Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών Και Μηχανικών Υπολογιστών

Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών
Εργαστήριο Υπολογιστικών Συστημάτων

Διδακτορική Διατριβή

Ελαχιστοποίηση Εκφράσεων Αποκλειστικού Ή - Κβαντικοί Αλγόριθμοι

Μαρίνος Η. Σαμψών

Επιβλέπων Καθηγητής: Γ. Παπακωνσταντίνου

Αθήνα, Ιούλιος 2009

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών
Εργαστήριο Υπολογιστικών Συστημάτων

Ελαχιστοποίηση Εκφράσεων "Αποκλειστικού Ή" - Κβαντικοί Αλγόριθμοι

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Μαρίνος Η. Σαμψών

Διπλωματούχος Μηχανικός Η / Υ και Πληροφορικής
Πολυτεχνικής Σχολής Πανεπιστημίου Πατρών (2004)

Συμβουλευτική Επιτροπή: Γεώργιος Παπακωνσταντίνου
Παναγιώτης Τσανάκας
Νεκτάριος Κοζύρης

Εγκρίθηκε από την επταμελή εξεταστική επιτροπή την .....

.....	.....	.....
Γεώργιος Παπακωνσταντίνου Καθηγητής Ε.Μ.Π.	Παναγιώτης Τσανάκας Καθηγητής Ε.Μ.Π.	Νεκτάριος Κοζύρης Αναπ. Καθηγητής Ε.Μ.Π.
.....	.....	.....
Κυριάκος Χιτζανίδης Καθηγητής Ε.Μ.Π.	Ανδρέας-Γεώργιος Σταφυλοπάτης Καθηγητής Ε.Μ.Π.	Θεόδωρος Ανδρόνικος Λέκτορας Ιόνιου Πανεπιστήμιου

.....
Δημήτριος Σούντρης
Επίκ. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2009

.....

Μαρίνος Η. Σαμψών

Πρόλογος - Ευχαριστίες

Στο πλαίσιο αυτής της διατριβής, μου δόθηκε η ευκαιρία από τον καθηγητή μου, κ. Γ. Παπακωνσταντίνου, να ασχοληθώ ερευνητικά με τομείς ιδιαίτερα απαιτητικούς και ενεργούς, που αποτελούν αυτές τις μέρες την αιχμή του δόρατος της βασικής έρευνας. Στο ”ταξίδι” αυτό, ο κ. Παπακωνσταντίνου στάθηκε ακούραστος αρωγός και συνοδοιπόρος και για αυτό τον ευχαριστώ θερμά. Το πραγματικό πάθος του για την έρευνα, οι αστείρευτες γνώσεις του, η ακεραιότητα του χαρακτήρα του, το ήθος του και η γενικότερη στάση του αποτελούν για εμένα πηγή έμπνευσης και δύναμης.

Το Εργαστήριο Υπολογιστικών Συστημάτων της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Ε.Μ.Π. αποτέλεσε το χώρο στον οποίο περνούσα το μεγαλύτερο μέρος της μέρας μου τα τελευταία χρόνια. Υπήρξε ένας χώρος σκέψης και έμπνευσης που ήταν απαλλαγμένος από κάθε είδους ανταγωνισμό και καχυποψία. Για αυτό το λόγο αξίζουν συγχαρητήρια στα μέλη ΔΕΠ του εργαστηρίου Καθ. Γ. Παπακωνσταντίνου, Καθ. Π. Τσανάκα και Αν. Καθ. Ν. Κοζύρη, αλλά και σε όλα τα μέλη του εργαστηρίου.

Νιώθω την ανάγκη να ευχαριστήσω ιδιαίτερα τα μέλη της ερευνητικής μου ομάδας Δ. Βουδούρη και Μ. Καλαθά, που υπήρξαν ουσιαστικοί συνεργάτες στην έρευνα και πολύ καλοί φίλοι, η συνεργασία των οποίων υπήρξε εξαιρετικά πολύτιμη για την εκπόνηση της διατριβής αυτής. Επίσης θα ήθελα να ευχαριστήσω και τον φίλο και παλιό συνεργάτη Δ. Κασερίδη που δεν αρνήθηκε ποτέ να βοηθήσει, όταν χρειάστηκε, στην ανεύρεση της απαραίτητης βιβλιογραφίας.

Τα χρόνια που ήμουν στο Εργαστήριο Υπολογιστικών Συστημάτων είχα την ευκαιρία να γνωρίσω πολλούς αξιόλογους φίλους με τους οποίους περάσαμε ατελείωτες ώρες στο εργαστήριο, αλλά και έξω από αυτό. Αισθάνομαι ιδιαίτερα τυχερός και ευγνώμων που γνώρισα και με τίμησαν με ειλικρινή φιλία και συμπαράσταση τους ο Α. Δημόπουλο, ο Χ. Παυλάτο, Ι. Ρυακιωτάκη, ο Β. Κούκη και ο Δ. Καμενόπουλο. Το ίδιο ισχύει και για τους υπόλοιπους υποψήφιους διδάκτορες και γραμματείς που βρέθηκαν στο εργαστήριο αυτά τα χρόνια.

Τέλος, θα ήθελα επίσης να ευχαριστήσω θερμά τους γονείς μου, τον αδερφό μου, τη σύντροφό μου και την ευρύτερη οικογένειά μου για την αμέριστη συμπαράσταση στο εγχείρημα που αποφάσισα να αναλάβω πριν από σχεδόν 5 χρόνια.

Περίληψη

Η σημερινή εποχή χαρακτηρίζεται από την ολοένα αυξανόμενη ενσωμάτωση των ηλεκτρονικών υπολογιστών και των ενσωματωμένων συστημάτων σε όλες τις πτυχές της καθημερινής μας ζωής. Τα ολοκληρωμένα κυκλώματα συνεχώς σμικρύνονται, γίνονται ταχύτερα, απαιτούν όλο και μικρότερα ποσά ενέργειας με τη βοήθεια νέων υλικών και αρχιτεκτονικών. Αυτό έχει ως αποτέλεσμα οι ηλεκτρονικές συσκευές να βρίσκουν όλο και περισσότερες εφαρμογές σε όλους τους τομείς της ζωής μας και με τον καιρό να μετατρέπονται σε ένα αόρατο και απαραίτητο στρώμα διεπαφής μας με το περιβάλλον.

Το αντικείμενο με το οποίο ασχολείται μέχρι στιγμής η παρούσα διατριβή είναι η ελαχιστοποίηση λογικών εκφράσεων ”αποκλειστικού ή” (XOR) για τυχαία λογική συνάρτηση, και πιο συγκεκριμένα με τη μείωση των όρων από τους οποίους αυτή αποτελείται καθώς και με την απεικόνιση τέτοιων εκφράσεων σε αρχιτεκτονικές νέων τεχνολογιών όπως οι κβαντικοί υπολογιστές. Ένα ολοκληρωμένο κύκλωμα αποτελεί την πρακτική υλοποίηση μιας τέτοιας λογικής έκφρασης. Κατά συνέπεια, γίνεται προσπάθεια για την βελτιστοποίηση λογικών κυκλωμάτων. Η πιο γνωστή τέτοια κατηγορία εκφράσεων είναι οι λεγόμενες εκφράσεις ESOP (Exclusive or Sum Of Products), όπου μια λογική συνάρτηση εκφράζεται ως άθροισμα XOR από λογικά γινόμενα. Μια άλλη πιο γενική κατηγορία είναι οι ESCT (Exclusive or Sum of Complex Terms) εκφράσεις, οι οποίες μπορούν να θεωρηθούν ως επέκταση των ESOP, αφού πλέον οι όροι ονομάζονται σύνθετοι (complex terms) και δεν περιλαμβάνουν μόνο τη λογική πράξη ΚΑΙ ανάμεσα στις μεταβλητές, αλλά εν γένει οποιαδήποτε λογική πράξη (συνάρτηση δύο εισόδων μιας εξόδου). Η σημασία των παραπάνω εκφράσεων τονίζεται και από το γεγονός ότι μπορούν, με τετριμμένο τρόπο, να απεικονισθούν σε αντιστρέψιμες αρχιτεκτονικές. Ένα αντιστρέψιμο λογικό κύκλωμα έχει μικρότερες απώλειες ενέργειας σε σχέση με ένα τυπικό λογικό κύκλωμα και για το λόγο αυτό η σύνθεση αντιστρέψιμων κυκλωμάτων θεωρείται το μέλλον στη λογική σχεδίαση. Ένα ακόμα σημαντικό τους πλεονέκτημα είναι ότι μπορούν να χρησιμοποιηθούν και για τη σύνθεση κβαντικών κυκλωμάτων. Η ελαχιστοποίηση αυτών των εκφράσεων καθώς και οι κβαντικές επεκτάσεις τους είναι το κύριο αντικείμενο έρευνας με το οποίο ασχολείται αυτή η εργασία.

Η εργασία αυτή ασχολείται καταρχήν, με το θεωρητικό υπόβαθρο της ελαχιστοποίησης τέτοιων εκφράσεων. Αποδεικνύονται θεωρήματα τα οποία υποδεικνύ-

ουν μια μεθοδολογία για την εύρεση ελάχιστης ESCT έκφρασης για οποιαδήποτε πλήρως ορισμένη λογική συνάρτηση μοναδικής εξόδου, αλλά με περιορισμό ως προς τον αριθμό των όρων σε μια ελάχιστη έκφρασή της ή με περιορισμό ως προς τον αριθμό των μεταβλητών εισόδου της. Γίνεται, επιπλέον, μελέτη πώς τα παραπάνω συμπεράσματα μπορούν να χρησιμοποιηθούν για ευριστική ελαχιστοποίηση συναρτήσεων που δεν εμπίπτουν στους παραπάνω περιορισμούς. Στη συνέχεια τα παραπάνω πορίσματα επεκτείνονται, ευριστικά, για ατελώς ορισμένες λογικές συναρτήσεις πολλών εξόδων.

Η παραπάνω θεωρητική μελέτη του προβλήματος ελαχιστοποίησης εκφράσεων ”αποκλειστικού ή”, χρησιμοποιείται για την υλοποίηση συμβατικών και κβαντικών αλγορίθμων οι οποίοι, όπως φαίνεται και από τα πειραματικά αποτελέσματα, δίνουν καλύτερα αποτελέσματα από τους αντίστοιχους της διεθνούς βιβλιογραφίας. Πιο συγκεκριμένα, οι κβαντικοί αλγόριθμοι που μπορούν να χρησιμοποιηθούν για την ακριβή ελαχιστοποίηση εκφράσεων ”αποκλειστικού ή” και καταδεικνύουν τη σαφή υπεροχή των κβαντικών υπολογιστών έναντι των κλασικών τους αναλόγων.

Τέλος, πραγματοποιείται εφαρμογή των παραπάνω αποτελεσμάτων στο πεδίο της κρυπτογράφησης και των ασφαλών υπολογισμών. Πιο συγκεκριμένα, γίνεται χρήση των αλγορίθμων ελαχιστοποίησης εκφράσεων ESCT για την επίτευξη έως και 39% λιγότερου κόστους επικοινωνίας σε σχέση με τις υπόλοιπες αντίστοιχες προσπάθειες της βιβλιογραφίας.

Κατά τη διάρκεια της εκπόνησης της συγκεκριμένης διατριβής έχουν προκύψει οι δημοσιεύσεις που παρουσιάζονται στον κατάλογο δημοσιεύσεων που ακολουθεί:

Abstract

The current era in computer engineering, is characterized by the continuously increasing incorporation of computers and embedded systems in the all aspects of our daily life. The integrated circuits continuously shrink, become faster, require less energy with the help of new materials and architectures. As a result, the electronic appliances find more and more applications in all the aspects of our life and, as the time passes, they become an invisible and essential layer of interface with the environment.

The research object with which deals the present thesis is the minimization of logic ”eXclusive OR” or (XOR) expressions for an arbitrary logic function, and more particularly, with the reduction of number of terms that constitute this

function, as well as with the mapping of such expressions in architectures of new technologies such as quantum computers. An integrated circuit is the practical realization of such a logic expression. Accordingly, there is great effort for the optimization of logic circuits. The most popular such category of expressions is the so-called ESOP (Exclusive or Sum Of Products) expressions, where a logic function is expressed as XOR sum of products. Another more general category are the ESCT (Exclusive or Sum of Complex Terms) expressions, that can be considered as an extension of ESOPs, since the terms are now complex (complex terms) and do not include only the logic function AND between the variables, but also any logic function (of two inputs and one output). The importance of the above expressions is also stressed by the fact that they can, in a trivial manner, be mapped in reversible architectures. A reversible logic circuit has smaller losses of energy in comparison to a conventional circuit and for this reason the composition of reversible circuits is considered the future in the logic design. Another important advantage, is that they can be also used for the composition of quantum circuits. The minimization of these expressions as well as their quantum extensions are the main object of research in this thesis.

This work deals firstly, with the theoretical background of the minimization of such expressions. Theorems are proved, which indicate a methodology for finding a minimal ESCT expression for any completely specified single output logic function, with the restriction of the number of terms in its minimal expression or with the restriction of the number of its input variables. Moreover, it is studied how the above conclusions can be used for heuristic minimisation of functions that do not fall in the above restrictions. Later on, the above conclusions are extended, heuristicaly, for incompletely specified multi-output logic functions.

The above theoretical study of the problem of ”exclusive or” minimization, is used for the realization of conventional and quantum algorithms which, as it appears also from the experimental results, give better results than the corresponding of the international bibliography. More specificaly, the quantum algorithms that can be used for the exact minimization of ”exclusive or” expressions, indicate the explicit supremacy of quantum computers against the conventional ones.

Finally, we apply the above results in the field of encryption and secure computation. More specificaly, the ESCT minimization algorithms are used to achieve up to 39% less cost of communication against the related corresponding efforts of bibliography.

Κατάλογος Δημοσιεύσεων

Περιοδικά

J1. D. Voudouris, M. Sampson, G. Papakonstantinou ”Exact ESCT Minimization for functions of up to six input variables”, Elsevier Integr. VLSI J. 41, 1 (Jan. 2008), 87-105.

J2. M. Sampson, D. Voudouris, G. Papakonstantinou, ”A Quantum algorithm for finding minimal exclusive-or expressions for incompletely specified Boolean functions”, Hermis-μπ Journal, Vol. 10, 2008, pp. 6-12.

J3. M. Sampson, D. Voudouris, G. Papakonstantinou, ”Using Simple Disjoint Decomposition to Perform Secure Computations”, Journal of Circuits, Systems and Computers, World Scientific Publishing Company, Submitted.

Συνέδρια

C1. Dimitrios Voudouris, Marinos Sampson and George Papakonstantinou, ”Variable Reordering for Reversible Wave Cascades”, HERCMA 2007, Athens, 2007.

C2. M. Sampson, D. Voudouris, M. Kalathas, G. Papakonstantinou, ”A Quantum Algorithm for finding Minimum Exclusive-Or Expressions for incompletely specified Boolean Functions”, HERCMA 2007, Athens, 2007.

C3. M. Sampson, D. Voudouris, G. Papakonstantinou, ”A Quantum Algorithm for Finding Minimum Exclusive-Or Expressions”, ISVLSI, pp. 416-421, IEEE Computer Society Annual Symposium on VLSI (ISVLSI ’07), 2007.

C4. D. Voudouris, M. Sampson, G. Papakonstantinou, ”Finding minimal esct expressions for boolean functions with weight of up to 7”, in International Conference on Computer Design, CDES08, Las Vegas, 2008. CDES08, 2008.

C5. M. Sampson, D. Voudouris, G. Papakonstantinou, ”A Quantum Algorithm for Finding Minimum Exclusive-Or Expressions for Multi-Output Incompletely Specified Boolean Functions”, in International Conference on Computer Design, CDES08, Las Vegas, 2008. CDES08, 2008.

C6. M. Sampson, D. Voudouris, G. Papakonstantinou, ”Secure computations in minimal model using simple ESCT decomposition”, 16th International Conference on Software, Telecommunications and Computer Networks, SoftCOM 2008, 25-27 Sept. 2008, Page(s):380 – 383.

C7. M. Sampson, D. Voudouris, G. Papakonstantinou, ”Utilization of Variable Reordering in Quantum ESCT Minimization”, HERCMA 2009, Athens, 2009, accepted, to be presented.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1

Εισαγωγή

Η άλγεβρα του Boole αποτέλεσε και αποτελεί το θεμέλιο λίθο για την ανάπτυξη των σύγχρονων υπολογιστών. Με την ανακάλυψη του τρανζίστορ και στη συνέχεια την αλματώδη εξέλιξη στο χώρο των λογικών κυκλωμάτων υψηλής ολοκλήρωσης (VLSI - Very Large Scale Integration), η έρευνα στο χώρο των προβλημάτων της άλγεβρας του Boole γνωρίζει τρομακτική άνθηση τα τελευταία χρόνια. Παράλληλα, η σημερινή τεχνολογία σπρώχνει τα επίπεδα ολοκλήρωσης όλο και πιο μακρυά στη προσπάθεια για πιο γρήγορους και πιο μικρούς υπολογιστές. Σύντομα δεν θα υπάρχει περαιτέρω περιθώριο συρρίκνωνσης των κυκλωμάτων αφού έχουμε αγγίξει το ατομικό επίπεδο και η επιστήμη των υπολογιστών θα στραφεί σε άλλες πιο αποδοτικές τεχνολογίες όπως αυτή των κβαντικών υπολογιστών.

Ένα από τα προβλήματα με το οποίο θα ασχοληθεί η συγκεκριμένη διδακτορική διατριβή είναι η *ελαχιστοποίηση λογικών παραστάσεων*. Πιο συγκεκριμένα, γνωρίζουμε ότι η υλοποίηση κάθε λογικού κυκλώματος στηρίζεται σε μια λογική συνάρτηση Boole. Εν γένει, η συνάρτηση αυτή μπορεί να είναι πολλών μεταβλητών και πολλών εξόδων, και περιγράφει τη συμπεριφορά του κυκλώματος ανάλογα με τις διαφορετικές τιμές εισόδων που δέχεται. Κάθε τέτοια συνάρτηση μπορεί να έχει διαφορετικές εκφράσεις (δηλ τρόπους αναπαράστασης). Κάποιες από τις παραπάνω μορφές αναπαράστασης εκφράζονται ως λογικό άθροισμα όρων ”λογικού ή” ή ”αποκλειστικού ή”. Οι εκφράσεις αυτές έχουν το σημαντικό πλεονέκτημα ότι μπορούν εύκολα να απεικονισθούν σε αρχιτεκτονικές FPGA (Field Programmable Gate Array). Το πρόβλημα σε αυτές τις περιπτώσεις είναι η εύρεση των εκφράσεων με τους λιγότερους δυνατούς όρους, γιατί κάτι τέτοιο θα οδηγήσει στην κατασκευή ολοκληρωμένων κυκλωμάτων με όσο το δυνατόν μικρότερο μέγεθος.

Η έρευνα στράφηκε, αρχικά, στις εκφράσεις SOP, οι οποίες απεικονίζουν λο-

γικές συναρτήσεις ως ”λογικό άθροισμα ή” (OR) από λογικά γινόμενα (SOP - Sum of Products). Σύντομα όμως τη θέση τους πήραν οι εκφράσεις ”λογικού αθροίσματος αποκλειστικού ή” (XOR) με όρους λογικά γινόμενα (ESOP - Exclusive or Sum of Product Terms), γιατί σε σύγκριση με τις πρώτες έχουν κάποια σημαντικά πλεονεκτήματα. Το πάνω όριο στον αριθμό των λογικών γινομένων σε μια έκφραση ESOP για μια συνάρτηση n μεταβλητών είναι $29 \cdot 2^{n-7}, n > 6$ ενώ στις εκφράσεις SOP είναι: 2^{n-1} [1]. Επιπλέον είναι σημαντικά πιο αποδοτικές για συγκεκριμένες κατηγορίες εφαρμογών όπως οι τηλεπικοινωνίες [2]. Με λίγα λόγια, στις εκφράσεις ESOP, έχουμε λιγότερους όρους (στην ελάχιστη έκφραση) από ότι στις εκφράσεις SOP. Επιπλέον τα κυκλώματα που χρησιμοποιούν πύλες XOR, αποδεικνύεται, ότι ελέγχονται πολύ πιο εύκολα και απαιτούν για τον παραπάνω έλεγχο λιγότερο πλεονάζον υλικό και μικρότερες ακολουθίες ελέγχου [2]. Το ”επόμενο βήμα” στην έρευνα είναι οι εκφράσεις λογικού αθροίσματος ”αποκλειστικού ή” σύνθετων όρων(ESCT - Exclusive or Sum of Complex Terms), οι οποίες μπορούν να οδηγήσουν σε μικρότερα κυκλώματα σε σχέση με τις εκφράσεις ESOP. Ένα ακόμα μεγάλο τους πλεονέκτημα είναι ότι μπορούν να χρησιμοποιηθούν για την υλοποίηση αντιστρέψιμων (reversible) και κβαντικών κυκλωμάτων (quantum circuits). Με άλλα λόγια αναδεικνύεται η ανάγκη για μελέτη των κβαντικών επεκτάσεων αυτών των εκφράσεων. Αυτό είναι και το άλλο σκέλος της παρούσας διατριβής.

Είναι γνωστό ότι το πρόβλημα της εύρεσης ελάχιστης ESOP έκφρασης για μια τυχαία λογική συνάρτηση ανήκει στην κατηγορία των NP-hard προβλημάτων, κατά συνέπεια δεν μπορεί να επιλυθεί σε πολυωνυμικό χρόνο. Το αντίστοιχο πρόβλημα της εύρεσης ελάχιστης ESCT έκφρασης είναι, τουλάχιστον, το ίδιο δύσκολο.

Η έρευνα στο χώρο της ελαχιστοποίησης εκφράσεων ESCT δεν έχει προχωρήσει σε αντίστοιχο βαθμό με αυτήν στο χώρο των εκφράσεων ESOP, παρόλο που οι κυτταρικές δομές (και οι εκφράσεις που αντιστοιχούν σε αυτές) για την υλοποίηση λογικών εκφράσεων δεν είναι κάτι καινούργιο για την ερευνητική κοινότητα. Στη δεκαετία του 60, σημαντικό βάρος είχε δοθεί στην ανάπτυξη της σχετικής θεωρίας, όμως η τότε υπάρχουσα τεχνολογική υποδομή καθιστούσε αδύνατη την αποδοτική υλοποίηση τέτοιων διατάξεων [3]. Έτσι η έρευνα αδρανοποιήθηκε. Σήμερα όμως, που το τεχνολογικό υπόβαθρο υπάρχει, η έρευνα στο πεδίο αυτό αναθερμάνθηκε. Μεγάλη ώθηση δόθηκε και από την ραγδαία ανάπτυξη της τεχνολογίας των FPGAs και των LUT FPGAs (Look Up Table FPGAs) τα οποία ταιριάζουν τέλεια στην πρακτική υλοποίηση των παραπάνω θεωρητικών αποτελεσμάτων.

1.1 Ορισμός και σημασία του προβλήματος

Το πρόβλημα που αναλύεται στην παρούσα διατριβή είναι το ακόλουθο:

Έστω μια λογική συνάρτηση n μεταβλητών εισόδου $x_1, \ldots, x_n$. Αναζητούνται εκείνες οι εκφράσεις που έχουν μορφή:

$F = P_1 \oplus P_2 \oplus \ldots \oplus P_m$

και ο αριθμός των όρων m είναι ο ελάχιστος δυνατός. Στην έκφραση F οι όροι P_i είναι συναρτήσεις ειδικής μορφής που εξαρτώνται από τις μεταβλητές $x_1, \ldots, x_n$.

Στη παρούσα διατριβή αναπτύσσεται τόσο ο απαραίτητος θεωρητικός φορμαλισμός για την ακριβή και ευριστική ελαχιστοποίηση εκφράσεων "αποκλειστικού ή" δίνοντας ιδιαίτερο βάρος στις εκφράσεις ESCT και κατόπιν επιχειρείται η ανάπτυξη ενός υπολογιστικού και θεωρητικού πλαισίου για την αποδοτική μεταφορά των αλγορίθμων αυτών σε κβαντικά κυκλώματα. Η κύρια συμβολή είναι η ανάπτυξη κβαντικών αλγορίθμων και κυκλωμάτων για την επίλυση αυτών των ιδιαίτερα υπολογιστικά δύσκολων προβλημάτων με στόχο την σημαντική βελτίωση της υπολογιστικής πολυπλοκότητας και τον προσδιορισμό μιας γενικότερης πλατφόρμας επίλυσης προβλημάτων ελαχιστοποίησης *εκφράσεων αποκλειστικού ή*. Επιπλέον, γίνεται εφαρμογή αυτών των αλγορίθμων και εκφράσεων στο πεδίο της κρυπτογράφησης με ιδιαίτερα ικανοποιητικά αποτελέσματα.

Οι εκφράσεις ESOP και ESCT έχουν κάποια συγκριτικά πλεονεκτήματα σε σχέση με άλλες λογικές εκφράσεις. Αυτές συνοψίζονται ως:

- Οι εκφράσεις ESOP και ESCT αποτελούν κάποιες από τις γενικότερες μορφές αθροίσματος "αποκλειστικού ή" και για το λόγο αυτό μπορούν να προσφέρουν εκφράσεις με το μικρότερο δυνατό αριθμό όρων. Αναλυτικότερα οι εκφράσεις "αποκλειστικού ή" και οι σχέσεις τους εξετάζονται στην ενότητα 2.2.

- Οι εκφράσεις ESOP και ESCT μπορούν, πολύ εύκολα, να απεικονισθούν ως αντιστρέψιμα λογικά κυκλώματα. Τα πλεονεκτήματα και η αντιστοίχιση των εκφράσεων ESCT με τυπικές αντιστρέψιμες πύλες παρουσιάζονται στην ενότητα 2.3.

- Οι εκφράσεις ESOP και οι εκφράσεις ESCT μπορούν να απεικονισθούν σε σύγχρονες αρχιτεκτονικές FPGA. Μια τέτοια απεικόνιση παρουσιάζεται στην ενότητα 2.4.

Γενικά μικρότερες λογικές αναπαραστάσεις μιας λογικής συνάρτησης συνεπάγονται και μικρότερες υλοποιήσεις, κάτι που οδηγεί σε μικρότερο κόστος παραγωγής, ελαχιστοποίηση καταναλισκόμενης ενέργειας και μικρότερες θερμικές απώλειες. Αν και σήμερα ο βαθμός ολοκλήρωσης είναι τόσο μεγάλος που αρκετές λογικές μονάδες χωρούν στο ολοκληρωμένο κύκλωμα ενός μικροεπεξεργαστή, είναι σαφές ότι η αγορά θέλει να υπάρχει όλο και μεγαλύτερη υποστήριξη σε υλικό για όλο και πιο πολλά κομμάτια εφαρμογών, με αποτέλεσμα να εξακολουθεί να υπάρχει συνωστισμός. Επίσης το πρόβλημα της καταναλισκώμενης ισχύος ανα μονάδα επιφάνειας δυσκολεύει την κατάσταση ακόμα περισσότερο.

1.2 Σύνοψη συναφούς βιβλιογραφίας

Ο επιστημονικός χώρος της ελαχιστοποίησης λογικών παραστάσεων είναι ζωντανός εδώ και, περίπου, μισό αιώνα. Όσο η βιομηχανία παραγωγής ολοκληρωμένων κυκλωμάτων αναπτύσσεται, τόσο εντονότερη θα γίνεται η ανάγκη για τη βελτιστοποίηση των παραγόμενων προϊόντων της, τόσο σε επίπεδο υλικού όσο και σε επίπεδο μεθόδων σύνθεσης των ολοκληρωμένων κυκλωμάτων.

Όπως αναφέρθηκε και προηγουμένως οι εκφράσεις ”αποκλειστικού ή” είναι ιδιαίτερα σημαντικές και για το λόγο αυτό έχουν μελετηθεί σε σημαντικό βαθμό από τη διεθνή επιστημονική κοινότητα. Ανάμεσά τους οι εκφράσεις ESOP έχουν τύχει της μεγαλύτερης αναγνώρισης λόγω του συνδυασμού απλότητας και αποδοτικότητας στο μέγεθος της υλοποίησης, που προσφέρουν.

Έχουν προταθεί αλγόριθμοι για την εύρεση της ελάχιστης, ως προς τον αριθμό των όρων, ESOP έκφρασης για μια τυχαία λογική συνάρτηση αλλά με περιορισμούς ως προς τον αριθμό των μεταβλητών εισόδου ή των αριθμό των όρων στην ελάχιστη ESOP έκφρασή της. Οι αλγόριθμοι αυτοί μετασχηματίζουν το πρόβλημα της εύρεσης ελάχιστης έκφρασης ESOP σε κάποιο ισοδύναμο όπως το πρόβλημα της εύρεσης ελάχιστου μονοπατιού σε γράφο (συνάρτηση Helliwell [4, 5]) ή ορίζουν και εκμεταλλεύονται κλάσεις ισοδυναμίας δηλαδή σύνολα συναρτήσεων με τον ίδιο αριθμό όρων στην ελάχιστη ESOP έκφρασή τους [6, 1]. Το πρόβλημα στην τελευταία περίπτωση ανάγεται στον εντοπισμό της κλάσης ισοδυναμίας της συνάρτησης εισόδου. Τέλος μια άλλη προσέγγιση [7] κατασκευάζει και εντοπίζει ελάχιστες ESOP εκφράσεις για συναρτήσεις μέχρι 6 μεταβλητών εισόδου ελέγχοντας όλες τις δυνατές συναρτήσεις μικρότερου αριθμού μεταβλητών εισόδου, χρησιμοποιώντας παράλληλα κανόνες αποφυγής ορισμένων από αυτές σε περίπτωση που δεν μπορούν να βοηθήσουν στον εντοπισμό ελάχιστων ESOP εκφράσεων για τη

συνάρτηση εισόδου. Οι σημαντικότεροι ακριβείς αλγόριθμοι για ESOP εκφράσεις παρουσιάζονται στις εργασίες [8, 9, 10] και στηριζόμενοι στη μέθοδο της αποσύνθεσης μιας λογικής συνάρτησης σε απλούστερες (με μικρότερο αριθμό μεταβλητών εισόδου) μπορούν να εντοπίσουν ελάχιστες ESOP εκφράσεις για οποιαδήποτε λογική συνάρτηση, ανεξαρτήτως του αριθμού των μεταβλητών εισόδου της, αλλά με περιορισμούς στον αριθμό όρων στην ελάχιστη ESOP έκφραση της. Στις ίδιες εργασίες παρουσιάστηκαν και ευριστικές επεκτάσεις τους.

Άλλοι αλγόριθμοι ρίχνουν το βάρος τους στην ταχύτητα εύρεσης ”καλών” εκφράσεων ESOP οι οποίες θα είναι σχεδόν ελάχιστες χωρίς όμως να πιστοποιούν το βέλτιστο της παραγόμενης έκφρασής. Οι αλγόριθμοι αυτοί δεν περιορίζονται από τον αριθμό των μεταβλητών της συνάρτησης εισόδου ή τον αριθμό των όρων. Ο πιο ονομαστός είναι ο αλγόριθμος Exorcism-4 [11] ο οποίος ορίζει το μετασχηματισμό Exorlink και τον χρησιμοποιεί για το μετασχηματισμό όρων σε άλλους ισοδύναμους με σκοπό τη μετέπειτα ελαχιστοποίησή τους. Άλλοι, λιγότερο αποδοτικοί, αλγόριθμοι στην ίδια κατηγορία παρουσιάζονται στις εργασίες [12, 13, 14].

Παρόλο που το πρόβλημα της ελαχιστοποίησης εκφράσεων ESOP έχει μελετηθεί εκτενώς στο παρελθόν και έχουν προταθεί αλγόριθμοι τόσο για ακριβείς όσο και για σχεδόν ακριβείς λύσεις, εντούτοις παραμένει ακόμα ανοικτό. Στο πρόβλημα της ελαχιστοποίησης ESCT εκφράσεων υπάρχουν λίγες προσπάθειες. Οι πρώτες εργασίες στο πεδίο αυτό δημοσιεύθηκαν τη δεκαετία του 70 [15, 16, 17, 18, 19, 16] και για ένα μεγάλο διάστημα η έρευνα στο χώρο αυτό έπαψε. Τα τελευταία χρόνια, όμως, αναθερμάνθηκε το ενδιαφέρον για τις λογικές αυτές εκφράσεις και για τις εφαρμογές τους.

Επισημαίνεται ότι δεν έχει προταθεί μεθοδολογία, τουλάχιστον όσο μπορούμε να γνωρίζουμε, για την εύρεση ελάχιστης ESCT έκφρασης για τυχαία λογική συνάρτηση εκτός από αυτήν της εργασίας [19]. Οι υπόλοιποι αλγόριθμοι που προτείνονται είναι ευριστικοί και στηρίζονται, στις περισσότερες περιπτώσεις, σε τετριμμένη επέκταση των ήδη υπαρχόντων μεθοδολογιών για την ελαχιστοποίηση εκφράσεων ESOP. Σε πολλές, μάλιστα, περιπτώσεις οι εκφράσεις που παράγονται δεν είναι, ακριβώς, εκφράσεις ESCT αλλά παρεμφερείς τους.

Στις εργασίες [20, 3] χρησιμοποιούνται τεχνικές όπως η αναδιάταξη των μεταβλητών εισόδου και μετασχηματισμού κύβων. Οι τεχνικές αυτές στηρίζονται σε αντίστοιχες μεθοδολογίες από την ελαχιστοποίηση εκφράσεων ESOP και αποτελούν, συνήθως, απλοϊκές επεκτάσεις τους. Σε άλλες περιπτώσεις πολύτιμη λογική χρησιμοποιείται για να παραχθούν ”καλές” εκφράσεις [21, 22] αλλά οι εκφράσεις αυτές είναι παραλλαγές και επεκτάσεις των ESCT. Στις εργασίες [23, 24] προτείνε-

ται μια συστηματική μέθοδος για τη δημιουργία εκφράσεων ESCT επεκτείνοντας την πράξη EXORLINK. Η καινούργια αυτή πράξη ονομάζεται m-link. Μια επέκταση του παραπάνω αλγορίθμου για ατελώς ορισμένες συναρτήσεις προτείνεται στην εργασία [25] αλλά στις εκφράσεις που παράγονται οι όροι μπορούν να ενώνονται τόσο με την πράξη ”αποκλειστικό ή” όσο και με την πράξη ”λογικό ή”, κατά συνέπεια είναι παρεμφερείς των ESCT εκφράσεων. Στις εργασίες [26, 27] προτείνεται αλγόριθμος που στηρίζεται στην αποσύνθεση της συνάρτησης εισόδου σε άλλες απλούστερες και αποτελεί, στην ουσία, μια επέκταση των PSDKRO εκφράσεων που θα παρουσιαστούν στη συνέχεια. Τέλος στην εργασία [28] προτείνεται αλγόριθμος για τη δημιουργία σχεδόν ελάχιστων ESCT εκφράσεων για ατελώς ορισμένες λογικές συναρτήσεις αλλά η μεθοδολογία αυτή δεν υλοποιήθηκε και κατά συνέπεια δεν μπορεί να εξεταστεί ως προς την αποτελεσματικότητά της.

Σε ότι αφορά τις εργασίες για την ανάπτυξη κβαντικών αλγορίθμων για την ελαχιστοποίηση λογικών συναρτήσεων, διαπίστωνει κανείς ότι αυτές είναι πραγματικά ελάχιστες. Στην εργασία [29], προτείνεται ένας αλγόριθμος για την ελαχιστοποίηση FPRM (Fixed Polarity Reed Muller) εκφράσεων βασισμένος στον κβαντικό αλγόριθμο του Grover στον οποίο θα αναφερθούμε εκτενώς στα επόμενα κεφάλαια.

1.3 Συμβολή διατριβής

Είναι φανερό από τα προηγούμενα ότι υπάρχει ένα μεγάλο ”κενό” στο χώρο της ελαχιστοποίησης εκφράσεων ESCT και ακόμα μεγαλύτερο στις κβαντικές επεκτάσεις του προβλήματος. Στη διατριβή αυτή αναπτύσσεται σαφές θεωρητικό υπόβαθρο για την εύρεση ελάχιστων ESCT εκφράσεων για συναρτήσεις με περισσότερες από 5 μεταβλητές εισόδου. Επιπλέον, τα αποτελέσματα των αλγορίθμων της διεθνούς βιβλιογραφίας για την ελαχιστοποίηση εκφράσεων ESCT δεν είναι αρκετά ικανοποιητικά. Σε συνεργασία με τον Δ. Βουδούρη και σε συνέχεια της διατριβής του [30] παρουσιάζονται ακριβείς μεθοδολογίες για την εύρεση ελάχιστων ESCT εκφράσεων για συναρτήσεις με αριθμό μεταβλητών εισόδου το πολύ 6 ή με αριθμό όρων το πολύ 7 στην ελάχιστη ESCT έκφραση της συνάρτησης εισόδου. Παράλληλα, αναπτύχθηκαν και οι πρώτοι κβαντικοί αλγόριθμοι για την επίλυση των παραπάνω προβλημάτων με εντυπωσιακά μικρότερη πολυπλοκότητα. Με αυτό τον τρόπο δομήθηκε μια γενικότερη πλατφόρμα σε επίπεδο κβαντικών αλγορίθμων / κυκλωμάτων που κατέστησε δυνατή και τη μελέτη και άλλων παρεμφερών προβλημάτων όπως την ελαχιστοποίηση αντίστοιχων μη πλήρως ορισμένων ή και πολλα-

πλών εξόδων εκφράσεων ESCT και ESOP.

Το κίνητρο πίσω από αυτή τη προσπάθεια είναι η επέκταση της δουλειάς που έχει γίνει στο τομέα της ελαχιστοποίησης εκφράσεων ESOP και ESCT από τους Γ. Παπακωνσταντίνου, Σ. Στεργίου και Δ. Βουδούρη και κυρίως το πέρασμα στο επόμενο σκαλοπάτι που είναι οι κβαντικοί υπολογιστές. Αν και το πέρασμα αυτό δεν είναι εύκολο, καθώς η απαιτούμενη μεθοδολογία και ο τρόπος σκέψης είναι εντελώς διαφορετικά, η μέχρι τώρα πορεία έχει δώσει απτά και ενθαρρυντικά αποτελέσματα τα οποία αποδεικνύουν την ανωτερότητα των κβαντικών υπολογιστών έναντι των κλασικών, σε δύσκολα υπολογιστικά προβλήματα της τάξης NP (Non Polynomial time).

Δεδομένης της ισχυρής σχέσης των εκφράσεων ESCT με τις αντιστρέψιμες πύλες και τα κβαντικά κυκλώματα, έγινε μελέτη της επέκτασης ορισμένων εκ των παραπάνω θεωρητικών πορισμάτων στο χώρο των κβαντικών υπολογισμών με πολύ καλά αποτελέσματα.

Τέλος, εξετάστηκε η χρήση των ESCT εκφράσεων στο τομέα της κρυπτογράφησης με εξαιρετικά αποτελέσματα στο κόστος επικοινωνίας σε σχέση με τα αντίστοιχα αποτελέσματα της βιβλιογραφίας. Η δουλειά αυτή γενικεύτηκε ώστε να γίνει χρήση των πιο γενικών SDDs (Simple Disjoint Decompositions) προτείνοντας μια γενική πλατφόρμα κρυπτογράφησης.

Κεφάλαιο 2

Θεωρητικό Υπόβαθρο

Στο κεφάλαιο αυτό αναλύονται βασικές ιδιότητες των εκφράσεων "αποκλειστικού ή". Παρουσιάζεται η σχέση των διαφόρων εκφράσεων "αποκλειστικού ή" και αποδεικνύεται ότι οι εκφράσεις ESOP και ESCT είναι οι πιο γενικές εκφράσεις αθροίσματος XOR και κατά συνέπεια οδηγούν σε εκφράσεις με τον μικρότερο δυνατό αριθμό όρων (Ενότητα 2.2). Ένα ακόμα σημαντικό χαρακτηριστικό τους είναι η αντιστρεψιμότητα η οποία αναλύεται στην Ενότητα 2.3.

Πριν όμως από τα παραπάνω, παρουσιάζονται οι απαραίτητες βασικές έννοιες και ορισμοί ώστε ο αναγνώστης να μπορεί να προχωρήσει απρόσκοπτα στην ανάγνωση της διατριβής.

2.1 Βασικές έννοιες

2.1.1 Δυαδική Λογική (Binary Logic)

Ορισμός 1 *Έστω X δυαδική μεταβλητή με τιμές από το $V = \{0, 1\}$ και $S \subseteq V$. Τότε $X, \bar{X}, 1$ είναι literals (διπλέτες) της X.*

Ορισμός 2 *Μια λογική συνάρτηση Boole n μεταβλητών εισόδου και μιας εξόδου (single-output Switching Function ή single-output Boolean Function) είναι μια αντιστοίχιση: $f : \{0, 1\}^n \rightarrow \{0, 1\}$.*

Ορισμός 3 *Μια λογική συνάρτηση Boole n μεταβλητών εισόδου και m εξόδων (multi-output Switching Function ή multi-output Boolean Function) είναι μια αντιστοίχιση: $f : \{0, 1\}^n \rightarrow \{0, 1\}^m$. Γενικά μια τέτοια συνάρτηση μπορεί να θεωρηθεί ως m διαφορετικές συναρτήσεις n μεταβλητών και μιας εξόδου.*

Ορισμός 4 *Μια υποσυνάρτηση* f_i, $i = 0, 1, 2$ *μιας συνάρτησης* $f(x_1, x_2, \ldots, x_n)$ *ως προς τη δυαδική μεταβλητή* x_1 *ορίζεται ως:*

$f_1 = f(1, x_2, \ldots, x_n)$; $f_0 = f(0, x_2, \ldots, x_n)$; $f_2 = f_1 \oplus f_0$;

όπου το σύμβολο $\oplus$ *υποδηλώνει λογικό άθροισμα αποκλειστικού ή (XOR-sum). Στη συνέχεια (για ευκολία) θα δηλώνουμε την μεταβλητή* x_1 *(δηλαδή αυτή ως προς την οποία ισχύουν οι παραπάνω σχέσεις) ως* x.

***Παράδειγμα* 1** *Η λογική συνάρτηση:* $f(x_1, x_2, x_3) = x_1x_2x_3 \oplus \bar{x_1}\bar{x_2}\bar{x_3}$ *έχει υποσυναρτήσεις ως προς τη μεταβλητή* x_1 *τις:* $f_0 = \bar{x_2}\bar{x_3}$, $f_1 = x_2x_3$, $f_2 = x_2x_3 \oplus \bar{x_2}\bar{x_3}$.

Ορισμός 5 *Έστω μια λογική συνάρτηση* f *που εξαρτάται από* $(n+1)$ *μεταβλητές εισόδου. Υπολογίζοντας τις υποσυναρτήσεις της* f *και αναδρομικά τις υποσυναρτήσεις των υποσυναρτήσεων, δημιουργείται ένα τριαδικό δέντρο με βάθος το πολύ* n *και* 3^n *φύλλα. Το δέντρο αυτό ονομάζεται δέντρο γεννήτρια (generator tree) της συνάρτησης* f. *Η παραπάνω αναδρομή πραγματοποιείται έως ότου εντοπιστεί υποσυνάρτηση η οποία είναι σταθερά (0 ή 1) ή βρεθεί φύλλο (οι συναρτήσεις των φύλλων μπορεί να είναι μίας ή δύο μεταβλητών εισόδου).*

Μια λογική συνάρτηση μπορεί να γραφτεί με τη βοήθεια των υποσυναρτήσεών της ως:

$$\begin{aligned} f &= \bar{x}_1 f^{\{0\}} \oplus x_1 f^{\{1\}} \\ f &= f^{\{0\}} \oplus x_1 f^{\{0,1\}} \\ f &= f^{\{1\}} \oplus \bar{x}_1 f^{\{0,1\}} \end{aligned} \tag{2.1}$$

Οι τρεις παραπάνω σχέσεις ονομάζονται: Shannon (Boole), θετικό και αρνητικό Davio ανάπτυγμα (ή αποσύνθεση) αντίστοιχα, όπου x_1 είναι δυαδική μεταβλητή.

Ορισμός 6 *Έστω μια λογική συνάρτηση* $f(x_1, x_2, \ldots, x_n)$. *Έστω επίσης literal* $x_i^* = x_i, \bar{x}_i$ *της κάθε μεταβλητής* $x_i, i = 1, \ldots, n$. *Ένα λογικό γινόμενο της μορφής:* $\bigcap_{i=1}^{n}(x_i)$ *ονομάζεται ελαχιστόρος (minterm) της συνάρτησης* f ($\bigcap$ *είναι η λογική πράξη "ΚΑΙ").*

Μια τυχαία λογική συνάρτηση n μεταβλητών εισόδου έχει 2^n διαφορετικούς ελαχιστόρους και μπορεί να αναπαρίσταται ως λογικό άθροισμα ελαχιστόρων: $f = \bigcup_{j=1}^{2^n}(\bigcap_{i=1}^{n}(x_i)$ ($\bigcup$ είναι η λογική πράξη ή). Η μορφή αυτή είναι μοναδική για τη συνάρτηση f. Επίσης η παραπάνω μορφή μπορεί να εκφραστεί, ισοδύναμα, και ως άθροισμα "αποκλειστικό ή": $f = \sum_{j=1}^{2^n} \oplus (\bigcap_{i=1}^{n}(x_i)$.

Πίνακας 2.1: Πίνακας αληθείας συνάρτησης 3 μεταβλητών.

1η διάταξη μεταβλητών				**2η διάταξη μεταβλητών**			
x_3	x_2	x_1	$f(x_3, x_2, x_1)$	x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0	0	0	0	0
0	0	1	0	0	0	1	1
0	1	0	0	0	1	0	0
0	1	1	1	0	1	1	1
1	0	0	1	1	0	0	0
1	0	1	1	1	0	1	1
1	1	0	1	1	1	0	1
1	1	1	1	1	1	1	1

Ορισμός 7 *Η αναπαράσταση ελαχιστόρων (MT) μίας switching συνάρτησης n μεταβλητών f είναι ένα bit διάνυσμα μεγέθους 2^n, όπου το i-στο bit είναι 1 όταν ο i-στος ελαχιστόρος της f είναι αντίστοιχα 1.*

Στη συνέχεια όταν θέλουμε να δηλώσουμε MT αναπαράσταση μιας λογικής συνάρτησης θα την περικλείουμε σε αγκύλες και θα την δηλώνουμε χρησιμοποιώντας δεκαεξαδικά ψηφία.

Η αναπαράσταση MT εξαρτάται από τη διάταξη μεταβλητών που θα θεωρήσουμε.

***Παράδειγμα* 2** *Η λογική συνάρτηση με πίνακα αληθείας τον Πίνακα 2.1 έχει την MT αναπαράσταση: $[F8]$ όταν θεωρήσουμε ότι η μεταβλητή x_3 είναι η πιο σημαντική και η x_1 είναι η λιγότερο σημαντική. Εάν θεωρήσουμε ότι η μεταβλητή x_1 είναι η πιο σημαντική και η x_3 η λιγότερο σημαντική τότε η MT αναπαράσταση είναι: $[EA]$.*

Είναι προφανές ότι αν η MT αναπαράσταση μιας λογικής συνάρτησης f έχει $2n$ bits, τότε οι f_0, f_1 είναι τα n δεξιά και τα n αριστερά bits, αντίστοιχα, της αναπαράστασης. Η f_2 είναι το XOR των δύο MT αναπαραστάσεων των f_0 και f_1.

***Παράδειγμα* 3** *Έστω η συνάρτηση $f = [81]$. Τότε: $f_0 = [1], f_1 = [8], f_2 = [9]$.*

2.1.2 Πολύ-τιμη Λογική (Multi-valued Logic)

Η άλγεβρα Boole στηρίζεται στο δυαδικό σύστημα αρίθμησης. Κάθε μεταβλητή μπορεί να έχει δύο πιθανές τιμές (0 ή 1). Μπορούμε όμως να θεωρήσουμε μεταβλητές (πολύ-τιμες) που μπορούν να πάρουν περισσότερες τιμές (multi-valued

variables) επεκτείνοντας ουσιαστικά την άλγεβρα Boole. Η πολύτιμη λογική θα μας φανεί πολύ χρήσιμη στο πρόβλημα της ελαχιστοποίησης λογικών συναρτήσεων πολλών εξόδων.

Ορισμός 8 *Έστω X με τιμές από το $V = \{0, \ldots, v-1\}$ και $S \subseteq V$. Τότε X^S είναι literal της X ώστε $X^S = 1$ όταν $X \in S$ και $^S = 0$ όταν $X \in V \backslash S$. Στην περίπτωση που $S = V$, τότε $X^S = 1$ και μπορεί να αγνοηθεί στο λογικό γινόμενο.*

Ορισμός 9 *Έστω X^{S_1}, X^{S_2} δύο literals της πολύ-τιμης μεταβλητής . Τότε $X^{S_1} \oplus X^{S_2} \equiv X^{(S_1 \cup S_2) \backslash (S_1 \cap S_2)}$.*

Ορισμός 10 *Μια συνάρτηση μιας εξόδου που εξαρτάται, όμως, από πολύ-τιμες μεταβλητές εισόδου, είναι μια απεικόνιση της μορφής: $f : V_1 \times V_2 \times \cdots \times V_n \rightarrow \{0, 1\}$, όπου: $V_i = \{0, \ldots, v_i - 1\}$.*

Ορισμός 11 *Έστω: $V_1 = \{0, \ldots, u-1\}, V_i = \{0, 1\}, i = 2, \ldots, n, T = \{0, 1, d\}$. Μια ατελώς ορισμένη συνάρτηση πολλών εξόδων με n εισόδους και m εξόδους είναι μια απεικόνιση της μορφής: $f : V_1 X V_2 X \ldots X V_n \rightarrow T^m$. Οι ελαχιστόροι για τους οποίους $f = d$ ονομάζονται αδιάφοροι ελαχιστόροι (don't care terms) της συνάρτησης. Στις περιπτώσεις αυτές η τιμή της f είναι απροσδιόριστη. Το σύνολο των ελαχιστόρων για τους οποίους $f = 1$ αποτελούν το ON set της συνάρτησης ενώ οι υπόλοιποι αποτελούν το OFF set. Οταν $u = 2$ τότε η f είναι ατελώς ορισμένη λογική συνάρτηση n εισόδων m εξόδων που εξαρτάται από δυαδικές μεταβλητές.*

Στη συγκεκριμένη διδακτορική διατριβή μας απασχολούν απεικονίσεις της μορφής $f : \{0, 1\} X \{0, 1\} \ldots X \{0, \ldots, u-1\} \rightarrow \{0, 1, x\}$, δηλ απεικονίσεις που εξαρτώνται από μία μόνο πολύ-τιμη μεταβλητή, ενώ οι υπόλοιπες είναι δυαδικές.

Ορισμός 12 *Η αναπαράσταση ελαχιστόρων πολλαπλών μεταβλητών (MVMT) m μίας συνάρτησης $(n+1)$ μεταβλητών $f : \{0, 1\} \times \cdots \times \{0, 1\} \times \{0, \ldots, v-1\} \rightarrow \{0, 1\}$ ορίζεται ως ένα bit διάνυσμα μεγέθους $2^{n + \lceil \lg(v) \rceil}$. Έστω $x_1^{\{a_1\}} \cdots x_n^{\{a_n\}} X^S$ λογικό γινόμενο, όπου $a_i \in \{0, 1\}$ και $S \subseteq \{0, \ldots, v-1\}$. Έστω $p_1 = a_1 2^{n-1} + \ldots + a_{n-1} 2^1 + a_n 2^0$ και $p_2 = 2^{\lceil log(u) \rceil}$. Τότε O είναι ένα bit διάνυσμα με μέγεθος p_2 του οποίου το i-στο bit είναι 1 αν $i \in S$. Τότε τα bits $[(p_1 \cdot p_2 + p_2 - 1)..(p_1 \cdot p_2)]$ της MVMT m είναι ταυτόσημα με το O.*

***Παράδειγμα* 4** *Έστω μια συνάρτηση $f : \{0, 1\} X \{0, 1\} X \{0, 1\} X \{0, 1\} X \{0, \ldots, u-1\} \rightarrow \{0, 1\}$. Η αναπαράσταση MVMT της f μπορεί να θεωρηθεί ως η υπέρθεση των*

παρακάτω 5 *συναρτήσεων μοναδικής εξόδου που εξαρτώνται από δυαδικές μεταβλητές:* $f^0 = [d3d4], f^1 = [c1d5], f^2 = [d1cf], f^3 = [d5cb], f^4 = [c13b]$. *Η αναπαράσταση MVMT της* f *είναι:* $[1f1f000d0008011f0f0f10131c071c1e]$. *Πιο συγκεκριμένα, για να φανεί καλύτερα πως παράχθηκε η παραπάνω MVMT αναπαράσταση, θα αναλύσουμε την κατασκευή των τελευταίων δύο ψηφίων* $(1e)$. *Τα ψηφία αυτά δημιουργήθηκαν από τα τελευταία bits των MT αναπαραστάσεων των* $f^0, \ldots, f^4$ *(τα οποία είναι:* 11110*) αφού πρώτα συμπληρώθηκαν με μηδενικά ώστε ο αριθμός τους να φτάσει στο επιθυμητό* $2^{\lceil log(u) \rceil} = 8$ *που προβλέπει ο προηγούμενος ορισμός. Έτσι τα τελευταία ψηφία της MVMT αναπαράστασης είναι:* $00011110 = [1e]$.

Κατά αντιστοιχία με την αναπαράσταση MT οι MVMT αναπαραστάσεις των f_0, f_1 είναι τα n δεξιά και τα n αριστερά bits αντίστοιχα της αναπαράστασης MVMT (που αποτελείται από $2n$ bits), αρκεί η μεταβλητή x να είναι δυαδική. Η f_2 είναι το XOR των δύο MVMT αναπαραστάσεων.

Επειδή η έξοδος μιας απεικόνισης της μορφής: $f : \{0,1\}X\{0,1\} \ldots X\{0, \ldots, u-1\} \rightarrow \{0,1\}$ είναι δυαδική, ισχύουν και για αυτές τις απεικονίσεις όλες οι ιδιότητες και τα θεωρήματα που ισχύουν για τις λογικές συναρτήσεις που εξαρτώνται από δυαδικές μεταβλητές, αρκεί οι παραπάνω ιδιότητες να εφαρμόζονται σε δυαδικές μεταβλητές. Για παράδειγμα τα αναπτύγματα Shannon και Davio που είδαμε προηγουμένως ισχύουν και για τις προαναφερθέντες απεικονίσεις, αρκεί η μεταβλητή x να είναι δυαδική.

2.1.3 Βασικές έννοιες εκφράσεων ESOP

Οι επόμενοι ορισμοί αφορούν πολύ-τιμες μεταβλητές αλλά μπορούν εύκολα να οριστούν και για δυαδικές μεταβλητές.

Ορισμός 13 *Έστω* $X_i^{S_i}$ *literals λογικών μεταβλητών. Τότε* $C = X_1^{S_1} \cdots X_n^{S_n}$ *είναι ένα λογικό γινόμενο ή κύβος μιας λογικής συνάρτησης* f *που εξαρτάται από τις μεταβλητές* $X_1, \ldots, X_n$.

Ορισμός 14 *Ένα MVESOP ή κάλυμμα (cover) είναι μια έκφραση της μορφής:* $\bigoplus \sum C_i$, *που αναπαριστά μια λογική συνάρτηση* f, *όπου* C_i *είναι κύβοι της* f.

***Παράδειγμα* 5** $X_1^{\{0,2\}} X_2^{\{0,1\}} \oplus X_1^{\{1,2\}} X_3^{\{0\}}$ *είναι ένα MVESOP της λογικής συνάρτησης* $f : \{0, \ldots, 3\} \times \{0, \ldots, 3\} \times \{0,1\} \rightarrow \{0,1\}$.

Ορισμός 15 *Ένα ελάχιστο (ή ακριβές) MVESOP μιας λογικής συνάρτησης* f *είναι ένα κάλυμμα της συνάρτησης αυτής που αποτελείται από τον ελάχιστο αριθμό κύβων ανάμεσα σε όλα τα δυνατά MVESOPs της* f.

Μια αναπαράσταση ελαχιστόρων είναι μοναδική για μια λογική συνάρτηση. Δεν ισχύει το ίδιο και για μια αναπαράσταση MVESOP.

Ορισμός 16 *Το ESOP μέγεθος $s(e)$ ενός MVESOP e είναι ο αριθμός των κύβων του. Το ESOP βάρος $w(f)$ μιας λογικής συνάρτησης f είναι ο αριθμός των κύβων σε ένα ελάχιστο MVESOP της f.*

Ορισμός 17 *Έστω e ένα MVESOP της συνάρτησης f και $l(e)$ είναι το άθροισμα όλων των μη πλεονάζοντων literals σε όλους τους κύβους στο e. Το βάρος των literals $l(f)$ της f είναι το ελάχιστο $l(e)$ ανάμεσα σε όλα τα ελάχιστα MVESOPs e της f.*

Όταν όλες οι μεταβλητές της συνάρτησης είναι δυαδικές τότε ένα MVESOP λέγεται, απλούστερα, έκφραση ESOP.

Η εφαρμογή των αναπτυγμάτων Shannon και Davio για μια λογική συνάρτηση, που περιέχει το πολύ μία πολύ-τιμη μεταβλητή, παράγει MVESOP εκφράσεις. Άμεση συνέπεια του γεγονότος αυτού είναι ότι από την εφαρμογή των παραπάνω αναπτυγμάτων μπορεί να παραχθεί ένα άνω όριο για το ESOP βάρος μιας συνάρτησης ως $w(f) \leq MAX(w(f_0) + w(f_1), w(f_0) + w(f_2), w(f_1) + w(f_2)))$.

