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

ΜΕΤΑΦΡΑΣΗ ΑΠΟ ΤΗ ΓΛΩΣΣΑ ΚΒΑΝΤΙΚΟΥ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ nQML ΣΕ ΚΒΑΝΤΙΚΑ ΚΥΚΛΩΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΙΩΑΝΝΗΣ Κ. ΡΟΥΣΕΛΑΚΗΣ

Επιβλέπων: Νικόλαος Παπασπύρου
Επίκουρος Καθηγητής Ε.Μ.Π.

Αθήνα, Δεκέμβριος 2007

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

ΜΕΤΑΦΡΑΣΗ ΑΠΟ ΤΗ ΓΛΩΣΣΑ ΚΒΑΝΤΙΚΟΥ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ nQML ΣΕ ΚΒΑΝΤΙΚΑ ΚΥΚΛΩΜΑΤΑ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΙΩΑΝΝΗΣ Κ. ΡΟΥΣΕΛΑΚΗΣ

Επιβλέπων: Νικόλαος Παπασπύρου
Επίκουρος Καθηγητής Ε.Μ.Π.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 13η Δεκεμβρίου 2007.

.....	.....	.....
Νικόλαος Παπασπύρου Επίκ. Καθηγητής Ε.Μ.Π.	Ευστάθιος Ζάχος Καθηγητής Ε.Μ.Π.	Κωνσταντίνος Σαγώνας Αν. Καθηγητής Ε.Μ.Π.

Αθήνα, Δεκέμβριος 2007

.....

Ιωάννης Κ. Ρουσελάκης
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικών Υπολογιστών Ε.Μ.Π.

Περίληψη

Σκοπός αυτής της διπλωματικής εργασίας είναι η μελέτη κβαντικών γλωσσών προγραμματισμού και η ανάπτυξη κβαντικών κυκλωμάτων για μία συγκεκριμένη γλώσσα, την nQML. Κατ' επέκταση μελετήσαμε το μοντέλο του κβαντικού προγραμματισμού και τους κανόνες που διέπουν την κατασκευή κβαντικών κυκλωμάτων. Οι κβαντικοί αλγόριθμοι συνήθως υλοποιούνται με τη βοήθεια κβαντικών κυκλωμάτων, όμως για να χρησιμοποιηθεί το κβαντικό μοντέλο υπολογισμών από προγραμματιστές απαιτείται και η κατασκευή κατάλληλων γλωσσών προγραμματισμού. Με αυτό τον τρόπο θα γεφυρωθεί το χάσμα ανάμεσα στον κλασικό και στον κβαντικό τρόπο σκέψης. Τα κβαντικά κυκλώματα θα χρησιμοποιηθούν πλέον για την περιγραφή των εντολών της γλώσσας προγραμματισμού και μελλοντικά θα αποτελέσουν τα στοιχειώδη τμήματα από τα οποία θα αποτελείται ένας κβαντικός υπολογιστής.

Το κβαντικό μοντέλο προγραμματισμού επωφελείται από την ιδιότητα της υπέρθεσης καταστάσεων κβαντικών σωματιδίων με αποτέλεσμα να υπάρχουν κβαντικοί αλγόριθμοι αποδεδειγμένα ταχύτεροι από τους αντίστοιχους κλασικούς. Ειδικότερα ο αλγόριθμος του Shor για την παραγοντοποίηση μεγάλων αριθμών έχει τραβήξει το ενδιαφέρον της ερευνητικής κοινότητας.

Οι προσπάθειες για την κατασκευή λειτουργικών κβαντικών υπολογιστών έχουν οδηγήσει στη μελέτη των κβαντικών κυκλωμάτων από τα οποία αποτελούνται. Σε αυτή την εργασία είδαμε διάφορες ιδιότητες των κβαντικών κυκλωμάτων και μελετήσαμε τους τρόπους κατασκευής τους από απλά δομικά στοιχεία.

Μας απασχόλησαν οι γλώσσες QPL, QML και φυσικά η γλώσσα nQML. Βασιζόμενοι στα θεωρήματα των κβαντικών κυκλωμάτων σχεδιάσαμε τα κατάλληλα κβαντικά κυκλώματα, τα οποία υλοποιούν κάθε εντολή της γλώσσας. Τέλος υλοποιήσαμε αυτόν τον μεταφραστή σε γλώσσα Haskell.

Λέξεις κλειδιά

Κβαντικός προγραμματισμός, γλώσσες κβαντικού προγραμματισμού, κβαντικά κυκλώματα, κβαντικές πύλες, n-QML, κυκλώματα FQC, αλγόριθμος Shor, αλγόριθμος Grover, αλγόριθμος Deutsch.

Abstract

The purpose of this diploma thesis is the study of quantum programming languages and the design of quantum circuits for a particular language, n-QML. As a result we studied the quantum programming model and the rules that apply to the construction of quantum circuits. Quantum algorithms are usually implemented with quantum circuits, but programmers need a suitable programming language in order to use the quantum programming model of computation. In that way the distance between the quantum and classical school of thought will shrink. Quantum circuits will be used only to describe the commands of the language and in the future they will become the building blocks of a functional quantum computer.

The quantum programming model makes use of the state superposition property of quantum particles and as a result there are quantum algorithms that are proven to be faster than the corresponding classical ones. Especially Shor's algorithm for factoring large numbers has created a huge interest among scientists for quantum computation.

Attempts to construct a functional quantum computer have led to the study of quantum circuits. In this thesis we studied several properties of quantum circuits and different ways to construct them from simple structural elements.

We examined the languages QPL, QML and of course nQML. Based on the theorems regarding quantum circuits we designed the suitable quantum circuits, which implement every nQML command. Finally we implemented that translator program in Haskell.

Keywords

Quantum programming, quantum programming languages, quantum circuits, quantum gates, n-QML, FQC circuits, Shor's algorithm, Grover's algorithm, Deutsh's algorithm.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή της διπλωματικής μου κ. Νικόλαο Παπασπύρου γιατί μου έδωσε την ευκαιρία να ασχοληθώ με πολλά ενδιαφέροντα μαθήματα και ένα ενδιαφέρον θέμα διπλωματικής. Επίσης ευχαριστώ τον καθηγητή κ. Ευστάθιο Ζάχο για την προθυμία να βοηθήσει τους φοιτητές του και την προσπάθεια να τους εμφυσήσει τη δίψα για γνώση. Τέλος ευχαριστώ όλους τους συμφοιτητές μου για τις ωραίες στιγμές που περάσαμε μαζί αυτά τα πέντε χρόνια.

Ιωάννης Κ. Ρουσελάκης,
Αθήνα, 13 Δεκεμβρίου 2007

Περιεχόμενα

Κατάλογος πινάκων

Κατάλογος σχημάτων

1 Εισαγωγή

1.1 Σκοπός

Σκοπός αυτής της διπλωματικής εργασίας είναι η μελέτη ενός νέου και αρκετά υποσχόμενου πεδίου της επιστήμης των υπολογιστών, του μοντέλου των κβαντικών υπολογισμών. Θα μελετήσουμε επίσης τα κβαντικά κυκλώματα, τα οποία αποτελούν μια όψη αυτού του μοντέλου από τη σκοπιά του υλικού (hardware), και τις κβαντικές γλώσσες προγραμματισμού, οι οποίες είναι η σκοπιά του λογισμικού (software). Ο τελικός στόχος της εργασίας είναι η ανάπτυξη κβαντικών κυκλωμάτων για μία συγκεκριμένη κβαντική γλώσσα, την nQML. Αυτή πρόκειται για μία κβαντική γλώσσα που αναπτύχθηκε στο Εθνικό Μετσόβιο Πολυτεχνείο και αποτελεί μετεξέλιξη μιας παλαιότερης γλώσσας, της QML. Όλες αυτές οι γλώσσες καθώς υπακούουν σε ένα μοντέλο ξένο προς την κοινή λογική παρουσιάζουν αρκετές διαφοροποιήσεις και δυσκολίες σε σχέση με τις συμβατικές γλώσσες προγραμματισμού. Η μελέτη τους και η κατασκευή κυκλωμάτων για αυτές βοηθάει στην καλύτερη κατανόησή τους και επομένως και στην ευκολότερη επινόηση κβαντικών αλγορίθμων που επιλύουν δύσκολα προβλήματα. Τέλος υλοποιήσαμε και ένα πρόγραμμα στη γλώσσα Haskell το οποίο κατασκευάζει τα ζητούμενα κυκλώματα σύμφωνα με τους κανόνες κατασκευής.

1.2 Ιστορία του μοντέλου κβαντικού υπολογισμού

Τα πρώτα δημοσιεύματα που προετοίμασαν το έδαφος για την ανάπτυξη κβαντικών αλγορίθμων έγιναν τη δεκαετία του 1970. Κάποια από αυτά ήταν η διατύπωση του θεωρήματος του Holevo (1973) ότι n qubits δεν μπορούν να μεταφέρουν περισσότερα από n κλασικά bits πληροφορίας, μια απόδειξη της μη αποδοτικής προσομοίωσης κβαντικών συστημάτων σε κλασικούς υπολογιστές, (R. P. Poplavskii, 1975) και μια πρώτη προσέγγιση της κβαντικής θεωρίας πληροφορίας (Roman Ingarden, 1976).

Όμως το ουσιαστικό βήμα που έστρεψε το ενδιαφέρον της ερευνητικής κοινότητας προς τους κβαντικούς υπολογιστές έγινε το 1981 με τη διάλεξη του διάσημου φυσικού και νομπελίστα Richard Feynman στο First Conference on the Physics of Computation που έγινε στο MIT και τη δημοσίευση (1) που ακολούθησε το 1982 από τον ίδιο. Στο άρθρο αυτό επισήμανε ότι ένα κβαντομηχανικό σύστημα R σωματιδίων δεν μπορεί να προσομοιωθεί αποδοτικά με ένα συνηθισμένο υπολογιστή χωρίς εκθετική επιβράδυνση στην αποδοτικότητα της προσομοίωσης. Παρ' όλα αυτά ένα σύστημα R σωματιδίων στην κλασική φυσική είναι δυνατόν να προσομοιωθεί αρκετά καλά με μόνο πολυωνυμική επιβράδυνση. Ο κύριος λόγος για τον οποίο συμβαίνει αυτό είναι ότι το μέγεθος της περιγραφής ενός συστήματος σωματιδίων είναι γραμμικό ως προς R στην κλασική φυσική (αρκεί να δοθούν οι συντεταγμένες και οι ορμές των σωματιδίων με την απαιτούμενη ακρίβεια), ενώ στην κβαντική φυσική είναι εκθετικό. Ο ίδιος ο Feynman γράφει:

> *Αλλά η πλήρης κβαντομηχανική περιγραφή για ένα μεγάλο σύστημα με R σωματίδια δίνεται από μια συνάρτηση $\psi(x_1, x_2, \dots, x_R, t)$ της οποίας λαμβάνουμε το πλάτος για να βρούμε τα σωματίδια $x_1, x_2, \dots, x_R$ και συνεπώς*

επειδή έχει τόσες πολλές μεταβλητές δεν είναι δυνατόν να προσομοιωθεί με ένα κανονικό υπολογιστή με αριθμό στοιχείων ανάλογο του R ή του N.

Ο Feynman πρότεινε επίσης ότι αυτή η επιβράδυνση μπορεί να αποφευχθεί χρησιμοποιώντας έναν υπολογιστή ο οποίος λειτουργεί με βάση τους νόμους της κβαντικής μηχανικής, ο οποίος θα είναι στη ουσία και ο ίδιος ένα κβαντικό σύστημα. Ουσιαστικά η ίδια η διεξαγωγή ενός κβαντικού πειράματος «υπολογίζει» το αποτέλεσμα του πειράματος αν αυτό προσομοιωνόταν σε υπολογιστή. Αυτή η ιδέα προτείνει, τουλάχιστον υπονοεί, ότι ένας κβαντικός υπολογιστής μπορεί να δουλεύει εκθετικά γρηγορότερα από έναν ντετερμινιστικό κλασικό υπολογιστή και να χρησιμοποιείται για όλα τα προβλήματα, κλασικά ή κβαντικά. Στο ίδιο άρθρο ο Feynman εξετάζει επίσης το πρόβλημα της προσομοίωσης ενός κβαντομηχανικού συστήματος με έναν πιθανοτικό υπολογιστή όμως καταλήγει ότι εξαιτίας των φαινομένων συμβολής πρόκειται για ένα δυσεπίλυτο πρόβλημα.

Κβαντομηχανικά μοντέλα υπολογισμού είχαν εφευρεθεί ήδη από το 1982 από τον Benioff (2), αλλά ο David Deutsch στο (3) έδειξε ότι το μοντέλο του Benioff μπορεί να προσομοιωθεί τέλεια από ένα συνηθισμένο υπολογιστή. Το 1985 στο παραπάνω άρθρο ο Deutsch ήταν ο πρώτος που έθεσε τα θεμέλια για τη θεωρία των κβαντικών υπολογισμών εισάγοντας ένα πλήρως κβαντικό μοντέλο για τους υπολογισμούς και δίνοντας την περιγραφή ενός Καθολικού Κβαντικού Υπολογιστή (Universal Quantum Computer). Αυτός ο υπολογιστής είναι το αντίστοιχο της μηχανής Turing στο κβαντικό πεδίο. Επίσης ο Deutsch όρισε σε μεταγενέστερη δημοσίευση τα κβαντικά δίκτυα. Η κατασκευή της καθολικής κβαντικής μηχανής Turing βελτιώθηκε από τους Bernstein και Vazirani στο (4), όπου έδειξαν πώς να κατασκευαστεί μια καθολική κβαντική μηχανή ικανή να προσομοιώνει τη λειτουργία οποιασδήποτε άλλης κβαντικής μηχανής με πολυωνυμική επιβράδυνση.

Η μεγάλη έκρηξη στο ενδιαφέρον της επιστημονικής κοινότητας έγινε το 1994 με την ανακάλυψη του αλγορίθμου παραγοντοποίησης του Shor (5). Ο αλγόριθμος αυτός καταφέρνει να λύσει το πρόβλημα της παραγοντοποίησης μεγάλων αριθμών, όπως και το πρόβλημα του διακριτού λογάριθμου, σε πολυωνυμικό χρόνο. Τα δύο αυτά προβλήματα δεν έχει αποδειχθεί ότι δεν λύνονται σε πολυωνυμικό χρόνο με κλασικούς αλγόριθμους αλλά αυτή είναι η κοινή πεποίθηση των επιστημόνων μέχρι στιγμής. Η μεγάλη σημασία του αλγορίθμου του Shor προκύπτει από το γεγονός ότι η αξιοπιστία του διάσημου κρυπτοσυστήματος RSA (δημοσίου κλειδιού) το οποίο έχει σχεδιαστεί για μυστικές επικοινωνίες βασίζεται στην υπόθεση ότι η παραγοντοποίηση μεγάλων ακεραίων αποτελεί ένα δυσεπίλυτο (intractable) πρόβλημα. Ο Shor έδειξε ότι αυτό δεν ισχύει αν κάποιος καταφέρει να κατασκευάσει ένα κβαντικό υπολογιστή. Επομένως μυστικές υπηρεσίες, κυβερνήσεις και οποιοσδήποτε που ασχολείται με την κρυπτογραφία έχει συμφέρον να εφευρεθούν λειτουργικοί κβαντικοί υπολογιστές – κβαντικοί υπολογιστές μεγάλης κλίμακας.

Επόμενος σημαντικός σταθμός ήταν το 1996 που ανακαλύφθηκε ο αλγόριθμος κβαντικής αναζήτησης του Lov Grover. Με αυτό τον αλγόριθμο είναι δυνατόν να βρεθεί ένα στοιχείο σε μια αταξινόμητη λίστα μήκους n σε χρόνο $O(\sqrt{n})$. Αντίθετα για τους κλασικούς αλγόριθμους το κάτω όριο είναι $O(n)$. Επομένως παρ'όλο που δεν παρουσιάζει αυτός ο αλγόριθμος εκθετική επιτάχυνση όπως ο αλγόριθμος παραγοντοποίησης παρουσιάζει την απόδειξη ότι οι κβαντικοί υπολογιστές είναι ισχυρότεροι σε ορισμένες περιπτώσεις από τους κλασικούς.

Από το 1998 μέχρι και σήμερα οι εξελίξεις στον χώρο των κβαντικών υπολογιστών αφορούν κυρίως στην κατασκευή του υλικού από το οποίο θα αποτελούνται. Έτσι το 1998 κατασκευάστηκαν οι πρώτοι κβαντικοί υπολογιστές 2 και 3 qubit και εκτελέστηκε ο αλγόριθμος του Grover. Επόμενος σταθμός είναι το 2001 που έγινε η πρώτη εκτέλεση του αλγορίθμου του Shor σε κβαντικό υπολογιστή στο ερευνητικό κέντρο της IBM στο Almaden και στο πανεπιστήμιο του Stanford. Ο αριθμός $15 = 3 \times 5$ παραγοντοποιήθηκε χρησιμοποιώντας 10^{18} πανομοιότυπα μόρια.

Από τότε μέχρι σήμερα εκατοντάδες ερευνητικά κέντρα προσπαθούν να κατασκευάσουν αξιόπιστους κβαντικούς υπολογιστές χρησιμοποιώντας διαφορετικά υλικά. Η μεγαλύτερη δυσκολία ανακύπτει από δύο αντικρουόμενες προϋποθέσεις. Από τη μία η μνήμη ενός υπολογιστή η οποία αποτελείται από μικροσκοπικά κβαντικά συστήματα πρέπει να απομονωθεί όσο τέλεια γίνεται για να προστατευθεί από καταστροφική αλληλεπίδραση με το περιβάλλον. Από την άλλη η «κβαντική κεντρική μονάδα επεξεργασίας» δεν πρέπει να είναι εντελώς απομονωμένη, αφού οι υπολογισμοί πρέπει να είναι συνεχείς, και ένας «ελεγκτής» πρέπει να ελέγχει ότι το κβαντικό σύστημα εξελίσσεται με το ζητούμενο τρόπο. Μάλιστα το πρόβλημα ότι ανεξέλεγκτα σφάλματα είναι δυνατόν να προκύψουν κατά τη διάρκεια των υπολογισμών δεν είναι καινούριο: στην κλασική θεωρία πληροφορίας θεωρούμε συχνά ένα θορυβώδες κανάλι το οποίο μπορεί να αλλοιώσει τα μηνύματα. Η δουλειά του παραλήπτη είναι να εξάγει την σωστή πληροφορία από το παραμορφωμένο μήνυμα χωρίς επιπλέον μετάδοση πληροφορίας. Η κλασική θεωρία πληροφορίας ασχολείται με αυτό το πρόβλημα και το συμπέρασμα που προκύπτει χάρη στην εργασία του Claude Shannon είναι το εξής: Για ένα σχετικά θορυβώδες κανάλι υπάρχει ένα σύστημα κωδικοποίησης των μηνυμάτων το οποίο μας επιτρέπει να μειώσουμε την πιθανότητα σφάλματος στη μετάδοση όσο θέλουμε.

Αρχικά ήταν κοινή η άποψη ότι ένα αντίστοιχο μοντέλο ήταν αδύνατο για τους κβαντικούς υπολογισμούς ακόμη και σε θεωρητικό επίπεδο, κυρίως εξαιτίας του θεωρήματος «Μη Αντιγραφής», το οποίο έλεγε ότι η κβαντική πληροφορία είναι αδύνατον να διπλασιαστεί με ακρίβεια. Παρ' όλα αυτά το 1995 ο Shor έδειξε στο (6) ότι μπορούμε να κατασκευάσουμε σχήματα διόρθωσης λαθών για τους κβαντικούς υπολογιστές, και άρα θεμελίωσε την θεωρία των κβαντικών κωδικών διόρθωσης σφαλμάτων. Αυτή η θεωρία είναι ακόμα αντικείμενο μελετών και ίσως οδηγήσει μια μέρα στην κατασκευή κβαντικών υπολογιστών μεγάλης κλίμακας.

1.3 Ιστορία των γλωσσών κβαντικού προγραμματισμού

Συνηθίζεται οι κβαντικοί αλγόριθμοι να περιγράφονται με κβαντικά κυκλώματα και πύλες. Αυτή η προσέγγιση είναι αναμενόμενη αφού οι επιτρεπόμενες διεργασίες στα κβαντικά bit περιγράφονται στο χαμηλότερο επίπεδο. Ο κβαντικός υπολογισμός είναι ένας ιδιαίτερος τρόπος σκέψης σε αντίθεση με τον κλασικό υπολογισμό ο οποίος είναι συμβατός με την κοινή λογική. Όπως θα δούμε και παρακάτω οι μόνες διεργασίες που μπορεί να κάνει κάποιος με τα κβαντικά bits είναι η αναδιάταξη τους, η εφαρμογή ενός ορθομοναδιαίου μετασχηματισμού και η μέτρηση τους. Αυτοί οι μετασχηματισμοί υλοποιούνται με κβαντικές πύλες και κυκλώματα και άρα οι αλγόριθμοι θα υλοποιούνται με τον ίδιο τρόπο.

Το μειονέκτημα όμως αυτής της προσέγγισης είναι ότι μειώνεται η εκφραστικότητα του κβαντικού προγραμματισμού και η ευκολία κατασκευής νέων αλγορίθμων. Για παράδειγμα είναι πολύ δύσχρηστος ο προγραμματισμός σε assembly ενώ πολύ

ευκολότερος σε υψηλότερου επιπέδου γλώσσες προγραμματισμού. Για αυτό το λόγο αναπτύχθηκαν οι πρώτες γλώσσες κβαντικού προγραμματισμού. Το κοινό χαρακτηριστικό τους είναι ότι χειρίζονται ένα η περισσότερα κβαντικά bits μαζί με τα επιπλέον κλασικά bits ώστε να μπορούν να υλοποιήσουν και κλασικούς αλγόριθμους. Χωρίζονται όμως σε διάφορες κατηγορίες.

Μια πρώτη κατηγοριοποίησή τους είναι σε τρία υποσύνολα παρόμοια με τα αντίστοιχα των συμβατικών γλωσσών. Αυτά είναι οι προστακτικές γλώσσες κβαντικού προγραμματισμού, οι συναρτησιακές γλώσσες και όλες οι υπόλοιπες. Αρχικά αναπτύχθηκαν οι προστακτικές γλώσσες των οποίων τα προγράμματα αποτελούνται από μια ακολουθία εντολών προστακτικής φύσεως κατ' αναλογία με τις αντίστοιχες γλώσσες του συμβατικού υπολογισμού. Ακόμη και σήμερα βέβαια οι περισσότεροι αλγόριθμοι ακολουθούν υποσυνείδητα αυτό το μοντέλο και συνεχίζεται η ανάπτυξη τους. Αργότερα εμφανίστηκε η μεγάλη τάση των συναρτησιακών γλωσσών οι οποίες ταιριάζουν αρκετά καλά στο κβαντικό μοντέλο καθώς κάθε αλγόριθμος πρόκειται ουσιαστικά για συνεχείς μετασχηματισμούς πάνω σε μια ποσότητα κβαντικής πληροφορίας. Τέλος στην τρίτη κατηγορία ανήκουν γλώσσες διαφορετικών μορφών.

Εκτός από αυτήν την κατηγοριοποίηση υπάρχει και ο χωρισμός των κβαντικών γλωσσών σε δύο τάξεις: αυτές που επιτρέπουν μόνο κλασική ροή ελέγχου και αυτές που επιτρέπουν και κβαντική ροή ελέγχου. Η πρώτη και απλούστερη αποτελείται από γλώσσες οι οποίες επιτρέπουν την κβαντική υπέρθεση μόνο στην κατάσταση των qubits (κβαντικά bit). Αντίθετα ο έλεγχος του προγράμματος γίνεται με κλασικό τρόπο. Συνοπτικά η υπέρθεση είναι η ικανότητα των κβαντικών συστημάτων να βρίσκονται σε περισσότερες από μία καταστάσεις ταυτόχρονα. Στο πρώτο είδος γλωσσών οι οποίες αναφέρονται ως "quantum data, classical control paradigm" τα προγράμματα ακολουθούν μια συγκεκριμένη ροή και απλώς επεξεργάζονται κβαντικά bits. Η δεύτερη κατηγορία είναι οι γλώσσες που επιτρέπουν και κβαντικό έλεγχο: "quantum data and control paradigm". Σε αυτές το πρόγραμμα μπορεί να βρίσκεται σε υπέρθεση δύο δυνατών μονοπατιών υπολογισμού. Φυσικά και τα δεδομένα που χειρίζονται μπορούν να είναι σε υπέρθεση. Η κβαντική μηχανή Turing του Deutsch λειτουργούσε σύμφωνα με αυτό το μοντέλο.

1.3.1 Προστακτικές γλώσσες

Η ιστορία των γλωσσών κβαντικού προγραμματισμού ήταν αρχικά συνυφασμένη με τα μοντέλα που ανακαλύφθηκαν. Όπως είδαμε η κβαντική μηχανή Turing (QTM) του Deutsch εφευρέθηκε το 1985. Αυτή είχε μια στοιχειώδη ψευδογλώσσα - οδηγίες προστακτικής μορφής. Το 1993 οι Bernstein και Vazirani εκτός από την βελτίωση της μηχανής πρότειναν και κάποια προγραμματιστικά δομικά στοιχεία. Πιθανότατα όμως η πρώτη πρόταση για μια σαφώς ορισμένη κβαντική γλώσσα προγραμματισμού, σε αντίθεση με τις περιγραφές QTM μηχανών, ήρθε το 1996 με την εργασία του Knill. Αυτός ορίζει έναν προστακτικό ψευδοκώδικα ο οποίος έτρεχε σε ένα μοντέλο κβαντικής μηχανής τυχαίας πρόσβασης (Quantum Random Access Machine – QRAM) αντίστοιχο με το κλασικό μοντέλο RAM. Ο Knill κατανοεί ότι ο κβαντικός ψευδοκώδικας δεν αποτελεί από μόνος του μια υλοποιήσιμη κβαντική γλώσσα αλλά είναι ένα σημαντικό βήμα εμπρός σε σχέση με τις εκ των υστέρων περιγραφές του πως πρέπει να υλοποιούνται οι κβαντικοί υπολογισμοί. Κατά τη διάρκεια μιας περιόδου αρκετών χρόνων (1998, 2000, 2001, 2002, 2003) ο Ömer ανέπτυξε την QCL, την πρώτη πραγματική κβαντική γλώσσα προγραμματισμού, με σύνταξη αρκετά παρόμοια της C.

Μάλιστα υλοποίησε και ένα λειτουργικό προσομοιωτή της γλώσσας. Η QCL περιέχει μία πλήρη κλασική γλώσσα προγραμματισμού ως υποσύνολο και παρέχει ένα σύνολο χρήσιμων κβαντικών δομών υψηλού επιπέδου όπως διαχείριση μνήμης και αυτόματη παραγωγή ελεγχόμενων εκδόσεων τελεστών. Οι Sanders&Zuliani (2000) και Zuliani (2001) ορίζουν την προστακτική γλώσσα qQCL, η οποία βασίζεται σε μια αυστηρή γλώσσα εντολών (guarded-command language).

1.3.2 Συναρτησιακές γλώσσες

Ο Maymin (1996) ορίζει δύο επεκτάσεις του λ-λογισμού. Η πρώτη, ένας πιθανοτικός λ-λογισμός (λ^p-λογισμός) ενσωματώνει κατανομές όρων επιτρέποντας σε συναρτήσεις να επιστρέφουν τυχαία αποτελέσματα. Η δεύτερη, ένας κβαντικός λ-λογισμός (λ^q-λογισμός), επεκτείνει την έννοια αυτή επιτρέποντας στους όρους να αντιπροσωπεύονται και από αρνητικές κατανομές. Επομένως υπάρχει η δυνατότητα αφαιρετικής συμβολής δύο όρων όταν δύο κατανομές συνδυάζονται. Κάτι παρόμοιο είναι δυνατό και στο μοντέλο κβαντικού υπολογισμού όπως θα δούμε σε επόμενες ενότητες. Βέβαια αυτό περιορίζει τους όρους σε διαφορές φάσεων μόνο 180°, όμως ο Maymin αποδεικνύει ότι ο λ^q-λογισμός μπορεί να λύσει με αποδοτικό τρόπο NP-πλήρη προβλήματα! Τελικά όμως φαίνεται ότι ο λογισμός αυτός είναι αυστηρά πιο εκφραστικός από το μοντέλο κβαντικού προγραμματισμού το οποίο μπορεί να υλοποιηθεί φυσικά. Ο Van Tonder (2004) όρισε επίσης ένα κβαντικό λ-λογισμό, λ_q, ο οποίος είναι μια γλώσσα αγνού κβαντικού προγραμματισμού, δηλαδή δεν επιτρέπονται μετρήσεις. Οι Valiron (2004a,b) και οι Valiron&Selinger (2005; 2006) ορίζουν μια συναρτησιακή γλώσσα υψηλού επιπέδου, την QPL, η οποία ακολουθεί το σχήμα «κβαντικών δεδομένων και κλασικού ελέγχου». Η γλώσσα βασίζεται στο λ-λογισμό κλήσης κατά τιμή και περιλαμβάνει τόσο κλασικά όσο και κβαντικά δεδομένα. Υπάρχει ένα γραμμικό σύστημα τύπων και αποδεικνύονται ιδιότητες διατήρησης και ασφάλειας τύπων. Οι Altenkirch και Grattage (2005a; 2005b) μία πρώτης-τάξεως συναρτησιακή γλώσσα, την QML, στην οποία η ροή του ελέγχου όπως και τα δεδομένα μπορούν να είναι κβαντικά. Η σημασιολογία της QML ακολουθεί το παράδειγμα του Selinger (2004c) με όρους υπερτελεστών και πινάκων πυκνότητας και μία μετάφραση σε κβαντικά κυκλώματα. Ακολουθεί και αυτή γραμμικό σύστημα τύπων. Μετεξέλιξη της QML αποτελεί η γλώσσα nQML των Lampis, Ginis, Papakyriakou, Papaspyrou (2006) και η οποία είναι αυτή με την οποία θα ασχοληθούμε στην εργασία. Επιτρέπει νέες δομές ελέγχου και είναι απλούστερη χωρίς να χάνει σε εκφραστικότητα. Η σημασιολογία της μέχρι στιγμής αποτελείται μόνο από τελεστές σε πίνακες πυκνότητας και όχι από κβαντικά κυκλώματα.

1.3.3 Άλλες κατηγορίες γλωσσών

Πρόκειται για γλώσσες που ενσωματώνουν στοιχεία ξένα προς τις δύο προηγούμενες κατηγορίες και είναι σχετικά νέες. Για παράδειγμα οι Gay&Nagarajan (2005; 2006) ορίζουν το λογισμό διαδικασιών CQP (Communicating Quantum Processes) και οι Jorand&Larire (2004) την QPAlg (Quantum Process Algebra). Και οι δύο γλώσσες μπορούν να περιγράψουν συστήματα τα οποία συνδυάζουν κλασικό και κβαντικό υπολογισμό και επικοινωνία και ο στόχος τους είναι να υποστηρίξουν τον φορμαλισμό του ορισμού και της επαλήθευσης κβαντικών κρυπτογραφικών πρωτοκόλλων. Ο Παπανικολάου (2004) περιγράφει συνοπτικά τον ορισμό της γλώσσας QSPEC, η οποία

υποστηρίζει τις δηλώσεις ταυτόχρονων διαδικασιών, με επικοινωνία, με ένα προστακτικό στυλ βασισμένο στις γλώσσες Promela και Probmela.

1.4 Σύνοψη της εργασίας

Η υπόλοιπη εργασία οργανώνεται ως εξής:

- Στο κεφάλαιο 2 παρουσιάζεται το μοντέλο του κβαντικού υπολογισμού και εξηγούνται οι βασικές λειτουργίες που μπορούν να γίνουν στα κβαντικά bits. Ταυτόχρονα δίνεται το μαθηματικό υπόβαθρο των κβαντικών υπολογισμών, το οποίο χρησιμοποιείται στα επόμενα κεφάλαια της εργασίας.
- Ολόκληρο το κεφάλαιο 3 αφορά στα κβαντικά κυκλώματα. Δείχνουμε τους συμβολισμούς που χρησιμοποιούνται για την παράσταση των κυκλωμάτων και τα διάφορα θεωρήματα που αφορούν στην κατασκευή τους. Ιδιαίτερη σημασία δίνεται στην κατασκευή κυκλωμάτων από πλήρη σύνολα πυλών καθώς με αυτόν τον τρόπο πιστεύεται ότι θα υλοποιηθούν οι κβαντικοί υπολογιστές του μέλλοντος.
- Το κεφάλαιο 4 είναι μια περιληπτική περιγραφή δύο γλωσσών κβαντικού προγραμματισμού προγενέστερων της nQML. Πρόκειται για μια εισαγωγή σε γλώσσες οι οποίες βρίσκονται πιο κοντά στο κλασικό μοντέλο προγραμματισμού ώστε να γίνει ευκολότερη η μετάβαση στην nQML.
- Στο κεφάλαιο 5 παρουσιάζεται η γλώσσα nQML και εξηγείται το σύστημα τύπων και η σημασιολογία της, τα οποία είναι απαραίτητα για την κατασκευή κυκλωμάτων.
- Στο κεφάλαιο 6 γίνεται η μετάφραση των εντολών της nQML σε κυκλώματα, που είναι και ο στόχος της εργασίας. Αρχικά ορίζεται η κλάση των κυκλωμάτων που θα δημιουργηθούν από την γλώσσα και έπειτα σχολιάζεται η μετατροπή κάθε εντολής ξεχωριστά.
- Τέλος στο κεφάλαιο 7 παρουσιάζονται τα συμπεράσματα της εργασίας και μελλοντικές ερευνητικές κατευθύνσεις που είναι δυνατόν να ακολουθηθούν.

2 Κβαντικοί Υπολογισμοί

2.1 Εισαγωγή

Οι κβαντικοί υπολογισμοί βασίζονται στις αρχές της κβαντομηχανικής οι οποίες είναι αντίθετες προς την κοινή λογική και εμπειρία. Εδώ θα αναφερθούμε επιγραμματικά στις αρχές οι οποίες είναι σημαντικές για τους κβαντικούς υπολογισμούς.

