Μ.Π.Λ.Α
ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗ ΛΟΓΙΚΗ ΚΑΙ
ΘΕΩΡΙΑ ΑΛΓΟΡΙΘΜΩΝ ΚΑΙ ΥΠΟΛΟΓΙΣΜΟΥ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κβαντική Φυσική και Υπολογιστές: Αλγόριθμοι, Πολυπλοκότητα & Θεωρία Παιγνίων

Ξενοφώντας Ι. Ραφιός

Επιβλέπων: Παγουρτζής Άρης

Αθήνα, 2006

Η παρούσα Διπλωματική Εργασία
εκπονήθηκε στα πλαίσια των σπουδών
για την απόκτηση του
Μεταπτυχιακού Διπλώματος ειδίκευσης
στη
Λογική και Θεωρία Αλγορίθμων και Υπολογισμού
που απονέμει το
Τμήμα Μαθηματικών
Του
Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών

Εγκρίθηκε την 14/04/2006 από Εξεταστική Επιτροπή
αποτελούμενη από τους:

Ονοματεπώνυμο	Βαθμίδα	Υπογραφή
1. Α. Παγουρτζής	Λέκτορας Σχολής Η.Μ.Μ.Υ, Ε.Μ.Π	.....
2. Ε.Ζάχος	Καθηγητής Σχολής Η.Μ.Μ.Υ, Ε.Μ.Π	.....
3. Φ.Αφράτη	Καθηγήτρια Σχολής Η.Μ.Μ.Υ, Ε.Μ.Π	.....
4. Η.Κουτσουπιάς	Καθηγητής Τμήματος Πληρ. & Τηλεπ., Ε.Κ.Π.Α	.....

Αφιερώνεται στην οικογένειά μου και σε όλους όσους με στήριξαν.

Πρόλογος

Η εργασία αυτή πραγματοποιήθηκε στα πλαίσια της διπλωματικής εργασίας του Μεταπτυχιακού προγράμματος « Μαθηματική Λογική, Θεωρία Υπολογισμού & Αλγορίθμων» κατά το ακαδημαϊκό έτος 2005-2006 και εκπονήθηκε με τη συνεργασία και την επίβλεψη του κ. Άρη Παγουρτζή. Το θέμα της είναι «Κβαντική φυσική & Υπολογιστές: Αλγόριθμοι, Πολυπλοκότητα & Θεωρία παιγνίων». Θα ήθελα να ευχαριστήσω τον κ. Παγουρτζή για τη συνεχή και πολύτιμη βοήθειά του καθώς και για την αμέριστη συμπαράστασή του καθ' όλη τη διάρκεια της συνεργασίας μας.

Θα ήθελα, ακόμη, να εκφράσω τις ευχαριστίες μου στον επιβλέποντα της διπλωματικής μου εργασίας, Καθηγητή του Ε.Μ.Π κ. Ευστάθιο Ζάχο γιατί ήταν ένας από τους κύριους λόγους που διάλεξα το μεταπτυχιακό αυτό.
Ευχαριστώ επίσης τους καθηγητές του Τμήματος Μαθηματικών κ. Δημητρακόπουλο & κ. Μοσχοβάκη που μου έδωσαν την ευκαιρία να παρακολουθήσω το μεταπτυχιακό αυτό, αλλά και για τις γνώσεις που αποκόμισα μέσα από τις διδασκαλίες τους.

Ευχαριστώ, ακόμη, την οικογένειά μου και κυρίως όλους όσους με στήριξαν για την πραγματοποίηση και την ολοκλήρωση αυτής της εργασίας.

Ραφιός Ξενοφώντας

Αθήνα , Απρίλιος 2006

Περιεχόμενα

Κεφάλαιο 1

Εισαγωγή

Οι σημερινοί υπολογιστές λειτουργούν με βάση την ίδια θεμελιώδη αρχή, με τις μηχανικές διατάξεις που οραματίστηκε ο Charles Babage το 19ο αιώνα και τυποποίησε αργότερα ο Alan Turing: Μια ευσταθής κατάσταση της μηχανής αναπαριστά έναν αριθμό. Όμως ο φυσικός κόσμος περιγράφεται από τους νόμους της κβαντικής φυσικής, οι οποίοι μας καλούν να αντιμετωπίσουμε τους υπολογιστές διαφορετικά. Η κβαντική φυσική προσφέρει πανίσχυρες μεθόδους για το χειρισμό της πληροφορίας τις οποίες μόλις αρχίσαμε να κατανοούμε. Οι κβαντικοί υπολογιστές ενώνουν δύο από τις σημαντικότερες εννοιολογικές επαναστάσεις του 20ου αιώνα: την επιστήμη της πληροφορίας και την κβαντική φυσική.

Ο πρώτος που πρόβλεψε την ασυνήθιστη δύναμη των κβαντικών υπολογιστών το 1982 [16] ήταν ο Richard Feynman, ένας εξαίρετος φυσικός (ο οποίος τιμήθηκε με το βραβείο Νόμπελ για την συμβολή του στην κατανόηση του φωτός). Ο Feynman είχε παρατηρήσει πως πολύ συχνά, περίπλοκοι υπολογισμοί που απαιτούν υπερβολικό χρόνο για να ολοκληρωθούν, καταλήγουν σε εξισώσεις που περιγράφουν συγκεκριμένα φυσικά φαινόμενα. Αντί, λοιπόν, να προσπαθήσει κάποιος να λύσει την εξίσωση, θα μπορούσε απλώς να εκτελέσει ένα πείραμα, να δημιουργήσει δηλαδή το αντίστοιχο κβαντικό φαινόμενο και να καταγράψει το αποτέλεσμα. Το εν λόγω αποτέλεσμα θα ήταν και η λύση της εξίσωσής του!
Αρκεί, λοιπόν να εντοπίσει κανείς φυσικές διεργασίες οι οποίες περιγράφονται από μαθηματικά, αντίστοιχα με τα μαθηματικά που προσπαθεί να λύσει. Η ίδια η φύση θα του δώσει την απάντηση!

Η ιδέα του Feynman είχε μεγάλη απήχηση στην επιστημονική κοινότητα και μάλιστα στα τέλη της δεκαετίας του 80, ο David Deutsch από το πανεπιστήμιο της Οξφόρδης δημοσίευσε μια θεωρητική εργασία στην οποία έδειχνε ότι θα μπορούσε ένας υπολογισμός να κωδικοποιηθεί σε ένα κβαντικό σύστημα. Το 1994 ο Peter Shor, εργαζόμενος στα εργαστήρια Bell, δημοσίευσε έναν κβαντικό αλγόριθμο ο οποίος εκτελεί παραγοντοποίηση πολύ μεγάλων αριθμών με εξαιρετικά μεγάλη ταχύτητα. Μετά από αυτήν την ανακάλυψη, η επιστημονική κοινότητα άρχισε να εργάζεται πιο εντατικά πάνω στην ανάπτυξη ενός κβαντικού υπολογιστή, δοκιμάζοντας ποικίλα κβαντικά συστήματα, χωρίς όμως ιδιαίτερα θετικά αποτελέσματα. Ο λόγος είναι πως τα περισσότερα κβαντικά συστήματα είναι ιδιαίτερα ευαίσθητα στην αλληλεπίδραση με το περιβάλλον τους, και υπόκεινται σε μια διαδικασία που ονομάζεται «αποσυνοχή-αποσυμφωνία» (decoherence), εξαιτίας της οποίας

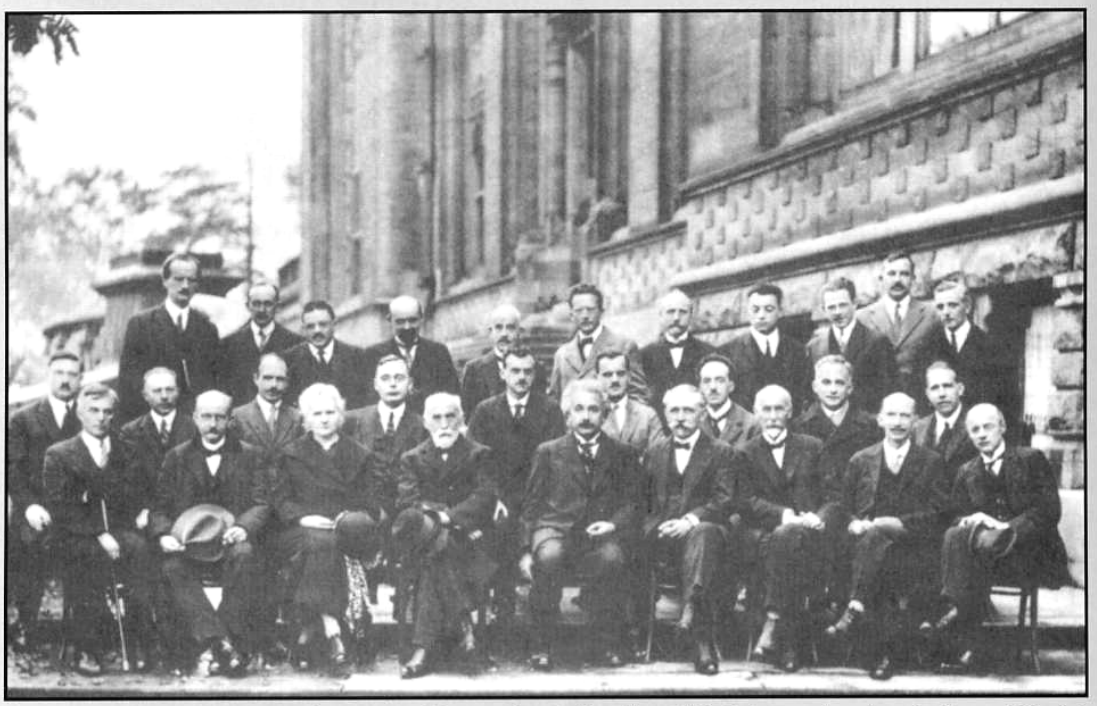
καταστρέφονται οι κβαντικές ιδιότητες του συστήματος. Και αλληλεπίδραση με το περιβάλλον είναι ακόμα και η ίδια η παρατήρηση του συστήματος!

Η εργασία αυτή συνδυάζει τρία διαφορετικά επιστημονικά πεδία, την κβαντική φυσική, τη θεωρία αλγορίθμων και τη θεωρία παιγνίων.
Θα συνδέσουμε πρώτα τα δύο πρώτα πεδία μιλώντας για κβαντικούς αλγορίθμους και στη συνέχεια θα εφαρμόσουμε τις ιδέες αυτές στη θεωρία παιγνίων όπου θα μελετήσουμε 5 κβαντικά παιχνίδια.

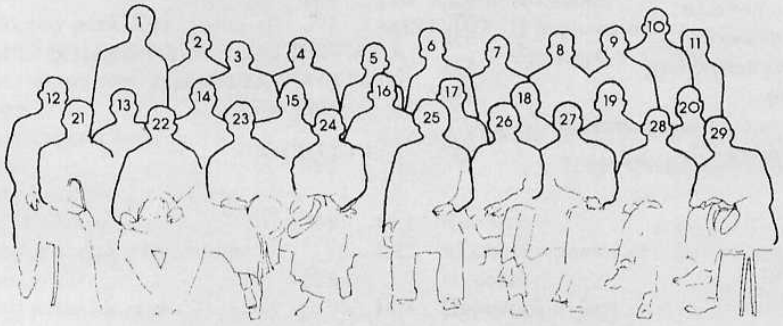
Ο στόχος της εργασίας αυτής είναι καταρχήν να εξηγήσει πως μπορούν να εφαρμοστούν οι νόμοι της κβαντικής φυσικής στη θεωρία αλγορίθμων μελετώντας 3 κβαντικούς αλγόριθμους. Ο πρώτος, ο αλγόριθμος του Deutsch, είναι εισαγωγικός. Οι αλγόριθμος αναζήτησης του Grover είναι σημαντικός γιατί μπορεί να λύσει μια σειρά NP-complete προβλημάτων $\sqrt{N}$ φορές πιο γρήγορα απ' ότι οι κλασικοί αλγόριθμοι. Η μελέτη του αλγορίθμου του Shor είναι πολύ σημαντική γιατί ο αριθμός των βημάτων που χρειάζεται για να παραγοντοποιήσει έναν αριθμό είναι πολύ μικρότερος σε σχέση με τον κλασικό (πολυωνυμικός χρόνος σε αντίθεση με εκθετικό χρόνο που χρειάζεται ο καλύτερος κλασικός αλγόριθμος) και ήταν αυτός που έδωσε ώθηση στο πεδίο των κβαντικών υπολογισμών.

Μελετώντας, λοιπόν, τους προηγούμενους αλγορίθμους έχουμε ως στόχο να κατανοήσουμε πως λειτουργούν οι κβαντικοί υπολογισμοί, τι διαφορές έχουν από τους κλασικούς, ποιος είναι ο μηχανισμός που τους κάνει να είναι πιο γρήγοροι ή πολύ πιο γρήγοροι (Shor), τι διαφορά έχουν από τους πιθανοτικούς αλγόριθμους (pbit).

Τέλος θα προσπαθήσουμε να συνδέσουμε αυτές τις ιδέες με τη θεωρία παιγνίων για να κάνουμε μια εισαγωγή στη κβαντική θεωρία παιγνίων. Θα παρουσιάσουμε πέντε κβαντικά παιχνίδια όπου θα μας βοηθήσουν να κατανοήσουμε τις διαφορές μεταξύ κλασικής και κβαντικής θεωρίας παιγνίων αλλά και να καταλάβουμε καλύτερα πως λειτουργούν οι κβαντικοί αλγόριθμοι.



(Η φωτογραφία παραχωρήθηκε από τη Βιβλιοθήκη Niels Bohr του American Institute of Physics)



1. A. Piccard
2. E. Henriot
3. P. Ehrenfest
4. E. Herzen
5. Th. de Donder
6. E. Schrödinger
7. E. Verschaffelt
8. W. Pauli
9. W. Heisenberg
10. R.H. Fowler
11. L. Brillouin
12. P. Debye
13. M. Knudsen
14. W.L. Bragg
15. H.A. Kramers
16. P.A.M. Dirac
17. A.H. Compton
18. L.V. de Broglie
19. M. Born
20. N. Bohr
21. I. Langmuir
22. M. Planck
23. M. Curie
24. H.A. Lorentz
25. A. Einstein
26. P. Langevin
27. C.E. Guye
28. C.T.R. Wilson
29. O.W. Richardson

Στη μοναδική αυτή φωτογραφία διακρίνονται πολλοί διακεκριμένοι επιστήμονες οι οποίοι έλαβαν μέρος στο Πέμπτο Διεθνές Συνέδριο Φυσικής, που διοργανώθηκε το 1927 από το Ινστιτούτο Solvay στις Βρυξέλλες. Σε τέτοιου είδους συνέδρια, που από το 1911 πραγματοποιούνταν σε τακτική βάση, οι επιστήμονες είχαν την ευκαιρία να ανταλλάσσουν απόψεις και να ενημερώνονται για τις πολλές και συνταρακτικές εξελίξεις στους τομείς της ατομικής και της πυρηνικής φυσικής. Από τους κορυφαίους επιστήμονες που απαθανατίζονται εδώ, οι δεκαπέντε έχουν τιμηθεί με το βραβείο Νόμπελ της Φυσικής και οι τρεις με το βραβείο Νόμπελ της Χημείας.

Κεφάλαιο 2

Κβαντική Φυσική

2.1 Παλαιά Κβαντική Θεωρία

Το 1900 ο Max Planck για να ερμηνεύσει την ακτινοβολία που παράγει ένα θερμαινόμενο σώμα, εισήγαγε τη θεωρία των κβάντα φωτός, την οποία εφάρμοσε αργότερα ο Einstein, για να ερμηνεύσει το φωτοηλεκτρικό φαινόμενο.
Σύμφωνα με τη θεωρία αυτή το φώς εκπέμπεται και απορροφάται από τα άτομα της ύλης όχι κατά συνεχή τρόπο αλλά ασυνεχώς.
Ο Planck τιμήθηκε με βραβείο Νόμπελ φυσικής το 1918 «πρός αναγνώριση των υπηρεσιών του στην πρόοδο της φυσικής, με την ανακάλυψη των κβάντων ενέργειας».[1]
Αν δεν είχε ανακαλύψει τη θεωρία της σχετικότητας ο Einstein θα ήταν διάσημος για το ρόλο του στην ανάπτυξη της κβαντικής θεωρίας.
Το 1905 σε ηλικία 26 ετών δημοσιεύει πέντε θεωρητικές εργασίες σε περιοδικά φυσικής. Η μία από αυτές ήταν η εξήγηση του φωτοηλεκτρικού φαινομένου και αφορά τα ηλεκτρόνια που εκπέμπονται όταν φωτίσουμε μια μεταλλική επιφάνεια. Σύμφωνα με την πρόταση του Einstein κάθε είδους φως αποτελείται από κβάντα ενέργειας, σήμερα γνωστά ως φωτόνια.
Το επόμενο βήμα στην κβαντική επανάσταση έγινε από έναν νεαρό δανό φυσικό ονόματι Niels Bohr, ο οποίος έφτασε στην Αγγλία το 1911 εφοδιασμένος με ένα διδακτορικό δίπλωμα από την Κοπεγχάγη. Ο Bohr άρχισε την κβαντική του αναζήτηση όταν πήγε να εργαστεί με έναν από τους πιο επιφανείς επιστήμονες εκείνης της εποχής το φυσικό Ernest Rutherford. Ο Bohr έφτασε την περίοδο που ο Rutherford διατύπωνε το μοντέλο του για το άτομο. Είχε μόλις ανακαλύψει ότι τα άτομα αποτελούνται από έναν μικροσκοπικό πυρήνα στο κέντρο τους περιβαλλόμενο από τα ακόμη πιο μικρά ηλεκτρόνια.
Ο Bohr άρχισε προσπαθώντας να κατανοήσει τη δομή του ατομικού μοντέλου του Rutherford και τελικά ανέπτυξε ένα μοντέλο του ατόμου του Υδρογόνου (το πρότυπο του Bohr) το οποίο κατάφερε να ερμηνεύσει τα γραμμικά φάσματα του υδρογόνου στηριζόμενος στην παραδοχή ότι η στροφορμή του ηλεκτρονίου είναι κβαντωμένη και ίση με το ακέραιο πολλαπλάσιο της ποσότητας $h/(2\pi)$.
Το επόμενο βήμα έγινε το 1924 όταν ο νεαρός γάλλος Louis de Broglie υπέβαλλε τη διδακτορική του διατριβή κάνοντας μια τολμηρή πρόταση: αν το φως, που μας διευκολύνει να το θεωρούμε κύμα μπορεί να συμπεριφέρεται ως ρεύμα σωματιδίων τότε θα μπορούσε και κάθε υλικό

αντικείμενο να συσχετισθεί με ένα «υλικό κύμα», με μήκος κύματος που εξαρτάται από τη μάζα του αντικειμένου. Μάλιστα βρήκε έναν τύπο που συνδέει την ορμή ενός σωματιδίου με το μήκος κύματος του συσχετιζόμενου κύματος: όσο πιο μεγάλη ορμή έχει το σωματίδιο, τόσο πιο μικρό το μήκος κύματος. Αυτός είναι ο λόγος που δεν μπορούμε να ανιχνεύσουμε κυματική συμπεριφορά αντικειμένων της καθημερινής ζωής όπως άνθρωποι, μπάλες ή ακόμη και κόκκοι άμμου. Η σταθερά που συνδέει τα δύο μεγέθη (ορμή και μήκος κύματος) είναι η σταθερά του Planck.

Εκείνη την εποχή, η επαναστατική πρόταση του de Broglie ήταν πολύ ριζοσπαστική για να έχει την αποδοχή των άλλων επιστημόνων. Μάλιστα ήταν αβέβαιο αν θα αποκτούσε το διδακτορικό του δίπλωμα και την τελευταία στιγμή χρειάστηκε η παρέμβαση του Einstein για να μεταπειστούν οι εξεταστές.

Αυτή ήταν η παλιά κβαντική θεωρία.

2.2 Θεμελίωση της Κβαντομηχανικής

Η καινούργια κβαντική θεωρία ξεκίνησε το 1926 όταν σχεδόν ταυτόχρονα ο Schroedinger και ο Heisenberg εισήγαγαν ένα νέο μαθηματικό φορμαλισμό των νόμων της μηχανικής, γνωστό ως Κβαντομηχανική ή Κβαντική θεωρία.
Οι θεωρίες των δύο επιστημόνων είναι ισοδύναμες και διαφέρουν μόνο ως πρός το μαθηματικό τρόπο αντιμετώπισης των προβλημάτων. Ο Schroedinger χρησιμοποιεί διαφορικές εξισώσεις με μερικές παραγώγους ενώ ο Heisenberg άλγεβρα μητρών.
Πιο συγκεκριμένα εάν δηλώσουμε με ψ την κατάσταση του συστήματος που μας ενδιαφέρει να μελετήσουμε τη χρονική στιγμή t τότε η εξίσωση του Schroedinger δίνεται από τη σχέση:

$$-\frac{\hbar^2}{2m}\left(\frac{\partial^2}{\partial x^2}+\frac{\partial^2}{\partial y^2}+\frac{\partial^2}{\partial z^2}\right)\psi + V\psi = i\hbar\frac{\partial\psi}{\partial t}$$

όπου $\hbar$ η σταθερά του Planck, m η μάζα του σωματιδίου που περιγράφουμε, V είναι το δυναμικό όπου περιγράφει τις δυνάμεις που δρούν στο σωματίδιο, $\frac{\partial\psi}{\partial t}$ περιγράφει πως αλλάζει η ψ με την πάροδο του χρόνου και ψ η λύση της εξίσωσης του Schroedinger όπου ονομάζεται «κυματοσυνάρτηση» και περιγράφει την κατάσταση ενός σωματιδίου.
Η «κυματοσυνάρτηση» ψ δεν είναι μια μετρήσιμη ποσότητα. Εν τούτοις το τετράγωνο της απόλυτης τιμής της

$$|\psi(x,t)|^2$$

μας δείχνει την πιθανότητα ανά μονάδα μήκους ή την πυκνότητα πιθανότητας να βρεθεί το σωματίδιο σε κάποια θέση x τη χρονική στιγμή t. Δηλαδή η πιθανότητα να βρεθεί το σωματίδιο στο απειροστό διάστημα dx γύρω από το σημείο x , εκφρασμένη ως P(x)dx είναι:

$$P(x)dx = |\psi(x,t)|^2\,dx$$

Στην Νευτώνεια μηχανική – π.χ: σε μια διάσταση – η αντίστοιχη εξίσωση της εξίσωσης του Schroedinger είναι ο γνωστός δεύτερος νόμος του Νεύτωνα

$$m\ddot{x} = F(x)$$

όπου για τον προσδιορισμό της λύσης x(t) απαιτείται η γνώση όχι μόνο της αρχικής τιμής x(0) αλλά και της αρχικής τιμής της παραγώγου της v(0).
Στην περίπτωσή μας για τη λύση της εξίσωσης του Schroedinger η αναγκαία αρχική συνθήκη για να μπορέσουμε να βρούμε τι «πρόκειται να γίνει στο μέλλον» δηλαδή τη ψ(x,y,z,t) είναι η

$$\psi(x,y,z,0) = \psi(x,y,z)$$

δηλαδή η γνώση της κυματοσυνάρτησης σε μια δεδομένη χρονική στιγμή t=0.

2.3 Εξίσωση Schroedinger και κβαντικοί υπολογισμοί

Η εξέλιξη ενός απομονωμένου κβαντικού συστήματος δίνεται από την εξίσωση Schroedinger.

$$-i\frac{\partial}{\partial t}\psi(x,t) = \mathrm{H}\,\psi(x,t)$$

Μια λύση της προηγούμενης εξίσωσης είναι:

$$\psi(x,t) = e^{-i\int dtH}\psi(x,0)$$

Εάν ο Η είναι ερμιτιανός τότε ο $e^{-i\int dtH}$ είναι ορθομοναδιαίος τελεστής τον οποίο τον ονομάζουμε U και στους κβαντικούς υπολογισμούς είναι η αναπαράσταση του αλγορίθμου. [6]

Από τη λύση αυτή παρατηρούμε ότι ο τελεστής U= $e^{-i\int dtH}$ έχει την

ιδιότητα να διατηρεί την κατανομή πιθανότητας του σωματιδίου στο χώρο γιατί:

$$|\psi(x,t)|^2 = |\psi(x,0)|^2 \left|e^{-i\int dtH}\right|^2 = |\psi(x,0)|^2 .1 = |\psi(x,0)|^2$$

Πριν συνεχίσουμε θεωρούμε αναγκαίο να αναφερθούμε στην έννοια του τελεστή όπως και να ορίσουμε τον ερμιτιανό και τον ορθομοναδιαίο τελεστή αλλά και τους αντίστοιχους πίνακες.

Κεφάλαιο 3

Γραμμική Άλγεβρα

3.1 Τελεστές

Στην Κβαντική μηχανική χρησιμοποιούνται γραμμικοί διανυσματικοί χώροι με στοιχεία μιγαδικές γενικά συναρτήσεις. Οι χώροι αυτοί λέγονται χώροι Hilbert[3]. Μια από τις σπουδαιότερες έννοιες των χώρων αυτών είναι η έννοια της απεικονίσεως ενός χώρου S πάνω στον εαυτό του. Μια τέτοια απεικόνιση πραγματοποιείται με ένα τελεστή Α, που όταν δρά πάνω σε ένα στοιχείο του χώρου S, δηλαδή πάνω σε μια συνάρτηση ψ, δίνει ένα άλλο στοιχείο του χώρου S, δηλαδή μια άλλη συνάρτηση Φ,

$$\psi \in S : A\psi = \Phi \quad \in S$$

Μια χρήσιμη κατηγορία τελεστών είναι οι γραμμικοί τελεστές. Ορίζουμε δε ως γραμμικό τελεστή αυτόν, για τον οποίο ισχύει

$$A(C_1\psi_1 + C_2\psi_2) = C_1A\psi_1 + C_2A\psi_2$$

Όπου C_1,C_2σταθερές (και γενικά μιγαδικοί αριθμοί).
Αν εξετάσουμε τη σχέση

$$A\psi=\alpha\psi \quad (1)$$

τότε παρατηρούμε ότι αν επιδράσουμε τον τελεστή Α πάνω στη συνάρτηση ψ, τότε έχουμε πάλι τη συνάρτηση ψ επί κάποια σταθερά ποσότητα α. Είναι φανερό ότι για δοθέντα τελεστή Α η σχέση (1) δεν ικανοποιείται για κάθε συνάρτηση ψ. Δηλαδή η σχέση (1) είναι μιά εξίσωση. Οι συναρτήσεις που επαληθεύουν την παραπάνω εξίσωση λέγονται «ιδιοσυναρτήσεις» του τελεστή Α και οι τιμές της σταθεράς α για τις οποίες ισχύει η σχέση (1) λέγονται «ιδιοτιμές» του τελεστή Α. Ετσι η (1) προσδιορίζει τόσο τις ιδιοτιμές όσο και τις ιδιοσυναρτήσεις του τελεστή Α και είναι δυνατόν να έχουμε δύο ή και περισσότερες γραμμικά ανεξάρτητες ιδιοσυναρτήσεις που να αντιστοιχούν στην ίδια ιδιοτιμή του τελεστή Α [3].
Η μορφή ενός τελεστή εξαρτάται από τον εκάστοτε χρησιμοποιούμενο χώρο. Ετσι εάν έχουμε έναν χώρο όπου τα στοιχεία του είναι διανύσματα στήλης ο τελεστής μπορεί να έχει την μορφή πίνακα κάτι το οποίο συμβαίνει στην περίπτωσή μας.

3.2 Ερμιτιανοί τελεστές

Οι ιδιοτιμές ενός τελεστή είναι γενικά μιγαδικές. Υπάρχει μια κατηγορία τελεστών που έχουν μόνο πραγματικές ιδιοτιμές. Αυτή είναι η κατηγορία των ερμιτιανών τελεστών.
Ενας τελεστής Α είναι ερμιτιανός εάν ταυτίζεται με τον συζυγή του (adjoint operator).

$$A = A^{\dagger}$$

Ενας τελεστής είναι συζυγής όταν ισχύει:

$$\int \psi_1^{*} A \psi_2 = \int (A^{\dagger}\psi_1)^{*} \psi_2$$

Όπου ο «*» σημαίνει συζυγείς μιγαδικές ποσότητες.

3.3 Ερμιτιανοί πίνακες

Τους τελεστές μπορούμε να τους εκφράσουμε με την μορφή πινάκων. Ετσι στους ερμιτιανούς τελεστές αντιστοιχούν οι ερμιτιανοί πίνακες όπου έχουν την ιδιότητα να είναι ανάστροφοι και συζυγείς. Για παράδειγμα οι πίνακες Pauli είναι ερμιτιανοί.

$$X = \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Παρατηρήστε ότι ισχύει: $A = A^{\dagger}$

3.4 Ορθομοναδιαίοι Πίνακες (Unitary)

Ενας πίνακας U

$$U = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix}$$

είναι ορθομοναδιαίος αν και μόνον αν:

$$UU^{\dagger} = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \begin{bmatrix} u_{00}^{*} & u_{10}^{*} \\ u_{01}^{*} & u_{11}^{*} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Επίσης ένας πίνακας είναι ορθομοναδιαίος εαν $U^{-1} = U^{\dagger}$

Όπου $U^{\dagger} = (U^{*})^{\mathrm{T}}$

$U^{\dagger}$	conjugate transpose
U^{*}	ο συζυγής του U
U^{T}	ο ανάστροφος
U^{-1}	ο αντίστροφος πίνακας

3.5 Ενα παράδειγμα ορθομοναδιαίων τελεστών: Τελεστές περιστροφής

Τελεστές όπου

$$U = e^{-iH}$$

και Η ερμιτιανός είναι ορθομοναδιαίοι.

Παράδειγμα:

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos(\theta/2)\mathrm{I} - i\sin(\theta/2)\mathrm{X} = \begin{bmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ i\sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$$

$$\text{όπου} \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$R_Y(\theta) \equiv e^{-i\theta Y/2} = \cos(\theta/2)\mathrm{I} - i\sin(\theta/2)\mathrm{Y} = \begin{bmatrix} \cos(\theta/2) & \sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{bmatrix}$$

$$\text{όπου} \qquad \mathrm{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$R_Z(\theta) \equiv e^{-i\theta Z/2} = \cos(\theta/2)\mathrm{I} - i\sin(\theta/2)Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{bmatrix}$$

$$\text{όπου} \qquad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

αφού ισχύει:

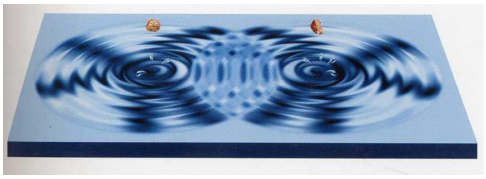
$$e^{-i\theta\vec{n}\vec{\sigma}} = e^{-i\theta(n_x X + n_Y Y + n_Z Z)} = \cos\theta * \mathrm{I} - i\sin(\theta)(\vec{n}\vec{\sigma})$$

Κεφάλαιο 4

Εισαγωγή στους κβαντικούς υπολογισμούς

4.1 Η έννοια υπέρθεση

Η ιδέα της υπέρθεσης δεν είναι μονοπώλιο της κβαντικής μηχανικής αλλά είναι μια γενική ιδιότητα όλων των κυμάτων.(Πιο συγκεκριμένα η υπέρθεση αποτελεί ιδιότητα όλων των κυμάτων που είναι λύσεις γραμμικών εξισώσεων.)



Όταν οι κυματισμοί συναντηθούν σχηματίζουν μια υπέρθεση που δίνουν μια εικόνα πολύ διαφορετική από τα δύο σύνολα ομόκεντρων κύκλων, λόγω της συμβολής.

4.2 Υπέρθεση-Το πείραμα των δύο σχισμών

Άτομα εκτοξεύονται ένα-ένα, κάποια απο αυτά περνάμε απο τις 2 σχισμές και φτάνουν στο πέτασμα.

Καθώς πληθαίνουν τα άτομα, στο πέτασμα εμφανίζονται ζώνες συμβολής όπως εάν στέλναμε φώς.

Εικόνα συμβολής έχουμε όμως μόνο όταν ένα κύμα διέλθει από τις 2 σχισμές.

Άρα το άτομο περνάει ταυτόχρονα και από τις 2 σχισμές;

Ξέρουμε ότι από τη λύση της εξίσωσης Schroedinger κάθε άτομο περιγράφεται από μια κυματοσυνάρτηση που εξελίσσεται χρονικά. Αυτή η κυματοσυνάρτηση έχει πιθανοκρατική φύση και μας δίνει μόνο την πιθανή θέση του ατόμου. Είναι σημαντικό να τονίσουμε ότι ενώ δεν μπορούμε να θεωρήσουμε τα μικροσκοπικά άτομα σα να έχουν μετατραπεί ξαφνικά σε μια

εξαπλωμένη κυματοσυνάρτηση, η τελευταία παρέχει το μοναδικό τρόπο για να παρακολουθήσουμε την πορεία του ατόμου από τη στιγμή που εκτοξεύεται μέχρι τη στιγμή που θα χτυπήσει σε συγκεκριμένο σημείο του πετάσματος.

