



SemNatComp: Σημασιολογικά μοντέλα και τεχνολογίες για φυσικούς υπολογισμούς

Ενδιάμεση Έκθεση Προόδου του Ερευνητικού Έργου
με κωδικό ΓΓΕΤ 11 ROM 11_1_ET30
Διμερούς συνεργασία Ελλάδας–Ρουμανίας 2011-12

Αθήνα, Απρίλιος 2013

Ενδιάμεση έκθεση προόδου

Επιστημονικός Υπεύθυνος: **Νικόλαος Παπασπύρου**, Επικ. Καθηγητής
Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Πολυτεχνειούπολη Ζωγράφου, 15780 Αθήνα
Τηλ. +30-210-7723393 • Fax +30-210-7722509 • E-mail: nickie@softlab.ntua.gr

Ρουμανική ομάδα, Επιστημονικός Υπεύθυνος: **Eneia Todoran**, Professor
Technical University of Cluj Napoca, Computer Science Department
28 Gh. Baritiu Street, 400027, Cluj-Napoca, Romania
Tel. +40-264-401481 • Fax +40-264-594491 • E-mail: eneia.todoran@cs.utcluj.ro

Πίνακας Περιεχομένων

ΕΙΣΑΓΩΓΗ	1
ΣΚΟΠΟΣ ΤΗΣ ΕΚΘΕΣΗΣ	1
ΣΥΝΤΟΜΗ ΠΕΡΙΓΡΑΦΗ ΤΟΥ ΕΡΓΟΥ	1
ΑΠΟΤΕΛΕΣΜΑΤΑ	2
ΔΙΑΡΘΡΩΣΗ ΤΗΣ ΕΚΘΕΣΗΣ	4
ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ ΜΕΧΡΙ ΣΗΜΕΡΑ ΕΡΓΟΥ ΤΗΣ ΡΟΥΜΑΝΙΚΗΣ ΟΜΑΔΑΣ	5
ΣΗΜΑΣΙΟΛΟΓΙΚΑ ΜΟΝΤΕΛΑ ΓΙΑ ΦΥΣΙΚΟΥΣ ΥΠΟΛΟΓΙΣΜΟΥΣ	5
ΑΝΑΛΛΟΙΩΤΕΣ ΥΠΟΛΟΓΙΣΜΩΝ ΣΕ ΣΗΜΑΣΙΟΛΟΓΙΑ ΜΕ ΣΥΝΕΧΕΙΕΣ ΓΙΑ ΤΑΥΤΟΧΡΟΝΙΣΜΟ	5
ΠΕΙΡΑΜΑΤΑ ΧΡΗΣΗΣ ΣΗΜΑΣΙΟΛΟΓΙΚΩΝ ΜΟΝΤΕΛΩΝ ΦΥΣΙΚΩΝ ΥΠΟΛΟΓΙΣΜΩΝ ΣΕ ΔΙΚΤΥΑ	6
ΣΗΜΑΣΙΟΛΟΓΙΑ ΓΛΩΣΣΩΝ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΜΩΝ ΚΑΙ ΚΒΑΝΤΙΚΑ ΚΥΚΛΩΜΑΤΑ	7
ΕΙΣΑΓΩΓΗ	7
Η ΓΛΩΣΣΑ ΚΒΑΝΤΙΚΟΥ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ NQML	11
ΜΕΤΑΓΛΩΤΤΙΣΗ ΤΗΣ NQML ΣΕ ΚΒΑΝΤΙΚΑ ΚΥΚΛΩΜΑΤΑ	16
ΒΙΒΛΙΟΓΡΑΦΙΑ	20
ΣΥΜΠΕΡΑΣΜΑΤΑ ΚΑΙ ΜΕΛΛΟΝΤΙΚΟΣ ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΣ	23

Εισαγωγή

Σκοπός της έκθεσης

Η έκθεση αυτή αποσκοπεί στο να παρουσιάσει τα αποτελέσματα του πρώτου χρόνου εκτέλεσης για το ερευνητικό έργο με ακρωνύμιο «SemNatComp» και τίτλο:

«Σημασιολογικά μοντέλα και τεχνολογίες για φυσικούς υπολογισμούς»
“Semantic models and technologies for natural computations”

που συγχρηματοδοτείται από τη Γενική Γραμματεία Έρευνας και Τεχνολογίας (ΓΓΕΤ) και την Ευρωπαϊκή Ένωση, στο πλαίσιο των Επιχειρησιακών Προγραμμάτων «Ανταγωνιστικότητα και Επιχειρηματικότητα» και «Περιφερειών σε Μετάβαση», στη δράση διμερούς ερευνητικής και τεχνολογικής συνεργασίας Ελλάδας–Ρουμανίας 2011-2012. Ο κωδικός αριθμός του έργου είναι ΓΓΕΤ 11 ROM 11_1_ET30.

Σύντομη περιγραφή του έργου

Στη σύγχρονη εποχή, η βιομηχανία των υπολογιστών αναζητά όλο και περισσότερη υπολογιστική ισχύ και ευελιξία στη διενέργεια υπολογισμών. Οι υποστηρικτές των φυσικών υπολογισμών (natural computing) θεωρούν ότι η αρχιτεκτονική υπολογιστών von Neumann δεν αποτελεί σήμερα την καλύτερη προσέγγιση στην ικανοποίηση αυτών των αναγκών και αναζητούν τη λύση σε μη συμβατικά υπολογιστικά μοντέλα, γλώσσες και αρχιτεκτονικές. Οι φυσικοί υπολογισμοί είναι το ερευνητικό πεδίο που μελετά ουσιαστικά τρεις κατηγορίες επιστημονικών μεθόδων: (1) αυτές που αναπτύσσουν νέες τεχνικές επίλυσης προβλημάτων, εμπνευσμένες από τη φύση, (2) αυτές που χρησιμοποιούν ηλεκτρονικούς υπολογιστές και μελετούν φυσικά φαινόμενα με όρους της θεωρίας πληροφορίας, και (3) αυτές που χρησιμοποιούν φυσικά υλικά (π.χ. μόρια) για τη διεξαγωγή υπολογισμών. Το προτεινόμενο ερευνητικό έργο έχει σκοπό να ακολουθήσει αυτήν την ερευνητική κατεύθυνση, αξιοποιώντας παράλληλα την προηγούμενη εμπειρία των δύο ερευνητικών ομάδων και τα προηγούμενα θεωρητικά και πειραματικά τους αποτελέσματα.

Το προτεινόμενο ερευνητικό έργο ασχολείται με την ανάπτυξη νέων τεχνικών αυστηρής τυπικής περιγραφής της σημασιολογίας και νέων πρωτότυπων τεχνολογιών για τη διενέργεια φυσικών υπολογισμών. Η έρευνα θα επικεντρωθεί σε γλώσσες και υπολογιστικά φαινόμενα βασισμένα στη βιολογία και την κβαντομηχανική. Θα αναπτυχθούν δηλωτικά μοντέλα (denotational models) για φυσικούς υπολογισμούς, και ιδιαίτερα για τους υπολογισμούς μεμβρανών (membrane computing) και τους κβαντικούς υπολογισμούς (quantum computing), με σκοπό τη βελτίωση της εκφραστικότητας και της αποτελεσματικότητας των τυπικών περιγραφών, ώστε να είναι δυνατή η χρήση τους σε (πολύπλοκα) φυσικά συστήματα.

