \sqrt{2}$$

διότι $Re(e^{i\theta}) = \cos\theta \leq 1$. Θέτωντας λοιπόν,

$$\mathbb{E}_k := \sum_x \||\psi_k^x\rangle - |x\rangle\|^2$$

παίρνουμε, από την τελευταία ανισότητα,

$$\mathbb{E}_k := \sum_x \||\psi_k^x\rangle - |x\rangle\|^2 \leq (2 - \sqrt{2})N. \tag{3.4}$$

Ορίζουμε τώρα,

$$\mathbb{F}_k := \sum_x \||x\rangle - |\psi_k\rangle\|^2$$

Λειτουργώντας όπως και πρίν, βλέπουμε εύκολα ότι $\||x\rangle - |\psi_k\rangle\|^2 = 2 - 2Re(\langle x|\psi_k\rangle)$ για κάθε x οπότε,

$$\mathbb{F}_k = \sum_x \||x\rangle - |\psi_k\rangle\|^2 = \sum_x \big(2 - 2Re(\langle x|\psi_k\rangle)\big) = 2N - 2\sum_x Re(\langle x|\psi_k\rangle).$$

Το άθροισμα $\sum_x Re(\langle x|\psi_k\rangle)$ μεγιστοποιείται όταν $|\psi_k\rangle = \frac{1}{\sqrt{2}}\sum_y |y\rangle$, δηλαδή όταν το $|\psi_k\rangle$ είναι μια ομοιόμορφη υπέρθεση των στοιχείων της υπολογιστικής βάσης (η μεγιστοποίηση αυτή επιτυγχάνεται χρησιμοποιώντας πολλαπλασιαστές *Langrange*). Κατά συνέπεια,

$$\mathbb{F}_k \geq 2N - 2\sum_x \sum_y \frac{1}{\sqrt{N}}\langle x|y\rangle = 2N - \frac{2}{\sqrt{N}}\sum_x \langle x|x\rangle = 2N - 2\frac{N}{\sqrt{N}} =$$

$$= 2N - 2\sqrt{N} \tag{3.5}$$

Θα εκτιμήσουμε τώρα την ποσότητα $\mathbb{D}_k$ αναζητώντας ένα κάτω φράγμα. Έχουμε,

$$\mathbb{D}_k = \sum_x \||\psi_k^x\rangle - |\psi_k\rangle\|^2 = \sum_x \|(|\psi_k^x\rangle - |x\rangle) + (|x\rangle - |\psi_k\rangle)\|^2 \geq$$

$$\geq \sum_x \left(\||\psi_k^x\rangle - |x\rangle\| - \||x\rangle - |\psi_k\rangle\|\right)^2 = \sum_x \||\psi_k^x\rangle - |x\rangle\|^2 + \sum_x \||\psi_k\rangle - |x\rangle\|^2 -$$

$$-2\sum_x \||\psi_k^x\rangle - |x\rangle\|.\||\psi_k\rangle - |x\rangle\| \geq \mathbb{E}_k + \mathbb{F}_k - 2\sqrt{\mathbb{E}_k\mathbb{F}_k} = (\sqrt{\mathbb{F}_k} - \sqrt{\mathbb{E}_k})^2,$$

με την τελευταία ανισότητα να προκύπτει άμεσα από την ανισότητα $Cauchy - Schwartz$. Αντικαθιστώντας τώρα τις εκτιμήσεις (3.4), (3.5) για τα $\mathbb{F}_k$,$\mathbb{E}_k$ στην τελευταία ανισότητα παίρνουμε,

$$\mathbb{D}_k \geq (\sqrt{\mathbb{F}_k} - \sqrt{\mathbb{E}_k})^2 \geq \left(\sqrt{2N + 2\sqrt{N}} - \sqrt{(2-\sqrt{2})N}\right)^2.$$

Για αρκετά μεγάλο N, μπορούμε να αγνοήσουμε το $\sqrt{N}$ στην πρώτη τετραγωνική ρίζα, καταλήγωντας

$$\mathbb{D}_k \geq \left(\sqrt{2} - \sqrt{2-\sqrt{2}}\right)^2 N = 0,421N$$

Δείξαμε επίσης ότι $\mathbb{D}_k \leq \mathbb{O}(4k^2)$. Συνοψίζοντας,

$$0,412N \leq \mathbb{D}_k \leq \mathbb{O}(4k^2)$$

οπότε,

$$k \geq \mathbb{O}\left(\sqrt{\frac{0,421N}{4}}\right)$$

Αποδείξαμε λοιπόν, ότι το πλήθος k των βημάτων τα οποία θα χρειαστεί οποιοσδήποτε αλγόριθμος αναζήτησης σε μια βάση δεδομένων μεγέθους N είναι της τάξεως του $\sqrt{N}$. Ο αλγόριθμος $Grover$ λοιπόν, είναι ο βέλτιστος τέτοιος αλγόριθμος.

Κεφάλαιο 4

Ο Αλγόριθμος του *P.Shor*.

4.1 Μετασχηματισμός *Fourier* σε αβελιανές ομάδες.

4.1.1 Η ομάδα Χαρακτήρων.

Έστω G μια αβελιανή ομάδα, και $(\mathcal{S}^1,.)$ η πολλαπλασιαστική ομάδα της $\mathcal{S}^1 = \{e^{2\pi ix} / \ x \in \mathbb{R},\ 0 \leq x < 1\}$, με την πράξη $e^{2\pi ix}.e^{2\pi iy} = e^{2\pi i(x+y)}$.

Η ομάδα Χαρακτήρων (ή δυϊκή ομάδα) $\widehat{G}$ της G, είναι η ομάδα όλων των συνεχών ομομορφισμών της G στην $\mathcal{S}^1$, με τον φυσιολογικό πολλαπλασιασμό $(f_1 f_2)(g) = f_1(g) f_2(g)$ για κάθε $f_1, f_2 \in \widehat{G},\ g \in G$. Τα στοιχεία της $\widehat{G}$ θα ονομάζονται Χαρακτήρες της G. Σύμφωνα με την επόμενη πρόταση, κάθε πεπερασμένη αβελιανή ομάδα είναι "ανακλαστική" ως προς τον παραπάνω ορισμό:

Πρόταση 4.1.1 *Έστω G μια πεπερασμένη αβελιανή ομάδα. Τότε, $G \simeq \widehat{G}$.*

Η απόδειξη είναι άμεση συνέπεια των ακόλουθων θεωρημάτων:

Θεώρημα 4.1.1 *Κάθε πεπερασμένη αβελιανή ομάδα G είναι ισομορφική με το ευθύ άθροισμα κυκλικών ομάδων, δηλαδή $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ... \times \mathbb{Z}_{m_n}$ όπου $\mathbb{Z}_i$ η κυκλική ομάδα τάξης $m_i \in \mathbb{N}$ για κάθε $i = 1, ..., n$.*

Θεώρημα 4.1.2 *Έστω $G_1,\ G_2$ πεπερασμένες κυκλικές ομάδες. Τότε, $\widehat{G_1 \times G_2} = \widehat{G_1} \times \widehat{G_2}$.*

Θεώρημα 4.1.3 *$\widehat{\mathbb{Z}_m} = \mathbb{Z}_m$, για κάθε $m \in \mathbb{N}$.*

Ας ορίσουμε τώρα αυστηρά τον ισομορφισμό $G \simeq \widehat{G}$. Έχουμε, $G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ... \times \mathbb{Z}_{m_n}$ και $\widehat{G} = \widehat{\mathbb{Z}_{m_1}} \times \widehat{\mathbb{Z}_{m_2}} \times ... \times \widehat{\mathbb{Z}_{m_n}}$. Ας ονομάσουμε $g_1, g_2, ..., g_n$ τους γεννήτορες των $\mathbb{Z}_{m_1}, \mathbb{Z}_{m_2}, ..., \mathbb{Z}_{m_n}$ αντίστοιχα. Ισχυριζόμαστε ότι οι χαρακτήρες

$$\widehat{\mathcal{X}}_{g_i} : \mathbb{Z}_{m_i} \mapsto \mathbb{C},$$

$$\widehat{\mathcal{X}}_{g_i}(g_i) = w_i,$$

$i = 1,..,n$ όπου w_i η πρωταρχική m_i-στη ρίζα της μονάδας, παράγουν τις αντίστοιχες δυϊκές ομάδες $\widehat{\mathbb{Z}}_i$, $i = 1,...,n$. Πράγματι, έστω $\widehat{\mathcal{X}} \in \widehat{\mathbb{Z}}_{m_i}$ για κάποιο $i = 1,...,n$. Ο $\widehat{\mathcal{X}}$ είναι ομομορφισμός, οπότε

$$\widehat{\mathcal{X}}(1) = 1 \Longleftrightarrow \widehat{\mathcal{X}}(g_i^{m_i}) = 1 \Longleftrightarrow (\widehat{\mathcal{X}}(g_i))^{m_i} = 1 \Longleftrightarrow \widehat{\mathcal{X}}(g_i) = w_i^m$$

για κάποιο $m \in \mathbb{N}$, αφού η w_i είναι πρωταρχική m_i-στη ρίζα της μονάδας. Τώρα, από τον ορισμό του $\widehat{\mathcal{X}}_{g_i}$, η τελευταία σχέση γίνεται $\widehat{\mathcal{X}}(g_i) = (\widehat{\mathcal{X}}_{g_i}(g_i))^m$, δηλαδή $\widehat{\mathcal{X}} \equiv (\widehat{\mathcal{X}}_{g_i})^m$ διότι g_i είναι γεννήτορας της $\widehat{\mathbb{Z}}_{m_i}$. Έπεται ότι ο $\widehat{\mathcal{X}}_{g_i}$ παράγει την $\widehat{\mathbb{Z}}_{m_i}$. Να παρατηρήσουμε εδώ ότι $|\mathbb{Z}_{m_i}| = |\widehat{\mathbb{Z}}_{m_i}| = m_i$, διότι

$$(\widehat{\mathcal{X}}(g_i))^{m_i} = (\widehat{\mathcal{X}_{g_i}}(g_i)^m)^{m_i} = (\widehat{\mathcal{X}_{g_i}}(g_i)^{m_i})^m = (w^{m_i})^m = 1 \Longleftrightarrow \widehat{\mathcal{X}}^m \equiv 1.$$

Έπεται λοιπόν φυσιολογικά ότι οι χαρακτήρες $\mathcal{X}_i$ της G, με $\mathcal{X}_i = (1,1,...,\widehat{\mathcal{X}}_i, 1,...,1)$, $i = 1,...,n$, είναι γεννήτορες της $\widehat{G}$ και η απεικόνιση

$$T : G \mapsto \widehat{G}$$

$$(1,1,...,g_k,...,1) \mapsto (1,1,...,\mathcal{X}_k,...,1)$$

είναι ισομορφισμός ομάδων, οπότε η $\widehat{G}$ είναι πεπερασμένη αβελιανή ομάδα και $|G| = |\widehat{G}|$.

Το επόμενο θεώρημα, υποδεικνύει ότι η G είναι αυτοπαθής, μια ιδιότητα που θα χρησιμοποιηθεί όταν ορίσουμε τον μετασχηματισμό *Fourier* στην $\mathbb{C}G$:

Θεώρημα 4.1.4 *Έστω Γ μια πεπερασμένη αβελιανή ομάδα. Τότε, $G \simeq \widehat{\widehat{G}}$ μέσω της κανονικής εμφύτευσης*

$$\Pi : G \longmapsto \widehat{\widehat{G}}$$

$$g \longmapsto g^{**},$$

όπου $g^{**}(\mathcal{X}) = \mathcal{X}(g)$ για κάθε $\mathcal{X} \in \widehat{G}$.

Μπορούμε λοιπόν να βλέπουμε τα στοιχεία της G σαν χαρακτήρες της $\widehat{G}$.

4.1.2 Η *group* άλγεβρα $\mathbb{C}G$ ως χώρος *Hilbert*.