Τη στιγμή που συναντά τις δύο σχισμές, η κυματοσυνάρτηση χωρίζεται στα δύο και κάθε μία από τις δύο συνιστώσες περνάει από μια σχισμή. Καθώς περνάει και από τις δύο σχισμές η κυματοσυνάρτηση του ατόμου είναι μια υπέρθεση των δύο συνιστωσών της, όπου η κάθε μία έχει το μέγιστο δυνατό πλάτος στην αντίστοιχη σχισμή. Αν η κατάσταση του ατόμου περιγραφόταν μόνο από μία από αυτές τις δύο συνιστώσες τότε θα λέγαμε ότι περνάει οπωσδήποτε από εκείνη τη σχισμή. Όμως η υπέρθεση των δύο συνιστωσών σημαίνει ότι υπάρχει ίση πιθανότητα να περάσει είτε από τη μία είτε από την άλλη σχισμή. Απ' την πίσω πλευρά των σχισμών, κάθε συνιστώσα διαχέεται εκ νέου και τα δύο σύνολα κυματισμών επικαλύπτονται έτσι ώστε η συνδυασμένη επίδρασή τους τη στιγμή που φτάνουν στο πέτασμα δίνει την χαρακτηριστική ταινιωτή εικόνα (όταν συμβάλλουν δύο πραγματικά κύματα). Μόνο που τώρα, δεν έχουμε να κάνουμε με ένα πραγματικό κύμα που πέφτει πάνω στο πέτασμα αλλά με αριθμούς που παρέχουν μια πιθανότητα για την άφιξη ενός σωματιδίου σε μια δεδομένη θέση. [1]

4.3 Η έννοια του Qubit

Στους κβαντικούς υπολογιστές φορέας της πληροφορίας δεν είναι το bit αλλά το qubit ή κβαντικό bit το οποίο μπορεί να λάβει τις τιμές 0 ή 1 ή οποιαδήποτε υπέρθεση αυτών. Η κατάσταση «0» μπορεί να περιγραφεί με πολλούς τρόπους (θα χρησιμοποιήσουμε δύο). Ένας είναι με χρήση πίνακα (περιγραφή Heisenberg), ο άλλος είναι με την περιγραφή Dirac όπου η κβαντική κατάσταση «0» περιγράφεται ως $|0>$ και η κατάσταση «1» ως $|1>$. Μπορούμε να περιγράψουμε την κατάσταση ενός κβαντικού bit ως:

$$|\psi> = \alpha\ |0> + \beta\ |1> \qquad \textbf{(περιγραφή Dirac)}$$

Όπου α, β είναι μιγαδικοί αριθμοί για τους οποίους ισχύει:

$$|\alpha|^2 + |\beta|^2 = 1$$

Ενώ το bit είναι ένας συγκεκριμένος αριθμός $,b \in \{0,1\}$, το qubit είναι ένα διάνυσμα ενός δισδιάστατου χώρου Hilbert , $q \in \{au + bd\}$.

Όπου:

$$u \leftrightarrow |u\rangle \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \leftrightarrow |0\rangle \leftrightarrow bit \quad 0$$

$$d \leftrightarrow |d\rangle \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \leftrightarrow |1\rangle \leftrightarrow bit \quad 1$$

και a,b είναι μιγαδικοί αριθμοί.

Τι μας δείχνουν οι συντελεστές a,b;

Οτι εάν κάνουμε μια μέτρηση τότε:

θα μετρήσουμε την κατάσταση «0» ή $|0>$ή $\begin{pmatrix}1\\0\end{pmatrix}$ με πιθανότητα $|a|^2$

και την κατάσταση «1» ή $|1>$ή $\begin{pmatrix}0\\1\end{pmatrix}$με πιθανότητα $|b|^2$.

Παράδειγματα ενός qubit:

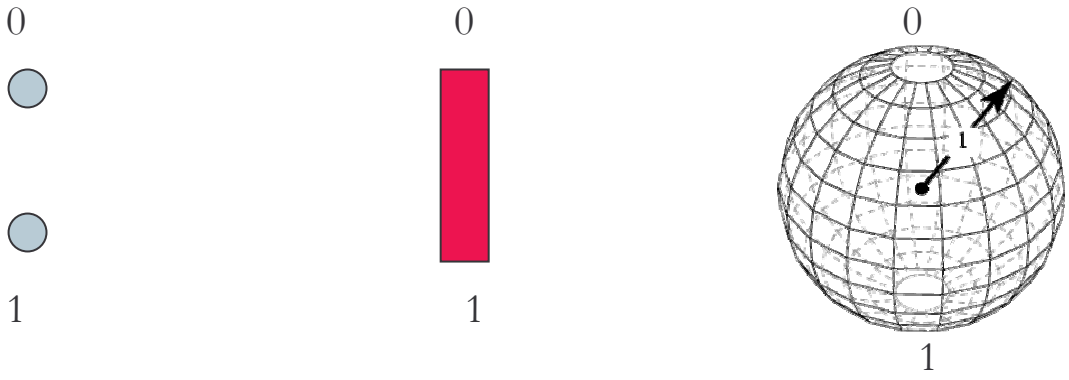
$$|\psi_1>=|1>\leftrightarrow\begin{pmatrix}0\\1\end{pmatrix} \qquad |\psi_2>=|0>\leftrightarrow\begin{pmatrix}1\\0\end{pmatrix}$$

$$|\psi_3>=\frac{1}{\sqrt{2}}(|0>+|1>)\leftrightarrow\begin{pmatrix}\frac{1}{\sqrt{2}}\\\frac{1}{\sqrt{2}}\end{pmatrix} \qquad |\psi_4>=\frac{3}{5}|0>-\frac{4}{5}|1>)\leftrightarrow\begin{pmatrix}\frac{3}{5}\\-\frac{4}{5}\end{pmatrix}$$

$$|\psi_5>=i\frac{3}{5}|0>-i\frac{4}{5}|1>)\leftrightarrow\begin{pmatrix}i\frac{3}{5}\\-i\frac{4}{5}\end{pmatrix}$$

4.4 Διαφορά μεταξύ bit, pbit και qubit

Bit Pbit Qubit



Όπως φαίνεται και από το σχήμα το bit μπορεί να βρίσκεται μόνο σε δύο καταστάσεις, το πιθανοτικό bit μπορεί να βρίσκεται στην κατάσταση «1» με πιθανότητα p και στην κατάσταση «0» με πιθανότητα 1-p (άρα αντιστοιχεί σε ευθύγραμμο τμήμα μήκους 1) ενώ το κβαντικό bit αν/χει σε σφαίρα ακτίνας 1 (και αυτό γιατί θέλουμε να ισχύει $|\alpha|^2+|\beta|^2=1$, με α,β μιγαδικούς αριθμούς**.** Η σφαίρα αυτή ονομάζεται Bloch σφαίρα και κάθε σημείο της αν/χει σε μια κατάσταση $|\psi>$ ενός κβαντικού bit).

4.5 Bloch Sphere

Γιατι όμως ένα qubit αν/χει σε μια σφαίρα;

Η bloch σφαίρα είναι η γενίκευση της αναπαράστασης ενός μιγαδικού z με μέτρο 1

$$|z|^2=1$$

σαν ένα σημείο ενός κύκλου.
Εάν z=x+iy όπου x,y πραγματικοί τότε:

$$|z|^2=z^*z=(x-iy)(x+iy)=x^2+y^2$$

Και επειδή $|z|^2=1$, ο μιγαδικός z αν/χει σε σημείο κύκλου με ακτίνα 1 . Ενα qubit μπορεί να γραφτεί ως :

$$|\psi>=\alpha|0>+\beta|1>$$

με

$$|\alpha|^2+|\beta|^2=1$$

Μπορούμε να εκφράσουμε την κατάσταση σε σφαιρικές συντεταγμένες:

$$|\psi>=r_a e^{i\phi_\alpha}|0>+r_\beta e^{i\phi_\beta}|1>$$

Με 4 πραγματικές παραμέτρους: $r_a,\varphi_\alpha,r_\beta,\varphi_\beta$

Επειδή οι μόνες μετρήσιμες ποσότητες είναι οι πιθανότητες $|\alpha|^2,|\beta|^2$, μπορούμε να πολλαπλασιάσουμε με τον παράγοντα $e^{i\gamma}$ χωρίς παρατηρήσιμες αλλαγές αφού δεν αλλάζουν οι πιθανότητες $|\alpha|^2,|\beta|^2$. Δηλ.

$$|e^{i\gamma}\alpha|^2=(e^{i\gamma}\alpha)^*(e^{i\gamma}\alpha)=(e^{-i\gamma}\alpha^*)(e^{i\gamma}\alpha)=\alpha^*\alpha=|\alpha|^2$$

Αν/χα και για το $|\beta|^2$

Πολ/ζουμε με το $e^{-i\phi_\alpha}$ την αρχική μας κατάσταση

$$|\psi>=r_a e^{i\phi_\alpha}|0>+r_\beta e^{i\phi_\beta}|1>$$

...και έχουμε...

$$|\psi'>= e^{-i\phi_\alpha} r_a e^{i\phi_\alpha}|0> + e^{-i\phi_\alpha} r_\beta e^{i\phi_\beta}|1> = r_a|0> + r_\beta e^{i\phi}|1>$$

...όπου $\varphi = \varphi_\beta - \varphi_\alpha$

Έτσι περιγράψαμε την τελική μας κατάσταση με 3 πραγματικές παραμέτρους: r_a , r_β, φ

Ισχύει ότι:

$$x = r\sin\theta\cos\phi$$
$$y = r\sin\theta\sin\phi$$
$$z = r\cos\theta$$

Έτσι μετονομάζοντας το r_a σε z και και γνωρίζοντας ότι r=1 μπορούμε να γράψουμε:

$$|\psi'>= z|0> + (x+iy)|1>$$
$$= \cos\theta|0> + \sin\theta(\cos\phi + i\sin\phi)|1> =$$
$$= \cos\theta|0> + e^{i\phi}\sin\theta|1>$$

Τώρα έχουμε 2 παραμέτρους που καθορίζουν σημεία σε μια σφαίρα.

Επειδή θέλουμε η γωνία θ να παίρνει τιμές απο 0 μέχρι π θα έχουμε τελικά:

$$|\psi> = \cos(\theta/2)|0> + e^{i\phi}\sin(\theta/2)|1>$$
$$\text{με } 0 \le \theta \le \pi \qquad \text{και} 0 \le \phi \le 2\pi$$

Ετσι για θ=0 θα έχουμε |ψ>=|0>

για θ=π θα έχουμε |ψ>=|1> και

για θ=π/2 και φ=0 έχουμε $|\psi> = \frac{1}{\sqrt{2}}(|0> + |1>)$.

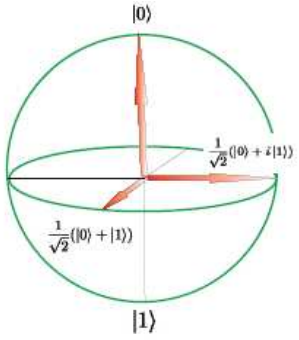
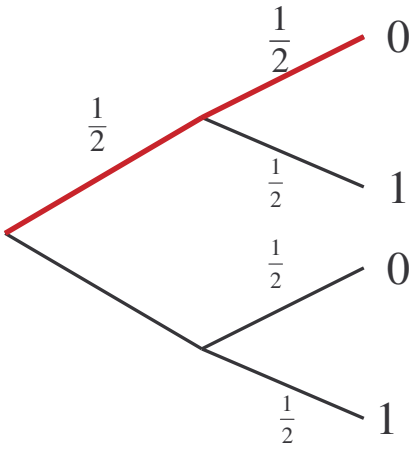


Figure 1: The Bloch Sphere

[15]

4.6 Κλασικές πιθανότητες

Ας θεωρήσουμε ένα υπολογιστικό δέντρο όπου κάθε φορά ενεργεί σαν ένα νόμισμα και μπορεί να βρεθεί με πιθανότητα 50% σε μία από τις 2 καταστάσεις («0» ή «1»)...



Η πιθανότητα να γίνει ο υπολογισμός που μας δείχνει το κόκκινο μονοπάτι είναι το γινόμενο των πιθανοτήτων ....

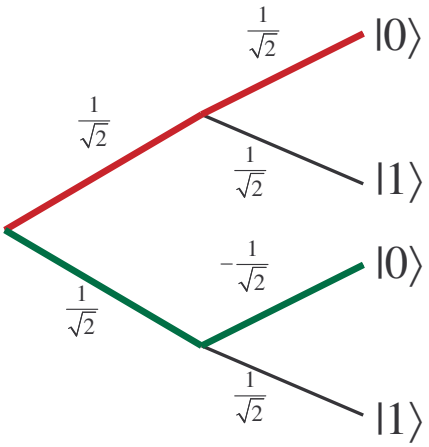
$$\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}$$

Η πιθανότητα ο υπολογισμός να μας δίνει απάντηση 0 είναι το άθροισμα των πιθανοτήτων των μονοπατιών που καταλήγουν σε κατάσταση 0.

$$\frac{1}{4}+\frac{1}{4}=\frac{1}{2}$$

4.7 Κβαντικές πιθανότητες

Τώρα τα πλάτη των ακμών μπορεί να είναι και μιγαδικοί αριθμοί....



Το πλάτος πιθανότητας του κόκκινου μονοπατιού είναι το γινόμενο των πλατών των κόκκινων ακμών...

$$\frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}}=\frac{1}{2}$$

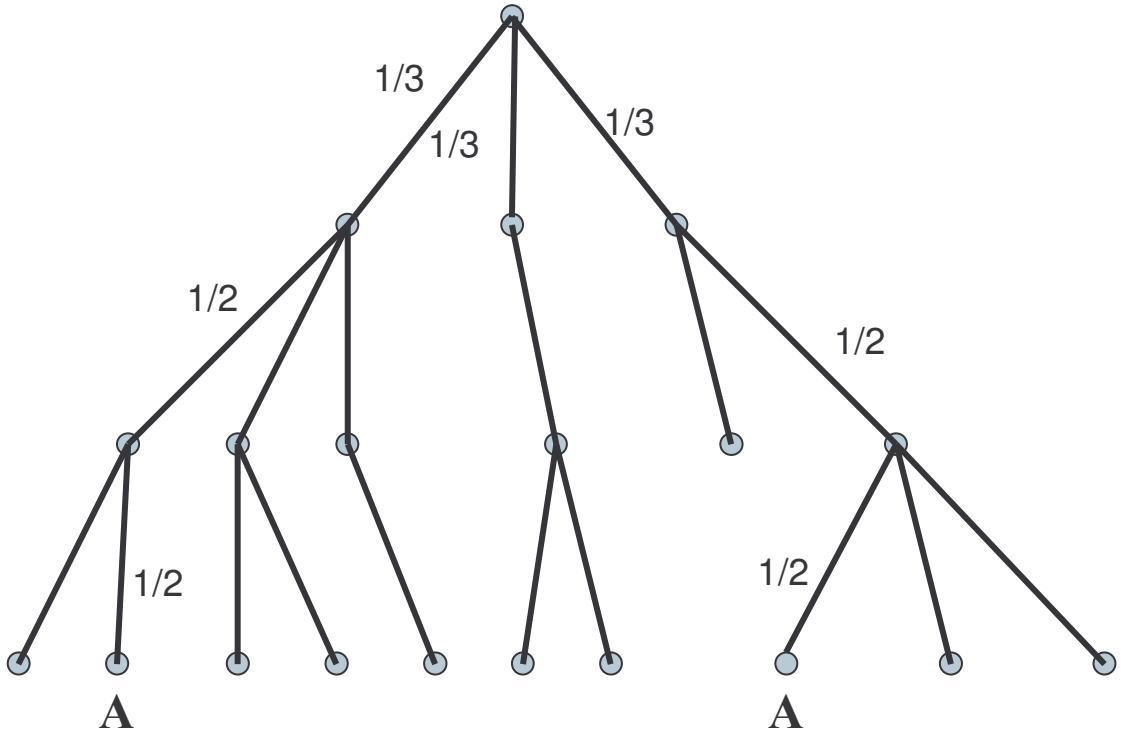
Το πλάτος πιθανότητας του πράσινου μονοπατιού είναι το γινόμενο των πλατών των πράσινων ακμών...

$$\frac{1}{\sqrt{2}}\cdot\left(-\frac{1}{\sqrt{2}}\right)=-\frac{1}{2}$$

Η πιθανότητα να εμφανισθεί η κατάσταση $|0>$ είναι ίση με το τετράγωνο του αθροίσματος των πλατών πιθανότητας των μονοπατιών που καταλήγουν σε κατάσταση $|0>$.

$$\left(\frac{1}{2}-\frac{1}{2}\right)^2=0!!!!$$

4.8 Παρουσίαση ενός κλασικού πιθανοτικού υπολογισμού σε μια μηχανή Turing ως ένα δέντρο



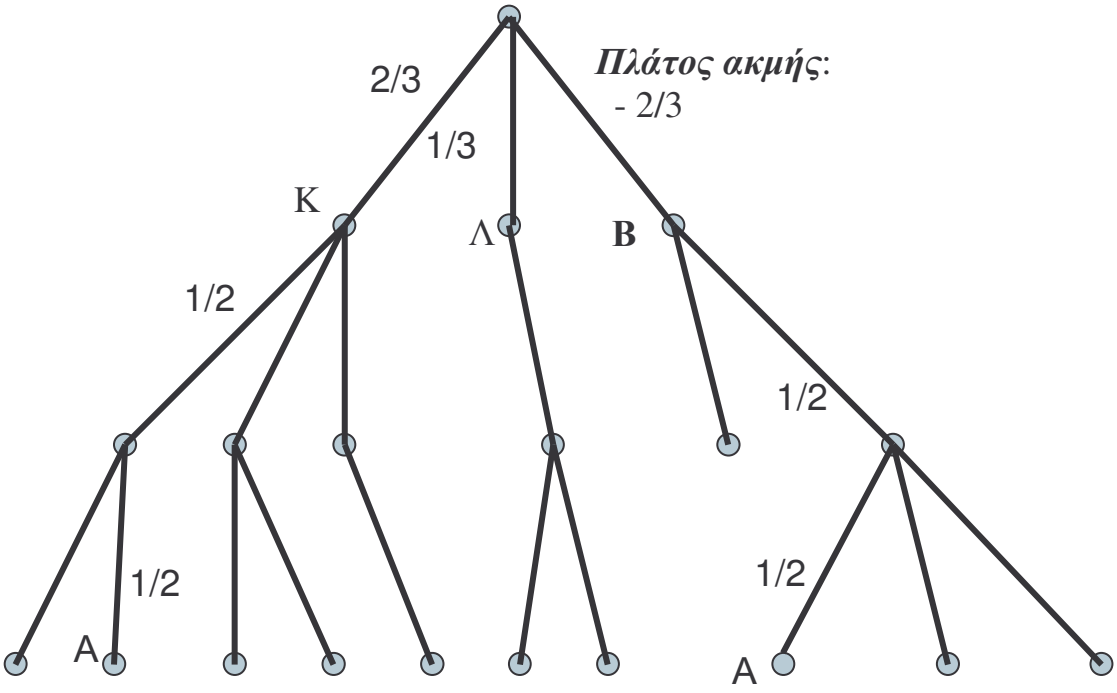
Η πιθανότητα να εμφανιστεί η κατάσταση Α είναι ίση με
(1/3)*(1/2)*(1/2)+ (1/3)*(1/2)*(1/2)=2/12

- Κάθε ***κόμβος*** αντιστοιχεί σε μια κατάσταση της μηχανής
- Κάθε ***επίπεδο του δέντρου*** αντιπροσωπεύει ένα βήμα υπολογισμού
- Η ***ρίζα*** αν/χεί στην αρχική κατάσταση της μηχανής
- Κάθε ***ακμή*** από ένα κόμβο-πατέρα σε ένα κόμβο παιδί είναι συσχετισμένη με την πιθανότητα ο υπολογισμός να οδηγηθεί από τον κόμβο πατέρα, στον κόμβο παιδί.
- Η πιθανότητα να επισκεφθούμε έναν κόμβο στη διάρκεια του υπολογισμού, η οποία λέγεται και ***πιθανότητα του κόμβου***, ισούται με το γινόμενο των πιθανοτήτων που σχετίζονται με τις πλευρές του μονοπατιού από τη ρίζα στον κόμβο αυτό.
- Η πιθανότητα να επισκεφθούμε μια συγκεκριμένη κατάσταση στο βήμα ι του υπολογισμού είναι απλά το άθροισμα των πιθανοτήτων όλων των κόμβων που αν/χουν στο επίπεδο ι.
- Το άθροισμα όλων των πιθανοτήτων των πλευρών που ξεκινούν από έναν κόμβο αλλά και το άθροισμα των πιθανοτήτων όλων των καταστάσεων ενός επιπέδου πρέπει να ισούται με 1. [4]

4.9 Κβαντικό Μοντέλο Υπολογισμού

Όπως μπορούμε να παρουσιάσουμε ένα κλασικό πιθανοτικό μοντέλο υπολογισμού σε μία μηχανή Turing ως δέντρο έτσι μπορούμε να κάνουμε και με ένα κβαντικό μοντέλο υπολογισμού.
Θα πρέπει όμως να ισχύει:

- Για κάθε κόμβο το άθροισμα των τετραγώνων των πλατών των πλευρών που οδηγούν στα παιδιά του πρέπει να είναι 1
- το άθροισμα των πιθανοτήτων κάθε κατάστασης σε κάθε επίπεδο πρέπει να είναι ίσος με 1.
  Δηλ.(πιθανότητα να έρθει η Α + πιθ Γ + .. =1)
- Η πιθανότητα να εμφανιστεί η κατάσταση Α είναι το τετράγωνο του αθροίσματος των πλατών όλων των κόμβων-φύλλων που αντιπροσωπεύουν αυτήν την κατάσταση.
- Μια κβαντική μηχανή πρέπει πάντα να εκτελεί ορθομοναδιαία βήματα.
- Τα ντετερμινιστικά και πιθανοτικά βήματα πρέπει να είναι αντιστρέψιμα. Τα υπολογιστικά βήματα που δεν παραβιάζουν τον παραπάνω περιορισμό λέγονται ορθομοναδιαία.
- Τα πιθανοτικά και ντετερμινιστικά μέρη ενός κβαντικού υπολογιστικού δέντρου δεν μπορούν να διαχωριστούν όπως στο κλασσικό μοντέλο και επομένως θα πρέπει πάντα να **διατηρούμε ολόκληρο το δέντρο στους κβαντικούς υπολογισμούς.**
  Δεν μπορούμε μετά από κάποιο σημείο του υπολογισμού να θεωρήσουμε ότι ακολουθούμε πλέον ένα συγκεκριμένο ντετερμινιστικό κλαδί αδιαφορώντας για το υπόλοιπο δέντρο.
  Αναφερόμαστε σ' ένα κβαντικό υπολογισμό σαν να βρίσκεται, σε κάθε βήμα, σε μια **υπέρθεση όλων των κλαδιών του δέντρου ταυτόχρονα** **[4]**



Η πιθανότητα να εμφανιστεί η κατάσταση Β ή το πλάτος της κατάστασης Β είναι:

$$(-2/3)^2 = 4/9$$

Η πιθανότητα να εμφανιστεί η κατάσταση Α είναι το τετράγωνο του αθροίσματος και όχι το άθροισμα των τετραγώνων :

$$[(2/3)*(1/2)*(1/2)-(-2/3)*(1/2)*(1/2)]^2$$

Δηλαδή

$$[(2/12)-(2/12)]^2$$

Αρα η πιθανότητα είναι

Ο !!!

4.10 Κβαντικοί καταχωρητές

Αν θέλουμε να αποθηκεύσουμε το νούμερο 4 το οποίο γράφεται σε δυαδική μορφή 100 παρατηρούμε ότι θα χρειαστούμε έναν 3-qubit καταχωρητή ο οποίος αναπαριστά τον αριθμό αυτόν σε πίνακα όπως παρακάτω:

$$|100\rangle = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\\0\\0\\0\\0\end{pmatrix}$$

Το $\otimes$ λέγεται γινόμενο Kronecker (tensor product) και ορίζεται ως εξής:

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}\otimes\begin{bmatrix}x & y\\ z & v\end{bmatrix} = \begin{bmatrix} a\begin{bmatrix}x & y\\ z & v\end{bmatrix} & b\begin{bmatrix}x & y\\ z & v\end{bmatrix}\\ c\begin{bmatrix}x & y\\ z & v\end{bmatrix} & d\begin{bmatrix}x & y\\ z & v\end{bmatrix}\end{bmatrix} = \begin{bmatrix}ax & ay & bx & by\\ az & av & bz & bv\\ cx & cy & dx & dy\\ cz & cv & dz & dv\end{bmatrix}$$

4.11 Διανύσματα / Περιγραφή Dirac/ Περιγραφή Heisenberg

Στη κβαντικομηχανική, ο χώρος των φυσικών καταστάσεων (ο χώρος των μιγαδικών διανυσμάτων με n διαστάσεις) δηλώνεται C^n (Hilbert space). Μπορούμε λοιπόν να θεωρήσουμε τις φυσικές καταστάσεις σαν διανύσματα ενός διανυσματικού χώρου.

Υπάρχουν δύο τρόποι για να περιγράψουμε μία κατάσταση.
Ο ένας είναι με χρήση πινάκων (περιγραφή Heisenberg) και ο άλλος είναι η περιγραφή Dirac.

Περιγραφή Dirac

Σύμφωνα με την περιγραφή αυτή μια κατάσταση ψ ή αλλιώς ένα διάνυσμα του χώρου Hilbert συμβολίζεται ως |ψ> και γράφεται ως γραμμικός συνδυασμός των διανυσμάτων βάσης του χώρου τα οποία συμβολίζονται με |0> ,|1> για n=2 (δισδιάστατος χώρος Hilbert) ή |00>,|01>,|10>,|11> όταν έχουμε χώρο 4 διαστάσεων, κ.λ.π.

Τα διανύσματα αυτά λέγονται διανύσματα καταστάσεως και συμβολίζονται με το συμβολισμό ket $|\ >$

Επειδή φυσική ερμηνεία έχει το γινόμενο

$$\psi^*(r,t)\psi(r,t)$$

(είναι η πιθανότητα να βρίσκεται το σωμάτιο στη θέση r τη χρονική στιγμή t)

θα πρέπει και στην περίπτωση των καταστατικών διανυσμάτων να ορίσουμε το συζυγές του ket $|\ >$.
Πράγματι το συζυγές του ket είναι ένα διάνυσμα, <u>το λεγόμενο bra</u>, που συμβολίζεται ως

$<|$ και αν/χεί στην συζυγή κυματοσυνάρτηση $\psi^*(r,t)$.

Για κάθε διάνυσμα $|\psi>$, το $\langle\psi|$

είναι ο συζυγής του $|\psi>$ δηλ. ο $|\psi\rangle^t$.

Δηλώνουμε $\langle\phi|\psi\rangle = \langle\phi|\cdot|\psi\rangle$ το εσωτερικό γινόμενο 2 διανυσμάτων $|\varphi>$, $|\psi>$.

Ιδιότητες του εσωτερικού γινομένου

1. $<\psi_1|\psi_2>=<\psi_2|\psi_1>^*$

Αρα: $<\psi_1|\psi_1>=<\psi_1|\psi_1>^*$ οπότε ο αριθμός $<\psi_1|\psi_1>$ είναι πραγματικός αριθμός.

2. Είναι μια πράξη γραμμική ως προς τα ket.

Δηλ. αν $|\psi_3>=\alpha|\psi_1>+\beta|\psi_2>$

τότε $<\psi_4|\psi_3>=\alpha<\psi_4|\psi_1>+\beta<\psi_4|\psi_2>$

Επίσης $<\psi_3|\psi_4>=\alpha^*<\psi_1|\psi_4>+\beta^*<\psi_2|\psi_4>$

3. Το εσωτερικό γινόμενο ενός διανύσματος με τον εαυτό του είναι θετικό και ορισμένο. Δηλαδή:

$<\psi|\psi> \geq 0$

Περιγραφή Heisenberg

Στην περιγραφή αυτή κάθε κατάσταση περιγράφεται με ένα μονοδιάστατο πίνακα μιας στήλης.

Παραδείγματα:

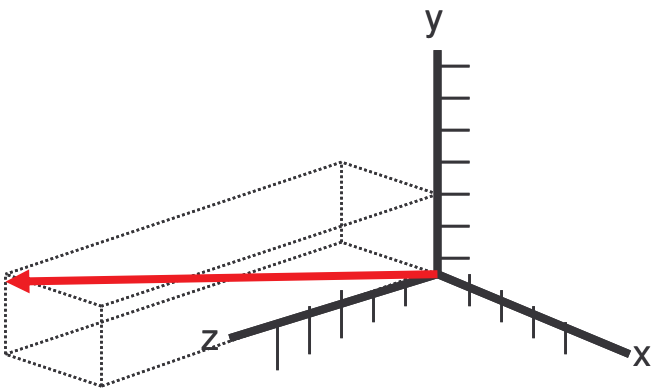
$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \leftrightarrow \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$|\psi_2 >= i\frac{3}{5}|0> -i\frac{4}{5}|1>) \leftrightarrow \begin{pmatrix} i\frac{3}{5} \\ -i\frac{4}{5} \end{pmatrix}$$

4.12 Τυπική κατάσταση διανύσματος κβαντικού συστήματος



Μια τυπική κατάσταση κβαντικού συστήματος στην περίπτωση όπου χρησιμοποιούμε 3 κβαντικά bit (κατάσταση αυτή αντιστοιχεί σ' ένα διάνυσμα ενός χώρου Hilbert με 2^3 διαστάσεις) είναι η:

$$|\psi> = \alpha_0 |000> + \alpha_1 |001> + \alpha_2 |010> + \alpha_3 |011> + \alpha_4 |100> + \alpha_5 |101> + \alpha_6 |110> + \alpha_7 |111>$$

όπου οι συντελεστές α_0, α_1, α_2,...,α_7 είναι μιγαδικοί αριθμοί (μιγαδικά πλάτη). Κάθε ένας από αυτούς αν υψωθεί στο τετράγωνο μας δίνει την πιθανότητα να εμφανιστεί η αντίστοιχη κατάσταση.
Είναι φανερό ότι το άθροισμα των πιθανοτήτων όλων των καταστάσεων πρέπει να ισούται με 1.
Παρακάτω φαίνεται ένα παράδειγμα:

Κατάσταση	Μιγαδικά Πλάτη	Πιθανότητα
	$a_i = x+iy$	x^2+y^2
000	.37+.04i	.14
001	.11+.18i	.04
010	.09+.31i	.10
011	.30+.30i	.18
100	.35+.43i	.31
101	.40+.01i	.16
110	.09+.12i	.02
111	.15+.16i	.05

Άθροισμα πιθανοτήτων =1

4.13 Κβαντικές Πύλες

Αν θέλουμε να μετασχηματίσουμε μια κατάσταση ενός κβαντικού συστήματος σε μια άλλη θα πρέπει να χρησιμοποιήσουμε ορθομοναδιαίους τελεστές (άρα ορθομοναδιαίους πίνακες – unitary matrices) οι οποίοι θα έχουν την ιδιότητα:

$$UU^{\dagger} = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \begin{bmatrix} u_{00}^{*} & u_{10}^{*} \\ u_{01}^{*} & u_{11}^{*} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Αυτό σημαίνει ότι για κάθε πίνακα U (μετασχηματισμό) υπάρχει ο αντίστροφός του. Σαν συνέπεια αυτού κάθε προηγούμενη κατάσταση μπορεί να ανακτηθεί από την τωρινή.

Ουσιαστικά αυτό συμβαίνει <u>γιατί οι κανόνες της κβαντομηχανικής απαιτούν η εξέλιξη στην κατάσταση ενός συστήματος να είναι αντιστρέψιμη στο χρόνο.</u>

Σαν συνέπεια οι πύλες που θα χρησιμοποιήσουμε στους κβαντικούς υπολογισμούς (κβαντικές πύλες) θα πρέπει να είναι αντιστρέψιμες. Αυτό σημαίνει ότι για κάθε πύλη (μετασχηματισμός) που θα χρησιμοποιήσουμε υπάρχει η αντίστροφή της.
Στο σημείο αυτό πρέπει να σημειώσουμε ότι μόλις γίνει μία μέτρηση ενός κβαντικού συστήματος «μεταφερόμαστε» στον κλασικό κόσμο όπου φυσικά δεν είναι αντιστρέψιμος στο χρόνο.

Παρακάτω αναφέρουμε μερικά παραδείγματα μετασχηματισμών:

<u>*Ο ταυτοτικός πίνακας*</u> (identity matrix) για ένα σύστημα 2 καταστάσεων («0» και «1»)

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

<u>*Οι 2x2 πίνακες Pauli είναι οι*</u>:

$$X = \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

<u>*Ο μετασχηματισμός Hadamard*</u>

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} (\sigma_x + \sigma_z)$$

<u>*Ο μετασχηματισμός U_f*</u>

Αντιστοιχεί σε πύλη 2 εισόδων αφού δρά σε 2 κβαντικά bit.

$$U_f|x\rangle|y\rangle = |x\rangle|y +_2 f(x)\rangle$$

$+_2$ σημαίνει άθροισμα modulo 2.

Το κβαντικό bit |x> ονομάζεται control qubit και δεν αλλάζει.

Το κβαντικό bit |y> ονομάζεται target qubit και η τιμή του εξαρτάται απο την τιμή του f(x) (Εάν είναι f(x)=0 ή f(x)=1).

Παράδειγμα : Εαν f(x)=x έχουμε τότε η αντίστοιχη πύλη λέγεται C-NOT ή Feynman και είναι το κβαντομηχανικό ανάλογο της XOR πύλης (γι'αυτό λέγεται και XOR gate). Πιο συγκεκριμένα:

$$U_f|x\rangle|y\rangle = |x\rangle|y +_2 x\rangle$$

Δέχεται τα |x> και |y> ως εισόδους και στη θέση του y εμφανίζει το άθροισμα modulo 2 των y και x.