Το κύριο αντικείμενο του προτεινόμενου έργου είναι:

- Η ανάπτυξη μιας γενικής θεωρίας για την περιγραφή της σημασιολογίας της παράλληλης επεξεργασίας και της επικοινωνίας, όπως αυτές εμφανίζονται στους φυσικούς υπολογισμούς.
- Η σχεδίαση και υλοποίηση πρωτότυπων γλωσσών εμπνευσμένων από φαινόμενα του φυσικού κόσμου.
- Η εφαρμογή τεχνικών των φυσικών υπολογισμών για την επίλυση υπολογιστικών προβλημάτων στις περιοχές της επεξεργασίας εικόνας και της όρασης υπολογιστών.

Τα κυριότερα αναμενόμενα αποτελέσματα του έργου είναι:

- Η σχεδίαση νέων δηλωτικών σημασιολογικών μοντέλων για φυσικούς υπολογισμούς, με χρήση συνεχειών και μονάδων.
- Η μελέτη ειδικών θεμάτων της σημασιολογίας των δομημένων συνεχειών για την παράλληλη επεξεργασία.
- Η ανάπτυξη πρωτότυπων υλοποιήσεων και η διεξαγωγή πειραμάτων σε δίκτυα ομότιμων υπολογιστών (peer-to-peer) και υπολογιστών σε συνδεσμολογία νέφους (cloud computing), χρησιμοποιώντας ειδικά σχεδιασμένες γλώσσες, εμπνευσμένες από το φυσικό κόσμο.
- Η μελέτη και διεξαγωγή πειραμάτων με σκοπό την αποτελεσματική εφαρμογή κατάλληλων τεχνικών των φυσικών υπολογισμών στον τομέα της επεξεργασίας εικόνας και της όρασης υπολογιστών.

Αποτελέσματα

Η εκτέλεση του ερευνητικού έργου ξεκίνησε επισήμως την 16/3/2012 με την υπογραφή της σύμβασης από τη ΓΓΕΤ. Ουσιαστικά, το έργο ξεκίνησε περίπου δύο μήνες αργότερα. Η καθυστέρηση οφείλεται αφενός στην αλληλογραφία από τη ΓΓΕΤ, αφετέρου στις γραφειοκρατικές ενέργειες που απαιτούνται για την έναρξη ερευνητικών προγραμμάτων στους ειδικούς λογαριασμούς. Η πρώτη οικονομική περίοδος έχει διάρκεια ενός έτους και ολοκληρώθηκε την 16/3/2013. Η παρούσα έκθεση αφορά την πρώτη οικονομική περίοδο.

Τα αποτελέσματα από την εκτέλεση του πρώτου έτους του έργου παρουσιάζονται αναλυτικά στα επόμενα κεφάλαια αυτής της έκθεσης. Στην ενότητα αυτή συνοψίζεται η εικόνα του έργου μετά το τέλος του 12ου μήνα εκτέλεσης.

Τήρηση χρονοδιαγράμματος

Το χρονοδιάγραμμα εκτέλεσης του ερευνητικού έργου φαίνεται στο Σχήμα 1. Κατά τη διάρκεια του πρώτου έτους ολοκληρώθηκαν οι δυο πρώτες φάσεις του έργου, συγκεκριμένα:

Φάση 1: Βιβλιογραφική έρευνα και αμοιβαίες παρουσιάσεις της ανεξάρτητης έρευνας των δυο πλευρών.

Η φάση αυτή αποσκοπούσε στη συλλογή και μελέτη βιβλιογραφίας σχετικής με το αντικείμενο του έργου, στη μεταφορά τεχνογνωσίας και θεωρητικής κατάρτισης καθώς και στην εξασφάλιση καλών συνθηκών συνεργασίας και επικοινωνίας μεταξύ των δυο πλευρών.

Φάση 2: Μελέτη, διερεύνηση και επαλήθευση θεωρητικών μοντέλων και πειραματικών εργαλείων των φυσικών υπολογισμών.

Η φάση αυτή αποσκοπούσε στη συνέχεια της συνεργασίας πάνω στη θεμελίωση της σημασιολογίας των γλωσσών προγραμματισμού με χρήση μονάδων και συνεχειών, στην επαλήθευση των αποτελεσμάτων με τεχνικές που προέρχονται από τη θεωρία των μετρικών χώρων και στη σχεδίαση θεωρητικών μοντέλων και πρωτότυπων υλοποιήσεων για τους φυσικούς υπολογισμούς.

Διάρκεια/Duration (σε μήνες/months):	6	12	18	24
ΦΑΣΕΙΣ/ PHASES (συνοπτικά/in brief)				
<u>Φάση 1:</u> Βιβλιογραφική έρευνα και αμοιβαίες παρουσιάσεις της ανεξάρτητης έρευνας των δυο πλευρών	↔			
<u>Φάση 2:</u> Μελέτη, διερεύνηση και επαλήθευση θεωρητικών μοντέλων και πειραματικών εργαλείων των φυσικών υπολογισμών		↔		
<u>Φάση 3:</u> Εφαρμογή των θεωρητικών μοντέλων και των πειραματικών εργαλείων στην ανάπτυξη πολύπλοκων συστημάτων φυσικών υπολογισμών			↔	
<u>Φάση 4:</u> Επικύρωση και επαλήθευση των αποτελεσμάτων				↔
ΕΚΘΕΣΕΙΣ ΠΡΟΟΔΟΥ				
ΤΕΛΙΚΗ ΕΚΘΕΣΗ FINAL REPORT				✉

Σχήμα 1: Χρονοδιάγραμμα εκτέλεσης του ερευνητικού έργου.

Επίσης, αμέσως μετά τη λήξη του πρώτου έτους, ξεκίνησαν οι εργασίες της τρίτης φάσης του έργου, συγκεκριμένα:

Φάση 3: Εφαρμογή των θεωρητικών μοντέλων και των πειραματικών εργαλείων στην ανάπτυξη πολύπλοκων συστημάτων φυσικών υπολογισμών.

Η φάση αυτή αποσκοπεί στην επέκταση των μοντέλων της δεύτερης φάσης, ώστε να αναπαριστούν πολύπλοκες δομές που συναντώνται στα συστήματα μεμβρανών και στους κβαντικούς υπολογισμούς, στη σχεδίαση γλωσσών προγραμματισμού για χρήση σε δίκτυα ομότιμων υπολογιστών και σε συνδεσμολογία νέφους, και στην ανάπτυξη πρωτότυπων υλοποιήσεων..

Η τέταρτη φάση του έργου προγραμματίζεται εξ ολοκλήρου για το δεύτερο έτος εκτέλεσης, συγκεκριμένα:

Φάση 4: Επικύρωση και επαλήθευση των αποτελεσμάτων.

Η φάση αυτή αποσκοπεί στην ανάπτυξη και αξιολόγηση μιας μεθοδολογίας για την δημιουργία δηλωτικών μοντέλων για συστήματα του φυσικού κόσμου, βασισμένης στην εμπειρία που αποκομίσθηκε στην τρίτη φάση, και στην ανάπτυξη εργαλείων επαλήθευσης για τις πρωτότυπες υλοποιήσεις που αναπτύχθηκαν.

Πίνακας 1. Συνοπτικά αποτελέσματα οικονομικής διαχείρισης.

