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

Κβαντικοί Υπολογισμοί και Κβαντικός Προγραμματισμός

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΒΡΕΤΤΟΣ Ε. ΜΟΥΛΟΣ

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

Αθήνα, Ιούλιος 2014

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

Κβαντικοί Υπολογισμοί και Κβαντικός Προγραμματισμός

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΒΡΕΤΤΟΣ Ε. ΜΟΥΛΟΣ

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

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 11η Ιουλίου 2014.

.....	.....	.....
Νικόλαος Παπασπύρου Αν. Καθηγητής Ε.Μ.Π.	Κωστής Σαγώνας Αν. Καθηγητής Ε.Μ.Π.	Ευστάθιος Ζάχος Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2014

Βρεττός Ε. Μουλός

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Ο σκοπός αυτής της διπλωματικής εργασίας είναι η μελέτη των κβαντικών υπολογισμών υπό το πρίσμα των κβαντικών γλωσσών προγραμματισμού. Στα πλαίσια αυτά εξετάσαμε την γλώσσα κβαντικού προγραμματισμού nQML και προχωρήσαμε στην προσθήκη ενός νέου τελεστή ο οποίος αντλεί στοιχεία από τον παράλληλο προγραμματισμό και τις κλασικές συναρτήσεις και προσπαθεί να τα προσαρμόσει στο κβαντικό μοντέλο υπολογισμού και την κβαντική εκδοχή του παραλληλισμού. Ο τελεστής αυτός εντάχθηκε ομαλά στην ήδη υπάρχουσα γλώσσα επεκτείνοντας το συντακτικό, το σύστημα τύπων και την σημασιολογία της. Επιπλέον, ορίσαμε μία νέα σημασιολογία για την γλώσσα η οποία βρίσκεται πολύ κοντά στο μαθηματικό μοντέλο των κβαντικών υπολογισμών, βοηθώντας έτσι στην κατανόηση της λειτουργίας της nQML αλλά και των κβαντικών υπολογισμών αυτών καθ αυτών. Η συνάρτηση που αποδίδει σημασία στις εκφράσεις της nQML υλοποιήθηκε σε Haskell και αυτή η υλοποίηση μας χρησίμευσε στο να υπολογίζουμε εύκολα και γρήγορα τις σημασίες εκφράσεων της nQML και να ελέγχουμε αν όντως ταιριάζουν με τα θεωρητικά αποτελέσματα. Τέλος, διατυπώσαμε τον αλγόριθμο του Shor σε nQML και παίρνοντας την σημασία του οδηγηθήκαμε στην σωστή παραγοντοποίηση του αριθμού 15.

Λέξεις κλειδιά

Κβαντικοί υπολογισμοί, κβαντικός προγραμματισμός, nQML, κβαντικός παραλληλισμός, σημασιολογία, αλγόριθμος Shor.

Abstract

The purpose of this diploma dissertation, is to study the quantum computations under the framework of quantum programming languages. Thus, we studied the quantum programming language nQML and we proceeded by adding a new operator, which incorporates elements from parallel programming and classical functions by adjusting them to the quantum computations model and the quantum version of parallelism. This operator was integrated normally in the pre-existing language by expanding its syntax, type system and semantics. Moreover, we defined a new semantics for this language which is very close to the mathematical model of quantum computations, thus helping comprehension of nQML functionality along with quantum computations by themselves. The function which interprets nQML's expressions was implemented in Haskell and this was useful in order to easily and rapidly calculate the meanings of different nQML expressions and to check whether they actually correspond to the theoretical results. Finally, we formulated Shor's algorithm in nQML and by computing its meaning we managed to correctly factor the number 15.

Key words

Quantum computations, quantum programming, nQML, quantum parallelism, semantics, Shor's algorithm.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα της εργασίας και καθηγητή μου κ. Νίκο Παπασπύρου για όλα αυτά που μου έμαθε όσο ήμουν στο πολυτεχνείο αλλά και για τον δρόμο που δείχνει ως άνθρωπος. Ευχαριστώ ακόμα τον καθηγητή κ. Στάθη Ζάχο για το εξαιρετικό έργο που προσφέρει στους φοιτητές οργανώνοντας χρόνια τώρα την εκπαίδευση τους γύρω από την θεωρητική πληροφορική. Οι γονείς μου επίσης έπαιξαν καθοριστικό ρόλο στην εκπαίδευση μου και στην στροφή μου προς τις θετικές επιστήμες για αυτό και τους ευχαριστώ. Τέλος, θέλω να ευχαριστήσω τους φίλους μου για τις όμορφες στιγμές που περάσαμε παρέα.

Βρεττός Ε. Μουλός,

Αθήνα, 11η Ιουλίου 2014

Η εργασία αυτή είναι επίσης διαθέσιμη ως Τεχνική Αναφορά CSD-SW-TR-3-2014, Εθνικό Μετσόβιο Πολυτεχνείο, Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών, Εργαστήριο Τεχνολογίας Λογισμικού, Ιούλιος 2014.

URL: `http://www.softlab.ntua.gr/techrep/`
FTP: `ftp://ftp.softlab.ntua.gr/pub/techrep/`

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Σκοπός αυτής της εργασίας είναι η μελέτη του κβαντικού μοντέλου υπολογισμού από την σκοπιά των κβαντικών γλωσσών προγραμματισμού. Ο κβαντικός προγραμματισμός εξ αιτίας των ιδιαίτερων χαρακτηριστικών που ενσωματώνει είναι πολύ ισχυρός αλλά ταυτόχρονα και δύσχρηστος. Στην κατεύθυνση αυτή γίνεται μία προσπάθεια εξομάλυνσης των δυσκολιών μέσω της εισαγωγής ενός κβαντικού τελεστή ο οποίος αντλεί στοιχεία από τον κλασικό παράλληλο προγραμματισμό. Στα πλαίσια αυτά μελετάται εκτενώς η γλώσσα κβαντικού προγραμματισμού nQML. Εξετάζουμε το συντακτικό της, το σύστημα τύπων της και δίνουμε ερμηνείες στις εκφράσεις της. Οι δύο ερμηνείες της nQML που παρουσιάζονται σε αυτή την εργασία έχουν επίσης υλοποιηθεί σε Haskell. Τέλος, αναλύουμε μερικούς βασικούς κβαντικούς αλγορίθμους και τους υλοποιούμε στην nQML προκειμένου να την δοκιμάσουμε ως γλώσσα προγραμματισμού στην πράξη.

1.1 Ιστορία του κβαντικού μοντέλου υπολογισμού

Η αρχή λειτουργίας ενός κβαντικού υπολογιστή βασίζεται στη κβαντομηχανική γεγονός που του δίνει την δυνατότητα να υπολογίζει συναρτήσεις με έναν εντελώς διαφορετικό τρόπο σε σχέση με έναν συνηθισμένο υπολογιστή ο οποίος λειτουργεί με βάση την κλασική φυσική. Ένα από τα σημαντικότερα πλεονεκτήματα ενός κβαντικού υπολογιστή είναι η δυνατότητα του να διενεργεί υπολογισμούς ενώ βρίσκεται σε κβαντική υπέρθεση, δηλαδή σε πολλές καταστάσεις ταυτόχρονα. Αξίζει όμως να σημειωθεί ότι ο κβαντικός υπολογιστής δεν επηρεάζει την κλάση των υπολογίσιμων συναρτήσεων, παρά μόνο υπολογίζει αποδοτικότερα ορισμένες συναρτήσεις σε σχέση με έναν κλασικό υπολογιστή.

Η ιδέα του κβαντικού υπολογιστή πρωτοεμφανίστηκε την δεκαετία του 80 από τον Feynman ο οποίος παρατήρησε ότι δεν μπορούσε να προσομοιώσει αποδοτικά κβαντικά συστήματα με συμβατικούς υπολογιστές και μάλιστα ότι η επιβράδυνση της προσομοίωσης αυξανόταν εκθετικά με το μέγεθος του συστήματος που έπρεπε να προσομοιωθεί. Έτσι λοιπόν πρότεινε τον κβαντικό υπολογιστή, έναν υπολογιστή ο οποίος θα βάσιζε την λειτουργία του ακριβώς σε αυτές τις φυσικές διαδικασίες που ήταν δύσκολο να προσομοιωθούν. Προς επιβεβαίωση του Feynman, ο Deutsch παρουσίασε τους πρώτους κβαντικούς αλγορίθμους οι οποίοι έδειχναν την υπεροχή του κβαντικού υπολογιστή.

Το 1994 ο Peter Shor διατύπωσε έναν κβαντικό αλγόριθμο για την παραγοντοποίηση αριθμών ο οποίος είναι εκθετικά ταχύτερος σε σχέση με οποιονδήποτε κλασικό αλγόριθμο για την παραγοντοποίηση γνωρίζουμε σήμερα. Το πρόβλημα της παραγοντοποίησης ανήκει στην κλάση πολυπλοκότητας NP, ενώ πιστεύεται ότι δεν ανήκει στην κλάση πολυπλοκότητας P και ως εκ τούτου θεωρείται πρακτικά μη επιλύσιμο. Για το λόγο αυτό, η παραγοντοποίηση και άλλα παρόμοια προβλήματα, όπως ο υπολογισμός διακριτού λογαρίθμου και η εύρεση της τάξης ενός στοιχείου, αποτελούν την βάση των σύγχρονων κρυπτοσυστημάτων, συμπεριλαμβανομένου και του ευρέος χρησιμοποιούμενου RSA. Γίνεται φανερό λοιπόν, πως αν κατασκευαστεί ένας κβαντικός υπολογιστής τότε με χρήση του αλγορίθμου παραγοντοποίησης του Shor πολλά από τα σύγχρονα κρυπτοσυστήματα θα αχρηστευθούν καθώς θα είμαστε σε θέση να αποκρυπτογραφήσουμε τα κρυπτοκείμενα τους σε πολυωνυμικό χρόνο.

Δύο χρόνια αργότερα, το 1996, ο Lov Grover εφηύρε έναν κβαντικό αλγόριθμο για γρήγορη αναζήτηση σε μια αταξινόμητη βάση δεδομένων. Ο αλγόριθμος του Grover είναι μονάχα πολυωνυμικά ταχύτερος από τους κλασικούς αλγόριθμους αναζήτησης, όμως είναι αποδεδειγμένα ταχύτερος από

τον καλύτερο κλασικό αλγόριθμο αναζήτησης σε αντίθεση με τον αλγόριθμο του Shor του οποίου η υπεροχή στηρίζεται στην υπόθεση ότι η παραγοντοποίηση είναι ένα υπολογιστικά δύσκολο πρόβλημα. Συνεπώς ο αλγόριθμος του Grover αποτελεί και μια θεωρητική επιβεβαίωση της υπεροχής ενός κβαντικού υπολογιστή έναντι ενός κλασικού υπολογιστή. Ο αλγόριθμος του Grover επιτυγχάνει τετραγωνική αύξηση στην ταχύτητα σε σχέση με τον καλύτερο κλασικό αλγόριθμο αναζήτησης, ο οποίος αποτελεί μια εξαντλητική αναζήτηση. Η αναζήτηση αποτελεί την βάση πολλών προβλημάτων της κλάσης NP και συνεπώς αν είχαμε στην διάθεση μας το κβαντικό hardware ώστε να αντικαταστήσουμε τον κλασικό αλγόριθμο αναζήτησης με τον αλγόριθμο του Grover τότε αυτομάτως θα βλέπαμε τρομερή επιτάχυνση στις εφαρμογές που τρέχουμε καθημερινά στους υπολογιστές μας.

Τόσο ο αλγόριθμος του Shor όσο και ο αλγόριθμος του Grover φανερώνουν το μεγάλο κέρδος σε απόδοση που μπορούμε να πάρουμε με την χρήση ενός κβαντικού υπολογιστή. Όμως προς το παρόν δεν υπάρχει κβαντικός υπολογιστής που να διαθέτει αξιόλογο αριθμό από κβαντικά bits ώστε να τρέξει χρήσιμους υπολογισμούς. Η μεγαλύτερη δυσκολία στην κατασκευή ενός κβαντικού υπολογιστή ο οποίος θα είναι σε θέση να λύνει προβλήματα ευρείας κλίμακας ανακύπτει από δύο αντικρουόμενες προϋποθέσεις. Από τη μία η μνήμη ενός κβαντικού υπολογιστή θα πρέπει να είναι όσο πιο απομονωμένη γίνεται για να προστατευθεί από την καταστροφική αλληλεπίδραση με το περιβάλλον. Από την άλλη η κβαντική κεντρική μονάδα επεξεργασίας δεν πρέπει να είναι εντελώς απομονωμένη, αφού οι υπολογισμοί είναι συνεχείς και ένας ελεγκτής πρέπει να ελέγχει ότι κβαντικό σύστημα εξελίσσεται με τον ζητούμενο τρόπο. Παρ' όλα αυτά, πειράματα με κβαντικούς υπολογιστές λαμβάνουν διαρκώς χώρα και δείχνουν να επαληθεύουν την θεωρεία. Για παράδειγμα, το 2001 ερευνητές κατάφεραν να παραγοντοποιήσουν το 15 χρησιμοποιώντας 7 κβαντικά bits.

1.2 Γλώσσες κβαντικού προγραμματισμού

Οι κβαντικοί αλγόριθμοι συνηθίζεται να μελετούνται είτε σε πολύ χαμηλό επίπεδο υπό την μορφή κβαντικών πυλών και κυκλωμάτων είτε σε πολύ υψηλό επίπεδο με την χρήση γραμμικής άλγεβρας. Ο σκοπός μια γλώσσας κβαντικού προγραμματισμού είναι γεφυρώσει το χάσμα αυτό προσφέροντας στον προγραμματιστή έναν ενδιάμεσο τρόπο περιγραφής των αλγορίθμων. Αν κάποια στιγμή ο κβαντικός υπολογιστής γίνει πραγματικότητα και διαδοθεί ευρέως τότε δεν μπορούμε σε καμία περίπτωση να απαιτήσουμε από τους προγραμματιστές να προγραμματίζουν σχεδιάζοντας κυκλώματα ή να διαθέτουν εκτεταμένες γνώσεις γραμμικής άλγεβρας. Αντίθετα αυτό το οποίο επιθυμούμε είναι να τους προσφέρουμε μια γλώσσα κβαντικού προγραμματισμού η οποία θα θυμίζει τις κλασικές γλώσσες προγραμματισμού τόσο ως προς το συντακτικό όσο και ως προς την σημασιολογία. Το έργο αυτό δεν είναι εύκολο καθώς το κβαντικό μοντέλο υπολογισμού είναι εκ φύσεως διαφορετικό από το κλασσικό μοντέλο υπολογισμού και επιβάλλει περιορισμούς τους οποίους δεν συναντάμε στο κλασσικό μοντέλο υπολογισμού. Ένας τέτοιος περιορισμός είναι το θεώρημα της μη κλωνοποίησης της κβαντικής πληροφορίας το οποίο θα δούμε αναλυτικά σε επόμενο κεφάλαιο.

Στην κατεύθυνση αυτή έχουν προταθεί κάποιες γλώσσες κβαντικού προγραμματισμού κάθε μία από τις οποίες συμβάλλει με τον τρόπο της στην επίλυση του προβλήματος τους σχεδιασμού μιας γλώσσας κβαντικού προγραμματισμού η οποία θα μπορέσει να χρησιμοποιηθεί ευρέος όταν ο κβαντικός υπολογιστής γίνει πραγματικότητα. Στο σημείο αυτό πρέπει να τονίσω ότι η επίλυση του προβλήματος αυτού δεν επαφίεται αποκλειστικά στους σχεδιαστές των γλωσσών προγραμματισμού καθώς προκείμενου να σχεδιαστεί μια καλή γλώσσα προγραμματισμού πρέπει να είναι σαφώς προδιαγεγραμμένο το είδος των αλγορίθμων που θα διατυπώνονται μέσω της γλώσσας. Κάτι τέτοιο όμως στην περίπτωση μας δεν ισχύει, αφού το πεδίο των κβαντικών υπολογισμών δεν έχει ωριμάσει αρκετά και η γκάμα των υπαρχουσών κβαντικών αλγορίθμων είναι περιορισμένη. Συνεπώς απαραίτητη προϋπόθεσή για να δούμε πραγματικά εύχρηστες γλώσσες κβαντικού προγραμματισμού είναι να ωριμάσει κι άλλο το πεδίο των κβαντικών υπολογισμών.

Οι πρώτες γλώσσες κβαντικού προγραμματισμού που παρουσιάστηκαν ήταν προστατικές και ακολουθούσαν κάποιες συμβάσεις για την διατύπωση κβαντικών αλγορίθμων σε ψευδοκώδικα οι οποίες προτάθηκαν από τον Knill. Ο κοινός παράγοντας αυτών των γλωσσών είναι ότι αποτελούνται

από μία ακολουθία λειτουργιών που μετασχηματίζουν την κατάσταση του κβαντικού υπολογιστή. Χαρακτηριστικό παράδειγμα αυτής της κατηγορίας γλωσσών είναι η QCL, η οποία αναπτύχθηκε από τον Ömer και της οποίας η σύνταξη είναι παρόμοια με της C.

Δεν άργησαν όμως να εμφανιστούν και οι συναρτησιακές γλώσσες κβαντικού προγραμματισμού. Το χαρακτηριστικό τους είναι ότι δεν επιδρούν μετασχηματίζοντας κάποια κατάσταση, αλλά αντιστοιχούν εισόδους σε εξόδους. Η πρώτη συναρτησιακή γλώσσα κβαντικού προγραμματισμού είναι η QPL η οποία προτάθηκε από τον Sellinger. Η QPL είναι συναρτησιακή υπό την έννοια ότι δεν προκαλεί παρενέργειες. Όμως δεν αντιμετωπίζει τις συναρτήσεις ως πρώτης τάξεως πολίτες και συνεπώς δεν περιλαμβάνει υψηλής τάξης χαρακτηριστικά σαν και αυτά που μας έχουν συνηθίσει οι κλασικές συναρτησιακές γλώσσες όπως η Haskell και η ML.

Όμως πέραν της κατηγοριοποίησης ως προς το είδος της γλώσσας, μπορούμε να τις κατηγοριοποιήσουμε και ως προς το είδος της ροής ελέγχου. Πιο συγκεκριμένα η QPL βασίζεται στην αρχή 'quantum data, classical control', δηλαδή στην ιδέα ότι η εκτέλεση ενός προγράμματος ακολουθεί μια συγκεκριμένη ροή ελέγχου όπως και η εκτέλεση ενός κλασικού προγράμματος. Από την άλλη μεριά, η επίσης συναρτησιακή γλώσσα QML του Altenkirch ακολουθεί το μοντέλο 'quantum data and control', δηλαδή ο υπολογισμός μπορεί να βρίσκεται σε πολλές καταστάσεις ταυτόχρονα.

Στα πλαίσια αυτής της διπλωματικής το μοντέλο 'quantum data and control' θα είναι που θα μας απασχολήσει. Πιο συγκεκριμένα θα δούμε πως μπορούμε να το διευρύνουμε ακόμα περισσότερο και να το εκλογικεύσουμε συγκρίνοντας το με τον παράλληλο προγραμματισμό. Για τον σκοπό αυτό θα βασιστούμε στην γλώσσα κβαντικού προγραμματισμού nQML η οποία σχεδιάστηκε στο ΕΜΠ από τον Μιχάλη Λάμπη και μελετήθηκε εκ νέου από τον Γιάννη Ρουσελάκη.

1.3 Οργάνωση της εργασίας

Το υπόλοιπο της εργασίας οργανώνεται ως εξής:

- Στο κεφάλαιο 2 δίνεται ένα μαθηματικό μοντέλο για τους κβαντικούς υπολογισμούς και εξηγούνται οι βασικές αρχές που διέπουν την κβαντομηχανική.
- Στο κεφάλαιο 3 παρουσιάζεται η αρχική μορφή της γλώσσας κβαντικού προγραμματισμού nQML. Η παρουσίαση αποτελείται από το συντακτικό της γλώσσας, το σύστημα τύπων της και μία σημασιολογία των εκφράσεων της υπό την μορφή κβαντικών κυκλωμάτων.
- Στο κεφάλαιο 4 εξετάζεται μία επέκταση της nQML, με έναν τελεστή που πιθανώς να αποδειχτεί χρήσιμος και βολικός για τον κβαντικό προγραμματισμό. Η δουλεία του προηγούμενου κεφαλαίου επεκτείνεται ώστε να ενσωματώνει τον νέο τελεστή και προτείνεται μία ακόμα σημασιολογία των εκφράσεων της nQML.
- Στο κεφάλαιο 5 δίνονται τρία χαρακτηριστικά παραδείγματα κβαντικών αλγορίθμων μαζί με τις υλοποιήσεις τους σε nQML. Παρουσιάζονται ο αλγόριθμος του Deutsch-Jozsa, ο αλγόριθμος του Grover και ο αλγόριθμος του Shor.
- Στο κεφάλαιο 6 παρουσιάζονται τα συμπεράσματα που προέκυψαν από αυτή την εργασία καθώς και μελλοντικές ερευνητικές κατευθύνσεις που μπορούν να ακολουθηθούν.

Κεφάλαιο 2

Κβαντικοί υπολογισμοί

2.1 Εισαγωγή

Οι κβαντικοί υπολογισμοί στηρίζονται στις αρχές της κβαντομηχανικής η οποία μελετά τον κόσμο των στοιχειωδών σωματιδίων όπως τα ηλεκτρόνια και τα φωτόνια. Όμως η φύση στο υπό ατομικό επίπεδο είναι τελείως διαφορετική από τη διαίσθηση μας για τον φυσικό κόσμο. Έτσι και οι κβαντικοί υπολογισμοί πολλές φορές παραβιάζουν την κοινή λογική και τον τρόπο που έχουμε συνηθίσει να σκεφτόμαστε.

Παραδόξως, οι θεμελιώδεις αρχές της κβαντομηχανικής μπορούν να διατυπωθούν πολύ απλά και συνοπτικά. Το ζήτημα είναι η κατανόησή και η εφαρμογή τους. Οι βασικότερες είναι οι εξής:

- Η αρχή της υπέρθεσης η οποία εξηγεί πως ένα σωματίδιο μπορεί να βρίσκεται ταυτόχρονα ανάμεσα σε δύο καταστάσεις.
- Η αρχή της μέτρησης η οποία μιλάει για το πώς μετρώντας ένα σωματίδιο μεταβάλλεται η κατάσταση του και πόση πληροφορία μπορούμε να πάρουμε από ένα σωματίδιο.
- Η αρχή της ορθομοναδιαίας εξέλιξης η οποία κυβερνά τον τρόπο με τον οποίο τα κβαντομηχανικά συστήματά εξελίσσονται στον χρόνο.

Η αρχή της υπέρθεσης είναι αυτή που δίνει στους κβαντικούς αλγορίθμους συγκριτικό πλεονέκτημα έναντι των κλασικών. Ας αναλογιστούμε ότι διαθέτουμε ένα κλασικό bit. Τότε αυτό ανά πάσα χρονική στιγμή θα έχει μία τιμή από το σύνολο $\{0, 1\}$. Αντιθέτως, ένα κβαντικό bit, το οποίο από εδώ και πέρα θα ονομάζουμε qubit, θα βρίσκεται σε μία υπέρθεση των τιμών του συνόλου $\{0, 1\}$, δηλαδή χοντρικά θα έχει ταυτόχρονα όλες τις τιμές του συνόλου $\{0, 1\}$. Ανάλογα, n κλασικά bits θα περιγράφουν μία τιμή του συνόλου $\{0, ..., 2^n - 1\}$, ενώ n qubits θα περιγράφουν ταυτόχρονα όλες τις τιμές του συνόλου $\{0, ..., 2^n - 1\}$. Έτσι λοιπόν, ενώ η διενέργεια ενός υπολογισμού πάνω σε n κλασικά bits θα μας δώσει μονάχα ένα αποτέλεσμα, αυτό που αντιστοιχεί στην αρχική τιμή των n bits, η διενέργειά του ίδιου υπολογισμού σε n qubits θα μας δώσει μία υπέρθεση όλων των δυνατών αποτελεσμάτων του υπολογισμού από την στιγμή που ξεκινάμε με μία υπέρθεση όλων των δυνατών τιμών για τα n qubits. Όμως στην πράξη δεν διαθέτουμε πρόσβαση σε όλα τα δυνατά αποτελέσματα, αλλά μπορούμε να δούμε μονάχα ένα πραγματοποιώντας μία μέτρηση. Έτσι οι κβαντικοί αλγόριθμοι καταφεύγουν σε τεχνάσματα προκειμένου να καταφέρουν από την υπέρθεση όλων των δυνατών αποτελεσμάτων εν τέλει να μετρήσουν το αποτέλεσμα που πραγματικά τους ενδιαφέρει.

Η μέτρησή ενός qubit προκαλεί την μετάβαση του σε μία ορισμένη κατάσταση και τη κατάρρευση της υπέρθεσης ως προς το συγκεκριμένο qubit. Εκ τότε, όσες φορές και να μετρήσουμε το εν λόγω qubit θα παίρνουμε το ίδιο αποτέλεσμα. Ουσιαστικά δηλαδή από την μέτρηση και μετά το qubit συμπεριφέρεται κλασικά. Εδώ πρέπει να επισημάνουμε ότι το qubit δεν σταμάτησε να είναι ένα κβαντικό σύστημα, απλά το συγκεκριμένο μέγεθος του απέκτησε μία ορισμένη τιμή. Σύμφωνα με την αρχή της απροσδιοριστίας του Heisenberg άλλες ιδιότητες του είναι πλέον απροσδιόριστες.

Τέλος τα κβαντικά συστήματα εξελίσσονται στον χρόνο με αντιστρέψιμο τρόπο. Αυτή η παράμετρος δυσχεραίνει την κατασκευή κβαντικών αλγορίθμων, καθώς πλέον οι αλγόριθμοι θα πρέπει να είναι αντιστρέψιμες διαδικασίες πράγμα που δεν συμβαίνει απαραίτητα στους κλασικούς αλγορίθμους. Αυτό θα είναι και ένα από τα θέματα που θα εξετάσουμε στα πλαίσια αυτής της εργασίας.

2.2 Η αρχή της υπέρθεσης

Ας θεωρήσουμε ένα σύστημα με k διακριτές καταστάσεις. Για παράδειγμα, το ηλεκτρόνιο σε ένα άτομο υδρογόνου μπορεί να βρίσκεται μόνο σε διακριτά επίπεδα ενέργειας, ξεκινώντας από την θεμελιώδη κατάσταση, την πρώτη διεγερμένη κατάσταση, την δεύτερη διεγερμένη κατάσταση και ου το κάθε εξής. Η αρχή της υπέρθεσης λέει ότι ένα κβαντικό σύστημα μπορεί να βρίσκεται σε μια γραμμική υπέρθεση, με μιγαδικούς συντελεστές, όλων των δυνατών κλασικών καταστάσεων.

Θα συμβολίζουμε με $|0\rangle$ την θεμελιώδη κατάσταση ενός συστήματος και με $|1\rangle$, ..., $|k-1\rangle$ τις επόμενες καταστάσεις του συστήματος. Ο συμβολισμός αυτό ονομάζεται ket και οφείλεται στον Dirac. Αυτές είναι οι k δυνατές κλασικές καταστάσεις του ηλεκτρονίου. Σύμφωνα με την αρχή της υπέρθεσης, εν γένει, η κβαντική κατάσταση του ηλεκτρονίου θα είναι της μορφής: $a_0 |0\rangle + a_1 |1\rangle + ... + a_{k-1} |k-1\rangle$, όπου οι συντελεστές $a_0, a_1, ..., a_{k-1}$ είναι μιγαδικοί αριθμοί τέτοιοι ώστε: $\sum_{i=0}^{k-1} |a_i|^2 = 1$. Ο συντελεστής a_i καλείται και πλάτος της κατάστασης $|i\rangle$. Για παράδειγμα, αν $k = 3$ η κβαντική κατάσταση του ηλεκτρονίου θα μπορούσε να είναι:

$$|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{2} |1\rangle + \frac{1}{2} |3\rangle$$

ή

$$|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{2} |1\rangle + \frac{i}{2} |3\rangle$$

ή

$$|\psi\rangle = \frac{1+i}{\sqrt{3}} |0\rangle - \frac{1-i}{3} |1\rangle + \frac{1+2i}{3} |3\rangle$$

Η αρχή της υπέρθεσης είναι μια από τις πιο μυστηριώδεις πτυχές της κβαντομηχανικής καθώς εναντιώνεται στης διαίσθηση μας για τον φυσικό κόσμο. Μπορούμε να σκεφτόμαστε ότι το ηλεκτρόνιο δεν αποφασίζει σε ποιά κατάσταση βρίσκεται και ότι το πλάτος a_i είναι ένα μέτρο της κλίσης του προς την κατάσταση $|i\rangle$. Όμως δεν μπορούμε να δούμε το πλάτος a_i ως την πιθανότητα το ηλεκτρόνιο να βρίσκεται στη κατάσταση $|i\rangle$, καθώς το a_i μπορεί να είναι αρνητικό ή ακόμα και μιγαδικό. Η αρχή της μέτρησης θα διαλευκάνει τον ρόλο των συντελεστών a_i.