Στα επόμενα, η G θα είναι πεπερασμένη αβελιανή ομάδα και $\widehat{G}$ η δυϊκή της. Θέτουμε,

$$\mathbb{C}G = \{f / \ f : G \longmapsto \mathbb{C}\}$$

$$\mathbb{C}\widehat{G} = \{\widehat{f} / \ \widehat{f} : \widehat{G} \longmapsto \mathbb{C}\}.$$

Η $\mathbb{C}G$ γίνεται άλγεβρα, με τις φυσιολογικές πράξεις που την ορίζουν ως διανυσματικό χώρο πάνω απο το $\mathbb{C}$:

$$(f_1+f_2)(g)=f_1(g)+f_2(g) \quad \text{για κάθε } g\in G,\ f_1,f_2\in \mathbb{C}G,$$
$$(\lambda f)(g)=\lambda f(g) \quad \text{για κάθε } \lambda\in\mathbb{C},\ f\in\mathbb{C}G,\ g\in G$$

και την συνέλιξη $*$ σαν πράξη πολλαπλασιασμού:

$$(f_1*f_2)(g)=\sum_{h\in G} f_1(h)f_2(h^{-1}g) \quad \text{για κάθε } g\in G,\ f_1,f_2\in\mathbb{C}G.$$

Αντίστοιχες είναι οι πράξεις στο $\mathbb{C}\widehat{G}$. Ορίζουμε τώρα εσωτερικό γινόμενο στις $\mathbb{C}G$, $\mathbb{C}\widehat{G}$. Για κάθε $f_1,f_2\in\mathbb{C}G$, $\widehat{f}_1,\widehat{f}_2\in\mathbb{C}\widehat{G}$,

$$\langle f_1,f_2\rangle := \frac{1}{|G|}\sum_{g\in G} f_1(g)\overline{f_2(g)}$$
$$\langle \widehat{f}_1,\widehat{f}_2\rangle := \frac{1}{|G|}\sum_{\mathcal{X}\in\widehat{G}} \widehat{f}_1(\mathcal{X})\overline{\widehat{f}_2(\mathcal{X})}.$$

Εύκολα αποδεικνύεται ότι οι $\mathbb{C}G$, $\mathbb{C}\widehat{G}$ είναι πλήρεις ως προς την νόρμα που επάγεται απο το εσωτερικό τους γινόμενο.

Να παρατηρήσουμε εδώ ότι κάθε $g\in\mathbb{G}$ μπορεί να θεωρηθεί ώς στοιχείο του $\mathbb{C}G$, διότι σε αυτό αντιστοιχεί η απεικόνιση

$$T_g : G \longmapsto \mathbb{C}$$

$T_g(g_0)=1$ αν $g=g_0$, και $T_g(g_0)=0$ αν $g\neq g_0$. Πράγματι $G\cong(\{T_g : g\in G\},*)$ ως ομάδες μέσω του ισομορφισμού $g\longleftrightarrow T_g$: Έστω $g_1,g_2\in G$. Τότε

$$(T_{g_1}*T_{g_2})(g_0)=\sum_{h\in G} T_{g_1}(h)T_{g_2}(h^{-1}g_0)=T_{g_2}(g_1^{-1}g_0)=T_{g_1g_2}(g_0)$$

για κάθε $g_0\in G$, οπότε η $g\longleftrightarrow T_g$ είναι ομομορφισμός ομάδων. Προφανώς, η απεικόνιση είναι $1-1$ και επι.

Ακόμα περισσότερο, η $\{\sqrt{|G|}g : g\in G\}$ είναι ορθοκανονική βάση για τον $\mathbb{C}G$: Η ορθοκανονικότητα είναι προφανής. Τώρα για κάθε $f\in\mathbb{C}G$ έχουμε ότι $f=\sum_{g\in G} f(g)g$, και $\langle f,g_0\rangle=\frac{1}{|G|}\sum_{g\in G} f(g)\overline{g_0(g)}=\frac{1}{|G|}f(g_0)$ για κάθε $g_0\in G$. Έπεται ότι $f=|G|\sum_{g\in G}\langle f,g\rangle g$.

Εντελώς ανάλογα, μέσω των αντίστοιχων απεικονίσεων $T_{\mathcal{X}}:\widehat{G}\longmapsto\mathbb{C}$ με $T_{\mathcal{X}}(\mathcal{X}_0)=1$ αν $\mathcal{X}=\mathcal{X}_0$ και $T_{\mathcal{X}}(\mathcal{X}_0)=0$ αν $\mathcal{X}\neq\mathcal{X}_0$, αποδεικνύουμε ότι η $\{\sqrt{|G|}\mathcal{X} : \mathcal{X}\in\widehat{G}\}$ είναι ορθοκανονική βάση για τον χώρο *Hilbert* $\mathbb{C}\widehat{G}$. Είμαστε πλέον έτοιμοι να ορίσουμε τον Μετασχηματισμό *Fourier* για την G:

Ορισμός 4.1.1 *Ο Μετασχηματισμός Fourier $\mathcal{F}$ για την G ορίζεται να είναι η απεικόνιση $\mathcal{F}:\mathbb{C}G\longmapsto\mathbb{C}\widehat{G}$, με τύπο*

$$\mathcal{F}(f)=\frac{1}{\sqrt{|G|}}\sum_{g\in G} f(g)\overline{g^{**}}=\frac{1}{\sqrt{|G|}}\sum_{\mathcal{X}\in\widehat{G}}\Big(\sum_{g\in G} f(g)\overline{\mathcal{X}}(g)\Big)\mathcal{X}=\sqrt{|G|}\sum_{\mathcal{X}\in\widehat{G}}\langle f,\mathcal{X}\rangle\mathcal{X}$$

για κάθε $f \in \mathbb{C}G$.

Για συντομία, θα συμβολίζουμε $\mathcal{F}(f) = \widehat{f}$. Έτσι, για κάθε $\mathcal{X}_0 \in \widehat{G}$,

$$\widehat{f}(\mathcal{X}_0) = \sqrt{|G|} \sum_{\mathcal{X} \in \widehat{G}} \langle f, \mathcal{X} \rangle \mathcal{X}(\mathcal{X}_0) = \sqrt{|G|} \langle f, \mathcal{X}_0 \rangle = \frac{1}{\sqrt{|G|}} \sum_{g \in G} f(g) \overline{\mathcal{X}_0(g)}.$$

Η γραμμικότητα της $\mathcal{F}$ είναι προφανής. Η επόμενη πρόταση, μας δίνει έναν τύπο αντιστροφής για την f, υποδεικνύοντας ότι η $\mathcal{F}$ είναι επί του $\mathbb{C}\widehat{G}$:

Πρόταση 4.1.2 *Αν* $f \in \mathbb{C}G$, *τότε*

$$f = \frac{1}{\sqrt{|G|}} \sum_{\mathcal{X} \in \widehat{G}} \widehat{f}(\mathcal{X}) \mathcal{X}.$$

Απόδειξη

Για κάθε $g_0 \in G$, έχουμε

$$\begin{aligned}
\Big(\frac{1}{\sqrt{|G|}} \sum_{\mathcal{X} \in \widehat{G}} \widehat{f}(\mathcal{X}) \mathcal{X}\Big)(g_0) &= \frac{1}{\sqrt{|G|}} \sum_{\mathcal{X} \in \widehat{G}} \Big(\frac{1}{\sqrt{|G|}} \sum_{g \in G} f(g) \overline{\mathcal{X}(g)}\Big) \mathcal{X}(g_0) = \\
&= \frac{1}{|G|} \sum_{\mathcal{X} \in \widehat{G}} \Big(\sum_{g \in G} f(g) \overline{\mathcal{X}(g)}\Big) \mathcal{X}(g_0) = \frac{1}{|G|} \sum_{g \in G} f(g) \sum_{\mathcal{X} \in \widehat{\mathbb{G}}} \overline{\mathcal{X}(g)} \mathcal{X}(g_0) = \\
&= \sum_{g \in G} f(g) \langle g, g_0 \rangle = f(g_0),
\end{aligned}$$

όπου στις τελευταίες ισότητες βλέπουμε τα στοιχεία της G σαν χαρακτήρες της $\widehat{G}$. Η αλλαγή σειράς άθροισης ισχύει, διότι τα αθροίσματα είναι πεπερασμένα. □

Ο τύπος του **Plancherel**, αποδεικνύει ότι ο $\mathcal{F}$ είναι γραμμική ισομετρία:

Θεώρημα 4.1.5 $\|f\| = \|\widehat{f}\|$ *για κάθε* $f \in \mathbb{C}G$.

Απόδειξη

Έχουμε, χρησιμοποιώντας την προηγούμενη πρόταση,

$$\begin{aligned}
\|f\|^2 = \langle f, f \rangle = \frac{1}{|G|} \sum_{g \in G} f(g) \overline{f(g)} = \\
= \frac{1}{|G|} \sum_{g \in G} \frac{1}{\sqrt{|G|}} \Big(\sum_{\mathcal{X} \in \widehat{G}} \widehat{f}(\mathcal{X}) \mathcal{X}(g)\Big) \overline{\Big(\frac{1}{\sqrt{|G|}} \sum_{\mathcal{X}_0 \in \widehat{G}} \widehat{f}(\mathcal{X}_0) \mathcal{X}_0(g)\Big)} = \\
= \frac{1}{|G|^2} \sum_{g \in G} \sum_{\mathcal{X} \in \widehat{G}} \sum_{\mathcal{X}_0 \in \widehat{G}} \widehat{f}(\mathcal{X}) \overline{\widehat{f}(\mathcal{X}_0)} \mathcal{X}(g) \overline{\mathcal{X}_0(g)} =
\end{aligned}$$

$$= \frac{1}{|G|^2} \sum_{\mathcal{X}\in\widehat{G}} \sum_{\mathcal{X}_0\in\widehat{G}} \widehat{f}(\mathcal{X})\overline{\widehat{f}(\mathcal{X}_0)}\Big(\sum_{g\in G} \mathcal{X}(g)\overline{\mathcal{X}_0(g)}\Big) =$$

$$= \frac{1}{|G|} \sum_{\mathcal{X}\in\widehat{G}} \sum_{\mathcal{X}_0\in\widehat{G}} \widehat{f}(\mathcal{X})\overline{\widehat{f}(\mathcal{X}_0)}\langle\mathcal{X},\mathcal{X}_0\rangle$$

$$= \frac{1}{|G|} \sum_{\mathcal{X}\in\widehat{G}} |\widehat{f}(\mathcal{X})|^2 = \langle\widehat{f},\widehat{f}\rangle = \|\widehat{f}\|^2.$$

□

Οι $\mathbb{C}G$, $\mathbb{C}\widehat{G}$ είναι λοιπόν ισομετρικά ισόμορφοι μέσω του μετασχηματισμού *Fourier*. Εντελώς ανάλογα, ορίζουμε τον αντίστροφο μετασχηματισμό *Fourier* $\mathcal{F}^{-1} : \mathbb{C}\widehat{G} \longmapsto \mathbb{C}G$, με τύπο

$$\mathcal{F}^{-1}(\widehat{f}) = \frac{1}{\sqrt{|G|}} \sum_{\mathcal{X}\in\widehat{G}} \widehat{f}(\mathcal{X})\mathcal{X},$$

για κάθε $\widehat{f} \in \widehat{G}$.

4.2 Διακριτός Μετασχηματισμός *Fourier* στο $\mathbb{Z}_n$.

Ο αλγόριθμος παραγοντοποίησης του *Shor*, χρησιμοποιεί τον μετασχηματισμό *Fourier* στην προσθετική ομάδα $\mathbb{Z}_n$. Ας δούμε λοιπόν λίγο πιο αναλυτικά όσα είπαμε παραπάνω, στην περίπτωση όπου $G = \mathbb{Z}_n$.

Θεωρούμε την προσθετική ομάδα των ακεραίων $modn$ ($\mathbb{Z}_n$) και ορίζουμε τον χώρο όλων των συναρτήσεων που απεικονίζουν τον $\mathbb{Z}^n$ στο $\mathbb{C}$:

$$\mathbb{C}(\mathbb{Z}_n) = \{f/f : \mathbb{Z}_n \mapsto \mathbb{C}\}.$$

Ο $\mathbb{C}(\mathbb{Z}_n)$ είναι διανυσματικός χώρος πάνω απο το $\mathbb{C}$ και κάθε συνάρτηση $f \in \mathbb{C}(\mathbb{Z}_n)$ αναπαρίσταται με φυσιολογικό τρόπο, μεσω της απεικόνισης

$$T : \mathbb{C}(\mathbb{Z}_n) \mapsto \mathbb{C}^n$$

$$T(f) = (f(0), f(1), ...f(n-1))$$

ως στοιχείο του $\mathbb{C}^n$. Ειδικότερα, $\mathbb{C}(\mathbb{Z}_n) \approx \mathbb{C}^n$ ως διανυσματικοί χώροι.