Ο πίνακας που αντιστοιχεί στον μετασχηματισμό C-not είναι:

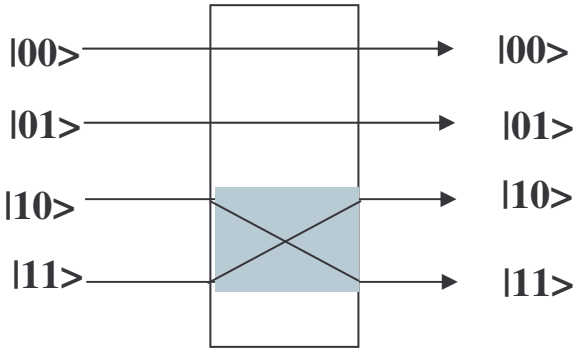
$$\begin{array}{c} \begin{matrix} 00 & 01 & 10 & 11 \end{matrix} \\ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} \end{array}$$

Επίσης ισχύει:

$$|x\rangle|0\rangle \rightarrow |x\rangle|x\rangle$$

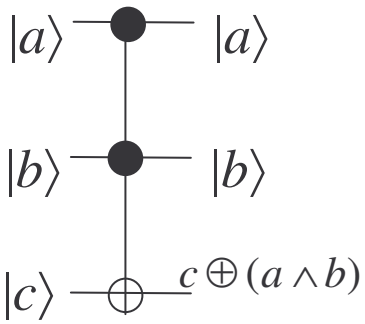
$$|x\rangle|1\rangle \rightarrow |x\rangle|not \quad x\rangle$$

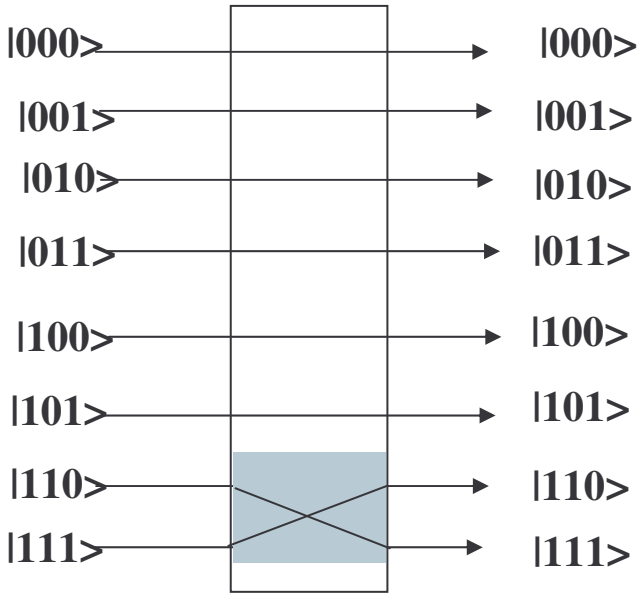
Παρατηρούμε επίσης ότι αν το x είναι 0 τότε y δεν αλλάζει τιμή, ενώ αν το x είναι 1 το y αλλάζει τιμή.



<u>Ο μετασχηματισμός Toffoli (C-C-Not)</u>

Είναι πύλη τριών εισόδων. Αυτό που κάνει είναι να αλλάζει το τελευταίο bit αν τα δύο πρώτα είναι 1.





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

Μπορεί να χρησιμοποιηθεί για να κατασκευάσουμε πύλες AND και πύλες NOT. Δηλαδή:

$$T\,|1,1,x>=|1,1,\neg x>$$
$$T\,|x,y,0>=|x,y,x\wedge y>$$

Άρα είναι ένα πλήρες σύνολο κβαντικών πυλών.

Επίσης είναι μια πύλη AND αν το τελευταίο bit είναι 0 ενώ είναι μια πύλη NAND αν το τελευταίο είναι 1.

Τι αποτέλεσμα έχουν αν δράσουν οι προηγούμενοι μετασχηματισμοί σε μια κβαντική κατάσταση;

Αν ονομάσουμε την κατάσταση |0> με u και την κατάσταση |1> με d τότε θα ισχύουν τα εξής:

<u>Ο ταυτοτικός πίνακας</u>

1u=u 1d=d

$$1[\frac{1}{\sqrt{2}}(u+d)] = \frac{1}{\sqrt{2}}(1u+1d)] = \frac{1}{\sqrt{2}}(u+d)$$

<u>Οι 2x2 πίνακες Pauli</u>

$$\sigma_x u = d, \quad \sigma_x d = u$$

$$\sigma_z u = u, \quad \sigma_z d = -d$$

$$\sigma_x[\frac{1}{\sqrt{2}}(u+d)] = \frac{1}{\sqrt{2}}(\sigma_x u + \sigma_x d)] = \frac{1}{\sqrt{2}}(d+u) = \frac{1}{\sqrt{2}}(u+d)$$

Ποιες οι ιδιότητες των πινάκων Pauli;

$$\sigma_x^2 = 1$$
$$\sigma_y^2 = 1$$
$$\sigma_z^2 = 1$$
$$\sigma_x\sigma_y = -\sigma_y\sigma_x = i\sigma_z$$
$$\sigma_y\sigma_z = -\sigma_z\sigma_y = i\sigma_x$$
$$\sigma_z\sigma_x = -\sigma_x\sigma_z = i\sigma_y$$

<u>Ο μετασχηματισμός Hadamard</u>

$$Hu = H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}(u+d) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$Hd = H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = \frac{1}{\sqrt{2}}(u-d) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Οπως αναφέραμε οι κβαντικές πύλες είναι αντιστρέψιμες. Στην περίπτωση του μετασχηματισμού H ο αντίστροφός του συμπίπτει με τον εαυτό του. Πράγματι:

H(Hu)=u
H(Hd)=d

<u>Ο μετασχηματισμός U_f</u>

Έστω ότι η y είναι η κατάσταση |0>-|1> τότε:

$$U_f|x\rangle\otimes(|0\rangle-|1\rangle)=|x\rangle\otimes[(|0\rangle-|1\rangle)+_2 f(x)]$$

Εάν η f(x)=0 έχουμε:

$$|x\rangle\otimes[(|0\rangle-|1\rangle)+_2 f(x)]=|x\rangle\otimes[(|0\rangle-|1\rangle)+_2 0]=$$

$$=|x\rangle\otimes[(|0\rangle-|1\rangle)]=|x\rangle\otimes(-1)^{f(x)}(|0\rangle-|1\rangle)$$

Εάν η f(x)=1 έχουμε:

$$|x\rangle\otimes[(|0\rangle-|1\rangle)+_2 f(x)]=|x\rangle\otimes[(|0\rangle-|1\rangle)+_2 1]=$$

$$=|x\rangle\otimes[(|1\rangle-|0\rangle)]=|x\rangle\otimes(-1)^{f(x)}(|0\rangle-|1\rangle)$$

Γενικά μπορούμε να πούμε ότι:`

$$U_f|x\rangle\otimes(|0\rangle-|1\rangle)=|x\rangle\otimes(-1)^{f(x)}(|0\rangle-|1\rangle)$$

<u>Ο μετασχηματισμός C-not (Feynman)</u>

Όπως αναφέραμε προηγουμένως ισχύει:

$$U_f|x\rangle|y\rangle=|x\rangle|y+_2 x\rangle$$

Έτσι αν δράσει ο μετασχηματισμός C-not στο |10>

$$U_f|1\rangle|0\rangle=|1\rangle|0+_2 1\rangle=|1\rangle|1\rangle$$

Σε περιγραφή Heisenberg η ίδια δράση

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

4.14 Εποπτικός τρόπος παρουσίασης των κβαντικών πυλών

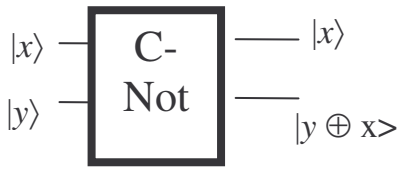
Οι προηγούμενες κβαντικές πύλες είναι μίας εισόδου (άρα και μίας εξόδου)

$$X=\sigma_X=\begin{bmatrix}0&1\\1&0\end{bmatrix}$$

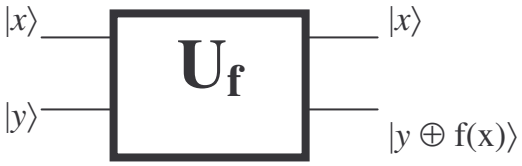
$$Y=\sigma_Y=\begin{bmatrix}0&-i\\i&0\end{bmatrix}$$

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

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



$$C-Not=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

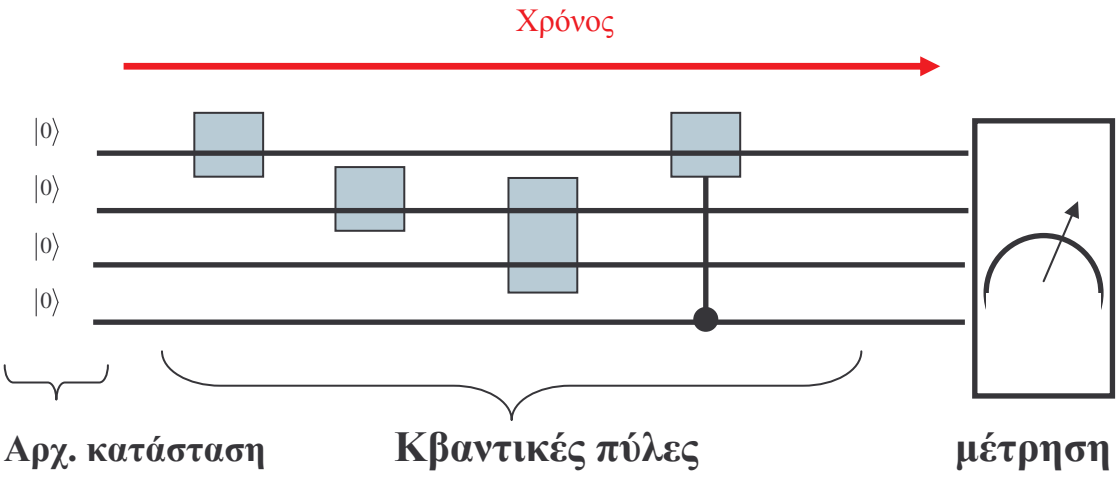


Εχουμε 4 περιπτώσεις αν θέλουμε να αντιστοιχήσουμε την πύλη αυτή σε πίνακα.

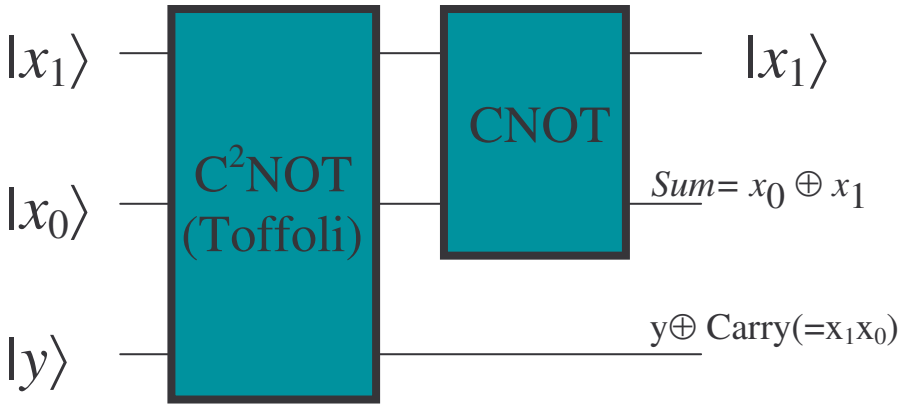
$$U_{f_1}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\qquad U_{f_1}=\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\qquad U_{f_3}=\begin{pmatrix}1&0&0&0\\1&0&0&0\\0&0&1&0\\0&0&1&0\end{pmatrix}\qquad U_{f_4}=\begin{pmatrix}0&1&0&0\\0&1&0&0\\0&0&0&1\\0&0&0&1\end{pmatrix}$$

4.15 Κβαντικά κυκλώματα

Τα κβαντικά κυκλώματα είναι επέκταση των κλασικών λογικών κυκλωμάτων. Θα αποτελούνται δηλαδή από κβαντικές πύλες που θα συνδέονται μεταξύ τους χωρίς ανάδραση με κβαντικά σύρματα. Κάθε σύρμα αντιπροσωπεύει το μονοπάτι ενός κβαντικού bit και περιγράφεται με μία κατάσταση σε ένα δισδιάστατο χώρο Hilbert με βάση τα διανύσματα |0> και |1>.



4.16 Ένα απλό κβαντικό κύκλωμα (ημιαθροιστής) (σε απλοποιημένη μορφή)



Παρατηρούμε ότι:
$1^{η}$) αν η είσοδος είναι |0,0,y> μετά την Toffoli θα έχουμε |0,0, y⊕0> και μετά την C-Not |0,0, y⊕0>. Αρα άθροισμα=0 και υπόλοιπο=0 όπως αναμέναμε.
$2^{η}$) αν η είσοδος είναι |0,1,y> μετά την Toffoli θα έχουμε |0,1, y⊕0> και μετά την C-Not |0,1, y⊕0>. Αρα άθροισμα=1 και υπόλοιπο=0 όπως αναμέναμε.

$3^{η}$) αν η είσοδος είναι |1,0,y> μετά την Toffoli θα έχουμε |1,0, y⊕0> και μετά την C-Not |1,1,0>. Αρα άθροισμα=1 και υπόλοιπο=0 όπως αναμέναμε.

$4^{η}$) αν η είσοδος είναι |1,1,y> μετά την Toffoli θα έχουμε: |1,1, y⊕1> και μετά την C-Not |1,0, y⊕1>. Αρα άθροισμα=0 και υπόλοιπο=1 όπως αναμέναμε.

4.17 Σύνδεση Κβαντικών Πυλών σε σειρά (Γινόμενο Πινάκων)

Εάν θέλουμε να συνδέσουμε κβαντικές πύλες σε σειρά αρκεί να πολλαπλασιάσουμε τους αντίστοιχους πίνακες.

Παράδειγμα: Εχουμε 2 πύλες Hadamard σε σειρά

$$\left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \right)^2 = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Αυτό σημαίνει με άλλα λόγια ότι: H(Hu)=u

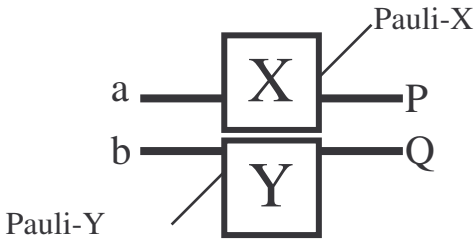
4.18 Παράλληλη Σύνδεση Κβαντικών Πυλών (Γινόμενο Kronecker)

Όταν έχουμε παράλληλη σύνδεση κβαντικών πυλών αρκεί να χρησιμοποιήσουμε το γινόμενο Kronecker (tensor product) για τους πίνακες που αντιστοιχούν στις πύλες αυτές.

Γινόμενο Kronecker:

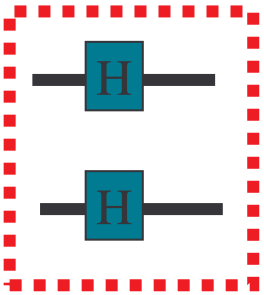
$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \otimes \begin{bmatrix} x & y \\ z & v \end{bmatrix} = \begin{bmatrix} a\begin{bmatrix} x & y \\ z & v \end{bmatrix} & b\begin{bmatrix} x & y \\ z & v \end{bmatrix} \\ c\begin{bmatrix} x & y \\ z & v \end{bmatrix} & d\begin{bmatrix} x & y \\ z & v \end{bmatrix} \end{bmatrix} = \begin{bmatrix} ax & ay & bx & by \\ az & av & bz & bv \\ cx & cy & dx & dy \\ cz & cv & dz & dv \end{bmatrix}$$

Παράδειγμα 1:



$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{array}{c} \begin{matrix} \mathbf{00} & \mathbf{01} & \mathbf{10} & \mathbf{11} \end{matrix} \\ \begin{pmatrix} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{pmatrix} \end{array} \begin{matrix} \\ \mathbf{00} \\ \mathbf{01} \\ \mathbf{10} \\ \mathbf{11} \end{matrix}$$

Παράδειγμα 2: *Παράλληλη σύνδεση δύο κβαντικών πυλών Hadamard*



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

Παράδειγμα 3: *Ο μετασχηματισμός Walsh-Hadamard* W_{2^n}

Ο μετασχηματισμός αυτός ορίζεται ως εξής:

$$W_2 = H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

$$W_{2^n} = \frac{1}{\sqrt{2^n}}\begin{pmatrix}W_{2^{n-1}} & W_{2^{n-1}}\\ W_{2^{n-1}} & -W_{2^{n-1}}\end{pmatrix}$$

Έτσι η πράξη

$$W_4 = W_2 \otimes W_2 = \frac{1}{2}\begin{pmatrix}W_2 & W_2\\ W_2 & -W_2\end{pmatrix} = H \otimes H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} =$$

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

Επίσης

$$W_8 = W_4 \otimes W_4 = \frac{1}{2}\begin{pmatrix}W_4 & W_4\\ W_4 & -W_4\end{pmatrix}$$

Άρα είναι σαν να έχουμε 4 πύλες H παράλληλες.

Δράση του μετασχηματισμού W_4 σε μια κβαντική κατάσταση

Όπως αναφέραμε ο μετασχηματισμός αυτός δεν είναι τίποτα άλλο παρά 2 πύλες H παράλληλες.

Το αποτέλεσμα της δράσης μιας πύλης H σε ένα κβαντικό bit $|0>$ είναι να δημιουργεί μια κατάσταση υπέρθεσης των $|0>$ και $|1>$.

$$Hu = H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}(u+d) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Το ίδιο συμβαίνει αν δράσει μια πύλη W_4 σε ένα σύστημα 2 κβαντικών bit τα οποία βρίσκονται στην κατάσταση $|00\rangle$ (Δηλαδή το κάθε ένα βρίσκεται στην κατάσταση $|0\rangle$). Δημιουργεί δηλαδή μια κατάσταση υπέρθεσης των καταστάσεων $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Πιο συγκεκριμένα:

$$W_4|uu\rangle = W_4|00\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

Γενικά ισχύει το εξής:

$$W_{2^n}|00...000\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$$

Επίσης αν η αρχική κατάσταση είναι η $|y\rangle$ τότε:

$$W_{2^n}|y\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{x.y}|x\rangle$$

όπου

$$x.y = x_{n-1}y_{n-1} + x_{n-2}y_{n-2} + ... + x_1y_1 + x_0y_0 \bmod 2$$

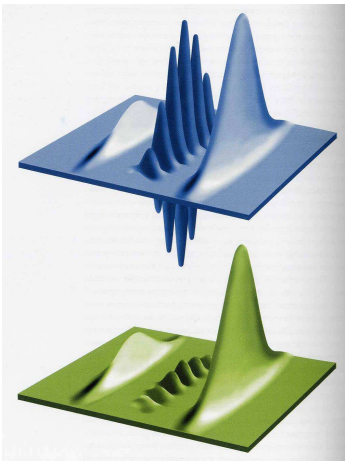
Παράδειγμα αν η αρχική μας κατάσταση είναι η $|110\rangle$ τότε:

$$|\psi\rangle = W_{2^3}|y\rangle = \frac{1}{\sqrt{2^3}}(|000\rangle + |001\rangle - |010\rangle - |011\rangle - |100\rangle - |101\rangle + |110\rangle + |111\rangle)$$

|y>	|x>	x.y	$(-1)^{x.y}$
|110>	|000>	0	1
|110>	|001>	0	1
|110>	|010>	1	-1
|110>	|011>	1	-1
|110>	|100>	1	-1
|110>	|101>	1	-1
|110>	|110>	2	1
|110>	|111>	2	1

4.19 Η έννοια Αποσυνοχή (Ασυμφωνία- Decoherence)

Είναι μια πραγματική φυσική διαδικασία που συμβαίνει οποτεδήποτε ένα κβαντικό σύστημα δεν είναι πλέον απομονωμένο από το μακροσκοπικό περιβάλλον του και η κυματοσυνάρτησή του εμπλέκεται με την πολύπλοκη κατάσταση του περιβάλλοντος – που μπορεί να είναι οτιδήποτε : φωτοευαίσθητο πέτασμα, μόρια αέρα, ηλεκτρονική διάταξη κ.λ.π. Αν η σύζευξη με το εξωτερικό «περιβάλλον» είναι αρκετά ισχυρή, τότε η αρχικά λεπτεπίλεπτη υπέρθεση χάνεται πολύ γρήγορα. Η αποσυνοχή είναι μια από τις ταχύτερες και αποτελεσματικότερες διεργασίες της φυσικής. Αυτή ακριβώς ή αξιοσημείωτη αποτελεσματικότητα είναι υπεύθυνη για την μέχρι τώρα αδυναμία ανακάλυψης της αποσυνοχής. Για την κατασκευή κβαντικών υπολογιστών είναι απαραίτητο να μπορούμε να ελέγχουμε τα φαινόμενα ασυμφωνίας.[1]



«Κατανομή Βίγκνερ»

Οι δυο οριζόντιοι άξονες συμβολίζουν τη θέση και την ορμή ενός κβαντικού σωματιδίου.

Οι ταλαντώσεις στο κέντρο αν/χούν στους όρους συμβολής.(υπέρθεση)

Οι δύο μεγάλες ανωμαλίες συμβολίζουν τις 2 δυνατές θέσεις του σωματιδίου.

Μετά από σύντομο χρονικό διάστημα η αποσυνοχή προκαλεί την εξάλειψη των όρων συμβολής.

Οι δύο φυσικά πραγματοποιήσιμες επιλογές παραμένουν ανεπηρέαστες.

4.20 Μέτρηση ενός κβαντικού συστήματος

Στο πείραμα των δύο σχισμών μέτρηση γίνεται όταν το σωμάτιο «κτυπάει» στο πέτασμα. Αυτό σημαίνει ότι καταρρέει η κυματοσυνάρτηση που περιγράφει την κατάσταση του σωματιδίου και πλέον το σωμάτιο βρίσκεται σε μια συγκεκριμένη θέση στο πέτασμα.

Όπως είπαμε αν ένα qubit βρίσκεται στην κατάσταση $|\psi> = \alpha\ |0> + \beta\ |1>$ και κάνουμε μια μέτρηση τότε έχουμε πιθανότητα $|a|^2$ να το «βρούμε» στην

κατάσταση $|0\rangle$ (ή u ή $\begin{pmatrix}1\\0\end{pmatrix}$) και $|b|^2$ να το «βρούμε» στην κατάσταση $|1\rangle$ (ή d ή $\begin{pmatrix}0\\1\end{pmatrix}$).

Πόσο σημαντική όμως είναι η απόφαση της μέτρησης ενός κβαντικού συστήματος και πόσο επηρεάζει την τελική κατάσταση του συστήματος;

Έστω ένα κύκλωμα στο οποίο τροφοδοτούμε ένα qubit στην κατάσταση $|0\rangle$ σε μια πύλη Hadamard και την έξοδό της την τροφοδοτούμε πάλι με μια πύλη Hadamard. Η έξοδος του κυκλώματος είναι η έξοδος της δεύτερης πύλης.

Περίπτωση1:
Τι θα γίνει αν κάνουμε μέτρηση αφού έχουν δράσει και οι δύο τελεστές Hadamard;
Από τη σχέση H(Hu)=u καταλαβαίνουμε ότι αν εκτελέσουμε μέτρηση στο τέλος (αφού έχουν δράσει και οι δύο πύλες) τότε η αρχική μας κατάσταση θα παραμείνει αμετάβλητη.

Περίπτωση 2:
Τι θα είχε γίνει αν είχαμε κάνει μέτρηση αφού είχε δράσει η πρώτη πύλη και πριν να δράσει η δεύτερη;

Βήμα 1:

$$Hu = H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(u+d) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Αν μετρήσουμε έχουμε 50% πιθανότητα να «δούμε» την κατάσταση u ($|0\rangle$) και 50% πιθανότητα να «δούμε» την κατάσταση d ($|1\rangle$).

Βήμα 2:

Αν μετρήσαμε την κατάσταση u τότε:

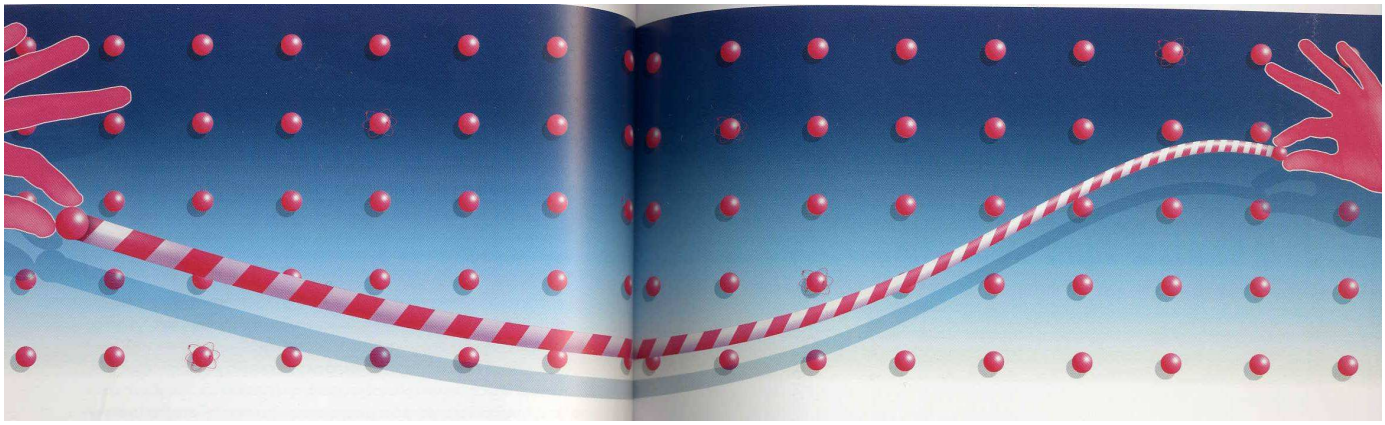
$$Hu = H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}(u+d) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

Αν μετρήσαμε την κατάσταση d τότε:

$$Hd = H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{1}{\sqrt{2}}(u-d) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Το οποίο σημαίνει ότι στην περίπτωση αυτή έχω τελικά 50% να μετρήσω την u και 50% να μετρήσω την d ενώ στην προηγούμενη περίπτωση (μία μέτρηση στο τέλος) είχα 100% πιθανότητα να μετρήσω την αρχική μου κατάσταση!!!

4.21 Η έννοια της Συμπλοκής (entanglement)



Όταν αλληλεπιδρούν δύο κβαντικά σωματίδια, η μοίρα τους συνυφαίνεται, όσο μακριά κι αν βρεθούν – μέχρις ότου ένα από τα αυτά ακουμπήσει μια μετρητική διάταξη. Η μαθηματική έκφραση του συσχετισμού τους είναι μία μόνο ενοποιημένη κυματοσυνάρτηση που περιέχει τη συνδυασμένη και κοινή πληροφορία για τις κβαντικές καταστάσεις και των δύο. Εάν ένα από τα σωματίδια οδηγηθεί σε υπέρθεση – αν, π.χ. συναντήσει μια διπλή σχισμή- το δεύτερο σωματίδιο θα οδηγηθεί επίσης σε υπέρθεση διαφορετικών καταστάσεων οι οποίες συσχετίζονται με την κάθε μία από τις δύο εναλλακτικές του πρώτου σωματιδίου. Η κυματοσυνάρτηση θα περιγράφει τώρα μια κατάσταση «συμπλοκής». Το πιο διάσημο παράδειγμα αυτής της κατάστασης περιγράφηκε από τον Einstein, Podolski και Rosen (το πείραμα EPR).

Ενα παράδειγμα συμβολής συσχετισμένων σωματιδίων (φωτονίων) στην καθημερινότητά μας αφορά την ασφάλεια των οικονομικών συναλλαγών μέσω ηλεκτρονικών συστημάτων. Μάλιστα έχει γίνει ήδη μεταφορά χρημάτων το 2004 από το Δημαρχείο της Βιέννης στην τράπεζα Αυστρίας Creditanstalt σε απόσταση 500 μέτρων. Φωτόνια προερχόμενα από μια δέσμη λέηζερ διέρχονται μέσα από ειδικό κρύσταλλο που μετατρέπει το κάθε φωτόνιο σε ζεύγος δύο συσχετισμένων φωτονίων. Συνεπώς από τον κρύσταλλο εξέρχεται μια σειρά ζευγών φωτονίων, στη συνέχεια δε το ένα από τα δύο συσχετιζόμενα φωτόνια του κάθε ζεύγους μεταφέρεται μέσω οπτικής ίνας από την τράπεζα στο Δημαρχείο. Εκεί καταγράφεται η πόλωση του κάθε φωτονίου που καταφθάνει. Δημιουργείται έτσι μια αλληλουχία καταστάσεων πόλωσης, που αντιστοιχίζεται σε μια αλληλουχία ψηφιακών στοιχείων 0 και 1 και δημιουργείται ένας κωδικός. Ο ίδιος κωδικός φθάνει και στο άλλο άκρο της οπτικής ίνας μέσω των συσχετισμένων «αδελφών» των αρχικών φωτονίων, όπου παρακολουθείται από ειδικούς. Αν, λοιπόν, κατά τη διάρκεια της συναλλαγής κάποιος παρέμβει για να αποκρυπτογραφήσει τον κωδικό θα επηρεάσει τις κβαντικές καταστάσεις που τον αποτελούν και θα τον καταστρέψει. Επιπλέον η μεταβολή αυτή θα γίνει

αντιληπτή ακαριαία από τους παρατηρητές των φωτονίων που είναι συσχετισμένα με αυτά που επιτελούν τη συναλλαγή, και θα παρέμβουν αμέσως.

Τα κβαντικά bit μπορούν να βρεθούν επίσης σε καταστάσεις συμπλοκής, όπου η κατάσταση του ενός συσχετίζεται στενά με την κατάσταση ενός άλλου.

Παράδειγμα η κατάσταση $|\psi>_{AB}=|00>_{AB}+|11>_{AB}$ είναι κατάσταση

συμπλοκής των 2 κβαντικών bit. Η κατάσταση αυτή δεν μπορεί να περιγραφεί ως 2 ξεχωριστές καταστάσεις (των 2 qubit) δηλαδή δεν υπάρχουν a_1,b_1,c_1,d_1 τ.ω:

$$(a_1|0\rangle_A+b_1|1\rangle_A)\otimes(a_2|0\rangle_B+b_2|1\rangle_B)=\frac{1}{\sqrt{2}}(|00>_{AB}+|11>_{AB})$$

γιατί

$$(a_1|0\rangle_A+b_1|1\rangle_A)\otimes(a_2|0\rangle_B+b_2|1\rangle_B)=(a_1a_2|00>_{AB}+a_1b_2|01>_{AB}+b_1a_2|10>_{AB}+b_1b_2|11>_{AB})$$

Αλλά για να φτάσω στην κατάσταση που θέλω θα πρέπει $a_1b_2=0$ το οποίο σημαίνει είτε ότι $a_1a_2=0$ είτε $b_1b_2=0$.

Στο πιο διάσημο κβαντικό πρόγραμμα, τον αλγόριθμο παραγοντοποίησης του Shor, η συμπλοκή χρησιμοποιείται για να επιτρέψει σε δύο ομάδες κβαντικών bit να αποθηκεύσουν μια συλλογή συσχετισμένων αριθμών, όπου κάθε αριθμός της δεύτερης ομάδας δίνεται από μια συγκεκριμένη μαθηματική πράξη (όπως η ύψωση στη δύναμη) του αν/χου αριθμού της πρώτης ομάδας.

Το κβαντικό πρόγραμμα διατάσσει τον υπολογιστή να χειριστεί την πρώτη ομάδα με τέτοιο τρόπο ώστε μέσα από το θαύμα της συμπλοκής, να αποκαλυφθεί μια κοινή ιδιότητα όλων των αριθμών της δεύτερης ομάδας, όπως το να είναι όλοι άρτιοι αριθμοί ή ότι είναι πολλαπλάσια κάποιου άγνωστου αριθμού που πρέπει να ανακαλυφθεί.

4.22 Παρατηρήσεις

1. Ενα κβαντικό σύστημα μπορεί να περιγραφεί από ένα μοναδιαίο διάνυσμα σ'ένα χώρο Hilbert. Για παράδειγμα η κατάσταση ενός qubit μπορεί να περιγραφεί με το διάνυσμα

$$|\psi> = \alpha\ |0> + \beta\ |1> \qquad \textbf{(περιγραφή Dirac)}$$

Όπου α, β είναι μιγαδικοί αριθμοί για τους οποίους ισχύει:

$$|\alpha|^2 + |\beta|^2 = 1$$

Το qubit είναι ένα διάνυσμα ενός δισδιάστατου χώρου Hilbert , $q \in \{au + bd\}$.

Όπου:

$$u \leftrightarrow |u\rangle \leftrightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix} \leftrightarrow |0\rangle \leftrightarrow bit \quad 0$$

$$d \leftrightarrow |d\rangle \leftrightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix} \leftrightarrow |1\rangle \leftrightarrow bit \quad 1$$

τα δύο διανύσματα βάσης του χώρου αυτού.

2. Η εξέλιξη ενός κβαντικού συστήματος περιγράφεται με ένα ορθομοναδιαίο μετασχηματισμό (unitary)

$$|\psi'\rangle = U|\psi\rangle$$

Χρειαζόμαστε ορθομοναδιαίους μετασχηματισμούς γιατί διατηρούν την ευκλείδεια νόρμα. Δηλαδή:

$$\||\psi'\rangle| = |U|\psi\rangle| = \||\psi\rangle| = 1$$

Ορθομοναδιαίοι μετασχηματισμοί σημαίνει

$$UU^{\dagger} = \begin{bmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{bmatrix} \begin{bmatrix} u_{00}^* & u_{10}^* \\ u_{01}^* & u_{11}^* \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

Αυτό έχει σαν συνέπεια ότι υπάρχει πάντα ο αντίστροφος μετασχηματισμός του U.
Άρα οι πύλες που θα χρησιμοποιήσουμε θα είναι αντιστρέψιμες. Δηλαδή ότι για κάθε πύλη θα υπάρχει η αντίστροφή της.