2.3 Η γεωμετρία του χώρου Hilbert

Όπως είδαμε η κβαντική κατάσταση ενός συστήματος που αποτελείται από k κλασικές καταστάσεις μπορεί να περιγραφεί από τα πλάτη $a_0, a_1, ..., a_{k-1} \in \mathbb{C}$, τα οποία πρέπει να ικανοποιούν την συνθήκη κανονικοποίησης: $\sum_{i=0}^{k-1} |a_i|^2 = 1$. Είναι φυσικό να αναπαραστήσουμε την κατάστασή του συστήματος ως ένα k-διάστατο διάνυσμα:

$$|\psi\rangle = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{pmatrix}$$

Η κανονικοποίηση των μιγαδικών συντελεστών σημαίνει ότι η κατάσταση του συστήματος είναι ένα μοναδιαίο διάνυσμα σε έναν k-διάστατο διανυσματικό χώρο που καλούμε χώρο Hilbert. Οι δύο αναπαραστάσεις για την κατάσταση ενός κβαντικού συστήματος που έχουμε δει ως τώρα είναι ισοδύνα-

μες μεταξύ τους. Αρκεί να θέσει κανείς:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, |k-1\rangle = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Η ισοδυναμία αυτή των περιγραφών φανερώνει μία γεωμετρία για τις πιθανές καταστάσεις ενός κβαντικού συστήματος: οι k διακριτές κλασικές καταστάσεις $|0\rangle, |1\rangle, ..., |k-1\rangle$ αναπαρίστανται από k μοναδιαία και ανά δύο κάθετα μεταξύ τους διανύσματα, δηλαδή αποτελούν μία βάση ενός k-διάστατου μιγαδικού διανυσματικού χώρου.

Επιπλέον ο χώρος αυτός είναι εφοδιασμένος με την πράξη του εσωτερικού γινομένου, η οποία για $|\phi\rangle = \sum_{i=0}^{k-1} a_i |i\rangle$ και $|\psi\rangle = \sum_{i=0}^{k-1} b_i |i\rangle$ ορίζεται ως:

$$\langle \phi, \psi \rangle = \sum_{i=0}^{k-1} a_i^* b_i$$

Εισαγάγουμε έναν ακόμα συμβολισμό που ονομάζεται bra και είναι το ανάστροφο συζυγές ενός ket:

$$\langle \phi | \equiv |\phi\rangle^\dagger$$

Όπως είναι αναμενόμενο από την καθετότητα μεταξύ δύο διανυσμάτων της βάσης, ισχύει ο κανόνας:

$$\langle i|j\rangle \equiv \langle i| \, |j\rangle = \delta_{ij}$$

Έτσι το εσωτερικό γινόμενο μπορεί να γραφεί και ως:

$$\langle \phi|\psi\rangle = \left(\sum_{i=0}^{k-1} a_i^* \langle i|\right) \cdot \left(\sum_{j=0}^{k-1} b_j |j\rangle\right) = \sum_{i=0}^{k-1}\sum_{j=0}^{k-1} a_i^* b_j \langle i|j\rangle = \sum_{i=0}^{k-1} a_i^* b_i$$

2.4 Η αρχή της μέτρησης

Η γραμμική υπέρθεση $|\phi\rangle = \sum_{i=0}^{k-1} a_i |i\rangle$ ανήκει στον ιδιωτικό κόσμο του ηλεκτρονίου. Η πρόσβαση σε αυτή την πληροφορία είναι πολύ περιορισμένη και δεν μπορούμε να γνωρίζουμε τα πλάτη a_i. Ο περιορισμός αυτός δεν είναι απλά τεχνικός αλλά βρίσκεται στην καρδιά του αξιώματος της μέτρησης της κβαντικής φυσικής. Μια μέτρηση σε ένα σύστημα με k καταστάσεις θα δώσει τον ακέραιο i με πιθανότητα $|a_i|^2$.

Μια σημαντική πτυχή της διαδικασίας της μέτρησης είναι ότι μεταβάλει την κατάσταση του συστήματος. Έτσι μετά από μία μέτρηση η νέα κατάσταση θα είναι ακριβώς αυτή που μετρήθηκε. Για παράδειγμα, αν το αποτέλεσμα της μέτρησης είναι j τότε το σύστημα αμέσως μετά την μέτρηση βρίσκεται στην κατάσταση $|j\rangle$. Αυτό έχει σαν συνέπεια ότι αμέσως μετά την μέτρηση δεν μπορούμε να αντλήσουμε άλλη πληροφορία για τα πλάτη a_i επαναλαμβάνοντας την μέτρηση.

2.5 Qubits

2.5.1 Δισδιάστατα κβαντικά συστήματα

Το qubit είναι ένα δισδιάστατο κβαντικό σύστημά και αποτελεί το βασικό δομικό στοιχείο που περικλείει όλες τις κβαντικές ιδιότητες. Για παράδειγμα, αν θέσουμε $k = 2$ στο άτομο του υδρογόνου τότε το ηλεκτρόνιο μπορεί να βρίσκεται στην θεμελιώδη κατάσταση ή στην πρώτη διεγερμένη κατάσταση ή σε μία υπέρθεση αυτών των δύο.

Η κατάσταση ενός qubit μπορεί να γραφεί ως ένα μοναδιαίο διάνυσμα $\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \in \mathbb{C}^2$. Ή με τον συμβολισμό του Dirac:

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \text{ με } \alpha, \beta \in \mathbb{C} \text{ και } |\alpha|^2 + |\beta|^2 = 1$$

.

Η υπέρθεση $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ ανήκει στον ιδιωτικό κόσμο του ηλεκτρονίου. Προκειμένου κάποιος παρατηρητής να μάθει την κατάσταση του ηλεκτρονίου πρέπει να διεξάγει μία μέτρηση. Η μέτρηση θα δώσει ως αποτέλεσμα ένα κλασικό bit πληροφορίας, 0 ή 1. Όμως μετά την μέτρηση η υπέρθεση καταρρέει και η νέα κατάσταση του qubit είναι ακριβώς το αποτέλεσμα της μέτρησης.

2.5.2 Κβαντικά συστήματα μεγαλύτερης διάστασης

Αρχικά ας εξετάσουμε ένα σύστημα αποτελούμενο από δύο qubits. Από την στιγμή που ένα ηλεκτρόνιο μπορεί να βρίσκεται στην θεμελιώδη ή στην πρώτη διεγερμένη κατάσταση, έχουμε ότι στην κλασική περίπτωση δύο ηλεκτρόνια βρίσκονται σε μία από τις τέσσερις καταστάσεις - $00,\ 01,\ 10,\ 11$ - και αναπαριστούν δύο bits κλασικής πληροφορίας. Από την αρχή της υπέρθεσης έχουμε ότι η κβαντική κατάσταση των δύο ηλεκτρονίων είναι μία υπέρθεση των τεσσάρων αυτών κλασικών καταστάσεων:

$$|\phi\rangle = a_{00}\,|00\rangle + a_{01}\,|01\rangle + a_{10}\,|10\rangle + a_{11}\,|11\rangle$$

όπου τα $a_{ij} \in \mathbb{C}$ και $\sum_{i=0}^{1}\sum_{j=0}^{1} |a_{ij}|^2 = 1$.

Όπως και στην περίπτωση του δισδιάστατου συστήματος, παρόλο που το σύστημα των δύο qubits περιγράφεται από τέσσερις μιγαδικούς συντελεστές το μεγαλύτερο μέρος της πληροφορίας δεν είναι προσβάσιμο μέσω της μέτρησης. Στην πραγματικότητα μια μέτρηση μπορεί να μας αποκαλύψει μονάχα δύο bits πληροφορίας. Η πιθανότητα το αποτέλεσμα της μέτρησης να είναι η συμβολοσειρά $x \in \{0,1\}^2$ ισούται με $|a_x|^2$ και επιπλέον μετά την μέτρηση η κατάσταση του συστήματος θα είναι η $|x\rangle$.

Ενδιαφέρον παρουσιάζει η περίπτωση όπου αντί να μετρήσουμε και τα δύο qubits ταυτόχρονα μετράμε, ας πούμε, μόνο το πρώτο. Σε αυτή την περίπτωση η πιθανότητα το αποτέλεσμα της μέτρησης να είναι 0 ισούται με: $|a_{00}|^2 + |a_{01}|^2$ και η νέα κατάσταση είναι η: $|\phi_{new}\rangle = \dfrac{a_{00}\,|00\rangle + a_{01}\,|01\rangle}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}$, ενώ η πιθανότητα το αποτέλεσμα της μέτρησης να είναι 1 ισούται με: $|a_{10}|^2 + |a_{11}|^2$ και η νέα κατάσταση είναι η: $|\phi_{new}\rangle = \dfrac{a_{10}\,|10\rangle + a_{11}\,|11\rangle}{\sqrt{|a_{10}|^2 + |a_{11}|^2}}$.

Ένα άλλο ερώτημα που τίθεται είναι: γνωρίζοντας τις μεμονωμένες καταστάσεις δύο qubit πως μπορούμε να υπολογίσουμε την σύνθετη κατάσταση του συνολικού συστήματος των δύο qubit? Αν $\alpha_0\,|0\rangle + \alpha_1\,|1\rangle\,,\quad \beta_o\,|0\rangle + \beta_1\,|1\rangle$ είναι οι μεμονωμένες καταστάσεις των δύο qubit τότε η συνολική τους κατάσταση είναι η: $\alpha_0\beta_0\,|00\rangle + \alpha_0\beta_1\,|01\rangle + \alpha_1\beta_0\,|10\rangle + \alpha_1\beta_1\,|11\rangle$. Πρέπει να παρατηρήσουμε ότι δεν γίνεται οποιαδήποτε υπέρθεση δύο qubit να διασπαστεί σε δύο μεμονωμένες υπερθέσεις, μία για κάθε qubit. Για παράδειγμα μπορούμε να πάρουμε την κατάσταση: $|\Phi^+\rangle = \dfrac{1}{\sqrt{2}}\,|00\rangle + \dfrac{1}{\sqrt{2}}\,|11\rangle$. Το φαινόμενο αυτό καλείται entanglement. Όταν δύο qubit είναι entangled δεν μπορούμε να προσδιορίσουμε την κατάσταση του κάθε qubit ξεχωριστά.

Μέχρι τώρα είδαμε πως μπορούμε να πάρουμε δύο δισδιάστατα συστήματα και να τα συνδυάσουμε για να πάρουμε ένα 4-διάστατο σύστημα. Θα γενικεύσουμε την διαδικασία αυτή εισάγοντας την έννοια του τανυστικού γινομένου. Ας υποθέσουμε ότι έχουμε δύο κβαντικά συστήματα, το ένα έχει k δυνατές καταστάσεις και ζει σε έναν k-διάστατο χώρο Hilbert V με ορθοκανονική βάση την $\{|i\rangle : 0 \leq i < k\}$ ενώ το άλλο έχει l δυνατές καταστάσεις και ζει σε έναν l-διάστατο χώρο Hilbert W με ορθοκανονική βάση την $\{|i\rangle : 0 \leq i < l\}$. Ο συνδυασμός των δύο αυτών συστημάτων έχει ως αποτέλεσμα ένα σύστημα με kl διακριτές καταστάσεις το οποίο ζει σε έναν kl-διάστατο χώρο Hilbert τον οποίο συμβολίζουμε με $V \otimes W$ και του οποίου η ορθοκανονική βάση

είναι η: $\{|i\rangle \otimes |j\rangle : 0 \leq i < k, 0 \leq j < l\}$. Έτσι ένα στοιχείο του $V \otimes W$ θα είναι της μορφής: $\sum_{i=0}^{k-1} \sum_{j=0}^{l-1} a_{ij} |i\rangle \otimes |j\rangle$. Όπως γίνεται φανερό το σύστημά των δύο qubit ζει στον χώρο Hilbert $\mathbb{C}^2 \otimes \mathbb{C}^2$ ο οποίος είναι ισομορφικός με τον χώρο Hilbert $\mathbb{C}^4$ και έτσι μπορούμε να γράφουμε $|00\rangle$ εννοώντας $|0\rangle \otimes |0\rangle$.

2.6 Κβαντικές πύλες και κυκλώματα

2.6.1 Κβαντικές πύλες μίας εισόδου

Η τρίτη αρχή της κβαντομηχανικής μας λέει ότι τα κβαντικά συστήματα εξελίσσονται με ορθομοναδιαίο τρόπο στον χρόνο. Γεωμετρικά ένας ορθομοναδιαίος μετασχηματισμός είναι μία περιστροφή στον χώρο Hilbert και ως εκ τούτου αφήνει αμετάβλητο το μήκος του διανύσματος κατάστασης.

Το διάνυσμα κατάστασης ενός qubit ζει στον χώρο Hilbert $\mathbb{C}^2$, όπου ένας ορθομοναδιαίος μετασχηματισμός είναι απλά μία αντιστοιχία των διανυσμάτων βάσης $|0\rangle$ και $|1\rangle$ στα ορθοκανονικά διανύσματα $|u_0\rangle = a|0\rangle + b|1\rangle$ και $|u_1\rangle = c|0\rangle + d|1\rangle$. Ο ορθομοναδιαίος μετασχηματισμός προσδιορίζεται από τον πίνακα:

$$U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

Με $U^\dagger$ θα συμβολίζουμε τον ανάστροφο συζυγή του U, δηλαδή:

$$U^\dagger = \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix}$$

Από την απαίτηση τα $|u_0\rangle$ και $|u_1\rangle$ να είναι ορθοκανονικά εύκολα συνάγεται ότι: $UU^\dagger = U^\dagger U = I$. Επιπλέον μπορούμε να δείξουμε ότι: ένας γραμμικός μετασχηματισμός U είναι ορθομοναδιαίος αν και μόνο αν $UU^\dagger = U^\dagger U = I$.

Ας εξετάσουμε ορισμένα παραδείγματα ορθομοναδιαίων μετασχηματισμών που επιδρούν σε ένα qubit:

- Πύλη Hadamard.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

  Πρόκειται για μία από τις πιο σημαντικές πύλες. Αξίζει να παρατηρήσουμε ότι: $H^\dagger = H$ - επειδή ο H είναι πραγματικός και συμμετρικός- και $H^2 = I$.

- Πύλη περιστροφής. Η πύλη αυτή περιστρέφει το επίπεδο κατά γωνία θ.

$$R_\theta = \begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix}$$

- Πύλη NOT. Η πύλη αυτή μεταβάλει την τιμή ενός bit από 0 σε 1 και αντιστρόφως.

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

- Πύλη αντιστροφής φάσης.

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

2.6.2 Κβαντικές πύλες περισσοτέρων εισόδων

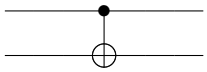
Αρχικά ας εξετάσουμε την εξέλιξη ενός συστήματος με δύο qubits, το διάνυσμα κατάστασης του οποίου ζει στον χώρο Hilbert $\mathbb{C}^4$. Στον χώρο αυτό ένα ορθομοναδιαίος μετασχηματισμός είναι ένας 4×4 πίνακας που ικανοποιεί την συνθήκη: $UU^\dagger = U^\dagger U = I$. Οι τέσσερις στήλες του U προσδιορίζουν τα τέσσερα ορθοκανονικά διανύσματα $|u_{00}\rangle, |u_{01}\rangle, |u_{10}\rangle$ και $|u_{11}\rangle$ τα οποία αποτελούν τις εικόνες των διανυσμάτων βάσης $|00\rangle, |01\rangle, |10\rangle$ και $|11\rangle$ μέσω του U.

Μία πολύ βασική πύλη δύο εισόδων είναι η πύλη ελεγχόμενου NOT ή CNOT:

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

Το πρώτο bit εισόδου της CNOT καλείται "bit ελέγχου" και το δεύτερο "bit στόχου". Αυτή η ονομασία προκύπτει από το γεγονός ότι το bit ελέγχου παραμένει αμετάβλητο ενώ το bit στόχου υφίσταται έναν μετασχηματισμό NOT αν και μόνο αν το bit ελέγχου είναι 1.

Το κύκλωμα που αντιστοιχεί στην πύλη CNOT είναι το ακόλουθο:



Τώρα, ας θεωρήσουμε ότι διαθέτουμε ένα κβαντικό σύστημα k καταστάσεων που ζει στο χώρο Hilbert V καθώς και ένα σύστημα l καταστάσεων που ζει στον χώρο Hilbert W. Το ερώτημα που τίθεται είναι σε πια κατάσταση θα βρεθεί ολόκληρο το σύστημα αν εφαρμόσουμε τον ορθομοναδιαίο μετασχηματισμό A στο πρώτο υποσύστημα και τον ορθομοναδιαίο μετασχηματισμό B στο δεύτερο υποσύστημα.

Η απάντηση αυτή είναι εύκολη για την περίπτωση μιας μη entangled κατάστασης $|u\rangle \otimes |w\rangle$ του $V \otimes W$. Η κατάσταση που προκύπτει στην περίπτωση αυτή είναι απλά η: $A|u\rangle \otimes B|w\rangle$. Όμως για την γενική περίπτωση μιας τυχούσας κατάστασης τα πράγματα είναι πιο σύνθετα καθώς πρέπει να ορίσουμε τον ορθομοναδιαίο μετασχηματισμό $A \otimes B$ ο οποίος δρα σε ολόκληρο το σύστημα επεκτείνοντας γραμμικά την δράση των A, B από μη entangled καταστάσεις σε entangled καταστάσεις.

Έτσι λοιπόν για παράδειγμα θα έχουμε:

- $(A \otimes B)(|0\rangle \otimes |0\rangle) = A|0\rangle \otimes B|0\rangle$
- $(A \otimes B)(|1\rangle \otimes |1\rangle) = A|1\rangle \otimes B|1\rangle$
- $(A \otimes B)\left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{\sqrt{2}}(A \otimes B)|00\rangle + \frac{1}{\sqrt{2}}(A \otimes B)|11\rangle =$

$$\frac{1}{\sqrt{2}}(A|0\rangle \otimes B|0\rangle + A|1\rangle \otimes B|1\rangle)$$

Για να το κάνουμε αυτό τυπικό, θεωρούμε $|e_1\rangle, ..., |e_k\rangle$ ως βάση του πρώτου συστήματος και $|f_1\rangle, ..., |f_l\rangle$ ως βάση του δευτέρου συστήματος οπότε μπορούμε να γράψουμε τους A, B ως $A = \sum_{i=1}^{k}\sum_{j=1}^{k} a_{ij}|e_i\rangle\langle e_j|$ και $B = \sum_{m=1}^{l}\sum_{n=1}^{l} b_{mn}|f_m\rangle\langle f_n|$. Η βάση ολόκληρου του συστήματος θα είναι: $|e_i\rangle \otimes |f_m\rangle$, για $i = 1, ..., k$ και $m = 1, ..., l$. Ο τελεστής $A \otimes B$ είναι:

$$A \otimes B = \left(\sum_{i=1}^{k}\sum_{j=1}^{k} a_{ij}|e_i\rangle\langle e_j|\right) \otimes \left(\sum_{m=1}^{l}\sum_{n=1}^{l} b_{mn}|f_m\rangle\langle f_n|\right) =$$

$$\sum_{i=1}^{k}\sum_{j=1}^{k}\sum_{m=1}^{l}\sum_{n=1}^{l} a_{ij}b_{mn}\left(|e_i\rangle\langle e_j| \otimes |f_m\rangle\langle f_n|\right) =$$

$$\sum_{i=1}^{k}\sum_{j=1}^{k}\sum_{m=1}^{l}\sum_{n=1}^{l} a_{ij}b_{mn}\left(|e_i\rangle \otimes |f_m\rangle\right)\left(\langle e_j| \otimes \langle f_n|\right)$$

Συνεπώς το $(i,m),(j,n)$ στοιχείο του $A \otimes B$ είναι το $a_{ij}b_{mn}$. Αν επιπλέον διατάξουμε την βάση $|e_i\rangle \otimes |f_m\rangle$ λεξικογραφικά, τότε ο ορθομοναδιαίος μετασχηματισμός $A \otimes B$ θα είναι:

$$\begin{pmatrix} a_{11}B & a_{12}B & \dots \\ a_{21}B & a_{22}B & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

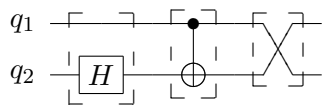
όπου στο i,j υπομπλόκ του $A \otimes B$, πολλαπλασιάζουμε το a_{ij} με τον B.

2.6.3 Κβαντικά κυκλώματα

Όσα έχουμε δει ως τώρα συνιστούν ένα μοντέλο των κβαντικών υπολογισμών το οποίο στηρίζεται στην γραμμική άλγεβρα και για αυτό το λόγο ίσος δεν είναι αρκετά απλό ώστε να μας δώσει μια καλή αίσθηση των κβαντικών υπολογισμών. Για αυτό θα εισάγουμε την χρήση των κβαντικών κυκλωμάτων, τα οποία δρουν όπως τα γνωστά σε όλους κλασικά λογικά κυκλώματα όμως με κάποιους επιπρόσθετους περιορισμούς οι οποίοι προέρχονται από την ιδιάζουσα φύση της κβαντομηχανικής. Ήδη και στην παρουσίαση των κβαντικών υπολογισμών υπό τον μανδύα της γραμμικής άλγεβρας έχουμε υπονοήσει την ύπαρξη της έννοιας των κβαντικών κυκλωμάτων καλώντας τους ορθομοναδιαίους μετασχηματισμούς πύλες.

Έτσι λοιπόν ένα κβαντικό κύκλωμα αποτελείται από ένα πεπερασμένο πλήθος από πύλες οι οποίες τροφοδοτούνται με qubits στις εισόδους τους και σαν αποτέλεσμα μετασχηματίζουν την κατάσταση αυτών των qubits. Όμως όπως είδαμε οι μετασχηματισμοί που λαμβάνουν χώρα είναι ορθομοναδιαίοι και συνεπώς αντιστρέψιμοι. Άρα πρέπει και οι πύλες που χρησιμοποιούμε να είναι αντιστρέψιμες και κατ επέκταση να έχουν τόσες εισόδους όσες και εξόδους. Αυτό εκ πρώτης όψεως φαίνεται καταστροφικό αφού οι συνηθισμένες λογικές πύλες όπως and, or, nand κλπ δεν είναι αντιστρέψιμες. Θα δούμε στην συνέχεια πως μπορούμε να το ξεπεράσουμε αυτό ορίζοντας τις αντίστοιχες αντιστρέψιμες πύλες. Επιπλέον στα λογικά κυκλώματα είμαστε συνηθισμένοι να χρησιμοποιούμε διακλαδώσεις που αντιπροσωπεύουν την αντιγραφή της κλασικής πληροφορίας. Όμως στα κβαντικά κυκλώματα κάτι τέτοιο δεν υφίσταται εξ αιτίας του θεωρήματος της μη κλωνοποίησης το οποίο θα δούμε στην συνέχεια.

Ας δούμε όμως ένα παράδειγμα κβαντικού κυκλώματος για να γίνουν τα πράγματα πιο κατανοητά.



Το κύκλωμα αυτό έχει δύο εισόδους q_1, q_2 και αποτελείται από τρεις φάσεις. Στην πρώτη φάση το qubit q_1 μένει ανεπηρέαστο ενώ στο qubit q_2 εφαρμόζεται μια πύλη Hadamard. Συνολικά λοιπόν στην πρώτη εφαρμόζεται ο μετασχηματισμός $I \otimes H$. Στην δεύτερη φάση εφαρμόζεται η πύλη CNOT που είδαμε στην προηγούμενη υποενότητα. Στην τρίτη φάση λαμβάνει χώρα μία μετάθεση των καλωδίων του κυκλώματος. Γενικά οποιαδήποτε μετάθεση καλωδίων αντιστοιχεί σε έναν ορθομοναδιαίο μετασχηματισμό και άρα μπορεί να χρησιμοποιηθεί σε ένα κβαντικό κύκλωμα. Εν προκειμένω έχουμε τον μετασχηματισμό: $|00\rangle \to |00\rangle, |01\rangle \to |10\rangle, |10\rangle \to |01\rangle, |11\rangle \to |11\rangle$ ο οποίος μας δίνει τον ορθομοναδιαίο πίνακα: $P = \left(\, |00\rangle \, \middle| \, |10\rangle \, \middle| \, |01\rangle \, \middle| \, |11\rangle \, \right)$. Καταλήγουμε λοιπόν ότι αυτό το κβαντικό κύκλωμα αντιστοιχεί στον ορθομοναδιαίο μετασχηματισμό $P \cdot CNOT \cdot (I \otimes H)$. Έτσι αν η αρχική

κατάσταση του συστήματος είναι η $a_{00}\left|00\right\rangle + a_{01}\left|01\right\rangle + a_{10}\left|10\right\rangle + a_{11}\left|11\right\rangle$ στο τέλος θα γίνει:

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}1&1&0&0\\1&-1&0&0\\0&0&1&1\\0&0&1&-1\end{pmatrix}\begin{pmatrix}a_{00}\\a_{01}\\a_{10}\\a_{11}\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}a_{00}+a_{01}\\a_{10}-a_{11}\\a_{00}-a_{01}\\a_{10}+a_{11}\end{pmatrix}$$

2.7 Το θεώρημα της μη κλωνοποίησης

Ενώ τα αξιώματα της κβαντομηχανικής είναι φαινομενικά απλά, ορισμένες από τις συνέπειες τους εναντιώνονται στην ανθρώπινη διαίσθηση. Μια τέτοια συνέπεια είναι το θεώρημα της μη κλωνοποίησης. Το θεώρημα αυτό μας λέει ότι δοθέντος ενός qubit το οποίο βρίσκεται σε μια τυχούσα κατάσταση $\left|\phi\right\rangle = \alpha_0\left|0\right\rangle + \alpha_1\left|1\right\rangle$ είναι γενικά αδύνατο να δημιουργήσουμε ένα αντίγραφο του.

Πιο συγκεκριμένα, το πρόβλημα μας είναι ο μετασχηματισμός της κατάστασης $\left|\phi\right\rangle \otimes \left|0\right\rangle$ στην κατάσταση $\left|\phi\right\rangle \otimes \left|\phi\right\rangle$. Από το αξίωμα της ορθομοναδιαίας εξέλιξης γνωρίζουμε ότι αν κάτι τέτοιο είναι εφικτό, τότε θα πρέπει να πραγματοποιείται με την επίδραση ενός ορθομοναδιαίου μετασχηματισμού U τέτοιου ώστε $U\left|\phi\right\rangle \otimes \left|0\right\rangle = \left|\phi\right\rangle \otimes \left|\phi\right\rangle$. Άρα μέσω του μετασχηματισμού U για δύο τυχούσες και ανεξάρτητες καταστάσεις $\left|\phi_1\right\rangle, \left|\phi_2\right\rangle$ θα έχουμε:

$$\left|\phi_1\right\rangle \otimes \left|0\right\rangle \xrightarrow{U} \left|\phi_1\right\rangle \otimes \left|\phi_1\right\rangle$$

$$\left|\phi_2\right\rangle \otimes \left|0\right\rangle \xrightarrow{U} \left|\phi_2\right\rangle \otimes \left|\phi_2\right\rangle$$

Όμως τότε $\left\langle\phi_1|\phi_2\right\rangle = \left\langle\left|\phi_1\right\rangle \otimes \left|0\right\rangle, \left|\phi_2\right\rangle \otimes \left|0\right\rangle\right\rangle = \left\langle\left|\phi_1\right\rangle \otimes \left|\phi_1\right\rangle, \left|\phi_2\right\rangle \otimes \left|\phi_2\right\rangle\right\rangle = \left\langle\phi_1|\phi_2\right\rangle^2 \implies \left\langle\phi_1|\phi_2\right\rangle = 0 \vee \left\langle\phi_1|\phi_2\right\rangle = 1$, όπου χρησιμοποιήσαμε το γεγονός ότι αφού ο U είναι τέτοιος ώστε $UU^\dagger = U^\dagger U = I$ διατηρεί το εσωτερικό γινόμενο. Δηλαδή τα $\left|\phi_1\right\rangle, \left|\phi_2\right\rangle$ είτε θα είναι συγγραμικά είτε θα είναι κάθετα μεταξύ τους. Άτοπο, καθώς υποθέσαμε ότι τα $\left|\phi_1\right\rangle, \left|\phi_2\right\rangle$ επιλέχθηκαν τυχαία.

