

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΜΑΤΙΚΗΣ



ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ & ΤΗΛΕΜΑΤΙΚΗ

*Μεταπτυχιακή
Διπλωματική Εργασία*

ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ

ΓΙΩΡΓΟΣ ΑΣΗΜΑΚΗΣ

ΧΑΡΟΚΟΠΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΜΑΤΙΚΗΣ



ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ & ΤΗΛΕΜΑΤΙΚΗ
2^η Κατεύθυνση - Τηλεπικοινωνίες

Μεταπτυχιακή
Διπλωματική Εργασία

ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ

Επιβλέπων Καθηγητής:

κ. ΘΩΜΑΣ ΚΑΜΑΛΑΚΗΣ

Copyright- © Γιώργος Π. Ασημάκης

Αθήνα – Ιανουάριος 2015

Απαγορεύεται η αναδημοσίευση ή η ανατύπωση ή η ηλεκτρονική αποθήκευση, ολικώς, μερικώς κατά παράφραση του περιεχομένου του παρόντος κειμένου χωρίς την έγγραφη άδεια του συγγραφέα.

Εστη Μακρίνα

και εστη Χριστίνα

«Οι παρενέργειες της φύσης και της παιδείας είναι παρόμοιες, επειδή η παιδεία μεταμορφώνει τον άνθρωπο, δημιουργώντας έτσι την φύση του. Η μόρφωση είναι ένα στολίδι για τους πλούσιους, ένα καταφύγιο για όσους έχουν ατυχήσει. Οι προσδοκίες ενός μορφωμένου ατόμου έχουν μεγαλύτερη αξία από τα υλικά αγαθά που κατέχει ένας αμαθής»

Δημόκριτος

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ ΚΑΙ ΠΙΝΑΚΩΝ	σελ. 9
ΙΣΤΟΡΙΚΟ ΧΡΟΝΟΛΟΓΙΟ ΚΒΑΝΤΙΚΗΣ ΦΥΣΙΚΗΣ	σελ. 11
ΠΕΡΙΛΗΨΗ	σελ. 13
ABSTRACT	σελ. 15
ΕΙΣΑΓΩΓΗ	σελ. 17

Α' ΜΕΡΟΣ – ΚΒΑΝΤΙΚΗ ΘΕΩΡΙΑ

ΚΕΦΑΛΑΙΟ 1 ^ο	σελ. 21
-------------------------	---------

Η ΠΑΛΑΙΑ ΚΒΑΝΤΙΚΗ ΘΕΩΡΙΑ

1.1	Εισαγωγή στην κβαντική θεωρία	σελ. 21
1.2	Ο κυματοσωματιδιακός χαρακτήρας της ύλης και η διττή φύση του φωτός	σελ. 22
1.3	Φωτοηλεκτρικό φαινόμενο	σελ. 24
1.4	Αρχή της αβεβαιότητας	σελ. 26
1.5	Το πρότυπο του Bohr	σελ. 28

ΚΕΦΑΛΑΙΟ 2 ^ο	σελ. 33
-------------------------	---------

ΚΒΑΝΤΙΚΟ ΠΛΑΙΣΙΟ, ΘΕΜΕΛΙΩΔΕΙΣ ΑΡΧΕΣ, ΑΙΤΗΜΑΤΑ ΚΑΙ ΜΑΘΗΜΑΤΙΚΟΣ ΦΟΡΜΑΛΙΣΜΟΣ

2.1	Χώρος Hilbert	σελ. 33
2.2	Η κυματοσυνάρτηση ψ	σελ. 34
2.3	Η εξίσωση του Schrödinger	σελ. 37
2.4	Ιδιοτιμές και ιδιοσυναρτήσεις	σελ. 39
2.5	Κυματικές συναρτήσεις στον χώρο των ορμών	σελ. 39
2.6	Εσωτερικό γινόμενο συναρτήσεων	σελ. 40

2.7	Εσωτερικό γινόμενο πινάκων	σελ. 42
2.8	Κβαντομηχανικοί τελεστές	σελ. 43
2.9	Τελεστές θέσης και ορμής	σελ. 46
2.10	Τελεστής Hamiltonian	σελ. 47
2.11	Τελεστής στροφορμής	σελ. 48
2.12	Αναπαράσταση καταστάσεων με πίνακες	σελ. 49
2.13	Αναπαραστάσεις τελεστών σε μορφή πινάκων	σελ. 49
2.14	Μέση τιμή	σελ. 50
2.15	Τυπική απόκλιση	σελ. 53
2.16	Σχέση αβεβαιότητας θέσης και ορμής	σελ. 53
2.17	Θεμελιώδεις αρχές	σελ. 54
2.18	Ο φορμαλισμός του Dirac	σελ. 56
2.19	Το σπιν	σελ. 58
2.20	Πηγάδι δυναμικού	σελ. 63

ΚΕΦΑΛΑΙΟ 3^ο**σελ. 67****ΚΒΑΝΤΙΚΑ ΠΑΡΑΔΟΞΑ**

3.1	Η έννοια της υπέρθεσης	σελ. 67
3.2	Κβαντική σήραγγα	σελ. 69
3.3	Το κβαντικό νόμισμα	σελ. 70
3.4	Μη τοπικότητα	σελ. 71
3.5	Αποσυννοχή	σελ. 72
3.6	Κβαντική διεμπλοκή	σελ. 73

ΜΕΡΟΣ Β' – ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ**ΚΕΦΑΛΑΙΟ 4^ο****σελ. 77****ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΚΑΙ ΣΤΟΙΧΕΙΑ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ**

4.1.	Εισαγωγή στους κβαντικούς υπολογιστές	σελ. 77
4.2.	Τα κβαντικά bit	σελ. 81
4.3.	Σφαίρα Bloch	σελ. 85
4.4.	Κβαντικός καταχωρητής	σελ. 88

ΚΕΦΑΛΑΙΟ 5^ο **σελ. 93**

ΤΕΧΝΟΛΟΓΙΑ ΚΑΤΑΣΚΕΥΗΣ ΚΑΙ ΔΟΜΗ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

5.1.	Κβαντικός επεξεργαστής	σελ. 93
5.2	Τεχνολογική δομή κβαντικών υπολογιστών	σελ. 94
5.3	Κβαντικές τελείες	σελ. 98
5.4	D-Wave κβαντικός υπολογιστής	σελ. 103
5.5	Ερευνητικές προσπάθειες και καινοτομίες	σελ. 107
5.6	Κβαντικοί υπολογιστές και αποσυνοχή	σελ. 109

ΚΕΦΑΛΑΙΟ 6^ο **σελ. 111**

ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ

6.1	Εισαγωγή στις κβαντικές πύλες	σελ. 111
6.2	Κβαντική πύλη αδρανείας	σελ. 114
6.3	Κβαντική πύλη μετατόπισης φάσης	σελ. 116
6.4	Κβαντική πύλη NOT	σελ. 117
6.5	Κβαντική πύλη Hadamand	σελ. 118
6.6	Κβαντική πύλη ελεγχόμενου ΟΧΙ	σελ. 120
6.7	Κβαντική πύλη εναλλαγής	σελ. 121
6.8	Κβαντική πύλη ελεγχόμενης μετατόπισης φάσης	σελ. 123
6.9	Κβαντική πύλη διπλά ελεγχόμενου ΟΧΙ	σελ. 125
6.10	Κβαντική πύλη Fredkin	σελ. 127
6.11	Κβαντικές πύλες και πίνακες Pauli	σελ. 130

ΚΕΦΑΛΑΙΟ 7^ο **σελ. 131**

ΚΒΑΝΤΙΚΑ ΚΥΚΛΩΜΑΤΑ

7.1	Βασικά στοιχεία	σελ. 131
7.2	Μελέτη κβαντικών κυκλωμάτων	σελ. 133
7.3	Κβαντικό κύκλωμα κβαντικής διεμπλοκής	σελ. 141

ΚΕΦΑΛΑΙΟ 8^ο **σελ. 147**

ΚΒΑΝΤΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ

- | | | |
|-----|---------------------------------------|----------|
| 8.1 | Εισαγωγή στους κβαντικούς αλγορίθμους | σελ. 147 |
| 8.2 | Κβαντικός αλγόριθμος του Deutsch | σελ. 148 |
| 8.3 | Κβαντικός αλγόριθμος του Grover | σελ. 154 |

ΚΕΦΑΛΑΙΟ 9^ο **σελ. 161**

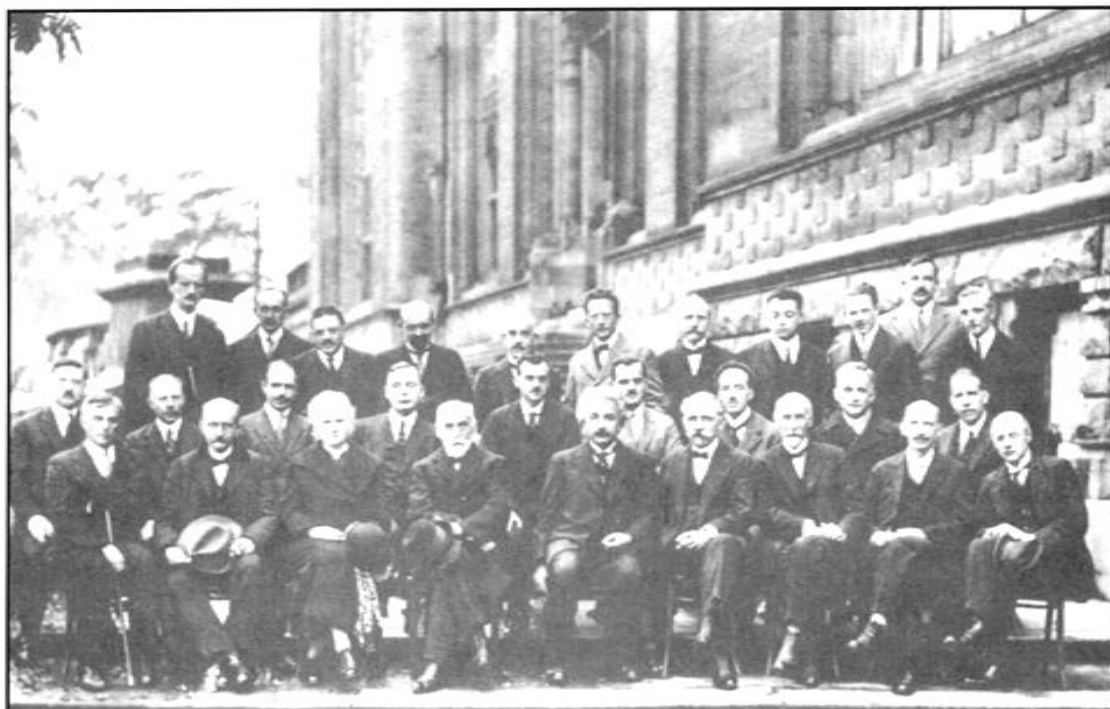
ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

- | | | |
|-----|------------------------------------|----------|
| 9.1 | Στοιχεία κρυπτογραφίας | σελ. 161 |
| 9.2 | Κρυπτογραφία και κβαντική μηχανική | σελ. 166 |
| 9.3 | Κβαντικός μετασχηματισμός Fourier | σελ. 169 |
| 9.4 | Κβαντικός αλγόριθμος του Shor | σελ. 170 |

ΣΥΜΠΕΡΑΣΜΑΤΑ **σελ. 177****ΠΑΡΑΡΤΗΜΑ Α΄** **σελ. 179****ΠΑΡΑΡΤΗΜΑ Β΄** **σελ. 189****ΠΑΡΑΡΤΗΜΑ Γ΄** **σελ. 191****ΒΙΒΛΙΟΓΡΑΦΙΑ** **σελ. 195**

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ ΚΑΙ ΠΙΝΑΚΩΝ

Σχήμα	Περιγραφή	Σελίδα
1.1	Φωτοηλεκτρικό φαινόμενο	25
1.2, 1.3, 1.4	Αρχή αβεβαιότητας του Heisenberg	27
1.5, 1.6	Ενεργειακές στάθμες - Θεωρία του Bohr	29
2.1	Πηγάδι Δυναμικού	63
2.2	Κυματοσυναρτήσεις διεγερμένων καταστάσεων	64
2.3	Ενεργειακές στάθμες	65
3.1	Κβαντική Σήραγγα	70
3.2	Η γάτα του Schrödinger	74
4.1	Νόμος του Gordon Moore	78
4.2	Αποτόπωση στον χώρο κβαντικής κατάστασης	82
4.3, 4.4	Ενεργειακές στάθμες κβαντικών καταστάσεων	82-83
4.5, 4.6, 47	Σφαίρα Bloch	85-86-89
5.1	Κβαντικός επεξεργαστής-συσσκευή κοιλότητας	94
5.2, 5.3, 5.4	Πυρηνικός μαγνητικός συντονισμός - NMR-	96-97
5.5, 5.6, 5.7, 5.8	Κβαντικές τελείες	99-100-102
5.9, 5.10	D-Wave Κβαντικός υπολογιστής	104-105
6.1, 6.2	Δράσεις σε πύλες	112-113
6.3	Κβαντική πύλη αδρανείας	115
6.4	Κβαντική πύλη μετατόπισης φάσης	117
6.5	Κβαντική πύλη NOT	117
6.6	Κβαντική πύλη Hadamard	119
6.7	Κβαντική πύλη ελεγχόμενου OXI	120
6.8	Κβαντική πύλη εναλλαγής	122
6.9	Κβαντική πύλη ελεγχόμενης μετατόπισης φάσης	124
6.10	Κβαντική πύλη ελεγχόμενου OXI	126
6.11	Κβαντική πύλη Fredkin	128
6.12	Πίνακες Pauli	129
7.1	Γενικό κβαντικό κύκλωμα	132
7.2 - 7.7,	Παραδείγματα κβαντικών κυκλωμάτων	133 με 140
7.8, 7.9	Κβαντικό κύκλωμα κβαντικής διεμπλοκής	142-143
7.10, 7.11	Καταστάσεις Bell	146
8.1, 8.2	Αλγόριθμος του Deutsch	148-149
8.3	Αλγόριθμος του Grover	155
8.4	Κβαντικό Oracle	155
8.5	Γεωμετρική εικόνα δράσης αλγόριθμου Grover	157
8.6	Επεξεργασία αλγόριθμου Grover	158
9.1	Εκπομπή κβαντικών σωματιδίων και παρατηρητές	167
9.2	Αλγόριθμος του Shor	171



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



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

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.

(Από το βιβλίο *Σύγχρονη φυσική* του Serway, ΠΕΚ-ΙΤΕ)

ΙΣΤΟΡΙΚΟ ΧΡΟΝΟΛΟΓΙΟ ΚΒΑΝΤΙΚΗΣ ΦΥΣΙΚΗΣ [2]

- 400 π.χ. **Δημόκριτος** – Θεωρία του ατόμου.
- 320 π.χ. **Αριστοτέλης** – Φυσική περιγραφή της κίνησης
- 1865 **Maxwell** – Διατύπωση της ηλεκτρομαγνητικής θεωρίας του φωτός.
- 1896 Φαινόμενο **Zeeman** – Οι φασματικές γραμμές ακτινοβολίας του φωτός διαφέρουν όταν αυτό παράγεται από μαγνητικό πεδίο.
- 1897 **J.J.Thomson** – Ανακάλυψη του ηλεκτρονίου.
- 1898 **Heinrich Herz** – Φαινόμενο φωτοηλεκτρισμού.
- 1905 **Albert Einstein** – Διατύπωση ειδικής θεωρίας σχετικότητας και της περίφημης εξίσωσης $E=mc^2$.
- 1911 **Rutherford** – Πυρηνική μοντέλο ατόμου, ανακάλυψη πυρήνα.
- 1912 **Albert Einstein** – Βαρύτητα και καμπύλωση στο χώρο και το χρόνο.
- 1913 **Niels Bohr** – Μοντέλο ατομικής δομής. Τα ηλεκτρόνια περιστρέφονται γύρω από το πυρήνα του ατόμου εκτελώντας κυκλική τροχιά.
- 1918 **Max Planck** – Βραβείο Νόμπελ για την θεωρία των κβάντα.
- 1919 **Rutherford** – Μελέτη πρωτονίου.
- 1921 **Albert Einstein** – Βραβείο Νόμπελ για την θεωρία του φωτοηλεκτρικού φαινομένου.
- 1922 **Niels Bohr** – Βραβείο Νόμπελ για την εκπομπή ηλεκτρομαγνητικών φασμάτων των ατόμων.
- 1923 **De Broglie** – Κυματική φύση σωματιδίων.
- 1923 **Millikan** – Βραβείο Νόμπελ για την πειραματική μελέτη του φωτοηλεκτρικού φαινομένου.
- 1924 Στατιστική **Bose / Einstein** για την διατύπωση της θεωρίας μέτρησης των κβαντικών σωματιδίων.
- 1926 **Schrödinger** – Διατύπωση κυματικής εξίσωσης.
- 1926 Διατύπωση στατιστικής **Fermi / Dirac**.
- 1927 **Heisenberg** – Θεωρία αβεβαιότητας ή απροσδιοριστίας.
- 1927 **Niels Bohr** – Σχολή Κοπεγχάγης και κβαντική θεωρία.
- 1928 **Dirac** – Μελέτη κβαντική για το ηλεκτρόνιο.
- 1929 **Hubble** – Διαστολή σύμπαντος
- 1932 Ανακάλυψη πρωτονίου.
- 1932 **Heisenberg** – Περιγραφή της διάσπασης του ατόμου.

- 1943 **O. Stern** – Βραβείο Νόμπελ για την ανακάλυψη της μαγνητικής ροπής του πρωτονίου.
- 1947 Ανακάλυψη τρανζίστορ.
- 1948 **Feynman** – Θεωρία κβαντικής ηλεκτροδυναμικής (QED).
- 1959 **Feynman** – Πρώτη παρουσίαση νανοτεχνολογίας και σύληψη της ιδέας των κβαντικών υπολογιστών.
- 1960 **Maiman** – Κατασκευή του λέιζερ.
- 1981 **Feynman / MIT university** – Συνέδριο με θέμα την φυσική στην επιστήμη των υπολογιστών.
- 1985 **Deutsch** - Περιγραφή του θεωρητικού καθολικού κβαντικού υπολογιστή
- 1994 **Shor** – Μαθηματικό βραβείο Fields για την παραγοντοποίηση μεγάλων αριθμών πιο γρήγορα από τους κλασσικούς υπολογιστές
- 1996 **Grover** - Αλγόριθμος για την επιτάχυνση εύρεση στοιχείου σε μια μη κατανεμημένη (αταξινόμητη) βάση δεδομένων.
- 2011 **D-Wave** – Εμπορική εκμετάλλευση του μονόλιθου της D-Wave Ins.
- 2012 **Serge Haroche / David J. Wineland** - Βραβείο Νόμπελ

Σήμερα Εντατική Έρευνα ανά τον κόσμο στους κβαντικούς υπολογιστές.

ΠΕΡΙΛΗΨΗ

Η παρούσα μεταπτυχιακή διπλωματική εργασία πραγματεύεται τους κβαντικούς υπολογιστές. Έχει σκοπό την παρουσίαση των πτυχών της τεχνολογίας των κβαντικών υπολογιστών ξεκινώντας από τις βασικές κβαντομηχανικές αρχές που τους διέπουν και καταλήγοντας στο συμπέρασμα της μάλλον αναγκαίας και ίσως αναπόφευκτης δημιουργίας τους στο κοντινό μέλλον.

Οι κβαντικοί υπολογιστές για την ανάπτυξη και υλοποίησή τους, εφαρμόζουν τους νόμους της κβαντικής μηχανικής. Η κβαντική μηχανική είναι ένα από τα σπουδαιότερα επιτεύγματα που ανέπτυξε η ανθρώπινη σκέψη τον προηγούμενο αιώνα και χρησιμοποιήθηκε σε ένα ευρύ φάσμα τεχνολογικών εφαρμογών. Τις τελευταίες όμως δεκαετίες με αφορμή την ολοένα και μεγαλύτερη ανάγκη επεξεργασίας της πληροφορίας για μεγαλύτερο όγκο μεταφοράς δεδομένων και μεγαλύτερη ταχύτητα επεξεργασίας πληροφοριών, έχουν γίνει εκτεταμένες έρευνες από μεγάλα πανεπιστήμια και ιδιωτικές εταιρείες κολοσσούς στον τομέα της πληροφορικής, με αποτέλεσμα να αναδυθεί μια νέα πρωτότυπη και πολλά υποσχόμενη επιστήμη των κβαντικών υπολογιστών.

Η έρευνα για τους κβαντικούς υπολογιστές βασίστηκε στην εξέλιξη της κβαντικής μηχανικής και για την ανάπτυξή της, στηρίχθηκε στις αρχές της κβαντικής θεωρίας μέσω της οποίας ερευνητικά έγιναν αξιόλογες προτάσεις για την δημιουργία υψηλών ταχυτήτων επεξεργασίας δεδομένων. Οι κβαντικοί υπολογιστές άνοιξαν ένα σημαντικό τομέα σύζευξης της φυσικής επιστήμης και των υπολογιστών. Τα Qubits, οι κβαντικοί καταχωρητές καθώς και η αξιοποίηση κβαντικών παραδόξων και αρχών όπως η κβαντική υπέρθεση και η κβαντική διεμπλοκή οδήγησε στην δημιουργία των κβαντικών υπολογισμών με την χρήση των qubits των καταχωρητών και των κβαντικών πολών.

Η χρήση λοιπόν των κβαντικών υπολογιστών προσφέρει αφ' ενός υψηλές ταχύτητες μεταφοράς δεδομένων και ασφαλείς επικοινωνίες με την κβαντική κρυπτογραφία, αφ' ετέρου όμως συνοδεύεται και από ανεπιθύμητα εμπόδια όπως αλληλεπιδράσεις μεταξύ των κβαντικών καταχωρητών που δημιουργούν σφάλματα.

Οι κβαντικοί υπολογιστές ανοίγουν ένα νέο πεδίο εξέλιξης και εφαρμογών που έχει να κάνει με τον τρόπο και τα υλικά κατασκευής τους, ώστε να καταστούν προσφιλείς και εύκολοι στην χρήση τους για το ευρύ κοινό, όπως έγινε με την χρήση

των προσωπικών κλασσικών υπολογιστών, αποφεύγοντας προβλήματα υπερθέρμανσης και σφαλμάτων λειτουργίας κατά την διάρκεια χρήσης των κβαντικών υπολογιστών.

Στον κλάδο των υπολογιστών με οδηγό την κβαντική φυσική, μελετήθηκαν και αναπτύχθηκαν κβαντικά κυκλώματα, κβαντικές πύλες, κβαντικοί υπολογισμοί, κβαντική κρυπτογραφία. Αυτό οδηγεί όλο και περισσότερους φυσικούς σε ερευνητική ενασχόληση στο αντικείμενο των κβαντικών υπολογιστών. Άλλωστε η έρευνα που γίνεται είναι ιδιαίτερα πληθωρική και το 2012 το βραβείο Νόμπελ κατέληξε στους Serge Haroche (από την Γαλλία) και David J. Wineland (από την Αμερική) οι οποίοι βρήκαν τρόπους για να μετρούν κβαντικά σωματίδια χωρίς να τα καταστρέφουν, κάτι που μέχρι τότε θεωρούνταν αδύνατο [51]. Η Σουηδική Βασιλική Ακαδημία Επιστημών που απένειμε το βραβείο Νόμπελ διατύπωσε την άποψη πως με την δουλειά των βραβευθέντων μπορεί να οδηγηθούμε στην ολοκληρωτική κατασκευή ενός νέου είδους υπολογιστή, εξαιρετικά γρήγορου που θα είναι βασισμένος στην κβαντική φυσική και ίσως ο κβαντικός ηλεκτρονικός υπολογιστής να αλλάξει την καθημερινή μας ζωή, τον αιώνα που διανύουμε, με τον ίδιο ριζικό τρόπο που την άλλαξε ο κλασικός ηλεκτρονικός υπολογιστής τον περασμένο αιώνα [51].

Η διπλωματική εργασία αποτυπώνει τα σημαντικά στοιχεία που στοιχειοθετούν σήμερα την δομή των κβαντικών υπολογιστών ξεκινώντας από τις γενικές αρχές, κανόνες και το μαθηματικό πλαίσιο που αποτελούν την κβαντική θεωρία και έπειτα παρουσιάζονται οι δομές, οι τεχνολογίες, τα κυκλώματα, οι πύλες, οι υπολογισμοί, οι αλγόριθμοι και η κρυπτογραφία που έχουν αναπτυχθεί με την ερευνητική αξιοποίηση των κβαντικών υπολογιστών. Το ερώτημα που δημιουργείται είναι αν η υλοποίησή τους θα γίνει άμεσα τα επόμενα χρόνια ή θα πρέπει να περάσει μία ή περισσότερες δεκαετίες προκειμένου αυτό που έλαβε χώρα πριν λίγα χρόνια με την πώληση του πρώτου κβαντικού υπολογιστή της Καναδικής εταιρείας D-Wave, να γίνει για το απλό εταιρικό και καταναλωτικό κοινό διαθέσιμο για προσωπική ή επαγγελματική χρήση.

ABSTRACT

This project presents quantum computers. The purpose of this project is to present the technology of quantum computers starting from the basic principles of quantum mechanical principles that govern them and concluding that the creating of quantum computers will be necessary and perhaps inevitable creation in the near future.

For the development of quantum computers is necessary the use of quantum mechanics. Quantum mechanics is one of the greatest achievements that human has developed in the last century and has been used in a wide range of technological applications. The last decades, because of the need to elaborate greater data base, extensive research by major universities and private companies have taken place in IT. As a result, a new very promising science of quantum computers has developed.

Quantum computers research was based on the development of quantum mechanics and on the principles of quantum theory whereby research made valuable suggestions for the creation of high speed data processing. Quantum computers have opened an important field coupling of physics and computer science. The qubits, quantum registers and the use of quantum paradoxes and principles such as quantum superposition and quantum entanglement led to the creation of quantum calculations using the registers of qubits and quantum gates.

The use of quantum computers therefore offers one part high speed data transfer and secure communications with quantum cryptography, on the other hand, however, is accompanied by unwanted obstacles such as interactions between quantum registers which generate errors.

Quantum computers open a new field of development and applications that is related to the way and materials, in order to become cherished and easy to use for the general public, as was the use of conventional personal computers, avoiding overheating problems and malfunctions during use of quantum computers.

In the field of computer-driven quantum physics, quantum circuits, quantum gates, quantum calculations, quantum cryptography have been studied and developed. This leads to more and more physical involvement in research in the subject of quantum computers. After all the research that takes place is very circumstantial and in 2012 Nobel Prize went to Serge Haroche (from France) and David J. Wineland (from America) who found ways to measure quantum particles

without damaging them, which until then thought to be impossible [51]. The Royal Swedish Academy of Sciences who awarded the Nobel Prize, took the view that the work of the laureates can lead to the complete construction of a new kind of computer, extremely fast, which will be based on quantum physics and perhaps the quantum computer will change our daily life in this century, in the same way that it was changed by the classic computer last century. [51].

This project captures the important elements that constitute today the structure of quantum computers starting from general principles, rules and mathematical framework that form the quantum theory, and presents also, the structures, technologies, circuits, gates, calculations, algorithms and cryptography developed by the research use of quantum computers.

ΕΙΣΑΓΩΓΗ

Το κίνητρο για την συγγραφή της συγκεκριμένης μεταπτυχιακής διπλωματικής εργασίας προέκυψε από τις ελπιδοφόρες ενδείξεις πανεπιστημίων και ερευνητικών ομάδων υψηλής τεχνολογίας σε πολλές χώρες του εξωτερικού, οι οποίες οδηγούν στην δημιουργία και αξιοποίηση των κβαντικών υπολογιστών και αποτυπώνουν ένα νέο τρόπο λειτουργίας αρκετά διαφορετικό από αυτό των κλασικών υπολογιστών και πολύ ελπιδοφόρο, με τεράστιες δυνατότητες επεξεργασίας δεδομένων. Στην χώρα μας αυτή η ερευνητική προσπάθεια δεν έχει βρει πρόσφορο έδαφος ίσως γιατί το αντικείμενο είναι ιδιαίτερα εξειδικευμένο και απαιτεί γνώσεις κβαντικής μηχανικής σε συνδυασμό με χρήση κανόνων πληροφορικής. Οι ενδείξεις από πανεπιστήμια του εξωτερικού οδηγούν στο άμεσο μέλλον, στην εκμάθηση και παρουσίαση των κβαντικών υπολογιστών σε πανεπιστήμια και σχολές θετικών επιστημών και δεν είναι υπερβολή να πούμε πως είναι προ των πυλών ένας νέος κλάδος επιστήμης που συνδέει την φυσική με την πληροφορική.

Η εργασία αποτελείται από δύο μέρη. Το πρώτο δίνει έμφαση στην ανάπτυξη της κβαντικής θεωρίας τονίζοντας τις βασικές αρχές και κανόνες του μαθηματικού φορμαλισμού και πλαισίου της κβαντικής μηχανικής. Συγκεκριμένα στο πρώτο κεφάλαιο παρουσιάζεται η παλαιά κβαντική θεωρία αναφέροντας αυτά που ανέπτυξαν οι θεμελιωτές της κβαντικής επιστήμης και που έδωσαν την ώθηση για την ανάπτυξη της φυσικής και των τεχνολογικών εφαρμογών (π.χ. δημιουργία τρανζίστορ) των αιώνων που μας πέρασε. Στο δεύτερο κεφάλαιο παρουσιάζεται το γενικό πλαίσιο και οι βασικές αρχές μέσα από την μαθηματική θεμελίωση της κβαντικής μηχανικής. Επίσης στο τρίτο και τελευταίο κεφάλαιο του πρώτου μέρους αναλύονται τα κβαντικά παράδοξα τα οποία αποτελούν αναπόσπαστο μέρος και βάση για την ανάπτυξη της λειτουργίας των κβαντικών υπολογιστών.

Στο δεύτερο και σπουδαιότερο μέρος της διπλωματικής εργασίας παρουσιάζεται μια πλήρη εικόνα όλων των καινοτομιών και τρόπου λειτουργίας, επεξεργασίας, δομής και πλεονεκτημάτων τόσο στην κρυπτογραφία όσο και στην απεριόριστη επεξεργασία δεδομένων πληροφορίας των κβαντικών υπολογιστών, σε σχέση με τους κλασσικούς. Συγκεκριμένα στο τέταρτο κεφάλαιο υπάρχει μια παρουσίαση του κβαντικού καταχωρητή και επεξεργαστή με σκοπό την εισαγωγή και κατανόηση της λειτουργίας των κβαντικών υπολογιστών. Στο πέμπτο κεφάλαιο

αποδίδονται οι τεχνολογικές καινοτομίες και οι τεχνολογικοί τρόποι κατασκευής. Στο επόμενο κεφάλαιο υπάρχει μια πλήρης μελέτη και παρουσίαση των κβαντικών πυλών που χρησιμοποιούν οι κβαντικοί υπολογιστές για να πραγματοποιήσουν τους υπολογισμούς τους. Επίσης στο 7^ο κεφάλαιο αναπτύσσονται τα κβαντικά κυκλώματα με υποδειγματικά λυμένα παραδείγματα λειτουργίας τους. Επίσης στο όγδοο κεφάλαιο εξηγούνται οι κβαντικοί αλγόριθμοι και δίνεται ιδιαίτερη έμφαση στον αλγόριθμο του Deutsch και Grover. Τέλος στο τελευταίο κεφάλαιο αποτυπώνεται η κβαντική κρυπτογραφία και δίνονται παραδείγματα της σπουδαιότητας και σημαντικότητας της μέσω του αλγορίθμου του Shor, που μάλλον θα προσφέρει στο μέλλον όταν καταστεί δυνατή η εκτεταμένη χρήση των κβαντικών υπολογιστών και της κβαντικής κρυπτογραφίας ασφαλείς από εξωτερικούς εισβολείς, επικοινωνίες.

Στα παραρτήματα παρουσιάζονται μαθηματικά εργαλεία, φυσικές σταθερές και ένας συγκριτικός πίνακας των κβαντικών πυλών. Η υλοποίηση της εργασίας έγινε με χρήση εκτεταμένων πηγών οι οποίες αναγράφονται αναλυτικά στην βιβλιογραφία. Συγκεκριμένα έγινε αξιοποίηση επιστημονικών δημοσιευμένων paper σε τομείς έρευνας των κβαντικών υπολογιστών με αντικείμενο μελέτης ανάλογου των περιεχομένων των κεφαλαίων της εργασίας (4 έως 9). Επίσης υποστηρικτικό υλικό αντλήθηκε και από την Ελληνική βιβλιογραφία, από site τεχνολογίας και από κάθε διαδικτυακή πηγή που προσφέρει χρήσιμες επιστημονικές πληροφορίες (όπως αυτές που αναγράφονται στην βιβλιογραφία στο τέλος της εργασίας). Τέλος θα ήθελα να ευχαριστήσω τον Θ. Καμαλάκη και όσους με υποστήριξαν για την ολοκλήρωση αυτής της εργασίας.

Ο αναγνώστης μετά από ουσιώδη μελέτη της μεταπτυχιακής διπλωματικής εργασίας θα είναι σε θέση να αποδίδει τις βασικές αρχές λειτουργίας των κβαντικών υπολογιστών και να υλοποιεί κβαντικούς υπολογισμούς για κυκλώματα και περιπτώσεις κρυπτογραφίας ενώ θα μπορεί και να αξιολογήσει όλα τα δεδομένα που θα παρουσιάζονται σε βάθος χρόνου τα προσεχή χρόνια και δεκαετίες σχετικά με την εξέλιξη και την αξιοποίηση των κβαντικών υπολογιστών από ερευνητικές ομάδες και περιπτώσεις εργασιών.

ΜΕΡΟΣ Α΄

ΚΒΑΝΤΙΚΗ ΘΕΩΡΙΑ

*Η παιδεία γενικά,
η αναζήτηση της αλήθειας και της ομορφιάς,
είναι πεδία που μας επιτρέψανε να μείνουμε
παιδιά σε όλη τη ζωή.*

Άλμπερτ Αϊνστάιν

ΚΕΦΑΛΑΙΟ 1^ο

Η ΠΑΛΑΙΑ ΚΒΑΝΤΙΚΗ ΘΕΩΡΙΑ

1.1 ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΒΑΝΤΙΚΗ ΘΕΩΡΙΑ

Η ανάπτυξη της κβαντικής μηχανικής χωρίζεται σε δύο χρονικές περιόδους. Από τα τέλη του 19^{ου} αιώνα μέχρι το 1923 – η λεγόμενη περίοδος της παλαιάς κβαντικής θεωρίας- και από το 1923 μέχρι σήμερα με την επιστήμη της κβαντικής μηχανικής να έχει εισέλθει δυναμικά στην επιστήμη των υπολογιστών.

Ο όρος quantum προέρχεται από την αντίστοιχη λατινική λέξη που ερμηνεύεται ως το «ποσό» ή «η μικρή ποσότητα» και αναφέρεται σε ποσότητες ενός φυσικού μεγέθους οι οποίες παίρνουν διακριτές τιμές. Η κβαντική θεωρία αποτελεί βασικό συστατικό κάθε θεωρίας που έχει να κάνει με τον μικρόκοσμο.

Η κβαντική μηχανική υπερκεράζει την κλασσική μηχανική και δίνει εξηγήσεις σε πληθώρα επιστημονικών πεδίων όπως χαρακτηριστικά, της κυματοσωματιδιακής δομής της ύλης, της κβάντωσης των φυσικών μεγεθών κ.α.

1.2 Ο ΚΥΜΑΤΟΣΩΜΑΤΙΔΙΑΚΟΣ ΧΑΡΑΚΤΗΡΑΣ ΤΗΣ ΥΛΗΣ ΚΑΙ Η ΔΙΤΤΗ ΦΥΣΗ ΤΟΥ ΦΩΤΟΣ

Ο **James Clerk Maxwell**, απέδειξε ότι το φως είναι εγκάρσια ηλεκτρομαγνητικά κύματα. Οι **Tomas Young** και **Christian Huygens** μέσα από πειραματικές εφαρμογές έδειξαν πως το φως έχει κυματική φύση με μορφή εγκάρσιων κυμάτων. Ο **Albert Einstein** διατύπωσε πως η διάδοση του φωτός πραγματοποιείται σε μικρά πακέτα ενέργειας τα οποία καλούνται φωτόνια ή κβάντα (δηλαδή quantum, που σημαίνει «ποσό»). Τα σωματίδια αυτά έχουν ενέργεια που είναι αναλογική με την συχνότητα επί την σταθερά του **Planck** h ($h=6,626 \cdot 10^{-34}$ J · sec) [2]. Η ενέργεια τους είναι ίση με

$$E = h \cdot f$$

Τα φωτόνια διαδίδονται με την ταχύτητα του φωτός ($c=3 \cdot 10^8 \frac{m}{s}$) και έχουν μηδενική μάζα ηρεμίας. Η συχνότητα τους f θα είναι ανάλογη του μήκους κύματος λ :

$$\lambda = \frac{c}{f} \Leftrightarrow f = \frac{c}{\lambda}.$$

Η ενέργεια των φωτονίων θα είναι:

$$E = hf = h \frac{c}{\lambda} \Rightarrow E = \frac{hc}{\lambda}$$

Επίσης η ορμή τους θα είναι ανάλογη της ενέργειας:

$$p = \frac{E}{c} = \frac{\frac{hc}{\lambda}}{c} = \frac{h}{\lambda} \Rightarrow p = \frac{h}{\lambda}$$

Αν μάλιστα εισάγουμε ένα κυματικό αριθμό ίσο με $k = \frac{2\pi}{\lambda}$, και με γνωστό ότι $\hbar = \frac{h}{2\pi}$

(η **ανηγμένη σταθερά του Planck, παράρτημα Β'**), τότε η ορμή γίνεται ίση με

$$p = \frac{h}{\lambda} = \frac{\hbar 2\pi}{\frac{2\pi}{k}} \Rightarrow p = \hbar \cdot k$$

Το φως έχει ταυτόχρονα σωματιδιακό και κυματικό χαρακτήρα. Η **κβαντική ηλεκτροδυναμική -Quantum electrodynamics, QED-** τις πρώτες δεκαετίες του 20^{ου} αιώνα, επικύρωσε πλήρως την διττή φύση του φωτός. Η σωματιδιακή φύση του φωτός εκδηλώνεται πλήρως σε φαινόμενα αλληλεπίδρασης της ύλης με το φως (όπως συμβαίνει με το φωτο-ηλεκτρικό φαινόμενο) [2]. Η κυματική φύση του φωτός

εκδηλώνεται σε φαινόμενα περίθλασης και συμβολής. Στην **ειδική θεωρία της σχετικότητας** η ενέργεια ενός φωτονίου θα είναι ίση με

$$E^2 = (pc)^2 + (mc^2)^2 \Rightarrow E = \sqrt{(pc)^2 + (mc^2)^2}.$$

Τα φωτόνια όμως έχουν μηδενική μάζα ηρεμίας, $m=0$. Τότε από την ενέργεια της σχετικότητας προκύπτει ότι

$$E^2 = (pc)^2 + (mc^2)^2 \stackrel{m=0}{\Rightarrow} E = pc \Rightarrow p = \frac{E}{c}.$$

Η ενέργεια επομένως κάθε ηλεκτρομαγνητικού κύματος είναι κβαντωμένη δηλαδή υλοποιείται σε πακέτα -κβάντα- φωτός ή φωτόνια. Τα κυματοσωματιδιακά χαρακτηριστικά κάθε φωτονίου δίνονται από την σχέση

$$E = h \cdot f \text{ και } E = pc$$

Στην **κλασσική φυσική** δε, ένα φωτόνιο με κυματοσωματιδιακό χαρακτήρα μάζας m , και ατομικό αριθμό z , θα έχει ενέργεια ανάλογη της κινητικής και της δυναμικής του, ίση με

$$E = T + V = \frac{p^2}{2m} + \frac{z^2 e}{r}.$$

Νωρίτερα από τον Αϊνστάιν ο **Max Planck** διατύπωσε [2], πως κάθε σύστημα έχει ενέργεια ίση με $E = nhf$. Σύμφωνα με την κβαντική θεωρία του, το φως εκπέμπεται και απορροφάται από τα άτομα της ύλης «ασυνεχώς». Από το άτομο δεν εκπέμπονται με συνεχή τρόπο κύματα αλλά φωτόνια τα οποία χαρακτηρίζονται από μία συχνότητα και μία συγκεκριμένη ποσότητα ενέργειας. Δηλαδή το φως δεν μπορεί από την στιγμή που έχει κυκλική συχνότητα και μεταβάλλεται περιοδικά να πάρει οποιαδήποτε τιμή ενέργειας. Η ενέργειά του θα έχει πάντα διακριτή τιμή [2]. Θα είναι

$$E = nhf = nh \frac{\omega}{2\pi} = \hbar \omega \Rightarrow E = \hbar \omega$$

όπου $\hbar = \frac{h}{2\pi}$, ω η κυκλική συχνότητα και n ο κβαντικός αριθμός (θετικές ακέραιες τιμές) $n = 1, 2, 3, \dots$

Καταλήγουμε με τον πιο σαφή τρόπο, **πως το φως εκτός από κυματική έχει και σωματιδιακή υφή και χαρακτήρα**. Η ενέργεια των ηλεκτρομαγνητικών κυμάτων όπως προαναφέρθηκε είναι εκφρασμένη σε πακέτα ενέργειας τα φωτόνια ή κβάντα φωτός.