Κονδύλιο	Ποσό	Διατέθηκε
Νέοι ερευνητές	6,000.00	0.00
Ανταλλαγές - μετακινήσεις	5,500.00	2,040.00
Αναλώσιμα	500.00	0.00
Έξοδα κοινών δημοσιεύσεων	3,000.00	0.00
Συνολικός προϋπολογισμός έργου	15,000.00	2,040.00

Λόγω της καθυστερημένης έναρξης του έργου, έχει γίνει προσπάθεια για την επιτάχυνση των φάσεων 2 έως και 4. Για τη φάση 1 αυτό δεν ήταν δυνατό, καθώς η επίσκεψη των μελών της Ρουμανικής ομάδας στην Ελλάδα είχε προγραμματιστεί για τις αρχές Οκτωβρίου 2012 και δεν ήταν δυνατό να μετατεθεί νωρίτερα. Εκτιμάται ότι η ολοκλήρωση του έργου θα γίνει μέχρι την καταληκτική ημερομηνία που ορίζει το χρονοδιάγραμμα.

Επίσης, λόγω της καθυστέρησης (περίπου 1,5 έτους) μεταξύ της υποβολής της πρότασης και της έναρξης του, κανείς από τους δύο υποψήφιους διδάκτορες που ονομάζονται στην πρόταση δεν ήταν σε θέση να συνεισφέρει στο έργο ως νέος ερευνητής, είτε λόγω στρατιωτικής θητείας είτε λόγω επαγγελματικών υποχρεώσεων. Ως εκ τούτου, κατά τη διάρκεια του πρώτου έτους εκτέλεσης του ερευνητικού έργου, στο φυσικό αντικείμενο έχουν συνεισφέρει κυρίως τα μέλη ΔΕΠ του Εργαστηρίου Τεχνολογίας Λογισμικού: Νικόλαος Παπασπύρου και Κωνσταντίνος Σαγώνας. Κατά τη διάρκεια του δεύτερου έτους εκτέλεσης θα προστεθεί ένας νέος υποψήφιος διδάκτωρ του Εργαστηρίου Τεχνολογίας Λογισμικού, ο οποίος θα εργασθεί ως νέος ερευνητής (σχετικό αίτημα κατατίθεται στη ΓΓΕΤ).

Οικονομική διαχείριση

Αναλυτικός απολογισμός από τη διαχείριση των οικονομικών στοιχείων του ερευνητικού προγράμματος, όπως προκύπτει από τα αρχεία του Ερευνητικού Πανεπιστημιακού Ινστιτούτου Συστημάτων Επικοινωνιών και Υπολογιστών, κατατίθεται ανεξάρτητα ως «Ενδιάμεση Έκθεση Πιστοποίησης», όπως ζητείται από τη ΓΓΕΤ. Σύμβαση έργου νέρου ερευνητή δεν έχει ακόμη υπογραφεί, για τους λόγους που αναφέρονται παραπάνω. Τα παραστατικά των μέχρι σήμερα δαπανών είναι στη διάθεση των ελεγκτών της ΓΓΕΤ.

Στην ενότητα αυτή δίνονται συνοπτικά τα αποτελέσματα της οικονομικής διαχείρισης για την περίοδο από 16/3/2012 ως 16/3/2013. Τα στοιχεία αυτά δίνονται στον Πίνακα 1.

Διάρθρωση της έκθεσης

Το υπόλοιπο της έκθεσης είναι οργανωμένο σε τρία κεφάλαια, ως εξής:

- **Κεφάλαιο 2:** Συνοπτική παρουσίαση του ερευνητικού έργου της Ρουμανικής ομάδας, στο πλαίσιο της ανταλλαγής ερευνητικής εμπειρίας και τεχνογνωσίας (φάση 1).
- **Κεφάλαιο 3:** Συνοπτική παρουσίαση του ερευνητικού έργου της Ελληνικής ομάδας που σχετίζεται με κβαντικούς υπολογισμούς.
- **Κεφάλαιο 4:** Ενδεικτικός προγραμματισμός των εργασιών του δεύτερου έτους εκτέλεσης.

Παρουσίαση του μέχρι σήμερα έργου της Ρουμανικής ομάδας

Η παρουσίαση που ακολουθεί είναι πολύ συνοπτική και αναφέρεται σε εργασίες μελών της ερευνητικής ομάδας του Technical University Cluj Napoca καθώς και σε προγενέστερες κοινές εργασίες με μέλη της ελληνικής ομάδας. Τα ερευνητικά αποτελέσματα που προέκυψαν στη διάρκεια της μέχρι τώρα εκτέλεσης του έργου από την επέκταση και εξέλιξη κοινής προγενέστερης ερευνητικής δουλειάς στην περιοχή της σημασιολογίας του ταυτοχρονισμού πρόκειται να υποβληθούν προς δημοσίευση εντός του δεύτερου έτους εκτέλεσης του έργου.

Σημασιολογικά μοντέλα για φυσικούς υπολογισμούς

Η μαθηματική μεθοδολογία των μετρικών χώρων μπορεί να χρησιμοποιηθεί για τον ορισμό μίας δηλωτικής σημασιολογίας (denotational semantics) για τους φυσικούς υπολογισμούς και για το συσχετισμό αυτού με την απλούστερη λειτουργική σημασιολογία (operational semantics) μίας αφηρημένης γλώσσας ταυτόχρονου προγραμματισμού που ενσωματώνει τα παρακάτω χαρακτηριστικά: παράλληλη σύνθεση που βασίζεται στο μέγιστο παραλληλισμό και υπολογισμούς που καθορίζονται από ένα πολυσύνολο κανόνων επαναγραφής (rewriting rules). Η σημασιολογία μπορεί να εκφραστεί απλά με την τεχνική των συνεχειών για ταυτοχρονισμό (continuations for concurrency), που είναι το αντικείμενο προγενέστερης κοινής ερευνητικής δουλειάς των δύο ομάδων.

Σχετική είναι η παρακάτω δημοσίευση των μελών της Ρουμανικής ομάδας.

G. Ciobanu, E.N. Todoran. Relating two metric semantics for parallel rewriting of multisets. In *Proceedings of the 14th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing*, Timisoara, Romania. Pages 273-280. ISBN: 978-1-4673-5026-6. September 2012.

Αναλλοίωτες υπολογισμών σε σημασιολογία με συνέχειες για ταυτοχρονισμό

Σε συνέχεια των δύο προηγούμενων κοινών δημοσιεύσεων της Ελληνικής και της Ρουμανικής ομάδας:

E. N. Todoran, N. Papaspyrou. Continuations for parallel logic programming. In *Proceedings of the 2nd International ACM-SIGPLAN Conference on Principles and Practice of Declarative Programming*, pages 257-267, ACM Press, 2000.

E. N. Todoran, N. Papaspyrou. Continuations for prototyping concurrent languages. Technical Report CSD-SW-TR-1-06, National Technical University of Athens, School of Electrical and Computer Engineering, Software Engineering Laboratory, 2006.

και μετά από συζητήσεις και προγραμματισμό που προέκυψαν κατά τη διάρκεια της πρώτης φάσης του έργου, η Ρουμανική ομάδα εξέτασε τον τρόπο προσδιορισμού αναλλοίωτων (invariants) σε ταυτόχρονους υπολογισμούς που εκφράζονται με χρήση της σημασιολογίας συνεχειών για ταυτοχρονισμό. Σχετική είναι η παρακάτω δημοσίευση των μελών της Ρουμανικής ομάδας.