***Παράδειγμα* 6** *Έστω η λογική συνάρτηση $f : \{0,1\}\{0,1\}\{0,1\}\{0,1\} \rightarrow \{0,1\} = [1230]$. Οι υποσυναρτήσεις της είναι: $f_1[12], f_0 = [30], f_2 = [22]$. Ισχύει: $w(f_0) = w(f_2) = 1, w(f_1) = 2$ και μια ελάχιστη ESOP έκφραση τους είναι: $f_1 = (\bar{x_1}\bar{x_2})x_3 \oplus x_1\bar{x_2}\bar{x_3} = [10] \oplus [02], f_0 = \bar{x_2}x_3 = [30], f_2 = x_1\bar{x_2} = [22]$. Έτσι μπορούμε να παράγουμε τρεις ESOP εκφράσεις για τη συνάρτηση f χρησιμοποιώντας τα αναπτύγματα Shannon, θετικό και αρνητικό Davio $f = [((\bar{x_1}\bar{x_2})x_3 \oplus x_1\bar{x_2}\bar{x_3})x_4] \oplus [\bar{x_2}x_3\bar{x_4}], f = [x_1\bar{x_2}x_4] \oplus [\bar{x_2}x_3], f = [x_1\bar{x_2}\bar{x_4}] \oplus [(\bar{x_1}\bar{x_2})x_3 \oplus x_1\bar{x_2}\bar{x_3}]$. Προφανώς οι δύο από αυτές τις εκφράσεις αποτελούνται από 3 όρους και μία από 2 όρους. Άρα τελικά μπορούμε να βρούμε μια ESOP έκφραση με 2 όρους, οπότε το ESOP βάρος της συνάρτησης μπορεί να είναι το πολύ 2.*

Ορισμός 18 *Ένα -ισοδύναμο μιας ESOP έκφρασης για μια συνάρτηση f ορίζεται αυτό που έχει πλήθος όρων ίσο με: $k + w(f)$.*

***Παράδειγμα* 7** *Έστω μια λογική συνάρτηση $f : \{0,1\}\{0,1\}\{0,1\}\{0,1\} \rightarrow \{0,1\} = [1111]$. Η συνάρτηση αυτή έχει ESOP βάρος 1 και μια ελάχιστη ESOP έκφραση είναι: $f = \bar{x_1}\bar{x_2}$. Μια 1-ισοδύναμη της είναι: $f = (\bar{x_1}\bar{x_2})x_3 \oplus (\bar{x_1}\bar{x_2})\bar{x_3}$.*

2.1.4 Βασικές έννοιες εκφράσεων ESCT

Ορισμός 19 *Ένας σύνθετος όρος (complex term ή Maitra term) μπορεί να οριστεί αναδρομικά ως:*

- *Μία σταθερή (*0 *ή* 1*) λογική συνάρτηση είναι ένας σύνθετος όρος.*
- *Ένα literal μιας δυαδικής μεταβλητής είναι ένας σύνθετος όρος.*
- *Αν* M_i *είναι ένας σύνθετος όρος και* G *μια τυχαία λογική συνάρτηση (δύο εισόδων, μιας εξόδου), τότε:* $M_{i+1} = G(a, M_i)$ *είναι ένας σύνθετος όρος.*

Διαφορετικά ο σύνθετος όρος ορίζεται ως:
$U_i = G_{i,n}(x_n, G_{i,n-1}(x_{n-1}, G_{i,n-2}(x_{n-2}, \ldots, G_{i,1}(x_1, y)\ldots)))$,
όπου $G_{i,j}$ είναι μια οποιαδήποτε λογική συνάρτηση δύο εισόδων μιας εξόδου (ονομάζεται κύτταρο Maitra) και y σταθερή είσοδος.

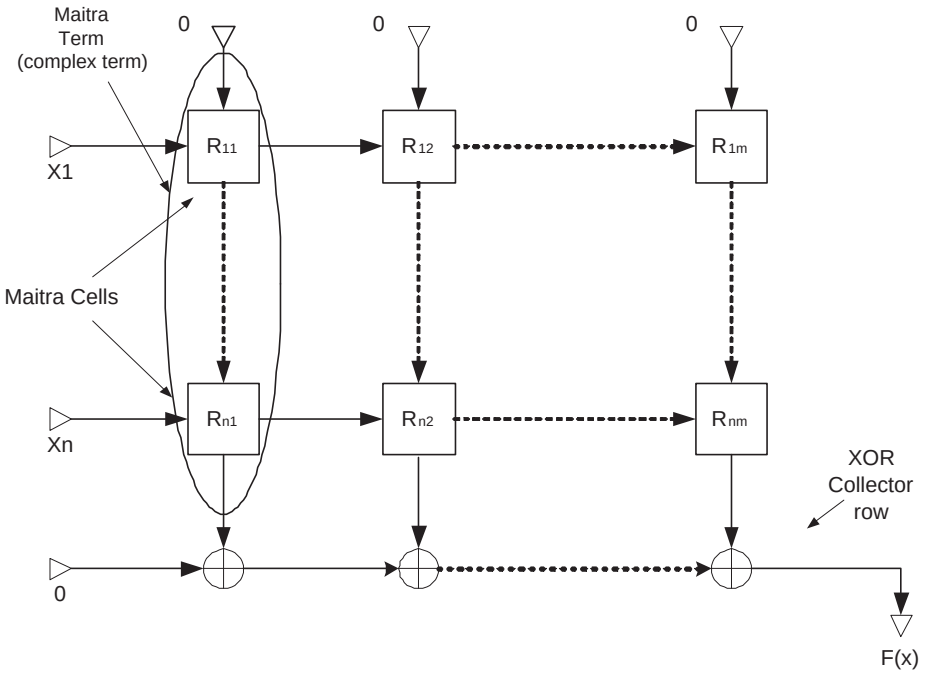
Από τον παραπάνω ορισμό είναι αυτονόητο, ότι ένας σύνθετος όρος ορίζει μια συγκεκριμένη διάταξη για τις μεταβλητές του. Δηλαδή στον παραπάνω ορισμό η μεταβλητή x_n είναι η πιο σημαντική μεταβλητή, η x_{n-1} η αμέσως πιο σημαντική κ.ο.κ. ενώ η λιγότερο σημαντική μεταβλητή είναι η x_0.

Ορισμός 20 *Ένα λογικό άθροισμα αποκλειστικού ή (XOR) από σύνθετους όρους (ή πιο απλά μια έκφραση ESCT - Exclusive or Sum of Complex Terms) μπορεί να οριστεί ως:* $Q = \sum_{i=1}^{m} \oplus M_i$*, όπου* $s(Q) = m$ *είναι ο αριθμός των όρων μέσα στην έκφραση (μέγεθος της έκφρασης). Όλοι οι όροι μέσα στην έκφραση πρέπει να έχουν την ίδια διάταξη μεταβλητών (variable ordering).*

Τις παραπάνω εκφράσεις μελέτησε πρώτος ο K. K. Maitra το 1962 (για αυτό το λόγο πολλές φορές ονομάζονται και εκφράσεις Maitra) [31]. Μια τέτοια έκφραση μπορεί πολύ εύκολα να απεικονιστεί στο υλικό με τη βοήθεια της κυτταρικής διάταξης της εικόνας 2.1 (κυτταρική διάταξη Maitra - Maitra Cellular Array).

Κάθε τέτοια διάταξη αποτελείται από μια ακολουθία κυττάρων, που κάθε ένα από αυτά έχει δύο εισόδους και μία έξοδο. Επιπλέον (στην αρχική μορφή του) κάθε ένα μπορεί να υλοποιεί οποιαδήποτε από τις δεκαέξι πιθανές συναρτήσεις δύο-εισόδων μίας-εξόδου. Συνήθως μία από τις δύο εισόδους του πρώτου κυττάρου, τροφοδοτείται με σταθερό 0 ή 1 (για συμμετρία με τα υπόλοιπα) Η υλοποιηθείσα συνάρτηση λαμβάνεται από την έξοδο του τελευταίου κυττάρου.

Κάθε σύνθετος όρος μιας έκφρασης ESCT αντιστοιχεί σε μια στήλη της παραπάνω αρχιτεκτονικής. Παρατηρούμε ότι ένας σύνθετος όρος αντιστοιχεί σε μια



Σχήμα 2.1: Κυτταρική διάταξη Maitra.

ακολουθία από κύτταρα, τα οποία υλοποιούν την πράξη G στον αντίστοιχο ορισμό. Για το λόγο αυτό πολλές φορές ο σύνθετος όρος ταυτίζεται με το ισοδύναμό του, την αλυσίδα Maitra (Maitra cascade), στο επίπεδο υλοποίησης. Το πρώτο κύτταρο Maitra θεωρείται εκείνο που έχει τη μία είσοδο σταθερή και ίση με 0 (λιγότερο σημαντική μεταβλητή), ενώ τελευταίο εκείνο που βρίσκεται πλησιέστερα στο συλλέκτη XOR (πιο σημαντική μεταβλητή).

Αποδεικνύεται [15] πως τα παραπάνω κύτταρα δεν είναι απαραίτητο να υλοποιούν οποιαδήποτε λογική συνάρτηση δύο μεταβλητών. Ένα σύνολο από μόνο 6 λογικές συναρτήσεις είναι πλήρες. Οι αλυσίδες Maitra τα οποία χρησιμοποιούν κύτταρα που υλοποιούν συναρτήσεις από ένα τέτοιο σύνολο, ονομάζονται περιορισμένες αλυσίδες Maitra (Restricted Maitra Cascades) και γενικά οδηγούν σε μικρότερες υλοποιήσεις, αφού απαιτούνται μόνο 3 bits ανά κύτταρο για την περιγραφή τους, σε αντίθεση με τα 4 bits που απαιτούνται αν το κάθε κύτταρο πρέπει να υλοποιεί και τις 16 πιθανές συναρτήσεις δύο μεταβλητών εισόδου, μιας εξόδου. Στη συνέχεια όταν αναφερόμαστε σε αλυσίδες Maitra (ή σύνθετους όρους) θα εννοούμε περιορισμένες αλυσίδες Maitra (και κατά συνέπεια οι σύνθετοι όροι που θα χρησιμοποιούνται από το σημείο αυτό και έπειτα θα χρησιμοποιούν συναρτήσεις G από το περιορισμένο σετ). Υπάρχουν πολλά τέτοια πιθανά σύνολα λογικών συναρτήσεων και ένα τυπικό φαίνεται στον πίνακα 2.2.

Πίνακας 2.2: Τυπικό σετ συναρτήσεων κυττάρου Maitra.

Κύτταρο	Λογική Συνάρτηση
1	$x + y$
2	$\bar{x} + y$
3	$\bar{x}y$
4	xy
5	$x \oplus y$
6	y

Από τους προηγούμενους ορισμούς είναι προφανές ότι οι εκφράσεις ESCT είναι γενικότερες των εκφράσεων ESOP. Συγκεκριμένα μια έκφραση ESOP είναι μια έκφραση ESCT όταν δεν επιτρέπεται μέσα στους σύνθετους όρους να χρησιμοποιούνται οι πράξεις "λογικό ή" (OR) και "λογικό αποκλειστικό ή" (XOR). Οι εκφράσεις ESOP, λοιπόν, είναι υποσύνολο των εκφράσεων ESCT.

Κατά αντιστοιχία με την ελάχιστη ESOP έκφραση και το ESOP βάρος μπορούν να οριστούν η ελάχιστη ESCT έκφραση και το ESOP βάρος.

Ορισμός 21 *Ελάχιστη (ή ακριβής) (minimal ή exact) ESCT έκφραση μιας λογικής συνάρτησης f είναι η έκφραση η οποία περιέχει τον ελάχιστο αριθμό σύνθετων όρων σε σχέση με οποιαδήποτε άλλη ESCT έκφραση για τη συγκεκριμένη συνάρτηση.*

Ορισμός 22 *Το ESCT βάρος (ή απλά βάρος) μιας λογικής συνάρτησης ορίζεται ως ο αριθμός των σύνθετων όρων σε μια ελάχιστη ESCT έκφραση της συνάρτησης.*

Πρέπει να τονιστεί ότι το ESCT βάρος εξαρτάται από τη διάταξη των μεταβλητών (πόσο σημαντική είναι η κάθε μεταβλητή) που χρησιμοποιούμε, ενώ αυτό δεν συμβαίνει στις εκφράσεις ESOP.

***Παράδειγμα* 8** *Έστω η λογική συνάρτηση: $f = (x_1 \oplus x_2)x_3x_4$ (η διάταξη των μεταβλητών είναι: $x_4 \supset x_3 \supset x_2 \supset x_1$). Είναι προφανές ότι η συνάρτηση αυτή έχει ESCT βάρος 1. Αν θεωρήσουμε την επόμενη διάταξη μεταβλητών $x_4 \supset x_1 \supset x_2 \supset x_3$ τότε παίρνουμε: $f = x_3x_2x_4 \oplus x_3x_1x_4$ και έχει βάρος 2.*

***Παράδειγμα* 9** *Μια συνάρτηση ονομάζεται "υλοποιήσιμη ως ένας όρος" (cascade realizable) όταν έχει βάρος 1.*

Έχει αποδειχτεί [15] ότι μια συνάρτηση 2 μεταβλητών έχει πάντα βάρος 1.

Ορισμός 23 *Ορισμός 13 . Ένα -wισοδύναμο (k-wequivalent) μιας ESCT έκφρασης για μια συνάρτηση f ορίζεται αυτό που έχει πλήθος όρων ίσο με: $k + w(f)$.*

Ένας σύνθετος όρος μπορεί να αναπαρασταθεί από την ακολουθία των συναρτήσεων G ή διαφορετικά από τα Maitra cells που χρησιμοποιεί. Δηλαδή (θεωρώντας ότι μιλάμε για restricted maitra cascades) μπορεί να αναπαρασταθεί από την ακολουθία των δεικτών του Πίνακα 2.2 που υποδηλώνει τις αντίστοιχες πράξεις (θεωρούμε ότι για την πρώτη πράξη η αρχική είσοδος είναι 0). Αυτή η αναπαράσταση θα χρησιμοποιηθεί στη συνέχεια της συγκεκριμένης εργασίας (cell representation). Για να δηλώνουμε τη συγκεκριμένη αναπαράσταση θα την περικλείουμε σε παρενθέσεις.

***Παράδειγμα* 10** *Ο σύνθετος όρος: $P = (x_1 + x_2)\bar{x_3} \oplus x_4$ αναπαρίσταται ως: (1135) (βλέπε Πίνακα 2.2).*

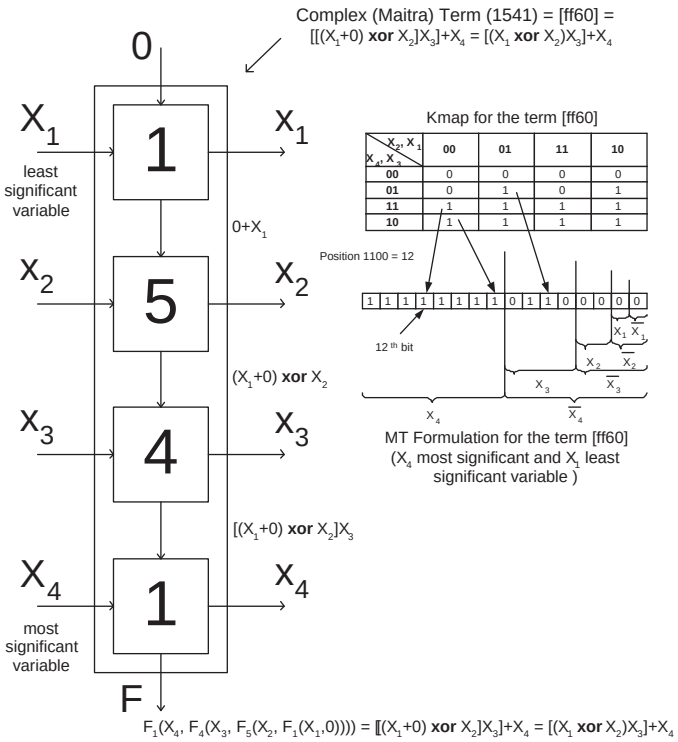
***Παράδειγμα* 11** *Έστω η συνάρτηση: $f = (x1 \oplus x2)x3 + x4 = [FF60]$. Η συνάρτηση αυτή μπορεί να αναπαρασταθεί (θεωρώντας ως διάταξη μεταβλητών την: x_4, x_3, x_2, x_1 με την κάθε μεταβλητή να είναι πιο σημαντική από αυτές που βρίσκονται δεξιά της) ως ένας μόνο σύνθετος όρος: $F_1(x_4, F_5(x_3, F_4(x_2, F_1(x_1, 0)))) = (x4 + (x3(x2 \oplus (x1 + 0))))$. Χρησιμοποιώντας την αναπαράσταση cell ο σύνθετος όρος γράφεται: (1541). Η αντιστοιχία όλων των αναπαραστάσεων του παραπάνω σύνθετου όρου, καθώς και ο πίνακας Karnaugh του παρουσιάζονται στην Εικόνα 2.2.*

Ορισμός 24 *"Επίπεδο σταθερής εισόδου" (Constant Input Level) ή σύντομα CIL(c) ενός σύνθετου όρου c είναι ο αριθμός των Maitra cells στον όρο που έχουν μία από τις εισόδους τους σταθερό 0.*

Με άλλα λόγια το CIL είναι ο αριθμός των Maitra cells του σύνθετου όρου τύπου 6, στην αρχή του όρου (Πίνακας 2.2).

***Παράδειγμα* 12** *Ισχύει: $CIL(66612) = 3$.*

Ένας σύνθετος όρος αφορά συναρτήσεις που εξαρτώνται από δυαδικές μεταβλητές εισόδου. Μπορούμε, κατά αντιστοιχία, να ορίσουμε το ισοδύναμό του για λογικές συναρτήσεις που έχουν μια μεταβλητή πολύ-τιμη.



Σχήμα 2.2: Πίνακας Karnaough και μετατροπή σε αναπαράσταση cell της συνάρτησης $[ff60]$.

Ορισμός 25 *Έστω x_i δυαδικές μεταβλητές και y πολύ-τιμη σταθερά που παίρνει τιμές από το σύνολο: $\{0,\ldots,u-1\}$, $G_i : \{0,1\}X\{0,1\} \rightarrow \{0,1\}, 2 \leq i \leq n$ είναι μια τυχαία λογική συνάρτηση και G_1 είναι μια απεικόνιση της μορφής: $\{0,1\}X\{0,\ldots,u-1\} \rightarrow \{0,1\}$. Τότε η απεικόνιση:*
$U_i = G_n(x_n, G_{n-1}(x_{n-1}, G_{n-2}(x_{n-2},\ldots,G_1(x_1,y)\ldots)))$ είναι ένας mv όρος (mv-term).

Κατά αντιστοιχία με τον ορισμό του σύνθετου όρου, οι συναρτήσεις G_i ($2 \leq i \leq n$) του mv όρου προέρχονται από τον Πίνακα 2.2. Η απεικόνιση G_1 ορίζεται κατά αντιστοιχία με τις συναρτήσεις του Πίνακα 2.2 και η MVMT αναπαράσταση της είναι η υπέρθεση των αναπαραστάσεων MT κάθε συνάρτησης που παράγεται όταν θέσουμε ως είσοδο κάθε bit της πολύ-τιμης σταθεράς y στη συνάρτηση G_1.

***Παράδειγμα* 13** *Έστω ένας mv όρος με πολύ-τιμη σταθερά $y = (3)$ και $G_1(x,y) = 4$ (σύμφωνα με τον Πίνακα 2.2 είναι η συνάρτηση xy). Τότε για κάθε bit της $y = 0011$ κατασκευάζουμε την MT αναπαράσταση της συνάρτησης xy (Maitra cell function 4). Αυτό σημαίνει: $F_4(x,0) = [00]$ (αριστερότερο bit), $F_4(x,0) = [00]$, $F_4(x,1) = [10]$, $F_4(x,1) = [10]$ (δεξιότερο bit) (χρησιμοποιούμε δυαδική αναπαράσταση στην MT για καλύτερη κατανόηση). Κατά συνέπεια και σύμφωνα με τον ορισμό της MVMT αναπαράστασης ο mv όρος είναι: $[00110000]$ ή στη συνήθη δεκαεξαδική μορφή: $[30]$.*

Ένας mv όρος μπορεί να αναπαρασταθεί είτε με την MVMT αναπαράστασή του είτε ως ένας σύνθετος όρος (μια σειρά από Maitra cells που την ονομάζουμε 2v-term) μαζί με μια πολύ-τιμη σταθερά (y) που την ονομάζουμε mv-var. Η αναπαράσταση αυτή (cell representation) είναι ίδια με αυτή του σύνθετου όρου με τη διαφορά ότι εδώ έχουμε και την mv-var να περικλείεται από άγκιστρα.

***Παράδειγμα* 14** *Ο mv όρος $(\{3\}434) = yx_1\bar{x_2}x_r$, όπου y είναι πολύ-τιμη σταθερά και x_1, x_2, x_3 είναι δυαδικές μεταβλητές έχει 2v-term: (434) και mv-var: 3. Η MVMT αναπαράστασή του είναι: $[0030000]$.*

Σημειώνεται ότι η συμπεριφορά και οι ιδιότητες ενός mv όρου είναι ίδιες με εκείνες ενός σύνθετου όρου, αρκεί αυτές να αφορούν δυαδική μεταβλητή του.

Όπως αναφέρθηκε ήδη, η εφαρμογή των αναπτυγμάτων Shannon και Davio για μια λογική συνάρτηση παράγει ESOP εκφράσεις. Δεδομένου ότι οι εκφράσεις ESOP είναι υποσύνολο των εκφράσεων ESCT, τα παραπάνω δημιουργούν και εκφράσεις ESCT. Άμεση συνέπεια του γεγονότος αυτού είναι ότι από την εφαρμογή

των παραπάνω αναπτυγμάτων μπορεί να παραχθεί ένα άνω όριο για το ESCT βάρος μιας συνάρτησης ως $w(f) \leq MAX(w(f_0) + w(f_1), w(f_0) + w(f_2), w(f_1) + w(f_2)))$.

2.1.5 Συγγενείς Όροι

Δύο σύνθετοι όροι μπορεί να "μοιάζουν" μεταξύ τους. Ο βαθμός ομοιότητας τους αποτυπώνεται στη θεωρία των Συγγενών Όρων.

Ορισμός 26 *Τα κύτταρα Maitra του Πίνακα 2.2 μπορούν να χωριστούν σε τρία σύνολα (κλάσεις κυττάρων Maitra) ανάλογα με την ομοιότητά τους. Η πρώτη κλάση περιέχει τα κύτταρα με δείκτες* 1 *και* 3*. Η δεύτερη περιέχει τα κύτταρα με δείκτες* 2 *και* 4*. Η τρίτη περιέχει τα κύτταρα με δείκτες* 5 *και* 6*. Συγκεκριμένα για τα κύτταρα που η μία από τις εισόδους τους είναι βραχυκυκλωμένη σε σταθερή είσοδο (εδώ έχουμε κάνει την παραδοχή ότι η είσοδος αυτή είναι μηδέν), οι κλάσεις είναι μόνο* 2*. Η πρώτη αποτελείται από cells τύπου* $(1, 2)$ *και η δεύτερη από το cell τύπου* 6*.*

Η ομοιότητα αυτή θα φανεί στο Λήμμα 2, καλύτερα.

Ορισμός 27 *Το "αντιπροσωπευτικό Maitra cell" (Representative Maitra cell) για την κλάση Maitra cell (1,3) είναι το 3. Το "αντιπροσωπευτικό Maitra cell" για την κλάση Maitra cell (2,4) είναι το 4. Το "αντιπροσωπευτικό Maitra cell" για την κλάση Maitra cell (5,6) είναι το 6. Συγκεκριμένα για τα Maitra cells που έχουν τη μία είσοδό τους βραχυκυκλωμένη στο σταθερό 0, τότε για την κλάση (1,2) ο αντιπρόσωπος είναι το 1 και για την (6) είναι προφανώς το 6.*

Ορισμός 28 *Ένας γεννήτωρ σύνθετος όρος (generator complex term) αποτελείται μόνο από αντιπροσωπευτικά Maitra cells.*

Ορισμός 29 *Δύο σύνθετοι όροι (με τον ίδιο αριθμό Maitra cells) έχουν τον ίδιο γεννήτορα σύνθετο όρο αν τα αντίστοιχα Maitra cells τους ανήκουν στην ίδια κλάση. Αυτοί οι δύο σύνθετοι όροι ονομάζονται "συγγενείς".*

Ορισμός 30 *Δύο ESCT εκφράσεις ανήκουν στην ίδια γεννήτρια κλάση εάν για κάθε σύνθετο όρο στην πρώτη έκφραση υπάρχει ένας σύνθετος όρος στη δεύτερη, που είναι συγγενής με τον πρώτο.*

***Παράδειγμα* 15** *Οι σύνθετοι όροι* (1234) *και* (1414) *είναι συγγενείς αφού όλα τα Maitra cells τους ανήκουν στην ίδια κλάση. Ο γεννήτωρ σύνθετος όρος τους είναι ο*

(1434). *Οι επόμενες δύο ESCT εκφράσεις:* $Q = (1234) + (6215)$ *και* $R = (1414) + (6116)$ *ανήκουν στην ίδια γεννήτρια κλάση αφού οι όροι* (1234) *και* (1414) *είναι συγγενείς και επιπλέον οι όροι* (6215) *και* (6116) *είναι συγγενείς.*

Οι δύο τελευταίοι ορισμοί δημιουργούν κλάσεις από σύνθετους όρους και ESCT εκφράσεις.

Ορισμός 31 *(m-Ισοδύναμη έκφραση - m-equivalent expression) Δύο ESCT εκφράσεις είναι m-ισοδύναμες αν ανήκουν στην ίδια γεννήτρια κλάση και απεικονίζουν την ίδια λογική συνάρτηση* f.

***Παράδειγμα* 16** *Έστω μια ESCT έκφραση* $Q = (1234) \oplus (1414)$ *της συνάρτησης* $f = [f300]$. *Η ESCT έκφραση* $K = (2412) \oplus (2232)$ *είναι m-ισοδύναμη της Q αφού οι δύο αυτές εκφράσεις απεικονίζουν την ίδια συνάρτηση και οι όροι* $(1234), (2412)$ *και* $(1414), (2232)$ *είναι ανά δύο συγγενείς.*

2.2 Κλάσεις εκφράσεων αποκλειστικού ή

Μια τυχαία λογική συνάρτηση μπορεί να εκφραστεί με τη βοήθεια του τελεστή "αποκλειστικό ή". Οι εκφράσεις που μας απασχολούν στη συγκεκριμένη διδακτορική διατριβή (ESOP και ESCT), ανήκουν στην κατηγορία των διεπίπεδων εκφράσεων με συλλέκτη "αποκλειστικό ή" (XOR). Είναι γνωστό [2] ότι οι εκφράσεις ESOP είναι οι πιο γενικές εκφράσεις της παραπάνω κατηγορίας αν ο μόνος τελεστής που χρησιμοποιείται εκτός του συλλέκτη XOR είναι η λογική πράξη ΚΑΙ. Όπως θα φανεί σε επόμενα κεφάλαια, οι εκφράσεις ESCT είναι ακόμα πιο γενικές από τις εκφράσεις ESOP (αν και πολλές φορές δεν θεωρούνται διεπίπεδες). Κρίνεται λοιπόν σκόπιμο να γίνει μια σύντομη αναφορά στα είδη των διεπίπεδων εκφράσεων με συλλέκτη "αποκλειστικό ή" ώστε να τονιστεί ακόμα περισσότερο η σημασία των εκφράσεων ESOP και ESCT για την υλοποίηση λογικών συναρτήσεων.

Έστω μια λογική συνάρτηση f με n μεταβλητές εισόδου. Η συνάρτηση αυτή μπορεί να γραφτεί χρησιμοποιώντας τα αναπτύγματα Shannon, θετικό και αρνητικό Davio (όπως θα φανεί αργότερα).

2.2.1 Positive Polarity Reed-Muller Expressions (PPRM)

Χρησιμοποιώντας το ανάπτυγμα θετικό Davio για να εκφράσουμε τη συνάρτηση f, συναρτήσει της πρώτης της μεταβλητής, θα δημιουργηθεί μια έκφραση XOR.

Αν εκτελέσουμε την ίδια διαδικασία, αναδρομικά, και για τις συναρτήσεις στο δέντρο γεννήτρια της f, τότε θα προκύψει μια έκφραση XOR η οποία θα έχει όλα τα literals των μεταβλητών στη θετική μορφή τους (δεν θα υπάρχει $x_i, i = 1, \ldots, n$). Η έκφραση που θα προκύψει ονομάζεται Positive Polarity Reed-Muller Expression (PPRM για συντομία).

Μια έκφραση PPRM είναι μοναδική για μια συγκεκριμένη λογική συνάρτηση. Ο μέσος όρος από λογικούς όρους σε μια τέτοια έκφραση είναι 2^{n-1}.

***Παράδειγμα* 17** *Η επόμενη έκφραση:* $f = 1 \oplus x_1 \oplus x_2 \oplus x_1x_2$ *είναι PPRM.*

2.2.2 Fixed Polarity Reed-Muller Expressions (FPRM)

Αντίστοιχη με την PPRM είναι η έκφραση Fixed Polarity Reed-Muller (FPRM για συντομία), με τη διαφορά ότι για κάθε μεταβλητή της παραπάνω αναδρομικής διαδικασίας, μπορούμε να επιλέξουμε τη χρήση είτε του θετικού είτε του αρνητικού Davio αναπτύγματος. Στην έκφραση FPRM κάθε μεταβλητή μπορεί να βρίσκεται είτε στην κανονική (x) είτε στην συμπληρωματική της μορφή ($\bar{x}$), αλλά δεν μπορεί να βρίσκεται ταυτόχρονα και στις δύο.

Για μια τυχαία συνάρτηση n μεταβλητών μπορούν να υπάρχουν 2^n διαφορετικές εκφράσεις FPRM.

***Παράδειγμα* 18** *Η επόμενη έκφραση:* $f = x_1x_2 \oplus \bar{x_3}\bar{x_4}$ *είναι FPRM.*

2.2.3 Kronecker Expressions (KRO)

Αντίστοιχη με την FPRM είναι η έκφραση Kronecker, με τη διαφορά ότι για κάθε μεταβλητή της παραπάνω αναδρομής διαδικασίας, μπορούμε να επιλέξουμε είτε τη χρήση του αναπτύγματος Shannon είτε κάποιο από τα αναπτύγματα Davio.

Για μια τυχαία συνάρτηση n μεταβλητών μπορούν να υπάρχουν 3^n διαφορετικές εκφράσεις Kronecker.

***Παράδειγμα* 19** *Η επόμενη έκφραση:* $f = x_1x_2x_3 \oplus \bar{x_1}\bar{x_2}\bar{x_3}$ *είναι Kronecker.*

2.2.4 Pseudo Reed-Muller Expressions (PSDRM)

Αν εκφράσουμε την αρχική μας συνάρτηση f χρησιμοποιώντας τα αναπτύγματα Davio τότε δημιουργείται μια έκφραση XOR. Αν εκτελέσουμε την ίδια διαδικασία,

αναδρομικά στο δέντρο γεννήτρια, αλλά χρησιμοποιώντας, ενδεχομένως, διαφορετική σχέση για την κάθε συνάρτηση, τότε θα προκύψει μια έκφραση XOR η οποία ονομάζεται Pseudo Reed-Muller Expression (PSDRM για συντομία).

Για μια συγκεκριμένη διάταξη μεταβλητών μιας λογικής συνάρτηση n μεταβλητών μπορούν να υπάρχουν 2^{2^n-1} διαφορετικές εκφράσεις PSDRM.

***Παράδειγμα* 20** *Η επόμενη έκφραση:* $f = \bar{x_2}\bar{x_3}\bar{x_4} \oplus x_1\bar{x_3}\bar{x_4} \oplus x_1\bar{x_2}barx_4 \oplus x_1x_2\bar{x_3}$ *είναι PSDRM.*

2.2.5 Pseudo Kronecker Expressions (PSDKRO)

Αντίστοιχη με την PSDRM είναι η έκφραση Pseudo Kronecker (PSDKRO για συντομία), με τη διαφορά ότι σε κάθε στάδιο της αναδρομής μπορούμε να επιλέξουμε οποιοδήποτε από τα αναπτύγματα Shannon και Davio.

Για μια συγκεκριμένη διάταξη μεταβλητών μιας λογικής συνάρτηση n μεταβλητών μπορούν να υπάρχουν 3^{2^n-1} διαφορετικές εκφράσεις PSDKRO.

2.2.6 Generalized Reed-Muller Expressions (GRM)

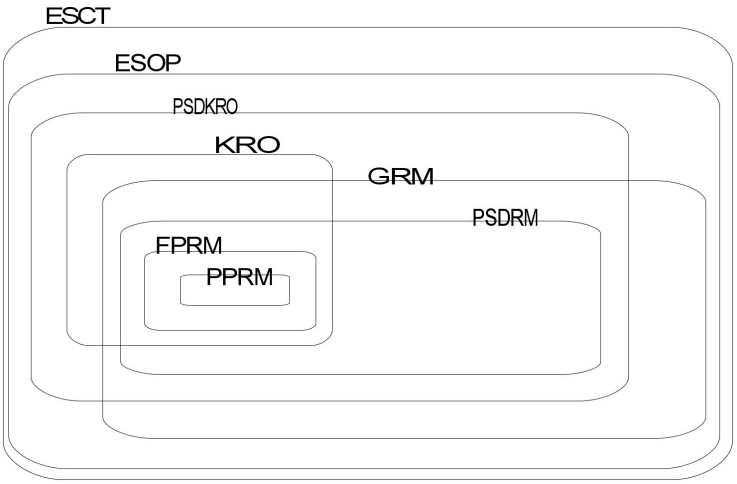
Έστω μια έκφραση PPRM για τη λογική συνάρτηση f. Αν αντιστρέψουμε την πολικότητα κάθε literal των μεταβλητών εισόδου της f τυχαία, τότε η παραγόμενη έκφραση ονομάζεται Generalized Reed-Muller (GRM για συντομία).

Για μια λογική συνάρτηση n μεταβλητών μπορούν να υπάρχουν $2^{n2^{n-1}}$ διαφορετικές εκφράσεις GRM.

***Παράδειγμα* 21** *Η επόμενη έκφραση:* $f = x_1 \oplus x_2 \oplus \bar{x_1}\bar{x_2}$ *είναι GRM.*

Οι παραπάνω εκφράσεις δεν είναι ισοδύναμες. Κάποιες από αυτές είναι υποκατηγορίες κάποιων άλλων. Εκτός από τις παραπάνω εκφράσεις υπάρχουν και οι εκφράσεις ESOP και ESCT που είναι πιο γενικές. Οι σχέσεις μεταξύ των εκφράσεων φαίνονται στην εικόνα 2.3.

Οι εκφράσεις ESCT και ESOP, όπως φαίνεται και από την παραπάνω εικόνα, είναι πιο γενικές από τις υπόλοιπες εκφράσεις XOR. Επιπλέον απαιτούν, κατά μέσο όρο, και μικρότερο αριθμό όρων για να απεικονίσουν μια τυχαία συνάρτηση.



Σχήμα 2.3: Σχέση μεταξύ των διαφορετικών κλάσεων εκφράσεων XOR.

2.3 Αντιστρέψιμες Λογικές Πύλες

Η επιστήμη της σύνθεσης λογικών κυκλωμάτων βασισμένων σε αντιστρέψιμες πύλες (reversible logic gates) έχει βασιστεί στην αρχή των von Neumann-Landauer (NVL) [32] η οποία υποστηρίζει ότι οι κοινές μη αντιστρέψιμες λογικές πύλες, μοιραία, χάνουν ενέργεια απλά και μόνο επειδή κάποιες από τις δυνατές καταστάσεις εξόδου εξαφανίζονται. Χονδρικά η ενέργεια που χάνεται για κάθε έξοδο αντιστοιχεί στην ενέργεια του σήματος και οφείλεται στο λεγόμενο θερμικό θόρυβο (thermal noice). Η παραπάνω απώλεια ενέργειας αντιστοιχεί τόσο στην απώλεια πληροφορίας όσο και στην απώλεια λόγω τεχνολογικών παραγόντων (ατέλειες κατασκευής λογικών πυλών κτλ). Για κάθε bit πληροφορίας που χάνεται λόγω της μη αντιστρεψιμότητας παράγεται $KTln2$ joules ενέργειας που διαχέεται στο περιβάλλον (K είναι η σταθερά του Boltzmann και T είναι η θερμοκρασία λειτουργίας). Αντίθετα, λογικά κυκλώματα που συντίθενται από αντιστρέψιμες λογικές πύλες μπορούν να ξαναχρησιμοποιήσουν ένα κλάσμα της ενέργειας που χάνεται από το θερμικό θόρυβο και οφείλεται στην απώλεια της πληροφορίας. Μάλιστα, θεωρητικά, το κλάσμα αυτό μπορεί να φτάσει το 100%. Η άλλη παράμετρος απώλειας ενέργειας που οφείλεται σε τεχνολογικούς παράγοντες (κατασκευαστικές ατέλειες) αναμένεται να μειώνεται όσο η τεχνολογία βελτιώνεται. Παρόλα αυτά, τουλάχιστον μέχρι τώρα, η δεύτερη παράμετρος απώλειας ενέργειας είναι σημαντικά μεγαλύτερη από την πρώτη (τουλάχιστον στις επικρατέστερες τεχνολογίες παρασκευής ολοκληρωμένων κυκλωμάτων όπως στα κυκλώματα CMOS - Complementary Metal-Oxide Semiconductor). Κατά συνέπεια η σύνθεση κυκλωμάτων χρησιμοποιώντας αντιστρέψιμες πύλες δεν προσφέρει κάποιο ουσιαστικό πλεονέκτημα προς το παρόν.

Είναι προφανές από τα παραπάνω ότι οι αντιστρέψιμες λογικές πύλες θα γίνονται όλο και πιο ελκυστικές για τη σύνθεση λογικών κυκλωμάτων λόγω της έμφυτης αυτής ιδιότητάς τους να μην χάνουν ενέργεια λόγω απώλειας πληροφορίας. Η σύνθεση δηλαδή αντιστρέψιμων κυκλωμάτων θα βοηθήσει στην περαιτέρω μείωση των απωλειών ενέργειας. Όπως επίσης θα φανεί στο κεφάλαιο για τους κβαντικούς αλγορίθμους, όλες οι κβαντικές πύλες είναι αντιστρέψιμες και όλες οι αντιστρέψιμες πύλες μπορούν να αποτελέσουν κβαντικούς τελεστές. Οποιαδήποτε, λοιπόν, μέθοδος σύνθεσης κυκλωμάτων που στηρίζεται σε αντιστρέψιμες πύλες, εκτός της μειωμένης κατανάλωσης σε ενέργεια, προσφέρει και τη (θεωρητική) δυνατότητα της απευθείας σύνθεσης και του αντίστοιχου κβαντικού κυκλώματος.

Οι περισσότερες από τις κλασικές λογικές πύλες που χρησιμοποιούνται για τη σύνθεση λογικών συναρτήσεων είναι μη αντιστρέψιμες (irreversible logic gates).

Πίνακας 2.3: Τυπικές αντιστρέψιμες λογικές πύλες.

Πύλη	**Είσοδοι/Έξοδοι**	**Μαθηματική περιγραφή**
Μιας εισόδου μιας εξόδου.		
Ταυτότητας(Identity)	a/b	$b = a$
Αντιστροφής(NOT)	a/b	$b = \bar{a}$
Δύο εισόδων δύο εξόδων.		
Αποκλειστικό ή(XOR - CNOT)	$a, b/c, d$	$c = a, d = a \oplus b$
Feynman	$a, b/c, d$	$c = a, d = a + b$
Τριών εισόδων τριών εξόδων.		
Fredkin(Controlled swap)	$a, b, c/d, e, f$	Αν $c = 0 \Rightarrow d = a, e = b, f = c$, Αν $c = 1$: $d = b, e = a, f = c$
Fredkin(Controlled swap)	a,b,c/d,e,f	Αν $c = 0 \Rightarrow d = a, e = b, f = c$ Αν c=1: d=b, e=a, f=c
Toffoli(CC-NOT)	a,b,c/d,e,f	$d = a, e = b,$ Αν $a, b \neq 1 \Rightarrow f = c.$ Αν $a = b = 1 \Rightarrow f =!c.$ Εναλλακτικά: $d = a, e = b, f = c \oplus ab$

Τέτοιες πύλες είναι οι γνωστές μας "λογικό και" (AND) και "λογικό ή" (OR). Παρόλα αυτά υπάρχουν και λογικές πύλες που είναι αντιστρέψιμες, όπως η πύλη "λογικό αποκλειστικό ή" (XOR), όταν επεκταθεί να έχει δύο εισόδου και δύο εξόδους. Μια λογική πύλη λέγεται αντιστρέψιμη όταν αντιστοιχεί με μοναδικό τρόπο κάθε διάνυσμα εισόδου σε ένα και μοναδικό διάνυσμα εξόδου και αντίστροφα (1 - 1 απεικόνιση). Το παραπάνω γεγονός υπονοεί, επίσης, ότι οι αντιστρέψιμες πύλες έχουν τον ίδιο αριθμό εισόδων και εξόδων. Ισχύει ακόμα ότι ένα λογικό κύκλωμα που συντίθεται από αντιστρέψιμες λογικές πύλες είναι και το ίδιο αντιστρέψιμο.

Στη συνέχεια θα γίνει μια σύντομη αναφορά στις πιο γνωστές στοιχειώδεις αντιστρέψιμες λογικές πύλες της βιβλιογραφίας, οι οποίες χρησιμοποιούνται για τη σύνθεση αντιστρέψιμων λογικών κυκλωμάτων (Πίνακας 2.3).

Ανάμεσα στις παραπάνω είναι γνωστό ότι η πύλη Toffoli είναι καθολική (universal) δηλ μπορεί να χρησιμοποιηθεί από μόνη της για την υλοποίηση οποιουδήποτε λογικού κυκλώματος.

Η πύλη Toffoli ($\{a_1, \ldots a_n\} \rightarrow \{b_1, \ldots, b_n\}$) μπορεί να επεκταθεί ώστε να ορίζεται για τη γενική περίπτωση των n εισόδων n εξόδων ως:

$$\left\{\begin{array}{l} b_1 = a_1 \\ b_2 = a_2 \\ \ldots \\ b_{n-1} = a_{n-1} \\ b_n = a_n \oplus a_1 a_2 \ldots a_{n-1} \end{array}\right\}$$

Περαιτέρω γενίκευση (Γενικευμένη πύλη Toffoli) της παραπάνω πύλης παρουσιάστηκε στις εργασίες [33, 34, 28] και ο τυπικός της ορισμός ακολουθεί.

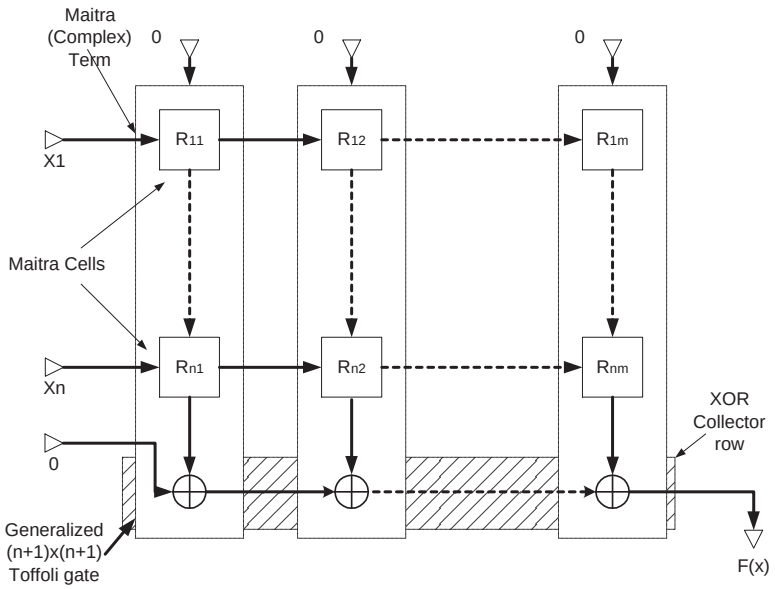
Ορισμός 32 *Μια k*k γενικευμένη πύλη Toffoli ($k * k$ Generalized Toffoli gate) ορίζεται ως:*

$$\left\{\begin{array}{l} b_1 = a_1 \\ b_2 = a_2 \\ \ldots \\ b_{n-1} = a_{n-1} \\ b_n = a_n \oplus f(a_1 a_2 \ldots a_{n-1}) \end{array}\right\}$$

, όπου A_i, P_i είναι οι είσοδοι και οι έξοδοι αντίστοιχα της πύλης και $f(a_1 a_2 \ldots a_{n-1})$ είναι μια τυχαία συνάρτηση $n-1$ μεταβλητών.

Στην εργασία [28] αποδεικνύεται ότι η κυτταρική αρχιτεκτονική Maitra (και κατά συνέπεια οποιαδήποτε ESCT έκφραση) αντιστοιχείται σε μια συστοιχία από γενικευμένες πύλες Toffoli. Μια άτυπη απόδειξη του παραπάνω ακολουθεί.

Μια αλυσίδα Maitra (και άρα ένας σύνθετος όρος) που αποτελείται από n κύτταρα μαζί με το αντίστοιχο κύτταρο XOR είναι μια γενικευμένη πύλη Toffoli $(n+1) * (n+1)$, αφού, σύμφωνα με τον Ορισμό 19 και την εικόνα 2.4, ισχύει: $P_1 = A_1 = X_1, P_2 = A_2 = X_2, \ldots, P_n = A_n = X_n, A_{n+1} = 0, P_{n+1} = f_n(A_1 A_2 \ldots A_n) \oplus A_{n+1}$ και $f_n = G_{i,n}(x_n, G_{i,n-1}(x_{n-1}, G_{i,n-2}(x_{n-2}, \ldots G_{i,1}(x_1, 0)\ldots)))$ είναι το αποτέλεσμα ενός μιας αλυσίδας Maitra(σύμφωνα με τον ορισμό του σύνθετου όρου). Από το παραπάνω έπεται ότι και μια ESCT έκφραση μπορεί να να απεικονιστεί ως αντιστρέψιμο κύκλωμα αφού αποτελείται από αντιστρέψιμες πύλες.



Σχήμα 2.4: Αρχιτεκτονική Maitra ως πύλες Toffoli.

2.4 Απεικόνιση ESCT εκφράσεων σε ολοκληρωμένα κυκλώματα FPGA

Οι εκφράσεις ESCT είναι λογικές εκφράσεις οι οποίες μπορούν να απεικονισθούν στην αρχιτεκτονική κυτταρικής διάταξης Maitra. Το σημαντικό πλεονέκτημα της παραπάνω αρχιτεκτονικής είναι η απλότητα των κυττάρων της (κύτταρα δύο εισόδων, μιας εξόδου που χρειάζεται να απεικονίζουν το πολύ έξι διαφορετικές λογικές συναρτήσεις) καθώς και η κανονικότητα της ίδιας της διάταξης, αφού τα κύτταρα τοποθετούνται σε γραμμές και στήλες. Ένα ακόμα πολύ σημαντικό χαρακτηριστικό είναι η περιορισμένη συνδεσιμότητα μεταξύ των κυττάρων. Κάθε κύτταρο χρειάζεται να συνδέεται μόνο με τα διπλανά του. Αυτό αποτελεί σημαντικό πλεονέκτημα αφού περιορίζεται η χρήση διαδρόμων (buses) που καταλαμβάνουν σημαντικό χώρο σε ένα ολοκληρωμένο κύκλωμα ενώ δημιουργούν και προβλήματα αφού μπορούν να οδηγήσουν σε μειωμένη απόδοση των ολοκληρωμένων κυκλωμάτων εάν αποτελέσουν σημεία συμφόρησης στην ανταλλαγή πληροφορίας μεταξύ των κυττάρων. Παρόλα αυτά, μέχρι τη στιγμή αυτή, δεν υπάρχει διαθέσιμη εμπορική υλοποίηση της κυτταρικής αρχιτεκτονικής Maitra.

Τα σημερινά εμπορικά ολοκληρωμένα κυκλώματα (VLSI - Very Large Scale Integration) μπορούν να χωριστούν σε δύο βασικές κατηγορίες. Τα ολοκληρωμένα κυκλώματα ASIC (Application Specific Integrated Circuit) και τα ολοκληρωμένα κυκλώματα FPGA (Field Programmable Gate Array). Για την κατασκευή μεγάλων εφαρμογών και μεγάλων ποσοτήτων ολοκληρωμένων κυκλωμάτων προτιμούνται τα κυκλώματα ASIC αφού με την τεχνική αυτή παράγονται ολοκληρωμένα κυκλώματα εξειδικευμένα για τη συγκεκριμένη εφαρμογή. Τα ολοκληρωμένα κυκλώματα FPGA, από την άλλη πλευρά, αποτελούν αρχιτεκτονικές γενικού τύπου που περιέχουν προγραμματιζόμενα κύτταρα και προγραμματιζόμενες συνδέσεις μεταξύ τους.

Από την παραπάνω περιγραφή γίνεται προφανές ότι η κυτταρική διάταξη Maitra θα μπορούσε εύκολα να κατασκευαστεί ως ολοκληρωμένο κύκλωμα FPGA. Δεδομένου όμως ότι δεν υπάρχει διαθέσιμη εμπορική υλοποίηση, μπορούν να βρεθούν παρόμοιες αρχιτεκτονικές FPGA στις οποίες να μπορούν να απεικονισθούν, αρκετά εύκολα, οι εκφράσεις ESCT.

Μία από τις εμπορικές αρχιτεκτονικές στην οποία μπορεί εύκολα να απεικονισθούν οι εκφράσεις ESCT είναι το ολοκληρωμένο FPGA Atmel 6000 [35]. Άλλες αρχιτεκτονικές, όπως η σειρά Concurrent Logic Cli 6000, είναι επίσης ιδιαίτερα ελκυστικές για την υλοποίηση ESCT εκφράσεων.

Κεφάλαιο 3

Ελαχιστοποίηση Εκφράσεων ESCT

Στο κεφάλαιο αυτό θα παρουσιαστεί ο θεωρητικός φορμαλισμός για την εύρεση ελάχιστων ESCT εκφράσεων για τυχαία λογική συνάρτηση. Η θεωρητική αυτή προσέγγιση αποτελεί τη ραχοκοκαλιά της διδακτορικής διατριβής. Όπως θα φανεί και στη συνέχεια, υπάρχουν αρκετές ομοιότητες στην ελαχιστοποίηση εκφράσεων ESCT με την ελαχιστοποίηση εκφράσεων ESOP. Θα γίνει όμως φανερό, ότι η ελαχιστοποίηση ESCT εκφράσεων είναι σημαντικά πιο δύσκολη από την αντίστοιχη των ESOP εκφράσεων αλλά, προφανώς, δίνει καλύτερα αποτελέσματα (μικρότερο αριθμό όρων). Ακολουθούνται τρεις βασικές προσεγγίσεις.

3.1 Βασικά θεωρήματα για τις εκφράσεις ESCT

Αρχικά θα γίνει μια παραδοχή για τη μορφή των σύνθετων όρων (Maitra cascades διαφορετικά) που θα χρησιμοποιηθεί στη συνέχεια. Η πρώτη είσοδος της πρώτης πράξης του σύνθετου όρου (αυτή που είναι "μακρύτερα" από το συλλέκτη XOR, εικόνα 2.1) θα θεωρούμε ότι είναι πάντα 0 (για λόγους συμμετρίας). Για το λόγο αυτό τα πρώτα αυτά cells θα είναι τύπου $1, 2$ ή 6 (Πίνακας 2.2), αφού αυτά καλύπτουν όλα τα δυνατά αποτελέσματα. Επίσης οι σύνθετοι όροι που θα παρουσιαστούν είναι περιορισμένοι (restricted). Τέλος όταν λέμε βάρος μιας συνάρτησης θα εννοούμε το ESCT βάρος της.

Το επόμενο Λήμμα παρουσιάζει τη μέθοδο συνένωσης δύο Maitra cells.

Λήμμα 1 *(Ένωση δύο Maitra cells) Η σχέση* $G_{r1}(x, y_1) \oplus G_{r2}(x, y_2) = G_r(x, y_1 \oplus y_2)$ *όπου* $y_1 \neq y_2, \bar{y_2}$ *ισχύει εάν:*

$(y_1, y_2, y) = (1, 1, 3), (1, 3, 1), (3, 3, 3), (2, 4, 2), (2, 2, 4), (4, 4, 4), (5, 6, 5), (5, 5, 6), (6, 6, 6).$

Πίνακας 3.1: Πίνακας συνένωσης n Maitra Cells.

Δείκτες r_i Maitra Cells εισόδου	Δείκτης r Maitra Cell αποτελέσματος
Περιττός αριθμός από cells με τύπο 1 και οποιοσδήποτε με τύπο 3	1
Περιττός αριθμός από cells με τύπο 2 και οποιοσδήποτε με τύπο 4	2
Άρτιος αριθμός από cells με τύπο 1 και οποιοσδήποτε με τύπο 3	3
Άρτιος αριθμός από cells με τύπο 2 και οποιοσδήποτε με τύπο 4	4
Περιττός αριθμός από cells με τύπο 5 και οποιοσδήποτε με τύπο 6	5
Άρτιος αριθμός από cells με τύπο 5 και οποιοσδήποτε με τύπο 6	6

Απόδειξη.
Το παραπάνω λήμμα μπορεί να αποδειχτεί πολύ εύκολα εξαντλητικά.
◇

Η γενίκευση του παραπάνω Λήμματος ακολουθεί.

Λήμμα 2 *(Ένωση n Maitra cells) Η σχέση $\sum \oplus F_{r_i}(x, y_i) = F_r(x, \sum \oplus y_i)$, $y_i \neq y_k, y_i \neq \bar{y_k}, \forall k \neq i$ ισχύει σύμφωνα με τον Πίνακα 3.1.*
Απόδειξη.
Στην πρώτη περίπτωση του Πίνακα 3.1, σύμφωνα με το Λήμμα 1, για να δημιουργήσουμε ένα Maitra cell τύπου 1, πρέπει να ενώσουμε ένα τύπου 1 και ένα τύπου 3. Ένα Maitra cell τύπου 3 μπορεί να δημιουργηθεί ενώνοντας οποιοδήποτε αριθμό από cells τύπου 3 και μονό αριθμό από cells τύπου 1. Έτσι χρειαζόμαστε μονό αριθμό από cells τύπου 1 και οποιοδήποτε αριθμό από cells τύπου 3 για να δημιουργήσουμε ένα cell τύπου 1. Αντίστοιχα και για τις υπόλοιπες περιπτώσεις.
◇

Το προηγούμενο λήμμα δηλώνει ότι μπορούμε να ενώσουμε οποιοδήποτε αριθμό από Maitra cells τύπου 1 ή 3 σε ένα μόνο cell τύπου 1 ή 3. Το ίδιο ισχύει για τα cells $(2, 4)$ και $(5, 6)$. Κατά συνέπεια το παραπάνω λήμμα υποδηλώνει ότι υπάρχουν τρεις διαφορετικές κλάσεις από πράξεις (Maitra cells) στους σύνθετους όρους. Οποιοσδήποτε αριθμός από cells της ίδιας κλάσης συμπυκνώνεται σε ένα cell της ίδιας κλάσης. Ο όρος G_r που δημιουργείται από την εφαρμογή των παραπάνω λημμάτων ονομάζεται "κανονικοποιημένος σύνθετος όρος" μιας και καταλήγει σε ένα μόνο Maitra cell του οποίου η είσοδος είναι άθροισμα XOR από άλλους σύνθετους όρους.

Πίνακας 3.2: Ένωση Maitra Cells με κοινές ή αντίστροφες εισόδους.

$y^1 = y$	$y^2 = y$	$y^3 = y$	$y^1 = y$	$y^2 = y$	$y^3 = \bar{y}$
r	**q**	**g**	**r**	**q**	**g**
1	4	5	1	2	6
1	5	4	1	6	4
3	4	6	2	3	5
3	6	4	2	5	1
4	5	1	2	6	3
4	6	3	3	5	4
$y^1 = y$	$y^2 = \bar{y}$	$y^3 = y$	$y^1 = y$	$y^2 = \bar{y}$	$y^3 = y$
r	**q**	**g**	**r**	**q**	**g**
1	4	6	3	4	5
1	6	2	3	5	2
2	1	5	5	1	2
2	3	6	5	4	3
2	5	3	6	3	2
2	6	1	6	4	1

Είδαμε ότι τα προηγούμενα λήμματα ισχύουν μόνο αν οι είσοδοι των Maitra cells δεν είναι ίδιες ή συμπληρωματικές. Το επόμενο λήμμα αποσαφηνίζει τις περιπτώσεις αυτές που απομένουν.

Λήμμα 3 *Αν $F_r(x, y^1), F_q(x, y^2), F_g(x, y^3)$ είναι τρία Maitra cells με $y^1, y^2, y^3 = y, \bar{y}$, τότε η εξίσωση: $F_r(x, y^1) \oplus F_q(x, y^2) = F_g(x, y^3)$ ισχύει σύμφωνα με τον πίνακα 3.2.*

Απόδειξη.

Μπορεί, πολύ εύκολα, να αποδειχτεί εξαντλητικά.

◇

Γνωρίζουμε ότι τα αναπτύγματα Shannon και Davio μπορούν να χρησιμοποιηθούν για την παραγωγή MVESOP (άρα και ESOP) εκφράσεων για μια τυχαία συνάρτηση f αν έχουμε τις ESOP (ελάχιστες ή μη) εκφράσεις των υποσυναρτήσεών της. Δεδομένου ότι μια ESCT έκφραση είναι γενικότερη από μια ESOP, είναι προφανές ότι τα παραπάνω αναπτύγματα μπορούν να χρησιμοποιηθούν και για την παραγωγή ESCT εκφράσεων. Στο επόμενο Θεώρημα παρουσιάζονται αναπτύγματα που παράγουν αποκλειστικά ESCT εκφράσεις.