Μπορούμε να επεκτείνουμε τις συναρτήσεις $f \in \mathbb{C}(\mathbb{Z}_n)$ με περιοδικό τρόπο σε όλο το $\mathbb{Z}$, θέτωντας $\overline{f}(z) = f(zmodn)$, $z \in \mathbb{Z}$.

Εφοδιάζουμε τώρα τον $\mathbb{C}(\mathbb{Z}_n)$ με το εσωτερικό γινόμενο

$$\langle .,. \rangle : \mathbb{C}(\mathbb{Z}_n) \times \mathbb{C}(\mathbb{Z}_n) \mapsto \mathbb{C}$$

$$\langle f, g \rangle = \sum_{x=0}^{n-1} f(x)\overline{g}(x)$$

για κάθε $f,\ g \in \mathbb{C}(\mathbb{Z}_n)$, όπου $\overline{f}(x)$ ο μιγαδικος συζυγής του $f(x)$.

Εύκολα ελέγχουμε ότι ο $\mathbb{C}(\mathbb{Z}_n)$ είναι χώρος $Hilbert$ ως προς την επαγόμενη νόρμα. Το σύνολο $\{e_0, e_1, ..., e_{n-1}\}$, όπου

$$e_j(m) = \begin{cases} 1 & m = j \\ 0 & m \neq j \end{cases}, \qquad m \in \mathbb{Z}_n,$$

είναι μια ορθοκανονική βάση του $\mathbb{C}(\mathbb{Z}_n)$. Έτσι λοιπόν, κάθε $f \in \mathbb{C}(\mathbb{Z}_n)$ γράφεται μοναδικά ως προς τα στοιχεία αυτής της βάσης ως $f = \sum_{k=0}^{n-1} f(k)e_k$.

Είμαστε πλέον έτοιμοι να ορίσουμε (σε αντιστοιχία με την γενική περίπτωση) την έννοια του διακριτού μετασχηματισμού $Fourier$ (DFT) στον $\mathbb{Z}_n$. Θεωρούμε κατ' αρχήν το σύνολο

$$E = \{E_0, E_1, ..., E_{n-1}\} \subseteq \mathbb{C}(\mathbb{Z}_n)$$

όπου

$$E_0(k) = \frac{1}{\sqrt{n}}$$

$$E_1(k) = \frac{1}{\sqrt{n}} e^{\frac{2\pi\imath k}{n}}$$

$$\vdots$$

$$E_m(k) = \frac{1}{\sqrt{n}} e^{\frac{2\pi\imath m k}{n}}$$

$$\vdots$$

$$E_{n-1}(k) = \frac{1}{\sqrt{n}} e^{\frac{2\pi\imath (n-1) k}{n}}$$

για k,$m \in 0, 1, ...n-1$.

Πρόταση 4.2.1 *Το σύνολο E αποτελεί ορθοκανονική βάση του $\mathbb{C}(\mathbb{Z}_n)$.*

Απόδειξη

Έστω $l, m \in \mathbb{Z}_n$. Τότε,

$$\langle E_l, E_m \rangle = \sum_{k=0}^{n-1} E_l(k)\overline{E_m}(k) = \sum_{k=0}^{n-1} \frac{1}{\sqrt{n}} e^{\frac{2\pi\imath l k}{n}} \overline{\frac{1}{\sqrt{n}} e^{\frac{2\pi\imath m k}{n}}}$$

$$= \frac{1}{n} \sum_{k=0}^{n-1} (e^{\frac{2\pi\imath (l-m)}{n}})^k$$

Διακρίνουμε δύο περιπτωσεις:

(i) $l = m$: Τότε, $e^{\frac{2\pi\imath (l-m)}{n}} = 1$, οπότε $\langle E_l, E_m \rangle = 1$

(ii) $l \neq m$: Τότε στο δεύτερο μέλος της ισότητας εμφανίζεται η γεωμετρική σειρά $\sum_{k=0}^{n-1} z^k$. Έχουμε λοιπόν,

$$\langle E_l, E_m\rangle = \frac{1}{n}\frac{1-(e^{\frac{2\pi\imath(l-m)}{n}})^n}{1-e^{\frac{2\pi\imath(l-m)}{n}}} = 0$$

διότι $e^{2\pi\imath(l-m)} = 1$.
Τελικά, $\langle E_l, E_m\rangle = \begin{cases} 1 & l = m \\ 0 & l \neq m \end{cases}$ □

Ορισμός 4.2.1 *Θεωρούμε την απεικόνιση*

$$L : \mathbb{C}(\mathbb{Z}_n) \mapsto \mathbb{C}(\mathbb{Z}_n)$$

$$f \mapsto \widehat{f}$$

με $\widehat{f}(m) = \sum_{k=0}^{n-1} f(k)e^{-\frac{2\pi\imath km}{n}} = \sqrt{n}\langle f, E_m\rangle$ *για κάθε* $m \in \mathbb{Z}_n$.
Ο τελεστής L *θα λέγεται* ***Διακριτός Μετασχηματισμός*** *Fourier* (DFT) *στον* $\mathbb{Z}_n$.

Παρατηρήσεις:

(1) ο DFT είναι 1-1, επί, γραμμικός τελεστής.
(2) (**Αντίστροφος μετασχηματισμός**) Για κάθε $z \in \mathbb{Z}, f \in \mathbb{C}(\mathbb{Z}_n)$,

$$f(z) = \sum_{k=0}^{n-1} \widehat{f}(k)e^{-}\frac{2\pi\imath kz}{n}.$$

(3) (**Τύπος του** *Plancherel*)

$$\|f\|^2 = \frac{1}{n}\sum_{k=0}^{n-1} |\widehat{f}(k)|^2 = \frac{1}{n}\|\widehat{f}\|^2$$

Οι αποδείξεις έχουν δωθεί στην γενική περίπτωση. Ας δούμε τον DFT σε μορφή πίνακα:
Έστω μια $f \in \mathbb{C}(\mathbb{Z}_n)$. Τότε

$$\widehat{f}(x) = \sum_{y=0}^{n-1} f(y)e^{-}\frac{2\pi\imath xy}{n} = \sum_{y=0}^{n-1} f(y)(e^{-}\frac{2\pi\imath}{n})^x y.$$

Γράφουμε τώρα

$$f = (f(0), f(1), ..., f(n-1))^T$$

$$\widehat{f} = (\widehat{f}(0), \widehat{f}(1), ..., \widehat{f}(n-1))^T$$

$$w_n = exp(\frac{2\pi i}{n})$$

και

$$F_n = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w & w^2 & \cdots & w^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{n-2} & w^{2(n-2)} & \dots & w^{(n-2)(n-1)} \\ 1 & w^{n-1} & w^{2(n-1)} & \dots & w^{(n-1)(n-1)} \end{bmatrix} = \left(w^{ij}\right)_{0\leq i,j\leq n-1}$$

Τότε, σύμφωνα με τα παραπάνω, έχουμε ότι $\widehat{f} = F_n f$, δηλαδή ο F_n είναι ο πίνακας που αντιστοιχεί στον DFT. Δίνουμε τώρα έναν ακόμα ορισμό:

Ορισμός 4.2.2 *Εστω $f = (f(0), f(1), ..., f(n-1)) \in \mathbb{C}(\mathbb{Z}_n)$. Ορίζουμε την απεικόνιση $\overline{f} : \mathbb{Z}_n \mapsto \mathbb{C}$ με τύπο,*

$$\overline{f}(m) = \frac{1}{n}\sum_{k=0}^{n-1} f(k) e^{\frac{2\pi i k m}{n}}.$$

*Η $\overline{f}$ θα λέγεται **Αντίστροφος Διακριτός Μετασχηματισμός** $Fourier$ $(IDFT)$ της f.*

Έχουμε, σε αντιστοιχία με όσα είπαμε πριν,

$$\overline{f}(x) = \frac{1}{n}\sum_{k=0}^{n-1} f(y) e^{\frac{2\pi i x y}{n}} = \frac{1}{n}\sum_{k=0}^{n-1} f(y)\overline{w_n^{xy}},$$

όπου $w_n = exp(\frac{2\pi i}{n})$. Έπεται ότι $F_n^{-1} = \overline{F_n}$. Από την τελευταία ανισότητα έπεται ότι ο DFT είναι $unitary$ τελεστής.

4.3 *Quantum Fourier Transform (Q.F.T.).*

Ο χβαντικός μετασχηματισμος $Fourier$ $(Q.F.T.)$ είναι μια εναλλακτική μορφή του $D.F.T.$, που αντιστοιχεί στο χώρο καταστάσεων ενός χβαντικού συστήματος.

Ας θεωρήσουμε ένα χβαντικό σύστημα αποτελούμενο απο $n - qubits$. Τότε, η ορθοκανονική βάση του χώρου $Hilbert$ που περιγράφει το χβαντικό σύστημα είναι η

$$\{|\alpha_{n-1}\alpha_{n-2}...\alpha_0\rangle : \alpha_i = 0 \text{ ή } 1, \text{ για κάθε } i = 0, 1, .., n-1\}.$$

Μας ενδιαφέρουν οι ομάδες $\mathbb{Z}_k$, όπου $k = 2^n$ για κάποιο $n \in \mathbb{N}$. Για κάθε $x \in \mathbb{Z}_{2^n}$, θα συμβολίζουμε με $|x\rangle$ το διάνυσμα βάσης που αντιστοιχεί στην δυαδική αναπαράσταση του x:

$$|x\rangle = |x_{n-1}x_{n-2}...x_0\rangle, \; x = \sum_{i=0}^{n-1} x_i 2^i.$$

Ο $Q.F.T.$ δρα στα διανύσματα βάσης του χώρου καταστάσεων ως εξής:

Για κάθε $0 \leq \alpha < q$,

$$Q.F.T. : |\alpha\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} exp(\frac{2\pi i a c}{q})|c\rangle$$

όπου $q = dimH$, H ο χώρος $Hilbert$ που αντιστοιχεί στον χώρο καταστάσεων και $|0\rangle, ..., |q-1\rangle$ τα διανύσματα βάσης του H (από εδώ και πέρα, $q = 2^n$ για κάποιο $n \in \mathbb{N}$).

Ο $Q.F.T.$ επεκτείνεται φυσιολογικά σε όλο τον H μέσω γραμμικότητας. Έτσι, αν $\sum_\alpha f(\alpha)|\alpha\rangle$, $\sum_c \widehat{f}(c)|c\rangle \in H$ και $Q.F.T. : \sum_\alpha f(\alpha)|\alpha\rangle \mapsto \sum_c \widehat{f}(c)|c\rangle$, τότε οι συντελεστές $\widehat{f}(c)$ είναι οι τιμές που δίνει ο $D.F.T.$ της f στα στοιχεία του $\mathbb{Z}_{2^n}$:

$$\widehat{f}(c) = \frac{1}{\sqrt{q}} \sum_\alpha exp(\frac{2\pi i \alpha c}{q}) f(\alpha)$$

όπου $c \in \mathbb{Z}_{2^n}$, $c = \sum_{i=0}^{n-1} c_i 2^i$, δηλαδή $|c\rangle = |c_{n-1} c_{n-2} ... c_0\rangle$.

Ο μετασχηματισμός $Q.F.T.$ περιγράφεται λοιπόν από έναν $2^n \times 2^n$ πίνακα, τα στοιχεία του οποίου (στην θέση (α, c)) είναι τα $\frac{1}{\sqrt{q}} exp(\frac{2\pi i \alpha c}{q})$.

Για την κατασκευή του κβαντικού αλγορίθμου για τον $Q.F.T.$, θα χρειαστούμε δύο πολύ βασικούς $unitary$ τελεστές:

(1) Τον τελεστή $Hadamard$ Aj, ο οποίος δρα μεμονωμένα σε κάθε $qubit$ του διανύσματος βάσης $|\alpha\rangle = |\alpha_{n-1} \alpha_{n-2} ... \alpha_0\rangle$,

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

$j = 0, 1, ..., n-1$, όπου ο πίνακας αντιστοιχεί στα διανύσματα βάσης $|0\rangle, |1\rangle$ του $\mathbb{C}^2$.