E. N. Todoran. A study on the relationship between direct semantics and continuation semantics for concurrency. *Automation, Computers, Applied Mathematics*, vol. 21(1), pp. 3-17. ISSN 1221-437X, 2012.

Πειράματα χρήσης σημασιολογικών μοντέλων φυσικών υπολογισμών σε δίκτυα

Η Ρουμανική ομάδα πειραματίστηκε με τη χρήση υλοποιήσεων υπολογισμών για δικτύα ομότιμων υπολογιστών (peer to peer) και υπολογιστών σε συνδεσμολογία νέφους (cloud computing), βασισμένων σε τυπικές περιγραφές γραμμένες σε στοχαστική άλγεβρα διεργασιών (stochastic process algebra). Η δραστηριότητα αυτή εντάσσεται στη δεύτερη φάση του έργου και αποσκοπεί στη διερεύνηση της χρησιμότητας των σημασιολογικών μοντέλων των φυσικών υπολογισμών στα εν λόγω δίκτυα. Σχετική δημοσίευση πρόκειται να υποβληθεί.

Σημασιολογία γλωσσών κβαντικών υπολογισμών και κβαντικά κυκλώματα

Η παρουσίαση που ακολουθεί περιέχει αποσπάσματα από εργασίες μελών της ερευνητικής ομάδας του Εργαστηρίου Τεχνολογίας Λογισμικού. Τα ερευνητικά αποτελέσματα που προέκυψαν στη διάρκεια της εκτέλεσης του έργου από την επέκταση και εξέλιξη προγενέστερης ερευνητικής δουλειάς στην περιοχή των κβαντικών γλωσσών προγραμματισμού πρόκειται να υποβληθούν προς δημοσίευση εντός του δεύτερου έτους εκτέλεσης του έργου.

Εισαγωγή

Ιστορία του μοντέλου κβαντικού υπολογισμού

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

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

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

$x_1, x_2, \dots, x_R$ και συνεπώς επειδή έχει τόσες πολλές μεταβλητές δεν είναι δυνατόν να προσομοιωθεί με ένα κανονικό υπολογιστή με αριθμό στοιχείων ανάλογο του R ή του N .

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

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

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

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

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

Από τότε μέχρι σήμερα εκατοντάδες ερευνητικά κέντρα προσπαθούν να κατασκευάσουν αξιόπιστους κβαντικούς υπολογιστές χρησιμοποιώντας διαφορετικά υλικά. Η μεγαλύτερη δυσκολία ανακύπτει από δύο

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

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

Ιστορία των γλωσσών κβαντικού προγραμματισμού

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

Το μειονέκτημα όμως αυτής της προσέγγισης είναι ότι μειώνεται η εκφραστικότητα του κβαντικού προγραμματισμού και η ευκολία κατασκευής νέων αλγορίθμων. Για παράδειγμα είναι πολύ δύσκολος ο προγραμματισμός σε assembly ενώ πολύ ευκολότερος σε υψηλότερου επιπέδου γλώσσες προγραμματισμού. Για αυτό το λόγο αναπτύχθηκαν οι πρώτες γλώσσες κβαντικού προγραμματισμού. Το κοινό χαρακτηριστικό τους είναι ότι χειρίζονται ένα ή περισσότερα κβαντικά bits μαζί με τα επιπλέον κλασικά bits ώστε να μπορούν να υλοποιήσουν και κλασικούς αλγόριθμους. Χωρίζονται όμως σε διάφορες κατηγορίες.

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

Εκτός από αυτήν την κατηγοριοποίηση υπάρχει και ο χωρισμός των κβαντικών γλωσσών σε δύο τάξεις: αυτές που επιτρέπουν μόνο κλασική ροή ελέγχου και αυτές που επιτρέπουν και κβαντική ροή ελέγχου. Η πρώτη και απλούστερη αποτελείται από γλώσσες οι οποίες επιτρέπουν την κβαντική υπέρθεση μόνο στην κατάσταση των qubits (κβαντικά bit). Αντίθετα ο έλεγχος του προγράμματος γίνεται με κλασικό τρόπο.

Συνοπτικά η υπέρθεση είναι η ικανότητα των κβαντικών συστημάτων να βρίσκονται σε περισσότερες από μία καταστάσεις ταυτόχρονα. Στο πρώτο είδος γλώσσών οι οποίες αναφέρονται ως “quantum data, classical control paradigm” τα προγράμματα ακολουθούν μια συγκεκριμένη ροή και απλώς επεξεργάζονται κβαντικά bits. Η δεύτερη κατηγορία είναι οι γλώσσες που επιτρέπουν και κβαντικό έλεγχο: “quantum data and control paradigm”. Σε αυτές το πρόγραμμα μπορεί να βρίσκεται σε υπέρθεση δύο δυνατών μονοπατιών υπολογισμού. Φυσικά και τα δεδομένα που χειρίζονται μπορούν να είναι σε υπέρθεση. Η κβαντική μηχανή Turing του Deutsch λειτουργούσε σύμφωνα με αυτό το μοντέλο.

Προστακτικές γλώσσες

Η ιστορία των γλώσσών κβαντικού προγραμματισμού ήταν αρχικά συνυφασμένη με τα μοντέλα που ανακαλύφθηκαν. Όπως είδαμε η κβαντική μηχανή Turing (QTM) του Deutsch εφευρέθηκε το 1985. Αυτή είχε μια στοιχειώδη ψευδογλώσσα - οδηγίες προστακτικής μορφής. Το 1993 οι Bernstein και Vazirani εκτός από την βελτίωση της μηχανής πρότειναν και κάποια προγραμματιστικά δομικά στοιχεία. Πιθανότατα όμως η πρώτη πρόταση για μια σαφώς ορισμένη κβαντική γλώσσα προγραμματισμού, σε αντίθεση με τις περιγραφές QTM μηχανών, ήρθε το 1996 με την εργασία του Knill. Αυτός ορίζει έναν προστακτικό ψευδοκώδικα ο οποίος έτρεχε σε ένα μοντέλο κβαντικής μηχανής τυχαίας πρόσβασης (Quantum Random Access Machine – QRAM) αντίστοιχο με το κλασικό μοντέλο RAM. Ο Knill κατανοεί ότι ο κβαντικός ψευδοκώδικας δεν αποτελεί από μόνος του μια υλοποιήσιμη κβαντική γλώσσα αλλά είναι ένα σημαντικό βήμα εμπρός σε σχέση με τις εκ των υστέρων περιγραφές του πως πρέπει να υλοποιούνται οι κβαντικοί υπολογισμοί. Κατά τη διάρκεια μιας περιόδου αρκετών χρόνων (1998, 2000, 2001, 2002, 2003) ο Ömer ανέπτυξε την QCL, την πρώτη πραγματική κβαντική γλώσσα προγραμματισμού, με σύνταξη αρκετά παρόμοια της C. Μάλιστα υλοποίησε και ένα λειτουργικό προσομοιωτή της γλώσσας. Η QCL περιέχει μία πλήρη κλασική γλώσσα προγραμματισμού ως υποσύνολο και παρέχει ένα σύνολο χρήσιμων κβαντικών δομών υψηλού επιπέδου όπως διαχείριση μνήμης και αυτόματη παραγωγή ελεγχόμενων εκδόσεων τελεστών. Οι Sanders&Zuliani (2000) και Zuliani (2001) ορίζουν την προστακτική γλώσσα qQCL, η οποία βασίζεται σε μια αυστηρή γλώσσα εντολών (guarded-command language).