Επίσης μπορούμε να «δούμε» τους ορθομοναδιαίους αυτούς μετασχηματισμούς ως στροφές των μιγαδικών διανυσμάτων (καταστάσεων ψ) οι οποίοι μάλιστα έχουν την ιδιότητα να διατηρούν το μήκος των διανυσμάτων αυτών.
Ο Bennett [22] έχει αποδείξει ότι κάθε κλασικό κύκλωμα μπορεί να προσομοιωθεί αποδοτικά με ένα αντιστρέψιμο κύκλωμα.

3. Εάν μετρήσουμε την κατάσταση $|\psi>$ του κβαντικού μας συστήματος σε μια ορθοκανονική βάση $|e_1>$, $|e_2>$, …., $|e_d>$ θα βρούμε ένα από αυτά τα διανύσματα βάσης $|e_j>$ με πιθανότητα

$$P(j) = \left|\langle e_j | \psi \rangle\right|^2$$

Δηλαδή η πιθανότητα να βρούμε ένα από αυτά τα διανύσματα βάσης είναι ίση με την προβολή του διανύσματος $|\psi>$ ή $\vec{\psi}$ πάνω στο διάνυσμα βάσης που ψάχνουμε υψωμένη στο τετράγωνο.

4. Ο χώρος των καταστάσεων ενός σύνθετου κβαντικού συστήματος είναι το γινόμενο Kronecker (tensor product) των χώρων των καταστάσεων των επιμέρους κβαντικών συστημάτων.

Δηλαδή ο χώρος των καταστάσεων όταν έχουμε 2 qubits είναι ο

$$C^2 \otimes C^2 = C^4$$

με τέσσερα διανύσματα βάσης:

$$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$$

τα οποία μπορούμε να τα γράψουμε και ως:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

5. Η δύναμη των κβαντικών αλγορίθμων προέρχεται:

Α) λόγω του κβαντικού παραλληλισμού (quantum parallelism)

Β) λόγω της κβαντικής συμπλοκής (entanglement)
Κβαντικός παραλληλισμός σημαίνει ότι μπορούν να γίνουν ταυτόχρονα πολλές πράξεις. Όταν ένα διάνυσμα ενός διανυσματικού χώρου με 2^n διαστάσεις περιστρέφεται λόγω κάποιου ορθομοναδιαίου μετασχηματισμού αυτό σημαίνει ότι γίνονται ταυτόχρονα 2^n πράξεις οι οποίες υπολογίζουν τις νέες συνιστώσες του τελικού διανύσματος.

Κεφάλαιο 5

Κβαντικοί Αλγόριθμοι

5.1 Το πρόβλημα του Deutsch

Εστω συνάρτηση f: {0,1} → {0,1}

Έστω ένα μαντείο όπου μπορούμε να ρωτήσουμε ποιο θα είναι το αποτέλεσμα της f αν έχουμε ως είσοδο κάποιο $x \in \{0,1\}$.

Τότε υπάρχουν τέσσερις πιθανές συναρτήσεις:

$$f(x)=0,\ f(x)=1,\ f(x)=x,\quad f(x)=\bar{x}$$

Οι δύο πρώτες περιπτώσεις είναι σταθερές συναρτήσεις, ενώ οι δύο τελευταίες είναι balanced.

Το πρόβλημα του Deutsch είναι το εξής:

Καθορίστε εάν η f(x) είναι σταθερή ή balanced κάνοντας στο μαντείο όσο λιγότερες ερωτήσεις γίνεται .

Κλασική απάντηση

Κλασικά θα πρέπει να ρωτήσουμε 2 φορές το μαντείο για να λύσουμε το πρόβλημα του Deutsch.

Ποιο το αποτέλεσμα της f για x=0?
Ποιο το αποτέλεσμα της f για x=1?

Και αυτό γιατί υπάρχουν τέσσερις περιπτώσεις:

x	$f_1(x)$
0	0
1	0

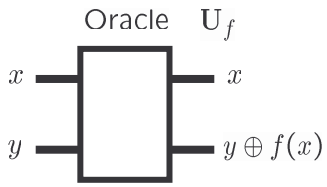
x	$f_2(x)$
0	1
1	1

x	$f_3(x)$
0	0
1	1

X	$f_4(x)$
0	1
1	0

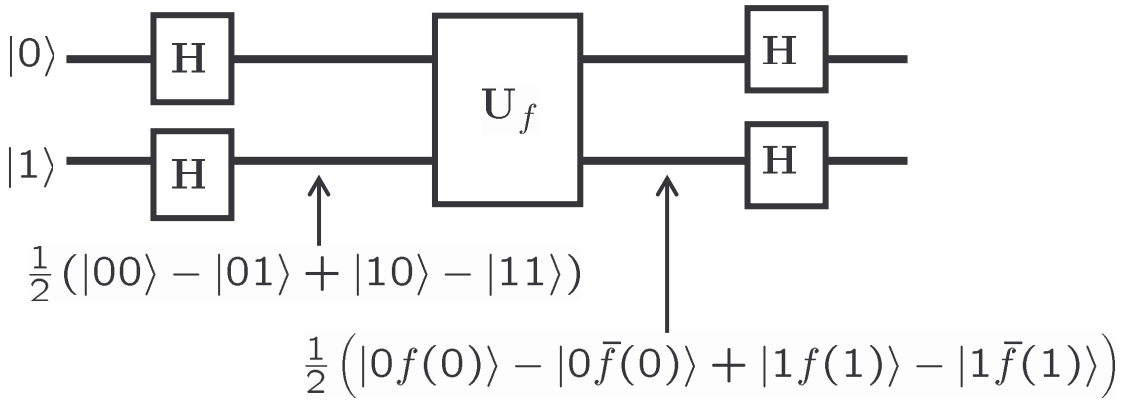
Κβαντική Απάντηση

Για την κβαντική λύση θα χρειαστούμε ένα μαντείο U_f το οποίο δεν είναι τίποτα άλλο παρά ο μετασχηματισμός U_f που περιγράψαμε στην παράγραφο ..... , 4 κβαντικές πύλες Hadamard και 2 κβαντικά bit.



$x, y, f(x) \in \{0, 1\}$

Πιο συγκεκριμένα θα κατασκευάσουμε ένα κβαντικό κύκλωμα όπου η αρχική κατάσταση θα είναι 2 κβαντικά bit , το ένα στην κατάσταση $|0>$ και το άλλο στην κατάσταση $|1>$, όπως φαίνεται στο σχήμα:



Μετά τις 2 πρώτες πύλες η κατάσταση μας θα είναι η:

$$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Και αυτό γιατί οι δύο παράλληλες πύλες Hadamard αντιστοιχούν σε πίνακα:

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

Επίσης η αρχική μας κατάσταση σε περιγραφή Heisenberg γράφεται ως: $\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

Τελικά μετά τις 2 πύλες H έχουμε:

$$\left(\frac{1}{2}\right)\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \left(\frac{1}{2}\right)\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}$$

Δηλαδή την κατάσταση:

$$\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

Το μαντείο έχει ως αποτέλεσμα τα εξής:

|xy>→|x y⊕f(x)>
|00> → |0 0⊕ f(0)> = |0 f(0)>
|01> → |0 1⊕f(0)> = |0 $\overline{f(0)}$>
|10> → |1 0⊕ f(1)> = |1 f(1)>
|11> → |1 1⊕ f(1)> = |1 $\overline{f(1)}$>

Ετσι η κατάσταση μετά το μαντείο είναι:

$$\frac{1}{2}\left(|0f(0)\rangle - |0\bar{f}(0)\rangle + |1f(1)\rangle - |1\bar{f}(1)\rangle\right)$$

Τι γίνεται μετά τις 2 τελευταίες Hadamard;

Έχουμε 4 περιπτώσεις και αυτό γιατί το μαντείο μας μπορεί να είναι:

$$U_{f_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad U_{f_1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad U_{f_3} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad U_{f_4} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Περίπτωση 1η: Εάν $f_1(x)= \bar{x}$ (balanced) το μαντείο θα είναι το

$$U_{f_1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Τότε η κατάστασή μας μετά το μαντείο θα είναι

$$\frac{1}{2}(|01\rangle - |00\rangle + |10\rangle - |11\rangle)$$

ή αλλιώς (σε περιγραφή Heisenberg)

$$\frac{1}{2}\begin{pmatrix}-1\\1\\1\\-1\end{pmatrix}$$

Μετά τις δύο τελευταίες Hadamard θα έχουμε: $$\left(\frac{1}{4}\right)\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix}\begin{pmatrix}-1\\1\\1\\-1\end{pmatrix}=-1\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Αυτό σημαίνει ότι θα μετρήσουμε με πιθανότητα 100% την κατάσταση

$$\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Περίπτωση 2^n: Εάν $f_2(x)=x$ (balanced) το μαντείο θα είναι το

$$U_{f_1}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

Τότε η κατάστασή μας μετά το μαντείο θα είναι

$$\frac{1}{2}(|00\rangle-|01\rangle+|11\rangle-|10\rangle)$$

ή αλλιώς (σε περιγραφή Heisenberg)

$$\frac{1}{2}\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}$$

Μετά τις δύο τελευταίες Hadamard θα έχουμε:

$$\left(\frac{1}{4}\right)\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix}\begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Αυτό σημαίνει ότι θα μετρήσουμε με πιθανότητα 100% την κατάσταση $\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$

Περίπτωση 3η: Εάν $f_3(x)=0$ (σταθερή) το μαντείο θα είναι το

$$U_{f_3}=\begin{pmatrix}1&0&0&0\\1&0&0&0\\0&0&1&0\\0&0&1&0\end{pmatrix}$$

Τότε η κατάσταση μας μετά το μαντείο θα είναι

$$\frac{1}{2}(|00\rangle-|01\rangle+|10\rangle-|11\rangle)$$

ή αλλιώς (σε περιγραφή Heisenberg)

$$\frac{1}{2}\begin{pmatrix}-1\\1\\-1\\1\end{pmatrix}$$

Μετά τις δύο τελευταίες Hadamard θα έχουμε:

$$\left(\frac{1}{4}\right)\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix}\begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}=\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$$

Αυτό σημαίνει ότι θα μετρήσουμε με πιθανότητα 100% την κατάσταση $\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$

Περίπτωση 4η: Εάν $f_4(x)=1$ (σταθερή) το μαντείο θα είναι το

$$U_{f_4}=\begin{pmatrix}0&1&0&0\\0&1&0&0\\0&0&0&1\\0&0&0&1\end{pmatrix}$$

Τότε η κατάσταση μας μετά το μαντείο θα είναι

$$\frac{1}{2}(|01\rangle - |00\rangle + |11\rangle - |10\rangle)$$

ή αλλιώς (σε περιγραφή Heisenberg)

$$\frac{1}{2}\begin{pmatrix} -1 \\ 1 \\ -1 \\ 1 \end{pmatrix}$$

Μετά τις δύο τελευταίες Hadamard θα έχουμε:

$$\left(\frac{1}{4}\right)\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} -1 \\ 1 \\ -1 \\ 1 \end{pmatrix} = -1\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

Αυτό σημαίνει ότι θα μετρήσουμε με πιθανότητα 100% την κατάσταση $\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$

Τελικά κάνοντας **μόνο μία ερώτηση** στο μαντείο καταλαβαίνουμε εάν η συνάρτηση είναι σταθερή ή balanced. Και αυτό αφού αν μετρήσουμε την κατάσταση

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

καταλαβαίνουμε ότι είναι σταθερή ενώ αν μετρήσουμε την κατάσταση

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

καταλαβαίνουμε ότι είναι balanced.

5.2 Γενίκευση του προηγούμενου προβλήματος
Deutsch-Jozsa Problem (1992)

Εστω $f:\{0,1\}^n \rightarrow \{0,1\}$

Όπου είναι δεδομένο ότι η *f μπορεί να είναι είτε:*

α) Σταθερή

$$f(x) = b \ \forall x$$

B) Balanced

$x \in S$ f(x)=1 εάν αλλιώς f(x)=0

όπου το S έχει 2^{n-1} στοιχεία

Να βρεθεί εάν η f(x) είναι σταθερή ή balanced χρησιμοποιώντας το μικρότερο αριθμό ερωτήσεων.

Κλασική απάντηση

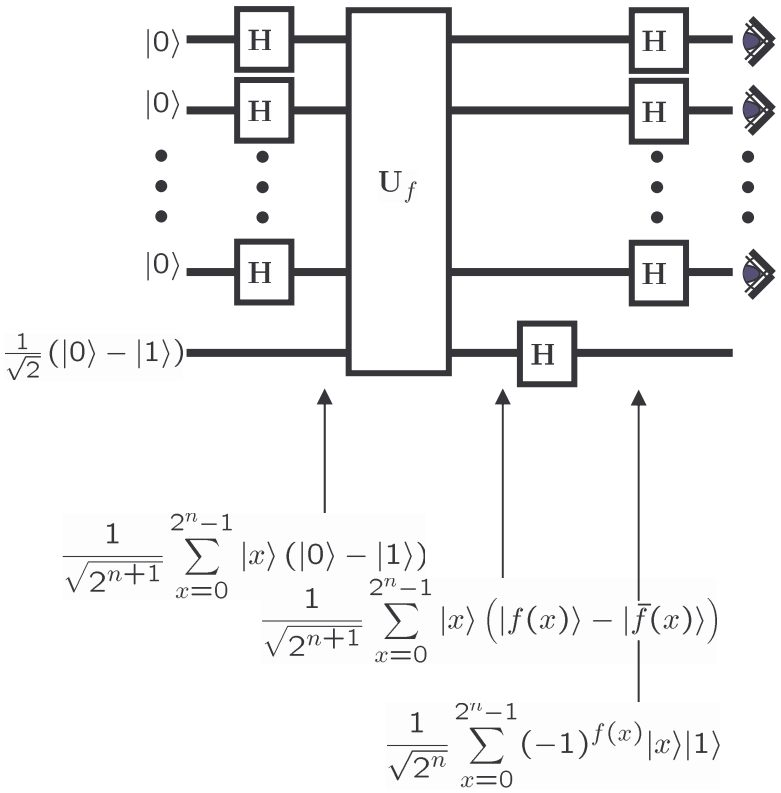
Κλασικά θα πρέπει να ρωτήσουμε $2^{(n-1)}+1$ φορές το μαντείο για να λύσουμε το πρόβλημα του Deutsch. Π.χ:

Ποιο το αποτέλεσμα της f για x=0?
Ποιο το αποτέλεσμα της f για x=1?
.....
Ποιο το αποτέλεσμα της f για $x=2^{n-1}$ *?*
Ποιο το αποτέλεσμα της f για $x=2^{n-1}+1$ *?*

Κβαντική απάντηση

Χρειαζόμαστε 1 ερώτηση!

Αρκεί το κατάλληλο κύκλωμα.



Βήμα1:

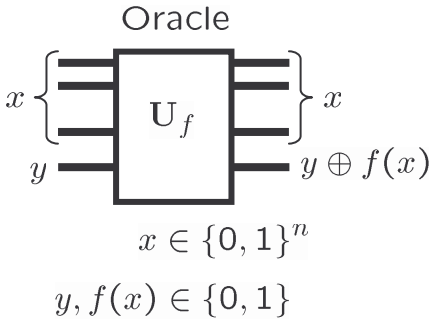
Αρχική κατάσταση που αποτελείται από n καταστάσεις $|0>$ και $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ την

Βήμα2:

n παράλληλες πύλες Hadamard οι οποίες δρουν στις n καταστάσεις $|0>$ και έχουν σαν αποτέλεσμα η κάθε μία από αυτές να βρεθεί σε μία υπέρθεση καταστάσεων $|0>$ και $|1>$.

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x>(|0>-|1>)$$

Βήμα3: Μετά το μαντείο U_f



θα βρεθούμε στην κατάσταση

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x>(|f(x>-|\overline{f(x)}>)$$

ή

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x>(-1)^{f(x)}(|0>-|1>)$$

Βήμα4:

Το τελευταίο qubit περνάει από μια πύλη Hadamard οπότε η κατάσταση του συστήματος γίνεται τώρα

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x>|1>$$

Αφού όπως είπαμε μια πύλη Hadamard όταν δρά στον τελεστή $|1>$ ή d έχει ως αποτέλεσμα :

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

Αλλά αφού οι κβαντικές πύλες είναι αντίστροφες τότε θα ισχύει

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

Βήμα5:

Γίνεται μέτρηση.
Αν η f είναι σταθερή τότε αυτό θα έχει αποθηκευτεί στη φάση.
Πιο συγκεκριμένα εάν f(x)=0 για κάθε x τότε πριν τις Hadamard η κατάσταση θα είναι:

$$(+1)\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x>|1>$$

Εάν f(x)=1 για κάθε x τότε πριν τις Hadamard η κατάσταση θα είναι:

$$(-1)\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x>|1>$$

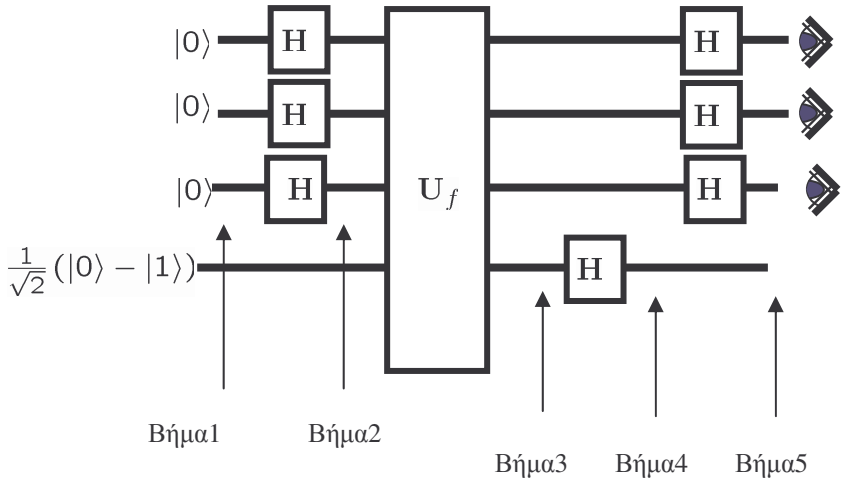
Και στις δύο περιπτώσεις όμως το αποτέλεσμα της μέτρησης θα είναι το ίδιο

|0000....000000>

Εάν η f(x) δεν είναι σταθερή θα μετρήσουμε οποιαδήποτε άλλη κατάσταση εκτός από την $|0000...000000>$.

Ετσι με 1 ερώτηση έχουμε βρεί εάν η f είναι σταθερή ή όχι.

Παράδειγμα (για 3 qbits)



Βήμα1:

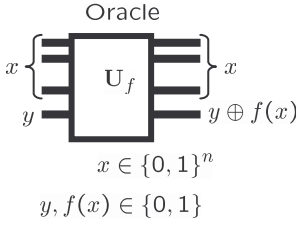
Αρχική κατάσταση που αποτελείται από 3 καταστάσεις $|0>$ και τη $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Βήμα2:

3 παράλληλες πύλες Hadamard οι οποίες δρουν στις 3 καταστάσεις $|0>$ και έχουν σαν αποτέλεσμα η κάθε μία από αυτές να βρεθεί σε μία υπέρθεση καταστάσεων $|0>$ και $|1>$.

$$\frac{1}{\sqrt{2^{3+1}}}\sum_{x=0}^{8-1}|x>(|0>-|1>)=\frac{1}{\sqrt{2^{3+1}}}(|000>+|001>+...+|111>)(|0>-|1>)$$

Βήμα3: Μετά το μαντείο



U_f

θα βρεθούμε στην κατάσταση

$$\frac{1}{\sqrt{2^{3+1}}}\sum_{x=0}^{8-1}|x>(|f(x>-|\overline{f(x)}>)=\frac{1}{\sqrt{2^{3+1}}}(|000>+|001>+...+|111>)(|f(x)>-|\overline{f(x)}>)$$

ή

$$\frac{1}{\sqrt{2^{3+1}}}\sum_{x=0}^{8-1}|x>(-1)^{f(x)}(|0>-|1>)=$$

$$=\frac{1}{\sqrt{2^{3+1}}}((-1)^{f(000)}|000>+(-1)^{f(001)}|001>+...+(-1)^{f(111)}|111>)(|0>-|1>)$$

ή

$$\frac{1}{\sqrt{2^{3+1}}}\sum_{x=0}^{8-1}|x>(-1)^{f(x)}(|0>-|1>)=$$

$$\frac{1}{\sqrt{2^{3+1}}}((-1)^{f(000)}|000>+(-1)^{f(001)}|001>+...+(-1)^{f(111)}|111>)(|0>-|1>)$$

Βήμα4:

$$\frac{1}{\sqrt{2^{3+1}}}\sum_{x=0}^{8-1}(-1)^{f(x)}|x>|1>=\frac{1}{\sqrt{2^{3+1}}}((-1)^{f(000)}|000>+(-1)^{f(001)}|001>+...+(-1)^{f(111)}|111>)|1>$$

Βήμα5: Γίνεται μέτρηση.

<u>Περίπτωση 1η :</u>

Αν η <u>f είναι σταθερή</u> τότε αυτό θα έχει αποθηκευτεί στη φάση.

Πιο συγκεκριμένα εάν f(x)=0 για κάθε x τότε πριν τις Hadamard η κατάσταση θα είναι:

$$\frac{1}{\sqrt{2^3}}\{|000>+|001>+|010>+|011>+|100>+|101>+|110>+|111>\}$$

και το αποτέλεσμα που θα μετρήσουμε θα είναι:

$$|000>$$

Εάν f(x)=1 για κάθε x τότε πριν τις Hadamard η κατάσταση θα είναι:

$$(-1)^1\frac{1}{\sqrt{2^3}}\{|000>+|001>+|010>+|011>+|100>+|101>+|110>+|111>\}$$

Αλλά και πάλι το αποτέλεσμα που θα μετρήσουμε θα είναι το ίδιο: |000>

Περίπτωση 2^n :

Η f δεν είναι σταθερή τότε θα μετρήσουμε οποιαδήποτε άλλη κατάσταση εκτός από την |000>. Παράδειγμα εάν:

$$\frac{1}{\sqrt{2^3}}\{|000>-|001>+|010>-|011>-|100>+|101>-|110>+|111>\}$$

Τότε το αποτέλεσμα θα είναι: **|101>**

Η φιλοσοφία του Αλγόριθμου του Deutsch

Από τη στιγμή που έχουμε μια υπέρθεση όλων των εισόδων, μπορούμε να μάθουμε μια ιδιότητα της f η οποία εξαρτάται από όλες τις τιμές της f(x) με το να τη «χρησιμοποιήσουμε» μόνο μια φορά. Η ιδιότητα αυτή κωδικοποιείται ως πληροφορία της φάσης.

5.3 Αλγόριθμος του Grover
Αλγόριθμος Αναζήτησης (...1996)

Το πρόβλημα:

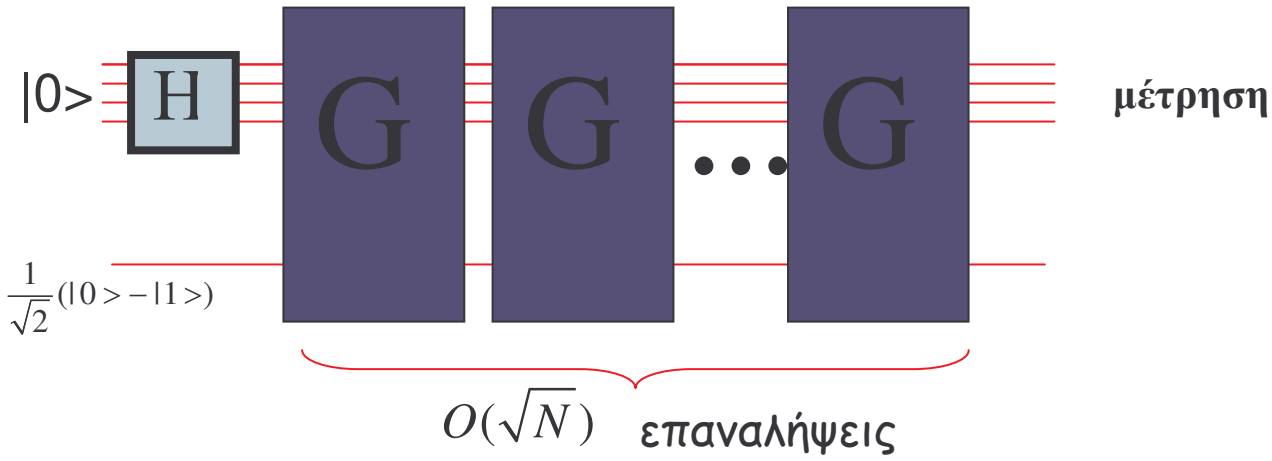
«Εστω μία μη ταξινομημένη βάση που περιέχει N αντικείμενα, από τα οποία μόνο ένα ικανοποιεί μια συνθήκη. Ποιο το αντικείμενο αυτό;»

Κλασική Λύση: Κατά μέσο όρο χρειαζόμαστε N/2 βήματα δηλ. O(N)

Κβαντική Λύση: $O(\sqrt{N})$ βήματα

ΚΒΑΝΤΙΚΗ ΑΠΑΝΤΗΣΗ:

Το κύκλωμα που θα χρησιμοποιήσουμε είναι το εξής:



Βήμα 1: Αρχική κατάσταση

Αποτελείται από n qubit στην κατάσταση $|0>$ και 1 qubit στην κατάσταση $\frac{1}{\sqrt{2}}(|0>-|1>)$

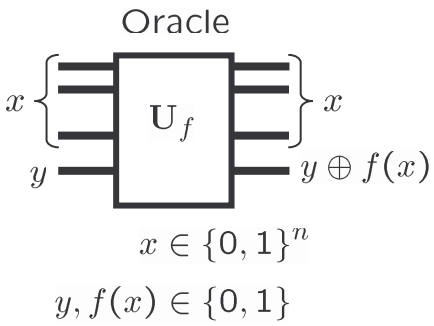
Βήμα 2:

n παράλληλες πύλες Hadamard οι οποίες δρουν στις n καταστάσεις $|0>$ και έχουν σαν αποτέλεσμα η κάθε μία από αυτές να βρεθεί σε μία υπέρθεση καταστάσεων $|0>$ και $|1>$.

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x>(|0>-|1>)$$

Μετασχηματισμός G

Βήμα 3: (πρώτο βήμα στο G)



Μαντείο Ο: δηλαδή ο μετασχηματισμός U_f.

Πιο συγκεκριμένα είναι ο μετασχηματισμός U_{fa} .
Το αποτέλεσμα του μετασχηματισμού είναι να αλλάζει το πρόσημο του |x>=|a> το οποίο και ψάχνουμε και να αφήνει όλες τις άλλες καταστάσεις (πρόσημα) ίδιες (ίδια).

Παράδειγμα για 3 qubits: (Εστω ότι ψάχνουμε το |101>)

Η κατάσταση του συστήματός μας μετά τις πρώτες 8 Hadamard θα είναι

$$\frac{1}{\sqrt{2^{3+1}}}\sum_{x=0}^{8-1}|x>(|0>-|1>)=\frac{1}{\sqrt{2^{3+1}}}(|000>+|001>+...+|111>)(|0>-|1>)$$

Μετά το μετασχηματισμό U_{fa} θα έχουμε την:

$$\frac{1}{\sqrt{2^{3+1}}}\sum_{x=0}^{8-1}|x>(|f(x>-|\overline{f(x)}>)=\frac{1}{\sqrt{2^{3+1}}}(|000>+|001>+...+|111>)(|f(x)>-|\overline{f(x)}>)$$

ή

$$\frac{1}{\sqrt{2^{3+1}}}\sum_{x=0}^{8-1}|x>(-1)^{f(x)}(|0>-|1>)=$$

$$=\frac{1}{\sqrt{2^{3+1}}}((-1)^{f(000)}|000>+(-1)^{f(001)}|001>+...+(-1)^{f(111)}|111>)(|0>-|1>)$$

ή

$$\frac{1}{\sqrt{2^{3+1}}}\sum_{x=0}^{8-1}|x>(-1)^{f(x)}(|0>-|1>)=$$

$$=\frac{1}{\sqrt{2^{3+1}}}((-1)^{f(000)}|000>+(-1)^{f(001)}|001>+...+(-1)^{f(101)}|101>+(-1)^{f(111)}|111>)(|0>-|1>)$$

ή

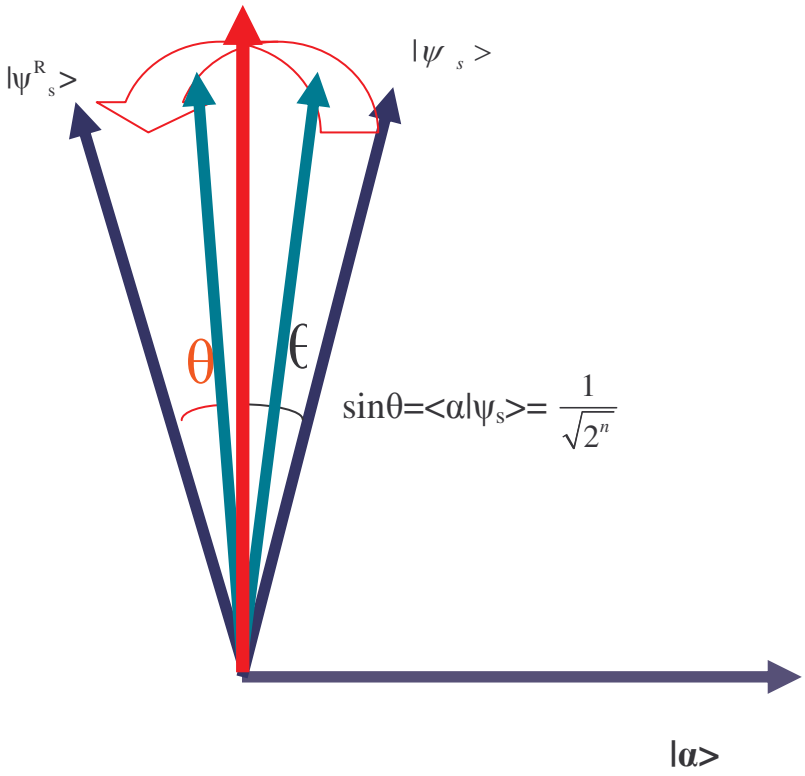
$$\frac{1}{\sqrt{2^{3+1}}}\sum_{x=0}^{8-1}|x>(-1)^{f(x)}(|0>-|1>)=$$

$$=\frac{1}{\sqrt{2^{3+1}}}(|000>+|001>+...+(-1)|101>+|111>)(|0>-|1>)$$

Βήμα 3: (πρώτο βήμα στο G)

(ΓΕΩΜΕΤΡΙΚΗ ΕΞΗΓΗΣΗ)

Θα αναφέρουμε τώρα μια γεωμετρική εξήγηση για το τι ακριβώς κάνει το μαντείο O



Στην ουσία αυτό που κάνει το μαντείο είναι να περιστρέφει το αρχικό διάνυσμα ψ_S του n-διάστατου χώρου Hilbert μέχρι να «φτάσει» το συμμετρικό του διάνυσμα ως προς το υπερεπίπεδο που είναι ορθογώνιο στο διάνυσμα $|\alpha>$ που ψάχνουμε.

