



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ  
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ  
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Τίτλος Διπλωματικής

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

ΗΛΙΑΝΑΣ Θ. ΜΠΕΤΣΟΥ

Επιβλέπων: Επιβλέπων  
Τίτλος

Αθήνα, Ιούνιος 2019





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

## Τίτλος Διπλωματικής

### ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της

**ΗΛΙΑΝΑΣ Θ. ΜΠΕΤΣΟΥ**

**Επιβλέπων:** Επιβλέπων  
Τίτλος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την Ημερομηνία Παρουσίασης.

(Υπογραφή)

(Υπογραφή)

(Υπογραφή)

.....  
Επιβλέπων  
Τίτλος

.....  
1ος Εξεταστής  
Τίτλος

.....  
2ος Εξεταστής  
Τίτλος

Αθήνα, Ιούνιος 2019





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

Copyright ©–All rights reserved Ηλιάνα Μπέτσου, 2019.

Με την επιφύλαξη παντός δικαιώματος.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα.

Το περιεχόμενο αυτής της εργασίας δεν απηχεί απαραίτητα τις απόψεις του Τμήματος, του Επιβλέποντα, ή της επιτροπής που την ενέκρινε.

### **Υπεύθυνη Δήλωση**

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

(Υπογραφή)

.....

Ηλιάνα Μπέτσου



# Περίληψη

Λέξεις Κλειδιά





# Abstract

Keywords



*Αφιέρωση*



# Ευχαριστίες

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



# Περιεχόμενα

Περίληψη	i
Abstract	iii
Ευχαριστίες	vii
Περιεχόμενα	x
<b>1 Introduction and Overview</b>	<b>1</b>
1.1 History . . . . .	1
1.2 Future Directions . . . . .	1
<b>2 Fundamentals</b>	<b>3</b>
2.1 Overview . . . . .	3
2.2 Quantum Computation . . . . .	3
2.2.1 Qubits . . . . .	3
2.2.2 Quantum Circuits . . . . .	3
2.3 The Dirac notation nad Hilbert spaces . . . . .	3
2.4 Quantum Circuits . . . . .	3
2.4.1 The quantum Circuit model . . . . .	3
2.4.2 Quantum Gates . . . . .	3
2.4.3 Universal Quantum Gates . . . . .	3
<b>3 Introduction to Computer Science</b>	<b>5</b>
3.1 Overview . . . . .	5
3.2 Turing Machines . . . . .	5
3.3 Computanional Complexity . . . . .	5
3.4 Problems in classes P and NP . . . . .	5
<b>4 Quantum Algorithms</b>	<b>7</b>
4.1 Probabilistic Versus Quantum Algorithms . . . . .	7
4.2 Quantum Parallelism . . . . .	9
4.3 Deutsch's Algorithm . . . . .	10

4.4	Deutsch-Jozsa Algorithm . . . . .	10
4.5	Simon's Algorithm . . . . .	10
4.6	Grover's Algorithm . . . . .	10
4.7	Quantum Search Algorithms . . . . .	10
<b>5</b>	<b>The quantum Fourier Transformation</b>	<b>11</b>
5.1	FFT . . . . .	11
5.2	Κβαντική Διεμπλοκή . . . . .	15
5.2.1	Κβαντική Διεμπλοκή και Υπέρθωση . . . . .	16
5.3	Quantum Fourier Transformation . . . . .	17
5.3.1	Περιοδικότητα . . . . .	21
<b>6</b>	<b>The Shor's Code</b>	<b>23</b>
6.1	Quantum error-correction . . . . .	23
<b>7</b>	<b>RSA Cryptosystem</b>	<b>25</b>
<b>8</b>	<b>Future Work/What's Happening Now</b>	<b>27</b>
<b>9</b>	<b>Summary</b>	<b>29</b>
<b>A'</b>	<b>Παράδειγμα Παραρτήματος</b>	<b>31</b>
A'.1	Πρώτη ενότητα . . . . .	31
A'.2	Μελλοντικές Επεκτάσεις . . . . .	31



