ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Προσομοίωση και εκτέλεση κβαντικών αριθμητικών κυκλωμάτων σε κβαντικό υπολογιστή IBM-Q

Θεόδωρος Μαγκλάρας

Επιβλέπων:

Κουσουρής Κωνσταντίνος,
Αναπληρωτής Καθηγητής ΕΜΠ

Αθήνα, Σεπτέμβριος 2024

Ευχαριστίες

Θα ήθελα να ευχαριστήσω ιδιαίτερως τον κύριο Κωνσταντίνο Κουσουρή, Αναπληρωτή Καθηγητή στο ΕΜΠ, τόσο για τη θετική του διάθεση καθ' όλη τη διάρκεια της συνεργασίας μας, όσο και για την ανάθεση και την επίβλεψη της παρούσας Διπλωματικής Εργασίας. Θέλω, επίσης, να ευχαριστήσω από καρδιάς τον κύριο Χρήστο Μάρκου, Διευθυντή του ΙΠΣΦ-ΕΚΕΦΕ "Δημόκριτος", και τον κύριο Δάκη Παυλίδη, Ε.ΔΙ.Π. στο ΠΑ.ΠΕΙ. στο Τμήμα Πληροφορικής, για την ευκαιρία που μου έδωσαν να πραγματοποιήσω τη Διπλωματική μου Εργασία σε συνεργασία με το ΕΚΕΦΕ «Δημόκριτος» και να αποκομίσω πολύ σημαντική εμπειρία στα εργαστήρια και την επιστημονική ομάδα του Ινστιτούτου ΙΠΣΦ. Ευχαριστώ ολόψυχα τους γονείς και την οικογένειά μου για την απόλυτη και ουσιαστική στήριξή τους σε όλα μου τα βήματα καθ' όλη τη διάρκεια των σπουδών μου, αλλά και όλους εκείνους και εκείνες που όλα αυτά τα χρόνια με έκαναν να βλέπω την επιστήμη, τον κόσμο και την ίδια τη ζωή με άλλη ματιά.

Θεόδωρος Μαγκλάρας

Περίληψη

Το πρόβλημα της ανάπτυξης αλγορίθμων για την εκτέλεση αριθμητικών κυκλωμάτων σε κβαντικούς υπολογιστές αποτελεί ένα ταχέως εξελισσόμενο πεδίο, καθώς επιτρέπει την διεύρυνση των προβλημάτων και εφαρμογών που μπορούμε να διαχειριστούμε με τη βοήθεια των κβαντικών υπολογιστών, αλλά και αναδεικνύει σημαντικές πλευρές των φυσικών ιδιοτήτων των κβαντικών συστημάτων.

Ένα από αυτά τα προβλήματα είναι η δημιουργία αποδοτικών αλγορίθμων για την εκτέλεση απλών αριθμητικών πράξεων, όπως η πρόσθεση ή ο πολλαπλασιασμός με σταθερό αριθμό, με τρόπο που να ελαχιστοποιούνται οι απαιτούμενοι υπολογιστικοί πόροι. Αυτό μπορεί να επιτευχθεί με την ανάπτυξη αλγορίθμων που μειώνουν ή ακόμα και μηδενίζουν τον αριθμό των απαιτούμενων ancilla bits (βοηθητικών bits για την προσωρινή αποθήκευση πληροφορίας), ελαχιστοποιώντας, παράλληλα, το βάθος(depth) του κβαντικού κυκλώματος. Τύπος τέτοιων αλγορίθμων, με τους οποίους ασχολείται και η παρούσα Διπλωματική Εργασία, είναι οι αλγόριθμοι που βασίζονται επάνω στον Κβαντικό Μετασχηματισμό Fourier (Quantum Fourier Transform - QFT). Οι συγκεκριμένοι αλγόριθμοι έχουν τη δυνατότητα να εκτελούν τις συγκεκριμένες αριθμητικές πράξεις χωρίς την ανάγκη χρήσης ancilla bits και με γραμμική αύξηση της ποσότητας του βάθους, με αποτέλεσμα να μειώνουν σημαντικά τους απαιτούμενους πόρους. Παράλληλα, μπορούμε να αναπτύξουμε περαιτέρω αυτούς τους αλγορίθμους αξιοποιώντας διάφορες παραλλαγές τους, μέσω των οποίων μπορούμε να βελτιώσουμε σημαντικά τα αποτελέσματά μας. Σε επόμενα κεφάλαια θα παρουσιαστεί ο QFT που βασίζεται μόνο σε τοπικές αλληλεπιδράσεις μεταξύ των qubits, ο Banded QFT στον οποίο το κάθε qubit αλληλεπιδρά με συγκεκριμένο μόνο αριθμό γειτονικών qubits που ορίζει ο χρήστης, καθώς και το συνδυασμό τους.

Στο πρώτο τμήμα της Διπλωματικής Εργασίας παρουσιάζονται τα βασικά κβαντομηχανικά εργαλεία, τα οποία είναι απαραίτητα για την κατανόηση της λειτουργίας των κβαντικών υπολογιστών και την εκτέλεση κβαντικών αλγορίθμων, και βασικά σημεία θεωρίας σχετικά με βασικούς κβαντικούς αλγορίθμους. Στη συνέχεια, ακολουθεί αναλυτική μαθηματική επεξήγηση του QFT στην κανονική, αλλά και στις προλεχθείσες παραλλαγές του, έτσι ώστε να αναπτυχθεί ο αλγόριθμος για την εκτέλεση της μαθηματικής πράξης πολλαπλασιασμού με σταθερό αριθμό. Ακολουθούν τα αποτελέσματα που αποκτήθηκαν κατά την προσομοίωση των αποτελεσμάτων του κβαντικού κυκλώματος που δημιουργήθηκε με τη χρήση βιβλιοθήκης Qiskit και προσομοιωτών που παρέχονται και τα αποτελέσματα της εκτέλεσης του κβαντικού κυκλώματος σε πραγματικό κβαντικό υπολογιστή IBM-Q. Τα αποτελέσματα παρουσιάζονται αναλυτικά και ακολουθούν βασικά συμπεράσματα για την ακρίβεια και την αποδοτικότητα της συγκεκριμένης μεθόδου.

Abstract

The problem of developing algorithms for executing arithmetic circuits on quantum computers is a rapidly evolving field, as it allows the expansion of problems and applications that can be handled with the help of quantum computers, but also highlights important aspects of the physical properties of quantum systems.

One of these problems is to create efficient algorithms for performing simple arithmetic operations, such as addition or multiplication by a fixed number, in a way that minimizes the required computational resources. This can be achieved by developing algorithms that reduce or even eliminate the number of required ancilla bits (ancillary bits that temporarily store information), minimizing in the same time the depth of the quantum circuit. One type of such algorithms, with which this Diploma Thesis deals, are the algorithms based on the Quantum Fourier Transform (QFT).These algorithms have the ability to perform the specific arithmetic operations without the need to use ancilla bits and with a linear increase in the amount of depth, thus significantly reducing the required resources. At the same time, we can further develop these algorithms by using different variations of them, through which we can significantly improve our results. In subsequent chapters we will present QFT based only on local interactions between qubits, Banded QFT in which each qubit interacts with only a certain number of user-defined neighboring qubits, as well as their combination.

The first part of the Thesis presents the basic quantum mechanical tools, which are necessary for understanding the operation of quantum computers and the execution of quantum algorithms, and basic points of theory about basic quantum algorithms. Then follows a detailed mathematical explanation of the QFT in its original form, but also in its different variations that were metnioned before, so as to develop the algorithm for performing the mathematical operation of multiplication by a fixed number. The next part presents the results obtained by simulating the quantum circuits using the Qiskit library on simulators and the results of running the quantum circuit on a real IBM-Q quantum computer. The results are presented in detail, followed by basic conclusions about the accuracy and efficiency of this specific method.

Κατάλογος Σχημάτων

Περιεχόμενα

1 Βασικά Θεμέλια του Quantum Computing

1.1 Βασικές έννοιες των Qubits

Στην παρούσα Διπλωματική Εργασία θα γίνει επανειλημμένα η χρήση της έννοιας των qubits (Quantum Bits). Σε αυτήν την ενότητα θα παρουσιαστούν τα βασικά σημεία γύρω από τη φύση των qubits και των κβαντικών πυλών, μέσω των οποίων μπορούμε να επιδράμε στις καταστάσεις τους.

Προτού ορίσουμε τα qubits, είναι χρήσιμο να ορίσουμε κάποιες βασικές ποσότητες που θα χρησιμοποιήσουμε στη συνέχεια. Στην κβαντομηχανική τα ket $|0\rangle$ και $|1\rangle$ χρησιμοποιούνται για να περιγράψουν την υπολογιστική βάση ενός κβαντικού συστήματος. Μαθηματικά, αναπαριστούν τα παρακάτω διανύσματα-στήλες:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{και} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1}$$

Τα bra $\langle 0|$ και $\langle 1|$ είναι τα ανάστροφα διανύσματα των $|0\rangle$ και $|1\rangle$. Το γινόμενο (braket) ενός bra, έστω $|\varphi\rangle$, με ένα ket, έστω $|\psi\rangle$, συμβολίζεται ως $\langle\varphi|\psi\rangle$ και αντιστοιχεί στην πράξη του εσωτερικού γινομένου, δηλαδή έχει ως αποτέλεσμα μια βαθμωτή ποσότητα, στη γενική μορφή έναν μιγαδικό αριθμό. Το αντίστοιχο γινόμενο (ketbra) $|\varphi\rangle\langle\psi|$ είναι μια μαθηματική πράξη που δίνει ως αποτέλεσμα έναν πίνακα (ή τελεστή) και όχι βαθμωτό μέγεθος.

Περιγράφουμε το qubit ως ένα αφηρημένο μαθηματικό αντικείμενο με κάποιες συγκεκριμένες ιδιότητες. Αυτό, φυσικά, δεν σημαίνει ότι δεν αντιστοιχεί σε φυσικά συστήματα με συγκεκριμένες ιδιότητες, ωστόσο, στην παρούσα ενότητα θα ασχοληθούμε κυρίως με την αφηρημένη μαθηματική τους υπόσταση. Με αυτόν τον τρόπο, μπορούμε να δημιουργήσουμε μια γενική θεωρία για τους κβαντικούς υπολογισμούς και την επεξεργασία της κβαντικής πληροφορίας, η οποία δε θα εξαρτάται από κάποιο συγκεκριμένο σύστημα. Όπως το κλασσικό bit βρίσκεται σε μια κατάσταση -είτε 0 είτε 1- το qubit επίσης βρίσκεται σε μια κατάσταση, π.χ. $|0\rangle$, $|1\rangle$ [1]. Μπορούν, όμως, να περιγραφούν και από καταστάσεις που δεν εμπίπτουν σε αυτόν τον περιορισμό. Η κατάσταση μπορεί να περιγραφεί από μια κυματοσυνάρτηση $|\psi\rangle$, η οποία μπορεί να είναι οποιοδήποτε μοναδιαίο διάνυσμα στον 2-διάστατο μιγαδικό διανυσματικό χώρο με βάση $|0\rangle$ και $|1\rangle$ (υπολογιστική βάση). Η γενική κατάσταση ενός qubit είναι η

$$|\psi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \tag{2}$$

όπου τα α_0 και α_1 είναι δύο μιγαδικοί αριθμοί με μοναδικό περιορισμό την απαίτηση η κυματοσυνάρτηση $|\psi\rangle$ να είναι μοναδιαίο διάνυσμα στο μιγαδικό διανυσματικό χώρο, να ικανοποιείται, δηλαδή, η συνθήκη κανονικοποίησης

$$|\alpha_0|^2 + |\alpha_1|^2 = 1 \tag{3}$$

Η κατάσταση $|\psi\rangle$ δημιουργείται από την υπέρθεση των καταστάσεων $|0\rangle$ και $|1\rangle$ με πλάτη a_0 και a_1 αντίστοιχα. Η παραπάνω γενική περιγραφή μπορεί να επεκταθεί για να περιγράψει την κατάσταση 2 qubits ως μια οποιαδήποτε κανονικοποιημένη

$$|\psi\rangle = \alpha_{00}|0\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{4}$$

με τον ίδιο περιορισμό για τα πλάτη

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \tag{5}$$

Η γενική, επομένως, περιγραφή για n qubits, των οποίων η κατάσταση μπορεί να είναι οποιαδήποτε υπέρθεση των 2^n διαφορετικών κλασσικών καταστάσεων, με πλάτη των οποίων το τετραγωνικό άθροισμα ισούται με τη μονάδα, δίνεται από τη σχέση

$$|\psi\rangle = \sum_{0 \le n \le 2^n} |\alpha_x|^2 |x\rangle_n \text{ και ισχύει } \sum_{0 \le n \le 2^n} |\alpha_x|^2 = 1 \tag{6}$$

1.2 Κβαντικές Πύλες

Ορίζουμε ως κβαντική πύλη 1-qubit (1-qubit Quantum Gate) κάθε μοναδιαίο τελεστή που δρα επάνω σε ένα 2-διάστατο κβαντικό σύστημα [2]. Κάποιες από τις βασικές κβαντικές πύλες που χρησιμοποιούμε είναι οι

a) **Πύλη NOT και πύλες Pauli**

$\begin{pmatrix}1\\0\end{pmatrix} \to \begin{pmatrix}0\\1\end{pmatrix}$ που αντιστοιχεί στον πίνακα $\begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$

$\sigma_0 \equiv I \equiv \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$, $\sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$,

$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix}0 & -i\\i & 0\end{bmatrix}$, $\sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}$

Η πύλη NOT συχνά προσδιορίζεται με το σύμβολο X και είναι μία από τις 4 πύλες Pauli. Επίσης, για τις πύλες Pauli ισχύει ότι $X^2 = Y^2 = Z^2 = I$

b) **Πίνακες Περιστροφής**

Με βάση τους πίνακες Pauli μπορούμε να ορίσουμε τους πίνακες στροφής:

$R_x(\theta) \equiv e^{\frac{-i\theta X}{2}} \equiv \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} X$, με πίνακα $R_x(\theta) = \begin{bmatrix}\cos\frac{\theta}{2} & -i\sin\frac{\theta}{2}\\-i\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}$

$R_y(\theta) \equiv e^{\frac{-i\theta Y}{2}} \equiv \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} Y$, με πίνακα $R_y(\theta) = \begin{bmatrix}\cos\frac{\theta}{2} & -\sin\frac{\theta}{2}\\\sin\frac{\theta}{2} & \cos\frac{\theta}{2}\end{bmatrix}$

$R_z(\theta) \equiv e^{\frac{-i\theta Z}{2}} \equiv \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z$, με πίνακα $R_z(\theta) = \begin{bmatrix} e^{\frac{-i\theta}{2}} & 0 \\ 0 & e^{\frac{i\theta}{2}} \end{bmatrix}$

c) **Πύλη Hadamard**

$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, με πίνακα $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

Για την πύλη Hadamard ισχύει, επίσης, η ιδιότητα $H^2 = I$

d) **Phase P**

$|0\rangle \to |0\rangle$, $|1\rangle \to e^{i\theta} |1\rangle$, με πίνακα $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix} = e^{i\frac{\theta}{2}} * R_z(\theta)$

Οι μοναδιαίες 1-qubit κβαντικές πύλες U μετατρέπουν μια κβαντική κατάσταση $|\psi\rangle$ σε μια άλλη κβαντική κατάσταση U$|\psi\rangle$. Για κάθε 1-qubit πύλη U, μπορούμε να ορίσουμε την controlled-U πύλη, που συμβολίζεται με C-U, η οποία θα είναι μια 2-qubit πύλη που αντιστοιχεί στην ακόλουθη διαδικασία

C-U $|0\rangle |\psi\rangle \to |0\rangle |\psi\rangle$, C-U $|1\rangle |\psi\rangle \to |1\rangle U |\psi\rangle$ [2]

Στη συγκεκριμένα εργασία θα χρησιμοποιήσουμε επανειλημμένα τις πύλες C-Phase οι οποίες αποτελούν βασικό συστατικό του μετασχηματισμού QFT, καθώς και τις πύλες C-NOT για να δημιουργήσουμε κβαντικά κυκλώματα με αμιγώς τοπικές αλληλεπιδράσεις.

e) **Controlled-Phase Πύλες**

C-Phase $= I \otimes |0\rangle \langle 0| + P \otimes |1\rangle \langle 1| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{bmatrix}$

f) **Controlled-NOT Πύλες**

C-NOT $= I \otimes |0\rangle \langle 0| + NOT \otimes |1\rangle \langle 1| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$

2 Κβαντικοί Αλγόριθμοι

Ένα κρίσιμο ερώτημα είναι τί είδους υπολογισμούς μπορούμε να πραγματοποιήσουμε χρησιμοποιώντας κβαντικά κυκλώματα και ποια είναι η απόδοσή τους συγκριτικά με τα κλασσικά λογικά κυκλώματα. Το ενδιαφέρον γύρω από τους κβαντικούς υπολογιστές σχετίζεται άμεσα με την ικανότητά τους να ολοκληρώνουν εργασίες με καλύτερο και πιο αποτελεσματικό τρόπο σε σχέση με τους κλασσικούς υπολογιστές. Σε αυτήν την ενότητα, θα δοθούν μερικά επιχειρήματα που τεκμηριώνουν την συγκριτική ικανότητα των κβαντικών υπολογιστών, καθώς και μερικά παραδείγματα προβλημάτων στα οποία παρατηρείται υψηλότερη απόδοση.

2.1 Κλασσικοί υπολογισμοί στον κβαντικό υπολογιστή

Όπως είναι αναμενόμενο, μπορούμε να προσομοιώσουμε κλασσικά λογικά κυκλώματα χρησιμοποιώντας κβαντικά κυκλώματα. Ο λόγος, ωστόσο, που που τα κβαντικά κυκλώματα δεν μπορούν να χρησιμοποιηθούν απευθείας για προσομοίωση κλασσικών κυκλωμάτων είναι, διότι οι μοναδιαίες κβαντικές λογικές πύλες είναι δομικά αντιστρεπτές [2], ενώ πολλές κλασσικές πύλες, όπως η NAND, είναι δομικά μη-αντιστρεπτές [1].

Οποιοδήποτε κλασσικό κύκλωμα μπορεί να αντικατασταθεί από ένα αντίστοιχο κύκλωμα που αποτελείται μόνο από αντιστρεπτά στοιχεία χρησιμοποιώντας μια αντιστρεπτή πύλη που είναι γνωστή ως πύλη Toffoli [1]. Η πύλη Toffoli έχει ως είσοδο τρία bits και ως έξοδο επίσης τρία bits. Δύο από τα bits λειτουργούν ως bits-ελέγχου (control bits), τα οποία μένουν ανεπηρέαστα από τη δράση της πύλης Toffoli. Το τρίτο bit είναι bit-στόχος (target bit) το οποίο αλλάζει τιμή εάν και τα δύο control bits έχουν τιμή ίση με 1, και σε αντίθετη περίπτωση δεν υφίσταται καμία μεταβολή [3]. Παρατηρούμε, ότι εφαρμόζοντας την πύλη Toffoli δύο φορές σε ένα σύνολο από bits έχει το εξής αποτέλεσμα

$$(a, b, c) \rightarrow (a, b, c \oplus ab) \rightarrow (a, b, c)$$

και, άρα, η πύλη Toffoli είναι μια αντιστρεπτή πύλη καθώς είναι η ίδια αντίστροφη του εαυτού της.

Η πύλη Toffoli μπορεί να χρησιμοποιηθεί για να προσομοιώσει τις πύλες NAND, όπως φαίνεται στο παραπάνω σχήμα, αλλά και άλλες διεργασίες, όπως τη FANOUT. Με αυτές τις δύο λειτουργίες είναι εφικτό να προσομοιώσουμε όλα τα άλλα στοιχεία ενός κλασσικού κυκλώματος, και άρα ένα οποιοδήποτε κλασσικό κύκλωμα μπορεί να προσομοιωθεί από ένα ισοδύναμο αντιστρεπτό κύκλωμα [3].

Παρά το γεγονός ότι περιγράφηκε ως μια κλασσική πύλη, η πύλη Toffoli μπορεί να εφαρμοστεί και ως κβαντική πύλη. Εξ' ορισμού, η κβαντική λογική εφαρμογή της πύλης Toffoli απλώς μεταθέτει τις καταστάσεις της υπολογιστικής βάσης με τον ίδιο τρόπο που το κάνει η κλασσική πύλη Toffoli. Για παράδειγμα, μία κβαντική πύλη Toffoli η οποία δρα επάνω στην κατάσταση $|110\rangle$κάνει flip στην τιμή του τρίτου qubit δημιουργώντας την κατάσταση $|111\rangle$. Η κβαντική πύλη Toffoli μπορεί να χρησιμοποιηθεί για να προσομοιώσουμε μη-αντιστρεπτές κλασσικές

Inputs			Ouputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

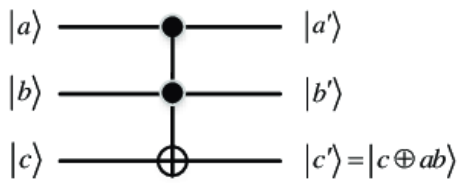


Figure 1: Πίνακας αληθείας και κύκλωμα πύλης Toffoli [4]

λογικές πύλες με τρόπο αντίστοιχο της κλασσικής και εξασφαλίζει ότι οι κβαντικοί υπολογιστές είναι ικανοί να πραγματοποιήσουν οποιοδήποτε υπολογισμό που μπορεί να πραγματοποιηθεί από κλασσικό υπολογιστή.

Οι κβαντικοί υπολογιστές, επίσης, έχουν τη δυνατότητα να προσομοιώσουν αποτελεσματικά μη-ντετερμινιστικούς κλασσικούς υπολογιστές, δηλαδή υπολογιστές που έχουν τη δυνατότητα να δημιουργούν τυχαία bits για την εκτέλεση υπολογισμών. Για να διεξάγει τέτοιες προσομοιώσεις, ο κβαντικός υπολογιστής παράγει «τυχαίες ρίψεις δίκαιου κέρματος» («random fair coin tosses»), το οποίο μπορεί να συμβεί προετοιμάζοντας ένα qubit στην κατάσταση $|0\rangle$, στέλνοντας το μέσα από μια πύλη Hadamard για να παράγουμε την κατάσταση $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ και μετά μετρώντας την κατάσταση. Το αποτέλεσμα θα είναι είτε $|0\rangle$ είτε $|1\rangle$ με πιθανότητα 50/50.

Φυσικά, η ικανότητα των κβαντικών υπολογιστών να προσομοιώνουν αποτελεσματικά κλασσικούς υπολογιστές δεν αρκεί για να αιτιολογήσει το μεγάλο επιστημονικό ενδιαφέρον για τη λειτουργία τους. Το πλεονέκτημά τους έγκειται στο γεγονός, ότι μπορούν να υπολογίσουν πολύ πιο περίπλοκες συναρτήσεις χρησιμοποιώντας qubits και κβαντικές πύλες.

2.2 Κβαντικός παραλληλισμός (quantum parallelism)

Ο κβαντικός παραλληλισμός είναι θεμελιώδες στοιχείο σε πολλούς κβαντικούς αλγορίθμους. Επιτρέπει οι κβαντικοί υπολογιστές να εκτιμούν μια συνάρτηση f(x) για πολλές διαφορετικές τιμές του x συγχρόνως [3].

Ας υποθέσουμε, ότι έχουμε μια συνάρτηση $f(x) : \{0,1\} \rightarrow \{0,1\}$.Ένας βολικός τρόπος να υπολογίσουμε αυτήν τη συνάρτηση σε έναν κβαντικό υπολογιστή είναι να θεωρήσουμε έναν υπολογιστή δύο qubits που ξεκινά από την κατάσταση $|x, y\rangle$. Με μια σωστή ακολουθία κβαντικών πυλών είναι εφικτό να μετασχηματίσουμε αυτήν την κατάσταση στην κατάσταση $|x, y \oplus f(x)\rangle$, όπου το $\oplus$ συμβολίζει την πρόσθεση modulo 2 και αντιστοιχεί στη δράση της πύλης XOR. Ο πρώτος καταχωρητής ονομάζεται καταχωρητής «δεδομένων» και ο δεύτερος καταχωρητής «στόχου». Δίνουμε στον μετασχηματισμό που ορίζεται από την απεικόνιση $|x, y\rangle$

$\rightarrow |x, y \oplus f(x)\rangle$ το όνομα U_f, ο οποίος εύκολα δείχνεται ότι είναι μοναδιαίος. Εάν $y = 0$, τότε η τελική κατάσταση του δεύτερου qubit είναι απλά η τιμή $f(x)$.

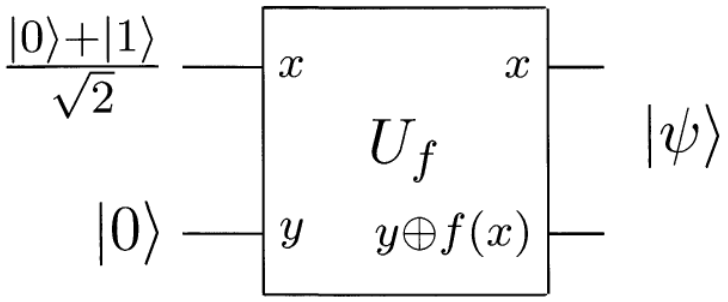


Figure 2: Κβαντικό κύκλωμα για τον υπολογισμό του f(0) και του f(1) συγχρόνως [3]

Ας θεωρήσουμε το κύκλωμα του παραπάνω σχήματος, το οποίο εφαρμόζει το μετασχηματισμό U_f σε μια είσοδο που είναι διαφορετική από την υπολογιστική βάση. Αντίθετα, ο καταχωρητής εισόδου προετοιμάζεται στην υπέρθεση $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, η οποία μπορεί να προκύψει με τη δράση μιας πύλης Hadamard επάνω στην κατάσταση $|0\rangle$. Η είσοδος στον μετασχηματισμό U_f θα είναι η κατάσταση

$$(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)|0\rangle = \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|0\rangle \quad (7)$$

Η έξοδος του U_f θα είναι η κατάσταση

$$U_f(\frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|0\rangle) = \frac{1}{\sqrt{2}}U_f|0\rangle|0\rangle + \frac{1}{\sqrt{2}}U_f|1\rangle|0\rangle = \quad (8)$$

$$= \frac{1}{\sqrt{2}}|0\rangle|0 \oplus f(0)\rangle + \frac{1}{\sqrt{2}}|1\rangle|0 \oplus f(1)\rangle = \frac{1}{\sqrt{2}}[(|0\rangle|f(0)\rangle) + (|1\rangle|f(1)\rangle)] \quad (9)$$

Οι διαφορετικές καταστάσεις περιέχουν πληροφορίες και για την f(0) και για την f(1). Είναι σαν να έχουμε εκτιμήσει την τιμή f(x) για δύο τιμές του x συγχρόνως, χαρακτηριστικό που ονομάζεται κβαντικός παραλληλισμός. Σε αντίθεση με τον κλασσικό παραλληλισμό, όπου πολλά κυκλώματα το καθένα από τα οποία είναι φτιαγμένο για να υπολογίζει την f(x) εκτελούνται συγχρόνως, στην κβαντική περίπτωση ένα μόνο κύκλωμα χρησιμοποιείται για να εκτιμήσει την συνάρτηση για πολλαπλές τιμές του x συγχρόνως, αξιοποιώντας την ικανότητα του κβαντικού υπολογιστή να είναι σε υπέρθεση διαφορετικών καταστάσεων.

Αυτή η διαδικασία μπορεί να γενικευτεί σε συναρτήσεις αυθαίρετου αριθμού bits, χρησιμοποιώντας έναν γενικό τελεστή που είναι γνωστός ως μετασχηματισμός Hadamard ή μετασχηματισμός Walsh-Hadamard. Αυτός ο τελεστής είναι απλώς n πύλες Hadamard που δρουν παράλληλα σε n qubits. Για παράδειγμα,

στην περίπτωση n=2 και με τα qubits προετοιμασμένα στην κατάσταση $|0\rangle$, η έξοδος είναι η

$$(\frac{|0\rangle + |1\rangle}{\sqrt{2}})(\frac{|0\rangle + |1\rangle}{\sqrt{2}}) = \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} \tag{10}$$

Συμβολίζουμε ως $H^{\otimes 2}$ την παράλληλη δράση δύο πυλών Hadamard. Πιο γενικά, το αποτέλεσμα της εκτέλεσης του μετασχηματισμού Hadamard σε n qubits που αρχικά είναι όλα στην κατάσταση $|0\rangle$ είναι το

$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle$, όπου $x = 0...2^n - 1$

όπου το άθροισμα είναι επάνω σε όλες τις πιθανές τιμές του x και συμβολίζουμε αυτή τη διαδικασία ως $H^{\otimes n}$. Ο μετασχηματισμός Hadamard παράγει μια ίσοπίθανη υπέρθεση όλων των καταστάσεων υπολογιστικής βάσης και, επιπλέον, το κάνει αυτό με εξαιρετικά αποδοτικό τρόπο, παράγοντας υπέρθεση 2^n καταστάσεων χρησιμοποιώντας n πύλες.