Θεώρημα 1 *(Αναπτύγματα ESCT) Για μια δεδομένη λογική συνάρτηση $f(\boldsymbol{x})$, όπου $\boldsymbol{x}$ είναι το διάνυσμα των μεταβλητών εισόδου και x είναι μια από τις μεταβλητές εισόδου, μπορούμε να την εκφράσουμε ως:*

$$f(\boldsymbol{x}) = (x + f_2) \oplus (x \oplus f_1) \tag{3.1}$$

$$f(\boldsymbol{x}) = (x + f_0) \oplus (x\bar{f}_1) \tag{3.2}$$

$$f(\boldsymbol{x}) = (x\bar{f}_2) \oplus (x \oplus f_0) \tag{3.3}$$

$$f(\boldsymbol{x}) = (x + \bar{f}_0) \oplus (\bar{x} + \bar{f}_1) \tag{3.4}$$

$$f(\boldsymbol{x}) = (\bar{x} + \bar{f}_2) \oplus \bar{f}_0 \tag{3.5}$$

$$f(\boldsymbol{x}) = (x + \bar{f}_2) \oplus \bar{f}_1 \tag{3.6}$$

$$f(\boldsymbol{x}) = (\bar{x}\bar{f}_2) \oplus (x \oplus \bar{f}_1) \tag{3.7}$$

$$f(\boldsymbol{x}) = (\bar{x}\bar{f}_0) \oplus (\bar{x} + f_1) \tag{3.8}$$

$$f(\boldsymbol{x}) = (\bar{x} + f_2) \oplus (x \oplus \bar{f}_0) \tag{3.9}$$

Απόδειξη.

Θα αποδείξουμε ότι τα παραπάνω αναπτύγματα είναι ισοδύναμα με τον ανάπτυγμα Shannon.

Για τη σχέση 3.1 ισχύει: $f = [x+f_2]\oplus[x\oplus f_1] = \overline{[\bar{x}\bar{f}_2]}\oplus[x\oplus f_1] = [\bar{x}(f_1 \oplus \bar{f}_0)]\oplus \overline{[x \oplus f_1]} = \bar{x}\bar{f}_0 \oplus \bar{x}f_1 \oplus \bar{x} \oplus f_1 = \bar{x}f_0 \oplus xf_1$

Για τη σχέση 3.2 ισχύει: $f = (x + f_0) \oplus (x\bar{f}_1) = \bar{x}\bar{f}_0 \oplus x\bar{f}_1 \oplus 1 = \bar{x}\bar{f}_0 \oplus x\bar{f}_1 \oplus (x \oplus \bar{x}) = \bar{x}f_0 \oplus xf_1$

Για τη σχέση 3.3 ισχύει: $f = \{x\bar{f}_2\}\oplus[x\oplus f_0] = x(f_0\oplus\bar{f}_1)\oplus x\oplus f_0 = \bar{x}f_0\oplus xf_1$

Οι σχέσεις 3.4, 3.5, 3.6 προέρχονται από τα αναπτύγματα Shannon, θετικό και αρνητικό Davio όταν αντιστρέψουμε κάθε όρο του αθροίσματος XOR. Οι σχέσεις 3.7, 3.8, 3.9 προέρχονται από τις σχέσεις 3.1, 3.2, 3.3 αντίστοιχα όταν αντιστρέψουμε κάθε όρο του αθροίσματος XOR.

◇

Το επόμενο Θεώρημα αποδεικνύει ότι τα παραπάνω αναπτύγματα παράγουν ESCT εκφράσεις για μια τυχαία συνάρτηση f από τις ESCT εκφράσεις των υποσυναρτήσεών της.

Θεώρημα 2 *Έστω μια λογική συνάρτηση f και f_0, f_1, f_2 είναι οι υποσυναρτήσεις της στη μορφή αθροίσματος XOR σύνθετων όρων. Τότε η εφαρμογή των αναπτυγμάτων του Θεωρήματος 1, οδηγεί στη δημιουργία εκφράσεων για την f, επίσης, στη μορφή αθροίσματος XOR σύνθετων όρων.*

Απόδειξη.

Στα παραπάνω αναπτύγματα κάθε όρος του αθροίσματος είναι στη μορφή $G(x, f_i)$*,*

όπου $G(x, f_i) = \begin{cases} x + f_i \\ \bar{x} + f_i \\ xf_i \\ \bar{x}f_i \\ x \oplus f_i \\ f_i \end{cases}$ *, όπου* f_i *is* f_0, f_1, f_2*.*

Οι παραπάνω πράξεις συγκροτούν το σετ πράξεων του Πίνακα 2.2, για το λόγο αυτό κάθε τέτοια μορφή G *μπορεί να υλοποιηθεί χρησιμοποιώντας μόνο ένα Maitra Cell. Ετσι εάν οι εκφράσεις των υποσυναρτήσεων που θα χρησιμοποιηθούν σε κάποιον από τους κανόνες του Θεωρήματος 1 έχουν μόνο ένα σύνθετο όρο, τότε και η έκφραση της* f *θα συγκροτεί ένα XOR άθροισμα από δύο σύνθετους όρους, οι οποίοι θα είναι οι όροι των υποσυναρτήσεων με ένα επιπλέον Maitra cell (μια επιπλέον πράξη στο τέλος από αυτές του Πίνακα 2.2). Εάν οι εκφράσεις των υποσυναρτήσεων αποτελούνται από περισσότερους σύνθετους όρους, τότε από το Λήμμα 1 μπορούμε να αποφασίσουμε το είδος των Maitra cells που θα προστεθούν στους όρους για τη δημιουργία της έκφρασης της λογικής συνάρτησης* f*.*

◇

Είναι προφανές ότι τα αναπτύγματα του Θεωρήματος 1, ενώ παράγουν εκφράσεις ESCT, δεν παράγουν εκφράσεις ESOP.

Στα επόμενα θεωρήματα αποδεικνύεται ότι μπορούμε να προβλέψουμε το βάρος συναρτήσεων που παράγονται με συγκεκριμένο τρόπο από μια αρχική συνάρτηση f, δεδομένου ότι γνωρίζουμε το βάρος της f.

Θεώρημα 3 *(Αντίστροφη συνάρτηση) Η αντίστροφη συνάρτηση ενός σύνθετου όρου είναι επίσης ένας σύνθετος όρος. Στον αντίστροφο σύνθετο όρο, όλα τα Maitra cells που ανήκουν στην πρώτη (πράξεις* $+x, +\bar{x}$*) και στη δεύτερη κλάση (πράξεις* $\cdot x, \cdot \bar{x}$*) αντικαθίστανται από τα έτερα της κλάσης. Τα Maitra cells της τρίτης κλάσης (πράξεις* $\oplus x, \cdot 1$*) μένουν τα ίδια. Για τα cells του σύνθετου όρου που έχουν μία από τις εισόδους τους βραχυκυκλωμένη στο 0, η πράξη* $(+x)$ *αντικαθίσταται από* $(+\bar{x})$ *και ανάποδα.*

Απόδειξη.

Μπορεί να αποδειχθεί πολύ εύκολα χρησιμοποιώντας επαγωγή (ξεκινώντας από σύνθετο όρο ενός Maitra cell).

◇

Πίνακας 3.3: Άθροισμα XOR ενός σύνθετου όρου με $x, \bar{x}$.

p	**q**	y_1	**r**	y_2
1	3	y	1	$\bar{y}$
3	1	y	3	$\bar{y}$
2	2	$\bar{y}$	4	y
4	4	$\bar{y}$	2	y
5	6	y	6	$\bar{y}$
6	5	y	5	$\bar{y}$

Πόρισμα 1 *Μια λογική συνάρτηση και η αντίστροφή της έχουν το ίδιο βάρος.*

◇

Θεώρημα 4 *(Σύνθετος όρος $\oplus x$) Το αποτέλεσμα του XOR αθροίσματος ενός σύνθετου όρου $G_n(x_n, G_{n-1}(x_{n-1}, G_{n-2}(x_{n-2}, \ldots, G_1(x_1, y)\ldots)))$ ($G_i, i = 1, \ldots, n$ είναι Maitra cells) με το literal x_n (η τελευταία μεταβλητή του σύνθετου όρου - αυτή που αντιστοιχεί στο τελευταίο Maitra cell δηλαδή αυτό που είναι πιο κοντά στο συλλέκτη XOR) είναι επίσης ένας μόνο σύνθετος όρος.*

Απόδειξη.

Μπορεί πολύ εύκολα να αποδειχτεί εξαντλητικά.

◇

Πόρισμα 2 *(Σύνθετος όρος $\oplus \bar{x}$) Το αποτέλεσμα του XOR αθροίσματος ενός σύνθετου όρου $G_n(x_n, G_{n-1}(x_{n-1}, G_{n-2}(x_{n-2}, \ldots, G_1(x_1, y)\ldots)))$ ($G_i, i = 1, \ldots, n$ είναι Maitra cells) με το literal x_n (η τελευταία μεταβλητή του σύνθετου όρου - αυτή που αντιστοιχεί στο τελευταίο Maitra cell δηλαδή αυτό που είναι πιο κοντά στο συλλέκτη XOR) είναι επίσης ένας μόνο σύνθετος όρος.*

◇

Οι κανόνες για να δημιουργήσουμε εκφράσεις σαν τις παραπάνω παρουσιάζονται στον Πίνακα 3.3. Ο αρχικός σύνθετος όρος είναι ο $F_p(x, y)$. Οι σύνθετοι όροι $F_q(x, y_1), F_r(x, y_2)$ είναι: $F_q(x, y_1) = F_p(x, y) \oplus x, F_r(x, y_2) = F_p(x, y) \oplus \bar{x}$.

Τα πορίσματα του Θεωρήματος 3 παρουσιάζονται στον πίνακα 3.4.

***Παράδειγμα* 22** *Έστω ο σύνθετος όρος $P = (x_1 \oplus x_2)x_3 + \bar{x_4}$ ή στη μορφή που θα χρησιμοποιηθεί στη συγκεκριμένη διατριβή: (1542) (Πίνακας 2.2). Ο αντίστροφος σύνθετος όρος είναι:* (2524). *Ο σύνθετος όρος που προκύπτει ως άθροισμα XOR του P με τις $x_4, \bar{x_4}$ (η x_4 είναι η πιο σημαντική μεταβλητή) είναι αντίστοιχα:* (2522) *και* (1544).

Πίνακας 3.4: Αντίστροφος σύνθετος όρος.

Καμία είσοδος δεν είναι σταθερή.

Αρχικό cell	Αντίστροφο cell
1	3
2	4
3	1
4	2
5	5
6	6

Μία από τις εισόδους είναι σταθερά 0.

Αρχικό cell	Αντίστροφο cell
1	2
2	1

Το cell τύπου 6 εφαρμόζει τον κανόνα στο επόμενο cell.

Στον Ορισμό 31 παρουσιάστηκε η έννοια της m-ισοδύναμης έκφρασης. Μια m-ισοδύναμη έκφραση F (m-equivalent expression) μιας ESCT έκφρασης (Q) για μια λογική συνάρτηση f προκύπτει με την εφαρμογή του Θεωρήματος 3 και 4 σε ζευγάρια από σύνθετους όρους μέσα στην έκφραση Q ή εφαρμόζοντας τους κανόνες αυτούς σε ζευγάρια όρων μέσα στις εκφράσεις των υποσυναρτήσεων της f στο δέντρο-γεννήτρια της.

***Παράδειγμα* 23** *Έστω η ESCT έκφραση* $Q = (1234) \oplus (2343)$ *της συνάρτησης* $f = [0B10]$. *Τότε μια m-ισοδύναμη έκφραση της* Q *είναι (εφαρμόζοντας το θεώρημα 3):* $K = (1234) \oplus x \oplus (2343) \oplus x = (2414) \oplus (2341)$.

Οι παραπάνω κανόνες παραγωγής m-ισοδύναμων εκφράσεων ισοδυναμούν με τα επιπλέον αναπτύγματα που παρουσιάστηκαν στο Θεώρημα 1. Δηλαδή τα αναπτύγματα του Θεωρήματος 1 είναι m-ισοδύναμες εκφράσεις αυτών που παράγονται από τα αναπτύγματα Shannon, θετικό και αρνητικό Davio.

Θεώρημα 5 *Κάθε ESCT έκφραση μιας λογικής συνάρτησης* f *(άρα και μια ελάχιστη) μπορεί πάντα να γραφτεί σε μία από τις παρακάτω κανονικοποιημένες (normalized η compact) μορφές (αποτελείται από τους "κανονικοποιημένους σύνθετους όρους"* F_p, F_q, F_r*):*

- $f = F_p(x_1, y)$, *με* $(p, y) = (1, f_0), (2, f_1), (3, f_0), (4, f_1), (5, f_0), (6, f_0)$.
- $f = F_p(x_1, y) \oplus F_q(x_1, z)$ *με* $(p, q, y, z) = (3, 4, f_0, f_1), (3, 6, f_2, f_1), (4, 6, f_2, f_0)$.

- $f = F_p(x_1, y) \oplus F_q(x_1, z) \oplus F_r(x_1, g)$ *με* $(p = 3, q = 4, r = 6)$ *και* $y \oplus z = f_2$, $y \oplus g = f_0$,$z \oplus g = f_1$.

Κάθε τέτοια μορφή έχει m-ισοδύναμες οι οποίες προκύπτουν σύμφωνα με τον Ορισμό 31. Όλες οι μορφές αυτές παρουσιάζονται στον Πίνακα 3.5.
Απόδειξη.
Κάθε ελάχιστη μορφή μιας λογικής συνάρτησης f στη μορφή XOR αθροίσματος από σύνθετους όρους θα είναι της μορφής:

$$f(x_1, \ldots, x_n) = F_1(x_1, y_1) \oplus F_2(x_1, y_2) \oplus \ldots F_n(x_1, y_n)$$

όπου $F_i, i = 1, \ldots, n$ είναι Maitra cells και $y_i, i = 1, \ldots, n$ είναι σύνθετοι όροι. Εξαιτίας του Λήμματος 1, η παραπάνω μορφή μπορεί να περιέχει το πολύ 3 "κανονικοποιημένους" όρους (όρους δηλαδή που έχουν ένα μόνο Maitra cell στο τέλος και η είσοδος τους είναι το XOR των εισόδων - Λήμματα 1,2, 3). Τα τελευταία αυτά Maitra cells των κανονικοποιημένων όρων θα ανήκουν σε διαφορετικές κλάσεις. Η συνάρτηση f μπορεί επίσης να αναπαρασταθεί και με τη βοήθεια του αναπτύγματος Shannon. Συγκρίνοντας το ανάπτυγμα Shannon με την παραπάνω μορφή προκύπτουν οι παραπάνω κανόνες που παρουσιάστηκαν στο θεώρημα μαζί με τις m-ισοδύναμες μορφές τους.
◇

***Παράδειγμα* 24** *Έστω $f(x_1, x_2, x_3, x_4) = [a7122347]$ και μια ελάχιστη ESCT έκφρασή της: $f = (13443) \oplus (11344) \oplus (26654) \oplus (61166) \oplus (12616)$, με x_4 να είναι η πιο σημαντική της μεταβλητή και x_1 η λιγότερο σημαντική μεταβλητή. Η παραπάνω έκφραση μπορεί να ξαναγραφτεί στην τρίτη κανονικοποιημένη μορφή ως: $F_3(x_4, (1344)) \oplus F_4(x_4, (1134) \oplus (2665)) \oplus F_6(x_4, (6116) \oplus (1261))$.*

Οι οριζόντιες γραμμές στον Πίνακα 3.5 δηλώνουν m-ισοδύναμες εκφράσεις. Διακρίνουμε τις επόμενες περιπτώσεις, στις οποίες η ανάλυση θα εστιαστεί στις ελάχιστες ESCT εκφράσεις αφού αυτές ενδιαφέρουν στη συγκεκριμένη διατριβή:

- Έστω ότι η ελάχιστη ESCT έκφραση είναι στην πρώτη κανονικοποιημένη μορφή $f = F_p(x_n, y)$. Ανάλογα με το ποια από τις τρεις υποσυναρτήσεις f_0, f_1, f_2 είναι σταθερή και εάν είναι 1 ή 0, η συνάρτηση f θα γραφτεί σε μία (**και μόνο μία**) από τις έξι μορφές που παρουσιάζονται στον Πίνακα 3.5.

  ***Παράδειγμα* 25** *Έστω $f(x_1, x_2, x_3, x_4) = (x_1 + x_2)x_3x_4$, όπου x_4 είναι η πιο σημαντική μεταβλητή και x_1 η λιγότερο σημαντική. Οι υποσυναρτήσεις*

Πίνακας 3.5: m-Ισοδύναμες μορφές του Θεωρήματος 5.

Πρώτη			Δεύτερη				Τρίτη					
Κανονικοποιημένη Μορφή												
p	y	σταθ. υποσυνάρτηση	p	q	y	z	p	q	r	f_0	f_1	f_2
1	f_0	$f_1 = 1$	3	4	f_0	f_1	3	4	6	$y \oplus g$	$z \oplus g$	$y \oplus z$
2	f_1	$f_0 = 1$	1	2	$\overline{f_0}$	$\overline{f_1}$	1	2	6	$\bar{y} \oplus g$	$\bar{z} \oplus g$	$\bar{y} \oplus \bar{z}$
3	f_0	$f_1 = 0$	1	4	f_0	$\overline{f_1}$	1	4	6	$\bar{y} \oplus \bar{g}$	$z \oplus \bar{g}$	$\bar{y} \oplus z$
4	f_1	$f_0 = 0$	3	2	$\overline{f_0}$	f_1	3	2	6	$y \oplus \bar{g}$	$\bar{z} \oplus \bar{g}$	$y \oplus \bar{z}$
5	f_0	$f_2 = 1$	3	6	f_2	f_1	1	4	6	$y \oplus g$	$\bar{z} \oplus g$	$y \oplus \bar{z}$
6	f_0	$f_2 = 0$	1	6	$\overline{f_2}$	$\overline{f_1}$	1	4	5	$y \oplus g$	$z \oplus g$	$y \oplus z$
			1	5	f_2	f_1	3	4	5	$y \oplus g$	$\bar{z} \oplus g$	$y \oplus \bar{z}$
			3	5	$\overline{f_2}$	$\overline{f_1}$	3	2	6	$\bar{y} \oplus g$	$z \oplus g$	$\bar{y} \oplus z$
			4	6	f_2	f_0	3	2	5	$\bar{y} \oplus g$	$\bar{z} \oplus g$	$\bar{y} \oplus \bar{z}$
			2	6	$\overline{f_2}$	$\overline{f_0}$	1	2	5	$\bar{y} \oplus g$	$z \oplus g$	$\bar{y} \oplus z$
			4	5	$\overline{f_2}$	f_0	3	4	6	$\bar{y} \oplus \bar{g}$	$\bar{z} \oplus \bar{g}$	$\bar{y} \oplus \bar{z}$
			2	5	f_2	$\overline{f_0}$	3	4	5	$\bar{y} \oplus \bar{g}$	$z \oplus \bar{g}$	$\bar{y} \oplus z$
							1	4	6	$\bar{y} \oplus \bar{g}$	$\bar{z} \oplus \bar{g}$	$\bar{y} \oplus \bar{z}$
							1	2	6	$y \oplus \bar{g}$	$z \oplus \bar{g}$	$y \oplus z$
							1	2	5	$y \oplus \bar{g}$	$\bar{z} \oplus \bar{g}$	$y \oplus \bar{z}$
							3	2	5	$y \oplus \bar{g}$	$z \oplus \bar{g}$	$y \oplus z$

της f, ως προς τη μεταβλητή x_4, είναι: $f_0 = 0, f_1 = f_2 = (x_1 + x_2)x_3$. Είναι εμφανές ότι η f_0 είναι σταθερή και ίση με 0. Άρα, σύμφωνα με την πρώτη στήλη του Πίνακα 3.5: $f = F_4(x_1x_2x_3, x_4) = (x_1 + x_2)x_3x_4$. Δεν υπάρχει άλλη ελάχιστη ESCT έκφραση για την f που να ανήκει στην πρώτη κανονικοποιημένη μορφή.

***Παράδειγμα* 26** *Έστω $f(x_1, x_2, x_3, x_4) = \bar{x_1}\bar{x_2}\bar{x_3}x_4 \oplus \bar{x_1}\bar{x_2}\bar{x_3} \oplus 1$, όπου x_4 είναι η πιο σημαντική μεταβλητή και x_1 η λιγότερο σημαντική. Οι υποσυναρτήσεις της f, ως προς τη μεταβλητή x_4, είναι: $f_0 = x_1 + x_2 + x_3, f_1 = 1, f_2 = \bar{x_1}\bar{x_2}\bar{x_3}$. Είναι εμφανές ότι η f_1 είναι σταθερή και ίση με 1. Άρα, σύμφωνα με την πρώτη στήλη του Πίνακα 3.5: $f = F_1(\bar{x_1}\bar{x_2}\bar{x_3}, x_4) = x_1 + x_2 + x_3 + x_4$. Δεν υπάρχει άλλη ελάχιστη ESCT έκφραση για την f που να ανήκει στην πρώτη κανονικοποιημένη μορφή.*

- Έστω ότι η ελάχιστη ESCT έκφραση είναι στην δεύτερη κανονικοποιημένη μορφή $f = F_p(x_n, y) \oplus F_q(x_n, z)$. Υπάρχουν δώδεκα διαφορετικές περιπτώσεις που πρέπει να εξεταστούν, αλλά μπορούμε να τις χωρίσουμε σε τρεις κατηγορίες.

  - Στην πρώτη κατηγορία ισχύει: $(p, q) = (3, 4), (1, 2), (1, 4), (3, 2)$. Η περίπτωση $(p, q) = (3, 4)$ αντιστοιχεί στο ανάπτυγμα Shannon. Όλες οι περιπτώσεις της κατηγορίας εμφανίζονται μαζί. Αυτό σημαίνει ότι όταν υπάρχει μια ελάχιστη ESCT έκφραση στη μορφή του αναπτύγματος Shannon, τότε θα υπάρχουν, επίσης, άλλες τρεις ελάχιστες ESCT εκφράσεις με δείκτες $(p, q) = (1, 2), (1, 4), (3, 2)$. Οι εκφράσεις αυτές είναι m-ισοδύναμες της έκφρασης που παράγεται από το ανάπτυγμα Shannon. Το γεγονός αυτό υποδηλώνεται από την πρώτη οριζόντια γραμμή στη δεύτερη στήλη του Πίνακα 3.5 (2η κανονικοποιημένη μορφή).
  - Στη δεύτερη κατηγορία ισχύει: $(p, q) = (3, 6), (1, 6), (1, 5), (3, 5)$. Όπως και στην προηγούμενη περίπτωση, οι δείκτες $(p, q) = (3, 6)$ αντιστοιχούν στο ανάπτυγμα Negative Davio. Αυτό σημαίνει ότι όταν υπάρχει μια ελάχιστη ESCT έκφραση στη μορφή του αναπτύγματος Negative Davio, τότε θα υπάρχουν, επίσης, άλλες τρεις ελάχιστες ESCT εκφράσεις με δείκτες $(p, q) = (1, 6), (1, 5), (3, 5)$. Οι εκφράσεις αυτές είναι m-ισοδύναμες της έκφρασης που παράγεται από το ανάπτυγμα Negative Davio. Το γεγονός αυτό υποδηλώνεται από την δεύτερη οριζόντια γραμμή στη δεύτερη στήλη του Πίνακα 3.5.
  - Στη τρίτη κατηγορία ισχύει: $(p, q) = (4, 6), (2, 6), (4, 5), (2, 5)$. Όπως και στις δύο προηγούμενες περιπτώσεις, οι δείκτες $(p, q) = (4, 6)$ αντιστοιχούν στο ανάπτυγμα Positive Davio. Αυτό σημαίνει ότι όταν υπάρχει μια ελάχιστη ESCT έκφραση στη μορφή του αναπτύγματος Positive Davio, τότε θα υπάρχουν, επίσης, άλλες τρεις ελάχιστες ESCT εκφράσεις με δείκτες$(p, q) = (2, 6), (4, 5), (2, 5)$. Οι εκφράσεις αυτές είναι m-ισοδύναμες της έκφρασης που παράγεται από το ανάπτυγμα Positive Davio. Το γεγονός αυτό υποδηλώνεται από την τρίτη οριζόντια γραμμή στη δεύτερη στήλη του Πίνακα 3.5.

***Παράδειγμα* 27** *Έστω $f(x_1, x_2, x_3) = x_1x_2x_3 \oplus \bar{x_1}\bar{x_2}\bar{x_3}$, όπου x_3 είναι η πιο σημαντική μεταβλητή και x_1 η λιγότερο σημαντική. Η έκφραση ESCT $x_1x_2x_3 \oplus \bar{x_1}\bar{x_2}\bar{x_3}$ είναι ελάχιστη για την f και αντιστοιχεί στο ανάπτυγμα Shannon με δείκτες $(p, q) = (3, 4)$ (ως προς τη μεταβλητή x_3). Οι υποσυναρτήσεις της f,*

ως προς τη μεταβλητή x_3, είναι: $f_0 = \bar{x_1}\bar{x_2}, f_1 = x_1x_2$. Αλλά, σύμφωνα με το Θεώρημα 5, υπάρχουν τρεις, ακόμα, ελάχιστες ESCT εκφράσεις για την f:

$$f = F_1(\bar{f_0}, x_3) \oplus F_2(\bar{f_1}, x_3) = (x_1 + x_2 + x_3) \oplus (\bar{x_1} + \bar{x_2} + \bar{x_3}) \quad (3.10)$$

$$f = F_1(f_0, x_3) \oplus F_4(\bar{f_1}, x_3) = (\bar{x_1}\bar{x_2} + x_3) \oplus ((\bar{x_1} + \bar{x_2})x_3) \quad (3.11)$$

$$f = F_3(\bar{f_0}, x_3) \oplus F_2(f_1, x_3) = ((x_1 + x_2)\bar{x_3}) \oplus (x_1x_2 + \bar{x_3}) \quad (3.12)$$

Είναι εμφανές ότι η ESCT έκφραση που αντιστοιχεί στο ανάπτυγμα Shannon και οι προηγούμενες τρεις είναι m-ισοδύναμες, αφού η εξίσωση 3.10 είναι το ανάπτυγμα Shannon αν αντιστρέψουμε τους $F_3(f_0, x_3)$ και $F_4(f_1, x_3)$. Η εξίσωση 3.11 είναι το ανάπτυγμα Shannon εάν δημιουργήσουμε το άθροισμα XOR των $F_3(f_0, x_3)$, $F_4(f_1, x_3)$ με τη μεταβλητή x_3. Η εξίσωση 3.12 είναι το ανάπτυγμα Shannon εάν δημιουργήσουμε το άθροισμα XOR των $F_3(f_0, x_3)$, $F_4(f_1, x_3)$ με το literal $\bar{x_3}$.

- Έστω ότι η ελάχιστη ESCT έκφραση είναι στην τρίτη κανονικοποιημένη μορφή $f = F_p(x_n, y) \oplus F_q(x_n, z) \oplus F_r(x_n, g)$. Υπάρχει μόνο μία περίπτωση που πρέπει να εξεταστεί, για δείκτες: $(p, q, r) = (3, 4, 6)$. Αυτή η περίπτωση αντιστοιχεί στη γενική μορφή μιας έκφρασης ESOP: $f(x_1, \ldots, x_n) = y\bar{x_n} \oplus zx_n \oplus g$ (η μεταβλητή x_n είναι η πιο σημαντική). Οι υπόλοιπες δεκαπέντε περιπτώσεις στην τρίτη στήλη του Πίνακα 3.5 (3η κανονικοποιημένη μορφή) είναι, απλά, m-ισοδύναμες μορφές της προηγούμενης. Δημιουργούνται ως αθροίσματα XOR των ζευγαριών $(F_p, F_q), (F_p, F_r), (F_q, F_r)$ με το 1 ή το literal x_n ή το literal $\bar{x_n}$. Εάν υπάρχει μια ελάχιστη έκφραση ESCT στην τρίτη κανονικοποιημένη μορφή του Θεωρήματος 5, τότε θα υπάρχουν και άλλες δεκαπέντε ελάχιστες εκφράσεις ESCT για τη συνάρτηση αυτή. Η διαδικασία που ακολουθούμε για τη δημιουργία των εκφράσεων αυτών και οι κατάλληλοι δείκτες φαίνονται στην τρίτη στήλη του Πίνακα 3.5.

***Παράδειγμα* 28** *Έστω η $f(x_1, x_2, x_3, x_4, x_5) = [a7122347]$ και μια ελάχιστη ESCT έκφρασή της: $Q_1 = (23122) \oplus (26654) \oplus (21221) \oplus (61166) \oplus (12616) = F_2(x_5, (2312)) \oplus F_4(x_5, (2665)) \oplus F_1(x_5, (2122)) \oplus F_6(x_5, (6116)) \oplus F_6(x_5, (1261)) = ((23122) \oplus (26654)) \oplus ((21221)) \oplus ((61166) \oplus (12616))$ ή στην κανονικοποιημένη της μορφή, χρησιμοποιώντας και το Λήμμα 1 και θεωρώντας τη μεταβλητή x_5 ως πιο σημαντική: $F_2(x_5, (2312) \oplus (2665)) \oplus F_1(x_5, (2122)) \oplus F_6(x_5, (6116) \oplus (1261))$. Όπως φαίνεται από το Θεώρημα*

5, υπάρχουν δεκαπέντε, ακόμα, ελάχιστες ESCT εκφράσεις για την f. Μια από αυτές έχει δείκτες$(p, q, r) = (3, 4, 6)$. Πράγματι αν αλλάξουμε την F_1 σε F_3, την F_2 σε F_4, το y σε $\bar{y}$ and το z σε $\bar{z}$, σύμφωνα με τον Πίνακα 3.5 (πρώτη και δεύτερη γραμμή στη στήλη για την τρίτη κανονικοποιημένη μορφή), τότε: $Q_2 = F_3(x_5, \overline{(2122)}) \oplus F_4(x_5, \overline{(2313) \oplus (2665)}) \oplus F_6(x_5, (6116) \oplus (1261)) = F_3(x_5, (1344)) \oplus F_4(x_5, (1134) \oplus (2665)) \oplus F_6(x_5, (6116) \oplus (1261)) = (13443) \oplus (11344) \oplus (26654) \oplus (61166) \oplus (12616)$. *Προφανώς:* $w(Q_2) = w(Q_1) = 5$. *Σημειώνεται ότι το προηγούμενο αποτέλεσμα αποκτάται και εάν αντιστρέψουμε τους όρους (23122) και (21221) στην έκφραση* Q_1.

Η παραπάνω ανάλυση μας κάνει, ήδη, εμφανείς τις ομοιότητες που υπάρχουν ανάμεσα στην ελαχιστοποίηση εκφράσεων ESCT και στην ελαχιστοποίηση εκφράσεων ESOP. Είδαμε ότι τόσο στη δεύτερη όσο και στην τρίτη κανονικοποιημένη μορφή, οι "βασικές" ελάχιστες ESCT εκφράσεις είναι και ελάχιστες εκφράσεις ESOP. Απλά υπάρχουν και m-ισοδύναμες αυτών που είναι εκφράσεις ESCT, χωρίς να είναι και εκφράσεις ESOP. Η βασική διαφορά έγκειται στην πρώτη κανονικοποιημένη μορφή, όπου υπάρχουν περιπτώσεις που μια ελάχιστη έκφραση ESCT δεν μπορεί να απεικονιστεί σε μια αντίστοιχή της ελάχιστη έκφραση ESOP (συγκεκριμένα όταν υπάρχουν υποσυναρτήσεις σταθερές και ίσες με 1).

3.2 Γενίκευση Θεωρίας Ελαχιστοποίησης εκφράσεων ESCT

Έχουμε δει, στην έως τώρα θεωρία, ότι μια λογική συνάρτηση μιας εξόδου μπορεί πάντα να γραφτεί σε μία από τις τρεις κανονικοποιημένες μορφές του Θεωρήματος 5. Επιπλέον είδαμε ότι για να γνωρίζουμε μια ελάχιστη ESCT μορφή για λογικές συναρτήσεις έως 5 μεταβλητών εισόδου, χρησιμοποιούμε τις ελάχιστες ESCT εκφράσεις των υποσυναρτήσεών της.

Στο κεφάλαιο αυτό θα επιχειρηθεί η γενίκευση της θεωρίας ελαχιστοποίησης εκφράσεων ESCT για λογικές συναρτήσεις n μεταβλητών εισόδου. Τα θεωρήματα του κεφαλαίου αυτού έχουν πρωτίστως θεωρητική σημασία αφού η υλοποίηση τους (με τη βοήθεια Η/Υ) είναι ανέφικτη, τουλάχιστον για συναρτήσεις με μεγάλο αριθμό μεταβλητών εισόδου. Παρόλα αυτά τα επόμενα θεωρήματα θα μας οδηγήσουν στην κατασκευή πρακτικού αλγορίθμου (XMin6) ο οποίος εντοπίζει ακριβείς ESCT εκφράσεις για συναρτήσεις μέχρι 6 μεταβλητές εισόδου. Παράλληλα μας δίνουν τα απαραίτητα εφόδια για να επιχειρήσουμε μια πρώτη προσέγ-

γιση στο πρόβλημα της ενοποίησης της θεωρίας ελαχιστοποίησης για εκφράσεις ESOP και εκφράσεις ESCT.

Το επόμενο Λήμμα μας δείχνει ότι μπορούμε να βρούμε ένα φράγμα ανάμεσα στο άθροισμα των βαρών δύο υποσυναρτήσεων μιας λογικής συνάρτησης και στο πραγματικό βάρος της συνάρτησης αυτής.

Λήμμα 4 *Εάν f_i, f_j είναι δύο υποσυναρτήσεις μιας λογικής συνάρτησης f που εξαρτάται από $n+1$ μεταβλητές εισόδου, k_1, k_2, g είναι λογικές συναρτήσεις n μεταβλητών, $g \in R$, όπου R ένα συγκεκριμένο σύνολο συναρτήσεων και:*

- $f_i = k_1 \oplus_3$
- $f_j = k_2 \oplus_3$
- $s(f) = w(k_1) + w(k_2) + w(k_3)$, $k_3 = g \in R$ *ώστε* $s(f) = MIN_{\forall g}(w(f_i \oplus g) + w(f_j \oplus g) + w(g))$

τότε $[w(f_i) + w(f_j)] - s(f) = [w(f_i) + w(f_j)] - [w(k_1) + w(k_2) + w(k_3)] \leq MAX(w(k_3))$ *και* k_3 *είναι εκείνες οι συναρτήσεις* g *για τις οποίες βρίσκουμε το ελάχιστο* $s(f)$.

Απόδειξη.

Ισχύει: $f_i = k_1 \oplus k_3 \Leftrightarrow w(f_i) = w(k_1 \oplus k_3) \leq w(k_1) + w(k_3) \Rightarrow w(f_i) \leq w(k_1) + w(k_3)$. *Αντίστοιχα:* $w(f_j) \leq w(k_2) + w(k_3)$. *Κατά συνέπεια:* $[w(f_i) + w(f_j)] - [w(k_1) + w(k_2) + w(k_3)] \leq w(k_3)$. *Και επειδή οι* k_3 *μπορούν να έχουν διαφορετικά βάρη χρησιμοποιούμε το πάνω όριο των βαρών των* k_3 *δηλαδή:* $[w(f_i) + w(f_j)] - [w(k_1) + w(k_2) + w(k_3)] \leq MAX(w(k_3))$

$\diamond$

Το Λήμμα 4 μπορεί να χρησιμοποιηθεί για την εύρεση ενός ακριβέστερου πάνω ορίου για το βάρος μιας τυχαίας λογικής συνάρτησης σε σχέση με αυτό που προκύπτει από την εφαρμογή των αναπτυγμάτων Shannon, θετικού και αρνητικού Davio. Θυμίζουμε ότι ένα πάνω όριο για το ESCT βάρος μιας συνάρτησης μπορεί να βρεθεί ως: $w(f) \leq MAX(w(f_0) + w(f_1), w(f_0) + w(f_2), w(f_1) + w(f_2)))$. Το παραπάνω Λήμμα ισχύει για κάθε δυνατό ζεύγος υποσυναρτήσεων μιας συνάρτησης $(f_0, f_1), (f_0, f_2), (f_1, f_2)$ και δηλώνει ότι η διαφορά του πραγματικού βάρους μιας λογικής συνάρτησης f από την εκτίμηση που προκύπτει ως $w(f_i) + w(f_j)$ και $f_i \neq f_j, i, j = 0, 1, 2$ είναι πάντα φραγμένη. Εάν η εκτίμηση του βάρους είναι: $w(f_0) + w(f_1), w(f_0) + w(f_2), w(f_1) + w(f_2)$, τότε το φράγμα προκύπτει από τον Πίνακα 3.5 και είναι: $w(g), w(y), w(z)$ αντίστοιχα.

Στα επόμενα θεωρήματα η θεωρία ελαχιστοποίησης ESCT εκφράσεων γενικεύεται για συναρτήσεις n μεταβλητών εισόδου. Από τα θεωρήματα αυτά παράγεται ως συμπέρασμα η μεθοδολογία για την ελαχιστοποίηση λογικών συναρτήσεων με αριθμό μεταβλητών εισόδου το πολύ 6.

Θεώρημα 6 *Κάθε ελάχιστη ESCT έκφραση για μια λογική συνάρτηση f που εξαρτάται από n μεταβλητές εισόδου μπορεί να παραχθεί ενώνοντας (πραγματοποιώντας άθροισμα XOR) οποιαδήποτε λογική συνάρτηση $n-1$ μεταβλητών (έστω g) με τις υποσυναρτήσεις f_0, f_1 της f. Η ελάχιστη μορφή θα είναι: $Q = F_p(x, f_0^* \oplus g) \oplus F_q(x, f_1^* \oplus g) \oplus F_r(x, g)$ και $p = 1, 3, q = 2, 4, r = 5, 6, f_i^* = f_i, \bar{f}_i, i = 0, 1$. Οι συνδυασμοί των (p, q, r, f_0^*, f_1^*) προκύπτουν από τον Πίνακα 3.5.*

Απόδειξη.

Κάθε ελάχιστη ESCT μορφή της συνάρτησης f (ας την ονομάσουμε E) μπορεί να γραφτεί σε μία από τις κανονικοποιημένες μορφές του Θεωρήματος 5. Διακρίνονται οι ακόλουθες περιπτώσεις:

- *Εάν η ESCT έκφραση E είναι στην πρώτη μορφή του Θεωρήματος 5, τότε μια από τις υποσυναρτήσεις της f είναι σταθερή 0 ή 1 (έστω f_i). Κάθε ελάχιστη ESCT έκφραση για την f θα παραχθεί από τις ελάχιστες ESCT εκφράσεις των συναρτήσεων $f_0 \oplus g$, $f_1 \oplus g$, επιλέγοντας $g = 0$ ή 1. Για παράδειγμα αν $f_2 = 1$ και επιλέγοντας $g = 0$, τότε:*

  $f = x(f_1 \oplus 0) \oplus \bar{x}(f_0 \oplus 0) \oplus 0$ = *($f_1 = 1 \Leftrightarrow f_0 = \bar{f}_1$)*

  $\bar{x}\bar{f}_1 \oplus xf_1 = x \oplus f_1 = F_5(x, f_1)$

  (σύμφωνα με τον Πίνακα 3.5).

- *Έστω ότι η ESCT έκφραση E είναι στη δεύτερη μορφή του Θεωρήματος 5. Τότε κάθε ελάχιστη ESCT έκφραση για την f θα παραχθεί από τις ελάχιστες ESCT εκφράσεις των υποσυναρτήσεών της και θα αντιστοιχεί στα αναπτύγματα Shannon, Davio ή σε κάποιο από αυτά που παρουσιάστηκαν στο Θεώρημα 1. Κατά συνέπεια κάθε ελάχιστη ESCT έκφραση για την f θα παραχθεί από τις ελάχιστες ESCT εκφράσεις των συναρτήσεων: $f_0 \oplus g, f_1 \oplus g$ ή $\overline{f_0 \oplus g}, \overline{f_1 \oplus g}$ επιλέγοντας $g = f_0$ ή f_1 ή 0 ή 1. Προφανώς οι ελάχιστες ESCT εκφράσεις των $\overline{f_0 \oplus g}, \overline{f_1 \oplus g}$ παράγονται με τετριμμένο τρόπο (Θεώρημα 3) από τις ελάχιστες ESCT εκφράσεις των συναρτήσεων $f_0 \oplus g, f_1 \oplus g$. Για παράδειγμα επιλέγοντας $g = f_0$ και $(p, q, r) = (3, 4, 6)$ τότε η ελάχιστη ESCT έκφραση θα είναι: $F_3(x, f_0 \oplus f_0) \oplus F_4(x, f_1 \oplus f_0) \oplus f_0 = xf_2 \oplus f_0$ που αντιστοιχεί στο ανάπτυγμα θετικό Davio.*

- *Έστω ότι η ESCT έκφραση είναι στην τρίτη μορφή του Θεωρήματος 5. Τότε* ***κάθε*** *τέτοια ελάχιστη μορφή θα είναι:* $f = f_p(x, y) \oplus F_q(x, z) \oplus F_r(x, g)$ *όπου* $p = 1, 3, q = 2, 4, r = 5, 6$ *και* $f_0^* = y \oplus g, f_1^* = z \oplus g, f_0^* = f_0, \bar{f_0}), f_1^* = f_1, \bar{f}_1$. *Προφανώς δεν γνωρίζουμε τις συναρτήσεις* y, z, g *αλλά γνωρίζουμε τις υποσυναρτήσεις* f_0, f_1. *Γνωρίζουμε, επίσης, ότι οι συναρτήσεις* y, z, g *δεν εξαρτώνται από τη μεταβλητή* x. *Για να τις βρούμε δημιουργούμε τα αθροίσματα XOR όλων των δυνατών συναρτήσεων* g *με τις υποσυναρτήσεις* f_0, f_1 *ώστε να παράγουμε τις κατάλληλες* y, z *συναρτήσεις και τις αντίστοιχες ελάχιστες ESCT εκφράσεις τους. Οι ελάχιστες ESCT εκφράσεις για τις αντίστροφες* f_0, f_1 *παράγονται με τετριμμένο τρόπο από τις ελάχιστες ESCT εκφράσεις των υποσυναρτήσεων. Η ελάχιστη έκφραση για την* f *θα είναι:* $Q = F_p(x, f_0^* \oplus g) \oplus F_q(x, f_1^* \oplus g) \oplus F_r(x, g)$.

◇

Το συμπέρασμα από το προηγούμενο Θεώρημα είναι ότι μπορούμε, σε κάθε περίπτωση, να εντοπίζουμε οποιαδήποτε ελάχιστη ESCT έκφραση για μια λογική συνάρτηση αν μπορούμε να βρίσκουμε τις ελάχιστες ESCT εκφράσεις των αθροισμάτων XOR των υποσυναρτήσεών της f_0, f_1 με οποιαδήποτε λογική συνάρτηση g.

Πρέπει να σημειωθεί πως τα πορίσματα του Θεωρήματος 6 επεκτείνονται για οποιοδήποτε ζεύγος υποσυναρτήσεων μιας λογικής συνάρτησης (και όχι μόνο για τις f_0, f_1).

Το επόμενο θεώρημα αποτελεί άμεση απόρροια του Θεωρήματος 6 και βελτιώνει τα πορίσματά του, χρησιμοποιώντας όμως και την τρίτη υποσυνάρτηση f_2 για την παραγωγή ESCT εκφράσεων.

Θεώρημα 7 *Μια ελάχιστη ESCT έκφραση για μια λογική συνάρτηση* f *που εξαρτάται από* n *μεταβλητές εισόδου με βάρος το πολύ* W *μπορεί να παραχθεί ενώνοντας (πραγματοποιώντας άθροισμα XOR) λογικές συναρτήσεις* $n-1$ *μεταβλητών με βάρος το πολύ* $\lfloor \frac{W}{3} \rfloor$ *με τις υποσυναρτήσεις της* f.
Απόδειξη.
Κάθε ελάχιστη ESCT μορφή της συνάρτησης f *(ας την ονομάσουμε* E*) μπορεί να γραφτεί σε μία από τις κανονικοποιημένες μορφές του Θεωρήματος 5. Διακρίνονται οι ακόλουθες περιπτώσεις:*

- *Εάν η ESCT έκφραση* E *είναι στην πρώτη ή τη δεύτερη κανονικοποιημένη μορφή του Θεωρήματος 5, τότε είναι προφανές ότι μπορούμε να δημιουργή-*

σουμε ελάχιστες ESCT εκφράσεις για την f κατευθείαν από τις ελάχιστες ESCT εκφράσεις των υποσυναρτήσεών της.

- *Στην πρώτη περίπτωση (πρώτη κανονικοποιημένη μορφή), το βάρος της f είναι ίσο με αυτό κάποιας μη σταθερής υποσυνάρτησής της. Επιπλέον η ESCT έκφραση θα είναι της μορφής: $f = F_p(x, f_i)$, όπου f_i είναι κάποια μη σταθερή υποσυνάρτηση της f. Κατά συνέπεια όλες οι ελάχιστες ESCT εκφράσεις της f παράγονται από τις ελάχιστες ESCT εκφράσεις της f_i.*
- *Στη δεύτερη περίπτωση (δεύτερη κανονικοποιημένη μορφή), η E μπορεί πάντα να γραφτεί ως: $f = F_3(x, f_0) \oplus F_4(x, f_1)$ ή $f = F_3(x, f_2) \oplus F_6(x, f_1)$ ή $f = F_6(x, f_0) \oplus F_4(x, f_2)$. (υπάρχουν και άλλες δυνατές ESCT εκφράσεις στη δεύτερη κανονικοποιημένη μορφή, αλλά εκείνες είναι m-ισοδύναμες των τριών προαναφερθέντων και κατά συνέπεια έχουν τον ίδιο αριθμό όρων). Είναι προφανές ότι το βάρος της f είναι ίσο με: $w(f_0) + w(f_1), w(f_2) + w(f_1), w(f_2) + w(f_0)$ αντίστοιχα. Η ελάχιστη ESCT έκφραση της f περιέχει όλους τους σύνθετους όρους από δύο από τις υποσυναρτήσεις της ($(f_0, f_1), (f_1, f_2), (f_0, f_2)$ αντίστοιχα) με ένα επιπλέον κύτταρο Maitra που δηλώνεται από την κανονικοποιημένη μορφή που χρησιμοποιήθηκε.*

- *Εάν η είναι στην τρίτη κανονικοποιημένη μορφή του Θεωρήματος 5, τότε μπορεί πάντα να γραφτεί στην επόμενη μορφή: $f = F_3(x, y) \oplus F_4(x, z) \oplus F_6(x, g)$. Προφανώς τα y, z, g είναι ελάχιστες ESCT εκφράσεις και: $w(f) = w(y) + w(z) + w(g)$. Χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι: $w(y) \geq w(z) \geq w(g)$. Ισχύει: $w(f) = w(y) + w(z) + w(g) \geq 3 * w(g) \Leftrightarrow w(y) \leq \lfloor \frac{W}{3} \rfloor$. Στη περίπτωση αυτή μπορούμε να βρούμε την E εάν δημιουργήσουμε τα αθροίσματα XOR της συνάρτησης που αντιπροσωπεύει η ESCT έκφραση y με τις υποσυναρτήσεις f_2, f_0 ($f2 = y \oplus z, f0 = y \oplus g$, όπως φαίνεται στο Θεώρημα 5). Η ελάχιστη ESCT έκφραση E θα είναι: $f = F_3(x, f_0 \oplus g) \oplus F_4(x, f_1 \oplus g) \oplus F_6(x, g)$. Αντίστοιχη διαδικασία ακολουθούμε και όταν η z ή η g έχουν το μικρότερο βάρος.*

◇

Συμπερασματικά:

- Εάν μια υποσυνάρτηση της συνάρτησης εισόδου (f) είναι σταθερή (1 ή 0) τότε μπορούμε να βρούμε μια ελάχιστη ESCT έκφραση για f κατευθείαν από τις ελάχιστες ESCT εκφράσεις των μη σταθερών υποσυναρτήσεων της.

- Εάν υπάρχει μια ελάχιστη ESCT έκφραση της f στη δεύτερη κανονικοποιημένη μορφή του Θεωρήματος 5, τότε αυτή μπορεί να βρεθεί κατευθείαν από τις ελάχιστες ESCT εκφράσεις δύο εκ των υποσυναρτήσεών της. Για να βρούμε οποιαδήποτε τέτοια έκφραση πρέπει να ελέγξουμε όλα τα δυνατά ζεύγη των υποσυναρτήσεων $(f_0, f_1), (f_1, f_2), (f_0, f_2)$ και να ελέγξουμε τις εκφράσεις που παράγονται για ελαχιστότητα. Κατά συνέπεια το βάρος της f είναι: $w(f) = MIN(w(f_0) + w(f_1), w(f_1) + w(f_2), w(f_0) + w(f_2))$.

- Εάν υπάρχει ελάχιστη ESCT έκφραση της f στην τρίτη κανονικοποιημένη μορφή του Θεωρήματος 5, τότε θα πρέπει να δημιουργήσουμε τα αρθροίσματα XOR δύο εκ των υποσυναρτήσεων της f με κάθε δυνατή λογική συνάρτηση η οποία θα πρέπει να έχει βάρος το πολύ $\lfloor \frac{w(f)}{3} \rfloor$. Η παραπάνω διαδικασία θα πρέπει να εκτελεστεί για κάθε δυνατό ζεύγος υποσυναρτήσεων $((f_0, f_1), (f_1, f_2), (f_0, f_2))$. Στην περίπτωση αυτή το βάρος της f είναι:

$$\begin{aligned} w(f) = MIN_{\forall g}(&w(f_0 \oplus g) + w(f_1 \oplus g) + w(g), \\ &w(f_2 \oplus g) + w(f_1 \oplus g) + w(g), \\ &w(f_0 \oplus g) + w(f_2 \oplus g) + w(g)) \end{aligned} \tag{3.13}$$

  όπου g είναι μια λογική συνάρτηση με τον ίδιο αριθμό μεταβλητών με τις υποσυναρτήσεις της f και $w(g) \leq \lfloor \frac{w(f)}{3} \rfloor$.

***Παράδειγμα* 29** *Έστω λογική συνάρτηση* 4 *μεταβλητών εισόδου:* $f = [1234]$ *με ESCT βάρος* 3*. Οι υποσυναρτήσεις της έχουν βάρη:* $w(f_0) = w(f_1) = w(f_2) = 2$*. Σύμφωνα με το Θεώρημα 7 η ζητούμενη συνάρτηση* 3 *μεταβλητών εισόδου* g *που θα μας δώσει την ελάχιστη ESCT έκφραση για την* f *θα πρέπει να έχει βάρος το πολύ:* $3/3 = 1$*. Κατά συνέπεια ελέγχουμε όλες τις δυνατές* g *που εξαρτώνται από* 3 *μεταβλητές εισόδου και με βάρος* 1 *(δηλαδή αποτελούνται από έναν σύνθετο όρο). Δημιουργούμε δηλαδή τις συναρτήσεις* $f_0 \oplus g, f_1 \oplus g, f_2 \oplus g, g$ *και ελέγχουμε ποιος συνδυασμός τους, σύμφωνα με τη σχέση 3.13, δίνει το βάρος της συνάρτησης. Ανάμεσα σε αυτές υπάρχει η συνάρτηση:* $g = (136) = [22]$*. Ισχύει:* $w(g) = 1, w(f_1 \oplus g) = w([10]) = 1, w(f_2 \oplus g) = w([06]) = 1$*. Άρα ισχύει:* $w(f) = w(f_1 \oplus g) + w(f_2 \oplus g) + w(g) = 3$ *και η ελάχιστη ESCT έκφραση της* f *είναι:* $f = (6146) \oplus (2433) \oplus (1464) = [3030] \oplus [0004] \oplus [2200]$ *και παράγεται από τις ελάχιστες εκφράσεις των* $f_1 \oplus g, f_2 \oplus g, g$*.*

Συμπερασματικά μπορούμε να βρούμε το ESCT βάρος οποιασδήποτε λογικής συνάρτησης μοναδικής εξόδου που εξαρτάται από n μεταβλητές εισόδου αν γνωρί-

ζουμε (ή μπορούμε να βρούμε) το βάρος οποιασδήποτε λογικής συνάρτησης $n-1$ μεταβλητών εισόδου. Η παρατήρηση αυτή υποδεικνύει αναδρομική χρήση του Θεωρήματος 7 για την ελαχιστοποίηση μιας τυχαίας συνάρτησης (και των συναρτήσεων που θα προκύψουν κατά την εφαρμογή του θεωρήματος).

3.2.1 Θεωρητική Πολυπλοκότητα

Είναι εύκολο να προβλέψουμε την πολυπλοκότητα της αναδρομικής διαδικασίας που προτείνεται από το Θεώρημα 6. Για να βρεθεί το βάρος μιας συνάρτησης f με n μεταβλητές εισόδου πρέπει να δημιουργηθούν τα αθροίσματα XOR των υποσυναρτήσεων της f με οποιαδήποτε συνάρτηση με $n-1$ μεταβλητές εισόδου. Η κύρια υπολογιστική πολυπλοκότητα της μεθοδολογίας οφείλεται στο γεγονός αυτό. Είναι γνωστό ότι ο αριθμός των δυνατών λογικών συναρτήσεων με n μεταβλητές εισόδου είναι: 2^{2^n}. Η διαδικασία είναι αναδρομική και για κάθε συνάρτηση με i μεταβλητές εισόδου χρειάζεται να υπολογισθούν $2^{2^{i-1}}$ αθροίσματα XOR και μάλιστα 3 φορές (μία φορά για κάθε μία από τις επόμενες συναρτήσεις: $f_0^* \oplus g, f_1^* \oplus g, g$). Η διαδικασία σταματά στις 2 μεταβλητές εισόδου αφού εκεί το ESCT βάρος είναι πάντα 1. Κατά συνέπεια η υπολογιζόμενη πολυπλοκότητα για μια συνάρτηση με n μεταβλητές εισόδου είναι:

$\prod_{i=2}^{i\leq n-1}(3\cdot 2^{2^i}) = 3^n \cdot 2^{(\sum_{i=2}^{i\leq n-1}(2^i))} = 3^n \cdot 2^{(2^{n-1}-\frac{3}{2})} = O(3^n 2^{2^{n-1}}) = O(2^{2^{n-1}})$.

Στην πραγματικότητα, και χρησιμοποιώντας τις βελτιστοποιήσεις του Θεωρήματος 7, προτείνεται στη συγκεκριμένη διατριβή αναδρομική διαδικασία με πολυπλοκότητα μικρότερη από την προηγούμενη αφού δεν χρειάζονται $2^{2^{i-1}}$ αθροίσματα XOR σε κάθε επίπεδο αλλά μόνο εκείνα με τις συναρτήσεις που έχουν βάρος το πολύ $\lfloor W/3 \rfloor$, όπου W είναι το βάρος της συνάρτησης εισόδου f.

3.2.2 Εφαρμογή για συναρτήσεις μέχρι 6 μεταβλητές εισόδου

Σημειώνεται ότι η διαδικασία του Θεωρήματος 7 προσφέρεται για πρακτική υλοποίηση για συναρτήσεις με το πολύ 6 μεταβλητές εισόδου. Η πολυπλοκότητα του προβλήματος για συναρτήσεις με περισσότερες από 7 μεταβλητές εισόδου κάνει την πρακτική υλοποίηση απαγορευτική.

Άμεση απόρροια του Θεωρήματος 7 είναι τα παρακάτω Λήμματα που περιγράφουν τη διαδικασία για την εύρεση ελαχίστων ESCT εκφράσεων για λογικές συναρτήσεις με μέχρι 6 μεταβλητές εισόδου.

Πόρισμα 3 *Μια ελάχιστη ESCT έκφραση για μια λογική συνάρτηση f με το πολύ 5 μεταβλητές εισόδου μπορεί να παραχθεί δημιουργώντας τα αθροίσματα XOR λογικών συναρτήσεων με βάρος το πολύ 1 με τις υποσυναρτήσεις της f.*

Απόδειξη.

Είναι άμεση συνέπεια του Θεωρήματος 7, αφού το βάρος μιας λογικής συνάρτησης 5 μεταβλητών εισόδου είναι το πολύ 6 (αφού το βάρος μιας λογικής συνάρτησης 4 μεταβλητών είναι το πολύ 3 [18]). Σύμφωνα με το Θεώρημα 7, θα πρέπει να βρούμε εκείνες της συναρτήσεις 4 μεταβλητών εισόδου που έχουν βάρος το πολύ $w = 6/3 = 2$. Στην πραγματικότητα χρειάζεται να βρούμε, μόνο, εκείνες τις g που έχουν βάρος $w - 1 = 1$. Αυτό μας εγγυάται ότι το βάρος που θα μπορούμε να εντοπίσουμε είναι το πολύ 5. Κατά συνέπεια μια ελάχιστη ESCT έκφραση θα μπορεί να εντοπιστεί και για συναρτήσεις με βάρος 6, διότι η δημιουργία των αθροισμάτων XOR του Θεωρήματος 7 θα μας εξασφάλιζε ότι θα βρούμε στα σίγουρα ότι μια συνάρτηση έχει βάρος μικρότερο του 6 (και δεδομένου ότι το μέγιστο βάρος που μπορεί να έχει μια τέτοια συνάρτηση είναι 6). Στην περίπτωση αυτή η ελάχιστη έκφραση για την f θα δημιουργεί απευθείας (δεύτερη κανονικοποιημένη μορφή του Θεωρήματος 5) από τις ελάχιστες ESCT εκφράσεις των υποσυναρτήσεων της με βάρη 3.