Ο **De Broglie** διατύπωσε τον κυματικό χαρακτήρα της κίνησης της ύλης, σύμφωνα με τον οποίο ένα σωματίδιο έχει μήκος κύματος λ και συχνότητα f όταν το σωματίδιο είναι μάζας m και διαθέτει ενέργεια E και ορμή p . Διατύπωσε πως τα φωτόνια συμπεριφέρονται ως σωματίδια και υλικά κύματα. Η ορμή για ένα φωτόνιο με ενέργεια E θα είναι

$$p = \frac{E}{c} = \frac{\frac{hc}{\lambda}}{c} = \frac{h}{\lambda}.$$

Σωματίδια με ορμή p και ενέργεια E , έχουν μήκος κύματος λ , ίσο με $\lambda = \frac{h}{p}$. Επίσης έχουν και συχνότητα f , που δίνεται ίση με

$$E = hf \Leftrightarrow f = \frac{E}{h}.$$

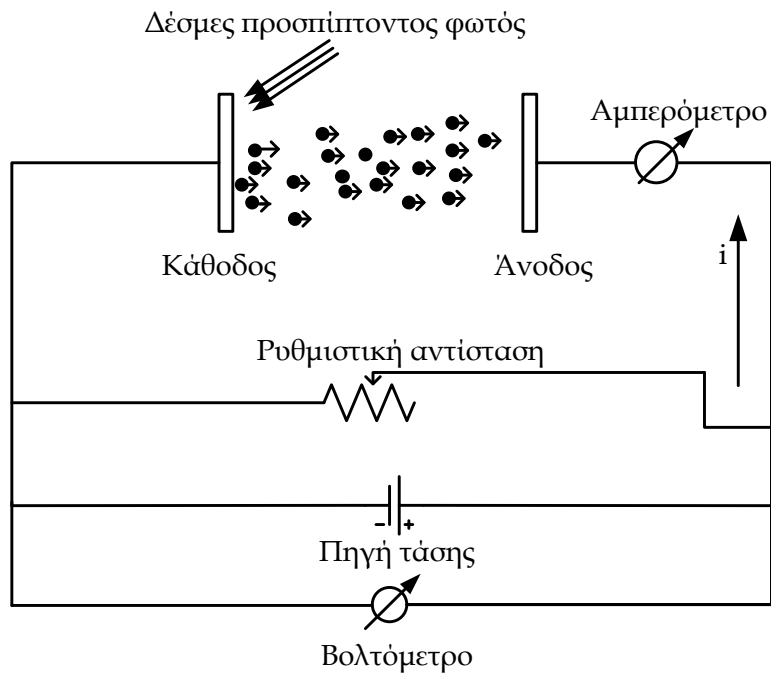
1.3 ΦΩΤΟΗΛΕΚΤΡΙΚΟ ΦΑΙΝΟΜΕΝΟ

Όταν φως προσπίπτει πάνω σε μεταλλικές επιφάνειες, εκπέμπονται από αυτές ηλεκτρόνια και αυτό ονομάζεται φωτοηλεκτρικό φαινόμενο. Τα ηλεκτρόνια που ελευθερώνονται κατά την πρόσπτωση, απορροφούν ενέργεια από την προσπίπτουσα ακτινοβολία και μπορούν έτσι να διαφύγουν από το εσωτερικό του μεταλλικού αγωγού υπερπηδώντας το φράγμα δυναμικής ενέργειας [2]. Το φωτοηλεκτρικό φαινόμενο παρατηρήθηκε για πρώτη φορά από τον **Herz**, αλλά η αλληλεπίδραση του φωτός με την ύλη ερμηνεύτηκε και εξηγήθηκε πλήρως από τον **Albert Einstein** (βραβείο νόμπελ φυσικής 1921) για την μελέτη του πάνω στο φαινόμενο [2].

Ένα φωτόνιο απορροφάται από ένα ηλεκτρόνιο και το ηλεκτρόνιο παίρνει όλη την ενέργεια του φωτονίου. Ένα μέρος της ενέργειας προσφέρεται για την διαφυγή από την επιφάνεια του μετάλλου δηλαδή για την εξουδετέρωση του έργου εξαγωγής W , ενώ το υπόλοιπο γίνεται κινητική ενέργεια του ηλεκτρονίου που εξέρχεται από το μέταλλο. Η μέγιστη κινητική ενέργεια $\frac{1}{2}mv^2$ που έχει το εκπεμπόμενο ηλεκτρόνιο είναι ανάλογη του έργου εξαγωγής W και της ενέργειας $E=hf$ που πήρε το ηλεκτρόνιο από το φωτόνιο.

Ισχύει επομένως ότι

$$E = W + \frac{1}{2}mv^2 \Rightarrow hf = W + \frac{1}{2}mv^2 \Rightarrow hf - W = \frac{mv^2}{2}$$



Σχήμα 1.1 [2]

Η **ελάχιστη συχνότητα** $f_{\min}$, που έχει ένα φωτόνιο ώστε αυτό να προκαλέσει την εκπομπή ενός φωτοηλεκτρονίου καλείται **συχνότητα κατωφλίου** [2] και είναι ίση με

$$hf_{\min} = W \Rightarrow f_{\min} = \frac{W}{h}$$

Δυναμικό αποκοπής V_o καλούμε την τιμή της αντιστροφής τάσης που διακόπτει εντελώς την ροή των ηλεκτρονίων, δηλαδή την δυναμική ενέργεια των ηλεκτρονίων [2]. Η τάση αυτή γίνεται επομένως ίση με την κινητική ενέργεια των ηλεκτρονίων και είναι

$$K_{\max} = \frac{1}{2}mv^2 = eV_o.$$

Ισοδύναμα δυναμικό αποκοπής V_o γίνεται [2]:

$$hf = K_{\max} + W \Rightarrow hf = eV_o + W \Rightarrow$$

$$V_o = \frac{hf}{e} - \frac{W}{e}.$$

1.4 ΑΡΧΗ ΤΗΣ ΑΒΕΒΑΙΟΤΗΤΑΣ

Στην κλασσική μηχανική το σημειακό σωματίδιο υπολογίζεται με μεγάλη ακρίβεια κάθε χρονική στιγμή σε όλες τις χωρικές συντεταγμένες. Στην **κβαντική μηχανική** όμως δεν μπορεί να υπολογιστεί με μεγάλη ακρίβεια ταυτόχρονα, η θέση και η ορμή ενός σωματιδίου. Αυτή την αδύνατη μέτρηση, ταυτόχρονα της ορμής και της θέσης, έρχεται ο Heisenberg και την εισαγάγει ως αρχή της αβεβαιότητας (ή αρχή της απροσδιοριστίας). Η αρχή της αβεβαιότητας του Heisenberg διατυπώνεται με την ανισότητα [2]

$$\Delta x \Delta p_x \geq \frac{\hbar}{2}$$

και αναφέρει πως η μέτρηση σωματιδίου με κυματοσωματιδιακό χαρακτήρα, ως προς την θέση του με σφάλμα υπολογισμού Δx και ως προς την ορμή του με σφάλμα υπολογισμού Δp , δίνει γινόμενο και των δύο σφαλμάτων που δεν μπορεί να υστερεί του αριθμού $\hbar = \frac{h}{2\pi}$ ώστε να είναι $\Delta x \Delta p_x \geq \frac{\hbar}{2}$. Η ανισότητα ουσιαστικά είναι μια αποτύπωση της διττής φύσης (κυματοσωματιδιακού χαρακτήρα) της ύλης.

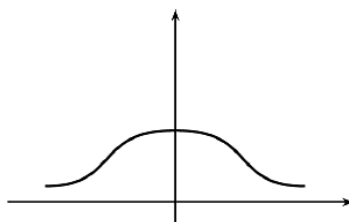
Παρατηρήσεις:

■ Διαφορετικός τρόπος έκφρασης της αρχή της αβεβαιότητας του Heisenberg μπορεί να γίνει με την ενέργεια και τον χρόνο ώστε να πάρει την μαθηματική μορφή της ανισότητας

$$\Delta E \Delta t \geq \frac{\hbar}{2}$$

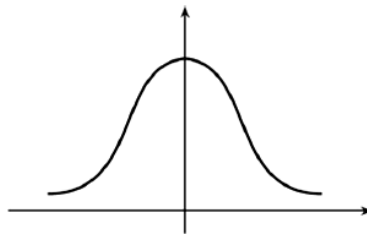
κάτι που οδηγεί στο συμπέρασμα ότι και η ενέργεια έχει έμφυτη απροσδιοριστία στον υπολογισμό της. Όσο μεγαλύτερος είναι ο χρόνος ζωής μιας ενεργειακής κατάστασης τόσο μικρότερη είναι η καθορισμένη ενέργεια. Αντίθετα για μικρό χρονικό διάστημα η αβεβαιότητα στην ενέργεια είναι μεγαλύτερη. Επίσης αν $\Delta t=0$ τότε $\Delta E \rightarrow \infty$ και αντιστρόφως αν η ενέργεια είναι πλήρως καθορισμένη ώστε $\Delta E=0$ τότε έχουμε άπειρο χρόνο ζωής $\Delta t \rightarrow \infty$ για την ενεργειακή στάθμη [2].

■ Όταν το Δx είναι μεγάλο και το Δp_x μικρό η μορφή της κυματοσυνάρτησης θα είναι φαρδιά και κοντή όπως στο επόμενο σχήμα [2].



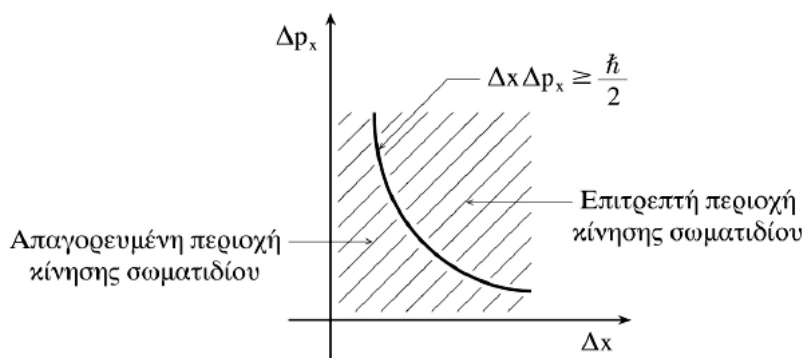
Σχήμα 1.2 [2]

■ Όταν το Δx είναι μικρό και το Δp_x μεγάλο η μορφή της κυματοσυνάρτησης θα είναι στενή και ψηλή όπως στο επόμενο σχήμα [2].



Σχήμα 1.3 [2]

■ Η αδύνατη μέτρηση ταυτοχρόνως της ορμής και θέσης ενός σωματιδίου που διατυπώνεται από την αρχή της αβεβαιότητας φαίνεται στο επόμενο σχήμα [2].



Σχήμα 1.4 [2]

1.5 ΤΟ ΠΡΟΤΥΠΟ ΤΟΥ BOHR

Οι κβαντικοί κανόνες σύμφωνα με τους Bohr και Sommerfeld αναφέρουν πως οι περιοδικές τροχιές είναι επιτρεπόμενες μόνο από το ολοκλήρωμα που περικλείει σε μια κλειστή διαδρομή τροχιάς στα όρια κίνησης, μία δράση ακέραιο πολλαπλάσιο της σταθεράς του Planck [2] κατά τέτοιο τρόπο ώστε να ισχύει για το ολοκλήρωμα της τροχιάς δράσης ότι

$$\oint p_q dq = nh$$

Το ολοκλήρωμα μπορεί να γραφεί και ως $\oint p_\theta d\theta = nh$, αλλάζοντας την μεταβλητή της ορμής στα όρια της κίνησης [2].

Μάλιστα μπορούμε να καταλήξουμε για μελέτη κίνησης της στροφορμής ενός υδρογονοειδούς συστήματος του οποίου τα πρωτόνια του πυρήνα έλκουν ένα ηλεκτρόνιο της εξωτερικής στιβάδας, πως η στροφορμή του είναι ίση με:

$$\oint p_\theta d\theta = nh \Rightarrow \oint L d\theta = nh \Rightarrow L \oint d\theta = nh \Rightarrow L 2\pi = nh \Rightarrow L = n \frac{h}{2\pi} \Rightarrow L = n\hbar.$$

Καταλήγουμε στο συμπέρασμα επομένως ότι η στροφορμή είναι κβαντωμένη ώστε

$$L = n\hbar$$

Στο άτομο κατά τον **Rutherford** ο πυρήνας έχει διάμετρο μήκους 10^{-18} cm και περιστρέφεται γύρω από αυτόν το ηλεκτρόνιο διαγράφοντας τροχιά διαμέτρου μήκους 10^{-8} cm που είναι και η έκταση που καταλαμβάνει το άτομο [2]. Για να προσδιορίσουμε την θέση του ηλεκτρονίου κάνουμε χρήση των μεταβλητών r και θ στις οποίες αντιστοιχούμε την ακτινική ορμή p_r και την στροφορμή p_θ αντίστοιχα [2]. Η ολική ενέργεια στα κλασσικά πλαίσια είναι

$$E = T + V = \frac{1}{2m} (p_r^2 + \frac{p_\theta^2}{r^2}) - \frac{e^2}{r}.$$

Όμως επειδή οι δυνάμεις που ασκούνται είναι κεντρικές θα είναι $p_\theta = L = \text{σταθ.}$. Στην απλή κυκλική τροχιά του ηλεκτρονίου δεν έχουμε p_r καθότι έχουμε σταθερή ακτίνα $r=R$. Τότε η ενέργεια στα κλασσικά πλαίσια θα γίνει

$$E = \frac{1}{2m} \frac{L^2}{R^2} - \frac{e^2}{R}.$$

Από το **θεώρημα Virial** όμως γνωρίζουμε ότι η κινητική ενέργεια είναι ανάλογη της δυναμικής και μάλιστα ίση με $T = -\frac{V}{2}$ ή $2T + V = 0$.

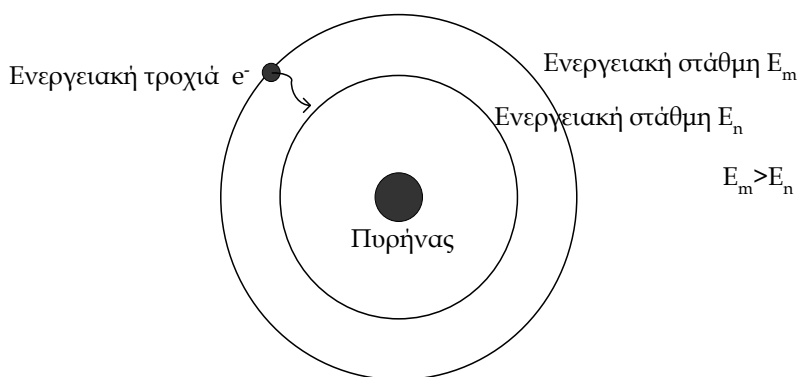
Αν εξετάσουμε κλασσικά την ενέργεια με την βοήθεια του θεωρήματος Virial θα έχουμε ότι

$$E = T + V = -\frac{V}{2} + V = \frac{1}{2}V = \frac{1}{2}\left(-\frac{e^2}{R}\right).$$

Οπότε καταλήγουμε στην κλασσική έκφραση της ενέργειας $E = -\frac{e^2}{2R}$. Αυτό το σημείο καλείται να βελτιώσει η παρέμβαση του Bohr θεωρώντας την στροφορμή κβαντωμένη ώστε να παίρνει συγκεκριμένες μόνο τιμές [2].

■ Οι συνθήκες της θεωρίας του Bohr [2]:

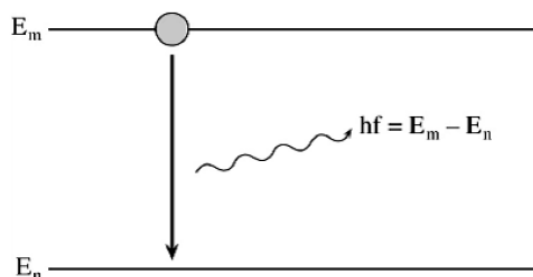
► Η πρώτη συνθήκη ορίζει ότι ακτινοβολία των φωτονίων που εκπέμπεται είναι κβαντωμένη. Ακτινοβολία εκπέμπεται σε μη στάσιμες καταστάσεις. Κατά την μετάπτωση ατόμων από μια ενεργειακή στάθμη μεγαλύτερης ενέργειας (E_m) σε μία άλλη μικρότερης (E_n), εκπέμπεται ακτινοβολούμενη ενέργεια, όπου με βάση την αρχή διατήρησης της ενέργειας, είναι ίση με $E = E_m - E_n$.



Σχήμα 1.5

Με γνωστό ότι $E = hf$, προκύπτει τελικά ότι

$$hf = E_m - E_n$$



Σχήμα 1.6 [2]

Όπως αποτυπώνεται στα προηγούμενα σχήματα 1.5 και 1.6, η ακτινοβολία εκπέμπεται μόνο για μετάπτωση από μια ανώτερη ενεργειακή στάθμη (E_m), σε μια κατώτερη ενεργειακή στάθμη (E_n) [2]. Ισχύει επομένως ότι η συχνότητα της ακτινοβολίας που απορροφάται ή εκπέμπεται για μεταπτώσεις ενεργειακών σταθμών μικρότερης ενέργειας είναι ίση με

$$hf = E_m - E_n \Rightarrow hf = \Delta E \Rightarrow f = \frac{\Delta E}{h}$$

► Η δεύτερη συνθήκη ορίζει τις επιτρεπόμενες κυκλικές τροχιές του ηλεκτρονίου. Το ηλεκτρόνιο κινείται σε διακριτές επιτρεπόμενες κυκλικές τροχιές γύρω από τον πυρήνα, για τις οποίες η στροφορμή είναι κβαντωμένη και είναι ακέραιο πολλαπλάσιο της σταθεράς του Planck. Δηλαδή

$$L = mvr = n\hbar$$

όπου ο n είναι ο κύριος κβαντικός αριθμός ίσος με $n=1,2,3,\dots$

Μελετώντας την κίνηση του ηλεκτρονίου γύρω από τον πυρήνα μπορούμε να εξάγουμε την ενέργεια που θα έχει για διάφορες επιτρεπτές διακριτές τροχιές γύρω από αυτόν. Το ηλεκτρόνιο εκτελεί κυκλική κίνηση καθορισμένης ακτίνας r σε ορισμένες όμως τροχιές γύρω από τον πυρήνα, λόγω της ηλεκτρικής δύναμης Coulomb η οποία παίζει ρόλο κεντρομόλου δύναμης [2]. Ισχύει επομένως ότι

$$F_C = F_K \Rightarrow \frac{ze^2}{r_n^2} = \frac{mv_n^2}{r_n} \Rightarrow mv_n^2 = \frac{ze^2}{r_n} \quad 1.1$$

Όμως για την στροφορμή ισχύει

$$L = mv_n r_n = n\hbar \Rightarrow v_n = \frac{n\hbar}{mr_n} \quad 1.2$$

Αντικαθιστώντας στην σχέση 1.1 την σχέση 1.2 προκύπτει ότι

$$mv_n^2 = \frac{ze^2}{r_n} \Rightarrow m \frac{n^2 \hbar^2}{m^2 r_n^2} = \frac{ze^2}{r_n} \Rightarrow r_n = \frac{n^2 \hbar^2}{me^2 z}$$

Οπότε και η ταχύτητα γίνεται ίση με

$$v_n = \frac{n\hbar}{mr_n} = \frac{n\hbar}{m \frac{n^2 \hbar^2}{me^2 z}} \Rightarrow v_n = \frac{e^2 z}{n\hbar}.$$

Η ολική ενέργεια είναι $E_n = T + V$, οπότε προκύπτει ότι [2] :

$$E_n = \frac{1}{2} mv_n^2 - \frac{ze^2}{r_n} \Rightarrow E_n = \frac{1}{2} m \left(\frac{e^2 z}{n\hbar} \right)^2 - \frac{ze^2}{\frac{n^2 \hbar^2}{me^2 z}} = \frac{1}{2} \frac{me^4 z^2}{n^2 \hbar^2} - \frac{mz^2 e^4}{n^2 \hbar^2} \Rightarrow E_n = -\frac{mz^2 e^4}{2n^2 \hbar^2}$$

Τελικά η ενέργεια για διάφορες τιμές ενεργειακών σταθμών θα είναι

$$E_n = -\frac{1}{n^2} \frac{mz^2 e^4}{2\hbar^2} \Rightarrow E_n = -\frac{z^2 13,6}{n^2} \text{eV}$$

όπου n κύριος κβαντικός αριθμός ($n=1,2,3\dots$).

Κατά τον Bohr λοιπόν ακτινοβολία έχουμε όταν μεταπηδά ένα ηλεκτρόνιο από μεγαλύτερη ενεργειακή στάθμη σε χαμηλότερη ενεργειακή στάθμη. Μέσω της ενέργειας που εκπέμπεται ($hf = E_m - E_n$), έχουμε ένα πλήθος συχνοτήτων που μπορούν να καθοριστούν από τα m και n (με $m > n$) [2].

Οι συχνότητες εκπομπής είναι

$$f_{\min} = \frac{E_m - E_n}{h}$$

και επειδή υπολογίστηκε ότι $E_n = -\frac{1}{n^2} \frac{me^4}{2\hbar^2}$, τότε αντικαθιστώντας προκύπτει ότι

$$f_{\min} = \frac{E_m - E_n}{h} \Rightarrow \frac{1}{\lambda_{\min}} = -\frac{me^4}{4\pi\hbar^3} \left(\frac{1}{m^2} - \frac{1}{n^2} \right) \quad \text{ή}$$

$$\frac{1}{\lambda_{\min}} = R_H \left(\frac{1}{n^2} - \frac{1}{m^2} \right)$$

$$\text{με } R_H = \frac{me^4}{4\pi\hbar^3} = 1,0973732 \cdot 10^7 \text{ m}^{-1}.$$

Για το άτομο του υδρογόνου H αντικαθιστούμε στις σχέσεις $r_n = \frac{n^2 \hbar^2}{me^2 z}$ και

$$E_n = -\frac{mz^2 e^4}{2n^2 \hbar^2}, \text{ όπου } n=1 \text{ και } z=1, \text{ οπότε προκύπτουν τα εξής [2]:}$$

α) η ακτίνα του ατόμου του υδρογόνου H , είναι ίση με

$$r_1 = \frac{\hbar^2}{me^2} = \alpha_0$$

όπου α_0 η πρώτη ακτίνα του Bohr, η οποία καθορίζει το μέγεθος του ατόμου και η οποία είναι ίση με $\alpha_0 = 53 \cdot 10^{-8} \text{ cm}$.

Η ακτίνα της n -στής σειράς μπορεί να γραφεί και ως

$$r_n = \frac{\eta^2 \hbar^2}{m e^2 z} \Rightarrow r_n = \eta^2 \alpha_0.$$

Οι επιτρεπόμενες τροχιές με τον κύριο κβαντικό αριθμό να είναι $n=1,2,3,\dots$ παίρνουν αντίστοιχα τις τιμές $\alpha_0, 4\alpha_0, 9\alpha_0, \dots$

β) η ενέργειά του ατόμου του υδρογόνου H γίνεται

$$E_1 = -13,6\text{eV}$$

που είναι η ενέργεια που ισοδυναμεί με το έργο ιονισμού του ατόμου του υδρογόνου.

Στην θεμελιώδη κατάσταση του ατόμου του υδρογόνου η ταχύτητα που περιστρέφεται το ηλεκτρόνιο είναι 137 φορές μικρότερη από την ταχύτητα του φωτός. Η ταχύτητα του ηλεκτρονίου στην πρώτη τροχιά του Bohr είναι ανάλογη μιας ποσότητας που καλείται **σταθερά της λεπτής υφής α** (με τιμή $\alpha = \frac{1}{137}$, παράρτημα

B) και είναι ανάλογη με $v = \alpha c$ [2].

ΚΕΦΑΛΑΙΟ 2^ο

ΚΒΑΝΤΙΚΟ ΠΛΑΙΣΙΟ, ΘΕΜΕΛΙΩΔΕΙΣ ΑΡΧΕΣ, ΑΙΤΗΜΑΤΑ ΚΑΙ ΜΑΘΗΜΑΤΙΚΟΣ ΦΟΡΜΑΛΙΣΜΟΣ

2.1 ΧΩΡΟΣ HILBERT

Ο **χώρος Hilbert** είναι ένας διανυσματικός χώρος πάνω στο πεδίο των μιγαδικών αριθμών και ουσιαστικά είναι χώρος που παίρνει άπειρες διαστάσεις. Για την μελέτη των κβαντικών υπολογιστών θα περιοριστούμε σε δύο ή τρεις διαστάσεις δηλαδή θα έχουμε ζεύγος διανυσμάτων που θα αναπαριστά δύο ή περισσότερα σωματίδια .

Η μαθηματική έννοια του χώρου **Hilbert**, γενικεύει την έννοια του Ευκλείδειου χώρου και επεκτείνει τις μεθόδους της γραμμικής άλγεβρας και του λογισμού από το δισδιάστατο και τρισδιάστατο επίπεδο Ευκλείδειου χώρου, σε χώρους με κάθε πεπερασμένο ή άπειρο αριθμό διαστάσεων. Ένας χώρος Hilbert είναι κατά κάποιο

τρόπο ένας «αφηρημένος χώρος» που διαθέτει τη δομή ενός εσωτερικού «προϊόντος» που επιτρέπει το μήκος και τη γωνία που πρέπει να μετρηθεί.

Έστω θεωρούμενο σύστημα με δύο σωματίδια. Τότε ο χώρος Hilbert θα είναι $H_1 \otimes H_2$ δηλαδή θα είναι τανυστικό γινόμενο των χώρων H_1 και H_2 και η διάσταση του χώρου θα είναι d^2 . Επίσης για N σωματίδια ο χώρος Hilbert θα είναι $H_1 \otimes H_2 \otimes H_3 \dots \otimes H_N$ και συνολικά θα είναι διάστασης, d^N .

2.2 Η ΚΥΜΑΤΙΚΗ ΣΥΝΑΡΤΗΣΗ

Όπως προαναφέρθηκε στο 1^ο κεφάλαιο, η ύλη συμπεριφέρεται ταυτοχρόνως ως κύμα και ως σωματίδιο. Κάθε κύμα περιγράφεται από μια ποσότητα μεταβαλλόμενη ως προς τον χρόνο και την θέση. Τα υλικά κύματα μπορούν να περιγραφούν από μια κυματική ουσυνάρτηση ψ . Αυτή η κυματοσυνάρτηση εξαρτάται από την θέση και τον χρόνο όλων των σωματιδίων του συστήματος που περιγράφει. Κάθε γενικευμένο κύμα περιγράφεται από την θεμελιώδη εξίσωση κυματικής [2]

$$\psi(x, t) = Ae^{i(kx - \omega t + \phi)}$$

Για κύματα που κατευθύνονται στον άξονα x η κυματική εξίσωση περιγράφεται από την σχέση

$$\left(\frac{\partial^2}{\partial x^2} - \frac{1}{v^2} \frac{\partial^2}{\partial t^2}\right)\psi = 0 \quad \text{ή} \quad \frac{\partial^2}{\partial x^2} \psi = \frac{1}{v^2} \frac{\partial^2}{\partial t^2} \psi$$

Με την χρήση της κυματικής συνάρτησης $\psi(\vec{r}, t)$ μπορούμε να υπολογίσουμε την μέση θέση και ταχύτητα, την μέση ορμή και μέση ενέργεια του σωματιδίου που δεν διαδίδεται σε υλικό μέσο αλλά στον χώρο στις τρεις διαστάσεις. Η κυματική συνάρτηση είναι το κεντρικό μέγεθος στην κβαντική μηχανική, στην οποία όμως δεν αντιστοιχεί κανένα φυσικό μέγεθος [2]. Η κυματική συνάρτηση παίρνει μιγαδικές τιμές και είναι ένα κύμα πιθανότητας. Χαρακτηριστικό μέγεθος είναι ο υπολογισμός της πιθανότητας να βρεθεί το σωματίδιο σε συγκεκριμένο όγκο και θέση μεταξύ οριοθετημένων τιμών. Το σωματίδιο δεν μπορούμε να το προσδιορίσουμε με απόλυτη ακρίβεια. Μπορούμε με τον υπολογισμό όμως της πιθανότητας παρατήρησής του στον χώρο να προσδιορίσουμε την κατανομή των θέσεων του [2].

■ Σε μία διάσταση [2] :

Η **πιθανότητα** ένα σωματίδιο να βρίσκεται μεταξύ των ορίων x και $x+dx$ στον χώρο, ισούται με

$$P(x)dx = |\psi(x)|^2 dx \quad \text{ή} \quad P(x)dx = \psi^*(x)\psi(x).$$

Εάν η κυματοσυνάρτηση ψ εξαρτάται από τον χρόνο τότε η πιθανότητα κάποιο σωματίδιο να βρίσκεται σε χρόνο t μεταξύ των ορίων x και $x+dx$ θα είναι σύμφωνα με την **ερμηνεία της σχολής της Κοπεγχάγης**¹, ίση με

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

Η πιθανότητα προσδιορισμού ενός σωματιδίου σε περιοχή με όρια κίνησης εντός του $x=a$ και $x=b$ θα είναι $P_{(a \leq x \leq b)} = \int_a^b |\psi(x)|^2 dx$. **Ποκνότητα πιθανότητας** καλείται η ποσότητα

$$p = |\psi(x)|^2 \Rightarrow p = \psi^*(x)\psi(x) = \frac{P(x)}{dx}.$$

Η Συνθήκη κανονικοποίησης δίνεται από την σχέση

$$P(x) = \int_{-\infty}^{+\infty} |\psi(x)|^2 dx = \int_{-\infty}^{+\infty} \psi^*(x)\psi(x)dx = 1$$

Συνθήκη κανονικοποίησης καλείται η σχέση που αφορά ένα σωματίδιο με πιθανότητα εύρεσης του σε όλο τον χώρο του άξονα x , ίση με 1. Η κυματική συνάρτηση ψ καλείται **κανονικοποιημένη** [2].

¹ Σύμφωνα με την **ερμηνεία της σχολής της Κοπεγχάγης** παρέχεται ο απόλυτος φορμαλισμός για την διεξαγωγή υπολογισμών στην κβαντική μηχανική. Η θεωρία αναπτύχθηκε στα τέλη της δεκαετίας του 1920 από τον Νιλς Μπόρ και ο μαθηματικός φορμαλισμός αποδίδει εξαιρετικά ακριβείς προβλέψεις και ουσιαστικά αντιπροσωπεύει την γνώση για το σύστημα, τις φυσικές μετρήσιμες μεταβλητές και δεν αφορά τόσο τις υποκείμενες φυσικές διαδικασίες που ίσως συμβαίνουν στο κβαντικό σύστημα]. Το τετράγωνο του μέτρου της σχέσης $P(x, t) = |\psi(x, t)|^2 dx$ εκφράζει την **πιθανότητα εύρεσης ενός σωματίου σε συγκεκριμένο σημείο του χώρου**. Κατά την διαδικασία της μέτρησης ενός κβαντομηχανικού συστήματος, η κυματοσυνάρτηση καταρρέει και λαμβάνει μια τυχαία τιμή, η οποία είναι το μέτρο της εν λόγω πιθανότητας [1, 14, 15, 44].

Εάν η κυματική συνάρτηση ψ εξαρτάται από τον χρόνο τότε η πιθανότητα ένα σωματίδιο να βρίσκεται στον επιτρεπόμενο χώρο του άξονα x σε χρόνο t , θα είναι

$$P(x, t) = \int_{-\infty}^{+\infty} |\psi(x, t)|^2 dx = 1.$$

Στάσιμες καταστάσεις καλούνται αυτές, στις οποίες η τιμή της πυκνότητας πιθανότητας $p = |\psi(x)|^2 = \psi^*(x)\psi(x)$ είναι σταθερή σε ένα σημείο και ανεξάρτητη του χρόνου.

■ Σε τρεις διαστάσεις [2] :

Η **πιθανότητα** ενός σωματιδίου να βρίσκεται σε όγκο από V έως $V+dV$ ισούται με

$$P(\vec{r})dV = |\psi(\vec{r})|^2 dV, \text{ όπου } dV = dx dy dz.$$

Εάν η κυματοσυνάρτηση ψ είναι εξαρτώμενη από τον χρόνο τότε η πιθανότητα ένα σωματίδιο σε χρόνο t να βρίσκεται στον όγκο dV , θα είναι ίση με

$$P(\vec{r}, t) = |\psi(\vec{r}, t)|^2 dV$$

Η **Συνθήκη κανονικοποίησης** δίνεται από την σχέση

$$P(\vec{r}, t) = \int_V |\psi(\vec{r}, t)|^2 dV = 1$$

όπου το $\psi(\vec{r}, t)$ είναι το πλάτος της πυκνότητας πιθανότητας.

Πυκνότητα πιθανότητας καλείται η ποσότητα

$$p = |\psi(\vec{r}, t)|^2 = \psi^*(\vec{r}, t)\psi(\vec{r}, t)$$

Η **Συνθήκη κανονικοποίησης** -κανονικοποίηση ή νορμαλισμός- δίνεται από την σχέση

$$P(\vec{r}) = \int_{-\infty}^{+\infty} |\psi(\vec{r})|^2 dV = \int_{-\infty}^{+\infty} \psi^*(\vec{r})\psi(\vec{r})dV = 1.$$

Συνθήκη κανονικοποίησης καλείται η σχέση που αφορά σε σωματίδιο με πιθανότητα εύρεσης του σε όλο τον όγκο V , ίση με 1. Η κυματική συνάρτηση ψ καλείται **κανονικοποιημένη**. Εάν η κυματική συνάρτηση ψ είναι εξαρτώμενη από τον χρόνο τότε η πιθανότητα ένα σωματίδιο να βρίσκεται σε χρόνο t στον επιτρεπόμενο χώρο θα είναι [2]:

$$P(\vec{r}, t) = \int_{-\infty}^{+\infty} |\psi(\vec{r}, t)|^2 dV = \int_{-\infty}^{+\infty} \psi^*(\vec{r}, t)\psi(\vec{r}, t)dV = 1.$$

Επειδή για το σωματίδιο θα υπάρχει κάποια πιθανότητα εύρεσης του στον χώρο όγκου dV , θα ισχύει η γενική συνθήκη κανονικοποίησης που δεν είναι άλλη από την αρχή διατήρησης της ολικής πιθανότητας και θα είναι ίση με $\int_V \psi^* \psi dV = 1$.

2.3 Η ΕΙΣΩΣΗ ΤΟΥ SCHRÖDINGER

Η κυματοσυνάρτηση ενός σωματιδίου μάζας m που κινείται χωρίς την επίδραση δυναμικού (με $\hat{p} = \hbar k$ και $E = \hbar\omega$) είναι η $\psi = e^{i(kx - \omega t + \phi)}$.

Με παραγώγιση ως προς τον χρόνο δίνει [2]

$$\frac{\partial}{\partial t} \psi = -\frac{iE}{\hbar} e^{i(kx - \omega t + \phi)} \quad 2.1$$

Αντικαθιστούμε τον τελεστή $\hat{E} = i\hbar \frac{\partial}{\partial t}$ στην σχέση 2.1 οπότε προκύπτει

$$\frac{\partial}{\partial t} \psi = -\frac{iE}{\hbar} e^{i(kx - \omega t + \phi)} \Rightarrow \hat{E} \psi = E\psi$$

Με παραγώγιση επίσης, ως προς τη θέση προκύπτει [2]

$$\frac{\partial}{\partial x} \psi = \frac{ip}{\hbar} e^{i(kx - \omega t + \phi)} \quad 2.2$$

Αντικαθιστούμε τον τελεστή $\hat{p} = -i\hbar \frac{\partial}{\partial x}$ στην σχέση 2.2 οπότε προκύπτει

$$\frac{\partial}{\partial x} \psi = \frac{ip}{\hbar} e^{i(kx - \omega t + \phi)} \Rightarrow \hat{p} \psi = p\psi.$$

Παρατηρείται πως η κυματοσυνάρτηση ψ με την σχέση ενέργειας και ορμής, $E = \frac{p^2}{2m}$

επαληθεύει την εξίσωση $\hat{E} \psi = \frac{\hat{p}^2}{2m} \psi$.