# Κεφάλαιο 1

## Introduction and Overview

### 1.1 History

### 1.2 Future Directions



## Κεφάλαιο 2

# Fundamentals

### 2.1 Overview

### 2.2 Quantum Computation

#### 2.2.1 Qubits

#### 2.2.2 Quantum Circuits

### 2.3 The Dirac notation nad Hilbert spaces

### 2.4 Quantum Circuits

#### 2.4.1 The quantum Circuit model

#### 2.4.2 Quantum Gates

#### 2.4.3 Universal Quantum Gates



## Κεφάλαιο 3

# Introduction to Computer Science

3.1 Overview

3.2 Turing Machines

3.3 Computational Complexity

3.4 Problems in classes P and NP



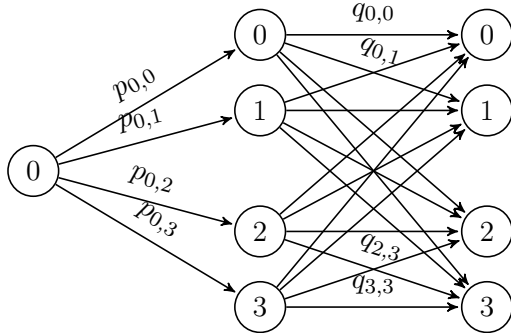
## Κεφάλαιο 4

# Quantum Algorithms

### 4.1 Probabilistic Versus Quantum Algorithms

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

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

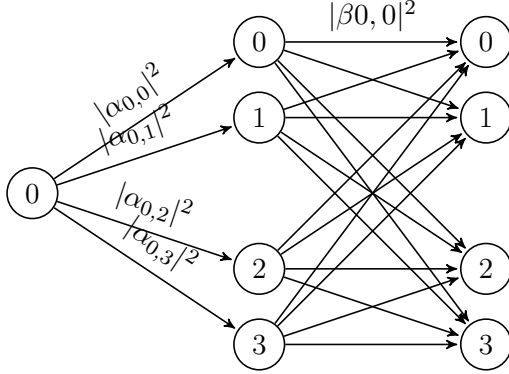


Αρχικοποιούμε τον καταχωρητή στο 0. Μετά το πρώτο βήμα, ο καταχωρητής είναι στην κατάσταση  $j$  με πιθανότητα  $p_{0,j}$ . Υποθέτουμε ότι θέλουμε να βρούμε τη συνολική πιθανότητα ότι ο υπολογισμός τερματίζει στην κατάσταση 3 μετά το δεύτερο βήμα. Αυτός ο υπολογισμός γίνεται σε δύο στάδια. Αρχικά υπολογίζουμε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

των κβαντικών πιθανοτικών πλατών. Δηλαδή  $p_{0,j} = |\alpha_{0,j}|^2$  και  $q_{j,k} = |\beta_{j,k}|^2$ . Άρα το τελικό αποτέλεσμα που προκύπτει είναι [6]:

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

Και εδώ έχουμε το προηγούμενο σχήμα με χρήση κβαντικών πλατών.



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

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

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

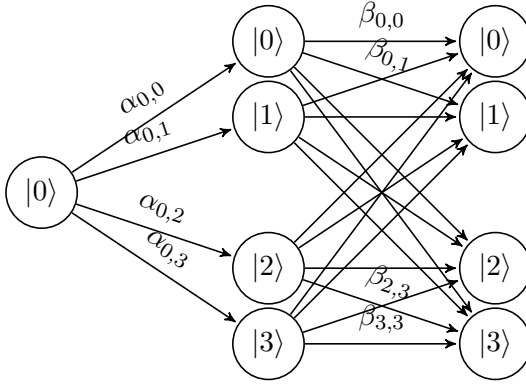
$$\begin{aligned} prob_3 &= \sum_j |\alpha_{0,j}|^2 |\beta_{j,3}|^2 \\ &= \sum_j |\alpha_{0,j} \beta_{j,3}|^2 \end{aligned}$$

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

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



Και λίγο πιο παραστατικά:



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

## 4.2 Quantum Parallelism

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

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

Έστω ένα κύκλωμα που εφαρμόζει την  $U_f$  σε μια είσοδο αλλά όχι σε υπολογιστική βάση. Τότε ο *dataregister* είναι προετοιμασμένος για την υπέρθεση  $(|0\rangle + |1\rangle)/\sqrt{2}$  το οποίο μπορούμε να το δημιουργήσουμε με μια πύλη *Hadamard*. Και εφαρμόζοντας την  $U_f$  έχουμε [7]:

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

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

Η παραπάνω διαδικασία/παράδειγμα θα μπορούσε να γενικευτεί σε συναρτήσεις με έναν τυχαίο αριθμό *bits* χρησιμοποιώντας τη γενική διαδικασία *HadamardTransform* ή *Walsh – HadamardTransform*. Η συγκεκριμένη διαδικασία είναι επί της ουσίας  $n$  πύλες *Hadamard* που δρουν παράλληλα σε  $nqubits$ .

