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

Τίτλος Διπλωματικής

Διπλωματικη Εργασια

της

ΗΛΙΑΝΑΣ Θ. ΜΠΕΤΣΟΥ

Επιβλέπων: Επιβλέπων
Τίτλος

Αθήνα, Ιούνιος 2019

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

Τίτλος Διπλωματικής

Διπλωματικη Εργασια

της

ΗΛΙΑΝΑΣ Θ. ΜΠΕΤΣΟΥ

Επιβλέπων: Επιβλέπων
Τίτλος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την Ημερομηνία Παρουσίασης.

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

Αθήνα, Ιούνιος 2019

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

Υπεύθυνη Δήλωση

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

(Υπογραφή)

.....
Ηλιάνα Μπέτσου

Περίληψη

Λέξεις Κλειδιά

Abstract

Keywords

Αφιέρωση

Ευχαριστίες

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

Περιεχόμενα

Κεφάλαιο 1

Introduction and Overview

1.1 History

1.2 Future Directions

Κεφάλαιο 2

Fundamentals

2.1 Overview

2.2 Quantum Computation

2.2.1 Qubits

2.2.2 Quantum Circuits

2.3 The Dirac notation nad Hilbert spaces

2.4 Quantum Circuits

2.4.1 The quantum Circuit model

2.4.2 Quantum Gates

2.4.3 Universal Quantum Gates

Κεφάλαιο 3

Introduction to Computer Science

3.1 Overview

3.2 Turing Machines

3.3 Computanional Complexity

3.4 Problems in classes P and NP

Κεφάλαιο 4

Quantum Algorithms

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. Η κυριότερη είναι η ιδιότητα των πολυωνύμων να χαρακτηρίζονται με δύο διαφορετικές μορφές.
Το πολυώνυμο $A(x)$ μπορεί να χαρακτηριστεί με τους εξής δύο τρόπους:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Συνοπτικά ο FFT έχει ώς εξής:

Fast Fourier Transform

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

5.2 Κβαντική Διεμπλοκή

Η κβαντική διεμπλοκή έχει τις ρίζες της σε ένα άρθρο των A. Einstein, B. Podolsky και N. Rosen [2]. Ο σκοπός του άρθρου ήταν να αποδείξουν ότι η κβαντική μηχανική δεν είναι μια πλήρης φυσική θεωρία, αλλά ότι από την κβαντική περιγραφή της φύσης λείπουν κάποιες παράμετροι. Αργότερα οι παράμετροι αυτές ονομάστηκαν ¨κρυμμένες μεταβλητές¨. Σαν μοντέλο για την απόδειξη τους, χρησιμοποίησαν ένα θεωρητικό πείραμα στο οποίο δύο κβαντικλα συστήματα, αφού αλληλεπιδράσουν μεταξύ τους απομακρύνονται το ένα από το άλλο. Τα δύο αυτά κβαντικά συστήματα παραμένουν διασυνδεδεμένα το ένα με το άλλο με έναν άγνωστο μη κλασσικό τρόπο. Αυτό έχει σαν αποτέλεσμα η μέτρηση μιας φυσικής ποσότητας του ενός, καθορίζει το αποτέλεσμα της μέτρησης της ίδιας φυσικής ποσότητας του άλλου. Το θεωρητικό αυτό πείραμα ονομάστηκε ¨παράδοξο EPR¨, από τα αρχικά των τριών ερευνητών. Η κβαντική διεμπλοκή είναι ίσως η πιο αινιγματική πλευρά της κβαντικής μηχανικής και δεν έχει κλασικό ανάλογο. Κάθε χρόνο πολλές δεκάδες άρθρα δημοσιεύονται σε επιστημονικά περιοδικά και περιγράφουν επιστημονικές εργασίες που έχουν ως στόχο την κατανόηση, το χειρισμό και τον υπολογισμό της κβαντικής διεμπλοκής. Για τους κβαντικούς υπολογιστές η κβαντική διεμπλοκή είναι ένας φυσικός πόρος, όπως η ενέργεια, τον οποίο μπορούμε να χρησιμοποιήσουμε για να εκτελέσουμε κβαντικούς υπολογισμούς και να αναπτύξουμε κβαντικούς αλγορίθμους [3]. 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.