Συναρτησιακές γλώσσες

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

Parakytakiou, Papaspyrou (2006). Επιτρέπει νέες δομές ελέγχου και είναι απλούστερη χωρίς να χάνει σε εκφραστικότητα. Η σημασιολογία της μέχρι στιγμής αποτελείται μόνο από τελεστές σε πίνακες πυκνότητας και όχι από κβαντικά κυκλώματα.

Άλλες κατηγορίες γλωσσών

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

Η γλώσσα κβαντικού προγραμματισμού nQML

Η γλώσσα nQML αποτελεί μετεξέλιξη της συναρτησιακής γλώσσας κβαντικού προγραμματισμού QML (Altenkirch και Grattage, 2005a; 2005b). Ο κύριος στόχος στην σχεδιάσή της είναι να δώσει στους προγραμματιστές αρκετή εκφραστικότητα ώστε να υλοποιήσουν εύκολα κβαντικούς αλγόριθμους, ενώ ταυτόχρονα τους εμποδίζει να παραβούν τους κανόνες των κβαντικών υπολογισμών. Η nQML είναι μια συναρτησιακή γλώσσα υψηλού επιπέδου που βασίζεται στο μοντέλο «κβαντικά δεδομένα και κβαντικός έλεγχος». Περιλαμβάνει δομές οι οποίες επιτρέπουν κάθε ορθομοναδιαίο μετασχηματισμό να εκφραστεί ως πρόγραμμα με προφανή τρόπο, χρησιμοποιώντας περίπου τον ίδιο συμβολισμό που χρησιμοποιείται από τους σχεδιαστές κβαντικών αλγορίθμων. Επίσης επιτρέπει οι κβαντικές μετρήσεις να διεξάγονται σε οποιοδήποτε σημείο της εκτέλεσης του προγράμματος.

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

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

Η λειτουργική σημασιολογία της nQML βασίζεται στη χρήση πινάκων πυκνότητας οι οποίοι περιγράφουν κβαντικές καταστάσεις. Ένα ορθό πρόγραμμα της γλώσσας αντιστοιχεί σε μία συνάρτηση από πίνακες πυκνότητας σε πίνακες πυκνότητας και έτσι περιγράφεται η επίδραση του προγράμματος σε μια τυχαία κβαντική κατάσταση. Ορθά προγράμματα τα οποία δεν διενεργούν μετρήσεις αντιστοιχίζονται επίσης σε ένα ορθομοναδιαίο πίνακα ο οποίος περιγράφει τον μετασχηματισμό που διενεργούν στην κβαντική κατάσταση. Η εκτέλεση ενός προγράμματος nQML μπορεί να προσομοιωθεί με μια ακολουθία βημάτων που επηρεάζουν την κβαντική κατάσταση είτε δηλώνοντας νέα qubits, είτε εφαρμόζοντας ορθομοναδιαίους μετασχηματισμούς σε υπάρχοντα qubits, είτε μετρώντας την τιμή τους.

Η σύνταξη της nQML

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

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

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

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

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

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

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

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

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

Το σύστημα τύπων της nQML

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

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

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

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

Για κάθε κβαντικό τύπο τ ορίζουμε $\mathbf{C}(\tau)$ να είναι ο αντίστοιχος κλασικός τύπος. Στον κλασικό τύπο $\mathbf{complex}$ δεν αντιστοιχεί κανένας κβαντικός τύπος. Γράφουμε $|\mathbf{C}(\tau)|$ για να δηλώσουμε το μέγεθος, σε κλασικά bit, του κλασικού τύπου στον οποίο αντιστοιχεί ο τ και $\mathbf{qbits}(\tau)$ το σύνολο των qubit της κατάστασης τα οποία χρησιμοποιούνται από τις εκφράσεις τύπου τ . Για παράδειγμα, $\mathbf{qbits}(\mathbf{qbit}[4] \otimes \mathbf{qbit}[2]) = \{2, 4\}$. Ένας κβαντικός τύπος καλείται αγνός (pure) εάν η αναπαράστασή του χρησιμοποιεί διακεκριμένα qubit. Σημειώστε ότι στη γενική περίπτωση $|\mathbf{qbits}(\tau)| \leq |\mathbf{C}(\tau)|$ με την ισότητα να ισχύει μόνο όταν ο τύπος είναι αγνός. Ένα κβαντικό περιβάλλον τύπων Γ είναι μια αντιστοίχιση μεταβλητών σε κβαντικούς τύπους και όμοια ένα κλασικό περιβάλλον τύπων Δ είναι μια αντιστοίχιση μεταβλητών σε κλασικούς τύπους. Με $\mathbf{\Gamma|_k}$ συμβολίζουμε το περιβάλλον Γ το οποίο δεν περιέχει μεταβλητές των οποίων οι τύποι χρησιμοποιούν το k -οστό qubit της κβαντικής κατάστασης.

Η σχέση παραγωγής τύπων στην nQML γράφεται ως εξής: $\mathbf{\Gamma; n} \vdash^a \mathbf{e; \tau; m}$. Όπως και στο σύστημα τύπων της QML υπάρχουν δύο σχέσεις: μία για αγνές κβαντικές καταστάσεις (δηλαδή χωρίς κβαντικές μετρήσεις) που συμβολίζεται $\mathbf{\Gamma; n} \vdash^o \mathbf{e; \tau; m}$ και μία για τη γενική περίπτωση που συμβολίζεται $\mathbf{\Gamma; n} \vdash \mathbf{e; \tau; m}$.

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

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

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

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

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

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

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

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

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

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

Λειτουργική σημασιολογία της nQML

Η λειτουργική σημασιολογία της γλώσσας χρησιμοποιεί πίνακες πυκνότητας οι οποίοι αναπαριστούν την κβαντική κατάσταση των καταχωρητών. Ο χώρος $S(n) \subset \mathbb{C}^{2^n \times 2^n}$ περιέχει πίνακες πυκνότητας. Η λειτουργία μιας τυχαίας ορθά γραμμένης έκφρασης e με κανόνα παραγωγής $\Gamma; n \vdash e; \tau; m$ είναι μία συνάρτηση της μορφής $S(n) \rightarrow S(n + m)$. Δηλαδή αντιστοιχίζει μια κβαντική κατάσταση εισόδου n qubit

σε μία κατάσταση εξόδου $\mathbf{n} + \mathbf{m}$ qubits. Οι αγνές κβαντικές εκφράσεις οι οποίες δεν διεξάγουν μετρήσεις αντιστοιχίζονται σε ορθομοναδιαίους μετασχηματισμούς. Συμβολίζουμε με $\mathbf{T}(\mathbf{n}) \subset \mathbb{C}^{2^n \times 2^n}$ το χώρο των ορθομοναδιαίων πινάκων μετασχηματισμού. Εάν $\mathbf{e}$ είναι μια ορθά τυπωμένη αγνή κβαντική έκφραση με κανόνα παραγωγής $\Gamma; \mathbf{n} \vdash^\circ \mathbf{e} : \tau; \mathbf{m}$ τότε η σημασία της είναι ένας πίνακας της μορφής $\mathbf{T}(\mathbf{n} + \mathbf{m})$. Η σημασιολογία της εισαγωγής αγνών κβαντικών εκφράσεων σε μη αγνές εκφράσεις δίνεται παρακάτω. Το τανυστικό γινόμενο του πίνακα $\mathbf{A} \in \Sigma(\mathbf{n})$ με τον πίνακα $\Delta_{\mathbf{m}}$ επεκτείνει κατάλληλα την κβαντική κατάσταση με $\mathbf{m}$ κινούμενα qubit τα οποία αρχικοποιούνται με μηδενικές τιμές.