Κεφάλαιο 3

Η γλώσσα κβαντικού προγραμματισμού nQML

3.1 Εισαγωγή

Οι περισσότερες γλώσσες κβαντικού προγραμματισμού που έχουν προταθεί έως τώρα στην βιβλιογραφία βασίζονται στην αρχή 'quantum data, classical control', δηλαδή στην ιδέα ότι ότι η εκτέλεση του προγράμματος ακολουθεί μια συγκεκριμένη ροή ελέγχου όπως και σε έναν κλασικό υπολογιστή. Από την άλλη μεριά, συναντάμε και γλώσσες που ακολουθούν το μοντέλο 'quantum data and control'. Αυτές οι γλώσσες χρησιμοποιούν κβαντική ροή ελέγχου, δηλαδή επιτρέπουν την εκτέλεση του προγράμματος να βρίσκεται σε μια υπέρθεση διαφόρων καταστάσεων ακριβώς όπως και τα κβαντικά δεδομένα τα οποία διαχειρίζεται το πρόγραμμα.

Η nQML είναι μία υψηλού επιπέδου συναρτησιακή γλώσσα που ακολουθεί το μοντέλο 'quantum data and control'. Σχεδιάστηκε από τον Μιχάλη Λάμπη και μελετήθηκε εκ νέου από τον Γιάννη Ρουσελάκη, ενώ είναι βασισμένη στην QML των Altenkirch και Grattage. Ο κύριος στόχος της nQML είναι να δώσει στον προγραμματιστή την απαραίτητη εκφραστική δύναμη ώστε να είναι σε θέση να υλοποιεί κβαντικούς αλγορίθμους, ενώ παράλληλα να τον προστατεύει από την παραβίαση των κανόνων της κβαντομηχανικής. Η nQML διαθέτει συνδυαστές που επιτρέπουν την εύκολη διατύπωση οποιουδήποτε ορθομοναδιαίου μετασχηματισμού και επιπλέον επιτρέπει την διεξαγωγή μετρήσεων σε οποιοδήποτε σημείο κατά την εκτέλεση του προγράμματος. Ένα από τα βασικά χαρακτηριστικά της είναι ότι συνοδεύεται από ένα απλό σύστημα τύπων. Ο ίδιος ο τύπος μια κβαντικής έκφρασης περιλαμβάνει πληροφορία για την θέση, στην συνολική κβαντική κατάσταση, των qubits που χρησιμοποιούνται από την έκφραση. Επιπλέον η πολλαπλή αναφορά στο ίδιο qubit μέσα στην ίδια έκφραση επιτρέπεται με τρόπο τέτοιο ώστε να μην παραβιάζεται το θεώρημα της μη κλωνοποίησης και έτσι ο προγραμματιστής είναι απαλλαγμένος από περιορισμούς γραμμικότητας στην χρήση των qubits που πολύ συχνά συναντάμε σε άλλες γλώσσες κβαντικού προγραμματισμού.

Όλες αυτές οι διευκολύνσεις που παρέχει η nQML στον προγραμματιστή συνοδεύονται με το κόστος της παραμέλησης σημαντικών πρακτικών ζητημάτων. Τέτοια ζητήματα είναι οι ατέλειες του κβαντικού hardware που έχουμε αυτή την στιγμή στην διάθεση μας, η ανάγκη για την διόρθωση κβαντικών σφαλμάτων που οφείλονται σε κβαντικό θόρυβο και αλληλεπίδραση του κβαντικού συστήματος με το περιβάλλον του, καθώς και το γεγονός ότι τελικά κάθε κβαντικό πρόγραμμα θα πρέπει να μεταφραστεί σε ένα κβαντικό κύκλωμα χρησιμοποιώντας μονάχα ορισμένες βασικές κβαντικές πύλες, πράγμα που σημαίνει ότι κάποιοι από τους ορθομοναδιαίους μετασχηματισμούς που περιγράφονται στην nQML θα πρέπει να προσεγγισθούν. Όμως παρόμοια προβλήματα αντιμετώπισαν και οι σχεδιαστές των κλασικών υπολογιστών πριν από κάποιες δεκαετίες και τελικά κατάφεραν να τα επιλύσουν με τρόπο τέτοιο ώστε ο προγραμματιστής σε μια γλώσσα υψηλού επιπέδου να είναι τέλειος απαλλαγμένος από τέτοια ζητήματα. Το ίδιο αναμένουμε να γίνει και στις κβαντικές γλώσσες προγραμματισμού κάτι που θα έχει ως αποτέλεσμά τα ζητήματα αυτά να αντιμετωπίζονται καθαρά από τους αρχιτέκτονες των κβαντικών υπολογιστών, τους σχεδιαστές των κβαντικών λειτουργικών συστημάτων και σε ένα μικρότερο βαθμό από τους σχεδιαστές των μεταγλωττιστών, αλλά όχι από τους σχεδιαστές των γλωσσών κβαντικού προγραμματισμού και τους προγραμματιστές.

3.2 Συντακτικό της γλώσσας

Το συντακτικό της nQML δίνεται από την ακόλουθη γραμματική, όπου υποθέτουμε ότι το το x αντιπροσωπεύει μία μεταβλητή και το λ μία μιγαδική σταθερά. Η γραμματική αυτή ορίζει δύο μη τερματικά σύμβολα. Οι κβαντικές εκφράσεις αναπαρίστανται με το σύμβολο e, ενώ οι κλασικές εκφράσεις με το σύμβολο c. Να σημειώσουμε ότι όπως φαίνεται από την γραμματική οι κλασικές εκφράσεις είναι χρήσιμες μόνο στον συνδυαστή κατασκευής ορθομοναδιαίων μετασχηματισμών $|e\rangle \to x, x'.c$.

$\langle e \rangle$ ::= x
| { (λ)**qfalse** + (λ')**qtrue** }
| **let** $x = e_1$ **in** e_2
| (e_1, e_2)
| **let** $(x_1, x_2) = e_1$ **in** e_2
| **if** e **then** e_1 **else** e_2
| **ifm** e **then** e_1 **else** e_2
| $|e\rangle \to x, x'.c$

$\langle c \rangle$ ::= x
| **false**
| **true**
| λ
| **let** $x = c_1$ **in** c_2
| (c_1, c_2)
| **let** $(x_1, x_2) = c_1$ **in** c_2
| **if** c **then** c_1 **else** c_2
| $c1 = c2$
| **int** c
| $c_1 + c_2$
| $c_1 - c_2$
| $c_1 * c_2$
| c_1 / c_2
| $c_1^{c_2}$

Οι μεταβλητές στην nQML αντιπροσωπεύουν αναφορές σε qubits τα οποία είναι μέρος της καθολικής κατάστασης του κβαντικού συστήματος. Υπάρχουν δύο τύποι κβαντικής πληροφορίας: τα qubits και τα γινόμενα. Ένα καινούριο qubit τοποθετείται στην καθολική κατάσταση με τον τελεστή { (λ)**qfalse** + (λ')**qtrue** }, με τον ίδιο τρόπο που καινούρια αντικείμενα δεσμεύονται στον σωρό ενός κλασικού υπολογιστή όταν χρησιμοποιείται ένας κατασκευαστής δεδομένων. Τα γινόμενα δημιουργούνται και αποσυνθέτονται με τους τελεστές (e_1, e_2) και **let** $(x_1, x_2) = e_1$ **in** e_2 αντίστοιχα.

Οι τρεις βασικοί τελεστές της nQML που δίνουν την ευχέρεια στον προγραμματιστή να υλοποιήσει εύκολα κβαντικούς αλγορίθμους είναι οι εξής:

- **ifm** e **then** e_1 **else** e_2: Με τον τελεστή αυτό πραγματοποιείται μέτρηση στην e η οποία πρέπει να είναι τύπου qubit. Ανάλογα με το αποτέλεσμα της μέτρησης εκτελείται ο κατάλληλος κλάδος της διακλάδωσης.

- **if** e **then** e_1 **else** e_2: Ο τελεστής αυτός επιτρέπει στον προγραμματιστή να πραγματοποιεί κβαντικές διακλαδώσεις. Η έκφραση e πρέπει να είναι τύπου qubit. Αν βρίσκεται σε μία εκ των δύο βασικών καταστάσεων $|0\rangle$ ή $|1\rangle$ τότε ο τελεστής λειτουργεί σαν έναν κλασικό τελεστή διακλάδωσης. Αν όμως η έκφραση e βρίσκεται σε μια κβαντική υπέρθεση τότε το πρόγραμμα προχωράει την εκτέλεση του όντας σε μία υπέρθεση των δύο διακλαδώσεων. Κατά κάποιο τρόπο σαν να εκτελεί και τις δύο διακλαδώσεις εν παραλλήλω.

- $|e\rangle \to x, x'.c$: Με αυτόν τον τελεστή ο προγραμματιστής μπορεί να εκφράσει οποιονδήποτε ορθομοναδιαίο μετασχηματισμό επιθυμεί. Το πλεονέκτημα του τελεστή αυτού είναι ότι δεν απαιτεί από τον προγραμματιστή να του δώσει στοιχείο προς στοιχείο τον ορθομοναδιαίο μετασχηματισμό, του οποίου τα στοιχεία είναι εκθετικά πολλά σε σχέση με τα qubits τα οποία μετασχηματίζει. Αντί αυτού ο προγραμματιστής μπορεί να δώσει μια περιγραφή του ορθομοναδιαίου μετασχηματισμού ως μία συνάρτηση από τις συντεταγμένες του στοιχείου προς το ίδιο το στοιχείο, δηλαδή έναν μιγαδικό αριθμό. Με αυτό τον τρόπο είναι σε θέση να περιγράψει συνοπτικά επαναλαμβανόμενα πρότυπα του μετασχηματισμού και έτσι να μειώσει δραστικά το μέγεθος του κώδικα που πληκτρολογεί.

  Κάθε ορθομοναδιαίο μετασχηματισμό μπορούμε να τον δούμε ως μία συνάρτηση της μορφής:

$$|x'\rangle \to \sum_{x=0}^{2^n-1} f(x, x') \, |x\rangle$$

  η οποία δέχεται ως είσοδο μία βασική κατάσταση $|x'\rangle$ και την μετασχηματίζει σε μία υπέρθεση βασικών καταστάσεων, όπου το πλάτος της κάθε μίας δίνεται ως συνάρτηση της κατάστασης εισόδου $|x'\rangle$ και της κατάστασης εξόδου $|x\rangle$. Με τον τελεστή $|e\rangle \to x, x'.c$ ο προγραμματιστής αρκείται στο να δώσει απλά την περιγραφή της $f(x, x')$ με τα x, x' ως μεταβλητές.

  Αδιαμφισβήτητα ο τελεστής αυτός προσφέρει μεγάλη ευκολία στο προγραμματιστή, όμως η αποδοτική υλοποίηση του φαίνεται να παρουσιάζει μεγάλες δυσκολίες. Πρακτικά ο μόνος τρόπος υλοποίησής του που μπορούμε να φανταστούμε αυτή την στιγμή είναι η αποτίμησή της συνάρτησης $f(x, x')$ για όλες τις δυνατές τιμές του πεδίου ορισμού της. Έτσι μπορούμε να υπολογίσουμε τον πίνακα που μας δίνει η $f(x, x')$ να ελέγξουμε ότι όντως είναι ορθομοναδιαίος και κατόπιν να προχωρήσουμε στην δημιουργία του κβαντικού κυκλώματος που τον προσεγγίζει με βάση τις πύλες που έχουμε στην διάθεση μας. Όμως το πεδίο ορισμού της $f(x, x')$ είναι εκθετικά μεγάλο ως προς το πλήθος των qubits που επηρεάζει ο μετασχηματισμός και συνεπώς το όποιο πλεονέκτημα μπορεί να μας προσφέρει ένας κβαντικός υπολογιστής εξανεμίζεται αφού ο υπολογισμός του ορθομοναδιαίου μετασχηματισμού είναι εκθετικός.

3.3 Το σύστημα τύπων

Η nQML υποστηρίζει δύο είδη τύπων: κβαντικούς τύπους (τ) και κλασικούς τύπους (ϕ). Για κάθε κβαντική έκφραση το σύστημα τύπων της nQML είναι σε θέση να γνωρίζει τα qubit στα οποία πρόκειται να βρεθεί η τιμή της έκφρασης. Η πληροφορία αυτή αποθηκεύεται στους τύπους και αποτελεί μία από τις καινοτομίες της nQML. Με αυτό τον τρόπο διασφαλίζεται ότι το ίδιο qubit δεν θα χρησιμοποιηθεί δύο φορές σε έναν μετασχηματισμό, κάτι που θα είχε σαν συνέπεια την παράβαση του θεωρήματος της μη κλωνοποίησης.

$$\begin{aligned} \langle \tau \rangle \quad &::= \textbf{qbit}[n] \\ &\mid \tau_1 \otimes \tau_2 \end{aligned}$$

$$\begin{aligned} \langle \phi \rangle \quad &::= \textbf{bit} \\ &\mid \phi_1 \times \phi_2 \\ &\mid \textbf{complex} \end{aligned}$$

Εδώ το n είναι ένας φυσικός αριθμός που δηλώνει ποίο ακριβώς qubit από την καθολική κατάσταση χρησιμοποιείται. Για παράδειγμα, μία έκφραση έχει τύπο $\textbf{qbit}[5]$ αν η τιμή της αποθηκεύεται στο πέμπτο qubit της καθολικής κατάστασης.

Το σύστημα τύπων περιλαμβάνει δύο σχέσεις τυποποίησης. Η σχέση $\Gamma; n \vdash^{\circ} e : \tau; m$ χρησιμοποιείται για τον έλεγχο τύπων των αγνών κβαντικών εκφράσεων, δηλαδή αυτών δεν περιλαμβάνουν

μέτρηση. Από την άλλη η σχέση $\Gamma; n \vdash e : \tau; m$ χρησιμοποιείται για τον έλεγχο τύπων οποιασδήποτε κβαντικής έκφρασης. Είναι φανερό λοιπόν ότι η πρώτη σχέση αποτελεί γνήσιο υποσύνολο της δεύτερης. Θα αναφερόμαστε και στις δύο σχέσεις τυποποίησης με τον συμβολισμό $\Gamma; n \vdash^{\alpha} e : \tau; m$ επιτρέποντας στο $^{\alpha}$ να είναι είτε $^{\circ}$ είτε το κενό. Από την στιγμή που οι τύποι της nQML διαθέτουν πληροφορία για την θέση των qubits, δεν γίνεται παρά η σχέση τυποποίησης να επεξεργάζεται και να διαδίδει την πληροφορία αυτή. Γράφοντας $\Gamma; n \vdash^{\alpha} e : \tau; m$, ο φυσικός αριθμός n αντιπροσωπεύει το πλήθος των qubit στην κβαντική κατάσταση πριν ξεκινήσει η αποτίμηση της έκφρασης e και ο φυσικός αριθμός m δηλώνει το πλήθος των qubit που δημιουργούνται από την έκφραση e.

Ας δούμε τώρα τον ορισμό της σχέσης τυποποίησης:

- Πρώτα από όλα, η σχέση υποσυνόλου η οποία συνδέει τις δύο σχέσεις τυποποίησης εκφράζεται με τον ακόλουθο κανόνα.

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

- Για τις μεταβλητές ψάχνουμε απλά τον τύπο τους στο περιβάλλον.

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

- Ο κατασκευαστής των qubit ελέγχει ότι οι παράμετροι λ, λ' ορίζουν έναν ορθομοναδιαίο μετασχηματισμό και προσθέτει ένα επιπλέον qubit στην κβαντική κατάσταση.

$$\frac{|\lambda|^2 + |\lambda'|^2 = 1 \qquad \lambda \cdot \overline{\lambda'} = \overline{\lambda} \cdot \lambda'}{\Gamma; n \vdash^{\circ} \{\ (\lambda)\mathbf{qfalse} + (\lambda')\mathbf{qtrue}\ \} : \mathbf{qbit}[n]; 1} \text{ (SUP)}$$

- Οι κανόνες για τον ορισμό σταθερών, την δημιουργία γινομένων και την αποσύνθεση γινομένων παρουσιάζουν μεγάλες ομοιότητες για αυτό και τους παραθέτουμε μαζί.

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

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

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

- Ο κανόνας τυποποίησης για τον τελεστή κβαντικής διακλάδωσης φροντίζει ώστε το qubit της συνθήκης να μην χρησιμοποιείται σε κανένα από τα δύο branches. Για το λόγο αυτό με $\Gamma|_k$ συμβολίζουμε το περιβάλλον Γ περιορισμένο ώστε να μην περιέχει μεταβλητές των οποίων οι τύποι χρησιμοποιούν το $k-$οστό qubit της κβαντικής κατάστασης. Αυτός ο περιορισμός τίθεται για να απλοποιηθεί τόσο η σημασιολογία του τελεστή όσο και ο κανόνας τυποποίησης.

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

- Ο κανόνας τυποποίησης για τον τελεστή που πραγματοποιεί μέτρηση σε ένα qubit και κατόπιν με βάση το αποτέλεσμα της μέτρησης πραγματοποιεί κλασική διακλάδωση δεν παρουσιάζει δυσκολίες.

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

- Για τον τελεστή $|e\rangle \to x, x'.c$ το σύστημα τύπων διασφαλίζει ότι ο τύπος τ της έκφρασης e θα είναι αγνός, δηλαδή δεν θα αναφέρετε παραπάνω από μία φορές σε ένα qubit, έτσι ώστε να μην παραβιάζεται το θεώρημα της μη κλωνοποίησης. Επιπλέον, αυτό είναι το μοναδικό σημείο στο οποίο κάνουμε χρήση του ελέγχου τύπων για κλασικές εκφράσεις. Με $C(\tau)$ συμβολίζουμε το κλασικό τύπο ο οποίος αντιστοιχεί στον κβαντικό τύπο τ. Ο έλεγχος τύπων για τις κλασικές εκφράσεις είναι τετριμμένος και για αυτό δεν θα επεκταθούμε περαιτέρω. Πρέπει να σημειώσουμε ότι θα μπορούσαμε να υπολογίσουμε πλήρως τον πίνακα που αντιστοιχεί στον μετασχηματισμό και να εξετάσουμε αν είναι ορθομοναδιαίος. Όμως κάτι τέτοιο θα καθιστούσε τον έλεγχο τύπων εκθετικό ως προς το πλήθος των qubit. Βέβαια και για την υλοποίηση του τελεστή δεν γνωρίζουμε κάτι καλύτερο από μία εκθετική υλοποίηση.

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

3.4 Δηλωτική σημασιολογία υπό την μορφή κβαντικών κυκλωμάτων

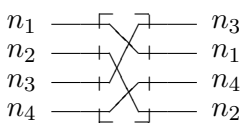
Όπως είδαμε τα κβαντικά κυκλώματα αποτελούν ένα μοντέλο των κβαντικών υπολογισμών. Ως εκ τούτου είναι εύλογο να επιχειρήσει να δώσει κάνεις την σημασία ενός προγράμματος nQML μέσω κβαντικών κυκλωμάτων. Επιπλέον, το κβαντικό κύκλωμα που αποτελεί την σημασία ενός προγράμματος nQML αποτελεί και μία ρεαλιστική υλοποίηση του προγράμματος, καθώς δεν πρόκειται για κάποια αφηρημένη μαθηματική έννοια αλλά για την περιγραφή ενός κυκλώματος. Για αυτό τον λόγο η απόδοση σημασιολογίας στα προγράμματα της nQML υπό την μορφή κβαντικών κυκλωμάτων μπορεί να θεωρηθεί και ως ένα είδος μεταγλώττισης τους.

Τα κυκλώματα ως μαθηματικά αντικείμενα μπορούμε να τα ορίσουμε με τον παρακάτω ορισμό σε Haskell.

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

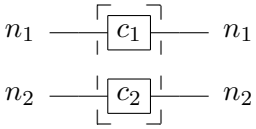
Οποιοδήποτε κβαντικό κύκλωμα που δρα σε n qubits μπορεί να κατασκευαστεί επαγωγικά χρησιμοποιώντας αυτούς τους κατασκευαστές. Ας τους δούμε αναλυτικότερα.

- *Wire* p: μεταθέτει τα qubit της κβαντικής κατάστασης. Η παράμετρος p πρέπει να είναι μία μετάθεση της λίστας $[0..n-1]$. Αν το i-οστό στοιχείο αυτής της μετάθεσης είναι το j αυτό σημαίνει ότι το καλώδιο στην i-οστή θέση της εισόδου γίνεται το καλώδιο στην j-οστή θέση της εξόδου. Η ταυτοτική μετάθεση αντιστοιχεί στον ταυτοτικό ορθομοναδιαίο μετασχηματισμό και αφήνει την κβαντική κατάσταση αμετάβλητη. Τα κυκλώματα που αντιστοιχούν σε μεταθέσεις καλωδίων θα τα σχεδιάζουμε για παράδειγμα έτσι:

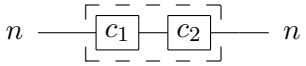


  Σε όλα τα κυκλώματά ο αριθμός δίπλα στα καλώδια θα δηλώνει την πολλαπλότητα των καλωδίων. Αν $n_1 = n_2 = n_3 = n_4 = 1$ τότε το ανωτέρω κύκλωμα μπορεί να γραφεί σε Haskell ως *Wire* $[1, 3, 0, 2]$.

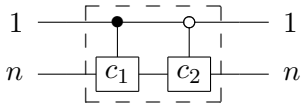
- *Par* c_1 c_2: συνδυάζει τα κυκλώματα c_1, c_2 εν παραλλήλω.



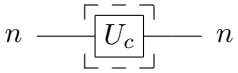
- *Seq* $c_1\ c_2$: συνδυάζει τα κυκλώματα c_1, c_2 εν σειρά. Τα δύο κυκλώματα πρέπει να έχουν τον ίδιο αριθμό καλωδίων n.



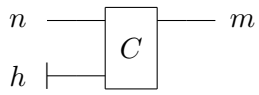
- *Cond* $c_1\ c_2$: δημιουργεί ένα κύκλωμα κβαντικής διακλάδωσης το οποίο ελέγχεται από ένα επιπλέον qubit. Τα κυκλώματα c_1 και c_2 πρέπει να έχουν τον ίδιο αριθμό καλωδίων n, ενώ το πλήθος των καλωδίων του συνολικού κυκλώματος θα είναι $n + 1$.



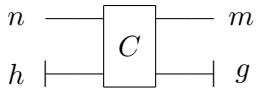
- *Unit* C: δημιουργεί ένα κύκλωμα το οποίο αντιστοιχεί στον ορθομοναδιαίο μετασχηματισμό C. Εν γένη το κύκλωμα αυτό θα δημιουργείται κατά προσέγγιση με βάση τις στοιχειώδεις πύλες που έχουμε στην διάθεση μας. Να τονίσουμε για μία ακόμα φορά ότι το μέγεθος του πίνακα C θα είναι εκθετικό ως προς τα qubits που μετασχηματίζει. Συνεπώς τα qubits που μετασχηματίζει ο C θα πρέπει να είναι αμελητέα το πλήθος σε σχέση τα συνολικά qubits της κβαντικής κατάστασης, διαφορετικά όλη η υπεροχή του κβαντικού υπολογισμού θα υποσκιάζεται πλήρως από την διαδικασία κατασκευής του κβαντικού κυκλώματος.



Διαχωρίζουμε τα κβαντικά κυκλώματα σε δύο κατηγορίες. Την κατηγορία των αγνών κυκλωμάτων, δηλαδή αυτών στα οποία δεν λαμβάνει χώρο κάποια μέτρηση και στην γενική κατηγορία των κβαντικών κυκλωμάτων. Προφανώς η πρώτη είναι γνήσιο υποσύνολο της δεύτερης. Από τα καλώδια εισόδου ενός κβαντικού κυκλώματος ξεχωρίζουμε ορισμένα τα οποία ονομάζουμε σωρό και αρχικοποιούμε κάθε ένα από αυτά στην κατάσταση $|0\rangle$. Από τα καλώδια εξόδου ενός κβαντικού κυκλώματος ξεχωρίζουμε ορισμένα τα οποία ονομάζουμε σκουπίδια και πρόκειται για αυτά που έχουν μετρηθεί και δεν μας είναι πλέον χρήσιμα. Συνεπώς η πλήρης περιγραφή του κυκλώματος αποτελείται πέραν από το κύκλωμα αυτό κάθε αυτό και από τέσσερις φυσικούς αριθμούς που προσδιορίζουν το πλήθος των εισόδων που δεν ανήκουν στον σωρό, το πλήθος των εξόδων που δεν είναι σκουπίδια, το πλήθος των εισόδων που ανήκουν στον σωρό και το πλήθος των εξόδων που είναι σκουπίδια. Στα κυκλώματα μας θα συμβολίζουμε τα καλώδια που αντιστοιχούν στον σωρό και στα σκουπίδια με κάθετες γραμμές. Έτσι ένα αγνό κύκλωμα θα είναι της μορφής:



αφού δεν διαθέτει καλώδια σκουπίδια, ενώ γενικά ένα κβαντικό κύκλωμα θα είναι της μορφής:



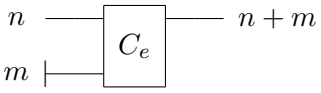
Και θα πρέπει βέβαια να ισχύει η σχέση $n + h = m + g$. Έτσι λοιπόν η σημασία των εκφράσεων που τυποποιούνται σύμφωνα με το αγνό σύστημα τύπων θα είναι ένα αγνό κύκλωμα, ενώ γενικά μία έκφραση nQML που επιδέχεται τύπου θα έχει ως σημασία ένα κβαντικό κύκλωμα.

Είμαστε τώρα έτοιμοι να δώσουμε μια ερμηνεία στην γλώσσα μας με την μορφή κβαντικών κυκλωμάτων. Θα ορίσουμε την ερμηνεία με επαγωγή στους κανόνες τυποποίησης.

- *Κανόνας EMB*

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

Η περίπτωση αυτή είναι τετριμμένη αφού το προκύπτον κύκλωμα ταυτίζεται με αυτό του επαγωγικού βήματος.



- *Κανόνας VAR*

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

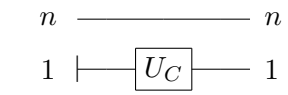
Απλή περίπτωση και αυτή αφού το προκύπτον κύκλωμα είναι απλά το ταυτοτικό κύκλωμα.

- *Κανόνας SUP*

$$\frac{|\lambda|^2+|\lambda'|^2=1 \qquad \lambda\cdot\overline{\lambda'}=\overline{\lambda}\cdot\lambda'}{\Gamma;n\vdash^{\circ}\ \{\ (\lambda)\mathbf{qfalse}+(\lambda')\mathbf{qtrue}\ \}:\mathbf{qbit}[n];1}\ (\text{SUP})$$

Σε αυτή την περίπτωση τα qubits της αρχικής κβαντικής κατάστασής μετασχηματίζονται από το ταυτοτικό κύκλωμα, ενώ στην νέα κατάσταση προστίθεται ένα ακόμα qubit το οποίο αρχικοποιείται στην κατάσταση $|0\rangle$ και κατόπιν μετασχηματίζεται με βάση τον ορθομοναδιαίο μετασχηματισμό:

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



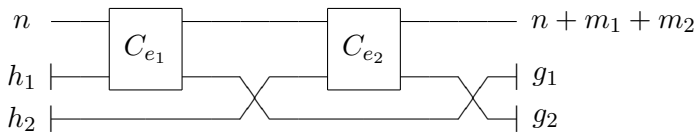
- *Κανόνες LET, PROD και LETPROD*

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

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

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

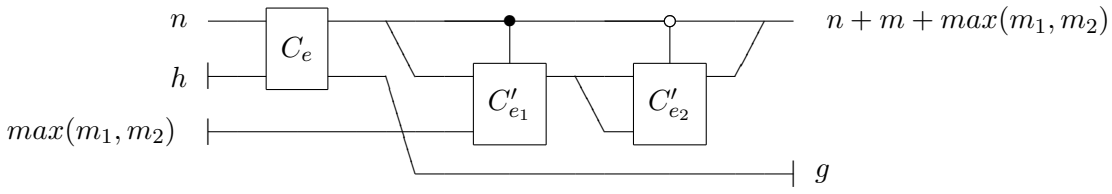
Και οι τρεις κανόνες δίνουν σαν αποτέλεσμα το ίδιο κύκλωμα για αυτό και τους παραθέτουμε μαζί. Ουσιαστικά πρόκειται για την σειριακή σύνθεση των κυκλωμάτων C_{e_1}, C_{e_2} που προκύπτουν από το επαγωγικό βήμα. Θα πρέπει να τονίσουμε ότι με βάση αυτό τον ορισμό η γλώσσα έχει call by value σημασιολογία και οι πλειάδες αποτιμώνται από αριστερά προς τα δεξιά.