(2) Τον τελεστή $B_{j,k}$, $0 \leq j, k \leq n-1$, ο οποίος θα δρα ταυτόχρονα στα $qubits$ του $|\alpha\rangle$ που βρίσκονται στις θέσεις j και k:

$$B_{j,k} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta_{j,k}} \end{bmatrix}$$

όπου $\theta_{j,k} = \frac{\pi}{2^{k-j}}$.

Αντίστοιχα, ο πίνακας $B_{j,k}$ αναφέρεται στην βάση $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ του $\mathbb{C}^2 \otimes \mathbb{C}^2$, δηλαδή στον επι μέρους χώρο καταστάσεων που αντιστοιχεί στα $qubits$ α_j και α_k. (Να παρατηρήσουμε εδώ ότι στα $qubits$ που θέλουμε να μένουν κάθε φορά αναλλοίωτα απο την δράση των $A_j, B_{j,k}$, θα εφαρμόσουμε τον ταυτοτικό τελεστή $\mathbb{I}$.)

Έστω λοιπόν οτι $\alpha = \sum_{i=0}^{n-1} \alpha_i 2^i$, δηλαδή $|\alpha\rangle = |\alpha_{n-1}, \alpha_{n-2}, ..., \alpha_0\rangle$. Για να επιτευχθεί ο κβαντικος μετασχηματισμός $Fourier$, αρκεί να εφαρμόσουμε στο $n-qubit$ $|\alpha\rangle$ την ακολουθία τελεστών

$$A_{n-1} B_{n-2,n-1} A_{n-2} B_{n-3,n-1} B_{n-3,n-2} A_{n-3} ..... A_1 B_{0,n-1} B_{0,n-2} .... B_{0,2} B_{0,1} A_0.$$

Εφαρμόζουμε λοιπόν τους τελεστές $\{A_i\}_{i=1}^{n-1}$ με αντίστροφη σειρά (από τον A_{n-1} στον A_1και μεταξύ των A_{j+1} και A_j, εφαρμόζουμε τους τελεστές $\{B_k\}_{j<k}$). Ισχυριζόμαστε ότι η δράση αυτών των τελεστών, απεικονίζει το $|\alpha\rangle$ στο $n-qubit$ $\frac{1}{\sqrt{q}}\sum_b exp(\frac{2\pi i\alpha c}{q})|b\rangle$, όπου $|b\rangle$ είναι το $n-qubit$ που προκύπτει αν διαβάσουμε τα $bits$ του $|c\rangle = |c_{n-1}, c_{n-2}, ..., c_0\rangle$ από δεξιά προς τα αριστερά. Αντιστρέφοντας λοιπόν την σειρά των $bits$ στο $|c\rangle$ (ένας υπολογισμός μηδενικής πολυπλοκότητας) παίρνουμε ακριβώς τον $Q.F.T.$ του $|\alpha\rangle$. Ας αποδείξουμε τώρα αυτόν τον ισχυρισμό:

Ας υποθέσουμε ότι, μετά την δράση αυτών των τελεστών, μεταβαίνουμε από την κατάσταση $|\alpha\rangle = |\alpha_{n-1}, \alpha_{n-2}, ..., \alpha_0\rangle$ στην κατάσταση $|b\rangle = |b_{n-1}, b_{n-2}, ..., b_0\rangle$ $(= |c_0, c_1, ..., c_{n-1}\rangle)$. Οι τελεστές A_j είναι n το πλήθος, οπότε το $|b\rangle$ θα έχει στον συντελεστή του τον παράγοντα $(\frac{1}{\sqrt{2}})^n = \frac{1}{\sqrt{2^n}} = \frac{1}{q}$, (έχουμε υποθέσει ότι $q = 2^n$). Αν παρατηρήσουμε τώρα τον τελεστή $B_{j,k}$ θα δούμε ότι δεν αλλάζει τις τιμές των $bits$ στο $n-qubit$ στο οποίο δρα, αλλά μονάχα την φάση τους. Οπότε, για να αλλάξουμε το bit α_j στο b_j, θα πρέπει να δράσουμε στο $|\alpha\rangle$ τον τελεστή A_j. Η δράση αυτή θα προσθέσει τον παράγοντα π στην φάση του b_j, εάν τα $\alpha_j = b_j = 1$ (διότι $-1 = e^{\pi i}$) και θα την αφήσει αναλλοίωτη σε κάθε άλλη περίπτωση. Αντίστοιχα, η δράση του $B_{j,k}$ στα $qubits$ που βρίσκονται στις θέσεις j, k θα προσθέσει τον παράγοντα $\frac{\pi}{2^{k-j}}$, στην φάση του $2-qubit$ b_jb_k (και κατ'επέκταση στην φάση του εξαγόμενου $n-qubit$ $|b\rangle$) αν και μόνο αν $a_j = b_k = 1$. Έτσι λοιπόν, η αλλαγή φάσης που πραγματοποιείται κατά την μετάβαση από το $|\alpha\rangle$ στο $|b\rangle$ θα είναι ίση με

$$\sum_{0\le j<n} \pi\alpha_j b_j + \sum_{0\le j<k<n} \frac{\pi}{2^{k-j}}\alpha_j b_k = \sum_{0\le j\le k<n} \frac{\pi}{2^{k-j}}\alpha_j b_k =$$

$$= \sum_{0\le j\le k<n} \frac{\pi}{2^{k-j}}\alpha_j c_{n-1-k}$$

διότι όπως είδαμε, $b_k = c_{n-1-k}$ για κάθε $k = 0, 1, ..., n-1$. Κάνοντας τώρα την αλλαγή μεταβλητής $n-k-1 = u$, το τελευταίο άθροισμα γίνεται

$$\sum_{0\le j+u<n} 2\pi\frac{2^j 2^u}{2^n}\alpha_j c_u$$

Τώρα, τα πολλαπλάσια του 2π δεν επηρεάζουν την φάση του $|\alpha\rangle$, μπορούμε λοιπόν να αθροίσουμε μονάχα πάνω από τα j, u που είναι μικρότερα του n, οπότε το παραπάνω άθροισμα είναι ίσο με το

$$\sum_{j,u=0}^{n-1} 2\pi\frac{2^j 2^u}{2^n}\alpha_j c_u = \frac{2\pi}{2^n}\sum_{j=0}^{n-1} 2^j\alpha_j \sum_{u=0}^{n-1} 2^u c_u = \frac{2\pi\alpha c}{q},$$

διότι $q = 2^n$, $\alpha = \sum_{j=0}^{n-1} 2^j\alpha_j$, $c = \sum_{u=0}^{n-1} 2^u c_u$.

Όμως το $\frac{2\pi\alpha c}{q}$ είναι ακριβώς η αλλαγή φάσης που πραγματοποιείται αν το $|\alpha\rangle$ απεικονιστεί στο $|b\rangle$ μέσω του κβαντικού μετασχηματισμού $Fourier$, αποδεικνύοντας έτσι τον ισχυρισμό μας.

4.4 Ο αλγόριθμος του *P.Shor*.

Θεωρούμε την πολλαπλασιαστική ομάδα των ακεραίων $modN$ $(\mathbb{Z}_N, .)$ και ένα στοιχείο $x \in \mathbb{Z}_N$ σχετικά πρώτο προς το N $\big(gcd(x,N)=1\big)$. Θεωρούμε επίσης την απεικόνιση

$$f_x : \mathbb{N} \mapsto \mathbb{Z}_N$$

$$f_x(\alpha) = x^\alpha mod N,$$

για κάθε $\alpha \in \mathbb{N}$.

Γνωρίζουμε ότι για κάθε $x \in \mathbb{Z}_N$, η f_x είναι περιοδική συνάρτηση, με περίοδο την τάξη του στοιχείου x στον $\mathbb{Z}_N$, το ελάχιστο δηλαδή $r \in \mathbb{N}$ για το οποίο ισχύει $x^r \equiv 1 mod N$.

Πράγματι, εάν r είναι η τάξη του x, τότε $f(\alpha+r) \equiv x^{\alpha+r} \equiv x^\alpha x^r \equiv x^\alpha = f(\alpha)$ για κάθε $\alpha \in \mathbb{N}$.

Ο υπολογισμός της περιόδου της f για δεδομένο $x \in \mathbb{Z}_N$ με $gcd(x,N)=1$, αποτελεί το θεμελιώδες κομμάτι του χβαντικου αλγορίθμου παραγοντοποίησης του *P.Shor*. Ο πρωταρχικός μας σκοπός είναι να περιγράψουμε τον αλγόριθμο ο οποίος υπολογίζει σε πολυωνυμικό χρόνο την περίοδο r για δεδομένα $x, N \in \mathbb{N}$. Θα αποδείξουμε έπειτα ότι το πρόβλημα προσδιορισμού της περιόδου είναι ισοδύναμο με το πρόβλημα παραγοντοποίησης ενός ακεραίου, δίνοντας έτσι έναν πολυωνυμικό αλγόριθμο για την ανάλυση οποιουδήποτε ακεραίου σε πρώτους παράγοντες.

4.4.1 Υπολογισμός της περιόδου της f_x.

Ξεκινάμε λοιπόν επιλέγοντας ένα $N \in \mathbb{N}$ και ένα $x \in \mathbb{Z}_n$ σχετικά πρώτο προς το N. Υπάρχει τουλάχιστον μια δύναμη του 2 στο διάστημα $[N^2, 2N^2]$, την οποία θα συμβολίζουμε με q. Έτσι, $q = 2^m$ για κάποιο $m \in \mathbb{N}$ τέτοιο ώστε $N^2 \leq 2^m < 2N^2$ (ο λόγος που επιλέξαμε μια δύναμη του 2, θα γίνει ξεκάθαρος στα επόμενα βήματα). Οι τρείς αυτοί αριθμοί x, N, q θα παραμείνουν αναλλοίωτοι ως προς τις τιμές τους καθ'όλη την διάρκεια του αλγορίθμου, οπότε θεωρούμε οτι το υπολογιστικό (χωρικό) τους κόστος είναι μηδενικό.

Περιορίζουμε τώρα την συνάρτηση f_x στο $\mathbb{Z}_q = \{0, 1, ..., q-1\}$. Έτσι, συμβολίζουμε ξανά με f_x την

$$f_x : \mathbb{Z}_q \mapsto \mathbb{Z}_n$$

$$f(\alpha) = x^\alpha mod N,$$

$\alpha = 0, 1, ..., q-1$.

Η αρχική κατάσταση του χβαντικού υπολογιστικού συστήματος αποτελείται από δύο πολλαπλά *qubits*: ένα $m-qubit$, το $|00...0\rangle$, στο οποίο θα εισαγάγουμε τους αριθμούς $0, 1, ..., q-1$ του πεδίου ορισμού της f_x, και ένα $(lengthN)-qubit$ (όπου $lengthN :=$ Το πλήθος των ψηφίων του N) στο οποίο θα εισαγάγουμε το σύνολο $\{f_x(\alpha) : \alpha \in \mathbb{Z}_q\}$ και το οποίο είναι στην μορφή $|00...0\rangle$. Έχοντας λοιπόν την αρχική κατάσταση ως $|0\rangle_1|0\rangle_2 = |00\rangle$, εφαρμόζουμε τον μετασχηματισμό *Hadamard* $\mathcal{H}$ σε κάθε $qubit$ του $|0\rangle_1$, παίρνοντας

$$|0\rangle_1|0\rangle_2 \xrightarrow{\mathcal{H}\otimes\mathbb{I}} \frac{1}{q}\sum_{\alpha=0}^{q-1}|\alpha\rangle|0\rangle$$

έχοντας έτσι στο πρώτο $m-qubit$ τους αριθμούς $0,1,...,q-1$ σε μια ομοιόμορφη υπέρθεση. Ακριβώς επειδή οι αριθμοί $0,1,...,q-1$ βρίσκονται στο πρώτο $qubit$, ο μετασχηματισμός

$$|\alpha,0\rangle \longrightarrow |\alpha,f(\alpha)\rangle = |\alpha,x^\alpha mod N\rangle$$

μπορεί να αντιστραφεί (Ο υπολογισμός του $q^\alpha mod N$ μπορεί να γίνει σε πολυωνυμικό χρόνο με κλασσικό τρόπο, χρησιμοποιώντας την ανάλυση του α στην δυαδική του μορφή). Αυτός ο μετασχηματισμός δρα γραμμικά στην υπέρθεση των $|\alpha,0\rangle$, δίνοντας

$$|\psi_1\rangle = \frac{1}{\sqrt{q}}\sum_{\alpha=0}^{q-1}|\alpha,0\rangle \longrightarrow \frac{1}{\sqrt{q}}\sum_{\alpha=0}^{q-1}|\alpha,f(\alpha)\rangle.$$

Παρατήρηση 1: Ξεκινήσαμε με δύο πολλαπλά $qubits$, τα οποία και διαχωρίζονται με τον προφανή τρόπο :

$$\frac{1}{\sqrt{q}}\sum_{\alpha=0}^{q-1}|\alpha,0\rangle = \left(\frac{1}{\sqrt{q}}\sum_{\alpha=0}^{q-1}|\alpha\rangle\right)\otimes|0\rangle$$

.