$$\mathbf{EMB}: \quad \llbracket \Gamma; \mathbf{n} \vdash^\circ \mathbf{e} : \tau; \mathbf{m} \rrbracket (\mathbf{A}) = \mathbf{T}(\mathbf{A} \otimes \Delta_{\mathbf{m}}) \mathbf{T}^*$$

όπου $\mathbf{T} = \llbracket \Gamma; \mathbf{n} \vdash^\circ \mathbf{e} : \tau; \mathbf{m} \rrbracket$

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

$$\mathbf{VAR}: \quad \llbracket \Gamma; \mathbf{n} \vdash^\circ \mathbf{x} : \tau; \mathbf{0} \rrbracket = \mathbb{I}_{\mathbf{n}}$$

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

Η σημασιολογία των δομών let, εισαγωγής γινομένου και απαλοιφής γινομένου είναι προφανής και παρόμοια. Σε κάθε μία από αυτές ο υπολογισμός ξεκινά με τον υπολογισμό της έκφρασης $\mathbf{e}_1$ και συνεχίζει με τον υπολογισμό του $\mathbf{e}_2$ στην αλλαγμένη κατάσταση. Οι μη αγνές περιπτώσεις είναι αρκετά όμοιες.

$$\mathbf{LET}^\circ: \quad \llbracket \Gamma; \mathbf{n} \vdash^\circ \text{let } \mathbf{x} = \mathbf{e}_1 \text{ in } \mathbf{e}_2 : \tau; \mathbf{m}_1 + \mathbf{m}_2 \rrbracket = \mathbf{T}_2(\mathbf{T}_1 \otimes \mathbb{I}_{\mathbf{m}_2})$$

όπου $\mathbf{T}_1 = \llbracket \Gamma; \mathbf{n} \vdash^\circ \mathbf{e}_1 : \tau_1; \mathbf{m}_1 \rrbracket$

$$\mathbf{T}_2 = \llbracket \Gamma, \mathbf{x} : \tau_1; \mathbf{n} + \mathbf{m}_1 \vdash^\circ \mathbf{e}_2 : \tau; \mathbf{m}_2 \rrbracket$$

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

$$\mathbf{IF}^\circ: \quad \llbracket \Gamma; \mathbf{n} \vdash^\circ \text{if } \mathbf{e} \text{ then } \mathbf{e}_1 \text{ else } \mathbf{e}_2 : \tau; \mathbf{m} + \max(\mathbf{m}_1, \mathbf{m}_2) \rrbracket = \mathbf{T}_C(\mathbf{T} \otimes \mathbb{I}_{\max(\mathbf{m}_1, \mathbf{m}_2)})$$

όπου $\mathbf{T} = \llbracket \Gamma; \mathbf{n} \vdash^\circ \mathbf{e} : qbit[\mathbf{k}]; \mathbf{m} \rrbracket$

$$\mathbf{T}_1 = \llbracket \Gamma|_{\mathbf{k}}; \mathbf{n} + \mathbf{m} \vdash^\circ \mathbf{e}_1 : \tau; \mathbf{m}_1 \rrbracket$$

$$\mathbf{T}_2 = \llbracket \Gamma|_{\mathbf{k}}; \mathbf{n} + \mathbf{m} \vdash^\circ \mathbf{e}_2 : \tau; \mathbf{m}_2 \rrbracket$$

$$\mathbf{T}'_1 = \text{except}(\mathbf{k}, \mathbf{T}_1) \otimes \mathbb{I}_{\max(\mathbf{m}_1, \mathbf{m}_2) - \mathbf{m}_2}$$

$$\mathbf{T}'_2 = \text{except}(\mathbf{k}, \mathbf{T}_2) \otimes \mathbb{I}_{\max(\mathbf{m}_1, \mathbf{m}_2) - \mathbf{m}_1}$$

$$\mathbf{T}_C = \text{cond}(\mathbf{k}, \mathbf{T}'_1, \mathbf{T}'_2)$$

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

$$\mathbf{IFM}: \quad \llbracket \Gamma; \mathbf{n} \vdash^\circ \text{ifm } \mathbf{e} \text{ then } \mathbf{e}_1 \text{ else } \mathbf{e}_2 : \tau; \mathbf{m} + \max(\mathbf{m}_1, \mathbf{m}_2) \rrbracket (\mathbf{A}) =$$

$$B_1 \otimes \Delta_{\max(m_1, m_2) - m_1} + B_2 \otimes \Delta_{\max(m_1, m_2) - m_2}$$

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

$$(B_t, B_f) = \text{measure}(k, B)$$

$$B_1 = \llbracket \Gamma; n + m \vdash e_1: \tau; m_1 \rrbracket(B_t \otimes \Delta_{m_1})$$

$$B_2 = \llbracket \Gamma; n + m \vdash e_2: \tau; m_2 \rrbracket(B_f \otimes \Delta_{m_2})$$

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

$$\text{TRANS}^\circ: \llbracket \Gamma; n \vdash^\circ |e\rangle \rightarrow x, x'.c: \tau; m \rrbracket = T_C T$$

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

$$T = \llbracket \Gamma; n \vdash^\circ e: \tau; m \rrbracket$$

$$C_{j,i} = \llbracket x: C(\tau), x': C(\tau) \vdash c: \text{complex} \rrbracket(\rho)$$

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

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

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

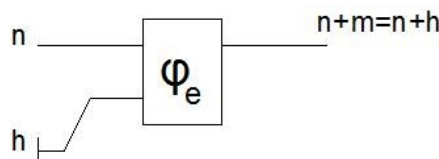
Μεταγλώττιση της nQML σε κβαντικά κυκλώματα

Στη συνέχεια παρουσιάζουμε μία δυνατή μεταγλώττιση προγραμμάτων της nQML σε κβαντικά κυκλώματα της κλάσης **FQC** (Grattage, 2006). Καθώς η σημασιολογία κάθε εντολής κρατάει και διαδίδει πληροφορίες για τον αριθμό των qubit της κατάστασης χρησιμοποιούμε τους σημασιολογικούς κανόνες ώστε ο αριθμός των καλωδίων στα κυκλώματα να συμφωνεί με τους κανόνες. Τα κυκλώματα κατασκευάζονται αναδρομικά, υποθέτοντας δηλαδή ότι έχουν ήδη κατασκευαστεί τα αντίστοιχα κυκλώματα των εκφράσεων που βρίσκονται στην υπόθεση των κανόνων. Αυτά συμβολίζονται ως ορθογώνια των οποίων το περιεχόμενο είναι ένα κύκλωμα της κλάσης **FQC** με καλώδια δεξιά και αριστερά τους (σωρός και σκουπίδια) στην περίπτωση που η παραγωγή της έκφρασης δεν είναι αγνή. Αν είναι αγνή (pure) παραλείπονται τα σκουπίδια. Φυσικά είναι δυνατόν και ο σωρός να είναι κενός αλλά στη γενική περίπτωση εισάγουμε καλώδια στο κύκλωμα.