Η πρώτη είναι η αρχή της υπέρθεσης η οποία λέει ότι ένα κβαντικό σύστημα μπορεί να βρίσκεται σε 2 ή περισσότερες καταστάσεις ταυτόχρονα. Στο παράδειγμα των υπολογιστών ενώ ένα bit μπορεί να είναι κάθε στιγμή σε μία από τις καταστάσεις 0 ή 1, ένα κβαντικό bit (ή qubit) μπορεί να βρίσκεται και στις δύο καταστάσεις ταυτόχρονα. Αυτή η εξωτική κατάσταση εκφράζεται στη φυσική πλήρως από την κυματοσυνάρτηση του σωματιδίου, το οποίο παριστάνει το qubit. Αυτό το σωματίδιο βρίσκεται τότε σε μια υπέρθεση καταστάσεων. Η κυματοσυνάρτηση του καθορίζει πλήρως τη συμπεριφορά του. Επομένως και ο τρόπος υπέρθεσης στην οποία βρίσκεται ένα qubit καθορίζει την μετέπειτα εξέλιξη του όπως θα δούμε παρακάτω. Σημειώνω ότι η υπέρθεση δεν είναι χαρακτηριστικό μόνο σωματιδίων αλλά και ολόκληρων συστημάτων (άλλωστε και τα σωματίδια δεν είναι στοιχειώδη). Επομένως είναι δυνατόν ένα σύστημα από qubits να βρίσκεται σε περισσότερες καταστάσεις από δύο σε αντίθεση με το μονό qubit. Για παράδειγμα μια συστοιχία n qubits μπορεί να είναι σε οποιεσδήποτε από τις καταστάσεις $\{0,1,\dots,2^n-1\}$ ταυτόχρονα.

Η δεύτερη αρχή είναι η αρχή της κβαντικής μέτρησης. Σύμφωνα με αυτή την αρχή κατά την μέτρηση ενός κβαντικού συστήματος η κυματοσυνάρτηση «καταρρέει» και το σύστημα μεταβαίνει σε μία συγκεκριμένη κατάσταση η οποία είναι και το αποτέλεσμα της μέτρησης. Οποιεσδήποτε άλλες μετρήσεις του ίδιου μεγέθους στο σύστημα θα δώσουν το ίδιο αποτέλεσμα. Ουσιαστικά δηλαδή από τη μέτρηση και μετά το qubit συμπεριφέρεται κλασικά. Φυσικά εδώ πρέπει να επισημάνω ότι το qubit δεν σταμάτησε να είναι κβαντικό σύστημα, απλώς το συγκεκριμένο μέγεθος του απέκτησε μια ορισμένη τιμή. Σύμφωνα με την αρχή της απροσδιοριστίας του Heisenberg άλλες ιδιότητες του παραμένουν απροσδιόριστες ή αλλιώς σε υπέρθεση.

Οι δύο παραπάνω αρχές έχουν ελεγχθεί πειραματικά και κανένα πείραμα δεν τις έχει θέσει υπό αμφισβήτηση. Από την πρώτη πηγάζουν τα πλεονεκτήματα των κβαντικών υπολογιστών. Ένας υπολογιστής που βρίσκεται σε πολλές καταστάσεις ταυτόχρονα αυξάνει το δυνατό παραλληλισμό και μάλιστα στην περίπτωση των κβαντικών υπολογισμών έχουμε εκθετική αύξηση. Ένα qubit το οποίο είναι ταυτόχρονα 0 και 1 θα μας δώσει στο τέλος των υπολογισμών ένα αποτέλεσμα το οποίο είναι υπέρθεση των αποτελεσμάτων που θα είχαμε πάρει αν το qubit ήταν 0 ή 1. Ομοίως η πραγματοποίηση ενός υπολογισμού n qubit θα μας δώσει υπέρθεση 2^n αποτελεσμάτων. Η δεύτερη αρχή όμως μειώνει κατά πολύ την αξία αυτού του παραλληλισμού και προκαλεί τις δυσκολίες στο σχεδιασμό κβαντικών αλγορίθμων. Σύμφωνα με αυτή είναι αδύνατο να μετρήσουμε όλες τις καταστάσεις στις οποίες βρίσκεται ο υπολογιστής μας αλλά μόνο μία. Όλες οι υπόλοιπες καταστρέφονται. Τέλος όπως θα δούμε παρακάτω οι νόμοι της κβαντομηχανικής εμπεριέχουν επιπλέον περιορισμούς, όπως η αντιστρεψιμότητα, οι οποίοι δυσκολεύουν περισσότερο το σχεδιασμό των κβαντικών αλγορίθμων.

2.2 Κβαντικά bit

Η πρωταρχική μονάδα δεδομένων ενός κβαντικού υπολογιστή είναι το qubit. Το κλασικό bit μπορεί να βρίσκεται όπως ξέρουμε στην κατάσταση 0 ή 1. Αντίθετα το κβαντικό bit μπορεί να βρίσκεται σε οποιαδήποτε κατάσταση της μορφής $q = a\mathbf{0} + b\mathbf{1}$ όπου $a, b \in \mathbb{C}$ και δεν είναι ταυτόχρονα 0. Δύο καταστάσεις q και q' για τις οποίες ισχύει $q = \gamma q'$ με $\gamma \in \mathbb{C}$ είναι ισοδύναμες. Συνήθως θεωρούμε την κανονικοποίηση $|a|^2 + |b|^2 = 1$ οπότε όλες οι ισοδύναμες καταστάσεις αντιπροσωπεύονται από μία μόνο. Τα a, b είναι μιγαδικοί αριθμοί και φυσικά δεν έχουν άμεση φυσική σημασία. Με την κανονικοποίηση όμως το τετράγωνο του μέτρου τους μας δίνει την πιθανότητα να μετρήσουμε την αντίστοιχη κατάσταση. Δηλαδή σε μία μέτρηση έχουμε $|a|^2$ πιθανότητα να μετρήσουμε 1 και $|b|^2$ να μετρήσουμε 0.

Σημειώνω σε αυτό το σημείο ότι ενώ δύο καταστάσεις μπορούν να δίνουν ακριβώς τα ίδια μετρήσιμα αποτελέσματα (ίδια με την έννοια της ίδιας κατανομής μετρήσεων) μπορεί να μην είναι ισοδύναμες. Για παράδειγμα οι καταστάσεις $\frac{1}{\sqrt{2}}\mathbf{1} + \frac{1}{\sqrt{2}}\mathbf{0}$ και $\frac{1}{\sqrt{2}}\mathbf{1} - \frac{1}{\sqrt{2}}\mathbf{0}$. Μόνο με περαιτέρω επεξεργασία τους μπορούμε να ξεχωρίσουμε την μία κατάσταση από την άλλη και όχι με μετρήσεις. Μάλιστα η πρώτη μέτρηση στην κάθε κατάσταση θα καταστρέψει την υπέρθεση και όλη η πληροφορία για τα a, b θα χαθεί.

Επομένως κάθε κατάσταση ενός qubit ορίζεται μονοσήμαντα από ένα ζεύγος μιγαδικών αριθμών και άρα πρόκειται για διανύσματα στο χώρο $\mathbb{C} \times \mathbb{C}$. Η βάση αυτού του χώρου είναι τα διανύσματα $\begin{pmatrix}1\\0\end{pmatrix}$ και $\begin{pmatrix}0\\1\end{pmatrix}$ τα οποία συμβολίζουν τις καταστάσεις 0 και 1 αντίστοιχα. Αυτές οι καταστάσεις ονομάζονται κλασικές καταστάσεις καθώς ένα κλασικό bit βρίσκεται σε μία από τις δύο. Στη βιβλιογραφία οι καταστάσεις των qubits συμβολίζονται ως $|q\rangle$ και οι δύο σταθερές καταστάσεις που αποτελούν και την βάση του χώρου ως $|0\rangle$ και $|1\rangle$. Όλες οι υπόλοιπες καταστάσεις αποτελούν υπέρθεση αυτών των δύο. Ο παραπάνω συμβολισμός ονομάζεται bracket notation ή Dirac notation και τα παραπάνω διανύσματα ονομάζονται ket. Υπάρχουν και bra τα οποία συμβολίζονται ως $\langle q|$ και είναι τα αναστροφοσυζυγή των προηγουμένων.

2.3 Σφαίρα Bloch

Μία άλλη όψη των ιδιοτήτων των κβαντικών bit, η οποία θα μας βοηθήσει σε επόμενο κεφάλαιο να κατανοήσουμε καλύτερα την επίδραση των μετασχηματισμών σε αυτά, είναι η σφαίρα Bloch.

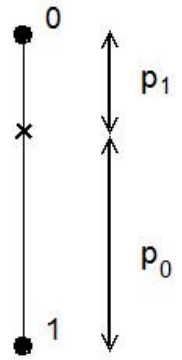
Αρχικά ας αναλογιστούμε την περίπτωση των ντετερμινιστικών κλασικών bit. Η κατάσταση ενός bit μπορεί να περιγραφεί από μία μόνο δυαδική τιμή ψ, η οποία θα είναι ίση με 0 ή με 1. Αυτή η περιγραφή μπορεί να εκφραστεί με όρους από το Σχήμα 2.1. Σε αυτό το σχήμα η κατάσταση δείχνεται με ένα σημείο σε μία από τις δύο θέσεις, που φαίνονται με τα δύο σημεία 0 και 1.

Σχήμα 2.1: Αναπαράσταση κλασικού bit

Έπειτα έχουμε την ελαφρώς πιο περίπλοκη κατάσταση ενός κλασικού bit του οποίου η τιμή δεν είναι γνωστή ακριβώς, αλλά ξέρουμε ότι μπορεί να είναι 0 ή 1 με πιθανότητες $\boldsymbol{p_0}$ και $\boldsymbol{p_1}$ αντίστοιχα. Καλούμε αυτό το bit ένα πιθανοτικό κλασικό bit. Η κατάσταση αυτού του bit περιγράφεται πλήρως από τις πιθανότητες $\boldsymbol{p_0}$ και $\boldsymbol{p_1}$, οι οποίες ικανοποιούν την εξίσωση $\boldsymbol{p_0 + p_1 = 1}$ (δείχνοντας ότι ξέρουμε ότι το bit πρέπει να είναι είτε 0 είτε 1). Μπορούμε να παραστήσουμε αυτές τις δύο πιθανότητες με το 2-διάστατο μοναδιαίο διάνυσμα

$$\begin{pmatrix} \boldsymbol{p_0} \\ \boldsymbol{p_1} \end{pmatrix}$$

του οποίου τα στοιχεία είναι πραγματικά και μη αρνητικά. Αυτή η περιγραφή μπορεί να εκφραστεί με όρους βασισμένους στο Σχήμα 2.2 που φαίνεται παρακάτω. Η κατάσταση μπορεί να ζωγραφιστεί ως ένα σημείο στη γραμμή μεταξύ των σημείων 0 και 1. Υποθέτουμε ότι το ευθύγραμμο τμήμα έχει μήκος 1 και η θέση του σημείου στη γραμμή καθορίζεται από τις πιθανότητες $\boldsymbol{p_0}$ και $\boldsymbol{p_1}$.



Σχήμα 2.2: Αναπαράσταση πιθανοτικού bit

Παρατηρήστε ότι με μόνο ένα αντίγραφο ενός τέτοιου πιθανοτικού bit, δεν είναι δυνατόν να μετρήσουμε τις $\boldsymbol{p_0}$ και $\boldsymbol{p_1}$ ακριβώς. Μόνο αν με κάποιο τρόπο μας είχαν δοθεί αρκετά ανεξάρτητα αντίγραφα του ίδιου πιθανοτικού bit (όπου κάθε αντίγραφο ανεξάρτητα παράγει έξοδο 0 με πιθανότητα $\boldsymbol{p_0}$ και 1 με πιθανότητα $\boldsymbol{p_1}$), τότε θα μπορούσαμε να συλλέξουμε αρκετά στατιστικά δεδομένα για τις τιμές $\boldsymbol{p_0}$ και $\boldsymbol{p_1}$. Στη γενική περίπτωση δεν μπορούμε να «κλωνοποιήσουμε» αυτό το bit και να πάρουμε δύο ή περισσότερα ανεξάρτητα αντίγραφα που θα μας επιτρέπανε να αποκτήσουμε καλές εκτιμήσεις των $\boldsymbol{p_0}$ και $\boldsymbol{p_1}$. Όπως ανέφερα και παραπάνω ίδια είναι η περίπτωση και για τα κβαντικά bit.

Στο τέλος ας θεωρήσουμε ένα κβαντικό bit του οποίου η κατάσταση περιγράφεται από ένα μοναδιαίο 2-διάστατο διάνυσμα στο $\mathbb{C}^{\boldsymbol{2}}$. Ένα σημαντικό χαρακτηριστικό των καταστάσεων αυτών είναι ότι η κατάσταση που περιγράφεται από το διάνυσμα $\boldsymbol{e^{i\theta}|\psi\rangle}$ είναι εντελώς ισοδύναμη με την κατάσταση που περιγράφεται από το διάνυσμα $\boldsymbol{|\psi\rangle}$,

όπου το $e^{i\theta}$ είναι οποιοσδήποτε μιγαδικός μοναδιαίου μέτρου. Δηλαδή οι δύο καταστάσεις όχι μόνο δίνουν τα ίδια αποτελέσματα σε μετρήσεις, αλλά και δεν μπορούν να διαχωριστούν με οποιονδήποτε μετασχηματισμό. Ουσιαστικά πρόκειται για διαφορετικό μαθηματικό τύπο για την ίδια φυσική κατάσταση. Για παράδειγμα η κατάσταση $|0\rangle + |1\rangle$ είναι η ίδια με αυτή που περιγράφεται από το διάνυσμα $e^{i\theta}|0\rangle + e^{i\theta}|1\rangle$. Όμως οι σχετικοί παράγοντες φάσης μεταξύ δύο ορθογώνιων καταστάσεων στην υπέρθεση είναι φυσικά σημαντικοί. Δηλαδή η κατάσταση που περιγράφεται από το διάνυσμα $|0\rangle + |1\rangle$ είναι φυσικά διαφορετική από την $|0\rangle + e^{i\theta}|1\rangle$. Παρόλο που οι δύο καταστάσεις δίνουν τα ίδια αποτελέσματα με απευθείας μέτρηση, ύστερα από κατάλληλο μετασχηματισμό είναι δυνατόν να διακριθεί η μία από την άλλη. Τυπικά θα μπορούσαμε να περιγράψουμε τις κβαντικές καταστάσεις με κλάσεις ισοδυναμίας μοναδιαίων διανυσμάτων, αλλά για απλότητα προσδιορίζουμε μόνο ένα μοναδιαίο διάνυσμα, έχοντας κατά νου ότι δύο διανύσματα με ολική διαφορά φάσης είναι ισοδύναμα.

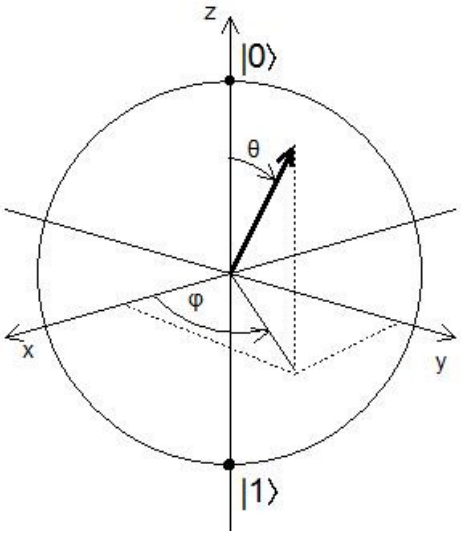
Επομένως σύμφωνα με την προηγούμενη παράγραφο μπορούμε να περιγράψουμε την πιο γενική κατάσταση $|\psi\rangle$ ενός qubit με ένα διάνυσμα της μορφής

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

(Αυτό είναι μοναδιαίο και έχει και οποιονδήποτε παράγοντα σχετικής φάσης)

Μια τέτοια κατάσταση παριστάνεται συχνά με ένα σημείο στην επιφάνεια μιας 3-διάστατης σφαίρας, γνωστής ως σφαίρας Bloch, η οποία φαίνεται στο Σχήμα 2.3. Οι δύο πραγματικές παράμετροι θ και φ είναι αρκετές για να περιγράψουν ένα διάνυσμα κατάστασης, αφού τα διανύσματα κατάστασης πρέπει να έχουν μέτρο 1 και είναι ισοδύναμα όσον αφορά μία συνολική διαφορά φάσης. Τα σημεία στην σφαίρα Bloch μπορούν να εκφραστούν και σε Καρτεσιανές συντεταγμένες ως

$$(x, y, z) = (\sin\theta\cos\varphi\,,\sin\theta\sin\varphi\,,\cos\theta)$$



Σχήμα 2.3: Αναπαράσταση κβαντικού bit - Σφαίρα Bloch

Μάλιστα αναφερόμαστε σε σφαίρα και όχι σφαιρική επιφάνεια επειδή στα εσωτερικά σημεία της σφαίρας Bloch αντιστοιχούν μικτές καταστάσεις ενός qubit (βλ. ενότητα 2.6). Αν ένα qubit βρίσκεται στη μικτή κατάσταση $\sum_i \lambda_i\{u_i\}$ και αν το διάνυσμα Bloch της $|u_i\rangle$ είναι το $(\alpha_{x,i}, \alpha_{y,i}, \alpha_{z,i})$ τότε το σημείο Bloch για ολόκληρη τη μικτή

κατάσταση είναι το $\sum_i \boldsymbol{\lambda_i}(\boldsymbol{\alpha_{x,i}}, \boldsymbol{\alpha_{y,i}}, \boldsymbol{\alpha_{z,i}}) = (\sum_i \boldsymbol{\lambda_i}\, \boldsymbol{\alpha_{x,i}}, \sum_i \boldsymbol{\lambda_i}\, \boldsymbol{\alpha_{y,i}}, \sum_i \boldsymbol{\lambda_i}\, \boldsymbol{\alpha_{z,i}})$ το οποίο στη γενική περίπτωση είναι εσωτερικό σημείο. Για παράδειγμα η πλήρως μικτή κατάσταση $\frac{\mathbf{1}}{\mathbf{2}}\{|\mathbf{0}\rangle\} + \frac{\mathbf{1}}{\mathbf{2}}\{|\mathbf{1}\rangle\}$ αντιπροσωπεύεται από το κέντρο της σφαίρας Bloch. Φυσικά υπάρχουν πολλοί κυρτοί συνδυασμοί επιφανειακών σημείων που αντιστοιχούν στην ίδια μικτή κατάσταση, κάτι το οποίο συμβαίνει όπως είδαμε και με τους πίνακες πυκνότητας μικτών καταστάσεων. Τέλος πρέπει να προσεχθεί το γεγονός ότι η σφαίρα Bloch παριστάνει την κατάσταση ενός qubit μόνο και όχι καταχωρητών.

2.4 Κβαντικοί καταχωρητές – Entanglement

Μια άλλη ιδιαιτερότητα των κβαντικών υπολογιστών είναι η συμπεριφορά πολλών qubit μαζί. Όπως γνωρίζουμε στους κλασικούς υπολογιστές η τιμή ενός bit είναι ανεξάρτητη από την τιμή ενός άλλου. Αντίθετα στους κβαντικούς υπολογιστές αυτό δεν ισχύει.

Όπως ανέφερα και παραπάνω ένα σύστημα πολλών qubits μπορεί να βρίσκεται σε υπέρθεση καταστάσεων σαν σύνολο. Για παράδειγμα ένα σύστημα δύο κβαντικών bit μπορεί να βρίσκεται στην κατάσταση $|q\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$ όπου δεν είναι όλα τα a, b, c, d μηδέν. Επομένως οι καταστάσεις δύο qubit ανήκουν στο διανυσματικό χώρο 4 διαστάσεων $\mathbb{C}^{\mathbf{4}}$.

Ας υποθέσουμε τώρα ότι δύο qubits q_1 και q_2 είναι ανεξάρτητα και βρίσκονται στις καταστάσεις $|q_1\rangle = \alpha|0\rangle + b|1\rangle$ και $|q_2\rangle = \gamma|0\rangle + \delta|1\rangle$. Τότε η κοινή τους κατάσταση θα είναι $|q_1\rangle|q_2\rangle = |q_1\rangle \otimes |q_2\rangle = \alpha\gamma|0\rangle|0\rangle + \alpha\delta|0\rangle|1\rangle + \beta\gamma|1\rangle|0\rangle + \beta\delta|1\rangle|1\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle$.

Παρατηρούμε ότι δεν μπορούν όλες οι καταστάσεις του διανυσματικού χώρου $\mathbb{C}^{\mathbf{4}}$ να γραφτούν ως καταστάσεις ανεξάρτητων qubits. Παράδειγμα αποτελεί η κατάσταση $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Για να γραφτεί αυτή ως γινόμενο δύο ανεξάρτητων καταστάσεων πρέπει $\alpha\delta = \beta\gamma = 0$ και $\alpha\gamma = \beta\delta = \frac{1}{\sqrt{2}}$ πράγμα αδύνατο. Σε αυτήν την περίπτωση λοιπόν τα δύο qubits δεν είναι ανεξάρτητα.

Γενικεύοντας ένας καταχωρητής n qubits βρίσκεται σε μία κατάσταση η οποία είναι ένα διάνυσμα του χώρου $\mathbb{C}^{\mathbf{2^n}}$ και είναι υπέρθεση των 2^n καταστάσεων $|00\ldots0\rangle, |00\ldots1\rangle, \ldots, |11\ldots1\rangle$.

Ο όρος entanglement (συμπλοκή) αναφέρεται σε δύο ή περισσότερα qubits τα οποία δεν είναι ανεξάρτητα αλλά είναι συζευγμένα όπως στο προηγούμενο παράδειγμα. Αυτό το φαινόμενο δημιουργεί την πολύ περίεργη «δράση από απόσταση» δύο σωματιδίων. Στην προηγούμενη περίπτωση μια μέτρηση στο πρώτο qubit προκαλεί κατάρρευση της κυματοσυνάρτησης και επηρεάζει και την τιμή του άλλου qubit να είναι ίση. Αν μετρηθεί 0 το πρώτο qubit τότε και το δεύτερο γίνεται 0 ακαριαία.

Όταν δύο κβαντικά bit δεν είναι συζευγμένα λέμε πως είναι ανεξάρτητα. Σε αυτή την περίπτωση η κοινή τους κατάσταση δίνεται όπως είδαμε αν πολλαπλασιάσουμε τις δύο καταστάσεις. Η αντίστοιχη πράξη από τη γραμμική άλγεβρα είναι το τανυστικό γινόμενο (tensor product). Αυτό ορίζεται ως εξής: Αν $u \in \mathbb{C}^n$ και $v \in \mathbb{C}^m$ τότε $w = u \otimes v \in \mathbb{C}^{mn}$ και $w_{(i,j)} = u_i \cdot v_j$. Αυτή η πράξη φαίνεται και στο πρώτο παράδειγμα των δύο ανεξάρτητων qubit q_1 και q_2.

2.5 Διεργασίες σε κβαντικά bits

Υπάρχουν μόνο δύο τρόποι με τους οποίους μπορούμε να χειριστούμε κβαντικά bits τα οποία βρίσκονται σε μια οποιαδήποτε κατάσταση. Ο ένας είναι οι ορθομοναδιαίοι μετασχηματισμοί και ο άλλος η μέτρηση. Φυσικά μετά την μέτρηση το qubit μεταβαίνει σε κλασική κατάσταση και θεωρητικά μπορούμε να το χειριστούμε με κλασικές πύλες αν αντιγράψουμε την τιμή του σε ένα κλασικό bit. Με ένα ορθομοναδιαίο μετασχηματισμό όμως μπορούμε να το επαναφέρουμε σε οποιαδήποτε κβαντική κατάσταση.

2.5.1 Ορθομοναδιαίοι μετασχηματισμοί

Η κατάσταση ενός κβαντικού συστήματος αλλάζει εφαρμόζοντας πάνω του έναν ορθομοναδιαίο μετασχηματισμό. Αρχικά εξετάζω την περίπτωση ενός μονού qubit. Η κατάσταση του είναι ένα διάνυσμα στον χώρο $\mathbb{C}^2$. Ένας μετασχηματισμός σε αυτή την κατάσταση ορίζεται ως ένας πίνακας 2×2 με στοιχεία μιγαδικούς αριθμούς. Ο μετασχηματισμός λέγεται ορθομοναδιαίος όταν ο αντίστοιχος πίνακας είναι ορθομοναδιαίος δηλαδή αν έχουμε τον πίνακα S ισχύει ότι $SS^* = I$ όπου S^* είναι ο αναστροφοσυζυγής πίνακας του S. Η κατάσταση του qubit μετασχηματίζεται τότε ως εξής:

$$\begin{pmatrix} a \\ b \end{pmatrix} \mapsto S \begin{pmatrix} a \\ b \end{pmatrix}$$

Όπως ανέφερα και παραπάνω η κατάσταση ενός καταχωρητή n qubits είναι ένα διάνυσμα στο χώρο $\mathbb{C}^{2^n}$. Επομένως οι αντίστοιχοι ορθομοναδιαίοι μετασχηματισμοί είναι διαστάσεων $2^n \times 2^n$. Αυτοί οι μετασχηματισμοί λέγονται και κβαντικές πύλες n qubits κυρίως όταν χρησιμοποιούνται στα κβαντικά κυκλώματα.

Μερικές από τις πιο χρήσιμες κβαντικές πύλες είναι οι εξής:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$

$$cH = \begin{pmatrix} I & 0 \\ 0 & H \end{pmatrix} \quad cX = \begin{pmatrix} I & 0 \\ 0 & X \end{pmatrix} \quad cY = \begin{pmatrix} I & 0 \\ 0 & Y \end{pmatrix} \quad cZ = \begin{pmatrix} I & 0 \\ 0 & Z \end{pmatrix} \quad cT = \begin{pmatrix} I & 0 \\ 0 & T \end{pmatrix}$$

$$SW = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Η πύλη H καλείται πύλη Hadamard και είναι πολύ σημαντική πύλη γιατί μέσω αυτής παράγουμε τις υπερθέσεις καταστάσεων. Ένα κβαντικό bit που βρίσκεται στην κατάσταση 0 αν περάσει μέσα από αυτή την πύλη θα βρεθεί στην κατάσταση $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ που είναι μία υπέρθεση των 0 και 1 με ίσες πιθανότητες.

Η πύλη X καλείται πύλη NOT επειδή όταν το qubit είναι σε κλασική κατάσταση είτε 0 είτε 1 το αντιστρέφει. Όταν είναι σε κβαντική υπέρθεση εναλλάσσει τις δύο

συντεταγμένες της κατάστασης. Δηλαδή $X\binom{\alpha}{\beta} = \binom{\beta}{\alpha}$. Οι πύλες X, Y, Z ονομάζονται πύλες Pauli προς τιμή του διάσημου φυσικού. Σχετίζονται με τις τρεις συνιστώσες του spin των σωματιδίων και παίζουν σπουδαίο ρόλο στο μοντέλο των κβαντικών κυκλωμάτων όπως θα δούμε σε επόμενο κεφάλαιο.

Οι πύλες στην δεύτερη σειρά αποτελούν τις controlled εκδοχές των πυλών της πρώτης σειράς. Δέχονται σαν είσοδο δύο qubits και αν το πρώτο είναι 1 εφαρμόζεται η μονή πύλη στο δεύτερο. Αν είναι 0 δεν γίνεται τίποτα· τους εφαρμόζεται όπως φαίνεται από τον πίνακα ο μοναδιαίος μετασχηματισμός. Φυσικά το πρώτο qubit μπορεί να βρίσκεται σε υπέρθεση καταστάσεων οπότε και η συνολική έξοδος θα είναι σε υπέρθεση. Μάλιστα τα δύο qubits παύουν να είναι ανεξάρτητα. Όπως θα δούμε σε επόμενο κεφάλαιο έχει αποδειχθεί ότι για οποιαδήποτε πύλη (ορθομοναδιαίο μετασχηματισμό) μπορεί να κατασκευαστεί η αντίστοιχη controlled εκδοχή της και αφού και η ίδια αποτελεί ορθομοναδιαίο μετασχηματισμό μπορεί να ελέγχεται από απεριόριστο αριθμό qubits.

Η πύλη T ονομάζεται και πύλη $\pi/8$ γιατί εφαρμόζει μια σχετική διαφορά φάσης στους δύο μιγαδικούς που αποτελούν το διάνυσμα κατάστασης ενός qubit. Η πύλη SW εκτελεί απλώς ένα swap στα δύο qubit στα οποία εφαρμόζεται.

Στην περίπτωση που θέλουμε να εφαρμόσουμε ένα μετασχηματισμό σε ένα σύνολο από qubits τότε πρέπει με τη βοήθεια του τανυστικού γινομένου να κατασκευάσουμε τον κατάλληλο ορθομοναδιαίο πίνακα. Το τανυστικό γινόμενο σε πίνακες ορίζεται ως εξής: Αν $A \in \mathbb{C}^{n\times n}$ και $B \in \mathbb{C}^{m\times m}$ τότε $C = A \otimes B \in \mathbb{C}^{nm\times nm}$ και $c_{(i,j),(i',j')} = a_{ii'}, b_{jj'}$. Για παράδειγμα αν έχουμε 4 qubits και θέλουμε να εφαρμόσουμε στο δεύτερο τον μετασχηματισμό X τότε κατασκευάζουμε τον πίνακα $I \otimes X \otimes I \otimes I$ (ο I είναι ο 2×2 μοναδιαίος πίνακας) και με αυτόν πολλαπλασιάζουμε την κατάσταση των 4 qubit, η οποία είναι τώρα ένα διάνυσμα $2^4 = 16$ στοιχείων. Στην περίπτωση πιο περίπλοκων μετασχηματισμών σε 2 ή περισσότερα qubits χρειάζονται συνθετότεροι πίνακες. Για παράδειγμα αν σε τρία qubits θέλουμε να εφαρμόσουμε controlled Hadamard στο πρώτο και στο τρίτο πρέπει πρώτα να εναλλάξουμε το δεύτερο με το τρίτο (πίνακας $I \otimes SW$) μετά να εφαρμόσουμε τον μετασχηματισμό στο πρώτο και στο δεύτερο (πίνακας $cH \otimes I$) και μετά να εναλλάξουμε πάλι το δεύτερο με το τρίτο (πίνακας $I \otimes SW$). Άρα ο συνολικός πίνακας μετασχηματισμού είναι ο $(I \otimes SW) \cdot (cH \otimes I) \cdot (I \otimes SW)$. Οι πίνακες I είναι 2×2 ενώ οι υπόλοιποι 4×4.

Όπως θα δούμε στην ενότητα των κβαντικών κυκλωμάτων, κάθε ορθομοναδιαίος μετασχηματισμός μπορεί να προσεγγιστεί με οποιαδήποτε ακρίβεια από ένα πλήρες σύνολο από πύλες $\{CNOT, H, \frac{\pi}{8}\}$.

2.5.2 Μετρήσεις

Η δεύτερη διεργασία που μπορούμε να εφαρμόσουμε στα κβαντικά bits είναι η μέτρηση. Πρόκειται για μια μη αντιστρέψιμη διαδικασία κατά την οποία προσπαθούμε να βρούμε την τιμή ενός qubit. Ο τρόπος μέτρησης δεν ενδιαφέρει για τον σκοπό της θεωρίας κβαντικών υπολογισμών και διαφέρει από υλοποίηση σε υλοποίηση. Τα χαρακτηριστικά στοιχεία της πράξης της μέτρησης που μας ενδιαφέρουν είναι ότι δίνει αποτέλεσμα είτε 0 είτε 1 με συγκεκριμένη πιθανότητα και ότι μετά τη μέτρηση η κυματοσυνάρτηση του qubit καταρρέει είτε στην κατάσταση $\binom{1}{0}$ είτε στην $\binom{0}{1}$.

Καθώς η δύναμη των κβαντικών αλγορίθμων βασίζεται στην υπέρθεση καταστάσεων η οποία καταστρέφεται από τις μετρήσεις συνήθως αυτές εκτελούνται είτε στην αρχή είτε στο τέλος των κβαντικών αλγορίθμων. Στην αρχή μπορεί να χρησιμοποιηθεί η μέτρηση για την αρχικοποίηση των qubits. Μετρώντας το qubit το θέτουμε στην κατάσταση 0 ή 1 και ανάλογα με το αποτέλεσμα και την τιμή που θέλουμε να πάρει εφαρμόζουμε σε αυτό τον αντιστρέψιμο μετασχηματισμό NOT. Παρακάτω θεωρούμε ότι μας δίνεται η δυνατότητα αρχικοποίησης ενός qubit στην τιμή 0 και αυτό γίνεται με την παραπάνω διαδικασία. Στο τέλος των αλγορίθμων οι μετρήσεις χρησιμοποιούνται για να μας δώσουν το ζητούμενο αποτέλεσμα.

Έστω για παράδειγμα ένα qubit στην κατάσταση $|q\rangle = a|0\rangle + b|1\rangle$. Τότε μια μέτρησή του θα μας δώσει αποτέλεσμα 1 με πιθανότητα $|a|^2$ και 0 με πιθανότητα $|b|^2$. Προφανώς απαιτείται τα a και b να είναι κανονικοποιημένα, δηλαδή $|a|^2 + |b|^2 = 1$. Σε αντίθετη περίπτωση οι αντίστοιχες πιθανότητες θα είναι $\frac{|a|^2}{|a|^2+|b|^2}$ και $\frac{|b|^2}{|a|^2+|b|^2}$. Περαιτέρω μέτρηση στο ίδιο qubit θα δώσει το ίδιο αποτέλεσμα με την πρώτη μέτρηση αφού η κατάσταση του qubit θα είναι πια κλασική. Ένα δεύτερο παράδειγμα είναι το σύστημα των δύο qubits $|q\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$. Υποθέτοντας ότι οι συντελεστές είναι κανονικοποιημένοι μέτρηση στο πρώτο qubit θα δώσει 0 με πιθανότητα $|a|^2 + |b|^2$ και 1 με πιθανότητα $|c|^2 + |d|^2$. Η νέα κατάσταση στην οποία θα καταρρεύσει τώρα το σύστημα θα είναι $|q\rangle = a|00\rangle + b|01\rangle$ στην πρώτη περίπτωση και $|q\rangle = c|10\rangle + d|11\rangle$ στην δεύτερη. Οι νέοι συντελέστες τώρα δεν είναι κανονικοποιημένοι επομένως για την πρώτη από τις δύο καταστάσεις οι πιθανότητα το δέυτερο qubit να δώσει 0 είναι $\frac{|a|^2}{|a|^2+|b|^2}$ και 1 $\frac{|b|^2}{|a|^2+|b|^2}$. Αντίστοιχα στην περίπτωση που το πρώτο qubit δώσει 1 τότε μέτρηση στο δεύτερο θα έχει πιθανότητες $\frac{|c|^2}{|c|^2+|d|^2}$ και $\frac{|d|^2}{|c|^2+|d|^2}$ για αποτελέσματα 0 και 1. Παρατηρούμε ότι η συνολική πιθανότητα παρατήρησης κάθε μίας εκ των καταστάσεων $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ είναι $|a|^2, |b|^2, |c|^2, |d|^2$ αντίστοιχα ανεξάρτητα από την σειρά των μετρήσεων. Στην κβαντομηχανική η σειρά των μετρήσεων επηρεάζει στην γενική περίπτωση τα αποτελέσματα κάτι το οποίο δεν συμβαίνει όμως στους κβαντικούς υπολογισμούς.