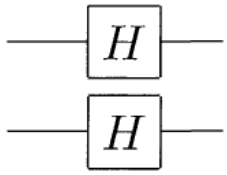


Figure 3: Ο μετασχηματισμός Hadamard $H^{\otimes 2}$ σε 2 qubits

Η εκτίμηση μιας συνάρτησης με είσοδο x από n bits και έξοδο f(x) ενός bit με κβαντικό παραλληλισμό μπορεί να γίνει με τον ακόλουθο τρόπο. Προετοιμάζουμε τα n+1 qubits στην κατάσταση $|0\rangle^{\otimes n} |0\rangle$, εφαρμόζουμε τον μετασχηματισμό Hadamard στα πρώτα n qubits και στη συνέχεια εφαρμόζουμε το κβαντικό κύκλωμα που αντιστοιχεί στο μετασχηματισμό U_f. Έτσι, παράγουμε την κατάσταση

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

Κατά κάποιον τρόπο, ο κβαντικός παραλληλισμός επιτρέπει όλες τις πιθανές τιμές της συνάρτησης f να εκτιμηθούν συγχρόνως, παρά το γεγονός ότι εκτιμάμε την f μόνο μια φορά. Ωστόσο, αυτός ο παραλληλισμός δεν είναι απευθείας χρήσιμος. Στο παράδειγμα του ενός qubit, η μέτρηση της κατάστασης πάνω στην υπολογιστική βάση θα έδινε είτε την κατάσταση $|0, f(0)\rangle$ με πιθανότητα 1/2 είτε την κατάσταση $|1, 1 \oplus f(1)\rangle$ με πιθανότητα 1/2. Μετά τη μέτρηση η κατάσταση θα ήταν είτε η $|f(0)\rangle$ είτε η $|f(1)\rangle$ και οποιαδήποτε επόμενη μέτρηση θα οδηγήσει στο ίδιο αποτέλεσμα. Αντίστοιχα στη γενική περίπτωση, η μέτρηση της κατάστασης

$\sum_x |x, f(x)\rangle$

θα μας δώσει την f(x) μόνο για μια τιμή του x. Απαιτείται, επομένως, κάτι περισσότερο από τον κβαντικό παραλληλισμό, χρειάζεται η δυνατότητα να μπορεί να εξαχθεί πληροφορία για περισσότερες της μιας τιμής του f(x) από τις καταστάσεις υπέρθεσης. Αυτό μπορεί να γίνει μέσω κβαντικών αλγορίθμων, όπως θα δούμε στη συνέχεια.

2.3 Είδη κβαντικών αλγορίθμων

Η υπόσχεση των κβαντικών υπολογιστών είναι ότι θα μπορούν να δώσουν λύση σε προβλήματα, τα οποία είναι αδύνατο να επιλυθούν στους κλασσικούς υπολογιστές όχι λόγω δομικών χαρακτηριστικών τους που τα καθιστούν μη-επιλύσιμα, αλλά εξαιτίας των τεράστιων υπολογιστικών πόρων που απαιτούνται. Με αυτό το σκοπό δημιουργούνται κβαντικοί αλγόριθμοι, οι οποίοι χωρίζονται σε δύο βασικές κλάσεις.

Η πρώτη κλάση αλγορίθμων βασίζεται επάνω στον QFT του Shor (Shor's QFT) και αποτελείται από αλγορίθμους που επιλύουν προβλήματα παραγοντοποίησης (factorizing) και διακριτού λογαρίθμου (discrete logarithm) παρέχοντας εκθετική αύξηση στην υπολογιστική ταχύτητα συγκριτικά με τους καλύτερους κλασσικούς αλγορίθμους. Η δεύτερη κλάση βασίζεται επάνω στον αλγόριθμο του Grover [1] για την πραγματοποίηση κβαντικής αναζήτησης (quantum searching). Και αυτοί οι αλγόριθμοι παρέχουν αξιοσημείωτη τετραγωνική αύξηση της υπολογιστικής ταχύτητας συγκριτικά με τους καλύτερους κλασσικούς. Οι αλγόριθμοι κβαντικής αναζήτησης αντλούν τη σημασία τους από τη διαδεδομένη χρήση αντίστοιχων τεχνικών στους κλασσικούς αλγορίθμους, το οποίο σε πολλές περιπτώσεις επιτρέπει την ευθεία προσαρμογή του κλασσικού αλγορίθμου σε ταχύτερο κβαντικό.

Ο QFT, με τον οποίο θα ασχοληθούμε αναλυτικά στην παρούσα εργασία, έχει πολλές ενδιαφέρουσες εφαρμογές. Μπορεί να χρησιμοποιηθεί, όπως ειπώθηκε και προηγουμένως, για να λύσουμε προβλήματα παραγοντοποίησης και διακριτού λογαρίθμου, τα αποτελέσματα των οποίων στη συνέχεια επιτρέπουν στον κβαντικό υπολογιστή να «σπάσει» πολλά από τα πιο δημοφιλή κρυπτοσυστήματα, συμπεριλαμβανομένου και του RSA [2]. Επίσης, ο QFT συνδέεται άμεσα με ένα σημαντικό μαθηματικό πρόβλημα, αυτό της εύρεσης μιας κρυμμένης υποομάδας που είναι γενίκευση της εύρεσης της περιόδου μιας περιοδικής συνάρτησης.

Αντίστοιχα, οι κβαντικοί αλγόριθμοι αναζήτησης έχουν πολλές πιθανές εφαρμογές. Μπορούν να χρησιμοποιηθούν για να εξαχθούν στατιστικά δεδομένα, όπως το ελάχιστο στοιχείο ενός μη-διατεταγμένου συνόλου. Μπορούν, επίσης, να χρησιμοποιηθούν για την επιτάχυνση αλγορίθμων που προορίζονται για NP(Nondeterministic, Polynomial Time, προβλήματα δηλαδή στα οποία η επιβεβαίωση της ορθότητας ενός αποτελέσματος απαιτεί πολυωνυμικό χρόνο). Τέλος, μπορούν να χρησιμοποιηθούν για την επιτάχυνση της αναζήτησης κλειδιών (keys) κρυπτοσυστημάτων, όπως το Data Encryption Standard (DES) [3].

Ο αριθμός των κβαντικών αλγορίθμων που γνωρίζουμε ότι έχουν πλεονέκτημα σε σχέση με τους κλασσικούς μοιάζει σε πρώτη ανάλυση αρκετά μικρός. Η

δυσκολία δημιουργίας τέτοιων αλγορίθμων οφείλεται σε δύο κατά βάση λόγους. Ο πρώτος σχετίζεται με την εγγενή δυσκολία κατασκευής αλγορίθμων είτε κλασσικών είτε κβαντικών, καθώς είναι μια πολύ απαιτητική διαδικασία που απαιτεί ευφυία και εφευρετικότητα ακόμα και για προβλήματα που φαίνονται ιδιαίτερα απλά, όπως ο πολλαπλασιασμός δύο αριθμών. Η κατασκευή κβαντικών αλγορίθμων είναι ακόμα δυσκολότερη, καθώς προστίθεται η επιπρόσθετη δυσκολία κατασκευής αλγορίθμων που θα είναι καλύτεροι και πιο αποδοτικοί από τους καλύτερους μέχρι τώρα γνωστούς κλασσικούς αλγορίθμους. Ο δεύτερος λόγος σχετίζεται με το γεγονός ότι η ανθρώπινη διαίσθηση είναι πολύ καλύτερα προσαρμοσμένη στα κλασσικά προβλήματα σε σχέση με τα κβαντικά. Η διαισθητική προσέγγιση των προβλημάτων οδηγεί τις περισσότερες φορές στη δημιουργία κλασσικών αλγορίθμων, για αυτό και η δημιουργία κβαντικών αλγορίθμων απαιτεί βαθιά γνώση και ειδικές τεχνικές.

3 Ο αλγόριθμος του Deutsch

Με βάση τα παραπάνω θα εξετάσουμε έναν πρώτο κβαντικό αλγόριθμο, τον αλγόριθμο Deutsch [1][2], καθώς είναι ένα πολύ καλό παράδειγμα κβαντικού αλγορίθμου που βασίζεται επάνω στον QFT. Αυτό, διότι παρά το γεγονός ότι είναι απλός και εύκολος στην κατανόηση αναδεικνύει τις βασικές ιδέες του κβαντικού παραλληλισμού και της κβαντικής παρεμβολής που, όπως αναφέρθηκε προηγουμένως, είναι ιδιαίτερα χρήσιμες σε όλους τους κβαντικούς αλγορίθμους.

Ας επιστρέψουμε στο αρχικό πρόβλημα του κβαντικού παραλληλισμού. Υποθέτουμε, ότι έχουμε μια συνάρτηση $f(x) : \{0,1\} \to \{0,1\}$ και θέλουμε να υπολογίσουμε την τιμή της ποσότητας $f(0) \oplus f(1)$. Υπενθυμίζεται, ότι αν $f(0) \oplus f(1) = 0$, τότε γνωρίζουμε ότι $f(0) = f(1)$ (χωρίς να γνωρίζουμε την συγκεκριμένη τιμή) και η f είναι σταθερή. Αν, όμως, $f(0) \oplus f(1) = 1$, τότε γνωρίζουμε ότι $f(0) \neq f(1)$ και η συνάρτηση είναι ισορροπημένη. Επομένως, ο καθορισμός της τιμής της ποσότητας $f(0) \oplus f(1)$ είναι ισοδύναμος με τον καθορισμό της συνάρτησης f ως σταθερή ή ισορροπημένη.

Ο αλγόριθμος Deutsch δείχνει πώς μπορούμε να εκμεταλλευτούμε την κβαντική παρεμβολή για να αποκτήσουμε παγκόσμια πληροφορία (global information) για την συνάρτηση f και το πώς αυτό μπορεί να γίνει πιο αποδοτικά από όσο είναι εφικτό κλασσικά. Το κύκλωμα που αντιστοιχεί στον αλγόριθμο φαίνεται στο παρακάτω σχήμα.

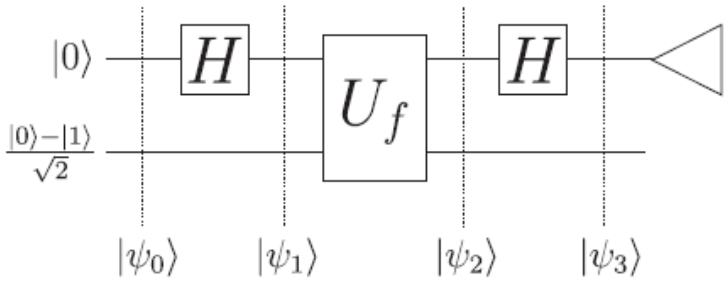


Figure 4: Κύκλωμα που υλοποιεί τον αλγόριθμο του Deutsch. Η μετρούμενη ποσότητα είναι ίση με $f(0) \oplus f(1)$ [2]

Αρχικά, το πρώτο qubit που βρίσκεται στην κατάσταση $|0\rangle$ προετοιμάζεται στην κατάσταση $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ με τη δράση μιας πύλης Hadamard και στη συνέχεια με τη δράση ενός μετασχηματισμού U_f [3]. Παρατηρούμε, ότι το δεύτερο bit εισόδου αρχικοποιείται στην κατάσταση $\frac{|0\rangle-|1\rangle}{2}$, η οποία μπορεί να δημιουργηθεί εύκολα εφαρμόζοντας μια πύλη Hadamard στην κατάσταση $|1\rangle$. Η δράση αυτής της πύλης Hadamard δεν φαίνεται στο παραπάνω σχήμα, ώστε να δοθεί έμφαση στη συμμετρία του κυκλώματος που είναι χαρακτηριστική αυτών των αλγορίθμων. Συνήθως, είναι βολικό να αναλύουμε τα κβαντικά κυκλώματα παρατηρώντας τις καταστάσεις των qubits σε κάθε στάδιο του κυκλώματος.

Πριν από αυτό, όμως, θα δείξουμε μια χρήσιμη σχέση. Προετοιμάζουμε τον

καταχωρητή στόχου στην κατάσταση $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ και αναλύουμε τη δράση του U_f επάνω σε μια αυθαίρετη βάση κατάστασης

$$U_f\,|x\rangle\,(\tfrac{|0\rangle-|1\rangle}{2}) \rightarrow (\tfrac{U_f|x\rangle|0\rangle-U_f|x\rangle|1\rangle}{\sqrt{2}}) = (\tfrac{|x\rangle|0\oplus f(x)\rangle-|x\rangle|1\oplus f(1)\rangle}{\sqrt{2}}) =$$

$$= |x\rangle\,(\frac{|0\oplus f(x)\rangle - |1\oplus f(1)\rangle}{\sqrt{2}}) \tag{11}$$

Γνωρίζουμε, ότι η δράση «$\oplus f(x)$» δεν έχει καμία επίδραση σε ένα bit εάν $f(x) = 0$ (π.χ. $a \oplus 0 = a$) και κάνει flip στην κατάστασή του εάν $f(x) = 1$. Ας θεωρήσουμε την έκφραση $\frac{1}{\sqrt{2}}(|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)$ για τις δύο περιπτώσεις $f(x) = 0$ και $f(x) = 1$

$$\text{f(x)} = 0 :\ \frac{|0\oplus f(x)\rangle - |1\oplus f(1)\rangle}{\sqrt{2}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{12}$$

$$\text{f(x)} = 1 :\ \frac{|0\oplus f(x)\rangle - |1\oplus f(1)\rangle}{\sqrt{2}} = \frac{|1\rangle - |0\rangle}{\sqrt{2}} = -(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{13}$$

Αυτές οι δύο πιθανότητες διαφέρουν κατά ένα παράγοντα -1, ο οποίος εξαρτάται από την τιμή της f(x). Επομένως, μπορούμε να γράψουμε

$$\frac{|0\oplus f(x)\rangle - |1\oplus f(1)\rangle}{\sqrt{2}} = (-1)^{f(x)}(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{14}$$

Επομένως, μπορούμε να γράψουμε την κατάσταση μετά τη δράση του U_f ως

$$|x\rangle\,(-1)^{f(x)}(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{15}$$

Συνδέοντας τον παράγοντα $(-1)^{f(x)}$ με το πρώτο qubit, παίρνουμε τη ζητούμενη σχέση

$$U_f\,|x\rangle\,(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \rightarrow (-1)^{f(x)}\,|x\rangle\,(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{16}$$

Αφού δείξαμε την παραπάνω σχέση, επιστρέφουμε στο κύκλωμα. Η κατάσταση εισόδου είναι η

$$|\psi_0\rangle = |0\rangle\,(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{17}$$

Μετά τη δράση της πρώτης πύλη Hadamard στο πρώτο qubit, η κατάσταση γίνεται

$$|\psi_1\rangle = (\frac{|0\rangle}{\sqrt{2}} + \frac{|1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \frac{|0\rangle}{\sqrt{2}}(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) + \frac{|1\rangle}{\sqrt{2}}(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{18}$$

Αξιοποιώντας τη σχέση που αποδείξαμε, μετά τη δράση της πύλης U_f έχουμε την κατάσταση

$$|\psi_2\rangle = \frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle\,(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) + \frac{(-1)^{f(1)}}{\sqrt{2}}|1\rangle\,(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{19}$$

$$= (\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) = \tag{20}$$

$$= (-1)^{f(0)}(\frac{|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{21}$$

όπου η τελευταία εξίσωση αξιοποιείται το γεγονός, ότι

$$(-1)^{f(0)}(-1)^{f(1)} = (-1)^{f(0)\oplus f(1)} \tag{22}$$

Εάν η f είναι σταθερή συνάρτηση, τότε έχουμε

$$|\psi_2\rangle = (-1)^{f(0)}(\frac{|0\rangle + |1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{23}$$

και άρα η τελική πύλη Hadamard στο πρώτο qubit μετασχηματίζει την κατάσταση στην

$$|\psi_3\rangle = (-1)^{f(0)}|0\rangle\,(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{24}$$

Η τετραγωνική νόρμα της βασικής κατάστασης $|0\rangle$ στο πρώτο qubit είναι ίση με 1. Αυτό σημαίνει, ότι για μια σταθερή συνάρτηση μια μέτρηση του πρώτου qubit είναι σίγουρο ότι θα επιστρέψει την τιμή $0 = f(0) \oplus f(1)$. Εάν η f είναι ισορροπημένη, τότε έχουμε για την κατάσταση $|\psi_2\rangle$

$$|\psi_2\rangle = (-1)^{f(0)}(\frac{|0\rangle - |1\rangle}{\sqrt{2}})(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{25}$$

και άρα η τελική πύλη Hadamard στο πρώτο qubit μετασχηματίζει την κατάσταση στην κατάσταση

$$|\psi_3\rangle = (-1)^{f(0)}|1\rangle\,(\frac{|0\rangle - |1\rangle}{\sqrt{2}}) \tag{26}$$

Σε αυτήν την περίπτωση, η τετραγωνική νόρμα της βασικής κατάστασης $|1\rangle$ του πρώτου qubit είναι ίση με 1. Αυτό σημαίνει, ότι για μια ισορροπημένη συνάρτηση μια μέτρηση του πρώτου qubit είναι σίγουρο ότι θα επιστρέψει την τιμή $1 = f(0) \oplus f(1)$. Άρα, μια μέτρηση του πρώτου qubit στο τέλος του κυκλώματος του αλγορίθμου Deutsch καθορίζει την τιμή $f(0) \oplus f(1)$ και άρα η συνάρτηση είναι σταθερή ή ισορροπημένη.

Μπορούμε να καταλάβουμε τον τρόπο με τον οποίο ο αλγόριθμος του Deutsch μπορεί να γενικευθεί, εάν θυμηθούμε ότι ο μετασχηματισμός $U_f\,|x, y\rangle \to |x, y \oplus f(x)\rangle$ αντιστοιχεί σε έναν τελεστή $\tilde{U}_{f(x)}$ ενός bit, η δράση του οποίου στο δεύτερο qubit

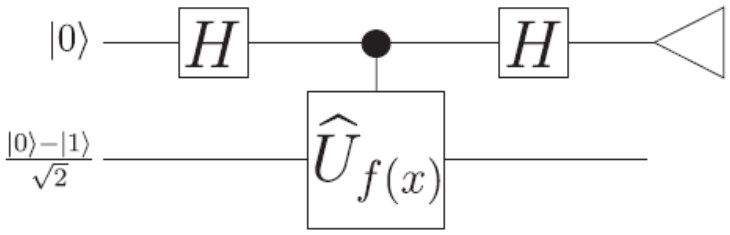


Figure 5: Το κύκλωμα του αλγορίθμου του Deutsch για τον τελεστή $\tilde{U}_{f(x)}$ αντί για τον U_f [2]

ελέγχεται από την κατάσταση του πρώτου qubit, όπως φαίνεται στο παρακάτω σχήμα.

Η κατάσταση $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ είναι ιδιοκατάσταση του $\tilde{U}_{f(x)}$ με ιδιοτιμή $(-1)^{f(x)}$. Κωδικοποιώντας αυτές τις ιδιοτιμές στους παράγοντες φάσης του qubit ελέγχου, μπορούμε να καθορίσουμε την τιμή $f(0) \oplus f(1)$ καθορίζοντας τον παράγοντα σχετικής φάσης μεταξύ της κατάστασης $|0\rangle$ και της κατάστασης $|1\rangle$. Ξεχωρίζουμε τις καταστάσεις $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ και $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ χρησιμοποιώντας μια πύλη Hadamard.

4 Κβαντικός Μετασχηματισμός Fourier (QFT) και εφαρμογές

Σε αυτό το κεφάλαιο θα αναπτύξουμε τον QFT, ο οποίος αποτελεί βασικό συστατικό για την κβαντική παραγοντοποίηση (quantum factoring) και πολλούς άλλους κβαντικούς αλγορίθμους. Ο QFT είναι ένας αποδοτικός κβαντικός αλγόριθμος μέσω του οποίου εκτελούμε μετασχηματισμό Fourier επάνω σε κβαντομηχανικά πλάτη. Επιτρέπει την εκτίμηση φάσης, την προσέγγιση, δηλαδή, των ιδιοτιμών ενός μοναδιαίου τελεστή υπό συγκεκριμένες συνθήκες. Αυτό επιτρέπει την επίλυση διαφόρων ενδιαφέροντων προβλημάτων, συμπεριλαμβανομένων του προβλήματος εύρεσης τάξης και το πρόβλημα της παραγοντοποίησης.

4.1 Κβαντικός Μετασχηματισμός Fourier (QFT)

Ένας από τους πιο χρήσιμους τρόπους να λύσουμε ένα πρόβλημα στα μαθηματικά είναι να το μετασχηματίσουμε σε ένα άλλο πρόβλημα του οποίου τη λύση γνωρίζουμε. Υπάρχουν πολλοί τέτοιοι μετασχηματισμοί που εμφανίζονται σε διάφορα προβλήματα. Μια σημαντική ανακάλυψη του quantum computation είναι το γεγονός, ότι κάποιοι τέτοιοι μετασχηματισμοί μπορούν να υπολογισθούν πολύ γρηγορότερα σε κβαντικούς υπολογιστές σε σχέση με τους κλασσικούς.

Ένας τέτοιος μετασχηματισμός είναι ο διακριτός μετασχηματισμός Fourier [3]. Ο διακριτός μετασχηματισμός Fourier λαμβάνει ως είσοδο ένα διάνυσμα μιγαδικών αριθμών,$x_0, ..., x_{N-1}$, όπου το μήκος N του διανύσματος είναι μια σταθερή παράμετρος. Η έξοδος του είναι τα μετασχηματισμένα δεδομένα, ένα διάνυσμα μιγαδικών αριθμών $y_0, ..., y_{N-1}$ που ορίζεται ως

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k/N} \tag{27}$$

Ο QFT είναι ακριβώς ο ίδιος μετασχηματισμός με μοναδική διαφορά τον συμβολισμό που χρησιμοποιείται. Ορίζουμε τον QFT επάνω σε μια ορθοκανονική βάση $|0\rangle, ..., |N-1\rangle$ ως ένα γραμμικό τελεστή με την ακόλουθη δράση στις καταστάσεις βάσεις

$$|j\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} \tag{28}$$

Ισοδύναμα, η δράση επάνω σε μια αυθαίρετη κατάσταση μπορεί να γραφεί ως

$$\sum_{j=0}^{N-1} x_j |j\rangle = \sum_{k=0}^{N-1} y_k |k\rangle \tag{29}$$

όπου τα πλάτη y_k είναι αυτά που αντιστοιχούν στα πλάτη x_j μέσω του διακριτού μετασχηματισμού Fourier. Παρά το γεγονός, ότι δεν είναι προφανές από τον ορισμό, ο μετασχηματισμός αυτός είναι μοναδιαίος και, άρα, μπορεί να χρησιμοποιηθεί σε έναν κβαντικό υπολογιστή. Αυτό θα το δείξουμε κατασκευάζοντας

ένα μοναδιαίο κβαντικό κύκλωμα που θα υπολογίζει τον μετασχηματισμό Fourier. Είναι, επίσης, εύκολο να αποδείξουμε απευθείας ότι ο μετασχηματισμός Fourier είναι μοναδιαίος.

Θεωρούμε $N = 2^n$, όπου ο n είναι κάποιος ακέραιος αριθμός, και τη βάση $|0\rangle, ..., |2^n - 1\rangle$ που είναι η υπολογιστική βάση για έναν κβαντικό υπολογιστή που αποτελείται από n qubits. Είναι χρήσιμο να γράψουμε την κατάσταση $|j\rangle$ στην δυαδική (binary) αναπαράσταση $j = j_1 j_2 ... j_n$. Πιο αυστηρά, $j = j_1 2^{n-1} + j_2 2^{n-2} + ... + j_n 2^0$. Είναι επίσης βολικό να χρησιμοποιήσουμε τον συμβολισμό $0.j_l j_{l+1} ... j_m$ για να αναπαραστήσουμε το δυαδικό κλάσμα (binary fraction) $j_l/2 + j_{l+1}/4 + ... + j_m/2^{m-l+1}$. Χρησιμοποιώντας αλγεβρικές πράξεις, μπορούμε να εκφράσουμε τον QFT στην παρακάτω αναπαράσταση γινομένου

$$|j_1, ..., j_n\rangle \rightarrow \frac{(|0\rangle + e^{2\pi i 0.j_n} |1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n} |1\rangle)}{2^{n/2}} \tag{30}$$

Αυτή η αναπαράσταση είναι τόσο χρήσιμη, που μπορούμε να τη θεωρήσουμε ισοδύναμο ορισμό του QFT. Αυτή η αναπαράσταση μας επιτρέπει να κατασκευάσουμε ένα αποδοτικό κβαντικό κύκλωμα υπολογισμού του μετασχηματισμού Fourier, που συνιστά μια απόδειξη ότι QFT είναι μοναδιαίος, και παρέχει πληροφορίες για τους αλγορίθμους που βασίζονται επάνω σε αυτόν. Το ισοδύναμο αποτέλεσμα της παραπάνω αναπαράστασης και του ορισμού του QFT προκύπτει με τη χρήση βασικής άλγεβρας.

$$|j\rangle \rightarrow \frac{1}{2^{n/2}} \sum_{k=0}^{2^n - 1} e^{2\pi i j k / 2^n} |k\rangle = \tag{31}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} ... \sum_{k_n=0}^{1} e^{2\pi i j \sum_{l=1}^{n} k_l 2^{-l}} |k_1, ..., k_n\rangle = \tag{32}$$

$$= \frac{1}{2^{n/2}} \sum_{k_1=0}^{1} ... \sum_{k_n=0}^{1} \bigotimes_{l=1}^{n} e^{2\pi i j k_l 2^{-l}} |k_l\rangle = \tag{33}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} [\sum_{k_l=0}^{1} e^{2\pi i j k_l 2^{-l}} |k_l\rangle] = \tag{34}$$

$$= \frac{1}{2^{n/2}} \bigotimes_{l=1}^{n} [|0\rangle + 2^{2\pi i j 2^{-l}} |1\rangle] = \tag{35}$$

$$= \frac{(|0\rangle + e^{2\pi i 0.j_n} |1\rangle)(|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n} |1\rangle)}{2^{n/2}} \tag{36}$$

Η αναπαράσταση αυτή καθιστά εύκολη τη δημιουργία ενός αποδοτικού κυκλώματος για τον QFT. Ένα τέτοιο κύκλωμα φαίνεται στην παρακάτω εικόνα (Figure 6) , όπου η πύλη R_k συμβολίζει τον μοναδιαίο μετασχηματισμό

$$R_k \equiv \text{diag}\begin{bmatrix} 1 & 1 & 1 & e^{2\pi i / 2^k} \end{bmatrix} \equiv \text{C-Phase} \tag{37}$$

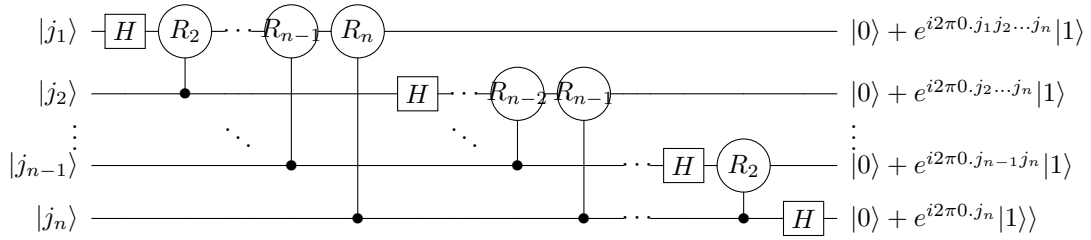


Figure 6: Αποδοτικό κβαντικό κύκλωμα για τον QFT

Για να δούμε, ότι το παρακάτω κύκλωμα υπολογίζει τον QFT ας θεωρήσουμε, ότι το κύκλωμα δέχεται ως είσοδο την κατάσταση $j_1...j_n$. Τότε, εφαρμόζοντας την πύλη Hadamard στο πρώτο bit παράγουμε την κατάσταση

$$\frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1}|1\rangle)|j_2...j_n\rangle, \tag{38}$$

καθώς $e^{2\pi i 0.j_1} = -1$ όταν $j_1 = 1$ και $+1$ αλλιώς. Εφαρμόζοντας την πύλη controlled-R2 παράγουμε την κατάσταση

$$\frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2}|1\rangle)|j_2...j_n\rangle \tag{39}$$

Συνεχίζουμε να εφαρμόζουμε τις πύλες controlled-R_3, R_4 μέχρι την R_n, κάθε μία από τις οποίες προσθέτει ένα επιπλέον bit στη φάση του συντελεστή της πρώτης κατάστασης $|1\rangle$. Στο τέλος της διαδικασίας, έχουμε την κατάσταση

$$\frac{1}{2^{1/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)|j_2...j_n\rangle$$

(40)

Στη συνέχεια, επαναλαμβάνουμε μια παρόμοια διαδικασία στο δεύτερο qubit. Η πύλη Hadamard δημιουργεί την κατάσταση

$$\frac{1}{2^{2/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2}|1\rangle)|j_3...j_n\rangle \tag{41}$$

και οι πύλες controlled-R_2 μέχρι R_{n-1} δημιουργούν την κατάσταση

$$\frac{1}{2^{2/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle)|j_3...j_n\rangle \tag{42}$$

Συνεχίζουμε στο ίδιο μοτίβο για όλα τα qubit, λαμβάνοντας την τελική κατάσταση

$$\frac{1}{2^{n/2}}(|0\rangle + e^{2\pi i 0.j_1 j_2 \ldots j_n}|1\rangle)(|0\rangle + e^{2\pi i 0.j_2 \ldots j_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.j_n}|1\rangle) \tag{43}$$

Οι διαδικασίες ανταλλαγής (swap), οι οποίες δεν φαίνονται στο παραπάνω σχήμα για λόγους ευκρίνειας, χρησιμοποιούνται στη συνέχεια για να επαναφέρουμε την σειρά των qubits. Μετά από αυτές, η κατάσταση των qubits είναι η

$$(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i j_{n-1} j_n}|1\rangle)...(|0\rangle + e^{2\pi i 0.j_1 j_2 ... j_n}) \tag{44}$$

Συγκρίνοντας αυτήν την σχέση με την αρχική εξίσωση, παρατηρούμε ότι αυτή είναι η επιθυμητή έξοδος του QFT. Αυτή η κατα-σκευή αποδεικνύει, επίσης, ότι ο QFT είναι μοναδιαίος, καθώς κάθε πύλη του κυκλώματος είναι μοναδιαία. Είναι, ακόμα, χρήσιμο να υπολογίσουμε τον αριθμό των πυλών που χρησιμοποιήσαμε σε αυτό το κύκλωμα. Ξεκινάμε χρησιμοποιώντας μία πύλη Hadamard και n-1 ελεγχόμενες πύλες περιστροφής στο πρώτο qubit, συνολικά δηλαδή n πύλες. Στη συνέχεια, εφαρμόζουμε μία πύλη Hadamard και n-2 ελεγχόμενες πύλες περιστροφής στο δεύτερο qubit, έχοντας συνολικά n+(n-1) πύλες. Συνεχίζοντας κατά αυτόν τον τρόπο, παρατηρούμε ότι απαιτούνται n+(n-1)+...+1 = n(n+1)/2 πύλες συνολικά, συν οι πύλες swap της σειράς των qubits. Απαιτούνται το μέγιστο n/2 swaps, και κάθε swap μπορεί να επιτευχθεί με τη χρήση τριών C-NOT πυλών. Επομένως, το κύκλωμα παρέχει έναν αλγόριθμο $\Theta(n^2)$ για την εκτέλεση του QFT [3].