Κανόνας EMB

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

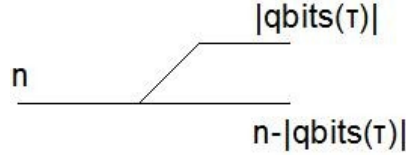
Ο κανόνας αυτός είναι προφανώς διαφανής στα κυκλώματα αφού απλώς δηλώνει τη σχέση $\text{FQC}^\circ \subset \text{FQC}$. Κάθε αγνό κύκλωμα μπορεί να θεωρηθεί και μη αγνό χωρίς καμία αλλαγή θεωρώντας ότι το σύνολο σκουπιδιών είναι κενό. Οι αριθμοί στα καλώδια της παρακάτω εικόνας αλλά και σε όλες τις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



Κανόνας VAR

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

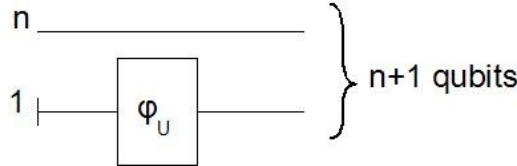
Και αυτός ο κανόνας είναι διαφανής αφού όπως αναφέραμε οι μεταβλητές είναι αναφορές σε qubits. Για να φανεί καλύτερα αυτό στο παρακάτω σχήμα αναδιατάσσουμε τα qubit της μεταβλητής x και τα φέρνουμε στο άνω μέρος του κυκλώματος. Φυσικά ο τύπος της x μπορεί να μην είναι αγνός και κάποια qubits να εμφανίζονται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



Κανόνας SUP

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

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

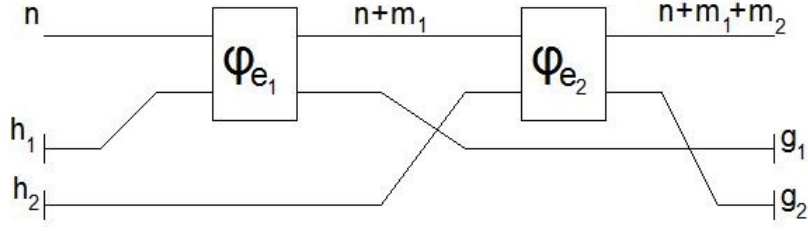


$$U = \begin{pmatrix} \lambda & \lambda' \\ \lambda' & -\lambda \end{pmatrix}$$

Κανόνας LET

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

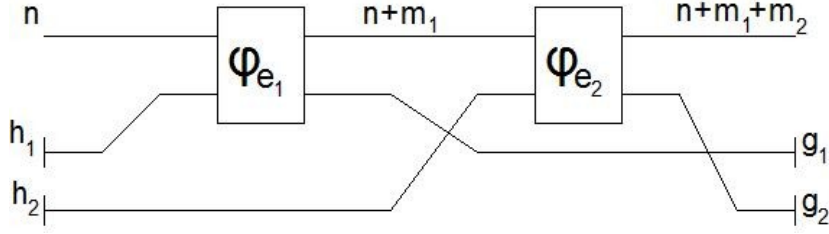
Σε αυτόν τον κανόνα υποθέτουμε ότι έχουν δημιουργηθεί εκ των προτέρων τα κυκλώματα για τον υπολογισμό των εκφράσεων e_1 και e_2 . Καθώς ο κανόνας δεν καθορίζει αν οι υπολογισμοί αυτοί είναι αγνοί ή όχι (αν δεν γίνονται μετρήσεις) θεωρώ την γενική περίπτωση και κάθε υπό-κύκλωμα εισάγεται με σωρό και με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



Κανόνας PROD

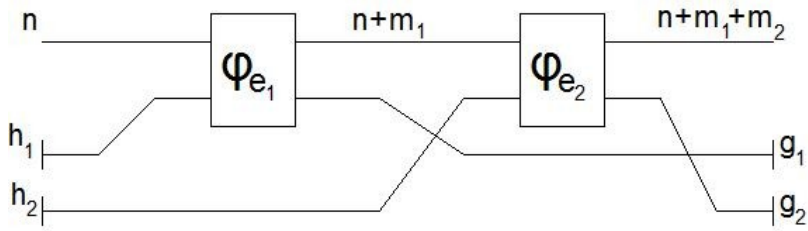
$$\frac{\Gamma; n \vdash^\alpha e_1: \tau_1; m_1 \quad \Gamma; n + m_1 \vdash^\alpha e_2: \tau_2; m_2}{\Gamma; n \vdash^\alpha (e_1, e_2): \tau_1 \otimes \tau_2; m_1 + m_2} \text{ (PROD)}$$

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



Κανόνας LETPROD

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



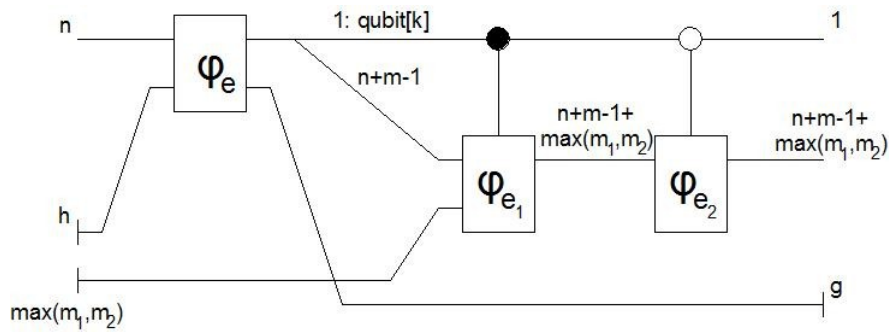
Κανόνας IF

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

Στο κύκλωμα αυτού του κανόνα πρώτα υπολογίζεται η έκφραση e : αυτή μπορεί να απαιτεί m qubit για τον υπολογισμό της, αλλά ο τελικός της τύπος πρέπει να είναι ένα μόνο qubit. Προσέξτε ότι τα υπόλοιπα qubit δεν είναι απαραίτητο να αποδεσμευτούν μαζί με τα (πιθανά) σκουπίδια της έκφρασης. Έπειτα υπολογίζονται οι δύο εκφράσεις e_1 και e_2 οι οποίες όμως έχουν τον περιορισμό να μην χρησιμοποιούν καθόλου το qubit του τύπου της έκφρασης e και να είναι αγνές, δηλαδή να μην παράγουν σκουπίδια. Ο πρώτος περιορισμός

φαίνεται στο κύκλωμα ξεχωρίζοντας το qubit και περνώντας το ως qubit ελέγχου στη δομή εκτέλεσης υπό συνθήκη.

Τέλος πρέπει να παρατηρήσουμε ότι τα επιπλέον qubit που μπορεί να χρησιμοποιεί η $\mathbf{e}_1$, τα $\mathbf{m}_1$ καλώδια, είναι δυνατόν να τα χρησιμοποιεί και η $\mathbf{e}_2$. Αυτό δεν αποτελεί πρόβλημα για τη λειτουργία του κυκλώματος καθώς υπό συνθήκη εκτέλεση εξασφαλίζει ότι κάθε κοινό qubit θα μεταβληθεί στο ποσοστό που του αναλογεί από την υπέρθεση του qubit ελέγχου. Ίσως ο πιθανός προγραμματιστής της γλώσσας θα πρέπει να προσέξει τους τύπους που δίνει στις μεταβλητές ώστε να παράγει το αποτέλεσμα που πράγματι θέλει. Για παράδειγμα αν χρησιμοποιεί την $\mathbf{e}_2$ ως συνάρτηση ανεξάρτητη της $\mathbf{e}_1$ πρέπει να προσέξει οι νέοι τύποι να μην μπλέκονται με ήδη δηλωμένους τύπους και άρα να αλλάξει τον κώδικά της (ουσιαστικά ορίζοντας πάντα νέα qubits-μεταβλητές).