Συνεχίζοντας με αντικατάσταση των τελεστών $\hat{E} = i\hbar \frac{\partial}{\partial t}$ και $\hat{p} = -i\hbar \frac{\partial}{\partial x}$ προκύπτει ότι

$$\hat{E} \psi = \frac{\hat{p}^2}{2m} \psi \Rightarrow i\hbar \frac{\partial}{\partial t} \psi = -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} \psi \quad 2.3$$

Οπότε με την χαμιλτονιανή για ένα σωματίδιο που κινείται ελεύθερα χωρίς την επίδραση δυναμικού να είναι ίση με $\hat{H} = \frac{\hat{p}_x^2}{2m}$, η προηγούμενη σχέση 2.3, δίνει ισοδύναμα

$$i\hbar \frac{\partial}{\partial t} \psi = -\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} \psi \Rightarrow i\hbar \frac{\partial \psi}{\partial t} = \hat{H} \psi$$

Επομένως η εξίσωση του Schrödinger για μονοδιάστατη κίνηση είναι η

$$i\hbar \frac{\partial \psi(x, t)}{\partial t} = \hat{H} \psi(x, t)$$

Για κίνηση ενός σωματιδίου σε μία διάσταση με την επίδραση εξωτερικού δυναμικού η χαμιλτονιανή είναι $\hat{H} = -\frac{\hbar^2}{2m} \frac{\partial}{\partial x} + V(x)$. Οπότε αντικαθιστώντας στην σχέση 2.3 θα γίνει ισοδύναμα

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

Επομένως η εξίσωση του Schrödinger για μονοδιάστατη κίνηση με επίδραση δυναμικού είναι η

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

Ομοίως για κίνηση σωματιδίου με επίδραση δυναμικού η εξίσωση του Schrödinger στις τρεις διαστάσεις είναι [2]:

$$i\hbar \frac{\partial \psi(\vec{r}, t)}{\partial t} = -\frac{\hbar^2}{2m} \nabla^2 \psi(\vec{r}, t) + V(\vec{r}) \psi(\vec{r}, t)$$

Χρονικά ανεξάρτητη εξίσωση του Schrödinger καλείται η εξίσωση

$$\hat{H} \psi(x) = E \psi(x)$$

Η εξίσωση ιδιοτιμών της χαμιλτονιανής είναι η $\hat{H} \psi(x) = E \psi(x)$.

2.4 ΙΔΙΟΤΙΜΕΣ ΚΑΙ ΙΔΙΟΣΥΝΑΡΤΗΣΕΙΣ

Η εξίσωση ιδιοτιμών δίνεται από την σχέση $\hat{A}^+ \psi = \lambda \psi$. Ο αριθμός λ είναι η ιδιοτιμή και η συνάρτηση ψ είναι η ιδιοσυνάρτηση του τελεστή. Η σταθερή ποσότητα λ είναι ένας μιγαδικός αριθμός. Η εξίσωση δηλώνει την δράση ενός τελεστή (θα αναλυθεί αμέσως μετά §2.8 και §2.9), $\hat{A}^+$ πάνω σε μία συνάρτηση ψ (που καλείται ειδικότερα ιδιοσυναρτήρηση του τελεστή $\hat{A}^+$), που αποτυπώνεται από το γινόμενο της συνάρτησης ψ πολλαπλασιασμένη με μία σταθερή ποσότητα λ . Οι ιδιοτιμές μπορούν να έχουν συνεχές φάσμα (όταν οι ιδιοτιμές του τελεστή παίρνουν κάθε τιμή) και διακριτό φάσμα (όταν οι ιδιοτιμές παίρνουν μόνο συγκεκριμένες τιμές) [2].

Μια συνάρτηση $\psi(x)$ μπορεί να γραφεί σαν γραμμικός συνδυασμός ιδιοσυναρτήσεων ψ_n ενός ερμιτιανού τελεστή με την μορφή

$$\psi(x) = \sum_n c_n \psi_n.$$

Ισχύουν οι εξής προτάσεις:

- Οι ερμιτιανοί τελεστές έχουν πραγματικές ιδιοτιμές και
- Οι ιδιοσυναρτήσεις ενός ερμιτιανού τελεστή που αντιστοιχούν και αντιπροσωπεύουν διαφορετικές ιδιοτιμές είναι πάντα μεταξύ τους ορθογώνιες.

2.5 ΚΥΜΑΤΙΚΕΣ ΣΥΝΑΡΤΗΣΕΙΣ ΣΤΟΝ ΧΩΡΟ ΤΩΝ ΟΡΜΩΝ

Η κυματική συνάρτηση $\psi = \sum_n c_n \psi_n$ εκφράζει την θέση του σωματιδίου στον χώρο. Η πυκνότητα πιθανότητας θα είναι (με ψ^* είναι η συζυγής συνάρτηση της ψ):

$$p = |\psi(x)|^2 = \psi^*(x)\psi(x)$$

και η πιθανότητα να βρεθεί το σωματίδιο σε θέση μεταξύ των ορίων $x, x+dx$ είναι

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

Η πυκνότητα πιθανότητας είναι μια θετική ποσότητα που διατηρείται και είναι ανεξάρτητη του χρόνου. Για να έχει νόημα η στατιστική της ερμηνεία, η ολική

πιθανότητα θα είναι $P(x, t) = \int_{-\infty}^{+\infty} |\psi(x)|^2 dx = \text{ανεξάρτητη του χρόνου.}$

Η ολική πιθανότητα δεν θα είναι της μορφής $P(x, t) = \int_{-\infty}^{+\infty} |\psi(x, t)|^2 dx$, επειδή αν και η ποσότητα της πιθανότητας είναι θετική, δεν είναι ανεξάρτητη του χρόνου.

Με τον ίδιο τρόπο μια κυματοσυνάρτηση μπορεί να γραφεί με μορφή ιδιοσυναρτήσεων ορμής. Η κυματοσυνάρτηση θα είναι

$$\psi(x) = \sum_p c_p \phi_p(x)$$

Όπου $|c_p|^2$ είναι η πιθανότητα το σωματίδιο να έχει ορμή p .

Το πλάτος πιθανότητας της ορμής $c(p)$ θα είναι ίσο με

$$c(p) = (\phi_p, \psi) = \int_{-\infty}^{+\infty} \phi_p^*(x) \psi(x) dx$$

Αποδεικνύεται ότι ιδιοσυνάρτηση του τελεστή της ορμής είναι η κυματοσυνάρτηση

$$\phi_p(x) = \frac{1}{\sqrt{2\pi\hbar}} e^{i\frac{p_x}{\hbar}x}.$$

Η κυματική συνάρτηση τότε θα είναι ανάλογη της ιδιοσυνάρτησης της ορμής ώστε

$$\psi(x) = \sum_p c_p \phi_p(x) = \int_{-\infty}^{+\infty} \frac{1}{\sqrt{2\pi\hbar}} c_p e^{i\frac{p_x}{\hbar}x} dp \Rightarrow \boxed{\psi(x) = \frac{1}{\sqrt{2\pi\hbar}} \int_{-\infty}^{+\infty} c_p e^{i\frac{p_x}{\hbar}x} dp}$$

Οι ιδιοτιμές έχουν **συνεχές φάσμα τιμών**.

2.6 ΕΣΩΤΕΡΙΚΟ ΓΙΝΟΜΕΝΟ ΣΥΝΑΡΤΗΣΕΩΝ

Εσωτερικό γινόμενο σε χώρους δύο μιγαδικών συναρτήσεων καλείται το γινόμενο [2]:

$$(\psi_1, \psi_2) = \int_V \psi_1^*(\vec{r}) \psi_2(\vec{r}) dV \quad \text{ή διαφορετικά} \quad (\psi, \phi) = \int_V \psi^*(\vec{r}) \phi(\vec{r}) dV$$

όπου ψ^* είναι η συζυγής συνάρτηση της ψ .

Σε **μία διάσταση** μεταξύ δύο συναρτήσεων το εσωτερικό γινόμενο είναι

$$(\psi_1, \psi_2) = \int_{-\infty}^{+\infty} \psi_1^*(x) \psi_2(x) dx \quad \text{ή διαφορετικά} \quad (\psi, \phi) = \int_{-\infty}^{+\infty} \psi^*(x) \phi(x) dx$$

Το εσωτερικό γινόμενο συμβολίζεται επίσης και με το λεγόμενο σύμβολο **-bracket-** ώστε [2]

$$(\psi_1, \psi_2) = \langle \psi_1 | \psi_2 \rangle \quad \text{ή} \quad (\psi, \phi) = \langle \psi | \phi \rangle$$

δηλαδή θα είναι

$$\langle \psi | \phi \rangle = \int_V \psi^*(\vec{r})\phi(\vec{r})dV \quad \text{ή} \quad \langle \psi_1 | \psi_2 \rangle = \int_V \psi_1^*(\vec{r})\psi_2(\vec{r})dV$$

Η λέξη **bracket** είναι σύνθετη και το σύμβολο $|\dots\rangle$ καλείται **ket**. Με την ονομασία **bra** καλείται το σύμβολο $\langle\dots|$ και είναι το συζυγές του **ket**.

Για το εσωτερικό γινόμενο ισχύουν οι εξής ιδιότητες [2]:

- $(\psi_1, \psi_2) = (\psi_2, \psi_1)^*$
- $(\alpha\psi_1, \psi_2) = \alpha^*(\psi_1, \psi_2)$, α μιγαδικός αριθμός
- $(\psi_1, \alpha\psi_2) = \alpha(\psi_1, \psi_2)$, α μιγαδικός αριθμός

■ **Ορθογώνιες συναρτήσεις ψ_1, ψ_2** καλούνται οι συναρτήσεις για τις οποίες ισχύουν [2]

$$(\psi_1, \psi_2) = \int_V \psi_1^*(\vec{r})\psi_2(\vec{r})dV = 0 \quad \text{ή} \quad (\psi_1, \psi_2) = \langle \psi_1 | \psi_2 \rangle = 0$$

■ **Κανονικοποιημένη συνάρτηση ψ** , καλείται αυτή για την οποία ισχύει:

$$(\psi, \psi) = \int_V \psi^*(\vec{r})\psi(\vec{r})dV = 1$$

■ **Ορθοκανονικοποιημένες συναρτήσεις ψ_1, ψ_2** καλούνται οι συναρτήσεις για τις οποίες ισχύουν [2]:

$$(\psi_n, \psi_m) = \int_V \psi_n^*(\vec{r})\psi_m(\vec{r})dV = \delta_{nm} = \begin{cases} 1, n=m \\ 0, n \neq 0 \end{cases}$$

όπου $\delta_{n,m}$ το λεγόμενο σύμβολο δέλτα του Kronecker.

Όταν είναι $n \neq m$ οι ιδιοσυναρτήσεις είναι ορθογώνιες ενώ όταν $n=m$ είναι κανονικοποιημένες.

Με την χρήση του συμβόλου Kronecker μπορούμε να υπολογίσουμε τον συντελεστή c_n . Για μια τυχαία συνάρτηση

$$\psi = \sum_n c_n \psi_n$$

είναι

$$(\psi_n, \psi_m) = \sum_m (\psi_n, c_m \psi_m) = \sum_m c_m (\psi_n, \psi_m) = \sum_m c_m \delta_{nm}.$$

Αν μάλιστα $n=m$ τότε $\delta_{nm}=1$, οπότε

$$(\psi_n, \psi_m) = \sum_m c_m = \sum_m c_m = c_n.$$

Τελικά ο συντελεστής είναι ίσος με

$$c_n = (\psi_n, \psi_m).$$

2.7 ΕΣΩΤΕΡΙΚΟ ΓΙΝΟΜΕΝΟ ΠΙΝΑΚΩΝ

Η κυματική συνάρτηση μπορεί να εκφραστεί με μορφή πινάκων, κάτι που οδηγεί και στην έκφραση του εσωτερικού γινομένου με την μορφή πίνακα [2]. Η κυματική συνάρτηση $|\psi\rangle$ είναι

$$|\psi\rangle = \sum_n c_n |\phi\rangle = \begin{bmatrix} a \\ b \\ c \\ \vdots \end{bmatrix} \Rightarrow |\phi\rangle = a \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \end{bmatrix} + b \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix} + \dots$$

Η κυματοσυνάρτηση $|\phi\rangle$ με τον ίδιο τρόπο επίσης θα είναι

$$|\phi\rangle = \sum_n c_n |\psi\rangle = \begin{bmatrix} a' \\ b' \\ c' \\ \vdots \end{bmatrix} \Rightarrow |\phi\rangle = a' \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \end{bmatrix} + b' \begin{bmatrix} 0 \\ 1 \\ 0 \\ \vdots \end{bmatrix} + \dots$$

Το εσωτερικό γινόμενο δύο κυματοσυναρτήσεων, τότε είναι

$$(\psi, \phi) = \langle \psi | \phi \rangle = \begin{bmatrix} a^* & b^* & c^* & \dots \end{bmatrix} \cdot \begin{bmatrix} a' \\ b' \\ c' \\ \vdots \end{bmatrix}.$$

Αν ο πίνακας είναι 2x2 τότε το εσωτερικό γινόμενο γίνεται ισοδύναμα [2]:

$$(\psi, \phi) = \langle \psi | \phi \rangle = \begin{bmatrix} a^* & b^* \end{bmatrix} \cdot \begin{bmatrix} a' \\ b' \end{bmatrix} = a^* a' + b^* b'.$$

2.8 ΚΒΑΝΤΟΜΗΧΑΝΙΚΟΙ ΤΕΛΕΣΤΕΣ

Τελεστή ορίζουμε ένα γενικό σύνολο μαθηματικών πράξεων. Ορίζουμε την μαθηματική ποσότητα που μπορεί να μετασχηματίσει μια συνάρτηση (ή ένα σύνολο μαθηματικών ποσοτήτων) σε κάποια άλλη, μπορεί δηλαδή να δράσει σε μία τυχαία κυματοσυνάρτηση και να δώσει μία άλλη στον ίδιο χώρο δράσης ώστε να ισχύει [2]

$$\hat{A}\psi = \phi.$$

Χαρακτηριστικοί τελεστές είναι ο τελεστής της παραγώγισης $\frac{d}{dx}$, ο τελεστής ανάδελτα

$\vec{\nabla}$ ή ο τελεστής Laplace ∇^2 . Ο συμβολισμός ενός τελεστή γίνεται με $\hat{A}$ ή με $\hat{B}$ ή με $\hat{C}$ ή με $\hat{D}$ κ.ο.κ..



Πράξεις Τελεστών [2]:

Η **Πρόσθεση** δύο τελεστών σε ένα διανυσματικό χώρο συμβολίζεται με $\hat{A} + \hat{B}$ ώστε δρώντας σε μια κυματοσυνάρτηση ψ να είναι

$$(\hat{A} + \hat{B})\psi = \hat{A}\psi + \hat{B}\psi.$$

Το **γινόμενο** δύο τελεστών σε ένα διανυσματικό χώρο συμβολίζεται με $\hat{A}\hat{B}$ ώστε δρώντας σε μια κυματοσυνάρτηση ψ να είναι

$$\hat{A}\hat{B}\psi = \hat{A}(\hat{B}\psi).$$

Η **Ισότητα** δύο τελεστών σε ένα διανυσματικό χώρο υπάρχει όταν ισχύει

$$\hat{A}\psi = \hat{B}\psi.$$

Άθροισμα δύο τελεστών ορίζουμε τον τελεστή $\hat{C}$ για τον οποίο ισχύει

$$\hat{C} = \hat{A}\psi + \hat{B}\psi.$$

■ Ιδιότητες Τελεστών [2]:

- Ταυτοτικός τελεστής καλείται αυτός για τον οποίο ισχύουν

$$\hat{A}\psi = \psi.$$

- Σταθερός τελεστής καλείται αυτός για τον οποίο ισχύουν

$$\hat{A}\psi = A\psi.$$

- Γραμμικός τελεστής καλείται αυτός για τον οποίο ισχύουν

$$\hat{A}(a\psi_1 + b\psi_2) = a\hat{A}\psi_1 + b\hat{A}\psi_2$$

όπου a, b μιγαδικοί και ψ_1, ψ_2 δύο τυχαίες κυματοσυναρτήσεις. Αν έχουμε γραμμικούς τελεστές τους $\hat{A}, \hat{B}$ τότε είναι γραμμικοί και οι τελεστές $\hat{A} + \hat{B}, \hat{A}\hat{B}$.

Ένας γραμμικός τελεστής μπορεί να δράσει σε οποιαδήποτε συνάρτηση

$$\psi = \sum_n c_n \psi_n,$$

ώστε

$$\hat{A}\psi = \hat{A} \sum_n c_n \psi_n = \sum_n c_n \hat{A}\psi_n$$

Στην κβαντομηχανική ισχύει η αντιμεταθετική ιδιότητα οπότε δεν ισχύει η μεταθετικότητα των τελεστών. Είναι δηλαδή

$$\hat{A}\hat{B} \neq \hat{B}\hat{A}.$$

- Μεταθέτης δύο τελεστών $\hat{A}$ και $\hat{B}$ καλείται αυτός για τον οποίο ισχύουν

$$[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$$

Για τους μεταθέτες ισχύουν οι εξής ιδιότητες :

- | | |
|--|---|
| ▪ $[\hat{A}, a\hat{B}] = a[\hat{A}, \hat{B}]$ | ▪ $[\hat{A}, \hat{B}\hat{C}] = \hat{A}[\hat{B}, \hat{C}] + [\hat{A}, \hat{C}]\hat{B}$ |
| ▪ $[\hat{A}, \hat{B} + \hat{C}] = [\hat{A}, \hat{B}] + [\hat{A}, \hat{C}]$ | ▪ $[\hat{A}, \hat{A}] = [\hat{B}, \hat{B}] = 0$ |
| ▪ $[\hat{A}, \hat{B} + \hat{C}] = [\hat{A}, \hat{B}]\hat{C} + \hat{B}[\hat{A}, \hat{C}]$ | ▪ $[\hat{A}, \hat{B}] = -[\hat{B}, \hat{A}]$ |

- Ερμιτιανός Τελεστής (ή αυτοσυζυγής) καλείται αυτός για τον οποίο ισχύει ότι

$$\hat{A}^+ = \hat{A},$$

δηλαδή έχει πραγματική μέση τιμή και πραγματικές ιδιοτιμές. Ερμιτιανός τελεστής καλείται αυτός για τον οποίο επομένως ισχύει

$$(\psi_1, \hat{A} \psi_2) = (\hat{A} \psi_1, \psi_2) \quad \text{ή} \quad \int \psi_1^* \hat{A} \psi_2 dV = \int (\hat{A} \psi_1)^* \psi_2 dV.$$

Για τους ερμιτιανούς τελεστές ισχύουν οι εξής ιδιότητες [2]:

- $\hat{A} \hat{B} = \hat{B} \hat{A}$
- $(\hat{A} + \hat{B})^+ = \hat{A}^+ + \hat{B}^+$
- $(\alpha \hat{A}^n)^+ = \alpha^* \hat{A}^n$

■ **Τελεστής parity (ή ανάκλασης ή αρτιότητας)** καλείται ο ερμιτιανός τελεστής που μετατρέπει το διάνυσμα θέσης $\vec{r}$ σε $-\vec{r}$ ώστε να ισχύει

$$\hat{P} \psi(\vec{r}) = \psi(-\vec{r})$$

■ **Συναφής (ή συζυγής) τελεστής** καλείται ο τελεστής για τον οποίο ισχύει ότι

$$\int (\psi_1^* \hat{A}) \psi_2 dV = \int (\hat{A}^+ \psi_1) \psi_2 dV \quad \text{ή} \quad (\psi_1, \hat{A} \psi_2) = (\hat{A}^+ \psi_1, \psi_2).$$

Για τον Συναφή ή συζυγή τελεστή ισχύουν οι εξής ιδιότητες :

- $(\hat{A}^+)^+ = \hat{A}$
- $(\hat{A}^i)^+ = (\hat{A}^+)^i$
- $(\alpha \hat{A})^+ = \alpha^* \hat{A}^+$
- $(\hat{A} + \hat{B})^+ = \hat{A}^+ + \hat{B}^+$
- $(\hat{A} \hat{B})^+ = \hat{B}^+ \hat{A}^+$

■ **Προβολικός Τελεστής** καλείται ο ερμιτιανός τελεστής που είναι ισοδύναμος με το τετράγωνό του, ώστε να είναι $\hat{P}^2 = \hat{P}$

■ **Μοναδιαίος τελεστής (ή unitarity)** καλείται ο τελεστής για τον οποίο ισχύει

$$\hat{U}^+ = \hat{U}^{-1}$$

Κάθε γραμμικός τελεστής $\hat{A}$ μπορεί να γραφεί με την μορφή **τετραγωνικού πίνακα A**. Για το στοιχείο (A_{nm}) του πίνακα A ισχύει

$$(A_{nm}) = (\psi_n, \hat{A} \psi_m)$$

- **Ερμιτανός πίνακας** καλείται αυτός που έχει πραγματικές ιδιότητες και ισχύει

$$(A^+_{nm}) = (A_{nm})$$

- **Τελεστής εναλλαγής** $\hat{P}$ καλείται αυτός για τον οποίο ισχύει

$$\hat{P} \psi(\vec{r}_1, \vec{r}_2) = \psi(\vec{r}_2, \vec{r}_1)$$

Ο τελεστής $\hat{P}^2$ όταν δράσει σε μία κυματική συνάρτηση θα δώσει ξανά την ίδια, δηλαδή θα ισχύει

$$\hat{P}^2 \psi(\vec{r}_1, \vec{r}_2) = \hat{P} \psi(\vec{r}_2, \vec{r}_1) = \psi(\vec{r}_1, \vec{r}_2) .$$

- **Συναφής πίνακας** καλείται αυτός για τον οποίο ισχύει

$$(A^+_{nm}) = (A_{nm})^*$$

Κβαντομηχανικούς τελεστές συναντάμε σε κάθε φυσικό μέγεθος. Για κινούμενο σωματίδιο στο χώρο, μπορούμε να αντιστοιχήσουμε τόσο για την θέση του όσο και για την ορμή του ένα κβαντομηχανικό τελεστή. Έτσι για την **θέση** x (στον άξονα κίνησης x) αντιστοιχεί ο τελεστής $\hat{x} = x$. Για την **ορμή** p_x αντιστοιχεί ο τελεστής $\hat{p}_x = -i\hbar \frac{\partial}{\partial x}$. Άρα για αναπαράσταση θέσης αντιστοιχούν $\hat{x} = x$ και $\hat{p}_x = -i\hbar \frac{\partial}{\partial x}$.

Για αναπαράσταση ορμής αντιστοιχούν οι τελεστές $\hat{p} = p$ και $\hat{x} = +i\hbar \frac{\partial}{\partial p}$ [2].

2.9 ΤΕΛΕΣΤΕΣ ΘΕΣΗΣ ΚΑΙ ΟΡΜΗΣ [2]

■ Σε μία διάσταση ο τελεστής θέσης είναι $\hat{x} = x$ και ο τελεστής της ορμής $\hat{p} = -i\hbar \frac{\partial}{\partial x}$.

■ Στις τρεις διαστάσεις ο τελεστής θέσης είναι $\hat{\vec{r}} = \vec{r}$ και ο τελεστής της ορμής $\hat{\vec{p}} = -i\hbar \vec{\nabla}$.

Για τους τελεστές μετάθεσης της θέσης και της ορμής ισχύουν κατόπιν απλής απόδειξης τα εξής:

- | | | | |
|-------|--|-------|---|
| i. | $\hat{p}_x^2 = -\hbar^2 \frac{\partial^2}{\partial x^2}$ (σε 1-διάσταση) | ix. | $\left[\hat{p}_x, f(x) \right] = -i\hbar \frac{\partial}{\partial x} f(x)$ |
| ii. | $\hat{p}_x^2 = -\hbar^2 \bar{\nabla}^2$ (σε 3 διαστάσεις) | x. | $\left[\hat{x}, \hat{x}^2 \right] = 0$ |
| iii. | $\left[\hat{x}, \hat{p}_x \right] = i\hbar,$ | xi. | $\left[\hat{p}_x, \hat{p}_x^2 \right] = 0$ |
| iv. | $\left[\hat{y}, \hat{p}_y \right] = i\hbar,$ | xii. | $\left[\hat{x}, \hat{y} \right] = 0$ |
| v. | $\left[\hat{z}, \hat{p}_z \right] = i\hbar$ | xiii. | $\left[\hat{x}, \hat{p}_y \right] = 0$ |
| vi. | $\left[\hat{x}, \hat{p}_x^n \right] = i\hbar n p_x^{n-1}$ | xiv. | $\left[\hat{p}_y, \hat{p}_z \right] = 0$ |
| vii. | $\left[\hat{x}, \hat{p}_x^2 \right] = 2i\hbar p_x$ | | |
| viii. | $\left[\hat{x}, f(p) \right] = i\hbar \frac{\partial}{\partial p} f(x)$ | | |

2.10 ΤΕΛΕΣΤΗΣ HAMILTONIAN

Ο τελεστής της χαμιλτονιανής $\hat{H}$ (Hamiltonian) δηλαδή της ενέργειας σωματιδίου μάζας m με κινητική ενέργεια T και δυναμική ενέργεια V [2], θα είναι :

■ για κίνηση σε μία διάσταση: $\hat{H} = T + V(x) \Rightarrow \hat{H} = \frac{\hat{p}_x^2}{2m} + \hat{V}(x)$ και για

■ για κίνηση σε τρεις διαστάσεις: $\hat{H} = T + V(\vec{r}) \Rightarrow \hat{H} = -\frac{\hbar^2}{2m} \bar{\nabla}^2 + V(\vec{r})$

(που προκύπτει με αντικατάσταση της ορμής $\hat{p} = -i\hbar \bar{\nabla}$).

2.11 ΤΕΛΕΣΤΗΣ ΣΤΡΟΦΟΡΜΗΣ

Για τον τελεστή της στροφορμής είναι $\hat{\vec{L}} = \hat{\vec{r}} \times \hat{\vec{p}}$. Οπότε αντικαθιστώντας με $\hat{\vec{p}} = -i\hbar \vec{\nabla}$ προκύπτει ότι $\hat{\vec{L}} = \hat{\vec{r}} \times (-i\hbar \vec{\nabla}) \Rightarrow \hat{\vec{L}} = -i\hbar \hat{\vec{r}} \times \vec{\nabla}$
Είναι

$$\hat{\vec{L}} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ \hat{x} & \hat{y} & \hat{z} \\ \hat{p}_x & \hat{p}_y & \hat{p}_z \end{vmatrix} \Rightarrow \hat{\vec{L}} = \vec{i}(\hat{y}\hat{p}_z - \hat{z}\hat{p}_y) - \vec{j}(\hat{x}\hat{p}_z - \hat{p}_x\hat{z}) + \vec{k}(\hat{x}\hat{p}_y - \hat{p}_x\hat{y}) \Rightarrow$$

$$\hat{\vec{L}} = \vec{i}\hat{L}_x + \vec{j}\hat{L}_y + \vec{k}\hat{L}_z \Rightarrow \begin{cases} \hat{L}_x = \hat{y}\hat{p}_z - \hat{z}\hat{p}_y \\ \hat{L}_y = \hat{z}\hat{p}_x - \hat{x}\hat{p}_z \\ \hat{L}_z = \hat{x}\hat{p}_y - \hat{y}\hat{p}_x \end{cases}$$

Μετά την αντικατάσταση των τελεστών της ορμής με $\hat{p}_x = -i\hbar \frac{\partial}{\partial x}$, $\hat{p}_y = -i\hbar \frac{\partial}{\partial y}$,

$\hat{p}_z = -i\hbar \frac{\partial}{\partial z}$ καταλήγουμε στην μορφή [2]:

$$\begin{cases} \hat{L}_x = -i\hbar(y \frac{\partial}{\partial z} - z \frac{\partial}{\partial y}) \\ \hat{L}_y = -i\hbar(z \frac{\partial}{\partial x} - x \frac{\partial}{\partial z}) \\ \hat{L}_z = -i\hbar(x \frac{\partial}{\partial y} - y \frac{\partial}{\partial x}) \end{cases}$$

Αποδεικνύεται ότι ισχύουν οι μεταθετικές σχέσεις για τους τελεστές της στροφορμής:

$$\begin{aligned} \bullet \quad [\hat{L}_z, \hat{L}_x] &= i\hbar \hat{L}_y & \bullet \quad [\hat{L}_x, \hat{L}_y] &= i\hbar \hat{L}_z \\ \bullet \quad [\hat{L}_y, \hat{L}_z] &= i\hbar \hat{L}_x & \bullet \quad [\hat{L}_n, \hat{L}^2] &= 0 \end{aligned}$$

με $n=1,2,3,\dots$

Επίσης για τους τελεστές μετάθεσης της στροφορμής και της ορμής αποδεικνύεται ότι ισχύει $[\hat{L}_z, \hat{p}_x] = i\hbar \hat{p}_y$.

2.12 ΑΝΑΠΑΡΑΣΤΑΣΗ ΚΑΤΑΣΤΑΣΕΩΝ ΜΕ ΠΙΝΑΚΕΣ

Κάθε κατάσταση $|\psi\rangle = \sum_n c_n |\phi_n\rangle$ σε μια ορθοκανονική βάση μπορεί να γραφεί σε μορφή πίνακα οποιονδήποτε n διαστάσεων:

$$|\phi_1\rangle = \begin{bmatrix} 1 \\ 0 \\ \cdot \\ 0 \end{bmatrix} \quad |\phi_2\rangle = \begin{bmatrix} 0 \\ 1 \\ \cdot \\ 0 \end{bmatrix} \quad |\phi_3\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ \cdot \\ 0 \end{bmatrix}$$

ώστε να έχει μορφή:

$$|\psi\rangle = \sum_n c_n |\phi_n\rangle \Rightarrow |\psi\rangle = c_1 |\phi_1\rangle + c_2 |\phi_2\rangle + c_3 |\phi_3\rangle + \dots \Rightarrow$$

$$|\psi\rangle = \sum_n c_n |\phi_n\rangle \Rightarrow |\psi\rangle = c_1 \begin{bmatrix} 1 \\ 0 \\ \cdot \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 \\ 1 \\ \cdot \\ 0 \end{bmatrix} + c_3 \begin{bmatrix} 0 \\ 0 \\ 1 \\ \cdot \\ 0 \end{bmatrix} + \dots \Rightarrow$$

$$|\psi\rangle = \begin{bmatrix} c_1 \\ 0 \\ \cdot \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ c_2 \\ \cdot \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ c_3 \\ \cdot \\ 0 \end{bmatrix} + \dots$$

2.13 ΑΝΑΠΑΡΑΣΤΑΣΕΙΣ ΤΕΛΕΣΤΩΝ ΣΕ ΜΟΡΦΗ ΠΙΝΑΚΩΝ

Κάθε τελεστής μπορεί να αναπαρασταθεί με μορφή πινάκων ώστε να είναι:

$$\hat{A}_{nm} = \begin{bmatrix} A_{11} & A_{12} & A_{13} & \dots & A_{1n} \\ A_{21} & A_{22} & A_{23} & \dots & \cdot \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ A_{m1} & A_{m2} & \dots & \dots & A_{mn} \end{bmatrix}$$

ή $\hat{A}_{nm} = \langle e_n | \hat{A} | e_m \rangle$, με τα μοναδιαία ιδιοδιανύσματα να είναι:

$$|e_1\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \dots \\ 0 \end{bmatrix}, |e_2\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \dots \\ 0 \end{bmatrix}, |e_3\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ \dots \\ 0 \end{bmatrix}.$$

Από την μορφή τελεστών σε πίνακες μπορούμε αν βρούμε ιδιοτιμές και ιδιοδιανύσματα πινάκων, αλλά και κάθε είδους τελεστή. Για τον **αυτοσυζυγή τελεστή** ισχύει

$$\hat{A}_{nm} = \hat{A}_{mn}^*.$$

Έστω δύο καταστάσεις $|n\rangle$ και $|m\rangle$. Για την Χαμιλτονιανή, θα ισχύει

$$\hat{H}|n\rangle = \frac{\hbar\omega}{2}\left(n + \frac{1}{2}\right)|n\rangle \quad 2.4$$

Όταν τα ιδιοδιανύσματα της $\hat{H}$ είναι $\langle n|m\rangle = \delta_{nm}$ (δηλαδή είναι ορθοκανονικά) τότε η μορφή σε πίνακα για κάθε ένα από αυτά θα είναι :

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \quad |2\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ \cdot \\ \cdot \\ 0 \end{bmatrix}, \quad |3\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ \cdot \\ 0 \end{bmatrix} \dots$$

Σε μορφή πίνακα η εξίσωση του **Schrödinger** $\hat{H}\psi(x) = E\psi(x)$ ή $i\hbar \frac{\partial \psi(x,t)}{\partial t} = \hat{H}\psi(x,t)$, γίνεται [2]:

$$i\hbar \frac{\partial}{\partial t} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \cdot \\ \cdot \\ c_n \end{bmatrix} = \begin{bmatrix} H_{11} & H_{12} & H_{13} & \dots & H_{1m} \\ H_{21} & H_{22} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ H_{n1} & H_{n2} & \cdot & \cdot & H_{nm} \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ \cdot \\ \cdot \\ c_m \end{bmatrix}$$

2.14 ΜΕΣΗ ΤΙΜΗ

Η μέση τιμή ως έννοια μαθηματικού μεγέθους, δίνεται από την σχέση

$$\langle A \rangle = \sum_n \alpha_n P_n$$

όπου P_n η πιθανότητα εμφάνισης των δυνατών τιμών a_n και $\sum_n a_n$ το αλγεβρικό άθροισμα όλων των δυνατών τιμών. Αν η μέτρηση αφορά τιμές συνεχούς φάσματος, δηλαδή όταν η μέτρηση αντιπροσωπεύει πιθανότητα τιμών συνεχούς και όχι διακριτού φάσματος, η μέση τιμή είναι ίση με

$$\langle A \rangle = \int_{-\infty}^{+\infty} \alpha P(\alpha) d\alpha \quad (\text{συνεχούς φάσματος [2]})$$

Η μέση τιμή ενός **φυσικού μεγέθους** που περιγράφεται από τον **ερμιτιανό** τελεστή $\hat{A}$ σε μια κατάσταση $\psi = \sum_n c_n \psi_n$ είναι ίση με

$$\langle A \rangle = \sum_n |c_n|^2 a_n \quad (\text{διακριτού φάσματος [2]})$$

Επίσης για **συνεχές φάσμα** τιμών, αλλά θα είναι

$$\langle A \rangle = \int_{-\infty}^{+\infty} \alpha |c(\alpha)|^2 d\alpha.$$

Παρατηρούμε ότι η πιθανότητα εμφάνισης των δυνατών τιμών a_n είναι

$$P_n = \sum_n |c_n|^2.$$

Η **μέση τιμή του τελεστή** $\hat{A}$ με ιδιοτιμή a_n μιας ιδιοκατάστασης ψ_n θα είναι ίση με

$$\langle A \rangle = (\psi, \hat{A} \psi)$$

Η μέση τιμή ενός φυσικού μεγέθους που περιγράφεται από τον ερμιτιανό τελεστή $\hat{A}$ σε μια οποιαδήποτε κατάσταση Ψ , είναι ίση με

$$\langle A \rangle = \frac{(\psi, \hat{A} \psi)}{(\psi, \psi)} = \frac{\sum_n |c_n|^2 a_n}{\sum_n |c_n|^2}.$$

Αν μάλιστα η συνάρτηση είναι κανονικοποιημένη $(\psi, \psi) = 1$, τότε ισχύει

$$\langle A \rangle = \frac{(\psi, \hat{A} \psi)}{(\psi, \psi)} = (\psi, \hat{A} \psi).$$

Η **μέση τιμή του τελεστή** $\hat{A}^2$ δίνεται από την σχέση

$$\hat{A}^2 = (\psi, \hat{A}^2 \psi).$$

Επίσης με βάση όσα προαναφέρθηκαν για την μέση τιμή, ισχύουν για **διακριτές** τιμές φάσματος ότι

$$\langle A^2 \rangle = \sum_n |c_n|^2 \alpha_n^2$$

και για συνεχές φάσμα τιμών

$$\langle A^2 \rangle = \int |c(\alpha)|^2 \alpha^2 d\alpha.$$

Στην κλασσική φυσική κάθε παρατηρήσιμο μέγεθος μπορούμε να το προσδιορίσουμε ακριβώς ως προς την κατάσταση του μέσω των $\vec{x}, \vec{p}, t$. Στην κβαντική μηχανική σημασία έχει η πιθανότητα ένα σωματίδιο να βρίσκεται κάθε στιγμή κάπου στο χώρο. Αυτή την πιθανότητα την υπολογίζουμε μέσω των παρατηρήσιμων μεγεθών εισάγοντας την μέση τιμή θέσης, ορμής και γενικών μεγεθών κυματοσυναρτήσεων $\psi(x,t)$.

Η μέση τιμή της θέσης ενός σωματιδίου σε μία διάσταση, γνωρίζοντας την κυματοσυνάρτησή του $\psi(x)$ (§2.4) είναι $\langle x \rangle = \int_{-\infty}^{+\infty} xP(x)dx$. Όπως προαναφέρθηκε η πυκνότητα πιθανότητας είναι μια θετική ποσότητα που διατηρείται οπότε για να έχει νόημα η στατιστική της ερμηνεία θα πρέπει η ολική πιθανότητα $P(x,t) = \int_{-\infty}^{+\infty} |\psi(x,t)|^2 dx$ να είναι ανεξάρτητη του χρόνου. Τελικά η μέση τιμή της θέσης ενός σωματιδίου σε μία διάσταση είναι η

$$\langle x \rangle = \int_{-\infty}^{+\infty} x|\psi(x,t)|^2 dx$$

Με τροποποίηση εξάγεται η ισοδύναμη

$$\langle x \rangle = \int_{-\infty}^{+\infty} x\psi^*\psi dx = \int_{-\infty}^{+\infty} \psi^*(x\psi)dx.$$

Στην κβαντική μηχανική αν γνωρίζουμε την κατάσταση του σωματιδίου μπορούμε να υπολογίσουμε την ορμή του p , μέσω της θέσης του x . Έτσι η ορμή ενός σωματιδίου θα είναι

$$\langle p_x \rangle = m \frac{d\langle x \rangle}{dt}$$

Επίσης αποδεικνύεται ότι η μέση τιμή της ορμής θα είναι ίση με

$$\langle p_x \rangle = \int_{-\infty}^{+\infty} \psi^*(p_x\psi)dx = \int_{-\infty}^{+\infty} \psi^*(-i\hbar \frac{\partial}{\partial x})\psi dx.$$

Όταν έχουμε λοιπόν μία κυματοσυνάρτηση $\psi(x,t)$ με $\int_{-\infty}^{+\infty} |\psi|^2 dx = 1$, η μέση τιμή ορμής και θέσης θα δίνεται από τις σχέσεις :

$$\langle x \rangle = \int_{-\infty}^{+\infty} \psi^* (\hat{x} \psi) dx \quad \text{και} \quad \langle p_x \rangle = \int_{-\infty}^{+\infty} \psi^* (\hat{p}_x \psi) dx$$

Για οποιοδήποτε φυσικό μέγεθος A , η μέση τιμή του θα δίνεται από την σχέση

$$\langle A \rangle = \int_{-\infty}^{+\infty} \psi^* (\hat{A} \psi) dx$$

2.15 ΤΥΠΙΚΗ ΑΠΟΚΛΙΣΗ

Τυπική απόκλιση ή διασπορά ή αβεβαιότητα ενός μεγέθους A , ορίζουμε την ποσοτική συγκέντρωση μιας στατιστικής κατανομής [2] και δίνεται από την σχέση

$$(\Delta A)^2 = \langle A^2 \rangle - \langle A \rangle^2 \quad \text{ή} \quad (\Delta A) = \sqrt{\langle A^2 \rangle - \langle A \rangle^2}.$$

Διασπορά είναι το «ποσό απόκλισης» από τον υπολογισμό της μέσης τιμής ενός φυσικού μεγέθους θέσης, ορμής κ.τ.λ [2].