- *Κανόνας IF*

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

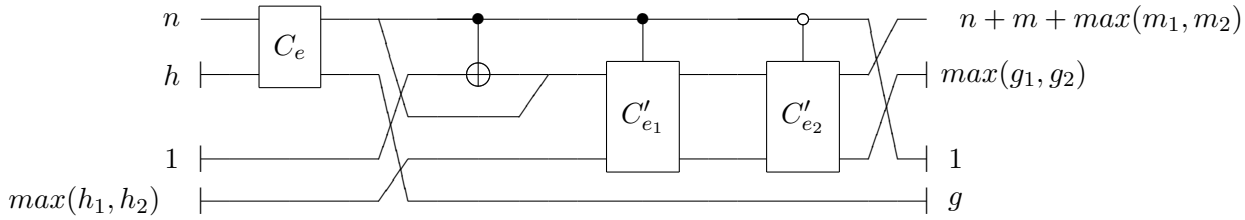
Στην περίπτωση αυτή, από το επαγωγικό βήμα έχουμε στην διάθεση μας τα κυκλώματα C_e, C_{e_1} και C_{e_2}. Αφού η κβαντική κατάσταση περάσει από το C_e, με μια μετάθεση φέρνουμε το qubit που αντιστοιχεί στην έκφραση e πρώτο και με βάση αυτό και τα C_{e_1}, C_{e_2} κατασκευάζουμε ένα κύκλωμα κβαντικής διακλάδωσης. Όπως είναι αναμενόμενο τα C_{e_1}, C_{e_2} είναι αγνά κυκλώματα, ενώ τα C'_{e_1}, C'_{e_2} είναι απλά παράλληλες συνθέσεις των C_{e_1}, C_{e_2} με ταυτοτικά κυκλώματα προκειμένου να δέχονται $max(m_1, m_2)$ καλώδια σωρού. Τέλος εφαρμόζουμε την αντίστροφη μετάθεση για να φέρουμε το qubit διακλάδωσης στην αρχική του θέση.



- *Κανόνας IFM*

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

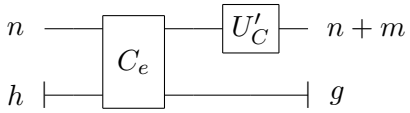
Αρκετά παρόμοια με την προηγούμενη περίπτωση. Η διαφορά τώρα είναι ότι το qubit διακλάδωσης αρχικά 'αντιγράφεται' μέσω μίας πύλης CNOT προκειμένου να μπορεί να χρησιμοποιηθεί στις δύο διακλαδώσεις και στο τέλος μετράμε το πρωτότυπο οπότε το αντίγραφο πηγαίνει στην κατάσταση που μετρήσαμε και το πρωτότυπο τοποθετείται στα σκουπίδια. Μία ακόμα διαφορά είναι ότι τώρα δεν είναι απαραίτητο τα C_{e_1}, C_{e_2} να είναι αγνά. Αυτή είναι η μοναδική περίπτωση κυκλώματος που δημιουργεί σκουπίδια, δηλαδή πραγματοποιεί μέτρηση.



- *Κανόνας TRANS*

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

Από το επαγωγικό βήμα διαθέτουμε το C_e το οποίο συνθέτουμε σειριακά με το U'_C το όποιο είναι το κύκλωμα που αντιστοιχεί στον ορθομοναδιαίο μετασχηματισμό C επεκτεταμένο ώστε να αφήνει αναλλοίωτα τα qubits που δεν συμμετέχουν στον μετασχηματισμό.



Κεφάλαιο 4

Κβαντικοί υπολογισμοί με κλασική χροιά στην nQML

4.1 Εισαγωγή

Μία από τις σπουδαιότερες λειτουργίες που επιτελεί μία γλώσσα προγραμματισμού είναι να προσφέρει στον προγραμματιστή τις κατάλληλες αφαιρέσεις οι οποίες θα τον διευκολύνουν στην διατύπωση αλγορίθμων, θα μειώσουν το μέγεθος του προγράμματος και θα το κάνουν πιο κατανοητό, θα επιτρέψουν την επαναχρησιμοποίηση του κώδικα και θα βοηθήσουν στην επέκταση και την συντήρηση των προγραμμάτων. Η ανάγκη για την εύρεση νέων αφαιρέσεων είναι ακόμα πιο επιβεβλημένη στις κβαντικές γλώσσες προγραμματισμού, καθώς πρόκειται για έναν κλάδο ο οποίος βρίσκεται σε πολύ πρώιμο στάδιο. Από τα δεδομένα που έχουμε συνηθίσει στις κλασικές γλώσσες προγραμματισμού είναι ανεπίτρεπτο ο κβαντικός προγραμματισμός να γίνεται προδιαγράφοντας ένα κβαντικό κύκλωμα ή ορίζοντας έναν ορθομοναδιαίο μετασχηματισμό. Αυτές οι λειτουργίες δεν πρέπει να βρίσκονται στην επιφάνεια, αλλά να είναι καλά κρυμμένες κάτω από τις κατάλληλες αφαιρέσεις.

Ουσιαστικά η μοναδική αφαίρεση που έχει γίνει στον κβαντικό προγραμματισμό είναι ο τελεστής της κβαντικής διακλάδωσης. Ο τελεστής αυτός εκμεταλλεύεται την αρχή της υπέρθεσης και δίνει την δυνατότητα στον υπολογισμό να προχωράει όντας σε μία υπέρθεση των δύο διακλαδώσεων, δηλαδή σαν να εκτελεί παράλληλα και τις δύο διακλαδώσεις. Πρόκειται για έναν τελεστή που γενικεύει τον τελεστή κλασικής διακλάδωσης και έτσι μπορεί να γίνει εύκολα κατανοητός και να χρησιμοποιηθεί ευρέος από έναν προγραμματιστή που έχει συνηθίσει να προγραμματίζει σε μία κλασική γλώσσα.

Στα πλαίσια αυτής της διπλωματικής γίνεται μία προσπάθεια δημιουργίας ενός τελεστή ο οποίος θα παρέχει στον προγραμματιστή αντίστοιχες διευκολύνσεις με αυτές του τελεστή κβαντικής διακλάδωσης. Δηλαδή θα παίρνει στοιχεία από τον κλασικό προγραμματισμό, με τα οποία οι προγραμματιστές είναι ήδη εξοικειωμένοι, και θα τα προσαρμόζει στα πλαίσια του κβαντικού προγραμματισμού. Ένα τέτοιο στοιχείο είναι και η χρήση παραλληλισμού στα κλασικά προγράμματα. Οι σημερινοί υπολογιστές έχουν στην διάθεση τους πολλούς επεξεργαστές και για αυτό τον λόγο γράφουμε παράλληλο κώδικα ο οποίος μοιράζει τους υπολογισμούς σε όλους τους διαθέσιμους επεξεργαστές. Αντίστοιχα στους κβαντικούς υπολογιστές έχουμε την αρχή της υπέρθεσης ή αλλιώς τον κβαντικό παραλληλισμό. Σε αυτή την περίπτωση ένας κβαντικός επεξεργαστής είναι σε θέση να διενεργεί ταυτόχρονα πολλούς υπολογισμούς χρησιμοποιώντας το γεγονός ότι το κβαντικό σύστημα βρίσκεται σε πολλές καταστάσεις ταυτόχρονα. Ο κβαντικός παραλληλισμός είναι που δίνει το συγκριτικό πλεονέκτημα στους κβαντικούς υπολογιστές έναντι των κλασικών. Είναι επόμενο λοιπόν να γίνει μία προσπάθεια μεταφοράς, γενίκευσης στοιχείων που έχουμε συνηθίσει από τον κλασικό παράλληλο προγραμματισμό στον κβαντικό προγραμματισμό. Στο έργο αυτό θα μας φανεί ιδιαίτερα χρήσιμο το γεγονός ότι οι Boolean συναρτήσεις μπορούν να υπολογιστούν από έναν κβαντικό υπολογιστή. Αυτό εκ πρώτης όψεως μπορεί να παρουσιάζει δυσκολίες καθώς όπως γνωρίζουμε οι κβαντικοί υπολογισμοί που δεν περιλαμβάνουν μέτρηση πρέπει να είναι αντιστρέψιμοι, ενώ γενικά οι Boolean συναρτήσεις δεν είναι. Οι δυσκολίες όμως θα ξεπεραστούν.

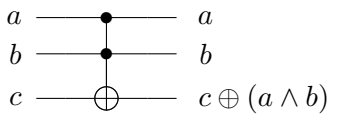
Συνοψίζοντας, έχουμε εντοπίσει δύο κλασικά στοιχεία, τον παραλληλισμό και τις Boolean συναρτήσεις, τα οποία φαίνεται να έχουν και κάποιο κβαντικό αντίτυπο. Θα δοκιμάσουμε λοιπόν να προσεγγίσουμε τις κβαντικές τους μορφές και να δούμε αν και κατά πόσο μπορούν να συνεισφέρουν στην δημιουργία αφαιρέσεων στον κβαντικό προγραμματισμό.

4.2 Μετατροπή κλασικών κυκλωμάτων σε κβαντικά

Όπως έχουμε δει, ένα κβαντικό κύκλωμα το οποίο δρα πάνω σε n qubits αντιστοιχεί σε έναν ορθομοναδιαίο μετασχηματισμό U διάστασης $2^n \times 2^n$. Αφού ο U είναι ορθομοναδιαίος μετασχηματισμός αυτό σημαίνει ότι ο $U^\dagger$ είναι ο αντίστροφος του. Συνεπώς, κάθε κβαντικό κύκλωμα έχει και το αντίστροφο του. Ορισμένα παραδείγματα από τους ορθομοναδιαίους μετασχηματισμούς που έχουμε δει μέχρι τώρα είναι: $H^{-1} = H^\dagger = H, \quad CNOT^{-1} = CNOT^\dagger = CNOT, \quad R_\theta^{-1} = R_\theta^\dagger = R_{-\theta}$.

Η αναγκαιότητα για αντιστρέψιμα κβαντικά κυκλώματα θέτει κάποιες δυσκολίες στην κατασκευή κβαντικών κυκλωμάτων από κλασικά κυκλώματα, καθώς τα κλασικά κυκλώματα στην πλειονότητα των περιπτώσεων δεν είναι αντιστρέψιμα. Πιο συγκεκριμένα ας υποθέσουμε ότι διαθέτουμε ένα κλασικό κύκλωμα το οποίο δέχεται ως είσοδο ένα $x \in \{0,1\}^n$ και στην έξοδο του παίρνουμε το $f(x) \in \{0,1\}^m$. Το κύκλωμα αυτό αντιστοιχεί σε έναν πίνακα μετασχηματισμού διάστασης $2^m \times 2^n$, ο οποίος δέχεται ως είσοδο ένα διάνυσμα βάσης $|x\rangle$ του χώρου $\mathbb{C}^{2^n}$ και δίνει ως έξοδο ένα διάνυσμα βάσης $|f(x)\rangle$ του χώρου $\mathbb{C}^{2^m}$. Όπως γίνεται εύκολα αντιληπτό προκείμενου το κλασικό κύκλωμα να είναι αντιστρέψιμο θα πρέπει πρώτα από όλα να ισχύει ότι $n = m$, δηλαδή ότι ο πίνακας μετασχηματισμού είναι τετραγωνικός, και έπειτα θα πρέπει η συνάρτηση $f : \{0,1\}^n \to \{0,1\}^n$ να είναι μία μετάθεση, δηλαδή ο πίνακας μετασχηματισμού να είναι αντιστρέψιμος και μάλιστα ο αντίστροφος του να ισούται με τον ανάστροφο συζυγή του. Οπότε σε αυτή την περίπτωση ο πίνακας μετασχηματισμού είναι ορθομοναδιαίος και όντως μπορούμε να μεταβούμε από το κλασικό στο αντίστοιχο κβαντικό κύκλωμα.

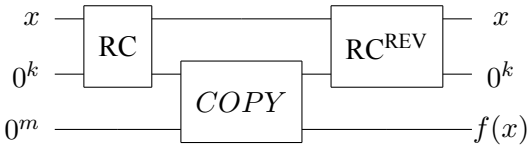
Ας δούμε όμως τι μπορούμε να κάνουμε στην γενική περίπτωση. Υποθέτουμε ότι τα κλασικά κυκλώματα για τα οποία θέλουμε να δώσουμε το κβαντικό ισοδύναμο θα αποτελούνται μόνο από μεταθέσεις των καλωδίων, πύλες NOT και πύλες AND, μία απαίτηση η οποία δεν βλάπτει την γενικότητα καθώς η πύλη NOT μαζί με την πύλη AND αποτελούν ένα καθολικό σύνολο πυλών. Οι μεταθέσεις των καλωδίων είναι αντιστρέψιμες όπως και οι πύλες NOT και ως εκ τούτου το πρόβλημα πηγάζει από την μη αντιστρεψιμότητα της πύλης AND όπως την έχουμε συνηθίσει. Από την στιγμή που δέχεται ως είσοδο δύο καλώδια και δίνει ως έξοδο μόνο ένα, σε αυτή την μορφή δεν θα μπορούσε να ήταν αντιστρέψιμη. Παρόλα αυτά υπάρχει μία άλλη πύλη, η πύλη Toffoli, η οποία προσομοιώνει την λειτουργία της AND και είναι αντιστρέψιμη. Η πύλη Toffoli δέχεται τρεις εισόδους, και ασφαλώς έχει τρεις εξόδους, όπου οι δύο πρώτες μεταφέρονται στην έξοδο αναλλοίωτες και λειτουργούν ως ελεγκτές της τρίτης. Δηλαδή αν οι δύο πρώτες είσοδοι έχουν την τιμή λογικό ένα τότε η τιμή της τρίτης αντιστρέφεται, ενώ διαφορετικά μένει αμετάβλητη. Το κύκλωμα της πύλης Toffoli είναι:



Η πύλη Toffoli μπορεί να προσομοιώσει την πύλη AND αφού $(a, b, 0) \xrightarrow{\text{Toffoli}} (a, b, 0 \oplus (a \wedge b)) = (a, b, a \wedge b)$. Άρα αν πάμε στο αρχικό κλασικό κύκλωμα C και αντικαταστήσουμε όλες τις πύλες AND με πύλες Toffoli τότε θα πάρουμε ένα αντιστρέψιμο κύκλωμα RC που θα υπολογίζει την ίδια συνάρτηση με το C, αλλά θα δέχεται μερικές επιπλέον εισόδους αρχικοποιημένες στης λογική τιμή μηδέν και θα δίνει μερικές επιπλέον εξόδους των οποίων το αποτέλεσμα δεν θα είναι προκαθορισμένο αλλά μία συνάρτηση της εισόδου. Για την ακρίβεια οι επιπλέον είσοδοι θα είναι τόσες όσες και οι πύλες Toffoli, ενώ οι επιπλέον έξοδοι θα είναι διπλάσιες από τις πύλες Toffoli.

Θα μπορούσαμε να σταματήσουμε εδώ καθώς έχουμε στην διάθεση μας ένα αντιστρέψιμο κύκλωμα, αλλά το γεγονός ότι αυτό δίνει πέραν του ζητούμενου υπολογισμού και μερικές επιπλέον εξόδους με ακαθόριστες τιμές μας προβληματίζει καθώς στην κβαντική περίπτωση μία από αυτές θα μπορούσε εξ αιτίας κάποιου σφάλματος να μετρηθεί και έτσι πιθανότατα να καταστρέψει το αποτέλεσμα του υπολογισμού. Για αυτό στόχος μας τώρα είναι να κάνουμε τις επιπλέον εξόδους να έχουν προκαθορισμένη τιμή. Για να το πετύχουμε αυτό θα χρησιμοποιήσουμε το γεγονός ότι το RC είναι ένα αντιστρέψιμο κύκλωμα, του οποίου το αντίστροφο είναι το RC^{REV}. Έτσι αφού η είσοδος περάσει από το κύκλωμα RC και γίνει ο ζητούμενος υπολογισμός, θα αντιγράψουμε μέσω μιας συστοιχίας πυ-

λών CNOT το αποτέλεσμα του υπολογισμού σε κάποια καινούρια bits ώστε στο τέλος να χρησιμοποιήσουμε το κύκλωμα RC^{REV} ώστε να επαναφέρουμε τα επιπλέον bit εξόδου από ακαθόριστες τιμές στην τιμή λογικό μηδέν. Η αντιγραφή του αποτελέσματος είναι επιβεβλημένη καθώς μετά την χρήση του κυκλώματος RC^{REV} το αποτέλεσμα $f(x) \in \{0,1\}^m$ μεταβαίνει σε 0^m. Τα βήματα που ακολουθούμε είναι τα εξής: $(x, 0^k, 0^m) \xrightarrow{\text{RC}} (\text{garbage}_x, f(x), 0^m) \xrightarrow{\text{COPY}} (\text{garbage}_x, f(x), f(x)) \xrightarrow{\text{RC}^{\text{REV}}} (x, 0^k, f(x))$. Και σε μορφή κυκλώματος:



Έχουμε λοιπόν ότι ο ορθομοναδιαίος μετασχηματισμός μέσω του οποίου μπορούμε να υπολογίσουμε μία συνάρτηση $f : \{0,1\}^n \to \{0,1\}^m$ είναι ο $U_f = (U_{RC} \otimes I_m)^\dagger \cdot (I_n \otimes U_{COPY}) \cdot (U_{RC} \otimes I_m)$. Μέσω του μετασχηματισμού αυτού στην κλασική περίπτωση έχουμε ότι: $|x\rangle \otimes |0^k\rangle \otimes |0^m\rangle \xrightarrow{U_f} |x\rangle \otimes |0^k\rangle \otimes |f(x)\rangle$, ενώ στην περίπτωση που έχουμε ως είσοδο μία υπέρθεση ο μετασχηματισμός λειτουργεί ως εξής: $\sum_{x\in\{0,1\}^n} a_x \cdot |x\rangle \otimes |0^k\rangle \otimes |0^m\rangle \xrightarrow{U_f} \sum_{x\in\{0,1\}^n} a_x \cdot |x\rangle \otimes |0^k\rangle \otimes |f(x)\rangle$.

4.3 Επέκταση του συντακτικού της nQML

Στο σημείο αυτό επεκτείνουμε το συντακτικό της nQML προσθέτοντας έναν καινούριο τελεστή στις κβαντικές εκφράσεις e και δημιουργώντας ένα ακόμα μη τερματικό σύμβολο b για τις Boolean εκφράσεις το οποίο εμφανίζεται μόνο στον καινούριο τελεστή.

⟨*e*⟩ ::= ...
| **spawn** $\backslash\ (x_1,\ \ldots,\ x_k) ->\ (b_1,\ \ldots,\ b_l)$

⟨*b*⟩ ::= x
| **false**
| **true**
| ! b
| b_1 & b_2
| b_1 | b_2
| b_1 @ b_2
| (b)

Ο ρόλος του τελεστή **spawn** $\backslash\ (x_1,\ \ldots,\ x_k) ->\ (b_1,\ \ldots,\ b_l)$ είναι να δέχεται ως όρισμα μία κλασική συνάρτηση $f : \{0,1\}^k \to \{0,1\}^l$ και να δημιουργεί μία υπέρθεση όλων των δυνατών τιμών του πεδίου ορισμού της, συζευγμένων με το αντίστοιχο αποτέλεσμα της εφαρμογής της συνάρτησης. Κάθε στοιχείο της υπέρθεσης αυτής θα εμφανίζεται με το ίδιο πλάτος. Όπως είναι φυσικό ο τελεστής αυτός θα αντλεί την σημασιολογία του υπό την μορφή κβαντικού κυκλώματος από την κατασκευή της προηγούμενης ενότητας. Η συνάρτηση που δίνεται ως όρισμα είναι μία απολύτως κλασική συνάρτηση σαν και αυτές που οι προγραμματιστές είναι συνηθισμένοι να γράφουν. Δεν υπεισέρχονται ούτε περιορισμοί γραμμικότητας, ούτε το θεώρημα της μη κλωνοποίησης. Ο προγραμματιστής είναι απολύτως ελεύθερος να χειριστεί τις μεταβλητές $x_1,\ \ldots,\ x_k$ ως κλασικές μεταβλητές. Ο τρόπος έκφρασης της συνάρτησης, σε αυτή την μορφή της nQML, ναι μεν είναι κάπως πρωτόγονος και δύσχρηστος πλην όμως είναι υπολογιστικά πλήρης για τις υπολογίσιμες συναρτήσεις $f : \{0,1\}^k \to \{0,1\}^l$ για κάθε $k, l \geq 1$. Σίγουρα θα μπορούσαμε να εισάγουμε τελεστές όπως η πρόσθεση, η αφαίρεση, ο πολλαπλασιασμός και άλλους ώστε να απλοποιήσουμε τα πράγματα. Επιπλέον, μπορούμε να ισχυριστούμε ότι ο τελεστής αυτός θα αφομοιωθεί εύκολα από έναν προγραμματιστή καθώς αντλεί στοιχεία από

τον παράλληλο προγραμματισμό. Μπορεί να ιδωθεί ως το έναυσμα του παράλληλου υπολογισμού της συνάρτησης $f : \{0,1\}^k \to \{0,1\}^l$ για κάθε τιμή του πεδίου ορισμού της σε έναν κλασικό υπολογιστή που διαθέτει 2^k επεξεργαστικές μονάδες. Στην πραγματικότητα όμως θα υπάρχει μονάχα μία κβαντική μονάδα επεξεργασίας. Αυτό το τεράστιο πλεονέκτημα θα συνοδεύεται με το γεγονός ότι δεν θα έχουμε άμεση πρόσβαση και στα 2^k αποτελέσματα, αλλά για να τα επεξεργαστούμε και να εξάγουμε τις πληροφορίες που μας ενδιαφέρουν θα πρέπει να καταφύγουμε σε κβαντικές στρατηγικές. Αυτές οι κβαντικές στρατηγικές δεν φαίνεται ακόμα πως μπορούν να μπουν σε ένα καλούπι καθώς διαφοροποιούνται από αλγόριθμο σε αλγόριθμο, αλλά και το ίδιο το δείγμα δεν είναι ακόμα αρκετά μεγάλο. Σίγουρα, αν κάποια στιγμή γίνει μία αφαίρεση στις κβαντικές στρατηγικές τότε θα έχει γίνει ένα μεγάλο βήμα για την δημιουργία μίας καλής και διαισθητικής γλώσσας κβαντικού προγραμματισμού.

4.4 Επέκταση του συστήματος τύπων της nQML

Θα συνεχίσουμε βλέποντας πως επηρεάζει ο νέος τελεστής την σχέση τυποποίησης αλλά και ποιος είναι ο κανόνας τυποποίησης του. Η σχέση τυποποίησης από πενταμελής γίνεται επταμελής ώστε να παρακολουθεί τα qubits σκουπίδια και την νέα κατηγορία από qubits που μπορεί να χρειάζεται μία κβαντική έκφραση για τον υπολογισμό της. Ένα qubit που ανήκει στην νέα αυτή κατηγορία έχει την ιδιότητα να ξεκινά πριν την αποτίμηση της έκφρασης στην κατάσταση $|0\rangle$, κατά τον υπολογισμό της έκφρασης να μεταβάλλεται η τιμή του και στο τέλος της αποτίμησης η τιμή του να επανέρχεται στην κατάσταση $|0\rangle$. Τα qubits που ανήκουν σε αυτήν την κατηγορία θα τα ονομάζουμε υπηρέτες. Τα qubits υπηρέτες είναι χρήσιμα μόνο στον καινούριο τελεστή που προσθέσαμε στην γλώσσα και εξ αιτίας της ιδιότητας τους, να ξεκινούν από την κατάσταση $|0\rangle$ και να καταλήγουν στην κατάσταση $|0\rangle$, μπορούν να επαναχρησιμοποιηθούν για τον υπολογισμό πολλών κβαντικών εκφράσεων. Έχουμε λοιπόν, ότι η σχέση τυποποίησης είναι της μορφής: $\Gamma; n \vdash^{\alpha} e : \tau; m; g; a$, όπου ο φυσικός αριθμός n αντιπροσωπεύει το πλήθος των qubit στην κβαντική κατάσταση πριν ξεκινήσει η αποτίμηση της έκφρασης e, ο φυσικός αριθμός m δηλώνει το πλήθος των qubit που δημιουργούνται από την έκφραση e, ο φυσικός αριθμός g αναπαριστά το πλήθος των μετρήσεων που πραγματοποιούνται κατά τον υπολογισμό της έκφρασης e και ο φυσικός αριθμός a αντιπροσωπεύει το πλήθος των qubit υπηρετών που απαιτούνται για τον υπολογισμό της έκφρασης e. Όπως είναι φυσικό οι αγνές εκφράσεις δεν δημιουργούν qubits σκουπίδια και έτσι όλα τα στοιχεία της αγνής σχέσης τυποποιήσης θα είναι της μορφής: $\Gamma; n \vdash e : \tau; m; 0; a$.

Ας δούμε τώρα τον ορισμό της σχέσης τυποποίησης:

- Πρώτα από όλα, η σχέση υποσυνόλου η οποία συνδέει τις δύο σχέσεις τυποποίησης εκφράζεται με τον ακόλουθο κανόνα.

$$\frac{\Gamma; n \vdash^{\circ} e : \tau; m; 0; a}{\Gamma; n \vdash e : \tau; m; 0; a} \text{ (EMB)}$$

- Για τις μεταβλητές ψάχνουμε απλά τον τύπο τους στο περιβάλλον. Η αποτίμηση μίας μεταβλητής δεν απαιτεί κάποιο qubit υπηρέτη.

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

- Ο κατασκευαστής των qubit ελέγχει ότι οι παράμετροι λ, λ' ορίζουν έναν ορθομοναδιαίο μετασχηματισμό και προσθέτει ένα επιπλέον qubit στην κβαντική κατάσταση. Η έκφραση αυτή δεν χρειάζεται qubits υπηρέτες προκειμένου να αποτιμηθεί.

$$\frac{|\lambda|^2 + |\lambda'|^2 = 1 \qquad \lambda \cdot \overline{\lambda'} = \overline{\lambda} \cdot \lambda'}{\Gamma; n \vdash^{\circ} \{\ (\lambda)\textbf{qfalse} + (\lambda')\textbf{qtrue}\ \} : \textbf{qbit}[n]; 1; 0; 0} \text{ (SUP)}$$

- Ο καινούριος τελεστής δεν έχει κάποια προϋπόθεση για την εφαρμογή του. Δημιουργεί $k+l$ νέα qubits, όπου στα k πρώτα αποθηκεύεται μία υπέρθεση όλων των δυνατών τιμών του πεδίου ορισμού της κλασικής συνάρτησης $\setminus\ (x_1,\ \ldots,\ x_k) ->\ (b_1,\ \ldots,\ b_l)$ και στα υπόλοιπα l η αντίστοιχη τιμή του αποτελέσματος της συνάρτησης. Ο κανόνας αυτός είναι και ο μοναδικός που δημιουργεί qubits υπηρέτες.

$$\frac{}{\begin{array}{c}\Gamma; n \vdash^{\circ} \textbf{spawn}\ \ \setminus\ (x_1,\ \ldots,\ x_k) ->\ (b_1,\ \ldots,\ b_l) : \\ (\textbf{qbit}[n] \otimes (\cdots \otimes (\textbf{qbit}[n+k-1]) \ldots)) \otimes (\textbf{qbit}[n+k] \otimes (\cdots \otimes (\textbf{qbit}[n+k+l-1]) \ldots)) ; \\ k+l; 0; \max\limits_{i \in \{1,\ldots,l\}} \{anc(b_i)\}\end{array}} \text{ (SPAWN)}$$

  Το πλήθος των qubit υπηρετών εξαρτάται από την κλασική συνάρτηση και δίνεται με την βοήθεια της σχέσης:

```
anc(x)       = 1
anc(false)   = 1
anc(true)    = 1
anc(!b)      = anc(b)
anc(b1 & b2) = 1 + anc(b1 & b2)
anc(b1 | b2) = anc(!(!b1) & (!b2)))
anc(b1 @ b2) = anc(!(!(b1 & (!b2))) & (!(!b1) & b2))))
anc((b))     = anc(b)
```

- Οι κανόνες για τον ορισμό σταθερών, την δημιουργία γινομένων και την αποσύνθεση γινομένων παρουσιάζουν μεγάλες ομοιότητες για αυτό και τους παραθέτουμε μαζί. Πρέπει να σημειώσουμε ότι η επαναχρησιμοποίηση των qubit υπηρετών φαίνεται από την επιλογή του $max(a_1, a_2)$ για την συνολική έκφραση.

$$\frac{\Gamma; n \vdash^{\alpha} e_1 : \tau_1; m_1; g_1; a_1 \qquad \Gamma, x : \tau_1; n + m_1 \vdash^{\alpha} e_2 : \tau; m_2; g_2; a_2}{\Gamma; n \vdash^{\alpha} \textbf{let}\ x = e_1\ \textbf{in}\ e_2 : \tau; m_1 + m_2; g_1 + g_2; max(a_1, a_2)} \text{ (LET)}$$

$$\frac{\Gamma; n \vdash^{\alpha} e_1 : \tau_1; m_1; g_1; a_1 \qquad \Gamma; n + m_1 \vdash^{\alpha} e_2 : \tau_2; m_2; g_2; a_2}{\Gamma; n \vdash^{\alpha} (e_1, e_2) : \tau_1 \otimes \tau_2; m_1 + m_2; g_1 + g_2; max(a_1, a_2)} \text{ (PROD)}$$

$$\frac{\Gamma; n \vdash^{\alpha} e_1 : \tau_1 \otimes \tau_2; m_1; g_1; a_1 \qquad \Gamma, x_1 : \tau_1, x_2 : \tau_2; n + m_1 \vdash^{\alpha} e_2 : \tau; m_2; g_2; a_2}{\Gamma; n \vdash^{\alpha} \textbf{let}\ (x_1, x_2) = e_1\ \textbf{in}\ e_2 : \tau; m_1 + m_2; g_1 + g_2; max(a_1, a_2)} \text{ (LETPROD)}$$

- Ο κανόνας τυποποίησης για τον τελεστή κβαντικής διακλάδωσης φροντίζει ώστε το qubit της συνθήκης να μην χρησιμοποιείται σε κανέναν από τους δύο κλάδους. Για το λόγο αυτό με $\Gamma|_k$ συμβολίζουμε το περιβάλλον Γ περιορισμένο ώστε να μην περιέχει μεταβλητές των οποίων οι τύποι χρησιμοποιούν το $k-$οστό qubit της κβαντικής κατάστασης. Αυτός ο περιορισμός τίθεται για να απλοποιηθεί τόσο η σημασιολογία του τελεστή όσο και ο κανόνας τυποποίησης. Και πάλι επιλέγουμε ως qubits υπηρέτες για την συνολική έκφραση το $max(a, a_1, a_2)$, επωφελούμενοι της ιδιότητας τους να μπορούν να επαναχρησιμοποιηθούν.

$$\frac{\Gamma; n \vdash^{\alpha} e : \textbf{qbit}[k]; m; g; a \qquad \Gamma|_k; n + m \vdash^{\circ} e_1 : \tau; m_1; 0; a_1 \qquad \Gamma|_k; n + m \vdash^{\circ} e_2 : \tau; m_2; 0; a_2}{\Gamma; n \vdash^{\alpha} \textbf{if}\ e\ \textbf{then}\ e_1\ \textbf{else}\ e_2 : \tau; m + max(m_1, m_2); g; max(a, a_1, a_2)} \text{ (IF)}$$

- Ο κανόνας τυποποίησης για τον τελεστή που πραγματοποιεί μέτρηση σε ένα qubit και κατόπιν με βάση το αποτέλεσμα της μέτρησης πραγματοποιεί κλασική διακλάδωση δεν παρουσιάζει δυσκολίες.