Οδηγηθήκαμε όμως, μέσω $unitary$ μετασχηματισμών, στην κατάσταση

$$|\psi_2\rangle = \frac{1}{\sqrt{q}}\sum_{\alpha=0}^{q-1}|\alpha,x^\alpha mod N\rangle$$

η οποία αυτή την φορά αποτελείται από δύο πολλαπλά $qubits$ τα οποία δεν μπορούν να διαχωριστούν μεταξύ τους, ακριβώς επειδή κάθε ένας από τους γραμμικούς παράγοντες $|\alpha,x^\alpha mod N\rangle$ περιέχει μια κοινή πληροφορία στα πολλαπλά $qubits$ $|\alpha\rangle,|x^\alpha mod N\rangle$, τον αριθμό α. Αυτή ακριβώς η ιδιότητα της τελευταίας κατάστασης όμως θα βοηθήσει, όπως θα δούμε αργότερα, να αποφύγουμε πολλούς υπολογισμούς, δίνοντας την πολυωνυμική πολυπλοκότητα στον αλγόριθμο που μελετάμε.

Σε αυτό το σημείο εφαρμόζουμε τον F_q διακριτό μετασχηματισμό $Fourier$ στο πρώτο $m-qubit$, με την δράση του σε κάθε γραμμικό παράγοντα να είναι

$$|\alpha\rangle \longrightarrow \frac{1}{\sqrt{q}}\sum_{c=0}^{q-1}\exp(\frac{2\pi i\alpha c}{q})|c\rangle$$

για κάθε $\alpha\in\mathbb{Z}_q$. Παίρνουμε λοιπόν, λόγω της γραμμικότητας του F_q,

$$|\psi_2\rangle = \frac{1}{\sqrt{q}}\sum_{\alpha=0}^{q-1}|\alpha,f(\alpha)\rangle \xrightarrow{F_q\otimes I} |\psi_3\rangle = \frac{1}{q}\sum_{\alpha=0}^{q-1}\sum_{c=0}^{q-1}\exp(\frac{2\pi i\alpha c}{q})|c\rangle|f(\alpha)\rangle \Longleftrightarrow$$

$$\Longleftrightarrow |\psi_3\rangle = \frac{1}{q}\sum_{\alpha=0}^{q-1}\sum_{c=0}^{q-1}\zeta^{\alpha c}|c\rangle|f(\alpha)\rangle$$

όπου $\zeta = \exp(\frac{2\pi i}{q})$.

Παρατήρηση 2: Στην τελευταία κατάσταση $|\psi_3\rangle$, τα διανύσματα $\{|c\rangle|f(\alpha)\rangle : c,\alpha \in \mathbb{Z}_q\}$ δεν είναι όλα διαφορετικά μεταξύ τους· για δεδομένο $c \in \mathbb{Z}_q$, έχουμε λόγω περιοδικότητας της $f(\alpha) = x^\alpha mod N$,

$$x^\alpha \equiv x^k mod N$$

για κάθε $k < P$ τέτοιο ώστε

$$x^{\alpha-k} \equiv 1 mod N,$$

δηλαδή $P/(\alpha-k)$ (όπου με P συμβολίζουμε την περίοδο της f_x). Έχουμε λοιπόν, $f(\alpha) = f(k)$ για κάθε $k < P$ τέτοιο ώστε $\alpha \equiv k mod P$. Κατά συνέπεια, η τελευταία κατάσταση $|\psi_3\rangle$ δεν βρίσκεται σε ομοιόμορφη υπέρθεση των διακριτών μεταξύ τους στοιχείων του συνόλου

$$\{|c\rangle / c = x^k mod N, \quad k \in \mathbb{Z}_q, \quad k < P\}$$

Ο αλγόριθμος του *Shor* εκμεταλλεύεται αυτή την πληροφορία για να εξάγει την τιμή της P με μεγάλη πιθανότητα (≈ 1).

Ας επανέλθουμε τώρα στην κατάσταση $|\psi_3\rangle$ και ας την γράψουμε με πιο απλό συμβολισμό:

Μπορούμε να αλλάξουμε την σειρά άθροισης, διότι τα αθροίσματα είναι πεπερασμένα, παίρνοντας

$$|\psi_3\rangle = \frac{1}{q}\sum_{\alpha=0}^{q-1}\sum_{c=0}^{q-1}\zeta^{\alpha c}|c\rangle|f(\alpha)\rangle = \frac{1}{q}\sum_{c=0}^{q-1}\sum_{\alpha=0}^{q-1}\zeta^{\alpha c}|c\rangle|f(\alpha)\rangle = \frac{1}{q}\sum_{c=0}^{q-1}|c\rangle\sum_{\alpha=0}^{q-1}\zeta^{\alpha c}|f(\alpha)\rangle$$

$$= \frac{1}{q}\sum_{c=0}^{q-1}|c\rangle|\mathbb{Y}(c)\rangle = \frac{1}{q}\sum_{c=0}^{q-1}\|\mathbb{Y}(c)\|\,|c\rangle\frac{|\mathbb{Y}(c)\rangle}{\|\mathbb{Y}(c)\|}$$

όπου έχουμε θέσει $\mathbb{Y}(c) = \sum_{c=0}^{q-1}\zeta^{\alpha c}|f(\alpha)\rangle$ για κάθε $c \in \mathbb{Z}_q$.

Σε αυτό το σημείο "μετράμε" το πρώτο πολλαπλό *qubit* στο $|\psi_3\rangle$. Η μέτρηση πραγματοποιείται ως προς την υπολογιστική βάση $\{|c\rangle\langle c| \otimes I : c \in \mathbb{Z}_q\}$ όπου ο ταυτοτικός τελεστής I εφαρμόζεται στο δεύτερο πολλαπλό *qubit*.

Μπορούμε να δούμε την μέτρηση σαν μια διακριτή τυχαία μεταβλητή $\mathbb{M}$ που παίρνει τις τιμές $0, 1, ..., q-1$ με συνάρτηση κατανομής

$$\mathbb{F}_{\mathbb{M}}(c) = \mathbb{P}(\mathbb{M} = c) = \frac{\|\mathbb{Y}(c)\|^2}{q^2}$$

για $c = 0, 1, ..., q-1$.

Ας δούμε τώρα πως οι τιμές που συγκεντρώνουν την μεγαλύτερη πιθανότητα να εμφανιστούν, δίνουν την τιμή της περιόδου P με αρκετά μεγάλη πιθανότητα:

Κατ' αρχήν είναι προφανές ότι η περίοδος P της f_x δεν είναι απαραίτητο να είναι διαιρέτης του q που έχουμε επιλέξει. Μελετώντας λοιπόν την γενικότερη περίπτωση, ας θεωρήσουμε ως Π, r τους μοναδικούς θετικούς ακεραίους που μας δίνει η ευκλείδια διαίρεση του q απο το P, δηλαδή $q = P\Pi + r$ όπου $0 \leq r \leq P-1$.

Θέτουμε επίσης, $q_0 = P\Pi$. Στην επόμενη πρόταση δίνονται οι ακριβείς τιμές για την συνάρτηση κατανομής $\mathbb{F}_{\mathbb{M}}$:

Πρόταση 4.4.1 *Για κάθε $c = 0, 1, ...q-1$, έχουμε*

$$\mathbb{F}_{\mathbb{M}}(c) = \mathbb{P}(\mathbb{M} = c) = \begin{cases} \frac{r\sin^2[\frac{\pi Pc}{q}(\frac{q_0}{P}+1)]+(P-c)sin^2(\frac{\pi Pc}{q}\frac{q_0}{P})}{q^2\sin^2(\frac{\pi Pc}{q})}, & Pc \neq 0 mod q \\ \frac{r(q_0+P)^2+(P-r)q_0^2}{q^2P^2}, & Pc = 0 mod q \end{cases}$$

Απόδειξη

Είδαμε ότι για κάθε $c \in \mathbb{Z}_q$, ισχύει

$$\mathbb{F}_M(c) = \frac{\|\mathbb{Y}(c)\|^2}{q^2} = \frac{\langle \mathbb{Y}(c)|\mathbb{Y}(c)\rangle}{q^2}$$

Τώρα,

$$|\mathbb{Y}(c)\rangle = \sum_{\alpha=0}^{q-1} \zeta^{\alpha c}|f(\alpha)\rangle \overset{q_0 \leq q}{=} \sum_{\alpha=0}^{q_0-1} \zeta^{\alpha c}|f(\alpha)\rangle + \sum_{\alpha=q_0}^{q-1} \zeta^{\alpha c}|f(\alpha)\rangle \tag{4.1}$$

Διαιρώντας τώρα το $\alpha \in \mathbb{Z}_q$ με την περίοδο P, παίρνουμε

$$\alpha = Px_1 + x_0, \quad 0 \leq x_0 \leq P-1.$$

Έπεται λοιπόν ότι,

$$\sum_{\alpha=0}^{q_0-1} \zeta^{\alpha c}|f(\alpha)\rangle = \sum_{x_0=0}^{P-1} \sum_{x_1=0}^{\frac{q_0}{P}-1} \zeta^{(Px_1+x_0)c}|f(Px_1+x_0)\rangle \tag{4.2}$$

και

$$\sum_{\alpha=q_0}^{q-1} \zeta^{\alpha c}|f(\alpha)\rangle = \sum_{x_0=0}^{r-1} \zeta^{(P\frac{q_0}{P}+x_0)c}|f(Px_1+x_0)\rangle \tag{4.3}$$

Από τις 4.1, 4.2, 4.3 χρησιμοποιώντας την περιοδικότητα της f, παίρνουμε,

$$|\mathbb{Y}(c)\rangle = \sum_{x_0=0}^{P-1} \sum_{x_1=0}^{\frac{q_0}{P}-1} \zeta^{(Px_1+x_0)c}|f(Px_1+x_0)\rangle + \sum_{x_0=0}^{r-1} \zeta^{(P\frac{q_0}{P}+x_0)c}|f(Px_1+x_0)\rangle =$$

$$\sum_{x_0=0}^{P-1} \zeta^{x_0 c} \sum_{x_1=0}^{\frac{q_0}{P}-1} \zeta^{Px_1 c}|f(Px_1+x_0)\rangle + \zeta^{Pc\frac{q_0}{P}} \left(\sum_{x_0=0}^{r-1} \zeta^{x_0 c}|f(x_0)\rangle \right)$$

$$\overset{r\leq P}{=}\sum_{x_0=0}^{r-1}\zeta^{x_0c}\sum_{x_1=0}^{\frac{q_0}{P}}\zeta^{Px_1c}|f(x_0)\rangle+\sum_{x_0=r}^{P-1}\zeta^{x_0c}\sum_{x_1=0}^{\frac{q_0}{P}-1}\zeta^{Px_1c}|f(x_0)\rangle.$$