Βήμα 4: (Δεύτερο βήμα στο μετασχηματισμό G)

Εφαρμόζουμε n παράλληλες Hadamard στα πρώτα n qubits (δηλ. τον μετασχηματισμό Walsh-Hadamard)

$$\mathbf{H}\,(\,\mathbf{U_{fa}}|\psi_s>\,)$$

Βήμα 5: (Τρίτο βήμα στο μετασχηματισμό G)

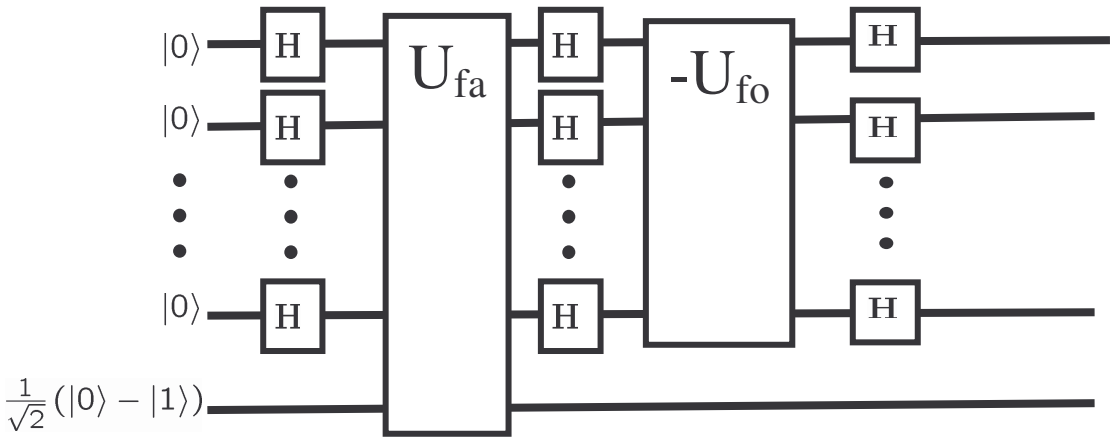
Εφαρμόζουμε το μετασχηματισμό $Z=-U_{fo}$ στα πρώτα n qubits

$$\mathbf{-U_{fo}\,H\,(\,U_{fa}}|\psi_s>\,)$$

Βήμα 6: (Τέταρτο βήμα στο μετασχηματισμό G)

Εφαρμόζουμε τη Hadamard ξανά στα πρώτα n qubits

$$\mathbf{-HU_{fo}\,H\,(\,U_{fa}}|\psi_s>)$$



Τι κάνει ο $-U_{fo}$; Αλλάζει τα πρόσημα σε όλες τις καταστάσεις εκτός από τη $|x>=|0>$

Παράδειγμα για 3 qubits:

$$-U_{f_0}=\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

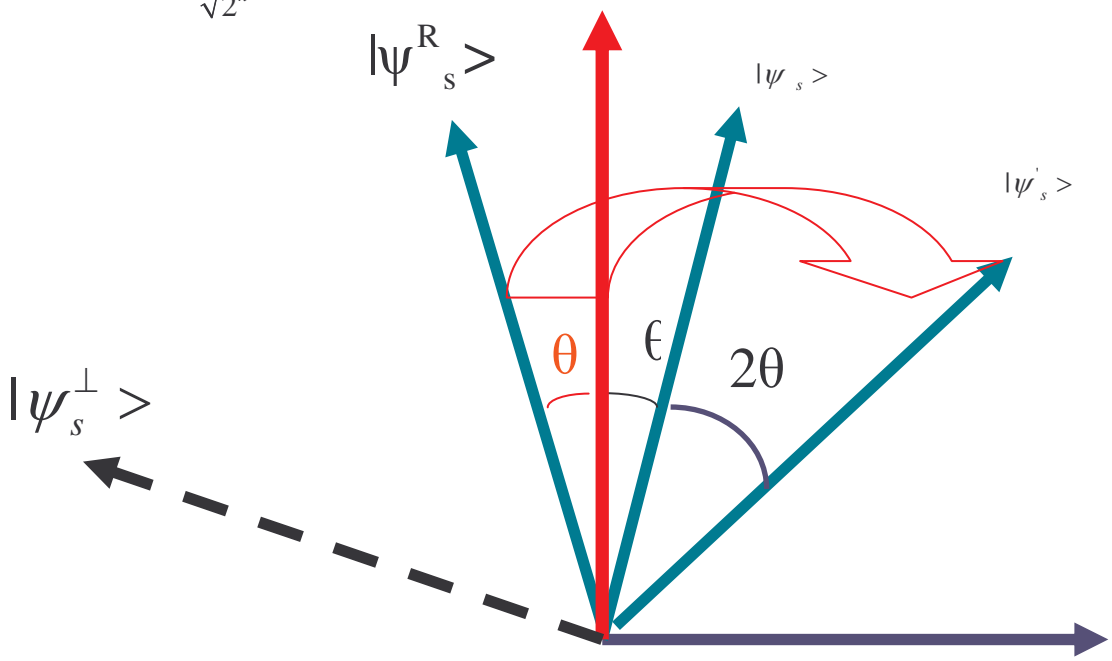
$$-U_{f_0}\,|000>=|000>$$

$$-U_{f_0}\,|001>=-|001>$$

Τι κάνει ο -$HU_{fo}H$; (Γεωμετρική εξήγηση)

Ο μετασχηματισμός **-H U_{fo}H** αν/χεί σε <u>περιστροφή</u> του διανύσματος $|\psi^R_s>$ μέχρι να «φτάσει» στο συμμετρικό του ως προς ένα υπερεπίπεδο που είναι ορθογώνιο στο $|\psi^{\perp}_s>$ (το διάνυσμα που είναι κάθετο στο $|\psi_s>$) .

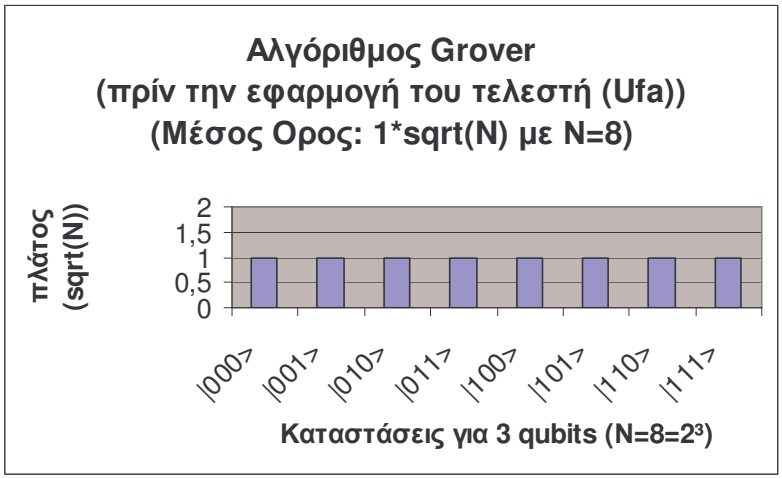
$\sin\theta=<\alpha|\psi_s>=\frac{1}{\sqrt{2^n}}$



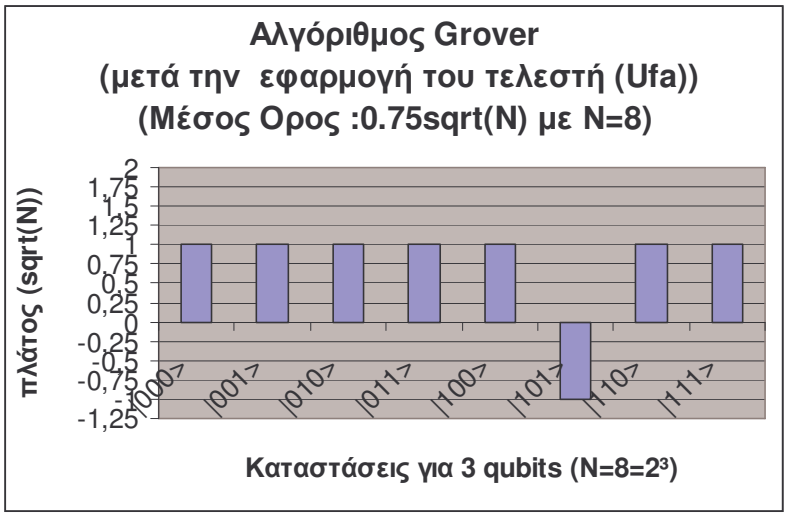
Τελικά έχουμε μια περιστροφή $R_sR_a=(-H\ U_{fo}H)(\ U_{f\alpha}\ )$ του αρχικού $|\psi_s>$ διανύσματος κατά 2θ έτσι ώστε να «πλησιάσει» στο ζητούμενο $|\alpha>$. Ο στόχος είναι να εκτελεσθεί η περιστροφή RsRa τόσες φορές όσες χρειάζεται έτσι ώστε το $|\psi_s>$ να πλησιάσει όσο πιο κοντά γίνεται το $|\alpha>$.

Τι κάνει ο -$HU_{fo}H$;

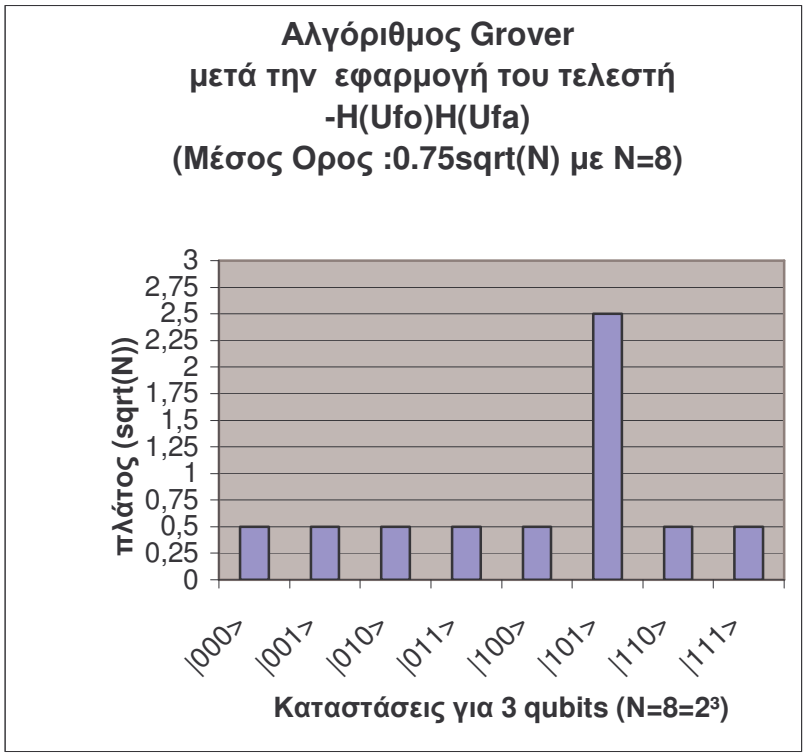
Στην ουσία αυτό που κάνει είναι να αντιστρέφει όλες τις καταστάσεις γύρω από το μέσο όρο. Ο μέσος όρος αρχικά είναι $\frac{1}{\sqrt{2^n}} = \frac{1}{\sqrt{N}}$. Στο παράδειγμα για n=3 έχουμε μέσο όρο $\frac{1}{\sqrt{2^3}} = \frac{1}{\sqrt{8}}$



Μετά την εφαρμογή του τελεστή U_{fa} όπως είπαμε το διάνυσμα που ψάχνουμε αλλάζει πρόσημο άρα ο συντελεστής του από +1 γίνεται -1, άρα αλλάζει ο μέσος όρος των συντελεστών των διανυσμάτων. Στο παράδειγμά μας από $\frac{1}{\sqrt{2^3}} = \frac{1}{\sqrt{8}}$ γίνεται $\frac{0.75}{\sqrt{2^3}} = \frac{0.75}{\sqrt{8}}$



Με την εφαρμογή του τελεστή $\mathbf{-HU_{fo}H}$ έχουμε αντιστροφή ως προς το μέσο όρο. Δηλαδή ο συντελεστής κάθε διανύσματος γίνεται από α_n , σε $2\bar{a}$ - α_n. Παράδειγμα για n=3 όλοι οι συντελεστές των διανυσμάτων εκτός αυτού που ψάχνουμε θα αλλάξουν τιμή και από $\frac{1}{\sqrt{2^3}}=\frac{1}{\sqrt{8}}$ θα γίνουν $\frac{0.5}{\sqrt{2^3}}=\frac{0.5}{\sqrt{8}}$ αφού ο $\bar{a}$ είναι $\frac{0.75}{\sqrt{2^3}}=\frac{0.75}{\sqrt{8}}$. Απ' την άλλη ο συντελεστής του διανύσματος που ψάχνουμε θα γίνει από $-\frac{1}{\sqrt{2^3}}=-\frac{1}{\sqrt{8}}$ σε $\frac{2.5}{\sqrt{2^3}}=\frac{2.5}{\sqrt{8}}$



Γιατί όμως γίνεται αντιστροφή ως προς το μέσο όρο;

HZH= H(2|0><0|-I)H = 2H|0><0|H-HIH = 2|ψ><ψ|-I

Αρα: HZH |α> =(2|ψ><ψ|-I) | α > == (2|ψ><ψ|-I)$\sum_n a_n |n\rangle = (\sum_n 2\bar{a} - a_n)|n\rangle$

Grover Iterate

$$HZH = 2|\psi\rangle\langle\psi| - I$$

$$(|\psi\rangle\langle\psi|)|\alpha\rangle = \frac{1}{N}\begin{bmatrix} 1 & 1 & 1 & & 1 \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & 1 & 1 & & 1 \\ & \vdots & & \ddots & \\ 1 & 1 & 1 & & 1 \end{bmatrix}\begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_N \end{bmatrix} = \begin{bmatrix} \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \\ \frac{\sum \alpha_n}{N} \\ \vdots \\ \frac{\sum \alpha_n}{N} \end{bmatrix}$$

Γραμμικός τελεστής $|\psi\rangle\langle\psi|$

Ο γραμμικός τελεστής $|\psi\rangle\langle\psi|$ απεικονίζει το διάνυσμα φ στην προβολή του φ πάνω στο διάνυσμα ψ, γι'αυτό και λέγεται τελεστής προβολής. Δηλαδή:

$$|\psi\rangle\langle\psi||\phi\rangle \to |\psi\rangle\langle\psi|\phi\rangle = \langle\psi|\phi\rangle|\psi\rangle$$

Επίσης αν έχουμε τον τελεστή $|\theta\rangle\langle\psi|$ τότε ισχύει:

$$|\theta\rangle\langle\psi||\phi\rangle \to |\theta\rangle\langle\psi|\phi\rangle = \langle\psi|\phi\rangle|\theta\rangle$$

Δηλαδή απεικονίζει το διάνυσμα φ στην προβολή του φ πάνω στο διάνυσμα θ.

Παράδειγμα 1:

$$\begin{aligned} &(|0\rangle\langle 1| + |1\rangle\langle 0|)(|0\rangle) \\ &= |0\rangle\langle 1\|0\rangle + |1\rangle\langle 0\|0\rangle \\ &= |0\rangle\langle 1|0\rangle + |1\rangle\langle 0|0\rangle \\ &= 0|0\rangle + 1|1\rangle \\ &= |1\rangle \end{aligned}$$

Όπου ο τελεστής $|0><1|+|1><0|$ αν/χεί στην πύλη NOT που όπως έχουμε πεί είναι τελεστής Pauli X:

$$X = \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Αρα αν $|u\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ και $|d\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ τότε: $\langle d| = \begin{pmatrix} 0 & 1 \end{pmatrix}$

και:

$$|u\rangle\langle d| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Παράδειγμα 2:

1.Στον αλγόριθμό μας ξεκινάμε από την κατάσταση $|0>$
2.Δρούμε με τον τελεστή H.

$$H|0>=|\psi>$$

Όπου:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ . \\ . \\ . \\ 1 \\ 1 \end{pmatrix}$$

και

$$\langle\psi| = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & . & . & . & 1 & 1 \end{pmatrix}$$

Ετσι:

$$|\psi\rangle\langle\psi| = \frac{1}{\mathrm{N}} \begin{pmatrix} 1 & 1 & 1 & . & . & . & 1 & 1 \\ 1 & 1 & . & . & . & . & . & 1 \\ 1 & 1 & 1 & . & . & . & . & 1 \\ . & . & . & 1 & . & . & . & 1 \\ . & . & . & . & 1 & . & . & 1 \\ . & . & . & . & 1 & 1 & . & 1 \\ . & . & . & . & . & 1 & 1 & 1 \\ 1 & . & . & . & . & . & . & 1 \end{pmatrix}$$

Πόσες φορές θα επαναλάβουμε την περιστροφή R_sR_a; (ή το μετασχηματισμό G)

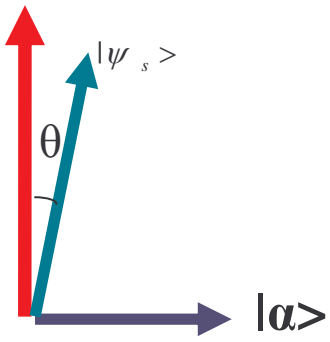
Θεωρείστε το αρχικό μας διάνυσμα $|\psi_s>$ το οποίο αρχικά βρίσκεται στο επίπεδο

των διανυσμάτων $|\alpha>$ και $|\alpha^{\perp}>$ με τη γωνία των $|\psi_s>$ και $|\alpha^{\perp}>$ ίση με θ. Αυτό σημαίνει ότι μπορούμε να γράψουμε το $|\psi_s>$ ως γραμμικό συνδυασμό των $|\alpha>$ και $|\alpha^{\perp}>$ έτσι ώστε:

$$|\psi_s>=\cos\theta\left|\alpha^{\perp}\right\rangle+\sin\theta\left|\alpha\right\rangle$$

Μετά από κ επαναλήψεις των $R_sR_a=(-H\,U_{f0}H)(U_{f\alpha})$ η κατάστασή μας γίνεται

$$(R_sR_a)^k|\psi_s>=\cos(2k+1)\theta\left|\alpha^{\perp}\right\rangle+\sin(2k+1)\theta\left|\alpha\right\rangle$$



Παρατηρείστε ότι εάν $\cos(2k+1)\theta=0$, $\sin(2k+1)\theta=1$ τότε:

$$(R_sR_a)^k|\psi_s>=\left|\alpha\right\rangle$$

Αρα η λύση θα είναι ο πιο κοντινός ακέραιος k για τον οποίο η γωνία $(2k+1)\theta=\pi/2$.

Δηλαδή:

$$k=[\frac{\pi}{4\theta}-\frac{1}{2}]_{near\,int\,eger}$$

Επειδή

$\sin\theta=<\alpha|\psi_S>=\frac{1}{\sqrt{2^n}}=\frac{1}{\sqrt{N}}$

Και για N μεγάλο: $\sin\theta\approx\theta$

Έχουμε:

$$k = [\frac{\pi}{4\theta} - \frac{1}{2}]_{near\,integer} = [\frac{\pi}{4}\sqrt{\mathrm{N}} - \frac{1}{2}]_{near\,integer}$$

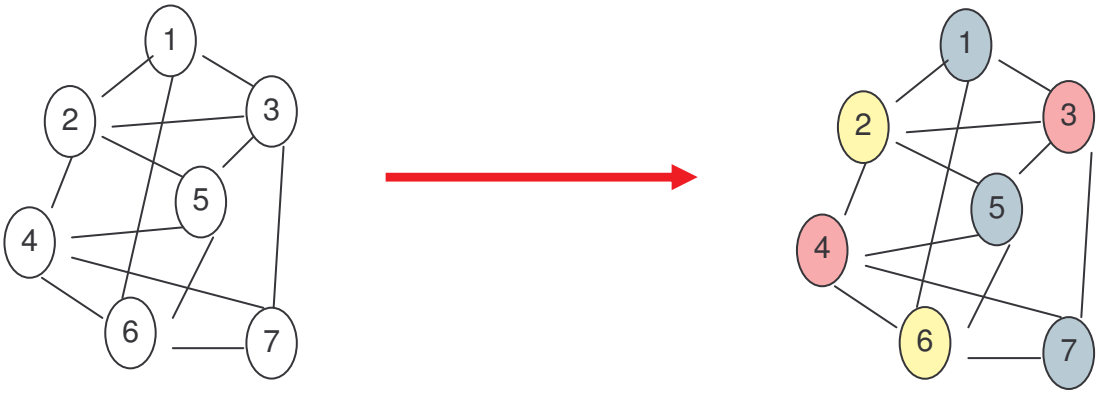
Τελικά χρειαζόμαστε $O(\sqrt{N})$ βήματα.

Τι άλλες εφαρμογές έχει ο αλγόριθμος του Grover;

Μπορεί να χρησιμοποιηθεί για τη λύση NP-complete προβλημάτων, όπως για παράδειγμα το πρόβλημα χρωματισμού ενός γράφου ή το πρόβλημα του του πλανόδιου πωλητή που θα αναφέρουμε παρακάτω.

Παράδειγμα 1:

Το πρόβλημα χρωματισμού ενός γράφου ***(The Graph Coloring Problem)***



Βάψε κάθε κόμβο με ένα χρώμα έτσι ώστε κάθε ζευγάρι κόμβων που ενώνεται με μία ακμή να έχει διαφορετικό χρώμα.
Ποιος ο μικρότερος αριθμός χρωμάτων;

Στο παράδειγμά μας η απάντηση είναι 3.
Γενικά είναι NP-complete πρόβλημα.

Μπορούμε να κατασκευάσουμε ένα μαντείο στο οποίο σαν είσοδο θα έχουμε όλες τις δυνατές περιπτώσεις χρωματισμού των κόμβων χρησιμοποιώντας ένα συγκεκριμένο αριθμό κ χρωμάτων και το οποίο θα αναζητάει αν υπάρχει κάποιο «good colorimg».

Παράδειγμα 2:

Το πρόβλημα του πλανόδιου πωλητή (TSP problem)

Δεδομένου ενός γράφου ο οποίος απεικονίζει χωριά-κόμβους τα οποία ενώνονται με συγκεκριμένες αποστάσεις-ακμές υπάρχει δρόμος που μπορεί να ακολουθήσει ένας πλανόδιος πωλητής έτσι ώστε να περάσει απ'όλα τα χωριά και να διανύσει απόσταση μικρότερη από κ;

Αν υπάρχουν N πόλεις θα χρειαστούμε κλασικά O(N!) βήματα ενώ χρησιμοποιώντας

τον κβαντικό αλγόριθμο αναζήτησης του Grover θα χρειαστούμε $O(\sqrt{N!})$

Πάλι θα είναι εκθετικός ο χρόνος αλλά θα έχουμε μια επιτάχυνση τετραγωνικής ρίζας.

Ο Αλγόριθμος Grover

1. χρησιμοποιείται για προβλήματα όπου δεν ξέρεις πολλά:

- Μη ταξινομημένες βάσεις δεδομένων
- NP-complete προβλήματα

2. $O(\sqrt{N})$ βήματα εάν ο κλασικός αλγόριθμος χρειάζεται O(N) βήματα.

Ο Αλγόριθμος του Grover είναι βέλτιστος

Στο άρθρο των Bennett, Bernstein, Brassard, Vazirani [39] αποδεικνύεται ότι ένα κβαντικό σύστημα απαιτεί τουλάχιστον $\Omega(\sqrt{\mathrm{N}})$ βήματα για την εύρεση ενός αντικειμένου (χωρίς να υπάρχει καμία γνώση για τη δομή της βάσης δεδομένων).

5.4 Αλγόριθμος του Shor
Αλγόριθμος Παραγοντοποίησης (1994)

Το πρόβλημα:

Είσοδος:	*Ενας θετικός, όχι πρώτος ακέραιος N*
Εξοδος:	*Ένας παράγοντας d του N, τ.ω:1<d<N και N=d*g για κάποιο αριθμό g*

Κλασική Λύση

Χρειάζεται $O(\exp[(\lg N)^{\frac{1}{3}}(\lg\lg N)^{\frac{2}{3}}])$ βήματα για έναν ακέραιο N.

Super-polymomial ως πρός τον αριθμό O(logN) των ψηφίων του N

Ο πιο γρήγορος αλγόριθμος παραγοντοποίησης χρειάζεται:

10^{10} χρόνια για έναν αριθμό με 400 ψηφία

Γι' αυτό και χρησιμοποιείται στην κρυπτογραφία (RSA)

Κβαντικός αλγόριθμος

Ο Shor πρότεινε έναν κβαντικό αλγόριθμο για την παραγοντοποίηση ακεραίων αριθμών ο οποίος χρειάζεται **πολυωνυμικό** χρόνο.

- *Λιγότερα από 3 χρόνια για έναν αριθμό με 400 ψηφία*

Ο αλγόριθμος αυτός δεν πραγματοποιεί κατευθείαν την παραγοντοποίηση του N αλλά αντί αυτού βρίσκει την τάξη P ενός στοιχείου m του δακτυλίου (mod n), δηλ. του Z^*_n.

Η τάξη ενός αριθμού m είναι ο ελάχιστος P τέτοιος ώστε $m^P = 1$ **(mod N).**

Το πρόβλημα τελικά ανάγεται στο:

Έστω ακέραιος m, να βρεθεί ο μικρότερος θετικός ακέραιος P τ.ω:

$$m^P \equiv 1 \bmod N$$

Γιατί;

Αν για παράδειγμα ο N είναι ο 33 και διαλέξουμε τυχαία έναν ακέραιο m μικρότερο του N (π.χ. m=5) τότε ο μικρότερος r για τον οποίο ισχύει

$$5^r = 1 \bmod 33 \qquad (1)$$

είναι για P = 10.

Επειδή ο P όμως είναι άρτιος μπορούμε να γράψουμε τη σχέση (1) ως εξής:

$$5^P - 1 = 0 \bmod 33 \Rightarrow 5^{(P/2)^2} - 1^2 = 0 \bmod 33 \Rightarrow$$
$$(5^{P/2} - 1)(5^{P/2} + 1) = 0 \bmod 33 \Rightarrow (5^{10/2} - 1)(5^{10/2} + 1) = 0 \bmod 33 \Rightarrow$$
$$3126 * 3124 = 0 \bmod 33$$

Τώρα υπάρχουν 3 περιπτώσεις:

1. Είτε ο $3126 = 5^5 + 1$ είναι πολλαπλάσιος του 33 (που δεν είναι)

[αλλιώς $(5^{r/2} + 1) = 0 \bmod 33$]

2. Είτε ο $3124 = 5^5 - 1$ είναι πολλαπλάσιος του 33

[που δεν μπορεί να είναι γιατί

$$(5^{r/2} - 1) = 0 \bmod 33 \Rightarrow 5^{r/2} = 1 \bmod 33$$

άρα θα υπήρχε μικρότερος αριθμός από τον r για τον οποίο θα ισχύει $5^{r'} = 1 \bmod 33$ που δε γίνεται]

3. Είτε ο 3126 περιέχει έναν παράγοντα του 33 και ο 3124 έναν άλλο, οπότε μία λύση θα είναι ο ΜΚΔ(3126,33) (=3) και μία άλλη ΜΚΔ(3124,33) (=11)

Τελικά αν βρούμε την περίοδο P για τον τυχαίο ακέραιο αριθμό m που διαλέξαμε και η περίοδος αυτή είναι άρτια και ισχύει ότι

$$(a^{P/2}+1) \neq 0 \bmod \mathrm{N}$$

τότε για να βρούμε έναν παράγοντα του αριθμού N αρκεί να υπολογίσουμε το

$$MK\Delta((a^{P/2}+1), \mathrm{N})$$

ή

$$MK\Delta((a^{P/2}-1), \mathrm{N})$$

Ο αλγόριθμος παραγοντοποίησης ενός ακέραιου αριθμού N

Βήμα 1:

Διάλεξε έναν τυχαίο θετικό ακέραιο 1<m<N

Χρησιμοποίησε τον αλγόριθμο του Ευκλείδη για να βρεις τον μέγιστο κοινό διαιρέτη ΜΚΔ(m,N)

Εάν ο ΜΚΔ(m,N) $\neq 1$ *τότε βρήκαμε έναν παράγοντα του N και τελειώσαμε, αλλιώς προχωράμε στο Βήμα 2.*
(χρόνος εύρεσης ΜΚΔ: $O(\lg^2 N)$)

Βήμα 2:

Χρησιμοποίησε έναν κβαντικό υπολογιστή για να υπολογίσεις την άγνωστη περίοδο P της συνάρτησης

$$\mathrm{N} \xrightarrow{f_N} \mathrm{N}$$
$$a \longrightarrow m^a \bmod N$$

Βήμα 3:

Εάν ο P είναι περιττός πήγαινε στο Βήμα1.

[Πιθανότητα να είναι περιττός είναι $(\frac{1}{2})^k$ όπου κ είναι ο αριθμός των διαφορετικών πρώτων παραγόντων του N].

Εάν ο P είναι άρτιος τότε πήγαινε στο Βήμα 4.

Βήμα 4:

Αφού η περίοδος P είναι άρτια

$$m^P - 1 = 0 \bmod N \Rightarrow m^{(P/2)^2} - 1^2 = 0 \bmod N \Rightarrow$$
$$(m^{P/2} - 1)(m^{P/2} + 1) = 0 \bmod N$$

Εάν $(m^{P/2} + 1) = 0 \bmod N$ *πήγαινε στο Βήμα 1, αλλιώς πήγαινε στο Βήμα 5.*

[Πιθανότητα να ισχύει $(m^{P/2} + 1) = 0 \bmod N$ είναι μικρότερη από $(\frac{1}{2})^{k-1}$ όπου κ είναι ο αριθμός των διαφορετικών πρώτων παραγόντων του N].

Βήμα 5:

Χρησιμοποίησε τον αλγόριθμο του Ευκλείδη για να υπολογίσεις τον μέγιστο κοινό διαιρέτη

$$d=\text{ΜΚΔ}(\ (m^{P/2} - 1)\ ,N)$$

Από τη στιγμή που $(m^{P/2} + 1) \neq 0 \bmod N$ ο d μπορεί να αποδειχθεί ότι είναι ένας (non trivial) παράγοντας του N.

Άρα και η απάντηση.

Συνοπτικά ο αλγόριθμος έχει ως εξής:

Αλγόριθμος παραγοντοποίησης N
Είσοδος: *Ενας θετικός, όχι πρώτος ακέραιος N*
Εξοδος:
*Ένας παράγοντας d του N, τ.ω:1<d<N και N=d*g για κάποιο αριθμό g*

Βήμα1α: Εάν N άρτιος τότε d=2

Βήμα1β: Εάν $N = p^k$ όπου p πρώτος τότε d=p

Βήμα1γ: Τυχαία διάλεξε έναν ακέραιο 1<m<N

Βήμα2:
Καθόρισε την τάξη P της m^{α} mod N χρησιμοποιώντας τον αν/χο κβαντικό αλγόριθμο

Βήμα3: Εάν P είναι περιττός τότε πήγαινε στο Βήμα1γ

Βήμα4:
Υπολόγισε το f=ΜΚΔ($m^{P/2}$ -1 ,N) και το g= ΜΚΔ($m^{P/2}$ -1 ,N)

Βήμα4α: Εάν 1<d= ΜΚΔ($m^{P/2}-1$,N) <N τότε εμφάνισε d

Βήμα4β: *Εάν 1<d*= ΜΚΔ($m^{P/2}+1$,N) <N τότε εμφάνισε d

Βήμα4γ: Εάν αποτύχουμε να βρούμε λύση πήγαινε στο βήμα1γ.

Βήμα 2: Το κβαντικό τμήμα του αλγορίθμου

1. Χρησιμοποιούμε δύο καταχωρητές: Ο πρώτος (αριστερός) μετά την μέτρηση θα μας δώσει έναν αριθμό ο οποίος με μεγάλη πιθανότητα θα είναι κοντά σ'ένα ακέραιο πολλαπλάσιο του αντιστρόφου της περιόδου. Ο δεύτερος χρειάζεται για να υπολογίσουμε τη συνάρτηση $m^x \bmod N$ για κάθε x του πρώτου καταχωρητή.

$$|\psi_0>=|00..0>|00..0>$$

2. Το κβαντικό τμήμα του αποτελείται από τρία βασικά στάδια. Στο πρώτο στάδιο εφαρμόζουμε έναν κατάλληλο μετασχηματισμό (Walsh-Hadamard ή παράλληλες πύλες Hadamard) έτσι ώστε ο αριστερός καταχωρητής να βρεθεί σε μια υπέρθεση όλων των βασικών καταστάσεων με τον ίδιο συντελεστή.

$$|\psi_1\rangle = F\,|00..0\rangle\otimes|00..0\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1} e^{(2\pi i x*0)/Q}\,|x\rangle\otimes|00...0\rangle$$

Παράδειγμα: για N=91 άρα $Q = 2^{14} = 16384$

$$|\psi_1\rangle = \frac{1}{\sqrt{16384}}(|0\rangle+|1\rangle+|2\rangle+...+|16383\rangle)\otimes|00...0\rangle$$

3 Το επόμενο στάδιο είναι να υπολογιστεί σ' ένα μόλις βήμα η πράξη $m^{\alpha} \bmod N$ για κάθε α που βρίσκεται σε υπέρθεση στον αριστερό καταχωρητή. Τα υπόλοιπα των διαιρέσεων αυτών βρίσκονται σε υπέρθεση με κατάλληλους συντελεστές και αποθηκεύονται στο δεξιό καταχωρητή.

$$f_m(|x\rangle\otimes|00..0\rangle)\rightarrow|x\rangle\otimes|m^x \bmod N\rangle$$

Παράδειγμα:

$$|\psi_2\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1}|x\rangle\,|m^x \bmod N\rangle =$$

$$= \frac{1}{\sqrt{Q}}(|0\rangle|1\rangle+|1\rangle|3\rangle+|2\rangle|9\rangle+|3\rangle|27\rangle+|4\rangle|81\rangle+|5\rangle|61\rangle+$$

$$+|6\rangle|1\rangle+|7\rangle|3\rangle+|8\rangle|9\rangle+|9\rangle|27\rangle+|10\rangle|81\rangle+|11\rangle|61\rangle+...$$

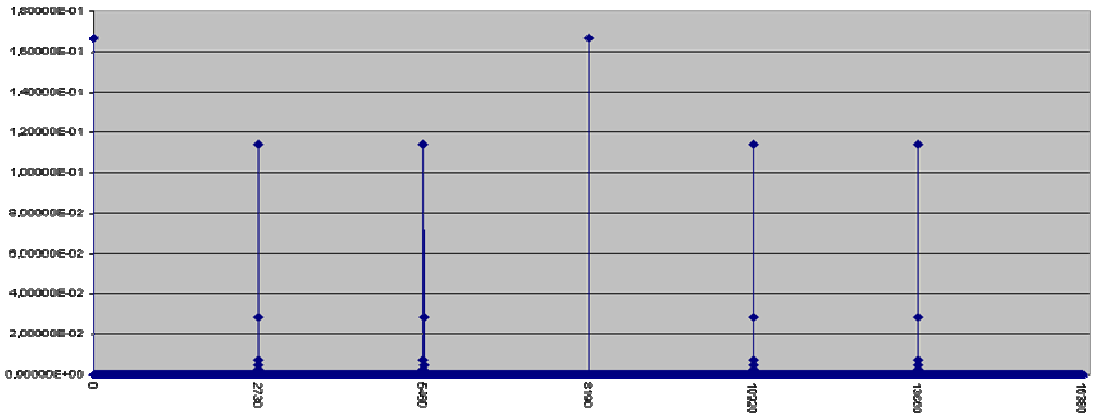
$$+|16380\rangle|1\rangle+...+|16383\rangle|27\rangle)$$

Αριστερός καταχωρητής	Δεξιός καταχωρητής
a	**m^a mod N**
0	1
1	3
2	9
3	27
4	81
5	61
6	1
7	3
8	9
9	27
10	81
11	61
12	1

3. Στο τρίτο στάδιο θα μπορούσαμε να εκτελέσουμε μια παρατήρηση στο δεξιό καταχωρητή. Αυτή η παρατήρηση θα έπρεπε να καταστρέψει την υπέρθεση των καταστάσεων στην οποία βρίσκεται και να δώσει, τυχαία, ως αποτέλεσμα μία από τις βασικές καταστάσεις στις οποίες βρίσκεται (ένα από τα υπόλοιπα της διαίρεσης). Στο παράδειγμά μας θα δώσει μία από τις τιμές 1,3,9,27,81,61.
   Επειδή όμως οι δύο καταχωρητές βρίσκονται σε κατάσταση συμπλοκής η υπέρθεση των καταστάσεων του αριστερού καταχωρητή θα καταρρεύσει σε μία από τις βασικές καταστάσεις α αυτού η οποία όμως θα πρέπει να έχει την ιδιότητα ότι η m^{α} mod N να είναι ίση με την τιμή του δεξιού καταχωρητή που μετρήσαμε.
   Δηλαδή αν μετρήσουμε στο δεξιό καταχωρητή την τιμή 1 τότε θα μετρήσουμε στον αριστερό καταχωρητή μία από τις καταστάσεις (μία από τις τιμές του α) για τις οποίες η πράξη m^{α} mod N είναι ίση με 1. Δηλαδή θα μετρήσουμε έναν από τους αριθμούς 0,6,12,18,.... οι οποίοι απέχουν όμως μεταξύ τους όσο η ζητούμενη περίοδος!!!