Σε αντίθεση με αυτόν, οι καλύτεροι κλασσικοί αλγόριθμοι για τον υπολογισμό του διακριτού μετασχηματισμού Fourier σε 2^n στοιχεία είναι αλγόριθμοι όπως ο Fast Fourier Transform (FFT), οι οποίοι υπολογίζουν τον διακριτό μετασχηματισμό Fourier χρησιμοποιώντας $\Theta(n2^n)$ πύλες. Αυτό σημαίνει, ότι απαιτούνται εκθετικά περισσότερες λειτουργίες για να υπολογισθεί ο μετασχηματισμός Fourier σε έναν κλασσικό υπολογιστή σε σχέση με την εφαρμογή του σε έναν κβαντικό υπολογιστή.

Σε πρώτη ανάγνωση, αυτό φαίνεται ιδιαίτερα σημαντικό, καθώς ο μετασχηματισμός Fourier είναι ένα πολύ σημαντικό στάδιο σε πάρα πολλές εφαρμογές επεξεργασίας δεδομένων. Για παράδειγμα, στην αναγνώριση φωνής από υπολογιστή, το πρώτο βήμα είναι ο μετασχηματισμός Fourier του ψηφιοποιημένου ήχου. Ωστόσο, στο ερώτημα εάν μπορούμε να αξιοποιήσουμε τον QFT για να επιταχύνουμε τον υπολογισμό των μετασχηματισμών Fourier, η απάντηση είναι ότι δεν υπάρχει μέχρι στιγμής γνωστός τρόπος για να μπορέσει να συμβεί αυτό. Το πρόβλημα είναι, ότι τα πλάτη σε έναν κβαντικό υπολογιστή δεν μπορούν να είναι απευθείας προσβάσιμα μέσω μέτρησης. Άρα, δεν υπάρχει τρόπος να καθοριστούν τα μετασχηματισμένα πλάτη της αρχικής κατάστασης. Άρα, είναι δυσκολότερο να βρούμε προβλήματα τα οποία λύνονται με αποδοτικό τρόπο μέσω του QFT.

Είναι, επίσης, χρήσιμο να ορίσουμε τον Αντίστροφο (Inverse) QFT. Η δράση του Inverse QFT επάνω σε μια βάση καταστάσεων $|0\rangle, |1\rangle, ..., |N-1\rangle$ δίνεται από τη σχέση

$$QFT^{-1}|x\rangle \rightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{2^{N-1}} e^{-2\pi i x/N}|y\rangle \tag{45}$$

Είναι προφανές, ότι

$$QFT * QFT^{-1} = \mathcal{I} \tag{46}$$

4.2 Χρήση QFT με τοπικές αλληλεπιδράσεις

Μπορούμε να αναπαραστήσουμε το κύκλωμα του QFT με αρχιτεκτονική μίας διάστασης τοπικού κοντινότερου γείτονα (1D-LNN) η οποία επιτρέπει μόνο τοπικές αλληλεπιδράσεις χρησιμοποιώντας πύλες SWAP, οι οποίες υλοποιούνται με τη διαδοχική εκτέλεση τριών πυλών CNOT μεταξύ των qubits που θέλουμε να κάνουμε swap. Το κύκλωμα φαίνεται παρακάτω για 6 qubits.

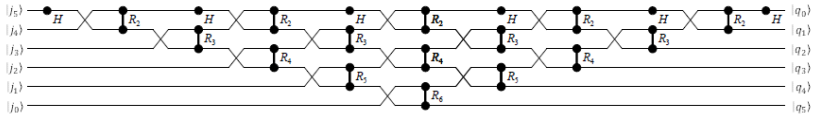


Figure 7: Κβαντικό κύκλωμα QFT με τοπικές αλληλεπιδράσεις για 6 qubits [5]

Αυτή η τοπολογία διατηρεί την πολυπλοκότητα $O(n^2)$ του QFT με την προϋπόθεση ότι η αρχιτεκτονική του υπολογιστή επιτρέπει την παράλληλη εκτέλεση πυλών. Η έξοδος του συγκεκριμένου κυκλώματος δίνει τα qubits με τη σωστή σειρά, άρα δε χρειάζεται στο τέλος της διαδικασίας να αντιστρέψουμε τη σειρά τους. Το βάθος(depth) του κυκλώματος είναι 2n-1 βήματα, θεωρώντας ότι παραπλήσιες πύλες που δρουν επάνω στο ίδιο qubit αντιστοιχούν σε ένα βήμα, ενώ το κβαντικό υπολογιστικό κόστος είναι n(n+1)/2 υπολογίζοντας με τον ίδιο τρόπο.

4.3 Banded QFT

Γνωρίζουμε, ότι μια ευθεία εφαρμογή του QFT απαιτεί n(n+1)/2 κβαντικές πύλες των δύο qubits. Αποδεικνύεται, επίσης, ότι ένα ισοδύναμο κύκλωμα το οποίο αποτελείται αποκλειστικά από κβαντικές πύλες ενός qubit και το οποίο καταλήγει σε μετρήσεις, είναι ακριβώς ισοδύναμο με τον κανονικό μετασχηματισμό. Η παρακάτω εικόνα (a) δείχνει της εφαρμογή ενός qubit του QFT για την ειδική περίπτωση των πέντε qubits. Κωδικοποιούμε τις C-R_k πύλες της εικόνας ως ϑ, καθώς ελέγχονται από κλασσικές εισόδους και δρουν συνεκτικά μόνο επάνω σε ένα qubit.

Το κύκλωμα αυτό εξακολουθεί να απαιτεί $\sim n^2$ πύλες, αλλά εφόσον εκτελούνται από πύλες ενός qubit, η πειραματική εφαρμογή αυτού του κυκλώματος είναι πολύ πιο απλή. Σε αντίθεση με την πλήρη εφαρμογή του QFT με πύλες των δύο qubits, όπου οι μετρήσεις μπορούν να συμβούν όλες συγχρόνως στο τέλος του κβαντικού υπολογισμού, οι μετρήσεις στην περίπτωση των πυλών ενός qubit συμβαίνουν σε αλληλουχία και τα αποτελέσματα των μετρήσεων χρησιμοποιούνται για τον έλεγχο τον πυλών στροφής φάσης ϑ.

Ο D. Coppersmith [7] έδειξε πρώτος, ότι ακόμα και αυτό το κύκλωμα μπορεί να βελτιωθεί περισσότερο χρησιμοποιώντας έναν προσεγγιστικό μετασχηματισμό, τον Banded QFT, ο οποίος απεικονίζεται στην εικόνα (b). Ο Banded QFT, που συμβολίζεται με $\tilde{U}_b^{(QFT)}$ προκύπτει από την κανονική εφαρμογή του QFT διατηρώντας τη σύζευξη ενός qubit μόνο με τους b σε αριθμό κοντινότερους γείτονες. Στην εικόνα (b) φαίνεται η περίπτωση, στην οποία ισχύει b=1. Ο Banded QFT παίρνει το όνομα τόσο από το σχήμα του κυκλώματος, στο οποίο οι

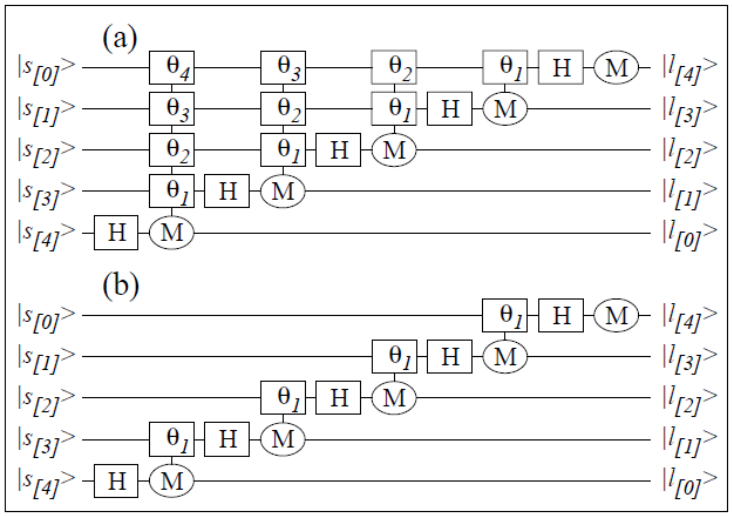


Figure 8: Κβαντικό κύκλωμα QFT 5 qubits, (a) b=4, (b) b=1 [6]

θέσεις των πυλών σχηματίζουν "ζώνες" (Figure 8), αλλά και επειδή ο πίνακας στον οποίο αντιστοιχεί ο συγκεκριμένος μετασχηματισμός είναι πίνακας ζώνης (band matrix), δηλαδή είναι ένας αραιός πίνακας, του οποίου τα μη-μηδενικά στοιχεία περιορίζονται σε μια διαγώνια ζώνη, περιλαμβάνοντας την κύρια διαγώνιο και μηδέν ή περισσότερες διαγωνίους σε κάθε πλευρά της κύριας.

5 Εφαρμογές του QFT

5.1 Εκτίμηση φάσης (Phase-estimation)

Ο QFT είναι καθοριστικός στη γενική διαδικασία που ονομάζεται εκτίμηση φάσης, που με τη σειρά της είναι βασική για πολλούς κβαντικούς αλγορίθμους. Ας υποθέσουμε, ότι ένας μοναδιαίος τελεστής U έχει ένα ιδιοδιάνυσμα $|u\rangle$ με ιδιοτιμή $e^{2\pi i\varphi}$, όπου η τιμή του φ είναι άγνωστη. Ο σκοπός της εκτίμησης φάσης είναι η εκτίμηση της τιμής του φ. Για να πραγματοποιήσουμε αυτήν την εκτίμηση, υποθέτουμε ότι έχουμε διαθέσιμα black boxes (ή αλλιώς oracles), τα οποία μπορούν να προετοιμάζουν την κατάσταση $|u\rangle$ και να εκτελούν την λειτουργία controlled-U^{2^j} για κατάλληλους μη-αρνητικούς ακεραίους j [3]. Η χρήση black boxes υποδεικνύει, ότι η εκτίμηση φάσης δεν είναι ένας πλήρης κβαντικός αλγόριθμος από μόνη της. Αντίθετα, μπορούμε να τη φανταστούμε ως «υπορουτίνα», η οποία όταν συνδυαστεί με άλλες υπορουτίνες μπορεί να χρησιμοποιηθεί για διάφορες υπολογιστικές διεργασίες. Σε συγκεκριμένες εφαρμογές της εκτίμησης φάσης θα πρέπει να κάνουμε ακριβώς αυτό, περιγράφοντας πώς λειτουργούν οι διεργασίες των black boxes και συνδυάζοντας αυτό με τη διαδικασία εκτίμησης φάσης ώστε να εκτελέσουμε χρήσιμες λειτουργίες.

Η κβαντική διαδικασία εκτίμησης φάσης χρησιμοποιεί δύο καταχωρητές (registers) [3]. Ο πρώτος καταχωρητής περιέχει t qubits στην κατάσταση $|0\rangle$. Ο τρόπος με τον οποίου επιλέγουμε το t βασίζεται σε δύο παράγοντες: πρώτον, τον αριθμό των ψηφίων ακριβείας που θέλουμε να έχει η εκτίμησή μας για το φ, και, δεύτερον, με τί πιθανότητα θέλουμε η εκτίμηση φάσης να είναι επιτυχημένη. Η εξάρτηση του t από αυτές τις ποσότητες αναδύεται από την παρακάτω ανάλυση.

Ο δεύτερος καταχωρητής ξεκινά από την κατάσταση $|u\rangle$ και εμπεριέχει όσα qubits είναι απαραίτητα για να αποθηκευτεί η $|u\rangle$. Η εκτίμηση φάσης γίνεται σε δύο στάδια. Στο πρώτο, εφαρμόζουμε το κύκλωμα που φαίνεται παρακάτω.

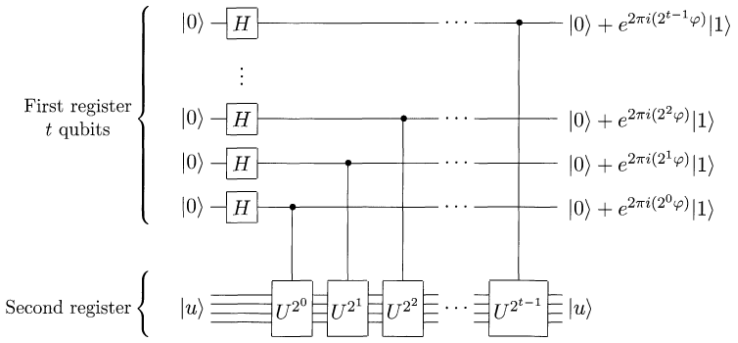


Figure 9: Πρώτο στάδιο της διαδικασίας Εκτίμησης Φάσης [3]

Το κύκλωμα αυτό ξεκινά με την εφαρμογή μιας πύλη Hadamard στον πρώτο καταχωρητή, ακολουθούμενη από την εφαρμογή controlled-U πυλών στο δεύτερο καταχωρητή, με το U να υψώνεται σε διαδοχικές δυνάμεις του δύο. Η τελική

κατάσταση για τον πρώτο καταχωρητή μπορεί εύκολα να δειχθεί, ότι είναι η

$$\frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle)(|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle)...(|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle) = \tag{47}$$

$$= \frac{1}{2^{t/2}} \sum_{k=0}^{2^t-1} e^{2\pi i \varphi k}|k\rangle \tag{48}$$

Από αυτήν την περιγραφή αφαιρούμε το δεύτερο καταχωρητή, καθώς παραμένει στην κατάσταση $|u\rangle$ καθ' όλη τη διάρκεια του υπολογισμού.

Το δεύτερο στάδιο της εκτίμησης φάσης είναι η εφαρμογή του Αντίστροφου QFT στο πρώτο qubit. Αυτό επιτυγχάνεται αντιστρέφοντας το κύκλωμα του QFT και μπορεί να γίνει σε $\Theta(t^2)$ βήματα. Το τρίτο και τελικό βήμα είναι να αναγνώσουμε την κατάσταση του πρώτου καταχωρητή, εκτελώντας μέτρηση στην υπολογιστική βάση. Θα δούμε, ότι αυτό παρέχει μια πολύ καλή εκτίμηση του φ. Παρακάτω, φαίνεται μια συνολική σχηματική απεικόνιση του αλγορίθμου.

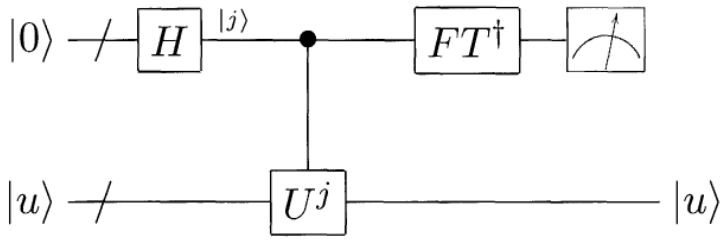


Figure 10: Συνολική σχηματική αναπαράσταση της διαδικασίας Εκτίμησης Φάσης [3]

Για να καταλάβουμε διαισθητικά τον τρόπο λειτουργίας της εκτίμησης φάσης, θα υποθέσουμε ότι το φ μπορεί να εκφραστεί σε ακριβώς t bits, ως $\varphi = \varphi_1\varphi_2...\varphi_t$. Τότε, η τελική κατάσταση που δείχθηκε προηγουμένως μπορεί να γραφεί ως

$$\frac{1}{2^{t/2}}(|0\rangle + e^{2\pi i 0.\varphi_t}|1\rangle)(|0\rangle + e^{2\pi i 0.\varphi_{t-1}\varphi_t}|1\rangle)...(|0\rangle + e^{2\pi i 0.\varphi_1\varphi_2...\varphi_t}|1\rangle) \tag{49}$$

Το δεύτερο στάδιο της εκτίμησης φάσης είναι να εφαρμόσουμε τον Inverse-QFT. Συγκρίνοντας, όμως, την προηγούμενη εξίσωση με τον QFT σε αναπαράσταση γινομένου, βλέπουμε, ότι η κατάσταση εξόδου από το δεύτερο στάδιο είναι η κατάσταση γινομένου $|\varphi_1...\varphi_t\rangle$. Μια μέτρηση στην υπολογιστική φάση, άρα, δίνει ακριβώς την τιμή του φ.

Συνοψίζοντας, ο αλγόριθμος εκτίμησης φάσης επιτρέπει την εκτίμηση της φάσης φ μιας ιδιοτιμής ενός μοναδιαίου τελεστή U, με δεδομένο το αντίστοιχο ιδιοδιάνυσμα $|u\rangle$. Ένα αναγκαίο χαρακτηριστικό αυτής της διαδικασίας είναι η ικανότητα του αντίστροφου QFT να εκτελεί το μετασχηματισμό

$$\frac{1}{2^{t/2}} \sum_{j=0}^{2^t} e^{2\pi i \varphi j}|j\rangle|u\rangle \rightarrow |\tilde{\varphi}\rangle|u\rangle \tag{50}$$

όπου με $|\tilde{\varphi}\rangle$ συμβολίζεται η κατάσταση που είναι μια καλή εκτίμηση της φ όταν μετρηθεί.

5.2 Εύρεση Τάξης (Order-finding)

Για θετικούς ακέραιους x και N με $x < N$ οι οποίοι δεν έχουν κοινούς παράγοντες, η τάξη του x modulo N ορίζεται ως ο μικρότερος θετικός ακέραιος, r, τέτοιος ώστε $x^r = 1(\text{mod N})$ [2]. Το πρόβλημα εύρεσης τάξης έχει σκοπό να προσδιορίσει την τάξη για κάποιους συγκεκριμένους x και N. Η εύρεση τάξης θεωρείται δύσκολο πρόβλημα στους κλασσικούς υπολογιστές υπό την έννοια, ότι δεν υπάρχει γνωστός αλγόριθμος που να λύνει το πρόβλημα χρησιμοποιώντας πολυωνυμικούς υπολογιστικούς όρους στα O(L) bits που απαιτούνται για να προσδιοριστεί το πρόβλημα, όπου $\text{L} \equiv [\log(\text{N})]$ είναι ο αριθμός των bits που απαιτούνται για προσδιοριστεί το N. Σε αυτό το κεφάλαιο θα δούμε πώς η εκτίμηση φάσης μπορεί να χρησιμοποιηθεί για να δημιουργήσουμε έναν αποδοτικό κβαντικό αλγόριθμο για την εύρεση τάξης.

Ο κβαντικός αλγόριθμος για την εύρεση τάξης είναι απλώς ο αλγόριθμος για την εκτίμηση φάσης, ο οποίος εφαρμόζεται στον μοναδιαίο τελεστή $U|y\rangle \equiv |xy(modN)\rangle$, όπου το y ανήκει στο $\{0,1\}^L$. Αξίζει να σημειωθεί, ότι στην ανάλυση που ακολουθεί, όταν $N \leq y \leq 2^L - 1$, χρησιμοποιούμε τη σύμβαση, ότι xy(modN) είναι απλά το y. Δηλαδή, ο τελεστής U δρα μη-τετριμμένα, όταν $0 \leq y \leq N-1$. Με απλούς υπολογισμούς μπούμε να δείξουμε, ότι οι καταστάσεις που ορίζονται από την παρακάτω σχέση

$$|u_s\rangle \equiv \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} exp[\frac{-2\pi isk}{r}] |x^k modN\rangle \tag{51}$$

για ακεραίους $0 \leq s \leq r-1$ είναι ιδιοκαταστάσεις του U, καθώς

$$U|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} exp[\frac{-2\pi isk}{r}] |x^{k+1} modN\rangle = exp[\frac{2\pi is}{r}] |u_s\rangle \text{ [3]} \tag{52}$$

Χρησιμοποιώντας τη διαδικασία της εκτίμησης φάσης μπορούμε να αποκτήσουμε με μεγάλη ακρίβεια τις αντίστοιχες ιδιοτιμές exp[2πi/r], από τις οποίες μπορούμε να βρούμε την τάξη r.

Υπάρχουν δύο σημαντικές προϋποθέσεις για να μπορέσουμε να χρησιμοποιήσουμε την διαδικασία της εκτίμησης φάσης. Θα πρέπει να έχουμε επαρκείς υπολογιστικούς όρους για να εφαρμόσουμε έναν τελεστή controlled-$U(2^j)$ για οποιονδήποτε ακέραιο j, και θα πρέπει να μπορούμε να προετοιμάσουμε αποτελεσματικά μια ιδιοκατάσταση $|u_s\rangle$ με μη-τετριμμένη ιδιοτιμή ή, τουλάχιστον, μια υπέρθεση τέτοιων καταστάσεων. Η πρώτη απαίτηση ικανοποιείται μέσω μιας διαδικασίας που ονομάζεται modular exponentiation, με την οποία μπορούμε να εκτελέσουμε μια ολόκληρη ακολουθία από controlled-$U(2^j)$ τελεστές που εφαρμόζονται από τη διαδικασία εκτίμησης φάσης χρησιμοποιώντας $O(L^3)$ πύλες (Παράρτημα C).

Η δεύτερη απαίτηση είναι πιο σύνθετη. Η προετοιμασία της $|u_s\rangle$ απαιτεί να γνωρίζουμε το r. Ευτυχώς, μία έξυπνη παρατήρηση μας επιτρέπει να αποφύγουμε

το πρόβλημα της προετοιμασίας του $|u_s\rangle$, η οποία είναι

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle \tag{53}$$

Κατά τη διαδικασία εκτίμησης φάσης, εάν χρησιμοποιήσουμε, ότι t = 2L + 1 + log(2+1/2ε) qubits στον πρώτο καταχωρητή, και προετοιμάσουμε τον δεύτερο καταχωρητή στην κατάσταση $|1\rangle$ -το οποίο είναι τετριμμένο- τότε για κάθε s από το 0 μέχρι το r-1, θα παρατηρήσουμε μια εκτίμηση της φάσης $\varphi \approx s/r$, με ακρίβεια 2L+1 bits, με πιθανότητα τουλάχιστον (1-ε)/r.

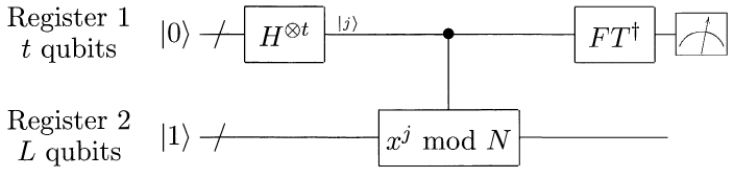


Figure 11: Κβαντικό κύκλωμα για τον αλγόριθμο Εύρεσης Τάξης [3]

5.3 Παραγοντοποίηση (factoring)

Για έναν δοσμένο σύνθετο ακέραιο αριθμό N, θέλουμε να βρούμε τους πρώτους αριθμούς που όταν πολλαπλασιαστούν μεταξύ τους θα δίνουν ως αποτέλεσμα τον N. Το πρόβλημα της παραγοντοποίησης είναι ισοδύναμο με το πρόβλημα της εύρεσης τάξης, υπό την έννοια ότι ένας γρήγορος αλγόριθμος για εύρεση τάξης μπορεί εύκολα να μετατραπεί σε έναν γρήγορο αλγόριθμο παραγοντοποίησης.

Η αναγωγή της παραγοντοποίησης στην εύρεση τάξης συμβαίνει σε δύο βασικά βήματα. Το πρώτο βήμα είναι να δείξουμε, ότι μπορούμε να υπολογίσουμε έναν παράγοντα του N εάν μπορέσουμε να βρούμε μια μη-τετριμμένη λύση $x \neq 1(\text{mod N})$ στην εξίσωση $x^2 = 1(\text{mod N})$. Το δεύτερο βήμα είναι να δείξουμε, ότι ένας τυχαία επιλεγμένος αριθμός y που είναι πρώτος του N είναι πιθανό να είναι τάξης r, η οποία είναι άρτια, και τέτοια ώστε $y^{r/2} \neq \pm 1(mod N$. Τότε, η λύση $x \equiv y^{r/2}$ (mod N) θα είναι μη-τετριμμένη για την εξίσωση $x^2 =$ (mod N). Αυτά τα δύο βήματα ενσωματώνονται στα ακόλουθα θεωρήματα.

Θεώρημα 1

Έστω N ένας σύνθετος αριθμός μεγέθους L bits, και έστω x μια μη-τετριμμένη λύση της εξίσωσης $x^2 = 1(\text{mod N})$ στο διάστημα $1 \leq x \leq N$, η οποία δεν είναι ούτε η $x = 1(\text{mod N})$ ούτε η x = N-1 = -1(mod N). Τότε, τουλάχιστον ένας από τους μέγιστους κοινούς διαιρέτες gcd(x-1,N) και gcd(x+1,N) είναι ένας μη-τετριμμένος παράγοντας του N, ο οποίος μπορεί να υπολογιστεί χρησιμοποιώντας $O(L^3)$ τελεστές.

Θεώρημα 2

Έστω $N = p_1^{a1}...p_m^{am}$ η πρώτη παραγοντοποίηση ενός περιττού σύνθετου θετικού ακεραίου. Έστω x ένας ακέραιος επιλεγμένος με ομοιόμορφη τυχαιότητα, ο οποίος υπόκειται στους περιορισμούς $1 \leq x \leq N-1$ και ο x είναι πρώτος του N. Έστω r η τάξη του x modulo N. Τότε,

p(r είναι άρτιος και $x^{r/2} \neq$ -1(mod N)) $\geq 1 - \frac{1}{2^m}$

Τα δύο αυτά θεωρήματα μπορούν να συνδυαστούν δημιουργώντας έναν αλγόριθμο, ο οποίος με μεγάλη πιθανότητα, επιστρέφει έναν μη-τετριμμένο παράγοντα του σύνθετου N. Όλα τα βήματα του αλγορίθμου μπορούν να εκτελεστούν αποδοτικά σε έναν κλασσικό υπολογιστή, εκτός από μια «υπορουτίνα» εύρεσης τάξης που χρησιμοποιείται στον αλγόριθμο. Επαναλαμβάνοντας τη διαδικασία μπορούμε να βρούμε μια πλήρη πρώτη παραγοντοποίηση του N [3]. Τα βήματα του αγορίθμου είναι συνοπτικά τα παρακάτω:

1) Αν ο N είναι άρτιος, επίστρεψε τον παράγοντα 2.

2) Διερεύνησε εάν ισχύει $N = a^b$ για ακεραίους $a \geq 1$ και $b \geq 1$, και εάν ναι, επίστρεψε τον παράγοντα a.

3) Τυχαία επίλεξε μια τιμή x στο διάστημα από 1 μέχρι N-1. Εάν gcd(x,N) ¿ 1, τότε επίστρεψε τον παράγοντα gcd(x,N).

4)Χρησιμοποίησε την υπορουτίνα εύρεσης τάξης για να βρεις την τάξη r του x modulo N.

5)Εάν το r είναι άρτιος και $x^{r/2} \neq$ -1(mod N), τότε υπολόγισε το gcd($x^{r/2}$-1, N) και το gcd($x^{r/2}$+1, N) και έλεγξε εάν ένα από αυτά είναι μη-τετριμμένος παράγοντας, επιστρέφοντας τον παράγοντα εάν αυτό ισχύει. Σε αντίθετη περίπτωση, ο αλγόριθμος αποτυγχάνει.

Τα βήματα 1 και 2 του αλγορίθμου είτε επιστρέφουν έναν παράγοντα ή, ειδάλλως, εξασφαλίζουν ότι ο N είναι ένας περιττός ακέραιος με παραπάνω από έναν πρώτους παράγοντες. Αυτά τα βήματα μπορούν να πραγματοποιηθούν χρησιμοποιώντας O(1) και $O(L^3)$ πράξεις, αντίστοιχα. Το βήμα 3 είτε επιστρέφει έναν παράγοντα, είτε παράγει ένα τυχαία επιλεγμένο στοιχείο x από το σύνολο $\{0, 1, 2, \ldots, N-1\}$.Το βήμα 4 καλεί την υπορουτίνα της εύρεσης τάξης, υπολογίζοντας την τάξη r του x modulo N. Το βήμα 5 ολοκληρώνει τον αλγόριθμο, καθώς το Θεώρημα 2 εξασφαλίζει ότι με πιθανότητα τουλάχιστον $\frac{1}{2}$ το r θα είναι άρτιος και $x^{r/2} \neq$ -1(mod N), και στη συνέχεια το θεώρημα 1 εξασφαλίζει ότι είτε ο gcd($x^{r/2}$ - 1, N) είτε ο gcd($x^{r/2}$ + 1, N) θα είναι μη-τετριμμένος παράγοντας του N.