◇

Πόρισμα 4 *Μια ελάχιστη ESCT έκφραση για μια λογική συνάρτηση f με το πολύ 6 μεταβλητές εισόδου μπορεί να παραχθεί δημιουργώντας τα αθροίσματα XOR λογικών συναρτήσεων με βάρος το πολύ 3 με τις υποσυναρτήσεις της f.*

Απόδειξη.

Είναι άμεση απόρροια του Θεωρήματος 7, αφού το βάρος μιας λογικής συνάρτησης 6 μεταβλητών μπορεί να είναι το πολύ 12 (αφού το βάρος μιας συνάρτησης 5 μεταβλητών μπορεί να είναι το πολύ 6). Χρησιμοποιώντας αντίστοιχη μεθοδολογία με την απόδειξη στο προηγούμενο πόρισμα, αποδεικνύεται ότι απαιτούνται αθροίσματα XOR με συναρτήσεις βάρους το πολύ 3.

◇

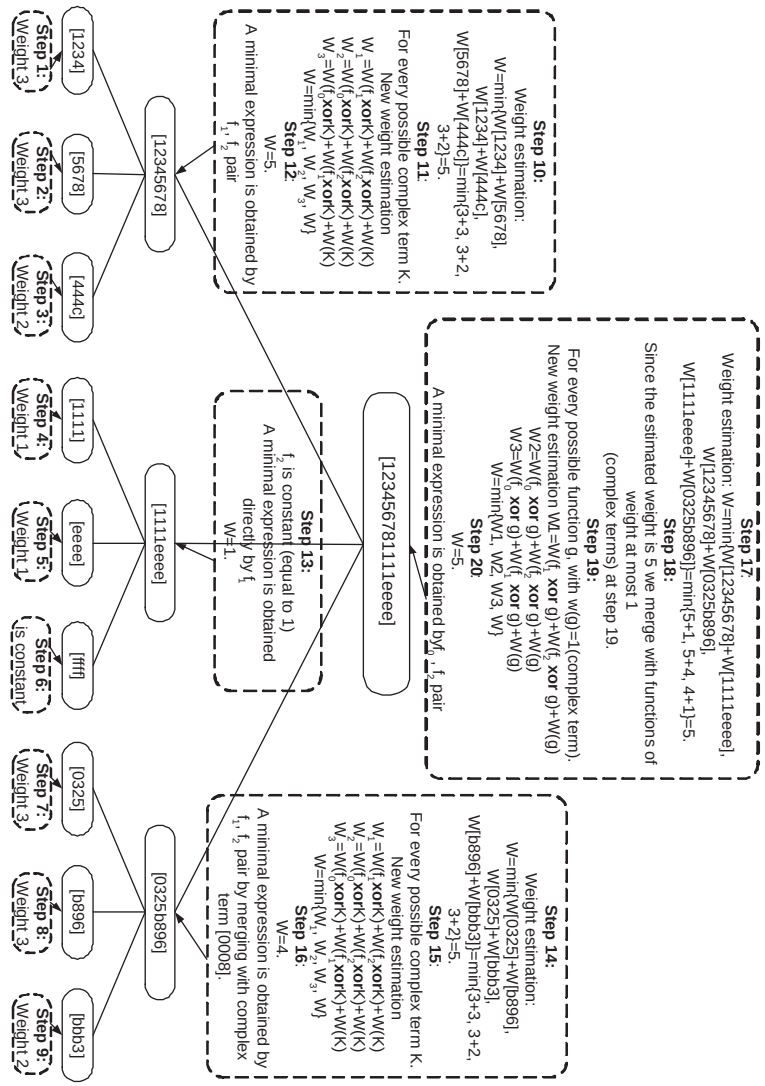
Χρησιμοποιώντας αναδρομικά τα Πορίσματα 3, 4 και το Θεώρημα 7 μπορούμε να βρούμε ελάχιστη λύση για μια τυχαία συνάρτηση 6 μεταβλητών εισόδου. Αυτό γίνεται δημιουργώντας το δέντρο-γεννήτρια και ελαχιστοποιώντας κάθε συνάρτηση-κόμβο του δέντρου αυτού. Για κάθε συνάρτηση-κόμβο του δέντρου f, εάν υπάρχει κάποια υποσυνάρτηση σταθερή τότε βρίσκουμε απευθείας ελάχιστες ESCT εκφράσεις της f από τις ελάχιστες ESCT εκφράσεις μιας μη σταθερής [36]. Στην αντίθετη περίπτωση θα υπάρχουν μόνο ελάχιστες ESCT εκφράσεις στη δεύτερη

ή την τρίτη μορφή του Θεωρήματος 5. Οι εκφράσεις της δεύτερης μορφής είναι εύκολο να βρεθούν αφού παράγονται απευθείας από τις ελάχιστες ESCT εκφράσεις των τριών υποσυναρτήσεων, μαζί με τις m-ισοδύναμές τους. Έτσι αρχικά δημιουργούνται οι εκφράσεις της δεύτερης μορφής και επιλέγονται τελικά εκείνες που έχουν τον ελάχιστο αριθμό όρων. Αυτό μας δίνει και μια αρχική εκτίμηση για το βάρος της συνάρτησης. Πρέπει, όμως, να ελεγχθεί αν υπάρχουν ελάχιστες ESCT εκφράσεις στην τρίτη μορφή του Θεωρήματος 5. Από όλες τις εκφράσεις της τρίτης μορφής επιλέγονται μόνο εκείνες με το μικρότερο αριθμό όρων. Ο αριθμός αυτός είναι και το πραγματικό βάρος της συνάρτησης και μπορεί να συμπίπτει (ή όχι) με την εκτίμηση για το βάρος που έχουμε από τις εκφράσεις της δεύτερης μορφής. Στην πρώτη περίπτωση θα υπάρχουν ελάχιστες ESCT εκφράσεις της συνάρτησης f τόσο στη δεύτερη όσο και στην τρίτη μορφή του Θεωρήματος 5, ενώ στη δεύτερη θα υπάρχουν μόνο στην τρίτη μορφή.

Η διαδικασία αυτή αποτυπώνεται στο παράδειγμα 30 και υλοποιείται από τον αλγόριθμο XMin6.

***Παράδειγμα* 30** *Έστω συνάρτηση* 6 *μεταβλητών εισόδου* $f = [123456781111eeee]$. *Για την ελαχιστοποίηση της θα περιγραφεί η αναδρομική διαδικασία που στηρίζεται στην εφαρμογή του Θεωρήματος 7 και των Πορισμάτων 3, 4. Το δέντρο-γεννήτρια της συνάρτησης παρουσιάζεται στην Εικόνα 3.1. Η χρονική αλληλουχία της διαδικασίας παρουσιάζεται ως το αντίστοιχο βήμα για κάθε κόμβο του δέντρου. Η διαδικασία παρουσιάζεται ως το επίπεδο των τεσσάρων μεταβλητών εισόδου, για λόγους απλότητας.*

Η διαδικασία ξεκινά με την εύρεση του βάρους των συναρτήσεων που έχουν 4 *μεταβλητές εισόδου (*9 *πρώτα βήματα). Στα βήματα* $10 - 12$ *ελαχιστοποιείται η συνάρτηση* $[12345678]$. *Θα ονομάσουμε τη συνάρτηση αυτή* g_1. *Επειδή η* g_1 *δεν έχει σταθερές υποσυναρτήσεις οι ελάχιστες ESCT εκφράσεις της θα είναι είτε στη δεύτερη είτε στην τρίτη μορφή του Θεωρήματος 5. Δημιουργούμε καταρχήν τις ESCT εκφράσεις της δεύτερης μορφής και παίρνουμε μια αρχική εκτίμηση για το βάρος της* g_1. *Η εκτίμηση αυτή είναι* 5 *(χρησιμοποιώντας το ανάπτυγμα αρνητικό Davio). Στο βήμα* 11 *όμως ελέγχεται αν υπάρχουν ελάχιστες μορφές στην τρίτη μορφή του Θεωρήματος 5. Δεδομένου ότι η εκτίμηση του βάρους είναι* 5 *θα πρέπει να ελεγχθούν εκείνες οι συναρτήσεις με βάρος το πολύ* $\lfloor 5/3 \rfloor = 1$. *Μετά τον έλεγχο (σύμφωνα με τη διαδικασία που υποδεικνύει το Θεώρημα 7) παρατηρείται ότι το πραγματικό βάρος της συνάρτησης είναι* 5, *οπότε υπάρχουν ελάχιστες ESCT εκφράσεις τόσο στη δεύτερη όσο και στην τρίτη μορφή του Θεωρήματος 5. Μια ελάχιστη ESCT έκφραση της* g_1 *είναι* $(24336) \oplus (62466) \oplus (13646) \oplus (14333) \oplus (24663)$.



Σχήμα 3.1: Παράδειγμα εύρεσης ελάχιστης λύσης της συνάρτησης $[123456781111eeee]$.

Στο βήμα 13 *η διαδικασία συνεχίζεται υπολογίζοντας το βάρος της συνάρτησης* $[1111eeee]$. *Θα την ονομάσουμε* g_2. *Επειδή η συνάρτηση αυτή έχει μια υποσυνάρτηση σταθερή (την* $[f\,f\,f\,f]$ *και ίση με* 1*) το βάρος της θα είναι ίσο με αυτό των υποσυναρτήσεών της* $[1111], [eeee]$. *Μια ελάχιστη μορφή της* g_2 *παράγεται απευθείας από την ελάχιστη μορφή της υποσυνάρτησής της* $[eeee] = (1166)$ *και θα είναι:* (11665).

Τα βήματα $14-16$ *είναι παρόμοια με τα* $10-12$. *Θα ονομάσουμε την αντίστοιχη συνάρτηση* $[0325b896]$ *ως* g_3. *Υπάρχει, όμως, μια μικρή διαφορά. Το εκτιμώμενο βάρος (βάσει της δεύτερης μορφής τους Θεωρήματος 5) είναι* 5. *Όμως στο βήμα* 15 *το πραγματικό βάρος της* g_3 *αποδεικνύεται ότι είναι* 4. *Άρα στην περίπτωση αυτή δεν υπάρχει ελάχιστη ESCT έκφραση στη δεύτερη μορφή του Θεωρήματος 5. Παρόλα αυτά υπάρχουν ελάχιστες ESCT εκφράσεις στην τρίτη μορφή. Για να δημιουργήσουμε*

μία από αυτές θα πρέπει να επιλέξουμε τη συνάρτηση $g = [0008]$ *(έχει βάρος* 1*), όπως προβλέπει το Θεώρημα 7. Στη συνέχεια θα δημιουργήσουμε τις συναρτήσεις* $f_1 \oplus g = [032d]$ *και* $f_2 \oplus g = [bbbb]$ *και θα βρούμε τις ελάχιστες ESCT εκφράσεις τους ακολουθώντας τη διαδικασία που ορίζει το Θεώρημα 7. Μια ελάχιστη ESCT έκφραση της* $f_1 \oplus g$ *είναι:* $(2153) \oplus (6234)$ *(βάρος* 2*) και μια ελάχιστη ESCT έκφραση της* $f_2 \oplus g$ *είναι:* (1266) *(βάρος* 1*). Η αντίστοιχη ελάχιστη ESCT έκφραση της* g_3 *είναι:* $(21536) \oplus (62346) \oplus (12663) \oplus (14334)$.

Στα τελευταία βήματα της διαδικασίας ($17 - 20$*) βρίσκουμε το βάρος της συνάρτησης εισόδου. Τα βήματα αυτά είναι παρόμοια με τα προηγούμενα. Τελικά το βάρος της συνάρτησης εισόδου είναι* 5 *και μια ελάχιστη ESCT έκφραση για αυτήν είναι:* $(215366) \oplus (623466) \oplus (126636) \oplus (143346) \oplus (116654)$.

3.3 Ακριβής Ελαχιστοποίηση για συναρτήσεις με ESCT βάρος το πολύ 7

Τα Θεωρήματα 6, 7 μας δίνουν μια γενική μεθοδολογία για την εύρεση ελάχιστης ESCT έκφρασης αλλά αποδεικνύονται ανεπαρκή για συναρτήσεις με περισσότερες από 6 μεταβλητές εισόδου. Μια τέτοια περίπτωση παρουσιάζεται στο παράδειγμα 31.

***Παράδειγμα* 31** *Έστω η λογική συνάρτηση* 5 *μεταβλητών εισόδου:* $g = [19cd0acc]$. *Κάθε όρος, στις εκφράσεις ESCT του παραδείγματος θα εκφράζεται χρησιμοποιώντας τόσο την αναπαράσταση MT όσο και την αναπαράσταση Cell. Το βάρος της* g *είναι ίσο με* 5 *και μια ελάχιστη ESCT έκφραση της* g *είναι:* $[00220022] \oplus [09000000] \oplus [00000a00] \oplus [000000ee] \oplus [10ef0000] = (13636) \oplus (25344) \oplus (16343) \oplus (11633) \oplus (11254)$.

Η παραπάνω έκφραση, όμως, δεν μπορεί να δημιουργηθεί από τη μεθοδολογία που προτείνεται από το [36] αφού αυτό παράγει μόνο μερικές από τις ελάχιστες ESCT εκφράσεις για συναρτήσεις 5 *μεταβλητών εισόδου. Παρόλο που το γεγονός αυτό δεν φαντάζει σημαντικό, γίνεται σημαντικό όταν προσπαθήσουμε να ελαχιστοποιήσουμε μια συνάρτηση* 6 *μεταβλητών εισόδου, την:* $f = [a75842a6be95486a]$ *(η* g *είναι υποσυνάρτηση της* f*).*

Μια ελάχιστη ESCT έκφραση της f *είναι:* $[0000000000220022] \oplus [0000000009000000] \oplus [7777888877778888] \oplus [0808080808080808] \oplus [00000a0000000000] \oplus [000000ee00000000] \oplus [10ef000000000000] = (136364) \oplus (253344) \oplus (146656) \oplus (614666) \oplus (163434) \oplus (116334) \oplus (112544)$. *Η έκφραση αυτή παράγεται από μια έκφραση της* f_0 *και από*

μια έκφραση της $f_2 = g$ συνενώνοντας δύο κοινούς σύνθετους όρους ($[00220022]$ *και* $[00090000]$*) ώστε να δημιουργηθούν οι όροι* $[0000000000220022], [0000000009000000]$ *της ESCT έκφρασης της f. Η εφαρμογή της θεωρίας από το [36] μας δίνει την ESCT έκφραση* $[00220022] \oplus [09000000] \oplus [f807f807] \oplus [4fb0b04f] = (13636) \oplus (25334) \oplus (22356) \oplus (24255)$ *για την f_0 που απαιτείται. Παρόλα αυτά, χρησιμοποιώντας το παραπάνω Θεώρημα δεν μπορούμε να παράγουμε την κατάλληλη ESCT έκφραση για την $g = f_2$.*

Στην ενότητα αυτή επεκτείνονται τα πορίσματα του [36] για συναρτήσεις με ESCT βάρος το πολύ 7 και ανεξαρτήτως του αριθμού των μεταβλητών εισόδου τους. Τα καινούργια θεωρήματα που αναπτύσσονται μας προσφέρουν τη δυνατότητα να βρίσκουμε όλες τις ελάχιστες ESCT εκφράσεις για συναρτήσεις με βάρος το πολύ 5 και τουλάχιστον μια ελάχιστη ESCT έκφραση για συναρτήσεις με βάρος το πολύ 7. Μπορούμε έτσι να αντιμετωπίσουμε περιπτώσεις, όπως αυτή του παραδείγματος 31.

Στις αποδείξεις των Θεωρημάτων 6, 7 είδαμε ότι όταν η ελάχιστη ESCT έκφραση μιας λογικής συνάρτησης f είναι στην πρώτη ή τη δεύτερη μορφή του Θεωρήματος 5, τότε μπορεί να παραχθεί απευθείας από τις ελάχιστες ESCT εκφράσεις των υποσυναρτήσεών της. Η "προβληματική" περίπτωση είναι όταν κάποια ελάχιστη ESCT έκφραση της f είναι στην τρίτη μορφή του Θεωρήματος 5. Στην περίπτωση αυτή δεν μπορούμε να βρούμε με εύκολο τρόπο την ελάχιστη ESCT έκφραση της f από τις ελάχιστες ESCT εκφράσεις των υποσυναρτήσεών της.

Έστω ότι μια ελάχιστη ESCT έκφραση Q της συνάρτησης εισόδου f παράγεται από τις ESCT εκφράσεις K_i, K_j των υποσυναρτήσεών της f_i, f_j αντίστοιχα. Κάνουμε τις ίδιες θεωρήσεις με αυτές του Θεωρήματος 6. Ισχύει: $w(y) \geq w(z) \geq w(g)$ (y, z, g οι συναρτήσεις της τρίτης μορφής του Θεωρήματος 5). Ακόμα:

$$w(f) = w(y) + w(z) + w(g) \geq 3 * w(g) \Leftrightarrow w(y) \leq \lfloor \frac{W}{3} \rfloor \tag{3.14}$$

Από το Θεώρημα 5 ισχύει: $f_i = K_i = y \oplus g^*, f_j = K_j = z \oplus g^*, g^* = g, \bar{g}$. Η ελάχιστη ESCT έκφραση Q είναι:

$$\begin{aligned} Q = F_p(x, y^*) \oplus F_q(x, z^*) \oplus F_r(x, g^*) = \\ F_p(x, f_i \oplus g^*) \oplus F_q(x, f_j \oplus g^*) \oplus F_r(x, g^*) \end{aligned} \tag{3.15}$$

$$_i = f_i = y \oplus g^* \tag{3.16}$$

$$K_j = f_j = z \oplus g^* \tag{3.17}$$

Η έκφραση Q, προφανώς, παράγεται από τις ελάχιστες ESCT εκφράσεις των συναρτήσεων: $y = f_i \oplus g^*, z = f_j \oplus g^*, g^*$, γιατί διαφορετικά θα μπορούσε να

βρεθεί μια άλλη ESCT έκφραση για την f με μικρότερο αριθμό όρων. Από τις σχέσεις 3.16, 3.17 προκύπτει το συμπέρασμα ότι υπάρχουν εκφράσεις K_i, K_j των υποσυναρτήσεων f_i, f_j που έχουν κοινούς ή/και αντίστροφους σύνθετους όρους (η συνάρτηση g). Επιπλέον οι εκφράσεις K_i, K_j δεν είναι απαραίτητο να είναι ελάχιστες (μπορούν να είναι w-ισοδύναμες). Ισχύει:

$f_i = y \oplus g^* \Rightarrow w(f_i) \leq w(y) + w(g^*)$ and $w(f_j) \leq w(z) + w(g^*)$.

Έτσι:

$w(f_i) + w(f_j) = w(y) + w(z) + w(g^*) + w(g^*) = w(f) + w(g) \Leftrightarrow w(f) = w(f_i) + w(f_j) - w(g)$ (since $w(g^*) = w(g)$).

Οι παραπάνω εξισώσεις μαζί με την εξίσωση 3.14 οδηγούν στο παρακάτω συμπέρασμα:

$$w(f_i) + w(f_j) - w(g) \leq w(f) \leq w(f_i) + w(f_j) \tag{3.18}$$

Επισημαίνεται ότι εξίσωση 3.14 ισχύει για εκείνο το ζεύγος υποσυναρτήσεων που οδηγεί στην ελάχιστη ESCT έκφραση στη μορφή 3 για τη συνάρτηση εισόδου, άρα και η εξίσωση 3.18.

Στον Πίνακα 3.6 εμφανίζονται όλες οι δυνατές περιπτώσεις $w(f), w(y), w(z), w(g)$, $w(f_i), w(f_j)$ που βασίζονται στην εξίσωση 3.18 και για βάρος της συνάρτησης εισόδου $w(f) \leq 7$. Στον πίνακα αυτό $w(y) + w(g)$ είναι ο αριθμός των σύνθετων όρων που η ESCT έκφραση K_i της υποσυνάρτησης f_i πρέπει να έχει για να δημιουργηθεί η Q. Αντίστοιχα, $w(z) + w(g)$ είναι ο αριθμός των σύνθετων όρων που πρέπει να έχει η ESCT έκφραση K_j της υποσυνάρτησης f_j για να δημιουργηθεί η Q. Οι εκφράσεις αυτές μπορούν, ενδεχομένως, να είναι ελάχιστες για τις υποσυναρτήσεις f_i, f_j.

Βασιζόμενοι στην προηγούμενη ανάλυση μπορούμε να διατυπώσουμε τα επόμενα θεωρήματα.

Θεώρημα 8 *Έστω f μια λογική συνάρτηση με $w(f) < 6$ και f_0, f_1, f_2 οι υποσυναρτήσεις της. Όλες οι ελάχιστες ESCT εκφράσεις της f μπορούν να βρεθούν από τις ελάχιστες ESCT εκφράσεις των f_0, f_1, f_2.*

Απόδειξη.

Έστω Q μια ελάχιστη ESCT έκφραση της f. Όλες οι ελάχιστες ESCT εκφράσεις των f_0, f_1, f_2 θεωρούνται γνωστές. Εάν η Q είναι στην πρώτη ή τη δεύτερη μορφή του Θεωρήματος 5 τότε η ανάλυση ακολουθεί αυτή του [36].

Αν η Q είναι στην τρίτη μορφή του Θεωρήματος 5 τότε πρέπει να αποδειχθεί ότι μπορεί να παραχθεί από τις ελάχιστες ESCT εκφράσεις των f_0, f_1, f_2.

Σύμφωνα με την εξίσωση 3.14: $w(g) \leq 1$*, αφού* $w(f) \leq 5$*. Σύμφωνα με τον Πίνακα 3.6 υπάρχουν* 2 *περιπτώσεις:*

1. $w(f) = w(f_i) + w(f_j)$*. Στην περίπτωση αυτή η ελάχιστη έκφραση* Q *της συνάρτησης εισόδου* f *παράγεται από μια ESCT έκφραση με* $w(f_i) + 1$ *(1-wequivalent) σύνθετους όρους για την* f_i *και με* $w(f_j)$ *σύνθετους όρους για την* f_j *ή από μια ESCT έκφραση με* $w(f_i)$ *σύνθετους όρους για την* f_i *και με* $w(f_j)+1$ *(1-wequivalent) σύνθετους όρους για την* f_j*. Για να δημιουργήσουμε την έκφραση* Q *από τις ελάχιστες ESCT εκφράσεις των* f_i, f_j *πρέπει να βρεθεί η κατάλληλη συνάρτηση* g *η οποία είναι αυτή για την οποία ισχύει:* $w(g^*) + w(f_i \oplus g^*) + w(f_j \oplus g^*) = w(f)$*. Η συνάρτηση* g^* *είναι, στην ουσία, ένας σύνθετος όροςμέσα στις ελάχιστες ESCT εκφράσεις των* f_i *ή* f_j *υποσυναρτήσεων, αντίστοιχα. Στην περίπτωση αυτή θα υπάρχουν και ελάχιστες ESCT εκφράσεις* Q *στη δεύτερη μορφή του Θεωρήματος 5.*

2. $w(f) = w(f_i)+w(f_j)-1$*. Στην περίπτωση αυτή η ελάχιστη ESCT έκφραση* Q *της συνάρτησης εισόδου* f *παράγεται από τις ελάχιστες ESCT εκφράσεις των* f_i, f_j*. Θα υπάρχει ένας κοινός ή αντίστροφος σύνθετος όρος ανάμεσα στις ελάχιστες ESCT εκφράσεις* K_i, K_j *των υποσυναρτήσεων* f_i, f_j*.*

Σε όλες τις προηγούμενες περιπτώσεις, επιπλέον ESCT εκφράσεις παράγονται ως m-ισοδύναμες (mequivalent expressions).

◇

Είναι προφανές ότι όλες οι ελάχιστες ESCT εκφράσεις για τη συνάρτηση εισόδου f μπορούν να βρεθούν μέσω του Θεωρήματος 8.

Θεώρημα 9 *Έστω* f *μια λογική συνάρτηση με* $5 < w(f) < 8$ *και* f_0, f_1, f_2 *οι υποσυναρτήσεις της. Τουλάχιστον μια ελάχιστη ESCT έκφραση της* f *μπορεί να βρεθεί από τις ελάχιστες ESCT εκφράσεις των* f_0, f_1, f_2*.*

Απόδειξη.

Έστω Q *μια ελάχιστη ESCT έκφραση της* f*. Όλες οι ελάχιστες ESCT εκφράσεις των* f_0, f_1, f_2 *θεωρούνται γνωστές. Σύμφωνα με τον Πίνακα 3.6, για όλες τις περιπτώσεις με* $w(f) > 5$*, εκτός της* 22*, μπορούμε να βρούμε όλες τις ελάχιστες ESCT εκφράσεις των* f_0, f_1, f_2 *αφού το βάρος τους είναι μικρότερο από* 6 *(Θεώρημα 8). Στην περίπτωση* 22 *μία από τις υποσυναρτήσεις (έστω η* f_i*) έχει βάρος ίσο με* 6*, οπότε δεν μπορούμε να έχουμε όλες τις ελάχιστες ESCT εκφράσεις της. Αλλά, σύμφωνα με τον ίδιο πίνακα, η ελάχιστη έκφραση της* f *παράγεται συνενώνοντας έναν ίδιο ή*

αντίστροφο σύνθετο όρο (g^*) μεταξύ ελαχίστων ESCT εκφράσεων των f_i, f_j. Για να βρούμε την ελάχιστη έκφραση της f πρέπει να δημιουργήσουμε κάθε δυνατή συνάρτηση $g^* \oplus f_i$ και $g^* \oplus f_j$ (g^* είναι ένας όρος μέσα στις ελάχιστες ESCT εκφράσεις της f_j). Αυτές οι συναρτήσεις g^* που παράγουν τις ελάχιστες ESCT εκφράσεις είναι εκείνες που ικανοποιούν την εξίσωση: $w(g^*) + w(f_i \oplus g^*) + w(f_j \oplus g^*) = w(f)$.

Για όλες τις υπόλοιπες περιπτώσεις πρέπει να αποδειχθεί ότι εάν η έκφραση Q είναι στην τρίτη μορφή του Θεωρήματος 5, τότε μπορεί να παραχθεί από τις ελάχιστες ESCT εκφράσεις των f_0, f_1, f_2.

Σύμφωνα με την εξίσωση 3.14: $w(g) \leq 2$, αφού $w(f) \leq 7$. Εάν $w(g) = 1$ τότε η ανάλυση ακολουθεί αυτή του Θεωρήματος 8.

Εάν $w(g) = 2$ τότε, σύμφωνα με τον Πίνακα 3.6, υπάρχουν 3 πιθανές περιπτώσεις:

1. *$w(f) = w(f_i) + w(f_j)$. Στη περίπτωση αυτή η ελάχιστη ESCT έκφραση Q της συνάρτησης εισόδου f παράγεται από μία ESCT έκφραση με $w(f_i) + 2$ σύνθετους όρους για την f_i (2-wισοδύναμη έκφραση) και με $w(f_j)$ σύνθετους όρους για την f_j **ή** από μία ESCT έκφραση με $w(f_i)$ σύνθετους όρους για την f_i και με $w(f_j) + 2$ σύνθετους όρους για την f_j (2-wισοδύναμη έκφραση) **ή** από μία ESCT έκφραση με $w(f_i) + 1$ σύνθετους όρους για την f_i (1-wισοδύναμη έκφραση) και με $w(f_j) + 1$ σύνθετους όρους για την f_j (1-wισοδύναμη έκφραση). Στις πρώτες δύο περιπτώσεις μπορούμε να δημιουργήσουμε την Q όπως στη περίπτωση 1 του Θεωρήματος 8 εντοπίζοντας εκείνους τους 2 σύνθετους όρους που συνιστούν τη συνάρτηση g και βρίσκονται μέσα στις ελάχιστες ESCT εκφράσεις των f_j, f_i αντίστοιχα. Στην τρίτη περίπτωση χρειάζονται 1-wισοδύναμες εκφράσεις και για την f_i και για την f_j, παρόλο που μόνο οι ελάχιστες ESCT εκφράσεις τους είναι διαθέσιμες. Για το λόγο αυτό δεν μπορούμε να δημιουργήσουμε την ελάχιστη έκφραση Q στην τρίτη μορφή του Θεωρήματος 5. Παρόλα αυτά, επειδή $w(f) = w(f_i) + w(f_j)$ θα βρούμε, τουλάχιστον, μια ελάχιστη ESCT έκφραση για τη συνάρτηση εισόδου f στη δεύτερη μορφή του Θεωρήματος 5.*

2. *$w(f) = w(f_i) + w(f_j) - 1$. Στην περίπτωση αυτή, η έκφραση Q δημιουργείται από μια ESCT έκφραση με $w(f_i) + 1$ σύνθετους όρους για την f_i και με $w(f_j)$ σύνθετους όρους για την f_j **ή** από μια ESCT έκφραση με $w(f_i)$ σύνθετους όρους για την f_i και με $w(f_j) + 1$ σύνθετους όρους για την f_j, σύμφωνα με τον Πίνακα 3.6. Η ανάλυση ακολουθεί αυτή των περιπτώσεων 1 of Theorem 8.*

3. *$w(f) = w(f_i) + w(f_j) + 2$. Στην περίπτωση αυτή η ελάχιστη ESCT έκφραση Q*

της συνάρτησης εισόδου f παράγεται από τις ελάχιστες ESCT εκφράσεις των υποσυναρτήσεων f_i, f_j. Θα υπάρχουν δύο κοινοί ή αντίστροφοι σύνθετοι όροι ανάμεσα στις ελάχιστες ESCT εκφράσεις των f_i, f_j.

Σε όλες τις προηγούμενες περιπτώσεις, επιπλέον ESCT εκφράσεις παράγονται ως m-ισοδύναμες εκφράσεις (mequivalent expressions).

◇

Η περίπτωση 1 του Θεωρήματος 9 δηλώνει ότι δεν μπορούμε να βρούμε όλες τις ελάχιστες ESCT εκφράσεις για μια συνάρτηση f με $5 < w(f) < 8$.

Παράδειγμα 32 *Έστω και πάλι η συνάρτηση g του παραδείγματος 31. Έστω ότι γνωρίζουμε τα βάρη των υποσυναρτήσεών της μαζί με τις ελάχιστες ESCT εκφράσεις τους. Το βάρος της g είναι 5 και η ελάχιστη ESCT έκφραση που θέλουμε να βρούμε αντιστοιχεί στην πέμπτη περίπτωση του Πίνακα 3.6 για $w(f) = 5$.*

Μια ελάχιστη ESCT έκφραση για την υποσυνάρτηση g_1 της g είναι: $[10ef] \oplus [0900] \oplus [0022]$ *και για την υποσυνάρτηση g_0 είναι:* $[0a00] \oplus [00cc]$. *Για να δημιουργήσουμε μια ESCT έκφραση για την g που περιέχει τους σύνθετους όρους* $[00220022], [09000000]$ *πρέπει να δημιουργήσουμε τη συνάρτηση* $[0022] \oplus g_0 = [0aee]$ *(πρώτη περίπτωση του Θεωρήματος 8). Μια ελάχιστη ESCT έκφραση για τη συνάρτηση αυτή είναι:* $[0a00] \oplus [00ee]$. *Σύμφωνα με το Θεώρημα 8 μια ελάχιστη έκφραση για την g είναι:* $[00220022] \oplus [09000000] \oplus [00000a00] \oplus [000000ee] \oplus [10ef0000]$.

Έχοντας την παραπάνω έκφραση για την $g = f_2$ και την έκφραση $[00220022] \oplus [09000000] \oplus [f807f807] \oplus [4fb0b04f]$ *για την f_0 μπορούμε να δημιουργήσουμε μια ελάχιστη ESCT έκφραση για την f, όπως είδαμε στο παράδειγμα 31:* $[0000000000220022] \oplus [0000000009000000] \oplus [7777888877778888] \oplus [0808080808080808] \oplus [00000a0000000000] \oplus [000000ee00000000] \oplus [10ef000000000000]$ *(περίπτωση 31 του Πίνακα 3.6).*

Αποτέλεσμα τη θεωρίας που αναπτύχθηκε στην ενότητα αυτή ήταν η δημιουργία του αλγορίθμου EW7MIN.

3.4 Ευριστικές Μεθοδολογίες

Τα θεωρήματα που αναπτύχθηκαν στο συγκεκριμένο κεφάλαιο ασχολούνται με το πρόβλημα της εύρεσης ελαχίστων ESCT εκφράσεων για πλήρως ορισμένες λογικές συναρτήσεις μοναδικής εξόδου. Τα θεωρήματα αυτά εγγυώνται το βέλτιστο της παραγόμενης λύσης. Στη διατριβή αυτή, όμως, ασχοληθήκαμε και με άλλα σημαντικά προβλήματα της ESCT ελαχιστοποίησης όπως την αναδιάταξη των μεταβλητών εισόδου μιας λογικής συνάρτησης με σκοπό την εύρεση μικρότερου ESCT

βάρους για αυτήν ή την εύρεση καλών ESCT εκφράσεων για ατελώς ορισμένες λογικές συναρτήσεις. Οι μεθοδολογίες που ακολουθούν ασχολούνται με τα παραπάνω ζητήματα αλλά δεν είναι ακριβείς δηλαδή δεν εγγυώνται το βέλτιστο της παραγόμενης λύσης. Για το λόγο αυτό καλούνται ευριστικές.

3.4.1 Αναδιάταξη μεταβλητών εισόδου

Μια λογική συνάρτηση n μεταβλητών μπορεί να εκφραστεί με παραπάνω από έναν τρόπους (εκφράσεις FPRM, ESOP, ESCT, αναπαράσταση MT κτλ). Αρκετές από αυτές τις εκφράσεις εξαρτώνται από τον τρόπο με τον οποίο θα επιλεγούν οι μεταβλητές εισόδου της συνάρτησης, δηλαδή από τη διάταξη "σημαντικότητας" των μεταβλητών. Συγκεκριμένα τόσο η αναπαράσταση MT (κατά συνέπεια και το δέντρο-γεννήτρια) όσο και οι εκφράσεις ESCT εξαρτώνται σημαντικά από τη διάταξη των μεταβλητών εισόδου που θα επιλεγεί, με άμεση συνέπεια το ESCT βάρος μιας λογικής συνάρτησης να μεταβάλλεται ανάλογα με τη διάταξη των μεταβλητών εισόδου που επιλέγεται. Να σημειώσουμε ότι αυτό δεν ισχύει για τις εκφράσεις ESOP όπου σε αυτές το ESOP βάρος είναι ανεξάρτητο της διάταξης των μεταβλητών εισόδου.

Είναι λοιπόν σημαντικό, όταν θέλουμε να βελτιώσουμε τα αποτελέσματα της ESCT ελαχιστοποίησης μιας λογικής συνάρτησης, να επιλέγουμε και μια καλή διάταξη στις μεταβλητές εισόδου της συνάρτησης (Variable Reordering).

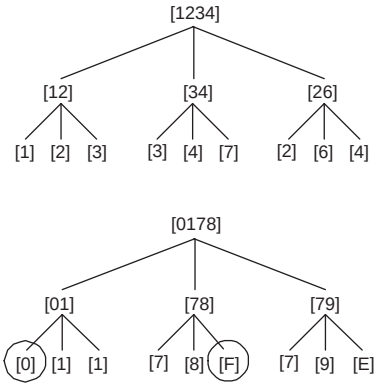
Στη συγκεκριμένη διδακτορική διατριβή μελετήθηκε το πρόβλημα της εύρεσης της βέλτιστης διάταξης των μεταβλητών εισόδου μιας λογικής συνάρτησης, της εύρεσης δηλαδή εκείνης της διάταξης που μας δίνει το καλύτερο δυνατό αποτέλεσμα ως προς το ESCT βάρος.

Η προτεινόμενη μεθοδολογία είναι ευριστική και στηρίζεται σε πόρισμα σύμφωνα με το οποίο η ύπαρξη μιας σταθερής υποσυνάρτησης f_i δεν αυξάνει το βάρος της συνάρτησης σε σχέση με αυτό μιας μη σταθερής υποσυνάρτησής της (f_j). Κατά συνέπεια, περιμένουμε ότι σε μια λογική συνάρτηση, όσο περισσότερες είναι οι σταθερές υποσυναρτήσεις μέσα στο δέντρο-γεννήτριά της και μάλιστα όσο πιο υψηλά (πιο κοντά στη ρίζα) βρίσκονται αυτές, τόσο μικρότερο θα είναι το βάρος της.

Η παραπάνω εικασία θα φανεί καλύτερα στα επόμενα παραδείγματα.

***Παράδειγμα* 33** *Έστω μια λογική συνάρτηση μοναδικής εξόδου και* 4 *μεταβλητών εισόδου:* $f(x_1, x_2, x_3, x_4) = [1234] = \bar{x_1}\bar{x_2}x_3x_4 \oplus x_1\bar{x_2}\bar{x_3}x_4 \oplus x_1\bar{x_2}x_3\bar{x_4} oplus \bar{x_1}\bar{x_2}x_3\bar{x_4} \oplus \bar{x_1}x_2\bar{x_3}\bar{x_4}$*. Η αναπαράσταση MT* $[1234]$ *προκύπτει όταν θεωρήσουμε ότι η πιο σημαντική μεταβλητή είναι η* x_4*, η αμέσως λιγότερο σημαντική η* x_3*, και οι δύο λιγότερο*

σημαντικές οι x_2, x_1 με λιγότερο σημαντική την τελευταία. Αν στην παραπάνω σειρά "σημαντικότητας" ανταλλάξουμε τις μεταβλητές x_4 και x_1 τότε η αναπαράσταση MT γίνεται $[0178]$. *Τα δέντρα-γεννήτριες για τις δύο παραπάνω διατάξεις μεταβλητών της ίδιας συνάρτησης παρουσιάζονται στην Εικόνα 3.2.*



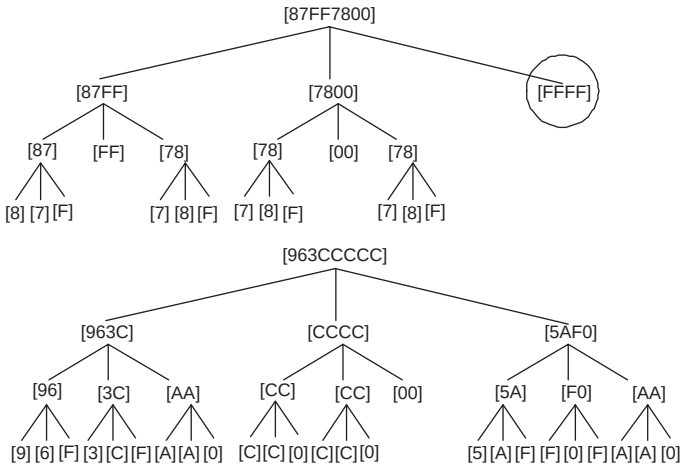
Σχήμα 3.2: Δέντρα-γεννήτριες για τις διατάξεις μεταβλητών $[1234]$ και $[0178]$.

Παρατηρούμε ότι η πρώτη διάταξη μεταβλητών $[1234]$ *δεν έχει σταθερές υποσυναρτήσεις μέχρι τις* 2 *μεταβλητές (στην ελαχιστοποίηση ESCT για συναρτήσεις μοναδικής εξόδου σταματάμε πάντα στις* 2 *μεταβλητές) ενώ η άλλη διάταξη έχει δύο σταθερές υποσυναρτήσεις στο επίπεδο των* 2 *μεταβλητών. Το γεγονός αυτό αλλάζει το βάρος της συνάρτησης ανάμεσα στις δύο διαφορετικές διατάξεις μεταβλητών. Η πρώτη έχει βάρος* 3 *(ελάχιστη ESCT έκφραση:* $(2433) \oplus (6246) \oplus (1364)$*) ενώ η δεύτερη έχει βάρος* 2 *(ελάχιστη ESCT έκφραση:* $(2334) \oplus (1453)$*).*

***Παράδειγμα* 34** *Έστω μια λογική συνάρτηση μοναδικής εξόδου και* 5 *μεταβλητών εισόδου. Επιλέγοντας μια διάταξη μεταβλητών, η αναπαράσταση MT είναι:* $f = [87ff7800]$. *Επιλέγοντας διαφορετική διάταξη μεταβλητών η αναπαράσταση MT είναι:* $f = [963ccccc]$. *Τα δέντρα-γεννήτριες που αντιστοιχούν στις διαφορετικές διατάξεις μεταβλητών φαίνονται στην Εικόνα 3.3.*

Παρατηρούμε ότι η πρώτη διάταξη μεταβλητών έχει μια σταθερή υποσυνάρτηση 1 *στο πρώτο επίπεδο αποσύνθεσης. Περιμένουμε λοιπόν η πρώτη διάταξη να έχει μικρότερο ESCT βάρος. Πράγματι το βάρος για την πρώτη διάταξη μεταβλητών είναι* 1 *(ελάχιστη ESCT έκφραση:* (14545)*) ενώ για τη δεύτερη είναι* 3 *(ελάχιστη ESCT έκφραση:* $(16634) \oplus (15566) \oplus (16563)$*).*

Η μεθοδολογία που αναπτύξαμε για την επιλογή καλής διάταξης μεταβλητών (ώστε να δίνει καλό ESCT βάρος), δεδομένης μιας λογικής συνάρτησης, είναι να



Σχήμα 3.3: Δέντρα-γεννήτριες για τις διατάξεις μεταβλητών $[87ff7800]$ και $[963ccccc]$.

ελέγχεται κάθε πιθανή διάταξη των μεταβλητών της. Για κάθε τέτοια διάταξη δημιουργείται το δέντρο-γεννήτρια και με βάση τον αριθμό και την θέση των σταθερών υποσυναρτήσεών της παράγεται το κέρδος (GAIN). Όσο υψηλότερο το κέρδος, τόσο πιο μικρό βάρος είναι πιθανό να έχει η συγκεκριμένη διάταξη μεταβλητών. Μάλιστα η παραπάνω μεθοδολογία βελτιώθηκε προϋπολογίζοντας τα πραγματικά βάρη για συναρτήσεις που έχουν το πολύ τέσσερις μεταβλητές εισόδου. Το κέρδος για αυτές είναι μεγαλύτερο όσο μικρότερο το βάρος. Έτσι η διαδικασία της αποσύνθεσης μπορεί να σταματά στο επίπεδο των 4 μεταβλητών εισόδου ώστε να έχουμε ακόμα πιο ακριβή αποτελέσματα.

Πίνακας 3.6: Βάρη για την τρίτη μορφή του Θεωρήματος 5 για $w(f) \leq 7$.

Case	$w(f)$	$w(y)$	$w(z)$	$w(g)$	$w(f_i)$	$w(f_j)$
1	3	1	1	1	2	2
2	4	2	1	1	3	2
3					2	2
4	5	3	1	1	4	2
5					3	2
6					4	1
7		2	2	1	3	3
8					2	3
9					3	2
10	6	4	1	1	5	2
11					4	2
12					5	1
13		3	2	1	4	3
14					3	3
15					4	2
16		2	2	2	4	4
17					4	3
18					4	2
19					3	4
20					2	4
21					3	3
22	7	5	1	1	6	2
23					5	2
24					6	1
25		4	2	1	5	3
26					4	3
27					5	2
28		3	3	1	4	4
29					3	4
30					4	3
31		3	2	2	5	4
32					4	4
33					3	4
34					5	3
35					5	2
36					4	3

Κεφάλαιο 4

Κβαντικοί Υπολογιστές

Στην ενότητα αυτή θα ασχοληθούμε με τους κβαντικούς υπολογιστές και με την κβαντική επέκταση κάποιων από τους αλγορίθμους που αναπτύξαμε έως τώρα στο πλαίσιο της διατριβής.

Μέχρι τώρα, όλα τα υπολογιστικά συστήματα είναι κλασικά και χρησιμοποιούν τη δίτιμη λογική (binary logic). Υπάρχουν όμως περιορισμοί ως προς την απόδοση που μπορούμε να επιτύχουμε, περιορισμοί που οι ίδιοι οι φυσικοί νόμοι μας επιβάλλουν. Ο πιο αξιόλογος από αυτούς είναι η πεπερασμένη ταχύτητα του ίδιου του φωτός. Τα εξαρτήματα ενός κλασικού υπολογιστικού συστήματος ανταλλάσσουν πληροφορία μεταξύ τους με τη μορφή μεταφοράς ενέργειας. Η ταχύτητα της παραπάνω ανταλλαγής είναι (στην καλύτερη περίπτωση) ίση με την ταχύτητα του φωτός. Έτσι για να διανυθεί μια απόσταση 30 εκατοστών, στο κενό, απαιτείται χρόνος 1 νανοδευτερόλεπτο. Στον ίδιο χρόνο η πληροφορία μεταδίδεται 20 εκατοστά σε έναν μεταλλικό αγωγό. Είναι, λοιπόν, αναπόφευκτο ότι στην προσπάθειά μας να αυξήσουμε την ταχύτητα ενός κλασικού υπολογιστικού συστήματος θα πρέπει να μειώσουμε τις αποστάσεις των εξαρτημάτων, φτάνοντας ενδεχομένως σε υποατομικά επίπεδα. Όταν όμως γίνει κάτι τέτοιο τότε οι καταστάσεις των εξαρτημάτων θα κυβερνώνται από την αρχή της απροσδιοριστίας του Heisenberg.

Επιπλέον η ίδια η τεχνολογία κατασκευής των ολοκληρωμένων κυκλωμάτων μας επιβάλλει περιορισμούς ως προς το ταβάνι της απόδοσης η οποία μπορεί να επιτευχθεί. Κάθε ολοκληρωμένο κύκλωμα αποβάλλει ενέργεια με τη μορφή θερμότητας. Η ενέργεια αυτή θα πρέπει να απομακρύνεται από το κύκλωμα. Όμως η ικανότητα μας να απομακρύνουμε την παραπάνω θερμότητα αυξάνεται με μικρότερο ρυθμό σε σχέση με το ρυθμό που αυξάνεται η δημιουργία της όσο το μέγεθος των ολοκληρωμένων κυκλωμάτων μειώνεται [37].

Η ιδέα της κατασκευής και χρήσης υπολογιστικών συστημάτων που θα χρη-

σιμοποιούν φαινόμενα και νόμους της κβαντικής μηχανικής είναι πλέον ευρέως διαδεδομένη και πλήθος ερευνητικών προσπαθειών στρέφεται προς αυτήν την κατεύθυνση. Η αρχική ιδέα για την ανάπτυξη των κβαντικών υπολογιστών ανήκει στον Richard P. Feynman (Βραβείο Nobel Φυσικής, 1965). Από διάφορα άρθρα που έχουν δημοσιευτεί μέχρι σήμερα, προκύπτει αναμφισβήτητα ότι ένας κβαντικός υπολογιστής μπορεί να εκτελέσει υπολογισμούς πολύ πιο γρήγορα και αποτελεσματικά από τα υπολογιστικά συστήματα που βασίζονται στα μικροηλεκτρονικά κυκλώματα. Ο όρος κβάντο (quantum, μικρή ποσότητα - προέρχεται από τη λέξη quantus που στα λατινικά σημαίνει πόσο) αναφέρεται σε διακριτές μονάδες που χαρακτηρίζουν συγκεκριμένες φυσικές ποσότητες, όπως η ενέργεια ενός ατόμου ύλης σε κατάσταση ηρεμίας.

Είναι γνωστό ότι τα υπολογιστικά συστήματα που χρησιμοποιούν κβαντικές πύλες έχουν ιδιαίτερες ιδιότητες. Οι κβαντικοί υπολογιστές επιτρέπουν την αποδοτική υλοποίηση των πιο πολύπλοκων φυσικών συστημάτων που μπορούμε να φανταστούμε. Επιτρέπουν, επίσης, την αποδοτική παραγοντοποίηση μεγάλων ακεραίων, με άμεσες εφαρμογές στην κρυπτογραφία. Ακόμα, οι κβαντικοί υπολογιστές επιταχύνουν σημαντικά τη διαδικασία αναγνώρισης προτύπων σε τυχαία δεδομένα.

Η μεγάλη έκρηξη στο πεδίο των κβαντικών υπολογιστών έλαβε χώρα το 1994, όταν ο Peter Shor δημοσίευσε ένα κβαντικό αλγόριθμο [38], ο οποίος μπορούσε σε πολυωνυμικό χρόνο να λύσει το πρόβλημα της παραγοντοποίησης ενός ακεραίου. Στους κλασσικούς υπολογιστές, η πολυπλοκότητα της επίλυσης του προβλήματος της παραγοντοποίησης ενός ακεραίου σε δύο πρώτους αριθμούς αυξάνεται εκθετικά ανάλογα με το πλήθος των ψηφίων. Η παραγοντοποίηση ενός αριθμούς σε δύο πρώτους αριθμούς είναι ιδιαίτερα σημαντική για την κρυπτογραφία και ειδικότερα για τον αλγόριθμο RSA, έναν αλγόριθμο κρυπτογράφησης που χρησιμοποιείται ευρέως.

Μετά τη δημοσίευση του αλγορίθμου του Shor, παρουσιάστηκε και ο αλγόριθμος του Lov Grover [39] για αναζήτηση σε μη δομημένες βάσεις δεδομένων. Αν και η λύση του Grover δεν πετυχαίνει τα εντυπωσιακά αποτελέσματα που πετυχαίνει ο αλγόριθμος του Shor σε σχέση με τους κλασσικούς υπολογιστές, είναι αποδεδειγμένα πιο αποδοτικός από το βέλτιστο αλγόριθμο των κλασσικών υπολογιστών για το συγκεκριμένο πρόβλημα.

Στη συγκεκριμένη εργασία μας ενδιαφέρει κυρίως ο αλγόριθμος του Grover ο οποίος αποτελεί και τη βάση για τους κβαντικούς αλγορίθμους που αναπτύξαμε.

4.1 Βασικές έννοιες κβαντικών υπολογισμών

Σε ένα κλασικό υπολογιστικό σύστημα, η βασική μονάδα πληροφορίας είναι το bit. Ένα bit μπορεί να πάρει δύο διαφορετικές τιμές: 0 ή 1.

Στους κβαντικούς υπολογιστές (και στους αντίστοιχους κβαντικούς υπολογισμούς) η βασική μονάδα πληροφορίας είναι το qubit. Το qubit έχει (όπως και το κλασικό bit) δύο βασικές καταστάσεις που συμβολίζονται με $|0>$ και $|1>$. Οι καταστάσεις αυτές αντιστοιχούν στις καταστάσεις 0 και 1 του κλασικού bit. Ένα qubit όμως μπορεί να βρίσκεται και ταυτόχρονα στις δύο αυτές καταστάσεις. Αυτή είναι και η θεμελιώδης διαφορά του qubit με το bit.

Γενικότερα ένα κβαντικό σύστημα που απεικονίζεται από ένα qubit μπορεί να βρίσκεται σε άπειρες διαφορετικές καταστάσεις (παρόλο που οι βασικές καταστάσεις είναι μόνο δύο). Σύμφωνα με τις αρχές της κβαντομηχανικής, η κατάσταση ενός κβαντικού φυσικού συστήματος δύο καταστάσεων παριστάνεται με ένα διάνυσμα σε ένα ιδιαίτερο διανυσματικό χώρο που ονομάζεται χώρος Hilbert και είναι ένας μιγαδικός διανυσματικός χώρος. Η κατάσταση ενός κβαντικού συστήματος περιγράφεται από ένα διάνυσμα κατάστασης της μορφής: $|R>= a|0> +b|1>$. Οι συντελεστές a, b ορίζουν πλάτη πιθανότητας και το τετράγωνο του κάθε συντελεστή δίνει την πιθανότητα το qubit που απεικονίζει το παραπάνω κβαντικό σύστημα να είναι στην κατάσταση $|0>$ και $|1>$ αντίστοιχα. Προφανώς πρέπει να ισχύει: $a^2+b^2 = 1$. Γενικότερα για την αναπαράσταση των διανυσμάτων κατάστασης ενός κβαντικού συστήματος χρησιμοποιείται η αναπαράσταση με διανύσματα bra και ket. Τα διανύσματα ket (που συμβολίζονται με $|>$) μπορούν να γραφούν ως πίνακες σε μία στήλη, που στην περίπτωση των κβαντικών συστημάτων δύο καταστάσεων έχουν δύο στοιχεία. Το διάνυσμα bra, από την άλλη μεριά, συμβολίζεται με $<|$ και προκύπτει από τον πίνακα που αντιστοιχεί στο διάνυσμα ket με τη μετατροπή της στήλης σε γραμμή και με την αντικατάσταση των στοιχείων από τα μιγαδικά συζυγή τους.

Έτσι το παραπάνω qubit θα γραφτεί με τη αναπαράσταση ket: $|0>= \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1>= \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ και άρα: $|R>= a|0> +b|1>= a \begin{bmatrix} 1 \\ 0 \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$, και με την αναπαράσταση bra: $<0| = \begin{bmatrix} 1 & 0 \end{bmatrix}, <1| = \begin{bmatrix} 0 & 1 \end{bmatrix}$ και άρα: $<R| = a^* <0| + b^* <1| = a^* \begin{bmatrix} 1 & 0 \end{bmatrix} + b^* \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} a^* & b^* \end{bmatrix}$ Γενικά, όπως και θα δούμε και στη συνέχεια, η χρήση των πινάκων διευκολύνει ιδιαίτερα τους υπολογισμούς και θα χρησιμοποιηθεί εκτενώς.

Επίσης, το εσωτερικό γινόμενο δύο καταστάσεων $|a>= k|0> +l|1>$ και $|b>= m|0> +n|1>$ είναι ένας αριθμός και συμβολίζεται με $<a|b>$, δηλαδή είναι το γινόμενο του bra της πρώτης κατάστασης επί το ket της δεύτερης. Με μορφή πινάκων το εσωτερικό γινόμενο γράφεται ως εξής:

$$<a|b>= \begin{bmatrix} k^* & l^* \end{bmatrix} \begin{bmatrix} m \\ n \end{bmatrix} = (k^*m + l^*n).$$

Όταν το εσωτερικό γινόμενο δύο καταστάσεων είναι μηδέν, τότε οι δύο καταστάσεις ονομάζονται ορθογώνιες. Όλες οι βασικές καταστάσεις είναι ορθογώνιες μεταξύ τους. Το γινόμενο bra επί ket της ίδιας βασικής κατάστασης είναι ίσο με τη μονάδα.

Σε αντίθεση με το εσωτερικό γινόμενο δύο καταστάσεων που είναι αριθμός, το εξωτερικό γινόμενο είναι ένας πίνακας. Το εξωτερικό γινόμενο των καταστάσεων $|a>= k|0> +l|1>$ και $|b>= m|0> +n|1>$ συμβολίζεται με $|a><b|$ και δίνεται από τη σχέση:

$$|a><b| = \begin{bmatrix} k \\ l \end{bmatrix} \begin{bmatrix} m^* & n^* \end{bmatrix} = \begin{bmatrix} km^* & kn^* \\ lm^* & ln^* \end{bmatrix}.$$

Τα παραπάνω συνοψίζονται στον επόμενο ορισμό.

Ορισμός 33 *Έστω ότι θεωρούμε ότι* $\{|0>, |1>\}$ *είναι η ορθοκανονική βάση του διδιάστατου χώρου Hilbert. Ένα qubit (*$|q>$*) είναι ένα κανονικοποιημένο διάνυσμα στο χώρο Hilbert δύο διαστάσεων.*

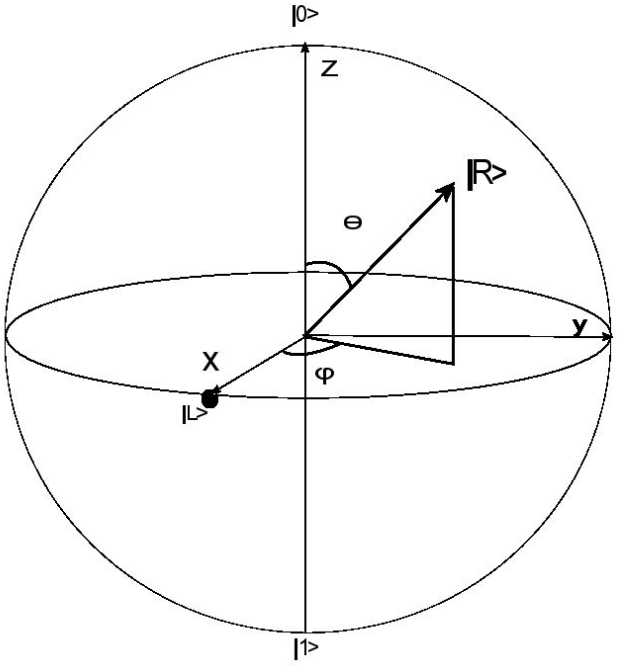
$$|q>= a|0> +b|1>= a \begin{bmatrix} 1 \\ 0 \end{bmatrix}, +b \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$$

όπου $|a|^2 + |b|^2 = 1$.

Από τα παραπάνω είναι προφανές ότι ένα κβαντικό σύστημα δεν είναι ντετερμινιστικό. Δηλαδή δεν μπορούμε με βεβαιότητα (στις περισσότερες περιπτώσεις) να προβλέψουμε σε ποια πραγματική κατάσταση βρίσκεται το σύστημα. Το κβαντικό σύστημα θα καταλήξει σε μια από τις βασικές του καταστάσεις όταν επιχειρήσουμε να μετρήσουμε την κατάσταση του (όταν δηλαδή θα προσπαθήσουμε να επέμβουμε σε αυτό).

4.1.1 Κβαντική Υπέρθεση

Συνοψίζοντας τα προηγούμενα, ένα κβαντικό σύστημα που εκφράζεται από ένα qubit μπορεί να βρίσκεται ταυτόχρονα και στις δύο βασικές του καταστάσεις. Αυτό το φαινόμενο ονομάζεται κβαντική υπέρθεση (quantum superposition) και αποτελεί ένα από τα πιο θεμελιώδη φαινόμενα της κβαντομηχανικής. Στην ουσία αυτό

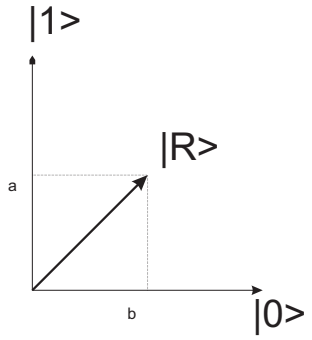


Σχήμα 4.1: Η κατάσταση ενός τυχαίου qubit $|R>$ απεικονιζόμενη σε σε μια σφαίρα Bloch. θ είναι η γωνία με τον άξονα z και ϕ η γωνία της προβολής του $|R>$ στο επίπεδο xy με τον άξονα x. Το $|L>$ είναι το qubit: $(|0>+|1>)/2^{1/2}$.