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

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

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

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

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

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

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

και τελικά

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

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

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

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

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

5.2.1 Κβαντική Διεμπλοκή και Υπέρθεση

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

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

5.3 Quantum Fourier Transformation

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

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

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

,όπου το ω είναι η Μοστή μιγαδική ρίζα της μονάδας. Οι κλασσικές μέθοδοι θα χρειαζόταν χρόνο $O(M^2)$, ενώ ο γρήγορος μετασχηματισμός $Fourier(FFT)$, μπορεί να κάνει ακριβώς το ίδιο σε χρόνο $O(MlogM)$. Παρά την μεγάλη αύξηση στην ταχύτητα που προκαλεί ο FFT, ο κβαντικός μετασχηματισμός $Fourier$, (QFT), καταφέρνει να μειώσει και άλλο τον χρόνο εκτέλεσης εκθετικά φτάνοντας τον σε $O(log^2M)$. Το αμέσως επόμενο ερώτημα που προκύπτει αφορά το πως είναι εφικτό ο QFT να έχει χρόνο μικρότερο από M που είναι το μήκος της εισόδου. Για να είναι εφικτό, κωδικοποιούμε την είσοδο σε μια υπέρθεση μεγέθους $m = logM\ qubits$. Η υπέρθεση αυτή αποτελείται από 2^m τιμές πλάτους. Θα μπορούσαμε να γράψουμε την υπέρθεση με τον εξής τρόπο: $|\alpha\rangle = \sum_{j=0}^{M-1} \alpha_j |j\rangle$, όπου το α_i είναι το εύρος της δυαδικής συμβολοσειράς $m-bit$ που αντιστοιχεί στο i με τον φυσικό τρόπο. Αυτό μας οδηγεί σε ένα βασικό σημείο: το $|j\rangle$ είναι επί της ουσίας ένας διαφορετικός τρόπος γραφής ενός διανύσματος, όπου ο δείκτης κάθε καταχώρησης γράφεται στο ειδικό σύμβολο της αγκύλης. Ξεκινώντας από την υπέρθεση $|\alpha\rangle$, ο QFT τρέχει σε $m = logM$ βήματα. Σε κάθε βήμα, η υπέρθεση εξελίσσεται έτσι ώστε να κωδικοποιεί τα ενδιάμεσα στάδια το ίδιο με τον κλασσικό FFT. Αυτό μπορεί να επιτευχθεί με m 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.

Το αμέσως επόμενο ερώτημα που προκύπτει αφορά το πως είναι εφικτό ο QFT να έχει χρόνο μικρότερο από M που είναι το μήκος της εισόδου. Για να είναι εφικτό, κωδικοποιούμε την είσοδο σε μια υπέρθεση μεγέθους $m = logM\ qubits$. Η υπέρθεση αυτή αποτελείται από 2^m τιμές πλάτους. Θα μπορούσαμε να γράψουμε την υπέρθεση με τον εξής τρόπο: $|\alpha\rangle = \sum_{j=0}^{M-1} \alpha_j |j\rangle$, όπου το α_i είναι το εύρος της δυαδικής συμβολοσειράς $m - bit$ που αντιστοιχεί στο i με τον φυσικό τρόπο. Αυτό μας οδηγεί σε ένα βασικό σημείο: το $|j\rangle$ είναι επί της ουσίας ένας διαφορετικός τρόπος γραφής ενός διανύσματος, όπου ο δείκτης κάθε καταχώρησης γράφεται στο ειδικό σύμβολο της αγκύλης. Ξεκινώντας από την υπέρθεση $|\alpha\rangle$, ο QFT τρέχει σε $m = logM$ βήματα. Σε κάθε βήμα, η υπέρθεση εξελίσσεται έτσι ώστε να κωδικοποιεί τα ενδιάμεσα στάδια το ίδιο με τον κλασσικό FFT. Αυτό μπορεί να επιτευχθεί με m 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 $\beta_0, \beta_1, ..., \beta_{M-1}$. Αντίθετα ο QFT, επιστρέφει την υπέρθεση $\sum_{j=0}^{M-1} \beta |j\rangle$. Τα δεδομένα αυτά όμως δεν είναι προσβάσιμα σε εμάς. Έτσι λοιπόν ο μόνος τρόπος για να αξιοποιήσουμε το αποτέλεσμα, είναι μετρώντας το. Η μέτρηση της κατάστασης του συστήματος αποδίδει μόνο $m = logM$ κλασσικά $bits$. Πιο συγκεκριμένα, η έξοδος είναι ο δείκτης j με πιθανότητα $|\beta_j|^2$. Ο QFT μπορεί να εφαρμοστεί για αυθαίρετες τιμές του M και μπορούμε να τον συνοψίσουμε ως εξής:

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

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

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

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

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

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

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

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

Ο μόνος τρόπος για να μην συμβεί αυτό, είναι όλα τα δείγματα να είναι πολλαπλάσια του $j \cdot \frac{M}{k}$, όπου το j είναι ακέραιος μεγαλύτερος του 1. Η πιθανότητα ένα τυχαίο δείγμα να είναι πολλαπλάσιο του $j \cdot \frac{M}{k}$ είναι το πολύ $\frac{1}{j} \leq \frac{1}{2}$ και η πιθανότητα να είναι όλα τα δείγματα πολλαπλάσια του $j \cdot \frac{M}{k}$ είναι το μέγιστο $\frac{1}{2^s}$. Όλα αυτά ισχύουν για συγκεκριμένο αριθμό j. Η πιθανότητα αυτό να συμβεί για μερικά j, όπου $j \leq k$ είναι το πολύ ίση με το άθροισμα όλων αυτών των πιθανοτήτων πάνω από τις διαφορετικές τιμές του j, που δεν είναι περισσότερες από $\frac{k}{2^s}$. Μπορούμε να μειώσουμε την πιθανότητα αποτυχίας επιλέγοντας το s έτσι ώστε να είναι κατάλληλο πολλαπλάσιο του $logM$. Όπως είδαμε αναλυτικά παραπάνω, ο διακριτός μετασχηματισμός $Fourier$ έχει σαν είσοδο ένα διάνυσμα μιγαδικών αριθμών $(x_0, ..., x_N - 1)$, όπου N είναι το μήκος τους διανύσματος. Η έξοδος μετά τη μετατροπή που εφαρμόζει ο αλγόριθμος είναι ένα διάνυσμα $y_0, ..., y_N - 1$, 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, χ.χ.

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

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

Συντομογραφίες - Αρκτικόλεξα - - Ακρωνύμια

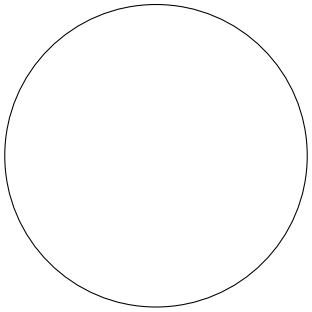
βλπ	βλέπε
κ.λπ.	και λοιπά
κ.ο.κ	και ούτω καθεξής
ΤΕΙ	Τεχνολογικό Εκπαιδευτικό Ίδρυμα
BPF	Band Pass Filter

Απόδοση ξενόγλωσσων όρων

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

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

Πρότυπο Σύστημα Ομότιμων Κόμβων Βασισμένο σε Σχήματα RDF



ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

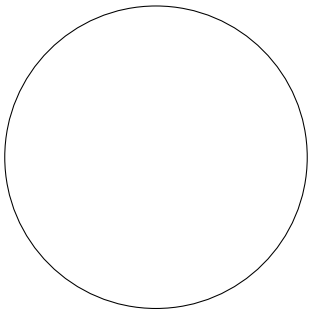
Κωνσταντίνος Δ. Δημητρίου

ΑΘΗΝΑ,
ΟΚΤΩΒΡΙΟΣ
2014

Θέση barcode

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

Πρότυπο Σύστημα Ομότιμων Κόμβων Βασισμένο σε Σχήματα RDF



ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κωνσταντίνος Δ. Δημητρίου

ΑΘΗΝΑ,
ΟΚΤΩΒΡΙΟΣ
2014

Θέση barcode

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Πρότυπο Σύστημα Ομότιμων Κόμβων Βασισμένο σε Σχήματα RDF

Κωνσταντίνος Δ. Δημητρίου

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2014

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Πρότυπο Σύστημα Ομότιμων Κόμβων Βασισμένο σε Σχήματα RDF

Κωνσταντίνος Δ. Δημητρίου

ΑΘΗΝΑ

ΟΚΤΩΒΡΙΟΣ 2014