6 Πολλαπλασιασμός με σταθερό αριθμό με χρήση QFT

6.1 Αλγόριθμος

Βασικό αντικείμενο της παρούσας Διπλωματικής Εργασίας είναι η χρήση QFT για την εκτέλεση της κβαντικής αριθμητικής πράξης του πολλαπλασιασμού με σταθερό αριθμό. Ο πολλαπλασιαστής που θα κατασκευάσουμε είναι ένας «in-place» πολλαπλασιαστής, δηλαδή δε χρησιμοποιεί ancilla qubits πέρα από αυτά που είναι αναγκαία για την αναπαράσταση των ακεραίων αριθμών. Ο πολλαπλασιαστής με σταθερά λ εκτελεί την πράξη του πολλαπλασιασμού modulo 2^n, όπου n είναι ο αριθμός των qubits. Συμβολίζουμε το κβαντικό κύκλωμα ως $MODMULC_\lambda$ [5].

$$|x\rangle \rightarrow |\lambda x \mod 2^n\rangle \tag{54}$$

Ο περιορισμός ο τελεστής να είναι μοναδιαίος, άρα και αντιστρέψιμος, επιβάλλει τον περιορισμό gcd(λ,2)=1, δηλαδή η σταθερά λ και ο αριθμός 2 -που είναι η διάσταση των qubits- να είναι πρώτοι μεταξύ τους. Με αυτόν τον τρόπο, μπορούμε να ορίσουμε έναν τελεστή που ονομάζεται modified QFT ($mQFT_\lambda$), ο οποίος για n qubits ορίζεται ως εξής:

$$mQFT_\lambda = \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \sum_{j=0}^{2^n-1} |k\rangle \langle j| \, e^{i\frac{2\pi}{2^n}\lambda jk} \tag{55}$$

Ο συγκεκριμένος ορισμός προκύπτει από το γεγονός, ότι αν εκτελέσουμε διαδοχικά τον $mQFT_\lambda$ με τον αντίστροφο QFT, θα πάρουμε τον επιθυμητό πολλαπλασιαστή με σταθερά λ. Η απόδειξη φαίνεται παρακάτω:

$$QFT^{-1} * mQFT_\lambda = \tag{56}$$

$$\frac{1}{2^n} \sum_{m=0}^{2^n-1} \sum_{r=0}^{2^n-1} |m\rangle \langle r| \, e^{-i\frac{2\pi}{2^n}mr} \sum_{k=0}^{2^n-1} \sum_{j=0}^{2^n-1} |k\rangle \langle j| \, e^{i\frac{2\pi}{2^n}\lambda jk} = \tag{57}$$

$$= \frac{1}{2^n} \sum_{m=0}^{2^n-1} \sum_{j=0}^{2^n-1} |m\rangle \langle j| \sum_{k=0}^{2^n-1} (e^{i\frac{2\pi}{2^n}(lj-m)})^k = \tag{58}$$

$$= \sum_{j=0}^{2^n-1} |\lambda j \pmod{2^n}\rangle \langle j| \tag{59}$$

Η προτελευταία εξίσωση προκύπτει κάνοντας χρήσης της ιδιότητας, ότι το άθροισμα ριζών της μονάδας ισούται με 0, όπως φαίνεται και από την παρακάτω σχέση:

$$\sum_{k=0}^{2^n-1} (e^{i\frac{2\pi}{2^n}(lj-m)})^k = \begin{cases} 2^n & \lambda j - m \pmod{2^n} \\ 0 & \lambda j - m \neq 0 \pmod{2^n} \end{cases} \tag{60}$$

Είναι προφανές από την εξίσωση (59), ότι ο τελεστής της εξίσωσης (56) μετασχηματίζει μια οποιαδήποτε υπολογιστική βάση $|l\rangle$ στην κατάσταση $|\lambda l \mod 2^n\rangle$ που είναι ακριβώς ο ορισμός του πολλαπλασιαστή.

Το κύκλωμα του $mQFT_\lambda$ είναι σχεδόν ίδιο με το κύκλωμα του απλού QFT, με εξαίρεση, ότι κάθε controlled R_k του QFT αντικαθίσταται στο συγκεκριμένο κύκλωμα με μία R_k^λ πύλη, το οποίο σημαίνει ότι οι γωνίες που χρησιμοποιούνται στις φάσεις αυτών των πυλών περιστροφής είναι πολλαπλάσια επί λ των αρχικών γωνιών που χρησιμοποιούνται στον απλό QFT.

Θεωρούμε, ότι ξεκινάμε με μια αυθαίρετη υπολογιστική βάση $|j\rangle = |j_{n-1}\rangle ... |j_1\rangle |j_0\rangle$. Ξεκινάμε από το πάνω qubit, που είναι και το πιο σημαντικό, το οποίο θεωρούμε ότι αρχικά βρίσκεται στην κατάσταση $|j_{n-1}\rangle$. Αρχικά, εφαρμόζουμε μια πύλη Hadamard, η οποία εκτελεί τον μετασχηματισμό

$$|j_{n-1}\rangle \xrightarrow{H} \frac{1}{\sqrt{2}} \sum_{m=0}^{n-1} e^{i2\pi(0.j_{n-1})m} |m\rangle \tag{61}$$

Η δράση της πύλης R_2^λ είναι

$$\frac{1}{\sqrt{2}} \sum_{m=0}^{n-1} e^{i2\pi(0.j_{n-1}j_{n-2})\lambda m} |m\rangle \tag{62}$$

και με αντίστοιχο τρόπο βρίσκουμε όλες τις ζητούμενες πύλες περιστροφής. Έτσι, φτάνουμε στην τελική κατάσταση

$$\frac{1}{\sqrt{2}} \sum_{m=0}^{n-1} e^{i2\pi(0.j_{n-1}j_{n-2}...j_0)\lambda m} |m\rangle \tag{63}$$

Με παρόμοια ανάλυση στα υπόλοιπα qubits που βρίσκονται αρχικά στην κατάσταση j_k, με k=n-2,. . . ,0 βρίσκουμε τις τελικές καταστάσεις

$$q_k = \frac{1}{\sqrt{2}} \sum_{m=0}^{n-1} e^{i2\pi(0.j_k j_{k-1}...j_0)\lambda m} |m\rangle \tag{64}$$

Αντιστρέφοντας τη σειρά των qubits στο τέλος, έχουμε την τελική κατάσταση γινομένου

$$|q_0\rangle |q_1\rangle ... |q_{n-1}\rangle = \tag{65}$$

$$\frac{1}{\sqrt{2^n}} (\sum_{m=0}^{n-1} e^{i2\pi\lambda(0.j_0)m})(\sum_{m=0}^{n-1} e^{i2\pi\lambda(0.\xi_1 j_0)m})...(\sum_{m=0}^{n-1} e^{i2\pi\lambda(0.j_{n-1}j_{n-2}...j_1 j_0)m}) \tag{66}$$

$$= \frac{1}{\sqrt{s^n}} \sum_{m=0}^{2^n-1} e^{i\frac{2\pi}{2^n}\lambda jk} |k\rangle \tag{67}$$

η οποία πράγματι αντιστοιχεί στον μετασχηματισμό που προκαλεί ο τελεστής mQFTλ σε μια αυθαίρετη υπολογιστική βάση καταστάσεων $|j\rangle$.

Αναφορικά με τον αντίστροφο του σταθερού πολλαπλασιαστή, αυτός μπορεί να προσεγγιστεί με τρεις διαφορετικούς τρόπους. Οι πρώτοι δύο προκύπτουν από την παρακάτω εξίσωση

$$MODMULC_{\lambda}^{-1} = [QFT^{-1} * mQFT_{\lambda}]^{-1} = mQFT_{\lambda}^{-1} * QFT[5] \tag{68}$$

Η τοπολογία του αντίστροφου $mQFT_{\lambda}$ στην παραπάνω σχέση είναι απλά ένα αντεστραμμένο οριζόντια κύκλωμα $mQFT_{\lambda}$, του οποίου οι controlled-R πύλες έχουν τις αντίθετες γωνίες. Μια άλλη κατασκευή του αντίστροφου μπορεί να προκύψει από την παρατήρηση, ότι

$$mQFT_{\lambda}^{-1} = mQFT_{-\lambda} \tag{69}$$

που μπορεί να γίνει από τις παραπάνω εξισώσεις για την τελική κατάσταση του κυκλώματος. Εναλλακτικά, παρατηρούμε, ότι

$$MODMULC_{\lambda^{-1}} * MODMULC_{\lambda} |x\rangle = |\lambda^{-1}\lambda x \pmod{2^n}\rangle = |x\rangle \tag{70}$$

για κάθε x, και άρα ο αντίστροφος πολλαπλασιαστής παραμέτρου λ είναι ένας ευθύς πολλαπλασιαστής με παράμετρο λ^{-1}.

$$MODMULC_{\lambda}^{-1} = MODMULC_{\lambda^{-1}} \tag{71}$$

Η κατασκευή, ωστόσο, ενός χρήσιμου πολλαπλασιαστή δεν μπορεί να εξαντλείται στις περιπτώσεις όπου $gcd(\lambda, 2^n) = 1$), αλλά θα πρέπει να περιλαμβάνει και περιπτώσεις των άρτιων αριθμών. Τότε το λ θα μπορεί να είναι οποισδήποτε ακέραιος αριθμός και, σύμφωνα με το Θεμελιώδες Θεώρημα της Αριθμητικής, μπορεί να παραγοντοποιηθεί ως $\lambda = g * 2^s$, όπου ισχύουν $gcd(g, 2^n) = 1$) και $0 < s < n = n_1 + n_2$[5]. Το n_1 είναι ο αριθμός των qubits που απαιτούνται για τον αριθμό του πολλαπλασιαστή και το n_2 είναι ίσο με $\log_2 \lambda$. Τότε, ο αρχικός πολλαπλασιασμός με τη σταθερά λ ανάγεται στον πολλαπλασιασμό με τη σταθερά g και σε μια αριστερή μετατόπιση κατά s qubits. Το κβαντικό κύκλωμα που προκύπτει πολλαπλασιάζει τη σταθερά g, η οποία αποτελείται από n_2 qubits, με την είσοδο μεγέθους n_1 qubits. Στη συνέχεια εφαρμόζουμε τον πολλαπλασιαστή $mQFT_{\lambda}$ πλάτους $n_1 + n_2$ qubits και αρχικοποιούμε τα επάνω n_2 qubits στην κατάσταση $|0\rangle$ και τα υπόλοιπα n_1 στην κατάσταση $|x\rangle$. Επιπλέον, χρησιμοποιείται ένας καταχωρήτης που αποτελείται από s qubits, ο οποίος αρχικά βρίσκεται στην κατάσταση $|0\rangle$ που χρησιμοποιείται για τη διεξαγωγή μιας "αριστερής" στροφής του γινομένου του πολλαπλασιασμού μαζί με αυτά τα s qubits όπως φαίνεται παρακάτω (Figure 12).

6.2 Ορισμός Συναρτήσεων

Για την υλοποίηση των ζητούμενων αριθμητικών κβαντικών πράξεων, δημιουργήσαμε στην γλώσσα Python διάφορες συναρτήσεις και προγράμματα. Η παρουσίαση τους γίνεται αναλυτικά στο Παράρτημα Α.

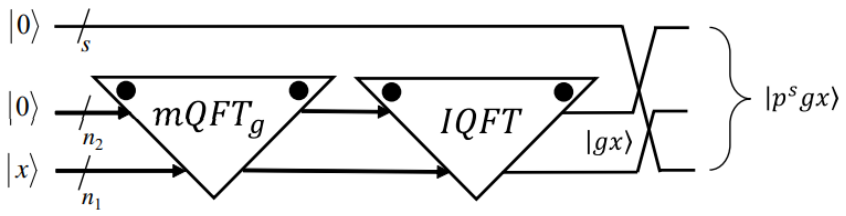


Figure 12: Πολλαπλασιαστής mQFT για οποιαδήποτε σταθερά λ [5]

7 Προσομοιώσεις και αποτελέσματα

Βασικός στόχος της συγκεκριμένης Διπλωματικής Εργασίας είναι η μελέτη της αξιοπιστίας και ακρίβειας του αλγορίθμου για πολλαπλασιασμό με σταθερό αριθμό με χρήση QFT. Για το σκοπό αυτό, διενεργήθηκαν πειράματα τόσο με τη χρήση κβαντικού υπολογιστή IBM-Q που θα αναλυθούν σε επόμενο κεφάλαιο, όσο και με χρήση προσομοιωτών. Αυτό είναι αναγκαίο για την επαλήθευση της ορθότητας των συναρτήσεων που κατασκευάστηκαν, καθώς το πρώιμο στάδιο στο οποίο βρίσκονται οι πραγματικοί κβαντικοί υπολογιστές έχει ως συνέπεια αυτοί να δίνουν αξιόπιστα αποτελέσματα μόνο υπό πολύ συγκεκριμένες προϋποθέσεις. Με τη χρήση προσομοιωτών, μπορούμε να εκτελέσουμε τα προγράμματα μας και να αντλήσουμε χρήσιμα αποτελέσματα επαληθεύοντας ή μη την αποδοτικότητα του αλγορίθμου.

Η γενική μεθοδολογία για την εκτέλεση κβαντικών αλγορίθμων με τη χρήση της βιβλιοθήκης Qiskit, περιλαμβάνει τέσσερα βασικά βήματα:

1. Στο πρώτο βήμα, ο χρήστης θα πρέπει να μεταφράσει το κλασσικό πρόβλημα το οποίο προσπαθεί να επιλύσει σε ένα ολοκληρωμένο κβαντικό κύκλωμα και τους αντίστοιχους κβαντικούς τελεστές. Παραδείγματος χάρη, ένας χρήστης που θέλει να προσομοιώσει χημικές διεργασίες θα πρέπει να δημιουργήσει ένα κβαντικό κύκλωμα το οποίο να αναπαριστά τη Χαμιλτονιανή Η του συστήματος.

2. Στο δεύτερο βήμα, ο χρήστης θα πρέπει να μετατρέψει το αφηρημένο κβαντικό κύκλωμα του πρώτου βήματος σε ένα νέο, βελτιστοποιημένο κύκλωμα με βάση το συγκεκριμένο hardware που θα διενεργήσει τους υπολογισμούς. Το βήμα αυτό μπορεί να περιλαμβάνει την προσαρμογή του κβαντικού κυκλώματος στην φυσική διάταξη των φυσικών qubits που θα χρησιμοποιηθούν, την μετατροπή των κβαντικών τελεστών σε βασικές πύλες που χρησιμοποιεί το hardware, την ελαχιστοποίηση του απαιτούμενου αριθμού πυλών και διεργασιών. Το βήμα αυτό είναι αναγκαίο, προκειμένου στο επόμενο βήμα, αυτό της εκτέλεσης, να βελτιστοποιηθεί η πιθανότητα επιτυχίας. Τα αφηρημένα κυκλώματα θα πρέπει να μετατραπούν σε κυκλώματα ISA (Instruction Set Architecture), τα οποία είναι τα μόνα που μπορούν να γίνουν κατανοητά από το κβαντικό hardware, καθώς ικανοποιούν περιορισμούς συνδεσιμότητας (coupling map). Το Qiskit έχει

ενσωματωμένες μεθόδους transpiling, με αποτέλεσμα ο χρήστης να χρειάζεται απλώς να τις εισάγει και να θέσει ως παραμέτρους το κύκλωμα και το συγκεκριμένο hardware στο οποίο θέλει να εκτελέσει το πρόγραμμα.

3. Στο τρίτο βήμα, ο χρήστης εκτελεί τα κυκλώματα στο επιθυμητό hardware και παράγει τα αποτελέσματα του κβαντικού υπολογισμού.

4. Στο τέταρτο και τελευταίο βήμα, ο χρήστης κάνει επεξεργασία των δεδομένων που έλαβε κατά την εκτέλεση των κβαντικών κυκλωμάτων. Το βήμα αυτό μπορεί να περιλαμβάνει διαφορετικά είδη κλασσικής επεξεργασίας δεδομένων, όπως απεικόνιση των αποτελεσμάτων ή τεχνικές μετριασμού των σφαλμάτων ανάγνωσης.

Στο συγκεκριμένο κεφάλαιο θα αναλυθούν τα πειράματα προσομοίωσης που διενεργήθηκαν, χρησιμοποιώντας τον προσομοιωτή BasicSimulator της κλάσης BasicSimulator του module qiskit.providers.basic_provider. Πρόκειται για έναν βασικό προσομοιωτή, ο οποίος προσομοιώνει τις διεργασίες και τα αποτελέσματα ενός κβαντικού υπολογιστή χωρίς την παρουσία θορύβου.

7.1 Original QFT

Χρησιμοποιώντας τη συνάρτηση Fmul που ορίζεται στο παράρτημα Α, θα εκτελέσουμε σε Jupyter notebooks τις παρακάτω εντολές, προκείμενου να μελετήσουμε κάποια πρώτα αποτελέσματα του αλγορίθμου που κατασκευάστηκε. Με τις εντολές που δίνουμε, το πρόγραμμα κατ' αρχάς εισάγει όλες τις απαραίτητες βιβλιοθήκες για την εκτέλεση της προσομοίωσης και στη συνέχεια ζητά από τον χρήστη να ορίσει τις τιμές του αριθμού των qubits, του αριθμού που θέλει να πολλαπλασιάσει και την τιμή της σταθερής παραμέτρου που ορίζεται ως «gamma». Εάν η τιμή gamma δεν ικανοποιεί τη συνθήκη gcd(2, gamma)=1, δηλαδή πρακτικά εάν η παράμετρος gamma οριστεί ως πολλαπλάσιο του 2, τότε το πρόγραμμα βγάζει σφάλμα και ζητάει νέα τιμή του gamma μέχρι να ικανοποιηθεί η παραπάνω συνθήκη. Στη συνέχεια, δημιουργείται ένα κβαντικό κύκλωμα, το οποίο αρχικοποιείται με βάση τον προς πολλαπλασιασμό αριθμό που έχει δώσει ο χρήστης και στη συνέχεια δίνεται ως είσοδος στη συνάρτηση Fmul προκειμένου να εκτελεστεί επάνω σε αυτό ο αλγόριθμος του QFT και στο τέλος αυτής της διαδικασίας διενεργείται μέτρηση των qubits του κυκλώματος. Έπειτα, καλείται ο προσομοιωτής, επάνω στις ιδιότητες του οποίου μετατρέπεται και προσαρμόζεται το κβαντικό κύκλωμα (transpiling).

Η προσομοίωση δίνει ως αποτέλεσμα τις πιθανές καταστάσεις που μπορούν να προκύψουν ως αποτέλεσμα της παραπάνω διαδικασίας με μια τιμή μετρήσεων counts για την κάθε μία, το συνολικό αριθμό των οποίων ορίζει ο χρήστης στην αρχή μέσω της μεταβλητής total_counts. Η κατάσταση που αντιστοιχεί στο μέγιστο αριθμό counts θεωρείται το «αποτέλεσμα» της διαδικασίας, το οποίο στη συνέχεια συγκρίνεται με το θεωρητικά αναμενόμενο αποτέλεσμα της πράξης του πολλαπλασιασμού. Για πιο ενδελεχή μελέτη των αποτελεσμάτων, ο χρήστης μπορεί στη συνέχεια να δημιουργήσει ιστογράμματα, προκειμένου να δει αναλυτικά τις πιθανές καταστά-

σεις και την πιθανότητα εμφάνισής τους, καθώς να παραστήσει γραφικά το κβαντικό κύκλωμα που έχει δημιουργηθεί προκειμένου να μελετήσει τα χαρακτηριστικά τους και να τα συγκρίνει με τα θεωρητικά αναμενόμενα.

Η ίδια διαδικασία θα χρησιμοποιηθεί με μικρές παραλλαγές για όλες τις προσομοιώσεις, αλλά και τα πειράματα που θα εκτελεστούν στον κβαντικό υπολογιστή της IBM στα πλαίσια της παρούσας Διπλωματικής Εργασίας.

Προτού δούμε συγκεκριμένα τα αποτελέσματα των προσομοίωσεων, ωστόσο, έχει σημασία να αναφερθεί ποια είναι τα αποτελέσματα που αναμένουμε να δούμε. Θεωρώντας, ότι διενεργείται μια «τέλεια» προσομοίωση ενός κβαντικού υπολογισμού χωρίς θόρυβο ή άλλους παράγοντες που μπορεί να επηρεάσουν τη διαδικασία, αναμένουμε το αποτέλεσμα της προσομοίωσης να είναι ακριβώς το επιθυμητό με πιθανότητα 1, δηλαδή η προσομοίωση να έχει ως αποτέλεσμα την κατάσταση που αντιστοιχεί στην επιθυμητή τιμή του πολλαπλασιασμού του αριθμού που δόθηκε από τον χρήση με την σταθερή παράμετρο gamma με αριθμό counts ίσο με την τιμή της μεταβλητής total_counts που έχει δώσει αρχικά ο χρήστης. Για παράδειγμα, εάν υποθέσουμε ότι ο χρήστης θέλει να κατασκευάσει ένα κύκλωμα τριών qubits με σκοπό να πολλαπλασιάσει τον αριθμό 2 με τη σταθερά πολλαπλασιασμού gamma 3 για συνολικό αριθμό total_counts = 1000, τότε αναμένουμε η προσομοίωση να έχει ως αποτέλεσμα την κατάσταση που αντιστοιχεί στον αριθμό 6 σε δυαδική μορφή με αριθμό counts = 1000, να είναι, δηλαδή, η μοναδική κατάσταση που είναι πιθανό να προκύψει.

Θα εκτελέσουμε προσομοίωση για αυτό ακριβώς το παράδειγμα, προκειμένου να εξετάσουμε την ορθότητα του συλλογισμού μας. Πράγματι, διεξάγοντας την παραπάνω διαδικασία παίρνουμε το παρακάτω ιστόγραμμα, το οποίο πληροί τα χαρακτηριστικά που περιγράφηκαν παραπάνω.

Παρατηρούμε, επίσης, ότι η γραφική απεικόνιση του κβαντικού κυκλώματος είναι ίδια με τη θεωρητικά αναμενόμενη όπως αυτή περιγράφηκε και απεικονίστηκε στο κεφάλαιο της θεωρητικής μελέτης του QFT.

Μπορούμε να δοκιμάσουμε την παραπάνω διαδικασία και για μεγαλύτερους αριθμούς, καθώς ο αλγόριθμος θα μπορούσε να λειτουργεί αποτελεσματικά για μικρές τιμές που απαιτούν απλούστερες υπολογιστικές διεργασίες, αλλά να χάνει την αξιοπιστία του για μεγαλύτερες τιμές. Στην πραγματικότητα, θα μελετήσουμε τα αποτελέσματα για μια «τυχαία» επιλογή των αριθμών που καλείται να δώσει ο χρήστης, τα οποία στη συνέχεια θα δοθούν ως είσοδος στην παραπάνω διαδικασία. Αυτό θα το επιτύχουμε, φτιάχνοντας ένα απλό πρόγραμμα παραγωγής ψευδοτυχαίων αριθμών με βάση τα modules math και random, το RNG, θέτοντας για λόγους υπολογιστικών πόρων ως μέγιστο αριθμό qubits τον αριθμό 20. Βρίσκουμε τις τιμές n=20 (αριθμός qubits), ninit=3 (αρχικός αριθμός που θα πολλαπλασιαστεί με τη σταθερά), gamma=150079 (σταθερά πολλαπλασιασμού). Με βάση αυτές τις τιμές, επαναλαμβάνουμε την παραπάνω διαδικασία και λαμβάνουμε το εξής ιστόγραμμα.

Παρατηρούμε, πως για τους τυχαίους αριθμούς λαμβάνουμε όντως την επιθυμητή κατάσταση με απόλυτη ακρίβεια, το οποίο αποδεικνύει, ότι ο αλγόριθμός

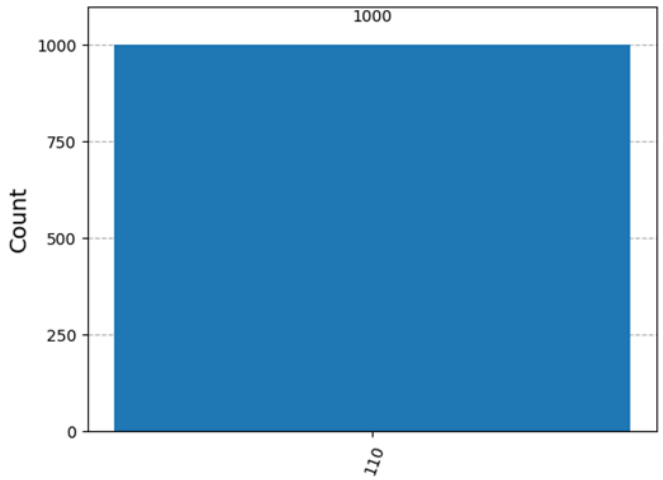


Figure 13: Ιστόγραμμα προσομοίωσης Original QFT για (3,2,3)

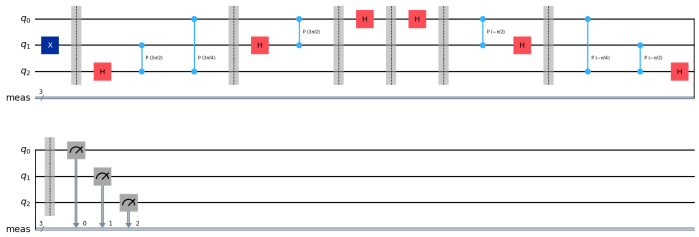


Figure 14: Κβαντικό κύκλωμα προσομοίωσης Original QFT (3,2,3)

μας είναι σωστός. Η γραφική απεικόνιση του κβαντικού κυκλώματος παραλείπεται, λόγω του τεράστιου μεγέθους της, καθώς δεν προσφέρει καμία πρόσθετη χρήσιμη πληροφορία ως προς την τοπολογία του κβαντικού κυκλώματος σε σχέση με την πολύ πιο απλή περίπτωση που μελετήθηκε προηγουμένως.

7.2 QFT με τοπικές αλληλεπιδράσεις (Local QFT)

Θα επαναλάβουμε την παραπάνω διαδικασία μελετώντας τα κβαντικά κυκλώματα mQFT που βασίζονται επάνω σε τοπικές μόνο αλληλεπιδράσεις [5] μέσω των συναρτήσεων mQFTlocal και mINVQFTlocal (Παράρτημα Α). Χρησιμοποιώντας το πρόγραμμα για τη δημιουργία τυχαίων αριθμών, θα μελετήσουμε την περίπτωση μικρών αριθμών για να ελέγξουμε σε ένα πρώτο επίπεδο την ορθότητα των αποτε-

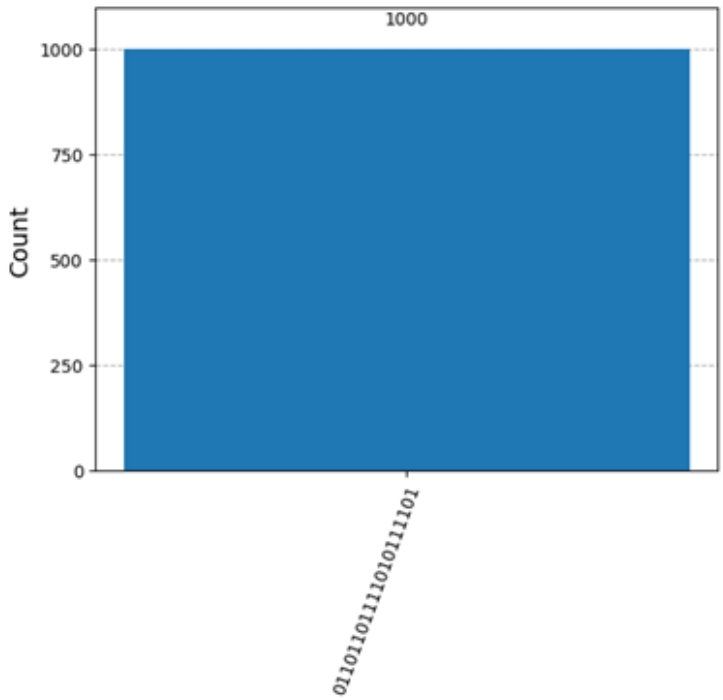


Figure 15: Ιστόγραμμα προσομοίωσης Original QFT (20,3,150079)

λεσμάτων, και στη συνέχεια για μεγαλύτερους αριθμούς, ώστε να γενικεύσουμε τα συμπεράσματά μας.

Για μέγιστο αριθμό qubits ίσο με 3, το RNG δίνει τις εξής τιμές n=2, ninit=1, gamma=3. Από αυτές, παίρνουμε το παρακάτω ιστόγραμμα και κύκλωμα.

Παρατηρούμε, ότι τα αποτελέσματα είναι τα αναμενόμενα. Δοκιμάζουμε τον αλγόριθμο για μεγαλύτερους αριθμούς βάζοντας στο πρόγραμμα τυχαίων αριθμών μέγιστο αριθμό qubits ξανά ίσο με το 20 και λαμβάνουμε τις τιμές n=19, ninit=9, gamma=32595 (Figure 17). Παρατηρούμε, ξανά, ότι όντως λαμβάνουμε το σωστό αποτέλεσμα.

7.3 Banded QFT

Σε αυτό το κεφάλαιο θα μελετήσουμε τη Banded εκδοχή του QFT, δηλαδή εκείνη την περίπτωση στην οποία το κάθε qubit αλληλεπιδρά μόνο με τους b κοντινότερους γείτονές του [6]. Η υλοποίηση αυτής της περίπτωσης δεν απαιτεί τη δημιουργία κάποιας νέας συνάρτησης, καθώς ο τρόπος με τον οποίο έχουμε εξαρχής κατασκευάσει τη συνάρτηση Fmul δίνει τη δυνατότητα να ορίσουμε τη μεταβλητή b. Εάν έχουμε n qubits, τότε εάν το b πάρει την τιμή n-1 θα έχουμε την περίπτωση του Original QFT, καθώς κάθε qubit θα αλληλεπιδράσει με όλους τους γείτονες που υπάρχουν. Σε αντίθετη περίπτωση, θα αλληλεπιδράσει με κάποιους μόνο από αυ-

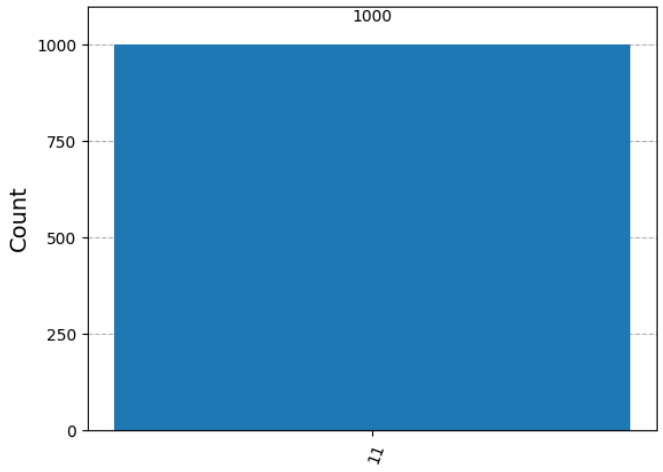


Figure 16: Ιστόγραμμα προσομοίωσης Local QFT (2,1,3)

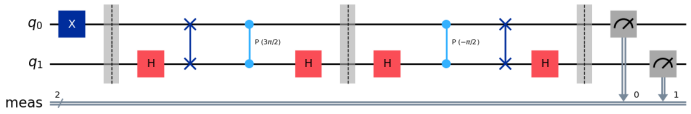


Figure 17: Κβαντικό κύκλωμα προσομοίωσης Local QFT (2,1,3)

τούς. Κατά την εκτέλεση του πειράματος, είναι βολικό το πρόγραμμα να ζητάει από το χρήστη να ορίσει την τιμή μιας παραμέτρου b' που αντιστοιχεί στον αριθμό των γειτόνων που ο χρήστης επιθυμεί να μην αλληλεπιδράσουν με το qubit. Τότε, η παράμετρος b της Fmul θα δίνεται από τη σχέση b= n - b' και με αυτόν τον τρόπο είναι πιο εύκολο να γίνει αντιληπτή η σχέση μεταξύ των δύο παραμέτρων n και b.