το φαινόμενο καθιστά δυνατή την ικανότητα που έχουν οι κβαντικοί υπολογιστές για μαζική παραλληλία στους υπολογισμούς. Η πιθανότητα ένα qubit να βρίσκεται στην κατάσταση $|0>$ (δηλαδή όταν θα κάνουμε τη μέτρηση να το βρούμε στην κατάσταση $|0>$) είναι a^2. Αντίστοιχα η πιθανότητα να βρίσκεται στην κατάσταση $|1>$ (δηλαδή όταν θα κάνουμε τη μέτρηση να το βρούμε στην κατάσταση $|1>$) είναι b^2. Όταν $a^2, b^2 \neq 0$ τότε το κβαντικό μας σύστημα λέμε ότι βρίσκεται σε κατάσταση υπέρθεσης (superposition state). Όταν το σύστημα δεν βρίσκεται σε κατάσταση υπέρθεσης τότε μπορούμε με απόλυτη βεβαιότητα να προβλέψουμε σε ποια από τις δύο βασικές του καταστάσεις βρίσκεται.

Εν γένει οι συντελεστές a, b είναι μιγαδικοί αριθμοί για το λόγο αυτό ένα διάνυσμα κατάστασης απεικονίζεται σε μια σφαίρα Bloch. Αν θεωρήσουμε ένα qubit της μορφής: $|R>= e^{i\gamma}[\cos\frac{\theta}{2}|0> + e^{i\phi}\sin\frac{\theta}{2}|1>] = a|0> + b|1>$ τότε η απεικόνισή του σε μια σφαίρα Bloch (έχει ακτίνα ίση με 1) φαίνεται στην εικόνα 4.1. Στην απεικόνιση αυτή $e^{i\gamma}$ είναι μια γενική διαφορά φάσης η οποία δεν είναι παρατηρήσιμη και συνήθως την αγνοούμε.

Πολλές φορές όμως, για λόγους απλότητας, χρησιμοποιούμε διδιάστατη απει-



Σχήμα 4.2: Διδιάστατη απεικόνιση ενός qubit.

κόνιση όπως στην εικόνα 4.2. Στην περίπτωση αυτή οι συντελεστές a, b θεωρούνται ως πραγματικοί αριθμοί. Άλλωστε αρκετοί από τους κβαντικούς τελεστές (κβαντικές πύλες) δεν ενεργούν καθόλου στη γωνία φάσης , οπότε μπορούμε, συνήθως, να την αγνοούμε.

Βεβαίως, τα παραπάνω μπορούν να γενικευθούν για κβαντικά συστήματα n βασικών καταστάσεων. Στην περίπτωση αυτή η κατάσταση ενός τέτοιου συστήματος θα ορίζεται ως: $|R >= a_1|T_1 > +a_2|T_2 > +... + a_n|T_n >$ όπου οι καταστάσεις $|T_i >$ για $i = 1, \ldots, n$ ορίζουν ορδομοναδιαίο σύστημα και είναι ανεξάρτητες μεταξύ τους. Επιπλέον θα ισχύει: $a_1^2 + a_2^2 + \ldots + a_n^2 = 1$. Ο χώρος Hilbert που απαιτείται για να απεικονιστεί ένα τέτοιο σύστημα είναι $2n$ διαστάσεων. Όπως και στα κλασικά υπολογιστικά συστήματα, έτσι και εδώ, μπορούμε να ορίσουμε κβαντικούς καταχωρητές οι οποίοι μπορούν να αποτελούνται από n qubits. Ένας κβαντικός καταχωρητής (όπως και ένας κλασικός) μπορεί να απεικονίσει 2^n διαφορετικούς αριθμούς. Όμως ένας κβαντικούς καταχωρητής που βρίσκεται σε υπέρθεση μπορεί να απεικονίσει όλους αυτούς τους αριθμούς ταυτόχρονα.

Κάτι τέτοιο μοιάζει πολύ εντυπωσιακό, αλλά τα πράγματα δεν είναι τόσο απλά. Ένας κβαντικός καταχωρητής μπορεί μεν να περιέχει πολλές καταστάσεις ταυτόχρονα, αλλά αυτό το πλήθος δεν είναι άμεσα προσβάσιμο σε εμάς. Μόλις επιχειρήσει κάποιος να μετρήσει αυτόν τον καταχωρητή αυτό που θα πάρει θα είναι μία μόνο τιμή, και όχι όλο το πλήθος το τιμών που περιείχε ο καταχωρητής. Ακόμα χειρότερα, αν επαναλάβουμε ακριβώς τη διαδικασία με την οποία φέραμε σε υπέρθεση τον καταχωρητή πιθανότητα πραγματοποιώντας πάλι μια μέτρηση να πάρουμε σαν αποτέλεσμα μια διαφορετική τιμή. Γενικά, μόλις πραγματοποιείται μια μέτρηση της φυσικής ποσότητας που περιγράφει την κβαντική κατάσταση του συστήματος, τότε η υπέρθεση στην οποία μπορεί να βρίσκεται καταρρέει σε μια μοναδική τιμή με πιθανότητα που καθορίζεται από το τετράγωνο του πλάτους που

είχε αυτή η κατάσταση στο διάνυσμα που περιέγραφε τον καταχωρητή. Με άλλα λόγια, μια μέτρηση καταστρέφει την υπέρθεση και ο καταχωρητής ”κλειδώνει” σε μια μοναδική κατάσταση-τιμή.

4.1.2 Συνεκτικότητα

Οι έννοιες της συνεκτικότητας και της μη συνεκτικότητας (coherence - decoherence) είναι στενά συνδεδεμένες με την έννοια της κβαντικής υπέρθεσης. Ένα κβαντικό σύστημα λέγεται ότι είναι συνεκτικό αν βρίσκεται σε γραμμική υπέρθεση των βασικών του καταστάσεων. Αν ένα τέτοιο σύστημα αλληλεπιδράσει με κάποιο τρόπο με το περιβάλλον του τότε η υπέρθεση θα καταστραφεί και θα χαθεί η συνεκτικότητά του. Συνεπώς, η διατήρηση της συνεκτικότητας του σημαίνει ότι το σύστημα βρίσκεται σε υπέρθεση και δεν είναι δυνατόν να γνωρίζουμε με σιγουριά την κατάστασή του.

4.1.3 Κβαντική Διεμπλοκή

Αντίστοιχα με την υπέρθεση, υπάρχει και ένα άλλο ενδιαφέρον και εκ πρώτης όψεως παράδοξο φαινόμενο, το φαινόμενο της κβαντικής διεμπλοκής (entanglement). Το φαινόμενο αυτό μπορεί να εμφανιστεί σε ένα σύστημα που αποτελείται από περισσότερα από 1 qubits. Πιο συγκεκριμένα, είναι μια πιθανή ιδιότητα που μπορεί να αποκτήσει μια κβαντική κατάσταση ενός συστήματος με περισσότερα από ένα στοιχεία (για λόγους απλότητας έστω qubits) κατά την οποία οι κβαντικές καταστάσεις των στοιχείων αυτών συνδέονται μεταξύ τους με τέτοιο τρόπο ώστε είναι πλέον αδύνατο να περιγραφεί το ένα στοιχείο χωρίς να λάβουμε υπόψη τα υπόλοιπα διεμπλεκόμενα στοιχεία, ασχέτως από την απόσταση που μπορεί να τα χωρίζει. Η κβαντική διεμπλοκή έχει τις ρίζες της σε ένα άρθρο των Albert Einstein, Boris Podolsky και Nathan Rosen, που δημοσιεύτηκε το 1935. Στόχος του άρθρου ήταν να αποδειχθεί ότι η κβαντική μηχανική δεν ήταν μια πλήρης φυσική θεωρία, αλλά ότι από την περιγραφή που προσφέρει για τη φύση λείπουν κάποιες παράμετροι που ονομάστηκαν ”*κρυμμενες παράμετροι*”. Στο άρθρο τους επινόησαν ένα θεωρητικό πείραμα κατά το οποίο δυο κβαντικά συστήματα αφού αλληλεπιδράσουν και έρθουν σε διεμπλοκή, απομακρύνονται το ένα από το άλλο. Η διεμπλοκή στην οποία βρίσκονται τα δύο συστήματα ορίζει ότι βρίσκονται συνδεδεμένα μεταξύ τους με έναν άγνωστο μη κλασσικό τρόπο. Σαν αποτέλεσμα, η μέτρηση μιας φυσικής ποσότητας του ενός καθορίζει το αποτέλεσμα της μέτρησης της ίδιας ποσότητας του άλλου. Το παραπάνω νοητικό πείραμα είναι γνωστό και σαν παράδοξο EPR από

τα αρχικά των τριών επιστημόνων και προκάλεσε μεγάλες διαμάχες. Για να εξηγηθεί το φαινόμενο έγινε ο ισχυρισμός ότι θα πρέπει να υπήρχαν κάποιες κρυμμένες μεταβλητές που θα έπαιρναν τιμή την ώρα που δημιουργούνταν η διεμπλοκή. Έτσι το διεμπλεγμένο ζεύγος εμφανιζόταν ότι διέθετε ένα κρυμμένο κανάλι επικοινωνίας το οποίο θα αναλάμβανε την ενημέρωση του ενός συστήματος όταν στο άλλο γινόταν μια μέτρηση ώστε να καταρρεύσει και αυτό στην κατάλληλη κατάσταση στιγμιαία, ασχέτως από την απόσταση που τα χώριζε. Το παράδοξο αυτό καταρρίφθηκε από τον Bell [40] ο οποίος ανέδειξε κάποιες αντιφάσεις στην θεώρηση του EPR. Όπως και να έχει η κβαντική διεμπλοκή αποτελεί την πιο αινιγματική πλευρά της κβαντικής μηχανικής γιατί ενώ έχει επιβεβαιωθεί θεωρητικά και πειραματικά θέτει σε πρώτη ανάγνωση σοβαρά επιστημονικά και φιλοσοφικά ερωτήματα. Η έρευνα στο αντικείμενο είναι εξαιρετικά ενεργή αφού όπως θα διαπιστώσουμε ο αποδοτικός χειρισμός αυτού του φαινομένου μας επιτρέπει να χειριστούμε την εγγενή ικανότητα για παραλληλια των κβαντικών συστημάτων.

Για τους κβαντικούς υπολογιστές, η κβαντική διεμπλοκή είναι ένας φυσικός πόρος, που μπορούμε να χρησιμοποιήσουμε για να εκτελέσουμε κβαντικούς υπολογισμούς και να αναπτύξουμε κβαντικούς αλγορίθμους. Η κατανόηση της φυσικής πίσω από αυτό το φαινόμενο ξεφεύγει από τους σκοπούς αυτής της διατριβής, αφού μας αρκεί να μάθουμε με ποιο τρόπο μπορούμε να τη χρησιμοποιούμε και να τη παράγουμε.

Το παρακάτω παράδειγμα θα αναδείξει τον τρόπο που παράγουμε και χρησιμοποιούμε το φαινόμενο της κβαντικής διεμπλοκής.

***Παράδειγμα* 35** *Έστω ένας κβαντικός καταχωρητής που αποτελείται από δύο qubits. Προφανώς υπάρχουν τέσσερις βασικές καταστάσεις για τον παραπάνω καταχωρητή:* $|00>, |01>, |10>, |11>$. *Οι καταστάσεις αυτές αντιστοιχούν σε κάθε δυνατό συνδυασμό των βασικών καταστάσεων των δύο qubits του καταχωρητή. Έστω ότι ο καταχωρητής αυτός έχει το παρακάτω διάνυσμα κατάστασης:* $\frac{\sqrt{2}}{2}|00> + \frac{\sqrt{2}}{2}|11>$. *Αυτό σημαίνει ότι ο παραπάνω καταχωρητής μπορεί να βρίσκεται στις καταστάσεις* $|00>, |11>$ *με ίδια πιθανότητα 50%. Στην περίπτωση αυτή τα δύο qubits του καταχωρητή είναι σε κατάσταση κβαντικής διεμπλοκής, διότι δεν μπορούμε να μετρήσουμε την κατάσταση του ενός, χωρίς να επηρεάσουμε και την κατάσταση του άλλου. Πράγματι, αν μετρήσουμε το πρώτο qubit, τότε θα το βρούμε με ίση πιθανότητα είτε στην κατάσταση* $|0>$ *είτε στην κατάσταση* $|1>$. *Όμως στην πρώτη περίπτωση και το δεύτερο qubit θα βρεθεί, σίγουρα, στην κατάσταση* $|0>$ *ενώ στην δεύτερη περίπτωση στην κατάσταση* $|1>$. *Δηλαδή στο σύστημά μας η κατάσταση του ενός qubit επηρεάζει άμεσα την κατάσταση του άλλου.*

Ορισμός 34 *Ένας κβαντικός τελεστής (ή κβαντική πύλη) είναι οποιοσδήποτε μαθηματικός μετασχηματισμός μπορεί να ασκηθεί σε ένα κβαντικό σύστημα (που αποτελείται από qubits και ενδεχομένως από κβαντικούς καταχωρητές) και να μετατρέψει, ίσως, την κατάστασή του.*

Δηλαδή οι κβαντικές πύλες είναι τελεστές του χώρου Hilbert και αυτό που κάνουν είναι να περιστρέφουν το διάνυσμα κατάστασης ενός κβαντικού συστήματος μέσα στο χώρο Hilbert. Τους κβαντικούς τελεστές τους περιγράφουμε με τη βοήθεια πινάκων nn όπου n είναι ο αριθμός των εισόδων και των εξόδων του τελεστή.

Βασικές προϋποθέσεις για να είναι ένα τελεστής του χώρου Hilbert κβαντική πύλη, είναι να μη μεταβάλλει το μήκος διανύσματος κατάστασης και να τηρεί τη χρονική συμμετρία των κβαντικών συστημάτων. Οι τελεστές με αυτές τις ιδιότητες ονομάζονται ορθομοναδιαίοι και περιγράφονται από ορθομοναδιαίους πίνακες. Η χρονική συμμετρία σημαίνει ότι αν με μία κβαντική πύλη G που αντιπροσωπεύει τον τελεστή G αλλάξουμε την κατάσταση ενός κβαντικού καταχωρητή από $|q_{R1}>$ σε $|q_{R2}>$, τότε πρέπει να δράσουμε στην κατάσταση $|q_{R2}>$ με την ίδια πύλη για να πάρουμε την κατάσταση $|q_{R1}>$:

$$\begin{aligned} G|q_{R1}> &= |q_{R2}> \\ G|q_{R2}> &= |q_{R1}> \end{aligned} \tag{4.1}$$

Το παραπάνω βέβαια γεγονός υποδηλώνει ότι όλες οι κβαντικές πύλες πρέπει να είναι αντιστρέψιμες. Επίσης αυτό μας δείχνει ότι οποιαδήποτε αντιστρέψιμη πύλη μπορεί να γίνει και κβαντικός τελεστής.

Οι πιο γνωστές κβαντικές πύλες είναι:

- Η κβαντική πύλη αδρανείας (μία είσοδος-έξοδος). Είναι, ουσιαστικά, η αντιστρέψιμη πύλη αδρανείας που παρουσιάστηκε σε άλλο κεφάλαιο. Περιγράφεται από τον πίνακα: $U = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.
- Η κβαντική πύλη αντιστροφής (μία είσοδος-έξοδος). Είναι, ουσιαστικά, η αντιστρέψιμη πύλη αντιστροφής που παρουσιάστηκε σε άλλο κεφάλαιο. Περιγράφεται από τον πίνακα: $U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.
- Η κβαντική πύλη Walsh-Hadamard (μία είσοδος-έξοδος). Η πιο "διάσημη" από τις κβαντικές πύλες. Δρώντας σε ένα σύστημα που βρίσκεται στη βασική κατάσταση 0, το φέρνει σε κατάσταση υπέρθεσης με όλες τις δυνατές

καταστάσεις να μπορούν να παρουσιαστούν ισοπίθανα. Περιγράφεται από τον πίνακα: $U = H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

- Η κβαντική πύλη μετατόπισης φάσης (μία είσοδος-έξοδος). Η πύλη αυτή αλλάζει τη γωνία φάσης φ ενός qubit. Περιγράφεται από τον πίνακα: $U = \begin{bmatrix} 1 & 0 \\ 0 & e^{2i} \end{bmatrix}$.
- Η κβαντική πύλη CNOT (δύο είσοδοι-έξοδοι). Είναι, ουσιαστικά, η αντιστρέψιμη πύλη CNOT που παρουσιάστηκε σε άλλο κεφάλαιο. Περιγράφεται από τον πίνακα: $CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$.
- Η κβαντική πύλη Toffoli (τρεις είσοδοι-έξοδοι). Αποτελεί, ουσιαστικά, την αντιστρέψιμη πύλη Toffoli που παρουσιάστηκε σε άλλο κεφάλαιο. Περιγράφεται από τον πίνακα: $G_{Toffoli} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$.

Ορισμός 35 *Ένας κβαντικός υπολογισμός είναι μια ακολουθία εφαρμογών κβαντικών πυλών σε κάποιο κβαντικό καταχωρητή.*

Συνήθως ένας κβαντικός υπολογισμός τερματίζεται με τη μέτρηση (παρατήρηση) κάποιου από τους κβαντικούς καταχωρητές του συστήματος. Στην περίπτωση αυτή το σύστημα θα ”καταρρεύσει” σε μια από τις βασικές του καταστάσεις.

Οι κβαντικές πύλες δεν είναι πύλες με την κλασσική έννοια από την άποψη ότι δεν υπάρχει ροή πληροφορίας μέσα από αυτές. Αποτελούν δράσεις πάνω σε καταχωρητές που έχουν σαν αποτέλεσμα την μεταβολή της κατάστασης των καταχωρητών αυτών. Εκτός από αυτή τη θεμελιώδη διαφορά με τις κλασσικές πύλες υπάρχουν και άλλοι περιορισμοί. Για παράδειγμα δεν επιτρέπεται η διακλάδωση (fan out) [41]. Αν θεωρήσουμε ότι υπήρχε μια τέτοια πύλη που επέτρεπε την διακλάδωση (ή κλωνοποίηση), δηλαδή την αντιγραφή ενός qubit μπορούμε εύκολα να

αποδείξουμε το άτοπο της υπόθεσης. Ας θεωρήσουμε ότι η πύλη αυτή επιδρά σε 2 qubits εκ των οποίων το ένα βρίσκεται στη κατάσταση $|0>$ και το άλλο στην κατάσταση $|q>$ με τέτοιο τρόπο ώστε να αλλάξει την κατάσταση του πρώτου qubit από $|0>$ σε $|q>$. Επομένως, μετά την επίδραση της πύλης και τα δύο qubits έχουν την ίδια κατάσταση $|q>$. Έστω ότι η πύλη αυτή περιγράφεται από τον ορθοομοναδιαίο τελεστή $\hat{C}$. Επίσης έστω ότι η πύλη αυτή ενεργεί σε δύο qubits $|q>$ και $|b>$ που είναι ορθογώνια μεταξύ τους. Ισχύει ότι $\hat{C}|q,0>=|q,q>$ και $\hat{C}|b,0>=|b,b>$. Θεωρούμε τώρα ένα τρίτο qubit του οποίου η κατάσταση είναι η υπέρθεση των άλλων δύο, δηλαδή $|c>=\frac{1}{\sqrt{2}}(|q>+|b>)$. Αν δράσουμε με το τελεστή και σε αυτό το qubit, θα πάρουμε
$\hat{C}|c,0>=\frac{1}{\sqrt{2}}\hat{C}(|q>+|b>)|0>=\frac{1}{\sqrt{2}}\hat{C}(|q,0>+|b,0>)=$
$\frac{1}{\sqrt{2}}(\hat{C}|q,0>+\hat{C}|b,0>)=\frac{1}{\sqrt{2}}(|q,q>+|b,b>)$. Αλλά πρέπει να ισχύει και
$\hat{C}|c,0>=|c,c>=\frac{1}{\sqrt{2}}(|q>+|b>)\frac{1}{\sqrt{2}}(|q>+|b>)=\frac{1}{2}(|qq>+|qb>+|bq>$
$+|bb>)$. Οι δύο τελευταίες εξισώσεις όμως δεν είναι ίσες με αποτέλεσμα να καταρρίπτεται η υπόθεσή μας.

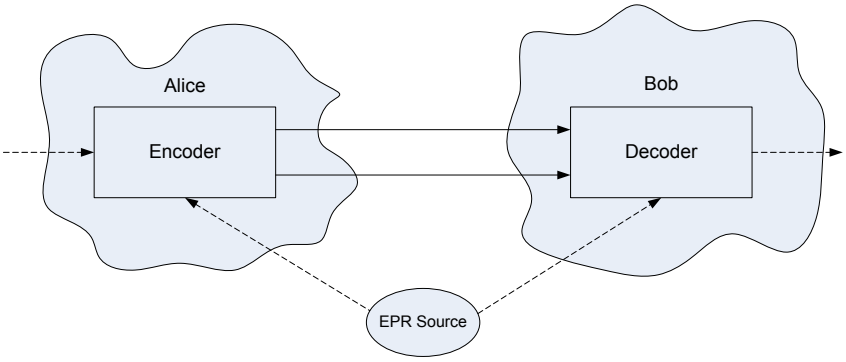
Οι κβαντικοί αλγόριθμοι συνήθως ακολουθούν κάποια βασική στρατηγική. Καταρχήν, υπάρχει ένας καταχωρητής ικανού μεγέθους ώστε να χωρέσει τα δεδομένα, κάποια βοηθητικά qubits ελέγχου και την έξοδό του αλγόριθμου. Ο καταχωρητής τίθεται σε υπέρθεση όσων καταστάσεων απαιτεί το πρόβλημα και στη συνέχεια επιδρούν πάνω του κάποιες κβαντικές πύλες μετασχηματίζοντάς τον. Στο τέλος συνήθως υπάρχει η μέτρηση του αποτελέσματος. Γενικότερος στόχος είναι χρησιμοποιώντας τους μετασχηματισμούς, να χειριστούμε με τέτοιο τρόπο τα πλάτη των υπερτιθέμενων καταστάσεων του καταχωρητή, ώστε πριν την τελική μέτρηση το πλάτος της κατάστασης που αναπαριστά τη λύση του προβλήματος να είναι όσο πιο κοντά στο 1 γίνεται. Από τα παραπάνω φαίνεται ότι οι κβαντικοί αλγόριθμοι είναι εκ φύσεως μη ντετερμινιστικοί (αν και υπάρχουν και ντετερμινιστικοί).

Παρακάτω ακολουθούν ορισμένα παραδείγματα πρακτικών εφαρμογών των κβαντικών πυλών.

4.1.4 Πυκνή Κωδικοποίηση (Dense Coding)

Η τεχνική αυτή χρησιμοποιεί ένα qubit σε συνδυασμό με ένα ζεύγος σε διεμπλοκή (EPR pair) για να κωδικοποιήσει και να μεταδώσει 2 κλασσικά bits. Εφόσον το διεμπλεγμένο ζεύγος, έστω $\psi_0=\frac{1}{\sqrt{2}}(|00>+|11>)$, μπορεί να διαμοιραστεί εκ των προτέρων, στην ουσία πραγματοποιείται η μετάδοση ενός μόνο qubit για να μεταδοθεί πληροφορία 2 κλασσικών bits. Το αποτέλεσμα αυτό είναι θεαματικό αφού όπως έχουμε δει μετά τη μέτρηση ένα qubit περιέχει πληροφορία ενός μόνο

bit. Ας δούμε το σχήμα 4.3.



Σχήμα 4.3: Παράδειγμα πυκνής κωδικοποίησης

Έστω ότι η Alice λαμβάνει 2 κλασσικά bits που κωδικοποιούν τους αριθμούς 0 έως 3. Ανάλογα με τον αριθμό που έχει λάβει, η Alice πραγματοποιεί έναν από τους 4 μετασχηματισμούς στο qubit από το ζεύγος ψ_0 που κατέχει, έστω , , , , όπου I είναι ο μετασχηματισμός αδράνειας, X ο μετασχηματισμός της αντιστροφής (NOT), ο Z η αλλαγή φάσης και ο Y ο συνδυασμός των δύο τελευταίων όπως φαίνεται παρακάτω.

$$I : |0> \Rightarrow |0>, |1> \Rightarrow |1>, I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$X : |0> \Rightarrow |1>, |1> \Rightarrow |0>, I = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y : |0> \Rightarrow -|1>, |1> \Rightarrow |0>, I = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

$$Z : |0> \Rightarrow |0>, |1> \Rightarrow -|1>, I = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Το γεγονός ότι πραγματοποιείται ένας από αυτούς τους μετασχηματισμούς στο ένα qubit του ζεύγους $|\psi_0>$, σημαίνει ότι στο άλλο θα πραγματοποιηθεί ο ταυτοτικός μετασχηματισμός I. Συνεπώς, για τη τιμή 0 έχουμε $|\psi_0> = (I \otimes I)|\psi_0> \Rightarrow |\psi_0> = \frac{1}{\sqrt{2}}(|00> + |11>)$, για τη τιμή 1 έχουμε $|\psi_1> = (X \otimes I)|\psi_0> \Rightarrow |\psi_1> = \frac{1}{\sqrt{2}}(|10> + |01>)$, για τιμή 2 έχουμε $|\psi_2> = (Y \otimes I)|\psi_0> \Rightarrow |\psi_2> = \frac{1}{\sqrt{2}}(-|10> + |01>)$ και για τη τιμή 3 έχουμε $|\psi_3> = (Z \otimes I)|\psi_0> \Rightarrow |\psi_3> = \frac{1}{\sqrt{2}}(|00> - |11>)$. Μετά τον μετασχηματισμό η Alice στέλνει το qubit στον Bob.

Ο Bob εφαρμόζει ένα CNOT μετασχηματισμό στα δύο qubits του διεμπλεγμένου ζεύγους και λαμβάνει:

$|\psi_0> = \frac{1}{\sqrt{2}}(|00> + |10>) = \frac{1}{\sqrt{2}}(|0> + |1>)|0>$

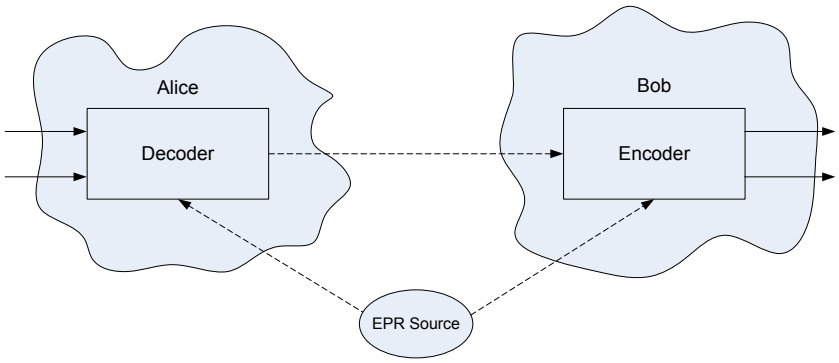
$|\psi_1> = \frac{1}{\sqrt{2}}(|11> + |01>) = \frac{1}{\sqrt{2}}(|1> + |0>)|1>$

$|\psi_2 >= \frac{1}{\sqrt{2}}(-|11 > +|01 >) = \frac{1}{\sqrt{2}}(-|1 > +|0 >)|1 >$
$|\psi_3 >= \frac{1}{\sqrt{2}}(|00 > -|10 >) = \frac{1}{\sqrt{2}}(|0 > -|1 >)|0 >$
Παρατηρούμε ότι τώρα ο Bob μπορεί να μετρήσει το δεύτερο qubit χωρίς να διαταράξει όλη τη κβαντική κατάσταση. Αν μετρήσει 0 τότε η κωδικοποιημένη τιμή θα είναι 0 ή 3, ενώ αν μετρήσει 1 θα είναι 1 ή 2.

Στη συνέχεια ο Bob εφαρμόζει τον μετασχηματισμό Hadamard στο πρώτο qubit και έχουμε:
$|\psi_0 >= \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0 > +|1 >) + \frac{1}{\sqrt{2}}(|0 > -|1 >)) = |0 >$
$|\psi_1 >= \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0 > -|1 >) + \frac{1}{\sqrt{2}}(|0 > +|1 >)) = |0 >$
$|\psi_2 >= \frac{1}{\sqrt{2}}(-\frac{1}{\sqrt{2}}(|0 > -|1 >) + \frac{1}{\sqrt{2}}(|0 > +|1 >)) = |1 >$
$|\psi_3 >= \frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}(|0 > +|1 >) - \frac{1}{\sqrt{2}}(|0 > -|1 >)) = |1 >$
Στο τέλος ο Bob μετράει το τελικό qubit και έτσι μπορεί να ξεχωρίσει μεταξύ των 0 και 3 και 1 και 2.

4.1.5 Τηλεμεταφορά

Σκοπός της τηλεμεταφοράς είναι να μεταφερθεί η κατάσταση ενός σωματιδίου (πχ φωτονίου) χρησιμοποιώντας κλασσικά bits και να ανακατασκευαστεί στον δέκτη. Εφόσον η κβαντική κατάσταση δε μπορεί να αντιγραφεί, η κατάσταση του αρχικού σωματιδίου θα καταστραφεί. Το πείραμα αυτό της τηλεμεταφοράς έχει πραγματοποιηθεί από διάφορες ερευνητικές ομάδες [42, 43, 44, 45, 46, 47, 48]. Σύμφωνα με το σχήμα 4.4 η Alice έχει ένα qubit του οποίου την κατάσταση δεν γνωρίζει και θέλει να τη στείλει στον δέκτη Bob μέσω ενός κλασσικού καναλιού. Έστω η κατάσταση του qubit περιγράφεται από τη σχέση $\phi = a|0 > +b|1 >$. Όπως και με τη περίπτωση της πυκνής κωδικοποίησης, η Alice και ο Bob κατέχουν καθένας ένα qubit από ένα ζεύγος σε διεμπλοκή έστω $\psi_0 = \frac{1}{\sqrt{2}}(|00 > +|11 >)$.



Σχήμα 4.4: Παράδειγμα τηλεμεταφοράς

Η Alice εφαρμόζει το βήμα της αποκωδικοποίησης της προηγούμενης ενότητας στο qubit $|\phi>$ που πρόκειται να μεταδοθεί και στο qubit του διεμπλεγμένου ζεύγους που κατέχει. Αρχικά έχουμε:
$|\phi> \otimes |\psi_0> = \frac{1}{\sqrt{2}}(a|0> \otimes (|00> + |11>) + b|1> (|00> + |11>)) = \frac{1}{sqrt2}(a|000> + a|011> + b|100> + b|111>)$. Τα δύο πρώτα qubits ελέγχονται από την Alice και το τελευταίο από τον Bob. Η Alice εφαρμόζει στη συνέχεια τους μετασχηματισμούς $C_{NOT} \otimes I$ και $H \otimes I \otimes I$ και έχουμε:
$(H \otimes I \otimes I)(C_{NOT} \otimes I)(|\phi> \otimes |\psi_0>) =$
$= (H \otimes I \otimes I)(C_{NOT} \otimes I)\frac{1}{sqrt2}(a|000> + a|011> + b|100> + b|111>) =$
$= (H \otimes I \otimes I)\frac{1}{sqrt2}(a|000> + a|011> + b|110> + b|101>) =$
$= \frac{1}{2}(a(|000> + |011> + |100> + |111>) + b(|010> + |001> - |110> - |101>)) =$
$= \frac{1}{2}(|00> (a|0> + b|1>) + |01> (a|1> + b|0>) + |10> (a|0> - b|1>) + |11> (a|1> - b|0>))$ Η Alice μετρά τα δύο πρώτα qubits για να πάρει ένα από τα $|00>, |01>, |10>, |11>$ με ίση πιθανότητα. Ανάλογα με το αποτέλεσμα της μέτρηση ο Bob θα έχει αντίστοιχα $(a|0> + b|1>), (a|1> + b|0>), (a|0> - b|1>), (a|1> - b|0>)$. Η Alice στέλνει το αποτέλεσμα της μέτρησής της στον Bob χρησιμοποιώντας τα δύο κλασσικά bits.

Να σημειωθεί ότι πραγματοποιώντας αυτή τη μέτρηση, η Alice άλλαξε για πάντα τη κατάσταση του qubit $|\phi>$, την οποία τώρα στέλνει στέλνει τώρα στον Bob. Αυτή η καταστροφή της αρχικής κατάστασης του $|\phi>$ είναι ο λόγος που το πείραμα αυτό δεν παραβιάζει την αρχή της μη αντιγραφής της κβαντικής κατάστασης.

Μόλις ο Bob λάβει τα δύο bits από την Alice γνωρίζει τον τρόπο με το οποίο πρέπει να συγκρίνει την κατάσταση του διεμπλεγμένου qubit που κατέχει με αυτού της Alice. Έτσι λοιπόν, αν έχει λάβει 00 τότε η κατάσταση είναι $(a|0> + b|1>)$ και αποκωδικοποιείται με τον μετασχηματισμό I, αν έχει λάβει 01 τότε η κατάσταση είναι η $(a|1> + b|0>)$ και αποκωδικοποιείται με τον μετασχηματισμό X, αν έχει λάβει 10 τότε η κατάσταση είναι $(a|0> - b|1>)$ και αποκωδικοποιείται με τον μετασχηματισμό Y και τέλος αν έχει λάβει 11 τότε η κατάσταση είναι $(a|1> - b|0>)$ και αποκωδικοποιείται με τον μετασχηματισμό Z. Ο Bob μπορεί λοιπόν πολύ εύκολα να αναδομήσει την αρχική κατάσταση $|\phi>$ της Alice εφαρμόζοντας τον κατάλληλο μετασχηματισμό στο δικό του, διεμπλεγμένο qubit.

4.1.6 Κβαντική Διόρθωση Λαθών

Ένα θεμελιώδες πρόβλημα για την κατασκευή κβαντικών υπολογιστών είναι ανάγκη για απομόνωση της κβαντικής κατάστασης. Οποιαδήποτε αλληλεπίδραση σωματιδίων που ενδεχομένως μπορεί να χρησιμοποιούνται για να αναπαραστήσουν μια κβαντική κατάσταση με το περιβάλλον, διαταράσσει την κβαντική κατάσταση και την κάνει να χάσει την συνεκτικότητά της ή να μετασχηματιστεί με τρόπο μη ορθομοναδιαίο. Παρόλα αυτά, χρησιμοποιώντας αλγόριθμους διόρθωσης λαθών μπορούμε να εξαλείψουμε το πρόβλημα αυτό σε μεγάλο βαθμό.

Σε γενικές γραμμές η κβαντική διόρθωση λαθών μοιάζει με τη κλασσική από την άποψη ότι χρησιμοποιούνται πλεονάζοντα bits για την ανίχνευση και διόρθωση λαθών. Βέβαια, η κβαντική διόρθωση λαθών είναι αρκετά πιο πολύπλοκη αφού έχουμε να κάνουμε με κβαντικές καταστάσεις και όχι δυαδικά δεδομένα. Στην περίπτωση των κβαντικών αλγορίθμων διόρθωσης λαθών θα πρέπει να ανακατασκευαστεί η κβαντική κατάσταση λαμβάνοντας υπόψη την αδυναμία αντιγραφής καταστάσεων κάτι που καθιστά το εγχείρημα πολύ δύσκολο με μια πρώτη ματιά. Αν το εξετάσει κανείς πιο βαθιά θα ανακύψει αρκετές ομοιότητες με τα συμβατικά μοντέλα.

Ας υποθέσουμε λοιπόν ότι τα λάθη προέρχονται από την αλληλεπίδραση μέρους του συνόλου των qubits με το περιβάλλον. Τα πιθανά λάθη θεωρούνται ότι μπορεί να είναι γραμμικοί συνδυασμοί καθόλου λαθών (μετασχηματισμός I), λάθη αντιστροφής qubit (μετασχηματισμός X), λάθη αλλαγής φάσης (μετασχηματισμός Z) και ο συνδυασμός των δύο τελευταίων (μετασχηματισμός Y). Συνεπώς ένα γενικό σφάλμα ενός qubit αναπαρίσταται σαν ένας μετασχηματισμός $e_1 I + e_2 X + e_3 Y + e_4 Z$. Έτσι για μια κατάσταση $|\psi>$ έχουμε: $|\psi> \Rightarrow (e_1 I + e_2 X + e_3 Y + e_4 Z)|\psi> = \sum_i e_i E_i |\psi>$. Στη γενική περίπτωση των κβαντικών καταχωρητών τα πιθανά σφάλματα εκφράζονται σαν γραμμικοί συνδυασμοί ορθομοναδιαίων τελεστών σφάλματος E_i. Τα σφάλματα μπορεί να είναι απλοί συνδυασμοί σφαλμάτων ενός qubit, όπως τανυστικά γινόμενα μετασχηματισμών ενός qubit I, X, Y, Z ή πιο σύνθετοι μετασχηματισμοί πολλών qubits. Σε κάθε περίπτωση, ένα σφάλμα μπορεί να αναπαρασταθεί σαν $\sum_i e_i E_i$, όπου E_i είναι τελεστής σφάλματος και e_i κάποιος συντελεστής.

Ένας κώδικας διόρθωσης λαθών για ένα σύνολο σφαλμάτων E_i αποτελείται από μια αντιστοίχηση C που ενσωματώνει n bits δεδομένων σε $n + k$ bits κώδικα μαζί με ένα τελεστή εξαγωγής συνδρόμου S_C που αντιστοιχίζει τα $n+k$ bits κώδικα σε ένα σύνολο δεικτών διορθώσιμων λαθών E_i τέτοιο ώστε $i = S_C(E_i(C(x)))$. Αν ισχύει $y = E_j(C(x))$ για κάποια άγνωστα αλλά διορθώσιμα σφάλματα, τότε το

σφάλμα $S_C(y)$ μπορεί να χρησιμοποιηθεί για να ανακτήσει μια σωστά κωδικοποιημένη τιμή $C(x)$ (πχ, $E^{-1}_{S_C(y)}(y) = C(x)$).

Ας θεωρήσουμε τώρα την περίπτωση ενός κβαντικού καταχωρητή. Η κατάστασή του μπορεί να είναι σε υπέρθεση των διανυσμάτων βάσης. Επίσης το σφάλμα μπορεί να είναι ένας συνδυασμός τελεστών σφάλματος E_i (που μπορούν να διορθωθούν). Προκύπτει ότι είναι δυνατόν να ανακτήσουμε την αρχική κατάσταση του κβαντικού καταχωρήτη.

Δεδομένου ενός κώδικα διόρθωσης σφαλμάτων C και ενός τελεστή εξαγωγής συνδρόμου S_C, μια κβαντική κατάσταση n-bit, έστω $|\psi>$ μπορεί να κωδικοποιηθεί σε μια κβαντική κατάσταση $n+k$-bit έστω $|\phi>= C|\psi>$. Ας υποθέσουμε ότι η αλληλεπίδραση με το περιβάλλον οδηγεί σε μια κατάσταση σφάλματος έστω $\sum_i e_i E_i|\phi>$ για ένα συνδυασμό διορθώσιμων σφαλμάτων E_i. Η αρχική κωδικοποίηση της κατάστασης $|\phi>$ μπορεί να ανακτηθεί με τον παρακάτω τρόπο.

1. Εφαρμογή του τελεστή εξαγωγής συνδρόμου S_C στην κβαντική κατάσταση (συμπλήρωση με όσα $|0>$ απαιτείται):
   $S_C\,(\sum_i e_i E_i|\phi>(\otimes|0>=$
   $=\sum_i e_i(E_i|\phi> \otimes|i>)$. Λόγω της κβαντικής παραλληλίας έχουμε μια υπέρθεση των διαφορετικών σφαλμάτων καθένα από τα οποία συσχετίζεται με αντίστοιχο δείκτη i.

2. Μέτρηση του $|i>$. Το αποτέλεσμα της μέτρησης καταλήγει σε μια τυχαία τιμή i_0 και η κατάσταση διαμορφώνεται σε $E_{i_0}|\phi, i_0>$.

3. Εφαρμογή του αντίστροφου μετασχηματισμού σφάλματος $E^{-1}_{i_0}$ στα πρώτα $n+k$ qubits του $E_{i_0}|\phi, i_0>$ για να λάβουμε τη σωστή κατάσταση $|\phi>$.

Ας σημειωθεί ότι στο βήμα 2 η υπέρθεση των σφαλμάτων καταρρέει σε ένα μόνο σφάλμα και επομένως στο βήμα 3 απαιτείται μόνο ένας αντίστροφος μετασχηματισμός.

Στην επόμενη ενότητα θα παρουσιαστούν συνοπτικά οι σημαντικότερες προσπάθειες για την πειραματική υλοποίηση κβαντικών κυκλωμάτων.

4.2 Πειραματικές Υλοποιήσεις Κβαντικών Κυκλωμάτων

Όπως μπορεί να διαπιστώσει κανείς ο χώρος Hilbert είναι εξαιρετικά μεγάλος. Για παράδειγμα, αν έχουμε 30 qubits τότε ο χώρος έχει $2^{30} \approx 10^9$ διαστάσεις. Αυτό αν-

τιστοιχεί σε περίπου 10 GB μόνο για το διάνυσμα καταστασης (με 5 bytes / αριθμό). Αν πάμε στα 300 qubits τότε έχουμε $2^{300} \approx 10^{90}$ διαστάσεις κάτι το οποίο είναι εντυπωσιακό αν λάβουμε υπόψη ότι το σύμπαν εκτιμάται ότι έχει 10^{80} περίπου άτομα. Αν λάβουμε τα παραπάνω υπόψη καθώς και το γεγονός ότι τα φαινόμενα της κβαντικής μηχανικής που καθιστούν το κβαντικό μοντέλο υπολογισμού τόσο αποδοτικό απαντώνται σε εξαιρετικά μικρές κλίμακες, είναι λογικό να συμπεράνουμε ότι το να κατασκευαστεί ένα χρήσιμος κβαντικός υπολογιστής θα είναι μια διαδικασία δύσκολη.

Οι κύριες στρατηγικές υλοποίησης των κβαντικών υπολογιστών είναι οι παρακάτω:

- **Παγίδες Ιόντων**. Πρόκειται για την αρχή των κβαντικών υπολογιστών που προτάθηκε αρχικά από τους Cirac και Zoller το 1995, ακολούθησε η υλοποίηση μιας CNOT το ίδιο έτος από τους Wineland et al, η υλοποίηση διεμπλοκής 4 ιόντων το 2000, αλγορίθμων μέχρι 3 qubits το 2004 και διεμπλοκή 8 ιόντων το 2005.

- **NMR**. Έχει υλοποιηθεί ο αλγόριθμος του Shor για τον αριθμό 15 το 2001. Παρόλα αυτά παρουσιάζει αρκετά προβλήματα για πάνω από 10 qubits.

- **Κβαντική Ηλεκτροδυναμική Οπής (Cavity QED)**. Πείραμα από τους Herbert Walther, Benjamin T H Varcoe, Berthold-Georg Englert and Thomas Becker (2006).

- **Γραμμική Οπτική (Linear Optics)**. Πρόκειται για αρκετά παλιά μέθοδο που έχει πετύχει την πρώτη διεμπλοκή καταστάσεων το 1972. Έχει επιτευχθεί διεμπλοκή 5 φωτονίων και επίδειξη πύλη CNOT, ενώ χρησιμοποιείται ήδη στην κβαντική κρυπτογραφία.

- **Κβαντικά Κυκλώματα Στερεής Κατάστασης**. Περιλαμβάνει τις κβαντικές κηλίδες (quantum dots) και θεωρείται αρκετά υποσχόμενη τεχνολογία ως προς τη σταθερότητα και την επεκτασιμότητα σε αριθμό qubits. Βέβαια υπάρχουν αρκετά θέμα ως προς τις παρεμβολές του περιβάλλοντος. Τελευταία υπάρχουν πολλά υποσχόμενες προσπάθειες.

- **Υπεραγώγιμα Κβαντικά Κυκλώματα**. Πρόκειται για υπεραγώγιμα κυκλώματα όπου επιχειρείται να κβαντική διεμπλοκή και υπέρθεση.

- **Τοπολογικοί Κβαντικοί Υπολογιστές**. Επιχειρείται να βρεθεί κατάλληλη τοπολογία για τα κυκλώματα ώστε να περιοριστεί ο αριθμός σφαλμάτων. Γί-

νεται χρήση ανιόντων, δηλαδή σωματιδίων που πρακτικά περιορίζουν τους βαθμούς ελευθερίας των κβαντικών συστημάτων στις 2 διαστάσεις και επομένως των σφαλμάτων.

Με τη χρήση των παραπάνω τεχνικών έχουν υλοποιηθεί και δοκιμαστεί γνωστοί κβαντικοί αλγόριθμοι που θα αναλυθούν παρακάτω όπως ο αλγόριθμος Deutsch-Jozsa, του Shor, το πείραμα της τηλεμεταφοράς, η ανίχνευση και διόρθωση λαθών κ.α..

Υπάρχουν συγκεκριμένα κριτήρια για να αξιολογηθεί μια πειραματική προσπάθεια στο πεδίο των κβαντικών υπολογιστών. Αυτά τα κριτήρια είναι γνωστά ως κριτήρια DiVincenzo [49] και σύμφωνα με αυτά ένας κβαντικός υπολογιστής πρέπει να πληρεί τα ακόλουθα:

1. Να είναι ένα φυσικό, καλά κλιμακούμενο σύστημα με επαρκώς καθορισμένα qubits.

2. Να έχει την δυνατότητα να αρχικοποιεί τα qubits.

3. Να έχει χρόνο συνεκτικότητας πολύ μεγαλύτερο από το χρόνο λειτουργίας.

4. Να έχει ένα πλήρες - παγκόσμιο σύνολο κβαντικών πυλών ενός και δύο qubits.

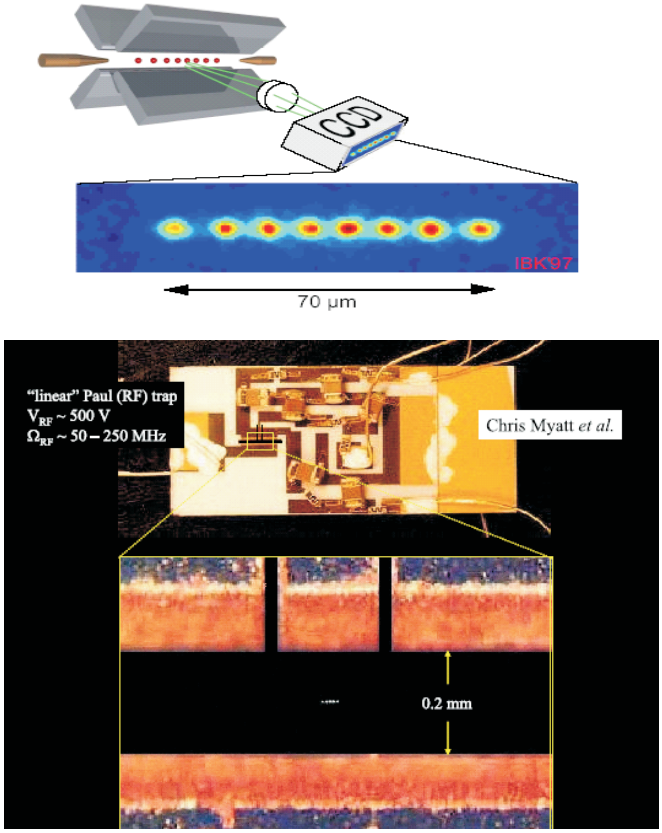
5. Να έχει τη δυνατότητα να μετατρέπει στατικά qubits σε μη στατικά και αντίστροφα.

6. Να έχει τη δυνατότητα να μεταδίδει με αξιοπιστία μη στατικά qubits μεταξύ καθορισμένων τοποθεσιών.

Παρακάτω θα αναφερθούμε σε μερικές από τις παραπάνω πειραματικές προσεγγίσεις έχοντας σαν γνώμονα την εκπλήρωση των κριτηρίων DiVincenzo.

4.2.1 Παγίδες Ιόντων

Οι παγίδες ιόντων (σχήμα 4.5) αποθηκεύουν τα qubits σαν εσωτερικές ενεργειακές στάθμες των ιόντων και οδηγούνται με παλμούς lazer. Η επέκταση γίνεται είτε με την αποθήκευση περισσότερων ιόντων στη παγίδα με γραμμικό τρόπο είτε με διαμερισμό της παγίδας και μετακίνηση των ιόντων. Γενικά απαιτείται κενό και πολύ χαμηλές θερμοκρασίες. Η αρχικοποίηση γίνεται μέσω της τεχνικής της οπτικής αντλίας. Ο μέγιστος χρόνος συνεκτικότητας είναι 30 λεπτά ενώ ο τυπικός είναι 1

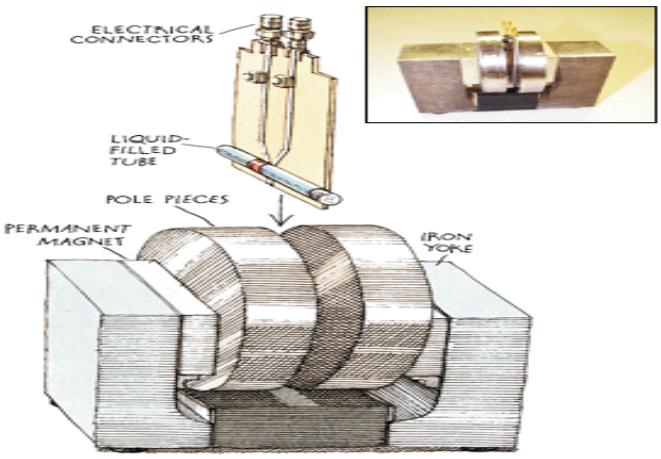


Σχήμα 4.5: Παγίδες Ιόντων.

msec λόγω του θορύβου από το μαγνητικό πεδίο. Έχουν υλοποιηθεί παγκόσμιες πύλες του ενός και των δυο qubits αν και οι τελευταίες υλοποιούνται δύσκολα. Τέλος οι μετρήσεις γίνονται με τη οπτικές μεθόδους.

4.2.2 Nuclear Magnetic Resonance (NMR)

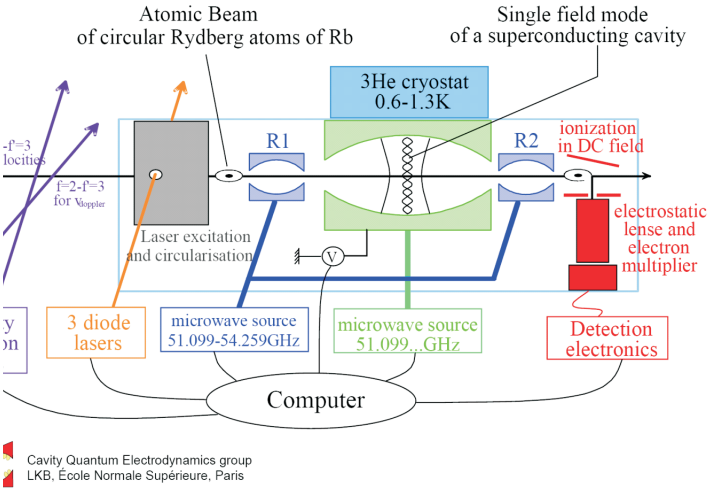
Πρόκειται για μια από τις πιο παλιές και ανεπτυγμένες μεθόδους. Πληροφορία αποθηκεύεται σε μια (μακροσκοπική) ποσότητα σωματιδίων (συνήθως κάποιο υγρό) σαν η μέση κατάσταση του spin των ατόμων. Μαγνητικά πεδία πραγματοποιούν τόσο τις δράσεις όσο και τις μετρήσεις. Η μέθοδος αυτή δεν κλιμακώνεται καλά (το μετρούμενο σήμα διαιρείται εκθετικά με τον αριθμό των qubits) και υπάρχει σημαντική δυσκολία στην αρχικοποίηση. Χρησιμοποιώντας τεχνικές NMR έχει υλοποιηθεί ο αλγόριθμος του Shor για τον αριθμό 15 στα εργαστήρια της IBM. Σε γενικές γραμμές επιτυγχάνεται πολύ μεγαλύτερος χρόνος συνεκτικότητας σε σχέση με το χρόνο υπολογισμού (1000 sec και 0,01-100 ms αντίστοιχα). Οι πύλες υλοποιούνται με παλμούς στο πεδίο συχνοτήτων. Στο σχήμα 4.6 φαίνεται η



Σχήμα 4.6: NMR.

σχεδιάγραμμα της συσκευής που υλοποιήθηκε στη IBM.

4.2.3 Cavity Quantum Electrodynamics

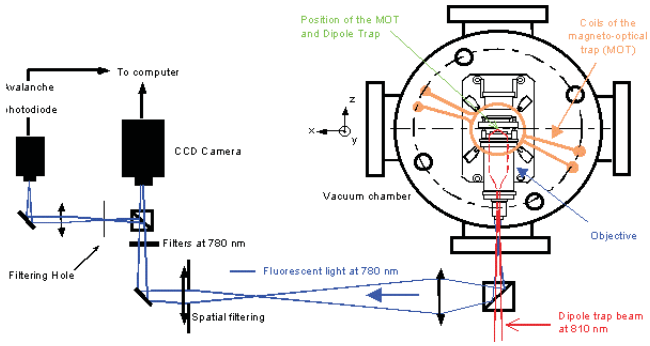


Σχήμα 4.7: Cavity QED.

Σε αυτή την προσέγγιση τα qubits αποθηκεύονται σε άτομα υψηλής ενέργειας. Επίσης φωτόνια που βρίσκονται σε μια υπεραγώγιμη κοιλότητα χρησιμοποιούνται για τη διεμπλοκή των ατόμων. Μοιάζει γενικά με τις παγίδες ιόντων. Η αρχικοποίηση του συστήματος γίνεται με οπτικό τρόπο πράγμα όμως που κάνει την κλιμάκωση δύσκολη. Οι τυπικοί χρόνοι συνοχής και εκτέλεσης είναι 30 ms και 20μs αντίστοιχα. Έχει κατασκευαστεί πειραματικά μια πύλη αλλαγής φάσης και

έχει επιτευχθεί διεμπλοκή μεταξύ 3 ατόμων. Στο σχήμα 4.7 φαίνεται η αρκετά πολύπλοκη δομή της διάταξης.

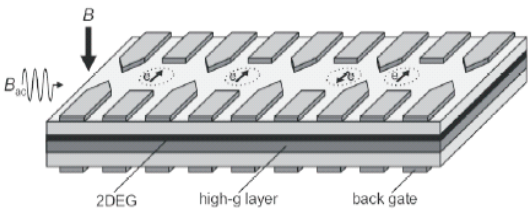
4.2.4 Ουδέτερα Άτομα



Σχήμα 4.8: Neutral Atoms.

Στην πρόκειται για συστήματα παγιδευμένων, με οπτικές μεθόδους, ουδέτερων ατόμων. Έχουν το πλεονέκτημα ότι είναι ουδέτερα και έτσι μπορούν να απομονωθούν σχετικά εύκολα από τις αλληλεπιδράσεις με το περιβάλλον αν και παρουσιάζονται προβλήματα σχετικά με τη διατήρηση της συνεκτικότητας όταν πραγματοποιείται μια δράση. Το πειραματικό αυτό μοντέλο παρέχει καλή κλιμάκωση και εύκολη αρχικοποίηση. Οι δράσεις πραγματοποιούνται με παλμούς ραδιοσυχνοτήτων, ενώ για δύο qbits με ελεγχόμενες συγκρούσεις μεταξύ ατόμων. Στο σχήμα 4.8 φαίνεται μια τέτοια πειραματική διάταξη.

4.2.5 Κβαντικά Κυκλώματα Στερεής Κατάστασης

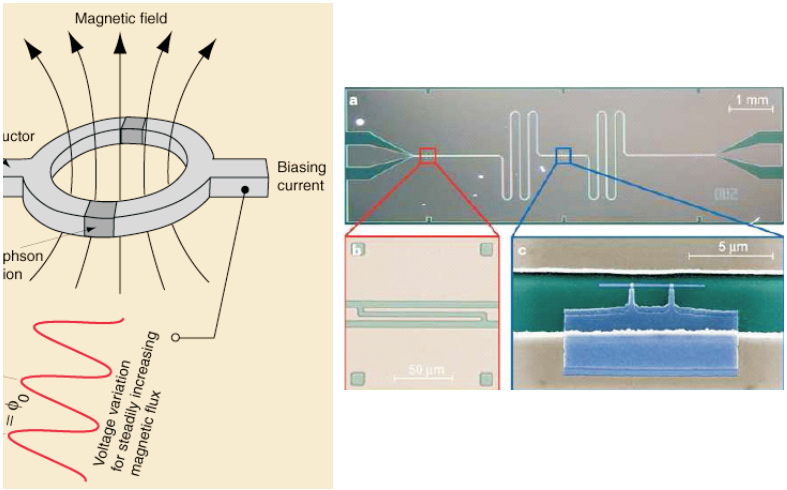


Σχήμα 4.9: Κβαντικά Κυκλώματα Στερεής Κατάστασης.

Σε αυτά τα συστήματα η πληροφορία κωδικοποιείται σαν το spin ενός ηλεκτρονίου που βρίσκεται σε μια κβαντική οπή (quantum dot). Οι υπολογισμοί γίνονται με την εφαρμογή ακτινοβολίας. Ο χρόνος συνοχής / υπολογισμού είναι αρκετά

μεγάλος (100 μs / 1 ns) και το σύστημα παρουσιάζει αρκετά καλή δυνατότητα κλιμάκωσης.