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

### 4.3 Deutsch's Algorithm

### 4.4 Deutsch-Jozsa Algorithm

### 4.5 Simon's Algorithm

### 4.6 Grover's Algorithm

### 4.7 Quantum Search Algorithms

## Κεφάλαιο 5

# The quantum Fourier Transformation

### 5.1 FFT

Οι πράξεις μεταξύ πολυωνύμων μεγάλου μεγέθους χρησιμοποιούνται ευρέως. Η ολοκλήρωση τους ‘χειροκίνητα’ είναι μια χρονοβόρα και δύσκολη διαδικασία. Η επίλυση σε αυτό έρχεται με τη χρήση του Γρήγορου Μετασχηματισμού [1] *Fourier (FFT)*.

Ο *FFT*, βασίζεται σε κάποιες βασικές αρχές και ιδιότητες [5]. Η κυριότερη είναι η ιδιότητα των πολυωνύμων να χαρακτηρίζονται με δύο διαφορετικές μορφές.

Το πολυώνυμο  $A(x)$  μπορεί να χαρακτηριστεί με τους εξής δύο τρόπους:

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

Πολύ συνοπτικά, ο *FFT* είναι ένας αλγόριθμος διαίρει-και-βασίλευε, που βασίζεται στις ιδιότητες των μιγαδικών ριζών της μονάδας. Χρησιμοποιεί τον διακριτό μετασχηματισμό *Fourier (DFT)* και τον αντίστροφο *DFT* για να μετατρέπει τις δύο μορφές αναπαράστασης του πολυωνύμου. Από την αναπαράσταση του πολυωνύμου βαθμού  $d$  μέσω συντελεστών, προκύπτει ένα διάνυσμα με τους συντελεστές  $\alpha = (a_0, a_1, \dots, a_d)$ . Η απεικόνιση ενός πολυωνύμου βαθμού  $d$  σε μορφή τιμών μας δίνει ένα πακέτο από  $d$  ζευγάρια της μορφής  $(x_0, y_0), (x_1, y_1), \dots, (x_d, y_d)$  τέτοια ώστε κάθε  $x_k$  να είναι διακριτοί αριθμοί και κάθε  $y_k = A(x_k)$  για κάθε  $k = 0, 1, \dots, d$ .

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

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

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

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

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

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

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

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

$$A(x_i) = A_e(x_i^2) + x_i A_o(x_i^2) \text{ και } A(-x_i) = A_e(x_i^2) - x_i A_o(x_i^2)$$

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

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

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

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

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

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

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

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

$$\begin{bmatrix} A(x_0) \\ A(x_1) \\ \vdots \\ A(x_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & x_0^2 & \dots & x_0^{n-1} \\ 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ & & \vdots & & \\ 1 & x_{n-1} & x_{n-1}^2 & \dots & x_{n-1}^{n-1} \end{bmatrix} \cdot \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{bmatrix}$$

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

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

$$M_n(\omega) = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(n-1)} \\ & & \vdots & & \\ 1 & \omega^j & \omega^{2j} & \dots & \omega^{(n-1)j} \\ & & \vdots & & \\ 1 & \omega^{(n-1)} & \omega^{2(n-1)} & \dots & \omega^{(n-1)(n-1)} \end{bmatrix}, \text{ όπου η πρώτη σειρά}$$

προκύπτει για  $\omega^0 = 1$ , η δεύτερη για  $\omega$ , η τρίτη για  $\omega^2$  μέχρι την τελευταία που προκύπτει

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

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

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

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

Συνοπτικά ο *FFT* έχει ως εξής:

## Fast Fourier Transform

---

```

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

```

---

## 5.2 Κβαντική Διεμπλοκή

Η κβαντική διεμπλοκή έχει τις ρίζες της σε ένα άρθρο των A. Einstein, B. Podolsky και N. Rosen [3]. Ο σκοπός του άρθρου ήταν να αποδείξουν ότι η κβαντική μηχανική δεν είναι μια πλήρης φυσική θεωρία, αλλά ότι από την κβαντική περιγραφή της φύσης λείπουν κάποιες παράμετροι. Αργότερα οι παράμετροι αυτές ονομάστηκαν "κρυμμένες μεταβλητές". Σαν μοντέλο για την απόδειξη τους, χρησιμοποίησαν ένα θεωρητικό πείραμα στο οποίο δύο κβαντικά συστήματα, αφού αλληλεπιδράσουν μεταξύ τους απομακρύνονται το ένα από το άλλο. Τα δύο αυτά κβαντικά συστήματα παραμένουν διασυνδεδεμένα το ένα με το άλλο με έναν άγνωστο μη κλασσικό τρόπο. Αυτό έχει σαν αποτέλεσμα η μέτρηση μιας φυσικής ποσότητας του ενός, καθορίζει το αποτέλεσμα της μέτρησης της ίδιας φυσικής ποσότητας του άλλου. Το θεωρητικό αυτό πείραμα ονομάστηκε "παράδοξο EPR", από τα αρχικά των τριών ερευνητών. Η κβαντική διεμπλοκή είναι ίσως η πιο ανιγματική πλευρά της κβαντικής μηχανικής και δεν έχει κλασσικό ανάλογο. Κάθε χρόνο πολλές δεκάδες άρθρα δημοσιεύονται σε επιστημονικά περιοδικά και περιγράφουν επιστημονικές εργασίες που έχουν ως στόχο την κατανόηση, το χειρισμό και τον υπολογισμό της κβαντικής διεμπλοκής. Για τους κβαντικούς υπολογιστές η κβαντική διεμπλοκή είναι ένας φυσικός πόρος, όπως η ενέργεια, τον οποίο μπορούμε να χρησιμοποιήσουμε για να εκτελέσουμε κβαντικούς υπολογισμούς και να αναπτύξουμε κβαντικούς αλγόριθμους [7]. Αυτό που έχει δηλαδή σημασία, δεν είναι να κατανοήσουμε τη φύση της κβαντικής διεμπλοκής (πράγμα που είναι ίσως αδύνατο), αλλά να μάθουμε να την παράγουμε και να τη χρησιμοποιούμε.

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

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

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

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

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

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

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

και τελικά

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

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

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

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

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

### 5.2.1 Κβαντική Διεμπλοκή και Υπέρθεση

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

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



### 5.3 Quantum Fourier Transformation

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

Στον γρήγορο μετασχηματισμό *Fourier* [5] παίρνουμε σαν είσοδο ένα μιγαδικό διάνυσμα  $M$ -διάστασης,  $\alpha$  και σαν έξοδο επιστρέφει ένα μιγαδικό διάνυσμα  $M$ -διάστασης,  $\beta$ . Έχουμε δηλαδή το εξής:

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

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

Ο κβαντικός μετασχηματισμός *Fourier* είναι ο ίδιος μετασχηματισμός με λίγο διαφορετικές συμβάσεις. Επί της ουσίας είναι ένας ορθομοναδιαίος συντελεστής του χώρου *Hilbert* [8]. Είναι ένας μετασχηματισμός που αποτελεί τη βάση για πολλούς κβαντικούς αλγορίθμους. Συνοπτικά μετασχηματίζει μια συνάρτηση από το πεδίο ορισμού του χρόνου (*timedomain*), στο πεδίο ορισμού της συχνότητας (*frequencydomain*), δηλαδή συναρτήσεις με περίοδο  $r$  σε συναρτήσεις που οι μη μηδενικές τιμές τους είναι μόνο τα πολλαπλάσια της συχνότητας  $\frac{1}{r}$  [4].

Το αμέσως επόμενο ερώτημα που προκύπτει αφορά το πως είναι εφικτό ο *QFT* να έχει χρόνο μικρότερο από  $M$  που είναι το μήκος της εισόδου. Για να είναι εφικτό, κωδικοποιούμε την είσοδο σε μια υπέρθεση μεγέθους  $m = \log M$  qubits. Η υπέρθεση αυτή αποτελείται από  $2^m$  τιμές πλάτους. Θα μπορούσαμε να γράψουμε την υπέρθεση με τον εξής τρόπο:  $|\alpha\rangle =$