Ο Banded QFT έχει εγγενώς μειωμένη ακρίβεια, καθώς βασίζεται επάνω στην αφαίρεση πυλών C-Phase, προκειμένου να μειώσει το υπολογιστικό κόστος. Είναι προφανές, ότι αν η παράμετρος b πάρει τιμές, οι οποίες έχουν ως αποτέλεσμα την αφαίρεση του μεγαλύτερου τμήματος (ή ακόμα και όλων) των πυλών, η ακρίβεια του αποτελέσματος θα είναι όλο και μικρότερη. Για αυτό το λόγο, χρειάζεται προσεκτική επιλογή της, ώστε να επιτυγχάνεται ισορροπία μεταξύ της μείωσης του υπολογιστικού κόστους σε σχέση με την ακρίβεια των μετρήσεων. Επίσης, ακριβώς λόγω της εγγενούς μειωμένης ακρίβειάς της σε σχέση με τον Original QFT ή τον QFT που βασίζεται μόνο επάνω σε τοπικές αλληλεπιδράσεις, δεν αποτελεί αξιόπιστη μέθοδο για την επαλήθευση μιας αλγοριθμικής διαδικασίας.

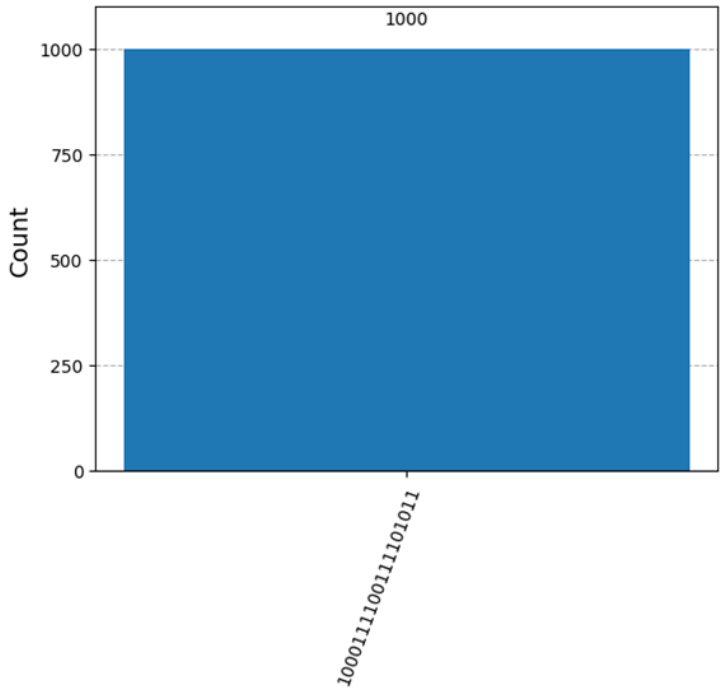


Figure 18: Ιστόγραμμα προσομοίωσης Local QFT (19,9,32595)

Για αρχή, θα παρουσιάσουμε, σε αναλογία με πριν, ενδεικτικά ιστογράμματα και γραφικές απεικονίσεις του BandedQFT για μικρές και μεγαλύτερες τιμές, ώστε να αποκτήσουμε μια διαίσθηση σε σχέση με τα αποτελέσματά του. Αυτό απαιτεί στο πρόγραμμα γέννησης ψευδοτυχαίων αριθμών να ορίσουμε μια ακόμα μεταβλητή b, η οποία θα παίρνει τιμές από το 1 έως το n-1. Λαμβάνουμε τις τιμές n=3, ninit=4, gamma=1, b=2 και παίρνουμε το παρακάτω ιστόγραμμα και κύκλωμα (Figure 18, 19).

Τα αποτελέσματα αυτά παρουσιάζουν ενδιαφέρον, διότι ενώ όντως το κβαντικό κύκλωμα φαίνεται να αποτελείται από qubits που αλληλεπιδρούν μόνο με τους n – 2 = 3 – 1 = 1 γείτονες, το αποτέλεσμα φαίνεται να έχει ακριβώς την ίδια ακρίβεια σε σχέση με τον Original QFT. Μάλιστα, θα μπορούσε κάποιος να υποθέσει, πως το κύκλωμα αυτό είναι ισοδύναμο με την περίπτωση ενός QFT μόνο με local interactions, με μόνη διαφορά την απουσία SWAP gates. Δηλαδή, να καταλήξει στο συμπέρασμα ότι μπορεί να έχει την ίδια ακρίβεια με τον local QFT γλιτώνοντας το υπολογιστικό κόστος των SWAP gates. Κάτι τέτοιο, φυσικά, δεν ισχύει όπως θα φανεί στην περίπτωση που οι τιμές των μεταβλητών είναι σημαντικά μεγαλύτερες.

Εκτελούμε εκ νέου το πρόγραμμα RNG και παίρνουμε τις τιμές n=11, ninit=3, gamma=453, b=9. Εκτελούμε ξανά το πρόγραμμα του Banded QFT με αυτές τις τιμές και παίρνουμε το παρακάτω ιστόγραμμα (Figure 20).

Παρατηρούμε, ότι για τις συγκεκριμένες τιμές η ακρίβεια της μέτρησης έχει μει-

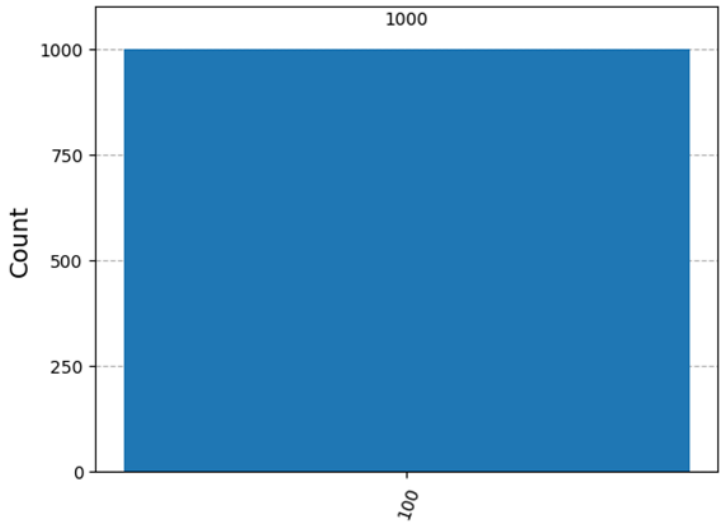


Figure 19: Ιστόγραμμα προσομοίωσης Banded QFT (3,4,1,2)

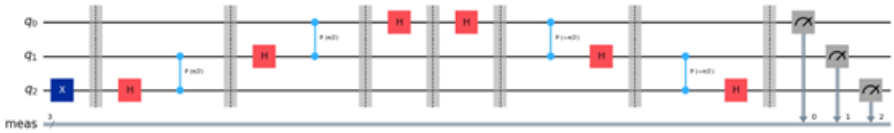


Figure 20: Κβαντικό κύκλωμα προσομοίωσης Banded QFT (3,4,1,2)

ωθεί σημαντικά, καθώς η κατάσταση που αντιστοιχεί στη σωστή τιμή εμφανίζεται μόνο στα 547 από τα 1000 counts, δηλαδή με πιθανότητα 54,7%. Το παράδειγμα αυτό είναι ενδεικτικό για τον τρόπο με τον οποίο ο μη προσεκτικός προσδιορισμός των μεταβλητών μπορεί να έχει τεράστια επίπτωση στην ακρίβεια των υπολογισμών μας.

Μπορούμε να ποσοτικοποιήσουμε την απόκλιση που έχουν τα αποτελέσματα του Banded QFT από αυτά του Original QFT, εισάγοντας μια στατιστική ποσότητα που θα μας φανεί ιδιαίτερα χρήσιμη κυρίως στο επόμενο κεφάλαιο.

Εάν συμβολίσουμε με U το ιδανικό κύκλωμα που προκύπτει από την προσομοίωση και V το κύκλωμα που προκύπτει από την εκτέλεση του προγράμματος στον πραγματικό κβαντικό υπολογιστή, τότε θα ορίσουμε την ποσότητα Total Variation Distance (TVD) ως

$$TVD(P_U, P_V) = \frac{1}{2} \sum_k |P_U(k) - P_V(k)| \tag{72}$$

όπου P_U, P_V είναι η κατανομή πιθανοτήτων των διαφόρων καταστάσεων που προκύπτουν ως έξοδος του κυκλώματος που απεικονίζονται με τη βοήθεια των

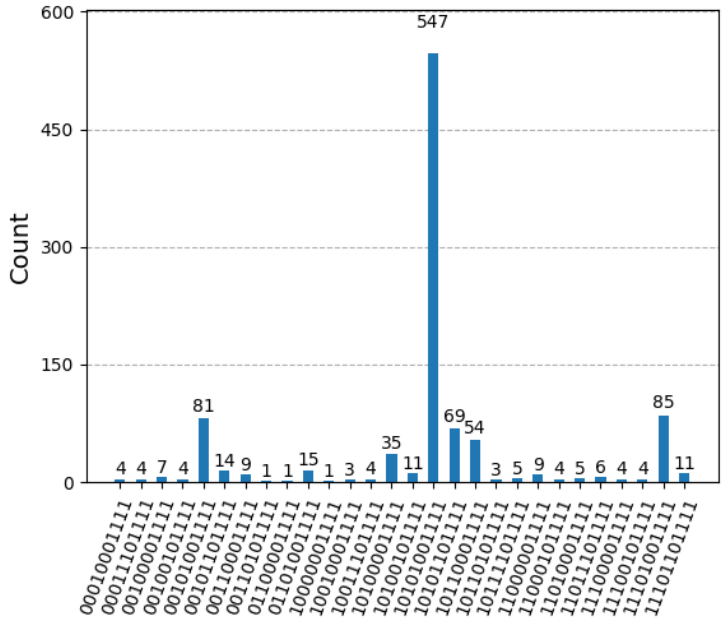


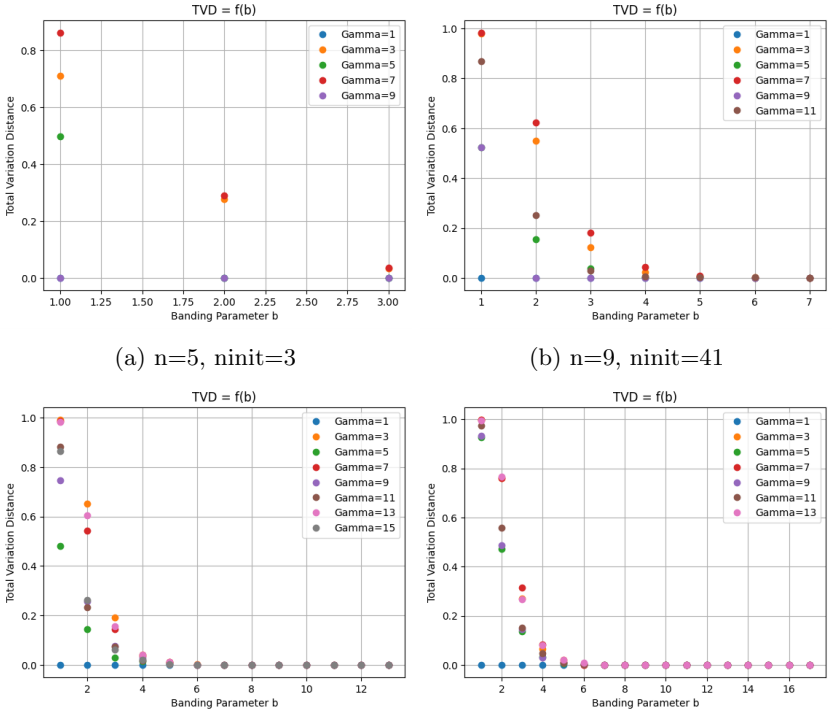
Figure 21: Ιστόγραμμα προσομοίωσης Banded QFT (11,3,453,9)

ιστογραμμάτων. Ορίζουμε την TVD με αυτόν τον τρόπο, διότι αποδεικνύεται, ότι $TVD(P_U, P_V) \leq E(U,V)$, όπου E είναι το μέτρο της απόστασης μεταξύ των δύο κυκλωμάτων, και δίνεται από τη σχέση

$$E(U,V) = \max_{|\psi\rangle} ||(U-V)|\psi\rangle|| = \max_{|\psi\rangle} ||U|\psi\rangle - V|\psi\rangle|| [8] \tag{73}$$

Χρησιμοποιώντας την Total Variation Distance, μπορούμε να εκφράσουμε την απόκλιση του Banded QFT από τον Original QFT ως συνάρτηση των παραμέτρων gamma και b, για σταθερή τιμή του αριθμού των qubits, το οποίο θα υπολογίσουμε δημιουργώντας το πρόγραμμα TVDBanded. Το TVDBanded λαμβάνει από το χρήστη δύο τιμές, την τιμή n του αριθμού των qubits και την τιμή ninit που είναι ο αριθμός προς πολλαπλασιασμό. Στη συνέχεια, εκτελεί μια επανάληψη επάνω στην παράμετρο πολλαπλασιασμού gamma από την τιμή 1 έως την τιμή που αντιστοιχεί στο ακέραιο μέρος της διαίρεσης της διάστασης dim $= 2^n$ του κυκλώματος προς τον αριθμό ninit. Με αυτόν τον τρόπο εξασφαλίζεται, ότι για τον δοσμένο αριθμό ninit, το γινόμενο ninit*gamma δε θα ξεπεράσει ποτέ τη διάσταση dim του προβλήματος δημιουργώντας άλλα προβλήματα. Μέσα στην επανάληψη gamma πραγματοποιείται μια δεύτερη επανάληψη επάνω στην παράμετρο b, η οποία λαμβάνει τιμές από το 1 μέχρι το n-2. Για κάθε τιμή του gamma και για κάθε τιμή του b, το πρόγραμμα υπολογίζει την TVD μεταξύ του Banded και του Original QFT. Στο τέλος, όλα αυτά τα δεδομένα απεικονίζονται σε μια γραφική παράσταση TVD=f(b) για διαφορετικές τιμές της σταθεράς gamma.

Θα χρησιμοποιήσουμε ξανά το πρόγραμμα RNG, υπολογίζοντας ψευδοτυχαίες τιμές μόνο για τις μεταβλητές n και ninit, έτσι ώστε να παραστήσουμε γραφικά ένα παράδειγμα αυτής της διαδικασίας, με σκοπό να εξάγουμε κάποια συμπεράσματα. Θα επαναλάβουμε τη διαδικασία 4 φορές σε διάφορα εύρη τιμών, που φαίνονται παρακάτω (Figure 21).



(a) n=5, ninit=3

(b) n=9, ninit=41

(c) n=15, ninit=2167

(d) n=19, ninit=37985

Figure 22: Γραφικές παραστάσεις TVD=f(b) για διάφορες τιμές της παραμέτρου gamma.

Είναι προφανές, ότι η μέθοδος είναι χρήσιμη βασικά για μεγάλο αριθμό qubits, καθώς τότε μπορούμε να γλιτώσουμε σημαντικό αριθμό πυλών χωρίς να χάνουμε ακρίβεια. Τα δύο τελευταία παραδείγματα είναι ενδεικτικά, καθώς μπορούμε να γλιτώσουμε πάνω από τις μισές αλληλεπιδράσεις με μακρινούς γείτονες έχοντας σχεδόν μηδενικό σφάλμα. Επίσης, σε όλες τις περιπτώσεις παρατηρούμε, ότι για πολλαπλασιασμό επί της μονάδας (gamma=1), η απόκλιση είναι μηδενική άσχετα με την τιμή της παραμέτρου b.

Στο επόμενο κεφάλαιο θα εξετάσουμε, πώς μπορούμε να χρησιμοποιήσουμε αυτήν την μεθοδολογία, ώστε να μειώσουμε το βάθος του κυκλώματος (depth) που θα εκτελέσουμε στον κβαντικό υπολογιστή.

8 Εκτέλεση σε πραγματικό κβαντικό υπολογιστή IBM-Q και αποτελέσματα

8.1 Εισαγωγή

Οι προσομοιώσεις που προηγήθηκαν δίνουν μια καλή «αίσθηση» της λειτουργίας των κβαντικών αλγορίθμων για πολλαπλασιασμό με σταθερό αριθμό, ωστόσο δεν αντικατοπτρίζουν ακριβώς τα αποτελέσματα της εκτέλεσής τους σε πραγματικό κβαντικό υπολογιστή. Στην παρούσα Διπλωματική Εργασία εκτελέστηκαν πάνω από 120 πειράματα στους διαθέσιμους προς χρήση κβαντικούς υπολογιστές IBM-Q, οι οποίοι βασίζονται στην υπεραγωγιμότητα μέσω Josephson junctions [9]. Η παρούσα εργασία δεν επικεντρώνεται αναλυτικά επάνω στις φυσικές διεργασίες της λειτουργίας του κβαντικού υπολογιστή, καθώς αυτές είναι τόσο πολύπλοκες που θα μπορούσαν να αποτελούν ξεχωριστή εργασία. Είναι αναγκαίο να ειπωθεί, όμως, ότι οι Josephson junctions («διακλαδώσεις» ή «συνδέσεις» Josephson) βασίζονται επάνω στο φαινόμενο Josephson, το οποίο παρατηρείται όταν δύο υπεραγωγοί χωρίζονται από έναν μονωτή. Τότε, παρατηρείται υπερ-ρεύμα I, το οποίο βρίσκεται σε θερμοδυναμική ισορροπία και συνεπώς δεν έχει απώλειες, υπό την έννοια ότι ρέει παρά το γεγονός ότι το χημικό δυναμικό των δύο υπεραγωγών είναι είναι εξ' ορισμού πανομοιότυπο εφόσον το σύστημα βρίσκεται σε θερμοδυναμική ισορροπία.

Εφαρμόζοντας μια πεπερασμένη διαφορά δυναμικού στη Josephson junction μπορεί και πάλι να παρατηρηθεί ροή υπερ-ρεύματος, δηλαδή ρεύμα το οποίο φέρεται από ζεύγη Cooper. Οι αλλαγές στην τάση αλλάζουν την ενέργεια των ηλεκτρονίων στους δύο υπεραγωγούς και άρα τη φάση τους, η οποία τότε δίνεται από τη σχέση φ=2eV/h. Η σχέση αυτή επιδρά στη δυναμική που αναπτύσσεται στη Josephson junction λόγω της εγγενούς συχνότητας 2eV/h. Η συχνότητα αυτή μπορεί να μετρηθεί στη συνέχεια εφαρμόζοντας εξωτερική ακτινοβολία ραδιοσυχνοτήτων (RF) και με αυτόν τον τρόπο, η σύνδεση μπορεί να δράσει ως μετατροπέας τάσης-συχνότητας με πολλές εφαρμογές [10].

Η διατήρηση του φυσικού συστήματος σε κατάσταση υπεραγωγιμότητας είναι μια πολύ δύσκολη διαδικασία και επηρεάζεται άμεσα τόσο από τον κάθε είδους θόρυβο του περιβάλλοντος, όσο και από την ίδια την τοπολογία του κβαντικού επεξεργαστή (QPU σε αναλογία του κλασσικού CPU) [11]. Η κατασκευή αποδοτικών κβαντικών υπολογιστών είναι ακόμα σε πρωτόλειο στάδιο, καθώς οι διαθέσιμοι προς χρήση στο κοινό κβαντικοί υπολογιστές μπορούν να υποστηρίξουν τη στιγμή συγγραφής της Διπλωματικής Εργασίας μέχρι 127 qubits. Τόσο η θεωρία όσο και η ίδια η πραγματικότητα, ωστόσο, αναδεικνύουν ότι ο περιορισμένος αριθμός των qubits δεν είναι η μόνη παράμετρος που θέτει δυσκολίες στην εκτέλεση πολύπλοκων κβαντικών υπολογισμών.

Ακριβώς επειδή η λειτουργία των κβαντικών υπολογιστών βασίζεται αποκλειστικά επάνω σε κβαντικές αλληλεπιδράσεις, όπως στην κβαντική σύμπλεξη, είναι πολύ εύκολο να προκύψει αποσυντονισμός (decoherence) στο κβαντικό σύστημα οδηγώντας πολύ γρήγορα σε -συχνά συνολική- απώλεια της ακρίβειας των υπολογισμών. Προφανώς, όσο μεγαλύτερος είναι ο αριθμός των qubits τόσο περισσότερες κβαντικές αλληλεπιδράσεις απαιτούνται και άρα είναι πιθανότερο να προκύ-

ψει αποσυντονισμός. Παράλληλα, όμως, ακόμα και για μικρό αριθμό qubits είναι πιθανό να προκύψει αποσυντονισμός εάν το πρόγραμμα που καλείται να εκτελέσει ο κβαντικός υπολογιστής είναι αρκετά πολύπλοκο απαιτώντας τα -έστω λίγα- qubits να πραγματοποιήσουν πολλές και σύνθετες αλληλεπιδράσεις μεταξύ τους.

Μια χρήσιμη ποσότητα για την περιγραφή αυτής της πολυπλοκότητας είναι το βάθος (depth) του κβαντικού κυκλώματος. Αν απεικονίζοντας ένα κβαντικό κύκλωμα θεωρήσουμε ότι αυτό μπορεί να χωριστεί σε μια ακολουθία από διακριτές time-slices, όπου η εφαρμογή μιας κβαντικής πύλης απαιτεί μια time-slice, τότε ορίζουμε ως βάθος (depth) τον συνολικό αριθμό των time-slices [2]. Ο αριθμός αυτός δεν ταυτίζεται απαραίτητα με τον συνολικό αριθμό των πυλών, καθώς πύλες που εφαρμόζονται σε διαφορετικά qubits μπορούν να εκτελούνται παράλληλα.

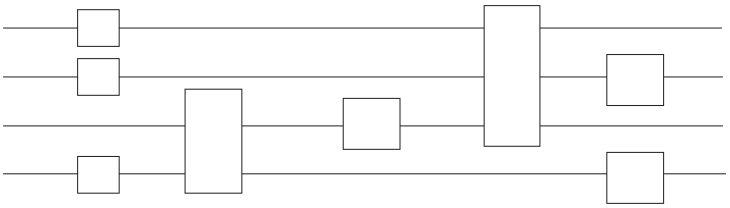


Figure 23: Κβαντικό κύκλωμα τεσσάρων qubits με βάθος(depth) 5 και συνολικό αριθμό πυλών 8 [2]

Το βάθος των κυκλωμάτων θα μας απασχολήσει ιδιαίτερα στην επόμενη ενότητα, καθώς ο QFT είναι ένας σχετικά πολύπλοκος αλγόριθμος, ο οποίος ακόμα και για μικρό αριθμό qubits, σύντομα δημιουργεί κβαντικά κυκλώματα που έχουν πολύ μεγάλο βάθος $\sim 2n^2$. Σε αυτό έρχεται να προστεθεί και η διαδικασία μετατροπής του κυκλώματος σε κύκλωμα που μπορεί να επεξεργαστεί ο κβαντικός υπολογιστής στο στάδιο του transpiling. Σε αυτό το στάδιο, οι κβαντικές πύλες του προγράμματός μας ανάγονται σε άλλες, με αναλογία που δεν είναι «1-1». Για παράδειγμα, οι πύλες C-Phase, που χρησιμοποιεί κατά κόρον ο αλγόριθμος του QFT, δεν εκτελούνται ως τέτοιες από τον κβαντικό υπολογιστή, αλλά αντίθετα ανάγονται σε ακολουθίες διαφόρων άλλων πυλών δημιουργώντας ένα transpiled κύκλωμα πολύ μεγαλύτερου βάθους από το αναμενόμενο.

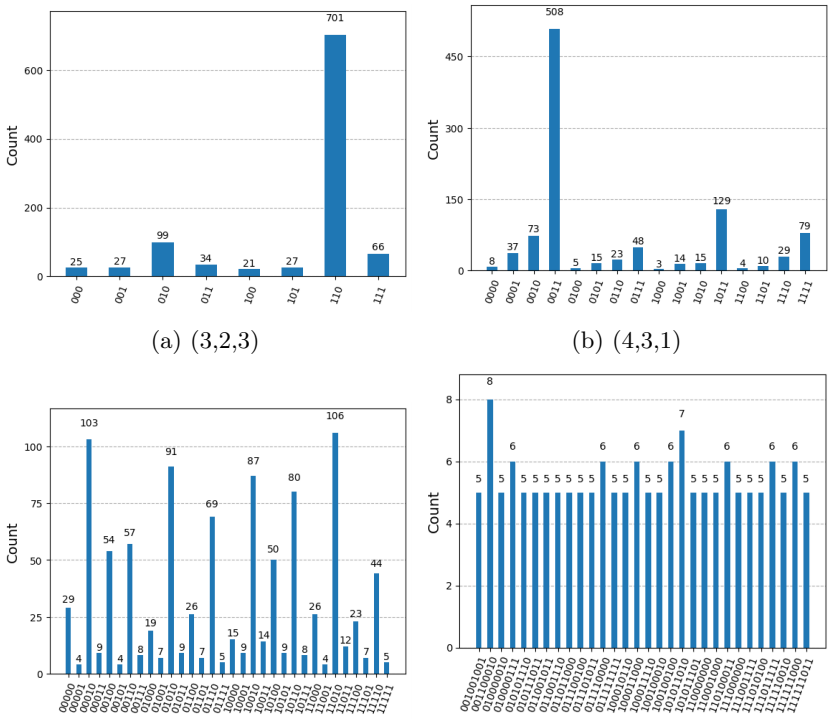
Είναι γνωστό και βιβλιογραφικά [12], ότι από ένα μέγεθος του depth και άνω, προκύπτει πλήρης αποσυντονισμός (decoherence) και οι υπολογισμοί παύουν να έχουν οποιαδήποτε ακρίβεια. Εμπειρικά, προσδιορίζεται αυτό το κατώφλι (threshold) περίπου στην τιμή depth = 200, το οποίο θα επαληθεύσουμε και εμείς πειραματικά στην ανάλυση που ακολουθεί.

Αξίζει να αναφερθεί, τέλος, ότι πέρα από τις προσπάθειες αναβάθμισης του υλικού (hardware) προκειμένου να κατασκευαστούν πιο σταθερά και «μονωμένα» από το θόρυβο του περιβάλλοντος κβαντικά συστήματα, η προσοχή των επιστημόνων έχει πέσει επάνω και στην ανάπτυξη της Κβαντικής Διόρθωσης Σφαλμάτων (Quantum Error Correction) [13] και την ανάπτυξη Fault-Tolerant Αλγορίθμων [14]. Με αυτόν τον τρόπο, οι κβαντικοί υπολογιστές θα μπορούν να εκτελέσουν

προβλήματα με σημαντικά μεγαλύτερη πολυπλοκότητα.

8.2 Original QFT

Θα χρησιμοποιήσουμε το πρόγραμμα παραγωγής ψευδοτυχαίων αριθμών RNG για να πάρουμε κάποιες «τυχαίες» τιμές, ώστε να μελετήσουμε τον αλγόριθμό μας. Οι τιμές αυτές είναι οι (n, ninit, gamma) : (3,2,3),(4,3,1),(5,6,3),(9,75,5). Για αυτές τις τιμές σε άυξοντα αριθμό qubits λαμβάνουμε τα παρακάτω αποτελέσματα (Figure 23).



(a) (3,2,3)

(b) (4,3,1)

(c) (5,6,3)

(d) Filtered (9,75,5)

Figure 24: Ιστογράμματα Original QFT σε κβαντικό υπολογιστή για διαφορετικές τιμές (n,ninit,gamma)

Στην περίπτωση (a) λαμβάνουμε το σωστό αποτέλεσμα (6) 701 φορές στις 1000 μετρήσεις, στην περίπτωση (b) 508 φορές στις 1000 μετρήσεις (σωστό αποτέλεσμα 3) και στην περίπτωση (c) 87 φορές στις 1000 μετρήσεις (σωστό αποτέλεσμα 18).

Στην περίπτωση (d) λόγω του μεγάλου αριθμού των πιθανών καταστάσεων δεν παρουσιάζεται το αρχικό ιστόγραμμα (καθώς δεν είναι ευκρινές), αλλά ένα «φιλτραρισμένο» ιστόγραμμα όπου αποτυπώνονται οι 30 καταστάσεις με το μεγαλύτερο αριθμό counts. Λαμβάνουμε το σωστό αποτέλεσμα (375) μόλις 1 φορά στις 1000 μετρήσεις. Καταλαβαίνουμε, ότι το αποτέλεσμα που μας δίνει η εκτέλεση του

προγράμματος δεν έχει καμία επιστημονική αξία. Εκτός του ότι η κατάσταση που αντιστοιχεί στο επιθυμητό αποτέλεσμα παρατηρείται με πιθανότητα 0,1%, δηλαδή δεν μπορεί να πραγματοποιηθεί οποιαδήποτε στατιστική μελέτη επάνω στο αποτέλεσμα, ο αριθμός των 1000 μετρήσεων φαίνεται να έχει «ισομοιραστεί» μεταξύ όλων των πιθανών κβαντικών καταστάσεων, καθώς ακόμα και αυτή με τη μεγαλύτερη πιθανότητα να παρατηρηθεί, παρατηρείται με πιθανότητα μόλις 0,8%. Το αποτέλεσμα αυτό εγείρει προβληματισμούς σε σχέση με την ορθότητα του αλγορίθμου μας, καθώς ήδη για αριθμό qubits ίσο με 4 η ακρίβεια είναι περίπου ίση με 50%.