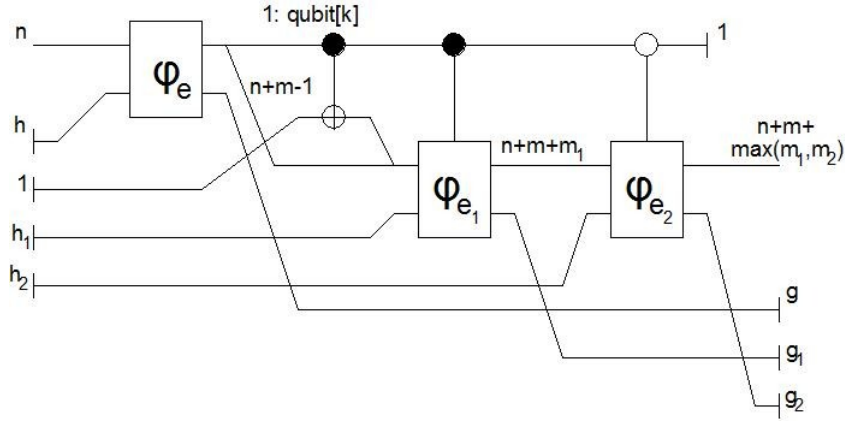
Κανόνας IFM

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

Ο κανόνας αυτός είναι όμοιος με τον κανόνα IF με τις διαφορές ότι επιτρέπονται και μη αγνές εκφράσεις στους δύο κλάδους, ότι οι δύο κλάδοι μπορούν να χρησιμοποιούν το qubit ελέγχου και ότι το qubit ελέγχου μετράται στο τέλος του κυκλώματος. Η πρώτη διαφορά φαίνεται από τα καλώδια σκουπιδιών των δύο εκφράσεων $\mathbf{e}_1$ και $\mathbf{e}_2$.

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

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

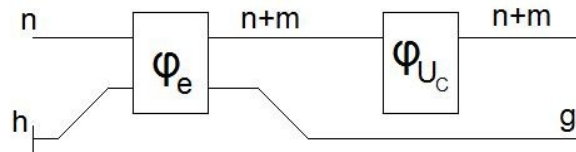


Κανόνας TRANS

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

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

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



Βιβλιογραφία

1. Feynman, Richard P. Simulating physics with computers. *International Journal of Theoretical Physics* 21:6/7. 1982, pp. 467-468.
2. Benioff, P. A. Quantum mechanical Hamiltonian models of discrete processes that erase their own histories: application to Turing machines. *International Journal of Theoretical Physics* 21:3/4. 1982, pp. 177-202.
3. Quantum theory, the Church-Turing principle and the universal quantum computer. Deutsch, David. 1985. *Proceedings of the Royal Society of London A* 400. pp. 97-117.

4. Bernstein, Ethan and Vazirani, Umesh. Quantum complexity theory. *SLAM Journal of Computing* 26:5. 1997, pp. 1411-1473.
5. Algorithms for quantum computation: discrete log and factoring. Shor, Peter W. 1994. *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pp. 20-22.
6. Shor, Peter W. Scheme for reducing decoherence in quantum computer memory. *Physical Review A* 52:4. 1995, pp. 2493-2496.
7. Selinger, Peter. Towards a Quantum Programming Language. *Mathematical Structures in Computer Science*. 2004, Vol. 14, 4, pp. 527-586.
8. Grattage, Jonathan and Altenkirch, Thorsten. QML: Quantum data and control. February 2005.
9. Grattage, Jonathan and Altenkirch, Thorsten. A compiler for a functional quantum programming language. January 2005.
10. Lampis, Michael, et al. Quantum data and control made easier. Elsevier Science B.V. 2006.
11. Grattage, Jonathan James. A functional quantum programming language. Thesis submitted to the University of Nottingham. September 2006.
12. Nielsen, Michael A. and Chuang, Isaac L. Quantum Computation and Quantum Information. s.l.: Cambridge University Press, 2000.
13. Hirvensalo, Mika. Quantum Computing. s.l.: Springer, 2001.
14. Kaye, Phillip, Laflamme, Raymond and Mosca, Michele. An Introduction to Quantum Computing. s.l.: Oxford University Press, 2007.

Συμπεράσματα και μελλοντικός προγραμματισμός

Οι δύο ομάδες που συμμετέχουν στο έργο θεωρούν την εξέλιξή του μέχρι σήμερα καθώς και την εν γένει μεταξύ τους συνεργασία ιδιαίτερα ικανοποιητική. Παρά τις δυσχερείς οικονομικές συνθήκες που συναντώνται στα πανεπιστήμια της Ελλάδας και της Ρουμανίας τα τελευταία χρόνια και που έχουν ως αποτέλεσμα την τραγική απομείωση της χρηματοδότησης βασικής έρευνας, όπως αυτή που διενεργείται σε αυτό το ερευνητικό έργο, οι δύο ομάδες προσβλέπουν στην υποβολή περισσότερων κοινών εργασιών προς δημοσίευση μέχρι το τέλος της εκτέλεσης του έργου.

Κατά τη διάρκεια του Απριλίου 2013 πρόκειται να πραγματοποιηθεί η επίσκεψη μικρής διάρκειας του επιστημονικού υπεύθυνου της Ελληνικής ομάδας στη Ρουμανία. Στην επίσκεψη αυτή, τα μέλη των δύο ομάδων θα συνεργαστούν με τους εξής στόχους:

1. Την ολοκλήρωση της μέχρι τώρα πραγματοποιηθείσας κοινής εργασίας πάνω στα σημασιολογικά μοντέλα φυσικών υπολογισμών που βασίζονται στις συνέχειες για ταυτοχρονισμό (continuations for concurrency) και την υποβολή κοινής εργασίας προς δημοσίευση σε επιστημονικό περιοδικό.
2. Τη διερεύνηση προοπτικών συνεργασίας σε περιοχές που μόνο η μία ομάδα έχει μέχρι σήμερα να παρουσιάσει δημοσιευμένο έργο, και συγκεκριμένα:
 - Την περιοχή των φυσικών υπολογισμών με μεμβράνες, όπου δραστηριοποιείται η Ρουμανική ομάδα, και
 - Την περιοχή των κβαντικών υπολογισμών, όπου δραστηριοποιείται η Ελληνική ομάδα.
3. Τον προγραμματισμό της τρίτης και της τέταρτης φάσης του έργου, κατά τη διάρκεια των οποίων θα γίνει η εφαρμογή των θεωρητικών μοντέλων που μελετήθηκαν για την ανάπτυξη πολύπλοκων συστημάτων φυσικών υπολογισμών. Για το σκοπό αυτό θα σχεδιαστούν και υλοποιηθούν κατάλληλες γλώσσες και θα αξιολογηθούν τα αποτελέσματα με συγκεκριμένες μελέτες περίπτωσης.