4.2.6 Υπεραγώγιμα qubits



Σχήμα 4.10: Υπεραγώγιμα qubits.

Η τεχνική αυτή βασίζεται στις διασταυρώσεις Josephson που πρακτικά είναι διηλεκτρικά φράγματα τοποθετημένα ανάμεσα σε υπεραγώγιμα υλικά (σχήμα 4.10). Τα qubits μπορούν να εκφραστούν σαν την κατεύθυνση του ρεύματος στον δακτύλιο. Η αρχικοποίηση γίνεται μέσω της μέτρησης, ενώ οι λειτουργίες ενός qubit γίνονται με μικροκύματα και δύο qubit με σύζευξη μέσω LC κυκλωμάτων.

Παρακάτω θα μελετήσουμε τους θεμελιώδεις κβαντικούς αλγόριθμους που αποτελούν τις βάσεις για τους κβαντικούς υπολογιστές, δίνοντας βάση στον αλγόριθμο του Grover που αποτελεί και το θεμέλιο των αλγορίθμων που προτείνονται, ώστε να αναδειχθεί επαρκώς ο ιδιαίτερος τρόπος λειτουργίας των κβαντικών υπολογιστών.

4.3 Ο αλγόριθμος των Deutsch-Jozsa

Ο αλγόριθμος αυτός προτάθηκε από τους David Deutsch και Richard Jozsa το 1992 [50]. Αποτελεί ένα από τα πρώτα παραδείγματα κβαντικών αλγορίθμων, που αναδεικνύει την μεγαλύτερη αποδοτικότητα τους σε σχέση με τους αντίστοιχους συμβατικούς, κάνοντας χρήση κβαντικών φαινομένων όπως η διεμπλοκή και η υπέρθεση.

Το πρόβλημα που καλείται να αντιμετωπίσει ο αλγόριθμος Deutsch-Jozsa έχει ως εξής. Θεωρούμε ότι έχουμε ένα μαύρο κουτί που εκτελεί υπολογισμούς βάσει μιας συνάρτησης $f(x_1, x_2, \ldots, x_n)$. Το κουτί αυτό παίρνει σαν είσοδο n bits $x_1, x_2, \ldots, x_n$ και επιστρέφει την τιμή $f(x_1, x_2, \ldots, x_n)$. Επίσης γνωρίζουμε ότι η συνάρτηση του μαύρου κουτιού είναι είτε *σταθερή* (επιστρέφοντας 0 ή 1 ανεξάρτητως της εισόδου της) ή *ζυγισμένη* (επιστρέφοντας 0 για τα μισά διανύσματα εισόδου και 1 για τα υπόλοιπα μισά). Το ζητούμενο είναι να προσδιοριστεί αν η συνάρτηση f είναι *σταθερή* ή *ζυγισμένη*.

Ένας συμβατικός αλγόριθμος θα χρειαστεί στη χειρότερη περίπτωση 2^{n-1} εκτιμήσεις της συνάρτησης. Αν χρησιμοποιηθούν πιθανοτικοί συμβατικοί αλγόριθμοι είναι δυνατόν η εκτίμηση να γίνει σε σταθερό αριθμό βημάτων, όμως δεν θα θα είμαστε σίγουροι για το αποτέλεσμα. Ο αλγόριθμος Deutsch-Jozsa μπορεί καταλήξει στο επιθυμητό αποτέλεσμα με μόλις μία εκτίμηση της f.

Τα βήματα του αλγορίθμου έχουν ως εξής. Πρώτα, χρησιμοποιώντας τελεστές Hadamard σε n qbits που το καθένα βρίσκεται αρχικά σε κατάσταση $|0>$ και σε ένα επιπλέον που βρίσκεται σε κατάσταση $|1>$ και θα αποτελέσει και το qbit του αποτελέσματος, λαμβάνουμε σε υπέρθεση όλες τις δυνατές 2^n καταστάσεις για την είσοδο. Για το επόμενο βήμα θεωρούμε μια κβαντική υλοποίηση της συνάρτησης f που πραγματοποιεί την αντιστοίχηση $|X> |y> \rightarrow |X> |f(X) \oplus y>$ (Oracle), όπου X το διάνυσμα εισόδου και y το qbit του αποτελέσματος. Εφαρμόζοντας αυτό, έχουμε στην ουσία στο qbit του αποτελέσματος το XOR άθροισμα όλων των δυνατών καταστάσεων εισόδου με την συνάρτηση f. Αν στη συνέχεια επαναφέρουμε τις n εισόδους με την εφαρμογή μετασχηματισμού Hadamard θα μπορούμε μετρώντας το qbit του αποτελέσματος να προσδιορίσουμε το ζητούμενο. Αν είναι μηδέν τότε η συνάρτηση είναι *σταθερή*, διαφορετικά είναι *ζυγισμένη*. Αυτό μπορεί να γίνει αντιληπτό και από τις παρακάτω εξισώσεις και το σχήμα 4.11 που περιγράφουν τα βήματα του αλγορίθμου.

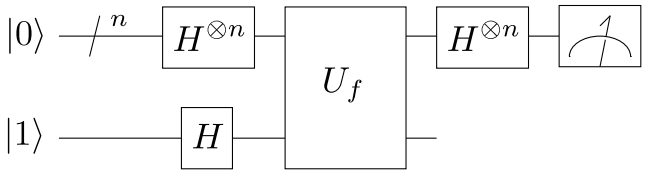
1. Αρχικοποίηση καταχωρητή. $|0>^{\otimes n} |1>$.

2. Εφαρμογή μετασχηματισμού Hadamard στον μεγέθους $n+1$ καταχωρητή. $\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x> (|0> - |1>)$.

3. Εφαρμογή του Oracle. $\frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x> (|f(x)> - |1 \oplus f(x)>)$.

4. Εφαρμογή μετασχηματισμού Hadamard στα πρώτα n του καταχωρητή.
   $\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y> =$
   $= \frac{1}{2^n} \sum_{y=0}^{2^n-1} [\sum_{x=0}^{2^n-1} (-1)^{f(x)} (-1)^{x \cdot y}] |y>$, όπου το $x \cdot y$ είναι το εσωτερικό γινόμενο.

5. Μέτρηση. $|\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|^2$.



Σχήμα 4.11: Διάγραμμα αλγορίθμου Deutsch-Jozsa.

Η επίδοση του παραπάνω αλγορίθμου μοιάζει εντυπωσιακή, αλλά υπάρχουν ορισμένοι περιορισμοί. Καταρχήν, το πρόβλημα που επιλύει δεν είναι ιδιαίτερα σημαντικό και δεν έχει εφαρμογές. Επίσης οι πιθανοτικοί συμβατικοί αλγόριθμοι δίνουν πολύ καλά αποτελέσματα και είναι ίσως πιο ρεαλιστικοί στη χρήση τους από τους ντετερμινιστικούς για το συγκεκριμένο πρόβλημα. Παρόλα αυτά, ο παραπάνω αλγόριθμος είναι μια από τις πρώτες προσπάθειες στο τομέα αυτό και αποτέλεσε πηγή έμπνευσης για άλλους πιο εντυπωσιακούς αλγορίθμους, αποκαλύπτοντας ορισμένες βασικές αρχές της σχεδίασης κβαντικών αλγορίθμων.

4.4 Ο αλγόριθμος του Shor

Ο αλγόριθμος του Shor [38], προτάθηκε από τον Peter Shor για την επίλυση του προβλήματος της παραγοντοποίησης ακέραιων αριθμών. Ο αλγόριθμος αυτός σε ένα κβαντικό υπολογιστή υπολογίζεται σε πολυωνυμικό χρόνο $O((\log N)^3)$, δείχνοντας ότι το πρόβλημα της παραγοντοποίησης ακεραίων ανήκει στην κλάση BQP (Bounded error, Quantum, Polynomial time). Κάτι τέτοιο τον καθιστά εκθετικά πιο γρήγορο από τον καλύτερο αντίστοιχο συμβατικό (τον general number field sieve ή GNFS), που έχει υπο-εκθετική πολυπλοκότητα $O(e^{(\log N)^{1/3}}(\log\log N)^{2/3})$.

Είναι σημαντικός αλγόριθμος διότι μπορεί, θεωρητικά, να χρησιμοποιηθεί για να ”σπάσει” το ευρέως χρησιμοποιούμενο σύστημα κρυπτογράφησης δημόσιου κλειδιού γνωστό και ως RSA. Το RSA βασίζεται στην υπόθεση ότι η παραγοντοποίηση μεγάλων αριθμών είναι υπολογιστικά ανέφικτη. Μέχρι στιγμής, όπως είναι γνωστό, αυτή η υπόθεση είναι έγκυρη για τους κλασικούς υπολογιστές. Κανένας κλασικός αλγόριθμος δεν είναι γνωστό ότι μπορεί να παραγοντοποιήσει σε πολυωνυμικό χρόνο. Ωστόσο, ο αλγόριθμος παραγοντοποίησης του Shor δείχνει ότι η παραγοντοποίηση είναι εξαιρετικά αποδοτική σε ένα κβαντικό υπολογιστή, συνεπώς ένας αρκετά μεγάλος κβαντικός υπολογιστής μπορεί να ”σπάσει” το RSA.

Ο συγκεκριμένος αλγόριθμος αποτέλεσε ένα ισχυρό κίνητρο για το σχεδιασμό και την κατασκευή κβαντικών υπολογιστών, αλλά και για τη μελέτη νέων κβαντικών αλγορίθμων. Στην ουσία αποτελεί ένα σημαντικό ορόσημο στη μέχρι τώρα ιστορία των κβαντικών υπολογιστών.

Το 2001, ο αλγόριθμος του Shor υλοποιήθηκε από μια ομάδα στη IBM, η οποία παραγοντοποίησε το 15 σε 3×5, χρησιμοποιώντας έναν κβαντικό υπολογιστή βασισμένο σε NMR με 7 qubits. Εντούτοις, μερικές αμφιβολίες έχουν εκφραστεί ως προς το εάν το πείραμα αυτό ήταν μια αληθινή επίδειξη του κβαντικού υπολογισμού, δεδομένου ότι δεν παρατηρήθηκε διεμπλοκή. Έκτοτε, διάφορες άλλες ομάδες έχουν εφαρμόσει τον αλγόριθμο του Shor με χρήση φωτονικών qbits, όπου παρατηρήθηκε διεμπλοκή [51].

Ο συγκεκριμένος αλγόριθμος, δεδομένου ενός φυσικού αριθμού (όχι πρώτου προφανώς) N, βρίσκει ένα αριθμό p ανάμεσα στο 1 και το N που διαιρεί τον N. Το πρόβλημα αναλύεται σε δύο μέρη, ένα συμβατικό και ένα κβαντικό:

1. Μια αναγωγή του προβλήματος της παραγοντοποίησης σε πρόβλημα εύρεσης της περιόδου μιας συνάρτησης, κάτι που μπορεί να γίνει σε ένα συμβατικό υπολογιστή.

2. Ένας κβαντικός αλγόριθμος για την επίλυση του προβλήματος εύρεσης της περιόδου μιας συνάρτησης.

Στην παρακάτω ανάλυση θα ασχοληθούμε με το κβαντικό κομμάτι του γενικότερου αλγορίθμου που ορίζεται ως εξής:

Αν δοθεί ένας ακέραιος n να βρεθεί η περίοδος της συνάρτησης $f_{x,a}(x) = a^x(modn)$, όπου a είναι ένας τυχαίος ακέραιος που είναι πρώτος ως προς το n.

Ο κβαντικός αυτός αλγόριθμος ξεκινά με δύο κβαντικούς καταχωρητές. Ο πρώτος θεωρούμε ότι ονομάζεται *reg1* και ο δεύτερος *reg2*. Οι δύο αυτοί καταχωρητές συναποτελούν ένα μεγαλύτερο καταχωρητή που τον ονομάζουμε *reg*. Θεωρούμε ότι η κατάσταση του *reg1* είναι $|\psi_1>$, του *reg2* είναι $|\psi_2>$ ενώ του *reg* είναι $|\psi>$ και ισχύει:
$|\psi>=|\psi_1>|\psi_2>=|\psi_1\psi_2>=|\psi_1,\psi_2>$

Η αρχική κατάσταση του *reg* είναι $|0,0>$. Για να αναλύσουμε ένα ακέραιο αριθμό n σε γινόμενο δύο πρώτων, επιλέγουμε έναν ακέραιο q τέτοιο ώστε

$2n^2 \leq q \leq 3n^2$

Στη συνέχεια, επιλέγουμε ένα αριθμό a τέτοιο ώστε να είναι πρώτος ως προς τον n. Έχοντας φροντίσει να έχουμε κατάλληλο αριθμό qubits για τον *reg1*, τον

φέρνουμε σε κατάσταση υπέρθεσης, ώστε να μπορεί να φιλοξενεί όλες τις δυνατές καταστάσεις από 0 έως $q-1$. Στην ουσία, δημιουργούμε την υπέρθεση όλων αυτών των ακεραίων που θα χρησιμοποιηθούν σαν ανεξάρτητες μεταβλητές εισόδου για την συνάρτηση $f_{x,a}(x) = a^x(modn)$ της οποίας θέλουμε να βρούμε την περίοδο.

Κατόπιν, εκμεταλλευόμενοι την κβαντική παραλλήλια, υπολογίζουμε σε ένα βήμα τις τιμές τις $f(x)$ για κάθε x και τις αποθηκεύουμε σε υπέρθεση στον καταχωρητή *reg2* που ουσιαστικά είναι ο καταχωρητής του αποτελέσματος. Με αυτό το τρόπο οι δύο καταχωρητές βρίσκονται σε κβαντική διεμπλοκή και με αυτόν τον τρόπο μια μέτρηση στον ένα καθορίζει την τιμή του άλλου.

Στο επόμενο βήμα πραγματοποιείται μέτρηση της κατάστασης του *reg2* με αποτέλεσμα να καταρρεύσει σε μία μόνο τιμή. Εφόσον ο *reg2* περιέχει σε υπέρθεση όλες τις τιμές της συνάρτησης, το αποτέλεσμα της μέτρησης θα είναι μια από αυτές τις τιμές, έστω k. Η διαδικασία όμως αυτή κρύβει και κάτι άλλο. Οι καταχωρητές *reg1* και *reg2* βρίσκονται σε διεμπλοκή κάτι που σημαίνει ότι η μέτρηση που πραγματοποιήθηκε θα καθορίσει και την κατάσταση του *reg1*. Άρα και ο *reg1* θα περιέχει μόνο τις τιμές εισόδου x της συνάρτησεις που ανταποκρίνονται στο μετρημένο αποτέλεσμα δηλαδή τιμές για τις οποίες ισχύει:

$$f_{x,a}(x) = a^x(modn) = k$$

Συνεπώς στον *reg1* θα περιέχονται σε υπέρθεση οι αριθμοί $\{x, x+r, x+2r, \ldots\}$ με πλάτη πιθανοτήτων ίσα μεταξύ τους. Όπως μπορεί κανείς εύκολα να αντιληφθεί k είναι η περίοδος της συνάρτησης.

Αν και τα πράγματα φαίνεται ότι έχουν τελειώσει κάπου εδώ, δεν ισχύει κάτι τέτοιο, για τον ίδιο λόγο που τόσο βολικά πήραμε το παραπάνω αποτέλεσμα. Για να εξάγουμε την περίοδο της συνάρτησης χρειαζόμαστε 2 τουλάχιστον μετρήσεις στον *reg1* που θα δώσουν δύο διαδοχικούς αριθμούς που βρίσκονται σε υπέρθεση εκεί, για παράδειγμα τους $x + 2r$ και $x + 3r$. Όμως αν πραγματοποιηθεί μια μέτρηση στον καταχωρήτη *reg1* θα έδινε έναν αριθμό και θα κατέστρεφε παράλληλα την υπέρθεση καθιστώντας την επόμενη μέτρηση πρακτικά άχρηστη, αφού θα παίρναμε τον ίδιο αριθμό. Επομένως το επόμενο στάδιο του αλγόριθμου είναι το πώς θα βρούμε την περίοδο που έχουμε ήδη "κρυμμένη" μέσα στον *reg1* χωρίς να διαταράξουμε την υπέρθεση. Αυτό μπορεί να γίνει με την βοήθεια του κβαντικού μετασχηματισμού Fourier.

Εφαρμόζοντας τον κβαντικό μετασχηματισμό Fourier στα περιεχόμενα του καταχωρητή *reg1*, θα αλλάξουν όπως και στη κλασσική περίπτωση τα πλάτη πιθανοτήτων των περιεχομένων του *reg1*. Πιο συγκεκριμένα, ο καταχωρητής *reg1* θα έχει

κορυφές στα σημεία που είναι ακέραια πολλαπλάσια της αντίστροφης περιόδου $1/r$. Κάτι τέτοιο συμβαίνει γιατί ο κβαντικός μετασχηματισμός Fourier της υπέρθεσης των καταστάσεων του *reg1* που αντιστοιχούν στις τιμές $\{x, x+r, x+2r, \ldots\}$ θα έχει σαν αποτέλεσμα μια νέα υπέρθεση στην οποία όμως τα πλάτη των πιθανοτήτων των καταστάσεων δεν θα είναι πλέον ίδια. Οι πιθανότητες των καταστάσεων που αντιστοιχούν σε ακέραια πολλαπλάσια της αντίστροφης περιόδου $1/r$ θα είναι πολύ μεγαλύτερες από τις υπόλοιπες και, συνεπώς, μια μέτρηση θα δώσει αποτέλεσμα που θα είναι σχεδόν σίγουρα ακέραιο πολλαπλάσιο της αντίστροφης περιόδου. Επαναλαμβάνοντας την όλη διαδικασία αρκέτες φορές (περίπου $\log(q)$), ώστε να βρεθούν αρκετά δείγματα ακεραίων πολλαπλασίων της αντίστροφης περιόδου, μπορούμε να τη υπολογίσουμε ακριβώς.

4.4.1 Τα βήματα του αλγορίθμου

Χρησιμοποιώντας μια πιο συστηματική προσέγγιση περιγράφονται παρακάτω τα βήματα του αλγορίθμου.

Έστω ότι θέλουμε να αναλύσουμε ένα ακέραιο αριθμό n σε γινόμενο 2 πρώτων αριθμών. Για να το πετύχουμε θα υπολογίσουμε τη περίοδο της συνάρτησης $f_{x,a}(x) = a^x(modn)$.

1. Επιλέγεται ένας φυσικός αριθμός q τέτοιος ώστε $2n^2 \leq q \leq 3n^2$.

2. Επιλέγεται τυχαία ένας αριθμός a που είναι πρώτος ως προς τον n.

3. Επιλέγεται ένας κβαντικός καταχωρητής *reg* που αποτελείται από δύο καταχωρητές *reg1* και *reg2* που βρίσκονται στην κατάσταση $|0>$. Η κατάσταση του *reg*, $|\psi>$ είναι:
   $|\psi>=|0,0>$

4. Φέρνουμε τον *reg1* σε κατάσταση υπέρθεσης όλων των βασικών καταστάσεων από 0 έως $q-1$, αφήνοντας τον *reg2* ανεπηρέαστο. Η κατάσταση του *reg* περιγράφεται τώρα από την σχέση:
   $|\psi>=\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x,0>$

5. Υπολογίζεται η τιμή της $f_{x,a}(x)$ για κάθε x (κάνοντας χρήση της κβαντικής παραλληλίας) και τα αποτελέσματα καταγράφονται στον καταχωρητή $reg2$ σε κατάσταση υπέρθεσης. Η κατάσταση του reg περιγράφεται από τη σχέση: $|\psi>=\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x,a^x(modn)>=\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|x,f_{x,a}(x)>$. Οι καταχωρητές βρίσκονται πλέον σε κβαντική διεμπλοκή.

6. Μετράται η κατάσταση του $reg2$. Η μέτρηση δίνει έστω τη τιμή k και ο $reg1$, λόγω διεμπλοκής περιέχει πια μόνο τις τιμές για τις οποίες $f_{x,a}(x) = k$. Οι αριθμοί αυτοί, έστω x' αποτελούν ένα σύνολο που περιγράφεται ώς εξής:
$A = \{x' : a^{x'}(mod n) = k\}$. Συνεπώς η κατάσταση του reg δίνεται πια από την σχέση:
$|\psi >= \frac{1}{\|A\|} \sum_{x' \in A} |x', k >$

7. Ο κβαντικός μετασχηματισμός Fourier δρα στον καταχωρητή $reg1$, αφήνοντας ανεπηρέαστο τον $reg2$. Ο μετασχηματισμός αυτός μετασχηματίζει κάθε κατάσταση $|x' >$ σε μια υπέρθεση καταστάσεων που δίνεται από τη σχέση:
$|x' > \mapsto \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i \frac{x'c}{q}} |c >$
Επομένως ο καταχωρητής reg πλέον περιγράφεται από τη σχέση:
$|\psi >= \frac{1}{\|A\|} \sum_{x' \in A} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i \frac{x'c}{q}} |c, k >$

8. Μετράται ο καταχωρητής $reg1$. Το αποτέλεσμα δίνει μια μόνο τιμή, c', η οποία είναι κάποιο ακέραιο πολλαπλάσιο λ του q/r, όπου r η περίοδος που πρέπει να προσδιοριστεί. Συνεπώς,
$c' = \lambda \frac{q}{r}$

9. Τα βήματα 3 έως 8 επαναλαμβάνονται περίπου $\log(q)$ φορές. Η διαδικασία αυτή προσφέρει αρκετά δείγματα πολλαπλασίων του $1/r$, δηλαδή δίνει τιμές όπως
$\lambda_1/r, \lambda_2/r, \lambda_3/r, \ldots$, όπου λ διάφοροι ακέραιοι, με αποτέλεσμα να είναι δυνατός ο υπολογισμός της περιόδου.

Αφού προσδιοριστεί η περίοδος r, οι δύο πρώτοι αριθμοί που το γινόμενό τους δίνει τον n μπορούν να προσδιοριστούν υπολογίζοντας το μέγιστο κοινό διαιρέτη του n και του $(a^{r/2} - 1)$ και τον μέγιστο κοινό διαιρέτη του n και του $(a^{r/2} + 1)$.

Χάρη σε αυτόν τον αλγόριθμο η Επιστήμη των Υπολογιστών έστρεψε ουσιαστικά το ενδιαφέρον της προς τους κβαντικούς υπολογιστές, βλέποντάς τους πια όχι σαν ασκήσεις επί χάρτου για την επίλυση πρακτικά ανούσιων μαθηματικών προβλήματων, αλλά σαν κάτι που είχε τη δυνατότητα να λύσει υπαρκτά δύσκολα προβλήματα με τάξεις μεγέθους μικρότερη πολυπλοκότητα. Ο αλγόριθμος του Shor είναι εξαιρετικά εντυπωσιακός και ο επόμενος αλγόριθμος, αν και δεν έχει τόσο εντυπωσιακά αποτελέσματα, ωστόσο θέτει τις βάσεις για μια γενικευμένη πλατφόρμα κατασκευής αλγορίθμων κάτι που είναι εξίσου, αν όχι περισσότερο σημαντικό.

4.5 Ο αλγόριθμος του Grover

Ο κβαντικός αλγόριθμος που θα μας απασχολήσει στη συγκεκριμένη διατριβή είναι ο αλγόριθμος του Grover. Η σειρά αλγόριθμων που προτείνουμε βασίζεται σε αυτόν. Στην ενότητα αυτή δίνουμε μια σύντομη περιγραφή του.

Ο Lov Grover με το άρθρο του "Η κβαντική μηχανή μπορεί να μας βοηθήσει να βρούμε μία βελόνα στα άχυρα" [39] απέδειξε ότι ένας κβαντικός υπολογιστής μπορεί να μας βοηθήσει να βρούμε ένα στοιχείο σε μία μη δομημένη βάση δεδομένων N στοιχείων, αν την ερευνήσουμε $\sqrt{N}$ φορές. Η βελτίωση που παρέχει αυτή η μέθοδος είναι ιδιαίτερα σημαντική, γιατί σε έναν κλασσικό υπολογιστή, στην καλύτερη περίπτωση, το στοιχείο μπορεί να βρεθεί στην πρώτη προσπάθεια αλλά στη χειρότερη περίπτωση το στοιχείο μπορεί να βρεθεί μετά από N προσπάθειες. Κατά μέσο όρο όμως γίνονται $N/2$ αναζητήσεις.

Αναλυτικότερα το πρόβλημα που επιλύει ο αλγόριθμος του Grover περιγράφεται ως εξής: Έστω μία μη δομημένη βάση δεδομένων που περιέχει στοιχεία. Κάθε στοιχείο της βάσης δεδομένων έχει έναν αριθμό από το 0 έως το $N-1$. Το στοιχείο που αντιστοιχεί στον αριθμό k συμβολίζεται με x. Χωρίς περιορισμό της γενικότητας μπορούμε να θεωρήσουμε:
$N = 2n - 1$ για $n = 1, 2, 3, \ldots$. (Αν έχουμε λιγότερα στοιχεία μπορούμε να προσθέσουμε εμείς όσα χρειάζονται για να φτάσουμε στον επιθυμητό αριθμό).

Κάθε στοιχείο αντιστοιχείται σε μία από τις βασικές καταστάσεις ενός κβαντικού καταχωρητή που περιλαμβάνει n qubits.

Θεωρούμε επίσης ότι διαθέτουμε ένα σύστημα το οποίο μπορεί να αναγνωρίσει αν κάποιο στοιχείο είναι αυτό που ζητάμε ή όχι. Το σύστημα αυτό ονομάζεται oracle και είναι μία λογική συνάρτηση f. Έτσι αν το στοιχείο που ψάχνουμε είναι το x_i, τότε έχουμε:

$$U = \left\{ \begin{array}{l} 1 \text{ αν } x = x_i \\ 0 \text{ αν } x \neq x_i \end{array} \right\}.$$

Αν και δεν παρουσιάζονται οι πύλες που υλοποιούν το κβαντικό oracle, όταν αυτό δράσει σε έναν κβαντικό καταχωρητή που βρίσκεται στην κατάσταση $|xy>$, τότε: $|xy> = |x> |y> \xrightarrow{O} |x> |f(x) \oplus y>$ όπου το $|y>$ είναι το qubit του oracle.

Κατά την αναζήτηση της βάσης δεδομένων, το qubit του oracle τίθεται στη βασική κατάσταση $|1>$ και στη συνέχεια δρα σε αυτό μία κβαντική πύλη Hadamard, η οποία έχει σαν αποτέλεσμα:
$|1> \xrightarrow{H} \frac{|0>-|1>}{\sqrt{2}}$.

Αν το κβαντικό oracle δράσει σε ένα τυχαίο στοιχείο της μη δομημένης βάσης

δεδομένων που αναπαρίσταται από την κατάσταση του κβαντικού καταχωρητή, το αποτέλεσμα που προκύπτει είναι:

$|x> (\frac{|0>-|1>}{\sqrt{2}}) \rightarrow^0 |x> |f(x) \oplus |\frac{|0>-|1>}{\sqrt{2}}$

Ισοδύναμα η δράση του κβαντικού oracle μπορεί να γραφεί (λόγω της μη μεταβολής του qubit του oracle):

$$|x> (\frac{|0>-|1>}{\sqrt{2}}) = \left\{ \begin{array}{c} |x> (\frac{|0>-|1>}{\sqrt{2}}) \text{ αν x δεν είναι το στοιχείο που ψάχνουμε} \\ -|x> (\frac{|0>-|1>}{\sqrt{2}}) \text{ αν x είναι το στοιχείο που ψάχνουμε} \end{array} \right\}.$$

ή

$$|x>= \left\{ \begin{array}{c} |x> \text{ αν x δεν είναι το στοιχείο που ψάχνουμε} \\ -|x> \text{ αν x είναι το στοιχείο που ψάχνουμε} \end{array} \right\}.$$

Πιο συνοπτικά: $|x> \rightarrow^0 (-1)^{f(x)}|x>$.

Συμπερασματικά, το κβαντικό oracle δρα στις βασικές καταστάσεις $|x>$ που αντιστοιχούν σε στοιχεία της μη δομημένης βάσης δεδομένων και έχει σαν αποτέλεσμα:

- Αν η βασική κατάσταση δεν αντιστοιχεί σε κατάσταση που ψάχνουμε, την αφήνει όπως ήταν.
- Αν η βασική κατάσταση αντιστοιχεί σε κατάσταση που ψάχνουμε, αλλάζει το πρόσημο της.

Το κβαντικό oracle είναι και αυτό ένας τελεστής του χώρου Hilbert. Αν το στοιχείο που ψάχνουμε αντιστοιχεί στην βασική κατάσταση $|x_i>$, ο τελεστής του κβαντικού oracle είναι: $\hat{O} = \hat{I} - 2|x_i X x_i|$, όπου η πράξη X συμβολίζει το τανυστικό γινόμενο.

Για να ερευνήσουμε τη μη δομημένη βάση δεδομένων που περιέχει στοιχεία με έναν κβαντικό υπολογιστή, αντιστοιχίζουμε κάθε ένα από τα στοιχεία με μία από τις βασικές καταστάσεις του κβαντικού καταχωρητή που περιλαμβάνει n qubits. Για να το πετύχουμε αυτό, θέτουμε τον κβαντικό καταχωρητή σε μία κατάσταση $|s>$, η οποία είναι υπέρθεση όλων των βασικών καταστάσεων με το ίδιο πλάτος πιθανότητας:

$$|s>= \frac{1}{\sqrt{N}}|0> + \frac{1}{\sqrt{N}}|1> + \ldots + \frac{1}{\sqrt{N}}|N-1>= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |0> . \qquad (4.2)$$

Ο τελεστής του Grover είναι:

$\hat{G} = -(\hat{I} - 2|sXs|) = 2(sXs)) - \hat{I}$.

Ο αλγόριθμος του Grover είναι μία διαδοχική εφαρμογή των τελεστών $\hat{O}$ και $\hat{G}$ στον κβαντικό καταχωρητή περίπου $[(\pi/4\sqrt{N})] - 0.5$ φορές. Τα βήματα του αλγορίθμου είναι:

1. Θέτουμε όλα τα qubits του κβαντικού καταχωρητή σε $|0\ >$, δηλαδή θέτουμε τον κβαντικό καταχωρητή στην κατάσταση $|000\ldots0\ >$. Στη συνέχεια δρούμε σε κάθε qubit του καταχωρητή με μία πύλη Hadamard και έτσι αυτός μεταβαίνει στην κατάσταση: $|s\ >= \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |x_j\ >$. Η κατάσταση $|s\ >$ είναι η υπέρθεση των βασικών καταστάσεων. Κάθε βασική κατάσταση αντιστοιχείται με ένα στοιχείο της μη δομημένης βάσης δεδομένων και έστω ότι αναζητείται το στοιχείο που αντιστοιχεί στην κατάσταση $|x_i\ >$.

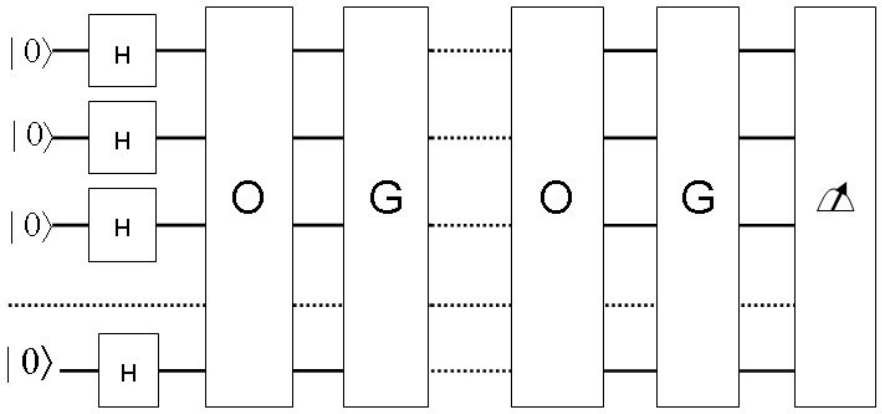
2. Δρούμε στον καταχωρητή με τον τελεστή: $\hat{O} = \hat{I} - 2|x_i X x_i|$

3. Δρούμε στον κβαντικό καταχωρητή με τον τελεστή: $\hat{G} = -(\hat{I} - 2|sXs|) = 2(sXs)) - \hat{I}$

4. Αν ο αριθμός των επαναλήψεων είναι μεγαλύτερος ή περίπου ίσος με $[(\pi/4\sqrt{N})] - 0.5$, τότε προχωράμε στο επόμενο βήμα. Αν ο αριθμός των επαναλήψεων είναι μικρότερος, τότε αυξάνεται ο αριθμός των επαναλήψεων κατά 1 και ο αλγόριθμος επαναλαμβάνεται από το προηγούμενο βήμα.

5. Τέλος, μετράμε την κατάσταση του κβαντικού καταχωρητή και αν το ζητούμενο στοιχείο βρίσκεται στη βάση τότε η κατάσταση του καταχωρητή αντιστοιχεί στο στοιχείο αυτό, διαφορετικά αντιστοιχεί σε κάποια τυχαία κατάσταση.

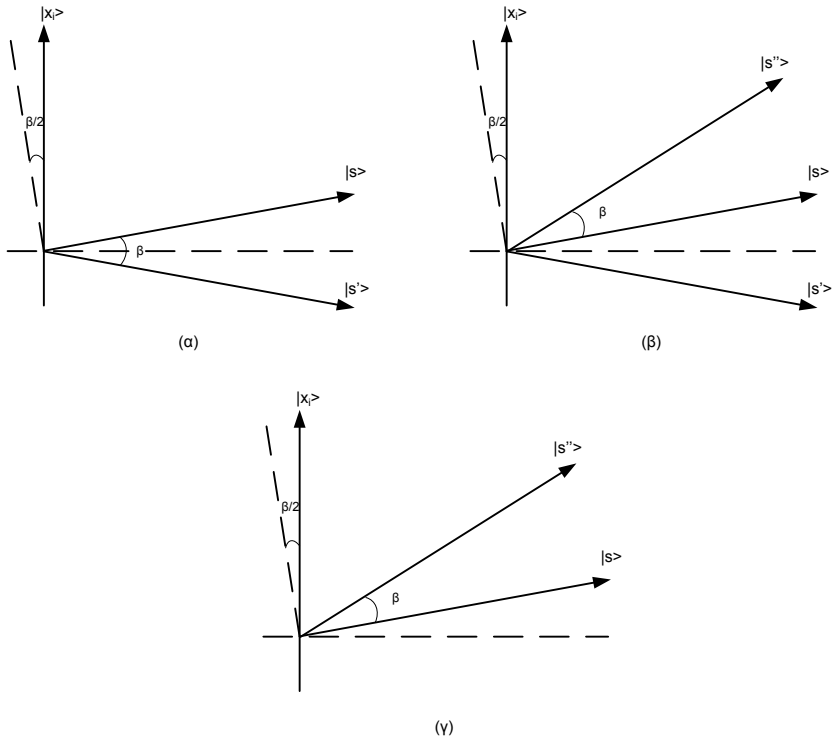
Σχηματικά ο παραπάνω αλγόριθμος παρουσιάζεται στην εικόνα 4.12.



Σχήμα 4.12: Ο αλγόριθμος τους Grover.

4.5.1 Γεωμετρική Ερμηνεία του Αλγορίθμου

Στο σχήμα 4.5.1 γίνεται μια απόπειρα για να ερμηνευτεί γεωμετρικά ο αλγόριθμος του Grover. Όπως φαίνεται, στο σχήμα 4.5.1(α) υπάρχει μια σχηματική αναπαράσταση του χώρου Hilbert με τα διανύσματα - καταστάσεις $|s>$ και $|x_i>$. Η κατάσταση $|s>$ είναι η υπέρθεση των N βασικών καταστάσεων του κβαντικού καταχωρητή (εξίσωση 4.5)και η $|x_i>$ αντιστοιχεί στο στοιχείο της μη δομημένης βάσης που αναζητούμε.



Σχήμα 4.13: (α) Η δράση του τελεστή $\hat{O}$ περιστρέφει την κατάσταση $|s>$ στην κατάσταση $|s'>$. (β) Η δράση του τελεστή $\hat{G}$ περιστρέφει την κατάσταση $|s'>$ στην κατάσταση $|s''>$. (γ) Η δράση των τελεστών $\hat{O}\hat{G}$ περιστρέφει την κατάσταση $|s>$ κατά γωνία β προς τη κατάσταση $|x_i>$ καταλήγοντας στη κατάσταση $|s''>$.

Σύμφωνα με την προηγούμενη ανάλυση, αρχικά δρα ο τελεστής $\hat{O} = \hat{I} - 2|x_i><x_i|$ στη κατάσταση $|s>$. Όπως είδαμε σαν αποτέλεσμα έχουμε την αλλαγή του πρόσημου μόνο της κατάστασης $|x_i>$ καταλήγοντας με αυτό το τρόπο στη κατάσταση:

$$|s'>=\hat{O}|s>=\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}\hat{O}|x_i>=\frac{1}{\sqrt{N}}(|x_0>+|x_1>+\ldots-|x_i>+\ldots+|x_{N-1}) \tag{4.3}$$

Η αλλαγή αυτή του πρόσημου γεωμετρικά σημαίνει ότι η νέα κατάσταση, $|s' >$, θα είναι κατοπτρική της προηγούμενης ($|s >$) ως προς το υπερεπίπεδο που είναι κάθετο στην $|x_i >$. Η τομή του υπερεπιπέδου αυτού με το χαρτί φαίνεται στο σχήμα (α) με διακεκομμένες γραμμές ανάμεσα στα διανύσματα των καταστάσεων $|s >$ και $|s' >$. Στο επόμενο βήμα, δρα ο τελεστής $\hat{G} = 2|s >< s| - \hat{I}$ που στην ουσία παράγει την κατοπτρική της $|s' >$ ως προς το υπερεπίπεδο που περιέχει την $|s >$ και είναι κάθετο με το επίπεδο του χαρτιού (σχήμα (β)). Ισχύει λοιπόν:

$$|s'' >= \hat{G}\hat{O}|s > \tag{4.4}$$

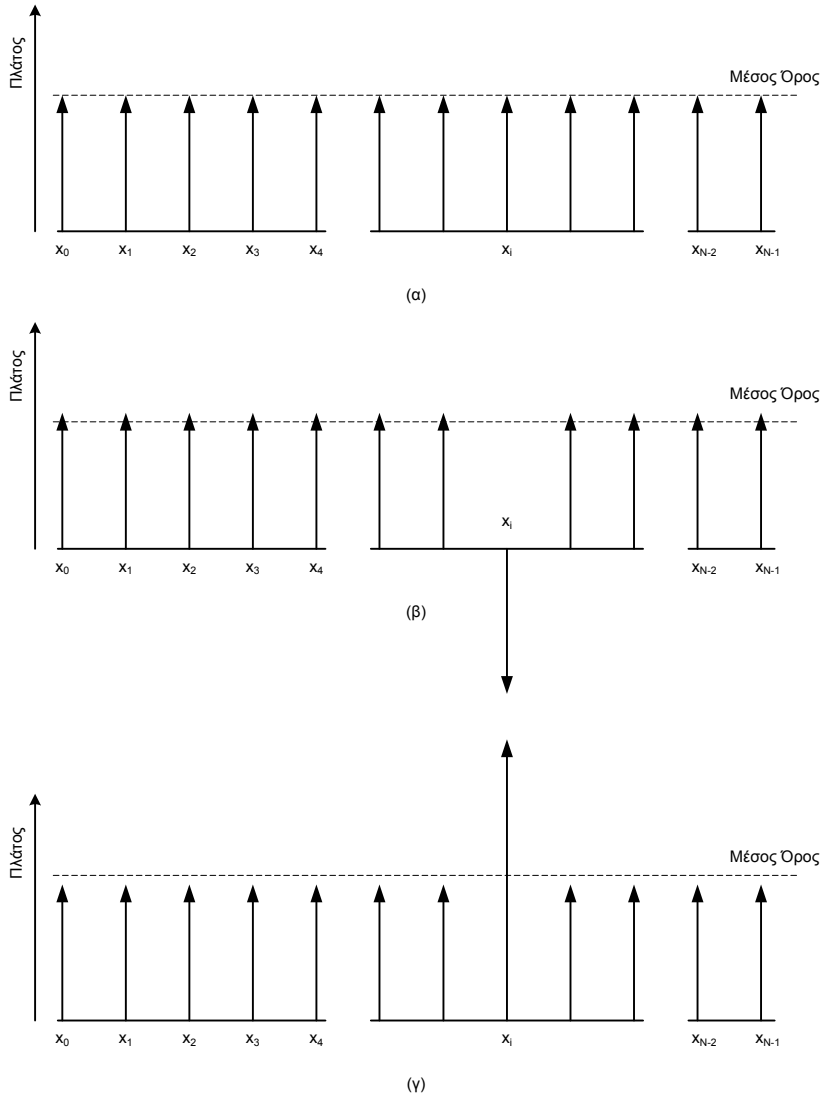
Αυτό πρακτικά σημαίνει ότι με μια επανάληψη του αλγορίθμου περιστρέφεται η κατάσταση $|s >$ κατά γωνία β προς την κατάσταση $|x_i >$ (σχήμα (γ)). Μετά από $[(\pi/4\sqrt{N})] - 0.5$ επαναλήψεις, η κατάσταση του κβαντικού καταχωρητή θα συμπέσει ή θα βρεθεί πολύ κοντά με τη κατάσταση που αναζητούμε. Σε αυτό το σημείο μπορούμε μετρώντας να είμαστε πρακτικά βέβαιοι ότι μετρώντας το καταχωρητή θα πάρουμε την κατάσταση $|x_i >$.

Μπορούμε να κατανοήσουμε την λειτουργία του αλγορίθμου εξετάζοντας από μια άλλη οπτική, αυτή των αλλαγών στα πλάτη των πιθανοτήτων των καταστάσεων σε κάθε βήμα. Το σχήμα 4.14 φαίνεται η επίδραση ενός κύκλου του αλγόριθμου στα πλάτη των πιθανοτήτων. Πίο συγκεκριμένα, αρχικά τα πλάτη όλων των βασικών καταστάσεων είναι ίσα με $1/\sqrt{N}$. Εφαρμόζοντας πρώτο τελεστή $\hat{O}$ βλέπουμε ότι το πλάτος της κατάστασης που αναζητούμε αποκτά αρνητικό πρόσημο. Στη συνέχεια με την εφαρμογή του επόμενου τελεστή $\hat{G}$ προκαλεί την αντιστροφή σε σχέση με το μέσο όρο των πλατών των καταστάσεων. Αυτό πρακτικά σημαίνει ότι μειώνονται λίγο τα πλάτη όλων των καταστάσεων πλην της $|x_i >$ διατηρώντας το θετικό πρόσημο και αυξάνεται σημαντικά το πλάτος της $|x_i >$ αποκτώντας θετικό πρόσημο. Επαναλαμβάνοντας τα βήματα του αλγορίθμου το πλάτος της $|x_i >$ αυξάνεται όλο και περισσότερο σε βάρος των πλατών των υπόλοιπων καταστάσεων μέχρι το τέλος των επαναλήψεων οπότε και είναι ίσο ή σχεδόν ίσο με 1.

4.5.2 Παρατηρήσεις

Στο σημείο αυτό είναι σκόπιμο να αναφερθούν ορισμένα ζητήματα που αφορούν τον συγκεκριμένο αλγόριθμο και τα αντιμετωπίσαμε καθώς αναπτύσσαμε τους δικούς μας κβαντικούς αλγόριθμους.

Ένα σημαντικό θέμα αποτελεί η συμπεριφορά του αλγορίθμου όταν η αρχική κατάσταση του καταχωρητή έχει μηδενικό πλάτος σε κάποιες βασικές καταστάσεις. Η βιβλιογραφία αναφέρεται σε αυτό το πρόβλημα σαν ενίσχυση πλάτους πι-



Σχήμα 4.14: (α) Τα πλάτη των πιθανοτήτων των καταστάσεων πριν την εφαρμογή των τελεστών $\hat{O}\hat{G}$. (β) Τα πλάτη μετά την εφαρμογή του $\hat{O}$. (γ) Τα πλάτη μετά την εφαρμογή του $\hat{G}$.

θανότητας και απαντήθηκε ανεξάρτητα από τους Gilles Brassard and Peter Høyer [52, 53] και τον Lov Grover [54]. Με το τρόπο αυτό μεγαλώνει το εύρος των εφαρμογών που μπορεί να καλύψει ο γενικευμένος αλγόριθμος.

Κατά τη μελέτη του αλγορίθμου του Grover διαπιστώθηκε ότι όταν το πεδίο αναζήτησης είναι πολύ μικρό (πχ 2 ή 4 στοιχεία) η λύση βρίσκεται με πιθανότητα σημαντικά μικρότερη από 1 φτάνοντας μέχρι και στο 50% στη περίπτωση των 2 στοιχείων. Αυτό προκύπτει από το γεγονός ότι η τελική πιθανότητα για την εύρεση της επιθυμητής κατάστασης είναι $1 - (1/N)$. Έτσι παρατηρείται το εκ πρώτης όψεως παράδοξο ότι όσο μεγαλύτερη είναι η βάση αναζήτησης τόσο μεγαλώνει η

πιθανότητα για την εύρεση της επιθυμητής κατάστασης.

Γενικά ο αλγόριθμος του Grover παρουσιάζει μια περιοδικότητα ως προς την εκτέλεσή του πράγμα που σημαίνει ότι είναι εξαιρετικά σημαντικό να σταματήσουμε την εκτέλεση σε $[(\pi/4\sqrt{N})] - 0.5$ βήματα. Αν συνεχίσουμε την εκτέλεση για περισσότερα βήματα τότε θα παρατηρήσουμε ότι το πλάτος της πιθανότητας για την εύρεση της επιθυμητής κατάστασης αρχίζει να μειώνεται με αποτέλεσμα να είναι πιθανό να πάρουμε λάθος αποτέλεσμα.

4.6 Περιγραφή προτεινόμενου αλγορίθμου για ελαχιστοποίηση ESOP/ESCT εκφράσεων

Ο αλγόριθμος που προτείνουμε (QMin) είναι στην ουσία ο αλγόριθμος του Grover με διαφορετικό Oracle. Είδαμε στην περιγραφή του αλγορίθμου του Grover ότι ο τελεστής Oracle αποφασίζει για το ποια στοιχεία θα επιλεγούν ώστε να εμφανιστούν στην έξοδο του κβαντικού υπολογισμού και ποια όχι. Στον QMin προτείνουμε ένα διαφορετικό τελεστή Oracle ο οποίος εξετάζει όλες τις δυνατές ESCT ή ESOP εκφράσεις μιας λογικής συνάρτησης και επιστρέφει 1 για εκείνες που έχουν βάρος κάτω από κάποιο όριο (threshold) και 0, άρα απορρίπτει, τις υπόλοιπες. Ο προτεινόμενος τελεστής Oracle ουσιαστικά στηρίζεται στο Θεώρημα 6, ενώ η λογική του προτεινόμενου αλγορίθμου έχει, ως κλασικό ανάλογο, τον αλγόριθμο XMin6.

Ο αλγόριθμος QMin μπορεί να παράγει ελάχιστες ESOP ή ESCT εκφράσεις για οποιαδήποτε λογική συνάρτηση μοναδικής εξόδου (αυτό ρυθμίζεται από το είδος των LUT τελεστών που θα χρησιμοποιηθούν. Περισσότερες λεπτομέρειες για αυτούς θα παρουσιαστούν στη συνέχεια). Στο τέλος του συγκεκριμένου κεφαλαίου ο αλγόριθμος QMin θα επεκταθεί ώστε να εντοπίζει ελάχιστες ESOP ή ESCT εκφράσεις για ατελώς ορισμένες λογικές συναρτήσεις μοναδικής εξόδου. Ο αλγόριθμος αυτός μπορεί να χρησιμοποιηθεί και για συναρτήσεις πολλών εξόδων, χρησιμοποιώντας το φορμαλισμό της χαρακτηριστικής συνάρτησης που παρουσιάστηκε σε προηγούμενο κεφάλαιο, αλλά στην περίπτωση αυτή οι ESOP ή ESCT εκφράσεις που θα δημιουργηθούν θα είναι σχεδόν ελάχιστες.

Ο αλγόριθμος QMin παρουσιάζεται στην εικόνα 4.15. Η διαφορά με τον αλγόριθμο του Grover είναι ο διαφορετικός τελεστής Oracle. Παρόμοια προσέγγιση είχε παρουσιαστεί και στην εργασία [29] όπου ένας καινούργιος τελεστής Oracle δημιουργούσε και εξέταζε εκφράσεις FPRM (Fixed Polarity Reed Muller) ώστε να εντοπίσει εκείνες οι οποίες είχαν αριθμό όρων κάτω από κάποιο καθορισμένο

όριο. Ο τελεστής Oracle, της εργασίας [29], αποτελείται από τρία διαφορετικά τμήματα. Το πρώτο είναι ο επεξεργαστής FPRM (FPRM processor) ο οποίος δημιουργεί όλες τις δυνατές FPRM εκφράσεις για τη συνάρτηση εισόδου. Το δεύτερο είναι αποτιμητής κόστους (cost evaluator), ο οποίος βρίσκει το μέγεθος της κάθε FPRM έκφρασης. Το τρίτο και τελευταίο τμήμα είναι ο συγκριτής (comparator) ο οποίος ελέγχει ποιες από τις εκφράσεις έχουν αριθμό όρων κάτω από το όριο.

Αν εξετάσουμε έναν κλασικό αλγόριθμο ελαχιστοποίησης ESCT ή ESOP εκφράσεων, όπως τον XMin6 για εκφράσεις ESCT ή τον αντίστοιχο αλγόριθμο για ESOP στην εργασία [7], η κύρια υπολογιστική επιβάρυνση προέρχεται από τους επαναληπτικούς βρόγχους (πχ for loops). Στο κεντρικό επαναληπτικό βρόγχο του Xmin6, ένα μεγάλο πλήθος συναρτήσεων $n-1$ μεταβλητών (n είναι ο αριθμός των μεταβλητών της συνάρτησης εισόδου) ενώνονται (δημιουργούνται τα αθροίσματα αποκλειστικό ή) με τις υποσυναρτήσεις της συνάρτησης εισόδου. Από τις ESCT εκφράσεις που θα δημιουργηθούν, θα επιλεγούν εκείνες με το μικρότερο αριθμό όρων (οι ελάχιστες).

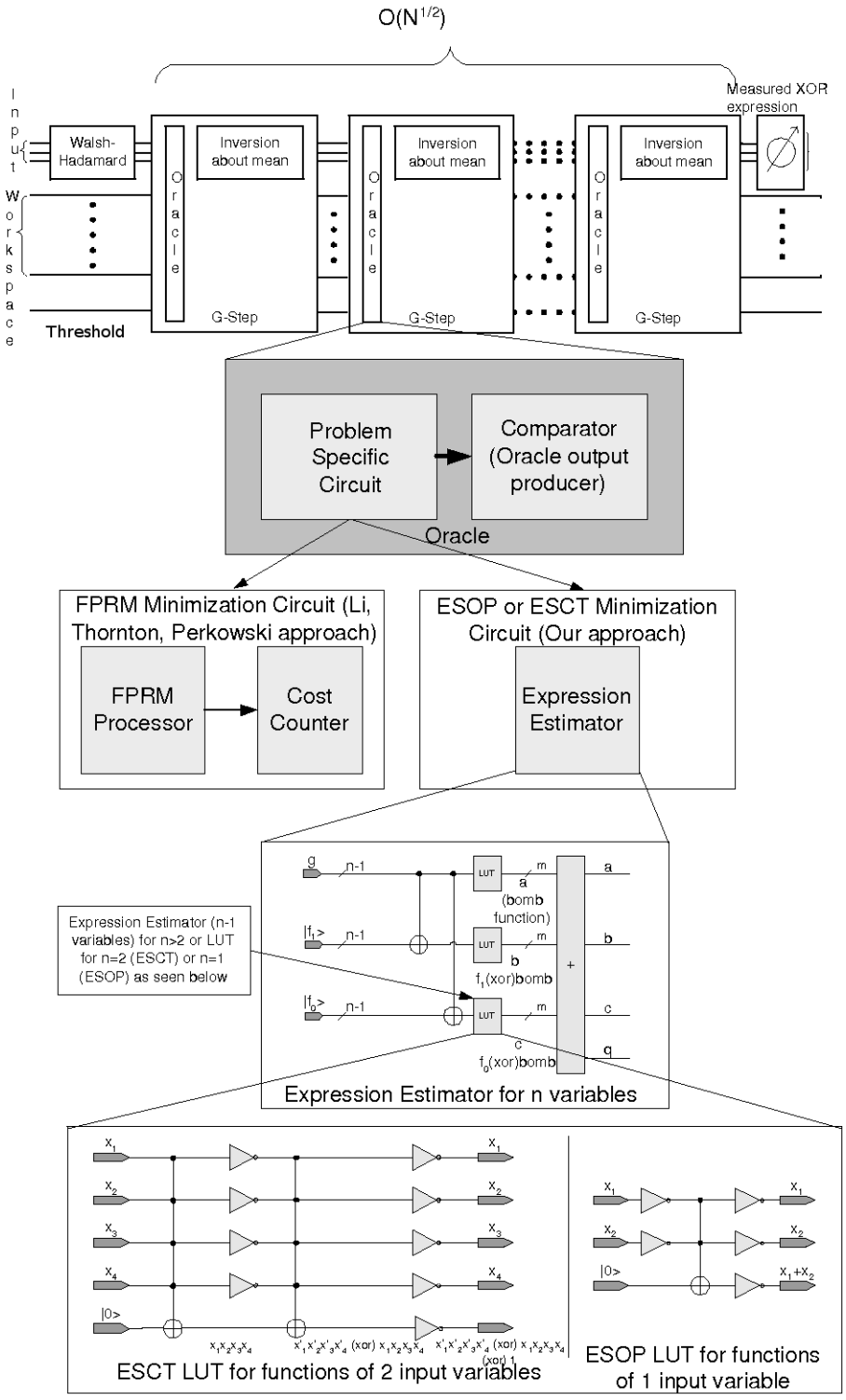
Στον προτεινόμενο αλγόριθμο QMin, όλες οι παραπάνω επαναλήψεις γίνονται σε ένα κβαντικό υπολογιστικό βήμα, χρησιμοποιώντας το φαινόμενο της κβαντικής υπέρθεσης. Αυτό μας δίνει σημαντική επιτάχυνση, σε σχέση με το κλασικό ανάλογο, και μας επιτρέπει να δημιουργούμε τα αθροίσματα "αποκλειστικού ή" σε ένα υπολογιστικό βήμα χωρίς μάλιστα να χρειαζόμαστε τις επιπλέον τεχνικές επιτάχυνσης που χρησιμοποιήθηκαν στον XMin6 (όπως πχ ότι οι συναρτήσεις που θα συμμετέχουν στα παραπάνω αθροίσματα είναι αυτές με βάρος μικρότερο του βάρους της συνάρτησης δια 3. Εδώ επιλέγουμε κάθε δυνατή συνάρτηση).

Ο προτεινόμενος κβαντικός τελεστής Oracle φαίνεται στην εικόνα 4.16 και είναι υπεύθυνος, ανάμεσα σε άλλα, για τη δημιουργία των προαναφερθέντων αθροισμάτων αποκλειστικού ή.

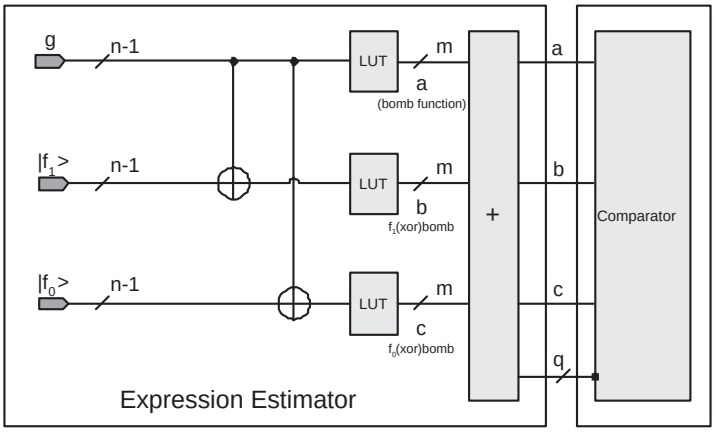
Παρατηρούμε ότι ο προτεινόμενος τελεστής Oracle αποτελείται από δύο διαφορετικά τμήματα. Το πρώτο ονομάζεται Expr-Estimator και είναι αυτό που υλοποιεί τα πορίσματα του Θεωρήματος 6. Το δεύτερο τμήμα ονομάζεται συγκριτής (comparator) και συγκρίνει τον αριθμό των όρων κάθε δημιουργούμενης ESOP ή ESCT έκφρασης με ένα συγκεκριμένο όριο (threshold), που θέτουμε εμείς. Επιστρέφει 1 αν ο παραπάνω αριθμός είναι μικρότερος ή ίσος με το όριο και 0 στις υπόλοιπες περιπτώσεις.

Θα περιγράψουμε καταρχήν τον Expr-Estimator.

Όπως μπορούμε να παρατηρήσουμε ο Expr-Estimator αποτελείται από 3 διαφορετικές γραμμές. Η πρώτη αρχικοποιείται από πύλες Walsh-Hadamard (βλέπε



Σχήμα 4.15: Ο αλγόριθμος QMin.



Σχήμα 4.16: Τελεστής Oracle του QMin.