Ωστόσο, με βάση τα όσα αναφέρθηκαν προηγουμένως είναι δόκιμο να μπορέσουμε να μελετήσουμε και άλλα χαρακτηριστικά του αλγορίθμου εκτός του πώς επηρεάζεται η ακρίβεια του σε σχέση με τον αριθμό των qubits. Για αυτό το λόγο θα πραγματοποιήσουμε μια γραφική παράσταση του βάθος (depth) ως συνάρτηση του αριθμού των qubits. Χρειάζεται προσοχή, ώστε να μετρήσουμε το βάθος του κυκλώματος μετά τη διαδικασία του transpiling, ώστε να έχουμε πραγματικά εικόνα σχετικά με το μέγεθος του κυκλώματος που εκτελεί ο κβαντικός υπολογιστής, άσχετα αν στη θεωρητική του εκδοχή όπως το κατασκευάζουμε εμείς είναι αισθητά μικρότερο. Γνωρίζουμε, ότι για κυκλώματα τιμής βάθους περίπου ίση με 200 επικρατεί αποσυντονισμός και τα αποτελέσματα παύουν να είναι ακριβή. Από τις μετρήσεις μας παρατηρούμε, ότι ήδη για n=4 qubits τα αποτελέσματα σταματούν να έχουν καλή στατιστική. Άρα, εάν στη γραφική παράσταση η τιμή n=4 qubits αντιστοιχεί περίπου σε βάθος depth=200, τότε μπορούμε να εξάγουμε δύο βασικά συμπεράσματα:

1. Μπορούμε να επαληθεύσουμε τον εμπειρικό κανόνα για την τιμή depth≈200.

2. Δεν έχει νόημα να κάνουμε μετρήσεις για μεγαλύτερο αριθμό qubits και μπορούμε να προσπαθήσουμε να περιγράψουμε την σταδιακή απώλεια ακρίβειας μέσω μιας στατιστικής ποσότητας που να τεκμηριώνει τις υποθέσεις μας.

Η γραφική παράσταση του βάθους του κβαντικού κυκλώματος ως συνάρτηση του αριθμού των qubits n για τον Original QFT φαίνεται παρακάτω (Figure 24).

Πράγματι, η γραφική παράσταση είναι διαφωτιστική. Πρώτον, παρατηρούμε, ότι η συνάρτηση του βάθος φαίνεται όντως να προσομοιάζει τη συμπεριφορά μιας τετραγωνικής συνάρτησης όπως αναμένουμε θεωρητικά. Δεύτερον, φαίνεται, ότι για n=4 το βάθος του κυκλώματος όντως είναι κοντά στην τιμή 200, άρα οι πειραματικές μας μετρήσεις φαίνεται όντως να επιβεβαιώνουν τον εμπειρικό κανόνα. Τρίτον, εξηγούνται τα αποτελέσματα που πήραμε για την περίπτωση (9,75,5) καθώς για n=9, το βάθος του κυκλώματος έχει τιμή μεγαλύτερη του 1250, δηλαδή επικρατεί πλήρης αποσυντονισμός και τα αποτελέσματα δεν έχουν καμία στατιστική αξία.

Θα αποδείξουμε τα λογικά αποτελέσματα της παραπάνω γραφικής παράσταση, χρησιμοποιώντας ξανά την στατιστική ποσότητα Total Variance Distance (TVD) μεταξύ του πραγματικού αποτελέσματος που λαμβάνουμε μέσω της προσομοίωσης του αλγορίθμου QFT και του αποτελέσματος που λαμβάνουμε από την εκτέλεση τον κβαντικό υπολογιστή. Η γραφική παράσταση της συνάρτησης της TVD ως προς ψευδοτυχαίες τιμές του αριθμού των qubits n φαίνονται παρακάτω (Figure

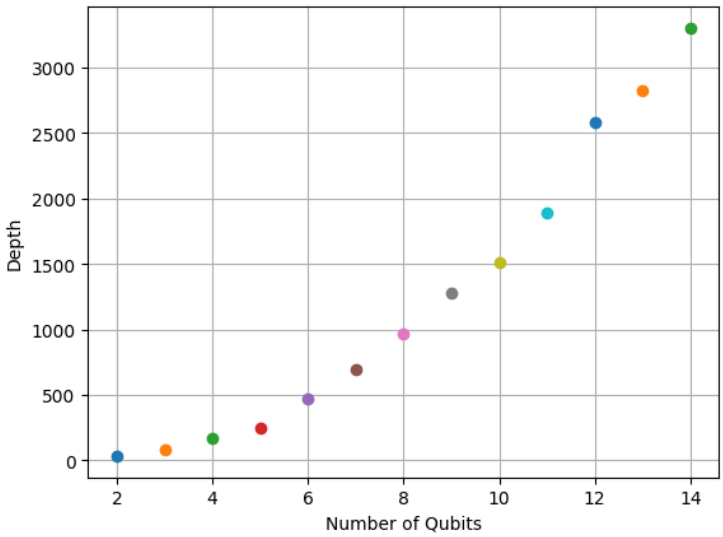


Figure 25: Γραφική παράσταση Depth = f(n)

25).

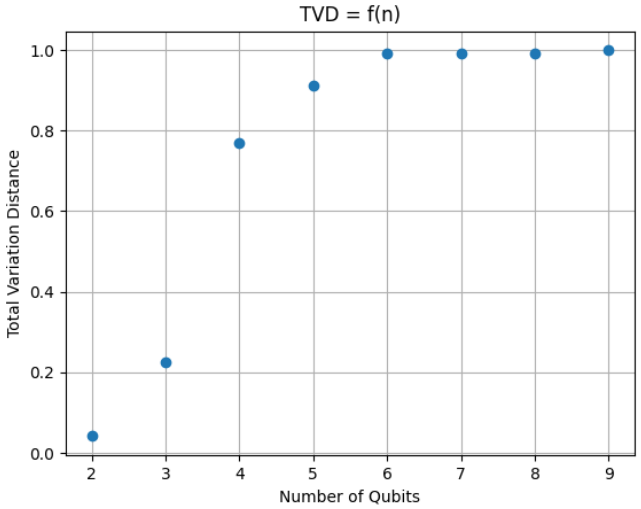


Figure 26: Γραφική παράσταση TVD = f(n)

Η γραφική παράσταση αποδεικνύει, ότι από n=3 σε n=4 qubits η TVD κάνει ένα «άλμα» το οποίο εξηγεί την απότομη μείωση της στατιστικής ακρίβειας. Επίσης, βλέπουμε, ότι για n=6 και άνω η TVD είναι πρακτικά ίση με τη μονάδα,

δηλαδή υπάρχει πρακτικά μηδενική ακρίβεια στα αποτελέσματα. Θα προσπαθήσουμε να βελτιώσουμε τη μελέτη της παραπάνω γραφικής παράστασης, επικεντρώνοντας την προσοχή μας στους μικρότερους αριθμούς qubits, για τον καθένα από τον οποίο θα εκτελέσουμε αρκετές φορές το πρόγραμμα TVD με χρήση ψευδοτυχαίων αριθμών και στη συνέχεια θα πραγματοποιήσουμε γραφική παράσταση (Figure 26) χρησιμοποιώντας τις μέσες τιμές της TVD αυτών των μετρήσεων, οι οποίες φαίνονται στον παρακάτω πίνακα (Table 1).

number of qubits	**number**	**gamma**	**TVD**	**TVD_mean**
	3	1	0.042	
2	2	1	0.043	0.048
	1	3	0.059	
	2	3	0.226	
3	1	5	0.251	0.216
	7	1	0.171	
	12	1	0.77	
4	5	3	0.608	0.722
	2	7	0.787	
	6	3	0.913	
5	3	7	1.00	0.948
	3	9	0.932	
	8	7	0.992	
6	20	3	0.98	0.978
	5	11	0.963	
	17	7	0.992	
7	9	13	0.985	0.989
	5	25	0.991	

Table 1: Πίνακας τιμών TVD και μέσης τιμής TVD για διαφορετικές τιμές n, ninit, gamma για τον QFT

Από τη γραφική παράσταση βλέπουμε, ότι όντως επαληθεύονται τα παραπάνω αποτελέσματα.

8.3 QFT με τοπικές αλληλεπιδράσεις (Local QFT)

Θα επαναλάβουμε την παραπάνω διαδικασία για την περίπτωση κυκλωμάτων που βασίζονται μόνο σε local αλληλεπιδράσεις και σε όλα τα στάδια θα χρησιμοποιήσουμε τους ίδιους ψευδοτυχαίους αριθμούς με την περίπτωση του Original QFT, ώστε η σύγκριση των αποτελεσμάτων να είναι όσο το δυνατόν πιο αξιόπιστη. Επομένως, θα εξετάσουμε ξανά τα αποτελέσματα για τις περιπτώσεις (n, ninit, gamma) : (3,2,3),(4,3,1),(5,6,3),(9,75,5) πραγματοποιώντας τα ιστογράμματα (Figure 27).

Στην περίπτωση (a) λαμβάνουμε το σωστό αποτέλεσμα (6) 485 φορές στις 1000 μετρήσεις, στην περίπτωση (b) 161 φορές στις 1000 μετρήσεις (σωστό αποτέλεσμα

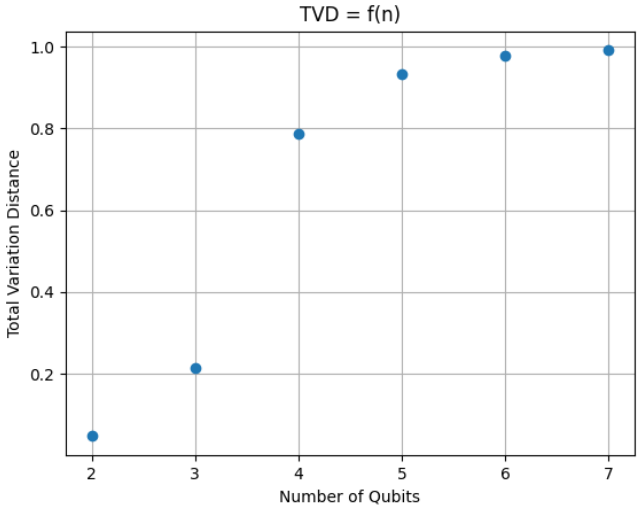
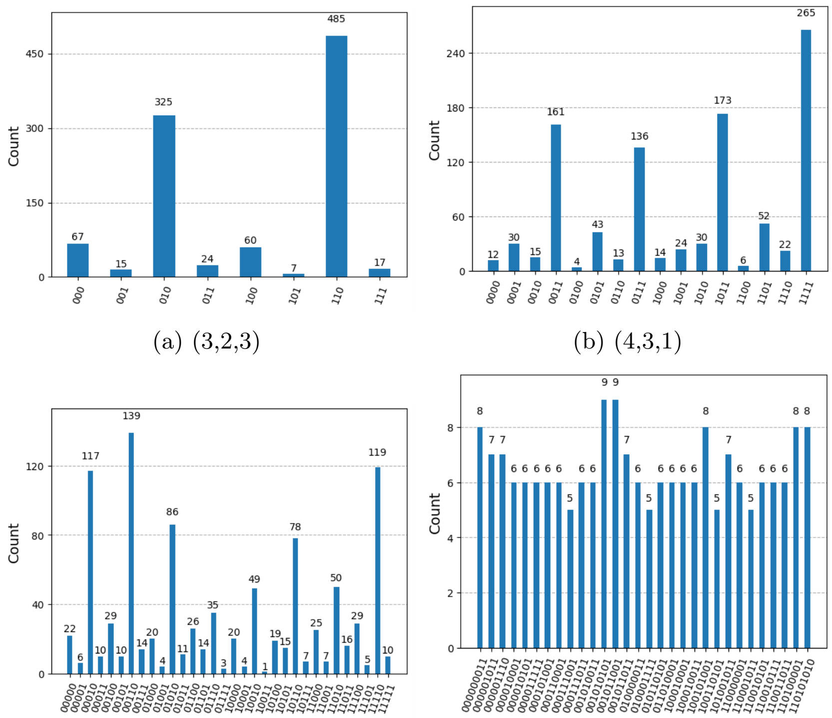


Figure 27: Γραφική παράσταση TVD = f(n) χρησιμοποιώντας το μέσο όρο ψευδοτυχαίων τιμών

3) και στην περίπτωση (c) 49 φορές στις 1000 μετρήσεις (σωστό αποτέλεσμα 18).

Στην περίπτωση (c) λόγω του μεγάλου αριθμού των πιθανών καταστάσεων παρουσιάζεται ξανά το «φιλτραρισμένο» ιστόγραμμα όπου αποτυπώνονται οι 30 καταστάσεις με το μεγαλύτερο αριθμό counts. Λαμβάνουμε το σωστό αποτέλεσμα (375) μόλις 1 φορά στις 1000 μετρήσεις. Παρατηρούμε, ότι τα αποτελέσματα παρουσιάζουν ομοιότητα με αυτά που βρήκαμε στην περίπτωση του Original QFT, με εξαίρεση ίσως, ότι οι τιμές φαίνεται πως ξεκινούν να χάνουν την ακρίβεια τους από ακόμα μικρότερες τιμές n. Από τη θεωρία, γνωρίζουμε πως το βάθος των κυκλωμάτων που βασίζονται μόνο σε τοπικές αλληλεπιδράσεις αυξάνεται σύμφωνα με μια γραμμική σχέση $\sim 4n$, άρα αυτό θα μπορούσε να εξηγεί την γρήγορη αύξηση του βάθους ήδη από μικρές τιμές του n. Αρκεί να επιβεβαιώσουμε αυτή τη θεωρητική πρόβλεψη δημιουργώντας όπως και πριν τη γραφική παράσταση του βάθους του κυκλώματος μετά το transpiling ως συνάρτηση του αριθμού των qubits n (Figure 28).

Πράγματι, παρατηρούμε, πως το βάθος φαίνεται να ικανοποιεί μια γραμμική σχέση. Η γραφική παράσταση δίνει εξήγηση στο γιατί η ακρίβεια μειώνεται ήδη για n=3, καθώς ήδη στα 3 qubits το βάθος του κβαντικού κυκλώματος πλησιάζει την τιμή 200. Η γραμμική σχέση, παρ' όλα αυτά, δεν έχει ως συνέπεια μόνο την γρήγορη αύξηση του βάθους ήδη από τις μικρές τιμές n. Παράλληλα με αυτό, εξασφαλίζει για τις μεγάλες τιμές του αριθμού των qubits μικρότερη τιμή βάθους σε σχέση με τον Original QFT που ικανοποιεί μια τετραγωνική σχέση. Πράγματι, αν συγκρίνουμε τις δύο γραφικές παραστάσεις είναι σαφές αυτό το πλεονέκτημα. Για παράδειγμα, αν προσέξουμε το παράδειγμα για n=8, στην περίπτωση του Local QFT το βάθος είναι περίπου ίσο με 800, ενώ για την ίδια τιμή qubits στην



(a) (3,2,3) (b) (4,3,1)

(c) (5,6,3) (d) Filtered (9,75,5)

Figure 28: Ιστογράμματα Local QFT σε κβαντικό υπολογιστή για διαφορετικές τιμές (n,ninit,gamma)

περίπτωση του Original QFT το βάθος είναι περίπου ίσο με 1500. Αυτή είναι μια πολύ σημαντική ένδειξη, διότι υποδηλώνει πως για κβαντικούς υπολογιστές που μπορούν να υποστηρίξουν χωρίς decoherence μεγαλύτερες τιμές βάθους, η εφαρμογή του Local QFT μπορεί να είναι πιο αποδοτική δίνοντας στο χρήστη την ικανότητα να αξιοποιεί στους υπολογισμούς του μεγαλύτερο αριθμό qubits για την ίδια τιμή βάθους.

Θα επιδιώξουμε ξανά να αποδείξουμε τις παραπάνω υποθέσεις χρησιμοποιώντας τη στατιστική ποσότητα TVD πρώτα για ένα μεγάλο σχετικά εύρος τιμών (Figure 29) και -εφ' όσον υπάρχει αναλογία με την προηγούμενη ενότητα- για μια περιοχή μικρότερων τιμών του αριθμού των qubits.

Εφ' όσον υπάρχει αντιστοιχία με τον Original QFT θα πραγματοποιήσουμε τη γραφική παράσταση (Figure 30) χρησιμοποιώντας τις μέσες τιμές των μετρήσεων που πραγματοποιήσαμε, χρησιμοποιώντας τους ίδιους ψευδοτυχαίους αριθμούς (Table 2).

Συμπεραίνουμε πως επαληθεύονται τα παραπάνω αποτελέσματα. Είναι σημαντικό, επίσης, να αναφερθεί, ότι όλες οι παραπάνω μετρήσεις που διεξήχθησαν στον κβαντικό υπολογιστή (jobs) απαιτούν ελάχιστο πραγματικό χρόνο για να

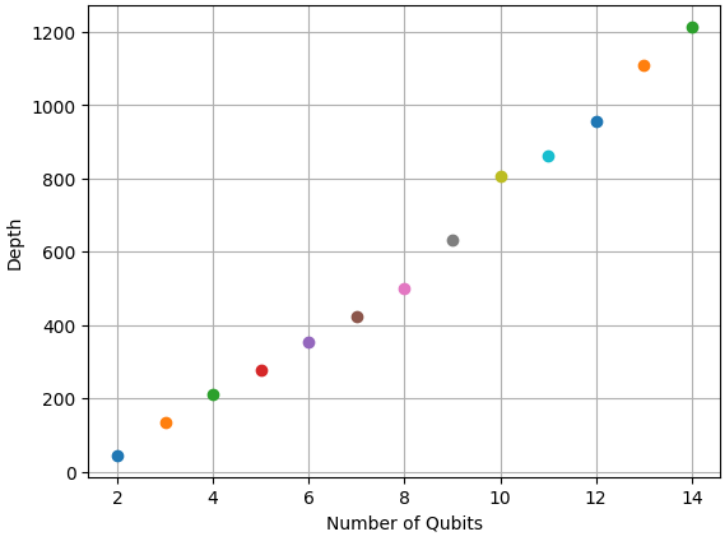


Figure 29: Γραφική παράσταση depth = f(n) για τον Local QFT

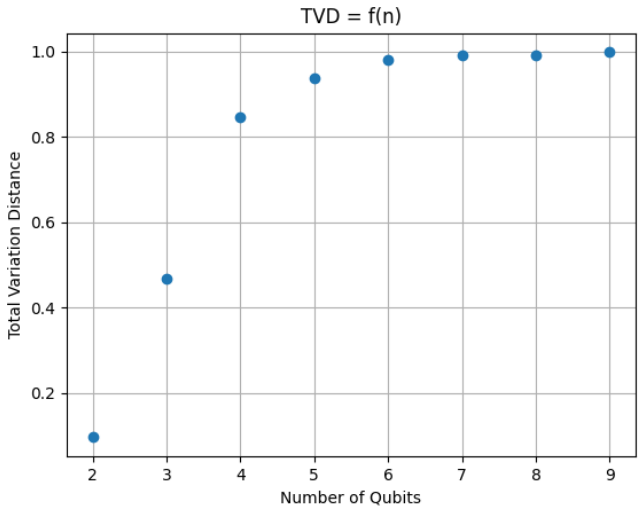


Figure 30: Γραφική παράσταση TVD = f(n) για τον Local QFT

ολοκληρωθούν. Κάθε job απαιτεί περίπου 1 δευτερόλεπτο πραγματικού χρόνου, ώστε τα αποτελέσματα του job να είναι διαθέσιμα στο χρήστη μέσω ενός μοναδικού job_id που περιέχει όλες τις απαραίτητες πληροφορίες. Παρά το γεγονός ότι η εκτέλεση προγραμμάτων στους κβαντικούς υπολογιστές της IBM απαιτούν ελάχιστο πραγματικό χρόνο για να εκτελεστούν, η διαδικασία αυτή συνολικά είναι ιδιαίτερα

number of qubits	number	gamma	TVD	TVD_mean
	3	1	0.042	
2	2	1	0.043	0.042
	1	3	0.059	
	2	3	0.226	
3	1	5	0.251	0.153
	7	1	0.171	
	12	1	0.77	
4	5	3	0.608	0.836
	2	7	0.787	
	6	3	0.913	
5	3	7	1.00	0.916
	3	9	0.932	
	8	7	0.992	
6	20	3	0.98	0.981
	5	11	0.963	
	17	7	0.992	
7	9	13	0.985	0.994
	5	25	0.991	

Table 2: Πίνακας τιμών TVD και μέσης τιμής TVD για διαφορετικές τιμές n, ninit, gamma για τον Local QFT

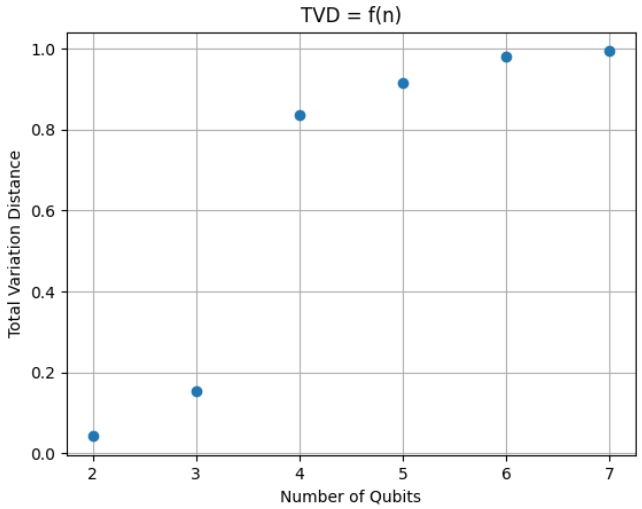


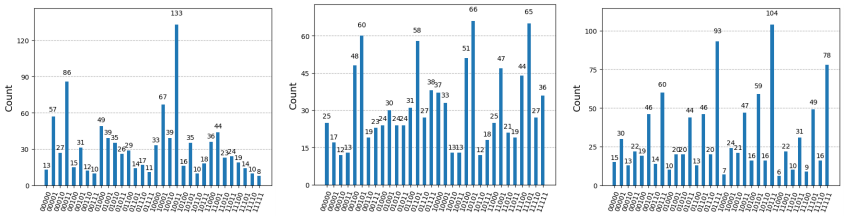
Figure 31: Γραφική παράσταση TVD = f(n) για τον Local QFT χρησιμοποιώντας μέσους όρους ψευδοτυχαίων τιμών

χρονοβόρα. Αυτό, διότι λόγω του μεγάλου αριθμού jobs που αποστέλλονται από τους χρήστες παγκοσμίως, το κάθε job τοποθετείται σε μια ουρά προτεραιότητας (queue). Η αναμονή σε αυτήν την ουρά μπορεί να διαρκέσει από λεπτά μέχρι αρκετές ώρες ανάλογα με τον αριθμό και την πολυπλοκότητα των jobs που έχουν σταλεί προς εκτέλεση. Επίσης, ο κάθε χρήστης μπορεί να στείλει παράλληλα μέχρι 3 jobs στην ουρά προτεραιότητας, έτσι ώστε όλοι οι χρήστες να μπορούν να έχουν ισότιμη πρόσβαση στον κβαντικό υπολογιστή. Επομένως, παρόλο που ο πραγματικός χρόνος εκτέλεσης των προγραμμάτων μας είναι ελάχιστος, το χρονικό διάστημα από την αποστολή των προγραμμάτων μέχρι την εκτέλεση και την παραλαβή των αποτελεσμάτων τους μπορεί να είναι ιδιαίτερα μεγάλο.

8.4 Banded QFT

Όπως δείχθηκε στο προηγούμενο κεφάλαιο των προσομοιώσεων, η ακρίβεια του Banded QFT εξαρτάται έντονα από την τιμή της παραμέτρου b που προσδιορίζει τον αριθμό των πλησιέστερων γειτόνων με τους οποίους θα αλληλεπιδράσει το qubit. Μπορούμε να αποκτήσουμε μια διαίσθηση της δράσης του Banded QFT μελετώντας τη γραφική παράσταση της προσομοίωσης n=5, ninit=3. Η τιμή n=5 γνωρίζουμε, ότι είναι στην περιοχή όπου τα φαινόμενα αποσυντονισμού είναι ήδη αρκετά έντονα καθώς το βάθος υπερβαίνει ήδη την τιμή 200 με βάση τις γραφικές παραστάσεις που έχουμε σχεδιάσει παραπάνω.

Η υπόθεση είναι να εκτελέσουμε Banded QFT για n=5, ninit=3, gamma=3 και τιμή της παραμέτρου b=2 και b=3, ώστε αποφανθούμε συγκρίνοντας τα αποτελέσματα αυτά με τα αποτελέσματα του Original QFT για τις ίδιες τιμές σχετικά με το αν η προσεκτική χρήση του Banded QFT μπορεί να είναι χρήσιμη για την βελτίωση της ακρίβειας των υπολογισμών. Τα αποτελέσματα φαίνονται στα παρακάτω ιστογράμματα(Figure 31).



(a) Original(5,3,3) (b) Banded(5,3,3,2) (c) Banded(5,3,3,3)

Figure 32: Συγκριτικά ιστογράμματα Original και Banded QFT σε κβαντικό υπολογιστή για (5,3,3)

Στην περίπτωση (a) το σωστό αποτέλεσμα (9) εμφανίζεται 39 φορές στις 1000 μετρήσεις, το βάθος του κυκλώματος είναι ίσο με depth=266 και έχει TVD=0.961. Στην περίπτωση (b) το σωστό αποτέλεσμα (9) εμφανίζεται 30 φορές στις 1000 μετρήσεις, έχει βάθος ίσο με depth=256 και TVD=0.874. Στην περίπτωση (c) το σωστό αποτέλεσμα (9) εμφανίζεται 20 φορές στις 1000 μετρήσεις, έχει βάθος ίσο με depth=236 και TVD=0.956.

Τα αποτελέσματα αυτά δεν είναι ιδιαίτερα ενθαρρυντικά για την υπόθεση που κάναμε, καθώς με τη χρήση του Banded QFT ούτε το βάθος φαίνεται να μειώνεται επαρκώς ώστε να αποφύγουμε τα φαινόμενα decoherence, ούτε η πιθανότητα να λάβουμε το σωστό αποτέλεσμα είναι μεγαλύτερη. Το αντίθετο, ο Original QFT παρουσιάζει τη μέγιστη πιθανότητα εύρεσης του σωστού αποτελέσματος. Επίσης, δε θα είχε νόημα να ερευνήσουμε τα αποτελέσματα για μεγαλύτερο αριθμό qubits, καθώς λόγω της τετραγωνικής αύξησης του βάθους συναρτήσει του αριθμού των qubits, ο ρυθμός με τον οποίο το βάθος θα αυξάνεται αυξάνοντας το n θα είναι πολύ μεγαλύτερος σε σχέση με το ρυθμό μείωσης του βάθους λόγω της αφαίρεσης πυλών μέσω του Banded QFT, ο οποίος, εξάλλου, όσο περισσότερες πύλες αφαιρεί από το κύκλωμα τόσο μειώνει την ακρίβεια της μέτρησης.

Περισσότερες πιθανότητες να εξάγουμε χρήσιμα αποτελέσματα έχουμε, ενδεχομένως, συνδυάζοντας τον Banded QFT με τον Local QFT, συνδυάζοντας τη γραμμική αύξηση του βάθους των κυκλωμάτων του ως συνάρτηση του n. Για το λόγο αυτό, θα κατασκευάσουμε μια νέα συνάρτηση, τη BandedLocalQFT. Η μεθοδολογία που θα ακολουθήσουμε είναι η εξής:

1. Από τη γραφική παράσταση QFTLocal_Depth=f(n) θα προσδιορίσουμε ποιες τιμές του n στα πλαίσια της γραμμικής αύξησης έχει νόημα να ελέγξουμε μέσω προσομοίωσης. Είναι προφανές, ότι ακόμα και στη γραμμική σχέση για μεγάλους αριθμούς n το βάθος είναι πολύ μεγαλύτερο του 200.

2. Στη συνέχεια θα πραγματοποιήσουμε μια γραφική παράσταση depth=f(b) χρησιμοποιώντας BandedLocalQFT για τις συγκεκριμένες τιμές που προσδιορίσαμε στο βήμα 1 χρησιμοποιώντας ξανά προσομοίωση.

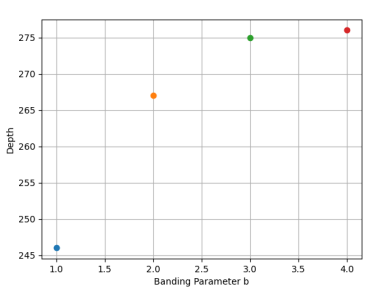
3. Θα κάνουμε, επίσης, τη γραφική παράσταση TVD=f(b), ώστε να προσδιορίσουμε ποιες είναι οι βέλτιστες τιμές, για τις οποίες στη συνέχεια θα ελέγξουμε εάν υπάρχει συγκριτικό πλεονέκτημα σε σχέση με τον Original QFT εκτελώντας τα προγράμματα στον πραγματικο κβαντικό υπολογιστή.