$\sum_{j=0}^{M-1} \alpha_j |j\rangle$ , όπου το  $\alpha_i$  είναι το εύρος της δυαδικής συμβολοσειράς  $m - \text{bit}$  που αντιστοιχεί στο  $i$  με τον φυσικό τρόπο. Αυτό μας οδηγεί σε ένα βασικό σημείο: το  $|j\rangle$  είναι επί της ουσίας ένας διαφορετικός τρόπος γραφής ενός διανύσματος, όπου ο δείκτης κάθε καταχώρησης γράφεται στο ειδικό σύμβολο της αγκύλης. Ξεκινώντας από την υπέρθεση  $|\alpha\rangle$ , ο  $QFT$  τρέχει σε  $m = \log M$  βήματα. Σε κάθε βήμα, η υπέρθεση εξελίσσεται έτσι ώστε να κωδικοποιεί τα ενδιάμεσα στάδια το ίδιο με τον κλασσικό  $FFT$ . Αυτό μπορεί να επιτευχθεί με  $m$  κβαντικές διεργασίες σε κάθε στάδιο. Επομένως, μετά από  $m$  τέτοια στάδια και  $m^2 = \log^2 M$  βασικές διεργασίες, καταλήγουμε στην υπέρθεση  $|\beta\rangle$  που ανταποκρίνεται στο επιθυμητό αποτέλεσμα του  $QFT$ .

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

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

**Method:** Using  $O(m^2) = O(\log^2 M)$  quantum operations perform the quantum FFT to obtain the superposition  $|\beta\rangle = \sum_j \beta_j |j\rangle$ .

**Output:** A random  $m$ -bit number  $j$ , from the probability distribution  $Pr[j] = |\beta_j|^2$ .

Ο κβαντικός μετασχηματισμός *Fourier* ορίζεται σε μια ορθοκανονική βάση  $|0\rangle, \dots, |N\rangle$  ως εξής [7]:

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

και άρα γράφεται:

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

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

$$|j_1, \dots, j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i 0 \cdot j_1} |1\rangle)(|0\rangle + e^{2\pi i 0 \cdot j_1 j_n} |1\rangle) \dots (|0\rangle + e^{2\pi i 0 \cdot j_1 j_2 \dots j_n} |1\rangle)}{2^{\frac{n}{2}}}$$

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

$$|j\rangle \rightarrow \frac{1}{2^{\frac{n}{2}}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i j k}{2^n}} |k\rangle \quad (5.1)$$

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

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

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

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

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

Και βλέπουμε ότι όντως ο  $QFT$  είναι *unitary*.

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

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

Ο κβαντικός μετασχηματισμός της υπέρθεσης, δίνεται από το παρακάτω:

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

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

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

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

**Παράδειγμα 5.1.** Η επίδραση του  $QFT$  σε ένα  $qubit$ .

Αρχικά υποθέτουμε ότι το  $qubit$  βρίσκεται στην κατάσταση  $|0\rangle$ . Άρα σύμφωνα με τα παραπάνω:

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

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

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

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

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

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

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

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

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

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

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

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

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

Ο  $QFT$  μας βοηθάει να βρίσκουμε με ευκολία την περίοδο μιας περιοδικής συνάρτησης. Σε έναν κβαντικό καταχωρητή μεγέθους  $qbits$ , που βρίσκεται σε υπέρθεση περιοδικών καταστάσεων περιόδου  $r$ , με τον  $QFT$  στον κβαντικό καταχωρητή θα μείνουν μόνο οι τιμές που είναι πολλαπλάσια του  $\frac{q}{r}$ . Αυτά τα πολλαπλάσια είναι ισοπίθανα άρα μια μέτρηση θα μας επιστρέψει ένα από αυτά. [5].

Προσπαθώντας να συνοψίσουμε κάπως όλα τα παραπάνω, ο κλασικός γρήγορος μετασχηματισμός *Fourier* ( $FFT$ ) έχει πλοποκότητα  $O(N \log N) = O(2^n n)$  με  $N = 2^n$ , είναι δηλαδή

πολύ γρήγορος. Ωστόσο ο κβαντικός μετασχηματισμός *Fourier* είναι ακόμα πιο γρήγορος με πολυπλοκότητα  $O(\log^2 N) - O(n^2)$  [2].