Καταλήξαμε σε μια ομοιόμορφη υπέρθεση των στοιχείων της $\{|f(x_0)\rangle : x_0 = 0,1,...,P-1\}$, τα στοιχεία της οποίας είναι διαφορετικά ανά δύο, διότι η f είναι $1-1$ στο $\mathbb{Z}_P$. Έπεται λοιπόν ότι,

$$\|\mathbb{Y}(c)\|^2=\langle\mathbb{Y}(c)|\mathbb{Y}(c)\rangle=\left(\sum_{x_0=0}^{r-1}|\zeta^{x_0c}|^2\right)\left|\sum_{x_1=0}^{\frac{q_0}{P}}\zeta^{Px_1c}\right|^2+\left(\sum_{x_0=r}^{P-1}|\zeta^{x_0c}|^2\right)\left|\sum_{x_1=0}^{\frac{q_0}{P}-1}\zeta^{Px_1c}\right|^2$$

$$=r\left|\sum_{x_1=0}^{\frac{q_0}{P}}\zeta^{Px_1c}\right|^2+(P-r)\left|\sum_{x_1=0}^{\frac{q_0}{P}-1}\zeta^{Px_1c}\right|^2.$$

Διακρίνουμε τώρα δυο περιπτώσεις:

(1) Εάν $Pc=0\ modq$, τότε q/Pc, οπότε $\zeta^{Pcx_1}=1$ για κάθε x_1 διότι ζ είναι q-στη ρίζα της μονάδας. Τότε,

$$\|\mathbb{Y}(c)\|^2=r(\frac{q_0}{P}+1)^2+(P-r)(\frac{q_0}{P})^2\Longleftrightarrow\mathbb{P}(\mathbb{M}=c)=\frac{\|\mathbb{Y}(c)\|^2}{q^2}=$$

$$=\frac{r(q_0+P)^2+(P-r)q_0^2}{q^2P^2}.$$

(2) Εάν $Pc\neq 0\ modq$, τότε αθροίζοντας τις δύο γεωμετρικές σειρές στην σχέση 1 παίρνουμε

$$\|\mathbb{Y}(c)\|^2=r\left|\frac{\zeta^{Pc(\frac{q_0}{P}+1)}-1}{\zeta^{Pc}-1}\right|^2+(P-r)\left|\frac{\zeta^{Pc\frac{q_0}{P}}-1}{\zeta^{Pc}-1}\right|^2=$$

$$\overset{\zeta=\exp\frac{2\pi i}{q}}{=}r\left|\frac{e^{\frac{2\pi}{q}Pc(\frac{q_0}{P}+1)i}-1}{e^{(\frac{2\pi Pc}{q})i}-1}\right|^2+(P-r)\left|\frac{e^{\frac{2\pi Pc}{q}\frac{q_0}{P}i}-1}{e^{\frac{2\pi iPc}{q}}-1}\right|^2.$$

Κάνοντας τώρα χρήση της ταυτότητας $|e^{i\theta}-1|^2=4\sin^2\frac{\theta}{2}$, παίρνουμε,

$$\mathbb{F}_{\mathbb{M}}(c)=\mathbb{P}(\mathbb{M}=c)=\frac{\|\mathbb{Y}(c)\|^2}{q^2}=\frac{r\sin^2[\frac{\pi Pc}{q}(\frac{q_0}{P}+1)]+(P-c)sin^2(\frac{\pi Pc}{q}\frac{q_0}{P})}{q^2\sin^2(\frac{\pi Pc}{q})}.$$

Παρατηρηση: Εάν το q που επιλέξαμε είναι πολλαπλάσιο της περιόδου P, τότε $r=0$, οπότε σε αυτή την περίπτωση η προηγούμενη πρόταση μας δίνει

$$\mathbb{F}_{\mathbb{M}}(c)=\mathbb{P}(\mathbb{M}=c)=\begin{cases}0, & Pc\neq 0modq\\ \frac{1}{P}, & Pc=0modq\end{cases}$$

Η επόμενη πρόταση μας δίνει, υπό ορισμένες συνθήκες, ένα κάτω φράγμα για την πιθανότητα να παρατηρήσουμε μια τιμή c. Αν στις τιμές της συνάρτησης

κατανομής της μέτρησης $\mathbb{M}$ αντικαταστήσουμε το Pc με το $\{Pc\}_q$, όπου $\{Pc\}_q$ ο αντιπρόσωπος στην κλάση $[Pc]_q$ του $\mathbb{Z}_q$ για τον οποίο $-\frac{q}{2} \leq \{Pc\}_q \leq \frac{q}{2}$, τότε θα πάρουμε τις εξής εκτιμήσεις:

Πρόταση 4.4.2

$$\mathbb{F}_{\mathbb{M}}(c) = \mathbb{P}(\mathbb{M} = c) \geq \begin{cases} \frac{4}{\pi^2 P}(1-\frac{1}{N})^2, & 0 < |\{Pc\}|_q \leq \frac{P}{2}(1-\frac{1}{N}) \\ \frac{1}{P}(1-\frac{1}{N})^2, & \{Pc\}_q = 0 \end{cases}$$

Απόδειξη

Έστω $0 < |\{Pc\}|_q \leq \frac{P}{2}(1-\frac{1}{N})$. Υπενθυμίζουμε ότι $N^2 \leq q \leq 2N^2$ από την υπόθεση. Έχουμε,

$$\left|\frac{\pi\{Pc\}_q}{q}(\frac{q_0}{P}+1)\right| \leq \frac{\pi P}{2q}\left(1-\frac{1}{N}\right)\left(\frac{q_0+P}{P}\right) \leq$$

$$\leq \frac{\pi}{2}\left(1-\frac{1}{N}\right)\left(\frac{q_0+P}{q}\right) \leq \frac{\pi}{2}\left(1-\frac{1}{N}\right)\left(\frac{q+P}{q}\right) = \frac{\pi}{2}\left(1-\frac{1}{N}\right)\left(1+\frac{P}{q}\right) \leq$$

$$\leq \frac{\pi}{2}\left(1-\frac{1}{N}\right)\left(1+\frac{N}{N^2}\right) = \frac{\pi}{2}\left(1-\frac{1}{N^2}\right) < \frac{\pi}{2}$$

Από την τελευταία ανισότητα έχουμε,

$$\left|\frac{\pi\{Pc\}_q}{q}\frac{q_0}{P}\right| \leq \left|\frac{\pi\{Pc\}_q}{q}(\frac{q_0}{P}+1)\right| < \frac{\pi}{2}$$

Τώρα, μπορούμε να χρησιμοποιήσουμε την εκτίμηση

$$\frac{4}{\pi^2}\theta^2 \leq \sin^2\theta \leq \theta^2$$

η οποία ισχύει για κάθε $\theta \in [-\frac{\pi}{2}, \frac{\pi}{2}]$, οπότε η προηγούμενη πρόταση θα μας δώσει,

$$\mathbb{P}(\mathbb{M}=c) = \frac{r\sin^2[\frac{\pi\{Pc\}_q}{q}(\frac{q_0}{P}+1)] + (P-r)sin^2(\frac{\pi\{Pc\}_q}{q}\frac{q_0}{P})}{q^2\sin^2(\frac{\pi\{Pc\}_q}{q})} \geq$$

$$\frac{r\frac{4}{\pi^2}\left(\frac{\pi\{Pc\}_q}{q}(\frac{q_0}{P}+1)\right)^2 + (P-r)\frac{4}{\pi^2}\left(\frac{\pi\{Pc\}_q}{q}\frac{q_0}{P}\right)^2}{q^2\left(\frac{\pi\{Pc\}_q}{q}\right)^2} =$$

$$= \frac{\frac{4}{\pi^2}\left(r(\frac{q_0}{P}+1)^2 + (P-r)(\frac{q_0}{P})^2\right)}{q^2} \geq \frac{4P(\frac{q_0}{P})^2}{\pi^2 q^2} =$$

$$= \frac{4q_0^2}{\pi^2 P q^2} \overset{q_0=q-r}{=} \frac{4}{\pi^2 P}\left(\frac{q-r}{q}\right)^2 = \frac{4}{\pi^2 P}\left(1-\frac{r}{q}\right)^2 \geq \frac{4}{\pi^2 P}\left(1-\frac{1}{N}\right)^2.$$

Αντίστοιχα, εαν $\{Pc\}_q = 0$ τότε $Pc =_q 0$ και η πρόταση 4 δίνει

$$\mathbb{P}(\mathbb{M} = c) = \frac{r(q_0+T)^2 + (T-r)q_0^2}{q^2T^2} \geq \frac{r{q_0}^2 + (T-r)q_0^2}{q^2T^2} = \frac{1}{T}\left(\frac{q_0}{q}\right)^2 =$$
$$= \frac{1}{T}\left(\frac{q-r}{q}\right)^2 = \frac{1}{T}\left(1-\frac{r}{q}\right)^2 \geq \frac{1}{T}\left(1-\frac{1}{N}\right)^2.$$

4.4.2 Συνεχή Κλάσματα.

Θα χρησιμοποιήσουμε τώρα το ακόλουθο θεώρημα απο την θεωρία των συνεχών κλασμάτων:

Θεώρημα 4.4.1 *Αν $|x - \frac{p}{q}| < \frac{1}{2q^2}$, τότε το $\frac{p}{q}$ είναι συγκλίνων κλάσμα στο x.*

Απόδειξη

Απο την υπόθεση, $|x - \frac{p}{q}| < \frac{1}{2q^2}$, οπότε υπάρχει $\theta \in (0, \frac{1}{2})$ τέτοιο ώστε $x - \frac{p}{q} = \frac{\varepsilon\theta}{q^2}$, όπου $\varepsilon = \pm 1$.

Τώρα, $\frac{p}{q} \in \mathbb{Q}$, οπότε αναπαρίσταται σαν πεπερασμένο συνεχές κλάσμα,

$$\frac{p}{q} = \alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cfrac{1}{\ddots + \frac{1}{\alpha_n}}}} := [\alpha_0, \alpha_1, ..., \alpha_n]$$

Για κάποια $\alpha_i, \in \mathbb{Q},\ i = 0, 1, ..., n$. Ονομάζουμε τα $\alpha_i,\ 0 \leq i \leq n$ συγκλίνωντα στο x. Το πλήθος των α_i στην παραπάνω αναπαράσταση του x μπορεί να επιλεγεί άρτιο ή περιττό, σύμφωνα με το επόμενο λήμμα:

Λήμμα 4.4.1 *Έστω οτι το x αναπαρίσταται ως συνεχές κλάσμα με περιττό (άρτιο) το πλήθος συγκλίνωντα α_n. Τότε, αναπαρίσταται και απο άρτιο (περιττό) πλήθος απο συγκλίνωντα α_n.*

Απόδειξη

Έστω $x = [\alpha_0, \alpha_1, ..., \alpha_n]$ η αναπαράσταση του x ως συνεχές κλάσμα. Τότε,
• Αν $\alpha_n = 1$,

$$x = \alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cfrac{1}{\ddots + \frac{1}{\alpha_n}}}} = \alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cfrac{1}{\ddots + \frac{1}{\alpha_{n-1}+1}}}}$$

οπότε $x = [\alpha_0, \alpha_1, ..., \alpha_{n-2}, \alpha_{n-1}, 1] = [\alpha_0, \alpha_1, ..., \alpha_{n-2}, \alpha_{n-1} + 1]$.
• Αν $\alpha_n \geq 2$, τότε

$$x = \alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cfrac{1}{\ddots + \frac{1}{\alpha_n}}}} = \alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cfrac{1}{\ddots + \cfrac{1}{\alpha_n - 1 + \frac{1}{1}}}}}$$

οπότε $x = [\alpha_0, \alpha_1, ..., \alpha_n] = [\alpha_0, \alpha_1, ..., \alpha_{n-1}, \alpha_n - 1, 1]$. □

Σύμφωνα λοιπόν με το παραπάνω λημμα, μπορούμε να υποθέσουμε ότι $\varepsilon = (-1)^{n-1}$, όπου $n \in N$ το πλήθος των συγκλίνωντων στην αναπαράσταση του $\frac{p}{q}$ ως συνεχές κλάσμα. Έστω τώρα ένα $w \in \mathbb{R}$ τέτοιο ώστε

$$x = \frac{wp_n + p_{n-1}}{wq_n + q_{n-1}}$$

όπου $\frac{p_n}{q_n}$ είναι το τελευταίο συγκλίνων κλάσμα του συνεχούς κλάσματος για το $\frac{p}{q}$, δηλαδή $\frac{p}{q} = \frac{p_n}{q_n}$ (εύκολα αποδεικνύεται ότι για κάθε n,

$$[\alpha_0, \alpha_1, ..., \alpha_n] = \frac{p_n}{q_n}$$

όπου p_n, q_n πρώτοι μεταξύ τους, οι οποίοι ορίζονται απο τους αναδρομικους τύπους

$$p_0 = \alpha_0,\ p_1 = \alpha_1\alpha_0 + 1,\ p_n = \alpha_n p_{n-1} + p_{n-2}$$
$$q_0 = 1, q_1 = \alpha_1,\ q_n = \alpha_n q_{n-1} + q_{n-2}).$$