Με βάση τη γραφική παράσταση Local_Depth=f(n), θα ελέγξουμε τις περιπτώσεις n=5 και n=6, καθώς για μεγαλύτερες τιμές του n το βάθος υπερβαίνει τον αριθμό 400, δηλαδή το διπλάσιο του εμπειρικού ορίου. Για την κατασκευή της γραφικής παράστασης Depth=f(n) θα χρησιμοποιήσουμε όπως και πριν τις τιμές (5,3,3) για διάφορες τιμές του b (Figure 32) και με χρήση του προγράμματος RNG κατασκευάζουμε ένα σύνολο τιμών για n=6, το οποίο είναι το (6,9,5) (Figure 33). Για την δημιουργία των γραφικών παραστάσεων depth=f(b) και TVD=f(b) θα δημιουργήσουμε δύο νέα προγράμματα, το QFTBandedLocal_Depth=f(b) και το TVDBandedLocal.

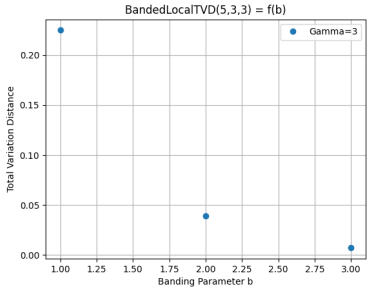
Με βάση τις γραφικές παραστάσεις, για την περίπτωση (5,3,3) θα κάνουμε τη σύγκριση για b=1, b=2 και b=3 (Figure 34).

Με βάση τις γραφικές παραστάσεις, για την περίπτωση (6,9,5) θα κάνουμε τη σύγκριση για b=1, b=2 και b=3 (Figure 35).

Η σύγκριση μεταξύ των δύο μεθόδων θα γίνει μελετώντας για κάθε μία από τις δύο περιπτώσεις δύο γραφικές παραστάσεις. Η πρώτη θα απεικονίζει το βάθος ως

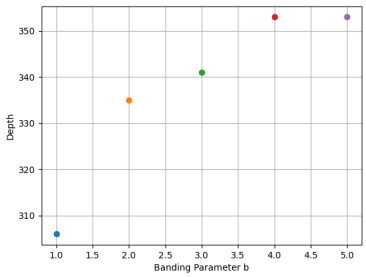


(a) Depth = f(b) (5,3,3)

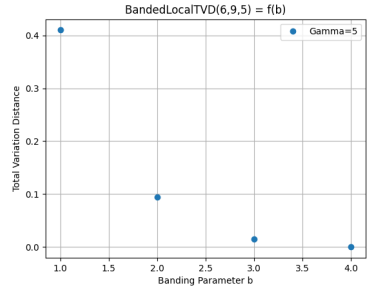


(b) TVD = f(b) (5,3,3)

Figure 33: Γραφικές παραστάσεις depth, TVD = f(b) για Local Banded QFT για τις την περίπτωση (5,3,3)



(a) Depth = f(b) (6,9,5)



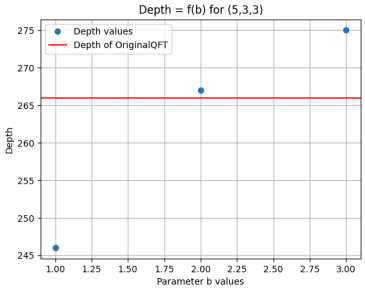
(b) TVD = f(b) (6,9,5)

Figure 34: Γραφικές παραστάσεις depth, TVD = f(n) για Local Banded QFT για την περίπτωση (6,9,5)

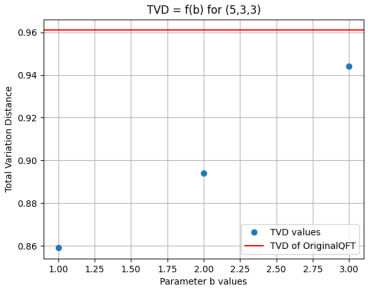
συνάρτηση του b και το δεύτερο την TVD ως συνάρτηση του b. Στις γραφικές παραστάσεις θα απεικονίζονται οι τιμές που προέκυψαν από την εκτέλεση των προγραμμάτων στον πραγματικό κβαντικό υπολογιστή, σε αντίθεση με τις παραπάνω γραφικές παραστάσεις που έχουν προκύψει μέσω προσομοίωσης, προκειμένου να μας κατατοπίσουν στο εύρος τιμών που έχει νόημα να διερευνήσουμε. Από τη δεύτερη γραφική παράσταση μπορούμε να προσδιορίσουμε αν μία από τις δύο μεθόδους έχει μεγαλύτερη ακρίβεια στους υπολογισμούς και, χρησιμοποιώντας το πρώτο, να εξετάσουμε τη συσχέτιση με το βάθος.

Αρχικά, θα μελετήσουμε την περίπτωση (5,3,3) δημιουργώντας τις παραπάνω γραφικές παραστάσεις (Figure 34) και στη συνέχεια την περίπτωση (6,9,5) (Figure 36).

Για την περίπτωση (5,3,3) παρατηρούμε, πως για όλες τις τιμές της παραμέτρου b, η TVD της BandedLocal μεθόδου είναι μικρότερη από την TVD της Original μεθόδου. Ακόμα και για τις τιμές b=2 και b=3, για τις οποίες το βάθος της BandedLocal είναι μεγαλύτερο από το βάθος της Original, και σε αυτές τις περιπτώσεις



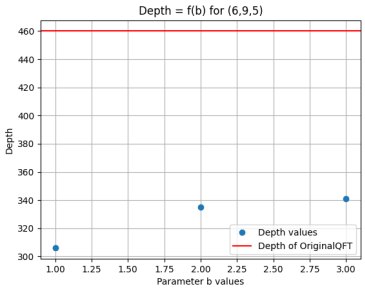
(a) Depth = f(b) (5,3,3)



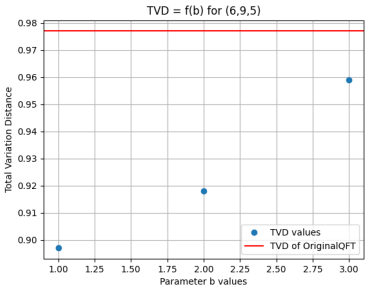
(b) TVD = f(b) (5,3,3)

Figure 35: Γραφικές παραστάσεις depth, TVD = f(b) για Local Banded QFT για την περίπτωση (5,3,3) σε πραγματικό κβαντικό υπολογιστή

παρατηρείται αντίστοιχο αποτέλεσμα για τιμές της TVD. Η συμπεριφορά της τιμής του βάθους μπορεί να οφείλεται στο γεγονός, ότι ο αριθμός των επιπλέον πυλών που δημιουργούνται κατά τη διάρκεια των swaps μεταξύ των qubits μπορεί να είναι μεγαλύτερος από τον αριθμό των C-Phase πυλών που αφαιρούνται λόγω της παραμέτρου b για τόσο μικρό αριθμό qubits, επομένως, το depth να είναι τελικά μεγαλύτερο συγκριτικά με την Original μέθοδο.



(a) Depth = f(b) (6,9,5)



(b) TVD = f(b) (6,9,5)

Figure 36: Γραφικές παραστάσεις depth, TVD = f(b) για Local Banded QFT για την περίπτωση (6,9,5) σε πραγματικό κβαντικό υπολογιστή

Στην περίπτωση (6,9,5) τα συγκριτικά πλεονεκτήματα της BandedLocal μεθόδου φαίνονται ακόμα καλύτερα, καθώς για όλες τιμές του b τόσο η TVD όσο και το βάθος της BandedLocal βρίσκονται κάτω από τις αντίστοιχες τιμές της Original. Αυτό είναι αναμενόμενο, καθώς οι συγκεκριμένες τιμές του b σηματοδοτούν μεγαλύτερη αφαίρεση πυλών και μείωση του depth σε σχέση με την προηγούμενη περίπτωση.

Και στις δύο περιπτώσεις επιβεβαιώνεται, ότι αύξηση του βάθους συνεπάγεται την αύξηση της TVD. Τα δεδομένα δεν είναι επαρκή για να μπορέσουμε

να εξακριβώσουμε τί είδους σχέση ικανοποιούν οι δύο ποσότητες. Ωστόσο, θα πραγματοποιήσουμε μια τελευταία ανάλυση των δεδομένων, πραγματοποιώντας μια γραφική παράσταση (Figure 36) για την περίπτωση (6,9,5) -τα αποτελέσματα της οποίας είναι πιο αντιπροσωπευτικά για περιπτώσεις μεγάλου αριθμού qubits- η οποία μπορεί να μας δώσει μια ποιοτική διαίσθηση σχετικά με τη συσχέτιση της TVD με το depth. Ο οριζόντιος άξονας θα αποτελείται από τις τιμές της διαφοράς του βάθους μεταξύ των δύο μεθόδων και ο κατακόρυφος από τη διαφορά της TVD μεταξύ των δύο μεθόδων.

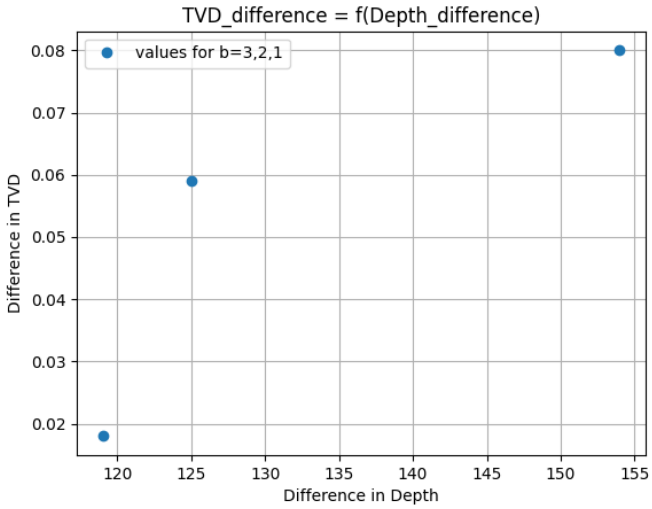
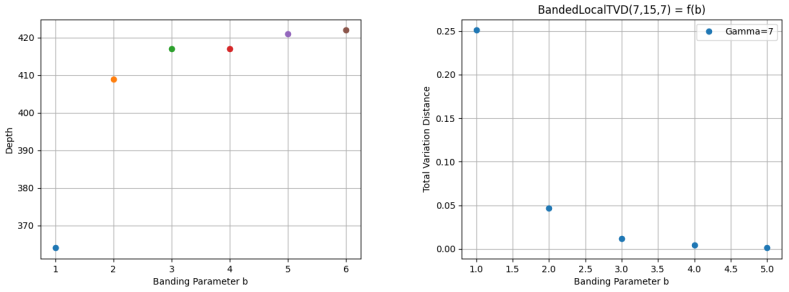


Figure 37: Γραφική παράσταση TVD_difference = f(Depth_Difference) μεταξύ των τιμών της διαφοράς του BandedLocal από τον Original για τις δύο μεταβλητές

Πράγματι, η γραφική παράσταση δίνει μια ποιοτική αίσθηση για τη συσχέτιση μεταξύ της TVD και του βάθους. Αν τη δούμε προσεκτικά, παρατηρούμε πως όσο μειώνεται η διαφορά του βάθους μεταξύ της Original και της Banded μεθόδου (δηλαδή για μεγαλύτερες τιμές του b), τόσο μειώνεται και η διαφορά στην TVD μεταξύ των δύο μεθόδων, δηλαδή η BandedLocal σταματά να έχει συγκριτικό πλεονέκτημα σε σχέση με την Original. Μάλιστα, λόγω των swap gates από τις οποίες αποτελείται, μπορούμε να υποθέσουμε ότι από ένα σημείο και μετά μπορεί να αποκτά ακόμα και μικρότερη ακρίβεια σε σχέση με την Original όπως είδαμε και προηγουμένως για την περίπτωση (5,3,3). Θα ήταν, επίσης, λάθος να υποθέσουμε πως η διαφορά στην TVD θα αυξάνεται διαρκώς όσο το b μειώνεται από την τιμή n-1 μέχρι την τιμή 1. Αυτό, διότι δεν πρέπει να ξεχνάμε πως εξαρχής η Banded μέθοδος εμπεριέχει εγγενώς μειωμένη ακρίβεια όσο μειώνεται ο αριθμός των γειτόνων με τους οποίους αλληλεπιδρά το κάθε qubit.

Επομένως, η πρόβλεψη της τιμής της διαφοράς είναι δύσκολο να γίνει με τα υπάρχοντα δεδομένα. Η τιμή θα μπορούσε να αυξάνεται διαρκώς, υποδηλώνοντας πως η αύξηση της ακρίβειας λόγω μείωσης του βάθους μέσω της αφαίρεσης C-

NOT πυλών θα υπερτερούσε της απώλειας ακρίβειας λόγω περιορισμού των προς αλληλεπίδραση γειτόνων που παρουσιάζει η μέθοδος BandedQFT. Θα μπορούσε, ωστόσο, η διαφορά αυτή να σταθεροποιείται ή ακόμα και να ξεκινά να μειώνεται πάνω από ένα όριο της παραμέτρου b. Η εκτίμηση αυτή δεν μπορεί να γίνει, διότι δεν είναι σαφής ο τρόπος με τον οποίο ο κβαντικός υπολογιστής κατά την διαδικασία του transpiling μετατρέπει τις αρχικές πύλες σε αλληλουχία νέων πυλών. Η γνώση αυτή θα επέτρεπε να προσδιοριστεί μαθηματικά το συγκεκριμένο όριο, έτσι ώστε ο χρήστης να προσδιορίσει τις τιμές των μεταβλητών για τις οποίες μεγιστοποιείται η ακρίβεια της μέτρησης. Αντίστοιχη εκτίμηση θα μπορούσε να γίνει και με τη μελέτη των αντίστοιχων γραφικών παραστάσεων που φαίνονται παραπάνω. Για μεγαλύτερους αριθμούς qubits τα δεδομένα της συμπεριφοράς της TVD σε σχέση με το βάθος θα ήταν περισσότερα και άρα θα μπορούσε να μελετηθεί με μεγαλύτερη ακρίβεια η συσχέτισή τους. Αυτό, ωστόσο, δεν είναι εφικτό την περίοδο συγγραφής της παρούσας εργασίας, διότι, όπως αναφέρθηκε και προηγουμένως, για μεγαλύτερες τιμές qubits το βάθος των κυκλωμάτων «εκτοξεύεται» αυτομάτως σε πολύ μεγάλες τιμές. Θα δείξουμε, ότι αυτό ισχύει μελετώντας την περίπτωση των 7 qubits και την κατάσταση (7,15,7).



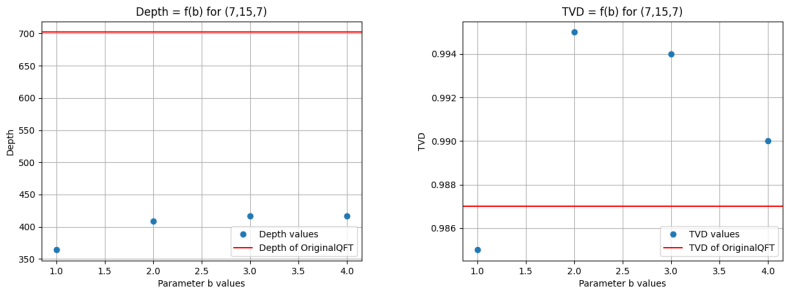
(a) Depth = f(b) (7,15,7)

(b) TVD = f(b) (7,15,7)

Figure 38: Γραφικές παραστάσεις depth, TVD = f(b) για Local Banded QFT για την περίπτωση (7,15,7)

Με βάση αυτές τις γραφικές παραστάσεις θα μελετήσουμε την περίπτωση (7,15,7) για τις τιμές της παραμέτρου b=1,2,3,4. Παίρνουμε τις παρακάτω γραφικές παραστάσεις (Figure 38).

Ενώ παρατηρούμε, ότι το depth για όλες τις τιμές του b είναι μικρότερο από τον OriginalQFT, η TVD είναι πολύ μεγάλη (σχεδόν ίση με 1) για όλες τις τιμές του b και, μάλιστα, μεγαλύτερη από την τιμή του OriginalQFT για τις τιμές b=2,3,4. Αυτό σημαίνει, ότι το βάθος του κυκλώματος είναι τόσο μεγάλο, έτσι ώστε να μην μπορούμε να βγάλουμε κανένα αξιόπιστο στατιστικό συμπέρασμα για τη συμπεριφορά των μεγεθών που μελετάμε. Επομένως, δεν έχει νόημα να κάνουμε περαιτέρω διερεύνηση για κυκλώματα μεγαλύτερου αριθμού qubits.



(a) Depth = f(b) (7,15,7) (b) TVD = f(b) (7,15,7)

Figure 39: Γραφικές παραστάσεις depth, TVD = f(b) για Local Banded QFT για την περίπτωση (7,15,7) σε πραγματικό κβαντικό υπολογιστή

8.5 Dynamical Decoupling

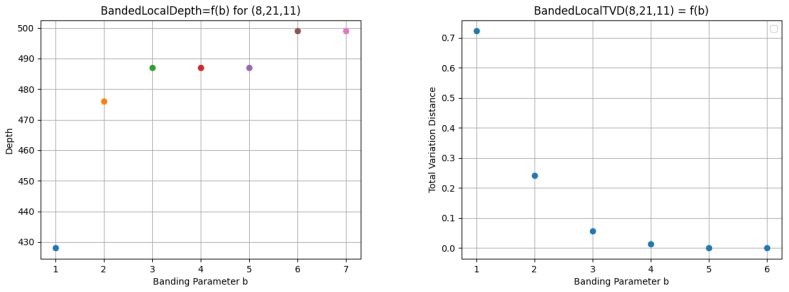
Όπως έχει ήδη περιγραφεί σε προηγούμενα κεφάλαια, όταν ένα κβαντικό σύστημα εκτελεί μια εργασία επεξεργασίας πληροφοριών, παρατηρούνται φαινόμενα αποσυντονισμού λόγω της αλληλεπίδρασης του συστήματος με το περιβάλλον, με αποτέλεσμα να δημιουργούνται πολύ μεγάλα σφάλματα στα τελικά αποτελέσματα, καθιστώντας τα ακόμα και εντελώς μη αξιοποιήσιμα. Η Δυναμική Αποσύνδεση (Dynamical Decoupling – DD) είναι μια μορφή καταπολέμησης των κβαντικών σφαλμάτων και βασίζεται στη λογική, ότι τροποποιώντας τον τρόπο με τον οποίο το σύστημα αλληλεπιδρά με το περιβάλλον, μπορούμε να δημιουργήσουμε μια κατάσταση κατά την οποία οι συνολικές αλληλεπιδράσεις να αλληλοαναιρούνται [15]. Με αυτόν τον τρόπο, η εξέλιξη του συστήματος αποσυνδέεται από την εξέλιξη του περιβάλλοντος που προκαλεί τον αποσυντονισμό [16]. Το Dynamical Decoupling, επομένως, αποτελεί μια τελείως διαφορετική μέθοδο βελτίωσης των αποτελεσμάτων. Οι προηγούμενες μέθοδοι βασίζονταν επάνω σε αλγοριθμικές μεθόδους απλοποίησης του κβαντικού κυκλώματος, με σκοπό τη μείωση του βάθους του, ώστε να βρίσκεται κάτω από ένα όριο στο οποίο τα φαινόμενα αποσυντονισμού αποβαίνουν καταστροφικά για τις μετρήσεις. Αντίθετα, το Dynamical Decoupling προσεγγίζει την πρόκληση της βελτίωσης των αποτελεσμάτων και της μείωσης των σφαλμάτων μέσω της επίδρασης στο φυσικό σύστημα, στο hardware, με σκοπό την ελαχιστοποίηση εξ'αρχής των φαινομένων αποσυντονισμού [17].

Υπάρχει τρόπος να συμπεριληφθούν στην εκτέλεση των προγραμμάτων μας Dynamical Decoupling μέθοδοι, με τη χρήση ενός «περάσματος» (pass) το οποίο λειτουργεί επάνω σε ένα φυσικό, προγραμματισμένο κύκλωμα. Το πέρασμα σαρώνει το κύκλωμα για περιόδους αδράνειας και στη συνέχεια εισάγει μια ακολουθία πυλών DD σε αυτά τα σημεία. Αυτές οι πύλες συνολικά ισοδυναμούν με τον ταυτοτικό τελεστή (μπορεί π.χ. να είναι αλληλουχία πυλών-X), οπότε δεν μεταβάλλουν τη λογική κατάσταση του κυκλώματος, αλλά έχουν ως αποτέλεσμα τη μείωση του decoherence σε αυτές τις περιόδους αδράνειας.

Θα εφαρμόσουμε την παραπάνω διαδικασία στο κβαντικό κύκλωμα του πολ-

λαπλασιασμού με σταθερό αριθμό με χρήση QFT, έτσι ώστε να εξακριβώσουμε εάν πράγματι μας επιτρέπει να αυξήσουμε τον αριθμό qubits που μπορούν να χρησιμοποιηθούν δίνοντας αξιόπιστα αποτελέσματα. Θα ελέγξουμε τη διαδικασία για την περίπτωση και του OriginalQFT και του BandedLocalQFT, με σκοπό να παραστήσουμε γραφικά για τις δύο μεθόδους τη σχέση της TVD με τον αριθμό των qubits δύο περιπτώσεις, χρήσης και μη χρήσης Dynamical Decoupling. Η γραφική παράσταση θα γίνει για εύρος τιμών του αριθμού των qubits n από 5 όπου σταματά η ακρίβεια των αποτελεσμάτων μέχρι τον αριθμό 9, όπου όλες οι μέθοδοι έχουν κατά πολύ εισέλθει σε περιοχή όπου επικρατεί πλήρης αποσυντονισμός και τα αποτελέσματα δεν έχουν καμία ακρίβεια.

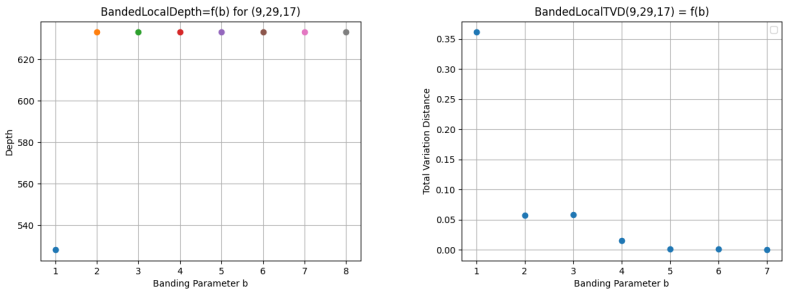
Τόσο για τον OriginalQFT αλγόριθμο, όσο και για τον BandedLocalQFT, έχουμε ήδη προσδιορίσει μέσω του προγράμματος RNG σύνολα τιμών (n, ninit, gamma) που να αντιστοιχούν σε n=5,6,7. Επαλαμβάνοντας την ίδια διαδικασία για τις περιπτώσεις n=8 και n=9, θα βρούμε ακόμα δύο σύνολα, τα (8,21,11) και (9,29,17). Για να χρησιμοποιήσουμε τη BandedLocalQFT μέθοδο (με και χωρίς χρήση Dynamical Decoupling) θα πρέπει να προσδιορίσουμε την τιμή της παραμέτρου b με την οποία θα αρχικοποιηθεί το κύκλωμα στις δύο αυτές περιπτώσεις. Αυτό θα το κάνουμε ακολουθώντας τη διαδικασία που χρησιμοποιήθηκε και προηγουμένως, δημιουργώντας για την κάθε μία δύο γραφικές παραστάσεις, μία για το βάθος του κυκλώματος και μία για την TVD ως συναρτήσεις της παραμέτρου b. Με αυτόν τον τρόπο, θα μπορέσουμε να προσδιορίσουμε τη βέλτιστη τιμή b, επιλέγοντας εκείνη η οποία συνδυάζει το μικρότερο δυνατό βάθος με τη μικρότερη δυνατή τιμή της TVD. Τα αποτελέσματα για τις δύο καταστάσεις φαίνονται παρακάτω (Figure 39, Figure 40).



(a) Depth = f(b) (8,21,11) (b) TVD = f(b) (8,21,11)

Figure 40: Γραφικές παραστάσεις depth, TVD = f(b) για Local Banded QFT για τις την περίπτωση (8,21,11)

Για την περίπτωση (8,21,11) οι πιθανές προς επιλογή τιμές είναι οι b=1 και η b=5. Η b=1, ενώ παρουσιάζει μεγάλη τιμή TVD έχει σημαντικά μικρότερο βάθος σε σχέση με τις υπόλοιπες τιμές, επομένως είναι η πρώτη πιθανή τιμή. Η τιμή b=2 απορρίπτεται, καθώς η διαφορά βάθους του κυκλώματος στο οποίο αντιστοιχεί σε σχέση με τις περιπτώσεις b=3,4,5 είναι πολύ μικρή, ενώ παράλληλα έχει υπερδιπλάσια τιμή TVD σε σχέση με αυτές τιμές. Η b=3 επίσης απορρίπτεται,



(a) Depth = f(b) (9,29,17) (b) TVD = f(b) (9,29,17)

Figure 41: Γραφικές παραστάσεις depth, TVD = f(b) για Local Banded QFT για τις την περίπτωση (9,29,17)

καθώς για σχεδόν ίδιο αριθμό βάθους έχει μεγαλύτερη τιμή TVD σε σχέση με την τιμή b=4 ή b=5. Το ίδιο ισχύει και για την τιμή b=4 ως προς την τιμή b=5. Για τιμές μεγαλύτερες του b=5, το βάθος του κυκλώματος γίνεται πολύ μεγάλο. Επομένως, η δεύτερη πιθανή τιμή είναι η b=5. Είναι αδύνατο να προβλέψουμε ποια από τις δύο περιπτώσεις θα έχει μεγαλύτερη ακρίβεια στο πραγματικό κβαντικό υπολογιστή, καθώς η πρώτη έχει μικρότερο βάθος κυκλώματος αλλά μεγάλη τιμή TVD, ενώ η δεύτερη μεγαλύτερο βάθος κυκλώματος αλλά πολύ μικρή τιμή TVD. Ο μόνος τρόπος να μην κάνουμε μια αυθαίρετη επιλογή, είναι να ελέγξουμε και τις δύο τιμές στον κβαντικό υπολογιστή και να επιλέξουμε εκείνη η οποία αντιστοιχεί σε μικρότερη τιμή της TVD, καθώς αυτό είναι το ποσοτικό κριτήριο που έχουμε θέσει για την ακρίβεια των χρησιμοποιούμενων μεθόδων. Και με χρήση DD και χωρίς, τα αποτελέσματα δείχνουν ότι για b=1 έχουμε ελάχιστα καλύτερη ακρίβεια (με χρήση DD περίπου 16% μικρότερη TVD και χωρίς περίπου 4% μικρότερη TVD). Άρα θα επιλέξουμε την τιμή b=1.

Για την περίπτωση (9,29,17) παρατηρούμε, ότι η βέλτιστη τιμή είναι η τιμή b=1 ξανά. Σε αυτή αντιστοιχεί σημαντικά μικρότερο βάθος κυκλώματος συγκριτικά με οποιαδήποτε άλλη τιμή του b, ενώ η TVD έχει σχετικά μικρή τιμή. Παράλληλα παρατηρούμε, ότι για οποιαδήποτε άλλη τιμή του b, το κύκλωμα ισοδυναμεί πρακτικά με το κύκλωμα του OriginalQFT (b=8), καθώς οι διαφορές στο βάθος είναι αμελητέες, παρατήρηση η οποία αποτελεί μία ακόμα ισχυρή ένδειξη ότι θα πρέπει να επιλέξουμε την τιμή b=1, εάν θέλουμε να αξιοποιήσουμε το συγκριτικό πλεονέκτημα του BandedLocalQFT συγκριτικά με τον OriginalQFT.

Με βάση τις αναλύσεις που έχουν γίνει σε προηγούμενες ενότητες, θα επιλέξουμε και για τα υπόλοιπα σύνολα τιμή παραμέτρου b=1 για τον BandedLocalQFT, και έτσι θα μελετήσουμε τα σύνολα (5,3,3,1),(6,9,5,1),(7,15,7,1),(8,21,11,1),(9,29,17,1). Η γραφική παράσταση TVD=f(n) για τις διαφορετικές μεθόδου με και χωρίς Dynamical Decoupling φαίνεται παρακάτω (Figure 41).

Η γραφική παράσταση παρουσιάζει πολύ μεγάλο ενδιαφέρον και από αυτήν μπορούμε να εξάγουμε κάποια σημαντικά συμπεράσματα:

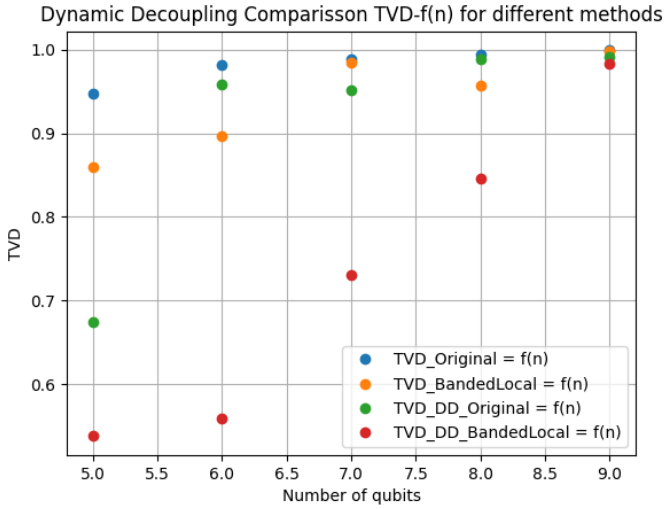


Figure 42: Γραφική Παράσταση TVD=f(n) για OriginalQFT και BandedLocalQFT με χρήση και χωρίς χρήση Dynamical Decoupling

a) Παρατηρούμε ότι για όλες τις τιμές του n, ο BandedLocalQFT παρουσιάζει μεγαλύτερη ακρίβεια σε σχέση με τον OriginalQFT.

b) Ο OriginalQFT με DD παρουσιάζει για όλες τις τιμές του n μικρότερη τιμή από τον OriginalQFT χωρίς DD.

c) Με εξαίρεση την τιμή n=5 όπου ο OriginalQFT με DD έχει αισθητά μικρότερη TVD από τον BandedLocalQFT, οι δύο μέθοδοι φαίνεται να έχουν παρόμοια ακρίβεια.

d) Όλες οι μέθοδοι πλην του BandedLocalQFT με DD για τιμές n=6 και άνω παρουσιάζουν πολύ μεγάλες τιμές της TVD, έχουν δηλαδή πάρα πολύ μικρή ακρίβεια στα αποτελέσματα.

e) Η μέθοδος BandedLocalQFT με DD φαίνεται να έχει πολύ σημαντικό προβάδισμα συγκριτικά με όλες τις υπόλοιπες μεθόδους για όλες τις τιμές του n. Έχει τη μεγαλύτερη ακρίβεια συγκριτικά με όλες τις μεθόδους που έχουν αναλυθεί στα πλαίσια της παρούσας εργασίας. Είναι ενδεικτικό, ότι η τιμή της TVD για n=8 της BandedLocalQFT με DD είναι μικρότερη από την τιμή της BandedLocalQFT χωρίς DD για n=5, δηλαδή παρουσιάζει μεγαλύτερη ακρίβεια ενώ χρησιμοποιεί τρία περισσότερα qubits.

f) Για n=9 όλες οι μέθοδοι συγκλίνουν στην τιμή TVD=1, καθώς το βάθος του κυκλώματος είναι πλέον υπερβολικά μεγάλο για να μπορέσουν να αντισταθμισ-

τούν τα φαινόμενα αποσυντονισμού.