- Απόκλιση θέσης δίνεται από την $(\Delta x)^2 = \langle x^2 \rangle - \langle x \rangle^2$ ή $(\Delta x) = \sqrt{\langle x^2 \rangle - \langle x \rangle^2}$.
- Απόκλιση ορμής δίνεται από την $(\Delta p)^2 = \langle p^2 \rangle - \langle p \rangle^2$ ή $(\Delta p) = \sqrt{\langle p^2 \rangle - \langle p \rangle^2}$.

2.16 ΣΧΕΣΗ ΑΒΕΒΑΙΟΤΗΤΑΣ ΘΕΣΗΣ ΚΑΙ ΟΡΜΗΣ

Η αρχή της αβεβαιότητας ή απροσδιοριστίας (§1.4) δίνεται από την σχέση του Heisenberg:

$$\Delta x \Delta p_x \geq \frac{\hbar}{2}$$

Αν η κίνηση του σωματιδίου που περιγράφεται από την αρχή της αβεβαιότητας είναι εκτός της μιας διάστασης x και στον άξονα y αλλά και στον άξονα z , τότε αντίστοιχα έχουμε [2] ισχύει

$$\Delta y \Delta p_y \geq \frac{\hbar}{2} \quad \text{και} \quad \Delta z \Delta p_z \geq \frac{\hbar}{2}.$$

Η σχέση εκφράζει το διευρυμένο ή μη εύρος που έχει η κυματική συνάρτηση $\psi(x)$. Δηλαδή όσο μεγαλύτερο είναι το Δx τόσο πιο μεγάλο πλάτος καταλαμβάνει η καμπύλη της $\psi(x)$. Αντιστρόφως όσο μικρότερο είναι το Δx τόσο πιο στενή περιοχή καταλαμβάνει η $\psi(x)$. Κατά ανάλογο τρόπο όσο μεγαλύτερη αβεβαιότητα ορμής Δp , έχουμε τόσο πλατυτέρα καμπύλη του πλάτους πιθανότητας της κυματοσυνάρτησης των ορμών παρατηρείται. Αντιθέτως όσο μικρότερο Δp έχουμε τόσο πιο στένωση παρουσιάζει η κυματοσυνάρτηση των ορμών (σχήματα 1.2 και 1.3).

Ένα σωματίδιο κινούμενο στον άξονα x έχει αβεβαιότητα θέσης που δίνεται από την μαθηματική σχέση

$$\Delta x = \sqrt{\langle x^2 \rangle - \langle x \rangle^2}$$

Η αβεβαιότητα της ορμής του θα δίνεται από την μαθηματική σχέση

$$\Delta p_x = \sqrt{\langle p_x^2 \rangle - \langle p_x \rangle^2}.$$

2.17 ΘΕΜΕΛΙΩΔΕΙΣ ΑΡΧΕΣ



Σε κάθε φυσικό μέγεθος αντιστοιχεί ένας ερμιτιανός γραμμικός τελεστής μέσω των αντικαταστάσεων αναπαράστασης για την θέση και την ορμή [2], ως εξής:

$$\begin{cases} x \mapsto \hat{x} = x \\ p_x \mapsto \hat{p}_x = -i\hbar \frac{\partial}{\partial x} \end{cases} \quad \text{ή για περισσότερες από μία διαστάσεις} \quad \begin{cases} \vec{r} \mapsto \hat{\vec{r}} = \vec{r} \\ \vec{p} \mapsto \hat{\vec{p}} = -i\hbar \vec{\nabla} \end{cases}$$



Κάθε σύστημα στην κβαντομηχανική αντιπροσωπεύεται από μία κυματοσυνάρτηση $\psi(x,t)$ ή $\psi(\vec{r},t)$ η οποία εμπεριέχει όλες τις πληροφορίες και στην οποία δεν αντιστοιχεί κάποιο φυσικό μέγεθος και είναι μιγαδική συνάρτηση [2]. Μέσω του τετραγώνου της κυματοσυναρτήσεως μπορούμε να υπολογίσουμε την πυκνότητα πιθανότητας ενός σωματιδίου να βρεθεί σε κάποια περιοχή του χώρου ώστε $p = |\psi(x)|^2$.



Η μέση τιμή μετρήσεων ενός φυσικού μεγέθους A είναι ίση με

$$\langle A \rangle = (\psi, \hat{A} \psi) = \int_V \psi^* (\hat{A} \psi) dV$$

ή με χρήση του συμβόλου **bracket** [2]

$$\langle A \rangle = \langle \psi | \hat{A} | \psi \rangle$$

Η κυματοσυνάρτηση ψ είναι κανονικοποιημένη, ισχύει δηλαδή ότι

$$(\psi, \psi) = \int \psi^*(\vec{r})\psi(\vec{r})dV = 1$$

Για την περιγραφή ενός φυσικού μεγέθους μέσω μιας μη κανονικοποιημένης κυματοσυνάρτησης, η μέση τιμή θα είναι ίση με

$$\langle A \rangle = \frac{(\psi, \hat{A}\psi)}{(\psi, \psi)}.$$



Για δύο μεγέθη A και B ισχύει η **γενικευμένη σχέση αβεβαιότητας** [2]

$$\Delta A \Delta B \geq \frac{1}{2} \left| \langle [\hat{A}, \hat{B}] \rangle \right|$$



Οι τιμές που προκύπτουν κατά την μέτρηση ενός φυσικού μεγέθους A , είναι οι ιδιοτιμές λ_n του ερμιτιανού τελεστή $\hat{A}$. Αν η τιμή που προκύπτει κατά την μέτρηση ενός φυσικού μεγέθους A ως περιγραφή της κατάστασής του, είναι ιδιοτιμή λ_n της κυματοσυνάρτησης ψ , τότε και η κυματοσυνάρτηση ψ είναι η ιδιοκατάσταση του συστήματος [2].



Εάν η κυματοσυνάρτηση είναι $\psi = \sum_n c_n \psi_n$ τότε οι ιδιοτιμές του ερμιτιανού τελεστή που θα περιγράφουν το φυσικό σύστημα θα έχουν **πιθανότητα** [2] υπολογισμού ιδιοτιμής ίση με

$$P_n = |c_n|^2 = |(\psi_n, \psi)|^2.$$



Η χρονική εξέλιξη ενός συστήματος κβαντικής μηχανικής περιγράφεται από την εξίσωση του Schrödinger [2]

$$\hat{H}\psi = E\psi$$

όπου $\hat{H}$ ο τελεστής της χαμιλτονιανής του συστήματος που είναι ίσος με

$$\hat{H} = \hat{T} + V = \frac{-\hbar^2}{2m} \vec{\nabla}^2 + V(\vec{r})$$

Η εξίσωση $\hat{H}\psi_n(x) = E\psi_n(x)$ καλείται **εξίσωση ιδιοτιμών** της Χαμιλτονιανής.

2.18 Ο ΦΟΡΜΑΛΙΣΜΟΣ ΤΟΥ DIRAC

Στην κβαντική μηχανική αντιστοιχεί ένα διάνυσμα για κάθε δυναμική κατάσταση. Αυτά τα διανύσματα ο Dirac τα ονόμασε *ket* και συμβολίζονται από την Αγγλική λέξη *bracket* δηλαδή παρένθεση (ή αγκύλη) με το μαθηματικό σύμβολο $|\psi\rangle$. Η λέξη *bracket* είναι σύνθετη και το σύμβολο $|\dots\rangle$ καλείται *ket*. Με την ονομασία *bra* καλείται το σύμβολο $\langle\dots|$ και είναι το συζυγές του *ket* [2].

Οι κβαντομηχανικές καταστάσεις περιγράφονται από το διάνυσμα $|\psi\rangle$. Το διάνυσμα $|\psi\rangle$ εμπεριέχει χρονική εξάρτηση. Το εσωτερικό γινόμενο, οι μέσες τιμές, οι ιδιοτιμές, οι ιδιοσυναρτήσεις, η κανονικοποίηση, η πληρότητα και η ορθοκανονικότητα μπορούν να εκφραστούν με τον φορμαλισμό του Dirac ενσωματώνοντας στις μαθηματικές εκφράσεις το σύμβολο *bra* και *ket* [2].

■ Η γενική εξίσωση του Schrödinger [2] για μια κατάσταση $|\psi(t)\rangle$ μπορεί να γραφεί και με την μορφή:

$$\hat{H}|\psi(t)\rangle = i\hbar \frac{\partial}{\partial t} |\psi(t)\rangle .$$

■ Το εσωτερικό γινόμενο [2] δύο διανυσμάτων $|\psi_1\rangle$ και $|\psi_2\rangle$ συμβολίζεται με:

$$\langle\psi_1|\psi_2\rangle$$

και είναι ισοδύναμο με την

$$\langle\psi_1|\psi_2\rangle = (\langle\psi_1|, |\psi_2\rangle) . \quad 2.5$$

Ισχύουν οι εξής **ιδιότητες** εσωτερικού γινομένου για τα διανύσματα $|\psi_1\rangle$ και $|\psi_2\rangle$:

- $\langle\psi|\psi\rangle \geq 0 \Rightarrow |\psi\rangle = 0$
- $\langle\psi_1|\psi_2\rangle = \langle\psi_2|\psi_1\rangle^*$
- $\langle\phi|\lambda_1\psi_1 + \lambda_2\psi_2\rangle = \lambda_1\langle\phi|\psi_1\rangle + \lambda_2\langle\phi|\psi_2\rangle$
- $\langle\psi_1 + \psi_2|\phi_1 + \phi_2\rangle = \langle\psi_1|\phi_1\rangle + \langle\psi_1|\phi_2\rangle + \langle\psi_2|\phi_1\rangle + \langle\psi_2|\phi_2\rangle$

■ Κάθε φυσικό μέγεθος μπορεί να αντιπροσωπεύεται από ένα ερμιτιανό τελεστή $\hat{A}$ [2]. Αν ένας τελεστής $\hat{A}$ δράσει σε μια κατάσταση $|\psi\rangle$ τότε μέσω του φορμαλισμού θα ισχύει $\hat{A}|\psi\rangle = |\phi\rangle$.

■ Η μέση τιμή [2] κάθε φυσικού μεγέθους θα είναι:

$$\langle A \rangle = \frac{\langle \psi | \hat{A} | \psi \rangle}{\langle \psi | \psi \rangle}.$$

Αν η $|\psi\rangle$ είναι κανονικοποιημένη ώστε $\langle \psi | \psi \rangle = 1$, τότε η μέση τιμή θα γίνει

$$\langle \hat{A} \rangle = \langle \psi | \hat{A} | \psi \rangle.$$

■ Κάθε γραμμικός τελεστής [2] μπορεί να δράσει σε μία κατάσταση $|\psi\rangle = \sum_n c_n |\psi_n\rangle$ και να δώσει

$$\hat{A}|\psi\rangle = \hat{A}(\sum_n c_n |\psi_n\rangle) = \sum_n c_n \hat{A}|\psi_n\rangle.$$

■ Για το μήκος του $|\psi\rangle$ ισχύει ότι $\|\psi\|^2 = \langle \psi | \psi \rangle$. Αν $\|\psi\|^2 = 1$ τότε το $|\psi\rangle$ είναι κανονικοποιημένο.

■ Ένας γραμμικός τελεστής $\hat{A}$ όταν δράσει σε ένα $|\psi\rangle$ τότε θα είναι

$$\hat{A}|\psi\rangle = \lambda|\psi\rangle.$$

Ιδιοδιανύσματα του $\hat{A}$, καλούνται τα $|\psi\rangle$ και ιδιοτιμές καλούνται οι αριθμοί λ .

■ Συζυγής τελεστής του γραμμικού τελεστή $\hat{A}$ καλείται ο τελεστής $\hat{A}^+$. Ισχύει ότι

$$\langle \psi | \hat{A} | \phi \rangle = \langle \phi | \hat{A}^+ | \psi \rangle^*.$$

Αν $|\phi\rangle = |\psi\rangle$ τότε $\langle \psi | \hat{A} | \psi \rangle = \langle \psi | \hat{A}^+ | \psi \rangle^*$.

Στον φορμαλισμό Dirac ο συζυγής του $|\psi\rangle$ είναι ο $\langle \psi |$. Ο συζυγής του $|\psi\rangle = \hat{A}|\psi\rangle$ είναι το $\langle \phi | = \langle \psi | \hat{A}^+$. Επίσης ο συζυγής της κατάστασης $|\psi\rangle = \sum_n c_n |\psi_n\rangle$ είναι $\langle \psi | = \sum_n \langle \psi_n | c_n^*$.

■ Η **πληρότητα** ενός συστήματος (όταν δηλαδή τα διανύσματα $|\psi\rangle$ του αυτόσυσζυγούς τελεστή $\hat{A}$ αποτελούν ένα πλήρες σύστημα), δίνεται μέσω του **φασματικού θεωρήματος** [2]

$$|\psi\rangle = \sum_n c_n |\psi_n\rangle .$$

■ **Ορθοκανονικές** είναι οι ιδιοκαταστάσεις ενός ερμιτιανού τελεστή όταν $\langle \psi_n | \psi_m \rangle = \delta_{nm}$. Αν το $\langle \psi_n |$ είναι **κανονικοποιημένο** στην μονάδα τότε για την ορθοκανονικότητα ισχύει

$$\langle \psi_n | \psi_m \rangle = \delta_{nm} \Rightarrow \langle \psi_n | \psi_m \rangle = \begin{cases} 0 & n \neq m \\ 1 & n = m \end{cases}$$

Δηλαδή καλούνται **ορθογώνιες δύο καταστάσεις** $|\psi_n\rangle$ και $|\psi_m\rangle$ όταν με $n \neq m$ ισχύει ότι:

$$\langle \psi_n | \psi_m \rangle = 0 .$$

Η **σχέση πληρότητας** μπορεί να γραφεί και με την μορφή

$$|\psi\rangle = \sum_n c_n |\psi_n\rangle \Rightarrow \sum_n |\psi_n\rangle \langle \psi_n| = 1 .$$

2.19 ΤΟ ΣΠΙΝ

Το σπίν είναι ένα κβαντομηχανικό μέγεθος που χαρακτηρίζει κάθε σωματίδιο. Το σπίν δεν παρουσιάζει κάποια αναλογία με την κλασσική φυσική, απλά μέσω αυτού αποτυπώνεται ένας ιδιαίτερος χαρακτήρας που παρουσιάζεται σε κάθε σωματίδιο. Η κατάσταση κάθε σωματιδίου αποδείχθηκε πειραματικά ότι επηρεάζεται από την ύπαρξη της μαγνητικής ροπής ($\vec{m} = \frac{e\vec{L}}{2m_e c}$) των σωματιδίων κάτι που κατευθύνει την κβαντική μηχανική στην παραδοχή της εσωτερικής στροφορμής δηλαδή του σπίν [2].

Οι κανόνες της άλγεβρας της στροφορμής είναι ίδιοι και για το σπίν. **Επιλέγουμε συμβατικά την z συνιστώσα του σπίν**. Επομένως κατόπιν εύκολης απόδειξης ισχύουν τα εξής:

$$\begin{array}{ll}
\text{i.} & [\hat{S}_z, \hat{S}_x] = i\hbar \hat{S}_y \\
\text{ii.} & [\hat{S}_y, \hat{S}_z] = i\hbar \hat{S}_x \\
\text{iii.} & [\hat{S}_x, \hat{S}_y] = i\hbar \hat{S}_z \\
\text{iv.} & [\hat{S}_\eta, \hat{S}^2] = 0 \text{ με } \eta=1,2,3,.. \\
\text{v.} & [\hat{S}_x, \hat{S}^2] = [\hat{S}_y, \hat{S}^2] = [\hat{S}_z, \hat{S}^2] = 0 \\
\text{vi.} & [\hat{S}^2, \hat{S}_i] = 0 \text{ με } i=x,y,z
\end{array}$$

➤ Οι τελεστές $\hat{S}_z$ και $\hat{S}^2$ έχουν κοινά ιδιοδιανύσματα που συμβολίζονται με $|s, m_s\rangle$ και οι τιμές τους είναι $s = 0, \frac{1}{2}, 1, \frac{3}{2}, \dots$ και $m_s = -s, -s+1, \dots, s-1, s$. Ισχύει ότι:

$$\hat{S}^2 |s, m_s\rangle = \hbar^2 s(s+1) |s, m_s\rangle \quad \text{και} \quad \hat{S}_z |s, m_s\rangle = m_s \hbar |s, m_s\rangle$$

■ Σημείωση [2] :

Τα περισσότερα στοιχειώδη σωματίδια έχουν **ημιακέραιο σπίν**. Όπως το ηλεκτρόνιο e^- που έχει $s = \frac{1}{2}$, αλλά και το πρωτόνιο, νετρόνιο κ.α..

Για σωματίδιο με $s = \frac{1}{2}$ θα είναι $m_s = \frac{1}{2}, -\frac{1}{2}$.

Οι ιδιοκαταστάσεις με σπίν ημιακέραιο είναι οι λεγόμενες καταστάσεις με σπίν πάνω ($|+\rangle$ ή $|\uparrow\rangle$) και σπίν κάτω ($|-\rangle$ ή $|\downarrow\rangle$). Μπορούμε να γράψουμε συντομογραφικά για τις ιδιοκαταστάσεις ότι ισχύει:

$$|s, m_s\rangle = \left| \frac{1}{2}, \pm \frac{1}{2} \right\rangle \equiv |\pm\rangle \quad \text{ή} \quad \left| \frac{1}{2}, +\frac{1}{2} \right\rangle = |+\rangle \quad \text{και} \quad \left| \frac{1}{2}, -\frac{1}{2} \right\rangle = |-\rangle$$

■ Σημείωση [2] :

Συμβολίζουμε $\left| \frac{1}{2}, +\frac{1}{2} \right\rangle = |+\rangle = |\uparrow\rangle = |1_+\rangle$ και $\left| \frac{1}{2}, -\frac{1}{2} \right\rangle = |-\rangle = |\downarrow\rangle = |1_-\rangle$.

Για διανυσματικό χώρο της μορφής $|\psi\rangle = c_1|+\rangle + c_2|-\rangle$ με c_1, c_2 μιγαδικούς αριθμούς, η πιθανότητα να βρούμε σωματίδιο κατά την κίνησή του στην κατάσταση $|+\rangle$ είναι $P_+ = |c_1|^2$. Η πιθανότητα να βρούμε το σωματίδιο στην κατάσταση $|-\rangle$ είναι $P_- = |c_2|^2$.

Επίσης οι συντελεστές c_1, c_2 μπορούν να γραφούν ως γραμμικός συνδυασμός της $|\psi\rangle = c_1|+\rangle + c_2|-\rangle$, δηλαδή

$$c_1 = \langle +|\psi\rangle \text{ και } c_2 = \langle -|\psi\rangle.$$

Προφανώς ισχύουν

$$\langle +|-\rangle = 0, \quad \langle -|+\rangle = 0, \quad \langle +|+\rangle = 1, \quad \langle -|-\rangle = 1. \quad 2.6$$

Για την περιγραφή μιας κατάστασης του σπίν, μπορεί να γίνει χρήση και διανυσμάτων στήλης ως γραμμικός συνδυασμός των ιδιοδιανυσμάτων του $\hat{S}_z$

$$X = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \text{ ή } X = c_1 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + c_2 \begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ ή } X = c_1 X_+ + c_2 X_-$$

$$\text{ή } \langle X_+ | X_- \rangle = \begin{bmatrix} c_1^* & c_2^* \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = c_1^* c_1 + c_2^* c_2$$

■ Πίνακες του Pauli [2]:

Είναι οι πίνακες που έχουν στις τρεις συνιστώσες x, y, z την μορφή (μέσω των οποίων πρόκειται να εκφράσουμε τους τελεστές του σπίν στις αντίστοιχες συντεταγμένες):

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \text{ και } \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Οι τελεστές του σπίν μπορούν να γραφούν με την μορφή πινάκων. Χρησιμοποιώντας του πίνακες του Pauli οι τελεστές του σπίν θα γίνουν:

$$\hat{S}_x = \frac{\hbar}{2} \sigma_x = \frac{\hbar}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \hat{S}_y = \frac{\hbar}{2} \sigma_y = \frac{\hbar}{2} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \text{ και } \hat{S}_z = \frac{\hbar}{2} \sigma_z = \frac{\hbar}{2} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

δηλαδή ισχύει γενικά και για τις τρεις συνιστώσες ότι

$$\hat{S}_n = \frac{\hbar}{2} \sigma \quad (\text{με } n=x, y, z)$$

Προφανώς ισχύει ότι

$$\hat{S}^2 = \hat{S}_x^2 + \hat{S}_y^2 + \hat{S}_z^2 \Rightarrow \hat{S}^2 = \frac{3\hbar^2}{4} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

■ Υπολογισμός των ιδιοτιμών και ιδιοδιανυσμάτων των τελεστών $\hat{S}_x, \hat{S}_y, \hat{S}_z$ [2] :

Η εξίσωση ιδιοτιμών για το σπιν της συνιστώσας x είναι

$$\hat{S}_x |X_{\pm}\rangle = m_{s_x} |X_{\pm}\rangle \Rightarrow \hat{S}_x |X_{\pm}\rangle - m_{s_x} |X_{\pm}\rangle = 0 \Rightarrow (\hat{S}_x - m_{s_x} I) |X_{\pm}\rangle = 0$$

και για να έχει λύση πρέπει η οριζουσα να είναι μηδέν ώστε:

$$|\hat{S}_x - m_{s_x} I| = 0 \Rightarrow \left| \frac{\hbar}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} - m_{s_x} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right| = 0 \Rightarrow \boxed{m_{s_x} = \pm \frac{\hbar}{2}}$$

Επομένως οι ιδιοτιμές και των τριών τελεστών $\hat{S}_x, \hat{S}_y, \hat{S}_z$ αποδεικνύεται με τον ίδιο τρόπο ότι είναι $m_s = \pm \frac{\hbar}{2}$.

Τα ιδιοδιανύσματα θα συμβολίζονται με $|X_+\rangle = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$ και $|X_-\rangle = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$. Τα ιδιοδιανύσματα για τους τελεστές $\hat{S}_x, \hat{S}_y, \hat{S}_z$ είναι τα εξής:

■ Για τον τελεστή $\hat{S}_x$ είναι

$$\begin{aligned} \hat{S}_x |X_{\pm}\rangle = m_{s_x} |X_{\pm}\rangle &\Rightarrow \hat{S}_x |X_{\pm}\rangle - m_{s_x} |X_{\pm}\rangle = 0 \Rightarrow (\hat{S}_x - m_{s_x} I) |X_{\pm}\rangle = 0 \Rightarrow \\ &\left(\frac{\hbar}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \pm \frac{\hbar}{2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} = 0 \Rightarrow \begin{cases} c_1 = c_2 \\ c_1 = -c_2 \end{cases} \end{aligned}$$

Οπότε για τα ιδιοδιανύσματα ισχύει

$$\begin{cases} |X_+\rangle = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \\ |X_-\rangle = \begin{bmatrix} c_1 \\ -c_2 \end{bmatrix} \end{cases} \Rightarrow \begin{cases} I = \langle X_+ | X_+ \rangle \Rightarrow I = \begin{bmatrix} c_1^* & c_2^* \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ c_2 \end{bmatrix} \stackrel{c_1=c_2}{=} 2|c_1|^2 \Rightarrow c_1 = \frac{1}{\sqrt{2}} \\ I = \langle X_- | X_- \rangle \Rightarrow I = \begin{bmatrix} c_1^* & -c_2^* \end{bmatrix} \cdot \begin{bmatrix} c_1 \\ -c_2 \end{bmatrix} \stackrel{c_1=-c_2}{=} 2|c_1|^2 \Rightarrow c_1 = \frac{1}{\sqrt{2}} \end{cases}$$

Τελικά για το ιδιοδιάνυσμα του τελεστή $\hat{S}_x$ είναι:

$$\text{Για ιδιοτιμή } m_{s_x} = +\frac{\hbar}{2} \text{ το ιδιοδιάνυσμα είναι } |X_+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}.$$

$$\text{Για ιδιοτιμή } m_{s_x} = -\frac{\hbar}{2} \text{ το ιδιοδιάνυσμα είναι } |X_-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}.$$

Επίσης η ιδιοκατάσταση του τελεστή $\hat{S}_x$ μπορεί να διαμορφωθεί ως γραμμικός συνδυασμός των ιδιοδιανυσμάτων $|+\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ και $|-\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ με την μορφή

$$|X_+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} |+\rangle + \frac{1}{\sqrt{2}} |-\rangle \Rightarrow |X_+\rangle = \frac{1}{\sqrt{2}} (|+\rangle + |-\rangle)$$

$$\text{και } |X_-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \end{bmatrix} - \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} |+\rangle - \frac{1}{\sqrt{2}} |-\rangle \Rightarrow |X_-\rangle = \frac{1}{\sqrt{2}} (|+\rangle - |-\rangle)$$

Ομοίως με την ίδια διαδικασία υπολογίζονται και για τους τελεστές $\hat{S}_y, \hat{S}_z$ τα ιδιοδιανύσματα τους. Οπότε προκύπτουν τα εξής:

■ Για τον τελεστή $\hat{S}_y$ [2] :

$$\text{με ιδιοτιμή } m_{s_y} = +\frac{\hbar}{2} \text{ το ιδιοδιάνυσμα είναι } |X_+\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix},$$

$$\text{με ιδιοτιμή } m_{s_y} = -\frac{\hbar}{2} \text{ το ιδιοδιάνυσμα είναι } |X_-\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix}.$$

■ Για τον τελεστή $\hat{S}_z$ [2] :

$$\text{με ιδιοτιμή } m_{s_z} = +\frac{\hbar}{2} \text{ το ιδιοδιάνυσμα είναι } |X_+\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\text{με ιδιοτιμή } m_{s_z} = -\frac{\hbar}{2} \text{ το ιδιοδιάνυσμα είναι } |X_-\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Στον επόμενο πίνακα φαίνονται συνολικά οι ιδιοτιμές και τα ιδιοδιανύσματα του σπίν στους άξονες x, y, z:

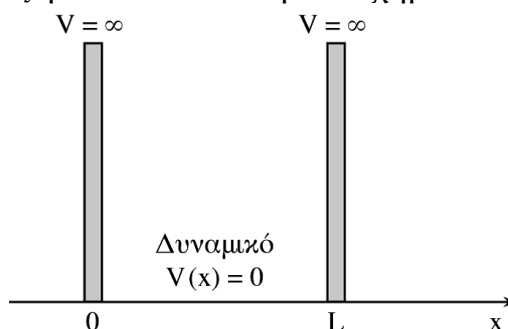
Άξονας μέτρησης του σπίν	Ιδιοτιμές	Ιδιοδιανύσματα
x	$+\frac{\hbar}{2}, -\frac{\hbar}{2}$	$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$
y	$+\frac{\hbar}{2}, -\frac{\hbar}{2}$	$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}, \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix}$
z	$+\frac{\hbar}{2}, -\frac{\hbar}{2}$	$\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Για το σπιν S με $s = \frac{1}{2}$ η μορφή του σε πίνακα (για τις τρεις συνιστώσες χρησιμοποιώντας του πίνακες του Pauli [2]) θα είναι

$$\hat{S}_x = \frac{\hbar}{2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \hat{S}_y = \frac{\hbar}{2} \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad \text{και} \quad \hat{S}_z = \frac{\hbar}{2} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

2.20 ΠΗΓΑΔΙ ΔΥΝΑΜΙΚΟΥ

Έστω σωματίδιο που κινείται εντός του πηγαδιού απείρου βάθους υπό την επίδραση δυναμικού όπως φαίνεται στο επόμενο σχήμα.



Σχήμα 2.1 [2]

Το πρόβλημα κίνησης εντός πηγαδιού απείρου βάθους έγκειται στον υπολογισμό των καταστάσεων συγκεκριμένης ενέργειας με το δυναμικό να έχει τιμές στο απειρόβαθο πηγάδι [2] ίσες με

$$V(x) = \begin{cases} +\infty & x < 0, x > L \\ 0 & 0 \leq x \leq L \end{cases}$$

Το σωματίδιο επειδή τα τοιχώματα του πηγαδιού είναι απείρου ύψους θέλει άπειρη ενέργεια για να διαφύγει από αυτές τις περιοχές δυναμικού, κάτι που δεν είναι δυνατόν να πραγματοποιηθεί (δηλαδή να αποκτήσει άπειρη ενέργεια και να διαφύγει από τα τοιχώματα). Η κυματοσυνάρτηση με συγκεκριμένη ενέργεια θα είναι η $\Phi(x, t) = \psi(x)e^{\frac{iE}{\hbar}t}$. Η $\psi(x)$ είναι ιδιοσυνάρτηση που παίρνει τιμές 0, για όρια κίνησης $x=0$ και $x=L$. Τελικά οι ιδιοσυναρτήσεις είναι οι εξής [2]:

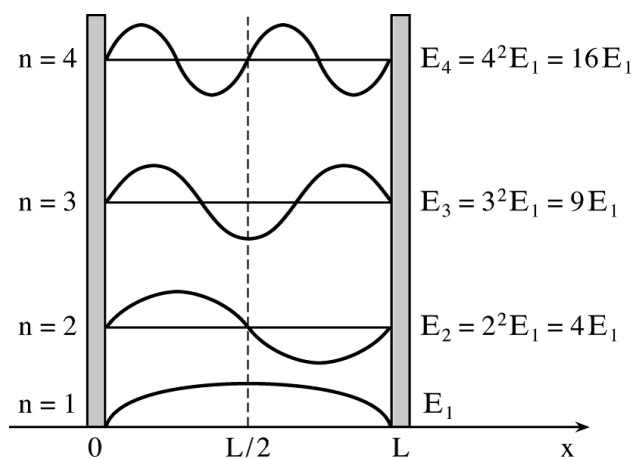
$$\psi(x) = \begin{cases} 0 & x > L, x < 0 \\ \sqrt{\frac{2}{L}} \sin \frac{n\pi}{L} x & 0 \leq x \leq L \end{cases}$$

Το ενεργειακό φάσμα θα δίνεται από την σχέση

$$E_n = n^2 \frac{\pi^2 \hbar^2}{2mL^2}$$

με τον κβαντικό αριθμό να είναι $n=1,2,3,\dots$

Οι κυματοσυναρτήσεις για διεγερμένες καταστάσεις $n=1,2,3,\dots$, έχουν τις ακόλουθες μορφές του σχήματος 2.2 :



Σχήμα 2.2 [2]

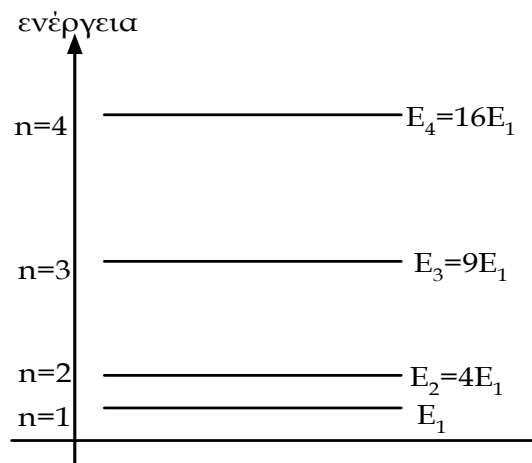
■ Παρατηρήσεις [2]:

- Το ενεργειακό φάσμα είναι πάντα ανάλογο της ενεργειακής πρώτης στάθμης ώστε

$$E_n = n^2 E_1 \quad \text{όπου} \quad E_1 = \frac{\pi^2 \hbar^2}{2mL^2} .$$

- Οι ιδιοσυναρτήσεις είναι άρτιες και περιττές. Το δυναμικό είναι συμμετρικό ως προς το κέντρο του.
- Όταν η θέση του σωματιδίου είναι στην βάση του πηγαδιού η ολική ενέργεια απειρίζεται και ο μόνος όρος που επιδρά στην ολική ενέργεια είναι η κινητική καθώς η δυναμική είναι μηδέν.

- Όσο πιο μικρή είναι η περιοχή που κινείται το σωματίδιο τόσο θα έχει μεγαλύτερη ενέργεια και η απόσταση μεταξύ των ενεργειακών σταθμών θα αυξάνεται.
- Όταν τείνει η μάζα $m \rightarrow 0$ και το μήκος $L \rightarrow 0$, τότε η ελάχιστη ενέργεια του σωματιδίου ανεβαίνει αρκετά πάνω από το βάθος του πυθμένα του πηγαδιού.
- Σε εφαρμογές οπτοηλεκτρονικής το κβαντικό πηγάδι δυναμικού σχηματίζεται όταν ανάμεσα σε 2 υμένια υλικού ευρέως χάσματος, παρεμβάλλεται υλικό μικρότερου χάσματος (π.χ. GaAs/AlAs/GaAs).
- Το διάγραμμα των ενεργειακών σταθμών ενός σωματιδίου έχει την μορφή του σχήματος.



Σχήμα 2.3 [2]

*«Είναι δύσκολο να αντιτάσσεται κανείς στις επιθυμίες του,
γιατί ότι θέλει το αγοράζει με τίμημα την ψυχή του».*

Ηράκλειτος

ΚΕΦΑΛΑΙΟ 3^ο

ΚΒΑΝΤΙΚΑ ΠΑΡΑΔΟΞΑ

3.1 Η ΕΝΝΟΙΑ ΤΗΣ ΥΠΕΡΘΕΣΗΣ

Η έννοια της υπέρθεσης αφορά όλα τα κύματα που ερμηνεύονται μέσω των γραμμικών εξισώσεων και είναι μια έννοια θεμελιώδης στην κβαντική φυσική. Η **αρχή της υπέρθεσης ή αρχή της επαλληλίας**, είναι βασική για τα κβαντικά συστήματα και την θεωρία τους. Σύμφωνα με αυτήν, για κάθε γραμμικό σύστημα το ολικό αποτέλεσμα ενός φαινομένου που αποτελείται από επί μέρους φαινόμενα, είναι ίσο με το άθροισμα των επί μέρους αποτελεσμάτων [12]. Κάθε κβαντικό σύστημα μπορεί να βρεθεί σε καταστάσεις υπερθέσεως δύο βασικών (ή και περισσότερων) καταστάσεων και θα αποδίδεται από την μαθηματική έκφραση που εμπερικλείει τα πλάτη πιθανότητας. Συγκεκριμένα έστω ένα άτομο υδρογόνου

(χαρακτηριστικό κβαντικό σύστημα το οποίο μελετήθηκε στην §1.5) που βρίσκεται στην θεμελιώδη κατάσταση, και το 0 αντιπροσωπεύεται από την ηλεκτρονιακή κατάσταση $|+\rangle$ ενώ το 1, από την κατάσταση $|-\rangle$. Τότε κάθε δυνατή κατάσταση θα είναι γραμμικός συνδυασμός της εξής μορφής:

$$|\psi\rangle = \alpha|+\rangle + \beta|-\rangle \quad 3.1$$

Αυτή η σχέση [1,11] που αποδίδει το διάνυσμα της κατάστασης $|\psi\rangle$ είναι η μαθηματική έκφραση της **υπέρθωσης**.

Τα πλάτη πιθανότητας είναι οι μιγαδικοί αριθμοί α και β και θα ισχύει

$$|\alpha|^2 + |\beta|^2 = 1 \quad 3.2$$

Από την έννοια της υπέρθεσης μπορούμε να καταλάβουμε πως δεν υπάρχει ακριβή δυνατότητα μέτρησης της κατάστασης ενός κβαντικού συστήματος (και ειδικότερα όπως θα αναπτύξουμε στο Β' μέρος, ενός κβαντικού υπολογιστή) που βρίσκεται σε υπέρθεση δύο (ή και περισσότερων) καταστάσεων. Η δυνατότητα που μας παρέχεται είναι ο σαφής υπολογισμός μιας εκ των δύο καταστάσεων.