Μια νέα κανονικοποίηση που χρησιμοποιείται συχνά γιατί απλοποιεί τους υπολογισμούς είναι να κανονικοποιούμε τα πλάτη της κάθε κατάστασης με βάση τη συνολική πιθανότητα να φθάσουμε στην κατάσταση αυτή. Με αυτό τον τρόπο όπως φαίνεται και από το παραπάνω παράδειγμα δεν χρειάζεται να κανονικοποιούμε τα πλάτη στη μονάδα μετά από κάθε μέτρηση.

2.6 Αγνές και μικτές καταστάσεις

Όπως ανέφερα παραπάνω η κατάσταση ενός καταχωρητή n qubits είναι ένα διάνυσμα του χώρου $\mathbb{C}^{2^n}$. Υπάρχει περίπτωση όμως να θέλουμε να αναπαραστήσουμε την ατελή μας γνώση για την κατάσταση του καταχωρητή. Για παράδειγμα ας θεωρήσουμε το μονό qubit στην κατάσταση $|q\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Έστω ότι κάποιος εκτελεί μια μέτρηση σε αυτό και κρατάει κρυφό το αποτέλεσμα. Τότε αυτό το qubit βρίσκεται σε μία από τις δύο καταστάσεις $|0\rangle$ και $|1\rangle$ με πιθανότητα $1/2$. Για έναν παρατηρητή οποίος δεν ξέρει το αποτέλεσμα της μέτρησης λέμε ότι το qubit βρίσκεται στην μικτή

κατάσταση $\frac{1}{2}\{|0\rangle\}+\frac{1}{2}\{|1\rangle\}$. Γενικά κάθε μικτή κατάσταση γράφεται στη μορφή $\lambda_1\{u_1\}+\lambda_2\{u_2\}+\ldots+\lambda_n\{u_n\}$ με $0\leq\lambda_i\leq 1$, $\sum_i\lambda_i=1$ και τα u_i αγνές καταστάσεις.

Πρέπει να σημειώσουμε ότι οι μικτές καταστάσεις δεν έχουν κάποιο φυσικό νόημα. Κάθε κβαντικό σύστημα βρίσκεται κάθε στιγμή σε μία αγνή κατάσταση (πιθανώς με υπέρθεση). Η μικτή κατάσταση δεν εκφράζει υπέρθεση αλλά τη μερική γνώση μας για την κατάσταση του συστήματος. Από αυτό φαίνεται ότι είναι δυνατόν ένα σύστημα να χαρακτηρίζεται από δύο ή περισσότερες μικτές καταστάσεις αλλά με μία μόνο αγνή κατάσταση.

Οι διεργασίες που μπορούμε να εφαρμόσουμε σε κβαντικές μικτές καταστάσεις είναι προφανώς οι ίδιες που μπορούμε να εφαρμόσουμε και στις αγνές καταστάσεις. Έτσι οι ορθομοναδιαίοι μετασχηματισμοί εφαρμόζονται πάνω στις αγνές καταστάσεις που αποτελούν τη μικτή κατάσταση. Δηλαδή $S\sum\lambda_i\{u_i\}=\sum\lambda_i\{Su_i\}$. Η μέτρηση σε μία μικτή κατάσταση έχει δύο περιπτώσεις. Αν γίνει γνωστό το αποτέλεσμά της στον παρατηρητή με τον οποίο έχει συσχετιστεί η μικτή κατάσταση τότε αυτή μεταβαίνει στην πιθανόν μικτή κατάσταση που αποτελείται από τις αγνές καταστάσεις που είναι συμβατές με την μέτρηση. Οι πιθανότητες κανονικοποιούνται κατάλληλα. Αν το αποτέλεσμα δεν γίνει γνωστό τότε η μικτή κατάσταση παραμένει αναλλοίωτη.

2.7 Πίνακες πυκνότητας

Εκτός από τα διανύσματα υπάρχει και ένας δεύτερος τρόπος παράστασης των καταστάσεων των κβαντικών καταστάσεων, ο οποίος είναι ενιαίος για τις αγνές και τις μικτές καταστάσεις. Αυτός ο τρόπος είναι οι πίνακες πυκνότητας.

Πρώτα θα δούμε τους πίνακες πυκνότητας στις αγνές καταστάσεις. Έστω ότι μία αγνή κατάσταση είναι η $u\in\mathbb{C}^{2^n}$ τότε ο πίνακας πυκνότητας ορίζεται ως ο $2^n\times 2^n$ πίνακας $D=uu^*=|q\rangle\langle q|$ (το ket είναι το αναστροφοσυζυγές του bra). Αυτός ο πίνακας περιγράφει την κατάσταση του συστήματος. Για παράδειγμα θεωρούμε την κατάσταση $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)=\begin{pmatrix}\frac{1}{\sqrt{2}}\\-\frac{1}{\sqrt{2}}\end{pmatrix}$. Αυτή έχει πίνακα πυκνότητας $\begin{pmatrix}\frac{1}{\sqrt{2}}\\-\frac{1}{\sqrt{2}}\end{pmatrix}\cdot\begin{pmatrix}\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\end{pmatrix}=\begin{bmatrix}\frac{1}{2} & -\frac{1}{2}\\-\frac{1}{2} & \frac{1}{2}\end{bmatrix}$. Παρατηρούμε ότι ο πίνακας πυκνότητας δεν καθορίζει μονοσήμαντα το διάνυσμα u αφού αν αυτό πολλαπλασιαστεί με μια σταθερά $\gamma\in\mathbb{C}$ με $|\gamma|=1$ τότε $\gamma u(\gamma u)^*=\gamma u\gamma^* u^*=|\gamma|^2uu^*=uu^*$. Όμως οι δύο καταστάσεις u και γu είναι ισοδύναμες επομένως αυτό είναι πλεονέκτημα των πινάκων πυκνότητας αφού έτσι όλες οι κανονικοποιημένες ισοδύναμες καταστάσεις εκφράζονται από έναν πίνακα.

Το μεγάλο πλεονέκτημα όμως των πινάκων πυκνότητας είναι στην αναπαράσταση των μικτών καταστάσεων. Η γενική περίπτωση μιας μικτής κατάστασης είναι η $\sum\lambda_i\{u_i\}$ όπου u_i είναι οι αγνές καταστάσεις. Τότε αυτή παριστάνεται από τον πίνακα πυκνότητας $\sum\lambda_i u_i u_i^*$. Έτσι με τον ίδιο τρόπο παριστάνονται τόσο οι αγνές όσο και οι μικτές καταστάσεις.

Ένα ενδιαφέρον χαρακτηριστικό των πινάκων πυκνότητας στις μικτές καταστάσεις είναι ότι παρουσιάζουν απώλεια πληροφορίας χωρίς όμως αυτό να αποτελεί μειονέκτημα. Αυτό φαίνεται καλύτερα στο παρακάτω παράδειγμα.

Θεωρώ το mixed state $\frac{1}{2}\{|0\rangle\}+\frac{1}{2}\{|1\rangle\}$ το οποίο έχει πίνακα πυκνότητας $\frac{1}{2}\begin{bmatrix}1 & 0\\ 0 & 0\end{bmatrix}+\frac{1}{2}\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}=\begin{bmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{2}\end{bmatrix}$.

Όμως τον ίδιο πίνακα έχει και το mixed state $\frac{1}{2}\left\{\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right\}+\frac{1}{2}\left\{\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\right\}$ ως εξής: $\frac{1}{2}\begin{bmatrix}\frac{1}{2} & \frac{1}{2}\\ \frac{1}{2} & \frac{1}{2}\end{bmatrix}+\frac{1}{2}\begin{bmatrix}\frac{1}{2} & -\frac{1}{2}\\ -\frac{1}{2} & \frac{1}{2}\end{bmatrix}=\begin{bmatrix}\frac{1}{2} & 0\\ 0 & \frac{1}{2}\end{bmatrix}$.

Όμως αυτό δεν αποτελεί μειονέκτημα των πινάκων πυκνότητας διότι οι δύο καταστάσεις έχουν τα ίδια παρατηρήσιμα αποτελέσματα. Υπάρχει όμως φυσική διαφορά ανάμεσα στις δύο καταστάσεις και άρα ένας παρατηρητής ο οποίος έχει παραπάνω γνώση για τις δύο καταστάσεις έχει τη δυνατότητα να τις διαχωρίσει. Αυτό το γεγονός βρίσκει εφαρμογή στην κβαντική κρυπτογραφία, που είναι έξω από τους σκοπούς αυτής της εργασίας και άρα εμείς θα θεωρούμε τις δύο μικτές καταστάσεις εντελώς ισοδύναμες. Ένα παράδειγμα της διαφοράς είναι το παράδειγμα στην παράγραφο 4.2.3.

Προκύπτει ότι για έναν πίνακα A έχω $A=\sum\lambda_i u_i u_i^*$ όπου τα λ_i είναι μη αρνητικές πραγματικές σταθερές με $\sum\lambda_i\leq 1$ και τα u_i μοναδιαία διανύσματα αν και μόνο αν ο πίνακας A είναι ερμιτιανός, θετικά ορισμένος με $tr(A)\leq 1$. Το ευθύ της πρότασης προκύπτει εύκολα από την παρατήρηση ότι $tr(u_i u_i^*)=\sum_{\mathrm{j}}\left|u_{i,j}\right|^2=1$ για μοναδιαία διανύσματα. Το ανάστροφο προκύπτει από το γεγονός ότι κάθε ερμιτιανός θετικά ορισμένος πίνακας A μπορεί να διαγωνιοποιηθεί ως $A=SDS^*$ με $D=\sum\lambda_i e_i e_i^*$ όπου e_i είναι τα διανύσματα της κανονικής βάσης του αντίστοιχου χώρου. Τότε θα ισχύει ότι $A=\sum\lambda_i(Se_i)(Se_i)^*$ και άρα τα λ_i είναι οι ιδιοτιμές του πίνακα A. Αν ο A είναι ένας πίνακας πυκνότητας που αντιστοιχεί σε αγνή κατάσταση τότε όλες οι ιδιοτιμές του είναι ίσες με το 0 εκτός από μία.

Συμπερασματικά ορίζουμε ως πίνακες πυκνότητες τους θετικά ορισμένους ερμιτιανούς πίνακες για τους οποίους ισχύει $tr(A)\leq 1$. Το σύνολο αυτών των πινάκων με διάσταση n το συμβολίζουμε με $D_n\subseteq\mathbb{C}^{n\times n}$.

2.8 Κβαντικές λειτουργίες και πίνακες πυκνότητας

Όπως ανέφερα και παραπάνω υπάρχουν δύο μόνο τρόποι με τους οποίους μπορούμε να επιδράσουμε σε ένα κβαντομηχανικό σύστημα. Αυτοί είναι οι ορθομοναδιαίοι μετασχηματισμοί και οι μετρήσεις. Εδώ θα δούμε την επίδραση τους στους πίνακες πυκνότητας που περιγράφουν το σύστημα.

Ένας ορθομοναδιαίος μετασχηματισμός καθορίζεται από τον πίνακά του, έστω S. Τότε εφαρμογή αυτού στην αγνή κατάσταση u δίνει την κατάσταση Su. Επομένως ο αρχικός πίνακας πυκνότητας uu^* θα μετασχηματίζεται στον πίνακα $Su(Su)^*=Suu^*S^*$. Και καθώς στις μικτές καταστάσεις ο μετασχηματισμός εφαρμόζεται ξεχωριστά σε κάθε αγνή κατάσταση από την οποία αποτελείται, ένας πίνακας πυκνότητας A μικτής κατάστασης μετασχηματίζεται στον SAS^*.

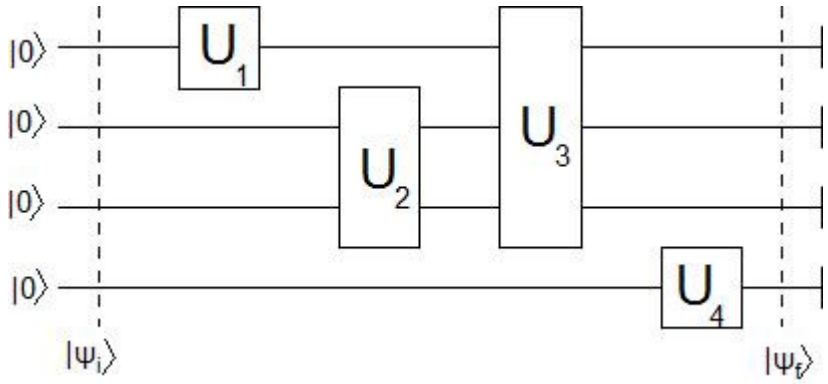
Αντίστοιχα μία μέτρηση μετατρέπει την αγνή κατάσταση $u = \begin{pmatrix} v \\ w \end{pmatrix}$ είτε στην $\begin{pmatrix} 0 \\ w \end{pmatrix}$ είτε στην $\begin{pmatrix} v \\ 0 \end{pmatrix}$ ανάλογα με το αποτέλεσμα της μέτρησης. Επομένως οι νέοι πίνακες πυκνότητας είναι είτε ο $\begin{pmatrix} 0 & 0 \\ 0 & ww^* \end{pmatrix}$ είτε ο $\begin{pmatrix} vv^* & 0 \\ 0 & 0 \end{pmatrix}$. Στην περίπτωση που γίνει η μέτρηση και το αποτέλεσμα ξεχαστεί τότε ο πίνακας πυκνότητας προκύπτει ότι είναι το άθροισμα των δύο τελευταίων, δηλαδή ο $\begin{pmatrix} vv^* & 0 \\ 0 & ww^* \end{pmatrix}$. Στις μικτές καταστάσεις με πίνακα πυκνότητας $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ το αποτέλεσμα μιας μέτρησης είναι οι πίνακες $\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$ ή $\begin{pmatrix} 0 & 0 \\ 0 & D \end{pmatrix}$.

3 Κβαντικά κυκλώματα

3.1 Εισαγωγή

Όλα τα παραπάνω αποτελούν ένα μαθηματικό υπόβαθρο το οποίο περιγράφει τους κβαντικούς υπολογισμούς. Ένα άλλο μοντέλο είναι αυτό των κβαντικών κυκλωμάτων και είναι αυτό με το οποίο θα ασχοληθώ κυρίως σε αυτή την διπλωματική εργασία. Το αντίστοιχο στους κλασικούς υπολογισμούς είναι τα λογικά κυκλώματα και οι λογικές πύλες. Όμως σε αντίθεση με τα κλασικά κυκλώματα τα κβαντικά κυκλώματα πρέπει να υπακούουν σε περαιτέρω περιορισμούς. Αυτοί είναι οι εξής:

- Οι μετρήσεις των qubits δεν γίνονται από το κβαντικό κύκλωμα αλλά θεωρούμε ότι γίνονται στο τέλος των υπολογισμών. Καταχρηστικά τις εισάγουμε στα κυκλώματα με ένα ειδικό σύμβολο. Φυσικά μπορεί να γίνει μέτρηση και στη μέση των υπολογισμών όμως όλες οι μετρήσεις μπορούν να μετατεθούν στο τέλος χωρίς να επηρεάσουν το τελικό αποτέλεσμα του αλγορίθμου.
- Δεν επιτρέπονται οι βρόχοι. Δηλαδή δεν μπορούμε να έχουμε ανάδραση από το ένα μέρος του κβαντικού κυκλώματος σε άλλο. Λέμε ότι το κύκλωμα πρέπει να είναι ακυκλικό. Αυτό έχει ως αποτέλεσμα κάθε κβαντικό κύκλωμα να σχεδιάζεται ως μια σειριακή ακολουθία μετασχηματισμών σε ένα σύνολο αρχικών qubits και να διαβάζεται από αριστερά προς τα δεξιά, όπως στο παρακάτω παράδειγμα.



Σχήμα 3.1: Παράδειγμα κβαντικού κυκλώματος. Η κατάσταση 4 qubit $|\mathbf{0}\rangle|\mathbf{0}\rangle|\mathbf{0}\rangle|\mathbf{0}\rangle$ εισέρχεται στο κύκλωμα από τα αριστερά. Τα κουτιά με επιγραφές $\boldsymbol{U_1, U_2, U_3, U_4}$ παριστάνουν κβαντικές πύλες που εφαρμόζονται στα qubit με τη σειρά που φαίνεται (από αριστερά προς τα δεξιά). Οι μικρές γραμμές στην δεξιά πλευρά του κυκλώματος δείχνουν ότι κάθε ένα από τα τέσσερα qubit της τελικής κατάστασης μετράται στη βάση του χώρου Hilbert ώστε να δώσει το αποτέλεσμα του κυκλώματος.

- Όλες οι πύλες έχουν ίσο αριθμό εισόδων και εξόδων. Αυτό είναι άμεση συνέπεια του γεγονότος ότι οι ορθομοναδιαίοι μετασχηματισμοί είναι υποχρεωτικά αντιστρέψιμοι.
- Επιπρόσθετα αν θεωρήσουμε ότι όλες οι αρχικοποιήσεις γίνονται στην αρχή του κυκλώματος και όλες οι μετρήσεις στο τέλος του, τότε το όλο κύκλωμα έχει ίσο αριθμό εισόδων και εξόδων αφού αποτελεί ένα μεγάλο ορθομοναδιαίο μετασχηματισμό. Από αυτό προκύπτει ότι το κύκλωμα δουλεύει και στην αντίθετη κατεύθυνση.
- Τα κλασικά κυκλώματα επιτρέπουν την ένωση δύο καλωδίων εξόδου · μια διαδικασία γνωστή ως FANIN. Το καλώδιο που προκύπτει από την ένωση είναι

το OR των δύο εισόδων. Προφανώς αυτή η λογική πράξη δεν είναι αντιστρέψιμη και επομένως δεν μπορεί να υλοποιηθεί σε κβαντικά κυκλώματα.

- Τέλος απαγορεύεται ο αντίστροφος μετασχηματισμός (FANOUT) καθώς και αυτός αποτελεί ένα μη αντιστρέψιμο μετασχηματισμό. Μάλιστα προκύπτει ότι ο διπλασιασμός ενός qubit απαγορεύεται από τους νόμους της κβαντικής μηχανικής. Σε επόμενη παράγραφο θα δούμε ένα παράδειγμα αυτού του γεγονότος σχεδιάζοντας ένα κύκλωμα που προσπαθεί να αντιγράψει ένα qubit.

3.2 Κβαντικές πύλες μίας εισόδου

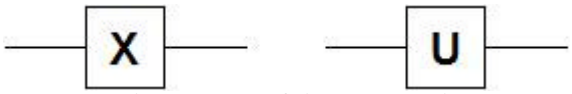
3.2.1 Βασικές πύλες

Τα κλασικά κυκλώματα αποτελούνται από καλώδια και λογικές πύλες. Τα καλώδια χρησιμοποιούνται για να μεταφέρουν πληροφορίες από το ένα μέρος του κυκλώματος στο άλλο, ενώ οι πύλες εκτελούν μετασχηματισμούς στις πληροφορίες αυτές. Στην περίπτωση των κλασικών πυλών μίας εισόδου υπάρχει μόνο μία μη τετριμμένη πύλη, η πύλη NOT. Αυτή εναλλάσσει τις κλασικές καταστάσεις 0 και 1, δηλαδή στον πίνακα αλήθειας 0→1 και 1→0. Στην περίπτωση των κβαντικών κυκλωμάτων υπάρχουν πολύ περισσότερες μη τετριμμένες πύλες μίας εισόδου.

Αρχικά εξετάζουμε την πύλη NOT για κβαντικά κυκλώματα. Όπως είδαμε και παραπάνω αυτή η πύλη υπάρχει και έχει πίνακα $\boldsymbol{X} = \begin{bmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{bmatrix}$. Παρατηρούμε ότι στις αμιγείς καταστάσεις $|0\rangle$ και $|1\rangle$ η πύλη αυτή λειτουργεί όπως και η κλασική πύλη. Τι γίνεται όμως στις υπερθέσεις; Η απάντηση είναι ότι η πύλη NOT (και οποιαδήποτε κβαντική πύλη) λειτουργεί γραμμικά πάνω στις υπερθέσεις καταστάσεων. Δηλαδή η κατάσταση $\boldsymbol{\alpha}|\mathbf{0}\rangle + \boldsymbol{\beta}|\mathbf{1}\rangle$ μετατρέπεται στην $\boldsymbol{\alpha}|\mathbf{1}\rangle + \boldsymbol{\beta}|\mathbf{0}\rangle$ · ως η πύλη να εφαρμοζόταν σε κάθε αμιγή κατάσταση μόνη της.

Το γιατί οι κβαντικές πύλες δρουν γραμμικά και όχι με κάποιον άλλο μη γραμμικό τρόπο είναι μια πολύ ενδιαφέρουσα ερώτηση και η απάντηση δεν είναι και τόσο προφανής. Προκύπτει ότι η γραμμική συμπεριφορά είναι γενικό χαρακτηριστικό των κβαντομηχανικών τελεστών και μάλιστα έχει εξακριβωθεί και πειραματικά. Επιπροσθέτως η μη γραμμική συμπεριφορά οδηγεί σε προφανή παράδοξα όπως ταξίδι στο χρόνο, επικοινωνία γρηγορότερη του φωτός και παραβίαση του δεύτερου νόμου της θερμοδυναμικής.

Ο συμβολισμός που θα χρησιμοποιήσουμε για τις πύλες ενός qubit φαίνεται παρακάτω για την πύλη X και για τυχαίο ορθομοναδιαίο μετασχηματισμό U.



Σχήμα 3.2: Κυκλωματικός συμβολισμός των πυλών NOT και U

Όπως ανέφερα και παραπάνω κάθε ορθομοναδιαίος πίνακας 2x2 ορίζει μια έγκυρη κβαντική πύλη μίας εισόδου. Επομένως το πολύ ενδιαφέρον επακόλουθο είναι ότι σε αντίθεση με τις κλασικές πύλες, όπου μόνο μία μη τετριμμένη πύλη υπάρχει – η NOT, υπάρχουν πολλές μη τετριμμένες κβαντικές πύλες μιας εισόδου. Δύο σημαντικές πύλες που θα χρησιμοποιήσουμε είναι οι εξής:

Η πύλη $\boldsymbol{Z} \equiv \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{-1} \end{bmatrix}$ η οποία αφήνει το $|\mathbf{0}\rangle$ ανεπηρέαστο και αλλάζει το $|\mathbf{1}\rangle$ σε $-|\mathbf{1}\rangle$. Θυμίζω ότι σε καταστάσεις υπέρθεσης δρα γραμμικά.

Και η πύλη $\boldsymbol{H} \equiv \frac{\mathbf{1}}{\sqrt{\mathbf{2}}}\begin{bmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{-1} \end{bmatrix}$ η οποία λέγεται πύλη Hadamard. Αυτή η πύλη περιγράφεται μερικές φορές ως η «τετραγωνική ρίζα της πύλης NOT» καθώς μετατρέπει το $|\mathbf{0}\rangle$ σε $(|\mathbf{0}\rangle + |\mathbf{1}\rangle)/\sqrt{\mathbf{2}}$, που είναι στη «μέση» των $|\mathbf{0}\rangle$ και $|\mathbf{1}\rangle$, και το $|\mathbf{1}\rangle$ στην $(|\mathbf{0}\rangle - |\mathbf{1}\rangle)/\sqrt{\mathbf{2}}$, που επίσης είναι στη «μέση» των $|\mathbf{0}\rangle$ και $|\mathbf{1}\rangle$. Όμως δεν ισχύει ότι η $\boldsymbol{H^2}$ είναι η πύλη NOT καθώς εύκολα βλέπει κανείς ότι $\boldsymbol{H^2 = I}$ και άρα εφαρμόζοντας δύο φορές την πύλη Hadamard σε ένα qubit το αφήνει ανεπηρέαστο.

3.2.2 Πύλες περιστροφών και εφαρμογή τους

Μια κβαντική πύλη U ενός qubit ξέρουμε ότι μετασχηματίζει μια κβαντική κατάσταση $|\boldsymbol{\psi}\rangle$ σε μία άλλη κατάσταση $\boldsymbol{U}|\boldsymbol{\psi}\rangle$. Χρησιμοποιώντας όρους της σφαίρας Bloch, η δράση της U στην $|\boldsymbol{\psi}\rangle$ μπορεί να θεωρηθεί ως μια μετακίνηση του διανύσματος που αντιστοιχεί στην $|\boldsymbol{\psi}\rangle$ στο διάνυσμα Bloch της $\boldsymbol{U}|\boldsymbol{\psi}\rangle$. Για παράδειγμα η πύλη NOT μεταφέρει την κατάσταση $|\mathbf{0}\rangle$ στην κατάσταση $|\mathbf{1}\rangle$ (και το αντίστροφο). Άρα στη σφαίρα Bloch μια τέτοια πράξη μπορεί να οπτικοποιηθεί ως μια περιστροφή γύρω από τον άξονα x κατά μία γωνία π.

Αν πάρουμε το εκθετικό των πυλών Pauli λαμβάνουμε κάποιους πολύ σημαντικούς ορθομοναδιαίους μετασχηματισμούς. Αυτές είναι οι πύλες περιστροφών (rotation gates), οι οποίες αντιστοιχούν σε περιστροφές γύρω από τους x-, y- και z- άξονες της σφαίρας Bloch. Ο ορισμός τους γίνεται σύμφωνα με τις πύλες Pauli και φαίνεται παρακάτω.

Πίνακας 3.1: Πύλες Pauli και πύλες περιστροφών

Πύλες Pauli	Πύλες περιστροφών
$\boldsymbol{X} \equiv \begin{bmatrix} \mathbf{0} & \mathbf{1} \\ \mathbf{1} & \mathbf{0} \end{bmatrix}$	$\boldsymbol{R_x(\theta)} \equiv \boldsymbol{e^{-\frac{i\theta X}{2}}} = \begin{bmatrix} \boldsymbol{\cos\frac{\theta}{2}} & \boldsymbol{-i\sin\frac{\theta}{2}} \\ \boldsymbol{-i\sin\frac{\theta}{2}} & \boldsymbol{\cos\frac{\theta}{2}} \end{bmatrix}$
$\boldsymbol{Y} \equiv \begin{bmatrix} \mathbf{0} & \boldsymbol{-i} \\ \boldsymbol{i} & \mathbf{0} \end{bmatrix}$	$\boldsymbol{R_y(\theta)} \equiv \boldsymbol{e^{-\frac{i\theta Y}{2}}} = \begin{bmatrix} \boldsymbol{\cos\frac{\theta}{2}} & \boldsymbol{-\sin\frac{\theta}{2}} \\ \boldsymbol{\sin\frac{\theta}{2}} & \boldsymbol{\cos\frac{\theta}{2}} \end{bmatrix}$
$\boldsymbol{Z} \equiv \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{-1} \end{bmatrix}$	$\boldsymbol{R_z(\theta)} \equiv \boldsymbol{e^{-\frac{i\theta Z}{2}}} = \begin{bmatrix} \boldsymbol{e^{-i\frac{\theta}{2}}} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{e^{i\frac{\theta}{2}}} \end{bmatrix}$

Αποδεικνύεται ότι οι τρεις πύλες $\boldsymbol{R_x, R_y, R_z}$ περιστρέφουν κάθε διάνυσμα Bloch κατά γωνία θ γύρω από τους αντίστοιχους άξονες x, y και z της σφαίρας Bloch. Η χρησιμότητα των τριών αυτών μετασχηματισμών φαίνεται στο παρακάτω θεώρημα.

Θεώρημα 3.2.1 *Έστω U μια ορθομοναδιαία πύλη μίας εισόδου. Τότε υπάρχουν πραγματικοί αριθμοί α, β, γ και δ τέτοιοι ώστε*

$$\boldsymbol{U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)}$$

Δηλαδή κάθε ορθομοναδιαίος μετασχηματισμός είναι ισοδύναμος με τρεις κατάλληλες περιστροφές γύρω από τους άξονες y και z και μια συνολική αλλαγή φάσης. Η τελευταία όπως είδαμε δεν αλλάζει την κατάσταση ενός qubit αλλά σε επόμενη παράγραφο που θα κατασκευάσουμε την ελεγχόμενη εκδοχή της πύλης U παίζει σημαντικό ρόλο. Η απόδειξη του θεωρήματος προκύπτει από το γεγονός ότι ο U είναι ορθομοναδιαίος και από τον ορισμό των πινάκων περιστροφής. Δεν υπάρχει κάποιος ειδικός ρόλος για τους άξονες y και z της σφαίρας Bloch. Είναι δυνατόν ο τυχαίος μετασχηματισμός να γραφτεί ως συνδυασμός περιστροφών γύρω από οποιουσδήποτε άλλους δύο μη παράλληλους άξονες της σφαίρας Bloch.
Από το προηγούμενο θεώρημα προκύπτει το εξής:

Θεώρημα 3.2.2 *Κάθε κβαντική πύλη μίας εισόδου μπορεί να γραφτεί στη μορφή*

$$\boldsymbol{U = e^{i\alpha} AXBXC}$$

όπου τα A, B, C είναι ορθομοναδιαίοι τελεστές οι οποίοι ικανοποιούν τη σχέση $\boldsymbol{ABC = I}$. *(Η Pauli πύλη X είναι η πύλη NOT).*

Σχήμα απόδειξης
Εύκολα φαίνεται ότι $\boldsymbol{XR_y(\theta)X = R_y(-\theta)}$ και $\boldsymbol{XR_z(\theta)X = R_z(-\theta)}$.
Από το προηγούμενο θεώρημα έχουμε ότι $\boldsymbol{U = e^{i\alpha} R_z(\beta)R_y(\gamma)R_z(\delta)}$ και λαμβάνουμε $\boldsymbol{A \equiv R_z(\beta)R_y(\gamma/2)}$, $\boldsymbol{B \equiv R_y(-\gamma/2)R_z(-(\delta+\beta)/2)}$ και $\boldsymbol{C \equiv R_z((\delta-\beta)/2)}$.
Αμέσως φαίνεται ότι $\boldsymbol{ABC = I}$ και

$$\boldsymbol{XBX = XR_y\left(-\frac{\gamma}{2}\right)R_z\left(-\frac{\delta+\beta}{2}\right)X = XR_y\left(-\frac{\gamma}{2}\right)XXR_z\left(-\frac{\delta+\beta}{2}\right)X = R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)}$$

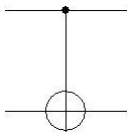
Άρα $\boldsymbol{AXBXC = R_z(\beta)R_y\left(\frac{\gamma}{2}\right)R_y\left(\frac{\gamma}{2}\right)R_z\left(\frac{\delta+\beta}{2}\right)R_z\left(\frac{\delta-\beta}{2}\right) = R_z(\beta)R_y(\gamma)R_z(\delta)}$ και $\boldsymbol{U = e^{i\alpha} AXBXC}$.

3.3 Ελεγχόμενες πύλες μίας εισόδου

3.3.1 Εισαγωγή

«Εάν το A είναι αληθές, τότε κάνε το B». Αυτός ο τύπος ελεγχόμενης διαδικασίας είναι ένας από τους πιο σημαντικούς στους υπολογισμούς, κλασικούς και κβαντικούς. Σε αυτό το μέρος εξηγώ πως περίπλοκες ελεγχόμενες διαδικασίες μπορούν να υλοποιηθούν χρησιμοποιώντας κβαντικά κυκλώματα που έχουν φτιαχτεί από στοιχειώδεις διεργασίες.

Η αρχέτυπη ελεγχόμενη διαδικασία είναι η ελεγχόμενη NOT που είδαμε σε προηγούμενη παράγραφο. Αυτή η πύλη, στην οποία θα αναφερόμαστε ως CNOT, είναι μια κβαντική πύλη με δύο qubits εισόδου, που λέγονται qubit ελέγχου και qubit στόχου. Σχεδιάζετε όπως στο παρακάτω σχήμα.



Σχήμα 3.3: Κυκλωματικός συμβολισμός της ελεγχόμενης πύλης NOT (CNOT). Η άνω γραμμή είναι το qubit ελέγχου, ενώ η κάτω το qubit στόχου.

Με όρους της βάσης του χώρου, η δράση της πύλης NOT δίνεται από $\boldsymbol{|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle}$ · δηλαδή εάν το bit ελέγχου είναι $\boldsymbol{|1\rangle}$ τότε το qubit στόχου αντιστρέφεται,

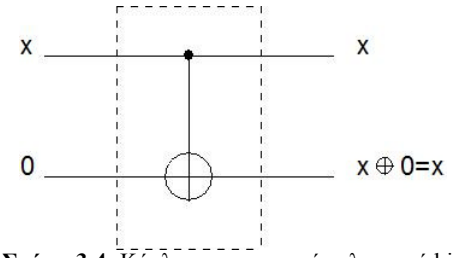
αλλιώς δεν αλλάζει καθόλου. Επομένως στη βάση $|\boldsymbol{\acute{\epsilon}\lambda\epsilon\gamma\chi o\varsigma, \sigma\tau\acute{o}\chi o\varsigma}\rangle$ η αναπαράσταση της πύλης CNOT σε πίνακα είναι

$$\begin{bmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{1} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{bmatrix}$$

3.3.2 No cloning theorem

Ένα πολύ σημαντικό θεώρημα στο οποίο θα αναφερθούμε πολλές φορές και γι αυτό του αφιερώνουμε αυτήν την παράγραφο είναι το θεώρημα «μη αντιγραφής» (no cloning theorem). Αυτό δηλώνει ότι είναι αδύνατον να κλωνοποιήσουμε – αντιγράψουμε ένα τυχαίο qubit.

Με τη βοήθεια της πύλης CNOT θα δείξουμε αυτή την ιδιότητα. Ας υποθέσουμε αρχικά ότι χρησιμοποιούμε κλασικό bit. Τότε για να το αντιγράψουμε μπορούμε να θέσουμε τη δεύτερη είσοδο της πύλης CNOT στο 0 και να εισάγουμε το bit προς αντιγραφή στην πρώτη είσοδο. Όπως αναφέραμε το πρώτο bit, έστω x, θα παραμείνει ανεπηρέαστο ενώ το δεύτερο θα γίνει $0 \oplus x = x$. Επομένως έχουμε καταφέρει να το διπλασιάσουμε.