Έχουμε τότε,

$$\frac{\varepsilon\theta}{q^2} = \frac{p}{q} - x \Longleftrightarrow \frac{\varepsilon\theta}{q_n^2} = \frac{p_n}{q_n} - x$$

διότι $\frac{p}{q} = \frac{p_n}{q_n}$ οπότε $q = q_n$, διότι $gcd(p, q) = 1$, $gcd(p_n, q_n) = 1$. Άρα

$$\frac{\varepsilon\theta}{q_n^2} = \frac{p_n}{q_n} - x = \frac{p_n}{q_n} - \frac{wp_n + p_{n-1}}{wq_n + q_{n-1}} = \frac{p_n q_{n-1} - q_{n-1}q_n}{q_n(wq_n + q_{n-1})} = \frac{(-1)^{n-1}}{q_n(wp_n + q_{n-1}}$$

$\Big($Να παρατηρήσουμε εδώ ότι, οι αναδρομικοί τύποι για τα p_n, q_n μας δίνουν

$$p_n q_{n-1} - p_{n-1}q_n = (\alpha_n p_{n-1} + p_{n-2})q_{n-1} - p_{n-1}(\alpha_n q_{n-1} + q_{n-2}) =$$
$$= -(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}),$$

οπότε παίρνουμε επαγωγικά,

$$p_n q_{n-1} - p_{n-1}q_n = (-1)^{n-1}(p_1 q_0 - p_0 q_1) = (-1)^{n-1}.\Big)$$

Έχουμε λοιπόν,

$$\frac{\varepsilon\theta}{q_n^2} = \frac{(-1)^{n-1}}{q_n(wp_n + q_{n-1})} \Longleftrightarrow \theta = \frac{q_n}{wq_n + q_{n-1}} \Longleftrightarrow w = \frac{1}{\theta} - \frac{q_{n-1}}{q_n} > 1,$$

διότι $q_{n-1} \leq q_n$ για κάθε $n \geq 1$ και $0 < \theta < \frac{1}{2}$.

Τελικά, $x = \frac{wp_n + p_{n-1}}{wq_n + q_{n-1}}$, όπου $w > 1$, $q_{n-1} \leq q_n$, $n \in \mathbb{N}$ και $p_n q_{n-1} - p_{n-1}q_n = (-1)^{n-1}$, οπότε σύμφωνα με το επόμενο θεώρημα το $\frac{p_n}{q_n} = \frac{p}{q}$ είναι συγκλίνων κλάσμα για το x:

Θεώρημα 4.4.2 *Αν $x = \frac{P\zeta + R}{Q\zeta + S}$, όπου $\zeta > 1$ και P, Q, R, $S \in \mathbb{Z}$ με $Q > S > 0$ και $PS - QR = \pm 1$, τότε τα $\frac{R}{S}$, $\frac{P}{Q}$ είναι συγκλίνοντα κλάσματα στην αναπαράσταση του x ως συνεχές κλάσμα.*

Απόδειξη

Γράφοντας το $\frac{P}{Q}$ ως απλό συνεχές κλάσμα $\frac{P}{Q} = [\alpha_0, \alpha_1, ..., \alpha_n] = \frac{p_n}{q_n}$ έχουμε, όπως και στην απόδειξη του θεωρήματος 4.4.1, $PS - QR = \pm 1 = (-1)^{n-1}$ όπου n το πλήθος των α_i στην παραπάνω αναπαράσταση του $\frac{P}{Q}$. Τώρα, $\frac{P}{Q} = p_n q_n$ και $gcd(P, Q) = 1$, $gcd(p_n, q_n) = 1$, οπότε $P = p_n$, $Q = q_n$ και

$$p_n S - q_n R = PS - QR = (-1)^{n-1} = p_n q_{n-1} - p_{n-1} q_n \iff$$

$$\iff p_n(S - q_{n-1}) = q_n(R - p_{n-1}) \Longrightarrow q_n / p_n(S - q_{n-1}) \overset{gcd(q_n, p_n)=1}{\Longrightarrow} q_n/(S - q_{n-1}).$$

Όμως, $q_n = Q > S > 0$ απο την υπόθεση και $q_n \geq q_{n-1} > 0$ για κάθε $n \in \mathbb{N}$, οπότε $|S - q_{n-1}| < q_n$.

Από τις δύο προηγούμενες σχέσεις έπεται ότι $S = q_{n-1}$. Λειτουργώντας αντίστοιχα, παίρνουμε $R = p_{n-1}$ οπότε

$$x = \frac{P\zeta + R}{Q\zeta + S} = \frac{p_n\zeta + p_{n-1}}{q_n\zeta + q_{n-1}} = [\alpha_0, \alpha_1, ..., \alpha_n, \zeta].$$

Αναλύοντας το ζ ως συνεχές κλάσμα, έχουμε

$$\zeta = [\alpha_{n+1}, \alpha_{n+2}, ...],$$

όπου $\alpha_{n-1} = [\zeta] \geq 1$, άρα

$$q = [\alpha_0, \alpha_1, ..., \alpha_n, \zeta] = [\alpha_0, \alpha_1, ..., \alpha_n, \alpha_{n+1}, \alpha_{n+2}, ...].$$

Έπεται οτι τα $\frac{p_{n-1}}{q_{n-1}} (= \frac{R}{S})$ και $\frac{p_n}{q_n} (= \frac{P}{Q})$ είναι συγκλίνωντα κλάσματα σε αυτή την αναπαράσταση του x ως συνεχές κλάσμα. □

Έπεται φυσιολογικά το επόμενο πόρισμα:

Πόρισμα 4.4.1 *Εστω $y \in \mathbb{Z}_Q$ και $\{Py\}_Q = Py - d(y)Q$ για κάποιο $d(y)$ τέτοιο ώστε $\{Py\}_Q = PymodQ$, $-\frac{Q}{2} \leq \{Py\}_Q \leq \frac{Q}{2}$. Εάν $|\{Py\}_Q| \leq \frac{P}{2}$, τότε το κλάσμα $\frac{d(y)}{P}$ είναι συγκλίνων στην αναπαράσταση του $\frac{y}{Q}$ ως συνεχές κλάσμα.*

Απόδειξη

Έχουμε, $\{Py\}_Q = Py - d(y)Q$, $|\{Py\}_Q| \leq \frac{P}{2}$, οπότε $|Py - Qd(y)| \leq \frac{P}{2} \Longleftrightarrow |y - Q\frac{d(y)}{P}| \leq \frac{1}{2} \Longleftrightarrow |\frac{y}{Q} - \frac{d(y)}{P}| \leq \frac{1}{2Q} \leq \frac{1}{2N^2} \leq \frac{1}{2P^2}$, διότι $Q \geq N^2$ και $P \leq N$. Το πόρισμα τώρα έπεται με εφαρμογή του θεωρήματος 4.4.2. □

Έχουμε λοιπόν, για κάποιο $n \in N$, $\frac{d(y)}{P} = \frac{p_n}{q_n}$ όπου τα p_n, q_n δίνονται απο τους αναδρομικούς τύπους που είδαμε προηγουμένως (το $n \in \mathbb{N}$ περιορίζεται σε ένα πεπερασμένο σύνολο της μορφής $\{0, 1, ..., m\}$ για κάποιο $m \in \mathbb{N}$, διότι $\frac{d(y)}{P} \in \mathbb{Q}$, οπότε το $\frac{d(y)}{P}$ έχει αναπαράσταση ως "πεπερασμένο" συνεχές κλάσμα, $\frac{d(y)}{P} = [\alpha_0, \alpha_1, ..., \alpha_m]$).

Γνωρίζουμε το Q και το y, το εξαγόμενο αποτέλεσμα απο την μέτρηση που πραγματοποιήσαμε στον χώρο καταστάσεων του

$$|\psi_2\rangle = \frac{1}{Q} \sum_{y=0}^{Q-1} \|\mathbb{Y}(y)\| \, |y\rangle \frac{\mathbb{Y}(y)}{\|\mathbb{Y}(y)\|}$$

ώς προς την υπολογιστική βάση $\{|0\rangle, |1\rangle, ..., |Q-1\rangle\}$. Τώρα, $gcd(p_n, q_n) = 1$, οπότε εάν ισχύει και ότι $gcd(d(y), P) = 1$ θα έχουμε

$$\frac{d(y)}{P} = \frac{p_n}{q_n} \Longrightarrow d(y) = p_n$$

και $\underline{p = q_n}$, οπότε εξάγουμε την ζητούμενη περίοδο απο τους αναδρομικούς τύπους για το q_n!!!

Ποιά είναι όμως η πιθανότητα το $d(y)$ που αντιστοιχεί στην τιμή $y \in \mathbb{Z}_Q$ να είναι τέτοιο ώστε $gcd(P, d(y)) = 1$; Εύκολα βλέπουμε ότι $d(y) = round\big(\frac{P}{Q}y\big) = 1$, όπου $round\{x\}$ η στρογγυλοποίηση του x. Έπεται λοιπόν ότι $d \leq P$ διότι $y \leq Q$ ($y \in \mathbb{Z}_Q$). Οι ακέραιοι που είναι μικρότεροι του P και σχετικά πρώτοι προς το P δίνονται απο την $\Phi(P)$, όπου Φ είναι η συνάρτηση του $Euler$. Έχουμε λοιπόν $\phi(P)$ το πλήθος ευνοϊκές τιμές για το y, κάθε μια απο τις οποίες εμφανίζεται με πιθανότητα

$$\mathbb{P}(M = y) \geq \frac{4}{\pi^2} \frac{1}{P} \big(1 - \frac{1}{N}\big).$$

Έπεται λοιπόν οτι

$$\mathbb{P}\bigg(M = y, y \in \mathbb{Z}_Q / gcd\big(d(y), P\big) = 1\bigg) \geq \frac{4}{\pi^2} \frac{\phi(P)}{P} \bigg(1 - \frac{1}{N}\bigg)^2$$

Στο "*Introduction to theory of Numbers*" των *Hardy & Wright* δίνεται η ακόλουθη εκτίμηση:

$$\liminf \frac{\phi(N)}{N/\ln\ln N} = e^{-\gamma},$$

όπου γ είναι η σταθερά του *Euler*, $\gamma = 0,5772...$

Έχουμε λοιπόν,

$$\liminf \frac{\phi(P)}{P/\ln\ln P} = e^{-\gamma} \Longleftrightarrow \frac{\phi(P)}{P/\ln\ln P} \geq e^{-\gamma} \Longleftrightarrow \frac{\phi(P)}{P} \geq \frac{e^{-\gamma}}{\ln\ln P},$$

οπότε,

$$\mathbb{P}\Big(M = y, y \in \mathbb{Z}_Q / gcd\big(d(y), P\big) = 1\Big) \geq \frac{4}{\pi^2}\ \frac{e^{-\gamma}}{\ln\ln P}\left(1 - \frac{1}{N}\right)^2 \geq$$

$$\geq \frac{4}{\pi^2}\ \frac{e^{-\gamma}}{\ln\ln N}\left(1 - \frac{1}{N}\right)^2,$$

διότι $P \leq N$. Έπεται λοιπόν ότι

$$\mathbb{P}\big(M = y, y \in \mathbb{Z}_Q / gcd(d(y), P) = 1\big) = \Omega\left(\frac{1}{\ln\ln N}\right).$$

Επαναλαμβάνοντας τελικά την μέτρηση της κατάστασης

$$|\psi_2\rangle = \frac{1}{Q}\sum_{y=0}^{Q-1} \|\mathbb{Y}(y)\rangle\| \, |y\rangle \frac{|\mathbb{Y}(y)\rangle}{\|\mathbb{Y}(y)\|}$$

$O(\ln\ln N)$ φορές, θα εξάγουμε την ζητούμενη περίοδο P με πιθανότητα ≈ 1.