   Επειδή όμως από ένα από αυτά τα νούμερα δεν μπορούμε να βρούμε τη ζητούμενη απόσταση (περίοδος) χρησιμοποιούμε ένα άλλο τέχνασμα. Υποβάλουμε τον αριστερό καταχωρητή σε μετασχηματισμό Fourier (κβαντικό μετασχηματισμό Fourier). Ο μετασχηματισμός αυτός μετασχηματίζει μια περιοδική ακολουθία αριθμών στο πεδίο των συχνοτήτων, δηλαδή σε μια άλλη ακολουθία όπου εκφράζει τη συγκέντρωση της ισχύος της ακολουθίας στις διάφορες συχνότητες που εμπεριέχονται σε αυτήν. Ένα σημαντικό χαρακτηριστικό του

μετασχηματισμού αυτού είναι ότι μεγιστοποιείται σε σημεία που αντιστοιχούν σε ακέραια πολλαπλάσια του αντιστρόφου της συχνότητας. Επομένως στην υπέρθεση που έχει δημιουργηθεί στον αριστερό καταχωρητή μετά την εφαρμογή του μετασχηματισμού Fourier οι βασικές εκείνες καταστάσεις που αντιστοιχούν σε ακέραια πολλαπλάσια του αντιστρόφου της περιόδου, όπως επίσης και εκείνες που αντιστοιχούν σε τιμές κοντά σε αυτά τα πολλαπλάσια, θα εμφανίζονται με μεγαλύτερους συντελεστές σε σχέση με τις υπόλοιπες καταστάσεις.



Στο διάγραμμα που παραθέτουμε φαίνεται η γραφική παράσταση του μέτρου του μετασχηματισμού Fourier της ακολουθίας που αναπαριστάται στην υπέρθεση του αριστερού καταχωρητή όταν N=91, Q=16384, m=3 και η ζητούμενη περίοδος είναι P=6.

Πρίν, λοιπόν, κάνουμε μια μέτρηση εφαρμόζουμε τον προηγούμενο μετασχηματισμό στον αριστερό καταχωρητή έτσι ώστε όταν γίνει η μέτρηση το νούμερο που θα βρούμε θα έχει μεγάλη πιθανότητα να είναι ακέραιο πολλαπλάσιο του αντιστρόφου της περιόδου ή να είναι κοντά σε αυτό.

Παράδειγμα :

Εστω ότι θέλουμε να παραγοντοποιήσουμε τον αριθμό N=91(=7*13)

Βήμα1: Διαλέγουμε ένα αριθμό Q έτσι ώστε να περιέχει ως παράγοντες κάποιους μικρούς πρώτους (έτσι ώστε ο μετασχηματιμός Fourier που χρησιμοποιείται στον κβαντικό αλγόριθμο να υλοποιείται αποδοτικά)

$$N^2 < Q < 2N^2 \Rightarrow 91^2 < Q = 2^{14} = 16384 < 2*91^2$$

Διαλέγουμε έναν τυχαίο ακέραιο m τ.ω: 1<m<N=91

Εστω m=3

Αφού ο ΜΚΔ(m,N)=ΜΚΔ(3,91)=1
Προχωράμε στο Βήμα2

Βήμα2: Θέλουμε να βρούμε την περίοδο της συνάρτησης $f(a) = 3^a \bmod 91$

Άγνωστο σε μάς η f έχει περίοδο P=6

a	m^a	m^a mod n
0	1	1
1	3	3
2	9	9
3	27	27
4	81	81
5	243	61
6	729	1
7	2187	3
8	6561	9
9	19683	27
10	59049	81
11	177147	61
12	531441	1

Βήμα 2.0_: Χρησιμοποιούμε 2 καταχωρητές, τους οποίους και αρχικοποιούμε έτσι ώστε η κατάστασή τους να γίνει:

$$|\psi_0>=|00..0>|00..0>$$

Ο κάθε καταχωρητής αποτελείται από L qubits (=14 στο παράδειγμα μας)

$$(N^2 < Q < 2N^2 \Rightarrow 91^2 < Q = 2^L = 2^{14} = 16384 < 2*91^2)$$

Βήμα 2.1_: Χρησιμοποιούμε ένα μετασχηματισμό Walsh-Hadamard

$$W_{Q=2^L}(= H \otimes H \otimes ... \otimes H)$$

(L παράλληλες πύλες Hadamard)

Ο Walsh-Hadamard μετασχηματισμός ορίζεται αναδρομικά ως εξής :

$$W_2 = H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad W_{2^n} = \frac{1}{\sqrt{2^n}}\begin{pmatrix}W_{2^{n-1}} & W_{2^{n-1}}\\ W_{2^{n-1}} & -W_{2^{n-1}}\end{pmatrix}$$

Παράδειγμα:

$$W_4 = W_2 \otimes W_2 = \frac{1}{2}\begin{pmatrix}1W_2 & 1W_2\\ 1W_2 & -1W_2\end{pmatrix} = \frac{1}{2}\begin{pmatrix}1 & 1 & 1 & 1\\ 1 & -1 & 1 & -1\\ 1 & 1 & -1 & -1\\ 1 & -1 & -1 & 1\end{pmatrix}$$

Ο μετασχηματισμός Hadamard είναι στην ουσία ένας κβαντικός μετασχηματισμός

Fourier για την περίπτωση όπου Q $=2^1$

Ο κβαντικός μετασχηματισμός Fourier είναι:

$$|\psi\rangle = F\,|\,y\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1} e^{2\pi i x y/Q}\,|\,x\rangle$$

Όπου x*y = $x_1 y_1 + x_2 y_2 + ... + x_n y_n$

Στην περίπτωση με Q=2 (τα x,y παίρνουν τιμές 0 ή 1 το κάθε ένα) έχουμε:

$$|\psi\rangle = F\,|\,y\rangle = \frac{1}{\sqrt{2}}\sum_{x=0}^{2-1} e^{2\pi i x y/2}\,|\,x\rangle$$

Άρα μπορεί να γραφεί σε μορφή πίνακα 2x2 όπου η πρώτη γραμμή αν/χεί στο x=0 ενώ η πρώτη στήλη αν/χεί στο ψ=0. Ετσι ο μετασχηματισμός F σε μορφή πίνακα είναι:

$$F = \frac{1}{\sqrt{2}}\begin{pmatrix} e^0 & e^0 \\ e^0 & e^{\pi i} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

όπου

$$e^{\pi i} = \cos(\pi) + i\sin(\pi) = -1 + 0 = -1$$

Άρα στη γενική περίπτωση ένας κβαντικός μετασχηματισμός με Q=2^L δεν είναι τίποτα άλλο παρά ένας Walsh-Hadamard μετασχηματισμός (δηλ. L παράλληλες πύλες Hadamard)

Βήμα 2.1: Χρησιμοποιούμε έναν μετασχηματισμό W_Q στον αριστερό καταχωρητή

ή εφαρμόζουμε στον αριστερό καταχωρητή τον μετασχηματισμό Fourier.

Ετσι καταλήγουμε στην κατάσταση:

$$|\psi_1\rangle = F\,|00..0\rangle \otimes |00..0\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1} e^{(2\pi i x*0)/Q}\,|x\rangle \otimes |00...0\rangle = \frac{1}{\sqrt{Q}}\sum_{x=0}^{Q-1} |x\rangle \otimes |00...0\rangle$$

Στο παράδειγμά μας (για $Q = 2^{14} = 16384$) σημαίνει

$$|\psi_1\rangle = \frac{1}{\sqrt{16384}}(|0\rangle + |1\rangle + |2\rangle + ... + |16383\rangle) \otimes |00...0\rangle$$

Έτσι ο αριστερός καταχωρητής βρίσκεται σε κατάσταση υπέρθεσης.

Βήμα 2.2:

Εφαρμόζουμε τον ορθομοναδιαίο μετασχηματισμό

$$f_m(|x\rangle \otimes |00..0\rangle) \to |x\rangle \otimes |m^x \bmod N\rangle$$

Ετσι η κατάσταση των δύο καταχωρητών γίνεται:

$$|\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |m^x \bmod N\rangle =$$

$$= \frac{1}{\sqrt{Q}} (|0\rangle|1\rangle + |1\rangle|3\rangle + |2\rangle|9\rangle + |3\rangle|27\rangle + |4\rangle|81\rangle + |5\rangle|61\rangle +$$
$$+ |6\rangle|1\rangle + |7\rangle|3\rangle + |8\rangle|9\rangle + |9\rangle|27\rangle + |10\rangle|81\rangle + |11\rangle|61\rangle + ...$$
$$+ |16380\rangle|1\rangle + ... + |16383\rangle|27\rangle)$$

Εάν μετρήσουμε τον δεξιό καταχωρητή τότε θα καταρρεύσει η κατάστασή του σε μια από τις τιμές που μπορεί να πάρει η $m^x \bmod N$

Εστω στη $Z = m^z \bmod N$

Στο παράδειγμά μας οι δυνατές τιμές είναι: |1>,|3>,|9>,|27>,|81>, |61>

Η κατάσταση όμως των 2 καταχωρητών είναι κατάσταση συμπλοκής (entanglement).

Αυτό σημαίνει ότι ταυτόχρονα θα καταρρεύσουν και οι καταστάσεις του αριστερού καταχωρητή και έτσι θα μετρήσουμε και μία από τις πιθανές καταστάσεις του αριστερού καταχωρητή. Ποιές είναι όμως αυτές οι πιθανές καταστάσεις;

Όσες καταστάσεις |x> έχουν $m^x \bmod N \neq Z$ θα έχουν πλάτος 0.

Ενώ για όσες ισχύει $m^x \bmod N = Z$ θα «επιζήσουν». Αρα τελικά θα μετρήσουμε μία από αυτές τις καταστάσεις.

Εάν για παράδειγμα η περίοδος είναι 6 τότε τα πλάτη των καταστάσεων θα ήταν:

....,0,0,0,c,0,0,0,0,0,c,0,0,0,0,0,c,0,0,0,0,0,c,0 ,…..

Το πλάτος θα ήταν μη μηδενικό σε κάθε $6^{η}$ τιμή.

Αυτές οι καταστάσεις προηγουμένως είχαν πλάτος $\frac{1}{\sqrt{Q}}$

Αλλά αυτές που θα επιζήσουν θα έχουν πλάτος $c = \frac{1}{\sqrt{Q/6}}$

Αν μπορούσαμε να μετρήσουμε 2 καταστάσεις τέτοιες τότε θα είχε λυθεί το πρόβλημα γιατί διαφέρουν μεταξύ τους από ένα αριθμό ο οποίος είναι ακέραιο

πολλαπλάσιο του P. Αλλά δυστυχώς δεν μπορούμε να μετρήσουμε 2 τέτοιες καταστάσεις λόγω των νόμων της κβαντικής φυσικής.

Ετσι δεν μετράμε αυτή τη στιγμή το δεξιό καταχωρητή αλλά προχωράμε στο επόμενο βήμα.

Βήμα 2.3

Εφαρμόζουμε ένα κβαντικό μετασχηματισμό Fourier στον αριστερό καταχωρητή. Ετσι:

$$|\psi_3\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} \frac{1}{\sqrt{Q}} \sum_{y=0}^{Q-1} e^{2\pi i x y / Q} \, |y\rangle \otimes |m^x \bmod N\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{16384}} \sum_{x=0}^{16383} \frac{1}{\sqrt{16384}} \sum_{y=0}^{16383} e^{2\pi i x y / 16384} \, |y\rangle \otimes |3^x \bmod 91\rangle$$

$$|\psi_3\rangle = \frac{1}{\sqrt{16384}} \sum_{x=0}^{16383} \frac{1}{\sqrt{16384}} \sum_{y=0}^{16383} e^{2\pi i x y / 16384} \, |y\rangle \otimes |3^x \bmod 91\rangle$$

Βήμα 2.4

Παρατηρούμε τους 2 καταχωρητές.

Έτσι θα μετρήσουμε μια συγκεκριμένη τιμή w για το y και μια τιμή $m^z \bmod N$

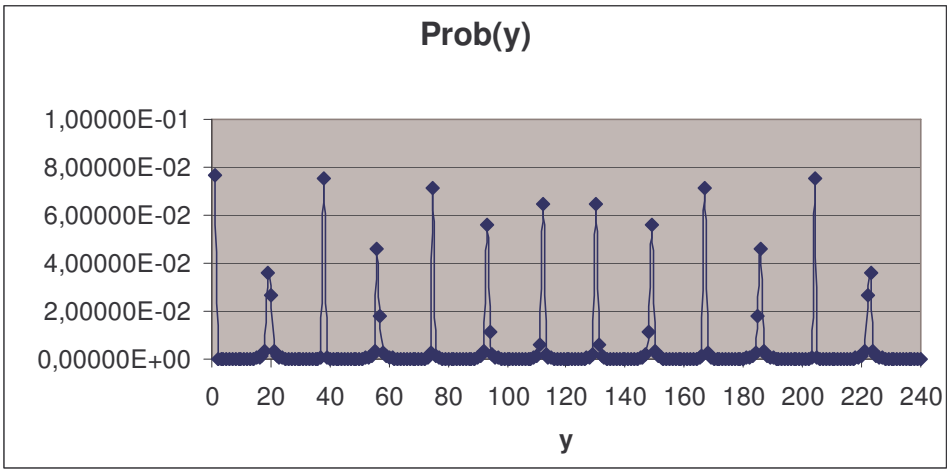
για το $m^x \bmod N$ **με πιθανότητα το τετράγωνο του πλάτους:** $\left| \frac{1}{Q} \sum_{x : m^x = m^z \bmod N} e^{2\pi i x w / Q} \right|^2$

Με μεγάλη πιθανότητα η παρατηρούμενη τιμή w είναι κοντά σε ένα ακέραιο

πολλαπλάσιο του $\frac{Q}{P}$ δηλ. $w \approx j\frac{Q}{P}$

Παράδειγμα:

Εάν Q=240 και P=13 θα μετρήσουμε κάποιο y με πιθανότητα μεγάλη κοντά σε ακέραιο πολ/σιο του Q/P



Πιθανότητα κοντά σε ακέραιο πολ/σιο του Q/P σημαίνει $\left|\frac{y}{Q}-\frac{j}{P}\right| \le \frac{1}{2Q}$

Χρησιμοποιώντας μια διαδικασία γνωστή ως continued fraction expansion μπορούμε να υπολογίσουμε τις καλύτερες προσεγγίσεις ενός αριθμού με κλάσματα σε πολυωνυμικό χρόνο.

Ετσι:

Μετράμε το y, βρίσκουμε το κλάσμα j/P και εάν το j είναι σχετικά πρώτο με το P τότε έχουμε βρεί την περίοδο.

Βήμα 2.5

Continued fraction expansion

$$\xi = \alpha_0 + \cfrac{1}{\alpha_1 + \cfrac{1}{\alpha_2 + \cfrac{1}{\alpha_3 + \cfrac{1}{\ldots + \cfrac{1}{\alpha_N}}}}}$$

με $\xi = \frac{p_n}{q_n}$ και $\gcd(p_n, q_n) = 1$

Επίσης :

$p_0 = a_0$ $\quad$ $q_0 = 1$

$q_1 = a_1$

$p_1 = a_1 a_0 + 1$ $\quad$ $q_n = a_n q_{n-1} + q_{n-2}$

$p_n = a_n p_{n-1} + p_{n-2}$

Παράδειγμα:
Έστω ότι θέλουμε όπως αναφέραμε να παραγοντοποιήσουμε το N=91, έχοντας διαλέξει ως τυχαίο αριθμό m το 3. Τότε είδαμε ότι το Q=16384. Έστω, λοιπόν, ότι μετράμε για y=13453.

$$\xi = \frac{y}{Q} = \frac{13453}{16384}$$

Ψάχνουμε να βρούμε δύο όρους p_n και q_n για τους οποίους ισχύει:

$$\xi = \frac{p_n}{q_n}$$

Δηλαδή βρίσκουμε την καλύτερη προσέγγιση με κλάσματα του αριθμού ξ.

Εχουμε λοιπόν:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
a_n	0	1	4	1	1	2	3	1	1	3	1	1	1	1	3
p_n	0	1	4	**5**	9	23	78	101	179	638	...				13453
q_n	1	1	5	**6**	11	28	123	218	777	...					16384

Δοκιμάζουμε και βλέπουμε ότι ο μικρότερος q_n για τον οποίο ισχύει

$$3^{q_n} = 1 \bmod 91$$

είναι ο 6.

Αρα η περίοδος είναι P=6.

Βήμα 3
Αφού P=6 είναι άρτιος τότε: προχωράμε στο βήμα 4

Βήμα 4

Αφού $3^{P/2} = 3^3 = 27 \neq -1 \bmod 91$

προχωράμε στο βήμα 5

Βήμα 5

Υπολογίζουμε με τον αλγόριθμο του Ευκλείδη το ΜΚΔ($(m^{P/2} - 1)$,N)=

=ΜΚΔ($(3^3 - 1)$,91) = ΜΚΔ(26,91)= **13**

Αρα βρήκαμε πράγματι έναν παράγοντα του 91.
Τέλος αλγορίθμου.

Ο αλγόριθμος του Shor είναι πιθανοτικός. Υπάρχει δηλαδή πιθανότητα να μην έχει ως έξοδο το σωστό αποτέλεσμα.

Πότε δεν θα έχουμε σωστό αποτέλεσμα;

1. Αν η περίοδος P είναι περιττός αριθμός.

2. Στην περίπτωση όπου η περίοδος είναι άρτια αλλά ισχύει ότι:

$$(m^{P/2} + 1) = 0 \bmod N$$

Οπότε d=ΜΚΔ($m^{P/2} + 1$, N) = N

3. Μπορεί η παρατηρούμενη τιμή w από τη μέτρηση του κβαντικού καταχωρητή στο βήμα 2.4 να μην είναι αρκετά κοντά σε ένα ακέραιο

πολλαπλάσιο του $\frac{Q}{P}$

4. Μπορεί η περίοδος P και το ακέραιο πολλαπλάσιο j να μην είναι σχετικά πρώτοι αριθμοί αλλά να έχουν έναν κοινό παράγοντα. Τότε αν χρησιμοποιήσουμε την

Continued fraction expansion ο παρανομαστής q θα είναι ένας παράγοντας της περιόδου P και όχι η περίοδος η ίδια.

Πόσες φορές πρέπει να επαναλάβουμε τον αλγόριθμο ώστε να έχουμε μεγάλη πιθανότητα να βρούμε το σωστό αποτέλεσμα;

Όπως αναφέραμε αν έχουμε το κλάσμα j/r και το j είναι σχετικά πρώτος με το P τότε εξάγουμε το P.
Πόσες είναι οι καταστάσεις

$$|\mathrm{w},\quad m^z \bmod N\quad >$$

οι οποίες μας δίνουν τη δυνατότητα να υπολογίσουμε την τιμή του P με αυτόν τον τρόπο;
Σύμφωνα με το Θ. Euler υπάρχουν φ(P) πιθανές τιμές του j που είναι σχετικά πρώτες με το P. Κάθε ένα από αυτά τα κλάσματα j/P είναι κοντά σ' ένα κλάσμα y/Q.

Επίσης υπάρχουν P πιθανές τιμές του

$$m^z \bmod N$$

αφού P είναι η τάξη του m.

Συνολικά υπάρχουν P* φ(P) διαφορετικές καταστάσεις

$$|\mathrm{w}\,,\ m^z \bmod N\quad >$$

Από τις οποίες μπορούμε να εξάγουμε το P.
Με δεδομένο ότι μια τέτοια κατάσταση έχει πιθανότητα εμφάνισης τουλάχιστον $1/3P^2$ μπορούμε να εξάγουμε το P με πιθανότητα εμφάνισης τουλάχιστον φ(P)/3P. Χρησιμοποιώντας το θεώρημα ότι

$$\phi(P)/P > \delta/\log\log P$$

για κάποια σταθερά δ, καταλήγουμε στο συμπέρασμα ότι επαναλαμβάνοντας τον αλγόριθμο O(loglogP) εξασφαλίζουμε μεγάλη πιθανότητα επιτυχίας.

Πολυπλοκότητα του αλγορίθμου

Είναι ίση με την πολυπλοκότητα του υπολογισμού του $m^a \bmod N$ που είναι το πιο δύσκολο σημείο του υπολογισμού και ισούται με

$$O(N^2 \log N \log\log N)$$

Κεφάλαιο 6

Κβαντική Πολυπλοκότητα

6.1 Κλασικές κλάσεις πολυπλοκότητας

Θα αναφερθούμε αρχικά στις γνωστές κλασικές κλάσεις πολυπλοκότητας και μετέπειτα στην κβαντική κλάση πολυπλοκότητας BQP όπως και στη σχέση που έχουν μεταξύ τους.

Κλάση P

Το σύνολο όλων των γλωσσών που μπορούν να υπολογιστούν σε πολυωνυμικό χρόνο από μια ντετερμινιστική Turing Μηχανή. Ένα πρόβλημα που ανήκει στην κλάση αυτή είναι « η εύρεση του συντομότερου μονοπατιού μεταξύ δύο κόμβων σ' ένα γράφο».

Κλάση NP

Το σύνολο όλων των γλωσσών που μπορούν να υπολογιστούν σε πολυωνυμικό χρόνο από μια μη ντετερμινιστική Turing Μηχανή. Ένα πρόβλημα που ανήκει στην κλάση αυτή είναι το πρόβλημα της παραγοντοποίησης ενός αριθμού ή το πρόβλημα SAT.
Αφού μια Turing Μηχανή είναι μια συγκεκριμένη περίπτωση μη ντετερμινιστικής μηχανής τότε $P \subseteq NP$.

Οι NP-complete γλώσσες

Τα δυσκολότερα προβλήματα στο NP είναι γνωστά ως NP-complete γλώσσες. Οι γλώσσες αυτές έχουν μια χαρακτηριστική ιδιότητα: μία λύση σ' ένα NP-complete πρόβλημα μπορεί να χρησιμοποιηθεί για να λυθεί ένα οποιοδήποτε πρόβλημα στο NP, μόνο με πολυωνυμικό χρόνο καθυστέρηση. Το κλασικό παράδειγμα μιας NP-complete γλώσσας είναι το SAT.

Είναι το P=NP;

Είναι το πιο διάσημο ανοικτό πρόβλημα στην επιστήμη της θεωρητικής πληροφορικής. Αν και φαίνεται «φανερό» δεν έχει αποδειχθεί ακόμη.

Η κλάση BPP

Είναι το σύνολο των γλωσσών που είναι αποδεκτές με πιθανότητα 2/3 από μια πιθανοτική μηχανή Turing σε πολυωνυμικό χρόνο.

Είναι φανερό ότι $P \subseteq BPP$. Είναι ανοικτό πρόβλημα εάν $P \subset BPP$ ή αν $P = BPP$. Επίσης είναι ανοικτό πρόβλημα εάν $BPP \subseteq NP$ ή $NP \subseteq BPP$.

Η κλάση PSPACE

Είναι το σύνολο των γλωσσών που είναι αποδεκτές από μια πιθανοτική μηχανή Turing που χρησιμοποιεί πολυωνυμικό «χώρο» (θέσεις της ταινίας) και απεριόριστο χρόνο. Είναι φανερό ότι η $BPP \subseteq PSPACE$ αφού μια μηχανή πολυωνυμικού χρόνου μπορεί να χρησιμοποιεί πολυωνυμικό χώρο της ταινίας. Είναι ανοικτό πρόβλημα εάν $BPP \subset PSPACE$, ενώ έχει αποδειχθεί ότι $NP \subseteq PSPACE$.

6.2 Κβαντικά υπολογιστικά μοντέλα

Κβαντικά κυκλώματα

Το κβαντικό ανάλογο σ' ένα κλασικό λογικό κύκλωμα το οποίο χρησιμοποιεί n bits είναι ένα κβαντικό κύκλωμα που χρησιμοποιεί n qubits. Ενα κβαντικό κύκλωμα αποτελείται από κβαντικές πύλες οι οποίες αντιστοιχούν σε ορθομοναδιαίους πίνακες (unitary). Το αποτέλεσμα της εφαρμογής μιας πύλης σε μια κβαντική κατάσταση είναι το γινόμενο του αντίστοιχου ορθομοναδιαίου (unitary) πίνακα σ' ένα διάνυσμα που αντιστοιχεί στην κατάσταση του κβαντικού συστήματος.
Μια διαφορά μεταξύ κλασικών και κβαντικών κυκλωμάτων είναι ότι τα κβαντικά κυκλώματα πρέπει να είναι αντιστρέψιμα. Αυτό οφείλεται στο ότι μόνο ορθομοναδιαίοι (unitary) μετασχηματισμοί μπορούν να χρησιμοποιηθούν.
Ο Bennet έδειξε ότι κάθε κλασικό κύκλωμα μπορεί να μετατραπεί σ' ένα ισοδύναμο αντιστρέψιμο κύκλωμα και ότι αυτό μπορεί να γίνει αποδοτικά[36].
Είναι φανερό ότι ένας κβαντικός υπολογιστής είναι τουλάχιστον τόσο ισχυρός όσο ένας κλασικός υπολογιστής.

Κβαντική Μηχανή Turing

Ορισμός :

> Εστω C το σύνολο που αποτελείται από τα $a \in C$ τέτοια ώστε υπάρχει ντετερμινιστικός αλγόριθμος που υπολογίζει το πραγματικό και φανταστικό μέρος του α με όριο σφάλματος 2^{-n} σε χρόνο πολυωνυμικό ως πρός το n. Μια κβαντική μηχανή Turing M ορίζεται ως η τριπλέτα (Σ,Q,δ), όπου Σ είναι το πεπερασμένο αλφάβητο με ένα σύμβολο # για το κενό, Q είναι το πεπερασμένο σύνολο καταστάσεων με αρχική κατάσταση q_o και τελική q_f, και δ η κβαντική συνάρτηση μετάβασης

$$\delta: Qx\Sigma - - > C^{\Sigma xQx\{L,R\}}$$

Η κβαντική μηχανή Turing έχει μια απεριόριστη ταινία διπλής κατεύθυνσης που δεικτοδοτείται με το Z και μία μοναδική κεφαλή ανάγνωσης/εγγραφής που κινείται πάνω στην ταινία. Για τον ορισμό των διαμορφώσεων, αρχικών διαμορφώσεων και τελικών διαμορφώσεων ισχύουν τα ίδια με τη γνωστή ντετερμινιστική μηχανή Turing.

Εστω S ο χώρος με εσωτερικό γινόμενο των πεπερασμένων μιγαδικών γραμμικών συνδυασμών των διαμορφώσεων της M με την ευκλείδια νόρμα.

Καλούμε κάθε στοιχείο $\phi \in S$ μια υπέρθεση καταστάσεων του M. Η κβαντική μηχανή M ορίζει ένα γραμμικό τελεστή $U_M : S \to S$, που ονομάζεται τελεστής χρονικής εξέλιξης ως εξής: Αν η M ξεκινά στη διαμόρφωση c με τρέχουσα κατάσταση p και διαβάζει ένα σύμβολο σ, τότε μετά από ένα βήμα θα βρίσκεται στην υπέρθεση των διαμορφώσεων $\psi=\Sigma_i a_i c_i$, όπου κάθε μη μηδενικό α_i αντιστοιχεί σε μια μετάβαση δ(p,σ,τ,q,d) και c_i είναι η καινούργια διαμόρφωση που προκύπτει μετά την εφαρμογή της μετάβασης στη c. Επεκτείνοντας αυτή την απεικόνιση σε ολόκληρο το χώρο S μέσω γραμμικότητας παίρνουμε το γραμμικό τελεστή U_M.

Ορισμός 2:

Λέμε ότι μια κβαντική μηχανή Turing είναι καλά-ορισμένη όταν ο τελεστής χρονικής εξέλιξης U_M διατηρεί την ευκλείδεια απόσταση.

Η ιδιότητα του καλά ορισμένου είναι απαραίτητη προϋπόθεση ώστε η κβαντική μηχανή να είναι συνεπής με την κβαντική φυσική.

Θεώρημα1:

Μια κβαντική μηχανή Turing είναι καλά ορισμένη αν και μόνο αν ο τελεστής χρονικής εξέλιξής της είναι ορθομοναδιαίος.

Θεώρημα2:

Κάθε αντιστρέψιμη μηχανή Turing είναι επίσης μία καλά ορισμένη μηχανή Turing.

Είδαμε στην προηγούμενη παράγραφο ότι ένας κβαντικός υπολογιστής είναι τουλάχιστον τόσο ισχυρός όσο ένας κλασικός. Τίθεται το ερώτημα του αν μπορεί ένας κβαντικός υπολογιστής να προσομοιωθεί αποδοτικά από έναν κλασικό υπολογιστή. Αυτό είναι επίσης ένα ανοικτό πρόβλημα. Οι Bernstein

και Vazirani απέδειξαν ότι μπορεί να προσομοιωθεί μια κβαντική μηχανή από μια κλασική μηχανή αλλά σε εκθετικό χρόνο και πολυωνυμικό χώρο [37].

6.3 Κλάση Πολυπλοκότητας BQP

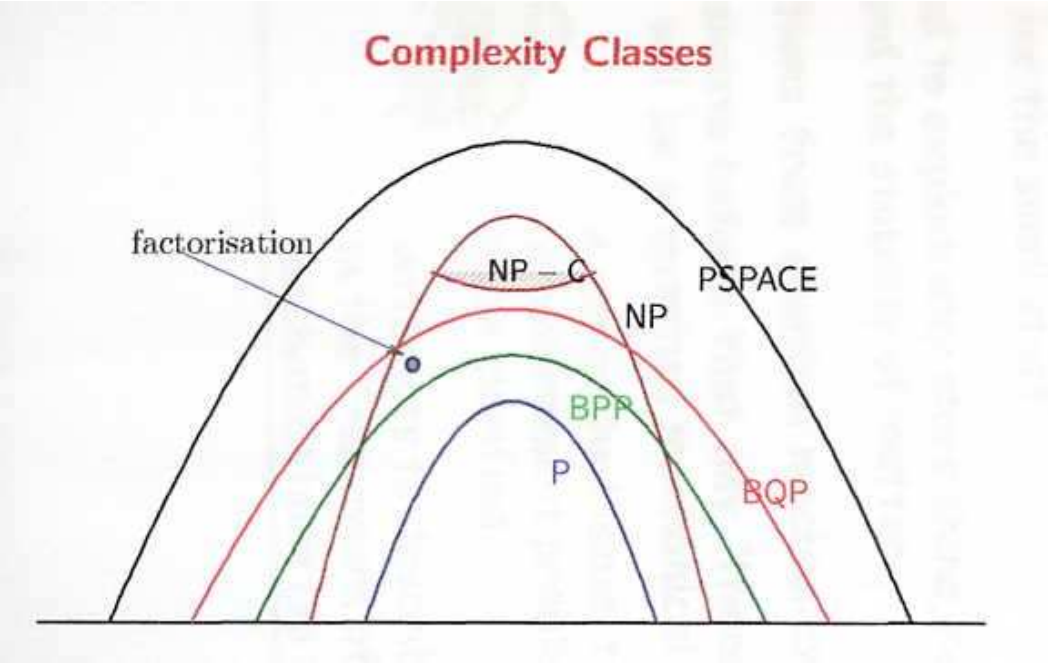
Η κλάση BQP είναι η κλάση όλων των γλωσσών που υπολογίζονται αποδοτικά σε έναν κβαντικό υπολογιστή. Πιο συγκεκριμένα είναι το σύνολο των γλωσσών που είναι αποδεκτές με πιθανότητα 2/3 από μια κβαντική μηχανή Turing σε πολυωνυμικό χρόνο. Οι Bernstein, Vazirani έδειξαν ότι για την κλάση BQP ισχύει ότι :

$$BPP \subseteq BQP$$

αφού οτιδήποτε μπορεί να υπολογιστεί σε μια κλασική μηχανή μπορεί να υπολογιστεί και σε μια κβαντική μηχανή.
Δεν είναι γνωστό όμως αν ισχύει:

$$BPP \subset BQP$$

Επίσης ο Shor έδειξε ότι το πρόβλημα της παραγοντοποίησης είναι στο BQP. Δεν είναι γνωστό όμως αν ανήκει στο BPP. Είναι άγνωστο αν το NP περικλείει το BQP ή όχι. Είναι γνωστό, όμως, ότι η κλάση BQP βρίσκεται ανάμεσα στις κλάσεις BPP και PSPACE (Αφού $BQP \subseteq PSPACE$). Ετσι η BQP περιέχει όλα τα προβλήματα που ανήκουν στην P και στην BPP και κάποια προβλήματα που ανήκουν στην NP (παραγοντοποίηση), πιθανώς κανένα που να ανήκει στην NP-complete και ίσως κάποια προβλήματα που να ανήκουν στην PSPACE και που δεν ανήκουν στην κλάση NP [38].