Σχήμα 3.4: Κύκλωμα αντιγραφής κλασικού bit

Ας περάσουμε τώρα στην κβαντική περίπτωση όπου το πρώτο qubit είναι στην κατάσταση $|\psi\rangle = a|0\rangle + b|1\rangle$ και το δεύτερο στην $|0\rangle$. Η κατάσταση εισόδου και των δύο qubit είπαμε ότι είναι το τανυστικό τους γινόμενο

$$[a|0\rangle + b|1\rangle]|0\rangle = a|00\rangle + b|10\rangle$$

Περνώντας όμως μέσα από την πύλη CNOT παίρνουμε αποτέλεσμα $\boldsymbol{a}|00\rangle + b|11\rangle$. Αυτή η κατάσταση δεν είναι στη γενική περίπτωση η διπλασιασμένη $|\psi\rangle$ δηλαδή η

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$

Εύκολα βλέπουμε ότι το κύκλωμα δουλεύει σαν κύκλωμα διπλασιασμού μόνο όταν $a = 0$ ή $b = 0$, δηλαδή μόνο όταν το qubit βρίσκεται σε κλασική κατάσταση!

Μάλιστα αποδεικνύεται ότι οποιοδήποτε πιθανό κύκλωμα αντιγραφής μπορεί να αντιγράφει μόνο δύο συγκεκριμένες ορθογώνιες καταστάσεις (δύο καταστάσεις για τις οποίες το εσωτερικό τους γινόμενο είναι $\langle\psi|\varphi\rangle = 0$). Η απόδειξη συνοπτικά είναι η εξής: Έστω ότι U είναι ένας ορθομοναδιαίος μετασχηματισμός που αντιγράφει κάθε κατάσταση, ήτοι $|\psi\rangle \otimes |s\rangle \overset{U}{\rightarrow} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$. Η $|s\rangle$ είναι μια αρχική σταθερή αγνή κατάσταση, όπως στο παράδειγμά μας η $|0\rangle$. Αφού το κύκλωμα δουλεύει με κάθε δυνατή κατάσταση θα ισχύει ότι

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

Παίρνοντας το εσωτερικό γινόμενο των δύο εξισώσεων έχουμε ότι

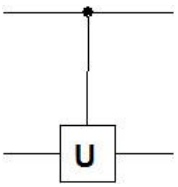
$$\big(U(|\psi\rangle \otimes |s\rangle)\big)^* U(|\varphi\rangle \otimes |s\rangle) = (|\psi\rangle \otimes |\psi\rangle)^*(|\varphi\rangle \otimes |\varphi\rangle) \Rightarrow$$
$$(|\psi\rangle \otimes |s\rangle)^* U^* U(|\varphi\rangle \otimes |s\rangle) = (|\psi\rangle \otimes |\psi\rangle)^*(|\varphi\rangle \otimes |\varphi\rangle) \Rightarrow$$
$$\boldsymbol{\langle \psi | \varphi \rangle = (\langle \psi | \varphi \rangle)^2}$$

Αλλά η εξίσωση $\boldsymbol{x = x^2}$ έχει μόνο δύο λύσεις, τις $\boldsymbol{x = 0}$ και $\boldsymbol{x = 1}$, και άρα είτε οι $\boldsymbol{|\psi\rangle}$ και $\boldsymbol{|\varphi\rangle}$ είναι ορθογώνιες είτε $\boldsymbol{|\psi\rangle = |\varphi\rangle}$. Άρα ένα κβαντικό κύκλωμα μπορεί να αντιγράφει μόνο το πολύ δύο ορθογώνιες καταστάσεις (όπως στο παράδειγμα οι $\boldsymbol{|0\rangle}$ και $\boldsymbol{|1\rangle}$) και άρα η κατασκευή κυκλώματος αντιγραφής είναι αδύνατη.

Υπάρχει και μια επιπλέον προσέγγιση στο θεώρημα, η οποία βασίζεται στη διαπίστωση ότι κάθε qubit περιέχει μέσα του κρυμμένη πληροφορία η οποία δεν είναι άμεσα προσβάσιμη με μετρήσεις. Αυτή η πληροφορία είναι κρυμμένη στην (πιθανώς άπειρη) αναπαράσταση των συντελεστών $\boldsymbol{a}$ και $\boldsymbol{b}$ του qubit $\boldsymbol{|q\rangle = a|0\rangle + b|1\rangle}$. Κατά την μέτρηση παίρνουμε 0 και 1 με πιθανότητες $\boldsymbol{|a|^2}$ και $\boldsymbol{|b|^2}$ και άρα χάνεται όλη η επιπλέον πληροφορία για τα $\boldsymbol{a}$ και $\boldsymbol{b}$ οριστικά. Αν όμως μπορούσαμε να το αντιγράψουμε τότε όλη αυτή η πληροφορία θα παρέμενε. Μάλιστα αν κατασκευάζαμε ένα αρκετά μεγάλο αριθμό ίδιων και ανεξάρτητων qubit και κάναμε στατιστική ανάλυση των μετρήσεων θα παίρναμε με όποια ακρίβεια επιθυμούσαμε τα $\boldsymbol{a}$ και $\boldsymbol{b}$. Σε ένα και μόνο σωματίδιο, π.χ. ένα πρωτόνιο, θα μπορούσαμε δηλαδή να αποθηκεύσουμε απεριόριστη ποσότητα πληροφορίας, π.χ. όλα τα βιβλία της γης, στην δυαδική αναπαράσταση των $\boldsymbol{a}$ και $\boldsymbol{b}$! Φυσικά κάτι τέτοιο δεν είναι δυνατό αφού το μόνο που μπορούμε να κάνουμε είναι να έχουμε συζευγμένα qubit και άρα ότι αποτέλεσμα μας δώσει η μέτρηση του πρώτου θα μας δώσουν και οι μετρήσεις όλων των υπολοίπων.

3.3.3 Κατασκευή τυχαίας ελεγχόμενης πύλης μίας εισόδου

Γενικότερα ας υποθέσουμε ότι U είναι ένας τυχαίος μονής εισόδου ορθομοναδιαίος μετασχηματισμός. Μια ελεγχόμενη U πύλη είναι ένας μετασχηματισμός δύο εισόδων, πάλι με ένα qubit ελέγχου και ένα qubit στόχου. Εάν το qubit ελέγχου είναι στην κατάσταση $\boldsymbol{|1\rangle}$ τότε ο μετασχηματισμός U εφαρμόζεται στο qubit στόχου, αλλιώς δεν αλλάζει. Δηλαδή $\boldsymbol{|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle}$. Η ελεγχόμενη U διαδικασία παριστάνεται από το κύκλωμα του ακόλουθου σχήματος.



Σχήμα 3.5: Κυκλωματικός συμβολισμός της ελεγχόμενης-U διαδικασίας. Η άνω γραμμή είναι το qubit ελέγχου, ενώ η κάτω το qubit στόχου. Εάν το qubit ελέγχου έχει τεθεί τότε ο U εφαρμόζεται στο qubit ελέγχου, αλλιώς δεν επηρεάζεται.

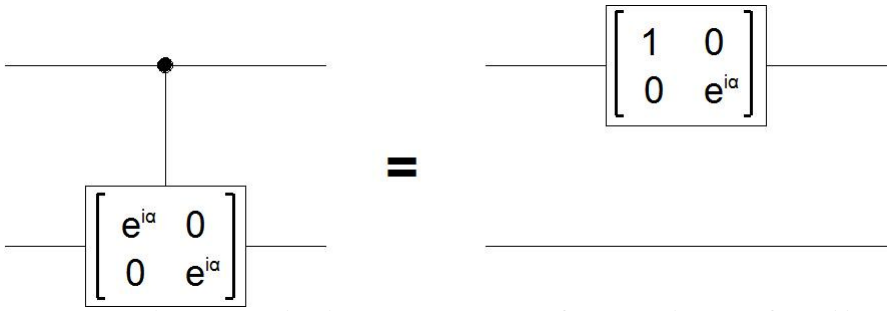
Ο στόχος μας είναι να υλοποιήσουμε τις ελεγχόμενες αυτές διαδικασίες για οποιαδήποτε πύλη ενός qubit U χρησιμοποιώντας μόνο πύλες ενός qubit και την πύλη

CNOT. Θα χρησιμοποιήσουμε μια διαδικασία δύο σταδίων η οποία βασίζεται στην αποσύνθεση $\boldsymbol{U = e^{i\alpha} AXBXC}$.

Το πρώτο στάδιο είναι να εφαρμόσουμε την αλλαγή φάσης $\boldsymbol{e^{i\alpha}}$ στο qubit στόχου ελεγχόμενη από το qubit ελέγχου. Δηλαδή, αν το qubit ελέγχου είναι $|\mathbf{0}\rangle$ τότε το qubit στόχου δεν αλλάζει, ενώ αν είναι $|\mathbf{1}\rangle$ μια αλλαγή φάσης $\boldsymbol{e^{i\alpha}}$ εφαρμόζεται στον στόχο. Ένα κύκλωμα το οποίο εκτελεί αυτή τη διαδικασία και χρησιμοποιεί μόνο μία πύλη μιας εισόδου φαίνεται στο δεξί μέρος της παρακάτω εικόνας. Για να επιβεβαιώσουμε ότι το κύκλωμα δουλεύει σωστά σημειώνω παρακάτω τα αποτελέσματα του δεξιού κυκλώματος στις διάφορες δυνατές καταστάσεις.

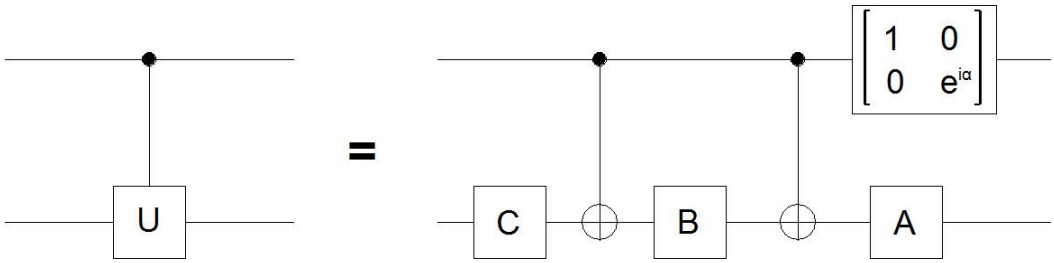
$$|\mathbf{00}\rangle \rightarrow |\mathbf{00}\rangle,\ |\mathbf{01}\rangle \rightarrow |\mathbf{01}\rangle,\ |\mathbf{10}\rangle \rightarrow \boldsymbol{e^{i\alpha}}|\mathbf{10}\rangle,\ |\mathbf{11}\rangle \rightarrow \boldsymbol{e^{i\alpha}}|\mathbf{11}\rangle$$

το οποίο είναι ακριβώς ότι κάνει το αριστερό κύκλωμα.



Σχήμα 3.6: Ελεγχόμενη πύλη ολίσθησης φάσης και ισοδύναμο κύκλωμα για δύο qubits

Το δεύτερο στάδιο είναι να ολοκληρώσουμε την κατασκευή της ελεγχόμενης U διαδικασίας με το κύκλωμα στο Σχήμα 3.7. Για να καταλάβουμε γιατί δουλεύει αυτό το κύκλωμα αρκεί να θυμηθούμε ότι σύμφωνα με το θεώρημα $\boldsymbol{ABC = I}$. Επομένως αν το qubit ελέγχου έχει τεθεί τότε ο μετασχηματισμός $\boldsymbol{e^{i\alpha} AXBXC = U}$ εφαρμόζεται στο δεύτερο qubit. Αν το qubit ελέγχου είναι $|\mathbf{0}\rangle$ τότε εφαρμόζεται ο μετασχηματισμός $\boldsymbol{ABC = I}$ δηλαδή καμία αλλαγή. Άρα το κύκλωμα είναι πράγματι ο ελεγχόμενος U μετασχηματισμός.



Σχήμα 3.7: Κύκλωμα υλοποίησης ελεγχόμενου-U μετασχηματισμού για ένα qubit. Για τα $\boldsymbol{U, \alpha, A, B}$ και $\boldsymbol{C}$ ισχύει $\boldsymbol{U = e^{i\alpha} AXBXC}$ και $\boldsymbol{ABC = I}$.

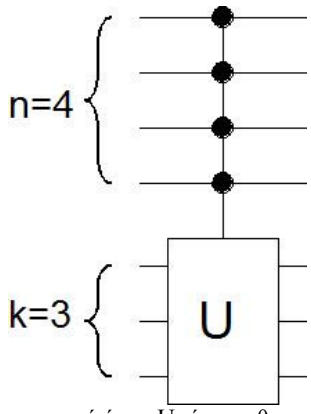
3.4 Ελεγχόμενες από πολλά qubit πύλες μίας εισόδου

Μέχρι εδώ ξέρουμε να κατασκευάζουμε πύλες 1 – qubit ελεγχόμενες από ένα άλλο qubit. Τι γίνεται όμως στην περίπτωση που θέλουμε οι πύλες μας να ελέγχονται από περισσότερα qubits; Ένα τέτοιο παράδειγμα είναι η πύλη Toffoli, η οποία αντιστρέφει το τρίτο qubit, το qubit στόχου, όταν τα δύο πρώτα qubits είναι 1. Γενικότερα ας

υποθέσουμε ότι έχουμε $\boldsymbol{n+k}$ qubits και U είναι ένας k – qubit ορθομοναδιαίος μετασχηματισμός. Τότε ορίζουμε την ελεγχόμενη πύλη $\boldsymbol{C^n(U)}$ με την εξίσωση

$$\boldsymbol{C^n(U)|x_1x_2\dots x_n\rangle|\psi\rangle = |x_1x_2\dots x_n\rangle U^{x_1x_2\dots x_n}|\psi\rangle}$$

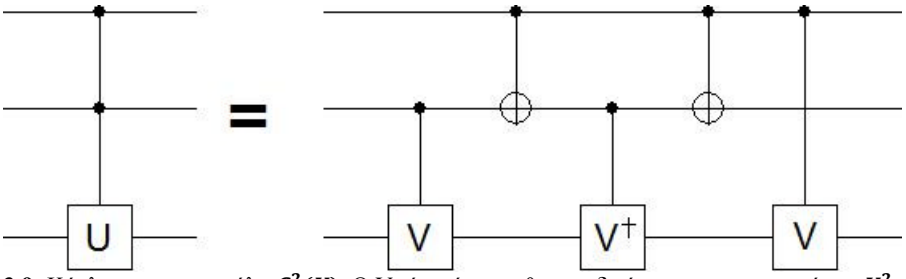
όπου $\boldsymbol{x_1x_2\dots x_n}$ στον εκθέτη του U είναι το γινόμενο των bits $\boldsymbol{x_1, x_2, \dots, x_n}$. Δηλαδή ο μετασχηματισμός U εφαρμόζεται στα τελευταία $\boldsymbol{k}$ qubits εάν τα πρώτα $\boldsymbol{n}$ qubits είναι όλα ίσα με ένα, αλλιώς δεν γίνεται τίποτα. Υπάρχει ειδικός συμβολισμός για τα κυκλώματα αυτών των διαδικασιών, ο οποίος φαίνεται στο παρακάτω σχήμα.



Σχήμα 3.8: Παράδειγμα $\boldsymbol{C^n(U)}$ μετασχηματισμού όπου U είναι ορθομοναδιαίος τελεστής k qubit, με $\boldsymbol{n=4}$ και $\boldsymbol{k=3}$.

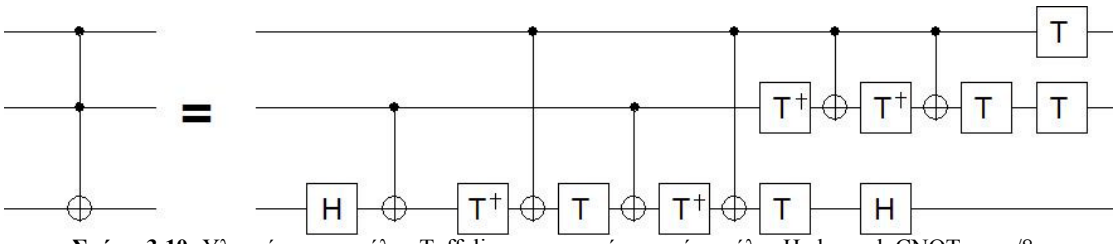
Στην παράγραφο αυτή θα ασχοληθούμε με την περίπτωση που $\boldsymbol{k=1}$ δηλαδή όταν η πύλη U παίρνει μόνο μία είσοδο. Για μεγαλύτερα $\boldsymbol{k}$ θα ασχοληθούμε σε επόμενη παράγραφο.

Αρχικά υποθέτουμε ότι U είναι ένας ορθομοναδιαίος μετασχηματισμός μίας εισόδου και V είναι ένας άλλος ορθομοναδιαίος μετασχηματισμός που τον έχουμε διαλέξει ώστε να ισχύει ότι $\boldsymbol{V^2 = U}$. Τότε η διεργασία $\boldsymbol{C^2(U)}$ υλοποιείται με το ακόλουθο κύκλωμα.



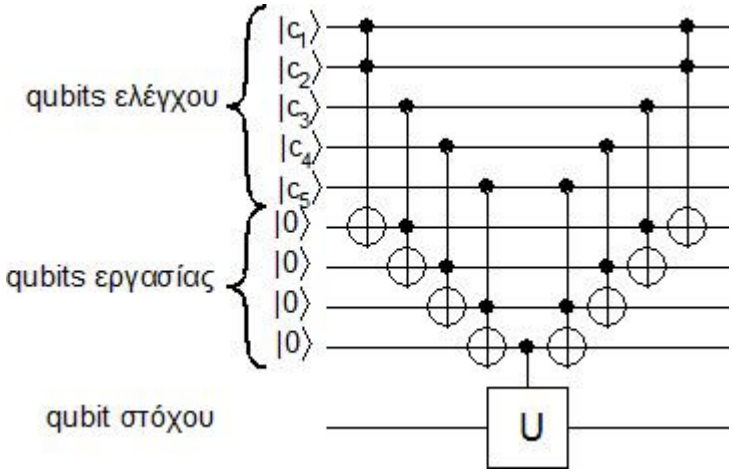
Σχήμα 3.9: Κύκλωμα για την πύλη $\boldsymbol{C^2(U)}$. Ο V είναι ένας ορθομοναδιαίος μετασχηματισμός με $\boldsymbol{V^2 = U}$. Η περίπτωση $\boldsymbol{V = \frac{(1-i)(I+iX)}{2}}$ αντιστοιχεί στην πύλη Toffoli.

Όπως είδαμε η πύλη Toffoli αποτελεί ειδική περίπτωση $\boldsymbol{C^2(U)}$ πύλης· η περίπτωση $\boldsymbol{C^2(X)}$. Ορίζοντας $\boldsymbol{V \equiv \frac{(1-i)(I+iX)}{2}}$ και βλέποντας ότι $\boldsymbol{V^2 = X}$ προκύπτει ότι το κύκλωμα της προηγούμενης εικόνας υλοποιεί την πύλη Toffoli. Καθώς τελικά θα αποδείξουμε ότι κάθε μετασχηματισμός μπορεί να προσεγγιστεί με οποιαδήποτε ακρίβεια από το σύνολο των πυλών Hadamard, CNOT και $\boldsymbol{\pi/8}$, είναι χρήσιμο να δώσουμε το κύκλωμα της πύλης Toffoli που αποτελείται μόνο από αυτές.



Σχήμα 3.10: Υλοποίηση της πύλης Toffoli χρησιμοποιώντας μόνο πύλες Hadamard, CNOT και π/8.

Επομένως μέχρι εδώ μπορούμε να κατασκευάσουμε το κύκλωμα της πύλης Toffoli. Για να προχωρήσουμε στο κύκλωμα $\boldsymbol{C^n(U)}$ με $\boldsymbol{n \geq 2}$ και U οποιοσδήποτε μετασχηματισμός ενός qubit χρησιμοποιούμε το ακόλουθο κύκλωμα.



Σχήμα 3.11: Δίκτυο που υλοποιεί το μετασχηματισμό $\boldsymbol{C^n(U)}$ στην περίπτωση που $\boldsymbol{n = 5}$.

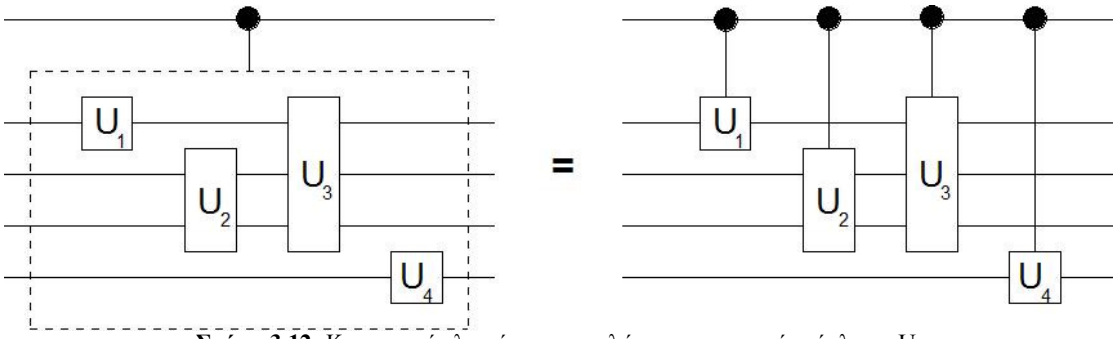
Το κύκλωμα δουλεύει σε τρία στάδια και χρησιμοποιεί ένα μικρό αριθμό $\boldsymbol{(n-1)}$ από qubits εργασίας, τα οποία όλα ξεκινάνε και καταλήγουν στην κατάσταση $\boldsymbol{|0\rangle}$. Υποθέτουμε ότι τα qubits ελέγχου είναι στην κατάσταση βάσης $\boldsymbol{|c_1, c_2, \dots, c_n\rangle}$. Το πρώτο στάδιο του κυκλώματος είναι να πάρει το λογικό ΚΑΙ (αντιστρέψιμο) όλων των qubit ελέγχου και να παράγει το γινόμενο $\boldsymbol{c_1 \cdot c_2 \cdot \dots \cdot c_n}$. Για να γίνει αυτό η πρώτη πύλη στο κύκλωμα πολλαπλασιάζει τα $\boldsymbol{c_1}$ και $\boldsymbol{c_2}$ χρησιμοποιώντας μια πύλη Toffoli αλλάζοντας την κατάσταση του πρώτου qubit εργασίας σε $\boldsymbol{|c_1 \cdot c_2\rangle}$. Η δεύτερη πύλη Toffoli πολλαπλασιάζει το $\boldsymbol{c_3}$ με το γινόμενο $\boldsymbol{c_1 \cdot c_2}$ και αλλάζει την κατάσταση του δεύτερου qubit εργασίας σε $\boldsymbol{|c_1 \cdot c_2 \cdot c_3\rangle}$. Συνεχίζοντας με τον ίδιο τρόπο το τελευταίο qubit εργασίας έχει την κατάσταση $\boldsymbol{|c_1 \cdot c_2 \cdot \dots \cdot c_n\rangle}$. Στο δεύτερο στάδιο ο μετασχηματισμός U εκτελείται στο qubit στόχου ελεγχόμενος από το τελευταίο qubit εργασίας. Δηλαδή ο U εκτελείται αν το γινόμενο όλων των qubit ελέγχου είναι 1· αν όλα έχουν τεθεί. Στο τελικό στάδιο απλώς το κύκλωμα αντιστρέφει τις διεργασίες του πρώτου σταδίου επιστρέφοντας όλα τα qubits ελέγχου στην κατάσταση $\boldsymbol{|0\rangle}$ και αφαιρώντας οποιαδήποτε φαινόμενα συμπλοκής μπορεί να είχαν δημιουργηθεί με αυτά. Συμπερασματικά το συνολικό αποτέλεσμα του κυκλώματος είναι να εφαρμόζεται ο μετασχηματισμός U στο qubit στόχου μόνο και μόνο αν όλα τα qubits ελέγχου έχουν τεθεί.

3.5 Πλήρη σύνολα κβαντικών πυλών

Μέχρι στιγμής οι μετασχηματισμοί που μπορούμε να ελέγξουμε δρουν πάνω σε ένα μόνο qubit. Όμως στη γενική περίπτωση ένας ενδιαφέρον κβαντικός αλγόριθμος

περιλαμβάνει μη τετριμμένους μετασχηματισμούς σε n qubits. Στους κλασικούς υπολογισμούς υλοποιούμε περίπλοκες διεργασίες ως μια ακολουθία πολύ απλούστερων ενεργειών. Πρακτικά θέλουμε να μπορούμε να διαλέξουμε τις κατάλληλες απλές ενέργειες από ένα σύνολο στοιχειωδών πυλών. Στους κβαντικούς υπολογισμούς θέλουμε να κάνουμε το ίδιο. Ο στόχος είναι να διαλέξουμε ένα πεπερασμένο σύνολο από πύλες έτσι ώστε, κατασκευάζοντας κυκλώματα με πύλες μόνο από αυτό το σύνολο, να μπορούμε να υλοποιήσουμε μη τετριμμένους και ενδιαφέροντες αλγόριθμος.

Στην περίπτωση μας αν καταφέρουμε το σύνολο να αποτελείται μόνο από πύλες μιας εισόδου και από πύλες τις οποίες μπορούμε να ελέγξουμε τότε θα μπορούμε να ελέγξουμε οποιονδήποτε μετασχηματισμό U οσονδήποτε εισόδων σύμφωνα με τις προηγούμενες παραγράφους. Αυτό γίνεται με την ακόλουθη κατασκευή, δηλαδή αναλύοντας την πύλη U σε απλούστερες πύλες και ελέγχοντας αυτές.



Σχήμα 3.12: Κατασκευή ελεγχόμενου κυκλώματος για τυχαίο κύκλωμα U

Όταν χρησιμοποιούμε ένα κύκλωμα από κβαντικές πύλες για να υλοποιήσουμε κάποιον επιθυμητό ορθομοναδιαίο μετασχηματισμό, πρακτικά επαρκεί να έχουμε μια υλοποίηση η οποία προσεγγίζει την επιθυμητή με κάποια συγκεκριμένη ακρίβεια. Φυσικά χρειάζεται να ποσοτικοποιήσουμε την ακρίβεια της προσέγγισης ενός ορθομοναδιαίου μετασχηματισμού. Έστω ότι προσεγγίζουμε τον επιθυμητό μετασχηματισμό U με κάποιον άλλο μετασχηματισμό V. Το σφάλμα της προσέγγισης ορίζεται ως

$$\boldsymbol{E(U,V) \equiv \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|}$$

Όταν λέμε ότι ο μετασχηματισμός U μπορεί να προσεγγιστεί με οποιαδήποτε ακρίβεια εννοούμε ότι αν μας δοθεί μια οποιαδήποτε ανοχή λάθους $\boldsymbol{\varepsilon > 0}$, τότε μπορούμε να υλοποιήσουμε έναν ορθομοναδιαίο μετασχηματισμό V τέτοιο ώστε $\boldsymbol{E(U,V) < \varepsilon}$.

Ορισμός 3.5.1 *Ένα σύνολο από πύλες ονομάζεται πλήρες εάν για κάθε ακέραιο* $\boldsymbol{n \geq 1}$*, κάθε n-qubit ορθομοναδιαίος μετασχηματισμός μπορεί να προσεγγιστεί με οποιαδήποτε ακρίβεια από ένα κβαντικό κύκλωμα που αποτελείται από πύλες μόνο από αυτό το σύνολο.*

Το να βρούμε κατάλληλο πλήρες σύνολο από πύλες έχει μεγάλη πρακτική σημασία όπως και θεωρητικό ενδιαφέρον. Αφού ένα πλήρες σύνολο πρέπει να μπορεί να υλοποιεί, για παράδειγμα, την πύλη CNOT, πρέπει να περιέχει τουλάχιστον μία μη τετριμμένη πύλη σε δύο ή περισσότερα qubits.

Ορισμός 3.5.2 *Μία 2-qubit πύλη λέμε ότι είναι πύλη συμπλοκής αν για κάποια κατάσταση εισόδου τύπου γινομένου* $\boldsymbol{|\psi\rangle|\varphi\rangle}$ *η έξοδος της πύλης δεν είναι τύπου γινομένου (δηλαδή τα qubits εξόδου είναι συζευγμένα).*

Το ακόλουθο θεώρημα πληρότητας είναι ένα πολύ χρήσιμο αρχικό σημείο.

Θεώρημα 3.5.3 *Ένα σύνολο αποτελούμενο από οποιαδήποτε 2-qubit πύλη συμπλοκής, μαζί με όλες τις πύλες 1-qubit, είναι πλήρες.*

Το παραπάνω θεώρημα υπονοεί, για παράδειγμα, ότι η πύλη CNOT μαζί με όλες τις πύλες μίας εισόδου αποτελούν πλήρες σύνολο. Μάλιστα το θεώρημα δίνει σύνολα τα οποία είναι ισχυρότερα από αυτά που απαιτεί ο ορισμός 3.5.1. Με μια πύλη συμπλοκής και όλες τις πύλες μίας εισόδου μπορούμε να υλοποιήσουμε κάθε ορθομοναδιαίο μετασχηματισμό n εισόδων *ακριβώς*. Το πρόβλημα με αυτό το σύνολο είναι ότι περιέχει άπειρα στοιχεία. Είναι πιο χρήσιμο να βρούμε ένα πεπερασμένο σύνολο πυλών που να είναι πλήρες. Μια προφανής κατεύθυνση είναι να ψάξουμε να βρούμε ένα πεπερασμένο σύνολο από 1-qubit πύλες που να προσεγγίζει οποιαδήποτε 1-qubit πύλη με οποιαδήποτε ακρίβεια.

Ορισμός 3.5.4 *Ένα σύνολο από πύλες είναι πλήρες για τις 1-qubit πύλες εάν οποιαδήποτε 1-qubit ορθομοναδιαία πύλη μπορεί να προσεγγιστεί με οποιαδήποτε ακρίβεια από ένα κβαντικό κύκλωμα που αποτελείται μόνο από πύλες από αυτό το σύνολο.*

Έχουμε δει ότι οποιοσδήποτε μετασχηματισμός μιας εισόδου γράφεται ως γινόμενο τριών μετασχηματισμών περιστροφής γύρω από οποιουσδήποτε δύο μη παράλληλους άξονες της σφαίρα Bloch (ο συνολικός παράγοντας φάσης δεν μας ενδιαφέρει εδώ αφού αν παραληφθεί προκύπτει ισοδύναμος μετασχηματισμός). Επομένως για οποιουσδήποτε δύο μη παράλληλους άξονες $\boldsymbol{l}$ και $\boldsymbol{m}$ το σύνολο που αποτελείται από τους μετασχηματισμούς περιστροφής $\boldsymbol{R_l(\beta)}$ και $\boldsymbol{R_m(\gamma)}$ για όλα τα $\boldsymbol{\beta, \gamma} \in \boldsymbol{[0, 2\pi)}$ είναι πλήρες για τις 1-qubit πύλες. Από αυτό προκύπτει το ακόλουθο θεώρημα.

Θεώρημα 3.5.5 *Εάν ένα σύνολο από δύο 1-qubit πύλες (περιστροφής)* $\boldsymbol{\mathcal{G} = \{R_l(\beta), R_m(\gamma)\}}$ *ικανοποιεί τις ιδιότητες:*
(i) l και m είναι μη παράλληλοι άξονες της σφαίρας Bloch και
(ii) $\boldsymbol{\beta, \gamma} \in \boldsymbol{[0, 2\pi)}$ *είναι πραγματικοί αριθμοί τέτοιοι ώστε* $\frac{\boldsymbol{\beta}}{\boldsymbol{\pi}}$ *και* $\frac{\boldsymbol{\gamma}}{\boldsymbol{\pi}}$ *να είναι άρρητοι*
τότε το $\boldsymbol{\mathcal{G}}$ *είναι πλήρες για τις 1-qubit πύλες.*

Η απόδειξη στηρίζεται στο γεγονός ότι εφαρμόζοντας αρκετές φορές την κάθε περιστροφή θα καταλήξουμε σε ένα σημείο της σφαίρας Bloch το οποίο θα είναι οσοδήποτε κοντά στην ζητούμενη περιστροφή. Για αυτό το λόγο απαιτείται οι γωνίες περιστροφής να μην είναι ρητά πολλαπλάσια του π ώστε ποτέ να μην επιστρέφουμε στις ίδιες γωνίες.

Συνεχίζοντας θα δώσουμε ένα παράδειγμα συνόλου που ικανοποιεί τις υποθέσεις του θεωρήματος 3.5.5. Υπενθυμίζουμε τις πύλες που θα χρησιμοποιήσουμε, οι οποίες είναι η πύλη Hadamard και πύλη $\boldsymbol{\pi/8}$.

Η πύλη Hadamard ορίζεται από τη δράση της στην βάση του διανυσματικού χώρου:

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

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

και άρα έχει πίνακα $\boldsymbol{H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}}$.
Η άλλη πολύ χρήσιμη πύλη είναι η $\boldsymbol{\pi/8}$ πύλη, T, η οποία δρα ως εξής:

$$\boldsymbol{T|0\rangle = |0\rangle}$$
$$\boldsymbol{T|1\rangle = e^{i\frac{\pi}{4}}|1\rangle}$$

με πίνακα $\boldsymbol{T} = \begin{bmatrix} \boldsymbol{1} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{e^{i\frac{\pi}{4}}} \end{bmatrix}$. Το όνομα της πύλης προκύπτει από το γεγονός ότι είναι ισοδύναμη με την $\begin{bmatrix} \boldsymbol{e^{-i\frac{\pi}{8}}} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{e^{i\frac{\pi}{8}}} \end{bmatrix}$ δηλαδή εκτελεί περιστροφή $\frac{\pi}{4}$ γύρω από τον άξονα z της σφαίρας Bloch.

Λήμμα 3.5.6 *Το σύνολο* $\boldsymbol{G = \{HTHT, THTH\}}$ *ικανοποιεί τις υποθέσεις του θεωρήματος 3.5.5.*

Από το παραπάνω λήμμα προκύπτει άμεσα ότι το σύνολο $\{\boldsymbol{H, T}\}$ είναι πλήρες για τις 1-qubit πύλες και άρα έχουμε ότι:

Θεώρημα 3.5.7 *Το σύνολο* $\{\boldsymbol{CNOT, H, T}\}$ *είναι πλήρες σύνολο πυλών.*

Επομένως μόνο με αυτές τις τρεις πύλες μπορούμε να κατασκευάσουμε οποιονδήποτε μετασχηματισμό n εισόδων και έπειτα με την κατασκευή που προτείναμε στην αρχή της παραγράφου μπορούμε να κατασκευάσουμε το ελεγχόμενο κύκλωμά του με όσα qubit ελέγχου θέλουμε. Αυτό είναι δυνατόν αφού και τις τρεις πύλες μπορούμε να τις ελέγξουμε με ένα qubit (η ελεγχόμενη πύλη CNOT είναι η πύλη Toffoli που ήδη την έχουμε κατασκευάσει από αυτές τις πύλες).