και εικόνα 4.16) και ουσιαστικά αντιστοιχεί στη συνάρτηση g του θεωρήματος 6. Προφανώς στη γραμμή αυτή δημιουργούνται σε υπέρθεση οι MT αναπαραστάσεις όλων των δυνατών συναρτήσεων $n-1$ μεταβλητών. Η δεύτερη και η τρίτη γραμμή αρχικοποιούνται με τις MT αναπαραστάσεις των υποσυναρτήσεων f_1, f_0 της συνάρτησης εισόδου. Οι πύλες CNOT δημιουργούν τα αθροίσματα XOR της πρώτης με τη δεύτερη γραμμή και της πρώτης με την τρίτη. Στην ουσία ο Expr-Estimator υλοποιεί τις τρεις συναρτήσεις που αναφέρει το θεώρημα 6: $g, f_1 \oplus g, f_0 \oplus g$. Σύμφωνα με το Θεώρημα αυτό αν ελέγξουμε όλες τις δυνατές g συναρτήσεις, θα βρούμε όλες τις ελάχιστες ESCT ή ESOP εκφράσεις της, δεδομένου ότι γνωρίζουμε τα ESCT ή ESOP βάρη τους αντίστοιχα. Τα βάρη αυτά μας τα δίνουν οι τελεστές LUT.

Οι τελεστές αυτοί μπορούν να θεωρηθούν ως μαύρα κουτιά που παίρνουν ως είσοδο την MT αναπαράσταση μιας συνάρτησης και μας επιστρέφουν το ESCT ή ESOP βάρος της. Ένας τρόπος να τους υλοποιήσουμε είναι να χρησιμοποιήσουμε τον τελεστή Expr-Estimator αναδρομικά για $n-1, n-2, \ldots, 2, 1$ μεταβλητές. Οι καταληκτικοί τελεστές που τερματίζουν την αναδρομή αυτή παρουσιάζονται στη συνέχεια.

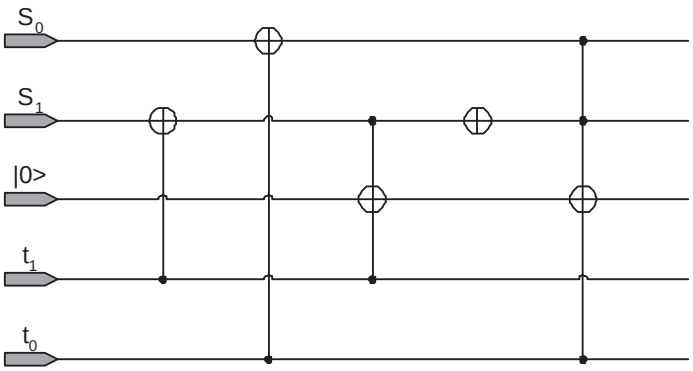
Εάν θέλουμε ο QMin να παράγει ελάχιστες ESCT εκφράσεις για τη συνάρτηση εισόδου, τότε η αναδρομή μας θα σταματήσει στο επίπεδο των 2 μεταβλητών. Ο αντίστοιχος τελεστής LUT παρουσιάζεται στην εικόνα 4.15 (κάτω αριστερά). Το κβαντικό αυτό κύκλωμα υλοποιεί τη συνάρτηση: $(x-1+x_2+x_3+x_4) \oplus x_1x_2x_3x_4$, όπου $x_i, i = 1, \ldots, 4$ είναι τα qubits που αντιστοιχούν στην αναπαράσταση MT της συνάρτησης εισόδου του τελεστή LUT. Επιστρέφει 0 μόνο για τις συναρτήσεις $[0]$ και $[F]$ και 1 σε όλες τις άλλες περιπτώσεις (θυμίζουμε ότι το ESCT βάρος

οποιασδήποτε συνάρτησης 2 μεταβλητών είναι 1 εκτός αν είναι σταθερή).

Εάν θέλουμε ο QMin να παράγει ελάχιστες ESOP εκφράσεις για τη συνάρτηση εισόδου, τότε η αναδρομή μας θα σταματήσει στο επίπεδο της 1 μεταβλητής. Ο αντίστοιχος τελεστής LUT παρουσιάζεται στην εικόνα 4.15 (κάτω δεξιά). Το κβαντικό αυτό κύκλωμα υλοποιεί τη συνάρτηση: $x_1 + x_2$, όπου $x_i, i = 1, 2$ είναι τα qubits που αντιστοιχούν στην αναπαράσταση MT της συνάρτησης εισόδου του τελεστή LUT. Επιστρέφει 0 μόνο για τη συνάρτηση $[0]$ και 1 σε όλες τις άλλες περιπτώσεις (θυμίζουμε ότι το ESOP βάρος οποιασδήποτε συνάρτησης μίας μεταβλητής είναι 1 εκτός αν αυτή είναι 0).

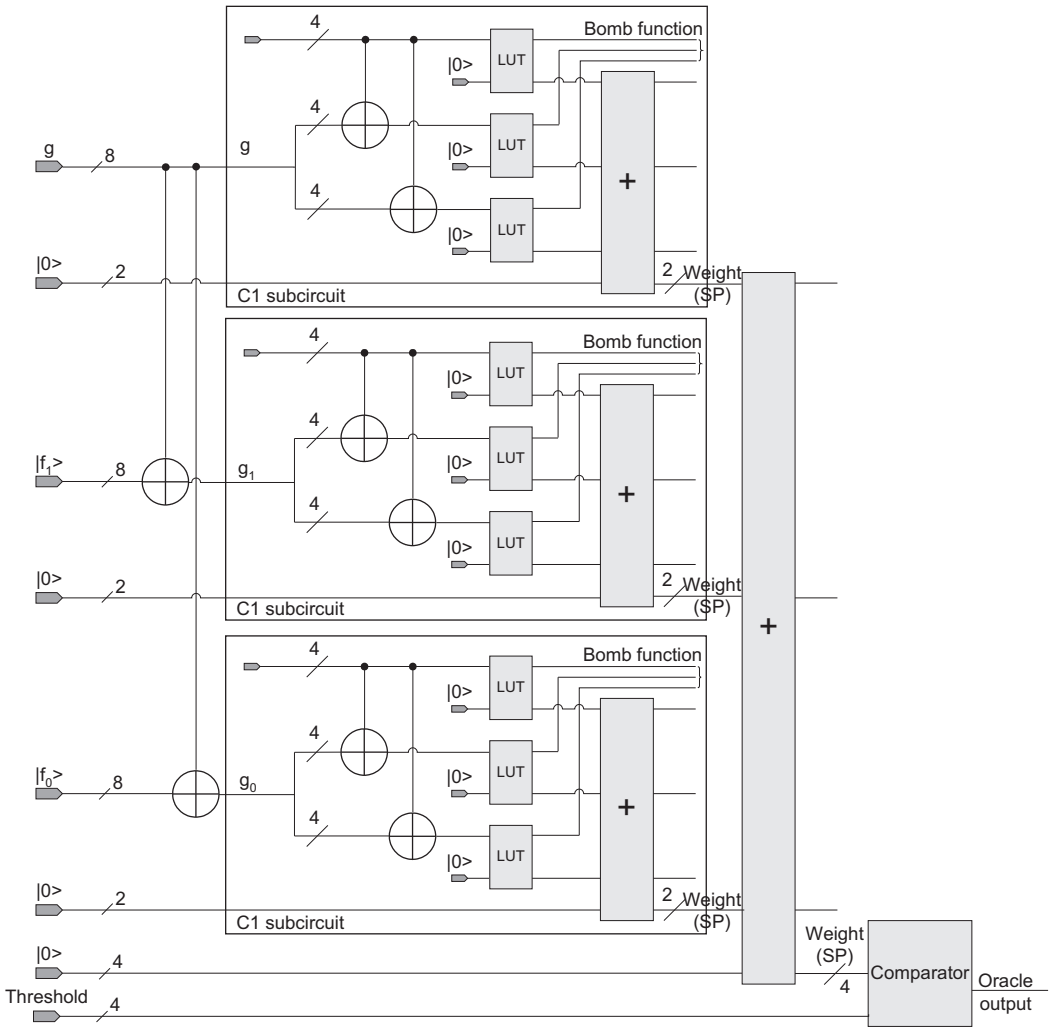
Έχοντας λοιπόν τις εξόδους των τελεστών LUT έχουμε τα βάρη των συναρτήσεων g, $f_1 \oplus g$, $f_0 \oplus g$ για όλες τις δυνατές συναρτήσεις g και μάλιστα σε υπέρθεση. Σύμφωνα λοιπόν με το Θεώρημα 6, για να βρούμε τον αριθμό των όρων για την κάθε ESCT ή ESOP έκφραση της συνάρτησης εισόδου, πρέπει απλά να προσθέσουμε τα αποτελέσματα των τελεστών LUT. Αυτό γίνεται χρησιμοποιώντας έναν κβαντικό αθροιστή. Τέτοιοι αθροιστές έχουν παρουσιαστεί στη διεθνή βιβλιογραφία [55].

Το έτερο τμήμα του τελεστή Oracle είναι ο comparator. Ένας τέτοιος κβαντικός τελεστής (για 2 qubit) παρουσιάζεται στην εικόνα 4.17. Πρέπει να σημειωθεί ότι ο comparator δεν μετέχει στην αναδρομή του Expr-Estimator, αλλά χρησιμοποιείται μόνο μια φορά (στο επίπεδο που αντιστοιχεί στη συνάρτηση εισόδου). Το κβαντικό αυτό κύκλωμα συγκρίνει το αριθμό των όρων των παραγομένων εκφράσεων από τον Expr-Estimator με το threshold και επιστρέφει 1 ή 0.



Σχήμα 4.17: Τελεστής comparator για 2 qubits.

***Παράδειγμα* 36** *Στην εικόνα 4.18 δίνουμε τον ολοκληρωμένο τελεστή Oracle που εντοπίζει ελάχιστες ESCT εκφράσεις για συναρτήσεις 4 μεταβλητών εισόδου.*



Σχήμα 4.18: Τελεστής Oracle αλγορίθμου QMin για εντοπισμό ελάχιστων ESCT εκφράσεων συναρτήσεων 4 μεταβλητών εισόδου.

Συνοψίζοντας τα παραπάνω, η είσοδος του αλγορίθμου είναι μια συνάρτηση σε αναπαράσταση MT. Οι έξοδοί του είναι οι a, b, c, q (βλέπε εικόνα 4.15) του τελεστή Oracle. Μετά από τις απαιτούμενες επαναλήψεις των τελεστών $\hat{O}, \hat{G}$ του αλγορίθμου του Grover, εκείνες οι εκφράσεις που έχουν αριθμό όρων κάτω από το threshold έχουν, πρακτικά, πιθανότητα εμφάνισης 1 ενώ οι υπόλοιπες έχουν πιθανότητα, πρακτικά, 0. Μετρώντας μία από τις εξόδους του κβαντικού κυκλώματος QMin, όλες οι έξοδοι θα ”καταρρεύσουν” σε μια από τις βασικές καταστάσεις που έχουν θετική πιθανότητα εμφάνισης, δηλαδή σε μια έκφραση από εκείνες που έχουν αριθμό όρων μικρότερο ή ίσο του threshold.

Παρακάτω παρατίθεται ο ψευδοκώδικας του αλγορίθμου:

procedure QMin(func)

Begin

for (each step of the Grover's Algorithm)

Begin

do in parallel for every possible g function //one step

$w(g) = Expr\_Estimator(g);$

$w(f_0 \oplus g) = Expr\_Estimator(f_0 \oplus g)$

$w(f_1 \oplus g) = Expr\_Estimator(f_1 \oplus g)$

End

$mark(func) = threshold > (w(f_0 \oplus g) + w(g_1 \oplus g) + w(g));$

$invertmarkedstates()$

$invertaboutmean()$

End

End

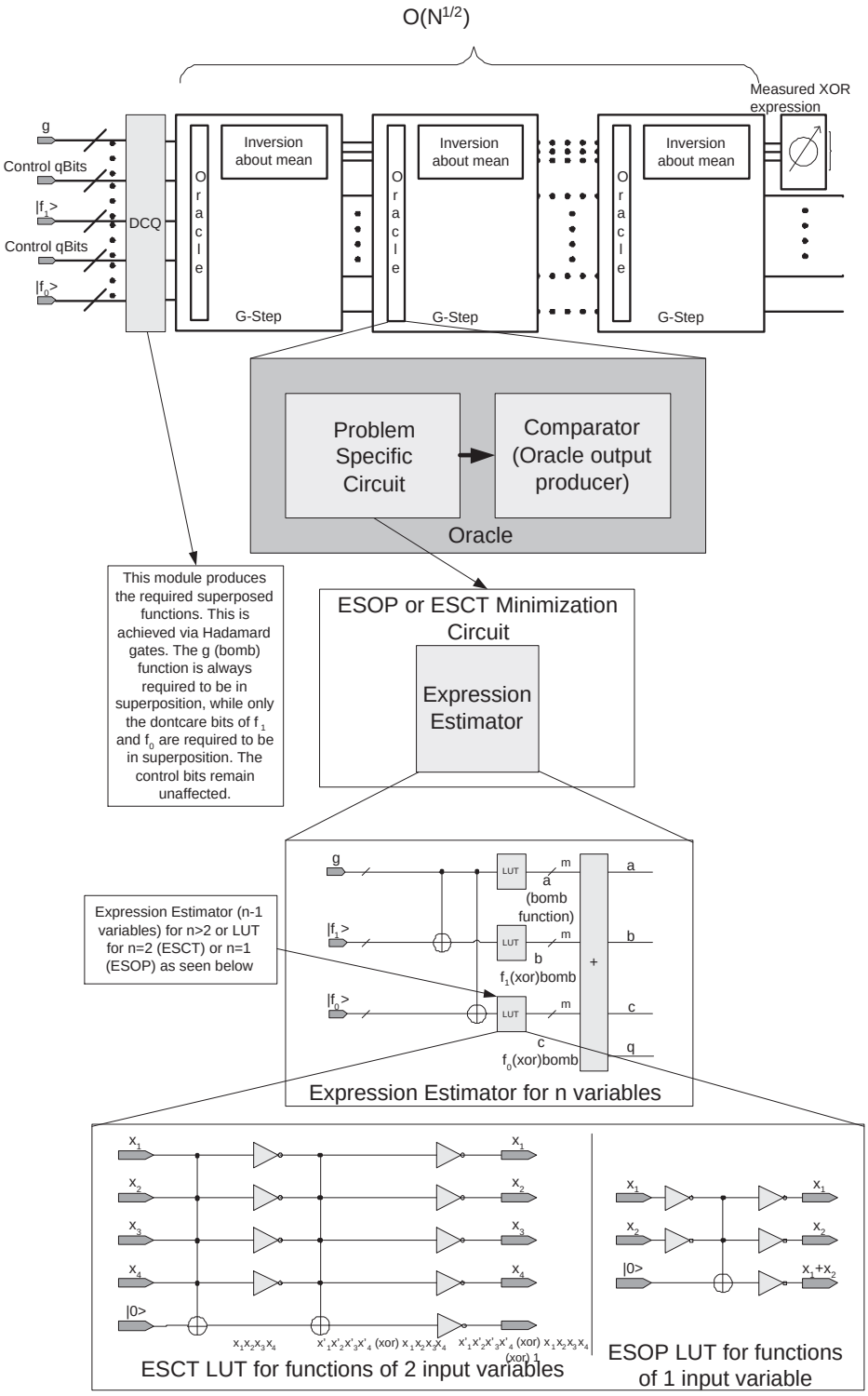
Με τον παραπάνω αλγόριθμο μπορούμε να βρούμε ελάχιστες ESOP ή ESCT εκφράσεις, πραγματοποιώντας διαδοχικές εκτελέσεις του QMin ρυθμίζοντας σε κάθε καινούργια εκτέλεση, κατάλληλα το threshold. Η αρχική τιμή του threshold μπορεί να δωθεί από τη χρήση ενός κλασικού αλγορίθμου ESOP ή ESCT ελαχιστοποίησης όπως ο EMin1 ή ο Find_Exact.

4.7 Επέκταση για ατελώς ορισμένες λογικές συναρτήσεις

Ο παραπάνω αλγόριθμος μπορεί, εύκολα, να επεκταθεί και για ατελώς ορισμένες λογικές συναρτήσεις. Σύμφωνα με τον ορισμό μιας ατελώς ορισμένης λογικής συνάρτησης κάποιοι από τους ελαχιστόρους της βρίσκονται στο ON set, κάποιοι στο OFF set και κάποιοι στο DC set (είναι αδιάφοροι).

Ένας ελαχιστόρος είναι αδιάφορος όταν δεν έχει καμιά σημασία αν θα τον τοποθετήσουμε στο ON set ή στο OFF set της συνάρτησης. Μπορεί, βέβαια, το γεγονός αυτό να μην έχει καμιά σημασία για τη συνάρτηση, αλλά επηρεάζει άμεσα το βάρος της. Κατά συνέπεια στην MT αναπαράσταση της συνάρτησης, ένας αδιάφορος ελαχιστόρος μπορεί να έχει τιμή 1 ή 0 ανάλογα με το ποια τιμή δίνει μικρότερο βάρος.

Για να βρούμε το βάρος μιας ατελώς ορισμένης λογικής συνάρτησης πρέπει να θέσουμε, διαδοχικά, κάθε αδιάφορο ελαχιστόρο στο ON set και στο OFF set και να δούμε ποια περίπτωση μας δίνει μικρότερο βάρος. Όπως μπορεί να γίνει εύκολα

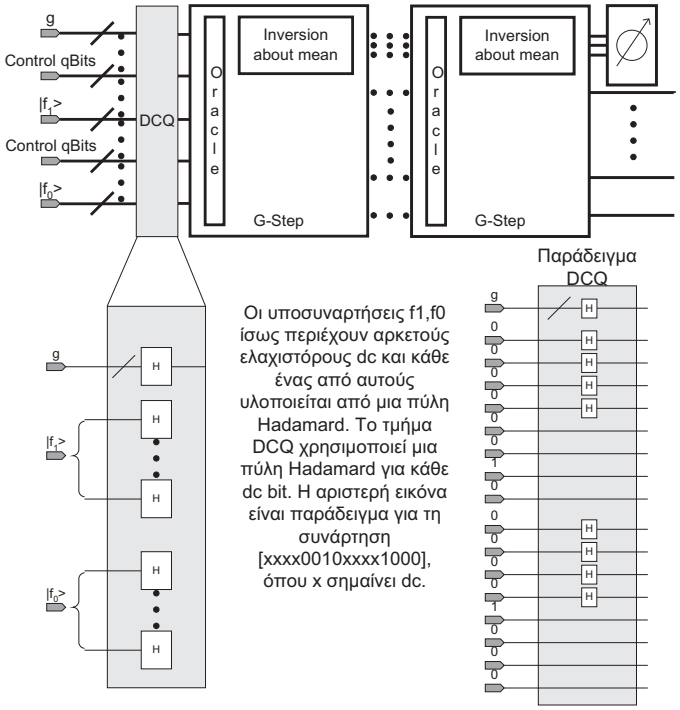


Σχήμα 4.19: Αλγόριθμος DCQMin.

αντιληπτό η διαδικασία αυτή είναι εξαιρετικά χρονοβόρα και απαιτητική για έναν κλασικό υπολογιστή, είναι όμως πολύ απλή για έναν κβαντικό υπολογιστή.

Η επέκταση του QMin είναι απλή. Αρκεί να προσθέσουμε μια σειρά από πύλες

Walsh-Hadamard στις γραμμές που δίνουν την MT αναπαράσταση της συνάρτησης εισόδου μας, και για εκείνους τους ελαχιστόρους που είναι αδιάφοροι. Αυτό μας θέτει τα qubits που αντιστοιχούν στους αδιάφορους ελαχιστόρους σε κατάσταση υπέρθεσης (δηλαδή είναι και 0 και 1, ακριβώς όπως ο ορισμός των αδιάφορων ελαχιστόρων). Οι εκφράσεις που θα δημιουργηθούν θα είναι οι ελάχιστες λαμβάνοντας υπόψην και τους αδιάφορους ελαχιστόρους.

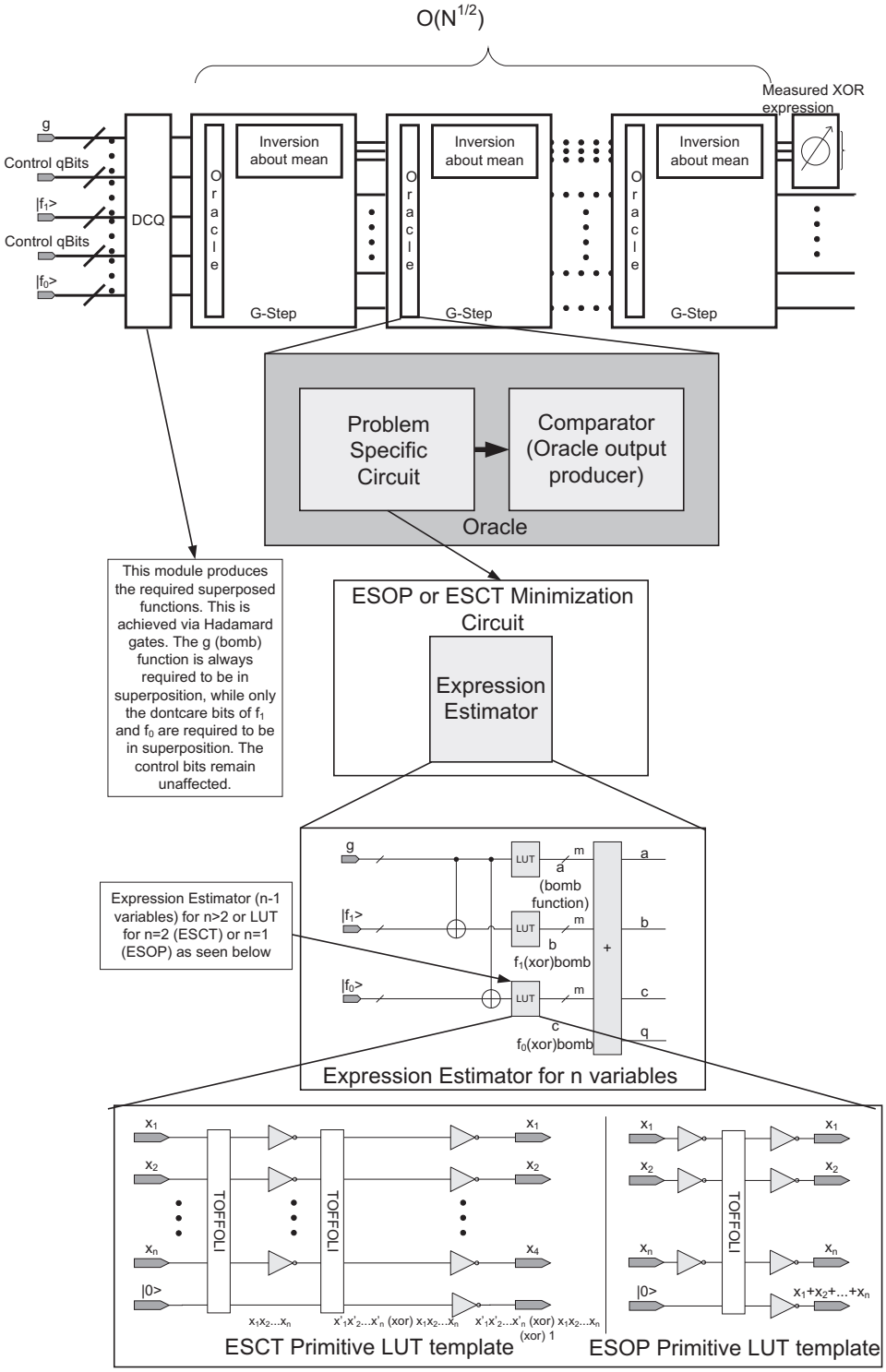


Σχήμα 4.20: Λεπτομέρεια και παράδειγμα DCQMin.

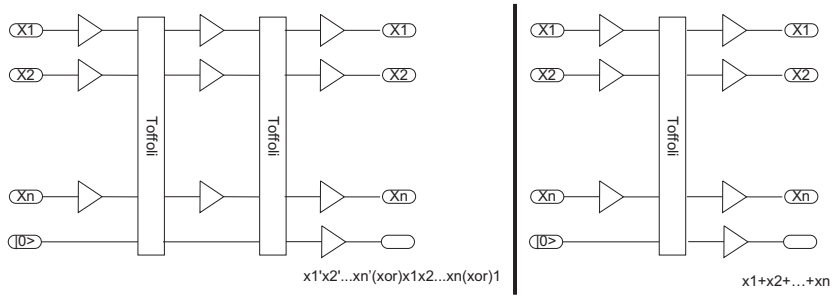
Η τροποποίηση αυτή του QMin οδηγεί στον αλγόριθμο DCQMin [56]. Ο αλγόριθμος αυτός παρουσιάζεται στην εικόνα 4.19, ενώ στην εικόνα 4.20 φαίνονται μόνο οι λεπτομέρειες της μονάδας αρχικοποίησης και αντίστοιχο παράδειγμα.

4.8 Επέκταση για συναρτήσεις πολλών εξόδων

Ο προτεινόμενος κβαντικός αλγόριθμος DCQMin μπορεί εύκολα να επεκταθεί για λογικές συναρτήσεις πολλών εξόδων χρησιμοποιώντας τη χαρακτηριστική συνάρτηση. Ο καινούργιος αλγόριθμος ονομάζεται MOQMin [57] και αποτελεί μια πιο γενική μορφή των αλγορίθμων που παρουσιάσθηκαν στο κεφάλαιο αυτό, αφού ελαχιστοποιεί ατελώς ορισμένες συναρτήσεις πολλών εξόδων και παράγει ESOP ή ESCT εκφράσεις. Ο αλγόριθμος MOQMin είναι ίδιος με τον DCQMin εκτός από



Σχήμα 4.21: Αλγόριθμος MOQMin.



Σχήμα 4.22: Καταληκτικοί τελεστές MOQMin.

το επίπεδο των καταληκτικών τελεστών LUT (στο επίπεδο δηλαδή που τελειώνει η αναδρομή). Στο σημείο αυτό της αναδρομής οι συναρτήσεις αντιστοιχούν σε πολύ-τιμες μεταβλητές της χαρακτηριστικής συνάρτησης. Οι καταληκτικοί τελεστές που τερματίζουν την αναδρομή εξαρτώνται από τον αριθμό των εξόδων της συνάρτησης εισόδου και ακολουθούν ένα συγκεκριμένο μοτίβο.

Για την περίπτωση των εκφράσεων ESOP πρέπει να υλοποιηθεί η πράξη ”λογικό ή” γιατί το βάρος του literal της πολύ-τιμης μεταβλητής είναι 0 μόνο όταν αυτή είναι 0 και 1 σε όλες τις υπόλοιπες περιπτώσεις. Αυτό μπορεί να υλοποιηθεί εύκολα χρησιμοποιώντας μια κβαντική πύλη Toffoli, όπου το/τα qubits ελέγχου της είναι ίσα με το 0, μαζί με τις απαραίτητες πύλες CNOT. Για την περίπτωση των εκφράσεων ESCT ο ίδιος τελεστής είναι ελαφρά πιο πολύπλοκος. Οι μόνες περιπτώσεις στις οποίες το βάρος θεωρείται ίσο με το 0 είναι όταν η πολύ-τιμη μεταβλητή είναι ίση με το 0 ή ίση με το 1. Σε όλες τις υπόλοιπες περιπτώσεις το βάρος της πολύ-τιμη μεταβλητής θεωρείται ίσο με 1. Έτσι ο καταληκτικός τελεστής για ESCT εκφράσεις μπορεί να υλοποιηθεί χρησιμοποιώντας δύο κβαντικές πύλες Toffoli και τις απαραίτητες πύλες CNOT. Ο αριθμός των qubits των παραπάνω τελεστών LUT εξαρτώνται από τον αριθμό των εξόδων της συνάρτησης εισόδου.

Η γενική μορφή του αλγορίθμου καθώς και των παραπάνω καταληκτικών τελεστών LUT παρουσιάζονται στις Εικόνες 4.21 και 4.22.

4.9 Επέκταση με χρήση αναδιάταξης των μεταβλητών εισόδου

Η τελευταία επέκταση του QMin έχει να κάνει με την ενσωμάτωση της αναδιάταξης των μεταβλητών εισόδου για την επίτευξη ακόμα καλύτερων αποτελεσμάτων. Ο νέος αλγόριθμος ονομάζεται ROQMin [58] και το ιεραρχικό του σχεδιάγραμμα

φαίνεται στην εικόνα 4.23. Ο συγκεκριμένος έχει αναπτυχθεί με δύο διαφορετικούς τρόπους εκ των οποίων ο δεύτερος βρίσκεται ακόμα σε ανάπτυξη. Γενικά ο αλγόριθμος αυτός αναφέρεται στην ελαχιστοποίηση αποκλειστικά εκφράσεων ESCT, αφού στις εκφράσεις ESOP δεν παίζει ρόλο η διάταξη των μεταβλητών εισόδου. Ο ρόλος της διάταξης των μεταβλητών εισόδου μπορεί να γίνει κατανοητός από το παρακάτω παράδειγμα. Έστω συνάρτηση f με $f(x_1, x_2, x_3) = (x_1 \oplus x_2)x_3$. Αν θεωρήσουμε ότι σαν περισσότερο σημαντική μεταβλητή τη x_3 και λιγότερο σημαντική την x_1 τότε το βάρος της f είναι 1 με ελάχιστη έκφραση την (154). Αν όμως θεωρήσουμε σαν περισσότερο σημαντική μεταβλητή τη x_1 και λιγότερο σημαντική την x_2 τότε η ίδια συνάρτηση έχει βάρος 2 με ελάχιστη έκφραση την $(614) \oplus (146)$. Από το παραπάνω φαίνεται ότι το ESCT βάρος μιας συνάρτησης εξαρτάται άμεσα από την διάταξη των μεταβλητών εισόδου. Συνεπώς είναι σημαντικό να μπορούμε να επιλέξουμε τη βέλτιστη διάταξη μεταβλητών εισόδου για να μπορούμε να βρούμε το καλύτερο βάρος της συνάρτησης. Το πρόβλημα αυτό είναι εξαιρετικά δύσκολο για ένα συμβατικό υπολογιστή αφού πέραν της εγγενούς δυσκολίας του βασικού πυρήνα του αλγόριθμου ελαχιστοποίησης θα πρέπει να εξεταστούν και όλες οι αναδιατάξεις των μεταβλητών εισόδου.

Παρακάτω παρατίθεται ο ψευδοκώδικας του ROQMin.

procedure ROQMin(func)

Begin

$Initialize()$ //Αρχικοποίηση των καταχωρητών της συνάρτησης ώστε να υπάρχουν σε υπέρθεση όλες οι δυνατές αναδιατάξεις μεταβλητών εισόδου

for (each step of the Grover's Algorithm)

Begin

do in parallel for every possible g function //one step

$w(g) = Expr\_Estimator(g)$;

$w(f_0 \oplus g) = Expr\_Estimator(f_0 \oplus g)$ //Άθροισμα XOR για κάθε δυνατή αναδιάταξη μεταβλητών εισόδου

$w(f_1 \oplus g) = Expr\_Estimator(f_1 \oplus g)$ //Άθροισμα XOR για κάθε δυνατή αναδιάταξη μεταβλητών εισόδου

End

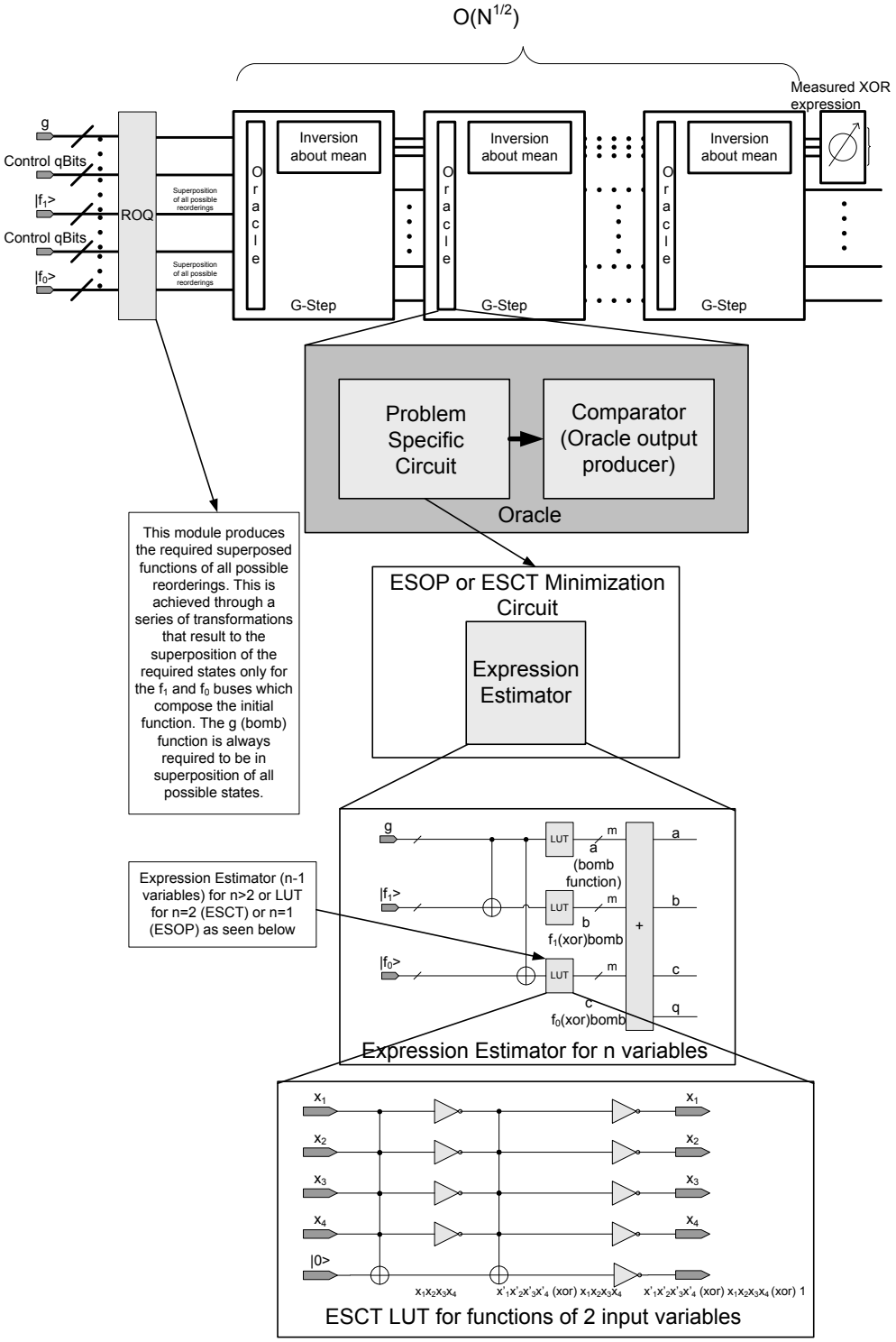
$mark(func) = threshold > (w(f_0 \oplus g) + w(g_1 \oplus g) + w(g))$;

$invertmarkedstates()$

$invertaboutmean()$

End

End



Σχήμα 4.23: Αλγόριθμος ROQMin.

Η διαφορά σε σχέση με τον QMin έγκειται στο στάδιο της αρχικοποίησης όπου και εφαρμόζοντας τη μέθοδο αρχικοποίησης κβαντικών καταχωρητών που παρουσιάζεται στο [59] μπορούμε να έχουμε στον καταχωρητή της συνάρτησης όλες τις

δυνατές αναδιατάξεις των μεταβλητών εισόδου. Αυτές είναι εύκολο να εξαχθούν από ένα συμβατικό αλγόριθμο όπως ο [60]. Παρόλα αυτά η αρχικοποίηση των καταχωρητών δεν είναι απλή υπόθεση όπως στους συμβατικούς υπολογιστές. Η μέθοδος που παρουσιάζεται αναλυτικά στο [59] σταδιακά "γεμίζει" τον καταχωρητή με τα επιθυμητά περιεχόμενα (bitvectors στη προκειμένη περίπτωση) κάνοντας χρήση μιας σειράς μετασχηματισμών Hadamard, CNOT, Fredkin και NOT. Πιο συγκεκριμένα, γίνεται χρήση τριών καταχωρητών που αρχικά βρίσκονται στην κατάσταση $|0 \ldots 0>$. Ο πρώτος είναι αυτός που στη πραγματικότητα θα περιέχει την υπέρθεση, ενώ οι άλλοι δύο χρησιμοποιούνται επικουρικά για να επιτρέπουν αλλαγές στον πρώτο και να "κλειδώνουν" τις παραγόμενες καταστάσεις. Στο πρώτο βήμα χρησιμοποιώντας πύλες NOT παράγουμε την πρώτη επιθυμητή κατάσταση. Στο επόμενο βήμα (βήμα παραγωγής κατάστασης) χρησιμοποιείται ένας μετασχηματισμός τύπου Hadamard που ουσιαστικά παράγει μια νέα κατάσταση σε υπέρθεση με την προηγούμενη. Στη συνέχεια, οι καταστάσεις που επηρεάζονται από το προηγούμενο βήμα "μαρκάρονται" στον βοηθητικό (2ο) καταχωρητή και κατόπιν ο τελευταίος καταχωρητής χρησιμοποιείται για "κλειδώσει" την επιθυμητή κατάσταση και να "ξεκλειδώσει" την άλλη κατάσταση, ενώ ο δεύτερος καταχωρητής επαναφέρεται στο $|0 \ldots 0>$. Επαναλαμβάνοντας τα παραπάνω βήματα τελικά λαμβάνουμε σε υπέρθεση όλες τις επιθυμητές καταστάσεις. Η πρόσθετη πολυπλοκότητα είναι $O(nm)$ όπου n ο αριθμός των μεταβλητών εισόδου και m ο αριθμός των αναδιατάξεων.

Η παραπάνω διαδικασία μπορεί να πραγματοποιηθεί και με ένα εναλλακτικό τρόπο που μοιάζει περισσότερο στη διαδικασία που ακολουθείται στον αλγόριθμο του Shor. Πιο συγκεκριμένα, μπορούμε αρχικά να θέσουμε τον καταχωρητή της συνάρτησης εισόδου σε υπέρθεση όλων των δυνατών καταστάσεων χρησιμοποιώντας πύλες Hadamard. Στη συνέχεια χρησιμοποιώντας ένα βοηθητικό καταχωρητή αποτελέσματος να εφαρμόσουμε μια δράση που θα αποτελεί την κβαντική υλοποίηση της συνάρτησης εισόδου. Με αυτόν το τρόπο ο δεύτερος καταχωρητής θα περιέχει όλα τα αποτελέσματα της συνάρτησης εισόδου. Στη συνέχεια μετρώντας ο πρώτος καταχωρητής θα περιέχει όλες τις εισόδους που αντιστοιχούν στο αποτέλεσμα της μέτρησης. Αν λάβουμε 0 μπορούμε να επαναλάβουμε την διαδικασία εώς ότου λάβουμε 1. Με αυτό το τρόπο ο καταχωρητής εισόδου θα περιέχει όλα τα bitvectors που αντιστοιχούν στις αναδιατάξεις των εισόδων. Είναι προφανές ότι πρόκειται για μια πιο απλή διαδικασία που όμως χρειάζεται ορισμένες βελτιώσεις στο βήμα της μέτρησης.

4.10 Προσομοίωση Oracle

Ο πυρήνας του αλγορίθμου, δηλαδή το Oracle, έχει προσομοιωθεί στον διαδικτυακό προσομοιωτή κβαντικών κυκλωμάτων του Fraunhofer Institut Rechnerarchitektur und Softwaretechnik (FIRST). Η υλικοτεχνική υποδομή του εξομοιωτή αποτελείται από ένα linux cluster με 32 κόμβους (AMD Athlon MP 2000+) με συνολική μνήμη 56 GB, διασυνδεδεμένους με ένα Myrinet-2000 οπτικό δίκτυο. Η υπάρχουσα υποδομή μπορεί να προσφέρει αρκετή υπολογιστική ισχύ για την εξομοίωση κβαντικών κυκλωμάτων έως 31 qubits.

Στα σχήματα 4.24, 4.25, 4.26 και 4.27 παρουσιάζονται snapshots των κυκλωμάτων του Expression Estimator και του Comparator για ESOP εκφράσεις 2 μεταβλητών εισόδου καθώς και snapshots των αποτελεσμάτων.

Ο συγκεκριμένος εξομοιωτής, όπως αναφέρθηκε παραπάνω, βασίζεται σε διαδραστικό περιβάλλον με το χρήστη μέσω διαδικτύου. Ο χρήστης πηγαίνοντας στη διεύθυνση www.qc.fraunhofer.de μπορεί να δει τη κεντρική σελίδα του εξομοιωτή. Απαιτείται εγγραφή στο site και μόλις ολοκληρωθεί αυτή η διαδικασία, ο χρήστης αποκτά προσωποποιημένο περιβάλλον εργασίας έχοντας δικό του φάκελο όπου μπορεί να αποθηκεύσει τα απαιτούμενα για την εξομοίωση αρχεία του καθώς και να διαπιστώσει την πορεία των εξομοιώσεών του.

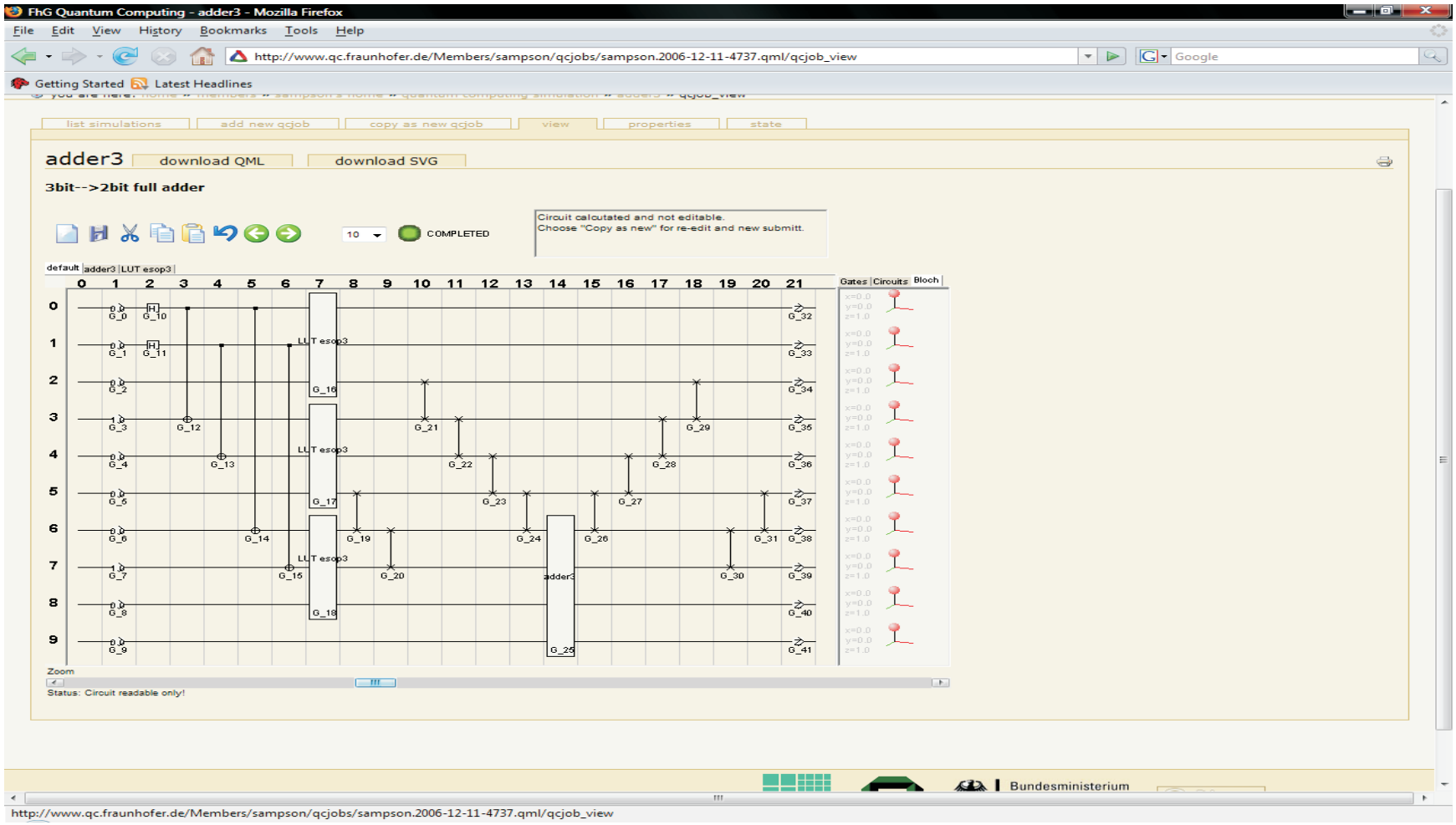
Μέσα από την λίστα των my simulations μπορεί ο χρήστης να δημιουργήσει μια νέα εξομοίωση ή να δει την κατάσταση των παλιών εργασιών εξομοιώσης που έχει πραγματοποιήσει. Οι εργασίες μπορούν να διαγραφούν, να μετονομαστούν, να αντιγραφούν ή να αλλάξουν κατάσταση από των χρήστη σαν να είναι αρχεία.

Δημιουργώντας μια νέα εξομοίωση, ο χρήστης μπορεί να διαλέξει τον τύπο της εξομοίωσης που θα πραγματοποιήσει ανάμεσα σε διάφορα templates όπως τον αλγόριθμο του Shor, του Grover για διαφορετικά πλήθη bits και το πείραμα της τηλεμεταφοράς. Το default template δίνει δυνατότητα να δημιουργηθεί το κβαντικό κύκλωμα από την αρχή με κάθε λεπτομέρεια. Επίσης πρέπει να δοθεί ένας τίτλος και μια περιγραφή για το πείραμα. Ακολουθώντας αυτά τα βήματα, καταλήγουμε στη σελίδα όπου ο χρήστης σχεδιάζει το κύκλωμά του και φαίνεται στο εικόνα 11. Όπως φαίνεται και από το σχήμα ο χρήστης χρησιμοποιώντας τα αντίστοιχα κουμπιά μπορεί να δημιουργήσει μια νέα εξομοίωση, να αποθηκεύσει την υπάρχουσα, να αντιγράψει / αποκόψει / επικολλήσει κβαντικές πύλες ή μέρη του κυκλώματος, να αναιρέσει τις αλλαγές που πραγματοποίησε, να προσθέσει ή να αφαιρέσει υπολογιστικά βήματα, να υποβάλλει προς εκτέλεση το κύκλωμά του και να καθορίσει τον αριθμό των qubits. Δεξιά της επιφάνειας εργασίας του κυκλώματος υπάρχει μια λίστα με πύλες που μπορούν να χρησιμοποιηθούν για τον σχεδιασμό του κυκλώμα-

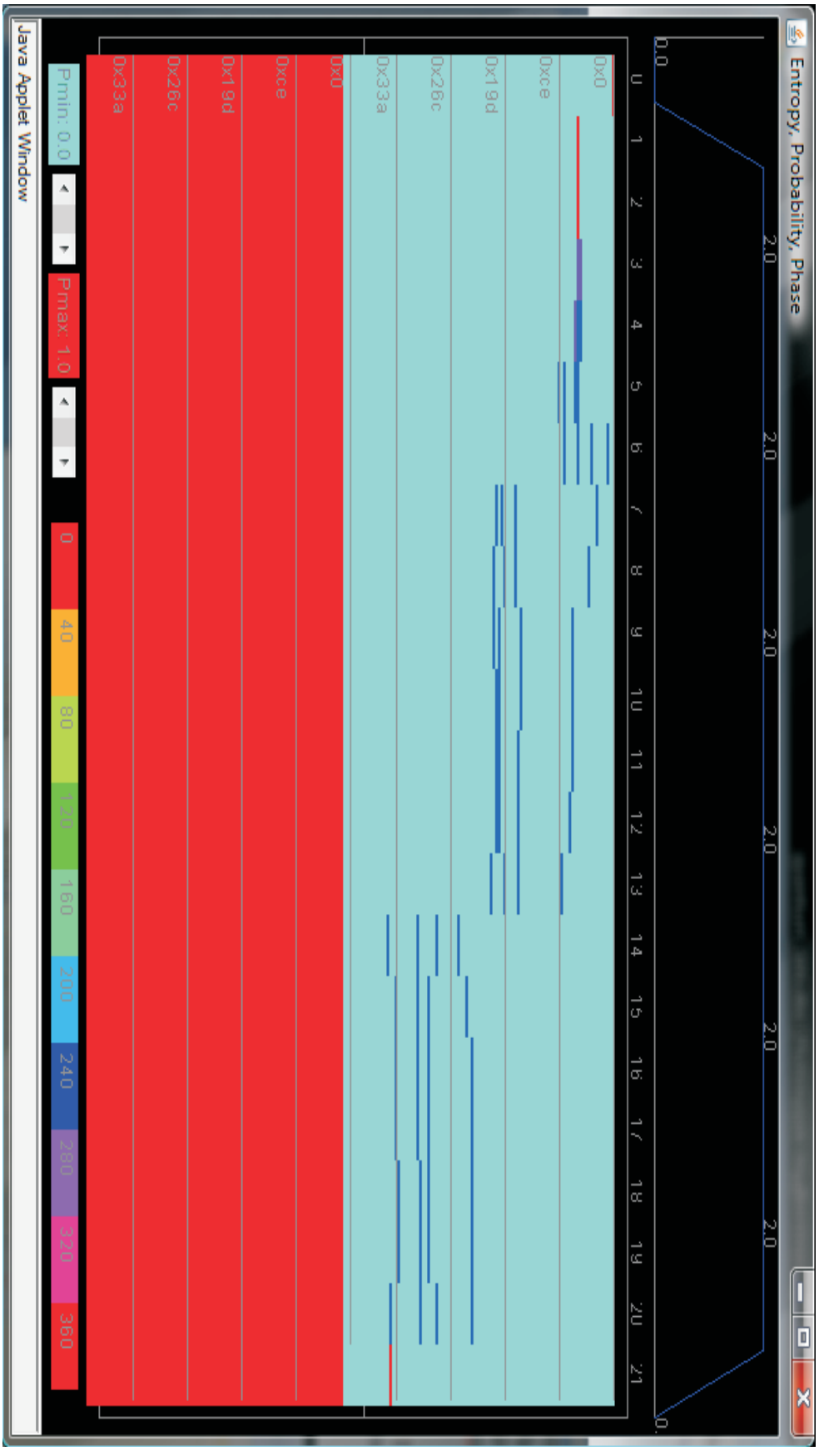
τος. Εκτός από τις βασικές πύλες υπάρχουν διαθέσιμα και βασικά υποκυκλώματα γνωστών αλγορίθμων όπως του Grover. Εκτός από τη λίστα με τα βασικά δομικά στοιχεία που παρέχονται υπάρχει και μια λίστα με υποκυκλώματα που έχουν επιλεγεί από το υπάρχον κύκλωμα. Τα υποκυκλώματα που υπάρχουν σε αυτή τη λίστα αφορούν την συγκεκριμένη εργασία εξομοίωσης και δεν όχι όλο τον εξομοιωτή. Τέλος, υπάρχει μια λίστα με τις σφαίρες bloch για κάθε bit που όμως παρέχουν δεδομένα μόνο αφού έχει πραγματοποιηθεί η εξομοίωση. Για την κατασκευή του κυκλώματος ο χρήστης πρέπει να επιλέξει την επιθυμητή πύλη από τη λίστα και στη συνέχεια να κάνει κλικ στο σημείο που θέλει να την τοποθετήσει. Έχοντας ολοκληρώσει το σχεδιασμό, ο χρήστης θα πρέπει να τοποθετήσει στο τέλος και ειδικές πύλες που πραγματοποιούν μέτρηση σε όσα qubit επιθυμούν. Στη συνέχεια πατώντας το κουμπί της εκτέλεσης το κύκλωμα στέλνεται στον server προς εξομοίωση και υπάρχει μια ένδειξη για το πόση ώρα αναμένεται να κρατήσει αυτή. Μόλις παρέλθει η ώρα αυτή, ο χρήστης θα πρέπει να κάνει ανανέωση στη σελίδα για να μπορεί να δει τα αποτελέσματα.

Τα αποτελέσματα που προκύπτουν παρουσιάζονται σε ένα νέο παράθυρο το οποίο χωρίζεται σε τρεις βασικές γραφικές παραστάσεις. Ο οριζόντιος άξονας αναπαριστά το χρόνο σε υπολογιστικά στάδια και για τις τρεις. Στη πρώτη φαίνεται η εξέλιξη της εντροπίας που υπολογίζεται με βάση τον τύπο:
$S(|\phi>) = -\sum_{i=0}^{2^N-1} p_i log_2(p_i)$, όπου $p_i = |<u_i|\phi>|^2$ είναι η πιθανότητα το σύστημα $V = \{|u_i>; 0 \leq i \leq 2^N\}$ να βρεθεί στην i-οστή βασική κατάσταση.

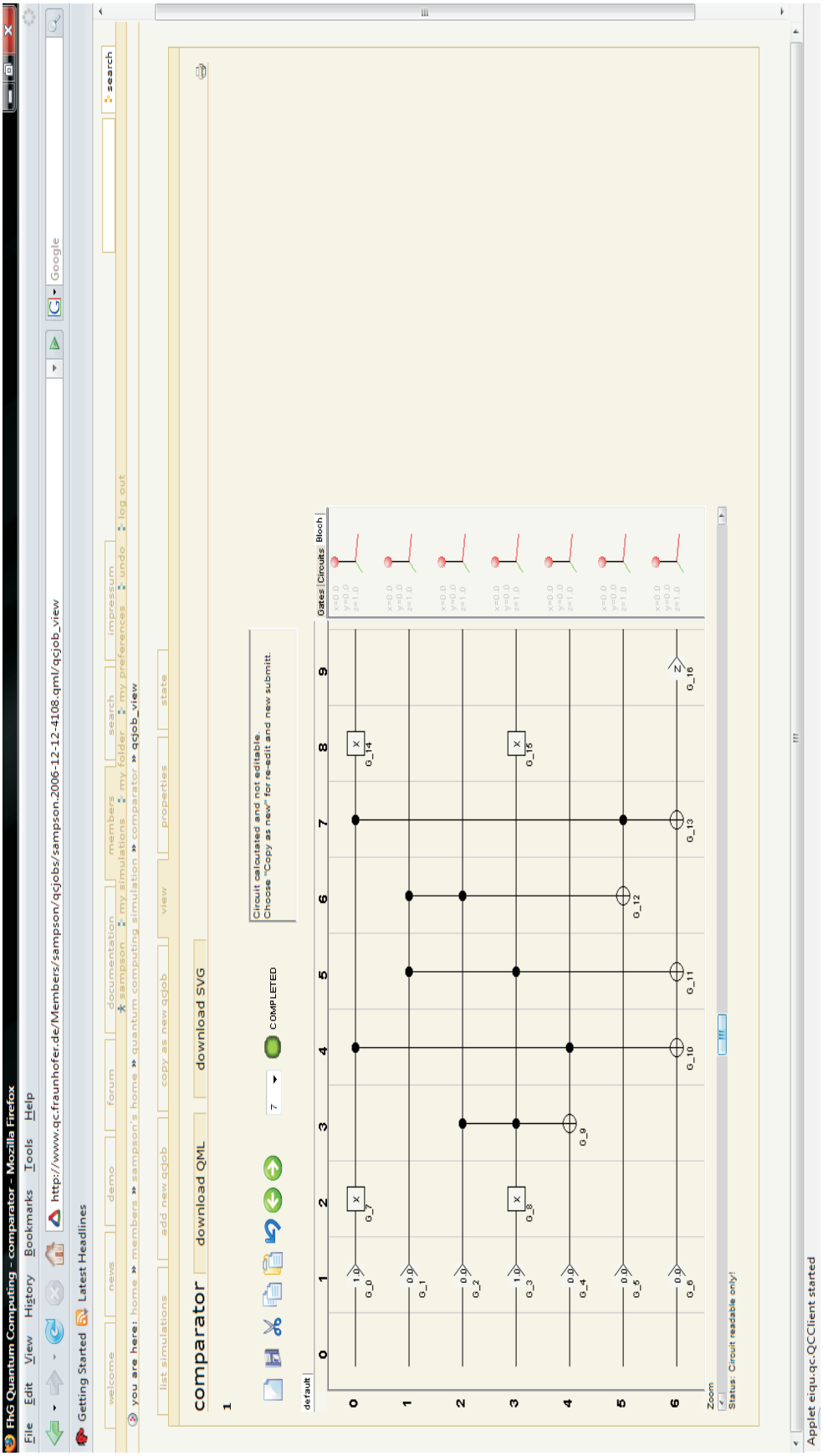
Στη δεύτερη γραφική παράσταση, φαίνεται η πιθανότητα του συστήματος να βρεθεί σε μια κατάσταση καθώς εξελίσσεται ο υπολογισμός. Οι καταστάσεις αναπαρίστανται στο δεκαεξαδικό σύστημα και η πιθανότητα αναπαρίσταται με χρώμα σύμφωνα με το υπόμνημα που βρίσκεται στο κάτω μέρος του παραθύρου. Τέλος, στην τρίτη γραφική παράσταση, φαίνεται με ποιο τρόπο αλλάζει η φάση των μιγαδικών πλατών των βασικών καταστάσεων. Και εδώ η κωδικοποίηση γίνεται με χρώμα.