Είναι σημαντικό να τονιστεί, ότι τα συγκεκριμένα ποσοτικά δεδομένα δεν είναι απαραίτητα αξιόπιστα, καθώς αντιστοιχούν σε συγκεκριμένες τιμές (n, ninit, gamma, b) που έχουν προκύψει από το πρόγραμμα RNG. Προφανώς, διαφορετικές τέτοιες τιμές, δηλαδή κβαντικά κυκλώματα που αρχικοποιούνται με διαφορετικές τιμές, είναι λογικό να παρουσιάζουν ποσοτικές διαφορές σε σχέση με την παραπάνω γραφική παράσταση. Για αυτό το λόγο, η παραπάνω ανάλυση είναι χρήσιμη κατά βάση ως προς τα ποιοτικά συμπεράσματα τα οποία δίνει, παρά τα αμιγώς ποσοτικά.

9 Συμπεράσματα και κατευθύνσεις

Στην παρούσα Διπλωματική Εργασία παρουσιάστηκαν οι βασικές αρχές των κβαντικών αλγορίθμων με εστίαση σε αυτούς που βασίζονται στον QFT. Τα κβαντικά αριθμητικά κυκλώματα που εκτελούν την πράξη του πολλαπλασιασμού με σταθερό αριθμό, αποτελούν ένα μόνο παράδειγμα των διαφόρων χρήσεων που μπορούν να έχουν οι αλγόριθμοι QFT στην εκτέλεση απλών -ή και πιο σύνθετων- διεργασιών.

Σκοπός της Εργασίας ήταν να προσεγγίσει το αντικείμενο από διαφορετικές οπτικές γωνίες. Αφ' ενός, από την πλευρά της θεωρητικής και μαθηματικής περιγραφής των κβαντικών αλγορίθμων, η οποία είναι αναγκαία βάση για την ανάπτυξη νέων, πιο αποδοτικών αλγορίθμων και μεθόδων. Αφ' ετέρου, την μελέτη των αλγορίθμων και σε πειραματικό επίπεδο, μέσω προσομοιώσεων αλλά και μετρήσεων με χρήση πραγματικού κβαντικού υπολογιστή. Μέσα από αυτή τη διαδικασία, ωστόσο, αναδείχθηκαν και όλοι οι περιορισμοί που συναντά μέχρι σήμερα ο ανερχόμενος κλάδος των κβαντικών υπολογιστών δημιουργώντας νέες προκλήσεις στους επιστήμονες. Όπως φάνηκε και από το προηγούμενο κεφάλαιο, η αντιμετώπιση των προκλήσεων αυτών δεν μπορεί να πραγματοποιηθεί απουσία μιας συνολικής και συνεκτικής προσέγγισης στους περιορισμούς, που να συνδυάζει την εξέλιξη στους τομείς τόσο των κβαντικών αλγορίθμων όσο και του κβαντικού hardware.

Μια στείρα αλγοριθμική-προγραμματική οπτική επάνω στα προβλήματα που ανακύπτουν δεν βλέπει τα τεράστια οφέλη που μπορεί να έχει η εξέλιξη στον τομέα του hardware και της επίδρασης επάνω στις φυσικές διεργασίες του πραγματικού, φυσικού κβαντικού υπολογιστή, όπως φάνηκε στο προηγούμενο κεφάλαιο με τη χρήση του Dynamical Decoupling, μια διαδικασία η οποία είναι αποκλειστικά φυσική και δεν έχει κανένα ιδιαίτερο προγραμματιστικό ενδιαφέρον. Αντίστροφα, μια προσέγγιση προσανατολισμένη αμιγώς επάνω στην ανάπτυξη του κβαντικού hardware και φυσικών μεθόδων μείωσης των σφαλμάτων και του decoherence, δε βλέπει τα τεράστια οφέλη που μπορεί να έχει η ανάπτυξη κβαντικών αλγορίθμων πιο αποδοτικών με βάση τις συγκεκριμένες δυνατότητες του υπάρχοντος hardware, αλλά και του Quantum Error Correction που αναπτύσσεται διαρκώς.

Παρά το γεγονός, επομένως, ότι ο κορμός της Διπλωματικής Εργασίας ήταν η ανάπτυξη αποδοτικών κβαντικών αλγορίθμων και κβαντικών κυκλωμάτων, το συμπέρασμα αυτής δεν μπορεί να είναι άλλο από το προαναφερθέν.

Οι κβαντικοί υπολογιστές βρίσκονται ακόμα σε ένα πρωτόλειο στάδιο, και άρα οι διεργασίες που μπορούν αυτοί να υλοποιήσουν έχουν σημαντικούς περιορισμούς. Οι αλγόριθμοι οι οποίοι χρησιμοποιήθηκαν για την πράξη του πολλαπλασιασμού αποτελούν σύνθετους κβαντικούς αλγορίθμους, με χρήση πολλών κβαντικών πυλών μεμονωμένα σε κάθε qubit αλλά και με πολλές αλληλεπιδράσεις μεταξύ τους. Το αποτέλεσμα αυτής της συνθετότητας είναι η αδυναμία οι αλγόριθμοι αυτοί να είναι χρήσιμοι και ακριβείς για μεγάλο αριθμό qubits, χωρίς αυτό, ωστόσο, να αναιρεί την ορθότητα της μεθόδου που χρησιμοποιήθηκε. Αντίθετα, πέρα από την επιβεβαίωση της χρησιμότητας του mQFT ως μέθοδο πολλαπλασιαστή -η οποία εξ'αρχής πιστοποιήθηκε μέσω των προσομοιώσεων- εξήχθησαν χρήσιμα ποιοτικά συμπεράσματα και αναπτύχθηκαν διάφορες εκδοχές του, οι οποίες δείχθηκε ότι δίνουν σημαντικό πλεονέκτημα, το οποίο μπορεί να ακόμα μεγαλύτερο όσο αυξάνεται

και η δυνατότητα των κβαντικών υπολογιστών να διενεργούν όλο και πιο σύνθετες διαδικασίες. Στην παρούσα συνθήκη αυτό δεν μπορεί να αποδειχθεί με αυστηρό τρόπο, μπορούν, ωστόσο, να αναδειχθούν οι μελλοντικές δυνατότητες.

Είναι σημαντικό να επαναληφθεί και να τονιστεί εκ νέου, ότι οι αναλύσεις που πραγματοποιήθηκαν στα παραπάνω κεφάλαια έχουν κατά βάση αξία ως προς τα ποιοτικά παρά τα ποσοτικά τους δεδομένα. Μελετήθηκαν, ουσιαστικά, συναρτήσεις τριών ή τεσσάρων μεταβλητών, οι οποίες επηρεάζουν σαφώς τα αποτελέσματα και τα πραγματικά κυκλώματα που εκτελεί ο κβαντικός υπολογιστής. Πολύ περισσότερο, όταν οι κβαντικές πύλες που δημιουργούν το εκάστοτε κβαντικό κύκλωμα με βάση τις ορισμένες από το χρήστη τιμές των συγκεκριμένων μεταβλητών ανάγονται σε σύνθετες αλληλουχίες νέων πυλών κατά τη διαδικασία του transpiling προκειμένου να μπορέσουν να εκτελεστούν από τον κβαντικό υπολογιστή. Πρόκειται για ιδιαίτερα σύνθετες και πολύπλοκες διαδικασίες, η μελέτη και βελτιστοποίηση των οποίων θα μπορούσε να αφορά ξεχωριστή έρευνα και μελέτη. Η χρήση ψευδοτυχαίων αριθμών εξασφαλίζει την απουσία οποιουδήποτε bias κατά τη μελέτη των διαφόρων χαρακτηριστικών των κυκλωμάτων που δημιουργήθηκαν, χωρίς, ωστόσο, αυτό να μπορεί να αποκλειστεί με βεβαιότητα το ενδεχόμενο οι μετρήσεις αυτές να μην μπορούν με ασφάλεια να αναχθούν σε γενικά συμπεράσματα.

Με βάση αυτά, αυτό που κατά βάση είναι χρήσιμο είναι τα ποιοτικά συμπεράσματα των παραπάνω αναλύσεων, ειδικά αν λάβουμε υπόψη ότι πολλά από τα δεδομένα και τις γραφικές παραστάσεις που τα απεικόνισαν λαμβάνουν χώρα σε περιοχές, όπου η τιμή της TVD είναι κοντά στη μονάδα, δηλαδή, τα ίδια τα αποτελέσματα έχουν στην πραγματικότητα ελάχιστη ακρίβεια. Αυτό δεν αναιρεί, ωστόσο, τη μεγάλη σημασία που έχει να μελετήσουμε τη συμπεριφορά διαφόρων διαφορετικών αλγορίθμων και μεθόδων και σε αυτές τις περιοχές, προκειμένου να εξάγουμε συμπεράσματα για τα συγκριτικά πλεονεκτήματα που μπορεί να έχουν κάποιοι αυτούς ως προς κάποιους άλλους. Τα συμπεράσματα αυτά θα μπορούν να εξαχθούν με πολύ μεγαλύτερη ακρίβεια όσο οι κβαντικοί υπολογιστές αναπτύσσονται. Είναι ενδεικτικό, ότι αν το εμπειρικό βάθος των κυκλωμάτων στο οποίο επικρατεί αποσυντονισμός διπλασιαζόταν από περίπου 200 σε περίπου 400 όλη η παραπάνω μελέτη θα αποτελείτο από πληθώρα νέων δεδομένων που θα έδιναν πολύ καλύτερη και ισχυρή ένδειξη για τα όσα παρουσιάστηκαν στην παρούσα Διπλωματική Εργασία.

Είναι βέβαιο, ότι η ανάπτυξη του κβαντικού hardware παράλληλα με την ενσωμάτωση τεχνικών Quantum Error Correction και Fault-Tolerant Αλγορίθμων στις κβαντικές πλατφόρμες, όπως το Qiskit, θα «απογειώσει» την επίδοση των κβαντικών υπολογιστών, καθιστώντας εφικτή τη βαθύτερη μελέτη σύνθετων αλγορίθμων όπως ο QFT, αλλά και ακόμα πιο περίπλοκων κβαντικών διεργασιών.

A Συναρτήσεις

A.1 Συνάρτηση Fmul

```
# Construct quantum circuit implementing constant multiplication
# |x> -> |gx> , x=0..2^n-1 based on QFT
# input: circuit (circuit structure)
#        n       (number of qubits)
#        gamma   (gamma constant)
#        b       (banding or approximation parameter)
#        verb    (verbose parameter: 0:don't log , 1:log)
# returns:
#        circuit (circuit structure)
def Fmul(qc, n, gamma, b, verb=1):
    N            = 2**n
    thresh0      = 2*pi/(2**(n+1))  # threshold to cancel rot
    ↪  gates
    mQFTcancelled= 0                # number of mQFT rot gates
    ↪  cancelled due to banding
    QFTcancelled = 0                # number of inv QFTrot gates
    ↪  cancelled due to banding
    totalgatescanc= 0               #number of total gates
    ↪  cancelled
    Nrot         = n*(n-1)/2        # number of rot gates in each
    ↪  QFT block

    if verb == 1:
        print()
        print('--------------------------------')
        print('Constructing modified QFT circuit')
        print('--------------------------------')
        print('qubits= ', n, 'gamma= ', gamma, 'banding= ', b)
        print()
        print('Conversion of rotation gates angles in 2π units')

    for y in range(n-1, -1, -1):
        qc.barrier()
        qc.h(y)
        for x in range(y-1, -1, -1):
            k        = y-x+1
            phi      = gamma*2*pi/(2**k)
            phiNormal= (phi/(2*pi) - floor(phi/(2*pi)))*2*pi
            phiQ     =
            ↪  round(phiNormal*2**(b+1)/(2*pi))*(2*pi)/(2**(b+1))
```

```
            if verb == 1:
                print('qubit', y, 'to qubit', x, 'gate:  ',
                ↪  end="")
                print("%.8f" % (phiNormal/(2*pi)), "  converted
                ↪  to ", "%.8f" % (phiQ/(2*pi)), end="")
                if phiNormal != phiQ:
                    print(' * ')
                else:
                    print()
            if abs(phiQ) >= thresh0:
                qc.cp(phiQ, x, y)
            else:
                mQFTcancelled += 1
                totalgatescanc +=1

    if verb == 1:
        print()
        print('-----------------------------------------------')
        print('modified QFT circuit constructed')
        print('-----------------------------------------------')
        print('rotation gates cancelled:', mQFTcancelled, 'out
        ↪  of:', Nrot)
        print()


    if (verb==1):
        print()
        print('-----------------------------------------------')
        print('Constructing inverse QFT circuit              ')
        print('-----------------------------------------------')
        print('qubits =',n,'gamma =',gamma,'banding =',b)
        print()
        print('Conversion of rotation gates angles in 2π units')
        print()
        print()

    for y in range(0,n,1):
    #print(y)
        qc.barrier()
        for x in range(0,y,1):
            k=y-x+1
            phi=-2*pi/(2**k)
            phiQ=round(phi*2**(b+1)/(2*pi))*(2*pi)/(2**(b+1))
            if (abs(phiQ) >= thresh0):
                qc.cp(phiQ,x,y)
            else:
```

```
                QFTcancelled=QFTcancelled+1
                totalgatescanc +=1
            if (verb==1):
                print('qubit',y,'to qubit',x,'gate: ', end="")
                print("%.8f" % (phi/(2*pi)) ,"  converted to
                ↪  ","%.8f" % (phiQ/(2*pi)),end="")
                if (phi!=phiQ):
                    print(' * ')
                else:
                    print()
        qc.h(y)

    if (verb==1):
            print()

            ↪  print('-----------------------------------------------')
            print('inverse QFT circuit constructed
            ↪  ')

            ↪  print('-----------------------------------------------')
            print('rotation gates cancelled:', QFTcancelled, 'out
            ↪  of:', Nrot)
            print('Total rotation gates canclled=
            ↪  ',totalgatescanc, 'out of', Nrot, 'gates')
            print()

    if (verb==0):
            print('Total rotation gates cancelled=
            ↪  ',totalgatescanc, 'out of', Nrot, 'gates')
            print()
#
# End of Fmul
#
```

A.2 Συνάρτηση mQFTlocal

```
# Construct quantum circuit implementing modified QFT with local
↪  communications
# |x> -> mQFT_gamma|x> , x=0..2^n-1
# input: circuit (circuit structure)
#        n       (number of qubits)
#        gamma   (gamma constant) (gamma=1 fornormal QFT)
#        verb    (verbose parameter: 0:don't log , 1:log)
# returns:
#        circuit (circuit structure)
```

```
def mQFTlocal(qc, n, gamma, verb=1):
    if (verb==1):
        print()
        print('-----------------------------------------------')
        print('Constructing modified QFT with local comms
        ↪  circuit')
        print('-----------------------------------------------')
        print('qubits =',n,'gamma =',gamma)
        print('-----------------------------------------------')
        print()


    xlimit=n-1;
    for x in range(1,xlimit+1):
        qc.barrier()
        ng=int((n-1)/2-abs(x-(n+1)/2))
        print('ng =',ng)
        for y in range(1,ng+1):
            y1=n-2*y
            y2=y1-1
            qc.swap(y1,y2)
        qc.h(n-1)
        for y in range(1,ng+1):
            k=2*y+1
            phi=gamma*2*pi/(2**k)
            y1=n-2*y
            y2=y1-1
            qc.cp(phi,y1,y2)
        ng=int((n-2)/2-abs(x-(n)/2))+1
        for y in range(1,ng+1):
            y1=n+1-2*y
            y2=y1-1
            qc.swap(y1,y2)
        for y in range(1,ng+1):
            k=2*y
            phi=gamma*2*pi/(2**k)
            y1=n+1-2*y
            y2=y1-1
            qc.cp(phi,y1,y2)
    qc.h(n-1)

#
# End of mQFTlocal
#
```

A.3 Συνάρτηση mINVQFTlocal

```
# Construct quantum circuit implementing inverse modified QFT
↪  with local communications
# |x> -> mQFT_gamma^{-1}|x>
# input: circuit (circuit structure)
#        n       (number of qubits)
#        gamma   (gamma constant) (gamma=1 fornormal QFT)
#        verb    (verbose parameter: 0:don't log , 1:log)
# returns:
#        circuit (circuit structure)
def mINVQFTlocal(qc, n, gamma, verb=1):
    if (verb==1):
        print()
        print('-------------------------------------------')
        print('Constructing modified QFT with local comms
        ↪  circuit')
        print('-------------------------------------------')
        print('qubits =',n,'gamma =',gamma)
        print()


    xlimit=n-1;
    for x in range(xlimit,0,-1):
        qc.barrier()
        qc.h(n-1)
        ng=int((n-2)/2-abs(x-(n)/2))+1
        for y in range(1,ng+1):
            k=2*y
            phi=-gamma*2*pi/(2**k)
            y1=n+1-2*y
            y2=y1-1
            qc.cp(phi,y1,y2)
        for y in range(1,ng+1):
            y1=n+1-2*y
            y2=y1-1
            qc.swap(y1,y2)
        ng=int((n-1)/2-abs(x-(n+1)/2))
        for y in range(1,ng+1):
            k=2*y+1
            phi=-gamma*2*pi/(2**k)
            y1=n-2*y
            y2=y1-1
            qc.cp(phi,y1,y2)
        for y in range(1,ng+1):
            y1=n-2*y
```

```
            y2=y1-1
            qc.swap(y1,y2)
    qc.h(n-1)

#
# End of mINVQFTlocal
#
```

B Προγράμματα

B.1 Πρόγραμμα κατασκευής ψευδοτυχαίων αριθμών RNG

```
import random
import math

def generate_numbers():
    # Generate a random number a
    n = random.randint(10,20)  # Adjust the range as needed
    upper_bound = 2 ** n

    ninit = random.choice([i for i in range(1, upper_bound + 1)])
    gamma

    # Generate c such that gcd(2, gamma) = 1 (gamma must be odd)
    gamma = random.choice([i for i in range(1, upper_bound + 1)
    ↪  if i % 2 == 1])

    # Generate ninit such that ninit * gamma <= 2^n
    max_ninit = upper_bound // gamma
    ninit = random.randint(1, max_ninit)

    # Generate a random number b
    b = random.randint(n-4,n)  # Adjust the range as needed

    return n, ninit, gamma, b

# Example usage
n, ninit, gamma, b = generate_numbers()
print(f"n: {n}, ninit: {ninit}, gamma: {gamma}, b: {b}")
print(f"ninit * gamma: {ninit * gamma} <= 2^n: {2 ** n}")
print(f"gcd(2, gamma): {math.gcd(2, gamma)}")
```

B.2 Πρόγραμμα υπολογισμού TVD

```
from qiskit_ibm_runtime import QiskitRuntimeService
from qiskit import QuantumCircuit, transpile
from qiskit.visualization import plot_histogram
import qlibf
from math import gcd
from qiskit.providers.basic_provider import BasicProvider
from qiskit.transpiler.preset_passmanagers import
↪  generate_preset_pass_manager
import numpy as np
import matplotlib.pyplot as plt

total_counts = 1000
gamma = None

# Ask for the number of qubits
N = int(input("Enter the number of available qubits: "))

# Define the fixed number of qubits for binary representation
dim = 2 ** N
print('The dimension of the problem is equal to', dim)

# Ask for the number
ninit = int(input("Enter your number: "))

# Convert the number to binary and format it to have a fixed
↪  width
binit = format(ninit, f'0{N}b')
print('Binary representation:', binit)

# Create the list of bits
ing = list(int(digit) for digit in binit)
print('The list of bits is', ing)

# Reverse the list of bits to match Qiskit's qubit indexing
ing.reverse()
print('Reversed list of bits for Qiskit:', ing)

# Determine the number of qubits
n = len(ing)

# Ask the user for the value of gamma
while True:
    try:
        gamma = int(input("Enter the value of gamma: "))
```

```
        print('Multiplier constant gamma is equal to', gamma)
        if gcd(2, gamma) != 1:
            raise ValueError("The greatest common divisor (gcd)
            ↪  between number 2 and gamma must be equal to 1.")
        break
    except ValueError as e:
        print(e)

b = int(input("Enter the banding parameter b: "))

# Create the quantum circuit
circuit = QuantumCircuit(n)

# Apply the user's binary number as the initial condition
for idx, bit in enumerate(ing):
    if bit == 1:
        circuit.x(idx)

# Apply the modified QFT algorithm
qlibf.Fmul(circuit, n, gamma, b, 0)
circuit.measure_all()

#Choose a backend
simulator = BasicProvider().get_backend('basic_simulator')

#Transpile the circuit for the simulator
trans_circuit = transpile(circuit, simulator)
trans_circuit.depth()

#Execute the transpiled circuit
job = simulator.run(trans_circuit, shots=total_counts)
result=job.result()
counts1 = result.get_counts()

service = QiskitRuntimeService(channel="ibm_quantum", token
↪  ='***')
job_id = '***'
job = service.job(job_id)

result=job.result()
counts2 = result.get_counts()

# Find the set of all keys in both dictionaries
all_keys = set(counts1.keys()).union(set(counts2.keys()))

# Create the difference dictionary
```

```
final_counts = {key: abs(counts2.get(key, 0) - counts1.get(key,
↪  0)) for key in all_keys}
#print("Difference counts:", final_counts)

#Normalize the counts to find probability
counts_normalized = {k: v / total_counts for k, v in
↪  final_counts.items()}
#print("Normalized counts:", counts_normalized)

TVD = 1/2 * sum(counts_normalized.values())
print('The Total Variation Distance is equal to', TVD)

#Plot the histogram
plot_histogram(final_counts)
```

C Modular Exponentiation

Θέλουμε να υπολογίσουμε την ακολουθία controlled-U^{2^j} τελεστών που χρησιμοποιούνται από την διαδικασία εκτίμησης φάσης ως τμήμα του αλγορίθμου εύρεσης τάξης. Θέλουμε, δηλαδή, να υπολογίσουμε τον μετασχηματισμό

$$|z\rangle|y\rangle \rightarrow |z\rangle U^{z_t 2^{t-1}} ... U^{z_1 2^0}|y\rangle = |z\rangle|x^{z_t 2^{t-1}} \times ... \times x^{z_1 2^0} y(modN)\rangle = \quad (74)$$

$$= |z\rangle|x^z y(modN)\rangle \quad (75)$$

Επομένως, η ακολουθία των controlled-U^{2^j} τελεστών που χρημοποιούνται στην εκτίμηση φάσης είναι ισοδύναμη με τον πολλαπλασιασμό των περιεχομένων του πρώτου καταχωρητή με το modular εκθετικό $x^z y(modN)$, όπου το z είναι τα περιεχόμενα του πρώτου καταχωρητή. Αυτός ο υπολογισμός μπορεί να γίνει εύκολα με τη βοήθεια τεχνικών αντιστρέψιμου υπολογισμού. Η βασική ιδέα είναι να υπολογίσουμε με αντιστρέψιμο τρόπο τη συνάρτηση $x^z y(modN)$ του z σε έναν τρίτο καταχωρήτη, και στη συνέχεια να πολλαπλασιάσουμε ξανά με αντιστρέψιμο τρόπο τα περιεχόμενα του δεύτερου καταχωρήτη με $x^z y(modN)$, διαγράφοντας τα περιεχόμενα του τρίτου καταχωρητή όταν ολοκληρωθεί η διαδικασία. Ο αλγόριθμος για τον υπολογισμό του modular εκθετικού περιλαμβάνει δύο στάδια.

Στο πρώτο στάδιο, χρησιμοποιείται modular πολλαπλασιασμός για τον υπολογισμό $x^2 y(modN)$, υψώνοντας στο τετράγωνο το x modulo N, στη συνέχεια για τον υπολογισμό $x^4 y(modN)$ υψώνοντας στο τετράγωνο το $x^2 y(modN)$ και συνεχίζοντας με τον ίδιο τρόπο υπολογίζοντας τα $x^{2^j} y(modN)$ για όλα τα j μέχρι την τιμή t-1. Το t είναι ίσο με $t = 2L + 1 + [log(2 + 1/2\varepsilon)] = O(L)$, επομένως ο συνολικός αριθμός t - 1 = O(L) πράξεων τετραγώνου έχει ο καθένας υπολογιστικό κόστος $O(L^2)$ και άρα συνολικά το πρώτο στάδιο έχει υπολογιστικό κόστος $O(L^3)$.

Το δεύτερο στάδιο βασίζεται στην παρατήρηση, ότι

$$x^z y(modN) = (x^{z_t 2^{t-1}}(modN))(x^{z_{t-1}2^{t-2}}(modN))...(x^{z_1 2^0}(modN)) \qquad (76)$$

Πραγματοποιώντας t - 1 modular πολλαπλασιασμούς με κόστος $O(L^2)$ ο καθένας, παρατηρούμε, ότι ότι το γινόμενο αυτό μπορεί να υπολογιστεί χρησιμοποιώντας $O(L^3)$. Το κόστος αυτό είναι επαρκώς αποδοτικό. Μπορούμε στη συνέχεια χρησιμοποιώντας διάφορες τεχνικές, να κατασκευάσουμε ένα αντιστρέψιμο κύκλωμα με δύο καταχωρητές t bit και L bit, το οποίο όταν αρχικοποιείται στην κατάσταση (z,y) έχει ως έξοδο $z, x^z y(modN)$ χρησιμοποιώντας $O(L^3)$ πύλες, το οποίο θα αντιστοιχεί σε ένα κβαντικό κύκλωμα που εκτελεί το μετασχηματισμό $|z\rangle\,|y\rangle \rightarrow |x^z y(modN)\rangle$.

Βιβλιογραφία

[1] N. D. Mermin, *Quantum Computer Science: An Introduction*. Cambridge University Press, 2007.

[2] P. Kaye, R. Laflamme, and M. Mosca, *An Introduction to Quantum Computing*. OUP Oxford, 2006.

[3] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge university press, 2010.

[4] W. Liu, Y. Xu, M. Zhang, J. Chen, and C.-N. Yang, "A Novel Quantum Visual Secret Sharing Scheme," *IEEE Access*, vol. 7, pp. 114374–114384, 2019.

[5] E. Floratos and A. Pavlidis, "A Novel Finite Fractional Fourier Transform and its Quantum Circuit Implementation on Qudits," *arXiv preprint arXiv:2409.05759*, 2024.

[6] Y. Nam and R. Blümel, "Scaling laws for Shor's Algorithm with a Banded Quantum Fourier Transform," *Physical Review A—Atomic, Molecular, and Optical Physics*, vol. 87, no. 3, p. 032333, 2013.

[7] D. Coppersmith, "An Approximate Fourier Transform useful in Quantum Factoring (2002)," *arXiv preprint quant-ph/0201067*, 2002.

[8] E. Knill, "Approximation by Quantum Circuits," *arXiv preprint quant-ph/9508006*, 1995.

[9] W. J. Gallagher, E. P. Harris, and M. B. Ketchen, "Superconductivity at IBM–a Centennial Review: Part I–Superconducting Computer and Device Applications," in *Proceedings of the IEEE/CSC ESAS European Superconductivity News Forum*, vol. 21, pp. 1–34, 2012.

[10] H. Bruus and K. Flensberg, *Many-Body Quantum Theory in Condensed Matter Physics: An Introduction*. OUP Oxford, 2004.

[11] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. Brandao, D. A. Buell, *et al.*, "Quantum Supremacy using a Programmable Superconducting Processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.

[12] E. Pelofske, A. Bärtschi, and S. Eidenbenz, "Quantum Annealing vs. QAOA: 127 qubit higher-order Ising Problems on NISQ computers," in *International Conference on High Performance Computing*, pp. 240–258, Springer, 2023.

[13] J. Roffe, "Quantum Error Correction: An Introductory Guide," *Contemporary Physics*, vol. 60, no. 3, pp. 226–245, 2019.

[14] Y. Kim, A. Eddins, S. Anand, K. X. Wei, E. Van Den Berg, S. Rosenblatt, H. Nayfeh, Y. Wu, M. Zaletel, K. Temme, *et al.*, "Evidence for the utility of Quantum Computing before Fault Tolerance," *Nature*, vol. 618, no. 7965, pp. 500–505, 2023.

[15] L. Viola and S. Lloyd, "Dynamical Suppression of Decoherence in two-state Quantum Systems," *Physical Review A*, vol. 58, no. 4, p. 2733, 1998.

[16] X. Peng, D. Suter, and D. A. Lidar, "High Fidelity Quantum Memory via Dynamical Decoupling: Theory and Experiment," *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 44, no. 15, p. 154003, 2011.

[17] W. Yang, Z.-Y. Wang, and R.-B. Liu, "Preserving qubit coherence by Dynamical Decoupling," *Frontiers of Physics in China*, vol. 6, pp. 2–14, 2011.