3.6 Αποδοτικότητα προσέγγισης ορθομοναδιαίων μετασχηματισμών

Μέχρι στιγμής δεν έχουμε αναφέρει πόσο γρήγορα μπορεί να γίνει η προσέγγιση ενός οποιοδήποτε ορθομοναδιαίου μετασχηματισμού από τις κατασκευές που αναφέραμε. Εάν επιθυμούμε να υλοποιήσουμε ένα δοσμένο μετασχηματισμό U (ο οποίος αντιστοιχεί σε κάποιο υπολογισμό), θέλουμε να μπορούμε να το κάνουμε αυτό χρησιμοποιώντας πολυωνυμικό αριθμό πυλών από το πλήρες σύνολο που διαθέτουμε. Εδώ το «πολυωνυμικός» σημαίνει «πολυωνυμικός ως προς $\frac{1}{\epsilon}$ και ως προς τον αριθμό $\boldsymbol{n}$ των qubit», όπου $\boldsymbol{\epsilon}$ είναι η ποιότητα προσέγγισης του U.

Ουσιαστικά οι περισσότεροι ορθομοναδιαίοι μετασχηματισμοί δεν είναι δυνατόν να προσεγγιστούν με αποδοτικό τρόπο από το πλήρες σύνολο που δώσαμε. Αυτό μπορεί να αποδειχθεί απαριθμώντας τα στοιχεία των δύο συνόλων (υπάρχουν πολλοί περισσότεροι μετασχηματισμοί από αποδοτικά κυκλώματα).

Η δυσκολία αποδοτικής υλοποίησης των ορθομοναδιαίων μετασχηματισμών δεν βρίσκεται στην πολυπλοκότητα προσομοίωσης τυχαίας πύλης μίας εισόδου από ένα πεπερασμένο σύνολο από πύλες 1-qubit, αφού η αποσύνθεση που προτάθηκε σε πίνακες περιστροφής από το θεώρημα 3.5.5 μπορεί να γίνει σε χρόνο πολυωνυμικό ως προς $\frac{1}{\epsilon}$ υποθέτοντας ότι μπορούμε να υπολογίσουμε n-bit προσεγγίσεις όλων των συντελεστών των πυλών σε πολυωνυμικό χρόνο ως προς n. Μάλιστα ένα αποτέλεσμα συλλογισμών γνωστό ως *Θεώρημα Soloway-Kitaev* είναι ότι μπορούμε να πετύχουμε πολύ καλύτερη απόδοση και να βρούμε ένα σύνολο $\boldsymbol{G}$ από πύλες 1-qubit τέτοιο ώστε οποιαδήποτε πύλη 1-qubit να μπορεί να προσεγγιστεί με οποιαδήποτε ακρίβεια χρησιμοποιώντας μια ακολουθία πολύ-λογαριθμικού πλήθους πυλών από το $\boldsymbol{G}$. Με άλλα λόγια αν θέλουμε να προσεγγίσουμε ένα δοσμένο μετασχηματισμό με σφάλμα

μικρότερο από ϵ μπορούμε να το κάνουμε με αριθμό πυλών που είναι πολυωνυμικός ως προς $\log\left(\frac{1}{\epsilon}\right)$.

Αξίζει να αναφερθούμε σε ορισμένες από τις συνέπειες του θεωρήματος Solovay-Kitaev. Ας υποθέσουμε ότι μας έχει δοθεί ένα κβαντικό κύκλωμα το οποίο αποτελείται από ορισμένες πύλες CNOT και m 1-qubit πύλες και θέλουμε να προσεγγίσουμε αυτό το κύκλωμα χρησιμοποιώντας πύλες μόνο από το πλήρες σύνολο $\{\boldsymbol{CNOT}\} \cup \boldsymbol{\mathcal{G}}$. Αν προσεγγίσουμε την κάθε 1-qubit πύλη με σφάλμα το πολύ $\frac{\epsilon}{m}$ τότε το συνολικό σφάλμα προσέγγισης του κυκλώματος θα είναι φραγμένο από ϵ. Άρα αν επιθυμούμε να προσεγγίσουμε το κύκλωμα με πύλες από το σύνολο $\{\boldsymbol{CNOT}\} \cup \boldsymbol{\mathcal{G}}$ και το συνολικό σφάλμα να είναι μικρότερο από ϵ, πρέπει να στοχεύσουμε να προσεγγίσουμε κάθε πύλη του κυκλώματος με σφάλμα μικρότερο από $\frac{\epsilon}{m}$. Μια ειδική μορφή του θεωρήματος Solovay-Kitaev απαντάει στο ερώτημα του πόσο αποδοτικά μπορεί να γίνει αυτό.

Θεώρημα 3.6.1 *(Solovay-Kitaev) Εάν $\boldsymbol{\mathcal{G}}$ είναι ένα πεπερασμένο σύνολο από 1-qubit πύλες οι οποίες ικανοποιούν τις υποθέσεις του θεωρήματος 3.7.2 και επίσης*
(iii) για κάθε πύλη $\boldsymbol{g} \in \boldsymbol{\mathcal{G}}$ η αντίστροφή της $\boldsymbol{g^{-1}}$ μπορεί να υλοποιηθεί ακριβώς με μια πεπερασμένη ακολουθία πυλών του $\boldsymbol{\mathcal{G}}$,
τότε κάθε 1-qubit πύλη μπορεί να προσεγγιστεί με σφάλμα το πολύ $\boldsymbol{\epsilon}$ χρησιμοποιώντας $\boldsymbol{O\left(\log^{c}\left(\frac{1}{\epsilon}\right)\right)}$ πύλες από το $\boldsymbol{\mathcal{G}}$, όπου $\boldsymbol{c}$ είναι μια θετική σταθερά (περίπου ίση με 2).

Επομένως σύμφωνα με το θεώρημα Solovay-Kitaev κάθε πύλη 1-qubit μπορεί να προσεγγιστεί με σφάλμα το πολύ $\frac{\epsilon}{m}$ χρησιμοποιώντας $\boldsymbol{O\left(\log^{c}\left(\frac{m}{\epsilon}\right)\right)}$ πύλες από το πεπερασμένο σύνολο $\boldsymbol{\mathcal{G}}$, το οποίο είναι πλήρες για τις 1-qubit πύλες και περιέχει τις αντίστροφες των πυλών του (ή οι αντίστροφες μπορούν να κατασκευαστούν ακριβώς από ένα πεπερασμένο αριθμό πυλών του συνόλου). Πρέπει να επισημάνουμε ότι αν είναι δυνατόν να υπολογιστούν n-bit προσεγγίσεις των συντελεστών των πυλών του $\boldsymbol{\mathcal{G}}$ σε πολυωνυμικό χρόνο ως προς n, τότε οι αποδοτικές υλοποιήσεις μπορούν να βρεθούν σε χρόνο πολυωνυμικό ως προς $\log\left(\frac{1}{\epsilon}\right)$.

Το σύνολο $\{\boldsymbol{H}, \boldsymbol{T}\}$ ικανοποιεί τις προϋποθέσεις του θεωρήματος. Άρα για ένα κύκλωμα που έχει m πύλες μίας εισόδου, η προσέγγιση του απαιτεί το πολύ

$$\boldsymbol{O\left(m\log^{c}\left(\frac{m}{\epsilon}\right)\right)}$$

πύλες από το πλήρες σύνολο. Αυτή είναι μια πολυλογαριθμική αύξηση ως προς το μέγεθος του αρχικού κυκλώματος, και το πιο πιθανό αποδεκτή για σχεδόν όλες τις εφαρμογές.

3.7 Υλοποίηση κυκλωμάτων σε Haskell

Σε αυτή την παράγραφο θα παρουσιάσουμε συνοπτικά τον τύπο των κυκλωμάτων που χρησιμοποιήσαμε στην υλοποίηση του προγράμματος Haskell το οποίο μεταφράζει τα προγράμματα της γλώσσας nQML σε κυκλώματα. Ο τύπος είναι ο εξής:

```
data Circ = Rot (C,C) (C,C)
          | Wire [Int]
          | Par Circ Circ
          | Seq Circ Circ
          | Cond Circ Circ
          | Unit Matrix
          deriving Eq
```

Το κύκλωμα Rot αποτελεί ένα απλό κύκλωμα περιστροφής μίας εισόδου. Τα περιεχόμενα του πίνακα μετασχηματισμού 2x2 δίνονται από τους τέσσερις μιγαδικούς αριθμούς που ακολουθούν. Αυτοί οι αριθμοί πρέπει να ικανοποιούν συνθήκες ορθογωνιότητας ώστε ο πίνακας να είναι ορθομοναδιαίος. Το κύκλωμα Wire είναι μια αναδιάταξη (permutation) των qubit που παίρνει ως είσοδο. Η λίστα ακεραίων που παίρνει σαν όρισμα καθορίζει τον τρόπο αναδιάταξης των καλωδίων. Για παράδειγμα το κύκλωμα Wire [1,0,2] εναλλάσσει τα δύο πρώτα qubit και αφήνει το τρίτο ανέπαφο. Φυσικά και αυτή η λίστα πρέπει να ικανοποιεί κάποιους περιορισμούς για να αποτελεί έγκυρη αναδιάταξη. Τα κυκλώματα Par, Seq και Cond δηλώνουν την παράλληλη, σειριακή και υπό συνθήκη σύνθεση δύο κυκλωμάτων. Στην παράγραφο 6.3 θα δούμε με περισσότερες λεπτομέρειες αυτές τις λειτουργίες. Όπως είδαμε παραπάνω τα πέντε πρώτα κυκλώματα αποτελούν ένα πλήρες σύνολο πυλών (και μάλιστα μπορούν να υλοποιήσουν οποιοδήποτε κύκλωμα ακριβώς). Όμως καθώς υπάρχει μια εντολή της nQML που χρησιμοποιεί τυχαίους ορθομοναδιαίους πίνακες αυθαίρετου αριθμού εισόδων, χρησιμοποιούμε το τελευταίο είδος κυκλώματος που παίρνει σαν όρισμα έναν τέτοιο πίνακα. Φυσικά αυτό μπορεί μόνο του να υλοποιήσει οποιαδήποτε κβαντική λειτουργία οσονδήποτε εισόδων.

Μερικές συναρτήσεις που χειρίζονται αυτά τα κυκλώματα είναι οι εξής:

```
arity :: Circ -> Int
comp :: Circ-> Matrix
rCircuit :: Circ -> Circ
```

Η πρώτη επιστρέφει τον αριθμό εισόδων του κυκλώματος και ελέγχει αν κάποια από τις απαραίτητες συνθήκες στα διάφορα κυκλώματα παραβιάζεται ή όχι. Η επόμενη επιστρέφει τον ορθομοναδιαίο πίνακα του κυκλώματος, ενώ η τελευταία επιστρέφει ένα κύκλωμα ισοδύναμο με αυτό που παίρνει ως όρισμα αλλά απλούστερο. Για παράδειγμα μια αναδιάταξη ακολουθούμενη από μία άλλη αναδιάταξη μπορούν να συγχωνευτούν σε μία μόνο. Αυτή η συνάρτηση είναι πολύ χρήσιμη καθώς τα κυκλώματα που παράγονται από τη γλώσσα γίνονται αρκετά πολύπλοκα και μεγάλα και η βελτιστοποίηση τους είναι απαραίτητη.

4 Γλώσσες κβαντικού προγραμματισμού

4.1 Εισαγωγή

Όπως ανέφερα και στην εισαγωγή μια γλώσσα υψηλού επιπέδου επιτρέπει στον προγραμματιστή να εκφράσει τις σκέψεις του και να εκμεταλλευτεί με καλύτερο τρόπο τις δυνατότητες που του δίνει το υλικό του υπολογιστή. Τα χαρακτηριστικά μιας γλώσσας είναι πολλά, όπως ο πλούτος και η ευκολία εκφραστικότητας. Ιδιαίτερα το δεύτερο παίζει σπουδαίο ρόλο στις γλώσσες κβαντικού υπολογισμού όπου οι έννοιες του μοντέλου υπολογισμού δεν συμβαδίζουν με την κοινή λογική. Δηλαδή η ίδια η γλώσσα θα πρέπει να επιτρέπει στο χρήστη της να μεταφέρει τις σκέψεις του σε αυτή χωρίς δυσκολία και να είναι έτσι δομημένη ώστε να προσφέρει προφανείς λύσεις σε προβλήματα που σε άλλες γλώσσες θεωρούνται δύσκολα.

Στους κλασικούς υπολογιστές η ανάπτυξη των γλωσσών υψηλού επιπέδου έγινε παράλληλα με την ανάπτυξη του υλικού των υπολογιστών και την αξιοποίηση των νέων δυνατοτήτων που αυτό πρόσφερε. Είναι αδύνατον να φανταστούμε την δημιουργία των σύγχρονων λειτουργικών συστημάτων χωρίς την ανάπτυξη των γλωσσών αυτών. Τις ίδιες ανάγκες καλούνται να καλύψουν και οι γλώσσες κβαντικού προγραμματισμού. Όμως αυτές έχουν ένα επιπλέον έργο να επιτελέσουν.

Πολύ πριν την ανάπτυξη γλωσσών υψηλού επιπέδου υπήρχαν αλγόριθμοι για διάφορα λογικά προβλήματα. Για παράδειγμα είχε ανακαλυφθεί ο αλγόριθμος πολλαπλασιασμού ακεραίων ή ο αλγόριθμος εύρεσης μέγιστου κοινού διαιρέτη. Οι γλώσσες υψηλού επιπέδου απλώς τυποποίησαν αυτές τις περιγραφές ώστε να εκτελεστούν αυτοί οι αλγόριθμοι σε υπολογιστή. Αντίθετα στο κβαντικό μοντέλο υπολογισμού υπάρχουν πολλοί λίγοι αλγόριθμοι που κάνουν κάτι ενδιαφέρον και μάλιστα οι διεργασίες που εκτελούν αντιβαίνουν στην κοινή λογική. Είναι πολύ απλούστερο να καταλάβει κάποιος την εντολή «Θέσε την τιμή του τάδε καταχωρητή στην τιμή 2» παρά «Θέσε τον τάδε κβαντικό καταχωρητή σε μια υπέρθεση τιμών 20 και 30 με τους τάδε παράγοντες μίξης». Μάλιστα είναι πολύ δύσκολο να προβλέψεις την συμπεριφορά του κβαντικού καταχωρητή σε μετέπειτα γραμμές προγράμματος.

Ένα στοιχείο που επιδεινώνει την κατάσταση είναι η σπανιότητα ενδιαφερόντων αλγορίθμων. Η εξοικείωση με τον κλασικό προγραμματισμό γίνεται με τη μελέτη πολλών και διαφορετικών αλγορίθμων, κάτι το οποίο δεν είναι δυνατό στην περίπτωση του κβαντικού μοντέλου. Επομένως μια καλή γλώσσα κβαντικού προγραμματισμού θα πρέπει να γεφυρώνει το χάσμα ανάμεσα στο κλασικό και το κβαντικό μοντέλου υπολογισμού και να βοηθάει στην ανάπτυξη χρήσιμων κβαντικών αλγορίθμων.

Παρακάτω παρουσιάζω συνοπτικά δύο γλώσσες, μία από κάθε κατηγορία κβαντικών γλωσσών, όπως αυτές παρουσιάστηκαν στην εισαγωγή.

4.2 QPL – “quantum data, classical control paradigm”

Στο (7) ο Peter Selinger περιγράφει την κβαντική γλώσσα QPL (Quantum Programming Language) η οποία ακολουθεί το μοντέλο κβαντικών δεδομένων και κλασικού ελέγχου. Αυτό σημαίνει ότι η ροή του προγράμματος είναι καθορισμένη σε μία και μόνο κατάσταση ενώ τα qubits μπορούν να βρίσκονται σε υπέρθεση καταστάσεων. Μπορούμε να φανταστούμε μία κλασική μονάδα ελέγχου να ελέγχει την εκτέλεση των κβαντικών εντολών πάνω σε κβαντικά bits. Σημειώνω ότι οι πιο σημαντικοί κβαντικοί

αλγόριθμοι χρειάζονται μόνο αυτόν τον τρόπο ελέγχου και μέχρι στιγμής δεν έχουν αναπτυχθεί κβαντικοί αλγόριθμοι που να απαιτούν υπέρθεση καταστάσεων στη ροή ελέγχου (ενδιαφέροντες αλγόριθμοι).

Ιδιαίτερα χαρακτηριστικά της γλώσσας QPL είναι τα εξής:

- Ξεχωριστή υποστήριξη κλασικών bits.
- Υποστήριξη οποιουδήποτε ορθομοναδιαίου μετασχηματισμού.
- Υποστήριξη loops.
- Υποστήριξη αναδρομικών συναρτήσεων.

Παρακάτω δίνω την σύνταξη της γλώσσας και εξηγώ τη σημασιολογία της.

4.2.1 Σύνταξη

Η γραμματική που παράγει τα προγράμματα της QPL είναι η εξής:

$$\begin{aligned}
&\boldsymbol{P ::= new\ bit\ b \coloneqq 0 \mid new\ qbit\ q \coloneqq 0 \mid discard\ x}\\
&\quad \boldsymbol{\mid b \coloneqq 0 \mid b \coloneqq 1 \mid q_1, q_2, \dots, q_n *= S}\\
&\quad \boldsymbol{\mid skip \mid P; Q}\\
&\quad \boldsymbol{\mid if\ b\ then\ P\ else\ Q \mid measure\ q\ then\ P\ else\ Q \mid while\ b\ do\ P}\\
&\quad \boldsymbol{\mid proc\ X[\Gamma \to \Gamma'] \{P\}\ in\ Q \mid y_1, y_2, \dots, y_m = X(x_1, x_2, \dots, x_n)}
\end{aligned}$$

4.2.2 Σημασιολογία

Η σημασιολογία κάθε προγράμματος δίνεται σαν μία συνάρτηση $\boldsymbol{D_n^a \to D_m^b}$ όπου τα n και m είναι ο αριθμός των qubits εισόδου και εξόδου αντίστοιχα ενώ τα a, b ο αριθμός των κλασικών bits εισόδου και εξόδου. Δηλαδή κάθε πρόγραμμα αντιστοιχίζει διανύσματα από πίνακες πυκνότητας σε διανύσματα από πίνακες πυκνότητας.

Οι εντολές new bit και new qbit δημιουργούν μια νέα μεταβλητή τύπου bit ή qbit αντίστοιχα με αρχική τιμή 0. Η εντολή discard καταστρέφει την μεταβλητή και στην περίπτωση που αυτή είναι τύπου qbit εκτελεί την μέτρηση του πρώτα και μετά «ξεχνάει» το αποτέλεσμα. Ο λόγος που γίνεται πρώτα η μέτρηση είναι ότι το qbit αυτό μπορεί να ήταν σε μία κατάσταση συζευγμένη με ένα άλλο και σε περίπτωση που δεν το μετρούσαμε δεν θα ξέραμε αν γινόταν κάποια μέτρηση μετέπειτα και άρα δεν θα μπορούσαμε να δώσουμε την σωστή σημασιολογία.

Η επόμενη εντολή που χρειάζεται σχολιασμό είναι η $\boldsymbol{q_1, q_2, \dots, q_n *= S}$ με την οποία εφαρμόζεται ο ορθομοναδιαίος μετασχηματισμός S στα qubits q_1 έως q_n. Ο πίνακας του S είναι μεγέθους $2^n \times 2^n$. Στην περίπτωση που τα qubits δεν είναι με τη σωστή σειρά τότε πρέπει να εφαρμοστεί μια αλλαγή βάσης με την ίδια εντολή να εφαρμοστεί ο S και μετά η αντίστροφη αλλαγή βάσης. Αν οι τελεστέοι είναι λιγότεροι από το πλήθος των qubits που αποτελούν το state ο S πρέπει να αντικατασταθεί από το κατάλληλο τανυστικό γινόμενο του με τους μοναδιαίους.

Πίνακας 4.1: Σημασιολογία QPL κβαντικό μέρος

Όρος	Πεδίο ορισμού	Συνάρτηση
$\boldsymbol{new\ qbit}$	$\boldsymbol{D_n \to D_{2n}}$	$\boldsymbol{A \to \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}}$
$\boldsymbol{discard}$	$\boldsymbol{D_n \to D_{n/2},\ \ n > 1}$	$\boldsymbol{\begin{pmatrix} A & B \\ C & D \end{pmatrix} \to A + D}$
$\boldsymbol{q_1, q_2, \dots, q_n *= S}$	$\boldsymbol{D_{2^n} \to D_{2^n}}$	$\boldsymbol{A \to SAS^*}$
$\boldsymbol{measure\ q\ then\ P\ else\ Q}$	$\boldsymbol{D_n \to D_m}$ με $\boldsymbol{\|P\|, \|Q\|: D_n \to D_m}$	$\boldsymbol{\begin{pmatrix} A & B \\ C & D \end{pmatrix} \to \|P\|\left(\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}\right) + \|Q\|\left(\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right)}$
$\boldsymbol{skip}$	$\boldsymbol{D_n \to D_n}$	$\boldsymbol{A \to A}$
$\boldsymbol{proc\ X: \Gamma \to \Gamma'\ \{P\}\ in\ Q}$	Ίδιο με της $\boldsymbol{\|Q\|}$	$\boldsymbol{\|Q\|}$ με $\boldsymbol{\|call\ X\| := \|P\|}$
$\boldsymbol{y_1, y_2, \dots, y_m = X(x_1, x_2, \dots, x_n)}$	$\boldsymbol{D_{2^n} \to D_{2^m}}$	Προκύπτει από προηγούμενο proc
$\boldsymbol{P; Q}$	$\boldsymbol{D_n \to D_m}$	$\boldsymbol{\|Q\|(\|P\|)}$ με $\boldsymbol{\|Q\|: D_k \to D_m}$ και $\boldsymbol{\|P\|: D_n \to D_k}$

Οι εντολές if και while χρησιμοποιούν κλασικά bits και επομένως η λειτουργία τους είναι όπως την γνωρίζουμε από τις κλασικές γλώσσες προγραμματισμού. Η εντολή measure q μετράει ένα qubit και ανάλογα με το αποτέλεσμα εκτελεί το κατάλληλο κομμάτι του προγράμματος.

Οι δύο τελευταίες εντολές αναφέρονται στον ορισμό και την κλήση συναρτήσεων. Ιδιαίτερο ενδιαφέρον παρουσιάζει η χρήση αναδρομικών κλήσεων. Η κλήση μιας μη αναδρομικής συνάρτησης μπορεί να αντικατασταθεί ουσιαστικά από μια μακροεντολή. Στην περίπτωση όμως αναδρομικών κλήσεων ακολουθούμε την εξής διαδικασία: Έστω X η αναδρομική διαδικασία. Τότε θα λέμε X(Y) την διαδικασία που είναι ίδια με την X μόνο που η αναδρομική κλήση έχει αντικατασταθεί με τον όρο Y. Ορίζουμε Y_0 ένα πρόγραμμα που δεν τερματίζει και έχει σημασιολογία $\|Y_0\| = 0$. Επίσης $Y_{i+1}=X(Y_i)$. Τότε η σημασιολογία του προγράμματος X θα είναι το όριο $\lim_{i\to\infty}\|Y_i\|$. Είναι πιθανό το trace του πίνακα που δίνεται σαν είσοδος σε μία αναδρομική συνάρτηση να είναι μεγαλύτερο από αυτό που προκύπτει σαν έξοδος. Η χρήση των αναδρομικών συναρτήσεων είναι το μόνο κομμάτι της γλώσσας που δεν διατηρεί το trace (οι ορθομοναδιαίοι μετασχηματισμοί το διατηρούν, όπως και οι μετρήσεις). Αυτό απεικονίζει το γεγονός ότι μπορούμε να έχουμε προγράμματα τα οποία δεν τερματίζουν ποτέ.

4.2.3 Παραδείγματα QPL

4.2.3.1 Ρίψη κέρματος

Έστω πως το ζητούμενο πρόγραμμα είναι να προσομοιώσουμε την ρίψη ενός κέρματος και ανάλογα με το αποτέλεσμα να εκτελέσουμε ένα συγκεκριμένο κομμάτι του

προγράμματος. Σημειώνουμε ότι στους κλασικούς υπολογιστές κάτι τέτοιο είναι αδύνατον καθώς δεν μπορούμε να πάρουμε αληθινά τυχαίες μεταβλητές. Η τυχαιότητα υλοποιείται με γεννήτριες ψευδοτυχαίων αριθμών. Έστω P και Q οι δύο κλάδοι που θέλουμε να εκτελέσουμε. Τότε το ζητούμενο πρόγραμμα είναι:

$$
\begin{aligned}
&new\ qbit\ q\\
&q *= H\\
&measure\ q\ then\ discard\ q; P\\
&\qquad\qquad else\ discard\ q; Q
\end{aligned}
$$

Έστω πως το παραπάνω πρόγραμμα δέχεται σαν είσοδο τον πίνακα πυκνότητας A. Τότε εφαρμόζοντας τους κανόνες της σημασιολογίας η εκχώρηση νέου qubit θα μας δώσει τον πίνακα $\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$. Έπειτα η εφαρμογή του μετασχηματισμού Hadamard, ο οποίος δημιουργεί τη ζητούμενη υπέρθεση στο νέο qubit, ισοδυναμεί με εφαρμογή του μετασχηματισμού $H \otimes I = \frac{1}{\sqrt{2}}\begin{pmatrix} I & I \\ I & -I \end{pmatrix}$ σε ολόκληρο το state. Σύμφωνα με την παράγραφο 2.8 η νέα κατάσταση θα έχει πίνακα πυκνότητας

$$\frac{1}{\sqrt{2}}\begin{pmatrix} I & I \\ I & -I \end{pmatrix}\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}\left(\frac{1}{\sqrt{2}}\begin{pmatrix} I & I \\ I & -I \end{pmatrix}\right)^{\dagger} = \frac{1}{2}\begin{pmatrix} A & A \\ A & A \end{pmatrix}$$

Η μέτρηση δίνει στον ένα κλάδο τον πίνακα $\frac{1}{2}\begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$ και στον άλλο $\frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & A \end{pmatrix}$. Η απόρριψη του qubit q δίνει ως αποτέλεσμα $\frac{1}{2}A$ και στους δύο κλάδους. Αυτός ο πίνακας δίνεται σαν είσοδος σε καθένα από τα προγράμματα P και Q και άρα το τελικό αποτέλεσμα του προγράμματος είναι $P\left(\frac{1}{2}A\right) + Q\left(\frac{1}{2}A\right) = \frac{1}{2}(P(A) + Q(A))$. Το τελευταίο προκύπτει από τη γραμμικότητα της σημασιολογίας της γλώσσας QPL και άρα το πρόγραμμα εκτελεί πράγματι μία από τις δύο υπορουτίνες στην είσοδο του με πιθανότητα $1/2$.

4.2.3.2 Ρίψη κέρματος ταυτόσημη με μέτρηση

Συνεχίζοντας στο ίδιο παράδειγμα θέτουμε $Q \coloneqq skip$ και $P \coloneqq q_0 *= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Αν η αρχική είσοδος του προγράμματος είναι ο πίνακας $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ τότε σύμφωνα με τα παραπάνω το αποτέλεσμα όλου του προγράμματος θα είναι:

$$\frac{1}{2}\left\{P\left(\begin{pmatrix} A & B \\ C & D \end{pmatrix}\right) + Q\left(\begin{pmatrix} A & B \\ C & D \end{pmatrix}\right)\right\} = \frac{1}{2}\left\{\begin{pmatrix} A & -B \\ -C & D \end{pmatrix} + \begin{pmatrix} A & B \\ C & D \end{pmatrix}\right\} = \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}$$

Όμως αυτός είναι ο ίδιος ακριβώς πίνακας πυκνότητας που θα προέκυπτε με μία μέτρηση στο πρώτο qubit του state! Επομένως όσον αφορά τη γλώσσα QPL το αποτέλεσμα των δύο προγραμμάτων είναι εντελώς ταυτόσημο.

Με ένα παράδειγμα όμως βρίσκουμε ότι πρόκειται για δύο διαφορετικές καταστάσεις. Έστω ότι η αρχική κατάσταση του προγράμματος αποτελείτο μόνο από ένα qubit στην κατάσταση $\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle$. Το πρόγραμμα είτε αφήνει την είσοδο ανέπαφη είτε αντιστρέφει τον συντελεστή του $|1\rangle$ (υπορουτίνες Q και P αντίστοιχα) με πιθανότητες $1/2$. Άρα οδηγεί στη μικτή κατάσταση $\frac{1}{2}\left\{\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle\right\} + \frac{1}{2}\left\{\frac{3}{5}|0\rangle - \frac{4}{5}|1\rangle\right\}$. Μία μέτρηση όμως θα το οδηγούσε στη μικτή κατάσταση $\frac{9}{25}\{|0\rangle\} + \frac{16}{25}\{|1\rangle\}$.

Όπως είπαμε οι δύο καταστάσεις έχουν τον ίδιο πίνακα πυκνότητας και δίνουν ίδια αποτελέσματα στις μετρήσεις. Αν όμως στην πρώτη περίπτωση ένας παρατηρητής μάθει το αποτέλεσμα της ρίψης του κέρματος μπορεί εφαρμόζοντας τον κατάλληλο αντίστροφο μετασχηματισμό να ξαναφέρει την κατάσταση του qubit στην αρχική χωρίς να την γνωρίζει εκ των προτέρων. Αντίθετα στη δεύτερη περίπτωση ακόμη και να ξέρει το αποτέλεσμα της μέτρησης δεν μπορεί να συμπεράνει ποιοι ήταν οι συντελεστές της κατάστασης. Αυτή η δυνατότητα που προσφέρει η γνώση κάποιας μέτρησης χρησιμοποιείται στην κβαντική κρυπτογραφία και είναι έξω από τους σκοπούς αυτής της εργασίας.

4.3 QML – "quantum data, quantum control paradigm"

Στο (8) ο Thorsten Altenkirch και ο Jonathan Grattage παρουσιάζουν μια συναρτησιακή γλώσσα κβαντικού προγραμματισμού. Το ιδιαίτερο χαρακτηριστικό της QML (Quantum Meta Language) είναι ότι εισάγει και κβαντικές δομές ελέγχου πέρα από τις κβαντικές δομές δεδομένων. Βασίζεται στην αυστηρή γραμμική λογική επιτηρώντας προσεκτικά τα μέρη που υπονοούν τη διενέργεια μέτρησης. Η λειτουργική σημασιολογία της δίνεται με κβαντικά κυκλώματα.

Η γλώσσα QML αποτελεί ένα πολύ ουσιαστικό βήμα προς την κατεύθυνση της κατασκευής μια πλήρως κβαντικής γλώσσας υψηλού επιπέδου. Προσπαθεί να ενσωματώσει τις βασικές έννοιες του κβαντικού μοντέλου, όπως η υπέρθεση και οι ελεγχόμενοι μετασχηματισμοί, με τέτοιο τρόπο ώστε ο προγραμματιστής να διευκολύνεται στη χρήση τους. Επιχειρεί να διατηρήσει ένα συναρτησιακό στυλ, ελέγχοντας όμως προσεκτικά μέσα από το σύστημα τύπων τα μέρη της γλώσσας που έχουν παρενέργειες (δηλαδή τις μετρήσεις).

4.3.1 Σύνταξη

Η γραμματική των προγραμμάτων της QML είναι η εξής:

$$
\begin{aligned}
&\boldsymbol{t ::= x \mid let\ x = t\ in\ u}\\
&\quad \mid \boldsymbol{x^{\vec{y}}} \mid (\ \ )\\
&\quad \mid \boldsymbol{(t,u)} \mid \boldsymbol{let\ (x,y) = t\ in\ u}\\
&\quad \mid \boldsymbol{qinl\ t} \mid \boldsymbol{qinr\ t}\\
&\quad \mid \boldsymbol{case\ t\ of}\ \{\boldsymbol{qinl\ x \Rightarrow u} \mid \boldsymbol{qinr\ y \Rightarrow u'}\}\\
&\quad \mid \boldsymbol{case^{\circ}\ t\ of}\ \{\boldsymbol{qinl\ x \Rightarrow u} \mid \boldsymbol{qinr\ y \Rightarrow u'}\}\\
&\quad \mid \{(\boldsymbol{\kappa})\boldsymbol{t} \mid (\boldsymbol{\iota})\boldsymbol{u}\}\\
&\quad \mid \boldsymbol{f\ \vec{t}}
\end{aligned}
$$

όπου τα διανύσματα $\vec{\boldsymbol{a}}$ αντιπροσωπεύουν μια ακολουθία από συντακτικά αντικείμενα, δηλαδή $\vec{\boldsymbol{a}} = \boldsymbol{\epsilon} \mid \boldsymbol{a}\vec{\boldsymbol{a}}$.

4.3.2 Ερμηνεία

Η σημασιολογία της QML δίνεται στο (9) με όρους κβαντικών κυκλωμάτων. Σε κάθε όρο αντιστοιχίζεται ένα κβαντικό κύκλωμα το οποίο σχηματίζεται επαγωγικά συνδέοντας κατάλληλα τα κυκλώματα που αντιστοιχούν στους υποόρους του. Η πρωτοτυπία της γλώσσας είναι ότι το σύστημα τύπων ακολουθεί αυστηρώς γραμμική

λογική και ότι χρησιμοποιεί δύο συστήματα τύπων, ένα αυστηρό και ένα γενικό. Όταν κάνει αυστηρό typecheck τα κυκλώματα που παράγονται δεν διεξάγουν μετρήσεις ενώ όταν κάνει γενικό μπορεί να διεξάγουν μετρήσεις και επομένως είναι μη αντιστρέψιμα. Καθώς όμως το σύστημα τύπων είναι γραμμικό οι Grattage και Altenkirch έπρεπε να βρουν ένα τρόπο να μοιράζουν τις μεταβλητές ανάμεσα στα context και επομένως να διπλασιάζουν qubit. Κάτι τέτοιο όπως είδαμε στην παράγραφο 3.3.2 δεν είναι δυνατό στο μοντέλο κβαντικού υπολογισμού και το καλύτερο που μπορούσαν να κάνουν ήταν να χρησιμοποιήσουν το κύκλωμα του σχήματος 3.3.2.χ το οποίο όπως είδαμε παράγει συζευγμένα qubit. Αυτό όμως δημιουργεί παρενέργειες στα προγράμματα της γλώσσας, οι οποίες πρέπει να ελέγχονται προσεκτικά από τον προγραμματιστή. Παρακάτω θα δούμε ένα παράδειγμα παρενεργειών.