Κεφάλαιο 7

Θεωρία Παιγνίων

7.1 Εισαγωγή

Ο όρος «παιχνίδι» εισήχθηκε για πρώτη φορά το 1921 από το Γάλλο μαθηματικό Emil Borel.

Το μαθηματικό θεμέλιο της *θεωρίας παιγνίων* του von Neumann είναι το "θεώρημα minimax", το οποίο διατύπωσε το 1928. Η σύνθεση του και οι εφαρμογές του περιγράφονται στο βιβλίο που έγραψε το 1944 μαζί με τον Morganstern: Θεωρία Παιγνίων και Οικονομική Συμπεριφορά.

Χάρις το βιβλίο αυτό διαδόθηκε ταχύτατα σε όλο τον κόσμο η μαθηματική θεωρία των παιγνίων και οι εφαρμογές της στην οικονομία, στην πολιτική, στη στρατιωτική επιστήμη, στην επιχειρησιακή έρευνα, στις επιχειρήσεις, στη νομοθεσία, στα αθλήματα, στη βιολογία, καθώς και σε διάφορα άλλα επιστημονικά πεδία. Σημαντική υπήρξε επίσης η επίδραση της στη στρατιωτική σκέψη.

Το θεώρημα minimax αναφέρει ότι για μία μεγάλη κλάση παιγνίων δύο ατόμων δεν υπάρχει λόγος να γίνεται το παίγνιο. Ο καθένας από τους δύο παίκτες μπορεί να θεωρήσει, για κάθε δυνατή στρατηγική του παιχνιδιού, την μεγίστη ζημιά που μπορεί να υποστεί ακολουθώντας αυτή την στρατηγική και ακολούθως να εκλέξει ως βέλτιστη στρατηγική εκείνη που του ελαχιστοποιεί την μέγιστη ζημία.

Εάν ένας παίκτης ακολουθήσει την διαδικασία αυτή, μπορεί να είναι στατιστικά βέβαιος ότι δεν θα χάσει περισσότερα από αυτή την τιμή που λέγεται τιμή minimax.

Η θεωρία των παιγνίων τώρα είναι ένας κλάδος των μαθηματικών, ο οποίος χρησιμοποιείται για την ανάλυση ανταγωνιστικών καταστάσεων που η έκβαση τους εξαρτάται όχι μόνο από τις επιλογές ενός ατόμου —ή και από την τύχη— αλλά και από τις επιλογές των άλλων ατόμων, ή παικτών.

Εφόσον η έκβαση ενός παιχνιδιού εξαρτάται από τις ενέργειες και τις αποφάσεις όλων των παικτών, καθένας από αυτούς προσπαθεί να προβλέψει τις επιλογές των υπολοίπων, με σκοπό να καθορίσει την δική του βέλτιστη επιλογή.

Το κυρίως αντικείμενο της θεωρίας παιγνίων είναι το πώς θα γίνουν αυτοί οι αλληλεξαρτώμενοι στρατηγικοί υπολογισμοί.

Η θεωρία παιγνίων υποδιαιρείται σε πολλούς μεγάλους τομείς. Οι σημαντικότεροι είναι:

• Δύο πρόσωπα εναντίον π προσώπων. Η θεωρία των δύο προσώπων ασχολείται με την βέλτιστη στρατηγική επιλογή δύο ατόμων, ενώ η θεωρία των π προσώπων (π>2) ενδιαφέρεται για τις συμμαχίες (ή συνασπισμούς) που θα μπορούσαν να κάνουν κάποιοι από αυτούς έτσι, ώστε τα μέλη της συμμαχίας να αποκομίσουν τα μέγιστα δυνατά κέρδη.

• Μηδενικό άθροισμα εναντίον μη μηδενικού αθροίσματος. Τα κέρδη κάθε παίκτη προστίθενται στο μηδέν (ή σε κάποιον άλλο σταθερό αριθμό) για κάθε έκβαση (γύρο) του παιχνιδιού. Αυτό συμβαίνει στα παιχνίδια μηδενικού αθροίσματος. Στα παιχνίδια μη μηδενικού αθροίσματος τα ποσά αθροίζονται σε κάθε έκβαση και, κατά συνέπεια, η αφετηρία δεν είναι κοινή για όλους τους παίκτες. Στα παιχνίδια μηδενικού αθροίσματος ό,τι ποσό κερδίζεται συνολικά τόσο ποσό χάνεται. Κατά συνέπεια το αλγεβρικό άθροισμα των ποσών είναι μηδέν. Αντίθετα, στα παιχνίδια μη μηδενικού αθροίσματος είναι δυνατόν σε κάποιο γύρο να χάσουν ή να κερδίσουν όλοι οι παίκτες (από το απόθεμα του παιχνιδιού).

• Συνεργασία εναντίον μη συνεργασίας. Ως παιχνίδια συνεργασίας χαρακτηρίζονται εκείνα, στα οποία οι παίκτες συνάπτουν συμβάσεις και θεσπίζουν κανονισμούς. Αντίθετα, στα παιχνίδια μη συνεργασίας, μπορεί να επιτρέπεται ή όχι η επικοινωνία μεταξύ των παικτών. Πάντως και στα παιχνίδια μη συνεργασίας αν αποφασιστεί κάποια συμφωνία, αυτή δεν πρέπει να παραβιαστεί με το αιτιολογικό ότι πρόκειται για παιχνίδι μη συνεργασίας. Κοινό γνώρισμα όλων των κλάδων της θεωρίας παιγνίων είναι η υπόθεση ότι οι παίκτες, μεταξύ πολλών κακών εκβάσεων, θα επιλέξουν την λιγότερο κακή.

Η κβαντική θεωρία παιγνίων είναι ένα κεφάλαιο των κβαντικών υπολογισμών και κρυσταλλώθηκε όταν ο φυσικός David Mayer έδωσε μια ομιλία στη Microsoft Corporation [19] όπου αναφέρθηκε στη σχέση μεταξύ κβαντικών παιχνιδιών και κβαντικών αλγορίθμων όπως και σε συγκεκριμένα παιχνίδια όπου ο κβαντικός παίκτης μπορεί να τα «πάει» καλύτερα απ' ότι «κλασικά».

Στη συνέχεια παρουσιάζουμε πέντε κβαντικά παιχνίδια με στόχο να κάνουμε μια εισαγωγή στη κβαντική θεωρία παιγνίων αλλά και να κατανοήσουμε πως συσχετίζονται οι κβαντικοί αλγόριθμοι με τα κβαντικά παιχνίδια.

7.2 Το «spin flip game»

Τα ηλεκτρόνια έχουν 2 καταστάσεις: με spin πάνω και με spin κάτω. Έστω ένα παιχνίδι μεταξύ 2 παικτών της Αλίκης και του Bob. Η Αλίκη πρώτα προετοιμάζει το ηλεκτρόνιο σε κατάσταση με spin «πάνω», ο Bob απαντάει χρησιμοποιώντας το μετασχηματισμό σ_x ή το μοναδιαίο μετασχηματισμό 1 και έτσι θα έχουμε:

$$\sigma_x u=d \quad \text{ή} \quad 1u=u$$

Μετά η Αλίκη (χωρίς να ξέρει την ενέργεια του Bob) έχει σειρά να παίξει χρησιμοποιώντας έναν από τους δύο μετασχηματισμούς. Μετά έρχεται η σειρά του Bob και τελικά γίνεται η μέτρηση. Εάν το ηλεκτρόνιο βρίσκεται στην κατάσταση u τότε ο Bob κερδίζει ένα Ευρώ αλλιώς κερδίζει η Αλίκη.

Η σειρά των πιθανών περιπτώσεων φαίνεται στον παρακάτω πίνακα.

Αλίκη/Bob	1,1	$1,\sigma_x$	σ_x,1	σ_x,σ_x
1	1,1,1	$1,1,\sigma_x$	σ_x,1,1	σ_x ,1,σ_x
σ_x	$1,\sigma_x$,1	$1,\sigma_x$, σ_x	σ_x,σ_x,1	$\sigma_x,\sigma_x,\sigma_x$

Για παράδειγμα 1, $1,\sigma_x$ σημαίνει ότι ο Bob έπαιξε σ_x , ακολούθησε η Αλίκη με το μετασχηματισμό 1 και τελικά ο Bob με τον μετασχηματισμό 1. Οπότε:

$$1,1,\ \sigma_x\, u=d$$

Η Αλίκη κερδίζει.

Η αντίστοιχη κατάσταση του spin σε κάθε κίνηση φαίνεται από τον παρακάτω πίνακα:

Αλίκη/Bob	1,1	$1,\sigma_x$	σ_x,1	σ_x,σ_x
1	u,u,u	d,d,d	d,u,u	u,d,d
σ_x	d,d,u	u,u,d	u,d,u	d,u,d

Ο τελευταίος πίνακας μας δίνει το payoff της Αλίκης, θετικό αν το spin είναι στην κατάσταση d, αρνητικό αν είναι στην κατάσταση u.

Αλίκη/Bob	1,1	$1,\sigma_x$	σ_x,1	σ_x,σ_x
1	-1	+1	+1	-1
σ_x	+1	-1	-1	+1

Αυτό είναι το Spin Flip Game όπου θα επεκταθούμε σε δύο κατευθύνσεις: αρχικά θα θεωρήσουμε κινήσεις με κάποια πιθανότητα να γίνουν και στη συνέχεια θεωρώντας κβαντική υπέρθεση καταστάσεων.
Ένα παιχνίδι μπορεί να οριστεί ως ένα σύνολο

Γ=Γ(παίκτες , κινήσεις ή ενέργειες , αποτελέσματα, payoffs).

Στο προηγούμενο παιχνίδι οι παίκτες ήταν η Αλίκη και ο Bob, οι κινήσεις ήταν οι μετασχηματισμοί $\boldsymbol{\sigma_x}$ **, 1** , τα αποτελέσματα ήταν οι καταστάσεις του spin του ηλεκτρονίου u ή d και τα payoffs τα +1, -1 σύμφωνα με το αν η τελική κατάσταση ήταν η d ή η u αντίστοιχα. Το προηγούμενο παιχνίδι ήταν ένα παιχνίδι 2 παικτών, zero-sum οπότε τα payoffs του Bob ήταν ακριβώς αντίθετα από της Αλίκης.

Στρατηγική (Strategy) είναι ένας κανόνας όπου καθορίζει μια κίνηση σε κάθε στάδιο του παιχνιδιού.

Κίνηση στο παράδειγμά μας είναι ένα στοιχείο του συνόλου $\{\mathbf{1}, \boldsymbol{\sigma_x}\}$.

Στρατηγική (Strategy) θα μπορούσε να οριστεί ως μια συνάρτηση f που αντιστοιχεί την κατάσταση του παιχνιδιού σ' ένα σύνολο κινήσεων. Επειδή όμως η κατάσταση του παιχνιδιού μπορεί να μην είναι γνωστή στον παίκτη που πρόκειται να παίξει θα μπορούσαμε να πούμε ότι η στρατηγική της Αλίκης είναι η συνάρτηση

f:{πληροφορίες της Αλίκης}→ {κινήσεις της Αλίκης}

Αντίστοιχα θα μπορούσαμε να πούμε για τον Bob. Στο παράδειγμά μας (μετά την αρχική κατάσταση) η Αλίκη είχε μόνο μία δυνατότητα να διαλέξει κίνηση άρα είχε μόνο μία στρατηγική στο δεύτερο βήμα, ενώ ο Bob είχε δύο στρατηγικές. Μία για την πρώτη κίνηση και μία για την τρίτη.

Στην οικονομία οι στρατηγικές εξαρτώνται σε μεγάλο βαθμό από τις πληροφορίες του κάθε παίκτη πριν παίξει. Εάν για παράδειγμα ο Bob μπορούσε να κάνει κβαντικές κινήσεις και η Αλίκη δεν μπορούσε τότε ο Bob θα είχε ένα πλεονέκτημα.

Λύνοντας ένα παιχνίδι σημαίνει να καθορίσουμε τις βέλτιστες στρατηγικές για τους παίκτες.

Το κεφάλαιο του τι πληροφορία έχει ο καθένας είναι πολύ σημαντικό. Στο παράδειγμά μας έχουμε θεωρήσει ότι ο κάθε ένας δεν ξέρει τι κίνηση έχει κάνει ο άλλος. Σε οποιαδήποτε άλλη περίπτωση δεν θα ήταν παιχνίδι.

Ας θεωρήσουμε τώρα ότι τις στρατηγικές f_a και f_b για την Αλίκη και τον Bob αντίστοιχα όπου:

f_a = να παίξει 1 με πιθανότητα p=1/2 και σ_x με πιθανότητα q=1/2

f_b = να παίξει 1 με πιθανότητα p=1/2 και σ_x με πιθανότητα q=1/2

Αυτές οι στρατηγικές καλούνται <u>mixed</u> καταστάσεις αφού περιέχουν κάποια πιθανότητα για να γίνει κάποια κίνηση.

Αν παρατηρήσουμε τον τελευταίο πίνακα τότε καταλαβαίνουμε ότι το αναμενόμενο payoff της Αλίκης είναι:

$$\bar{\pi}_A = \frac{1}{2}(+1) + \frac{1}{2}(-1) = 0$$

Αντίστοιχα για το Bob:

$$\bar{\pi}_B = \frac{1}{4}(+1) + \frac{1}{4}(-1) + \frac{1}{4}(-1) + \frac{1}{4}(+1) = 0$$

Γενικότερα μπορούμε να πούμε ότι αν θεωρήσουμε ότι έγιναν μια σειρά από N παιχνίδια

$$\Gamma_N\, \Gamma_{N-1}\, \Gamma_{N-2} \ldots \Gamma_3\, \Gamma_2\, \Gamma_1$$

Το payoff της Αλίκης (έστω x οι νίκες της Αλίκης) θα είναι ένα στοιχείο του συνόλου:

$$\Pi = \{f(x;N)\} = \{2x\text{-}N, \text{ για } x=0,1,\ldots,N\}$$

με πιθανότητα

$$P(\Pi) = \{f(x;N,p)\} = \{\{\binom{N}{x} p^x q^{N-x}, \gamma\iota\alpha \quad x = 0,1,\ldots,N\}$$

Για παράδειγμα για N=3 τα πιθανά payoffs είναι {-3,-1,+1,+3} και εάν η πιθανότητα είναι ½ τότε οι αντίστοιχες πιθανότητες είναι {(1/8), (3/8), (3/8),(1/8)}. Η Αλίκη έχει αναμενόμενο payoff $\bar{\pi}_A = 0$, αλλά εάν ο N είναι περιττός τότε το πραγματικό payoff της δεν θα είναι ποτέ 0.

Εάν θεωρήσουμε ότι οι κινήσεις της Αλίκης μπορούν να αναπαρασταθούν από τη mixed στρατηγική όπου θα έχουμε πιθανότητες για κάθε μία κίνηση

$$P_A = \{a_1, a_2, \ldots, a_m\}$$

και αντίστοιχα οι πιθανότητες για τις κινήσεις του Bob είναι οι

$$P_B = \{b_1, b_2, \ldots, b_n\}$$

τότε το payoff της Αλίκης μπορεί να αναπαρασταθεί από έναν πίνακα m x n . Τότε το αναμενόμενο payoff της Αλίκης θα είναι:

$$\bar{\pi} = \sum_{j=1}^{n} \sum_{i=1}^{m} \pi_{ij} a_i b_j$$

Το minmax θεώρημα αναφέρει ότι για κάθε παιχνίδι 2 παικτών το οποίο είναι zero – sum ισχύει:

$$\max_{P_A}(\min_{P_B} \bar{\pi}_A) = \min_{P_B}(\max_{P_A} \bar{\pi}_A)$$

Μια παραλλαγή του προηγούμενου παιχνιδιού

Η Αλίκη «κλέβει»:
Διαλέγει αρχική κατάσταση μια υπέρθεση των δύο καταστάσεων του spin.
Έτσι αρχική κατάσταση είναι η :

$$\frac{1}{\sqrt{2}}(u+d)$$

Έτσι ότι και να διαλέξει ο Bob η κατάσταση του παιχνιδιού παραμένει ίδια.

$$1[\frac{1}{\sqrt{2}}(u+d)] = \frac{1}{\sqrt{2}}(1u+1d) = \frac{1}{\sqrt{2}}(u+d)$$

$$\sigma_x[\frac{1}{\sqrt{2}}(u+d)] = \frac{1}{\sqrt{2}}(\sigma_x u+\sigma_x d) = \frac{1}{\sqrt{2}}(d+u) = \frac{1}{\sqrt{2}}(u+d)$$

Αλλά τελικά η Αλίκη ανακαλύπτει ότι επειδή μια μέτρηση στη κατάσταση $\frac{1}{\sqrt{2}}(u+d)$ δίνει με ίση πιθανότητα μία από τις 2 καταστάσεις u,d τότε έχει ίση πιθανότητα να κερδίσει ή να χάσει. Αρα το σύνολο των payoff είναι:

$$\Pi=\{-1,+1\}$$

και οι αντίστοιχες πιθανότητες είναι:

$$P(\Pi) = \{(\frac{1}{\sqrt{2}})^2,(\frac{1}{\sqrt{2}})^2\} = \{\frac{1}{2},\frac{1}{2}\}$$

Ο Bob «κλέβει»:

Ενώ η Αλίκη ετοιμάζει την αρχική κατάσταση δίνουμε τη δυνατότητα στον Bob να χρησιμοποιήσει τους μετασχηματισμούς σ_x και σ_z όπως και οποιοδήποτε γραμμικό συνδυασμό αυτών. Ετσι μπορεί να χρησιμοποιήσει τον μετασχηματισμό

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

Μετά την πρώτη κίνηση του Bob θα έχω:

$$\mathrm{H}u = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}(u+d)$$

Στη συνέχεια ότι και να διαλέξει η Αλίκη δεν πρόκειται να αλλάξει την κατάσταση. Τελικά ο Bob διαλέγει πάλι τον ίδιο μετασχηματισμό και θα έχουμε:

$$H(\mathrm{H}u) = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\ 1\end{pmatrix} = \frac{1}{2}\begin{pmatrix}2\\ 0\end{pmatrix} = u$$

Οπότε ότι και να κάνει η Αλίκη ο Bob θα κερδίζει πάντα.

7.3 Το παιχνίδι «μάντεψε ένα αριθμό» I

Η Αλίκη διαλέγει έναν αριθμό α που ανήκει στο σύνολο S={0,1,…,N-1} και ο Bob προσπαθεί να το μαντέψει έχοντας μόνο ένα αριθμό κ πρασπαθειών.
Η Αλίκη ενεργεί σε κάθε κίνησή της όπως το μαντείο $U_{fa} = R_a$ στον αλγόριθμο του Grover.
Συμφωνούν ως $N=2^{30}=1.073.741.824$. Η Αλίκη γνωρίζει ότι ο Bob κλασικά χρειάζεται N/2 προσπάθειες για να βρεί τον αριθμό με πιθανότητα 50% έτσι συμφωνεί με το Bob το κ να είναι 100.000.000 νομίζοντας ότι έχει το πλεονέκτημα. Απ' την άλλη όμως ο Bob σκοπεύει να χρησιμοποιήσει τον αλγόριθμο του Grover και ξέρει ότι χρειάζεται

$$k = [\frac{\pi}{4}\sqrt{2^{30}} - \frac{1}{2}]_{near\,\mathrm{int}\,eger} = 25.375$$

προσπάθειες.

Ο Bob αρχικώς εγκαθιστάει N+1 qubits όπως:

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|x>(|0>-|1>)$$

Στη συνέχεια στέλνει τα πρώτα n qubits στην Αλίκη και μετά η Αλίκη απαντάει χρησιμοποιώντας το μαντείο $U_{fa} = R_a$.

Ο Bob απαντάει με το μετασχηματισμό R_s όπως τον περιγράψαμε στον αλγόριθμο του Grover και αυτή η διαδικασία επαναλαμβάνεται μέχρις ότου η Αλίκη να κάνει k κινήσεις.

$$(R_sR_a)^k\,|\psi_{\,s}>=\cos(2k+1)\theta\left|\alpha^{\perp}\right\rangle+\sin(2k+1)\theta\left|\alpha\right\rangle$$

Γίνεται μέτρηση και ο Bob νικάει με πιθανότητα $|\sin(2k+1)\theta|^2$

Τελικά μετά από έναν αριθμό παιχνιδιών η Αλίκη καταλαβαίνει ότι ο Bob νικάει πάντα και μάλιστα ύστερα από τον ίδιο αριθμό κινήσεων(= 25.735)(αφού η πιθανότητα να κερδίσει είναι $p \geq 1-\frac{1}{N}$).

7.4 Το παιχνίδι «μάντεψε ένα αριθμό» II

Η Αλίκη λέει στον Bob ότι ο αριθμός k των προσπαθειών είναι πολύ μεγάλος οπότε ο Bob της λέει ότι μπορώ να χρησιμοποιήσω μόνο 2 προσπάθειες αρκεί να μου δίνεις κάποιες πληροφορίες χρησιμοποιώντας τον μετασχηματισμό

$$T_{bv}^{a} \mid \psi_s >= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} T_{bv}^{a} \mid x >= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{x.a} \mid x >$$

(αυτός δεν είναι τίποτα άλλο παρά ένας Walsh-Hadamard μετασχηματισμός, δηλαδή n παράλληλες πύλες Hadamard οι οποίες δρουν σε μια αρχική κατάσταση α την οποία όμως ψάχνουμε να βρούμε)

Ο μετασχηματισμός (μαντείο)

$$T_{bv}^{a} \mid x >= (-1)^{f_{bv}^{a}} \mid x >= (-1)^{x.a} \mid x >$$

λέγεται Bernstein-Vazirani.
Η συνάρτηση που χρησιμοποιείται είναι η:

$$f_{bv}^{a} : \{0,1\}^n -> \{0,1\} \qquad με \qquad f_{bv}^{a}(x,a) = x.a$$

Το παιχνίδι αρχίζει και ο Bob στέλνει στην Αλίκη την κατάσταση

$$\mid \psi_s >= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} \mid x > (\mid 0 > - \mid 1 >)$$

Η Αλίκη απαντάει:

$$T_{bv}^{a} \mid \psi_s >= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} T_{bv}^{a} \mid x >= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{x.a} \mid x >$$

Ο Bob απαντάει:

$$W_{2^n} = T_{bv}^{a} \mid \psi_s >= \mid a >$$

Και κερδίζει φυσικά.

7.5 Το «δίλημμα του φυλακισμένου» (prisoner dilemma)

Ο στόχος μας είναι να μελετήσουμε 2x2 παιχνίδια που δεν είναι zero-sum, όπως και την έννοια της ισορροπίας Nash και να επεκταθούμε σε κβαντικά παιχνίδια.
Έστω, λοιπόν, δύο φυλακισμένοι όπου ανάλογα τι κίνηση θα κάνουν έχουν δυνατότητα να μειώσουν την ποινή τους από 0 έως 5 χρόνια. Πιο συγκεκριμένα ο παρακάτω πίνακας μας δείχνει όλες τις πιθανές περιπτώσεις :

	Bob C ή |0>	**Bob D ή |1>**
Alice C ή |0>	(3,3)	(0,5)
Alice D ή |1>	(5,0)	(1,1)

Αυτό σημαίνει ότι εάν η Αλίκη και ο Bob καταδώσουν ο ένας τον άλλο (D) τότε ο καθένας θα κερδίσει μείωση ποινής 1 χρόνου, ενώ αν για παράδειγμα η Αλίκη καταδώσει (D) και ο Bob όχι (C) τότε η Αλίκη θα κερδίσει μείωση ποινής 5 ετών ενώ ο Bob 0 έτη.

Τι κίνηση θα διαλέξει ο καθένας;

Η στρατηγική που πρέπει να ακολουθήσει η Αλίκη είναι μια κίνηση s_A τέτοια ώστε το payoff της π_A να έχει την ιδιότητα

$$\pi_A(s_A, s_B^j) \geq \pi_B(s_A^i, s_B^j)$$

για όλα τα $s_A^i \in S_A, s_B^j \in S_B$
όπου $s_A^i \in S_A$ είναι οι δυνατές κινήσεις που μπορεί να κάνει η Αλίκη
και $s_B^j \in S_B$ οι δυνατές κινήσεις που μπορεί να κάνει ο Bob.

Τελικά η Αλίκη θα διαλέξει την κίνηση D γιατί αν διαλέξει ο Bob την κίνηση D τότε η Αλίκη θα κερδίσει 1 έτος (καλύτερα από 0 έτη στην περίπτωση που η Αλίκη έπαιζε την κίνηση C) ενώ αν ο Bob διαλέξει την κίνηση C τότε η Αλίκη θα κερδίσει 5 χρόνια (καλύτερα από 3 έτη).

Για παρόμοιους λόγους ο Bob θα διαλέξει την κίνηση D.

Η περίπτωση αυτή είναι παράδειγμα ισορροπίας Nash και το αποτέλεσμα (1,1) είναι ένα Nash equilibrium (σημείο ισορροπίας Nash).

Είναι σημείο ισορροπίας γιατί δοθέντος της κίνησης του ενός ο άλλος δεν έχει λόγο να αλλάξει κίνηση.

Δηλαδή αν ο Bob διαλέξει την κίνηση D τότε η Αλίκη δεν έχει λόγο να αλλάξει την κίνηση D αφού διαφορετικά θα είχε κέρδος πιο λίγα χρόνια . Απ' την άλλη αν ο Bob διαλέξει την κίνηση C τότε πάλι η Αλίκη δεν έχει λόγο να αλλάξει την κίνηση D. Αντίστοιχα και για τον Bob.

Το «δίλημμα του φυλακισμένου» (prisoner dilemma) (κβαντικό παιχνίδι)

Ένα κβαντικό παιχνίδι Γ είναι μια αλληλεπίδραση μεταξύ 2 ή περισσότερων παικτών με τα κατάλληλα στοιχεία:

$$\Gamma = \Gamma(\mathrm{H}, \Lambda, \{s_i\}_j, \{\pi_i\}_j)$$

όπου H είναι ο χώρος Hilbert, Λ η αρχική κατάσταση του παιχνιδιού, $\{s_i\}_j$ το σύνολο των κινήσεων του παίκτη j, ενώ $\{\pi_i\}_j$ το σύνολο των payoff του παίκτη j.
Ο στόχος του παιχνιδιού είναι να καθορίσουμε τις στρατηγικές οι οποίες μεγιστοποιούν το payoff του παίκτη j.

Στο κβαντικό παιχνίδι ο κάθε παίκτης έχει στην κατοχή του ένα qubit και μπορεί να εκτελεί μετασχηματισμούς σε αυτό. Κάθε qubit βρίσκεται στο H_2 με διανύσματα βάσης |C> και |D> και το παιχνίδι βρίσκεται στο $H_2 \otimes H_2$ με διανύσματα βάσης τα |CC>, |CD>,|DD>,|DC>. Το qubit της Αλίκης είναι το αριστερό σε κάθε ζευγάρι, ενώ του Bob είναι το δεξιό.

Η αρχική κατάσταση Λ του παιχνιδιού είναι η

$$\Lambda = U|CC>$$

όπου U είναι ένας ορθομοναδιαίος (unitary) τελεστής, ο οποίος είναι γνωστός στην Αλίκη και στον Bob, που επενεργεί και στα δύο qubit. Η Αλίκη και ο Bob μπορούν να χρησιμοποιήσουν σαν κινήσεις τις s_A και s_B με:

$$s_A = U_A$$
$$s_B = U_B$$

Όπου U_A και U_B ορθομοναδιαίοι τελεστές όπου ο καθένας επενεργεί μόνο στο qubit του αντίστοιχου παίκτη. Αφού έχουν κάνει τις κινήσεις τους οι δύο παίκτες θα έχουμε:

$$(U_A \otimes U_B)U|CC>$$

Στη συνέχεια επενεργεί ο πίνακας $U^\dagger$ οπότε:

$$U^{\dagger}(U_A \otimes U_B)U\,|CC>$$

Στη συνέχεια κάνουμε την μέτρηση όπου υπάρχουν 4 δυνατά αποτελέσματα. Ένα από τα 4 διανύσματα βάσης του χώρου Hilbert.

Εάν αντιστοιχίσουμε την κατάσταση |C> στο |0> και την κατάσταση |D> στο |1> τότε θα έχουμε:

$$|\psi_s>= U^{\dagger}(U_A \otimes U_B)U\,|00>$$

Όταν γίνει η μέτρηση θα έχουμε για το αναμενόμενο payoff:

$$\bar{\pi} = 1\left|\langle\psi_f\,|00\rangle\right|^2 + 4\left|\langle\psi_f\,|01\rangle\right|^2 + 0\left|\langle\psi_f\,|10\rangle\right|^2 + 3\left|\langle\psi_f\,|11\rangle\right|^2$$

Το $\left|\langle\psi_f\,|00\rangle\right|^2$ μας δείχνει την πιθανότητα να εμφανισθεί η κατάσταση |00> δηλαδή και οι δύο να μην καταδώσουν. Αντίστοιχα και για τις άλλες περιπτώσεις.

Οι πιθανότητες αυτές εξαρτώνται από τον αρχικό πίνακα U και από τις κινήσεις U_A και U_B των δύο παικτών.

<u>Ο στόχος του πίνακα U είναι να δημιουργήσει κατάσταση συμπλοκής μεταξύ των qubits της Αλίκης και του Bob. Χωρίς αυτήν την συμπλοκή το παιχνίδι δεν θα είχε διαφορά από το κλασικό παιχνίδι.</u>

Έστω ότι ο πίνακας U είναι ο $U = \frac{1}{\sqrt{2}}(1^{\otimes 2} + i\sigma_x^{\otimes 2})$ δηλαδή ο :

$$U = \frac{1}{\sqrt{2}}(1^{\otimes 2} + i\sigma_x^{\otimes 2}) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} + i\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Τότε μετά την εφαρμογή του U|00> έχουμε:

$$U|00>=\frac{1}{\sqrt{2}}(1^{\otimes 2}+i\sigma_x^{\otimes 2})|00>=\frac{1}{\sqrt{2}}\left\{\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}+i\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}\right\}\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=$$

$$=\frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+i\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right)=\frac{1}{\sqrt{2}}(|00>+i|11>)$$

Μετά ας θεωρήσουμε κάποιες κλασικές κινήσεις της Αλίκης και του Bob. Αν συνεργαστούν τότε θεωρούμε ότι χρησιμοποιούν αντίστοιχα τους πίνακες $U_A=U_B=1$ ενώ αν καταδώσουν τότε θεωρούμε ότι χρησιμοποιούν τους πίνακες $U_A=U_B=\sigma_x=\begin{pmatrix}0&1\\1&0\end{pmatrix}$

Έχουμε 4 περιπτώσεις:

Περίπτωση 1:
«Να μην καταδώσει κανένας από τους δύο»

$$(U_A\otimes U_B)U|00>=(1\otimes 1)U\frac{1}{\sqrt{2}}(|00>+i|11>)=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\frac{1}{\sqrt{2}}\left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+i\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}=$$

$$=\frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+i\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right)=\frac{1}{\sqrt{2}}(|00>+i|11>)$$

Περίπτωση 2:
«Η Αλίκη να καταδώσει»

$$(U_A \otimes U_B)U\,|00>=(\sigma_x \otimes 1)U\,\frac{1}{\sqrt{2}}(|00>+i\,|11>)=\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix}\frac{1}{\sqrt{2}}\left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+i\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}=$$

$$=\frac{1}{\sqrt{2}}\left(\begin{pmatrix}0\\0\\1\\0\end{pmatrix}+i\begin{pmatrix}0\\1\\0\\0\end{pmatrix}\right)=\frac{1}{\sqrt{2}}(|10>+i\,|01>)$$

Περίπτωση 3:
«Ο Bob να καταδώσει»

$$(U_A \otimes U_B)U\,|00>=(1\otimes \sigma_x)U\,\frac{1}{\sqrt{2}}(|00>+i\,|11>)=\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\frac{1}{\sqrt{2}}\left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+i\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}=$$

$$=\frac{1}{\sqrt{2}}\left(\begin{pmatrix}0\\1\\0\\0\end{pmatrix}+i\begin{pmatrix}0\\0\\1\\0\end{pmatrix}\right)=\frac{1}{\sqrt{2}}(|01>+i\,|10>)$$

Περίπτωση 4:
«Και οι δύο να καταδώσουν»

$$(U_A \otimes U_B)U\,|00>=(\sigma_x \otimes \sigma_x)U\,\frac{1}{\sqrt{2}}(|00>+i\,|11>)=\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}\frac{1}{\sqrt{2}}\left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+i\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}=$$

$$=\frac{1}{\sqrt{2}}\left(\begin{pmatrix}0\\0\\0\\1\end{pmatrix}+i\begin{pmatrix}1\\0\\0\\0\end{pmatrix}\right)=\frac{1}{\sqrt{2}}(|11>+i\,|00>)$$

Στη συνέχεια επενεργεί ο αντίστροφος του πίνακα U δηλαδή ο

$$U^{-1} = U^{\dagger}$$

Έτσι έχουμε:

$U^{\dagger}\frac{1}{\sqrt{2}}(|00>+i|11>)=|00>$ με πιθανότητα 1

Η κατάσταση $|00>$ σημαίνει ότι βρισκόμαστε στην περίπτωση όπου και οι δύο συνεργάζονται

$U^{\dagger}\frac{1}{\sqrt{2}}(|10>+i|01>)=|10>$ με πιθανότητα 1

$U^{\dagger}\frac{1}{\sqrt{2}}(|01>+i|10>)=|01>$ με πιθανότητα 1

$U^{\dagger}\frac{1}{\sqrt{2}}(|11>+i|00>)=|11>$ με πιθανότητα 1

Αρα:

	Bob $U_B=\sigma_x$ ($|0>$)	**Bob $U_B=1$ ($|1>$)**
Alice $U_A=\sigma_x$ ($|0>$)	(3,3)	(0,5)
Alice $U_A=1$ ($|1>$)	(5,0)	(1,1)

Αυτό ακριβώς είναι το κλασικό αποτέλεσμα.