Η μαθηματική έκφραση της επαλληλίας με τις δύο καταστάσεις να είναι οι $|+\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ και $|-\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$, σε μορφή πίνακα θα είναι η εξής:

$$|\psi\rangle = \alpha|+\rangle + \beta|-\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}.$$

Εάν επιλέξουμε να δράσει στην κατάσταση $|\psi\rangle$ ένας τυχαίος τελεστής ο οποίος έχει την μορφή του πίνακα, έστω ο $\hat{A} = \begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{bmatrix}$ τότε, αν η αρχική

κατάσταση $|\psi\rangle$ είναι έστω η $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$, τότε αυτή η κατάσταση θα μεταβεί σε μια νέα κβαντική κατάσταση υπέρθεσης, η οποία θα είναι δίνεται από την $|\phi\rangle$ και η οποία θα είναι ισοδύναμα $\hat{A} \cdot |\psi\rangle = |\phi\rangle$, οπότε

$$\hat{A} \cdot |\psi\rangle = |\phi\rangle \Rightarrow \begin{bmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix}$$

Τελικά το αποτέλεσμα της δράσης ενός τυχαίου τελεστή θα είναι η κατάσταση

$$|\phi\rangle = \begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{bmatrix} \quad \text{ή} \quad |\phi\rangle = \frac{1}{2}|+\rangle + \frac{\sqrt{3}}{2}|-\rangle$$

Παρατηρούμε ότι το άθροισμα των πιθανοτήτων είναι όντως σύμφωνα με την σχέση 3.2, ίσο με 1 καθώς

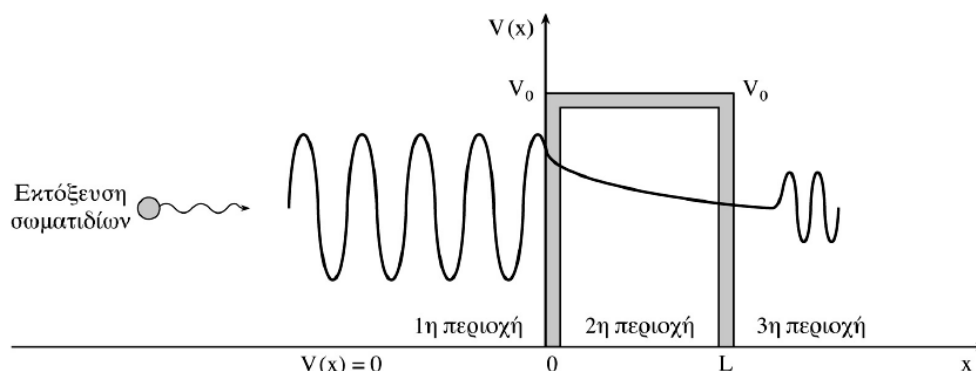
$$|\alpha|^2 + |\beta|^2 = \frac{1}{4} + \frac{3}{4} = 1.$$

3.2 ΚΒΑΝΤΙΚΗ ΣΗΡΑΓΓΑ

Ιδιαίτερο γνώρισμα επίσης της κβαντικής μηχανικής είναι η **κβαντική σήραγγα**. Το φαινόμενο, το σωματίδιο να εισέλθει στο φράγμα του δυναμικού αλλά και να διέλθει από το φράγμα δυναμικού καλείται φαινόμενο σήραγγας [2].

Το παράδοξο του φαινομένου της κβαντικής σήραγγας και η απόκλιση από την κλασσική λογική είναι στο ότι το σωματίδιο αν και προσπίπτει στο ενεργειακό φράγμα, ενδέχεται στον μικρόκοσμο να διαρρεύσει μέσα στο φράγμα και να διέλθει από την άλλη πλευρά του φράγματος (όπως επίσης μέρος του σωματιδίου μπορεί και να ανακλαστεί). Το ενδιαφέρον εδώ είναι πως ακόμη κι αν το σωματίδιο έχει πολύ μικρή ενέργεια για να ξεπεράσει το φράγμα, είναι αρκετά πιθανό να δημιουργήσει μια σήραγγα μέσα σε αυτό και να εξέλθει από το φράγμα ακολουθώντας την εκθετική μορφή του συντελεστή διέλευσης, κατά την διέλευση του φράγματος. Με «άλλα λόγια» μπορούμε να πούμε πως όταν ένας μεγάλος αριθμός σωματιδίων βρεθεί στη μία περιοχή ένα μικρό ποσοστό σωματιδίων θα καταφέρει να διαπεράσει το φράγμα (3^η περιοχή του επόμενου σχήματος 3.1) [2].

Λόγω του φαινομένου της σήραγγας σήμερα μας δίνεται η δυνατότητα χρήσης κινητών τηλεφώνων αλλά και σύγχρονων ηλεκτρονικών υπολογιστών, καθώς τα σημερινά chips των ηλεκτρονικών πλακετών βασίζονται στην λειτουργική τους δομή στο φαινόμενο της κβαντικής σήραγγας.



Σχήμα 3.1 [2]

Ένα προσπίπτον σωματίδιο πάνω σε φράγμα δυναμικού με ύψος δυναμικού V_0 θα αποτελείται από δύο αρμονικές κυματοσυναρτήσεις για τις περιοχές 1 και 3, και θα ακολουθεί εκθετική φθίνουσα πορεία για την 2^η περιοχή [2].

3.3 ΤΟ ΚΒΑΝΤΙΚΟ ΝΟΜΙΣΜΑ

Χαρακτηριστικό παράδειγμα εφαρμογής της κβαντικής υπέρθεσης είναι το κβαντικό νόμισμα. Έστω, ότι διαθέτουμε ένα νόμισμα του οποίου, αποτυπώνεται από ένα κλασσικό υπολογιστή κάθε φορά μετά από ένα «στρίψιμο», η πλευρά του. Τότε κάθε φορά μετά από ένα «στρίψιμο» του ο υπολογιστής θα δείχνει «Κορόνα» ή «Γράμματα» δηλαδή το νόμισμα θα είναι κάθε φορά σε μια μόνο από τις δύο θέσεις.

Στην κβαντική φυσική (και στον κβαντικό υπολογιστή) όμως, το νόμισμα μπορεί να δείχνει 25% κορόνα και 75% γράμματα. **Επίσης όμως**, μπορεί να δείχνει και 33% γράμματα και 67% κορόνα. Το νόμισμα δηλαδή, μπορεί να έχει οποιαδήποτε θέση [1, 14] μεταξύ των δύο πλευρών του και μόλις μετρηθεί η θέση του, να πάρει τελικά εκείνη που θα του έχει δείξει η τοποθέτησή μας και η βαρύτητα του στο τραπέζι.

Στην κλασσική φυσική λοιπόν, το νόμισμα μπορεί να βρεθεί μόνο στην κατάσταση «Κορόνα» ($|K\rangle$) ή στην κατάσταση «Γράμματα» ($|Γ\rangle$). Στην κβαντική φυσική, το νόμισμα δεν φέρει τις ίδιες ιδιότητες, αλλά το διάνυσμα της κατάστασης του μπορεί να έχει οποιαδήποτε τιμή είτε $|K\rangle$ είτε $|Γ\rangle$ είτε υπέρθεση αυτών των δύο καταστάσεων (§ 3.1) του και η κβαντική του κατάσταση θα δίνεται από την σχέση :

$$|\psi\rangle = \alpha|K\rangle + \beta|Γ\rangle$$

Παρατηρούμε πως όταν το νόμισμα βρίσκεται στην θέση «Κορόνα» η πιθανότητα να παρατηρήσουμε το νόμισμα στην κατάσταση $|K\rangle$ είναι $|\alpha|^2$, ενώ στην θέση «Γράμματα» είναι $|\beta|^2$. Θα πρέπει να είναι $|\alpha|^2 + |\beta|^2 = 1$. Υπενθυμίζεται ότι τα α και β είναι μιγαδικοί αριθμοί.

Σε μορφή πινάκων, η κβαντική κατάσταση του νομίσματος μπορεί να εκφραστεί ως «Κορόνα» με $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ή «Γράμματα» $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$.

3.4 ΜΗ ΤΟΠΙΚΟΤΗΤΑ

Στην κβαντική μηχανική οι φυσικοί έχουν αποδείξει την μη τοπικότητα, δηλαδή το ότι δύο κβαντικά σωματίδια μπορούν να διατηρήσουν επαφή όσο μακριά και αν βρίσκονται. Επομένως η ακαριαία επικοινωνία μεταξύ απομακρυσμένων κβαντικών αντικειμένων στην κβαντική φυσική είναι χαρακτηριστικό του κόσμου της και αυτή η μη τοπικότητα (δηλαδή η αυτόματη επικοινωνία απομακρυσμένων στοιχείων του κβαντικού κόσμου) οφείλεται στην φύση των κυματοσυναρτήσεων. Η υπέρθεση (δηλαδή η δυνατότητα που έχει ένα σωματίδιο να έχει συνδυασμό καταστάσεων την ίδια χρονική στιγμή) σε συνδυασμό με την μη τοπικότητα (δηλαδή π.χ. δύο σωματίδια μπορούν να διατηρήσουν επαφή έστω και αν το ένα είναι στο γήινο περιβάλλον και το άλλο σε κάποιο πολύ μακρινό πλανήτη [13]), δημιουργούν την βάση ύπαρξης μιας κυματοσυνάρτησης που περιγράφει την εμπλεκόμενη κατάσταση των σωματιδίων και το πείραμα που το αποτυπώνει είναι το EPR.

Έστω ότι διαθέτουμε μια πηγή εκπομπής φωτονίων (ανα ζεύγη), τα οποία προκύπτουν από την «εξαθλώση» ηλεκτρονίων με το ποζιτρόνιο (το αντισωματίο των ηλεκτρονίων με θετικό φορτίο). Η ΑΔΣΟ (αρχή διατήρησης στροφορμής) ορίζει ότι η συνολική στροφορμή του συστήματος των δύο φωτονίων πρέπει να είναι ίση με μηδέν (και ίση με αυτήν του e^- και e^+ [44]). Άρα αν το ένα σωματίο έχει spin +1, τότε το άλλο σωματίο θα πρέπει να έχει spin -1 (κατά τον ίδιο άξονα περιστροφής). Όμως όπως προαναφέρθηκε στην ερμηνεία της σχολής της Κοπεγχάγης (§2.2) αλλά και με βάση την αρχή της αβεβαιότητας (§1.4), η κατάσταση του spin για κάθε ένα εκ των δύο φωτονίων έχει 50% πιθανότητα να είναι είτε + είτε -.

Έστω τώρα δύο παρατηρητές A και B, οι οποίοι λαμβάνουν από την πηγή των φωτονίων ένα φωτόνιο ο καθένας. Με το **πείραμα EPR** αποδείχθηκε ότι αν ο παρατηρητής A κάνει μια μέτρηση του spin του φωτονίου που λαμβάνει, τότε ο παρατηρητής B παραδόξως, δεν θα ξέρει ακριβώς την τιμή που θα πάρει το spin του

δικού του φωτονίου, οπότε η αμοιβαία κατάρρευση της κυματοσυνάρτησης λαμβάνει χώρα στιγμιαία, ανεξαρτήτως της απόστασης που χωρίζει τα δύο σωματίδια (η ανταλλαγή πληροφοριών γίνεται με την ταχύτητα του φωτός). Η ένωση αυτή των σωματίων (και για κάθε τύπου σωματίο) ονομάζεται όπως θα αναλύσουμε σε επόμενη παράγραφο κβαντική διεμπλοκή και την χρησιμοποιούμε για την κβαντική κρυπτογραφία την οποία θα μελετήσουμε στο 9^ο κεφάλαιο. Επομένως σύμφωνα με το κβαντικό πείραμα EPR [13] όσο και αν απομακρύνουμε μεταξύ τους δύο εμπλεκόμενα σωματίδια αυτά παραμένουν συνδεδεμένα μέσω της κυματοσυνάρτησης που περιγράφει την κοινή τους κατάσταση. Όταν όμως γίνει μια μέτρηση ακρίβειας της θέσης του πρώτου σωματιδίου (ή οποιασδήποτε ιδιότητάς του) τότε καταρρέει η κοινή τους κυματοσυνάρτηση και το δεύτερο σωματίδιο αποκτά εκείνη την στιγμή την ιδιότητα του πρώτου. Αυτή η δράση αποτελεί την βάση της τεχνολογίας των κβαντικών υπολογιστών που πραγματεύεται αυτή η εργασία.

3.5 ΑΠΟΣΥΝΟΧΗ

Η αποσυννοχή είναι μια πραγματική διαδικασία της φύσης και συμβαίνει κάθε φορά όπου κάποιο κβαντικό σύστημα είναι μέλος ενός μακροσκοπικού συστήματος ενός φυσικού περιβάλλοντος και η κυματική του συνάρτηση συμπλέκεται με αυτό το μακροσκοπικό περιβάλλον με μια ουσιαστικά πολύπλοκη κατάσταση που μπορεί να είναι κάθε μορφής, την οποία εμείς θα την εξετάσουμε από την σκοπιά των ηλεκτρονικών υπολογιστικών διατάξεων. Αν το κβαντικό σύστημα συνδέεται πολύ ισχυρά με το εξωτερικό μακροσκοπικό περιβάλλον η κβαντική υπέρθεση εξασθενεί ή πιο σωστά χάνεται άμεσα. Ουσιαστικά η αποσυννοχή δείχνει την εξαφάνιση της κβαντικής υπέρθεσης όταν ένα κβαντικό σύστημα συνδέεται με κάποιο τρόπο με το περιβάλλον [13].

Η αποσυννοχή χρησιμοποιεί τον ήδη υπάρχοντα κβαντομηχανικό φορμαλισμό. Η ερμηνεία της βασίζεται στην συνεχή αλληλεπίδραση ενός κβαντικού συστήματος με το περιβάλλον του. Υποστηρίζει πως δεν υπάρχουν σε επίπεδο πρώτων αρχών απομονωμένα κβαντικά συστήματα στην φυσική κατάσταση και αυτή η συνεχής αλληλεπίδραση καθίσταται τελικά υπεύθυνη για την μετάβαση από τον κβαντομηχανικό κόσμο των υπερθέσεων και των πιθανοτήτων στον κλασικό μακρόκοσμο.

Στοιχεία του μαθηματικού φορμαλισμού της αποσυννοχής χρησιμοποιούνται και σε άλλες κατηγορίες ερμηνειών. Παρ' όλα αυτά, το παράδοξο της μέτρησης δεν λύνεται επί της ουσίας μέσω της συγκεκριμένης προσέγγισης της αποσυννοχής. Η

ερμηνεία της πάντως δίνει βαρύτητα στην συνεχόμενη αλληλεπίδραση κβαντικών συστημάτων, σε ένα τέτοιο πλαίσιο θεώρησης γνωστό ως το φαινόμενο της κβαντικής διεμπλοκής [14,15].

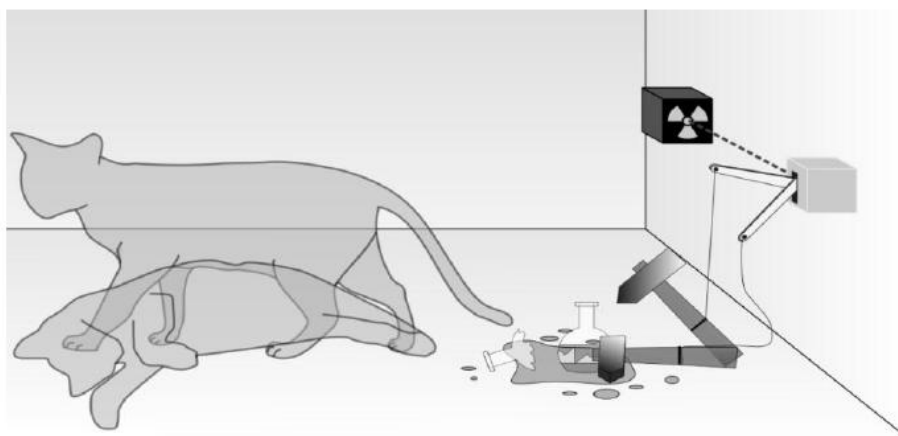
3.6 ΚΒΑΝΤΙΚΗ ΔΙΕΜΠΛΟΚΗ

Ένα από τα σημαντικά κβαντικά παράδοξα είναι το νοητό πείραμα που επινόησε ο **Erwin Schrödinger** το 1935 σύμφωνα με το οποίο μια γάτα μπορεί να είναι ταυτόχρονα ζωντανή και νεκρή (και συνοδεύτηκε από την δημιουργία του όρου κβαντική υπέρθεση αλλά και κβαντικές διεμπλεκόμενες καταστάσεις). Σύμφωνα με το νοητό πείραμα, μια γάτα κλείνεται σε θάλαμο για μέγιστη διάρκεια μιας ώρας, μαζί με μια διάταξη (πηγή ακτινοβολίας, με μηχανισμό μετρητή Geiger για την ακτινοβολία [9]) η οποία είναι ένα κβαντικό σύστημα που βρίσκεται σε επαλληλία καταστάσεων εκπομπής και μη εκπομπής (ισοπύθνα να εκπνευθεί ή όχι ακτινοβολία) εντός της εμβέλειας κίνησής της γάτας, στην οποία υπάρχει μια μικρή ποσότητα ραδιενεργής ουσίας ικανής ισοπύθνα να διασπάσει ή όχι ένα από τα άτομα της, στην χρονική διάρκεια της μιας ώρας. Εάν λοιπόν ενεργοποιηθεί ο μετρητής ελευθερώνεται από μια μικρή φιάλη υδροκυάνιο. Όταν ανοίξουμε τον θάλαμο (και καταρρεύσει η κυματοσυνάρτηση εξαιτίας της μέτρησης δηλαδή καταστραφεί η υπέρθεση), η γάτα θα είναι ή μόνο ζωντανή ή μόνο νεκρή, όχι όμως και τα δύο .

Συνεπώς μπορούμε να υποθέσουμε ότι η γάτα είναι ακόμα ζωντανή, εάν στο μεταξύ δεν έχει διασπαστεί κάποιο άτομο στην διάρκεια της μιας ώρας. Η κυματική συνάρτηση (§ 2.2) του συστήματος μπορεί να εκφράσει, αν υπάρχει σε αυτή την χρονική διάρκεια η ζωντανή και η νεκρή γάτα. Αν η γάτα επιζεί, θυμάται μόνο ότι ήταν ζωντανή.

Δημιουργείται πλέον το ερώτημα πότε παύει ένα κβαντικό σύστημα ή ένας μηχανισμός να υπάρχει σε μια κβαντική υπέρθεση καταστάσεων και γίνεται «το ένα ή το άλλο»; Σαφείς επεξηγήσεις απαιτούν για μακροσκοπικά αντικείμενα, όπως οι γάτες και οι φορητοί υπολογιστές, μια διαφορετική περιγραφή από αυτή που παρέχεται με την κλασσική μορφή της φυσικής λογικής.

Μπορούμε επομένως να ορίσουμε ως **κβαντική διεμπλοκή** [1, 8] δύο κβαντικά συστήματα τα οποία βρίσκονται σε κατάσταση η οποία δεν μπορεί να αποδοθεί με το τανυστικό (§ 2.1) γινόμενο των βασικών τους καταστάσεων.



Σχήμα 3.2 [9]

Η γάτα του Schrodinger: Μια γάτα, μια φιάλη με δηλητήριο και μια ραδιενεργή πηγή τοποθετούνται μέσα σε σφραγισμένο κουτί. Αν ο εσωτερικός ελεγκτής ανιχνεύσει ραδιενέργεια (π.χ. μια διάσπαση ατόμου) η φιάλη θρυμματίζεται, ελευθερώνοντας το δηλητήριο που σκοτώνει την γάτα. Η θεώρηση της Κοπεγχάγης (§2.2) για τη κβαντομηχανική υπονοεί ότι μετά από λίγο η γάτα είναι ταυτόχρονα ζωντανή και νεκρή. Όμως όταν κάποιος κοιτάει στο κουτί την βλέπει είτε ζωντανή είτε νεκρή [9].

ΜΕΡΟΣ Β΄

ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ

*Μόνο δύο πράγματα είναι απέραντα:
Το σύμπαν και η ανθρώπινη ανοησία.
Για το πρώτο δεν είμαι καθόλου σίγουρος.*

Άλμπερτ Αϊνστάιν

ΚΕΦΑΛΑΙΟ 4^ο

ΒΑΣΙΚΕΣ ΕΝΝΟΙΕΣ ΚΑΙ ΣΤΟΙΧΕΙΑ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

4.1 ΕΙΣΑΓΩΓΗ ΣΤΟΥΣ ΚΒΑΝΤΙΚΟΥΣ ΥΠΟΛΟΓΙΣΤΕΣ

Στις αρχές του 1980 οι Feynman και Benioff παρουσίασαν στο ευρύ κοινό την πρώτη ιδέα για τον κβαντικό υπολογιστή και υποστήριξαν ότι οι κβαντικοί υπολογιστές είναι το μέλλον της επιστήμης στους υπολογιστές. Στην εξέλιξη του χρόνου [17] αρκετοί επιστήμονες που ασχολούνται με την κβαντική μηχανική υποστήριξαν πως η λύση για την επίτευξη της επεξεργασίας μεγάλου όγκου δεδομένων σε ελάχιστο χρόνο θα παρέχεται από τους κβαντικούς υπολογιστές καθώς θα προσφέρουν μεγάλες ταχύτητες επεξεργασίας. Οι υπολογιστές αυτοί στηρίζουν τη λειτουργία τους στα κβάντα (άτομα, ιόντα ή μόρια [26]). Δεν υπάρχει φυσικός νόμος

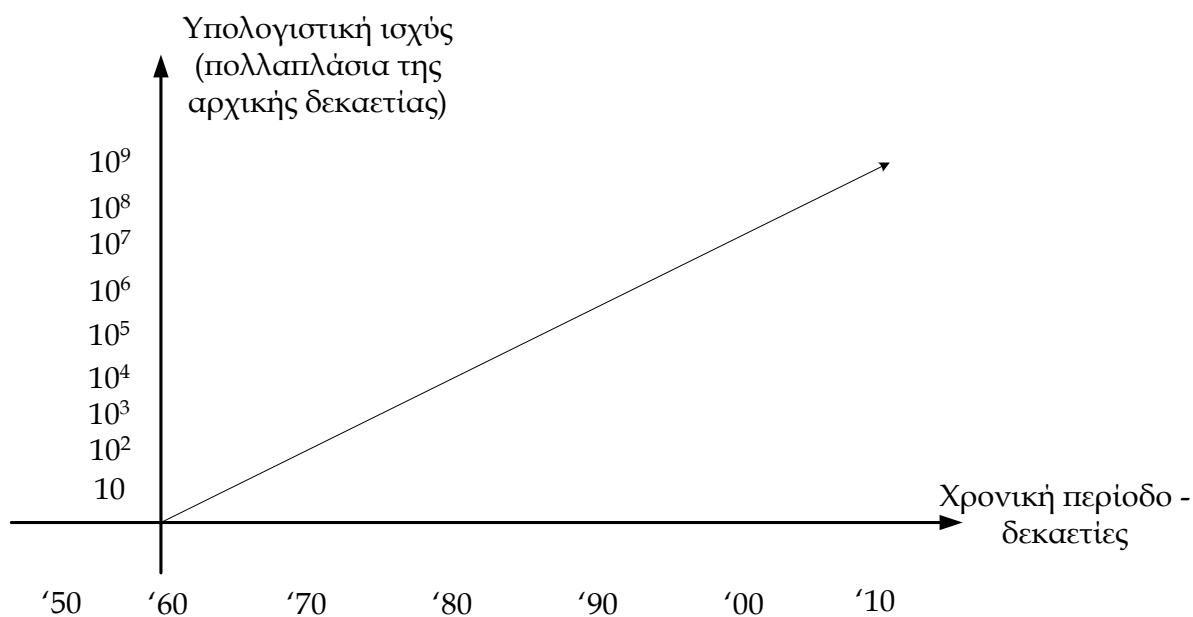
που να «απαγορεύει» τη σμίκρυνση των bits στο μέγεθος ενός ατόμου (δηλαδή τα γνωστά qubits όπως θα αναπτύξουμε στην επόμενη παράγραφο).

Στους κβαντικούς υπολογιστές υπάρχει η μονάδα κβαντικής πληροφορίας όπως αντίστοιχα υπάρχει στους κλασσικούς ηλεκτρονικούς υπολογιστές η μονάδα πληροφορίας που δεν είναι άλλο από το γνωστό μας bit. Συγκεκριμένα στους κβαντικούς υπολογιστές υπάρχει το κβαντικό σύστημα δύο καταστάσεων που ισοδυναμεί με την κβαντική πληροφορία όπως θα μελετήσουμε πιο κάτω.

Ουσιαστικά ο αιώνας που πέρασε μπορεί να χαρακτηριστεί ως ο αιώνας της φυσικής με την θεωρία της κβαντικής μηχανικής να είναι πρωτοστάτης στην εξέλιξη των τεχνολογιών. Η σημασία της κβαντικής μηχανικής είναι ζωτική καθώς έδωσε σημαντικό χέρι βοήθειας στην ανάπτυξη των ημιαγωγών και την δημιουργία των σημερινών ηλεκτρονικών υπολογιστών.

Το 2000 τον προσωπικό ηλεκτρονικό μου σταθερό υπολογιστή τον είχα συναρμολογήσει με επεξεργαστή Intel Celeron στα 1000 MHz με σκληρό δίσκο στα 20 GB και μνήμη Ram στα 256 MB. Σήμερα 15 χρόνια αργότερα αυτά τα χαρακτηριστικά είναι «αστεία». Αντιλαμβανόμαστε ότι η τεχνολογία και ο ρυθμός προόδου της στους ηλεκτρονικούς υπολογιστές έχει πολλαπλασιαστεί κατακόρυφα.

Αρχές του δεκαετίας του '60 ένας εκ των ιδρυτών του κολοσσού της Intel (ο Gordon Moore) προέβλεψε ότι η υπολογιστική ισχύς θα διπλασιαζόταν κάθε 1 ½ χρόνο. Μάλιστα αυτή η απόλυτα ακριβής πρόβλεψή του είναι διατυπωμένη και γνωστή ως ο νόμος του Moore [8, 13]. Αυτή η αλματώδης αύξηση της υπολογιστικής ισχύος συναρτήσει του χρόνου αποτυπώνεται στο επόμενο σχήμα 4.1.



Σχήμα 4.1

Με τους ρυθμούς που εξελίσσεται η τεχνολογία των υπολογιστών ενδέχεται την προσεχή δεκαετία να υποστεί ένα κλυδωνισμό αδιεξόδου, όσο αφορά την περαιτέρω ανάπτυξή της σε τέτοιο βαθμό που ίσως να είναι μονόδρομος η εξερεύνηση νέων δρόμων υπολογιστικής ισχύος, κάτι που οι φυσικοί ευελπιστούν να καλύψουν με την χρήση των κβαντικών υπολογιστών.

Το αδιέξοδο στην συνεχόμενη αύξηση της υπολογιστικής ισχύος θα οφείλεται στο ότι τα μικροσκοπικά ήδη σχήματα που φέρουν τα ολοκληρωμένα κυκλώματα στην επιφάνεια των τσιπ πυριτίου δεν θα μπορούν πλέον να γίνουν πιο συρρικνωμένα, καθώς η όλο και αυξανόμενη συρρίκνωση δημιουργεί τον λεγόμενο **θερμικό θόρυβο** η αντιμετώπιση του οποίου μάλλον καθίσταται αδύνατη. Άλλωστε όταν 10^3 τρανζίστορ πυριτίου χαραχτούν εξ' ολοκλήρου σε ένα τσιπ, τότε πλέον το λέιζερ κατασκευής τους θα έχει φθάσει στην περιοχή λειτουργίας της υπεριώδους ακτινοβολίας με αποτέλεσμα η **τεχνική χάραξης να μην επαρκεί πλέον για την περαιτέρω κατασκευή τρανζίστορ πυριτίου**. Μια ενδεχόμενη ερευνητική κατεύθυνση για την αποφυγή αυτού του προβλήματος ίσως να είναι η κατασκευή τσιπ από αρσενίδιο του γαλλίου [13], καθώς άγουν καλύτερα τα ηλεκτρικά φορτία λόγω της ατομικής του δομής.

Επίσης ένας άλλος ανασταλτικός παράγοντας για την περαιτέρω σμίκρυνση των σημερινών ολοκληρωμένων κυκλωμάτων είναι ο **φραγμός του Rayleigh** (η στατιστική κατανομή του οποίου εφαρμόζεται όταν δεν υπάρχει οπτική επαφή), σύμφωνα με τον οποίο δεν μπορεί να χαραχθεί πάνω σε τσιπ κάποιο σχέδιο κυκλώματος ανάλυσης μικρότερο από το $\frac{1}{2}$ του μήκους κύματος της δέσμης του λέιζερ χάραξης. Τα σύγχρονα τσιπάκια έχουν transistors στο μέγεθος των 180 nm, (400 φορές στενότερα από την ανθρώπινη τρίχα). Οι κατασκευαστές των τσιπ δεν μπορούν να κατασκευάσουν μικρότερα από 124 nm, σύμφωνα με την αρχή της οπτικής που είναι γνωστή σαν φραγμός ή κριτήριο του Rayleigh και έτσι τα όρια των σημερινών τεχνικών βρίσκονται περιορισμένα σε αυτή την περιοχή μεγέθους. Έχει προταθεί ερευνητικά να χρησιμοποιηθούν τα πεπλεγμένα φωτόνια αντί για τα συμβατικά φωτόνια των laser, τα οποία θα μπορούν να ξεπεράσουν οι τεχνικοί τα όρια των 124 nm, και να φτιαχτούν έτσι transistors μικρότερα από 64 nm [6, 13, 48]. Τα πεπλεγμένα αυτά φωτόνια έχουν την δυνατότητα να κινούνται ταυτόχρονα και να συμπεριφέρονται σαν ένα ενιαίο φωτόνιο καθώς τα πεπλεγμένα φωτόνια έχουν ως σύστημα το μισό μήκος κύματος από ό,τι έχουν ως ατομικά σωματίδια.

Σημαντικές έρευνες έχουν γίνει τα τελευταία χρόνια από επιστήμονες του εξωτερικού για την ανάπτυξη των κβαντικών τρανζίστορ. Σύμφωνα με τις πρώιμες ενδείξεις η δημιουργία τους βασίζεται στην μορφή των ιδιοτήτων που έχουν τα ηλεκτρόνια όταν βρίσκονται παγιδευμένα σε ένα πηγάδι δυναμικού (§ 2.20) διαστάσεων όχι μεγαλύτερα από ένα άτομο. Με την τεχνητή παγίδευση ηλεκτρονίων

σε τέτοια πηγάδια δυναμικού μπορεί να αξιοποιηθεί η συμπεριφορά τους όπως παρόμοια αξιοποιείται από τα κλασικά ημιαγώγιμα υλικά τρανζίστορ πυριτίου.

Πέραν της αδυναμίας ισχύος επεξεργασίας δεδομένων σε μικρό χρόνο και μη δυνατότητας περαιτέρω σμίκρυνσης των τρανζίστορ, η ανάγκη για ασφαλή επικοινωνία και μεθόδους αποτελεσματικής κρυπτογραφίας είναι πολλή μεγάλη σε σημείο που ο σημερινός υπολογιστής να μην μπορεί πλέον να ανταποκριθεί πλήρως στις απαιτήσεις, κυρίως στον τομέα απόρρητων προσωπικών ή πολιτικών – διπλωματικών στοιχείων καθώς και στον τομέα του ηλεκτρονικού εμπορίου.

Η Λειτουργία των κβαντικών υπολογιστών βασίζεται στην μνήμη τους η οποία ονομάζεται μαγνητική μνήμη τυχαίας προσπέλασης – MRAM- και θα αντικαταστήσει τις γνωστές RAM αντίστοιχα σε σύγκριση με τους συμβατικούς υπολογιστές. Με τις MRAM επιτυγχάνεται η υπέρθεση κατάστασης (§3.1) των μικροσωματίων με την εφαρμογή των μαγνητικών επιδράσεων πάνω στην ιδιοπεριστροφή των σωματίων αυτών. Είδη χρησιμοποιούνται κβαντικοί υπολογιστές σε πειραματικό ακόμη στάδιο από την εταιρεία IBM και από το Πανεπιστήμιο του Στάνφορντ και χρηματοδοτούνται μεταξύ άλλων από το Πεντάγωνο, την CIA και πολλές κυβερνητικές και άλλες οργανώσεις [17].

Βέβαια εκτός από τις ασύλληπτα για τα σημερινά δεδομένα προοπτικές που ανοίγονται με την χρήση των κβαντικών υπολογιστών, δημιουργούνται ταυτόχρονα και κάποια ερωτηματικά. Αν και έχουν γίνει σημαντικές έρευνες μόλις πρόσφατα πωλήθηκε ο πρώτος κβαντικός υπολογιστής για πειραματικούς κυρίως σκοπούς, ο μονόλιθος της D-ware (§5.4). Επίσης, προς το παρόν δεν είναι ακριβές ότι οι κβαντικοί υπολογιστές είναι εντελώς «αξιόπιστοι», καθώς ουσιαστικά δεν ξέρουμε ακόμα τα πλήρη στάδια κατασκευής τους στο κοντινό μέλλον. Αυτό οφείλεται εκτός από τις τεχνικές δυσκολίες στο hardware και στην δυσκολία δημιουργίας software κώδικα για τα δεδομένα υψηλής ταχύτητας αυτών των υπολογιστών καθώς η υπολογιστική τους δυνατότητα είναι τόσο μεγάλη, που δεν μπορεί κανείς να εξακριβώσει αν τα αποτελέσματα που θα δώσουν σε προβλήματα, είναι απολύτως σωστά ή όχι.

Οι κβαντικοί υπολογιστές λοιπόν ευελπιστούμε να ενώσουν αποτελεσματικά και με σημαντικά οφέλη για την τεχνολογική πρόοδο την επιστήμη της πληροφορικής με αυτή της κβαντικής φυσικής.

4.2 ΤΑ ΚΒΑΝΤΙΚΑ BIT

Στους κλασσικούς υπολογιστές βασική έννοια είναι το binary digit το γνωστό – συντομογραφικά– bit. Το bit αντιπροσωπεύει την μονάδα πληροφορίας και είναι το δυαδικό ψηφίο 0 ή 1, δηλαδή μπορεί να πάρει μόνο δύο τιμές την 0 και την 1. Επίσης υπάρχει και το πιθανοτικό bit , συντομογραφικά το pbit. Το πιθανοτικό bit μπορεί να βρίσκεται στην κατάσταση 1 με πιθανότητα p και στην κατάσταση 0 με πιθανότητα $q=1-p$ [3, 48].

Στους κβαντικούς υπολογιστές η μονάδα πληροφορίας είναι το quantum bit ή συντομογραφικά το qubit. Το qubit είναι ουσιαστικά η μονάδα πληροφορίας των κβαντικών υπολογιστών και είναι ένα κβαντικό σύστημα δύο καταστάσεων (§ 3.1) που αντίστοιχα συμβολίζονται με

$$|0\rangle \text{ και } |1\rangle.$$

Επίσης μπορεί να αποδοθούν και με την μορφή :

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |+\rangle \quad \text{και} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |-\rangle \quad 4.1$$

Οι κβαντικές καταστάσεις του qubit είναι ορθογώνιες μεταξύ τους και ισχύει σύμφωνα με τις σχέσεις 2.6 (§ 2.19):

$$\langle 0|1\rangle = 0, \quad \langle 1|0\rangle = 0, \quad \langle 1|1\rangle = 1, \quad \langle 0|0\rangle = 1$$

Μπορούμε να πούμε πως η βασική δομή λειτουργίας των κβαντικών υπολογιστών βασίζεται στα υποατομικά σωματίδια τα qubits τα οποία απλά αντικαθιστούν τα δυαδικά bits, δηλαδή τα ψηφία 1 και 0 (ή αλλιώς τους διακόπτες θέσης on-off). Οι δύο καταστάσεις που αποτελούν τη βάση του qubit μπορούν να αντιστοιχιστούν με τις προβολές του σπίν (§ 2.19) ενός σωματιδίου (π.χ. ηλεκτρονίου) με σπιν - 1/2. Η κατάσταση στην οποία το σπίν του ηλεκτρονίου είναι κάτω (§2.19) συμβολίζεται με $|1\rangle$ ενώ η πάνω συμβολίζεται με $|0\rangle$ [11, 18].

Όπως αναφέρθηκε στο Α' μέρος (§ 3.1) το qubit μπορεί να βρεθεί σε κατάσταση υπέρθεσης μεταξύ των δύο βασικών καταστάσεων και να πάρει οποιοσδήποτε τιμές καθώς το qubit είναι ένα διάνυσμα στον χώρο Hilbert (§2.1). Επομένως μια κατάσταση του qubit μπορεί να είναι λόγω υπέρθεσης (σχέση 3.1) η

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle \quad 4.2$$

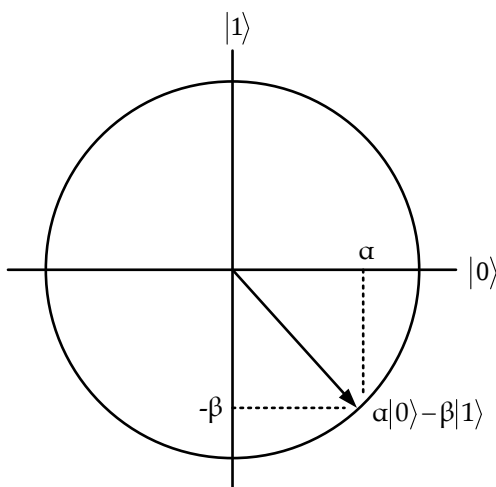
με α και β μιγαδικοί αριθμοί οι οποίοι θα ισοδυναμούν (σχέση 3.2) με

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

Η 4.2 μπορεί να πάρει και την μορφή

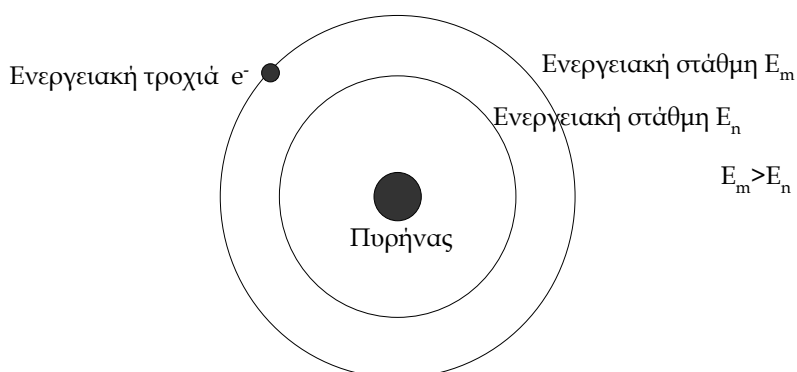
$$|q\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad 4.3$$

Η κατάσταση $|q\rangle = \alpha|0\rangle - \beta|1\rangle$ και η μέτρησή της στον χώρο αποτυπώνεται στο επόμενο σχήμα.



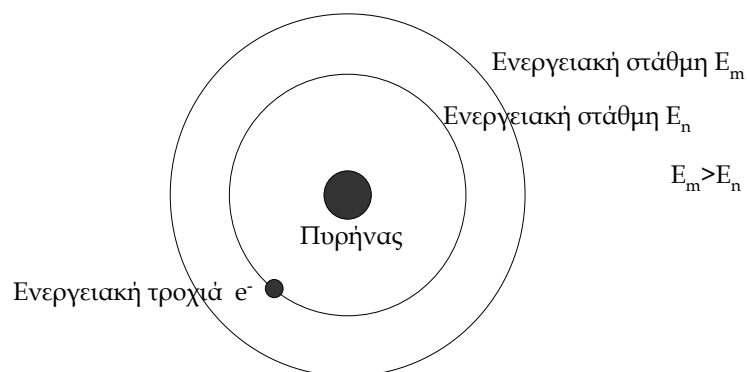
Σχήμα 4.2

Στα δύο επόμενα σχήματα φαίνεται ένα qubit που αποτελείται από ενεργειακά επίπεδα E_m και E_n σε ένα άτομο (με $E_m > E_n$).