Η ουσιαστική συνεισφορά της γλώσσας είναι η δομή $\boldsymbol{case}^{\circ}$ η οποία εκτελεί κβαντική διακλάδωση, δηλαδή είναι δυνατόν να δώσει υπέρθεση προγραμμάτων στην περίπτωση που η έκφραση που λάβει σαν είσοδο βρίσκεται σε υπέρθεση. Η δομή $\boldsymbol{case}$ εκτελεί κλασική διακλάδωση, δηλαδή μετράει το αποτέλεσμα της έκφρασης $\boldsymbol{t}$ και εκτελεί έναν από τους δύο κλάδους ανάλογα με το αποτέλεσμα.

Τέλος αναφέρουμε ότι με βάση τις εντολές που δώσαμε μπορούμε να κατασκευάσουμε άλλες εντολές οι οποίες είναι πιο κοντά στις δομές του κλασικού προγραμματισμού και τις οποίες θα χρησιμοποιήσουμε στα παρακάτω παραδείγματα. Αυτές είναι:

$\boldsymbol{qfalse} = \boldsymbol{qinr}(\ )$

$\boldsymbol{qtrue} = \boldsymbol{qinl}(\ )$

$\boldsymbol{if^{a}\ b\ then\ t\ else\ u} = \boldsymbol{case^{a}\ b\ of}\ \{\boldsymbol{inl\_} \Rightarrow \boldsymbol{t} | \boldsymbol{inr\_} \Rightarrow \boldsymbol{u}\}$ με $\boldsymbol{\alpha} = \circ$ ή κενό

4.3.3 Παραδείγματα

Το πιο απλό παράδειγμα είναι η πύλη NOT:

$$if^{\circ}\ x\ then\ qfalse\ else\ qtrue$$

Με αυτό το πρόγραμμα το x γίνεται η πρώτη είσοδος της πύλης NOT και το αποτέλεσμα είναι συζευγμένο με αυτό.

Άλλο παράδειγμα αποτελεί η πύλη Hadamard:

$$had\ x \equiv if^{\circ}\ x\ then\ \{qfalse | -qtrue\}\ else\ \{qfalse | qtrue\}$$

όπου ο τελεστής { | } δηλώνει υπέρθεση.

Ας δούμε τώρα ένα παράδειγμα όπου το μοίρασμα των μεταβλητών δημιουργεί παρενέργειες στο πρόγραμμα, οι οποίες δεν συμβαδίζουν με το συμβατικό μοντέλο προγραμματισμού.

Προφανώς έχουμε ότι $had\ \{qfalse | qtrue\} = qfalse$. Έστω το πρόγραμμα

$$let\ x = qfalse\ in\ (had\ x, had\ x)$$

Το μοίρασμα των context δημιουργεί δύο ψευδό-αντίγραφα του x και τα εισάγει στα δύο υποπρογράμματα $had\ x$. Αφού το x είναι $qfalse$ και το αντίγραφο του είναι $qfalse$ (θυμηθείτε ότι οι καταστάσεις $|0\rangle$ και $|1\rangle$ μπορούν να αντιγραφούν) και άρα το αποτέλεσμα του προγράμματος είναι το αναμενόμενο, δηλαδή $(\{qfalse | qtrue\}, \{qfalse | qtrue\})$. Έστω τώρα το πρόγραμμα

$$let\ x = \{qfalse|qtrue\}\ in\ (had\ x, had\ x)$$

Λογικά θα περιμέναμε το αποτέλεσμα να είναι $(qfalse, qfalse)$. Όμως εδώ το x βρίσκεται σε υπέρθεση η οποία όπως ξέρουμε δεν αντιγράφεται. Το x έχει κατάσταση $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}$ και με το μοίρασμα του σε δύο παίρνουμε την κατάσταση $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$ (δηλαδή τα δύο qubit είναι συζευγμένα). Εφαρμόζοντας διαδοχικά δύο φορές την πύλη Hadamard στο καθένα, δηλαδή τον πίνακα $(I \otimes H)(H \otimes I) = H \otimes H$, προκύπτει η κατάσταση $\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}$. Δηλαδή το αποτέλεσμα δεν είναι το αναμενόμενο, αφού πήραμε δύο qubit σε υπέρθεση καταστάσεων $\{qfalse|qtrue\}$ τα οποία είναι μάλιστα και συζευγμένα.

Γενικώς μπορούμε να πούμε ότι η τακτική του μοιράσματος μεταβλητών μειώνει αρκετά την αξία του συναρτησιακού μέρους της γλώσσας, διότι ένας όρος που έχει μια δεδομένη συμπεριφορά όταν χειρίζεται μια ανεξάρτητη μεταβλητή αποκτά μία άλλη, διαφορετική συμπεριφορά, όταν η μεταβλητή αυτή χρησιμοποιείται και από έναν άλλο όρο και μάλιστα αυτό εξαρτάται και από τον τρόπο που ο άλλος όρος χειρίζεται το δικό του αντίγραφο. Αυτό αντιπροσωπεύει μια εγγενή αδυναμία του κβαντικού υπολογιστικού μοντέλου, η οποία προκύπτει από το γεγονός ότι είναι αδύνατο να δημιουργήσουμε αντίγραφα ενός qubit. Δεν είναι όμως σαφές κάποιο πλεονέκτημα της λύσης που υλοποιήθηκε στην QML, λαμβάνοντας μάλιστα υπ' όψιν πως ο σχεδιασμός της γλώσσας κάνει μεγάλο κόπο για να απομονώσει τους όρους που έχουν παρενέργειες με μέτρηση. Ίσως θα ήταν πιο συνετό το βάρος της δημιουργίας ψευδό-αντιγράφων μιας μεταβλητής να πέφτει στον προγραμματιστή, όπου αυτό είναι αναγκαίο.

5 nQML

5.1 Εισαγωγή

Στο (10) περιγράφεται η γλώσσα προγραμματισμού με την οποία θα ασχοληθώ στις υπόλοιπες ενότητες της διπλωματικής εργασίας, η nQML, η οποία αποτελεί μετεξέλιξη της QML.

Ο κύριος στόχος στην σχεδίαση της nQML είναι να δώσει στους προγραμματιστές αρκετή εκφραστικότητα ώστε να υλοποιήσουν εύκολα κβαντικούς αλγόριθμους, ενώ ταυτόχρονα τους εμποδίζει να παραβούν τους κανόνες των κβαντικών υπολογισμών. Η nQML είναι μια συναρτησιακή γλώσσα υψηλού επιπέδου που βασίζεται στο μοντέλο «κβαντικά δεδομένα και κβαντικός έλεγχος». Περιλαμβάνει δομές οι οποίες επιτρέπουν κάθε ορθομοναδιαίο μετασχηματισμό να εκφραστεί ως πρόγραμμα με προφανή τρόπο, χρησιμοποιώντας περίπου τον ίδιο συμβολισμό που χρησιμοποιείται από τους σχεδιαστές κβαντικών αλγορίθμων. Επίσης επιτρέπει οι κβαντικές μετρήσεις να διεξάγονται σε οποιοδήποτε σημείο της εκτέλεσης του προγράμματος.

Η σχετική ευκολία χρήσης της γλώσσας έχει το μειονέκτημα ότι προϋποθέτει την παράλειψη αρκετών πρακτικών προβλημάτων, όπως την ύπαρξη ατελούς κβαντικού hardware, την ανάγκη για κβαντική διόρθωση σφαλμάτων και το γεγονός ότι κάθε κβαντικό πρόγραμμα θα πρέπει τελικά να υλοποιηθεί ως ένα κβαντικό κύκλωμα χρησιμοποιώντας μόνο ένα πεπερασμένο σύνολο πυλών και συνεπώς κάποιοι από τους ορθομοναδιαίους μετασχηματισμούς που επιτρέπονται στην nQML θα πρέπει να προσεγγιστούν. Όμως παρόμοια προβλήματα αντιμετώπιζαν οι ιδρυτές του κλασικού μοντέλου προγραμματισμού δεκαετίες πριν. Ευτυχώς έχουν επιλυθεί και οι λύσεις αυτές έχουν φτάσει σε ένα τέτοιο αφηρημένο επίπεδο ώστε οι άνθρωποι που χρησιμοποιούν τις σύγχρονες γλώσσες υψηλού επιπέδου δεν χρειάζεται να ξέρουν κάτι για τις υλοποιήσεις. Πιστεύουμε ότι το ίδιο μπορεί και πρέπει να γίνει για τις κβαντικές γλώσσες προγραμματισμού του μέλλοντος και ότι αυτά τα προβλήματα πρέπει να επιλυθούν όχι από το σχεδιαστή και τους χρήστες των γλωσσών αλλά από τον αρχιτέκτονα του κβαντικού υπολογιστή, το σχεδιαστή του λειτουργικού συστήματος και σε ένα μικρότερο ποσοστό το σχεδιαστή του compiler.

Η nQML έχει ένα απλό σύστημα τύπων και λειτουργική σημασιολογία. Με τον όρο απλός εννοούμε ότι και τα δύο χρησιμοποιούν δομές και τεχνικές οι οποίες είναι της ίδιας μορφής και πολυπλοκότητας με τις αντίστοιχες των κλασικών γλωσσών προγραμματισμού. Επομένως γίνονται εύκολα κατανοητές από τους αναγνώστες με βασικές γνώσεις σημασιολογίας γλωσσών και μια στοιχειώδη εξοικείωση του κβαντικού μοντέλου υπολογισμού. Το βασικότερο πρωτότυπο στοιχείο του συστήματος τύπων της nQML είναι ότι ο τύπος μιας κβαντικής έκφρασης περικλείει πληροφορία που δηλώνει τα συγκεκριμένα qubits της κβαντικής κατάστασης στα οποία είναι αποθηκευμένη η τιμή της έκφρασης. Η επαναχρησιμοποίηση qubit επιτρέπεται με τέτοιο τρόπο ώστε να μην παραβιάζονται οι κανόνες «μη αντιγραφής» και «μη απόρριψης». Οι προγραμματιστές έχουν την εντύπωση ότι ασχολούνται με μία κλασική γλώσσα χωρίς περιορισμούς γραμμικότητας.

Η λειτουργική σημασιολογία της nQML βασίζεται στη χρήση πινάκων πυκνότητας οι οποίοι περιγράφουν κβαντικές καταστάσεις. Ένα ορθό πρόγραμμα της γλώσσας αντιστοιχεί σε μία συνάρτηση από πίνακες πυκνότητας σε πίνακες πυκνότητας και έτσι περιγράφεται η επίδραση του προγράμματος σε μια τυχαία κβαντική κατάσταση. Ορθά προγράμματα τα οποία δεν διενεργούν μετρήσεις αντιστοιχίζονται επίσης σε ένα ορθομοναδιαίο πίνακα ο οποίος περιγράφει τον μετασχηματισμό που διενεργούν στην

κβαντική κατάσταση. Η εκτέλεση ενός προγράμματος nQML μπορεί να προσομοιωθεί με μια ακολουθία βημάτων που επηρεάζουν την κβαντική κατάσταση είτε δηλώνοντας νέα qubits, είτε εφαρμόζοντας ορθομοναδιαίους μετασχηματισμούς σε υπάρχοντα qubits, είτε μετρώντας την τιμή τους.

Σε αυτή τη διπλωματική θα δώσουμε τη σημασιολογία των προγραμμάτων με τη μορφή κβαντικών κυκλωμάτων, κάτι το οποίο θα δώσει καλύτερη κατανόηση των λειτουργιών τους. Ουσιαστικά η ακολουθία βημάτων θα αντιστοιχιστεί σε ακολουθία κυκλωμάτων.

5.2 Η σύνταξη της nQML

Η πλήρης σύνταξη της γλώσσας δίνεται με την ακόλουθη γραμματική. Υποθέτουμε ότι x είναι ένα αναγνωριστικό μεταβλητής και λ μία μιγαδική σταθερά. Η γραμματική ορίζει δύο συντακτικές κλάσεις. Οι κβαντικές εκφράσεις σημειώνονται με e· αντιπροσωπεύουν κβαντικά προγράμματα και η σύνταξη τους είναι παρόμοια με αυτή της QML. Οι κλασικές εκφράσεις σημειώνονται με c· χρησιμοποιούνται μόνο στην δομή κβαντικού μετασχηματισμού $|\boldsymbol{e}\rangle \rightarrow \boldsymbol{x}, \boldsymbol{x}'.\boldsymbol{c}$ και αντιπροσωπεύουν δύο τύπους πληροφορίας: μια δομή κλασικών bit ή ένα μιγαδικό αριθμό.

$$\begin{aligned}
\boldsymbol{e} ::= {} & \boldsymbol{x} \mid \{(\boldsymbol{\lambda})\boldsymbol{qfalse} + (\boldsymbol{\lambda}')\boldsymbol{qtrue}\} \mid \boldsymbol{let}\ \boldsymbol{x} = \boldsymbol{e_1}\ \boldsymbol{in}\ \boldsymbol{e_2} \\
& \mid (\boldsymbol{e_1}, \boldsymbol{e_2}) \mid \boldsymbol{let}\ (\boldsymbol{x_1}, \boldsymbol{x_2}) = \boldsymbol{e_1}\ \boldsymbol{in}\ \boldsymbol{e_2} \\
& \mid \boldsymbol{if\ e\ then\ e_1\ else\ e_2} \mid \boldsymbol{ifm\ e\ then\ e_1\ else\ e_2} \mid |\boldsymbol{e}\rangle \rightarrow \boldsymbol{x}, \boldsymbol{x}'.\boldsymbol{c} \\
\boldsymbol{c} ::= {} & \boldsymbol{x} \mid \boldsymbol{false} \mid \boldsymbol{true} \mid \boldsymbol{\lambda} \mid \boldsymbol{let}\ \boldsymbol{x} = \boldsymbol{c_1}\ \boldsymbol{in}\ \boldsymbol{c_2} \\
& \mid (\boldsymbol{c_1}, \boldsymbol{c_2}) \mid \boldsymbol{let}\ (\boldsymbol{x_1}, \boldsymbol{x_2}) = \boldsymbol{c_1}\ \boldsymbol{in}\ \boldsymbol{c_2} \mid \boldsymbol{if\ c\ then\ c_1\ else\ c_2} \\
& \mid \boldsymbol{int\ c} \mid \boldsymbol{c_1} + \boldsymbol{c_2} \mid \boldsymbol{c_1} - \boldsymbol{c_2} \mid \boldsymbol{c_1} * \boldsymbol{c_2} \mid \boldsymbol{c_1}/\boldsymbol{c_2} \mid \boldsymbol{c_1}^{\boldsymbol{c_2}} \mid \boldsymbol{c_1} = \boldsymbol{c_2} \mid \boldsymbol{c_1} < \boldsymbol{c_2}
\end{aligned}$$

Οι μεταβλητές στην nQML είναι στην ουσία αναφορές σε κβαντικές πληροφορίες οι οποίες είναι αποθηκευμένες σε μία καθολική κβαντική κατάσταση. Υπάρχουν δύο τύποι κβαντικής πληροφορίας: qubits και γινόμενα (products). Ένα νέο qubit διατίθεται στο πρόγραμμα όταν χρησιμοποιείται ο τελεστής υπέρθεσης $\{(\boldsymbol{\lambda})\boldsymbol{qfalse} + (\boldsymbol{\lambda}')\boldsymbol{qtrue}\}$, με τον ίδιο τρόπο που νέα αντικείμενα διατίθενται στο σωρό (heap) όταν ένας data constructor καλείται από μια γλώσσα συναρτησιακού προγραμματισμού. Τα γινόμενα εισάγονται και απαλείφονται με τις δομές $(\boldsymbol{e_1}, \boldsymbol{e_2})$ και $\boldsymbol{let}\ (\boldsymbol{x_1}, \boldsymbol{x_2}) = \boldsymbol{e_1}\ \boldsymbol{in}\ \boldsymbol{e_2}$. Η nQML επίσης εισάγει τρεις δομές ροής ελέγχου:

- $\boldsymbol{ifm\ e\ then\ e_1\ else\ e_2}$: Διεξάγει μία μέτρηση στην έκφραση $\boldsymbol{e}$, η οποία πρέπει να είναι τύπου qubit. Ανάλογα με το αποτέλεσμα εκτελεί έναν από τους δύο κλάδους. Είναι παρόμοια με μία κλασική τυχαία διακλάδωση, που βασίζεται στην ρίψη ενός «μη δίκαιου» νομίσματος με πιθανότητες εί από την κατάσταση του qubit που μετράμε.
- $\boldsymbol{if\ e\ then\ e_1\ else\ e_2}$: Επιτρέπει στους προγραμματιστές να εκτελούν κβαντικές διακλαδώσεις. Εάν η έκφραση $\boldsymbol{e}$, η οποία πρέπει να είναι τύπου qubit, είναι σε κλασική κατάσταση, τότε το αποτέλεσμα της εντολής είναι ίδιο με το αντίστοιχο της ifm. Αλλά αν το $\boldsymbol{e}$ είναι σε κβαντική υπέρθεση, το πρόγραμμα συνεχίζει σε κβαντική υπέρθεση και των δύο κλάδων· πιθανότατα δημιουργώντας συμπλοκή ανάμεσα στα qubits της κβαντικής κατάστασης.
- $|\boldsymbol{e}\rangle \rightarrow \boldsymbol{x}, \boldsymbol{x}'.\boldsymbol{c}$: Πρόκειται για ένα γενικό τρόπο για να εκφράσουμε οποιονδήποτε ορθομοναδιαίο μετασχηματισμό, στον οποίο πρέπει να βασιστούμε όταν ο μετασχηματισμός δεν μπορεί εύκολα να αποσυντεθεί σε μια

ακολουθία ελεγχόμενων διαδικασιών, που μπορούν να εκφραστούν με if. Το πλεονέκτημά του είναι ότι αντί να εξαναγκάζει τους προγραμματιστές να προϋπολογίζουν και να παρέχουν ολόκληρο τον ορθομοναδιαίο πίνακα του μετασχηματισμού, τους επιτρέπει να εκφράσουν αυτό τον πίνακα ως μια μιγαδική συνάρτηση της κατάστασης εισόδου και εξόδου των qubits που πρέπει να μετασχηματιστούν. Αυτή η μορφή οδηγεί σε μια συμπαγή και σαφή έκφραση πολλών χρήσιμων αλγορίθμων, όπως του κβαντικού μετασχηματισμού Fourier.

Σε κβαντική ψευδογλώσσα κάθε ορθομοναδιαίος μετασχηματισμός μπορεί να εκφραστεί στην εξής μορφή:

$$|\boldsymbol{i}\rangle \rightarrow \sum_{\boldsymbol{j=0}}^{\boldsymbol{2^n-1}} \boldsymbol{f(i,j)}|\boldsymbol{j}\rangle$$

όπου f(i,j) είναι μία συνάρτηση της κατάστασης εισόδου i των κβαντικών καταχωρητών και της κατάστασης εξόδου j. Η δομή $|\boldsymbol{e}\rangle \rightarrow \boldsymbol{x, x'. c}$ επιτρέπει στους προγραμματιστές να χρησιμοποιήσουν ακριβώς αυτόν τον φυσικό συμβολισμό: οι κλασικές μεταβλητές x και x' υποδηλώνουν την κατάσταση εισόδου και εξόδου αντίστοιχα και η κλασική έκφραση c υποδηλώνει το σώμα της συνάρτησης.

Με αυτό το συμβολισμό, εάν η συνάρτηση f είναι γνωστή, ο ορθομοναδιαίος πίνακας είναι δυνατόν να κατασκευαστεί εύκολα παίρνοντας $\boldsymbol{S_{i,j} = f(i,j)}$. Φυσικά δεν καταλήγουν όλες οι συναρτήσεις f σε ορθομοναδιαίους πίνακες και το σύστημα τύπων της nQML δεν μπορεί να ελέγξει αν ο προκύπτων μετασχηματισμός είναι πράγματι ορθομοναδιαίος. Το σύστημα τύπων των Altenkirch και Grattage QML μπορεί να το κάνει αυτό, κάνοντας όμως το μέγεθος του προγράμματος εκθετικό και περιπλέκοντας τους τύπους με περιορισμούς ορθογωνιότητας.

5.3 Το σύστημα τύπων της nQML

Υπάρχουν δύο είδη τύπων: κβαντικοί τύποι (τ) και κλασικοί τύποι (φ). Για κάθε κβαντική έκφραση το σύστημα τύπων αποθηκεύει τα συγκεκριμένα qubit της κατάστασης στα οποία είναι αποθηκευμένη η τιμή της έκφρασης. Αυτή η πληροφορία αποθηκεύεται στους τύπους. Χρησιμοποιείται για να διαφυλάξει τον κανόνα ότι το ίδιο qubit δεν μπορεί να χρησιμοποιηθεί δύο φορές σε ένα μετασχηματισμό, και επομένως να επιτρέπει επαναχρησιμοποίηση μεταβλητών χωρίς να παραβαίνει το θεώρημα «μη αντιγραφής».

$\boldsymbol{\tau ::= qbit[n] \mid \tau_1 \otimes \tau_2}$

$\boldsymbol{\varphi ::= bit \mid \varphi_1 \times \varphi_2 \mid complex}$

Για παράδειγμα μια έκφραση έχει τύπο $\boldsymbol{qubit[5]}$ αν η τιμή της έχει αποθηκευθεί στο πέμπτο qubit της κβαντικής κατάστασης.

Για κάθε κβαντικό τύπο τ ορίζουμε $\mathsf{C}(\boldsymbol{\tau})$ να είναι ο αντίστοιχος κλασικός τύπος. Στον κλασικό τύπο complex δεν αντιστοιχεί κανένας κβαντικός τύπος. Γράφουμε $|\mathsf{C}(\boldsymbol{\tau})|$ για να δηλώσουμε το μέγεθος, σε κλασικά bit, του κλασικού τύπου στον οποίο αντιστοιχεί ο τ και $\boldsymbol{qbits(\tau)}$ το σύνολο των qubit της κατάστασης τα οποία χρησιμοποιούνται από τις εκφράσεις τύπου τ. Για παράδειγμα, $\boldsymbol{qbits(qbit[4] \otimes qbit[2]) = \{2, 4\}}$. Ένας

κβαντικός τύπος καλείται αγνός (pure) εάν η αναπαράστασή του χρησιμοποιεί διακεκριμένα qubit. Σημειώστε ότι στη γενική περίπτωση $|\boldsymbol{qbits}(\boldsymbol{\tau})| \leq |\mathbb{C}(\boldsymbol{\tau})|$ με την ισότητα να ισχύει μόνο όταν ο τύπος είναι αγνός. Ένα κβαντικό περιβάλλον τύπων Γ είναι μια αντιστοίχηση μεταβλητών σε κβαντικούς τύπους και όμοια ένα κλασικό περιβάλλον τύπων Δ είναι μια αντιστοίχηση μεταβλητών σε κλασικούς τύπους. Με $\boldsymbol{\Gamma}|_{\boldsymbol{k}}$ συμβολίζουμε το περιβάλλον Γ το οποίο δεν περιέχει μεταβλητές των οποίων οι τύποι χρησιμοποιούν το k-οστό qubit της κβαντικής κατάστασης.

Η σχέση παραγωγής τύπων στην nQML γράφεται ως εξής: $\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\boldsymbol{\alpha}} \boldsymbol{e}: \boldsymbol{\tau}; \boldsymbol{m}$. Όπως και στο σύστημα τύπων της QML υπάρχουν δύο σχέσεις: μία για αγνές κβαντικές καταστάσεις (δηλαδή χωρίς κβαντικές μετρήσεις) που συμβολίζεται $\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\circ} \boldsymbol{e}: \boldsymbol{\tau}; \boldsymbol{m}$ και μία για τη γενική περίπτωση που συμβολίζεται $\boldsymbol{\Gamma}; \boldsymbol{n} \vdash \boldsymbol{e}: \boldsymbol{\tau}; \boldsymbol{m}$. Συμβολίζουμε και τις δύο ταυτόχρονα επιτρέποντας στον εκθέτη $\boldsymbol{\alpha}$ να είναι είτε $\circ$ είτε κενός. Αφού οι τύποι της nQML κρατάνε πληροφορίες που αφορούν τις θέσεις των qubit στην κβαντική κατάσταση του προγράμματος η σχέση τύπων πρέπει να επεξεργάζεται και να διαδίδει αυτές τις πληροφορίες. Στον τύπο $\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\boldsymbol{\alpha}} \boldsymbol{e}: \boldsymbol{\tau}; \boldsymbol{m}$ ο φυσικός αριθμός $\boldsymbol{n}$ στα αριστερά της σχέσης δηλώνει τον αριθμό των qubit της αρχικής κβαντικής κατάστασης, πριν να αρχίσει να υπολογίζεται η έκφραση $\boldsymbol{e}$. Προφανώς για όλα τα ζεύγη $(\boldsymbol{x}: \boldsymbol{\tau_x}) \in \boldsymbol{\Gamma}$ πρέπει να ισχύει ότι $\boldsymbol{qbits}(\boldsymbol{\tau_x}) \subseteq \{\boldsymbol{0}, \dots, \boldsymbol{n-1}\}$. Ο φυσικός αριθμός m που εμφανίζεται στο δεξί μέρος της σχέσης δηλώνει το πλήθος των καινούριων qubit, τα οποία προστίθενται στην κατάσταση κατά τη διάρκεια του υπολογισμού της $\boldsymbol{e}$. Η τελική κβαντική κατάσταση του προγράμματος μετά τον υπολογισμό έχει $\boldsymbol{n+m}$ qubits και προφανώς $\boldsymbol{qbits}(\boldsymbol{\tau}) \subseteq \{\boldsymbol{0}, \dots, \boldsymbol{n+m-1}\}$.

Οι κανόνες παραγωγής της nQML είναι παρόμοιοι με τους αντίστοιχους της QML των Altenkirch και Grattage, με εξαίρεση ότι το σύστημα τύπων δεν είναι γραμμικό και πρέπει να επεξεργάζονται πληροφορίες σχετικά με τα qubits. Για παράδειγμα ο τύπος για την κβαντική υπέρθεση ενός νέου qubit χρησιμοποιεί την θέση του στον τύπο επιστροφής:

$$\frac{|\boldsymbol{\lambda}|^2 + |\boldsymbol{\lambda'}|^2 = \boldsymbol{1}}{\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\circ} \{(\boldsymbol{\lambda})\boldsymbol{qfalse} + (\boldsymbol{\lambda'})\boldsymbol{qtrue}\}: \boldsymbol{qbit}[\boldsymbol{n}]; \boldsymbol{1}} \quad (\boldsymbol{SUP})$$

Οι κανόνες με περισσότερες από μία εκφράσεις πρέπει να συνδυάζουν προσεκτικά τα νέο – δημιουργημένα qubits, π.χ.

$$\frac{\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\boldsymbol{\alpha}} \boldsymbol{e_1}: \boldsymbol{\tau_1}; \boldsymbol{m_1} \qquad \boldsymbol{\Gamma}; \boldsymbol{n+m_1} \vdash^{\boldsymbol{\alpha}} \boldsymbol{e_2}: \boldsymbol{\tau_2}; \boldsymbol{m_2}}{\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\boldsymbol{\alpha}} (\boldsymbol{e_1}, \boldsymbol{e_2}): \boldsymbol{\tau_1} \otimes \boldsymbol{\tau_2}; \boldsymbol{m_1 + m_2}} \quad (\boldsymbol{PROD})$$

Οι πιο περίπλοκοι κανόνες παραγωγής τύπων της nQML είναι οι κανόνες των δομών ροής ελέγχου. Εξηγούμε τους δύο από αυτούς παρακάτω. Σε μία έκφραση κβαντικής διακλάδωσης $\boldsymbol{if\ e\ then\ e_1\ else\ e_2}$ το qubit ελέγχου δεν πρέπει να χρησιμοποιείται στους δύο κλάδους. Αυτός ο περιορισμός είναι απαραίτητος για να απλοποιήσουμε την σημασιολογία του if και να εξαλείψουμε την ανάγκη για ορθογώνιους κλάδους. Οι ορθομοναδιαίοι μετασχηματισμοί οι οποίοι δεν μπορούν εύκολα να περιγραφούν με μια σειρά ελεγχόμενων κβαντικών διαδικασιών γράφονται με ειδική εντολή στην nQML. Παρατηρήστε επίσης ότι το πλήθος των νέο – δημιουργημένων qubit είναι ίσο με το μέγιστο πλήθος των δύο κλάδων.

$$\frac{\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\boldsymbol{\alpha}} \boldsymbol{e}: \boldsymbol{qbit}[\boldsymbol{k}]; \boldsymbol{m} \qquad \boldsymbol{\Gamma}|_{\boldsymbol{k}}; \boldsymbol{n+m} \vdash^{\circ} \boldsymbol{e_1}: \boldsymbol{\tau}; \boldsymbol{m_1} \qquad \boldsymbol{\Gamma}|_{\boldsymbol{k}}; \boldsymbol{n+m} \vdash^{\circ} \boldsymbol{e_2}: \boldsymbol{\tau}; \boldsymbol{m_2}}{\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\boldsymbol{\alpha}} \boldsymbol{if\ e\ then\ e_1\ else\ e_2}: \boldsymbol{\tau}; \boldsymbol{m} + \max(\boldsymbol{m_1}, \boldsymbol{m_2})} \quad (\boldsymbol{IF})$$

Ο κανόνας για τη νέα δομή $|\boldsymbol{e}\rangle \to \boldsymbol{x}, \boldsymbol{x'}.\boldsymbol{c}$ είναι επίσης προφανής. Ένας ορθομοναδιαίος μετασχηματισμός εφαρμόζεται στα κβαντικά bits στα οποία είναι αποθηκευμένη η τιμή της έκφρασης $\boldsymbol{e}$. Ο τύπος $\boldsymbol{\tau}$ αυτής της έκφρασης πρέπει να είναι αγνός ώστε να ικανοποιείται το θεώρημα «μη αντιγραφής». Στην κλασική έκφραση $\boldsymbol{c}$, η οποία καθορίζει τα περιεχόμενα του μετασχηματισμού, οι δύο μεταβλητές $\boldsymbol{x}$ και $\boldsymbol{x'}$ πρέπει να έχουν ως τύπο το κλασικό αντίστοιχο $\mathsf{C}(\boldsymbol{\tau})$ της έκφρασης $\boldsymbol{e}$ ώστε να παίρνουν τις κλασικές τιμές της έκφρασης και να έχει νόημα ο μετασχηματισμός.

$$\frac{\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\alpha} \boldsymbol{e}: \boldsymbol{\tau}; \boldsymbol{m} \quad \boldsymbol{pure}(\boldsymbol{\tau}) \quad \boldsymbol{x}: \mathsf{C}(\boldsymbol{\tau}), \boldsymbol{x'}: \mathsf{C}(\boldsymbol{\tau}) \vdash \boldsymbol{c}: \boldsymbol{complex}}{\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\alpha} |\boldsymbol{e}\rangle \to \boldsymbol{x}, \boldsymbol{x'}.\boldsymbol{c}: \boldsymbol{\tau}; \boldsymbol{m}} \quad (\boldsymbol{TRANS})$$

Ο κανόνας παραγωγής των κλασικών εκφράσεων $\boldsymbol{\Delta} \vdash \boldsymbol{c}: \boldsymbol{\varphi}$ δεν παρουσιάζει δυσκολίες.