4.4.3 Από τον υπολογισμό της περιόδου μιας περιοδικής συνάρτησης, στην ανάλυση ενος ακεραίου σε πρώτους παράγοντες.

Στην προηγούμενη παράγραφο δώσαμε έναν αλγόριθμο πολυωνυμικής πολυπλοκότητας, ο οποίος υπολογίζει για δεδομένα $x, N \in \mathbb{N}$ την περίοδο της συνάρτησης $f_x(\alpha) = x^\alpha mod N$. Ας δούμε τώρα πώς αυτό μπορεί να μας βοηθήσει στο να παραγοντοποιήσουμε σε πολυωνυμικό χρόνο έναν ακέραιο αριθμό.

Έστω λοιπόν $N \in \mathbb{Z}$ ένας τέτοιος ακέραιος (ας τον υποθέσουμε περιττό) και έστω x να είναι ένα στοιχείο του $\mathbb{Z}_N$ σχετικά πρώτο προς το N. (Η επιλογή ενός τέτοιου στοιχείου μπορεί να γίνει σε πολυωνυμικό χρόνο χρησιμοποιώντας τον ευκλείδιο αλγόριθμο. Εάν $gcd(x, N) \neq 1$ τότε έχουμε βρεί έναν μη τετριμμένο διαιρέτη του N. Διαφορετικά, συνεχίζουμε με την διαδικασία που περιγράφεται παρακάτω).

Χρησιμοποιώντας τον αλγόριθμο του $Shor$, υπολογίζουμε την τάξη του x στον $\mathbb{Z}_n$, το ελάχιστο δηλαδή $r \in \mathbb{Z}_N$ για το οποίο $x^r = 1\ mod N$. Τότε,

$$x^r = 1\ mod N \Longleftrightarrow (x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1) = x^r - 1 = 0\ mod N \Longleftrightarrow$$

$$\Longleftrightarrow N/(x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1).$$

Εαν λοιπόν p είναι ένας πρώτος διαιρέτης του N, τοτε ο p θα διαιρεί και το γινόμενο $(x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1)$, οπότε θα είναι και $p/x^{\frac{r}{2}} - 1$ είτε $p/x^{\frac{r}{2}} + 1$. Έπεται

λοιπόν ότι, είτε ο $gcd(N, x^{\frac{r}{2}} - 1)$, είτε ο $gcd(N, x^{\frac{r}{2}} + 1)$ θα είναι παράγοντας του N, έχοντας πετύχει έτσι τον σκοπό μας.

Υπάρχουν δυστυχώς δύο περιπτώσεις στις οποίες η παραπάνω διαδικασία αποτυγχάνει. Η πρώτη περίπτωση είναι να επιλέξουμε ένα στοιχείο $x \in \mathbb{Z}_N$ του οποίου η τάξη r στον $\mathbb{Z}_N$ είναι περιττός αριθμός· τότε το $\frac{r}{2}$ δεν είναι ακέραιος, οπότε η παραπάνω διαδικασία δεν μπορεί να προχωρήσει. Η δεύτερη περίπτωση είναι το x που επιλέγουμε να είναι τέτοιο ώστε $x^{\frac{r}{2}} + 1 = 0\ modN$, οπότε $x^{\frac{r}{2}} - 1 = -2\ modN$, $gcd(N, x^{\frac{r}{2}} + 1) = N$ και $gcd(N, x^{\frac{r}{2}} - 1) = gcd(N, -2) = 1$ (το N είναι περιττός), παίρνοντας έτσι τους τετριμμένους παράγοντες $1, N$. Θα αποδείξουμε τώρα ότι, επιλέγοντας τυχαία ενα $x \in \mathbb{Z}_N$ σχετικά πρώτο προς το N και εφαρμόζοντας την παραπάνω διαδικασία, η πιθανότητα να πάρουμε ένα μη τετριμμένο διαιρέτη του N είναι κάτω φραγμένη απο το $1 - \frac{1}{2^{k-1}}$, όπου κ είναι το πλήθος των διακριτών μεταξύ τους πρώτων $p \neq 2$ στην ανάλυση του N σε πρώτους παράγοντες:

Θεώρημα 4.4.3 *Έστω ένας περιττός αριθμός N και $N = p_1^{\alpha_1} p_2^{\alpha_2} .... p_k^{\alpha_k}$ η ανάλυσή του σε πρώτους παράγοντες. Επιλέγουμε στην τύχη ένα y τέτοιο ώστε $gcd(y, N) = 1$. Αν r είναι η τάξη του y στον $\mathbb{Z}_N$, τότε*

$$\mathbb{P}(\textit{το } r \textit{ είναι άρτιος και } y^{\frac{r}{2}} \neq -1\ modN) \geq 1 - \frac{1}{2^{k-1}}.$$

Απόδειξη

Θα αποδείξουμε ότι

$$\mathbb{P}(\text{το } r \text{ είναι περιττός και } y^{\frac{r}{2}} = -1\ modN) \leq \frac{1}{2^{k-1}}.$$

Από την υπόθεση, $gcd(y, N) = 1$, οπότε $gcd(y, p_i^{\alpha_i}) = 1$ για κάθε $i = 1, ..., .k$. Έστω r_i η τάξη του y στον $\mathbb{Z}p_i^{\alpha_i}$. Τότε, $y^{r_i} = 1 mod p_i^{\alpha_i}$ για κάθε $i = 1, ..., k$. Εύκολα αποδεικνύεται ότι $r = lcm(r_1, ..., r_k)$.

Ισχυριζόμαστε ότι,

$$y^{\frac{r}{2}} = -1 mod N \Longleftrightarrow y^{\frac{r}{2}} = 1 mod p_i^{\alpha_i} \text{ για κάθε } i.$$

Πράγματι, αφού $p_i^{\alpha_i} / N$ για κάθε i, έπεται άμεσα ότι

$$y^{\frac{r}{2}} = -1 mod N \Longrightarrow y^{\frac{r}{2}} = 1 mod p_i^{\alpha_i} \text{ για κάθε } i.$$

Η αντίστροφη συνεπαγωγή αποδεικνύεται με χρήση του Κινέζικου Θεωρήματος Υπολοίπων. Πράγματι, σύμφωνα με αυτό, το σύστημα υπολοίπων

$$\begin{aligned} y^{\frac{r}{2}} &= -1 mod p_1^{\alpha_1} \\ y^{\frac{r}{2}} &= -1 mod p_2^{\alpha_2} \\ &\vdots \\ y^{\frac{r}{2}} &= -1 mod p_k^{\alpha_k}, \end{aligned}$$

έχει μοναδική λύση $modN$. Απο την αντίστροφη συνεπαγωγή, η $y^{\frac{r}{2}} = -1 modN$ είναι μια λύση του συστήματος, οπότε είναι και η μοναδική και η συνεπαγωγη έπεται άμεσα.

Τώρα, μπορούμε να γράψουμε τα r_i στην μορφή $r_i = s_i 2^{t_i}$ για κάποιους περιττούς s_i και κάποια $t_i \in \mathbb{N}$, $i = 1, ..., k$. Θέτωντας λοιπόν $s = lcm(s_1, ...s_k)$ και $t = max(t_1, ..., t_k)$, έχουμε

$$r = lcm(r_1, ..., r_k) = lcm(s_1 2^{t_1}, s_2 2^{t_2}, ..., s_k 2^{t_k}) = s 2^t.$$

Ισχυριζόμαστε τώρα ότι

$$y^{\frac{r}{2}} = -1 mod p_i^{\alpha_i} \text{ και } p_i^{\alpha_i} \neq 2 \Longrightarrow t_i = t,$$

για κάθε $i = 1, ..., k$. Πράγματι, έστω ένα i τέτοιο ώστε $y^{\frac{r}{2}} = -1 mod p_i^{\alpha_i}$, $p_i^{\alpha_i} \neq 2$ και $t_i < t$. Τότε $t_i \leq t-1$, οπότε $2^{t_i} / 2^{t-1}$ δηλαδή $2^{t_i} / \frac{r}{2}$. Παράλληλα, έχουμε οτι $s_i / \frac{r}{2}$. Έπεται λοιπόν ότι $s_i 2^{t_i} = r_i / \frac{r}{2}$, το οποίο όμως είναι άτοπο απο την υπόθεση, διότι $y^{\frac{r}{2}} = -1 mod p_i^{\alpha_i}$ και όπως είδαμε παραπάνω $y^{r_i} = 1 mod p_i^{\alpha_i}$, οπότε $1 = -1 mod p_i^{\alpha_i} \Longrightarrow p_i^{\alpha_i} = 2$.

Τώρα, έχουμε υποθέσει ότι ο N είναι περιττός, οπότε $p_i^{\alpha_i} \neq 2$ για κάθε $i = 1, ..., k$. Είδαμε ότι $r = lcm(r_1, ..., r_k)$, οπότε εύκολα βλέπουμε ότι ο r ειναι περιττός αν και μόνο αν ο r_i είναι περιττος, για κάθε i, οπότε τότε θα έχουμε $t_i = 0$ για κάθε i. Αν τώρα $y^{\frac{r}{2} = -1 mod N}$, τότε οι παραπάνω συνεπαγωγές μας δίνουν $t_i = t$ για κάθε $i = 1$. Έχουμε λοιπόν,

$$\mathbb{P}(\text{το } r \text{ είναι περιττός και } y^{\frac{r}{2}} = -1 mod N) \leq \mathbb{P}(\text{ όλα τα } t_i \text{ είναι ίσα}).$$

Τώρα, εύκολα ελέγχουμε ότι

$$\mathbb{P}(t_i = j) \leq \frac{1}{2}, \text{ για κάθε } i, j.$$

οπότε έχουμε τελικά,

$$\mathbb{P}(\text{όλα τα } t_i \text{ είναι ισα}) = \sum_j \mathbb{P}(t_1 = j, t_2 = j, ..., t_k = j) = \sum_j \prod_{i=1}^{k} \mathbb{P}(t_i = j),$$

διότι τα ενδεχόμενα $(t_i = j)_{i=1}^k$ είναι ανεξάρτητα, άρα

$$\mathbb{P}(\text{όλα τα } t_i \text{ είναι ίσα}) \leq \left(\sum_j \mathbb{P}(t_1 = j) \right) \frac{1}{2^{k-1}} = \frac{1}{2^{k-1}}.$$

□

Βιβλιογραφία

[1] A. Berthiaume, *Quantum computation*, Complexity Theory Retrospective II, 23-51, Springer-Verlag (1997).

[2] S.J.Lomonaco, *Shor's quantum factoring algorithm*, 181–192, Proc. Sympos. Appl. Math., 58, Amer. Math. Soc., Providence, RI, 2002, (http://xxx.lanl.gov/abs/quant-ph/0010034).

[3] *A.Ekert, R.Jozsa, Quantum computation and Shor's factoring algorithm*, . Rev. Modern Phys. 68 (1996), no. 3, 733–753.

[4] *R.Jozsa, Quantum algorithms and the Fourier transform*, R. Soc. Lond. Proc. Ser. A Math. Phys. Eng. Sci. 454 (1998), no. 1969, 323–337 (http://xxx.lanl.gov/abs/quant-ph/9707033).

[5] S.J.Lomonaco, *A Rosetta stone for quantum mechanics with an introduction to quantum computation*, 3–65, Proc. Sympos. Appl. Math., 58, Amer. Math. Soc., Providence, RI, 2002. (http://xxx.lanl.gov/abs/quant-ph/0007045).

[6] P.Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Rev. 41 (1999), no. 2, 303–332 (http://xxx.lanl.gov/abs/quant-ph/9508027).

[7] S.Gudder, *Quantum computation*, Amer. Math. Monthly 110 (2003), no. 3, 181–201.

[8] G.Hardy, E.M.Wright, 1965, *An introduction to the theory of numbers.*

[9] E.Rieffel, W.Polak, *An introduction to quantum computing for non-Physicists*, ACM Computing Surveys, Vol 32, No3, Sept.2000, pp.300-335.

[10] L.Grover, *Quantum mechanics helps in searching for a needle in a haystack.* (http://xxx.lanl.gov/abs/quant-ph/9706033).