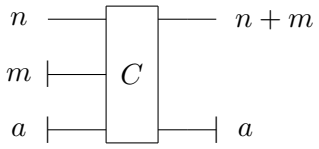
$$\frac{\Gamma; n \vdash e : \textbf{qbit}[k]; m; g; a \qquad \Gamma; n + m \vdash e_1 : \tau; m_1; g_1; a_1 \qquad \Gamma; n + m \vdash e_2 : \tau; m_2; g_2; a_2}{\Gamma; n \vdash \textbf{ifm}\ e\ \textbf{then}\ e_1\ \textbf{else}\ e_2 : \tau; m + max(m_1, m_2); 1 + g + g_1 + g_2; max(a, a_2, a_2)} \text{ (IFM)}$$

- Για τον τελεστή $|e\rangle \to x, x'.c$ το σύστημα τύπων διασφαλίζει ότι ο τύπος τ της έκφρασης e θα είναι αγνός, δηλαδή δεν θα αναφέρετε παραπάνω από μία φορές σε ένα qubit, έτσι ώστε να μην παραβιάζεται το θεώρημα της μη κλωνοποίησης. Επιπλέον, αυτό είναι το μοναδικό σημείο στο οποίο κάνουμε χρήση του ελέγχου τύπων για κλασικές εκφράσεις. Με $C(\tau)$ συμβολίζουμε το κλασικό τύπο ο οποίος αντιστοιχεί στον κβαντικό τύπο τ. Ο έλεγχος τύπων για τις κλασικές εκφράσεις είναι τετριμμένος και για αυτό δεν θα επεκταθούμε περαιτέρω.

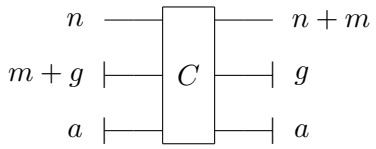
$$\frac{\Gamma; n \vdash^{\alpha} e : \tau; m; g; a \qquad \textbf{pure}(\tau) \qquad x : C(\tau), x' : C(\tau) \vdash c : \textbf{complex}}{\Gamma; n \vdash^{\alpha} |e\rangle \to x, x'.c : \tau; m; g; a} \text{ (TRANS)}$$

4.5 Επεκτεταμένη δηλωτική σημασιολογία υπό την μορφή κβαντικών κυκλωμάτων

Στο προηγούμενο κεφάλαιο είδαμε ότι μπορούμε να ερμηνεύσουμε τις εκφράσεις της nQML ως κβαντικά κυκλώματα. Μάλιστα επειδή η σημασιολογία αυτή είναι υπό την μορφή κυκλωμάτων, τα οποία μπορούν να αποτελέσουν μια φυσική υλοποίηση των προγραμμάτων, ισχυριστήκαμε ότι μπορούμε να δούμε την απόδοση ερμηνείας και ως ένα είδος μεταγλώττισης. Τώρα θα επεκτείνουμε την σημασιολογία αυτή ώστε να λαμβάνει υπόψιν τον νέο τελεστή και τα qubits υπηρέτες. Πλέον διαχωρίζουμε τα qubits εισόδου σε καθαρές εισόδους, σωρό και υπηρέτες, και τα qubits εξόδου σε καθαρές εξόδους, σκουπίδια και υπηρέτες. Προφανώς τα qubits υπηρέτες της εισόδου θα είναι τόσα όσα και τα qubits υπηρέτες της εξόδου, καθώς και οι συνολικές είσοδοι του κυκλώματος θα ισούνται με τις συνολικές του εξόδους. Ένα αγνό κύκλωμα, δηλαδή ένα κβαντικό κύκλωμα που δεν περιλαμβάνει μέτρηση, θα είναι πλέον της μορφής:



ενώ γενικά ένα κβαντικό κύκλωμα θα είναι της μορφής:



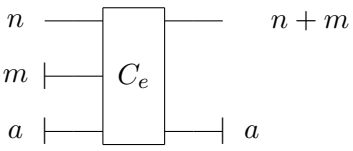
Έτσι λοιπόν η σημασία των εκφράσεων που τυποποιούνται σύμφωνα με το αγνό σύστημα τύπων θα είναι ένα αγνό κύκλωμα, ενώ γενικά μία έκφραση nQML που επιδέχεται τύπου θα έχει ως σημασία ένα κβαντικό κύκλωμα.

Είμαστε τώρα έτοιμοι να δώσουμε μια ερμηνεία στην γλώσσα μας με την μορφή κβαντικών κυκλωμάτων. Θα ορίσουμε την ερμηνεία με επαγωγή στους κανόνες τυποποίησης.

- *Κανόνας EMB*

$$\frac{\Gamma; n \vdash^{\circ} e : \tau; m; 0; a}{\Gamma; n \vdash e : \tau; m; 0; a} \text{ (EMB)}$$

Η περίπτωση αυτή είναι τετριμμένη αφού το προκύπτον κύκλωμα ταυτίζεται με αυτό του επαγωγικού βήματος.



- *Κανόνας VAR*

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

Απλή περίπτωση και αυτή αφού το προκύπτον κύκλωμα είναι απλά το ταυτοτικό κύκλωμα.

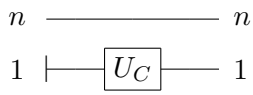
$$n \quad \text{———} \quad n$$

- *Κανόνας SUP*

$$\frac{|\lambda|^2+|\lambda'|^2=1 \qquad \lambda\cdot\overline{\lambda'}=\overline{\lambda}\cdot\lambda'}{\Gamma; n \vdash^{\circ} \{\ (\lambda)\mathbf{qfalse} + (\lambda')\mathbf{qtrue}\ \} : \mathbf{qbit}[n]; 1; 0; 0}\ (\text{SUP})$$

Σε αυτή την περίπτωση τα qubits της αρχικής κβαντικής κατάστασης μετασχηματίζονται από το ταυτοτικό κύκλωμα, ενώ στην νέα κατάσταση προστίθεται ένα ακόμα qubit το οποίο αρχικοποιείται στην κατάσταση $|0\rangle$ και κατόπιν μετασχηματίζεται με βάση τον ορθομοναδιαίο μετασχηματισμό:

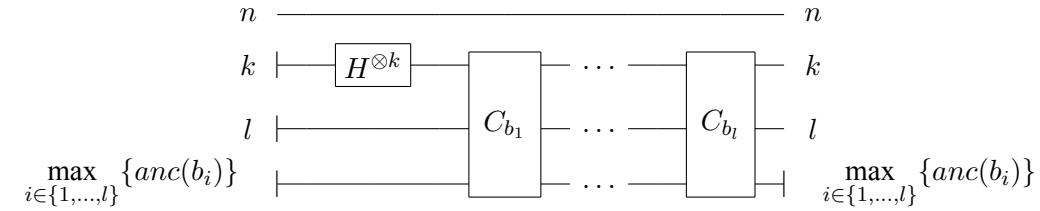
$$\begin{pmatrix} \lambda & \lambda' \\ \lambda' & -\lambda \end{pmatrix}$$



- *Κανόνας SPAWN*

$$\frac{}{\begin{array}{c}\Gamma; n \vdash^{\circ} \mathbf{spawn}\ \ \backslash\ (x_1,\ \ldots,\ x_k) ->\ (b_1,\ \ldots,\ b_l) : \\ (\mathbf{qbit}[n] \otimes (\cdots \otimes (\mathbf{qbit}[n+k-1])\ldots)) \otimes (\mathbf{qbit}[n+k] \otimes (\cdots \otimes (\mathbf{qbit}[n+k+l-1])\ldots))\,; \\ k+l; 0;\ \max\limits_{i\in\{1,\ldots,l\}}\{anc(b_i)\}\end{array}}\ (\text{SPAWN})$$

Η ερμηνεία του νέου τελεστή χρησιμοποιεί την κατασκευή κβαντικού κυκλώματος από κλασική συνάρτηση που είχαμε δει νωρίτερα στο κεφάλαιο. Το κβαντικό κύκλωμα που αντιστοιχεί στην Boolean συνάρτηση $\backslash\ x_1\ \ldots\ x_k -> b_i$, επαυξημένο με ταυτοτικά κυκλώματα ώστε να διαδίδει τα υπόλοιπα $l-1$ καλώδια των άλλων b_i και τα υπόλοιπα $\max\limits_{i\in\{1,\ldots,l\}}\{anc(b_i)\} - anc(b_i)$ qubits υπηρέτες, το συμβολίζουμε με C_{b_i}. Αυτή είναι η μοναδική περίπτωση κυκλώματος που δημιουργεί qubits υπηρέτες. Μάλιστα, εξ αιτίας της ιδιότητας τους να ξεκινάνε από την κατάσταση $|0\rangle$ και να καταλήγουν στην κατάσταση $|0\rangle$ μπορούμε να τα επαναχρησιμοποιούμε στους υπολογισμούς των b_i. Για αυτό τον λόγο τα συνολικά qubits υπηρέτες που δημιουργεί αυτή η έκφραση είναι $\max\limits_{i\in\{1,\ldots,l\}}\{anc(b_i)\}$.



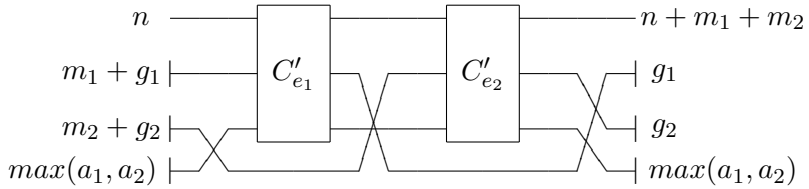
- *Κανόνες LET, PROD και LETPROD*

$$\frac{\Gamma; n \vdash^{\alpha} e_1 : \tau_1; m_1; g_1; a_1 \qquad \Gamma, x:\tau_1; n+m_1 \vdash^{\alpha} e_2 : \tau; m_2; g_2; a_2}{\Gamma; n \vdash^{\alpha} \mathbf{let}\ x = e_1\ \mathbf{in}\ e_2 : \tau; m_1+m_2; g_1+g_2; max(a_1,a_2)}\ (\text{LET})$$

$$\frac{\Gamma; n \vdash^{\alpha} e_1 : \tau_1; m_1; g_1; a_1 \qquad \Gamma; n + m_1 \vdash^{\alpha} e_2 : \tau_2; m_2; g_2; a_2}{\Gamma; n \vdash^{\alpha} (e_1, e_2) : \tau_1 \otimes \tau_2; m_1 + m_2; g_1 + g_2; max(a_1, a_2)} \text{ (PROD)}$$

$$\frac{\Gamma; n \vdash^{\alpha} e_1 : \tau_1 \otimes \tau_2; m_1; g_1; a_1 \qquad \Gamma, x_1 : \tau_1, x_2 : \tau_2; n + m_1 \vdash^{\alpha} e_2 : \tau; m_2; g_2; a_2}{\Gamma; n \vdash^{\alpha} \textbf{let } (x_1, x_2) = e_1 \textbf{ in } e_2 : \tau; m_1 + m_2; g_1 + g_2; max(a_1, a_2)} \text{ (LETPROD)}$$

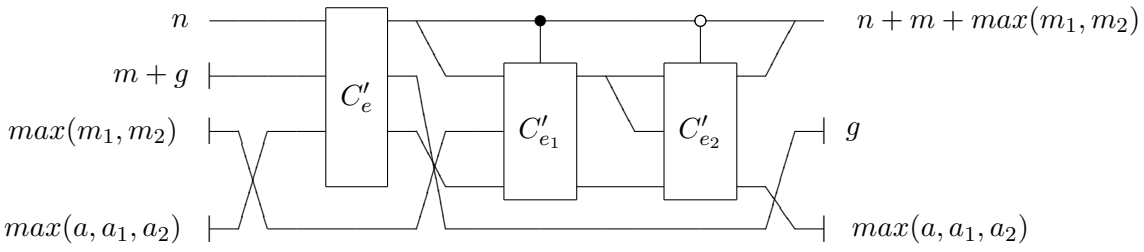
Και οι τρεις κανόνες δίνουν σαν αποτέλεσμα το ίδιο κύκλωμα για αυτό και τους παραθέτουμε μαζί. Ουσιαστικά πρόκειται για την σειριακή σύνθεση των κυκλωμάτων C_{e_1}, C_{e_2} που προκύπτουν από το επαγωγικό βήμα. Θα πρέπει να τονίσουμε ότι με βάση αυτό τον ορισμό η γλώσσα έχει call by value σημασιολογία και οι πλειάδες αποτιμώνται από αριστερά προς τα δεξιά. Επίσης, με C'_{e_1}, C'_{e_2} συμβολίζουμε την παράλληλη σύνθεση των C_{e_1}, C_{e_2} με ταυτοτικά κυκλώματα προκειμένου να δέχονται $max(a_1, a_2)$ qubits υπηρέτες.



- *Κανόνας IF*

$$\frac{\Gamma; n \vdash^{\alpha} e : \textbf{qbit}[k]; m; g; a \qquad \Gamma|_k; n + m \vdash^{\circ} e_1 : \tau; m_1; 0; a_1 \qquad \Gamma|_k; n + m \vdash^{\circ} e_2 : \tau; m_2; 0; a_2}{\Gamma; n \vdash^{\alpha} \textbf{if } e \textbf{ then } e_1 \textbf{ else } e_2 : \tau; m + max(m_1, m_2); g; max(a, a_1, a_2)} \text{ (IF)}$$

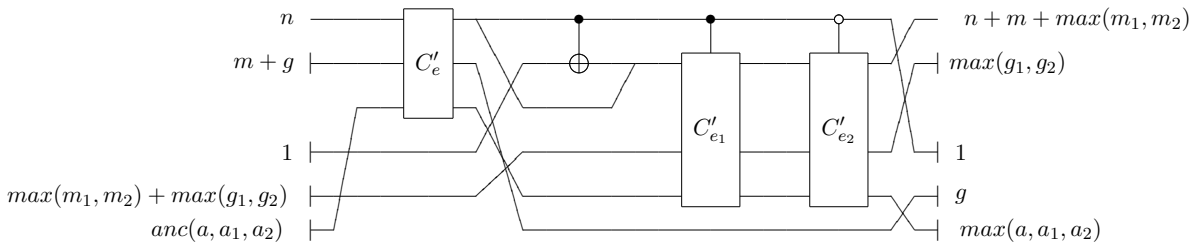
Στην περίπτωση αυτή, από το επαγωγικό βήμα έχουμε στην διάθεση μας τα κυκλώματα C_e, C_{e_1} και C_{e_2}. Αφού η κβαντική κατάσταση περάσει από το C'_e, το οποίο είναι απλά η παράλληλη σύνθεση του C_e με ένα ταυτοτικό κύκλωμα προκειμένου να δέχεται $max(a, a_1, a_2)$ qubits υπηρέτες, με μια μετάθεση φέρνουμε το qubit που αντιστοιχεί στην έκφραση e πρώτο και με βάση αυτό και τα C_{e_1}, C_{e_2} κατασκευάζουμε ένα κύκλωμα κβαντικής διακλάδωσης. Όπως είναι αναμενόμενο τα C_{e_1}, C_{e_2} είναι αγνά κυκλώματα, ενώ τα C'_{e_1}, C'_{e_2} είναι απλά παράλληλες συνθέσεις των C_{e_1}, C_{e_2} με ταυτοτικά κυκλώματα προκειμένου να δέχονται $max(m_1, m_2)$ qubits σωρού και $max(a, a_1, a_2)$ qubits υπηρέτες. Τέλος εφαρμόζουμε την αντίστροφη μετάθεση για να φέρουμε το qubit διακλάδωσης στην αρχική του θέση.



- *Κανόνας IFM*

$$\frac{\Gamma; n \vdash e : \textbf{qbit}[k]; m; g; a \qquad \Gamma; n + m \vdash e_1 : \tau; m_1; g_1; a_1 \qquad \Gamma; n + m \vdash e_2 : \tau; m_2; g_2; a_2}{\Gamma; n \vdash \textbf{ifm } e \textbf{ then } e_1 \textbf{ else } e_2 : \tau; m + max(m_1, m_2); 1 + g + g_2 + g_2; max(a, a_1, a_2)} \text{ (IFM)}$$

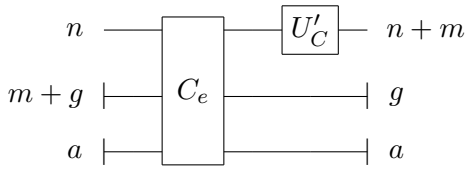
Αρκετά παρόμοια με την προηγούμενη περίπτωση. Η διαφορά τώρα είναι ότι το qubit διακλάδωσης αρχικά 'αντιγράφεται' μέσω μίας πύλης CNOT προκειμένου να μπορεί να χρησιμοποιηθεί στις δύο διακλαδώσεις και στο τέλος μετράμε το πρωτότυπο οπότε το αντίγραφο πηγαίνει στην κατάσταση που μετρήσαμε και το πρωτότυπο τοποθετείται στα σκουπίδια. Μία ακόμα διαφορά είναι ότι τώρα δεν είναι απαραίτητο τα C_{e_1}, C_{e_2} να είναι αγνά. Αυτή είναι η μοναδική περίπτωση κυκλώματος που δημιουργεί σκουπίδια, δηλαδή πραγματοποιεί μέτρηση.



- *Κανόνας TRANS*

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

Από το επαγωγικό βήμα διαθέτουμε το C_e το οποίο συνθέτουμε σειριακά με το U'_C το όποιο είναι το κύκλωμα που αντιστοιχεί στον ορθομοναδιαίο μετασχηματισμό C επεκτεταμένο ώστε να αφήνει αναλλοίωτα τα qubits που δεν συμμετέχουν στον μετασχηματισμό.



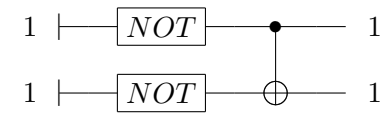
Η σημασιολογία αυτή ναι μεν φαίνεται να βρίσκεται κοντά σε μία φυσική υλοποίηση των προγραμμάτων nQML, αλλά δεν δίνει επαρκή πληροφορία για τις εκφράσεις της nQML οι οποίες θα περιμέναμε να έχουν τα ίδια αποτελέσματα μετά την εκτέλεση τους. Για παράδειγμα ας θεωρήσουμε τις εκφράσεις:

```
def e1 =
  let q1 = { (0)qfalse + (1)qtrue } in
  let q2 = { (0)qfalse + (1)qtrue } in
  if q1 then
    |q2> —> x,x' . if x = x' then 0 else 1
  else
    q2

def e2 =
  let q1 = { (0)qfalse + (1)qtrue } in
  let q2 = { (0)qfalse + (1)qtrue } in
  |q2> —> x,x' . if x = x' then 0 else 1
```

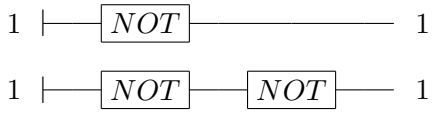
για τις οποίες αναμένουμε να δώσουν το ίδιο αποτέλεσμα όταν εκτελεστούν. Η σημασιολογία που ορίσαμε δεν είναι σε θέση να μας το αποδείξει άμεσα αυτό αφού δίνει δύο συντακτικά διαφορετικά κυκλώματα:

$$[\![\emptyset; 0 \vdash^{\circ} \texttt{e1} : \textbf{qbit}[1]; 2; 0; 0]\!] =$$



$$\not\equiv$$

$$[\![\emptyset; 0 \vdash^{\circ} \texttt{e1} : \textbf{qbit}[1]; 2; 0; 0]\!] =$$



4.6 Δηλωτική σημασιολογία υπό την μορφή διανυσμάτων κατάστασης

Σε αυτή την ενότητα θα δούμε μία άλλη μορφή σημασιολογίας για τα προγράμματα nQML. Η σημασιολογία αυτή απέχει κατά πολύ από μία φυσική υλοποίηση, όπως αυτή των κβαντικών κυκλωμάτων που είδαμε, αλλά βρίσκεται πολύ κοντά στο μαθηματικό μοντέλο των κβαντικών υπολογισμών. Τώρα δίνουμε σε κάθε πρόγραμμα nQML ως ερμηνεία μία συνάρτηση από διανύσματα κατάστασης σε σύνολα από ζεύγη πιθανοτήτων και διανυσμάτων κατάστασης. Έτσι μία κβαντική έκφραση e η οποία τυποποιείται με βάση την σχέση $\Gamma; n \vdash e : \tau; m$, δηλαδή πριν ξεκινήσει η αποτίμηση της e η κβαντική κατάσταση περιλαμβάνει n qubits ενώ αφού τελειώσει περιέχει $n+m$, θα έχει ως ερμηνεία μία συνάρτηση με τύπο $\mathbb{C}^{2^n} \to \text{Pow}\left(\mathbb{R} \times \mathbb{C}^{2^{n+m}}\right)$. Πρέπει να σημειώσουμε ότι η ερμηνεία αυτή αγνοεί τα qubit υπηρέτες καθώς λόγω της ιδιότητας τους να ξεκινάνε και να καταλήγουν στην κατάσταση $|0\rangle$ δεν προσφέρουν κάτι επιπλέον στο διάνυσμα κατάστασης παρά μόνο μερικά μηδενικά στο τέλος του. Επιπλέον ούτε τα qubits σκουπίδια εμπλέκονται σε αυτή την ερμηνεία. Για αυτό το λόγω επανερχόμαστε στην αρχική πενταμελή σχέση τυποποίησης. Σκοπός μας είναι σε κάθε κβαντική έκφραση της nQML να αντιστοιχίσουμε μία συνάρτηση που θα παίρνει ως όρισμα μία αρχική κβαντική κατάσταση και θα δίνει ως αποτέλεσμα όλες τις κβαντικές καταστάσεις που μπορούν να προκύψουν από την αρχική, αφού αποτιμήσουμε την κβαντική έκφραση, μαζί με την πιθανότητα που έχουν να προκύψουν. Προφανώς το άθροισμα των πιθανοτήτων θα ισούται με 1 και από τις εκφράσεις που δεν περιλαμβάνουν μέτρηση θα μπορεί να προκύψει μονάχα μία κατάσταση. Συνεπώς για τις αγνές εκφράσεις e, δηλαδή αυτές που τυποποιούνται σύμφωνα με την σχέση $\Gamma; n \vdash^\circ e : \tau; m$, μπορούμε να δώσουμε σαν ερμηνεία μία συνάρτηση με τύπο $\mathbb{C}^{2^n} \to \mathbb{C}^{2^{n+m}}$. Πρακτικά η σημασιολογία αυτή μας δείχνει με ποιόν τρόπο οι εκφράσεις της nQML μετασχηματίζουν μία αρχική κβαντική κατάσταση.

Αρχικά θα ερμηνεύσουμε τις αγνές εκφράσεις καθώς η ερμηνεία τους θα αποτελέσει συστατικό της γενικότερης ερμηνείας των εκφράσεων που επιδέχονται τύπο.

- Κανόνας VAR$^\circ$

$$\frac{(x : \tau) \in \Gamma}{[\![\Gamma; n \vdash^\circ x : \tau; 0]\!](s) = s} \ (\text{VAR}^\circ)$$

  Μία μεταβλητή δεν προκαλεί καμία μεταβολή στην κβαντική κατάσταση και συνεπώς η ερμηνεία της είναι η ταυτοτική συνάρτηση.

- Κανόνας SUP$^\circ$

$$\frac{|\lambda|^2 + |\lambda'|^2 = 1 \qquad \lambda \cdot \overline{\lambda'} = \overline{\lambda} \cdot \lambda'}{[\![\Gamma; n \vdash^\circ \{\ (\lambda)\mathbf{qfalse} + (\lambda')\mathbf{qtrue}\ \} : \mathbf{qbit}[n]; 1]\!](s) = s \otimes \left(\lambda\,|0\rangle + \lambda'\,|1\rangle\right)} \ (\text{SUP}^\circ)$$

  Ο κατασκευαστής κβαντικών δεδομένων απλά προσθέτει ένα καινούριο qubit στην αρχική κατάσταση.

- Κανόνας SPAWN$^\circ$

$$\frac{}{\begin{array}{c}[\![\Gamma; n \vdash^\circ \mathbf{spawn}\ \backslash\ (x_1,\ \ldots,\ x_k) ->\ (b_1,\ \ldots,\ b_l) : \\ (\mathbf{qbit}[n] \otimes (\cdots \otimes (\mathbf{qbit}[n+k-1]) \ldots)) \otimes (\mathbf{qbit}[n+k] \otimes (\cdots \otimes (\mathbf{qbit}[n+k+l-1]) \ldots))\,; \\ k+l]\!](s) = s \otimes \left(\displaystyle\sum_{i \in \{0,1\}^k} \frac{1}{2^{\frac{k}{2}}} \cdot |i\rangle \otimes |\{\backslash\ x_1\ \ldots\ x_k ->\ (b_1,\ \ldots,\ b_l)\}\,(i)\rangle\right)\end{array}} \ (\text{SPAWN}^\circ)$$

  Ο καινούριος τελεστής προσθέτει στην αρχική κατάσταση μία υπέρθεση όλων των δυνατών τιμών του πεδίου ορισμού της δοθείσας συνάρτησης συζευγμένων με την αντίστοιχη τιμή της συνάρτησης. Όλα τα πλάτη της υπέρθεσης είναι ίσα.