Σχήμα 4.3

Το ηλεκτρόνιο βρίσκεται στην ενεργειακή στάθμη E_m και αντιστοιχεί στην κβαντική κατάσταση $|1\rangle$

**Σχήμα 4.4**

Το ηλεκτρόνιο βρίσκεται στην ενεργειακή στάθμη E_n και αντιστοιχεί στην κβαντική κατάσταση $|0\rangle$

Κάθε qubit μπορεί να εμπεριέχει ένα μεγάλο αριθμό από πιθανές αξίες πέρα από το 0 ή το 1. Τα qubit μπορούν να φέρουν απίστευτες ποσότητες πληροφοριών. 100 qubit και μόνο, μπορούν να αποθηκεύσουν $2^{100}=1.267.650.600.288.229.401.496.703.205.375$ διαφορετικούς αριθμούς. Ποσότητα που αποτελεί περισσότερο από ένα τρις - εκατομμύριο φορές την αποθηκευτική ικανότητα όλων των υπολογιστών που έχουν φτιαχτεί ποτέ μέχρι σήμερα. Χαρακτηριστικός είναι ο επόμενος πίνακας στον οποίο φαίνεται η αναλογία των κλασσικών και κβαντικών bits και προφανώς απεικονίζεται με εντυπωσιακό τρόπο, η τεράστια δυνατότητα των κβαντικών υπολογιστών:

Ταυτόχρονη καταχώρηση 0 και 1	Κλασσικά bits	Κβαντικά bits
0 & 1	2	1
0&1, 0&1	$2^2=4$	2
0&1, 0&1, 0&1	$2^3=8$	3
0&1, 0&1, 0&1, 0&1	$2^4=16$	4
0&1, 0&1, 0&1, 0&1, 0&1	$2^5=32$	5
...	...	...
0&1, 0&1, ...0&1 (100 φορές)	2^{100}	100
...	...	...
0&1, 0&1, ...0&1 (300 φορές)	2^{300}	300
...	...	...
0&1, 0&1, ...0&1 (500 φορές)	2^{500}	500
...	...	...

Παρατηρούμε πως μόλις 300 qubits είναι ισοδύναμα με $2^{300}=2,037035976 \text{ e}+90$ αριθμούς! Συνοψίζοντας από τα χαρακτηριστικά που μέχρι τώρα αναφέρθηκαν οι δυνατότητες που ανοίγονται με την χρήση των qubits είναι πολλαπλάσιες συγκριτικά με τους κλασσικούς υπολογιστές. Με την χρήση δύο qubits μπορούμε να έχουμε το 0 και το 1 ταυτόχρονα σε όλους τους δυνατούς συνδυασμούς τους (σε αντίθεση συγκριτικά με τα σημερινά bits τα οποία να μεν μπορούν να κάνουν όλους τους συνδυασμούς αλλά όχι όμως ταυτόχρονα). Εξ' αιτίας της κατάστασης κβαντικής υπέρθεσης, η πολυπλοκότητα προβλημάτων είναι εύκολο να λυθεί. Όπως προαναφέρθηκε το qubit μπορεί να είναι ένα ηλεκτρόνιο, φωτόνιο, ένα ιόν ή ένα μόριο με αποτέλεσμα να υπάρχουν ταυτόχρονα πολλές αποτελεσματικές επιλογές για την αντιμετώπιση ζητούμενων προβλημάτων.

Ο πρώτος κβαντικός υπολογιστής πραγματοποιήθηκε ερευνητικά και παρουσιάστηκε από την Αμερικάνικη εταιρεία IBM το 1988 με χρήση 2 qubits. Μετά από 11 χρόνια [17] η ίδια εταιρεία κατασκεύασε ένα νέο κβαντικό υπολογιστή με 3 qubits, ενώ στις αρχές του millennium κατασκεύασε έναν με 5 qubits λειτουργίας. Σήμερα έχουμε εισέλθει στην εποχή των 7 και 9 qubits λειτουργίας κβαντικών υπολογιστών.

Τα πλεονεκτήματα λοιπόν, των κβαντικών υπολογιστών είναι αρκετά και έχουν να κάνουν με την τεράστια ταχύτητά τους ώστε η επίλυση προβλημάτων να είναι αρκετά εύκολη σε συνδυασμό με την άπλετη μνήμη και την απεριόριστη ισχύ τους. Όμως εκτός από τα θετικά των κβαντικών υπολογιστών υπάρχουν και κάποια ερωτηματικά που προς το παρόν είναι τροχοπέδη για την αξέλιξή τους καθώς δεν μπορούν να έχουν την «εικόνα» του σημερινού υπολογιστή, δηλαδή να κάνουν επεξεργασία εικόνας, ήχου και κειμένου ή να επισκέπτονται ιστοσελίδες. Επίσης τα υλικά κατασκευής προς το παρόν είναι μη λειτουργικά και μη «ανταποκρίσιμα» στην χρήση των υπολογιστών σε υψηλές θερμοκρασίες που αναπτύσσονται λόγω των υπερβολικά μεγάλων ταχυτήτων μεταφοράς δεδομένων. Επίσης όπως προαναφέρθηκε στο πρώτο μέρος η αποσυννοχή δημιουργεί προβλήματα και όπως θα δούμε η αντιμετώπιση και προσαρμογή των υλικών που αποτελούν τον κβαντικό υπολογιστή στην αλληλεπίδραση των qubits με το περιβάλλον δημιουργεί κατάρρευση της υπέρθεσης των δύο κβαντικών καταστάσεων.

Παραδείγματα qubits πέραν των αναφερομένων που περιγράφονται [3] από τις καταστάσεις

$$|q_1\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ και } |q_2\rangle = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

είναι με βάση την σχέση 4.3 και άλλα επιπλέον που εξάγονται όπως τα

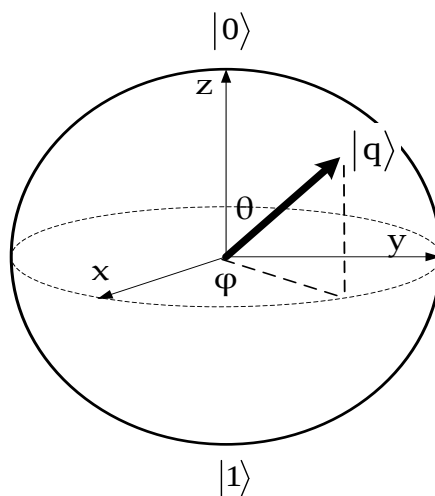
$$|q_3\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix},$$

$$|q_4\rangle = \frac{3}{\sqrt{5}}|0\rangle - \frac{1}{\sqrt{5}}|1\rangle = \begin{bmatrix} \frac{3}{\sqrt{5}} \\ -\frac{1}{\sqrt{5}} \end{bmatrix}, \quad |q_5\rangle = i\frac{4}{5}|0\rangle + i\frac{3}{5}|1\rangle = \begin{bmatrix} \frac{4i}{5} \\ \frac{3i}{5} \end{bmatrix} \quad \text{κ.α.}$$

4.3 ΣΦΑΙΡΑ BLOCH

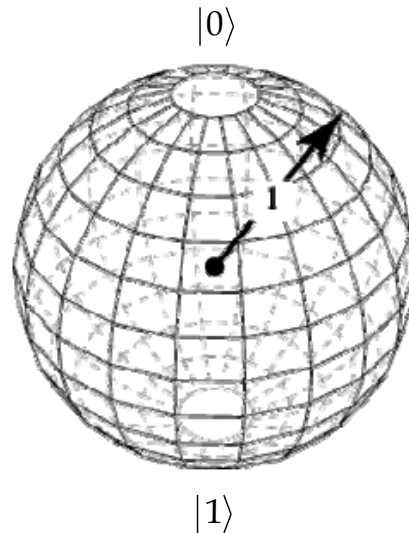
Στην Κβαντική μηχανική η σφαίρα Bloch είναι μια γεωμετρική αναπαράσταση του χώρου κατάστασης ενός κβαντικού συστήματος δύο καταστάσεων και δεν είναι ουσιαστικά τίποτα άλλο, από μια απεικόνιση των χαρακτηριστικών ενός qubit. Είναι μια σφαίρα που αποτυπώνει με γεωμετρικό τρόπο την αντιστοιχία μεταξύ στοιχείων της σφαίρας και των κβαντικών καταστάσεων. Το όνομά της απορρέει από τον φυσικό Felix Bloch.

Με απλά λόγια η σφαίρα Bloch αποτυπώνει το διάνυσμα δύο καταστάσεων του qubit που είναι ένα διάνυσμα δύο καταστάσεων στον χώρο Hilbert (§ 2.1) και απεικονίζεται στο επόμενο σχήμα 4.5 [1, 19]. Η ακτίνα της σφαίρας Bloch είναι μονάδα όσο και το μήκος του διανύσματος κατάστασης του qubit $|q\rangle$. Ο χώρος των καθαρών καταστάσεων ενός κβαντικού συστήματος δίνεται από τις ακτίνες στον χώρο Hilbert (δηλαδή τα σημεία που αναζητούνται στον προβαλλόμενο χώρο).



Σχήμα 4.5

Οι καταστάσεις $|0\rangle$ και $|1\rangle$ είναι ορθογώνιες μεταξύ τους και όταν το qubit βρίσκεται κατακόρυφο προς τα πάνω (όπως φαίνεται στο σχήμα στην θέση z) είναι αντίστοιχα στην βασική κατάσταση $|0\rangle$. Αντιστοίχως η κατακόρυφη προς τα κάτω θέση είναι η βασική κατάσταση $|1\rangle$. Στο επόμενο σχήμα 4.3 [3, 19], φαίνεται σε τρισδιάστατη μορφή η σφαίρα Bloch.



Σχήμα 4.6

Παρατηρώντας στο σχήμα 4.5 τις γωνίες θ και φ (προφανώς πραγματικοί αριθμοί) μπορούμε να εκφράσουμε την σχέση 4.2 μέσω αυτών των γωνιών σε μια γενικότερη μαθηματική διατύπωση καθώς οι γωνίες δείχνουν και κάποιο σημείο πάνω στην επιφάνεια της σφαίρας Bloch. Αυτό γίνεται γιατί η σφαίρα Bloch είναι με μέτρο την μονάδα, η γενίκευση της μορφής ενός μιγαδικού αριθμού (παράρτημα Α, § 3) που αναπαρίσταται στην σφαίρα. Ο μιγαδικός αριθμός αντιστοιχεί σε σημείο με ακτίνα 1 από την αρχή των αξόνων. Οι τιμές που παίρνει η γωνία θ είναι μεταξύ 0° και 180° δηλαδή $0 \leq \theta \leq 2\pi$. Επίσης η γωνία φ στην σφαίρα Bloch παίρνει τιμές μεταξύ 0° και 360° δηλαδή $0 \leq \varphi \leq 2\pi$ (η γωνία φ καλείται γωνία φάσης και παίζει σημαντικό ρόλο για τους υπολογισμούς των αλγόριθμων που θα αναπτυχθούν στο 8ο κεφάλαιο).

Επίσης αν κάνουμε χρήση των σφαιρικών συντεταγμένων (παράρτημα Α, §5.II) μπορούμε να εκφράσουμε την σχέση 4.2 $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ διαφορετικά, ως εξής:

$$|q\rangle = r_\alpha e^{i\varphi_\alpha} |0\rangle + r_\beta e^{i\varphi_\beta} |1\rangle \quad 4.4$$

Επειδή η πιθανότητα $|\alpha|^2$ είναι πραγματική και μετρήσιμη έχουμε ότι

$$|\alpha|^2 = \alpha \cdot \alpha^* = \alpha \cdot e^{i\phi} \cdot \alpha^* e^{-i\phi} = |\alpha \cdot e^{i\phi}|^2$$

Με χρήση αυτού μπορούμε να τροποποιήσουμε την $|q\rangle$ της σχέσης 4.4, ισοδύναμα ως εξής:

$$\begin{aligned} |q\rangle &= e^{i\varphi_\alpha} r_\alpha e^{-i\varphi_\alpha} |0\rangle + e^{i\varphi_\beta} r_\beta e^{-i\varphi_\alpha} |1\rangle = r_\alpha |0\rangle + r_\beta e^{i(\varphi_\beta - \varphi_\alpha)} |1\rangle \Rightarrow \\ |q\rangle &= r_\alpha |0\rangle + r_\beta e^{i\varphi} |1\rangle \end{aligned}$$

Όμως επειδή ισχύει (παράρτημα Α, §5.IV)

$$\begin{cases} x = r \sin \theta \cos \phi, \\ y = r \sin \theta \sin \phi, \\ z = r \cos \theta \end{cases}$$

και θέτοντας όπου $z=r_\alpha$, με γνωστό ότι $r=1$ και $e^{i\varphi} = x + yi$ (παράρτημα Α, §3) προκύπτει ότι

$$\begin{aligned} |q\rangle &= z|0\rangle + (x + iy)|1\rangle = r \cos \theta |0\rangle + (r \sin \theta \cos \phi + ir \sin \theta \sin \phi)|1\rangle \stackrel{r=1}{\Rightarrow} \\ |q\rangle &= \cos \theta |0\rangle + \sin \theta (\cos \phi + i \sin \phi) |1\rangle \Rightarrow |q\rangle = \cos \theta |0\rangle + \sin \theta e^{i\varphi} |1\rangle \end{aligned}$$

Επομένως η σχέση 4.2 μπορεί να γραφεί σε μια πιο γενική μορφή την

$$|q\rangle = \cos \theta |0\rangle + \sin \theta e^{i\varphi} |1\rangle \quad 4.5$$

Οι γωνίες όπως προαναφέρθηκε παίρνουν τιμές $0 \leq \theta \leq 2\pi$ και $0 \leq \varphi \leq 2\pi$. Τότε τελικά λόγω των περιορισμών τους, η σχέση 4.5 γίνεται ισοδύναμα

$$\boxed{|q\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\varphi} |1\rangle} \quad 4.6$$

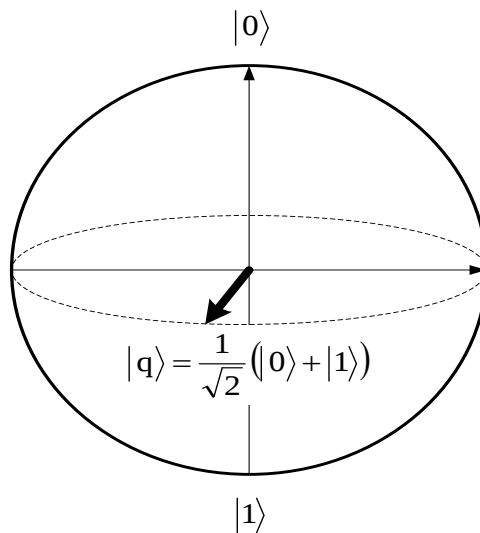
Προφανώς τα πλάτη δίνουν $\left| \cos \frac{\theta}{2} \right|^2 + \left| \sin \frac{\theta}{2} e^{i\varphi} \right|^2 = \left| \cos \frac{\theta}{2} \right|^2 + \left| \sin \frac{\theta}{2} \right|^2 = 1$.

Από την σχέση 4.6 για διάφορες τιμές γωνιών προκύπτουν και οι καταστάσεις. Συγκεκριμένα για $\theta=\pi$ προκύπτει η $|q\rangle = \cos \frac{\pi}{2} |0\rangle + \sin \frac{\pi}{2} e^{i\varphi} |1\rangle = |1\rangle$. Για $\theta=0^\circ$,

προκύπτει η $|q\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}|1\rangle = |0\rangle$. Επίσης για $\theta=90^\circ$ και $\varphi=0^\circ$ προκύπτει η κατάσταση

$$|q\rangle = \cos\frac{\pi}{2}|0\rangle + \sin\frac{\pi}{2}e^{i0}|1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad \text{ή} \quad |q\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Η κατάσταση αποτυπώνεται πάνω στην σφαίρα με την μορφή του επόμενου σχήματος



Σχήμα 4.7

4.4 ΚΒΑΝΤΙΚΟΣ ΚΑΤΑΧΩΡΗΤΗΣ

Ένα σύνολο από διατεταγμένα qubits (δύο ή περισσότερα στον χώρο Hilbert) αποτελεί ένα κβαντικό καταχωρητή. Στους κλασσικούς υπολογιστές ο καταχωρητής αποτελείται από ένα σύνολο bits. Η πληροφορία που μπορεί να αποθηκευθεί στον κβαντικό υπολογιστή είναι πολύ μεγαλύτερη συγκριτικά με την πληροφορία που αποθηκεύεται στους κλασσικούς υπολογιστές.

Η πληροφορία για παράδειγμα, δύο μόνο qubits είναι πολύ μεγαλύτερη από αυτή των δύο bits του κλασσικού υπολογιστή. Αυτό συμβαίνει γιατί στον δύο bit καταχωρητή των κλασσικών υπολογιστών αποθηκεύονται κάθε φορά δύο (ή τέσσερις) δυαδικοί σχηματισμοί, οι 00, 01, 10 και 11 (ή αλλιώς $|00\rangle, |01\rangle, |10\rangle, |11\rangle$). Αντιθέτως στον δύο qubit καταχωρητή ενός κβαντικού υπολογιστή μπορούν να

αποθηκευτούν και οι τέσσερις σχηματισμοί ταυτοχρόνως καθώς κάθε qubit αναπαριστά δύο τιμές. Δηλαδή ο κβαντικός υπολογιστής που αποτελείται από δύο qubits είναι ένα σύστημα τεσσάρων βασικών καταστάσεων λόγω υπέρθεσης και είναι ένας γραμμικός συνδυασμός σύμφωνα με την σχέση 4.2 και όσα ειπώθηκαν για το τανυστικό γινόμενο (§ 2.1), της εξής μορφής :

$$|q\rangle = |q_1 q_0\rangle \Rightarrow \quad 4.7$$

$$\begin{aligned} |q\rangle &= |q_1\rangle \otimes |q_0\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle) \Rightarrow \\ |q\rangle &= \alpha|0\rangle \otimes \gamma|0\rangle + \alpha|0\rangle \otimes \delta|1\rangle + \beta|1\rangle \otimes \gamma|0\rangle + \beta\delta|1\rangle \otimes |1\rangle \Rightarrow \\ |q\rangle &= \alpha\gamma|0\rangle \otimes |0\rangle + \alpha\delta|0\rangle \otimes |1\rangle + \beta\gamma|1\rangle \otimes |0\rangle + \beta\delta|1\rangle \otimes |1\rangle \end{aligned}$$

ή σε πιο απλή μορφή

$$|q\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \quad 4.8$$

Η σχέση 4.8 σε μορφή πίνακα είναι ισοδύναμα

$$|q\rangle = \alpha\gamma \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \alpha\delta \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \beta\gamma \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \beta\delta \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Τα άτομα που έχουν αλληλεπιδράσει «έστω και σε ένα βαθμό», διατηρούν ένα είδος δεσμού και μπορούν να εμπλέκονται μεταξύ τους σε ζεύγη. Γνωρίζοντας το spin του ενός ατόμου από το ζεύγος (πάνω ή κάτω), μπορούμε να καταλάβουμε ότι το spin του ζεύγους του θα έχει αντίθετη φορά. Λόγο του φαινομένου της υπέρθεσης, το άτομο που εξετάζεται δεν έχει πριν γίνει η μέτρησή του, spin, αλλά βρίσκεται ήδη και στις δύο καταστάσεις με spin πάνω και spin κάτω. Το spin ενός ατόμου που εξετάζεται καθορίζεται τη στιγμή της μέτρησης οπότε ανάλογα παίρνει και το άτομο με το οποίο αλληλεπιδρά την τιμή του (ο Einstein το αποκάλεσε “τρομακτική δραστηριότητα από απόσταση [24] – spooky action at a distance-”).

Ομοίως εργαζόμενοι για τρία qubits έχουμε συνολικά οκτώ δυνατές καταστάσεις υπερθέσεως.

$$|q\rangle = |q_2 q_1 q_0\rangle \Rightarrow |q\rangle = |q_2\rangle \otimes |q_1\rangle \otimes |q_0\rangle \Rightarrow$$

$$|q\rangle = \alpha|000\rangle + \beta|001\rangle + \gamma|010\rangle + \delta|011\rangle + \varepsilon|100\rangle + \zeta|101\rangle + \sigma|110\rangle + \theta|111\rangle \quad 4.9$$

Η σχέση 4.9 σε μορφή πίνακα είναι ισοδύναμα

$$|q\rangle = \alpha \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \gamma \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \delta \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + \varepsilon \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + \zeta \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + \sigma \tau \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} + \theta \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

Η κατάσταση ενός κβαντικού καταχωρητή που αποτελείται από n qubits θα δίνεται από την γενική έκφραση:

$$|q\rangle = |q_{n-1} \dots q_3 q_1 q_0\rangle \Rightarrow \quad 4.10$$

ή διαφορετικά

$$|q\rangle = a|0\dots 00\rangle + b|00\dots 1\rangle + c|0\dots 10\rangle + \dots + h|1\dots 11\rangle \quad 4.11$$

Υπάρχουν επίσης καταστάσεις δύο qubits οι οποίες δεν μπορούν να περιγραφούν ως συνδυασμός καταστάσεων δύο ανεξάρτητων qubits. Αυτές οι καταστάσεις είναι καταστάσεις που καλούνται καταστάσεις κβαντικής διεμπλοκής (ή διαφορετικά διαπλεγμένες) [6, 49]. Οπότε η κατάσταση $|q\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ δεν μπορεί να γραφεί σαν τανυστικό γινόμενο δύο ξεχωριστών καταστάσεων qubits της μορφής

$$|q\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)$$

Το qubit της κατάστασης $|1\rangle$, της κατάστασης $|q\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, έχει πιθανότητα 50% να βρίσκεται στην $|1\rangle$ και 50% να βρίσκεται στην $|0\rangle$. Ομοίως το qubit της κατάστασης $|0\rangle$, της κατάστασης $|q\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, έχει πιθανότητα 50% να βρίσκεται στην $|1\rangle$ και 50% να βρίσκεται στην $|0\rangle$. Δηλαδή η μέτρηση της κατάστασης του ενός εκ των δύο qubits καθορίζει την κατάσταση του άλλου και τα δύο qubits βρίσκονται σε κβαντική διεμπλοκή. Η κβαντική διεμπλοκή ερμηνεύτηκε με το πείραμα EPR (§ 3.6)

Πολλές φορές γίνεται «σύγχυση» μεταξύ της κβαντικής υπέρθεσης και της διεμπλοκής. Η διαφορά της υπέρθεσης με την διεμπλοκή είναι ότι στην υπέρθεση η κατάσταση $|q\rangle$ (π.χ. η $|q\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle)$) μπορεί να βρίσκεται στην κατάσταση $|0\rangle$ ή στην $|1\rangle$, να γραφεί ως τανυστικό γινόμενο δηλαδή να πάρει την μορφή $|q\rangle = |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |q_I\rangle \otimes |q_{II}\rangle$ και η μέτρηση του ενός qubit δεν επηρεάζει την μέτρηση του άλλου. Αυτό είναι κάτι που δεν συμβαίνει στην κβαντική διεμπλοκή (π.χ. όπως προαναφέρθηκε η $|q\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$) όπου για το qubit $|q\rangle$, η κατάσταση του $|0\rangle$ εξαρτάται από την κατάσταση $|1\rangle$ και επομένως η κατάσταση του ενός καθορίζει την κατάσταση του άλλου και δεν μπορεί η $|q\rangle$ να γραφεί ως τανυστικό γινόμενο καταστάσεων.

«Imagination is more important than knowledge»

Albert Einstein

ΚΕΦΑΛΑΙΟ 5^ο

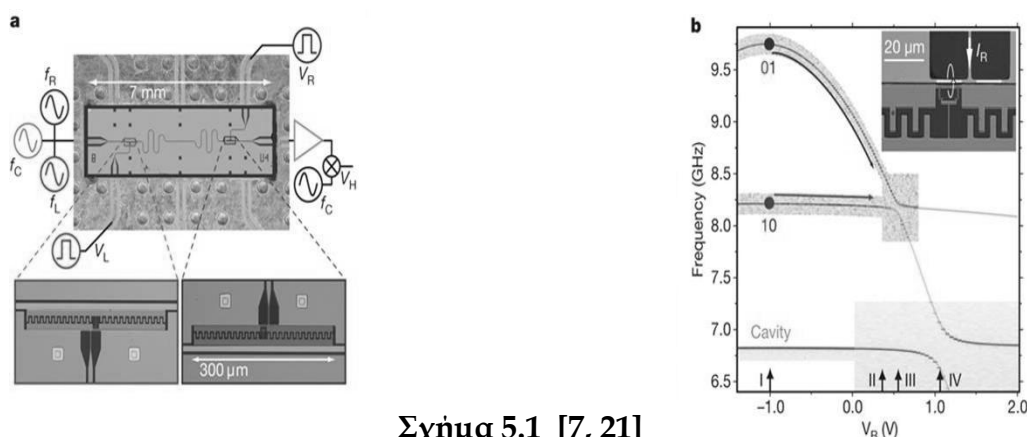
ΤΕΧΝΟΛΟΓΙΑ ΚΑΤΑΣΚΕΥΗΣ ΚΑΙ ΔΟΜΗ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

5.1 ΚΒΑΝΤΙΚΟΣ ΕΠΕΞΕΡΓΑΣΤΗΣ

Ο κβαντικός υπολογιστής αποτελείται από έναν ή περισσότερους κβαντικούς καταχωρητές αλλά και από ένα συνδυασμό κβαντικών πυλών. Η επεξεργαστική δομή των κβαντικών υπολογιστών διαφέρει συγκριτικά με την κεντρική μονάδα επεξεργασίας των κλασσικών υπολογιστών. Ο κλασσικός επεξεργαστής (c.p.u.) εκτελεί ένα συνδυασμό λογικών πράξεων μέσω ψηφιακών κυκλωμάτων με χρήση πυλών σε συνδυασμό με το λογισμικό που υποστηρίζει το υλικό του υπολογιστή. Στον κβαντικό επεξεργαστή δεν έχει ακόμα βρεθεί φόρμουλα λειτουργίας με προγραμματιζόμενη αρχιτεκτονική και επικοινωνία υλικού και λογισμικού και

ουσιαστικά είναι ένας όρος που δεν ταυτίζεται με τον επεξεργαστή των κλασσικών υπολογιστών.

Στα τέλη της προηγούμενης δεκαετίας ερευνητές από το τμήμα φυσικής του πανεπιστημίου Yale, με επικεφαλής τον κ. Leonard Dee Carlo, δημιούργησαν έναν κβαντικό επεξεργαστή τύπου στερεάς κατάστασης (solid state) χρησιμοποιώντας τεχνολογία τεχνικών παραγωγής των τσιπ πυριτίου. Σύμφωνα με την δημοσίευση της έρευνά τους, έγινε χρήση στερεών υλικών με προγράμματα επεξεργασίας κβαντικών αλγορίθμων [7]. Συγκεκριμένα η κατασκευή της ομάδας του πανεπιστημίου του Yale, αποτελείται από δύο «transmon qubits», δηλαδή από ένα φιλμ νιόβιου πάνω σε ένα λεπτό υπόστρωμα οξειδίου του αλουμινίου, όπου έχουν χαραχτεί κενά, τα οποία διατρέχει το ηλεκτρικό ρεύμα, ενώ τα δύο qubits βρίσκονται σε μια κοιλότητα που περιέχει μικροκύματα (micronaves) ώστε τα qubits να προκαλούν κβαντική υπέρθεση και διεμπλοκή με αποτέλεσμα η όλη διάταξη να τεθεί σε εφαρμογή για 1 nsec. Πάνω από 4 qubits η συσκευή παρουσιάζει σημαντικά προβλήματα λειτουργίας [20, 21]. Η δομή της συγκεκριμένης διάταξης φαίνεται στο επόμενο σχήμα.



Σχήμα 5.1 [7, 21]

Συσκευή με κοιλότητα, από δύο qubit

5.2 ΤΕΧΝΟΛΟΓΙΚΗ ΔΟΜΗ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Πολλές προσπάθειες έχουν γίνει σε **ερευνητικό επίπεδο** για την δημιουργία ενός κβαντικού υπολογιστή. Όπως προαναφέρθηκε στην προηγούμενη παράγραφο έχουν γίνει προσπάθειες κατασκευής κβαντικών υπολογιστών στερεάς κατάστασης, υπολογιστών κοιλότητας κβαντικής ηλεκτροδυναμικής (cavity QED) αλλά και άλλων τεχνολογιών όπως της παγίδευσης ιόντων (ion-traps), καθώς και υπολογιστές πυρηνικού μαγνητικού συντονισμού (NMR).

Ο κβαντικός υπολογιστής στερεάς κατάστασης [6] βασίζεται στην κίνηση των μορίων. Ερευνητές στην IBM έχουν κατασκευάσει κβαντικές πύλες με χρήση μίας στοίβας από μόρια μονοξειδίου του άνθρακα CO (διαστάσεων nm) τοποθετώντας ένα απλό μόριο CO παράλληλα με ένα από τα ζεύγη και τα τρία μόρια σχημάτισαν ένα σχήμα με την τοποθέτηση τριών σειρών ζευγών μορίων σε μορφή Y, με ένα απλό μόριο στο κεντρικό σημείο, όπου και συναντώνται οι σειρές. Δύο σειρές δρουν ως είσοδοι και η τρίτη ως έξοδος. Πειραματικά οι δομές ήταν αργές και χρησιμεύουν μόνο για απλή επεξεργασία κβαντικών υπολογισμών

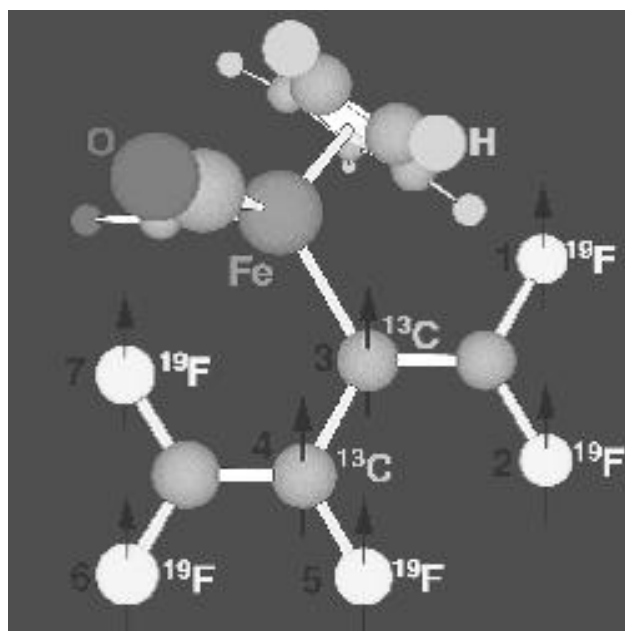
Ο κβαντικός υπολογιστής κοιλότητας κβαντομηχανικής ηλεκτροδυναμικής [6] είναι μια ενδιαφέρον ερευνητική προσπάθεια στην οποία γίνεται χρήση μιας, όπως είναι προφανές, κοιλότητας κβαντικής ηλεκτροδυναμικής -cavity QED-. Πιο συγκεκριμένα, η κβαντική ηλεκτροδυναμική είναι η κβαντική θεωρία που περιγράφει αλληλεπιδράσεις ακτινοβολίας με την φορτισμένη ύλη. Η κβαντική ηλεκτροδυναμική είναι ουσιαστικά μια φυσική θεωρία παρόμοιας μορφής και αιτιοκρατίας με τις εξισώσεις της ειδικής θεωρίας της σχετικότητας που διέτυπωσε ο Einstein. Η συγκεκριμένη θεωρία υποστηρίζει πως η δημιουργία ηλεκτρομαγνητικών δυνάμεων οφείλεται στην εκπομπή και την απορρόφηση σωματιδίων (φωτονίων), τα οποία αποτυπώνουν τις ιδιομορφίες των διαταραχών των ηλεκτρομαγνητικών πεδίων. Με την ίδια λογική μπορούν και τα ηλεκτρόνια να θεωρηθούν διαταραχές αντίστοιχων κβαντισμένων πεδίων. Αυτά όμως τα σωματίδια (φωτόνια) είναι κατά κάποιον τρόπο «εικονικά», δηλαδή δεν μπορούν να ανιχνευθούν με κάποιο τρόπο επειδή η ύπαρξή τους παραβιάζει την διατήρηση της ενέργειας (ΑΔΕ) και της ορμής (ΑΔΟ). Η κβαντική πληροφορία αποθηκεύεται σε εσωτερικές καταστάσεις των ατόμων και είναι εύκολο να δημιουργηθούν αλληλεπιδράσεις με τα qubits.

Ο κβαντικός υπολογιστής παγίδας ιόντων [6] προέκυψε από πειράματα ενός αριθμού ιόντων σε μια παγίδα λιθογραφικής κατασκευής. Συγκεκριμένα μια ιοντική παγίδα διαστάσεων 10^{-6} του μέτρου -μm- τοποθετήθηκε σε ένα ημιαγώγιμο τοίπι ώστε να παγιδευτεί ένα μόνο ιόν καδμίου το οποίο στη συνέχεια θα μετακινηθεί προς διαφορετικές θέσεις στην παγίδα ιόντων. Αυτό θα επιτευχθεί με συμμετοχή ηλεκτρικών σημάτων. Επίσης τα ιόντα βρίσκονται σε σειρά μέσα σε κενό και λείζερ χειρίζεται την κατάσταση κβαντικής διεμπλοκής η οποία εμποδίζει την ποιότητα και την χρήση μεγαλύτερων αριθμών ιόντων στην παγίδα. Η χρήση του κβαντικού αλγόριθμου του Grover (§8.3) είναι αυτός που χρησιμοποιείται για την εξέταση κάθε κβαντικής καταχώρησης.

Τέλος ο **πυρηνικός μαγνητικός συντονισμός** [6, 7] (nuclear magnetic resonance) -NMR- είναι μια ακόμα προσπάθεια για κατασκευή κβαντικών υπολογιστών που επιτεύχθη στα τέλη της δεκαετίας του 90. Εδώ ένας κβαντικός

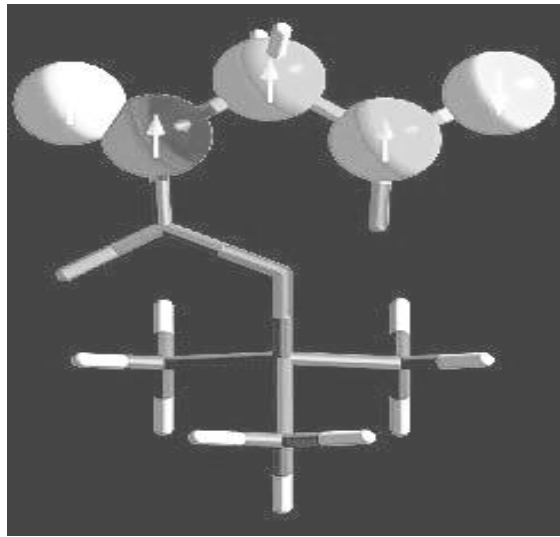
καταχωρητής είναι ένα μόριο που αποτελείται από δέκα άτομα. Κάθε qubit αναπαρίσταται με τον προσανατολισμό του σπιν του κάθε ατομικού πυρήνα στα άτομα του μορίου. Ο αριθμός των ατόμων ενός πυρηνικού μαγνητικού συντονισμού κβαντικού υπολογιστή είναι ίσος με τον αριθμό των ατόμων σε κάθε μόριο, σε θερμοκρασία δωματίου και έχει αποδειχθεί ότι είναι εύκολο να κατασκευαστεί με αυτή την τεχνολογία ένας κβαντικός υπολογιστής των 2 qubits. Προς το παρόν αυτή η τεχνολογία έχει προσομοιωθεί με χρήση ενός νέου μορίου που αποτελείται από 7 πυρηνικά σπιν, όπου το κάθε ένα μπορεί να αλληλεπιδρά με το άλλο, ενώ οι αλληλεπιδράσεις αυτές μπορούν να ανιχνευτούν με όργανα NMR, δηλαδή ουσιαστικά ένας κβαντικός υπολογιστής των 7 qubits (η τεχνική αυτή πραγματοποιήθηκε το 1998 με 2-qubit καταχωρητές, και κλιμακώθηκε σε 7 qubits στο Los Alamos National Lab, το 2000). Το πρώτο μοντέλο NMR κατέληξε να είναι σε αδιέξοδο όσον αφορά την κλιμάκωση των qubits.

Στα επόμενα σχήματα φαίνεται η «τεχνική» της τεχνολογίας του πυρηνικού μαγνητικού συντονισμού.