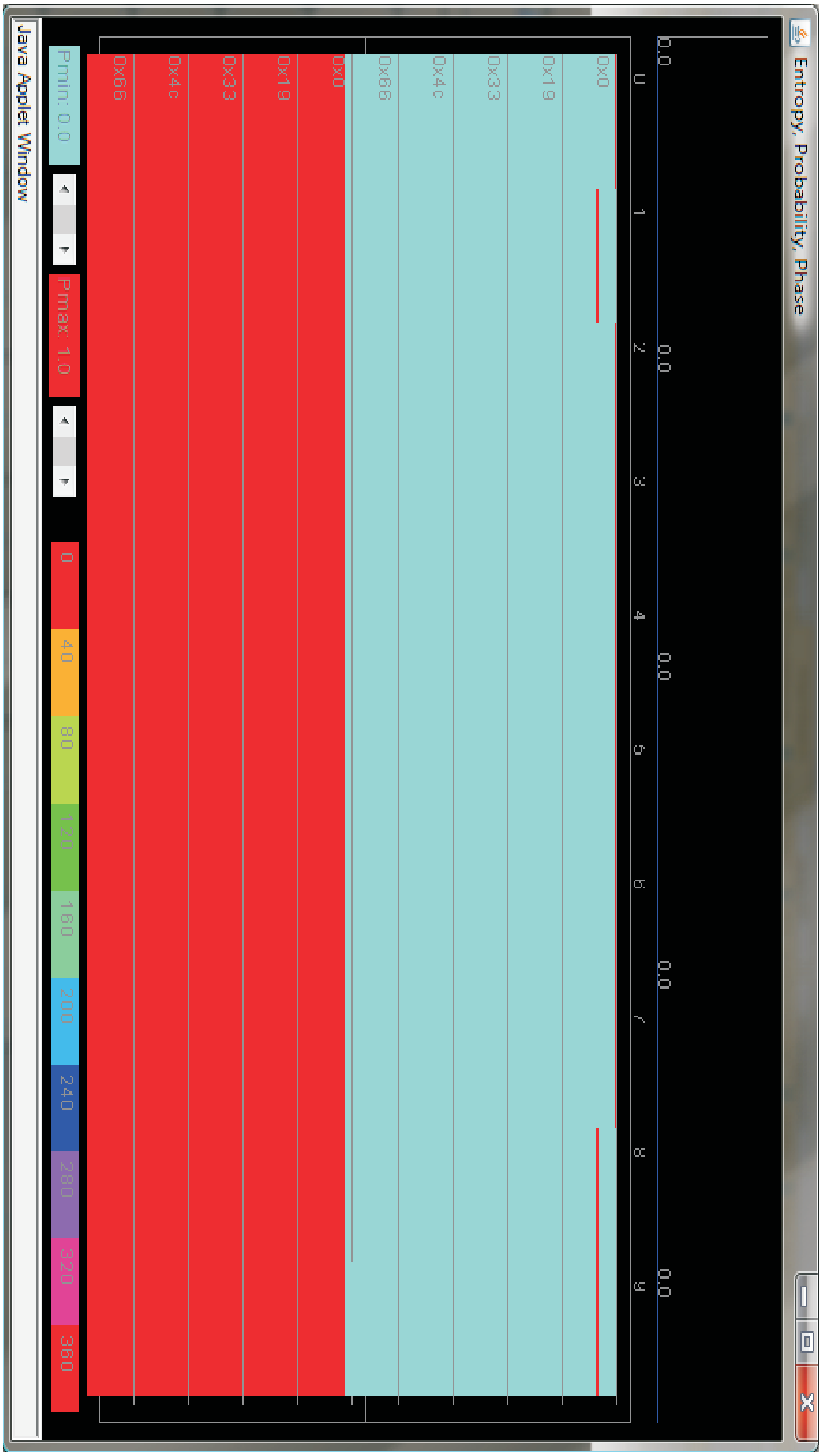
Σχήμα 4.24: Expression Estimator Circuit για ESOP 2 μεταβλητών εισόδου.



Σχήμα 4.25: Αποτελέσματα εξομοίωσης Expression Estimator.



Σχήμα 4.26: Comparator, 2x2 qubits.



Σχήμα 4.27: Αποτελέσματα Comparator.

Όπως είναι εύκολα αντιληπτό, η χρωματική κωδικοποίηση των αποτελεσμάτων δίνει μεν μια διαισθητική επισκόπηση των αποτελεσμάτων, αλλά δεν μπορεί να προσφέρει λεπτομερή απεικόνισή τους. Για να επιτευχθεί κάτι τέτοιο, ο χρήστης είναι δυνατόν να κάνει zoom σε μια περιοχή που θέλει να δει με μεγαλύτερη λεπτομέρεια χρησιμοποιώντας το ποντίκι για να μαρκάρει την περιοχή αυτή. Η διαδικασία μπορεί να επαναληφθεί μέχρι το επίπεδο των qubits όπου και φαίνονται αναλυτικά οι πιθανότητες. Εναλλακτικά, τα αποτελέσματα σε κάθε βήμα υπολογισμού είναι διαθέσιμα στο αρχείο της QML γλώσσας που χρησιμοποιείται για την αναπαράσταση του κυκλώματος και το οποίο μπορεί να κατεβάσει κάποιος όταν έχει ολοκληρωθεί η εξομοίωση. Η QML πλησιάζει αρκετά στη φυσική γλώσσα ώστε να είναι δυνατόν να εξάγει κάποιος τα ενδιάμεσα αποτελέσματα με σχετική ευκολία από τον τομέα <results> του αρχείου. Το κομμάτι αυτό μπορεί να φαίνεται όπως πιο κάτω.

4.11 Θεωρητική πολυπλοκότητα προτεινόμενων κβαντικών αλγορίθμων

Όπως φάνηκε στην Ενότητα 3.2.1 η θεωρητική πολυπλοκότητα του συμβατικού αλγορίθμου XMin, δεδομένης λογικής συνάρτησης εισόδου n μεταβλητών εισόδου, είναι (2^{2^n}).

Στον κβαντικό αλγόριθμο MOQMIN η υπολογιζόμενη χρονική πολυπλοκότητα προέρχεται τόσο από τις επαναλήψεις του αλγορίθμου του Grover όσο και από τους κβαντικούς τελεστές που χρησιμοποιούνται για τον υπολογισμό των διαφόρων φάσεων του τελεστή Oracle. Θεωρείται ότι κάθε κβαντικός τελεστής έχει χρονική πολυπλοκότητα σταθερή και ίση με 1. Είναι γνωστό ότι ο αλγόριθμος του Grover επαναλαμβάνει τον τελεστή Oracle για $\sqrt{}$ φορές όπου είναι ο αριθμός όλων των δυνατών στοιχείων. Θυμίζουμε ότι στον αλγόριθμό μας ο Grover εφαρμόζεται στη έξοδο για το βάρος της συνάρτησης εισόδου. Κατά συνέπεια αν έχουμε K bits για την απεικόνιση του βάρους της συνάρτησης εισόδου τότε όλα τα διαφορετικά "βάρη" που μπορούν να προκύψουν είναι 2^N και κατά συνέπεια χρειάζονται $(\sqrt{2^N})$ επαναλήψεις του τελεστή Oracle. Μένει λοιπόν να υπολογιστεί η πολυπλοκότητα του τελεστή Oracle. Λαμβάνοντας υπόψην την αναδρομική φύση του προτεινόμενου τελεστή Oracle του αλγορίθμου MOQMIN ισχύει: $O(1+(1+(\ldots+(1+3+K_0log(K_0))+\ldots)+K_{n-1}log(K_{n-1}))+K_nlog(K_n))+C$, όπου K_i και K είναι ο αριθμός των qubits που απαιτούνται για την απεικόνιση του βάρους της συνάρτησης στο κάθε επίπεδο της αναδρομής και C είναι ο αριθμός

των βημάτων που απαιτούνται από τον συγκριτή (Comparator). Στο τέλος της αναδρομής (επίπεδο 2 μεταβλητών για τις εκφράσεις ESCT και επίπεδο 1 μεταβλητής για τις εκφράσεις ESOP) η πολυπλοκότητα του καταληκτικού τελεστή LUT είναι: $O(1 + 3 + K_0 log(K_0))$ (προκύπτει εύκολα από την Εικόνα 4.15). Τέλος η πολυπλοκότητα του αθροιστή είναι $({}_i log(K_i))$. Έτσι η πολυπλοκότητα του αλγορίθμου MOQMIN είναι: $O(\sqrt{2^K}(1 + (1 + (\ldots + (1 + 3 + K_0 log(K_0)) + \ldots) + K_{n-1} log(K_{n-1})) + K_n log(K_n)) + C) = O(2^{K/2} \cdot (n + \sum_{i=0}^{n} K_i log(K_i)))$.

Χρησιμοποιώντας το ανάπτυγμα Shannon 2.1 μπορούμε εύκολα να υπολογίσουμε το χειρότερο άνω όριο για τα βάρη K και K_i για συναρτήσεις με περισσότερες από μία μεταβλητές εισόδου. Ισχύει: $K \leq log(2^n) \leq n$ (δεδομένου ότι το βάρος είναι το πολύ 1 για συνάρτηση μιας μεταβλητής εισόδου). Κατά συνέπεια η θεωρητική πολυπλοκότητα είναι $O(2^n)$.

Συγκρίνοντας τη πολυπλοκότητα του συμβατικού και του κβαντικού αλγορίθμου παρατηρείται ότι η πολυπλοκότητα του προβλήματος μειώνεται από διπλά εκθετική σε απλά εκθετική, κάτι που είναι ιδιαίτερα σημαντική βελτίωση. Παρόλα αυτά το πρόβλημα συνεχίζει να παραμένει ιδιαίτερα δύσκολο.

4.12 Μελλοντικές επεκτάσεις

Η δουλειά που παρουσιάστηκε παραπάνω, αν και έχει δώσει σημαντικά αποτελέσματα, δεν παύει να έχει περιθώρια βελτίωσης. Ενδεικτικά μπορούν να αναφερθεί η αναδιάρθρωση των κβαντικών αλγορίθμων που έχουν ήδη υλοποιηθεί ώστε να εκμεταλευτούν καλύτερα τις ειδικές ικανότες των κβαντικών υπολογιστών.

Κεφάλαιο 5

Κρυπτογράφηση με χρήση ESCT

Σε αυτήν την ενότητα θα παρουσιαστεί η εφαρμογή των προηγούμενων συμβατικών αλγορίθμων για την ελαχιστοποίηση ESCT εκφράσεων στον τομέα της κρυπτογράφησης.

Το πρόβλημα της εύρεσης ενός ελάχιστου μοντέλου για την διενέργεια ασφαλών υπολογισμών (secure computations) παρουσιάστηκε για πρώτη φορά από τους Feige, Kilian και Naor [61]. Πιο συγκεκριμένα, το πρόβλημα ορίζεται παρακάτω. Η Alice και ο Bob είναι δύο παίκτες που κατέχουν ιδιωτικά κλειδιά μεγέθους n bits $a \in \{0,1\}^n$ και $b \in \{0,1\}^n$ αντίστοιχα, καθώς επίσης μοιράζονται και μια τυχαία συμβολοσειρά. Και οι δύο έχουν σαν στόχο ένας τρίτος παίκτης, η Carol, να βρεί την έξοδο μιας συνάρτησης $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ χωρίς να αποκαλύψουν πληροφορίες σχετικά με τις εισόδους τους. Στους Alice και Bob επιτρέπεται να στείλουν ένα μοναδικό μήνυμα μέσω ενός ιδιωτικού καναλιού και θεωρούνται ότι δεν έχουν υπολογιστικούς περιορισμούς. Στο παρακάτω παράδειγμα θα γίνει περισσότερο κατανοητή η ιδέα πίσω από αυτό το μοντέλο.

Ας θεωρήσουμε την απλή περίπτωση όπου η Alice και ο Bob κατέχουν strings του ενός bit $a \in \{0,1\}$ και $b \in \{0,1\}$ αντίστοιχα. Επιθυμούν η Carol να μπορεί να υπολογίσει την συνάρτηση XOR $f(a,b) = a \oplus b$ χωρίς να χρειάζεται να αποκαλύψουν οποιαδήποτε πληροφορία σχετικά με τις εισόδους τους. Και οι δύο μοιράζονται ένα τυχαίο κλειδί $k \in \{0,1\}$. Αρχικά, η Alice στέλνει ένα μήνυμα ενός bit $a \oplus k$ μέσα από το ιδιωτικό κανάλι. Ο Bob κάνει το ίδιο στέλνοντας το μήνυμα $b \oplus k$. Η Carol λαμβάνει και τα δύο μηνύματα και υπολογίζει το $(a \oplus k) \oplus (b \oplus k) = a \oplus b$ που και και το επιθυμητό αποτέλεσμα. Είναι προφανές ότι τα μηνύματα που στέλνουν οι Alice και Bob παραμένουν κρυφά κατά τη διάρκεια όλης της διαδικασίας αφού στέλνονται μέσα από ιδιωτικά κανάλια και η Carol γνωρίζει μόνο το αποτέλεσμα της f αφού το string k είναι τυχαίο.

Από τα παραπάνω μπορούμε εύκολα να βρούμε το κόστος επικοινωνίας και τυχαιότητας αυτού του πρωτοκόλλου. Αν οι Alice και Bob στέλνουν n_a και n_b bits αντίστοιχα και το τυχαίο string είναι n_k bits τότε έχουμε ένα $(n_a, n_b; n_k)$-πρωτόκολλο. Αντίστοιχα το πρωτόκολλο του παραπάνω παραδείγματος είναι ένα $(1, 1; 1)$-πρωτόκολλο. Αντίστοιχα, οι Feige et. al. [61] παρουσιάζουν ένα πρωτόκολλο για ασφαλείς υπολογισμούς σύμφωνα με το οποίο για μια τυχαία συνάρτηση $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$, η ανταλλαγή μηνυμάτων έχει ως εξής: η Alice στέλνει ένα μήνυμα 2^n-bits, ενώ ο Bob στέλνει ένα μήνυμα $(n+1)$-bits στην Carol. Επιπλέον, χρησιμοποιείται ένα κοινό τυχαίο string μεγέθους $2^n + n$. Σε αυτήν την περίπτωση έχουμε ένα $(2^n, n+1; 2^n + n)$-πρωτόκολλο.

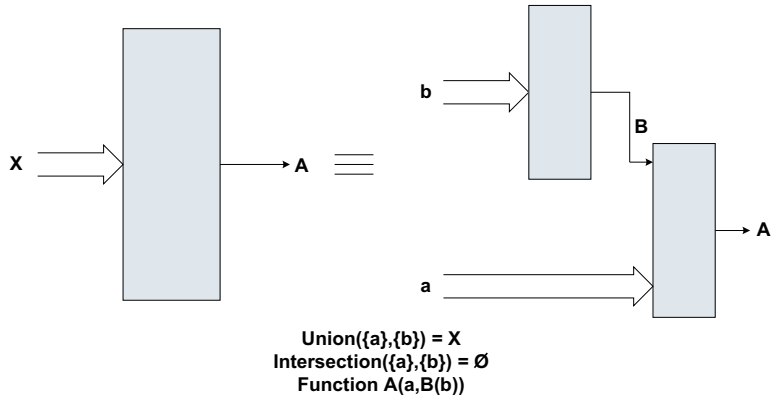
Το πρωτόκολλο που χρησιμοποιήθηκε στο πλαίσιο αυτής της εργασίας βασίζεται σε αυτό που παρουσιάστηκε από τους Mizuki et. al. [62, 63]. Το ελάχιστο μοντέλο που προτάθηκε βασίστηκε σε εκφράσεις ESOP καταλήγοντας με αυτό το τρόπο σε ένα $(2t, t+1; 3t)$-πρωτόκολλο, όπου t είναι ο αριθμός των όρων γινομένου μιας ελάχιστης έκφρασης ESOP της συνάρτησης $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$. Στην παραπάνω εργασία προτείνεται ένα πρωτόκολλο επικοινωνίας που βασίζεται στο γεγονός ότι κάθε συνάρτηση μπορεί να εκφραστεί με εκφράσεις ESOP. Η πολυπλοκότητα αυτού του πρωτοκόλλου είναι ευθέως ανάλογη του αριθμού των όρων γινομένου της ελάχιστης έκφρασης ESOP. Το πρωτόκολλο αυτό θα αναλυθεί λεπτομερώς στη συνέχεια.

Σε αυτήν την εργασία προτείνεται ένα γενικευμένο μοντέλο που δίνει αποτελέσματα καλύτερα από αυτά της βιβλιογραφίας. Πιο συγκεκριμένα, θα εξεταστεί η χρήση εκφράσεων αθροισμάτων αποκλειστικού Ή απλών ανεξάρτητων διασπάσεων (”exclusive-or” sum of simple disjoint decompositions (SDD)), ώστε να επιτευχθεί καλύτερη ελαχιστοποίηση του επικοινωνιακού κόστους. Ο προτεινόμενος γενικός φορμαλισμός εμπεριέχει ως ειδική περίπτωση την περίπτωση των εκφράσεων των Mizuki et. al. [62, 63]. Επιπλέον οι εκφράσεις ESCT υιοθετούνται σαν μια ειδική περίπτωση εκφράσεων αφού εξ ορισμού μπορούν να αντιστοιχηθούν σε ένα SDD και εμπεριέχουν τις εκφράσεις ESOP ως μια ειδική υποπερίπτωση. Ας σημειωθεί ότι η μοντελοποίηση με ESCT εκφράσεις βελτιώνει το επικοινωνιακό κόστος του προηγούμενου μοντέλου σε ποσοστό 40% περίπου.

5.1 Θεωρητικό Υπόβαθρο

Παρακάτω θα αναλυθεί το θεωρητικό υπόβαθρο για τις εκφράσεις SDD. Αντίστοιχη ανάλυση για τις ESCT εκφράσεις έχει γίνει σε προηγούμενο κεφάλαιο αλλά

επαναλαμβάνονται ορισμένα γενικά σημεία για λόγους επάρκειας.



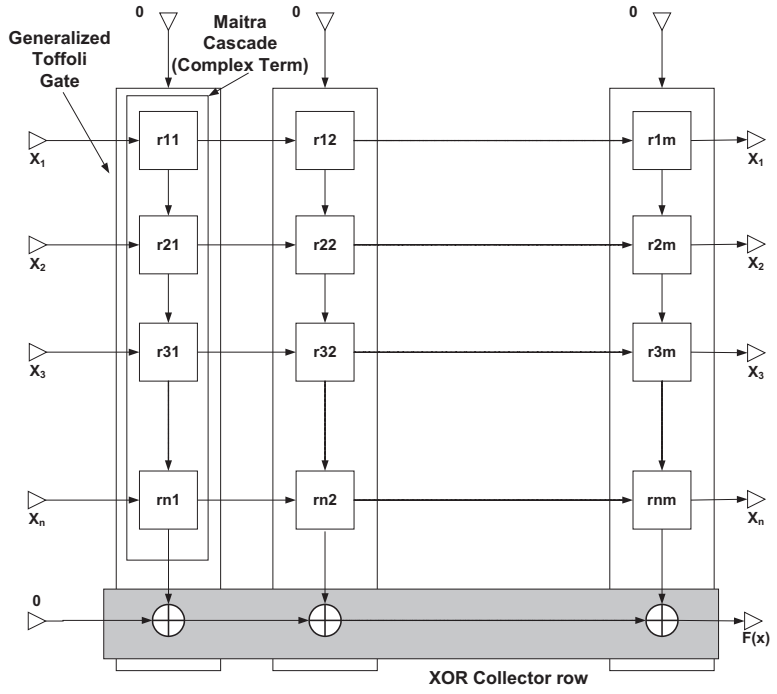
Σχήμα 5.1: Simple disjoint decomposition

Ο Ashenhurst [64] είχε εισάγει ένα εξαντλητικό μοντέλο για την σειριακή αποσύνθεση συναρτήσεων. Η βασική ιδέα ήταν να μετασχηματιστεί η συνάρτηση σε μια πολυεπίπεδη δομή που αποτελείται από σχετικά πιο απλές θεμελιώδεις δομές. Η διαδικασία αυτή δεν εξαρτάται από παραδοχές για την φύση αυτών δομών. Η SDD μιας συνάρτησης Boole είναι μια αναπαράσταση του τύπου $A(X) = A(a, B(b))$ με τα a και b να είναι σύνολα μεταβλητών που διαχωρίζουν το σύνολο X και οι A, B συναρτήσεις (σχήμα 5.1). Ο SDD έχει πολλές εφαρμογές στην επιστήμη των υπολογιστών και των διακριτών μαθηματικών, που περιλαμβάνουν την λογική σύνθεση [65], τα προβλήματα συνδυαστικής βελτιστοποίησης γράφων και δικτύων [66], την θεωρία της αξιοπιστίας (reliability theory) [67] και την θεωρία παιγνίων [68]. Είναι συνεπώς πολύ σημαντικό να υπάρχουν αποδοτικοί αλγόριθμοι που μπορούν να βρουν όλες τις δυνατές διασπάσεις για μια συνάρτηση. Παρόλα αυτά, σε ότι αφορά τις συναρτήσεις Boole, οι υπάρχουσες μέθοδοι έχουν να κάνουν είτε με την επίλυση NP-complete προβλημάτων ή έχουν εκθετικό χρόνο εκτέλεσης, όντας για αυτούς τους λόγους μη αποδοτικές.

Ας θεωρήσουμε δυαδικές μεταβλητές x_i, μια δυαδική σταθερά y και τυχαίες δυαδικές συναρτήσεις δύο εισόδων και μιας εξόδου G_i με $(1 \leq i \leq r)$. Τότε η
$U = G_r(x_r, G_{r-1}(x_{r-1}, G_{r-2}(x_{r-2}, \ldots, G_1(x_1, y))))$
είναι ένας σύνθετος όρος n μεταβλητών (ή όρος Maitra) που εξαρτάται από τις μεταβλητές $x_1, \ldots, x_r$. Οι συναρτήσεις G_i, όπως έχουμε δει, ονομάζονται cell functions.

Η συνάρτηση G_i μπορεί να είναι οποιαδήποτε συνάρτηση δύο εισόδων και μιας εξόδου. Όπως έχει αποδειχθεί από τον Minnick [15], είναι αρκετό η G_i να είναι μια από τις έξι συναρτήσεις $x + y$ (cell 1), $\overline{x} + y$ (cell 2), $\overline{x}y$ (cell 3), xy (cell 4),

$x \oplus y$ (cell 5), y (cell 6).



Σχήμα 5.2: Reversible wave cascade CA.

Μια έκφραση ESCT είναι πρακτικά ένα άθροισμα αποκλειστικού Ή σύνθετων όρων:

$$Q = \sum_{i=1}^{m} \oplus M_i,$$

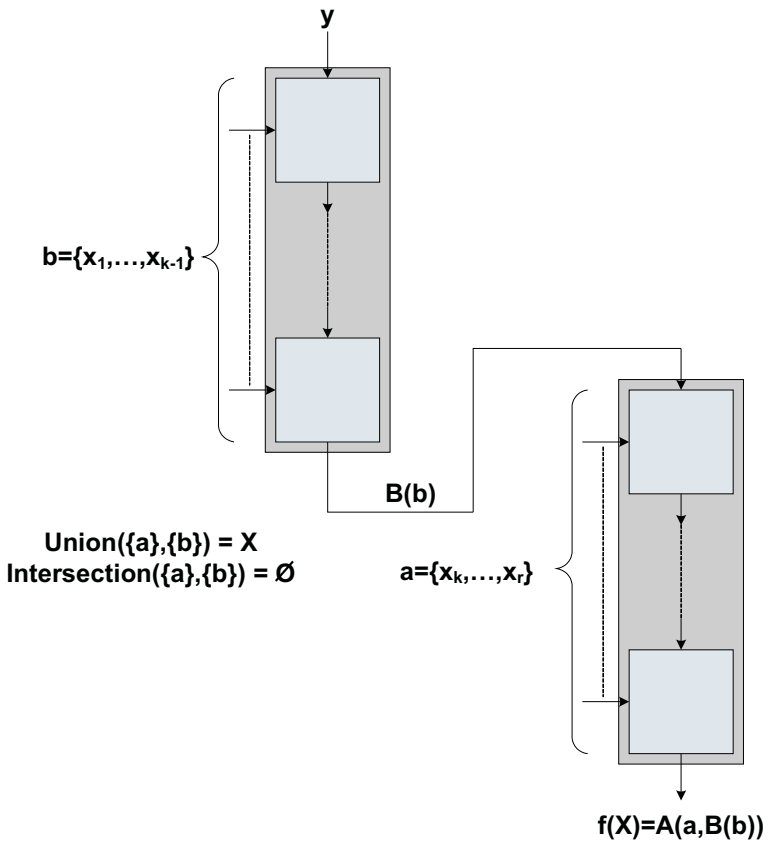
όπου οι M_i είναι σύνθετοι όροι και m το πλήθος τους στην έκφραση. Η αντίστοιχη αρχιτεκτονική φαίνεται στο σχήμα 5.2. Αν χρησιμοποιήσουμε μόνο κύτταρα τύπου 3, 4 ή 6 τότε οι εκφράσεις ESCT υποβιβάζονται σε εκφράσεις ESOP.

Είναι προφανές ότι απλά και μόνο με τη χρήση πιο σύνθετων εκφράσεων όπως οι ESCT μπορούμε να πετύχουμε πολύ μικρότερο αριθμό όρων. Πιο συγκεκριμένα, μια ESCT έκφραση μπορεί να έχει περίπου 40% λιγότερους όρους από την αντίστοιχη ESOP έκφραση.

Επιπλέον, έχουν αναπτυχθεί αρκετοί αλγόριθμοι (τόσο ακριβείς όσο και ευριστικοί) για την ελαχιστοποίηση ESOP και ESCT εκφράσεων. Όπως έχει αναφερθεί, υπάρχουν αλγόριθμοι για την ελαχιστοποίηση εκφράσεων ESOP ή ESCT για τυχαίες, πλήρως ορισμένες συναρτήσεις με περιορισμούς ως προς τον αριθμό μεταβλητών εισόδου ή τον αριθμό των όρων στην ελάχιστη έκφραση [36, 69, 70, 7, 71, 10, 1]. Άλλοι αλγόριθμοι έχουν σχεδιαστεί για να βρίσκουν σχεδόν ελάχιστες εκφράσεις ESOP ή ESCT για περισσότερες μεταβλητές εισόδου [71, 1, 28, 11, 26,

72]. Τέλος έχουν αναπτυχθεί ακόμα και κβαντικοί αλγόριθμοι για το σκοπό αυτό [73, 56, 57].

Είναι προφανές ότι οι ESCT εκφράσεις είναι μια ειδική περίπτωση εκφράσεων αθροίσματος αποκλειστικού Ή SDD εκφράσεων. Πράγματι, η έκφραση $G_r(x_r, G_{r-1}(x_{r-1}, G_{r-2}(x_{r-2}, \ldots, G_1(x_1, y))\ldots))$ μπορεί να γραφεί και $G_r(x_r, G_{r-1}(x_{r-1}, G_{r-2}(x_{r-2}, \ldots, G_k(x_k, G'))\ldots))$, όπου $G' = (x_{k-1}, G_{k-1}(\ldots, G_1(x_1, y)))$ ή διαφορετικά $G_r(x_r, G_{r-1}(x_{r-1}, \ldots, x_k, G'(x_{k-1}, \ldots, x_1))\ldots)) = G''(x_r, \ldots, x_k, G'(x_{k-1}, \ldots, x_1))$. Αυτό μπορεί να γίνει φανερό στο σχήμα 5.3 όπου $B(x_{n-1}, \ldots, x_1) = G'(x_{k-1}, \ldots, x_1)$ και $A(x_n, \ldots, x_k) = G''(x_n, \ldots, x_k)$, με $k = n$ και $r = 2n$.



Σχήμα 5.3: ESCT as special case of SDD with k=n and r=2n

5.2 Πρωτόκολλο με χρήση εκφράσεων SDD

Σε αυτή την ενότητα θα παρουσιαστεί το πρωτόκολλο επικοινωνίας. Το πρωτόκολλο αυτό βασίζεται σε αυτό των Mizuki et. al. [62, 63] με τη διαφορά ότι τώρα τροποποιήθηκε ώστε να μπορεί να χειρίζεται εκφράσεις SDD.

Ας υποθέσουμε ότι η Alice και ο Bob επιθυμούν να υπολογίσουν με ασφάλεια μια συνάρτηση f τέτοια ώστε $f : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ χωρίς να αποκαλυφθούν πληροφορίες που δεν είναι απαραίτητες για αυτή τη διαδικασία. Και οι δύο κατέχουν ιδιωτικές συμβολοσειρές εισόδου $a \in \{0,1\}^n$ και $b \in \{0,1\}^n$. Το βασικό σχήμα επικοινωνίας περιγράφεται παρακάτω.

1. Υπολογισμός μιας ελάχιστης (ή σχεδόν ελάχιστης) έκφρασης SDD για την f έστω $f(a,b) = A_1(a, B_1(b)) \oplus A_2(a, B_2(b)) \oplus \ldots \oplus A_t(a, B_t(b))$ όπου A_i και $B_i, 1 \leq i \leq t$ είναι σύνθετοι όροι τέτοιοι ώστε $A_i : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$ and $B_i : \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}$.

2. Για κάθε σύνθετο όρο $A_i(a, B_i(b))$, η Alice και ο Bob στέλνουν στην Carol μέσα από ιδιωτικό κανάλι την τιμή $A_i(a, B_i(b)) \oplus K^i$ όπου το $K^i \in \{0,1\}$ είναι ένα τυχαίο κλειδί γνωστό μόνο στον Bob.

3. Η Carol έχει λάβει t μηνύματα του ενός bit $A_i(a, B_i(b)) \oplus K^i, 1 \leq i \leq t$ και ο Bob μεταδίδει το μήνυμα $K^1 \oplus K^2 \oplus \ldots \oplus K^t$ (1-bit). Η Carol το μόνο που έχει να κάνει είναι να προσθέσει αυτό το μήνυμα σε αυτά που είχε λάβει προηγουμένως $\bigoplus_{i=1}^{t} A_i(a, B_i(b)) \oplus K^i$ έτσι ώστε να μάθει την τιμή της f.

5.2.1 Λεπτομερές Πρωτόκολλο

Προσαρμόζοντας την ανάλυση από τους Mizuki et. al. [62, 63] στο παρόν σχήμα επικοινωνίας λαμβάνουμε το παρακάτω πρωτόκολλο. Έστω A και B συναρτήσεις τέτοιες ώστε $A : \{0,1\}^n \rightarrow \{0,1\}$ και $B : \{0,1\}^n \rightarrow \{0,1\}$. Έστω επίσης $a \in \{0,1\}^n$ και $b \in \{0,1\}^n$ είναι οι συμβολοσειρές που κατέχουν η Alice και ο Bob αντίστοιχα. Ο στόχος είναι να μάθει η Carol την τιμή $A(a, B(b)) \oplus k$ όπου k είναι ένα τυχαίο κλειδί που γνωρίζει μόνο ο Bob.

Για να αναλυθεί περαιτέρω το πρωτόκολλο, θα πρέπει να οριστούν κάποιες ειδικές πράξεις. Δεδομένου ενός μηνύματος 2-bit (x, y), ορίζονται οι πράξεις **shift** και **get** ως εξής.

- **shift**$^0(x, y) = (x, y)$
- **shift**$^1(x, y) = (y, x)$
- **get**$^0(x, y) = x$
- **get**$^1(x, y) = y$

Με άλλα λόγια, η **shift**^{0} επιστρέφει τις εισόδους χωρίς αλλαγές, η **shift**^{1} ανταλλάσσει τις εισόδους, η **get**^{0} επιστρέφει το πρώτο bit της εισόδου και η **get**^{1} το δεύτερο bit.

Η Alice και ο Bob μοιράζονται ένα 3-bit τυχαίο κλειδί $((K^0, K^1), s)$. Τα δύο πρώτα bits χρησιμοποιούνται για την κρυπτογράφηση του μηνύματος και το τρίτο για την αναδιάταξη του μηνύματος. Η Alice και ο Bob πραγματοποιούν τα ακόλουθα βήματα.

- Το $B(b)$ μπορεί να είναι 0 ή 1. Λαμβάνοντας υπόψη όλες τις πιθανότητες, η Alice δημιουργεί ένα 2-bit μήνυμα $(A(a,0), A(a,1)$ και το κρυπτογραφεί χρησιμοποιώντας το κλειδί (K^0, K^1). Επομένως το μήνυμα τώρα είναι $(A(a,0) \oplus K^0, A(a,1) \oplus K^1$. Επιπλέον, η Alice αναδιατάσσει το μήνυμα χρησιμοποιώντας το τυχαίο bit s. Τώρα το μήνυμα γίνεται **shift**$^s((A(a,0) \oplus K^0, A(a,1) \oplus K^1)$ και στέλνεται στην Carol. Ανάλογα με τη τιμή του s το μήνυμα παίρνει τις δύο παρακάτω μορφές.

$$\begin{cases} (A(a,0) \oplus K^0, A(a,1) \oplus K^1)\ if\ \text{s=0} \\ (A(a,1) \oplus K^1, A(a,0) \oplus K^0)\ if\ \text{s=1} \end{cases}$$

- Από την άλλη μεριά ο Bob γνωρίζει ότι αν $B(b) = s$ τότε το πρώτο bit που θα λάβει η Carol θα είναι το σωστό. Σε διαφορετική περίπτωση, το σωστό bit είναι το δεύτερο. Συνεπώς ο Bob στέλνει στην Carol το $B(b) \oplus s$.

- Η Carol λαμβάνει την 1-bit τιμή **get**$^{B(b)\oplus s}$**shift**$^s((A(a,0) \oplus K^0, A(a,1) \oplus K^1)$ που είναι ίση με $A(a, B(b)) \oplus K^{B(b)}$ κάτι το οποίο μπορεί εύκολα να επαληθευτεί εξετάζοντας όλους τους συνδυασμούς της τιμής $B(b)$.

Το παραπάνω πρωτόκολλο, το οποίο είναι ένα $(2, 1; 3)$-πρωτόκολλο επιτυγχάνει ασφαλή υπολογισμό αφού μόνο η Alice και ο Bob γνωρίζουν το τυχαίο κλειδί $K^{B(b)}$.

5.2.2 Γενίκευση του Πρωτοκόλλου

Λαμβάνοντας υπόψη την παραπάνω ανάλυση, μπορούμε να διατυπώσουμε μια πιο γενικευμένη περιγραφή που πρωτοκόλλου.

Έστω συνάρτηση f τέτοια ώστε $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ και έστω η έκφραση $f(a,b) = A_1(a, B_1(b)) \oplus A_2(a, B_2(b)) \oplus \ldots \oplus A_t(a, B_t(b))$ είναι ένας SDD της συνάρτησης $f(a,b)$. Η Alice και ο Bob μοιράζονται ένα $3t$-bit τυχαίο κλειδί $(((K_1^0, K_1^1), s_1), ((K_2^0, K_2^1), s_2) \ldots ((K_t^0, K_t^1), s_t)$. Επίσης η Alice και ο Bob έχουν

ιδιωτικές συμβολοσειρές εισόδου $a \in \{0,1\}^n$ και $b \in \{0,1\}^n$ αντίστοιχα. Η επικοινωνία έχει ως εξής.

- Η Alice στέλνει ένα $2t$-bit μήνυμα στην Carol τέτοιο ώστε $(\mathbf{shift}^{s_1}(A_1(a,0) \oplus K_1^0, A_1(a,1) \oplus K_1^1)$, $\mathbf{shift}^{s_2}(A_2(a,0) \oplus K_2^0, A_2(a,1) \oplus K_2^1)$,…,$\mathbf{shift}^{s_t}(A_t(a,0) \oplus K_t^0, A_t(a,1) \oplus K_t^1))$
- Ο Bob στέλνει ακολούθως 2 διαφορετικά μηνύματα. Το πρώτο είναι ένα t-bit μήνυμα $(B_1(b) \oplus s_1, B_2(b) \oplus s_2, \ldots, B_t(b) \oplus s_t)$, ενώ το δεύτερο είναι ένα 1-bit μήνυμα $\bigoplus_{i=1}^{t} K_i^{B_i(b)} = K_1^{B_1(b)} \oplus K_2^{B_2(b)} \ldots K_t^{B_t(b)}$
- Τελικά η Carol υπολογίζει τη τιμή $\bigoplus_{i=1}^{t} \mathbf{get}^{B_i(b) \oplus s_i}(\mathbf{shift}^{s_i}(K_i^0, A_i(a, B_i(b)) \oplus K_i^1)) \oplus \bigoplus_{i=1}^{t} K_i^{B_i(b)}$

Από την παραπάνω ανάλυση, είναι προφανές ότι το προτεινόμενο πρωτόκολλο είναι ένα $(2t, t+1; 3t)$-πρωτόκολλο.

Το προτεινόμενο πρωτόκολλο έχει τις ίδιες ιδιότητες ασφάλειας και ομοιομορφίας με αυτό που προτάθηκε από τους Mizuki et. al. [62, 63]. Η κύρια διαφορά είναι η χρήση SDDs αντί για εκφράσεις ESOP για την αναπαράσταση της συνάρτησης. Στη πράξη μπορούμε να χρησιμοποιήσουμε εκφράσεις ESCT σαν μια ειδική περίπτωση SDD όπως έχει δειχθεί στην ενότητα 5.1. Για αυτό το σκοπό θέτουμε $r = 2n$ και $k = n$. Αυτό οδηγεί σε πολύ μικρότερο αριθμό όρων σε σχέση με τις εκφράσεις ESOP κάτι που καθορίζει την πολυπλοκότητα του πρωτοκόλλου.

Χρησιμοποιώντας αποτελέσματα από την βιβλιογραφία [70, 71, 28, 72, 36, 69, 60] προκύπτει ο παρακάτω πίνακας 5.1. Έχουν ληφθεί υπόψη οι καλύτερες λύσεις για εκφράσεις ESOP και ESCT για συναρτήσεις της βιβλιοθήκης MCNC [74]. Συνεπώς, μπορούμε να συμπεράνουμε ότι χρησιμοποιώντας εκφράσεις ESCT αντί για ESOP έχουμε μια αξιοσημείωτη μείωση στον αριθμό των όρων στο άθροισμα αποκλειστικού Ή και κατ' επέκταση στη πολυπλοκότητα επικοινωνίας του προτεινόμενου πρωτοκόλλου.

Παρά την ουσιαστική μείωση της πολυπλοκότητας επικοινωνίας, το πρόβλημα της αποδοτικής ελαχιστοποίησης για πολλές μεταβλητές παραμένει. Η πιο πολλά υποσχόμενη μέθοδος είναι αυτή που παρουσιάστηκε στο προηγούμενο κεφάλαιο και βασίζεται σε κβαντικούς υπολογιστές.

Πίνακας 5.1: Benchmark functions.

Name	ESOP Terms	ESCT Terms
5xp1	31	20
9sym	51	34
com1	9	6
inc	31	15
f51m	31	19
misex1	12	11
rd53	14	7
rd73	35	19
rd84	57	30
t481	13	10
Total	**280**	**171**
Average Terms	**28**	**17.1**
Reduction	**39%**	

Κεφάλαιο 6

Συμπεράσματα - Μελλοντικές

Στην εργασία αυτή παρουσιάστηκε ένα ιδιαίτερα ενδιαφέρον και δύσκολο πρόβλημα, αυτό της ελαχιστοποίησης λογικών εκφράσεων. Τομ πρόβλημα αυτό ανήκει στη κατηγορία των NP προβλημάτων και συνεπώς είναι αδύνατο να βρεθεί αλγόριθμος για την εύρεση εκφράσεων ESOP ή ESCT, ο οποίος θα είναι αρκετά αποδοτικός στη γενική περίπτωση. Συνεπώς, η τακτική μας προσανατολίστηκε στην εύρεση τεχνικών και μεθοδολογιών που θα βελτίωναν όσο το δυνατόν περισσότερο την απόδοση των αλγορίθμων. Επίσης, στη διατριβή αυτή παρουσιάστηκε ένας συμπαγές θεωρητικό πλαίσιο για την ακριβή ελαχιστοποίηση ESCT και ESOP εκφράσεων. Με αυτό τον τρόπο πετύχαμε πρακτικά την δημιουργία αλγορίθμου για την ακριβή ελαχιστοποίηση ESCT εκφράσεων μέχρι και 6 μεταβλητών εισόδου, αλλά και γενικότερα παρουσιάστηκε ο θεωρητικός φορμαλισμός για την ελαχιστοποίηση των εκφράσεων αυτών για τυχαία συνάρτηση, ανεξαρτήτως του βάρους της. Επιπλέον αναπτύχθηκε θεωρία για την εύρεση ελαχίστων εκφράσεων ESCT με 7 όρους το πολύ (ανεξαρτήτως του αριθμού των μεταβλητών εισόδου του).

Επιπλέον, μελετήθηκε η επίδραση της διάταξης των μεταβλητών εισόδου στο βάρος μιας έκφρασης ESCT. Όπως είναι γνωστό, η διάταξη των μεταβλητών εισόδου αποτελεί σημαντικό παράγοντα του βάρους της συνάρτησης. Στα πλαίσια αυτών των παρατηρήσεων αναπτύχθηκε ευριστικός αλγόριθμος για την εύρεση μια καλής τέτοιας αναδιάταξης.

Η πορεία της διατριβής ακολούθησε την φυσική εξέλιξη της αρχιτεκτονικής Maitra, που δεν είναι άλλη από τα κβαντικά κυκλώματα. Η έρευνα στο τομέα αυτό προχώρησε παράλληλα και συμπληρωματικά με τα προηγούμενα, αφού το ερευνητικό αυτό πεδίο είναι ακόμα στα αρχικά του στάδια. Πιο συγκεκριμένα αναπτύχθηκαν κβαντικοί αλγόριθμοι που λύνουν αποδοτικά τα παραπάνω προβλήματα,

πετυχαίνοντας θεαματική βελτίωση στην χρονική πολυπλοκότητα. Οι αλγόριθμοι αυτοί αν και έχουν εντελώς διαφορετική φιλοσοφία υλοποίησης βασίστηκαν στο ίδιο θεωρητικό υπόβαθρο με τα προηγούμενα προβλήματα. Αν και η λύση των κβαντικών κυκλωμάτων φαντάζει αρκετά μακρινή, οι εξελίξεις στο τομέα μας εκπλήσσουν καθημερινά. Φυσικά, οι κβαντικοί υπολογιστές δεν αποτελούν λύση για οποιοδήποτε δύσκολο πρόβλημα αφού υπάρχουν και εκεί εγγενείς περιορισμοί. Παρόλα αυτά, η πορεία των πραγμάτων δείχνει μέχρι στιγμής προς μια υβριδική τεχνολογία οπού κβαντικά κυκλώματα θα επεμβαίνουν για την επίλυση κάποιων δύσκολων προβλημάτων σε ένα συμβατικό ολοκληρωμένο κύκλωμα.

Τέλος, αναζητήθηκαν εφαρμογές των εκφράσεων ESCT στο τομέα της κρυπτογράφησης. Τα αποτελέσματα αυτής της μελέτης οδήγησαν στην εύρεσης σχημάτων κρυπτογράφησης βασισμένων σε εκφράσεις ESCT που παρουσιάζουν σημαντική βελτίωση (39%) στο κόστος επικοινωνίας σε σχέση με σχήματα κρυπτογράφησης βασισμένα σε εκφράσεις ESOP.

Το πεδίο έρευνας αφήνει πολλά περιθώρια για νέες αναζητήσεις. Ενδεικτικά, η ενοποίηση της θεωρίας ελαχιστοποίησης των εκφράσεων ESOP και ESCT αποτελεί ένα αρκετά ανεξερεύνητο πεδίο που παρουσιάζει μεγάλο ενδιαφέρον, αλλά και δυσκολίες. Έχουν γίνει ήδη κάποιες προσπάθειες για την ανάπτυξη κανόνων συγχώνευσης συγγενών όρων που αναδεικνύουν ουσιαστικά ομοιότητες των δύο θεωριών και στοχεύουν προς μια ενοποιημένη θεωρία, αλλά απαιτείται σημαντική δουλειά ακόμα.

Επιπλέον, έχει αρχίσει μια προσπάθεια για την μετατροπή του προβλήματος ελαχιστοποίησης λογικών παραστάσεων σε ένα πρόβλημα επίλυσης συστημάτων εξισώσεων. Πιο συγκεκριμένα, το πρόβλημα της ελαχιστοποίησης μιας συνάρτησης μετατρέπεται σε ένα σύστημα εξισώσεων δυαδικών μεταβλητών και περιορισμών που πρέπει να ικανοποιηθούν. Με αυτό το τρόπο, μπορούμε να εξετάσουμε με ευκολία την αποδοτικότητα διαφόρων αριθμητικών μεθόδων (επιλυτές συστημάτων, optimizers κτλ) και ενδεχομένως να πάρουμε καλύτερα αποτελέσματα.

Από τη σκοπιά των κβαντικών υπολογιστών, υπάρχουν διάφορα ανοικτά ζητήματα. Ένα από αυτά είναι η πρακτική αντιστοίχηση των κυψελωτών διατάξεων Maitra με βασικές κβαντικές πύλες με τρόπο που θα αποφευχθεί η ύπαρξη περιττών εισόδων ελέγχουν (garbage inputs). Το πρόβλημα αυτό είναι πολύ σημαντικό αφού όσα περισσότερα qubits έχει ένας κβαντικός καταχωρητής, τόσο δυσκολότερη είναι η κατασκευή του και λειτουργία του, λόγω του αυξημένου κινδύνου απώλειας της συνεκτικότητας. Ένα ακόμα ζήτημα είναι η βελτίωση των υπαρχόντων αλγορίθμων (ή τουλάχιστον η απόδειξη του βέλτιστου) με την υιοθέτηση ενός

νέου, ριζοσπαστικά διαφορετικού, θεωρητικού φορμαλισμού που θα εκμεταλλεύεται πλήρως τις δυνατότητες των κβαντικών αλγορίθμων.

Βιβλιογραφία

[1] A. Gaidukov. Algorithm to derive minimum esop for 6-variable function. In *5th IWBP*, September 2002.

[2] T. Sasao. *Switching theory for logic synthesis*. Kluwer Academic Publishers, 1999.

[3] H. Wu I. Schaefer, M. Perkowski. Multilevel logic synthesis for cellular fpgas based on orthogonal expansions. In *IFIP WG 10.5 Workshop on Applications of the Reed-Muller expansion in Circuit Design*, pages 42–51, Hamburg, Germany, 1993.

[4] M. Helliwell and M. Perkowski. A fast algorithm to minimize multi-output mixed-polarity generalized reed-muller forms. In *25th ACM/IEEE Conference on Design Automation*, pages 427–432, 1988.

[5] M. Chrzanowska-Jeske M. Perkowski. An exact algorithm to minimize mixed-radix exclusive sums of products for incompletely specified boolean functions. In *ISCAS 90*, pages 1625–1655, 1990.

[6] N. Koda and T. Sasao. Lp characteristic vector for logic functions, 1993.

[7] T. Sato T. Hirayama, Y. Nishitani. A faster algorithm of minimizing and-exor expressions. *IEICE Transactions on Fundamentals*, E85-A(12):2708–2714, 2002.

[8] S. Stergiou and G. Papakonstantinou. An efficient algorithm for exact esop minimization. In *The 2002 Int. Conf. on VLSI*, June 2002.

[9] S. Stergiou and G. Papakonstantinou. Towards a general novel exact esop minimization methodology. In *6th Intrn. Workshop on Appl. of the Reed Muller Expansion in Circuit Design*, March 2003.

[10] S. Stergiou and G. Papakonstantinou. Exact minimization of esop expressions with less than eight product terms. *Journal of Circuits, Systems, and Computers*, 13(1):1–15, 2004.

[11] A. Mishchenko and M. Perkowski. Fast heuristic minimization of exclusive sums-of-products. In *5th International Workshop on Applications of the Reed Muller Expansion in Circuit Design*, August 2001.

[12] T. Sasao. Exmin2: A simplification algorithm for exclusive-or sum-of-products expressions for multiple-valued input two-valued output functions. *IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems*, 12(5):621–632, May 1993.

[13] D. Popel A. Dani. Minimizing esop expressions using fractals. In *10th International Workshop on Post-Binary VLSI systems*, May 2001.

[14] V. Shmerko, D. Popel, R. Stankovic, V. Cheushev, and S. Yanushkevich. And/exor minimization of switching functions based on information-theoretical approach. *Facta Universitatis Journal, Series: Electronics and Energetics (Yugoslavia)*, 13(1):11–25, 2000.

[15] R.C Minnick. Cutpoint cellular logic. *IEEE Transactions on Electron. Computation*, EC-13, 1964.

[16] A. Mukhopadhayay. Unata cellular logic. *IEEE Transactions on Computers*, C-18(2):114–121, Feb 1969.

[17] G. Papakonstantinou. Cascade transformation. *IEEE Transactions on computers*, 25(1):93–95, 1976.

[18] G. Papakonstantinou. Modulo-2 expressions of switching functions. *Electronic Letters*, 12(10):244–245, 1977.

[19] G. Papakonstantinou. Synthesis of cutpoing cellular arrays with exclusive-or collector row. *Electronic Letters*, 13, 1977.

[20] M. Chrzanowska-Jeske M. Perkowski A. Sarabi, N. Song. A comprehensive approach to logic synthesis and physical design for two-dimensional logic arrays. In *Design Automation Conference*, pages 321–326, 1994.

[21] B. Becker P. Lindgren, R. Drechsler. Look-up table fpga synthesis from minimized multi-valued pseudo kronecker expressions. In *28th IEEE International Symposium on Multiple-Valued Logic*, pages 95–100, 1998.

[22] P. Lindgren, R. Drechsler, and B. Becker. Improved minimization methods of pseudo kronecker expressions for multiple output functions. In *International Symposium on Circuits and Systems*, pages 187–190, 1998.

[23] N. Song and M. Perkowski. Minimization of exclusive sums of multi-valued complex terms for logic cell arrays. In *28th IEEE Intl. Symposium on MV Logic*, pages 32–37, 1998.

[24] N. Song and M. Perkowski. A new approach to and/or/exor factorization for regular arrays. In *1998 Euromicro*, pages 269–276, Vasteras, Sweden, 1998.

[25] R. Drechsler G. Lee. Etdd-based synthesis of term-based fpgas for incompletely specified boolean functions. In *Asia and South Pacific Design Automation Conference 1998*, pages 75–80, 1998.

[26] G. Lee. Logic synthesis for celullar architecture fpga using bdd. In *Asia and South Pacific Design Automation Conference 1997*, pages 253–258, 1997.

[27] S. Park G. Lee. Logic synthesis for cellular architecture fpgas using exor ternary decision diagrams. *IEEE Transactions on fundamentals*, E80-A(10):1820–1825, 1997.

[28] M. Perkowski A. Mishchenko. Logic synthesis of reversible wave cascades. In *International Workshop on Logic And Synthesis 2002*, pages 197–202, New Orleans, Louisiana, 2002.

[29] M. Thornton L. Li and M. Perkowski. A quantum cad accelerator based on grover's algorithm for finding the minimum fixed polarity reed-muller form. In *Proc. of the ISMVL'06*, volume 00, pages 17–20, May 2006.

[30] Δ. Βουδούρης. *Διδακτορική Διατριβή - Ελαχιστοποίηση εκφράσεων αποκλειστικού Ή*. Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα, 2008.

[31] K.K. Maitra. Cascaded switching networks of two-input flexible cells. *IRE Trans. Electron. Computers*, 1962.

[32] Michael P. Frank. Introduction to reversible computing: motivation, progress, and challenges. In *CF '05: Proceedings of the 2nd conference on Computing frontiers*, pages 385–390, New York, NY, USA, 2005. ACM.

[33] A. De Vos and Y. Van Rentergem. Synthesis of reversible circuits. In *Proceedings of the 14-th International Workshop on Logic and Synthesis*, pages 101–108, 2005.

[34] Yvan Van Rentergem, Alexis De Vos, and Koen De Keyser. Six synthesis methods for reversible logic. *Open Systems & Information Dynamics*, 14(1):91–116, 2007.

[35] ATMEL Corporation. *ATMEL Coprocessor Field Programmable Gate Arrays, AT6000(LV) Series*. ATMEL Corporation, 1999.

[36] G. Papakonstantinou D. Voudouris, S. Stergiou. Minimization of reversible wave cascades. *IEICE Trans. on Fundamentals*, E88-A(4):1015–1023, 2005/04.

[37] Gabriela M. Marinescu Dan C. Marinescu. *Approaching Quantum Computing*. Prentice Hall, 2004.

[38] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. In *SIAM J. Computing 26*, pages 1484–1509, 1997.

[39] L.K. Grover. A fast quantum mechanical algorithm for database search. In *Proc. 28th Annual ACM Symposium on Theory of Computation*, pages 212–219, 1996.

[40] J.S. Bell. On the einstein-poldolsky-rosen paradox. *Physics*, 195(1), 1964.

[41] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. volume 299, page 802, 1982.

[42] K. Mattle M. Eibl H. Weinfurter D. Bouwmeester, J.-W. Pan and A. Zeilinger. Experimental quantum teleportation. volume 390.

[43] F. De Martini L. Hardy D. Boschi, S. Branca and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and einstein-podolsky-rosen channels. volume 80.

[44] W. Tittel H. Zbinden I. Marcikic, H. de Riedmatten and N. Gisin. Long-distance teleportation of qubits at telecommunication wavelengths. volume 421.

[45] R. Ursin et al. Quantum teleportation link across the danube. volume 430.

[46] P. Maunz D. Hayes L.-M. Duan S. Olmschenk, D. N. Matsukevich and C. Monroe. Quantum teleportation between distant matter qubits. volume 323.

[47] C. F. Roos W. Hänsel M. Ruth J. Benhelm G. P. T. Lancaster T. W. Körber C. Becher F. Schmidt-Kaler D. F. V. James M. Riebe, H. Häffner and R. Blatt. Deterministic quantum teleportation with atoms. volume 429.

[48] T. Schaetz J. Britton W. M. Itano J. D. Jost E. Knill C. Langer D. Leibfried R. Ozeri M. D. Barrett, J. Chiaverini and D. J. Wineland. Deterministic quantum teleportation of atomic qubits. volume 429.

[49] D.P. DiVincenzo D.A. Lidar D. Bacon, J. Kempe and K.B. Whaley. Encoded universality in physical implementations of a quantum computer. In *International Conference on Experimental Implementation of Quantum Computation, Sydney, Australia (IQC 01)*, page 257, 2001.

[50] David Deutsch and Richard Jozsa. Rapid solutions of problems by quantum computation. In *Proc. of the Royal Society of London*, volume 439, page 553, 1992.

[51] Gregory Breyta Costantino S. Yannoni Mark H. Sherwood Lieven M. K. Vandersypen, Matthias Steffen and Isaac L. Chuang. Experimental realization of shor's quantum factoring algorithm using nuclear magnetic resonance. volume 414.

[52] Gilles Brassard and Peter Høyer. An exact quantum polynomial-time algorithm for simon's problem. In *Proceedings of Fifth Israeli Symposium on Theory of Computing and Systems (IEEE Computer Society Press), 1997*, pages 12–23.

[53] Michele Mosca Gilles Brassard, Peter Høyer and Alain Tapp. Quantum amplitude amplification and estimation. In *arXiv:quant-ph/0005055*.

[54] L. K. Grover. Quantum computers can search rapidly by using almost any transformation. volume 80.

[55] Phil Gossett. Quantum carry-save arithmetic, 1998.

[56] G. Papakonstantinou M. Sampson, D. Voudouris. A quantum algorithm for finding minimal exclusive-or expressions for incompletely specified boolean functions. volume 10, pages 6–12, 2008.

[57] G. Papakonstantinou M. Sampson, D. Voudouris. A quantum algorithm for finding minimum exclusive-or expressions for multi-output incompletely specified boolean functions. In *in International Conference on Computer Design, CDES08, Las Vegas, 2008*, pages 105–111.

[58] G. Papakonstantinou M. Sampson, D. Voudouris. Utilization of variable reordering in quantum esct minimization. In *HERCMA 2009, Athens, Hellas (accepted, to be presented)*.

[59] D. Ventura and T. Martinez. Initializing the amplitude distribution of a quantum state. volume 12.

[60] G. Papakonstantinou D. Voudouris, M. Sampson. Variable reordering for reversible wave cascades. In *HERCMA 2007, Athens, Hellas*.

[61] J. Kilian U. Feige and M. Naor. A minimal model for secure computation. In *Proc. of the 26th ACM Symposium on Theory of Computing (STOC '94)*, pages 554 – 563, 1994.

[62] T. Otagiri T. Mizuki and H. Sone. Secure computations in a minimal model using multiple-valued esop expressions. In *Theory and Applications of Models of Computation, Third International Conference, TAMC 2006, Beijing, China, May 15-20, SpringerLink*, 2006.

[63] T. Otagiri T. Mizuki and H. Sone. An application of esop expressions to secure computations. volume 16, pages 191–198, 2007.

[64] R. L. Ashenhurst. The decomposition of switching functions. In *Proc. Int. Symp. Theory of Switching, Part I, Ann. Comput. Lab. Harvard Univ.*, pages 74–116, 1959.

[65] S. Hassoun and T. Sasao. *Logic Synthesis and Verification*. Kluwer Academic Publishers, 2002.

[66] R. H. Mohring and E. J. Radermacher. Substitution decomposition of discrete structures and connections to combinatorial optimization. volume 19, pages 251–264, 1984.

[67] W. Bimbdum and J. D. Esary. Modules of coherent binary systems. volume 13, pages 444–451, 1965.

[68] L. S. Shapley. Solutions of compound simple games. volume 52, pages 267–280, 1964.

[69] D. Voudouris and G. Papakonstantinou. Maitra cascade minimization. In *6th IWSBP, 2005, Freiberg (Sachsen), Germany*, pages 209–220.

[70] M. Sampson D. Voudouris and G. Papakonstantinou. Exact esct minimization for functions of up to six input variables. volume 41, 1 (Jan. 2008), pages 87–105, 2008.

[71] D. Voudouris S. Stergiou and G. Papakonstantinou. Multiple-valued exclusive-or sum-of-products minimization algorithms. volume E87-A, 2004.

[72] M. Kalathas D. Voudouris and G. Papakonstantinou. Decomposition of multi-output boolean functions. In *HERCMA 2005, Athens, Hellas*.

[73] G. Papakonstantinou M. Sampson, D. Voudouris. A quantum algorithm for finding minimum exclusive-or expressions. In *IEEE Computer Society Annual Symposium on VLSI, ISVLSI '07, 2007*, pages 416–421.

[74] Y. Saeyang. Logic synthesis and optimization benchmarks user guide, 1991.