- Κανόνες LET°, PROD° και LETPROD°

$$\frac{[\![\Gamma; n \vdash^\circ e_1 : \tau_1; m_1]\!] = f_1 \qquad [\![\Gamma, x : \tau_1; n + m_1 \vdash^\circ e_2 : \tau; m_2]\!] = f_2}{[\![\Gamma; n \vdash^\circ \textbf{let } x = e_1 \textbf{ in } e_2 : \tau; m_1 + m_2]\!] = f_2 \circ f_1} \text{ (LET}^\circ\text{)}$$

$$\frac{[\![\Gamma; n \vdash^\circ e_1 : \tau_1; m_1]\!] = f_1 \qquad [\![\Gamma; n + m_1 \vdash^\circ e_2 : \tau_2; m_2]\!] = f_2}{[\![\Gamma; n \vdash^\circ (e_1, e_2) : \tau_1 \otimes \tau_2; m_1 + m_2]\!] = f_2 \circ f_1} \text{ (PROD}^\circ\text{)}$$

$$\frac{[\![\Gamma; n \vdash^\circ e_1 : \tau_1 \otimes \tau_2; m_1]\!] = f_1 \qquad [\![\Gamma, x_1 : \tau_1, x_2 : \tau_2; n + m_1 \vdash^\circ e_2 : \tau; m_2]\!] = f_2}{[\![\Gamma; n \vdash^\circ \textbf{let } (x_1, x_2) = e_1 \textbf{ in } e_2 : \tau; m_1 + m_2]\!] = f_2 \circ f_1} \text{ (LETPROD}^\circ\text{)}$$

Και οι τρεις αυτοί κανόνες ερμηνεύονται με τον ίδιο τρόπο, δηλαδή ως η σύνθεση των ερμηνειών των εκφράσεων e_1 και e_2. Και αυτή η ερμηνεία αντιστοιχεί σε call by value σημασιολογία και αποτίμηση των πλειάδων από τα αριστερά προς τα δεξιά.

- Κανόνας IF°

$$\frac{\begin{array}{c}[\![\Gamma; n \vdash^\circ e : \textbf{qbit}[k]; m]\!] = f \\ [\![\Gamma|_k; n + m \vdash^\circ e_1 : \tau; m_1]\!] = f_1 \quad [\![\Gamma|_k; n + m \vdash^\circ e_2 : \tau; m_2]\!] = f_2\end{array}}{\begin{array}{l}[\![\Gamma; n \vdash^\circ \textbf{if } e \textbf{ then } e_1 \textbf{ else } e_2 : \tau; m + max(m_1, m_2)]\!](s) = \\ \Big(f_1(s_1) \otimes |0\rangle^{\otimes(max(m_1,m_2)-m_1)}\Big) + \Big(f_2(s_2) \otimes |0\rangle^{\otimes(max(m_1,m_2)-m_2)}\Big)\end{array}} \text{ (IF}^\circ\text{)}$$

όπου: $s_1 + s_2 = f(s)$
με: $s_1 = \sum_{i \in \{0,1\}^k} \sum_{j \in \{0,1\}^{n+m-(k+1)}} b_{ij} \cdot |i\rangle \otimes |1\rangle \otimes |j\rangle$
και: $s_2 = \sum_{i \in \{0,1\}^k} \sum_{j \in \{0,1\}^{n+m-(k+1)}} a_{ij} \cdot |i\rangle \otimes |0\rangle \otimes |j\rangle.$

Στην περίπτωση αυτή πρώτα αποτιμάται η συνθήκη δίνοντας την κατάσταση $f(s)$ η οποία στην συνέχεια διασπάται με βάση το k-οστό qubit στις s_1 και s_2 για να τροφοδοτήσουν τις συναρτήσεις f_1 και f_2 αντίστοιχα. Στο τέλος προσθέτουμε μηδενικά στην μικρότερη από τις δύο καταστάσεις.

- Κανόνας TRANS°

$$\frac{[\![\Gamma; n \vdash^\circ e : \tau; m]\!] = f \qquad \textbf{pure}(\tau) \qquad \{x : C(\tau), x' : C(\tau) \vdash c : \textbf{complex}\} = C}{[\![\Gamma; n \vdash^\circ |e\rangle \to x, x'.c : \tau; m]\!](s) = C' \cdot f(s)} \text{ (TRANS}^\circ\text{)}$$

Αρχικά αποτιμάται η έκφραση e για να προκύψει η κατάσταση $f(s)$, ενώ μετά επιδρά ο ορθομοναδιαίος μετασχηματισμός C' πάνω στην κατάσταση $f(s)$. Ο C' είναι ουσιαστικά μία επέκταση του ορθομοναδιαίου μετασχηματισμού C ώστε να λαμβάνει υπόψιν όλα τα qubits της κβαντικής κατάστασης. Η τυπική του μορφή είναι αρκετά τεχνική για αυτό και δεν δίνεται εδώ.

Κατόπιν ερμηνεύουμε γενικά μία έκφραση της nQML ως μία συνάρτηση από διανύσματα κατάστασης σε σύνολα από ζεύγη πιθανοτήτων και διανυσμάτων κατάστασης.

- *Κανόνας EMB*

$$\frac{[\![\Gamma; n \vdash^\circ e : \tau; m]\!] = f}{[\![\Gamma; n \vdash e : \tau; m]\!](s) = \{(1, f(s))\}} \text{ (EMB)}$$

Πολύ απλά μετατρέπουμε την συνάρτηση που έχουμε από το επαγωγικό βήμα ώστε αντί να επιστρέφει ένα διάνυσμα κατάστασης, να επιστρέφει ένα μονοσύνολο με μοναδικό στοιχείο αυτό το διάνυσμα κατάστασης το οποίο θα είναι η κατάσταση του συστήματος με πιθανότητα 1.

- *Κανόνες LET, PROD και LETPROD*

$$\frac{[\![\Gamma; n \vdash e_1 : \tau_1; m_1]\!] = f_1 \qquad [\![\Gamma, x : \tau_1; n + m_1 \vdash e_2 : \tau; m_2]\!] = f_2}{[\![\Gamma; n \vdash \textbf{let } x = e_1 \textbf{ in } e_2 : \tau; m_1 + m_2]\!](s) = \bigcup_{(p_1,s_1)\in f_1(s)} \{(p_1 \cdot p_2, s_2) : (p_2, s_2) \in f_2(s_1)\}} \text{ (LET)}$$

$$\frac{[\![\Gamma; n \vdash e_1 : \tau_1; m_1]\!] = f_1 \qquad [\![\Gamma; n + m_1 \vdash e_2 : \tau_2; m_2]\!] = f_2}{[\![\Gamma; n \vdash (e_1, e_2) : \tau_1 \otimes \tau_2; m_1 + m_2]\!](s) = \bigcup_{(p_1,s_1)\in f_1(s)} \{(p_1 \cdot p_2, s_2) : (p_2, s_2) \in f_2(s_1)\}} \text{ (PROD)}$$

$$\frac{[\![\Gamma; n \vdash e_1 : \tau_1 \otimes \tau_2; m_1]\!] = f_1 \qquad [\![\Gamma, x_1 : \tau_1, x_2 : \tau_2; n + m_1 \vdash e_2 : \tau; m_2]\!] = f_2}{[\![\Gamma; n \vdash \textbf{let } (x_1, x_2) = e_1 \textbf{ in } e_2 : \tau; m_1 + m_2]\!](s) = \bigcup_{(p_1,s_1)\in f_1(s)} \{(p_1 \cdot p_2, s_2) : (p_2, s_2) \in f_2(s_1)\}} \text{ (LETPROD)}$$

Η ερμηνεία των κανόνων είναι ουσιαστικά μία γενικευμένη σύνθεση των f_1 και f_2 για να διαχειριστούμε το γεγονός ότι πλέον οι ερμηνείες επιστρέφουν σύνολα από ζεύγη πιθανοτήτων και διανυσμάτων κατάστασης.

- *Κανόνας IF*

$$\frac{\begin{array}{c}[\![\Gamma; n \vdash e : \textbf{qbit}[k]; m]\!] = f \\ [\![\Gamma|_k; n + m \vdash^\circ e_1 : \tau; m_1]\!] = f_1 \quad [\![\Gamma|_k; n + m \vdash^\circ e_2 : \tau; m_2]\!] = f_2\end{array}}{\begin{array}{c}[\![\Gamma; n \vdash \textbf{if } e \textbf{ then } e_1 \textbf{ else } e_2 : \tau; m + max(m_1, m_2)]\!](s) = \\ \left\{\left(p, f_1(s_1) \otimes |0\rangle^{\otimes(max(m_1,m_2)-m_1)} + f_2(s_2) \otimes |0\rangle^{\otimes(max(m_1,m_2)-m_2)}\right) : (p, s_1 + s_2) \in f(s)\right\}\end{array}} \text{ (IF)}$$

με s_1 της μορφής: $\sum_{i\in\{0,1\}^k} \sum_{j\in\{0,1\}^{n+m-(k+1)}} b_{ij} \cdot |i\rangle \otimes |1\rangle \otimes |j\rangle$

και s_2 της μορφής: $\sum_{i\in\{0,1\}^k} \sum_{j\in\{0,1\}^{n+m-(k+1)}} a_{ij} \cdot |i\rangle \otimes |0\rangle \otimes |j\rangle$.

Στην περίπτωση αυτή πρώτα ερμηνεύουμε την συνθήκη για να πάρουμε ένα σύνολο από διανύσματα κατάστασης, κατόπιν διαχωρίζουμε κάθε ένα διάνυσμα κατάστασης με βάση το k-οστό qubit για να εφαρμόσουμε τελικά στο ένα μέρος την συνάρτηση f_1, στο άλλο την f_2 και να πάρουμε το άθροισμα των δύο επιμέρους καταστάσεων. Στο σημείο αυτό πρέπει να πούμε ότι οι συναρτήσεις f_1 και f_2 επιστρέφουν διανύσματα κατάστασης καθώς αποτελούν ερμηνείες εκφράσεων που τυποποιούνται στο αγνό σύστημα τύπων.

- *Κανόνας IFM*

$$\frac{\begin{array}{c}[\![\Gamma; n \vdash e : \textbf{qbit}[k]; m]\!] = f \\ [\![\Gamma|_k; n + m \vdash e_1 : \tau; m_1]\!] = f_1 \quad [\![\Gamma|_k; n + m \vdash e_2 : \tau; m_2]\!] = f_2\end{array}}{\begin{array}{c}[\![\Gamma; n \vdash \textbf{ifm } e \textbf{ then } e_1 \textbf{ else } e_2 : \tau; m + max(m_1, m_2)]\!](s) = \\ \bigcup_{(p,s_1+s_2)\in f(s)} \left\{\left(p \cdot \|s_1\|^2 \cdot p_1, s_1' \otimes |0\rangle^{\otimes(max(m_1,m_2)-m_1)}\right) : (p_1, s_1') \in f_1\left(\frac{s_1}{\|s_1\|^2}\right)\right\} \bigcup \\ \left\{\left(p \cdot \|s_2\|^2 \cdot p_2, s_2' \otimes |0\rangle^{\otimes(max(m_1,m_2)-m_2)}\right) : (p_2, s_2') \in f_2\left(\frac{s_2}{\|s_2\|^2}\right)\right\}\end{array}} \text{ (IFM)}$$

με s_1 της μορφής: $\sum_{i\in\{0,1\}^k} \sum_{j\in\{0,1\}^{n+m-(k+1)}} b_{ij} \cdot |i\rangle \otimes |1\rangle \otimes |j\rangle$

και s_2 της μορφής: $\sum_{i\in\{0,1\}^k} \sum_{j\in\{0,1\}^{n+m-(k+1)}} a_{ij} \cdot |i\rangle \otimes |0\rangle \otimes |j\rangle$.

Για να ερμηνεύσουμε αυτή την έκφραση είναι που αναγκαστήκαμε να κάνουμε τις συναρτήσεις μας να επιστρέφουν σύνολα από ζεύγη πιθανοτήτων και διανυσμάτων κατάστασης. Και αυτό γιατί η συνάρτηση που ερμηνεύει αυτή την έκφραση επιστρέφει ένα σύνολο που λαμβάνει υπόψιν του και τα δύο πιθανά αποτελέσματα της μέτρησης. Να σημειώσουμε εδώ ότι οι διαιρέσεις με $\|s_1\|^2, \|s_2\|^2$ είναι κάπως καταχρηστικές καθώς μπορεί κάποιο από αυτά να ισούται με μηδέν. Για να μην φορτώσουμε τους ορισμούς με πολλές περιπτώσεις ας πούμε λοιπόν ότι στην περίπτωση που κάποιο από τα δύο είναι μηδέν η αντίστοιχη συνάρτηση επιστρέφει το κενό σύνολο.

- *Κανόνας TRANS*

$$\frac{[\![\Gamma; n \vdash e : \tau; m]\!] = f \qquad \mathbf{pure}(\tau) \qquad \{x : C(\tau), x' : C(\tau) \vdash c : \mathbf{complex}\} = C}{[\![\Gamma; n \vdash |e\rangle \to x, x'.c : \tau; m]\!](s) = \left\{ \left(p, C' \cdot s'\right) : (p, s') \in f(s) \right\}} \text{ (TRANS)}$$

Αφού πάρουμε την ερμηνεία της έκφρασης e και της εφαρμόσουμε το αρχικό διάνυσμα κατάστασης προκύπτει ένα σύνολο από ζεύγη πιθανοτήτων και διανυσμάτων κατάστασης, όπου πολλαπλασιάζουμε το κάθε διάνυσμα κατάστασης με τον ορθομοναδιαίο μετασχηματισμό C' ενώ η πιθανότητα μένει αναλλοίωτη. Ο C' είναι η επέκταση του C ώστε να λαμβάνει υπόψιν όλα τα qubits της κβαντικής κατάστασης.

Με βάση αυτή την σημασιολογία είμαστε σε θέση να πάρουμε πιο εκλεπτυσμένες σημασίες για τις εκφράσεις της nQML σε σχέση με την σημασιολογία υπό την μορφή κβαντικών κυκλωμάτων. Τουλάχιστον μπορούμε να πούμε άμεσα ότι δύο εκφράσεις που περιμένουμε να δώσουν το ίδιο αποτέλεσμα έχουν και την ίδια σημασία. Αυτή την φόρα οι σημασίες των εκφράσεων:

```
def e1 =
  let q1 = { (0)qfalse + (1)qtrue } in
  let q2 = { (0)qfalse + (1)qtrue } in
  if q1 then
    |q2> —> x,x' . if x = x' then 0 else 1
  else
    q2

def e2 =
  let q1 = { (0)qfalse + (1)qtrue } in
  let q2 = { (0)qfalse + (1)qtrue } in
  |q2> —> x,x' . if x = x' then 0 else 1
```

ταυτίζονται αφού:

$$[\![\emptyset; 0 \vdash^{\circ} \texttt{e1} : \mathbf{qbit}[1]; 2]\!](s) = [\![\emptyset; 0 \vdash^{\circ} \texttt{e2} : \mathbf{qbit}[1]; 2]\!](s) = s \otimes |10\rangle = s \cdot |10\rangle \text{ για } s \in \mathbb{C}$$

Η σημασιολογία αυτή φαίνεται να μας προσφέρει έναν τρόπο να διαπιστώνουμε πότε δύο εκφράσεις της nQML πρόκειται να οδηγήσουν στην ίδια τελική κβαντική κατάσταση όταν εκτελεστούν. Για την συγκεκριμένη γλώσσα, αν και κβαντική, από την στιγμή που δεν περιέχει αναδρομή ούτε αναδρομικούς τύπους δεδομένων θα περιμέναμε ο έλεγχος της ισοδυναμίας δύο προγραμμάτων να είναι αλγοριθμικός. Και πράγματι είναι αφού αρκεί να υπολογίσουμε τις σημασίες τους υπό την μορφή συναρτήσεων από διανύσματα κατάστασης σε σύνολα από διανύσματα κατάστασης και να δούμε αν ταυτίζονται όταν εφαρμοστούν στην κατάσταση $1 \in \mathbb{C}$. Αυτό συμβαίνει διότι κατά την εκκίνηση τους τα προγράμματα δεν έχουν δεσμεύσει κανένα qubit και συνεπώς η ερμηνεία τους θα είναι μία συνάρτηση με πεδίο ορισμού το $\mathbb{C}^{2^0} = \mathbb{C}$, άρα είναι εύλογο από όλους τους μιγαδικούς αριθμούς με μέτρο την μονάδα να επιλέξουμε τον μιγαδικό αριθμό 1 ως αρχική κατάσταση των προγραμμάτων.

4.7 Παραδείγματα

Έχοντας στην διάθεση μας την σημασιολογία των εκφράσεων της nQML υπό την μορφή διανυσμάτων κατάστασης θα περάσουμε στην διατύπωση μερικών εκφράσεων και στον υπολογισμό της σημασίας τους ώστε να καταλάβουμε καλύτερα την εκφραστική δύναμη και το νόημα του τελεστή **spawn** της nQML.

Ξεκινάμε παρουσιάζοντας μία έκφραση της nQML η οποία αποτιμά εξαντλητικά την κλασική συνάρτηση $\mathrm{or} : \mathrm{Bool}^2 \to \mathrm{Bool}$ και αυτό το πετυχαίνει με μόλις μία κλήση της συνάρτησης. Στην πράξη βέβαια δεν έχουμε άμεση πρόσβαση στο αποτέλεσμα της εξαντλητικής αποτίμησης καθώς αυτό βρίσκεται στον ιδιωτικό χώρο του συστήματος στον οποίο έχουμε μόνο μερική πρόσβαση μέσω της διαδικασίας της μέτρησης. Έχουμε λοιπόν:

```
def or =
  let (arg, res) = spawn \ (a, b) -> (a | b) in res
```

με σημασία:

$$[\![\emptyset; 0 \vdash^{\circ} \texttt{or} : \mathbf{qbit}[2]; 3]\!]\,(1) = \frac{1}{2}\,|0\rangle\otimes|0\rangle\otimes|0\rangle + \frac{1}{2}\,|0\rangle\otimes|1\rangle\otimes|1\rangle + \frac{1}{2}\,|1\rangle\otimes|0\rangle\otimes|1\rangle + \frac{1}{2}\,|1\rangle\otimes|1\rangle\otimes|1\rangle$$

Συνεχίζουμε ορίζοντας την έκφραση που αποτιμά εξαντλητικά την αριστερή ολίσθηση κατά ένα σε καταχωρητή των τριών qubits:

```
def shl =
  spawn \ (a2, a1, a0) -> (a1, a0, false)
```

με σημασία:

$$[\![\emptyset; 0 \vdash^{\circ} \texttt{shl} : \tau; 6]\!]\,(1) = \frac{1}{2\sqrt{2}}\,|000\rangle \otimes |000\rangle + \frac{1}{2\sqrt{2}}\,|001\rangle \otimes |010\rangle + \frac{1}{2\sqrt{2}}\,|010\rangle \otimes |100\rangle +$$

$$\frac{1}{2\sqrt{2}}\,|011\rangle\otimes|110\rangle + \frac{1}{2\sqrt{2}}\,|100\rangle\otimes|000\rangle + \frac{1}{2\sqrt{2}}\,|101\rangle\otimes|010\rangle + \frac{1}{2\sqrt{2}}\,|110\rangle\otimes|100\rangle + \frac{1}{2\sqrt{2}}\,|111\rangle\otimes|110\rangle$$

Τέλος θα διατυπώσουμε μία έκφραση που αντιστοιχεί στην πρόσθεση δύο καταχωρητών των δύο qubits:

```
def add =
  spawn \ (a1, a0, b1, b0) -> (a1 @ b1 @ (a0 & b0), a0 @ b0)
```

με σημασία:

$$[\![\emptyset; 0 \vdash^{\circ} \texttt{add} : \tau; 6]\!]\,(1) = \frac{1}{4}\,|00\rangle \otimes |00\rangle \otimes |00\rangle + \frac{1}{4}\,|00\rangle \otimes |01\rangle \otimes |01\rangle + \frac{1}{4}\,|00\rangle \otimes |10\rangle \otimes |10\rangle +$$

$$\frac{1}{4}\,|00\rangle\otimes|11\rangle\otimes|11\rangle + \frac{1}{4}\,|01\rangle\otimes|00\rangle\otimes|01\rangle + \frac{1}{4}\,|01\rangle\otimes|01\rangle\otimes|10\rangle + \frac{1}{4}\,|01\rangle\otimes|10\rangle\otimes|11\rangle + \frac{1}{4}\,|01\rangle\otimes|11\rangle\otimes|00\rangle +$$

$$\frac{1}{4}\,|10\rangle\otimes|00\rangle\otimes|10\rangle + \frac{1}{4}\,|10\rangle\otimes|01\rangle\otimes|11\rangle + \frac{1}{4}\,|10\rangle\otimes|10\rangle\otimes|00\rangle + \frac{1}{4}\,|10\rangle\otimes|11\rangle\otimes|01\rangle + \frac{1}{4}\,|11\rangle\otimes|00\rangle\otimes|11\rangle +$$

$$\frac{1}{4}\,|11\rangle \otimes |01\rangle \otimes |00\rangle + \frac{1}{4}\,|11\rangle \otimes |10\rangle \otimes |01\rangle + \frac{1}{4}\,|11\rangle \otimes |11\rangle \otimes |10\rangle$$

Κεφάλαιο 5

Κβαντικοί αλγόριθμοι και υλοποίηση αυτών στην nQML

5.1 Ο αλγόριθμος Deutsch-Jozsa

5.1.1 Περιγραφή

Το πρόβλημα που επιλύει ο αλγόριθμος Deutsch-Jozsa είναι το εξής: δοθείσας μίας συνάρτησης $f : \{0,1\}^n \to \{0,1\}$ η οποία έχει την ιδιότητα είτε να είναι σταθερή είτε να είναι ισοζυγισμένη, δηλαδή να επιστρέφει 0 για τις μισές τιμές του πεδίου ορισμού της και 1 για τις άλλες μισές, καλούμαστε να βρούμε αν η συνάρτηση είναι σταθερή ή ισοζυγισμένη.

Ένας κλασικός αλγόριθμος στην χειρότερη περίπτωση θα απαιτούσε την αποτίμηση της συνάρτησης f για $2^{n-1}+1$ σημεία του πεδίου ορισμού της. Η χειρότερη περίπτωση προκύπτει όταν η f είναι σταθερή, οπότε για να δούμε ότι όντως δεν είναι ισοζυγισμένη πρέπει να την αποτιμήσουμε $2^{n-1}+1$ φορές. Στην καλύτερη περίπτωση βέβαια μας αρκεί να αποτιμήσουμε την f μόνο δύο φορές. Αυτό συμβαίνει όταν είναι ισοζυγισμένη και σταθούμε τυχεροί να πάρουμε δύο διαφορετικά αποτελέσματα στις δύο πρώτες αποτιμήσεις της f.

Ο αλγόριθμος Deutsch-Jozsa όμως στηριζόμενος στην κβαντομηχανική καταφέρνει να απαντήσει στο ερώτημα αυτό με μόλις μία αποτίμηση της f σε όλες τις περιπτώσεις. Ας δούμε πώς τα καταφέρνει. Αρχικά θεωρούμε ότι έχουμε στην διάθεση μας την συνάρτηση f ως ένα κβαντικό κύκλωμα C_f το οποίο μετασχηματίζει την είσοδο $|x\rangle \otimes |b\rangle$ σε $|x\rangle \otimes |b \oplus f(x)\rangle$, όπου παραλείπουμε τυχόν qubits υπηρέτες καθώς δεν προσφέρουν τίποτα στο διάνυσμα κατάστασης παρά μόνο μερικά μηδενικά. Ο αλγόριθμος εκκινεί από την κβαντική κατάσταση $|0\rangle^{\otimes(n+1)}$ και το πρώτο του μέλημα είναι να δημιουργήσει μία υπέρθεση όλων των δυνατών εισόδων εφαρμόζοντας τον μετασχηματισμό $\left(H^{\otimes n} \cdot I_n\right) \otimes (H \cdot NOT)$. Κατόπιν εφαρμόζουμε τον μετασχηματισμό C_f και το σύστημα μεταβαίνει στην κατάσταση:

$$\sum_{x\in\{0,1\}^n} \frac{1}{2^{\frac{n+1}{2}}} \cdot |x\rangle \otimes (|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle) =$$

$$\sum_{\substack{x\in\{0,1\}^n \\ f(x)=0}} \frac{1}{2^{\frac{n+1}{2}}} \cdot |x\rangle \otimes (|0\rangle - |1\rangle) + \sum_{\substack{x\in\{0,1\}^n \\ f(x)=1}} \frac{1}{2^{\frac{n+1}{2}}} \cdot |x\rangle \otimes (|1\rangle - |0\rangle) =$$

$$\sum_{\substack{x\in\{0,1\}^n \\ f(x)=0}} \frac{1}{2^{\frac{n+1}{2}}} \cdot |x\rangle \otimes (|0\rangle - |1\rangle) + \sum_{\substack{x\in\{0,1\}^n \\ f(x)=1}} \frac{-1}{2^{\frac{n+1}{2}}} \cdot |x\rangle \otimes (|0\rangle - |1\rangle) =$$

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

$$\left(\sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}}{2^{\frac{n}{2}}} \cdot |x\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$$

Το τελευταίο βήμα του αλγορίθμου είναι να εφαρμόσουμε τον μετασχηματισμό $\left(I_n \cdot H^{\otimes n}\right) \otimes (NOT \cdot H)$ για να πάρουμε την κατάσταση:

$$\left(\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}}{2^{\frac{n}{2}}} \cdot H^{\otimes n} \cdot |x\rangle \right) \otimes |0\rangle$$

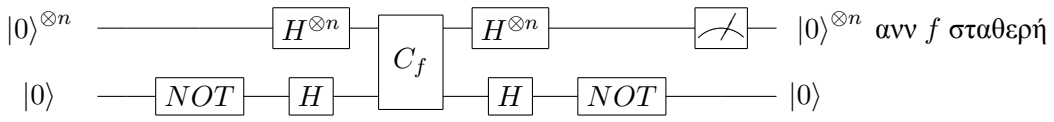
Χρησιμοποιώντας το γεγονός ότι: $H^{\otimes n} \cdot |x\rangle = \sum_{y \in \{0,1\}} \frac{(-1)^{x \cdot y}}{2^{\frac{n}{2}}} |y\rangle$, έχουμε ότι η κβαντική κατάσταση ισοδύναμα μπορεί να γραφεί ως:

$$\left(\sum_{x \in \{0,1\}^n} \frac{(-1)^{f(x)}}{2^{\frac{n}{2}}} \cdot \left[\sum_{y \in \{0,1\}} \frac{(-1)^{x \cdot y}}{2^{\frac{n}{2}}} |y\rangle \right] \right) \otimes |0\rangle =$$

$$\left(\sum_{y \in \{0,1\}^n} \left[\frac{1}{2^n} \cdot \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \cdot (-1)^{x \cdot y} \right] \cdot |y\rangle \right) \otimes |0\rangle$$

Παρατηρούμε ότι αν η συνάρτηση f είναι σταθερή τότε $\sum_{x \in \{0,1\}^n} (-1)^{f(x)} = \pm 2^n$, ενώ αν η f είναι ισοζυγισμένη τότε $\sum_{x \in \{0,1\}^n} (-1)^{f(x)} = 0$. Συνδυάζοντας αυτή την παρατήρηση με την τελική μορφή της κβαντικής κατάστασης βλέπουμε ότι αν η f είναι σταθερή και μετρήσουμε τα πρώτα n qubits τότε θα πάρουμε σαν αποτέλεσμα την κατάσταση $|0\rangle^{\otimes n}$ με πιθανότητα 1, ενώ αν η f είναι ισοζυγισμένη και μετρήσουμε τα πρώτα n qubits τότε θα πάρουμε σαν αποτέλεσμα την κατάσταση $|0\rangle^{\otimes n}$ με πιθανότητα 0. Έτσι από το αποτέλεσμα της μέτρησης μπορούμε να αποφανθούμε αν η f είναι σταθερή ή ισοζυγισμένη.

Το κβαντικό κύκλωμα που υλοποιεί τον αλγόριθμο Deutsch-Jozsa σύμφωνα με την παραπάνω περιγραφή είναι το ακόλουθο:



5.1.2 Υλοποίηση

Θα παρουσιάσουμε μία υλοποίηση του αλγορίθμου Deutsch-Jozsa σε nQML για την περίπτωση $n = 1$ όπου η συνάρτηση που μας δίνεται έχει τύπο $f : \{0,1\} \to \{0,1\}$ και είναι είτε σταθερή είτε ισοζυγισμένη. Υπάρχουν τέσσερις τέτοιες πιθανές συναρτήσεις και είναι οι $f(x) = 0, f(x) = 1$ οι οποίες είναι σταθερές και οι $f(x) = \neg x, f(x) = x$ οι οποίες είναι ισοζυγισμένες.