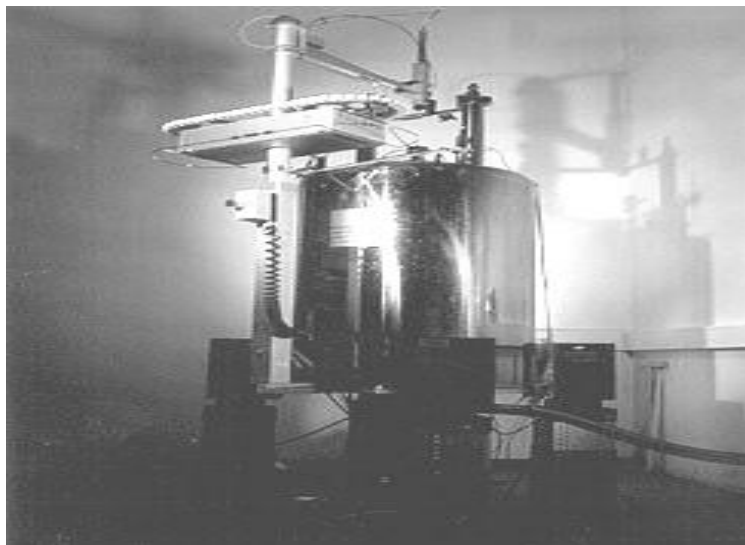


Σχήμα 5.4

Σχηματική αναπαράσταση 7-qubit μορίου NMR [7, 23, 25]

**Σχήμα 5.2**

Μοριακό υλικό του πρώτου 5-qubit NMR [7, 22]

**Σχήμα 5.3**

NMR spectrometer στο TU München [7, 23]

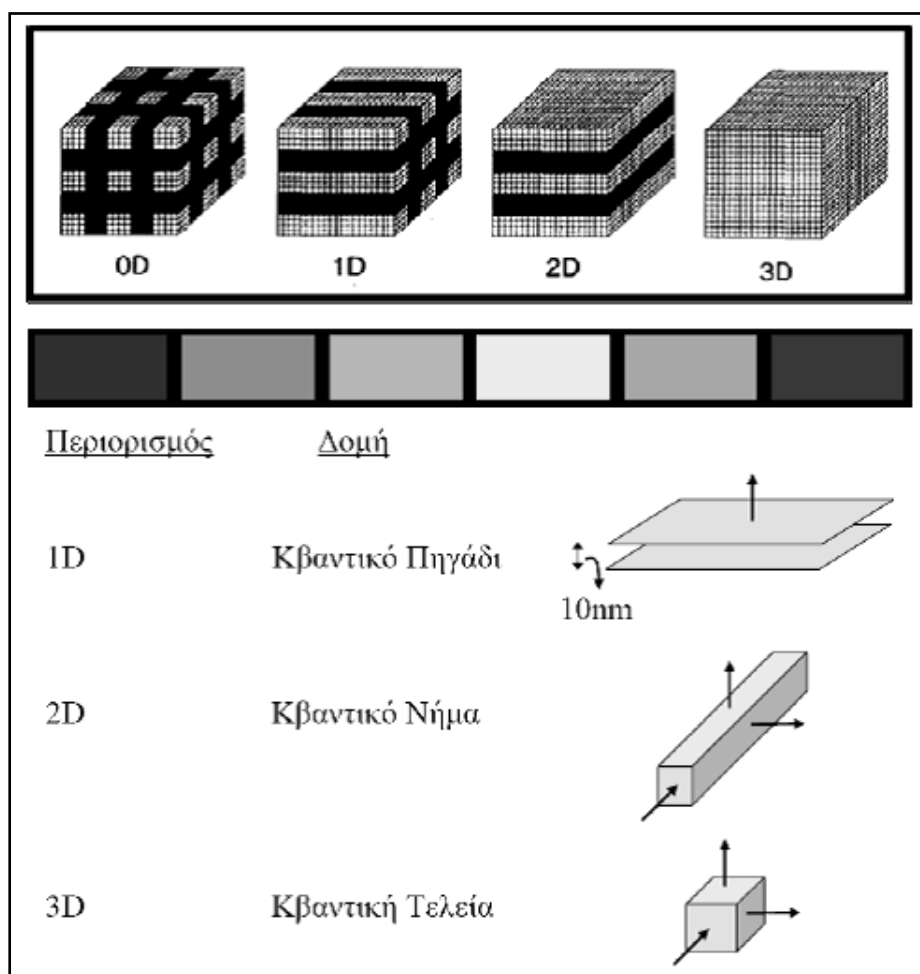
5.3 ΚΒΑΝΤΙΚΕΣ ΤΕΛΕΙΕΣ

Οι κβαντικές τελείες είναι ημιαγωγοί ή πιο ορθά ημιαγώγιμες νανοδομές με τη μορφή νανοσφαιριδίων ή άλλων σχημάτων των οποίων εξιτόνια² περιορίζονται στις τρεις χωρικές διαστάσεις. Ως αποτέλεσμα, αποκτούν ιδιότητες εξ' αιτίας αυτών των «χύμα» ημιαγωγών και των διακριτών μορίων. Οι κβαντικές τελείες ανακαλύφθηκαν στις αρχές της δεκαετίας του 1980 από τον Alexei Ekimov σε υάλινη μήτρα και από τον Louis E. Brus σε κολλοειδή διαλύματα. Ο όρος κβαντικές τελείες (Quantum Dots) επινοήθηκε από τον Mark Reed. Οι ερευνητές έχουν μελετήσει κβαντικές τελείες σε τρανζίστορ, στα ηλιακά κύτταρα, στα LED και σε λέιζερ διόδων. Έχουν διερευνηθεί, επίσης, κβαντικές τελείες ως «παράγοντες» για την ιατρική απεικόνιση με ελπίδα να τις χρησιμοποιήσουν ως qubits [30, 31].

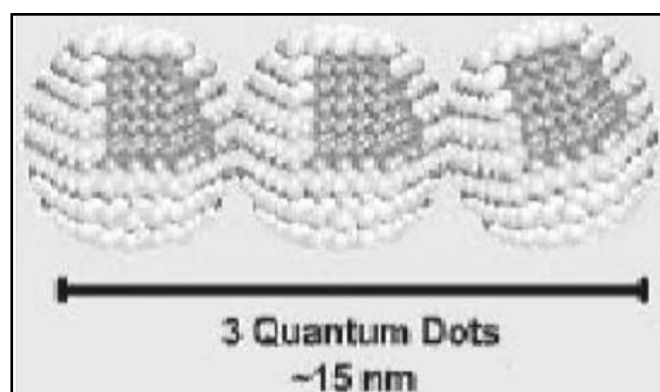
Με την έρευνα στις διαστάσεις ενός εκτεταμένου ημιαγωγού σε περιοχές νανομετρικών διαστάσεων, προκύπτουν νέες ιδιότητες που βασίζονται στην κβαντική μηχανική και στις ιδιότητες του ηλεκτρονίου και της κβάντωσης των ενεργειών του. Όταν μια από τις τρεις διαστάσεις μειωθεί κάτω από 10 nm και οι άλλες παραμείνουν σε περιοχές κλίμακας μικρομέτρων (μm) τότε εξετάζουμε ένα κβαντικό πηγάδι (§2.20). Όταν δύο από τις τρεις διαστάσεις βρεθούν κάτω από το όριο των 10 nm (νανοκλίμακα) εξετάζουμε το κβαντικό νήμα, ενώ όταν και οι τρεις διαστάσεις είναι κάτω από το όριο των 10 nm ασχολούμαστε με την κβαντική τελεία, την οποία πραγματευόμαστε για την αξιοποίηση της στους κβαντικούς κρυπτογραφικών σκοπών υπολογιστές.

Αυτό φαίνεται χαρακτηριστικά στο επόμενο σχήμα 5.5 που απεικονίζει τις δομές των χαμηλών διαστάσεων που προαναφέρθηκαν.

² Ένα φωτόνιο μπορεί να διεγείρει ένα ηλεκτρόνιο και αυτό να εγκαταλείψει την ζώνη σθένους αφήνοντας πίσω του μια οπή. Εάν η οπή παραμείνει στην ζώνη σθένους και το απομακρυσμένο ηλεκτρόνιο παραμείνει κοντά σε αυτή τη ζώνη, θα αναπτυχθούν ελκτικές δυνάμεις μεταξύ οπής και ηλεκτρονίου (Coulomb) και έτσι δημιουργείται ένα ζεύγος ηλεκτρονίου-οπής το οποίο καλείται εξιτόνιο.



Σχήμα 5.5 [31]

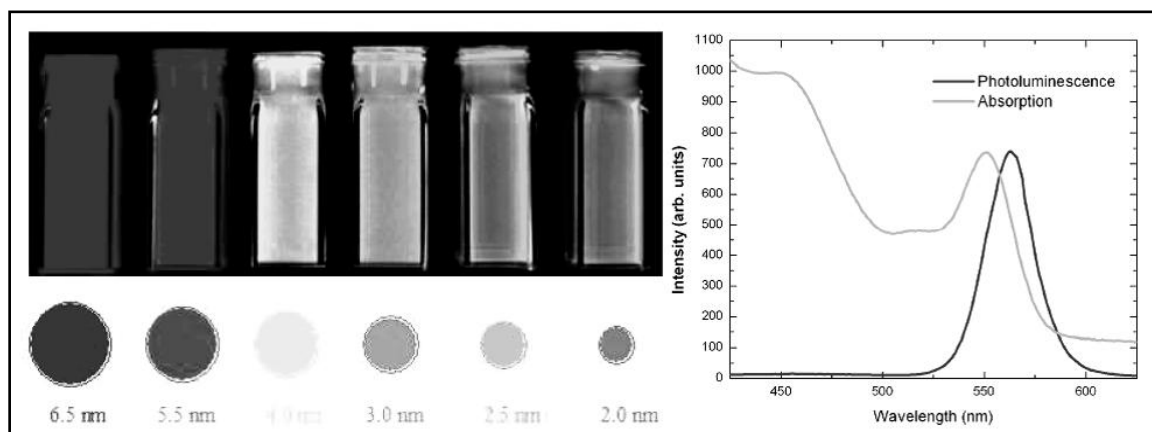


Σχήμα 5.6 [33]

Το πιο συνηθισμένο σχήμα κβαντικών τελειών είναι το σφαιρικό στο οποίο πιο εύκολος είναι ο υπολογισμός της εξίσωσης του Schrodinger (§ 2.3). Οι κβαντικές τελείες μπορούν να περιέχουν ηλεκτρόνια ή ζεύγη ηλεκτρονίων –

οπών τα οποία περιορίζονται σε μηδενικές διαστάσεις λόγω του μικρού μεγέθους των κβαντικών τελειών με αποτέλεσμα το υλικό να μην έχει συνεχές φάσμα και έτσι να παρουσιάζει γραμμικό ενεργειακό φάσμα.

Η κβαντική τελεία περιέχει ένα μικρό αριθμό (1 έως 100) ηλεκτρονίων της ζώνης αγωγιμότητας, οπές της ζώνης σθένους ή εξιτόνια (δηλαδή καθορισμένο αριθμό στοιχειωδών ηλεκτρικών φορτίων με δυνάμεις ηλεκτροστατικής φύσεως -Coulomb-). Μικρές κβαντικές τελείες μπορεί να είναι κολλοειδείς ημιαγωγοί νανοκρύσταλλοι (2-10 nm) δηλαδή με διάμετρο μέσα στον όγκο της κβαντικής τελείας από 100 έως 10^5 άτομα. Στις κβαντικές τελείες το ενεργειακό φάσμα ρυθμίζεται ανάλογα με το μέγεθός τους και το περιοριστικό τους δυναμικό.



Σχήμα 5.7 [31]

Όσο μεγαλύτερη είναι η κβαντική τελεία τόσο πιο ερυθρή είναι ενώ αντιθέτως όσο πιο μικρή τόσο πιο μπλέ εμφανίζεται όπως αποτυπώνεται αντίστοιχα στο σχήμα από αριστερά προς τα δεξιά.

Το ενεργειακό φάσμα που καθορίζει την ενέργεια φθορισμού και συνεπώς και το χρώμα του φθορίζοντος φωτός είναι αντιστρόφως ανάλογο με το τετράγωνο του μεγέθους της τελείας. Μεγάλες κβαντικές τελείες έχουν περισσότερα ενεργειακά επίπεδα με μικρότερη απόσταση μεταξύ τους. Αυτό σημαίνει ότι μπορούν μόνο να απορροφούν φωτόνια με λιγότερη ενέργεια και κυρίως αυτά που βρίσκονται στην κόκκινη περιοχή του φάσματος. Σημαντικό πλεονέκτημα των κβαντικών τελειών είναι η δυνατότητα που έχουν να μεταβάλλουν το μέγεθός τους [31].

Ερευνητές από το National Institute of Standards and Technology (NIST) και το Joint Quantum Institute (JQI) -ομάδας του NIST- ένα συνεργαζόμενο κέντρο του

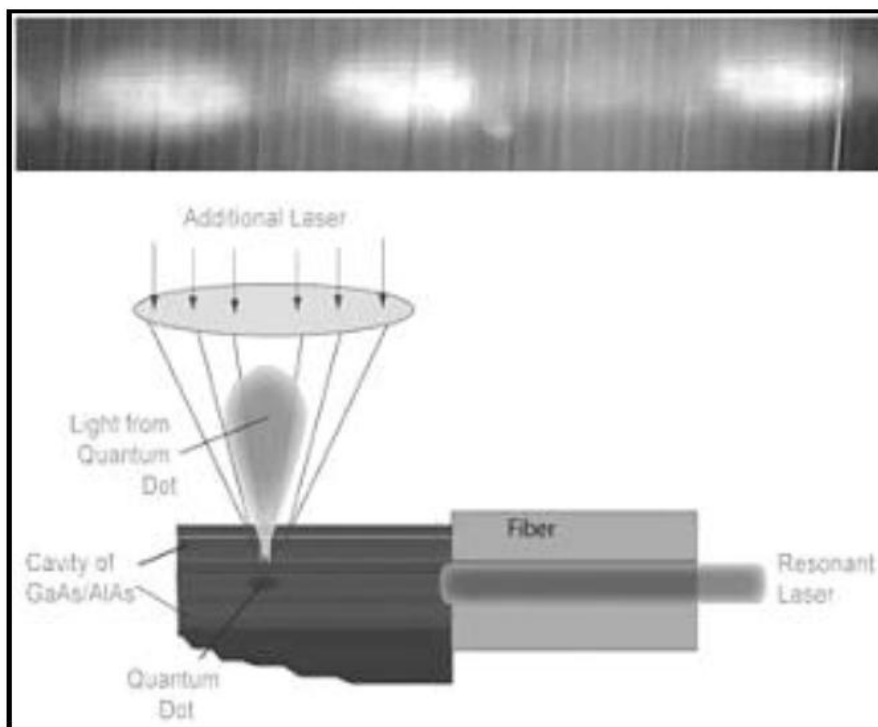
University of Maryland και του NIST, ανέφεραν έναν νέο τρόπο να ρυθμίζουν το προερχόμενο από τις κβαντικές τελείες, φως ελέγχοντάς το με ζεύγη laser. Η τεχνική τους (δημοσιεύτηκε στο *Physical Review Letters*), θα μπορούσε να βελτιώσει σημαντικά τις κβαντικές τελείες ως πηγή ζευγών «πλεγμένων» φωτονίων. Η επίτευξή της μπορεί να επιταχύνει την ανάπτυξη ισχυρών εξελιγμένων εφαρμογών κβαντικής κρυπτογραφίας που παρουσιάζεται ίσως, ως το κλειδί της τεχνολογίας του αιώνα που διανύουμε καθώς τα φωτόνια αυτά αποτελούν μια ιδιαίτερη συνέπεια της κβαντικής μηχανικής. Δύσκολα στην παραγωγή, παραμένουν διασυνδεδεμένα ακόμα και όταν απομακρυνθούν σε μεγάλες αποστάσεις. Απλά παρατηρώντας το ένα από αυτά ακαριαία επηρεάζει τις ιδιότητες του άλλου (μη τοπικότητα, §3.4). Το ζευγάρι αυτό μπορεί να χρησιμοποιηθεί στις κβαντικές επικοινωνίες για να περάσουν έναν κωδικό κλειδί το οποίο από τη φύση του είναι απόλυτα ασφαλές, καθώς κάθε προσπάθεια να κρυφακούσουν ή να εμποδίσουν τον κωδικό-κλειδί θα ανιχνευθεί αμέσως [29].

Ένας στόχος της ομάδας του NIST-JQI είναι να αναπτύξουν τις τεχνικές ώστε να καταστήσουν τις κβαντικές τελείες μία εύκολη πηγή ζευγών φωτονίων. Οι κβαντικές τελείες όπως προαναφέρθηκε, ανήκουν στις περιοχές νανοκλίμακας ενός ημιαγωγίμου υλικού παρόμοιου με το υλικό στους επεξεργαστές υπολογιστών, αλλά με ειδικές ιδιότητες χάρη στο πολύ μικρό τους μέγεθος. Παρ' όλο που μπορούν να συντεθούν από δεκάδες χιλιάδες άτομα, οι κβαντικές τελείες σε πολλές περιπτώσεις συμπεριφέρονται σχεδόν σα να είναι μεμονωμένα άτομα. Δυστυχώς αυτό, δεν είναι αρκετό όταν αφορά τελικά τον «εύθραυστο κόσμο» της κρυπτογραφίας και των τεχνολογιών πληροφορίας επόμενης γενιάς. Όταν ενεργοποιηθεί μια κβαντική τελεία εκπέμπει φωτόνια, ή «σωματίδια» φωτός, ακριβώς όπως κάνει ένα απομονωμένο άτομο. Αλλά οι ατέλειες στο σχήμα μιας κβαντικής τελείας προκαλούν, εκεί που θα έπρεπε να υπάρχει επικάλυψη ενεργειακών επιπέδων, το διαχωρισμό τους [29].

Για να ξεπεράσουν αυτό το πρόβλημα, η ομάδα του NIST-JQI χρησιμοποιεί laser για να ελέγξει με ακρίβεια τα επίπεδα ενέργειας των κβαντικών τελειών, ακριβώς όπως έκαναν οι φυσικοί με απλά άτομα από τα μέσα της δεκαετίας του '70 και ακόμα πιο πρόσφατα, με την ποικιλία τεχνητών κβαντικών τελειών. Με την συνήθη τους διάταξη, που περιλαμβάνει δύο laser - με το ένα να βρίσκεται πάνω από την κβαντική τελεία και το άλλο να την φωτίζει από το πλάι οι ερευνητές ήταν σε θέση να ελέγξουν τις ενεργειακές καταστάσεις σε μια κβαντική τελεία και να μετρήσουν απ' ευθείας τις εκπομπές της. Ρυθμίζοντας την ένταση των δεσμών του laser, μπορούσαν να διορθώσουν την προκαλούμενη εκ των ατελειών απόκλιση και να παράγουν ιδανικότερα σήματα. Έτσι, η ομάδα NIST-JQI ήταν η πρώτη που υποστήριξε ότι οι ρυθμιζόμενες με laser κβαντικές τελείες μπορούν αποτελεσματικά

να παράγουν φωτόνια ένα τη φορά, όπως απαιτείται στην κβαντική κρυπτογραφία [29] (και σε άλλες εφαρμογές π.χ. γνωματούσεις πυρηνικής φυσικής).

Η συσκευή προς το παρόν απαιτεί πολύ χαμηλές θερμοκρασίες και είναι μέσα σε υγρό ήλιο, είναι αρκετά μικρή ώστε να χωρέσει στην παλάμη του ανθρώπινου χεριού (μια «κομψή» κατασκευή που θα μπορούσε τελικά να αξιοποιηθεί σε εφαρμογές της κβαντικής κρυπτογραφίας).



Σχήμα 5.8 [29]

Σχηματική αναπαράσταση της πειραματικής συσκευής του NIST-JQI: Η εικόνα ενός αντιπροσωπευτικού δείγματος μικροσκοπίου STM (scanning tunneling microscope) δείχνει τις περιοχές μιας κβαντικής τελείας ίνδιου-αρσενικού που είναι τοποθετημένες σε γάλλιο-αρσενικό. Κάθε «τελεία» έχει περίπου 30nm μήκος - οι εξασθενημένες γραμμές είναι ξεχωριστές σειρές ατόμων. Περιορίζοντας το συντονισμό του laser στη σωστή γωνία για το φως της κβαντικής τελείας ελαχιστοποιείται η σκέδαση.

Πειραματικές εφαρμογές των κβαντικών τελειών οι οποίες δεν έχουν ευκρινείς διαστάσεις, εμφανίζουν οξύτερη πυκνότητα καταστάσεων από άλλες δομές με περισσότερες διαστάσεις οπότε έχουν και καλύτερες οπτικές και μεταφορικές ιδιότητες. Επίσης μεταβάλλουν γραμμικά το φως και ερευνάται σε επιπλέον τομείς η

δράση τους (όπως σε διόδους laser). Επίσης με την εφαρμογή μικρών τάσεων μπορεί να ελεγχθεί η ροή των ηλεκτρονίων μέσα από την κβαντική τελεία και έτσι μπορούν να γίνουν μετρήσεις ακριβείας όσον αφορά το spin ή άλλες ιδιότητες του ηλεκτρονίου. Για την δημιουργία κβαντικών τελειών υπάρχουν φυσικές και χημικές μέθοδοι [31].

Οι μέθοδοι με φυσικό τρόπο που παρασκευάζουν τις κβαντικές τελείες είναι α) η χάραξη, β) η διαμόρφωση ηλεκτρικού πεδίου, γ) η διάχυση ανάμεσα στο φράγμα και στο κβαντικό πηγάδι, δ) η δημιουργία σε μορφή ημιαγωγίων κρυστάλλων εμβυπτισμένων μέσα σε γυάλινες διηλεκτρικές μήτρες, ε) η επιλεκτική ανάπτυξη μιας ημιαγωγικής ένωσης με χαμηλότερο ενεργειακό χάσμα πάνω σε επιφάνεια μιας άλλης ένωσης με ευρύτερο χάσμα και στ) με αυτό-οργανωμένη ανάπτυξη.

Οι μέθοδοι με χημικό τρόπο αφορούν κυρίως την δημιουργία κβαντικών τελειών με προετοιμασία ημιαγωγίων νανοσωματιδίων που περιλαμβάνουν καθίζηση κολλοειδών σωματιδίων από ομογενές διάλυμα. Αυτή η καθίζηση οφείλεται στην ελεγχόμενη ελευθέρωση ιόντων.

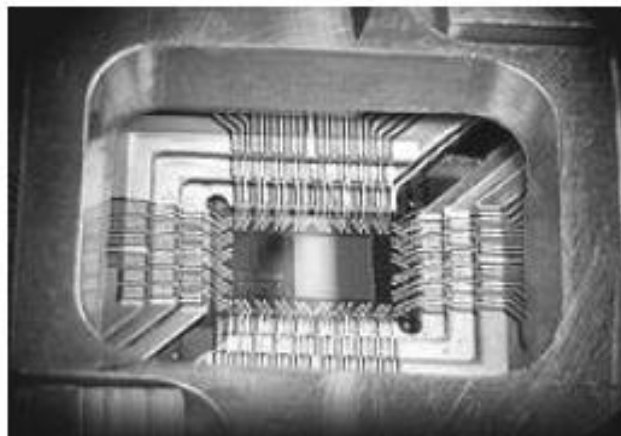
5.4 D-WAVE ΚΒΑΝΤΙΚΟΣ ΥΠΟΛΟΓΙΣΤΗΣ

Σύμφωνα με πρόσφατα δημοσιεύματα από ειδησιογραφικά site τεχνολογίας, ένας κβαντικός υπολογιστής αξίας 15 εκατομμυρίων δολαρίων, θα τοποθετηθεί σε εγκατάσταση της NASA. Ο υπολογιστής φέρει την ονομασία D-wave και τα τελευταία χρόνια γίνεται ιδιαίτερος «ντόρος» γύρω από αυτόν. Η αμερικανική διαστημική υπηρεσία θα συνεργάζεται για τον υπολογιστή με την Google και με την επιστημονική κοινότητα ώστε να αξιοποιούν τις μεγάλες δυνατότητες του νέου ισχυρού υπολογιστή, ο οποίος θεωρείται πως είναι 3.500 (και άνω, σε κάποιες περιπτώσεις) φορές πιο γρήγορος από τους σημερινούς «συμβατικούς» υπολογιστές [34].

Η канаδική εταιρεία D-Wave Systems είχε αμφισβητηθεί από πολλούς κατά το πέρασμα των χρόνων, όσον αφορά το κατά πόσον τα μηχανήματά της αξιοποιούν πλήρως τους νόμους της κβαντικής μηχανικής. Πριν λίγα χρόνια η Καναδική εταιρεία πούλησε το πρώτο κβαντικό μοντέλο της στη Lockheed Martin. Το μηχάνημα που θα χρησιμοποιούν η NASA και η Google θα αξιοποιεί τις αλληλεπιδράσεις 512 κβαντικών bit –qubits-, ενώ υπάρχουν σχέδια για αναβάθμιση στα 2.048 μέσα στα άμεσα χρόνια, τα οποία θα αυξήσουν σημαντικά τις ήδη τεράστιες δυνατότητες του κβαντικού συστήματος [34].

Η D-Wave ιδρύθηκε από τον Haig Farris, Geordie Rose, Bob Wiens, και Alexandre Zagoskin. Το όνομα της εταιρείας αναφέρεται στο πρώτο qubit «αρχιτεκτονικών σχεδίων τους», όπου γίνεται χρήση υπεραγωγών D-wave. Η εταιρεία και ο D-Wave λειτουργεί ως ένα παρακλάδι του Πανεπιστημίου Κολούμπια, διατηρώντας παράλληλα ισχυρούς δεσμούς με το Τμήμα Φυσικής και Αστρονομίας ενώ επίσης συνεργάστηκε για ερευνητικό σκοπό με πληθώρα μεγάλων πανεπιστημίων. Ο D-Wave λειτουργεί από διάφορα σημεία στο Βανκούβερ του Καναδά.

Ο D-Wave One είναι ένα ολοκληρωμένο κβαντικό σύστημα υπολογιστή που τρέχει σε έναν επεξεργαστή 128-qubit και ανακοινώθηκε επισήμως το 2011. Ο επεξεργαστής που χρησιμοποιείται στον D-Wave One με την κωδική ονομασία "Rainier", εκτελεί ένα μονό μαθηματικό διακριτό σύστημα βελτιστοποίησης χρησιμοποιώντας την κβαντική θεωρία. Ο D-Wave One αποτυπώνεται ως το πρώτο εμπορικά διαθέσιμο κβαντικό σύστημα υπολογιστών στον κόσμο (με τιμή που το 2011 κοστολογήθηκε στα 10 εκατομμύρια δολάρια) [36].



Σχήμα 5.9 [36]

Φωτογραφία από ένα τσιπ που κατασκευάστηκε από την D-Wave Systems Inc., και έχει σχεδιαστεί για να λειτουργεί ως ένα 128qubit υπεραγωγίσιμος αδιαβατικός επεξεργαστής κβαντικής βελτιστοποίησης (Rainier), τοποθετημένος σε ένα δείγμα.

Το 2012 ανακαλύφθηκε από την D-Wave ένας 512-qubit κβαντικός υπολογιστής. Ο λεγόμενος D-Wave Two χρησιμοποιεί μία τεχνική ονόματι quantum tunneling, η οποία του επιτρέπει να λύνει μαθηματικά προβλήματα σε κλάσματα δευτερολέπτου, ουσιαστικά δοκιμάζοντας όλες τις πιθανές λύσεις και επιλέγοντας την καλύτερη. Ο υπολογιστής θα εγκατασταθεί στο Ames Research Center στην

Καλιφόρνια, και οι επιδόσεις του θα αποτελέσουν κριτήριο πάνω στο κατά πόσον μπορεί η τεχνολογία κβαντικών υπολογιστών να βοηθήσει στην εξέλιξη του machine learning και της τεχνητής νοημοσύνης. Ερευνητές από πανεπιστήμια θα έχουν την ευκαιρία να αξιοποιήσουν το 20% του χρόνου του υπολογιστή, μέσω της USRA (Universities Space Research Association) [34]. Η Google από την πλευρά της, έχει ανακοινώσει ότι έχει ήδη αναπτύξει αλγορίθμους machine learning που λειτουργούν μέσα στον υπολογιστή του αποκαλούμενου Quantum Artificial Intelligence Lab. Η εταιρεία σκοπεύει να επικεντρωθεί σε τομείς του machine learning που έχουν να κάνουν με την αναγνώριση προσώπου και φωνής, τη συμπεριφορά βιολογικών οργανισμών και τη διαχείριση μεγάλων και εξαιρετικά σύνθετων συστημάτων.



Σχήμα 5.10 [34, 35]

Φαίνεται η εξωτερική μορφή του tower που έχει ο πρώτος κβαντικός υπολογιστής της D-Wave που βγήκε επισήμως στις αγορές υψηλής τεχνολογίας. Ονομάζεται και «μαύρος μονόλιθος». Η D-Wave είναι από τις

πρώτες εταιρείες που πειραματίζεται στην κατασκευή κβαντικών υπολογιστών για εμπορική χρήση. Όταν λέμε εμπορική φυσικά δεν εννοούμε τον απλό καταναλωτή αλλά μεγάλες εταιρείες που έχουν ανάγκη από τεράστια υπολογιστική δύναμη. Όπως προαναφέρθηκε οι κβαντικοί υπολογιστές δεν είναι υπολογιστές γενικής χρήσης αλλά μπορούν να κάνουν πιο συγκεκριμένες διεργασίες (για τον «μονόλιθο» της D-Wave One το υπερ-αγώγιμο *tsip -ο επεξεργαστής-* των 128 qubits καλείται Rainier). Επίσης ο «μονόλιθος» της D-Wave One είναι θωρακισμένος πίσω από το μαύρο κύβο με ειδικά φίλτρα για να προστατεύεται από κάθε εξωτερικό παράγοντα όπως χαρακτηριστικά τον θόρυβο, για να εκτελείται έτσι απερίσκεπτα η κβαντική επεξεργασία χωρίς να ανεβαίνει η θερμοκρασία (καθώς η ψύξη γίνεται σε θερμοκρασίες λίγο πάνω από το απόλυτο μηδέν).

Η Google αποφάσισε να δοκιμάσει αυτούς τους υπολογιστές για να δει πόσο ανταπεξέρχονται στις εργασίες που τους ανατίθενται. Έτσι η εταιρεία δημιούργησε κάποια «τεχνάσματα» τα οποία έδειξαν ότι τα συγκεκριμένα μηχανήματα είναι πολύ ανταποκρίσημα σε αυτό που κάνουν αλλά έχουν και τα όρια τους. Η γενιά κβαντικών υπολογιστών D-Wave two, είναι 35.500 φορές πιο γρήγορη από ένα υπολογιστή γενικής χρήσης όταν και οι D-Wave two τρέχουν ένα συγκεκριμένο πρόγραμμα. Ωστόσο μερικά από τα πλεονεκτήματα εξαφανίζονται όταν ένας υπολογιστής γενικής χρήσης τρέχει κώδικα που εξομοιώνει κβαντικούς υπολογισμούς. Παρόλο που το hardware του D-Wave είναι καλύτερο όταν έχει να κάνει με δομημένο κώδικα, σε τυχαία προβλήματα τρέχει όπως ένα συμβατικό σύστημα [35].

Η D-Wave όμως έχει επικριθεί από ορισμένους επιστήμονες στο κβαντικό πεδίο της πληροφορικής. Ανεξάρτητοι ερευνητές διαπίστωσαν ότι διάφορα πακέτα λογισμικού που τρέχουν σε ένα μονό πυρήνα επιτραπέζιου υπολογιστή μπορεί να λύσει τα ίδια προβλήματα από ό, τι ο υπολογιστής D-Wave (όπως για τετραγωνικά δυαδικά προβλήματα βελτιστοποίησης). Το 2007 ο καθηγητής στο Πανεπιστήμιο της Καλιφόρνια (UC) Berkeley, Umesh Vazirani, και ένας από τους ιδρυτές της κβαντικής θεωρίας πολυπλοκότητας ισχυρίστηκε ότι η επιτάχυνση των D-wave έναντι των κλασικών αλγορίθμων φαίνεται να βασίζεται σε μια «παρανόηση». Ισχυρίστηκε ότι η δύναμη των κβαντικών υπολογιστών και η ταχύτητά τους, δυστυχώς δεν είναι δεδομένη και χειροπιαστή και αν ακόμη δημιουργηθεί κατασκευαστικά ένας κβαντικός υπολογιστής, ο οποίος θα μπορεί να κλιμακωθεί σε χιλιάδες qubits, θα ήταν πιθανό να μην είναι πιο ισχυρός από ό, τι ένα έξυπνο κινητό τηλέφωνο νεότερης γενιάς. Πριν από το 2011, ο υπολογιστής D-Wave επικρίθηκε για

την έλλειψη αποδείξεων ότι ήταν στην πραγματικότητα είναι ένας αληθινός κβαντικός υπολογιστής. Τα ερωτήματα προέρχονταν, λόγω της έλλειψης πειστικών πειραματικών αποδείξεων της κβαντικής διεμπλοκής στο εσωτερικό των συσκευών D-Wave [37].

Τον Μάρτιο 2013 αρκετές ομάδες ερευνητών στο εργαστήριο «Adiabatic Quantum Computing» στο Ινστιτούτο Φυσικής του Λονδίνου προσκόμισαν αποδεικτικά στοιχεία -αν και χαρακτηρίστηκαν, μόνο έμμεσα- της κβαντικής διεμπλοκής στα τσιπ της D-Wave. Τον Μάιο του 2014, οι ερευνητές στο D-Wave, η Google, USC, το Simon Fraser University και το National Research Tomsk Polytechnic δημοσίευσε ένα έγγραφο που περιέχει τα πειραματικά αποτελέσματα οποία έδειξαν την παρουσία επίσης διεμπλοκής μεταξύ των qubits του D-Wave. Επίσης παρουσιάστηκε η φασματοσκοπία qubit σήραγγας που χρησιμοποιήθηκε για να μετρηθεί η ενέργεια - eigenspectrum - των συστημάτων δύο και οκτώ-qubits [36].

5.5 ΕΡΕΥΝΗΤΙΚΕΣ ΠΡΟΣΠΑΘΕΙΕΣ ΚΑΙ ΚΑΙΝΟΤΟΜΙΕΣ

Επιστήμονες υπό την ηγεσία του καθηγητή φυσικής Jeremy O' Brien, από το πανεπιστήμιο του Bristol της Αγγλίας, δίνουν πλέον τη δυνατότητα σε απλούς χρήστες του διαδικτύου να χρησιμοποιήσουν έναν κβαντικό επεξεργαστή του ιδρύματος. Το επιχείρημα πίσω από αυτή την καινοτόμα δράση, είναι η προσπάθεια δημιουργίας πεπειραμένων προγραμματιστών, για τη στιγμή που οι κβαντικοί υπολογιστές θα αποτελέσουν κομμάτι της καθημερινότητάς μας. Οι ερευνητές σχεδίασαν τον επεξεργαστή και δημιούργησαν αυτή την υπηρεσία στο διαδίκτυο, με το όνομα **QCloud** [39]. Ένα κβαντικό τσιπ επεξεργάζεται την πληροφορία που περιέχουν τα qubits. Μόνο μερικά εργαστήρια στον κόσμο έχουν τη δυνατότητα να εκτελέσουν πειράματα σε κβαντικούς επεξεργαστές (οργανισμοί όπως η NASA ή η Google). Ο επεξεργαστής του QCloud, λειτουργεί οδηγώντας ζεύγη από φωτόνια μέσα σε μια σειρά από οπτικά κανάλια. Καθώς διαδίδονται τα φωτόνια, «διεμπλέκονται» κβαντικά (δηλαδή η κβαντική μέτρηση των ιδιοτήτων του ενός, επηρεάζει τις ιδιότητες του άλλου, § 3.6). Ο χρήστης, προγραμματίζοντας τη συσκευή μπορεί να πραγματοποιήσει ένα πλήθος από υπολογισμούς ακόμα και μέσω εφαρμογής στο διαδίκτυο σε έκδοση προσομοίωσης του επεξεργαστή, μαζί με υλικό που βοηθάει τον χρήστη που δεν έχει εξοικειωθεί με το αντικείμενο. Ο επεξεργαστής αποτελείται από 2 qubits (η ομάδα του πανεπιστημίου πειραματίζεται και με επεξεργαστές των 6 και 8 qubits). Αν και στα πρώτα του βήματα, ο υπολογιστής του QCloud δε συγκρίνεται με τις επιδόσεις των εμπορικών υπολογιστών, η πρώτη φορά

που εφαρμόζεται η λογική των υπηρεσιών συννέφου (cloud services) στους κβαντικούς υπολογιστές είναι μια πολλά υποσχόμενη εξέλιξη.

Επίσης μια άλλη ερευνητική ομάδα (επιστήμονες, με επικεφαλής ερευνητές του πανεπιστημίου του Μπρίστολ) έχει προχωρήσει στη δημιουργία ενός νέου, πολλά υποσχόμενου, **κβαντικού τσιπ** που ανοίγει τον δρόμο για απολύτως ασφαλείς επικοινωνίες στα κινητά τηλέφωνα και για πολύ γρήγορους ηλεκτρονικούς υπολογιστές, με δυνατότητες σαφώς πέρα από αυτές των τωρινών συσκευών που βασίζονται στα συμβατικά τσιπ. Οι ερευνητές φιλοδοξούν το νέο τσιπ να κάνει τις ηλεκτρονικές συσκευές «άτρωτες» έναντι πιθανών απειλών από χάκερ και έτσι οι ηλεκτρονικές συναλλαγές των χρηστών με τράπεζες και γενικότερα ηλεκτρονικού εμπορίου, να διεξάγονται με μεγαλύτερη ασφάλεια. Για το νέο τσιπ, εκτός από το Μπρίστολ, έχουν συνεργαστεί το σκοτσέζικο πανεπιστήμιο Heriot-Watt, το ολλανδικό πανεπιστήμιο Delft και τρεις εταιρίες (η Ιαπωνική Toshiba, η Φινλανδική Nokia και η Βρετανική Oclaro). Το νέο κβαντικό τσιπ είναι κατασκευασμένο από πυρίτιο, χρησιμοποιεί το φως και είναι χιλιάδες φορές μικρότερο από τα υπάρχοντα. Οι ερευνητές θεωρούν εφικτή τη μαζική παραγωγή και αξιοποίησή του σε εμπορικά προϊόντα. Η χρησιμοποίηση του πυριτίου στο κβαντικό τσιπ έχει το μεγάλο πλεονέκτημα ότι παρέχει συμβατότητα με τα υπάρχοντα εξαρτήματα, που εδώ και χρόνια η βιομηχανία ηλεκτρονικών χρησιμοποιεί για την παραγωγή τσιπ για κινητά και υπολογιστές. Ο καθηγητής φυσικής Jeremy O' Brien του πανεπιστημίου του Μπρίστολ που εισηγείται των προσπάθειών ανάπτυξης του Q-Cloud υποστηρίζει ότι οι κβαντικοί επεξεργαστές θα ήταν δυνατό να ενσωματωθούν στα συμβατικά μικροηλεκτρονικά κυκλώματα το πολύ μέσα στα επόμενα άμεσα χρόνια. Αντίθετα με τα συμβατικά τσιπ πυριτίου που δουλεύουν μέσω «χειραγώγησης» του ηλεκτρικού ρεύματος που τα διατρέχει, τα κβαντικά τσιπ «χειραγωγούν» τα σωματίδια του φωτός, τα φωτόνια, για να εκτελέσουν τους υπολογισμούς τους. Ένα τσιπ με 100 φωτόνια θεωρητικά θα μπορούσε να λύσει τρισεκατομμύρια εξισώσεις ταυτόχρονα. Τα νέα κβαντικά κυκλώματα είναι συμβατά και με την τεχνολογία των οπτικών ινών που χρησιμοποιούνται στις υποδομές των ευρυζωνικών τηλεπικοινωνιακών δικτύων και του διαδικτύου διεθνώς, καθώς λειτουργούν στα ίδια μήκη κύματος. Τα φωτόνια των κβαντικών τσιπ και το φως που μεταφέρει τις πληροφορίες μέσω των οπτικών ινών, διέπονται από τους ίδιους κβαντικούς νόμους και θα λέγμε ότι «μιλούν την ίδια γλώσσα» [38].