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

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

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

### 5.3.1 Περιοδικότητα

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

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

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

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

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

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

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

Ο μόνος τρόπος για να μην συμβεί αυτό, είναι όλα τα δείγματα να είναι πολλαπλάσια του  $j \cdot \frac{M}{k}$ , όπου το  $j$  είναι ακέραιος μεγαλύτερος του 1. Η πιθανότητα ένα τυχαίο δείγμα να είναι πολλαπλάσιο του  $j \cdot \frac{M}{k}$  είναι το πολύ  $\frac{1}{j} \leq \frac{1}{2}$  και η πιθανότητα να είναι όλα τα δείγματα πολλαπλάσια του  $j \cdot \frac{M}{k}$  είναι το μέγιστο  $\frac{1}{2^s}$ . Όλα αυτά ισχύουν για συγκεκριμένο αριθμό  $j$ . Η

πιθανότητα αυτό να συμβεί για μερικά  $j$ , όπου  $j \leq k$  είναι το πολύ ίση με το άθροισμα όλων αυτών των πιθανοτήτων πάνω από τις διαφορετικές τιμές του  $j$ , που δεν είναι περισσότερες από  $\frac{k}{2^s}$ . Μπορούμε να μειώσουμε την πιθανότητα αποτυχίας επιλέγοντας το  $s$  έτσι ώστε να είναι κατάλληλο πολλαπλάσιο του  $\log M$ . Όπως είδαμε αναλυτικά παραπάνω, ο διακριτός μετασχηματισμός *Fourier* έχει σαν είσοδο ένα διάνυσμα μιγαδικών αριθμών  $(x_0, \dots, x_N - 1)$ , όπου  $N$  είναι το μήκος τους διανύσματος. Η έξοδος μετά τη μετατροπή που εφαρμόζει ο αλγόριθμος είναι ένα διάνυσμα  $y_0, \dots, y_N - 1$ , το οποίο ορίζεται ως εξής:

Ο κβαντικός μετασχηματισμός *Fourier*,

## Κεφάλαιο 6

# The Shor's Code

### 6.1 Quantum error-correction





## Κεφάλαιο 7

# RSA Cryptosystem



## Κεφάλαιο 8

# Future Work/What's Happening Now



## Κεφάλαιο 9

## Summary



## Παράρτημα Α΄

# Παράδειγμα Παραρτήματος

Α΄.1 Πρώτη ενότητα

Α΄.2 Μελλοντικές Επεκτάσεις





# Βιβλιογραφία

- [1] Fast fourier transform,  $\chi\cdot\chi$ .
- [2] Dawar Anuj. Quantum computing (lectures - university of cambridge), 2007-2008.
- [3] John Stewart Bell. On the Einstein Podolsky Rosen paradox. *Physics*, 1(3):195–200, 1964.
- [4] Cristian S. Calude και Gheorghe Păun. *Computing with Cells and Atoms: An Introduction to Quantum, DNA and Membrane Computing*. Taylor & Francis/Hemisphere, Bristol, PA, USA, 2001.
- [5] Sanjoy Dasgupta, Christos H. Papadimitriou και Umesh V. Vazirani. *Algorithms*. McGraw-Hill, 2008.
- [6] Phillip Kaye, Raymond Laflamme και Michele Mosca. *An Introduction to Quantum Computing*. Oxford University Press, Inc., New York, NY, USA, 2007.
- [7] Michael A. Nielsen και Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10την έκδοση, 2011.
- [8] Riley T. Perry. *The Temple of Quantum Computing*. 2006.



# Συντομογραφίες - Αρκτικόλεξα - - Ακρωνύμια

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



# Απόδοση ξενόγλωσσων όρων

## Απόδοση

αδερφός  
αμεταβλητότητα  
ανάκτηση πληροφορίας  
αντιμεταθετικότητα  
απόγονος  
απορρόφηση  
βάση δεδομένων  
γνώρισμα  
διαπροσωπεία  
διαφορά  
δικτυακός κατάλογος  
δικτυωτή δομή  
δομικές επερωτήσεις  
δομικές σχέσεις  
δομικό σχήμα  
εγκυρότητα  
ένωση

## Ξενόγλωσσος όρος

sibling  
idempotency  
information retrieval  
commutativity  
descendant  
absorption  
database  
attribute  
interface  
difference  
portal catalog  
lattice  
structural queries  
structural relationships  
schema  
validity  
union











ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ  
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ  
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**Πρότυπο Σύστημα Ομότιμων  
Κόμβων Βασισμένο σε Σχήματα RDF**

**Κωνσταντίνος Δ. Δημητρίου**

ΑΘΗΝΑ  
ΟΚΤΩΒΡΙΟΣ 2014



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ  
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ  
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**Πρότυπο Σύστημα Ομότιμων  
Κόμβων Βασισμένο σε Σχήματα RDF**

**Κωνσταντίνος Δ. Δημητρίου**

ΑΘΗΝΑ  
ΟΚΤΩΒΡΙΟΣ 2014