Για την απλούστευση της υλοποίησης θα χρησιμοποιήσουμε κάποιες παραμετρικές εκφράσεις οι οποίες δεν προβλέπονται από το συντακτικό της nQML. Για αυτό θα θεωρήσουμε ότι οι αυτές οι παραμετρικές εκφράσεις αντιστοιχούν σε μακροεντολές, δηλαδή ότι κάθε χρήση τους πρόκειται να αντικατασταθεί συντακτικά από το σώμα τους. Έτσι μπορούμε να ορίσουμε τις παραμετρικές εκφράσεις που αντιστοιχούν στις πύλες NOT και H και μετά να τις χρησιμοποιούμε κατά βούληση.

```
def not q = |q> –> x, x' .
  if x = x' then 0 else 1;

def had q = |q> –> x, x' .
  (if x then (if x' then –1 else 1) else 1) / sqrt(2);
```

Άλλη μία παρατυπία που θα κάνουμε είναι να γράφουμε **qfalse** εννοώντας { (1)**qfalse** + (0)**qtrue** } και **qtrue** εννοώντας { (1)**qfalse** + (0)**qtrue** }.

Με αυτές τις συμβάσεις, τις οποίες θα ακολουθήσουμε και στις επόμενες ενότητες, η υλοποίηση του αλγορίθμου Deutsch-Jozsa έχει ως εξής:

```
def Deutsch f =
  let (i, j) = (had qfalse, had qtrue) in
  let r = if f i then j else not j in
  ifm had i then qtrue else qfalse;
```

Έτσι μπορούμε για παράδειγμα να καλέσουμε `Deutsch` **not** και να πάρουμε:

$$[\![\emptyset; 0 \vdash^{\circ} \texttt{Deutsch}\ \textbf{not} : \textbf{qbit}[2]; 3]\!]\,(1) = \frac{-1}{\sqrt{2}}\,|101\rangle + \frac{1}{\sqrt{2}}\,|111\rangle$$

όπου το τρίτο qubit της κβαντικής κατάστασης βρίσκεται στην κατάσταση $|1\rangle$ δηλώνοντας ότι η $f(x) = \neg x$ είναι ισοζυγισμένη.

5.2 Αλγόριθμος Grover

5.2.1 Περιγραφή

Το πρόβλημα που επιλύει ο αλγόριθμος του Grover είναι το εξής: δοθείσας μίας συνάρτησης $f : \{0,1\}^n \to \{0,1\}$ με την ιδιότητα για ακριβώς ένα $a \in \{0,1\}^n$ να έχουμε $f(a) = 1$ καλούμαστε να βρούμε αυτό το μοναδικό a. Ένας κλασικός υπολογιστής στην χειρότερη περίπτωση θα απαιτούσε $\mathcal{O}(2^n)$ κλήσεις στην συνάρτηση f για να βρει αυτό το a, ενώ με τον αλγόριθμο του Grover σε έναν κβαντικό υπολογιστή είμαστε σε θέση να εντοπίσουμε το a με μεγάλη πιθανότητα μετά από $\mathcal{O}(\sqrt{2^n})$ κλήσεις της f.

Ο αλγόριθμος του Grover ενεργεί εκτελώντας κατ' επανάληψη δύο συγκεκριμένους ορθομοναδιαίους μετασχηματισμούς. Ο πρώτος από αυτούς είναι η εφαρμογή της συνάρτηση f. Υποθέτουμε ότι έχουμε την συνάρτηση f στην διάθεση μας ως έναν ορθομοναδιαίο πίνακα U_f ο οποίος μετασχηματίζει την είσοδο $|x\rangle \otimes |b\rangle$ σε $|x\rangle \otimes |b \oplus f(x)\rangle$. Οπότε μία κβαντική υπέρθεση μέσω του U_f μετασχηματίζεται ως εξής:

$$\sum_{x\in\{0,1\}^n} a_x \cdot |x\rangle \otimes \left(\frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\right) \xrightarrow{U_f} \sum_{x\in\{0,1\}^n} a_x \cdot |x\rangle \otimes \left(\frac{1}{\sqrt{2}}\,|0 \oplus f(0)\rangle - \frac{1}{\sqrt{2}}\,|1 \oplus f(1)\rangle\right) =$$

$$\sum_{\substack{x\in\{0,1\}^n \\ x\neq a}} a_x \cdot |x\rangle \otimes \left(\frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\right) + a_a \cdot |a\rangle \otimes \left(\frac{1}{\sqrt{2}}\,|1\rangle - \frac{1}{\sqrt{2}}\,|0\rangle\right) =$$

$$\sum_{\substack{x\in\{0,1\}^n \\ x\neq a}} a_x \cdot |x\rangle \otimes \left(\frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\right) - a_a \cdot |a\rangle \otimes \left(\frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\right) =$$

$$\sum_{x\in\{0,1\}^n} (-1)^{f(x)} \cdot a_x \cdot |x\rangle \otimes \left(\frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\right) =$$

$$\left(\sum_{x\in\{0,1\}^n} (-1)^{f(x)} \cdot a_x \cdot |x\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}\,|0\rangle - \frac{1}{\sqrt{2}}\,|1\rangle\right)$$

Το δεύτερο συστατικό στοιχείο του αλγόριθμου του Grover είναι ο ορθομοναδιαίος μετασχηματισμός, διάστασης $2^n \times 2^n$, ο οποίος ορίζεται ως:

$$D = \begin{pmatrix} \frac{2}{2^n} - 1 & \frac{2}{2^n} & \dots & \frac{2}{2^n} \\ \frac{2}{2^n} & \frac{2}{2^n} - 1 & \dots & \frac{2}{2^n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{2^n} & \frac{2}{2^n} & \dots & \frac{2}{2^n} - 1 \end{pmatrix}$$

Εύκολα μπορεί να διαπιστώσει κανείς ότι ο D είναι ορθομοναδιαίος. Ο μετασχηματισμός D έχει μία πολύ βασική ιδιότητα χάριν της οποίος αποκαλείται μετασχηματισμός της αντιστροφής ως προς το μέσο. Η ιδιότητα του αυτή είναι να μετασχηματίζει την κατάσταση $\sum_{x \in \{0,1\}^n} a_x \cdot |x\rangle$ σε $\sum_{x \in \{0,1\}^n} (2 \cdot \mu - a_x) \cdot |x\rangle$, όπου $\mu = \frac{1}{2^n} \cdot \sum_{x \in \{0,1\}^n} a_x$.

Έχοντας αυτά τα δύο εργαλεία στην διάθεση μας είμαστε έτοιμοι να διατυπώσουμε τα βήματα που ακολουθεί ο αλγόριθμος του Grover.

1. Ξεκινώντας από την κατάσταση $|0\rangle^{\otimes(n+1)}$ εφαρμόζουμε τον μετασχηματισμό $\left(H^{\otimes n} \cdot I_n\right) \otimes (H \cdot NOT)$ προκειμένου να μεταβούμε στην κατάσταση $\sum_{x \in \{0,1\}^n} \frac{1}{2^{\frac{n}{2}}} \cdot |x\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right)$.

   Αυτό είναι το βήμα κατά το οποίο τα πλάτη αρχικοποιούνται στις τιμές $d_x^{(1)} = d^{(1)} = \frac{1}{2^{\frac{n}{2}}}$ για $x \in \{0,1\}^n \setminus \{a\}$ και $d_a^{(1)} = \frac{1}{2^{\frac{n}{2}}}$.

2. Βρισκόμαστε στην i-οστή επανάληψη όπου τα πλάτη έχουν αρχικά τιμές $d_x^{(i)} = d^{(i)}$ για $x \in \{0,1\}^n \setminus \{a\}$ και $d_a^{(i)}$. Εφαρμόζουμε τον μετασχηματισμό U_f για να μεταβούμε από την κατάσταση $\sum_{\substack{x \in \{0,1\}^n \\ x \neq a}} d^{(i)} \cdot |x\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right) + d_a^{(i)} \cdot |a\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right)$ στην $\sum_{\substack{x \in \{0,1\}^n \\ x \neq a}} d^{(i)} \cdot |x\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right) - d_a^{(i)} \cdot |a\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right)$. Δηλαδή να αντιστρέψουμε το πλάτος της κατάστασης $|a\rangle$ αφήνοντας τα υπόλοιπα πλάτη αναλλοίωτα.

3. Εφαρμόζουμε το μετασχηματισμό $D \otimes I_1$ και έτσι η κατάσταση $\sum_{\substack{x \in \{0,1\}^n \\ x \neq a}} d^{(i)} \cdot |x\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right) - d_a^{(i)} \cdot |a\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right)$ γίνεται $\sum_{\substack{x \in \{0,1\}^n \\ x \neq a}} \left(2 \cdot \mu - d^{(i)}\right) \cdot |x\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right) + \left(2 \cdot \mu + d_a^{(i)}\right) \cdot |a\rangle \otimes \left(\frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle\right)$, όπου $\mu = \frac{1}{2^n} \cdot \left[\left(\sum_{\substack{x \in \{0,1\}^n \\ x \neq a}} d^{(i)}\right) - d_a^{(i)}\right] = d^{(i)} - \frac{d^{(i)} + d_a^{(i)}}{2^n}$. Έτσι τα πλάτη για την αρχή την $(i+1)$-οστής επανάληψης διαμορφώνονται σε $d^{(i+1)} = d^{(i)} - 2 \cdot \frac{d^{(i)} + d_a^{(i)}}{2^n}$ για $x \in \{0,1\}^n \setminus \{a\}$ και $d_a^{(i+1)} = 2 \cdot d^{(i)} + d_a^{(i)} - 2 \cdot \frac{d^{(i)} + d_a^{(i)}}{2^n}$.

4. Επαναλαμβάνουμε τα βήματα 2 και 3 $\mathcal{O}(\sqrt{2^n})$ φορές οπότε το πλάτος της κατάστασης $|a\rangle$ θα γίνει μεγαλύτερο από $\frac{1}{\sqrt{2}}$. Τέλος μπορούμε να μετρήσουμε τα πρώτα n qubits της κβαντικής κατάστασης και με πιθανότητα μεγαλύτερη από $\frac{1}{2}$ θα πάρουμε την κατάσταση $|a\rangle$ η οποία θα είναι και η λύση του προβλήματος μας.

Μένει να δείξουμε ότι όντως μετά από $\mathcal{O}(\sqrt{2^n})$ επαναλήψεις το πλάτος της κατάστασης $|a\rangle$ θα έχει γίνει μεγαλύτερο από $\frac{1}{\sqrt{2}}$. Ας θεωρήσουμε το ελάχιστο k τέτοιο ώστε $d_a^{(k)} > \frac{1}{\sqrt{2}}$ τότε επειδή $\sum_{\substack{x\in\{0,1\}^n \\ x\neq a}} \left(d^{(k)}\right)^2 = (2^n-1)\cdot\left(d^{(k)}\right)^2 = 1-\left(d_a^{(k)}\right)^2 < \frac{1}{2}$ έχουμε ότι $d^{(k)} < \sqrt{\frac{1}{2}\cdot\frac{1}{2^n-1}}$. Επειδή το k επιλέχθηκε ώστε να είναι ελάχιστο έχουμε ότι για $i=1,2,\ldots,k-1$ $d_a^{(i)} \leq \frac{1}{\sqrt{2}}$ και $d^{(i)} \geq \sqrt{\frac{1}{2}\cdot\frac{1}{2^n-1}} > \sqrt{\frac{1}{2}\cdot\frac{1}{2^n}}$. Συνεπώς $d_a^{(i+1)} - d_a^{(i)} = 2\cdot d^{(i)} - 2\cdot\frac{d^{(i)}+d_a^{(i)}}{2^n} = 2\cdot\frac{(2^n-1)\cdot d^{(i)} - d_a^{(i)}}{2^n} > 2\cdot\frac{\frac{2^n-1}{\sqrt{2\cdot 2^n}} - \frac{1}{\sqrt{2}}}{2^n} = \frac{1}{\sqrt{2\cdot 2^n}} + \frac{2^n - 2\cdot\sqrt{2^n}-2}{2^n\cdot\sqrt{2\cdot 2^n}}$. Όμως για $n\geq 3$, όπως θα είναι και οι περιπτώσεις για τις οποίες θέλουμε να χρησιμοποιήσουμε τον αλγόριθμο του Grover, έχουμε ότι $2^n - 2\cdot\sqrt{2^n} - 2 > 0$ και άρα τότε $d_a^{(i+1)} - d_a^{(i)} > \frac{1}{\sqrt{2\cdot 2^n}}$. Επιπλέον $d_a^{(k)} = d_a^{(1)} + \sum_{i=1}^{k-1}\left(d_a^{(i+1)} - d_a^{(i)}\right) > \frac{1}{2^n} + (k-1)\cdot\frac{1}{\sqrt{2\cdot 2^n}}$. Συνεπώς για το ελάχιστο αυτό k θα έχουμε ότι $k \leq \left\lceil\sqrt{2^n}\right\rceil + 1$, αφού $\frac{1}{2^n} + \left\lceil\sqrt{2^n}\right\rceil\cdot\frac{1}{\sqrt{2\cdot 2^n}} \geq \frac{1}{2^n} + \sqrt{2^n}\cdot\frac{1}{\sqrt{2\cdot 2^n}} = \frac{1}{2^n} + \frac{1}{\sqrt{2}} > \frac{1}{\sqrt{2}}$. Έτσι δείξαμε ότι αρκούν $\mathcal{O}(\sqrt{2^n})$ επαναλήψεις των βημάτων 2 και 3 ώστε να πάρουμε με πιθανότητα μεγαλύτερη από $\frac{1}{2}$ το ζητούμενο αποτέλεσμα.

5.2.2 Υλοποίηση

Θα περάσουμε τώρα σε μία υλοποίηση του αλγόριθμου του Grover στην περίπτωση που $n=2$. Σε αυτή την περίπτωση αρκεί μόλις μία επανάληψη για να πάρουμε το ζητούμενο αποτέλεσμα με πιθανότητα 1. Αυτό φαίνεται αποτιμώντας τις εξισώσεις $d_a^{(i+1)} = \frac{2\cdot(2^n-1)\cdot d^{(i)} + (2^n-2)\cdot d_a^{(i)}}{2^n}$ και $d^{(i)} = \sqrt{\frac{1-\left(d_a^{(i)}\right)^2}{2^n-1}}$ για $n=2$ και $i=1,2$. Από τις εξισώσεις αυτές προκύπτει ότι: $d_a^{(1)} = \frac{1}{2}$ και $d_a^{(2)} = 1$.

Για να υλοποιήσουμε τον αλγόριθμο θα ορίσουμε πρώτα τον μετασχηματισμό ο οποίος προκαλεί την αντιστροφή του προσήμου του πλάτους $d_a^{(i)}$. Για απλότητα αποφεύγουμε να χρησιμοποιήσουμε τον μετασχηματισμό κάποιας συνάρτησης f η οποία μετατρέπει την κατάσταση $|x\rangle\otimes|b\rangle$ στην κατάσταση $|x\rangle\otimes|b\oplus f(x)\rangle$, αλλά ορίζουμε το a του οποίου το πλάτος θέλουμε να αντιστρέψουμε, αυτό το οποίο θέλουμε να μας υπολογίσει ο αλγόριθμος, μέσα στον ίδιο τον μετασχηματισμό. Δηλαδή:

```
def query q = |q> -> x, x' .
  if x = x' then
    if int x = a then -1 else 1
  else
    0;
```

όπου το a είναι ένας φυσικός από το $\{(00)_2, (01)_2, (10)_2, (11)_2\}$.

Το επόμενο βήμα είναι να ορίσουμε τον μετασχηματισμό αντιστροφής ως προς το μέσο.

```
def diffusion q = |q> —> x, x' .
  if x = x' then 2 / 2^n − 1 else 2 / 2^n;
```

Και τέλος, έχοντας τους δύο αυτούς μετασχηματισμούς ως εργαλεία, να υλοποιήσουμε τα βήματα του αλγορίθμου.

```
def Grover =
  let qs = (had qfalse, had qfalse) in
  diffusion (query qs);
```

Τώρα αν θέσουμε $n = 2$, $a = (10)_2$ και καλέσουμε `Grover` θα πάρουμε:

$$[\![\emptyset; 0 \vdash^{\circ} \texttt{Grover} : \mathbf{qbit}[0] \otimes \mathbf{qbit}[1]; 2]\!]\,(1) = |10\rangle$$

το οποίο υποδηλώνει ότι με βάση αυτή την ερμηνεία των προγραμμάτων nQML η υλοποίηση υπολόγισε σωστά ότι $a = (10)_2$.

5.3 Αλγόριθμος Shor

5.3.1 Ο διακριτός μετασχηματισμός Fourier

Ο διακριτός μετασχηματισμός Fourier έχει ορισμένες ιδιότητες οι οποίες θα μας φανούν ιδιαίτερα χρήσιμες κατά την διατύπωση του αλγορίθμου εύρεσης περιόδου. Ο διακριτός μετασχηματισμός Fourier πάνω σε ένα N-διάστατο διάνυσμα ορίζεται ως:

$$QFT_N = \frac{1}{\sqrt{N}} \cdot \begin{pmatrix} \omega^{0\cdot 0} & \omega^{0\cdot 1} & \omega^{0\cdot 2} & \omega^{0\cdot 3} & \dots & \omega^{0\cdot (N-1)} \\ \omega^{1\cdot 0} & \omega^{1\cdot 1} & \omega^{1\cdot 2} & \omega^{1\cdot 3} & \dots & \omega^{1\cdot (N-1)} \\ \omega^{2\cdot 0} & \omega^{2\cdot 2} & \omega^{2\cdot 2} & \omega^{2\cdot 3} & \dots & \omega^{2\cdot (N-1)} \\ \omega^{3\cdot 0} & \omega^{3\cdot 1} & \omega^{3\cdot 2} & \omega^{3\cdot 3} & \dots & \omega^{3\cdot (N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \omega^{(N-1)\cdot 0} & \omega^{(N-1)\cdot 1} & \omega^{(N-1)\cdot 2} & \omega^{(N-1)\cdot 3} & \dots & \omega^{(N-1)\cdot (N-1)} \end{pmatrix}$$

όπου $\omega = e^{\frac{2\cdot\pi}{N}}$ είναι μία N-οστή ρίζα της μονάδας, δηλαδή μία λύση της εξίσωσης $z^N = 1$ στους μιγαδικούς αριθμούς. Ένας ισοδύναμος τρόπος να ορίσουμε τον QFT_N είναι να πούμε ότι είναι ένας $N \times N$ πίνακας όπου το στοιχείο που βρίσκεται στην i-οστή γραμμή και j-οστή στήλη του είναι το $\omega^{i\cdot j}$.

Ας δούμε τώρα ορισμένες χρήσιμες ιδιότητες του διακριτού μετασχηματισμού Fourier.

1. *Ο QFT_N είναι ορθομοναδιαίος*
   Πρώτα από όλα ο διακριτός μετασχηματισμός Fourier είναι ορθομοναδιαίος. Αυτό μας δίνει την δυνατότητα να τον χρησιμοποιούμε για να μετασχηματίζουμε και κβαντικές καταστάσεις. Αν συμβολίσουμε με F_j την j-οστή στήλη του QFT_N, δηλαδή:

   $$F_j = \frac{1}{\sqrt{N}} \cdot \begin{pmatrix} \omega^{0\cdot j} \\ \omega^{1\cdot j} \\ \vdots \\ \omega^{(N-1)\cdot j} \end{pmatrix}$$

   τότε αρκεί να δείξουμε ότι:

   $$F_i \cdot F_j^{\dagger} = \begin{cases} 1 & \text{αν } i = j \\ 0 & \text{αν } i \neq j \end{cases}$$

   Πράγματι:

   $$F_i \cdot F_j^{\dagger} = \frac{1}{N} \cdot \sum_{k=0}^{N-1} \omega^{i\cdot k} \cdot \left(\omega^{j\cdot k}\right)^* = \frac{1}{N} \cdot \sum_{k=0}^{N-1} \omega^{(i-j)\cdot k} =$$

$$\begin{cases} 1 & \text{αν } i = j \\ \dfrac{1}{N} \cdot \displaystyle\sum_{k=0}^{N-1} \left(\omega^{i-j}\right)^k = \dfrac{1}{N} \cdot \dfrac{\omega^{(i-j)\cdot N} - 1}{\omega^{i-j} - 1} = 0 & \text{αν } i \neq j \end{cases}$$

2. *Γραμμική ολίσθηση*
   Αν το διάνυσμα $a = \begin{pmatrix} a_0 & a_1 & \dots & a_{N-1} \end{pmatrix}^T$ έχει ως διακριτό μετασχηματισμό Fourier το $b = \begin{pmatrix} b_0 & b_1 & \dots & b_{N-1} \end{pmatrix}^T$ τότε το διάνυσμα $a' = \begin{pmatrix} a_{(0-j) \bmod N} & a_{(1-j) \bmod N} & \cdots & a_{((N-1)-j) \bmod N} \end{pmatrix}^T$ που αποτελεί μία γραμμική ολίσθηση των συντελεστών του αρχικού διανύσματος κατά j θα έχει ως διακριτό μετασχηματισμό Fourier το $b' = \begin{pmatrix} \omega^{0\cdot j} \cdot b_0 & \omega^{1\cdot j} \cdot b_1 & \dots & \omega^{(N-1)\cdot j} \cdot b_{N-1} \end{pmatrix}^T$, δηλαδή η i-οστή γραμμή του αρχικού μετασχηματισμού υφίσταται μία ολίσθηση φάσης κατά $\phi_i = \omega^{i\cdot j}$. Αυτό συμβαίνει διότι:

$$b'_i = \frac{1}{\sqrt{N}} \cdot \sum_{k=0}^{N-1} \omega^{i\cdot k} a'_k =$$

$$\frac{1}{\sqrt{N}} \cdot \sum_{k=0}^{N-1} \omega^{i\cdot k} a_{(k-j) \bmod N} =$$

$$\omega^{i\cdot j} \cdot \frac{1}{\sqrt{N}} \cdot \sum_{k=0}^{N-1} \omega^{i\cdot (k-j)} a_{(k-j) \bmod N} =$$

$$\phi_i \cdot \frac{1}{\sqrt{N}} \cdot \sum_{k=0}^{N-1} \omega^{i\cdot ((k-j) \bmod N)} a_{(k-j) \bmod N} =$$

$$\phi_i \cdot \frac{1}{\sqrt{N}} \cdot \sum_{l=0}^{N-1} \omega^{i\cdot l} a_l =$$

$$\phi_i \cdot b_i$$

.

3. *Σχέση περιόδου - μήκους κύματος*
   Αν διαθέτουμε ένα περιοδικό N-διάστατο διάνυσμα a με περίοδο r, όπου $r \mid N$, της μορφής:

$$a_i = \begin{cases} \sqrt{\dfrac{r}{N}} & \text{αν } i \equiv 0 \pmod{r} \\ 0 & \text{αν } i \not\equiv 0 \pmod{r} \end{cases}$$

   τότε αυτό έχει ως διακριτό μετασχηματισμό Fourier το περιοδικό διάνυσμα b με περίοδο $\dfrac{N}{r}$, ίση δηλαδή με το μήκος κύματος του a, που δίνεται από την σχέση:

$$b_i = \begin{cases} \sqrt{\dfrac{1}{r}} & \text{αν } i \equiv 0 \pmod{\frac{N}{r}} \\ 0 & \text{αν } i \not\equiv 0 \pmod{\frac{N}{r}} \end{cases}$$

   Πράγματι έχουμε ότι:

$$b_i = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \omega^{i\cdot k} \cdot a_k =$$

$$\frac{1}{\sqrt{N}} \cdot \sum_{l=0}^{\frac{N}{r}-1} \omega^{i\cdot (l\cdot r)} \cdot a_{l\cdot r} =$$

$$\frac{\sqrt{r}}{N} \cdot \sum_{l=0}^{\frac{N}{r}-1} \left(\omega^{i \cdot r}\right)^l =$$

$$\begin{cases} \frac{1}{\sqrt{r}} & \text{αν } i \equiv 0 \pmod{\frac{N}{r}} \\ \frac{\sqrt{r}}{N} \cdot \frac{\omega^{i \cdot N} - 1}{\omega^{i \cdot r} - 1} = 0 & \text{αν } i \not\equiv 0 \pmod{\frac{N}{r}} \end{cases}$$

5.3.2 Αλγόριθμος εύρεσης περιόδου

Την καρδιά του αλγόριθμου παραγοντοποίησης του Shor αποτελεί ο αλγόριθμος της εύρεσης της περιόδου μίας συνάρτησης $f : \{0,1\}^n \to \{0,1\}^m$ τέτοιας ώστε $f(x) = f(y)$ αν και μόνο αν $x \equiv y \pmod{r}$. Ο στόχος είναι δοθείσας της f να καταφέρουμε να βρούμε την περίοδο r. Κλασικά για να λύσουμε το πρόβλημα θα μας χρειαστούν $\mathcal{O}(r) = \mathcal{O}(2^n)$ κλήσεις της συνάρτησης f. Με έναν κβαντικό υπολογιστή όμως είμαστε σε θέση να καλέσουμε την f δίνοντας της ως όρισμα μία υπέρθεση όλων των δυνατών τιμών του $\{0,1\}^n$ και έτσι να πάρουμε μία υπέρθεση τιμών αποτελεσμάτων, η οποία θα είναι περιοδική ως προς τα αποτελέσματα και όλα αυτά με μόλις μία κλήση της f.

Προς διευκόλυνση της παρουσίασης και της κατανόησης του αλγορίθμου, θα εξετάσουμε την περίπτωση όπου $r \mid N = 2^n$, δηλαδή $r = 2^k$ για κάποιο k. Εκ πρώτης όψεως, κάποιος θα χαρακτήριζε αδιάφορη αυτή την περίπτωση καθώς τότε μπορούμε να υπολογίσουμε αποδοτικά την περίοδο και με κλασικούς τρόπους. Όμως τα αποτελέσματα που ισχύουν σε αυτή την περίπτωση, εξακολουθούν να ισχύουν με πολύ μικρή απόκλιση και στην περίπτωση όπου $N = 2^n \gg r^2$ και τότε δεν μπορούμε να καταφύγουμε σε κάποια κλασική αποδοτική λύση. Ας δούμε λοιπόν τα βήματα του αλγορίθμου όταν $r = 2^k$:

1. Αρχικά διαθέτουμε την κατάσταση $|0\rangle^{\otimes(n+m)}$ στην οποία εφαρμόζουμε τον μετασχηματισμό $H^{\otimes n} \otimes I_m$ για να μεταβούμε στην κατάσταση $\sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{N}} \cdot |x\rangle \otimes |0\rangle^{\otimes m}$. Δηλαδή τώρα έχουμε σχηματίσει μία υπέρθεση όλων των δυνατών τιμών του πεδίου ορισμού της f.

2. Σε αυτό το βήμα εφαρμόζουμε την συνάρτηση f η οποία θεωρούμε ότι μας έχει δοθεί ως ένας ορθομοναδιαίος μετασχηματισμός U_f ο οποίος μετασχηματίζει την κατάσταση $|x\rangle \otimes |0\rangle^{\otimes m}$ σε $|x\rangle \otimes |f(x)\rangle$. Έτσι η νέα κβαντική κατάσταση του συστήματος θα είναι $\sum_{x \in \{0,1\}^n} \frac{1}{\sqrt{N}} \cdot |x\rangle \otimes |f(x)\rangle$. Ας μην ξεχνάμε όμως ότι η f είναι περιοδική με περίοδο r και ότι μέσα στο διάστημα μίας περιόδου είναι $1-1$. Άρα η κβαντική κατάσταση μπορεί να γραφεί και ως:

$$\sum_{x_0=0}^{r-1} \frac{1}{\sqrt{r}} \cdot \left[\sum_{i=0}^{\frac{N}{r}-1} \sqrt{\frac{r}{N}} \cdot |x_0 + i \cdot r\rangle \otimes |f(x_0)\rangle \right]$$

3. Αν τώρα πραγματοποιήσουμε μία μέτρηση στα τελευταία m qubits της κβαντικής κατάστασης, σε αυτά δηλαδή που βρίσκεται η τιμή της f, και πάρουμε ως αποτέλεσμα $|f(x_0)\rangle$ για κάποιο $x_0 \in \{0, 1, \ldots, r-1\}$ θα καταλήξουμε με μία υπέρθεση όλων των δυνατών τιμών της προεικόνας του $f(x_0)$ η οποία είναι το σύνολο $\{x_0,\ x_0 + 1 \cdot r,\ x_0 + 2 \cdot r,\ \ldots,\ x_0 + \left(\frac{N}{r} - 1\right) \cdot r\}$. Θα προκύψει δηλαδή η κατάσταση $\sum_{i=0}^{\frac{N}{r}-1} \sqrt{\frac{r}{N}} \cdot |x_0 + i \cdot r\rangle \otimes |f(x_0)\rangle$.