Μπορούμε όμως να αλλάξουμε τις κινήσεις των παικτών ώστε να μην είναι πια κλασικές. Για παράδειγμα μπορούμε να χρησιμοποιήσουμε και εκτός από τους μετασχηματισμούς $1,\sigma_x$ και τον μετασχηματισμό Hadamard.

Ετσι αν η Αλίκη χρησιμοποιήσει τον μετασχηματισμό **1** και ο Bob τον μετασχηματισμό **H** τότε:

$$(U_A \otimes U_B)U\,|00>=(1\otimes H)\frac{1}{\sqrt{2}}(|00>+i\,|11>)=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1&0&0\\1&-1&0&0\\0&0&1&1\\0&0&1&-1\end{pmatrix}\frac{1}{\sqrt{2}}\left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+i\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}=$$

$$=\frac{1}{2}\begin{pmatrix}1\\1\\0\\0\end{pmatrix}+\frac{1}{2}i\begin{pmatrix}0\\0\\1\\-1\end{pmatrix}=\frac{1}{2}(|00>+|01>+i\,|10>-i\,|11>)$$

Και αν χρησιμοποιήσουμε τον αντίστροφο μετασχηματισμό $U^{-1}=U^{\dagger}$ τότε:

$$U^{\dagger}(U_A \otimes U_B)U\,|00>=U^{\dagger}(1\otimes H)\frac{1}{\sqrt{2}}(|00>+i\,|11>)=U^{\dagger}\frac{1}{\sqrt{2}}\begin{pmatrix}1&1&0&0\\1&-1&0&0\\0&0&1&1\\0&0&1&-1\end{pmatrix}\frac{1}{\sqrt{2}}\left\{\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+i\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\right\}=$$

$$=U^{\dagger}\left\{\frac{1}{2}\begin{pmatrix}1\\1\\0\\0\end{pmatrix}+\frac{1}{2}i\begin{pmatrix}0\\0\\1\\-1\end{pmatrix}\right\}=$$

$$=\frac{1}{\sqrt{2}}\left\{\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}-i\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}\right\}\left\{\frac{1}{2}\begin{pmatrix}1\\1\\0\\0\end{pmatrix}+\frac{1}{2}i\begin{pmatrix}0\\0\\1\\-1\end{pmatrix}\right\}=\frac{1}{\sqrt{2}}\frac{1}{2}\left\{\begin{pmatrix}1\\1\\0\\0\end{pmatrix}+i\begin{pmatrix}0\\0\\1\\-1\end{pmatrix}-i\begin{pmatrix}0\\0\\1\\1\end{pmatrix}+\begin{pmatrix}-1\\1\\0\\0\end{pmatrix}\right\}=$$

$$=\frac{1}{\sqrt{2}}\frac{1}{2}\left\{\begin{pmatrix}0\\2\\0\\0\end{pmatrix}-i\begin{pmatrix}0\\0\\0\\2\end{pmatrix}\right\}=\frac{1}{\sqrt{2}}(|01>-i\,|11>)$$

Αυτό σημαίνει ότι η Αλίκη θα έχει πιθανότητα 50% να έχει payout 0 και 50% να έχει payout 1. Αρα $\bar{\pi}_{\mathrm{A}}=0{,}5$ και $\bar{\pi}_{\mathrm{B}}=(5+1)/2=3$.

Αν υποθέσουμε ότι ο Bob «παίζει» τον μετασχηματισμό H και η Αλίκη τον **1** τότε :

$$U^{\dagger}(U_A \otimes U_B)U\,|00>=U^{\dagger}(H\otimes 1)\frac{1}{\sqrt{2}}(|00>+i\,|11>)=\frac{1}{\sqrt{2}}(|10>-i\,|11>)$$

Μια μέτρηση στην κατάσταση αυτή θα μας δώσει με ίση πιθανότητα payout για την Αλίκη 5 ή 1 και για τον Bob 0 ή 1.
Αρα :

$$\bar{\pi}_{\mathrm{A}}=(5+1)/2=3 \;\; και \;\; \bar{\pi}_{\mathrm{B}}=(0+1)/2=0.5\,.$$

Οι υπόλοιπες περιπτώσεις είναι οι εξής:

«Να χρησιμοποιήσουν και οι δύο τον μετασχηματισμό H»

$$U^{\dagger}(U_A \otimes U_B)U\,|00>=U^{\dagger}(H\otimes H)\frac{1}{\sqrt{2}}(|00>+i\,|11>)=\frac{1}{2}(|00>+|11>-i\,|01>-i\,|10>)$$

$$\bar{\pi}_{\mathrm{A}}=\frac{1}{4}3+\frac{1}{4}1+\frac{1}{4}0+\frac{1}{4}5=2\frac{1}{4} \qquad \bar{\pi}_{\mathrm{B}}=2\frac{1}{4}$$

«Η Αλίκη τον μετασχηματισμό H και ο Bob τον σ_x»

$$U^{\dagger}(U_A \otimes U_B)U\,|00>=U^{\dagger}(H\otimes \sigma_x)\frac{1}{\sqrt{2}}(|00>+i\,|11>)=\frac{1}{\sqrt{2}}(|11>-i\,|10>)$$

$$\bar{\pi}_{\mathrm{A}}=\frac{1}{2}1+\frac{1}{2}5=3 \qquad \bar{\pi}_{\mathrm{B}}=\frac{1}{2}$$

«Ο Bob τον μετασχηματισμό H και η Αλίκη τον σ_x»

$$U^{\dagger}(U_A \otimes U_B)U\,|00>=U^{\dagger}(\sigma_x\otimes H)\frac{1}{\sqrt{2}}(|00>+i\,|11>)=\frac{1}{\sqrt{2}}(|11>-i\,|01>)$$

$$\bar{\pi}_{\mathrm{A}}=\frac{1}{2} \qquad \bar{\pi}_{\mathrm{B}}=3$$

Εάν λοιπόν επιτρέψουμε να γίνουν οι κινήσεις σ_x και H τότε ο πίνακας όπου μας δείχνει τα payoff του κάθε ένα είναι τα εξής:

	Bob **1**	Bob $\boldsymbol{\sigma_x}$	Bob **H**
Αλίκη **1**	(3,3)	(0,5)	$(\frac{1}{2},3)$
Αλίκη $\boldsymbol{\sigma_x}$	(5,0)	(1,1)	$(\frac{1}{2},3)$
Αλίκη **H**	$(3,\frac{1}{2})$	$(3,\frac{1}{2})$	$(2\frac{1}{4},2\frac{1}{4})$

Παρατηρούμε ότι η κατάσταση (1,1) δεν είναι πια σημείο ισορροπίας Nash. Αλλά το αποτέλεσμα $(2\frac{1}{4},2\frac{1}{4})$ που αντιστοιχεί στις κινήσεις (H,H) είναι τώρα σημείο ισορροπίας. Nash.

Θα μπορούσαμε να επεκταθούμε χρησιμοποιώντας πιο πολλές κινήσεις όπως για παράδειγμα όλες τις προηγούμενες μαζί με τον μετασχηματισμό σ_z. Τότε ο πίνακας των payoff θα γίνει:

	Bob **1**	Bob $\boldsymbol{\sigma_x}$	Bob **H**	Bob $\boldsymbol{\sigma_z}$
Αλίκη **1**	(3,3)	(0,5)	$(\frac{1}{2},3)$	(1,1)
Αλίκη $\boldsymbol{\sigma_x}$	(5,0)	(1,1)	$(\frac{1}{2},3)$	(0,5)
Αλίκη **H**	$(3,\frac{1}{2})$	$(3,\frac{1}{2})$	$(2\frac{1}{4},2\frac{1}{4})$	$(1\frac{1}{2},4)$
Αλίκη $\boldsymbol{\sigma_z}$	(1,1)	(5,0)	$(4,1\frac{1}{2})$	(3,3)

Το σημείο ισορροπίας Nash θα είναι τώρα το (3,3) που αντιστοιχεί στις κινήσεις $(\boldsymbol{\sigma_z, \sigma_z})$**.**

Ποιο είναι όμως το νόημα του ορθομοναδιαίου πίνακα U τον οποίο εφαρμόζουμε στην αρχική κατάσταση |00>;

Ίσως ένας τρίτος παίκτης ή κάποιος διαιτητής ή κάποιος συνεργάτης και των δύο παικτών που βοηθάει να μεγιστοποιηθεί το σημείο ισορροπίας Nash.

7.6 Το παιχνίδι «Η μάχη των δύο φύλων»

Η Αλίκη και ο Bob θέλουν να περάσουν ένα βράδυ μαζί αλλά διαφωνούν στον τρόπο διασκέδασης. Η Αλίκη προτιμάει να πάνε στην όπερα ενώ ο Bob να δούνε τηλεόραση στο σπίτι. Έτσι ο αντίστοιχος πίνακας των payoff σε κάθε μία περίπτωση είναι ο παρακάτω:

	Bob Όπερα	**Bob TV**
Αλίκη Όπερα (O)	(α,β)	(γ,γ)
Αλίκη TV (T)	(γ,γ)	(β,α)

όπου α>β>γ.
Εδώ έχουμε δύο σημεία ισορροπίας Nash. Τις περιπτώσεις (O,O) και (T,T). Αλλά υπάρχει και ένα τρίτο αρκεί να χρησιμοποιήσουμε mixed στρατηγικές δηλαδή να θεωρήσουμε ότι υπάρχει πιθανότητα p η Αλίκη να διαλέξει να πάνε στην Όπερα και 1-p να διαλέξει να δούν τηλεόραση , ενώ για τον Bob υπάρχει πιθανότητα q να διαλέξει την όπερα και 1-q να δούν τηλεόραση.
Ο υπολογισμός δίνει ότι οι πιθανότητες

$$p = \frac{\alpha - \gamma}{\alpha + \beta - 2\gamma} \quad \text{και} \quad q = \frac{\beta - \gamma}{\alpha + \beta - 2\gamma}$$

μεγιστοποιούν τα αναμενόνενα payoff και τελικά θα έχουμε:

$$\bar{\pi}_A(p,q) = \bar{\pi}_B(p,q) = \frac{\alpha\beta - \gamma^2}{\alpha + \beta - 2\gamma}.$$

Αλλά παρατηρούμε ότι ισχύει: $\alpha > \beta > \frac{\alpha\beta - \gamma^2}{\alpha + \beta - 2\gamma}$

Άρα το τρίτο αυτό Nash ισοζύγιο είναι χειρότερο από τα άλλα.

Τι θα γίνει αν χρησιμοποιήσουμε κβαντικές στρατηγικές;

Θεωρούμε αρχικά ότι $|O> \rightarrow |0>$ και $|T> \rightarrow |1>$ και εμπλέκουμε τις καταστάσεις με τον πίνακα U

$$U = \frac{1}{\sqrt{2}}(1^{\otimes 2} + i\sigma_x^{\otimes 2})$$

Οπότε όπως και στο προηγούμενο παιχνίδι :

$$U|00> = \frac{1}{\sqrt{2}}(1^{\otimes 2} + i\sigma_x^{\otimes 2})|00> = \frac{1}{\sqrt{2}}(|00> + i|11>)$$

Επιτρέπουμε και στους δύο παίκτες να χρησιμοποιήσουν τις εξής κινήσεις:

1, σ_x, H, σ_z.

Ετσι καταλήγουμε στον παρακάτω πίνακα:

	Bob **1**	Bob σ_x	Bob **H**	Bob σ_z
Αλίκη **1**	(α,β)	(γ,γ)	$(\frac{\beta+\gamma}{2},\frac{\alpha+\gamma}{2})$	(β,α)
Αλίκη σ_x	(γ,γ)	(β,α)	$(\frac{\beta+\gamma}{2},\frac{\alpha+\gamma}{2})$	(γ,γ)
Αλίκη **H**	$(\frac{\beta+\gamma}{2},\frac{\alpha+\gamma}{2})$	$(\frac{\beta+\gamma}{2},\frac{\alpha+\gamma}{2})$	$(\frac{\alpha+\beta+2\gamma}{4},\frac{\alpha+\beta+2\gamma}{4})$	$(\frac{\alpha+\gamma}{2},\frac{\beta+\gamma}{2})$
Αλίκη σ_z	(β,α)	(γ,γ)	$(\frac{\alpha+\gamma}{2},\frac{\beta+\gamma}{2})$	(α,β)

Από τον πίνακα παρατηρούμε

- ότι το κλασικό παιχνίδι περιέχεται στο κβαντικό
- ότι τώρα έχουμε ένα σημείο ισορροπίας Nash, το (β,α) όπου αν/χει στις κινήσεις (σ_x, σ_x). **Το οποίο σημαίνει ότι τελικά προτιμάνε να δούν τηλεόραση!!!**

Θα μπορούσαμε όμως να χρησιμοποιήσουμε mixed στρατηγικές και στην περίπτωση του κβαντικού παιχνιδιού.

Αν θεωρήσουμε ότι ο κάθε παίκτης χρησιμοποιεί 2 μετασχηματισμούς – κινήσεις **(**τους **1,**σ_z**)** και ότι υπάρχει πιθανότητα p να « παίξει » η Αλίκη τον μετασχηματισμό **1** και 1-p να « παίξει » τον σ_z όπως και ότι υπάρχει q πιθανότητα να «παίξει» ο Bob τον **1** και 1-q να « παίξει » τον σ_z τότε:

το αναμενόμενο payoff της Αλίκης θα είναι

$$\bar{\pi}_A = pqa + p(1-q)\beta + (1-p)q\beta + (1-p)(1-q)\alpha$$

Και για να βρούμε για πιο p έχουμε μέγιστο αναμενόμενο payoff αρκεί:

$$\frac{\partial \bar{\pi}_A}{\partial p} = q\alpha + (1-q)\beta + -q\beta - (1-q)a = 0$$

Λύνοντας ως πρός q θα έχουμε q=1/2. Αντίστοιχα p=1/2.
Ετσι οι mixed στρατηγικές

$$(\frac{1}{2}1+\frac{1}{2}\sigma_z,\frac{1}{2}1+\frac{1}{2}\sigma_z)$$

έχουν ως αναμενόμενα payoffs τα $(\frac{\alpha+\beta}{2},\frac{\alpha+\beta}{2})$ που είναι και σημείο ισορροπίας Nash. Ισότητα, λοιπόν, μεταξύ των δύο φύλων!

Κεφάλαιο 8

Επίλογος

Η εργασία αυτή είχε δύο βασικούς στόχους: την κατανόηση της δύναμης των κβαντικών αλγορίθμων και ως συνέπεια των κβαντικών υπολογιστών, αλλά και την εισαγωγή στη κβαντική θεωρία παιγνίων.

Έτσι συνδυάζει τις αρχές της κβαντικής φυσικής με τη θεωρία αλγορίθμων αλλά και τη θεωρία παιγνίων. Επίσης συνδυάζει αρχές και νόμους της κβαντικής φυσικής με προβλήματα της θεωρίας αλγορίθμων όπως αυτά της παραγοντοποίησης ενός αριθμού, της αναζήτησης ενός στοιχείου από μια μη ταξινομημένη βάση δεδομένων αλλά και άλλα προβλήματα που μπορούν να λυθούν με βάση τις λύσεις στα προηγούμενα, όπως αυτά του χρωματισμού ενός γράφου (Graph Coloring Problem) , αλλά και του πλανόδιου πωλητή (TSP problem).

Στη θεωρία παιγνίων αναφερόμαστε σε κβαντικές στρατηγικές οι οποίες μας οδηγούν σε διαφορετικά σημεία ισορροπίας Nash απ' ότι στην κλασική περίπτωση. Παρατηρούμε από τα πέντε κβαντικά παιχνίδια που παρουσιάζουμε ότι η κβαντική θεωρία παιγνίων «περικλείει» την κλασική θεωρία παιγνίων αφού μπορούμε να πάρουμε τα αποτελέσματα που θα παίρναμε από την κλασική θεωρία με τη χρήση κατάλληλων στρατηγικών.

Κορυφαίοι επιστήμονες «παρελαύνουν» στην εργασία αυτή αφού η «ιστορία» ξεκινάει από το 1900 με τον Νομπελίστα Φυσικό Max Planck, τον Albert Einstein, τον Niels Bohr, Ernest Rutherford, W. Heisenberg, E.Schrodinger, P.A.M. Dirac τον επίσης κορυφαίο νομπελίστα φυσικό και δάσκαλο R. Feynman αλλά και τους D.Deutsch, Grover και φυσικά τον P.Shor ο οποίος με τον αλγόριθμό του για την παραγοντοποίηση ενός αριθμού έδωσε νέα ώθηση στον κλάδο της θεωρητικής πληροφορικής που ονομάζεται κβαντικοί υπολογισμοί. Αξίζει ακόμα να αναφερθούμε στους Von Neumann, J.Nash και τέλος στον David Mayer για τη συμβολή τους στην ανάπτυξη της θεωρίας παιγνίων αλλά και της κβαντικής θεωρίας παιγνίων αντίστοιχα.

Αρχικά παρουσιάσαμε τον αλγόριθμο του Deutsch και τη γενίκευση του, όπου μπορούμε να ξεχωρίζουμε αν μια συνάρτηση είναι σταθερή ή όχι. Στη συνέχεια μελετήσαμε τον αλγόριθμο αναζήτησης του Grover ο όποιος είναι πιο γρήγορος κατά ένα παράγοντα τετραγωνικής ρίζας σε σχέση με αντίστοιχο κλασικό αλγόριθμο. Ο αλγόριθμος αυτός είναι σημαντικός γιατί μας βοηθάει να λύσουμε μια σειρά NP-complete προβλημάτων στον ίδιο χρόνο (επιτάχυνση τετραγωνικής ρίζας) έτσι ώστε να συμπεράνουμε τελικά ότι οι κβαντικοί υπολογιστές είναι πιο γρήγοροι από τους κλασικούς μεν, αλλά απ'

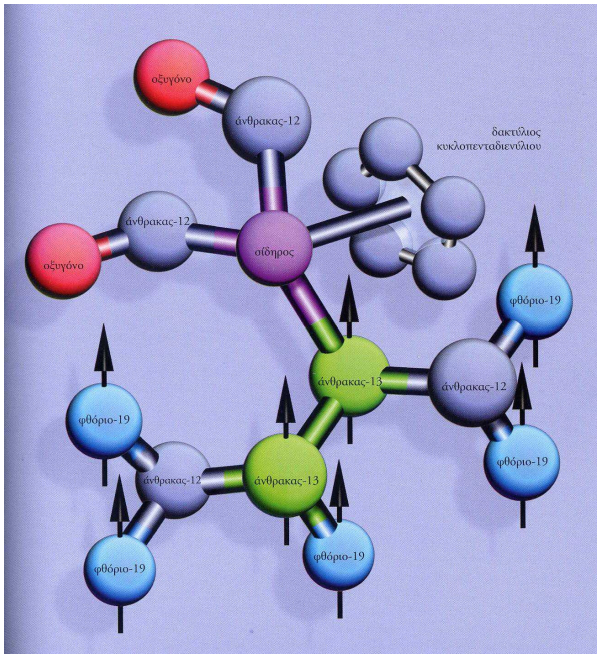
την άλλη δεν έχουμε βρεί κανένα κβαντικό αλγόριθμο για NP-complete πρόβλημα όπου να έχουμε εκθετική επιτάχυνση. Όχι μόνο αυτό αλλά το 1997 αποδείχθηκε ότι ο αλγόριθμος του Grover είναι βέλτιστος [23].

Στη συνέχεια αναφερθήκαμε στον αλγόριθμο παραγοντοποίησης του Shor όπου προσπαθήσαμε να κατανοήσουμε που οφείλεται αυτή η εκθετική επιτάχυνση σε σχέση με τον καλύτερο κλασικό αλγόριθμο. Καταλήξαμε, λοιπόν, ότι η υπέρθεση των qubits, ο κβαντικός παραλληλισμός (quantum parallelism) δηλαδή οι πράξεις που γίνονται ταυτόχρονα σε όλα τα qubits όπως και το φαινόμενο της κβαντικής συμπλοκής (quantum entanglement) αλλά και ο κατάλληλος τρόπος να τα χρησιμοποιήσεις όλα αυτά είναι οι λόγοι που είναι τόσο γρήγορος αυτός ο αλγόριθμος.
Επίσης αναφερθήκαμε και στην κλάση πολυπλοκότητας BQP και στη σχέση της με τις γνωστές κλάσεις πολυπλοκότητας P, BPP, NP,PSPACE.

Ποια η πρόοδος όμως των κβαντικών αλγορίθμων; Αν και έχει περάσει πάνω από μια δεκαετία από τη στιγμή που ο Shor ανακάλυψε τον αλγόριθμο παραγοντοποίησης (1994), εκτός από τον αλγόριθμο του Grover (1996), δεν έχουμε κάποια σημαντική πρόοδο [41]. Δεν έχουν ανακαλυφθεί σημαντικοί νέοι κβαντικοί αλγόριθμοι. Ο ίδιος ο Shor χωρίζει τους κβαντικούς αλγόριθμους σε τρείς κατηγορίες : σε αλγόριθμους όπου προσπαθούμε να βρούμε την εύρεση της περιόδου μιας συνάρτησης (π.χ: παραγοντοποίηση), σε αυτούς που στηρίζονται στο σκεπτικό του αλγόριθμου αναζήτησης του Grover και σε αυτούς όπου γίνεται προσομοίωση της κβαντομηχανικής.

Μια άλλη ερώτηση που θα μπορούσε να κάνει κανείς είναι αν έχει κατασκευαστεί κάποιος κβαντικός υπολογιστής ή αν είναι δυνατόν ποτέ να κατασκευαστεί ένας κβαντικός υπολογιστής. Στο σημείο αυτό μπορούμε να πούμε ότι έχει ήδη κατασκευαστεί ένας κβαντικός υπολογιστής. Πιο συγκεκριμένα το 2001 οι ερευνητές της IBM είχαν κατορθώσει να υλοποιήσουν σε ένα κβαντικό σύστημα τον αλγόριθμο του Shor, βρίσκοντας τους πρώτους παράγοντες του 15. Στο σχήμα που παραθέτουμε βλέπουμε τη δομή του πρώτου κβαντικού υπολογιστή στον κόσμο. Είναι ένα μόριο στο οποίο 2 άτομα άνθρακα-13 και 5 άτομα φθορίου, σχηματίζουν 7 qubits με βάση την ιδιότητα spin κάθε ατόμου. Τα spin αυτά βρίσκονται σε αλληλεπίδραση (όπως απαιτεί και ο αλγόριθμος του Shor) αλλά μπορούν να τεθούν χωριστά σε κάποια αρχική τιμή spin. Για την εκτέλεση του αλγορίθμου του Shor κατασκευάστηκαν δισεκατομμύρια παρόμοια μόρια τα οποία και τοποθετήθηκαν από τους ερευνητές της IBM σε ένα διάλυμα ενός δοκιμαστικού σωλήνα. Αρχικά, τα spin των ατόμων τους ευθυγραμμίστηκαν με χρήση ισχυρών μαγνητικών πεδίων, ενώ στη συνέχεια τα άτομα των μορίων αυτών αφέθηκαν να εκτελέσουν τον αλγόριθμο του Shor με χρήση παλμών κατάλληλης ραδιοσυχνότητας. Τέλος, η «απάντηση» αναγνωρίστηκε μέσω του φάσματος μαγνητικού συντονισμού των μορίων.

Βέβαια ο κβαντικός υπολογιστής χρειάζεται να διανύσει μεγάλη απόσταση για να γίνει πρακτικός και εύκολα διαθέσιμος στον οποιοδήποτε. Το πιο σημαντικό πρόβλημα αυτή τη στιγμή είναι η ασυμφωνία (αποσυνοχή) (decoherence) δηλαδή η καταστροφή του κβαντικού συστήματος εξαιτίας αλληλεπίδρασης με το περιβάλλον.



Τέλος έγινε αναφορά σε πέντε κβαντικά παιχνίδια με σκοπό την εισαγωγή στη κβαντική θεωρία παιγνίων. Ξεκινήσαμε με το spin-flip game, γράψαμε την κλασική εκδοχή του παιχνιδιού με την απαραίτητη θεωρία και στη συνέχεια μελετήσαμε την κβαντική εκδοχή του παιχνιδιού. Είδαμε τι μπορεί να γίνει αν οι παίκτες χρησιμοποιήσουν διαφορετικούς μετασχηματισμούς εκτός από τους **1 (ναι)** ή **σ_x(όχι).** Στη συνέχεια ασχοληθήκαμε με το παιχνίδι «Μάντεψε ένα αριθμό Ι» («guess a number I») που χρησιμοποιεί τον κβαντικό αλγόριθμο του Grover όπως και μια παραλλαγή αυτού το «Μάντεψε ένα αριθμό ΙΙ» («guess a number II»). Μελετήσαμε στη συνέχεια το «δίλημμα του φυλακισμένου» («prisoner's dilemma») στην κλασική όσο και στην κβαντική εκδοχή του όπου βρήκαμε ότι αν χρησιμοποιήσουμε καταρχήν τις κινήσεις **1 (ναι)** ή **σ_x(όχι)** τα αποτελέσματα θα ήταν τα ίδια με αυτά της κλασικής εκδοχής, ενώ αν «αφήσουμε» τους παίκτες να χρησιμοποιήσουν και άλλες κινήσεις (π.χ.: μετασχηματισμό Hadamard) τότε παρατηρούμε νέα σημεία ισορροπίας Nash. Τέλος ασχοληθήκαμε με «τη μάχη των δύο φύλων» («battle of the sexes game») όπου χρησιμοποιήσαμε mixed κβαντικές στρατηγικές για να βρούμε πάλι διαφορετικά σημεία ισορροπίας Nash σε σχέση με την κλασική περίπτωση, όπου πάλι έχουμε mixed στρατηγικές.

Γιατί όμως να ασχοληθεί κάποιος με τη κβαντική θεωρία παιγνίων;

Ίσως γιατί τελικά η αγορά ακολουθεί κβαντικούς νόμους. Όπως και η φύση «παίζει» κβαντικά παιχνίδια και αν θεωρήσουμε ότι ο ανθρώπινος εγκέφαλος δεν είναι τίποτα άλλο παρά ένας κβαντικός υπολογιστής [24] θα μπορούσαμε να πούμε ότι οι ανθρώπινες αποφάσεις δεν είναι τίποτα άλλο παρά κβαντικές κινήσεις σε παιχνίδια που ακολουθούν κβαντικούς κανόνες.

ΠΗΓΕΣ ΦΩΤΟΓΡΑΦΙΚΟΥ ΥΛΙΚΟΥ

Raymond A.Servey-Clement J. Moses- Curt A. Moyer, *Σύγχρονη Φυσική* , Πανεπιστημιακές Εκδόσεις Κρήτης,2004, Σελ.12,
Jim Al-Khalili *Quantικά Παράδοξα,*2005, Σελ.21,45,47,120.

ΑΝΑΦΟΡΕΣ

[1] Jim Al-Khalili *Quantικά Παράδοξα,*2005

[2] J.Orlin Grabbe *An Introduction to Quantum Game Theory,*2005

[3] Γ.Ι.Ανδριτσόπουλος *Εισαγωγή στην Κβαντομηχανική,* Τρίτη Έκδοση,1984

[4] Ιορδάνης Κερενίδης *Κβαντικοί Υπολογισμοί(Διπλωματική Εργασία)* 2000

[5] J.Preskill *Σημειώσεις του μαθήματος Κβαντικοί Υπολογιστές στο Πανεπιστήμιο του Caltech,* http://www.theory.caltech.edu/people/preskill/ph229

[6] Michele Mosca, *Σημειώσεις του μαθήματος Κβαντικοί Υπολογιστές στο Πανεπιστήμιο του Waterloo*

[7] E.Knill,R.Laflamme,H.Barnum,D.Dalvit,J.Dziarmaga,et.al *Introduction to Quantum Information Processing,*March 29,2002

[8] Samuel J. Lomonaco, *A Lecture on Shor's Quantum Factorimg Algorithm Version 1.1,* 2000

[9]Peter Shor, *Polynomial-time Algorithms for Prime Factorization and discrete logarithms on a quantum computer ,* 1994

[10] Peter Shor, *Quantum Computing*, 1991

[11] Umesh Vazirani, *Fourier Transforms and Theoretical Computer Science,*1999

[12] Artur Ekert, Patrick Hayden and Hitoshi Inamori, *Basic Concepts in quantum computation*, 2000

[13] Marek Perkowski- Portland Quantum Logic Group, *From Quantum Gates to Quantum Learning: recent research and open problems in quantum circuits*

[14] Marek Perkowski, Department of Electrical Engineering, Portland State University, *Review of basic quantum and Deutsch-Jozsa,*2005

[15] Ian Glendinning, *The Bloch Sphere,* February 16, 2005

[16] Feynman Richard P., *'Simulating Physics with Computers'*, International Journal of theoretical Physics,21, 1982, 467
[17]Μαρία Κοκόνου, *Κβαντική Συσχέτιση*, Περισκόπιο της επιστήμης , 11/2005

[18]Rieffel Eleanor, *An Introduction to Quantum Computing for Non-Physicists,*19 Jan 2000.

[19]Meyer David., *"Quantum Games and Quantum Algorithms", arXiv: quant-ph/0004092 v2*,3 May 2000.

[20]Raymond A.Servey-Clement J. Moses- Curt A. Moyer, *Σύγχρονη Φυσική* , Πανεπιστημιακές Εκδόσεις Κρήτης,2004

[21] Meyer David., *"Quantum Strategies", arXiv: quant-ph/9804010 v1*, 3 Apr 1998.

[22] Eleanor Rieffel, « An Introduction to Quantum Computing for Non-Physicists », *arXiv: quant-ph/9809016 v2*, 3 Apr 1998.

[23]C.Bennet, E.Bernstein, C.Brassard, U.Vazirani *Strengths and weaknesses of quantum computing*, SIAM Journal of Computing, 1997

[24] Penrose Roger, *The Emperor's New Mind*, Oxgord University Press,1989.

[25]D.Deutsch, Quantum theory, *the Church-Turing principle and the universal quantum computer*, Proc. Roy. Soc. London Ser. A 400 (1985) 96-117

[26] D.Deutsch and R.Jozsa (1192), Rapid solution of problems by quantum computation, Proc. Roy. Soc. London Ser. A, 439, pp. 669-677

[27]Π.Ε.Νάστου,Π.Γ.Σπυράκης,Γ.Κ.Σταματίου, *Σύγχρονη Κρυπτογραφία*, Ελληνικά Γράμματα, Αθήνα 2003

[28]Bernstein E. and U. Vazirani, "Quantum complexity theory", in Proceedings of the 25th Annual ACM Symposium on the theory of Computing San Diego, Calif, 16-18 May 1993, New York: Acm, 1993, 11-20, http://www.cs.berkley.edu/~vazirani/pubs/bv.ps

[29] D.Deutsch, 'It from Qubit', Sept 2002, http://www.qubit.org/people/david/Articles/ItfromQubit.pdf

[30]Lomonaco, Jr. Samuel J., 'A lecture on Grover's quantum search algorithm', arXiv:quant-ph/0010040 v2 18 Oct 2000

[31] Lomonaco, Jr. Samuel J., 'A lecture on Shor's quantum factoring algorithm', arXiv:quant-ph/0010034 v1 9 Oct 2000

[32] Meyer David., *"Quantum Games and Quantum algorithms", arXiv: quant-ph/0004092 v2*, 3 May 2000.

[33]Neumann John von and Oscar Morgenstern, The theory of games and economic behavior, New York: Wiley, 1944.

[34]Piotrowski Edward W. and Jan Sladkowski, 'An invitation to quantum game theory', arXIv: quantum-ph/0211191 v1 28 Nov 2002

[35] Stanford Encyclopedia of Philosophy, 'Evoluytionary game theory', http://plato.stanford.edu/entries/game-evolutionary/.

[36]Bennet, C, *"Logical reversibility of computation",* IBM J. Res. Develop., Vol. 17,1973,pp.525-532

[37] Bernstein E. and U. Vazirani, "Quantum complexity theory", Special issue on Quantum Computation of the Siam Journal of Computing, Oct, 1997

[38]Steane, M. "A quantum computer only needs ona universe", lanl e-print quant-ph/0003084, Mar.2003

[39] C.Bennett, E.Bernstein,G. Brassard, U. Vazirani, *Strength and weakness of quantum computing,* SIAM Journal of Computing, 1997.

[40]Eric Bernstein, Kenny Huang, Amir Kamil, Jimmy Kittyachavalit *Quantum Computability and Complexity and the Limits of Quantum Computation*, University of California, Berkley, December 7, 2003

[41] Shor W. Peter, *Progress in quantum algorithms*, 14 September 2005