5.4 Λειτουργική σημασιολογία της nQML

Η λειτουργική σημασιολογία της γλώσσας χρησιμοποιεί πίνακες πυκνότητας οι οποίοι αναπαριστούν την κβαντική κατάσταση των καταχωρητών. Ο χώρος $\boldsymbol{S}(\boldsymbol{n}) \subset \mathbb{C}^{\boldsymbol{2^n} \times \boldsymbol{2^n}}$ περιέχει πίνακες πυκνότητας. Η λειτουργία μιας τυχαίας ορθά γραμμένης έκφρασης $\boldsymbol{e}$ με κανόνα παραγωγής $\boldsymbol{\Gamma}; \boldsymbol{n} \vdash \boldsymbol{e}: \boldsymbol{\tau}; \boldsymbol{m}$ είναι μία συνάρτηση της μορφής $\boldsymbol{S}(\boldsymbol{n}) \to \boldsymbol{S}(\boldsymbol{n} + \boldsymbol{m})$. Δηλαδή αντιστοιχίζει μια κβαντική κατάσταση εισόδου n qubit σε μία κατάσταση εξόδου $\boldsymbol{n} + \boldsymbol{m}$ qubits. Οι αγνές κβαντικές εκφράσεις οι οποίες δεν διεξάγουν μετρήσεις αντιστοιχίζονται σε ορθομοναδιαίους μετασχηματισμούς. Συμβολίζουμε με $\boldsymbol{T}(\boldsymbol{n}) \subset \mathbb{C}^{\boldsymbol{2^n} \times \boldsymbol{2^n}}$ τον χώρο των ορθομοναδιαίων πινάκων μετασχηματισμού. Εάν $\boldsymbol{e}$ είναι μια ορθά τυπωμένη αγνή κβαντική έκφραση με κανόνα παραγωγής $\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\circ} \boldsymbol{e}: \boldsymbol{\tau}; \boldsymbol{m}$ τότε η σημασία της είναι ένας πίνακας της μορφής $\boldsymbol{T}(\boldsymbol{n} + \boldsymbol{m})$. Η σημασιολογία της εισαγωγής αγνών κβαντικών εκφράσεων σε μη αγνές εκφράσεις δίνεται παρακάτω. Το τανυστικό γινόμενο του πίνακα $\boldsymbol{A} \in \boldsymbol{\Sigma}(\boldsymbol{n})$ με τον πίνακα $\boldsymbol{\Delta_m}$ επεκτείνει κατάλληλα την κβαντική κατάσταση με $\boldsymbol{m}$ καινούρια qubit τα οποία αρχικοποιούνται με μηδενικές τιμές.

$$\boldsymbol{EMB}: \quad [\![\boldsymbol{\Gamma}; \boldsymbol{n} \vdash \boldsymbol{e}: \boldsymbol{\tau}; \boldsymbol{m}]\!](\boldsymbol{A}) = \boldsymbol{T}(\boldsymbol{A} \otimes \boldsymbol{\Delta_m})\boldsymbol{T}^*$$

$$\text{όπου } \boldsymbol{T} = [\![\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\circ} \boldsymbol{e}: \boldsymbol{\tau}; \boldsymbol{m}]\!]$$

Η χρησιμοποίηση μιας μεταβλητής δεν έχει καμία επίδραση στην κβαντική κατάσταση καθώς όπως είπαμε οι μεταβλητές είναι απλώς αναφορές στην θέση που είναι αποθηκευμένη η τιμή της μεταβλητής. Παρ' όλα αυτά οι υπερθέσεις επεκτείνουν την κατάσταση διαθέτοντας στο πρόγραμμα ένα νέο qubit και αρχικοποιώντας το κατάλληλα.

$$\boldsymbol{VAR}: \quad [\![\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\circ} \boldsymbol{x}: \boldsymbol{\tau}; \boldsymbol{0}]\!] = \mathbb{I}_{\boldsymbol{n}}$$

$$\boldsymbol{SUP}: \quad [\![\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\circ} \{(\boldsymbol{\lambda})\boldsymbol{qfalse} + (\boldsymbol{\lambda'})\boldsymbol{qtrue}\}: \boldsymbol{qbit}[\boldsymbol{n}]; \boldsymbol{1}]\!] = \mathbb{I}_{\boldsymbol{n}} \otimes \begin{pmatrix} \boldsymbol{\lambda} & \boldsymbol{\lambda'} \\ \boldsymbol{\lambda'} & -\boldsymbol{\lambda} \end{pmatrix}$$

Η σημασιολογία των δομών let, εισαγωγής γινομένου και απαλοιφής γινομένου είναι προφανής και παρόμοια. Σε κάθε μία από αυτές ο υπολογισμός ξεκινά με τον υπολογισμό της έκφρασης $\boldsymbol{e_1}$ και συνεχίζει με τον υπολογισμό του $\boldsymbol{e_2}$ στην αλλαγμένη κατάσταση. Οι μη αγνές περιπτώσεις είναι αρκετά όμοιες.

$$\boldsymbol{LET}^{\circ}: \quad [\![\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\circ} \boldsymbol{let}\ \boldsymbol{x} = \boldsymbol{e_1}\ \boldsymbol{in}\ \boldsymbol{e_2}: \boldsymbol{\tau}; \boldsymbol{m_1} + \boldsymbol{m_2}]\!] = \boldsymbol{T_2}\big(\boldsymbol{T_1} \otimes \mathbb{I}_{\boldsymbol{m_2}}\big)$$

$$\text{όπου } \boldsymbol{T_1} = [\![\boldsymbol{\Gamma}; \boldsymbol{n} \vdash^{\circ} \boldsymbol{e_1}: \boldsymbol{\tau_1}; \boldsymbol{m_1}]\!]$$

$$\boldsymbol{T_2} = [\![\boldsymbol{\Gamma}, \boldsymbol{x}: \boldsymbol{\tau_1}; \boldsymbol{n} + \boldsymbol{m_1} \vdash^{\circ} \boldsymbol{e_2}: \boldsymbol{\tau}; \boldsymbol{m_2}]\!]$$

Η περίπτωση του if είναι ελαφρώς πολυπλοκότερη. Ο υπολογισμός της έκφρασης ξεκινάει με την υπόθεση του if. Οι πίνακες που αντιστοιχούν στους δύο κλάδους υπολογίζονται και η (ανύπαρκτη) επίδρασή τους στο bit ελέγχου αφαιρείται χρησιμοποιώντας την βοηθητική συνάρτηση except. Τότε οι δύο εκφράσεις υπολογίζονται ελεγχόμενες από το qubit ελέγχου $\boldsymbol{e}$. Η μη αγνή περίπτωση είναι εντελώς όμοια.

$$\boldsymbol{IF^{\circ}}: \quad \left[\!\left[\boldsymbol{\Gamma; n \vdash^{\circ} if\ e\ then\ e_1\ else\ e_2 : \tau; m + \max(m_1, m_2)}\right]\!\right] = \boldsymbol{T_C}(\boldsymbol{T} \otimes \mathbb{I}_{\boldsymbol{\max(m_1, m_2)}})$$

$$\text{όπου } \boldsymbol{T} = [\![\boldsymbol{\Gamma; n \vdash^{\circ} e : qbit[k]; m}]\!]$$

$$\boldsymbol{T_1} = [\![\boldsymbol{\Gamma|_k; n + m \vdash^{\circ} e_1 : \tau; m_1}]\!]$$

$$\boldsymbol{T_2} = [\![\boldsymbol{\Gamma|_k; n + m \vdash^{\circ} e_2 : \tau; m_2}]\!]$$

$$\boldsymbol{T_1'} = \boldsymbol{except(k, T_1)} \otimes \mathbb{I}_{\boldsymbol{\max(m_1, m_2) - m_2}}$$

$$\boldsymbol{T_2'} = \boldsymbol{except(k, T_2)} \otimes \mathbb{I}_{\boldsymbol{\max(m_1, m_2) - m_1}}$$

$$\boldsymbol{T_C} = \boldsymbol{cond(k, T_1', T_2')}$$

Περιέργως η εντολή ifm η οποία διενεργεί και μέτρηση είναι πιο ευκολονόητη. Η υπόθεση υπολογίζεται και μετά μετράται το κατάλληλο qubit. Η βοηθητική συνάρτηση measure επιστρέφει δύο πίνακες πυκνότητας οι οποίοι αντιστοιχούν στην κατάρρευση ενός qubit στην κλασική κατάσταση. Τότε οι δύο κλάδοι συνδυάζονται. Κάθε κλάδος υπολογίζεται με βάση την αντίστοιχη κατάσταση που προέκυψε μετά την μέτρηση και το άθροισμά τους είναι το συνολικό αποτέλεσμα.

$$\boldsymbol{IFM}: \quad \left[\!\left[\boldsymbol{\Gamma; n \vdash^{\circ} ifm\ e\ then\ e_1\ else\ e_2 : \tau; m + \max(m_1, m_2)}\right]\!\right](\boldsymbol{A}) =$$

$$\boldsymbol{B_1} \otimes \boldsymbol{\Delta}_{\boldsymbol{\max(m_1, m_2) - m_1}} + \boldsymbol{B_2} \otimes \boldsymbol{\Delta}_{\boldsymbol{\max(m_1, m_2) - m_2}}$$

$$\text{όπου } \boldsymbol{B} = [\![\boldsymbol{\Gamma; n \vdash e : qbit[k]; m}]\!](\boldsymbol{A})$$

$$\left(\boldsymbol{B_t, B_f}\right) = \boldsymbol{measure(k, B)}$$

$$\boldsymbol{B_1} = [\![\boldsymbol{\Gamma; n + m \vdash e_1 : \tau; m_1}]\!](\boldsymbol{B_t} \otimes \boldsymbol{\Delta_{m_1}})$$

$$\boldsymbol{B_2} = [\![\boldsymbol{\Gamma; n + m \vdash e_2 : \tau; m_2}]\!](\boldsymbol{B_f} \otimes \boldsymbol{\Delta_{m_2}})$$

Τελικά στη λειτουργία της εντολής $\boldsymbol{|e\rangle \to x, x'.c}$ ο ορθομοναδιαίος μετασχηματισμός $\boldsymbol{C}$ υπολογίζεται. Καθώς ο $\boldsymbol{C}$ εφαρμόζεται μόνο στα qubits που χρησιμοποιεί η $\boldsymbol{e}$ πρέπει να επεκταθεί κατάλληλα ώστε να δρα σε ολόκληρη την κβαντική κατάσταση.

$$\boldsymbol{TRANS^{\circ}}: \quad [\![\boldsymbol{\Gamma; n \vdash^{\circ} |e\rangle \to x, x'.c : \tau; m}]\!] = \boldsymbol{T_C T}$$

$$\text{όπου } \boldsymbol{T_C} = \boldsymbol{expand(n, qbits(\tau), C)}$$

$$\boldsymbol{T} = [\![\boldsymbol{\Gamma; n \vdash^{\circ} e : \tau; m}]\!]$$

$$\boldsymbol{C_{j,i}} = [\![\boldsymbol{x : C(\tau), x' : C(\tau) \vdash c : complex}]\!](\boldsymbol{\rho})$$

$$\text{όπου } \boldsymbol{\rho} = \boldsymbol{\rho_0}\{\boldsymbol{x \mapsto val_\tau(i)}\}\{\boldsymbol{x' \mapsto val_\tau(j)}\}$$

$$\forall \boldsymbol{i, j}: \boldsymbol{0 \le i, j < 2^k}, \text{ όπου } \boldsymbol{k = |qbits(\tau)|}$$

Η σημασιολογία των κλασικών εκφράσεων είναι καθορισμένη από τον κλασικό υπολογισμό και δεν παρουσιάζει δυσκολίες.

5.5 Υλοποίηση της γλώσσας nQML σε Haskell

Σε προηγούμενη διπλωματική εργασία υλοποιήθηκε η nQML σε Haskell και εδώ απλώς παραθέτουμε τον κώδικα που ορίζει τους όρους της γλώσσας οι οποίοι είναι άμεση απόρροια από τη σύνταξη:

```
type I            = String

data Expr         = Var I
                  | Super (Complex Double) (Complex Double)
                  | Let I Expr Expr
                  | Prod Expr Expr
                  | LetP I I Expr Expr
                  | If Expr Expr Expr
                  | IfM Expr Expr Expr
                  | Trs Expr I I CExpr
                  | App I [Expr]                  -- for macros!
                  deriving (Eq, Read, Show)
```

6 Μετάφραση nQML σε κυκλώματα

6.1 Εισαγωγή

Σε αυτήν την ενότητα παρουσιάζω την πρωτότυπη εργασία της μετάφρασης των εντολών της γλώσσας nQML σε κυκλώματα. Όπως είδαμε η σημασιολογία των εντολών της γλώσσας είναι οι ορθομοναδιαίοι πίνακες και μετασχηματισμοί. Όμως οι περισσότεροι ενδιαφέροντες κβαντικοί αλγόριθμοι υλοποιούνται με τη βοήθεια κβαντικών κυκλωμάτων· κάτι αναμενόμενο αφού οι στοιχειώδεις λειτουργίες του κβαντικού προγραμματισμού βρίσκονται πολύ πιο κοντά στο επίπεδο του hardware και εξαρτώνται ισχυρά από αυτό. Οι γλώσσες προγραμματισμού από την άλλη προσπαθούν να ισχυροποιήσουν τα κβαντικά προγράμματα και να δημιουργήσουν ένα αφαιρετικό μοντέλο το οποίο επιτρέπει στους προγραμματιστές να μην ασχολούνται με τις υλοποιήσεις στο υλικό των κβαντικών υπολογιστών. Φυσικά σε τελική ανάλυση οι λειτουργίες της γλώσσας θα πρέπει να υλοποιηθούν σε υλικό.

Αυτή η ενότητα εξυπηρετεί λοιπόν δύο σκοπούς. Πρώτον βοηθάει στην καλύτερη κατανόηση των προγραμμάτων καθώς η μετάφραση τους σε κυκλώματα τα κάνει πιο «χειροπιαστά» γιατί όπως είπαμε οι αλγόριθμοι υλοποιούνται σε κυκλώματα. Δεύτερον δίνει μια πρώτη ιδέα για το πώς πρόκειται να λειτουργήσουν οι κβαντικοί υπολογιστές του μέλλοντος και ποιες λειτουργίες θα πρέπει να υλοποιούν ώστε να εκτελούν εντολές της nQML ή άλλης παρόμοιας γλώσσας.

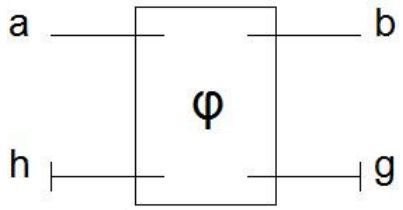
6.2 Κλάσεις κυκλωμάτων

Στο (11) ορίζονται διάφορες κατηγορίες κβαντικών κυκλωμάτων με βάση τις οποίες κατασκευάζονται τα διάφορα κβαντικά κυκλώματα με τα οποία ορίζεται η σημασιολογία της γλώσσας QML. Τις ίδιες κατηγορίες θα χρησιμοποιήσουμε και εμείς για να μεταφράσουμε τις εντολές τις nQML σε κυκλώματα.

Αρχικά ορίζεται η κατηγορία $\boldsymbol{FQC}^{\simeq}$ η οποία περικλείει τους πεπερασμένους κβαντικούς μετασχηματισμούς (Finite Quantum Computations), οι οποίοι έχουν τον περιορισμό ότι είναι αντιστρέψιμοι (εκθέτης $\simeq$). Τα μέλη της κατηγορίας είναι μορφισμοί – συναρτήσεις από ένα πλήθος $\boldsymbol{a}$ qubit σε ένα πλήθος $\boldsymbol{b}$ qubit. Έτσι ορίζουμε υποκατηγορίες $\boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}\ \boldsymbol{b}$ οι οποίες περιέχουν όλα τα κυκλώματα με $\boldsymbol{a}$ qubit εισόδου και $\boldsymbol{b}$ qubit εξόδου. Όπως ανέφερα οι μετασχηματισμοί αυτοί είναι αντιστρέψιμοι και άρα πρέπει η είσοδος να έχει το ίδιο μέγεθος με την έξοδο ή αλλιώς λέμε ότι $\boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}\ \boldsymbol{b} = \{\}$ όταν $\boldsymbol{a} \neq \boldsymbol{b}$. Ορίζουμε επίσης ότι $\boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}\ \boldsymbol{a} = \boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}$ που είναι το σύνολο των αντιστρέψιμων μετασχηματισμών πάνω σε ένα σύνολο $\boldsymbol{a}$ qubit. Όλα τα κυκλώματα της κατηγορίας $\boldsymbol{FQC}^{\simeq}$ (που αποτελείται από όλες τις υποκατηγορίες $\boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}$) κατασκευάζονται αναδρομικά από ένα αριθμό στοιχειωδών κυκλωμάτων και πράξεων ανάμεσά τους όπως θα δούμε στην επόμενη ενότητα.

Ο Grattage επεκτείνει την κατηγορία των αντιστρέψιμων κυκλωμάτων ορίζοντας την κατηγορία $\boldsymbol{FQC}$ οι οποία αποτελείται επιπλέον από τα μη αντιστρέψιμα κβαντικά κυκλώματα. Η μη αντιστρεψιμότητα περιλαμβάνει μετρήσεις ή / και αρχικοποιήσεις νέων qubit: διεργασίες που δεν είναι αντιστρέψιμες. Έτσι τα νέα κυκλώματα περιέχουν και δύο νέα σύνολα qubit, εισόδου και εξόδου, που ονομάζονται σωρός (heap) και σκουπίδια (garbage), αντίστοιχα. Τα qubits στο σωρό θεωρούμε ότι είναι πάντα αρχικοποιημένα σε μια τιμή της βάσης του διανυσματικού χώρου, συνήθως $|\mathbf{0}\rangle$, και

συμβολίζονται στο κύκλωμα με $\vdash$. Αντίθετα τα qubits στα σκουπίδια είναι τα qubits που απελευθερώνονται από το πρόγραμμα ή γίνεται μια κβαντική μέτρηση πάνω τους (επομένως ίσως αποτελούν και το αποτέλεσμα του αλγορίθμου· δεν είναι άχρηστα!) και συμβολίζονται με $\dashv$. Ουσιαστικά κάθε κύκλωμα της κατηγορίας $\boldsymbol{FQC\ a\ b}$ ($\boldsymbol{a}$ είσοδοι - $\boldsymbol{b}$ έξοδοι) είναι μια τριάδα $\boldsymbol{\varphi = (h, g, \varphi')}$ όπου $\boldsymbol{h} \in \mathbb{N}$ είναι το μέγεθος σε qubits του σωρού, όλα αρχικοποιημένα σε $|\mathbf{0}\rangle$, $\boldsymbol{g} \in \mathbb{N}$ είναι το πλήθος των σκουπιδιών και $\boldsymbol{\varphi' \in FQC^{\simeq}\ c}$ ένας αντιστρέψιμος μετασχηματισμός με $\boldsymbol{c = a + h = b + g}$. Ο γενικός συμβολισμός αυτών των κυκλωμάτων φαίνεται στο παρακάτω σχήμα.



Σχήμα 6.1: Κυκλωματικός συμβολισμός ενός υπολογισμού στο $\boldsymbol{FQC}$, όπου $\boldsymbol{\varphi}$ ένας αντιστρέψιμος μετασχηματισμός στο $\boldsymbol{FQC^{\simeq}}$. Φαίνονται οι είσοδοι και έξοδοι, σωρού και σκουπιδιών αντίστοιχα.

Φυσικά κάθε μετασχηματισμός που ανήκει στην κατηγορία $\boldsymbol{FQC^{\simeq}}$ ανήκει και στην κατηγορία $\boldsymbol{FQC}$ αν θεωρήσουμε μηδενικό μέγεθος σωρού και σκουπιδιών. Για παράδειγμα αν $\boldsymbol{\varphi \in FQC^{\simeq}\ a}$ κατασκευάζουμε τον $\boldsymbol{\varphi' \in FQC\ a\ a}$ με $\boldsymbol{\varphi' = (0, 0, \varphi)}$.

Τέλος ιδιαίτερο ενδιαφέρον παρουσιάζει η κατηγορία των κυκλωμάτων τα οποία δεν περιλαμβάνουν μετρήσεις αλλά μπορούν να περιλαμβάνουν αρχικοποιήσεις. Αυτή η κατηγορία των αγνών ή αυστηρών υπολογισμών (θυμηθείτε τις αγνές παραγωγές εκφράσεων τις γλώσσας nQML) συμβολίζεται με $\boldsymbol{FQC^{\circ}}$ και αποτελείται από τα κυκλώματα με κενό το σύνολο των σκουπιδιών, δηλαδή $\boldsymbol{\alpha = (h, \varphi) \in FQC^{\circ}\ a\ b}$. Όπως φαίνεται $\boldsymbol{g = 0}$ και άρα παραλείπεται στον ορισμό το σύνολο των σκουπιδιών. Οι αγνοί κβαντικοί υπολογισμοί δεν είναι απλώς αντιστρέψιμοι μετασχηματισμοί, καθώς επιτρέπονται αρχικοποιημένες είσοδοι. Παρόλα αυτά η έλλειψη σκουπιδιών εξόδου σημαίνει ότι οι μορφισμοί του $\boldsymbol{FQC^{\circ}}$ μπορούν να μοντελοποιηθούν ως γραμμικοί μετασχηματισμοί από αγνές κβαντικές καταστάσεις σε αγνές κβαντικές καταστάσεις. Αυτό το έχουμε ξαναδεί στη σημασιολογία της nQML όπου οι αγνές εκφράσεις αντιστοιχίζονται σε πίνακες μετασχηματισμού (γραμμικοί ορθομοναδιαίοι) ενώ οι μη αγνές σε συναρτήσεις. Οι μετρήσεις της κλάσης $\boldsymbol{FQC}$ προκαλούν την κατάρρευση των κυματοσυναρτήσεων των qubit και επομένως οδηγούν σε πιθανοτικά αποτελέσματα. Συνεπώς οι μη αντιστρέψιμοι μετασχηματισμοί δεν μπορούν να μοντελοποιηθούν χρησιμοποιώντας γραμμικές αντιστοιχήσεις μεταξύ αγνών καταστάσεων. Προκύπτει ότι το σύνολο $\boldsymbol{FQC^{\circ}}$ είναι το μεγαλύτερο υποσύνολο της κατηγορίας $\boldsymbol{FQC}$ το οποίο μπορεί να μοντελοποιηθεί χρησιμοποιώντας γραμμικούς μετασχηματισμούς.

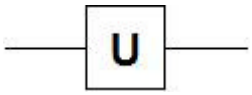
Τελικά από τους ορισμούς των $\boldsymbol{FQC^{\simeq}}$ (όχι σωρός ή σκουπίδια), $\boldsymbol{FQC^{\circ}}$ (όχι σκουπίδια αλλά επιτρέπεται σωρός) και $\boldsymbol{FQC}$ (επιτρέπεται και σωρός και σκουπίδια) προκύπτει ότι:

$$\boldsymbol{FQC^{\simeq} \subset FQC^{\circ} \subset FQC}$$

6.3 Κατασκευή κυκλωμάτων $FQC^{\simeq}$

Αρχικά θα ασχοληθούμε με την αναδρομική κατασκευή των αντιστρέψιμων κυκλωμάτων, δηλαδή κυκλωμάτων της κλάσης $\boldsymbol{FQC}^{\simeq}$. Όπως είδαμε και παραπάνω κάθε κύκλωμα που ανήκει στην κλάση $\boldsymbol{FQC}$ που είναι η γενική μορφή των κβαντικών κυκλωμάτων αποτελείται στην ουσία από ένα αντιστρέψιμο κύκλωμα με αρχικοποιήσεις στην αρχή και μετρήσεις στο τέλος. Τα κυκλώματα στην κατηγορία $\boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}$ που είναι τα αντιστρέψιμα κβαντικά κυκλώματα με $\boldsymbol{a}$ εισόδους ορίζονται επαγωγικά ως εξής:

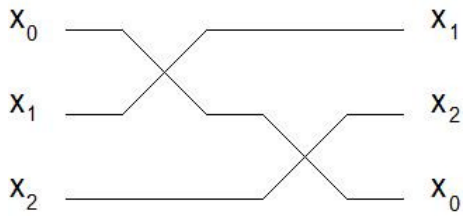
- Περιστροφές – Rotation
  $\boldsymbol{rot\ u} \in \boldsymbol{FQC}^{\simeq}\ \boldsymbol{1}$: Δηλώνει μια περιστροφή που δρα πάνω σε ένα μόνο qubit, όπου ο $\boldsymbol{u}$ είναι ένας ορθομοναδιαίος πίνακας. Η αντίστροφη διαδικασία είναι ο αναστροφοσυζυγής μετασχηματισμός δηλαδή ο $\boldsymbol{\varphi^{-1} = rot\ u^{\dagger}} \in \boldsymbol{FQC}^{\simeq}\ \boldsymbol{1}$. Σε κυκλωματικό διάγραμμα αυτός ο μετασχηματισμός συμβολίζεται ως εξής:

  Σχήμα 6.2: Αυθαίρετο κύκλωμα rotation

  Ο πίνακας $\boldsymbol{u}$ πρέπει να είναι ορθομοναδιαίος και της μορφής $\begin{pmatrix} \boldsymbol{\lambda_0} & \boldsymbol{\lambda_1} \\ \boldsymbol{\kappa_0} & \boldsymbol{\kappa_1} \end{pmatrix}$ με $\boldsymbol{\lambda_0^* \kappa_0 + \lambda_1^* \kappa_1 = 1}$. Ο αντίστροφος του δίνεται από τον $\boldsymbol{u^{\dagger}} = \begin{pmatrix} \boldsymbol{\lambda_0} & \boldsymbol{\lambda_1} \\ \boldsymbol{\kappa_0} & \boldsymbol{\kappa_1} \end{pmatrix}^{\dagger} = \begin{pmatrix} \boldsymbol{\lambda_0^*} & \boldsymbol{\kappa_0^*} \\ \boldsymbol{\lambda_1^*} & \boldsymbol{\kappa_1^*} \end{pmatrix}$. Ειδική περίπτωση αποτελεί η άρνηση που είναι το κύκλωμα $\boldsymbol{rot\ X}$ με $\boldsymbol{X} = \begin{pmatrix} \boldsymbol{0} & \boldsymbol{1} \\ \boldsymbol{1} & \boldsymbol{0} \end{pmatrix}$.

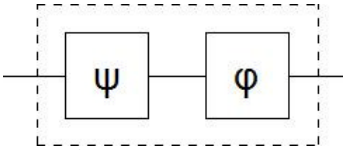
- Καλωδιώσεις – Wires
  Κάθε πιθανή αναδιάταξη των qubits είναι ένας έγκυρος μετασχηματισμός και στο κυκλωματικό διάγραμμα φαίνεται ως ένα ανακάτεμα των καλωδίων όπως στο σχήμα.

  Σχήμα 6.3: Παράδειγμα κυκλώματος wires

  Είναι το κύκλωμα $\boldsymbol{wires\ \varphi} \in \boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}$ όπου $\boldsymbol{\varphi}$ ο ισομορφισμός $\boldsymbol{\varphi}: [\boldsymbol{a}] \simeq [\boldsymbol{a}]$ και $[\boldsymbol{a}]$ είναι το αρχικό τμήμα του φυσικού $\boldsymbol{a}$, το οποίο ορίζεται ως $\{\boldsymbol{i} \in \mathbb{N} \mid \boldsymbol{i} < \boldsymbol{a}\}$. Η έκφραση περιγράφει κάθε δυνατή αναδιάταξη, συμπεριλαμβανομένης και της ταυτοτικής $\boldsymbol{id_a = wires\ id}$ με την οποία δεν συμβαίνει καμία αλλαγή. Η αναδιάταξη είναι τετριμμένα αντιστρέψιμη και η τάξη του κυκλώματος είναι ίση με τον αριθμό των καλωδίων στο κύκλωμα, που είναι το $\boldsymbol{a}$ του ισομορφισμού.

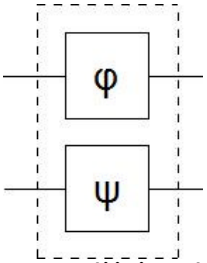
- Σειριακή σύνθεση
  Δεδομένων δύο κυκλωμάτων $\boldsymbol{\varphi} \in \boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}$ και $\boldsymbol{\psi} \in \boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}$, δηλαδή δύο κυκλωμάτων με τον ίδιο αριθμό qubit, μπορεί να κατασκευαστεί η σύνθεσή τους $\boldsymbol{\varphi} \circ \boldsymbol{\psi} \in \boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}$ που συμβολίζεται ως εξής:



Σχήμα 6.4: Κύκλωμα σειριακής σύνθεσης

  Τα καλώδια εξόδου του πρώτου κυκλώματος οδηγούνται στις εισόδους του δεύτερου, κάτι το οποίο είναι δυνατό αφού τα δύο κυκλώματα είναι ίδιας τάξης. Η τάξη του προκύπτοντος κυκλώματος είναι προφανώς επίσης $\boldsymbol{a}$. Ο αντίστροφος μετασχηματισμός είναι ο $\boldsymbol{\psi^{-1}} \circ \boldsymbol{\varphi^{-1}} \in \boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}$ αφού υπάρχουν οι μετασχηματισμοί $\boldsymbol{\psi^{-1}}, \boldsymbol{\varphi^{-1}}$.

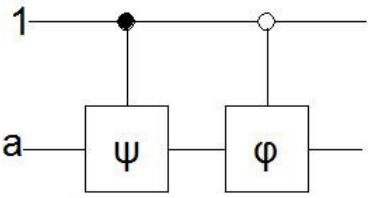
- Παράλληλη σύνθεση
  Δεδομένων δύο κυκλωμάτων $\boldsymbol{\varphi} \in \boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}$ και $\boldsymbol{\psi} \in \boldsymbol{FQC}^{\simeq}\ \boldsymbol{b}$ μπορεί να κατασκευαστεί η παράλληλη σύνθεσή τους $\boldsymbol{\varphi} \otimes \boldsymbol{\psi} \in \boldsymbol{FQC}^{\simeq}\ (\boldsymbol{a} + \boldsymbol{b})$ που συμβολίζεται ως εξής:



Σχήμα 6.5: Κύκλωμα παράλληλης σύνθεσης

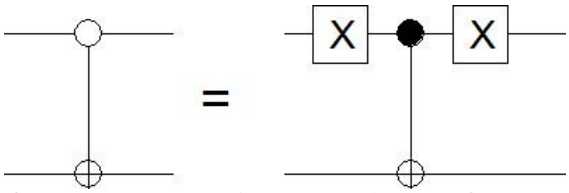
  Αυτή η κατασκευή συνδυάζει τα δύο κυκλώματα εν παραλλήλω και μπορούμε να πούμε ότι αποτελεί το τανυστικό γινόμενο των δύο κυκλωμάτων και των κβαντικών καταστάσεων των επιμέρους qubit. Η τάξη του νέου κυκλώματος είναι ίση με το άθροισμα των τάξεων των δύο υπό – κυκλωμάτων, δηλαδή $\boldsymbol{a} + \boldsymbol{b}$. Το αντίστροφο κύκλωμα είναι προφανώς το $\boldsymbol{\varphi^{-1}} \otimes \boldsymbol{\psi^{-1}} \in \boldsymbol{FQC}^{\simeq}\ (\boldsymbol{a} + \boldsymbol{b})$.

- Εκτέλεση υπό συνθήκη
  Δεδομένων δύο κυκλωμάτων $\boldsymbol{\varphi}, \boldsymbol{\psi} \in \boldsymbol{FQC}^{\simeq}\ \boldsymbol{a}$ κατασκευάζουμε την υπό συνθήκη εκτέλεση: $\boldsymbol{if\ qubit\ then\ \psi\ else\ \varphi}$ με το κύκλωμα $\boldsymbol{\varphi|\psi} \in \boldsymbol{FQC}^{\simeq}\ (\boldsymbol{1} + \boldsymbol{a})$. Φυσικά η διαφορά από την κλασική αυτή εντολή είναι ότι το qubit ελέγχου μπορεί να βρίσκεται σε κβαντική υπέρθεση και επομένως κάθε υπό-κύκλωμα εφαρμόζεται στις ανάλογες συνιστώσες των qubit εισόδου. Το κυκλωματικό διάγραμμα είναι το παρακάτω:



Σχήμα 6.6: Κύκλωμα υπό-συνθήκη εκτέλεσης

Ο συμβολισμός με το άσπρο κυκλάκι είναι ουσιαστικά το αντίστοιχο με την υπό συνθήκη εκτέλεση αλλά μόνο αν το qubit ελέγχου είναι 0. Το κύκλωμα μπορεί να κατασκευαστεί από τις πύλες του πλήρους συνόλου που δώσαμε ως εξής:



Σχήμα 6.7: Ελεγχόμενη διαδικασία με μία NOT πύλη να εφαρμόζεται στο δεύτερο qubit, με την προϋπόθεση το πρώτο qubit να έχει τεθεί στο μηδέν.

Όπως αναφέραμε στην ενότητα των κβαντικών κυκλωμάτων κάθε τέτοια ελεγχόμενη κατασκευή είναι δυνατή, αφού κάθε κύκλωμα (και ειδικότερα αυτά της κλάσης $\boldsymbol{FQC}^{\simeq}$) μπορεί να αναλυθεί σε κυκλώματα αποτελούμενα μόνο από μετασχηματισμούς 1-qubit και πύλες CNOT. Εάν είτε το $\boldsymbol{\varphi}$ είτε το $\boldsymbol{\psi}$ είναι το ταυτοτικό κύκλωμα τότε ο αντίστοιχος κλάδος απαλείφεται εντελώς. Τέλος το αντίστροφο κύκλωμα δίνεται πάλι με τη χρήση των $\boldsymbol{\varphi^{-1}}$ και $\boldsymbol{\psi^{-1}}$ και είναι το $\boldsymbol{\varphi^{-1}|\psi^{-1}} \in \boldsymbol{FQC}^{\simeq}\ (\boldsymbol{1+a})$.

6.4 Κατασκευή κυκλωμάτων $\boldsymbol{FQC}$

Όπως ανέφερα και παραπάνω κάθε κύκλωμα της κλάσης $\boldsymbol{FQC}^{\simeq}$ μπορεί να επεκταθεί στην κλάση $\boldsymbol{FQC}$. Επομένως μπορούμε να πούμε ότι η κλάση $\boldsymbol{FQC}$ περιέχει αρχικά όλα τα κυκλώματα που δημιουργούνται με αυτό τον τρόπο. Επίσης πρέπει να δώσουμε και ορισμούς σύνθεσης κυκλωμάτων.

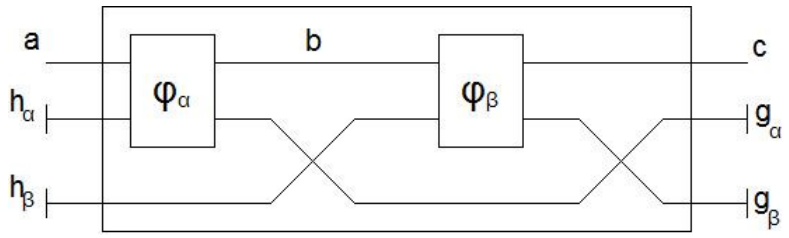
Η σειριακή σύνθεση δύο κυκλωμάτων τα οποία δίνονται ως μέλη της $\boldsymbol{FQC}$ ορίζεται με τον ίδιο τρόπο όπως και στην κατηγορία των αντιστρέψιμων κυκλωμάτων. Δοσμένων δύο κυκλωμάτων $\boldsymbol{\alpha} = (\boldsymbol{h_\alpha}, \boldsymbol{g_\alpha}, \boldsymbol{\varphi_\alpha}) \in \boldsymbol{FQC\ a\ b}$ και $\boldsymbol{\beta} = (\boldsymbol{h_\beta}, \boldsymbol{g_\beta}, \boldsymbol{\varphi_\beta}) \in \boldsymbol{FQC\ b\ c}$ η σειριακή τους σύνθεση δίνεται από το κύκλωμα $\boldsymbol{\beta} \circ \boldsymbol{\alpha} = (\boldsymbol{h}, \boldsymbol{g}, \boldsymbol{\varphi}) \in \boldsymbol{FQCa\ c}$ όπου

$$\boldsymbol{h} = \boldsymbol{h_\alpha} + \boldsymbol{h_\beta}$$

$$\boldsymbol{g} = \boldsymbol{g_\alpha} + \boldsymbol{g_\beta}$$

$$\boldsymbol{\varphi_{\beta\circ\alpha}} = (\boldsymbol{\varphi_\beta} \otimes \boldsymbol{id_{g_\alpha}}) \circ (\boldsymbol{\varphi_\alpha} \otimes \boldsymbol{id_{h_\beta}})$$

του οποίου το διάγραμμα φαίνεται παρακάτω.



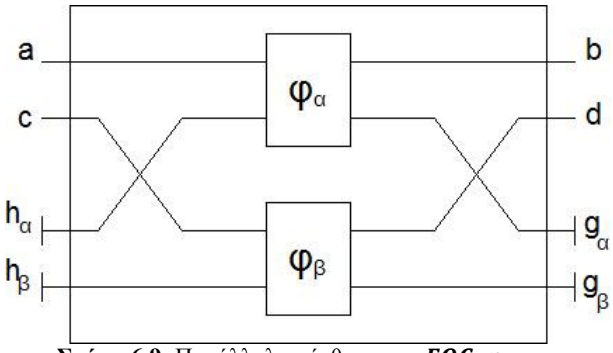
Σχήμα 6.8: Σειριακή σύνθεση στο $\boldsymbol{FQC}$: $\boldsymbol{\varphi_{\beta\circ\alpha}}$.

Η παράλληλη σύνθεση δύο κυκλωμάτων $\boldsymbol{\alpha = (h_\alpha, g_\alpha, \varphi_\alpha) \in FQC\ a\ b}$ και $\boldsymbol{\beta = (h_\beta, g_\beta, \varphi_\beta) \in FQC\ c\ d}$ γίνεται με παρόμοιο τρόπο. Είναι το κύκλωμα $\boldsymbol{\alpha \otimes \beta = (h, g, \varphi) \in FQC\ (a + c)\ (b + d)}$ όπου

$$\boldsymbol{h = h_\alpha + h_\beta}$$

$$\boldsymbol{g = g_\alpha + g_\beta}$$

$$\boldsymbol{\varphi_{\alpha\otimes\beta} = \varphi_\alpha \otimes \varphi_\beta}$$



Σχήμα 6.9: Παράλληλη σύνθεση στο $\boldsymbol{FQC}$: $\boldsymbol{\varphi_{\alpha\otimes\beta}}$.