4. Σε αυτό το σημείο ναι μεν διαθέτουμε μία υπέρθεση των τιμών του συνόλου $\{x_0,\ x_0 + 1 \cdot r,\ x_0 + 2 \cdot r,\ \ldots,\ x_0 + \left(\frac{N}{r} - 1\right) \cdot r\}$, το οποίο είναι πολύ θετικό καθώς ανά δύο οι τιμές

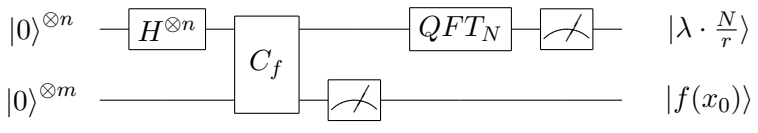
αυτές διαφέρουν κατά ένα πολλαπλάσιο της περιόδου, όμως πρέπει να αντιμετωπίσουμε την εμφάνιση του x_0 το οποίο είναι τυχαίο και έτσι καταστρέφει την επαναληψιμότητα της διαδικασίας καθώς σε κάθε επανάληψη είναι πολύ πιθανό να παίρνουμε και διαφορετικό x_0. Για να απαλλαγούμε λοιπόν από το x_0 θα καταφύγουμε στις ιδιότητες του διακριτού μετασχηματισμού Fourier. Από την σχέση περιόδου - μήκους κύματος του διακριτού μετασχηματισμού Fourier έχουμε ότι: $\sum_{i=0}^{\frac{N}{r}-1} \sqrt{\frac{r}{N}} \cdot |i \cdot r\rangle \xrightarrow{QFT_N} \sum_{i=0}^{r-1} \frac{1}{\sqrt{r}} \cdot |i \cdot \frac{N}{r}\rangle$. Τώρα αν συνδυάσουμε το προηγούμενο αποτέλεσμα με την ιδιότητα της γραμμικής ολίσθησης έχουμε: $\sum_{i=0}^{\frac{N}{r}-1} \sqrt{\frac{r}{N}} \cdot |x_0 + i \cdot r\rangle \xrightarrow{QFT_N} \sum_{i=0}^{r-1} \omega^{i \cdot \frac{N}{r} \cdot x_0} \cdot \frac{1}{\sqrt{r}} \cdot |i \cdot \frac{N}{r}\rangle$. Με αυτό τον τρόπο καταφέρνουμε να δημιουργήσουμε καταστάσεις που είναι πολλαπλάσια του $\frac{N}{r}$ και μεταφέρουμε την επίδραση του τυχαίου x_0 σε έναν ασήμαντο συντελεστή φάσης. Ο συντελεστής αυτός είναι ασήμαντος καθώς το μέτρο του είναι 1 και έτσι δεν επηρεάζει την πιθανότητα να μετρήσουμε την αντίστοιχη κατάσταση. Συνοψίζοντας ο μετασχηματισμός που εφαρμόζουμε σε αυτό το βήμα είναι ο $QFT_N \otimes I_m$.

5. Έχοντας στη διάθεση μας την κατάσταση $\sum_{i=0}^{r-1} \omega^{i \cdot \frac{N}{r} \cdot x_0} \cdot \frac{1}{\sqrt{r}} \cdot |i \cdot \frac{N}{r}\rangle \otimes f(x_0)$, απλά μετράμε τα πρώτα n qubits για να πάρουμε ένα πολλαπλάσιο του $\frac{N}{r}$.

6. Ο αλγόριθμος επαναλαμβάνεται εξ αρχής έως ότου συγκεντρώσουμε αρκετά πολλαπλάσια του $\frac{N}{r}$ ώστε παίρνοντας τον μέγιστο κοινό διαιρέτη τους να καταλήξουμε στο $\frac{N}{r}$ αυτό καθ' αυτό. Τώρα αφού γνωρίζουμε το N και το $\frac{N}{r}$ μπορούμε να υπολογίσουμε και το r.

Μένει να δούμε πόσες περίπου φορές θα χρειαστεί να επαναλάβουμε τον αλγόριθμο έως ότου συγκεντρώσουμε αρκετά πολλαπλάσια του $\frac{N}{r}$, ώστε να αρκούν για να δώσουν μέσω του μέγιστου κοινού διαιρέτη το $\frac{N}{r}$. Ας υποθέσουμε ότι μετά από t επαναλήψεις του αλγορίθμου μέσω του μέγιστου κοινού διαιρέτη βρίσκουμε $\lambda \cdot \frac{N}{r}$ για κάποιο $\lambda \geq 2$. Αυτό σημαίνει ότι σε κάθε μία από τις t επαναλήψεις βρήκαμε ένα πολλαπλάσιο του $\lambda \cdot \frac{N}{r}$. Όμως στο σύνολο $\{0, 1, \ldots, N-1\}$ υπάρχουν το πολύ $\frac{r}{\lambda}$ πολλαπλάσια του $\lambda \cdot \frac{N}{r}$. Ενώ συνολικά τα πολλαπλάσια του $\frac{N}{r}$ στο $\{0, 1, \ldots, N-1\}$ είναι r. Συνεπώς: $Pr\left[\text{ο μ.κ.δ. μετά από τα t επαναλήψεις να είναι } \lambda \cdot \frac{N}{r}\right] \leq \left(\frac{\frac{r}{\lambda}}{r}\right)^t = \left(\frac{1}{\lambda}\right)^t \leq \left(\frac{1}{2}\right)^t$. Άρα μετά από $\mathcal{O}(logN)$ επαναλήψεις του αλγορίθμου με πολύ μεγάλη πιθανότητα μέσω του μέγιστου κοινού διαιρέτη θα έχουμε βρει το $\frac{N}{r}$.

Το κβαντικό κύκλωμα που υλοποιεί μία επανάληψη του αλγορίθμου εύρεσης περιόδου σύμφωνα με την παραπάνω περιγραφή είναι το ακόλουθο:



5.3.3 Αλγόριθμος παραγοντοποίησης

Θα εξετάσουμε τώρα ίσως τον πιο σημαντικό αλγόριθμο που έχει παρουσιαστεί ως τώρα, τον αλγόριθμο του Shor. Ο αλγόριθμος του Shor δοθέντος ενός σύνθετου αριθμού N υπολογίζει αποδοτικά έναν μη τετριμμένο διαιρέτη του, δηλαδή έναν διαιρέτη διαφορετικό από το 1 και το N. Έχουν προταθεί διάφοροι κλασικοί αλγόριθμοι που λύνουν το ίδιο πρόβλημα, όμως όλοι έχουν εκθετική πολυπλοκότητα. Αντιθέτως, ο αλγόριθμος του Shor επωφελούμενος των κβαντομηχανικών φαινομένων είναι ο μόνος γνωστός ως τώρα πιθανοτικός αλγόριθμος με πολυωνυμική πολυπλοκότητα.

Το πρόβλημα της παραγοντοποίησης του N είναι ισοδύναμο με την εύρεση μίας μη τετριμμένης ρίζας της μονάδας modulo N, δηλαδή ενός αριθμού x τέτοιου ώστε $x^2 \equiv 1 \pmod N$ και $x \not\equiv \pm 1 \pmod N$. Έχοντας στην διάθεση μας ένα τέτοιο x μπορούμε να αποδείξουμε ότι οι $gcd(N, x+1)$ και $gcd(N, x-1)$ θα είναι παράγοντες του N. Αυτό συμβαίνει διότι $N \mid (x-1)\cdot(x+1)$, ενώ $N \nmid (x \pm 1)$. Σε αυτό το γεγονός στηρίζεται και ο αλγόριθμος του Shor ο οποίος υπολογίζει μία μη τετριμμένη ρίζα της μονάδας modulo N.

Τα βήματα του αλγορίθμου είναι τα εξής:

1. Αν ο N είναι άρτιος τότε ο 2 είναι ένας παράγοντας του N.

2. Ελέγχουμε, κλασικά, αν ο N είναι της μορφής $N = b^c$, όπου $b, c \geq 2$. Αν όντως είναι αυτής της μορφής το πρόβλημα λύθηκε καθώς ο b είναι παράγοντας του N. Ο έλεγχος αυτός μπορεί να γίνει εξετάζοντας για όλα τα $d \in \{2, 3, \ldots, \lfloor log_2\, N \rfloor\}$ αν κάποιος από τους δύο φυσικούς αριθμούς που βρίσκονται αριστερά και δεξιά του $N^{\frac{1}{d}}$, υψωμένος στην d μας δίνει το N. Οπότε η πολυπλοκότητα αυτού του βήματος είναι $\mathcal{O}\left((log\, N)^3\right)$.

3. Επιλέγουμε ένα τυχαίο a τέτοιο ώστε $0 < a < N$. Αν $gcd(N, a) > 1$ τότε ο $gcd(N, a)$ είναι ένας μη τετριμμένος διαιρέτης του N και το πρόβλημα λύθηκε.

4. Χρησιμοποιώντας τον κβαντικό αλγόριθμο εύρεσης περιόδου της προηγούμενης ενότητας υπολογίζουμε την περίοδο της συνάρτησης $f(x) = a^x \ mod\ N$ για $x \in \{0, 1, \ldots, 2^m - 1\}$, όπου $2^m \gg N^2$. Αυτή η επιλογή του πεδίου ορισμού της συνάρτησης οφείλεται στο γεγονός ότι ο αλγόριθμος εύρεσης περιόδου προκειμένου να δώσει το επιθυμητό αποτέλεσμα πρέπει να έχει ως είσοδο ένα σύνολο $\{0, 1, \ldots, 2^m - 1\}$, όπου r η περίοδος και $2^m \gg r^2$. Εν προκειμένω η περίοδος είναι της τάξης του N.

5. Έχοντας στην διάθεση μας την περίοδο r της συνάρτησης $f(x) = a^x \ mod\ N$ κατ ουσίαν έχουμε την τάξη του στοιχείου a, δηλαδή τον μικρότερο θετικό φυσικό αριθμό τέτοιον ώστε $a^r \equiv 1 \pmod N$. Αν η τάξη r είναι περιττή τότε επιστρέφουμε στο βήμα 3 και επιλέγουμε νέο a. Παρομοίως πράττουμε αν η τάξη είναι άρτια αλλά $a^{\frac{r}{2}} \equiv -1 \pmod N$. Διαφορετικά, αποκλείεται $a^{\frac{r}{2}} \equiv 1 \pmod N$ αφού r είναι η τάξη του a και συνεπώς $a^{\frac{r}{2}}$ είναι μία μη τετριμμένη ρίζα της μονάδας modulo N.

Τώρα μένει να δούμε πόσο εύκολο είναι να βρούμε ένα a που θα οδηγήσει στην επιτυχή ολοκλήρωση του βήματος 5. Αποδεικνύεται ότι αν ο N είναι περιττός και δεν είναι της μορφής $N = p^c$, όπου p πρώτος, και το a επιλεγεί τυχαία ώστε $gcd(N, a) = 1$ και r είναι η τάξη του a τότε $Pr\left[\text{r άρτιος και } a^{\frac{r}{2}} \not\equiv -1 \pmod N\right] \geq \frac{1}{2}$. Συνεπώς μετά από μερικές επαναλήψεις των βημάτων 3-5 θα βρούμε με πολύ μεγάλη πιθανότητα μία μη τετριμμένη ρίζα της μονάδας. Συνολικά λοιπόν, η πολυπλοκότητα του αλγορίθμου του Shor απαρτίζεται από $\mathcal{O}\left((log\, N)^3\right)$ κλασικά βήματα για τον υπολογισμό του μέγιστου κοινού διαιρέτη, την ύψωση σε δύναμη με υπόλοιπο και τον έλεγχο του αν $N = b^c$ και από την πολυπλοκότητα του κβαντικού υπολογισμού για την εύρεση της περιόδου της συνάρτησης $f(x) = a^x \ mod\ N$. Για το μέρος της εύρεσης της περιόδου όπως είδαμε πρέπει να επαναλάβουμε $\mathcal{O}(log\, N)$ ένα κβαντικό κύκλωμα το οποίο αποτελείται από το κύκλωμα της $f(x) = a^x \ mod\ N$ και το κύκλωμα του QFT_N. Επιπλέον, μπορούμε να κατασκευάσουμε κβαντικό

κύκλωμα για την $f(x) = a^x \ mod \ N$ πολυπλοκότητας $\mathcal{O}\left((log\ N)^3\right)$ και κβαντικό κύκλωμα για τον QFT_N πολυπλοκότητας $\mathcal{O}\left((log\ N)^2\right)$. Άρα, η πολυπλοκότητα του αλγορίθμου του Shor είναι $\mathcal{O}\left((log\ N)^4\right)$.

5.3.4 Υλοποίηση

Θα περάσουμε τώρα σε μία υλοποίηση του αλγορίθμου του Shor για την περίπτωση που θέλουμε να βρούμε έναν παράγοντα του $N = 15$. Ως a επιλέγουμε το 2, του οποίου η τάξη είναι $r = 4$ και πράγματι το $2^{\frac{r}{2}}$ είναι μία μη τετριμμένη ρίζα της μονάδας. Αφού το $N = 15$ πρέπει να δημιουργήσουμε μία υπέρθεση της συνάρτησης $f(x) = 2^x \ mod \ 15$ στο σύνολο $\{0, 1, \ldots, 2^8 - 1\}$ καθώς $2^8 > 15^2$. Άρα θα χρησιμοποιήσουμε 8 qubits για τα ορίσματα της f και 4 qubits για τα αποτελέσματα της. Ξεκινάμε υλοποιώντας τον διακριτό μετασχηματισμό Fourier:

```
def Fourier r = |r> -> x, x' .
  1/(2^(n/2)) * e^(2 * pi * i * int x * int x' / (2^n));
```

Και με βάση την παραμετρική έκφραση του διακριτού μετασχηματισμού Fourier η υλοποίηση του αλγορίθμου του Shor είναι η εξής:

```
def Shor =
  let (x, y) = spawn \ (b7, b6, b5, b4, b3, b2, b1, b0) -> (..., ..., ..., ...) in
  Fourier x;
```

όπου στις ... πρέπει να τοποθετήσουμε τις Boolean εκφράσεις που μας δίνουν τις τιμές των bits της $f(x) = 2^x \ mod \ 15$. Ένας τρόπος να υπολογίσουμε αυτές τις Boolean εκφράσεις, σε καμία περίπτωση ο καλύτερος καθώς δημιουργεί Boolean εκφράσεις εκθετικού μήκους, είναι να αποτιμήσουμε την $f(x) = 2^x \ mod \ 15$ για κάθε $b \in \{0, 1, \ldots, 2^8 - 1\}$ και κατόπιν ως Boolean έκφραση του i-οστού bit της f, για $i = 0, 1, 2, 3$, να πάρουμε την έκφραση:

$$\bigvee_{\substack{b \in \{0,1,\ldots,2^8-1\} \\ (f(b))_i = 1}} \bigwedge_{j=0}^{7} g\,(b, j)$$

όπου:

$$(x)_j = \left(x \ mod \ 2^{j+1}\right) \ div \ 2^j$$

και

$$g(x, j) = \begin{cases} x_j & \text{αν } (x)_j = 1 \\ \neg x_j & \text{αν } (x)_j = 0 \end{cases}$$

Τώρα αν θέσουμε $n = 8$ και καλέσουμε `Shor` θα πάρουμε:

$$[\![\emptyset; 0 \vdash^{\circ} \texttt{Shor} : \tau; 12]\!]\,(1) =$$

$$\frac{1}{4} \cdot |0\rangle \otimes \left(|2^0\rangle + |2^1\rangle + |2^2\rangle + |2^3\rangle\right) + \frac{1}{4} \cdot |64\rangle \otimes \left(|2^0\rangle + i \cdot |2^1\rangle - |2^2\rangle - i \cdot |2^3\rangle\right) +$$

$$\frac{1}{4} \cdot |128\rangle \otimes \left(|2^0\rangle - |2^1\rangle + |2^2\rangle - |2^3\rangle\right) + \frac{1}{4} \cdot |192\rangle \otimes \left(|2^0\rangle - i \cdot |2^1\rangle - |2^2\rangle + i \cdot |2^3\rangle\right)$$

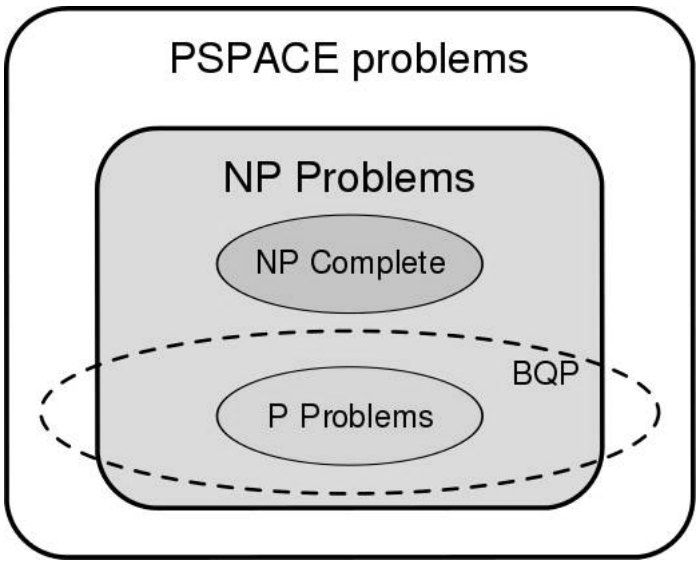
το οποίο δηλώνει ότι: $\dfrac{2^8}{r} = gcd(0, 64, 128, 192) = 64 \implies r = \dfrac{2^8}{64} = 4$. Συνεπώς δύο παράγοντες του 15 είναι οι $gcd(15, 2^{\frac{4}{2}} + 1) = 5$ και $gcd(15, 2^{\frac{4}{2}} - 1) = 3$.

5.4 Στοιχεία κβαντικής θεωρίας πολυπλοκότητας

Στην θεωρεία πολυπλοκότητας με BQP, από τα αρχικά Bounded Error, Quantum, Polynomial, συμβολίζουμε την κλάση των προβλημάτων απόφασης που λύνονται από έναν κβαντικό υπολογιστή σε πολυωνυμικό χρόνο με την πιθανότητα η απάντηση να είναι λανθασμένη να είναι φραγμένη από μία σταθερά γνησίως μικρότερη του $\frac{1}{2}$. Έτσι μπορούμε να επαναλάβουμε τον αλγόριθμο αρκετές φορές ώστε η πλειοψιφία των αποτελεσμάτων που θα πάρουμε να εκφράζει το σωστό αποτέλεσμα με πιθανότητα όσο κοντά στο 1 θέλουμε. Το κλασικό ανάλογο της κλάσης BQP είναι η κλάση BPP.

Η σχέση της κλάσης προβλημάτων BQP με τις NP, NP-complete και P δεν έχει μέχρι σήμερα αποσαφηνιστεί. Πιστεύεται όμως ότι η P είναι υποσύνολο της BQP, καθώς και ότι η NP-complete είναι ξένη με την BQP. Το πρόβλημα απόφασης που αντιστοιχεί στην παραγοντοποίηση ακεραίων, δηλαδή δοθέντων φυσικών αριθμών N και M με $1 \leq M \leq N$ να απαντηθεί αν υπάρχει διαιρέτης d του N τέτοιος ώστε $1 < d < M$, είναι ένα παράδειγμα προβλήματος που ανήκει στην BQP αλλά πιστεύεται ότι δεν ανήκει στην BPP. Μέχρι στιγμής δεν έχει αποδειχθεί ότι κάποιο NP-complete πρόβλημα ανήκει στην BQP.

Να σημειώσουμε εδώ για μία ακόμα φορά ότι οι κβαντικοί υπολογισμοί δεν αλλοιώνουν την έννοια του υπολογίσιμου. Δηλαδή τα υπολογιστικά όρια των κβαντικών υπολογιστών είναι τα ίδια με αυτά των κλασικών, δεν μπορούν να λύσουν προβλήματα όπως το halting problem. Απλά σε κάποιες περιπτώσεις ορισμένοι υπολογισμοί πραγματοποιούνται αποδοτικότερα από έναν κβαντικό υπολογιστή σε σχέση με έναν κλασικό.



Σχήμα 5.1: Η πιθανολογούμενη σχέση της BQP με άλλες κλάσης πολυπλοκότητας

Κεφάλαιο 6

Συμπεράσματα

6.1 Συνεισφορά

Η συνεισφορά της εργασίας στην προσπάθεια για την δημιουργία καλών γλωσσών κβαντικού προγραμματισμού μπορεί να συνοψιστεί ως εξής:

- Προτάθηκε ένας καινούριος τελεστής ο οποίος μπορεί να προσφέρει διαίσθηση στον προγραμματιστή καθώς ενσωματώνει ιδέες από τον παράλληλο προγραμματισμό και τις κλασικές συναρτήσεις. Ο τελεστής αυτός φαίνεται να παραμετροποιεί ικανοποιητικά την βασική πηγή υπεροχής των κβαντικών υπολογισμών που είναι η αρχή της υπέρθεσης ή αλλιώς ο κβαντικός παραλληλισμός. Επιπλέον, εξ αιτίας αυτού του τελεστή εισήχθησαν τα qubits υπηρέτες στην nQML. Η χρήση qubits υπηρετών σε μία γλώσσα κβαντικού προγραμματισμού φαίνεται επιβεβλημένη, ειδικά αν σκεφτεί κανείς πόσο δυσκολεύει το έργο κατασκευής ενός κβαντικού υπολογιστή όσο το πλήθος των qubits που διαθέτει γίνεται μεγαλύτερο. Τόσο ο νέος τελεστής όσο και τα qubits υπηρέτες ενσωματώθηκαν ομαλά στο συντακτικό, στο σύστημα τύπων και στην σημασιολογία υπό την μορφή κβαντικών κυκλωμάτων της nQML.
- Παρουσιάστηκε και υλοποιήθηκε σε Haskell μία νέα σημασιολογία για τα προγράμματα nQML. Η σημασιολογία αυτή αν και απέχει από μία φυσική υλοποίηση έχει να προσφέρει στην κατανόηση της λειτουργίας της nQML και των κβαντικών υπολογισμών γενικότερα, καθώς βρίσκεται πολύ κοντά στο μαθηματικό μοντέλο των κβαντικών υπολογισμών.
- Υλοποιήθηκε σε nQML ο αλγόριθμος του Shor. Σε αυτή την υλοποίηση έπαιξε καταλυτικό ρόλο ο νέος τελεστής. Μέσω της υλοποίησης της σημασιολογίας της nQML σε Haskell υπολογίστηκε και η σημασία του προγράμματος nQML που υλοποιεί τον αλγόριθμο του Shor και είδαμε ότι συμφωνεί με τα θεωρητικά αποτελέσματα.

6.2 Μελλοντική έρευνα

Η περιοχή της κβαντομηχανικής και των εφαρμογών της είναι ένας νέος επιστημονικός χώρος που εξελίσσεται διαρκώς. Οι κβαντικοί υπολογιστές βρίσκονται ακόμα σε πολύ πρώιμο στάδιο, καθώς αυτοί που έχουμε στην διάθεση μας αποτελούνται μόλις από μερικές δεκάδες qubits. Το πεδίο των κβαντικών υπολογισμών δεν έχει ακόμα ωριμάσει αρκετά, αφού οι κβαντικοί αλγόριθμοι που έχει να παρουσιάσει είναι ελάχιστοι. Και όσο για τις κβαντικές γλώσσες προγραμματισμού, αυτές βρίσκονται στο επίπεδο της προδιαγραφής κβαντικών κυκλωμάτων ή ορθομοναδιαίων μετασχηματισμών. Όπως φαίνεται λοιπόν υπάρχει άπλετος χώρος για ερευνητική δράση και πάρα πολλά ζητήματα τα οποία πρέπει να λυθούν ώστε να μπορούμε να αντιμετωπίζουμε μία μέρα τους κβαντικούς υπολογιστές όπως αντιμετωπίζουμε σήμερα τους κλασικούς υπολογιστές.

Αναφορικά με τις κβαντικές γλώσσες προγραμματισμού και τις προεκτάσεις της συγκεκριμένης εργασίας, σίγουρα θα ήταν επιθυμητή η βελτίωση του τρόπου με τον οποίο ο προγραμματιστής διατυπώνει τις κλασικές συναρτήσεις που αποτελούν τα ορίσματα του νέου τελεστή. Δεν περιμένουμε στην πράξη να ορίζει κανείς μία συνάρτηση ως μία Boolean έκφραση αποτελούμενη από τους συνδέσμους not και and απλά και μόνο επειδή αυτοί οι δύο σύνδεσμοι επαρκούν για να περιγράψει κανείς

όλες τις Boolean εκφράσεις. Αντιθέτως, θα ήταν αρκετά βολικό να προσφέραμε απευθείας στον προγραμματιστή την δυνατότητα να χρησιμοποιήσει τελεστές όπως η πρόσθεση, ο πολλαπλασιασμός, η ακέραια διαίρεση και η ύψωση σε δύναμη.

Σε επόμενη φάση, σκόπιμο θα ήταν να επανεξετάσουμε πως μπορούμε να συνδέσουμε τον κβαντικό παραλληλισμό με τον κλασικό παραλληλισμό. Το πρόβλημα αυτό φαίνεται να είναι πιο δύσκολο στο στάδιο όπου διαθέτουμε μία υπέρθεση και θέλουμε να αντλήσουμε από αυτή την υπέρθεση την πληροφορία που μας ενδιαφέρει. Η δυσκολία εντοπίζεται στο ότι από τους αλγορίθμους που γνωρίζουμε μέχρι τώρα ο τρόπος άντλησης της πληροφορίας φαίνεται να είναι ιδιαίτερα τεχνασματικός και ξεχωριστός για κάθε αλγόριθμο. Συνεπώς, για να κινηθούμε προς αυτή την κατεύθυνση θα διευκόλυνε η εμφάνιση νέων κβαντικών αλγορίθμων ώστε να μεγαλώσει το δείγμα μας και να έχουμε καλύτερες πιθανότητες να εντοπίσουμε πρότυπα.

Βιβλιογραφία

[Alte05] T. Altenkirch and J. Grattage, "A functional quantum programming language", in *Proceedings of the 20th Annual IEEE Symposium on Logic in Computer Science*, pp. 249–258, IEEE Computer Society, 2005.

[Alte09] T. Altenkirch and A. S. Green, "The quantum IO monad", in *Semantic Techniques in Quantum Computation*, Cambridge University Press, 2009.

[Deut92] D. Deutsch and R. Jozsa, "Rapid solutions of problems by quantum computation", *Proceedings of the Royal Society of London*, vol. A 439, pp. 553–558, December 1992.

[Gay06] S. J. Gay, "Quantum programming languages: Survey and bibliography", *Mathematical Structures in Computer Science*, vol. 16, no. 4, pp. 581–600, August 2006.

[Grat06] J. Grattage, *QML: A functional quantum programming language*, Ph.D. thesis, School of Computer Science and Scool of Mathematical Sciences, The University of Nottingham, September 2006.

[Gree13] A. S. Green, P. L. Lumsdaine, N. J. Ross, P. Selinger and B. Valiron, "Quipper: A scalable quantum programming language", in *Proceedings of the 34th Annual ACM SIGPLAN Conference on Programming Languages Design and Implementation*, June 2013.

[Grov96] L. K. Grover, "A fast quantum mechanical algorithm for database search", in *Proceedings of the 28th annual ACM Symposium on the Theory of Computing*, pp. 212–219, Philadelphia, PA, May 1996.

[Knil96] E. Knill, "Conventions for quantum pseudocode", Technical Report LAUR-96-2724, Los Alamos National Laboratory, 1996.

[Lamp08] M. Lampis, K. G. Ginis, M. A. Papakyriakou and N. S. Papaspyrou, "Quantum data and control made easier", *Electronic Notes in Theoretical Computer Science*, vol. 210, pp. 85–105, July 2008.

[Rous13] Y. Rouselakis, N. S. Papaspyrou, Y. Tsiouris and E. N. Todoran, "Compilation to Quantum Circuits for a Language with Quantum Data and Control", in *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems*, pp. 1537–1544, 2013.

[Sand00] J. W. Sanders and P. Zuliani, "Quantum programming", in *Proceedings of the 5th International Conference on Mathematics of Program Construction*, pp. 80–99, London, 2000.

[Seli04] P. Selinger, "Towards a quantum programming language", *Mathematical Structures in Computer Science*, vol. 14, no. 4, pp. 527–586, 2004.

[Seli06] P. Selinger and B. Valiron, "A lambda calculus for quantum computation with classical control", *Mathematical Structures in Computer Science*, vol. 16, no. 3, pp. 527–552, 2006.

[Shor97] P. W. Shor, "Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.

[Vedr96] V. Vedral, A. Barenco and A. Ekert, "Quantum Networks for Elementary Airthmetic Operations", *Physical Review A*, 1996.

[vTon04] A. van Tonder, "A lambda calculus for quantum computation", *SIAM Journal on Computing*, vol. 33, no. 5, pp. 1109–1135, 2004.

[Öme03] B. Ömer, *Structured quantum programming*, Ph.D. thesis, Institute of Information Systems, Technical University of Vienna, May 2003.