Η εκτέλεση υπό συνθήκη είναι προφανής καθώς η συνθήκη εφαρμόζεται απλώς στο αντιστρέψιμο τμήμα του κυκλώματος.

Παρατηρήστε ότι σε όλες τις συνθέσεις τα καλώδια αρχικοποίησης και μετρήσεων μετακινούνται πάντα στην αρχή και το τέλος του κυκλώματος αντίστοιχα. Επομένως κάθε κύκλωμα $\boldsymbol{FQC}$ αποτελείται πάντα από ένα αντιστρέψιμο τμήμα στο κέντρο και διάφορα καλώδια να εξέρχονται ή να εισέρχονται από αυτό. Αρχικοποιήσεις ή μετρήσεις στο κεντρικό τμήμα δεν γίνονται.

6.5 Υλοποίηση κυκλωμάτων FQC σε Haskell

Για τη υλοποίηση των κυκλωμάτων FQC ορίσαμε ένα νέο τύπο κυκλωμάτων στον οποίο αποθηκεύονται οι αριθμοί των εισόδων, εξόδων, καλωδίων σωρού και σκουπιδιών.

```
data Fqc = Fqc {a :: Int,b :: Int,h :: Int,g :: Int, revCirc::Circ}
```

Παρακάτω φαίνονται οι δηλώσεις των συναρτήσεων που παράγουν την σειριακή και παράλληλη σύνθεση κυκλωμάτων όπως επίσης και δύο συναρτήσεις που υπολογίζουν το αποτέλεσμα των κυκλωμάτων με είσοδο διάφορα state. Η τελευταία συνάρτηση παίρνει ένα κύκλωμα που δεν έχει εισόδους (μόνο καλώδια σωρού) και παράγει το

αποτέλεσμα με τα αρχικά qubit στην κατάσταση 0. Αυτή είναι και η περίπτωση όλων των πλήρων προγραμμάτων nQML.

```
seqFqc :: Fqc -> Fqc -> Fqc
parFqc :: Fqc -> Fqc -> Fqc
fqc2Mat :: Fqc -> Matrix
eval :: Fqc -> Vector -> Vector
evalNoInp :: Fqc -> Vector
```

6.6 Μετάφραση εντολών – κανόνων

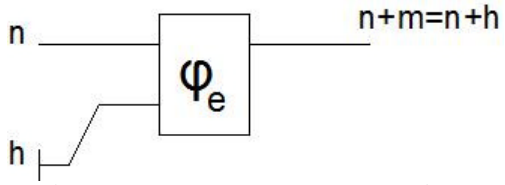
Στις ακόλουθες υποενότητες εξετάζω κάθε μεμονωμένη εντολή της γλώσσας και σχεδιάζω το αντίστοιχο κύκλωμα της κλάσης $\boldsymbol{FQC}$. Οι πράξεις που χρησιμοποιώ είναι αυτές που αναφέρθηκαν παραπάνω για τα μέλη της κλάσης (συνθέσεις, παράλληλες συνθέσεις κτλ.). Καθώς η σημασιολογία κάθε εντολής κρατάει και διαδίδει πληροφορίες για τον αριθμό των qubit της κατάστασης χρησιμοποιώ τους σημασιολογικούς κανόνες ώστε ο αριθμός των καλωδίων στα κυκλώματα να συμφωνεί με τους κανόνες. Τα κυκλώματα κατασκευάζονται αναδρομικά, υποθέτοντας δηλαδή ότι έχουν ήδη κατασκευαστεί τα αντίστοιχα κυκλώματα των εκφράσεων που βρίσκονται στην υπόθεση των κανόνων. Αυτά συμβολίζονται ως ορθογώνια των οποίων το περιεχόμενο είναι ένα κύκλωμα της κλάσης $\boldsymbol{FQC}^{\simeq}$ με καλώδια δεξιά και αριστερά τους (σωρός και σκουπίδια) στην περίπτωση που η παραγωγή της έκφρασης δεν είναι αγνή. Αν είναι αγνή (pure) όπως είπαμε παραλείπονται τα σκουπίδια. Φυσικά είναι δυνατόν και ο σωρός να είναι κενός αλλά στη γενική περίπτωση εισάγουμε καλώδια στο κύκλωμα.

Σχετικά με την υλοποίηση σε Haskell κάθε κανόνας (εκτός από τον EMB) αντιστοιχεί σε μία συνάρτηση η οποία λαμβάνει τα απαραίτητα υπό-κυκλώματα σαν ορίσματα και παράγει το κύκλωμα που προκύπτει με βάση τα παρακάτω σχήματα και τη σημασιολογία της γλώσσας.

6.6.1 Κανόνας EMB

$$\frac{\boldsymbol{\Gamma; n \vdash^{\circ} e : \tau; m}}{\boldsymbol{\Gamma; n \vdash e : \tau; m}} \quad (\boldsymbol{EMB})$$

Ο κανόνας αυτός είναι προφανώς διαφανής στα κυκλώματα αφού απλώς δηλώνει τη σχέση $\boldsymbol{FQC}^{\circ} \subset \boldsymbol{FQC}$. Κάθε αγνό κύκλωμα μπορεί να θεωρηθεί και μη αγνό χωρίς καμία αλλαγή θεωρώντας ότι το σύνολο σκουπιδιών είναι κενό. Οι αριθμοί στα καλώδια της παρακάτω εικόνας αλλά και σε όλες τις επόμενες δηλώνουν το πλήθος των καλωδίων.

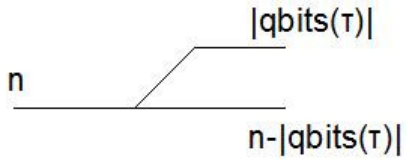


Σχήμα 6.10: Κύκλωμα EMB, το οποίο ανήκει στο $\boldsymbol{FQC}^{\simeq}$ άρα και στο $\boldsymbol{FQC}$.

6.6.2 Κανόνας VAR

$$\frac{(\boldsymbol{x}:\boldsymbol{\tau}) \in \boldsymbol{\Gamma}}{\boldsymbol{\Gamma};\boldsymbol{n} \vdash^{\circ} \boldsymbol{x}:\boldsymbol{\tau};\boldsymbol{0}} \quad (\boldsymbol{VAR})$$

Και αυτός ο κανόνας είναι διαφανής αφού όπως αναφέραμε οι μεταβλητές είναι αναφορές σε qubits. Για να φανεί καλύτερα αυτό στο παρακάτω σχήμα αναδιατάσσουμε τα qubit της μεταβλητής $\boldsymbol{x}$ και τα φέρνουμε στο άνω μέρος του κυκλώματος. Φυσικά ο τύπος της $\boldsymbol{x}$ μπορεί να μην είναι αγνός και κάποια qubits να εμφανίζονται δύο ή περισσότερες φορές στον τύπο όμως αυτό θα επιλυθεί σε επόμενη διεργασία στην περίπτωση που ίσως μετασχηματιστεί η x.

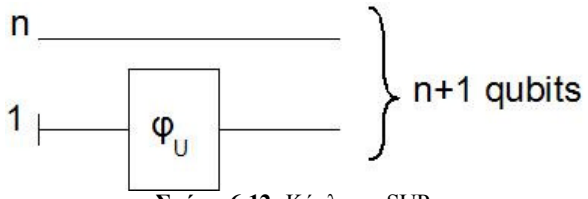


Σχήμα 6.11: Κύκλωμα VAR. Πρόκειται απλώς για "ομαδοποίηση" των καλωδίων του τύπου τ, μια αναδιάταξη.

6.6.3 Κανόνας SUP

$$\frac{|\boldsymbol{\lambda}|^{\boldsymbol{2}} + |\boldsymbol{\lambda}'|^{\boldsymbol{2}} = \boldsymbol{1}}{\boldsymbol{\Gamma};\boldsymbol{n} \vdash^{\circ} \{(\boldsymbol{\lambda})\boldsymbol{qfalse} + (\boldsymbol{\lambda}')\boldsymbol{qtrue}\}:\boldsymbol{qbit}[\boldsymbol{n}];\boldsymbol{1}} \quad (\boldsymbol{SUP})$$

Αυτός ο κανόνας δημιουργεί το μόνο κύκλωμα της γλώσσας το οποίο δεν απαιτεί να έχει προηγηθεί κατασκευή υπό-κυκλωμάτων, δηλαδή αποτελεί το πρωταρχικό στοιχείο των κυκλωμάτων της γλώσσας από το οποίο κατασκευάζονται όλα τα προγράμματα. Το κύκλωμα δουλεύει αρχικοποιώντας ένα qubit στην κατάσταση $|\boldsymbol{0}\rangle$ και μετά εφαρμόζοντας πάνω σε αυτό ένα μετασχηματισμό περιστροφής που το φέρνει στη ζητούμενη υπέρθεση. Τα συνολικά qubits του κυκλώματος αυξάνονται κατά 1 και δεν υπάρχουν σκουπίδια όπως υποδηλώνει και το $\vdash^{\circ}$ στον κανόνα.



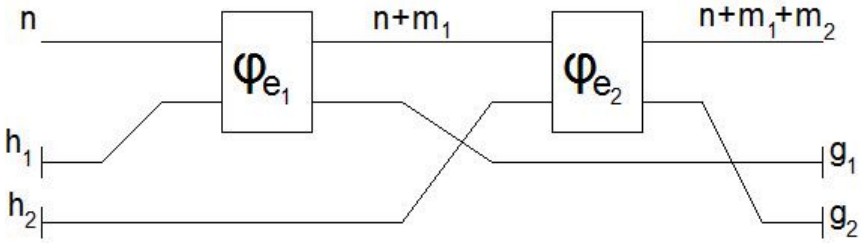
Σχήμα 6.12: Κύκλωμα SUP

$$U = \begin{pmatrix} \lambda & \lambda' \\ \lambda' & -\lambda \end{pmatrix}$$

6.6.4 Κανόνας LET

$$\frac{\Gamma; n \vdash^{\alpha} e_1 : \tau_1; m_1 \qquad \Gamma, x : \tau_1; n + m_1 \vdash^{\alpha} e_2 : \tau; m_2}{\Gamma; n \vdash^{\alpha} let\ x = e_1\ in\ e_2 : \tau; m_1 + m_2} \quad (LET)$$

Σε αυτόν τον κανόνα υποθέτουμε ότι έχουν δημιουργηθεί εκ των προτέρων τα κυκλώματα για τον υπολογισμό των εκφράσεων e_1 και e_2. Καθώς ο κανόνας δεν καθορίζει αν οι υπολογισμοί αυτοί είναι αγνοί ή όχι (αν δεν γίνονται μετρήσεις) θεωρώ την γενική περίπτωση και κάθε υπό-κύκλωμα εισάγεται με σωρό και με σκουπίδια. Φυσικά κάποιο από τα δύο σύνολα ή και τα δύο μπορεί να είναι κενά. Το κύκλωμα υπολογίζει πρώτα την έκφραση e_1 και έπειτα την έκφραση e_2. Μέσα στην έκφραση e_2 όπου εμφανίζεται η μεταβλητή x θεωρούμε ότι καλείται ο κανόνας VAR και τα καλώδια που αποτελούν τον τύπο της x (ίδιος με της e_1) αναδιατάσσονται κατάλληλα. Οι αριθμοί των qubit στα δεξιά και αριστερά μέρη των κανόνων δηλώνουν τους αριθμούς των καλωδίων τα οποία εισέρχονται και εξέρχονται αντίστοιχα από κάθε επιμέρους κύκλωμα (αυτά που εξέρχονται είναι ίσα με αυτά που εισέρχονται συν τον αριθμό στο αριστερό μέρος) χωρίς να υπολογίζουμε τα καλώδια αρχικοποιήσεων και σωρού. Το ίδιο δηλώνουν και στους υπόλοιπους κανόνες. Ουσιαστικά το κύκλωμα αποτελεί την σειριακή σύνθεση των δύο κυκλωμάτων $\varphi_{e_2} \circ \varphi_{e_1}$.

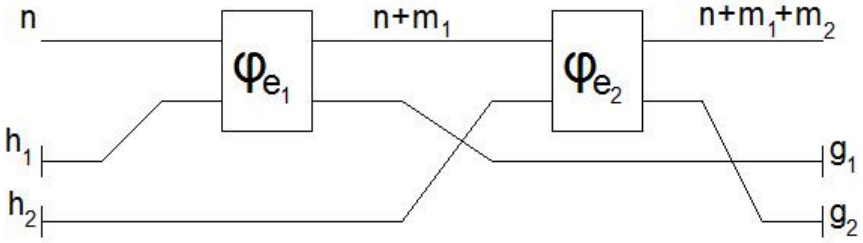


Σχήμα 6.13: Κύκλωμα LET

6.6.5 Κανόνας PROD

$$\frac{\Gamma; n \vdash^{\alpha} e_1 : \tau_1; m_1 \qquad \Gamma; n + m_1 \vdash^{\alpha} e_2 : \tau_2; m_2}{\Gamma; n \vdash^{\alpha} (e_1, e_2) : \tau_1 \otimes \tau_2; m_1 + m_2} \quad (PROD)$$

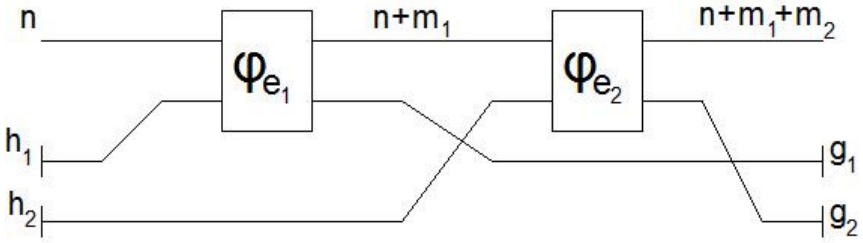
Αυτός ο κανόνας όπως και ο επόμενος είναι εντελώς παρόμοιοι με το προηγούμενο κύκλωμα όπως άλλωστε αναφέραμε και όταν δηλώναμε τη σημασιολογία της γλώσσας με πίνακες πυκνότητας. Είναι η σύνθεση $\varphi_{e_2} \circ \varphi_{e_1}$ και οι μόνες διαφορές είναι στις αναδιατάξεις των καλωδίων ανάλογα με τους υπολογισμούς που πρέπει να εκτελεστούν στις επόμενες εκφράσεις. Προφανώς ο compiler της γλώσσας θα πρέπει να αποθηκεύει τους τύπους κάθε μεταβλητής και να κατασκευάζει έπειτα τα κατάλληλα κυκλώματα καλωδιώσεων-αναδιατάξεων κατά την κλήση του κανόνα VAR.



Σχήμα 6.14: Κύκλωμα PROD

6.6.6 Κανόνας LETPROD

$$\frac{\Gamma; n \vdash^{\alpha} e_1 : \tau_1 \otimes \tau_2; m_1 \qquad \Gamma, x_1 : \tau_1, x_2 : \tau_2; n + m_1 \vdash^{\alpha} e_2 : \tau; m_2}{\Gamma; n \vdash^{\alpha} let\ (x_1, x_2) = e_1\ in\ e_2 : \tau; m_1 + m_2} \quad (LETPROD)$$



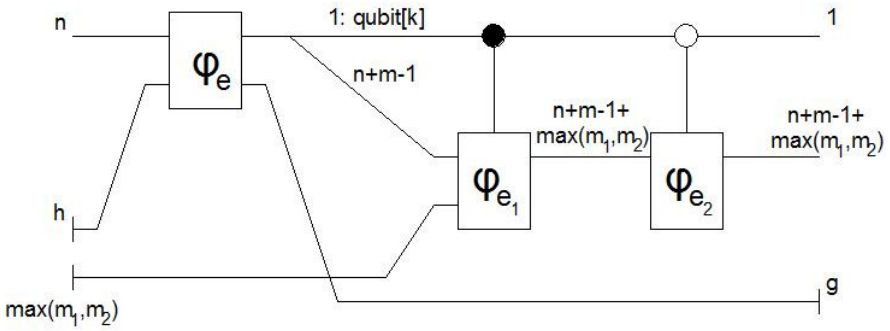
Σχήμα 6.15: Κύκλωμα LETPROD

6.6.7 Κανόνας IF

$$\frac{\begin{array}{c}\Gamma; n \vdash^{\alpha} e : qbit[k]; m \\ \Gamma|_k; n + m \vdash^{\circ} e_1 : \tau; m_1 \qquad \Gamma|_k; n + m \vdash^{\circ} e_2 : \tau; m_2\end{array}}{\Gamma; n \vdash^{\alpha} if\ e\ then\ e_1\ else\ e_2 : \tau; m + \max(m_1, m_2)} \quad (IF)$$

Στο κύκλωμα αυτού του κανόνα πρώτα υπολογίζεται η έκφραση e· αυτή μπορεί να απαιτεί m qubit για τον υπολογισμό της, αλλά ο τελικός της τύπος πρέπει να είναι ένα μόνο qubit. Προσέξτε ότι τα υπόλοιπα qubit δεν είναι απαραίτητο να αποδεσμευτούν μαζί με τα (πιθανά) σκουπίδια της έκφρασης. Έπειτα υπολογίζονται οι δύο εκφράσεις e_1 και e_2 οι οποίες όμως έχουν τον περιορισμό να μην χρησιμοποιούν καθόλου το qubit του τύπου της έκφρασης e και να είναι αγνές, δηλαδή να μην παράγουν σκουπίδια. Ο πρώτος περιορισμός φαίνεται στο κύκλωμα ξεχωρίζοντας το qubit και περνώντας το ως qubit ελέγχου στη δομή εκτέλεσης υπό συνθήκη.
Τέλος πρέπει να παρατηρήσουμε ότι τα επιπλέον qubit που μπορεί να χρησιμοποιεί η e_1, τα m_1 καλώδια, είναι δυνατόν να τα χρησιμοποιεί και η e_2. Αυτό δεν αποτελεί πρόβλημα για τη λειτουργία του κυκλώματος καθώς υπό συνθήκη εκτέλεση εξασφαλίζει ότι κάθε κοινό qubit θα μεταβληθεί στο ποσοστό που του αναλογεί από την υπέρθεση του qubit ελέγχου. Ίσως ο πιθανός προγραμματιστής της γλώσσας θα πρέπει να προσέξει τους τύπους που δίνει στις μεταβλητές ώστε να παράγει το αποτέλεσμα που πράγματι θέλει. Για παράδειγμα αν χρησιμοποιεί την e_2 ως συνάρτηση ανεξάρτητη της e_1 πρέπει να προσέξει οι νέοι τύποι να μην μπλέκονται με ήδη δηλωμένους τύπους

και άρα να αλλάξει τον κώδικά της (ουσιαστικά ορίζοντας πάντα νέα qubits-μεταβλητές).



Σχήμα 6.16: Κύκλωμα IF

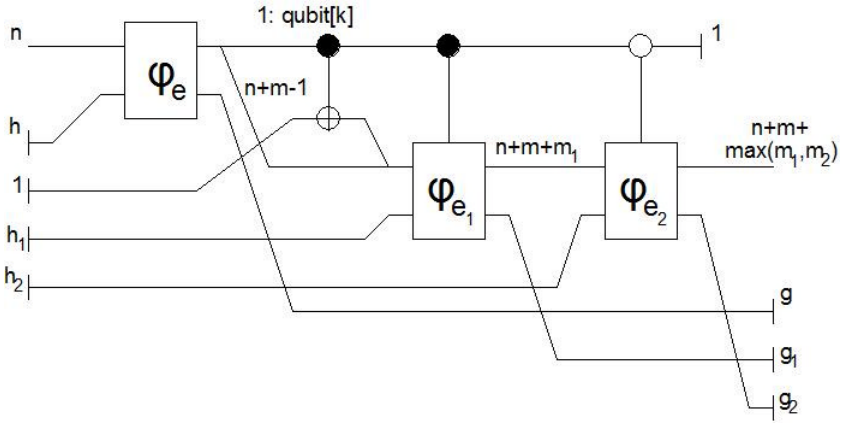
6.6.8 Κανόνας IFM

$$\frac{\boldsymbol{\Gamma; n \vdash e: qbit[k]; m} \quad \boldsymbol{\Gamma; n+m \vdash e_1: \tau; m_1} \quad \boldsymbol{\Gamma; n+m \vdash e_2: \tau; m_2}}{\boldsymbol{\Gamma; n \vdash ifm\ e\ then\ e_1\ else\ e_2: \tau; m + \max(m_1, m_2)}} \quad (\boldsymbol{IFM})$$

Ο κανόνας αυτός είναι όμοιος με τον κανόνα IF με τις διαφορές ότι επιτρέπονται και μη αγνές εκφράσεις στους δύο κλάδους, ότι οι δύο κλάδοι μπορούν να χρησιμοποιούν το qubit ελέγχου και ότι το qubit ελέγχου μετράται στο τέλος του κυκλώματος. Η πρώτη διαφορά φαίνεται από τα καλώδια σκουπιδιών των δύο εκφράσεων $\boldsymbol{e_1}$ και $\boldsymbol{e_2}$.

Όσον αφορά τη δεύτερη διαφορά, για να μπορούν να χρησιμοποιούν οι δύο κλάδοι το qubit ελέγχου πρέπει ιδανικά να το διπλασιάσουμε ώστε να χρησιμοποιείται και στο άνω καλώδιο ελέγχου και μέσα στα υπό-κυκλώματα ταυτόχρονα. Κάτι τέτοιο όμως παραβαίνει το θεώρημα «μη αντιγραφής» και το καλύτερο που μπορούμε να κάνουμε είναι να αρχικοποιήσουμε ένα νέο qubit και να το αντιστρέψουμε με μία πύλη CNOT που ελέγχεται από το qubit ελέγχου. Φυσικά κάτι τέτοιο όπως έχουμε δει δημιουργεί δύο συζευγμένα qubit και όχι δύο ανεξάρτητα, όμως αυτό δεν επηρεάζει την ορθή λειτουργία του κυκλώματος. Αυτό συμβαίνει λόγω της τρίτης διαφοράς που είναι η μέτρηση του qubit ελέγχου στο τέλος του κυκλώματος. Αυτή εξαναγκάζει το qubit ελέγχου να μεταβεί σε κλασική κατάσταση και επομένως και το νέο qubit να μεταβεί στην ίδια κατάσταση αφού είναι συζευγμένα. Συνεπώς το qubit ελέγχου της κλασικής κατάστασης μπόρεσε να αντιγραφεί επιτυχώς και καθώς σε αυτό το if επιθυμούμε κλασικό έλεγχο και όχι κβαντικό όπως στο προηγούμενο το κύκλωμα εκτελεί ακριβώς τη ζητούμενη λειτουργία. Μια λεπτομέρεια αυτής της κατασκευής είναι ότι ο compiler της γλώσσας πρέπει να δώσει στο νέο qubit τύπο $\boldsymbol{qbit[k]}$ και όποτε χρειάζεται σε περαιτέρω υπολογισμούς να χρησιμοποιεί σταθερά ένα από τα δύο qubit· και τα δύο θεωρούνται κλειδωμένα στην ίδια κλασική κατάσταση.

Παρατηρούμε ότι αυτό το κύκλωμα είναι το μόνο που δημιουργεί κλάδο σκουπιδιών και άρα όλοι οι πιθανοί κλάδοι σκουπιδιών των υπό-κυκλωμάτων της γλώσσας προέρχονται από μια τέτοια εντολή. Επίσης μόνο η εντολή IFM και η SUP δημιουργούν νέες μεταβλητές και άρα όλα τα καλώδια σωρού προέρχονται από μία από τις δύο αυτές εντολές.



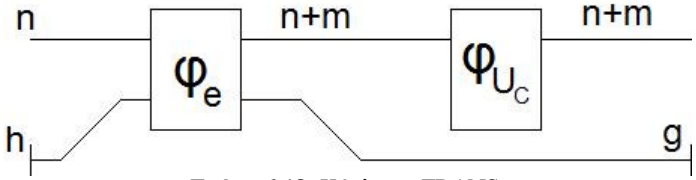
Σχήμα 6.17: Κύκλωμα IFM

6.6.9 Κανόνας TRANS

$$\frac{\Gamma; n \vdash^{\alpha} e : \tau; m \quad pure(\tau) \quad x : \mathrm{C}(\tau), x' : \mathrm{C}(\tau) \vdash c : complex}{\Gamma; n \vdash^{\alpha} |e\rangle \to x, x'.\, c : \tau; m} \quad (TRANS)$$

Τελευταίος είναι ο κανόνας TRANS που εφαρμόζει έναν οποιονδήποτε ορθομοναδιαίο μετασχηματισμό σε ένα σύνολο από qubits. Αρχικά υπολογίζει την έκφραση e και έπειτα στα qubits της έκφρασης που προέκυψαν εφαρμόζει το μετασχηματισμό. Προφανώς αυτή η εντολή υπερκαλύπτει όλες τις προηγούμενες αφού μπορεί να εφαρμόσει οποιονδήποτε μετασχηματισμό σε οποιονδήποτε αριθμό qubit (οι μετρήσεις δεν μπορούν να εκτελεστούν αλλά μπορούμε να τις εκτελέσουμε στο τέλος). Το κύκλωμα είναι τετριμμένο, αλλά δεν είναι καθόλου χρήσιμο.

Ο λόγος είναι προφανώς η αυθαίρετη πολυπλοκότητα της εντολής. Καταρχήν το κύκλωμα του μετασχηματισμού δεν ανήκει εν γένει στην κλάση FQC . Αυτό διότι η κλάση αυτή περιέχει μετασχηματισμούς μονού qubit και συνθέσεις τους· όχι τυχαίου αριθμού qubit. Για να ανήκει πρέπει να προσεγγίσουμε το μετασχηματισμό με ένα πεπερασμένο πλήθος πυλών μονού qubit, κάτι το οποίο όπως είπαμε στην ενότητα των κβαντικών κυκλωμάτων έχει εκθετική πολυπλοκότητα. Μάλιστα μόνο και μόνο για να υπολογιστεί ο πίνακας μετασχηματισμού (σε αυτή τη μορφή δίνεται στον compiler) απαιτείται εκθετικός αριθμός λειτουργιών ως προς τον αριθμό των qubit. Αν αναπτυχθεί compiler για την πλήρη γλώσσα nQML, δηλαδή που να επιτρέπει μετασχηματισμούς αυθαίρετου αριθμού qubit, τότε η μετάφραση θα γίνεται σε εκθετικό χρόνο. Προφανώς θα πρέπει να προστεθούν επιπλέον περιορισμοί σε αυτή την εντολή (π.χ. να επιτρέπονται μόνο μετασχηματισμοί ενός qubit) ώστε να αποφευχθεί η απαράδεκτη αυτή λειτουργία.



Σχήμα 6.18: Κύκλωμα TRANS

7 Συμπεράσματα

7.1 Συνεισφορά

Η συνεισφορά της εργασίας και τα συμπεράσματα που προέκυψαν είναι τα παρακάτω:

- Υλοποιήθηκαν τα κβαντικά κυκλώματα για τη γλώσσα nQML, γεγονός που επιτρέπει την καλύτερη κατανόηση των χαρακτηριστικών της γλώσσας και κατ' επέκταση των προγραμμάτων που γράφονται σε αυτήν. Ουσιαστικά πρόκειται για μοντελοποίηση της γλώσσας στο φυσικό επίπεδο, όπου φαίνονται οι φυσικές διεργασίες που πρέπει να εκτελεστούν στα κβαντικά σωματίδια ώστε να εκτελεστεί το πρόγραμμα.
- Υλοποιήθηκε πρόγραμμα που κάνει την μετάφραση σε κυκλώματα και μας έδωσε μια ιδέα της δομής ενός compiler κβαντικής γλώσσας, καθώς τα κυκλώματα αποτελούν τη «γλώσσα μηχανής» ενός κβαντικού συστήματος, που θα είναι ο κβαντικός υπολογιστής.
- Παρατηρήθηκε η έλλειψη χρήσιμων κβαντικών αλγορίθμων, οι οποίοι θα βοηθούσαν στον καλύτερο έλεγχο της υλοποίησης των κυκλωμάτων, αλλά θα έδιναν και καλύτερη κατανόηση όσον αφορά την εκφραστικότητα της γλώσσας και τις δυνατότητες του κβαντικού μοντέλου.

7.2 Μελλοντική έρευνα

Η βασική κατεύθυνση έρευνας η οποία διαφαίνεται από το τελευταίο συμπέρασμα είναι η κατασκευή περισσότερων και χρήσιμων κβαντικών αλγορίθμων. Μόνο με αυτό τον τρόπο θα γίνει η εξοικείωση με το κβαντικό μοντέλο υπολογισμού και θα μπορέσουμε κατανοήσουμε την εκφραστικότητα μιας συγκεκριμένης γλώσσας προγραμματισμού. Φυσικά κάτι τέτοιο είναι πολύ δύσκολο καθώς το ίδιο το φυσικό μοντέλο στο οποίο βασίζονται οι κβαντικοί υπολογισμοί. Επίσης είναι απαραίτητο να δημιουργηθεί μια καλή βιβλιοθήκη αλγορίθμων για να αξιολογηθούν οι δυνατότητες των κβαντικών υπολογισμών.

Όσον αφορά στην γλώσσα nQML θα μπορούσαν να προστεθούν επιπλέον δομές οι οποίες δίνουν μεγαλύτερη εκφραστικότητα στα προγράμματα και θα πλησιάζουν τις κλασικές γλώσσες προγραμματισμού χωρίς όμως να παραβιάζονται οι νόμοι της κβαντομηχανικής. Τέτοιες δομές είναι η κλήση συναρτήσεων, οι βρόχοι και η αναδρομή. Είδαμε ότι αυτά τα χαρακτηριστικά υπάρχουν σε άλλες γλώσσες, όπως η QPL, οι οποίες όμως έχουν λιγότερες δυνατότητες σε άλλους τομείς. Η προσθήκη τέτοιων δομών αποτελεί πρόκληση για την nQML καθώς θα πρέπει να γίνει πολύ προσεκτικά ώστε να μην υπάρχουν παρενέργειες ανάμεσα στα qubit και ταυτόχρονα να είναι εύκολη η χρήση τους από τον προγραμματιστή. Ακόμη μπορούν να προστεθούν τύποι δεδομένων υψηλότερου επιπέδου, σε αντιστοιχία με τις κλασικές γλώσσες, όπως κβαντικοί τύποι ακεραίων και πράξεις ανάμεσα τους.

Τα παραπάνω αποτελούν προκλήσεις και για την κατασκευή κυκλωμάτων. Για παράδειγμα ξέρουμε ότι στα κβαντικά κυκλώματα απαγορεύεται η ανάδραση και άρα λειτουργίες όπως η αναδρομή πρέπει να υλοποιηθούν πολύ προσεκτικά. Με την εισαγωγή κβαντικού ελέγχου και δομών υψηλότερου επιπέδου προκύπτουν και εννοιολογικές δυσκολίες καθώς θα ήταν δυνατόν να δημιουργηθούν για παράδειγμα λίστες qubit που είναι υπέρθεση μιας λίστας με μήκος ένα και μίας με μήκος δύο. Κάτι

τέτοιες δομές θα πρέπει να υλοποιούνται με φυσικά-εφικτό τρόπο στα κβαντικά κυκλώματα. Τέλος θα ήταν χρήσιμο να υλοποιηθούν κβαντικά κυκλώματα που υλοποιούν χρήσιμες κβαντικές λειτουργίες, όπως αθροιστές, πολλαπλασιαστές κτλ. κβαντικών ακεραίων. Δυστυχώς μια τέτοια κατεύθυνση έχει τη δυσκολία ότι δε γνωρίζουμε ακόμα ποιες είναι οι χρήσιμες λειτουργίες των κβαντικών αλγορίθμων εξαιτίας της σπανιότητας τους.

Τέλος η βασικότερη κατεύθυνση έρευνας σχετική με τους κβαντικούς υπολογισμούς είναι η κατασκευή ενός κβαντικού υπολογιστή. Παρόλο που και στο κλασικό μοντέλο υπολογισμού η θεωρητική εργασία είχε υλοποιηθεί πριν την εξέλιξη των υπολογιστών, η έκρηξη στις γλώσσες προγραμματισμού έγινε στις τελευταίες δεκαετίες όπου οι υπολογιστές έγιναν γρηγορότεροι και έτρεχαν μεγαλύτερα προγράμματα. Τότε εμφανίστηκε η ανάγκη για εκφραστικές γλώσσες προγραμματισμού. Όπως είδαμε στην εισαγωγή αυτές οι προσπάθειες προχωρούν με αρκετά αργό ρυθμό και με περιορισμένα αποτελέσματα.

Βιβλιογραφία

1. **Feynman, Richard P.** Simulating physics with computers. *International Journal of Theoretical Physics 21:6/7.* 1982, pp. 467-468.
2. **Benioff, P. A.** Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: application to Turing machines. *International Journal of Theroretical Physics 21:3/4.* 1982, pp. 177-202.
3. *Quantum theory, the Church-Turing principle and the universl quantum computer.* **Deutsch, David.** 1985. Proceedings of the Royal Sociaety of London A 400. pp. 97-117.
4. **Bernstein, Ethan and Vazirani, Umesh.** Quantum complexity theory. *SIAM Journal of Computing 26:5.* 1997, pp. 1411-1473.
5. *Algorithms for quantum computation: discrete log and factoring.* **Shor, Peter W.** 1994. Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science - FOCS. pp. 20-22.
6. **Shor, Peter W.** Scheme for reducing decoherence in quantum computer memory. *Physical Review A 52:4.* 1995, pp. 2493-2496.
7. **Selinger, Peter.** Towads a Quantum Programming Language. *Mathematical Structures in Computer Science.* 2004, Vol. 14, 4, pp. 527-586.
8. **Grattage, Jonathan and Altenkirch, Thorsten.** *QML: Quantum data and control.* February 2005.
9. —. *A compiler for a functional quantum programming language.* January 2005.
10. **Lampis, Michael, et al.** Quantum data and control made easier. *Elsevier Science B.V.* 2006.
11. **Grattage, Jonathan James.** A functional quantum programmign language. *Thesis submitted to the University of Nottingham.* September 2006.
12. **Nielsen, Michael A. and Chuang, Isaac L.** *Quantum Computation and Quantum Information.* s.l. : Cambridge University Press, 2000.
13. **Hirvensalo, Mika.** *Quantum Computing.* s.l. : Springer, 2001.
14. **Kaye, Phillip, Laflamme, Raymond and Mosca, Michele.** *An Introduction to Quantum Computing.* s.l. : Oxford University Press, 2007.