Η μνήμη των κβαντικών υπολογιστών καλείται **μαγνητική μνήμη τυχαίας προσπέλασης – MRAM**- και μέσω της MRAM επιτυγχάνεται η υπέρθεση κατάστασης των μικροσωματίων με την εφαρμογή των μαγνητικών επιδράσεων πάνω στην ιδιοπεριστροφή των σωματίων αυτών. Επιστημονική ομάδα από τον Καναδά, τη Βρετανία και τη Γερμανία, με επικεφαλής τον Καναδό καθηγητή Michael Thewould

του πανεπιστημίου Shaimon Freizer κατάφεραν να σπάσουν το παγκόσμιο ρεκόρ κβαντικής μνήμης, διατηρώντας σταθερή μια εύθραυστη κβαντική σχέση επί 39 λεπτά σε συνθήκες δωματίου (25° C) για τρεις ώρες, σε συνθήκες κοντά στο απόλυτο μηδέν. Αυτό το επίτευγμα ξεπερνά ακόμα ένα τεχνικό εμπόδιο καθώς το προηγούμενο ανεπίσημο ρεκόρ μνήμης (ανεπίσημο, αφού δεν υπάρχει «κβαντικό βιβλίο Γκίνες») ήταν 25 δευτερόλεπτα σε συνθήκες δωματίου (3 min σε χαμηλή θερμοκρασία και είχε επιτευχθεί από τον Thandeous Land από το πανεπιστήμιο Stanford). Αυτό έχει ως αποτέλεσμα την δυνατότητα για την πραγματικά μακρόχρονη αποθήκευση κβαντικών πληροφοριών σε συνθήκες δωματίου. Η σημασία του νέου ρεκόρ είναι ακριβώς ότι οι επιστήμονες κατόρθωσαν να σταθεροποιήσουν την κβαντική μνήμη για χρόνο σχεδόν 100 φορές μεγαλύτερο από ό,τι είχαν πετύχει ως τώρα. Η ερευνήτρια Stagan Seamons του Τμήματος Υλικών του πανεπιστημίου της Οξφόρδης επισήμανε πως απομένουν ακόμα πολλές τεχνικές δυσκολίες να ξεπεραστούν, προτού καταστεί εφικτό να εκτελεστούν μεγάλης κλίμακας κβαντικοί υπολογισμοί. Το μεγαλύτερο εμπόδιο είναι να τοποθετηθούν διαφορετικά qubits σε διαφορετικές καταστάσεις και να τεθεί υπό έλεγχο ο τρόπος που αντιδρούν μεταξύ τους [46].

5.6 ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ ΚΑΙ ΑΠΟΣΥΝΟΧΗ

Η διόρθωση σφαλμάτων είναι απαραίτητη στην υλοποίηση των κβαντικών υπολογιστών γιατί τα κβαντικά συστήματα αλληλεπιδρούν με το περιβάλλον και αυτή η αλληλεπίδραση μπορεί να οδηγήσει σε κατάρρευση του συστήματος. Οπότε για την επιτυχή λειτουργία των κβαντικών υπολογιστών είναι απαραίτητη η ύπαρξη μηχανισμών που θα διορθώνει τα λάθη και τα σφάλματα. Ένα από τα σημαντικά λάθη που μπορεί να παρουσιαστούν είναι η αποσυννοχή (§ 3.6).

Αλληλεπιδράσεις μεταξύ των κβαντικών καταχωρητών και τυχαίων καταστάσεων με το περιβάλλον οδηγούν στην κατάρρευση της κατάστασης του συστήματος. Αυτό ουσιαστικά είναι μια «μέτρηση» του καταχωρητή η οποία είναι μία μη αντιστρεπτή διεργασία. Αν το σύστημα βρίσκεται σε μια αρχική κατάσταση και μετρηθεί μια άλλη κατάσταση, ένα δεύτερο qubit, τότε η κατάσταση του συστήματος καταρρέει και κατά συνέπεια χάνεται με μη αναστρέψιμο τρόπο η αποθηκευμένη πληροφορία [6]. Η επίλυση αυτού του προβλήματος είναι εξαιρετικά δύσκολη και η επαναφορά του συστήματος μετά από τέτοια λάθη είναι σχεδόν αδύνατη.

Στους κβαντικούς υπολογιστές φαντάζει αρκετά δύσκολο η ανάπτυξη κωδικών για την αποσφαλμάτωση και την διόρθωση των κβαντικών καταστάσεων λόγω των κβαντικών αρχών (αβεβαιότητας) σε αντίθεση με τους κλασσικούς υπολογιστές όπου για τον περιορισμό των σφαλμάτων, γίνεται χρήση κωδικοποίησης καθ' ενός bit ως μια «τριπλέτα» από όμοια bits. Τότε αν ένας θόρυβος αντιστρέψει ένα bit, το σφάλμα μπορεί να διορθωθεί αντικαθιστώντας το μεμονωμένο bit της «τριπλέτας» από αυτά τα όμοια bit.. Στους κβαντικούς υπολογιστές αυτή η μέθοδος δεν κωδικοποιείται με επιτυχία καθώς δεν μπορούμε να εξετάσουμε κάθε αντίγραφο ενός qubit χωρίς να καταστρέψουμε όλα τα αντίγραφα (η κβαντική θεωρία απαγορεύει να φτιάξουμε ένα άγνωστο qubit με αξιοπιστία ως προς ένα αντίγραφο του). Το αποτέλεσμα αυτό είναι γνωστό ως θεώρημα της αδυναμίας κλωνοποίησης [6, 49].

Την δεκαετία του 1990 ερευνητές από την IBM υποστήριξαν ότι η κβαντική διόρθωση σφαλμάτων θα καταστεί αναγκαία για τους κβαντικούς υπολογιστές, αλλά οι κλασικοί κώδικες δεν μπορούν να χρησιμοποιηθούν στον κβαντικό κόσμο και απέδειξαν πως μπορούμε να κάνουμε κβαντική διόρθωση σφαλμάτων, χωρίς να χρειάζεται να ξέρουμε τις καταστάσεις των qubits. Όπως και με τον κώδικα της «τριπλέτας», κάθε τιμή παριστάνεται με ένα σύνολο από qubits. Τα qubits αυτά οδεύουν μέσα από ένα κβαντικό κύκλωμα το οποίο βρίσκει με επιτυχία ένα σφάλμα στα qubits χωρίς να αναγνωρίσει πραγματικά ποιες είναι οι ξεχωριστές καταστάσεις τους. Η προστασία των κβαντικών καταστάσεων από τον θόρυβο και τα σφάλματα υλοποιήθηκε με τη χρήση ενός συνδυασμού ιδεών της κλασσικής πληροφορικής και κβαντικής θεωρίας, με θεωρήσεις όπως ότι φυσικά συστήματα μπορεί να έχουν ένα τύπο φυσικής ανοχής στο θόρυβο και θα μπορούν να χρησιμοποιήσουν την κβαντική διόρθωση σφαλμάτων, χωρίς την επέμβαση κώδικα και επίσης θα μπορούν να επιδείξουν θετική συμπεριφορά ως προς την αντίσταση στην καταστροφή της κβαντικής υπέρθεσης των καταστάσεων [6].

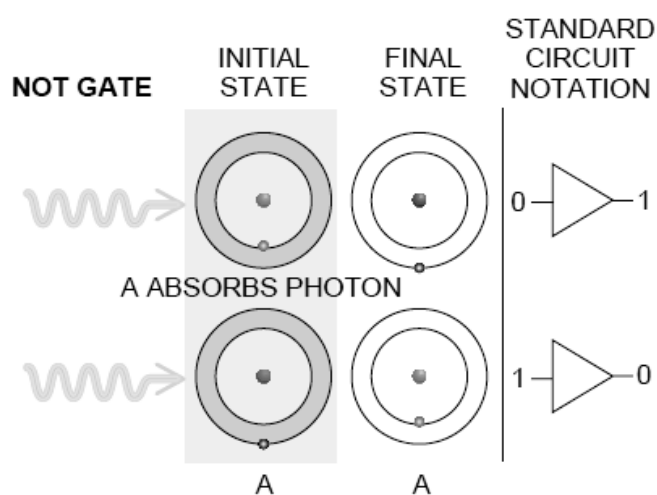
ΚΕΦΑΛΑΙΟ 6^ο

ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ

6.1 ΕΙΣΑΓΩΓΗ ΣΤΙΣ ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ

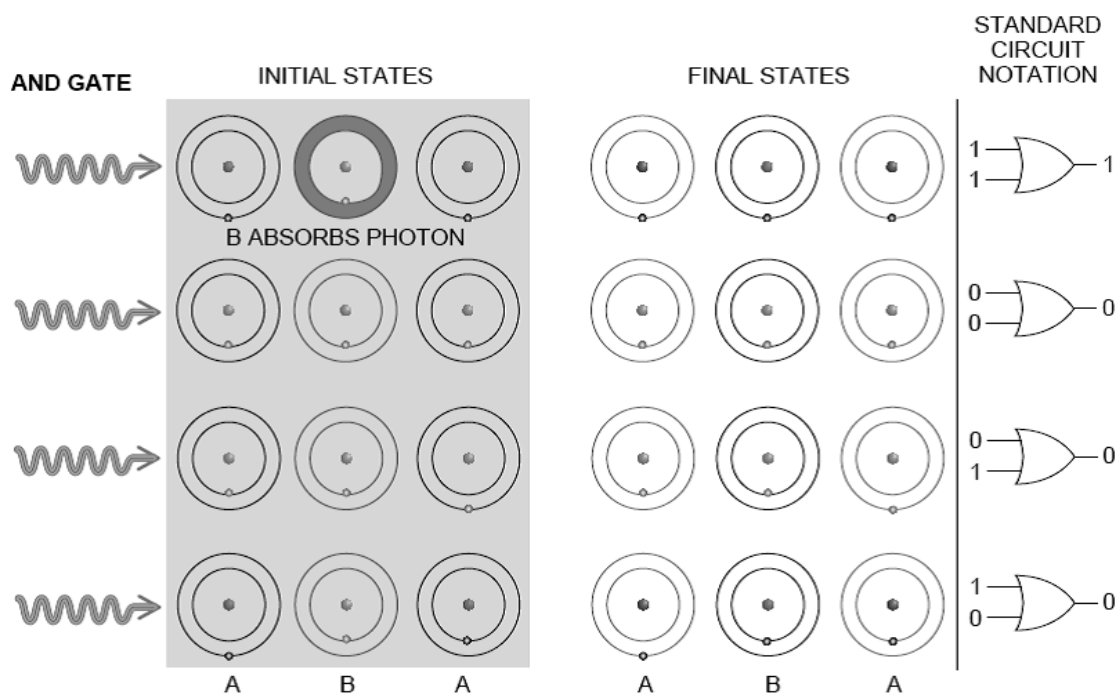
Οι κβαντικές πύλες των κβαντικών υπολογιστών δεν είναι φυσικά συστήματα όπως συμβαίνει στους κλασσικούς υπολογιστές, αλλά αντιπροσωπεύουν δράσεις που ασκούνται σε qubits ή σε κβαντικούς καταχωρητές. Σε αντίθεση με τους κλασσικούς υπολογιστές που αποτελούνται από κυκλώματα, ολοκληρωμένα και αγωγούς χάραξης πάνω στο τυπωμένο κύκλωμα για να διέρχεται το ηλεκτρικό ρεύμα μέσω του οποίου μεταφέρεται η πληροφορία την οποία οι λογικές ψηφιακές πύλες την μετατρέπουν μετά από ψηφιακή επεξεργασία από είσοδο σε έξοδο (με τον πίνακα αληθείας ή το αντίστοιχο λογικό κύκλωμα), στους κβαντικούς υπολογιστές η πληροφορία δε διέρχεται μέσα από τις κβαντικές πύλες αλλά βρίσκεται αποθηκευμένη σε qubits ή σε κβαντικούς καταχωρητές και παραμένει εκεί.

Οι κβαντικές πύλες είναι τελεστές του χώρου Hilbert που δρουν σε qubits και σε κβαντικούς καταχωρητές αλλάζοντας την κατάσταση τους (οι τελεστές αυτοί είναι unitary και εξ' ορισμού είναι αντιστρέψιμοι σε χώρους Hilbert § 2.8). Οι καταστάσεις των qubits και των κβαντικών καταχωρητών είναι διανύσματα στον χώρο Hilbert. Δηλαδή οι κβαντικές πύλες περιστρέφουν τα διανύσματα κατάστασης των qubits και των κβαντικών καταχωρητών χωρίς να αλλάζουν το μήκος τους, το οποίο είναι πάντα ίσο με τη μονάδα. Αυτές οι δράσεις που ασκούνται σε qubits και καταχωρητές από τις κβαντικές πύλες είναι τελεστές σε μορφή ορθομονοδιαίων πινάκων.



Σχήμα 6.1 [26]

Η πύλη NOT δεν χρειάζεται τίποτα περισσότερο από λίγο «χτύπημα», όπως δείχνει ο συμβολισμός στα δεξιά: εάν το A είναι 0, δίνει 1 και αντιστρόφως αν το A είναι 1 δίνει 0. Με χρήση ατόμων, αυτό μπορεί να γίνει με την εφαρμογή ένας παλμού του οποίου η ενέργεια ισούται με τη διαφορά μεταξύ της A αρχικής κατάστασης των ηλεκτρονίων του ατόμου, (που είναι η χαμηλότερη ενέργεια του επιπέδου, που δείχνεται ως του εσωτερικού δακτυλίου) και της διεγερμένης κατάστασης του (που εμφανίζεται ως εξωτερικός δακτύλιος). Σε αντίθεση με την συμβατική πύλη NOT των κλασσικών υπολογιστών, η κβαντική πύλη μπορεί να αναστρέψει τα bits στα μισά του δρόμου [26].



Σχήμα 6.2 [26]

Η πόλη ΚΑΙ εξαρτάται επίσης, από τις ατομικές αλληλεπιδράσεις. Έστω τρία άτομα τα A, B και A, «καθισμένα» δίπλα το ένα στο άλλο. Η διαφορά στην ενέργεια μεταξύ τους αρχικό (αρχικής ενέργειας) και των καταστάσεων του B είναι συνάρτηση των καταστάσεων και των δύο A. Έστω ότι το B είναι σε αρχική ενεργειακή κατάσταση. Τότε εφαρμόζεται παλμός του οποίου η ενέργεια ισούται με τη διαφορά μεταξύ των δύο καταστάσεων της B μόνο όταν το άτομο είναι γειτονικό του A και είναι 1. Εάν λοιπόν στην πραγματικότητα οι A καταστάσεις είναι 1, αυτός ο παλμός θα αναστρέψει το B (πάνω σειρά), αλλιώς θα αφήσει αμετάβλητο το B (όλες οι άλλες σειρές) [26].

Σημαντική διαφορά επομένως μεταξύ κλασσικών και κβαντικών πυλών είναι ότι στις κβαντικές πύλες η πληροφορία είναι αποθηκευμένη σε qubits ενώ στους κλασσικούς υπολογιστές προφανώς η πληροφορία προκύπτει μετά από επεξεργασία από τις πύλες. Οι κβαντικές πύλες είναι ένας «ιδιότυπος» τύπος κυκλώματος, το οποίο πραγματοποιεί πράξεις σε qubits για κάποιο χρονικό διάστημα, ενώ σε αντίθεση με τις κλασσικές, είναι πάντα αντιστρεπτές οπότε θα έχουν τον ίδιο αριθμό εισόδων και εξόδων [1, 6, 7, 26, 27].

Όλες οι κλασσικές λογικές πύλες μπορούν να υλοποιηθούν και με χρήση των κβαντικών λογικών πυλών. Δηλαδή οι κλασσικοί υπολογισμοί και η μετάδοση της πληροφορίας μπορεί να γίνει πράξη με την χρήση ενός κβαντικού υπολογιστή.

Συνοπτικά οι βασικές κβαντικές λογικές πύλες είναι οι εξής:

- Κβαντική πύλη αδράνειας
- Κβαντική πύλη Hadamard,
- Κβαντικές πύλες μετατόπισης φάσης,
- Ελεγχόμενες κβαντικές πύλες, δηλαδή
 - πύλη ελεγχόμενης άρνησης (CNOT),
 - πύλη ελεγχόμενης μετατόπισης φάσης (CΦ) ,
 - πύλη διπλά ελεγχόμενης άρνησης (CCNOT),
- Κβαντική πύλη Fredkin,
- Κβαντική πύλη Toffoli
- Κβαντικές πύλες Pauli, δηλαδή
 - κβαντική πύλη Pauli-X,
 - κβαντική πύλη Pauli-Y,
 - κβαντική πύλη Pauli-Z,

Οι κβαντικές πύλες μπορούν να δράσουν σε ένα ή δύο ή τρία qubits. Αντιστοίχως σε ένα qubits δρουν οι πύλες αδρανείας (I), μετατόπισης φάσης (Φ) και η πύλη Hadamard (H). Σε δύο qubits η πύλη ελεγχόμενου ΟΧΙ, CNOT και ελεγχόμενης φάσης CΦ και σε τρία η διπλά ελεγχόμενου ΟΧΙ η CCNOT και η πύλη Fredkin (F). Όλες αυτές θα αναλυθούν στις επόμενες παραγράφους.

6.2 ΚΒΑΝΤΙΚΗ ΠΥΛΗ ΑΔΡΑΝΕΙΑΣ

Η κβαντική πύλη αδράνειας δρα σε ένα qubit. Η πύλη αδρανείας συμβολίζεται με I και περιγράφει την δράση ενός τελεστή που καλείται τελεστής αδρανείας και ο οποίος αφήνει αμετάβλητη την κατάσταση του qubit σύμφωνα με την σχέση

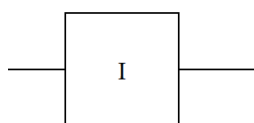
$$I|q\rangle = |q\rangle \quad 6.1$$

Η πύλη αδρανείας (όπως και οι επόμενες κβαντικές πύλες που δρουν σε ένα qubit) περιστρέφει το διάνυσμα κατάστασης ενός qubit μέσα στη σφαίρα Bloch, δηλαδή μεταβάλλονται οι γωνίες θ και ϕ , όπως φαίνεται στο σχήμα 4.5), αφήνοντας όμως αμετάβλητη την κατάσταση του.

Η κβαντική πύλη αδράνειας περιγράφεται από τον ακόλουθο πίνακα:

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad 6.2$$

Σε δίκτυα ο συμβολισμός της πύλης αδρανείας είναι ο εξής:



Η πληροφορία λοιπόν διέρχεται και μεταβιβάζεται μέσα από την πύλη. Συμβολίζουμε την κατάσταση του qubit πριν τη δράση του τελεστή με $|q_I\rangle$ (input). Ενώ μετά την δράση την συμβολίζουμε με $|q_o\rangle$ (output). Από τις ιδιότητες που φαίνονται στον πίνακα αληθείας οι καταστάσεις του qubit είναι αμετάβλητες.

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»	
Πύλη Αδρανείας	Input ($ q_I\rangle$)	Output ($ q_o\rangle$)
	$ q_I\rangle = 0\rangle$	$ q_o\rangle = 0\rangle$
	$ q_I\rangle = 1\rangle$	$ q_o\rangle = 1\rangle$
	$ q_I\rangle = q\rangle$	$ q_o\rangle = q\rangle$

Σχήμα 6.3

■ Τα χαρακτηριστικά του πίνακα προκύπτουν εύκολα μετά από τις ανάλογες πράξεις από την δράση της κβαντικής πύλης αδρανείας στις αρχικές καταστάσεις. Για την αρχική κατάσταση $|0\rangle$ η δράση της πύλης θα δώσει

$$|q_I\rangle \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = |0\rangle \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |0\rangle = |q_o\rangle$$

Επίσης για την κατάσταση $|1\rangle$ παρατηρούμε πως επίσης παραμένει αναλλοίωτη καθώς ισχύει

$$|q_1\rangle \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = |1\rangle \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |1\rangle = |q_0\rangle$$

Και τέλος

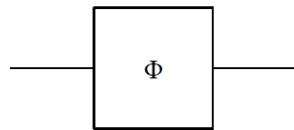
$$(\alpha|0\rangle + \beta|1\rangle) \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$$

6.3 ΚΒΑΝΤΙΚΗ ΠΥΛΗ ΜΕΤΑΤΟΠΙΣΗΣ ΦΑΣΗΣ

Η κβαντική πύλη μετατόπισης φάσης δρα σε ένα qubit. Συμβολίζεται με Φ και περιγράφεται από τον πίνακα:

$$\Phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} \quad 6.3$$

Σε δίκτυα ο συμβολισμός της πύλης μετατόπισης φάσης είναι ο εξής:



Η δράση της πύλης αυτής αλλάζει μόνο τη γωνία φάσης του qubit. Πράγματι έστω ένα qubit (input) σύμφωνα με την σχέση 4.3,

$$|q_1\rangle = \alpha|0\rangle + \beta|1\rangle$$

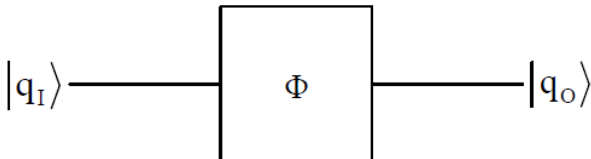
τότε με την δράση της κβαντικής πύλης μετατόπισης φάσης Φ , η νέα κατάστασή του θα είναι

$$|q_0\rangle = \alpha|0\rangle + \beta e^{i\varphi}|1\rangle.$$

Αυτό εύκολα αποδεικνύεται καθώς

$$|q_1\rangle \cdot \Phi = (\alpha|0\rangle + \beta|1\rangle) \cdot \Phi = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta e^{i\varphi} \end{bmatrix} = \alpha|0\rangle + \beta e^{i\varphi}|1\rangle = |q_0\rangle$$

Ο συμβολισμός και ο πίνακας αληθείας που αποδίδει τις χαρακτηριστικές ιδιότητες της πύλης μετατόπισης φάσης φαίνεται στο επόμενο σχήμα.

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»	
 Πύλη Μετατόπισης Φάσης	Input ($ q_I\rangle$)	Output ($ q_O\rangle$)
	$ q_I\rangle = 0\rangle$	$ q_O\rangle = 0\rangle$
	$ q_I\rangle = 1\rangle$	$ q_O\rangle = e^{i\varphi} 1\rangle$
	$ q_I\rangle = \alpha 0\rangle + \beta 1\rangle$	$ q_O\rangle = \alpha 0\rangle + \beta e^{i\varphi} 1\rangle$

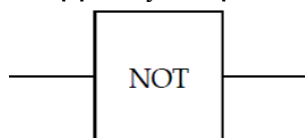
Σχήμα 6.4

6.4 ΚΒΑΝΤΙΚΗ ΠΥΛΗ NOT

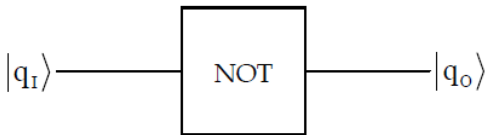
Η **κβαντική πύλη NOT** λειτουργεί όπως και η κλασσική πύλη NOT και δρα σε ένα qubit . Μετατρέπει την κατάσταση από 0 σε 1 και από 1 σε 0. Η κβαντική πύλη NOT περιγράφεται από τον πίνακα

$$\text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad 6.4$$

Σε δίκτυα η κβαντική πύλη NOT συμβολίζεται με



Ο συμβολισμός και ο πίνακας αληθείας που αποδίδει τις χαρακτηριστικές ιδιότητες της πύλης μετατόπισης φάσης φαίνεται στο επόμενο σχήμα.

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»	
 Πύλη NOT	Input ($ q_I\rangle$)	Output ($ q_O\rangle$)
	$ q_I\rangle = 0\rangle$	$ q_O\rangle = 1\rangle$
	$ q_I\rangle = 1\rangle$	$ q_O\rangle = 0\rangle$
	$ q_I\rangle = \alpha 0\rangle + \beta 1\rangle$	$ q_O\rangle = \alpha 1\rangle + \beta 0\rangle$

Σχήμα 6.5

■ Τα χαρακτηριστικά του πίνακα προκύπτουν εύκολα μετά από τις ανάλογες πράξεις. Πράγματι είναι

$$\begin{aligned}\text{NOT}|0\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |1\rangle \\ \text{NOT}|1\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |0\rangle \\ \text{NOT}(\alpha|0\rangle + \beta|1\rangle) &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = \beta|0\rangle + \alpha|1\rangle\end{aligned}$$

6.5 ΚΒΑΝΤΙΚΗ ΠΥΛΗ HADAMARD

Η **κβαντική πύλη Hadamard** δρα επίσης σε ένα μόνο qubit. Συμβολίζεται με H^3 και περιγράφεται από τον ακόλουθο πίνακα:

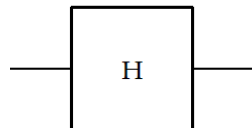
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad 6.5$$

Σημαντική ιδιότητα του πίνακα H είναι ότι ισχύει

$$H \cdot H^* = I$$

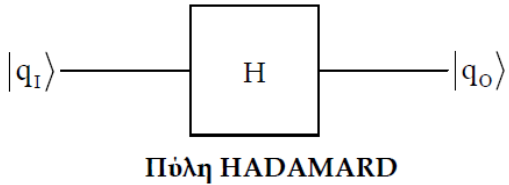
όπου I είναι ο μοναδιαίος πίνακας και H^* είναι ο συζυγής του πίνακα H .

Σε δίκτυα ο συμβολισμός της πύλης Hadamard είναι ο εξής:



Η πύλη Hadamard δρα σε qubits που βρίσκονται σε μία από τις δύο βασικές καταστάσεις και τα θέτει σε μία κατάσταση που είναι υπέρθεση των βασικών καταστάσεων. Επίσης όταν δρα σε qubits που βρίσκονται στην υπέρθεση καταστάσεων επιστρέφει τα qubits στις βασικές τους καταστάσεις. Ο συμβολισμός και ο πίνακας αληθείας που αποδίδει τις χαρακτηριστικές ιδιότητες της πύλης μετατόπισης φάσης φαίνεται στο επόμενο σχήμα.

³ Ο μετασχηματισμός του H , στη βιβλιογραφία αναφέρεται και ως Walsh-Hadamard.

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»	
	Input ($ q_I\rangle$)	Output ($ q_O\rangle$)
	$ q_I\rangle = 0\rangle$	$ q_O\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$
	$ q_I\rangle = 1\rangle$	$ q_O\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$
	$ q_I\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$	$ q_O\rangle = 0\rangle$
	$ q_I\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$	$ q_O\rangle = 1\rangle$

Σχήμα 6.6

■ Τα χαρακτηριστικά του πίνακα προκύπτουν εύκολα μετά από τις ανάλογες πράξεις. Πράγματι είναι

$$|q_I\rangle \cdot H = |1\rangle \cdot H = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) = |q_O\rangle$$

Ομοίως,

$$|q_I\rangle \cdot H = |0\rangle \cdot H = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \left(\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = |q_O\rangle$$

Επίσης

$$|q_I\rangle \cdot H = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \cdot H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle = |q_O\rangle$$

$$|q_I\rangle \cdot H = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \cdot H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle = |q_O\rangle$$

Ο μετασχηματισμός από την πύλη Hadamard χρησιμοποιείται σε πολλούς κβαντικούς αλγορίθμους και θα τον συναντήσουμε στην συνέχεια στο 8^ο κεφάλαιο στους κβαντικούς αλγόριθμους. Ο μετασχηματισμός H, επίσης πλεονεκτεί λόγω της ιδιότητας που φέρει στο να δημιουργεί ομοιόμορφη υπέρθεση των διανυσμάτων της υπολογιστικής βάσης πολλών qubits (n των αριθμό qubits). Μπορούμε να εκφράσουμε μια γενικότερη δράση του Hadamard ως τανυστικό γινόμενο των καταστάσεων

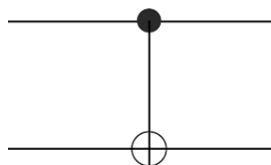
$$\begin{aligned}
 H^v |0 \dots 0\rangle &= H(|0\rangle \otimes |0\rangle \otimes \dots |0\rangle) = H|0\rangle \otimes H|0\rangle \otimes \dots H|0\rangle = \\
 &= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \cdot \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \dots \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}^v} \sum_0^{2^v-1} |i\rangle
 \end{aligned}$$

6.6 ΚΒΑΝΤΙΚΗ ΠΥΛΗ ΕΛΕΓΧΟΜΕΝΟΥ ΟΧΙ

Η **κβαντική πύλη ελεγχόμενου ΟΧΙ** δρα σε δύο qubit (εκ των οποίων το ένα καλείται ελέγχου -controlled- και το άλλο καλείται στόχος -target- και συμβολίζονται αντίστοιχα με c και t). Η κβαντική πύλη ελεγχόμενου ΟΧΙ συμβολίζεται με CNOT (Controlled NOT) και περιγράφεται από τον πίνακα

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad 6.6$$

Ο συμβολισμός της πύλης ελεγχόμενου ΟΧΙ σε δίκτυα, είναι ο εξής:



Η λειτουργία της πύλης CNOT είναι η εξής: όταν η κατάσταση του qubit c είναι 1, η πύλη αλλάζει την κατάσταση του qubit t , ενώ όταν η κατάσταση του qubit c είναι 0 η κατάσταση του qubit t μένει αναλλοίωτη.

Ο συμβολισμός και ο πίνακας αληθείας που αποδίδει τις χαρακτηριστικές ιδιότητες της πύλης μετατόπισης φάσης φαίνεται στο επόμενο σχήμα.

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»	
Πύλη Ελεγχόμενου ΟΧΙ	Input ($ c_I t_I\rangle$)	Output ($ c_o t_o\rangle$)
	$ c_I t_I\rangle = 00\rangle$	$ c_o t_o\rangle = 00\rangle$
	$ c_I t_I\rangle = 01\rangle$	$ c_o t_o\rangle = 01\rangle$
	$ c_I t_I\rangle = 10\rangle$	$ c_o t_o\rangle = 11\rangle$
	$ c_I t_I\rangle = 11\rangle$	$ c_o t_o\rangle = 10\rangle$

Σχήμα 6.7

■ Τα χαρακτηριστικά του πίνακα του προηγούμενου σχήματος προκύπτουν εύκολα μετά από τις ανάλογες πράξεις. Πράγματι

$$|00\rangle \cdot \text{CNOT} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

Επίσης

$$|01\rangle \cdot \text{CNOT} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle$$

Ομοίως

$$|10\rangle \cdot \text{CNOT} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle$$

και τέλος

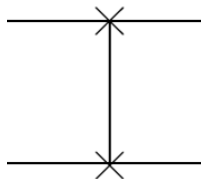
$$|11\rangle \cdot \text{CNOT} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

6.7 ΚΒΑΝΤΙΚΗ ΠΥΛΗ ΕΝΑΛΛΑΓΗΣ

Η κβαντική πύλη εναλλαγής καλείται **SWAP**. Περιγράφεται από τον πίνακα

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad 6.7$$

Ο συμβολισμός της πύλης για δίκτυα είναι ο εξής



Η κβαντική πύλη εναλλαγής δρα σε δύο qubits ένα ελέγχου που συμβολίζεται με c και ένα στόχου που συμβολίζεται με t . Η πύλη εναλλάσσει τα περιεχόμενα των καταστάσεων από 1 σε 0 και από 0 σε 1. Ο συμβολισμός και ο πίνακας αληθείας που αποδίδει τις χαρακτηριστικές ιδιότητες της πύλης μετατόπισης φάσης φαίνεται στο επόμενο σχήμα.

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»	
Πύλη Εναλλαγής	Input ($ c_I t_I\rangle$)	Output ($ c_o t_o\rangle$)
	$ c_I t_I\rangle = 00\rangle$	$ c_o t_o\rangle = 00\rangle$
	$ c_I, t_I\rangle = 01\rangle$	$ c_o t_o\rangle = 10\rangle$
	$ c_I, t_I\rangle = 10\rangle$	$ c_o t_o\rangle = 01\rangle$
	$ c_I, t_I\rangle = 11\rangle$	$ c_o t_o\rangle = 11\rangle$

Σχήμα 6.8

■ Τα χαρακτηριστικά του πίνακα του προηγούμενου σχήματος προκύπτουν εύκολα μετά από τις ανάλογες πράξεις. Πράγματι είναι

$$|00\rangle \cdot \text{SWAP} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

Επίσης

$$|01\rangle \cdot \text{SWAP} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

Ομοίως

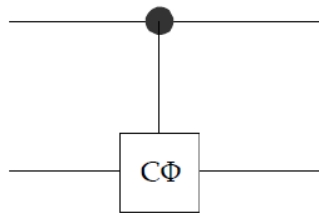
$$|10\rangle \cdot \text{SWAP} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle$$

και τέλος

$$|11\rangle \cdot \text{SWAP} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |11\rangle$$

6.8 ΚΒΑΝΤΙΚΗ ΠΥΛΗ ΕΛΕΓΧΟΜΕΝΗΣ ΜΕΤΑΤΟΠΙΣΗΣ ΦΑΣΗΣ

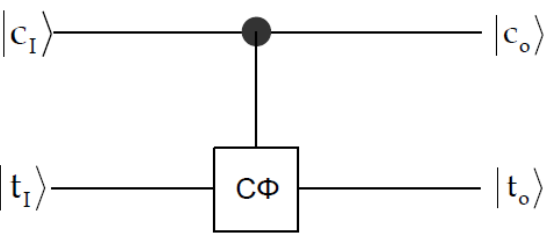
Η κβαντική πύλη ελεγχόμενης μετατόπισης φάσης συμβολίζεται με $C\Phi$ και δρα σε δύο qubits (εκ των οποίων το ένα καλείται ελέγχου -controlled- και το άλλο καλείται στόχος -target- και συμβολίζονται αντίστοιχα με c και t). Η κβαντική πύλη ελεγχόμενης μετατόπισης φάσης $C\Phi$ ή $C\Phi$ ή Φ ή F πολλαπλασιάζει την κατάσταση του qubit στόχου με τον παράγοντα φάσης $e^{i\varphi}$ μόνο όταν η κατάσταση του qubit c και t είναι $|11\rangle$, ενώ οι άλλες κβαντικές καταστάσεις των qubits ελέγχου και στόχου παραμένουν οι ίδιες. Ο συμβολισμός της κβαντικής πύλης ελεγχόμενης μετατόπισης φάσης για δίκτυα, δίνεται από την μορφή



Η κβαντική πύλη ελεγχόμενης μετατόπισης φάσης περιγράφεται από τον ακόλουθο πίνακα:

$$C\Phi = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{bmatrix} \quad 6.8$$

Ο συμβολισμός και ο πίνακας αληθείας που αποδίδει τις χαρακτηριστικές ιδιότητες της πύλης ελεγχόμενης μετατόπισης φάσης φαίνεται στο επόμενο σχήμα.

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»	
 Πύλη Ελεγχόμενης Μετατόπισης Φάσης	Input ($ c_I t_I\rangle$)	Output ($ c_o t_o\rangle$)
	$ c_I t_I\rangle = 00\rangle$	$ c_o t_o\rangle = 00\rangle$
	$ c_I t_I\rangle = 01\rangle$	$ c_o t_o\rangle = 01\rangle$
	$ c_I t_I\rangle = 10\rangle$	$ c_o t_o\rangle = 10\rangle$
	$ c_I t_I\rangle = 11\rangle$	$ c_o t_o\rangle = e^{i\varphi} 11\rangle$

Σχήμα 6.9

■ Τα χαρακτηριστικά του πίνακα του προηγούμενου σχήματος προκύπτουν εύκολα μετά από τις ανάλογες πράξεις. Πράγματι είναι

$$|00\rangle \cdot C\Phi = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |00\rangle$$

Επίσης

$$|01\rangle \cdot C\Phi = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle$$

Ομοίως

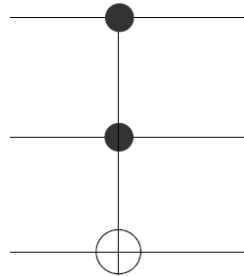
$$|10\rangle \cdot C\Phi = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |10\rangle$$

και τέλος

$$|11\rangle \cdot C\Phi = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ e^{i\varphi} \end{bmatrix} = e^{i\varphi} |11\rangle$$

6.9 ΚΒΑΝΤΙΚΗ ΠΥΛΗ ΔΙΠΛΑ ΕΛΕΓΧΟΜΕΝΟΥ ΟΧΙ Ή TOFFOLI GATE

Η κβαντική πύλη διπλά ελεγχόμενου ΟΧΙ ή πύλη Toffoli δρα σε τρία qubits. Το σύμβολό της είναι CCNOT⁴. Τα δύο qubits ονομάζονται qubits ελέγχου και συμβολίζονται αντίστοιχα με c_1 και c_2 , ενώ το άλλο qubit καλείται στόχος και συμβολίζεται με t . Η πύλη CCNOT αλλάζει την κατάσταση του qubit στόχου, όταν και τα δύο qubits ελέγχου βρίσκονται στην κατάσταση 1. Δεν αλλάζει την κατάσταση του qubit στόχου σε κάθε άλλη περίπτωση. Ο συμβολισμός της κβαντικής πύλης διπλά ελεγχόμενου ΟΧΙ για δίκτυα, δίνεται από την μορφή

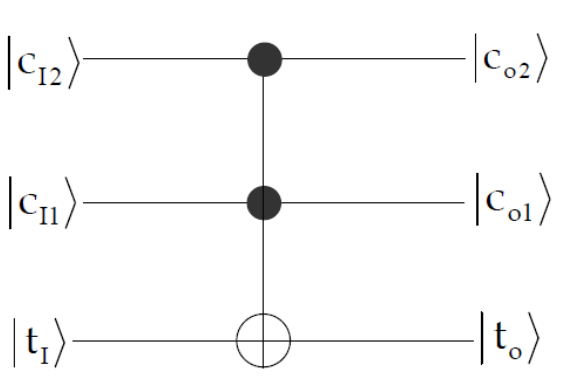


Η κβαντική πύλη διπλά ελεγχόμενου ΟΧΙ δίνεται από τον πίνακα:

$$CCNOT = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \quad 6.9$$

⁴ Η κβαντική πύλη διπλά ελεγχόμενου ΟΧΙ συνηθίζεται να καλείται CCNOT σε σχέση με την ονομασία πύλης Toffoli.

Ο συμβολισμός και ο πίνακας αληθείας που αποδίδει τις χαρακτηριστικές ιδιότητες της πύλης μετατόπισης φάσης φαίνεται στο επόμενο σχήμα.

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»	
 Πύλη Διπλά Ελεγχόμενου ΟΧΙ	Input ($ c_{I2} c_{I1} t_I\rangle$)	Output ($ c_{o2} c_{o1} t_o\rangle$)
	$ c_{I2} c_{I1} t_I\rangle = 000\rangle$	$ c_{o2} c_{o1} t_o\rangle = 000\rangle$
	$ c_{I2} c_{I1} t_I\rangle = 001\rangle$	$ c_{o2} c_{o1} t_o\rangle = 001\rangle$
	$ c_{I2} c_{I1} t_I\rangle = 010\rangle$	$ c_{o2} c_{o1} t_o\rangle = 010\rangle$
	$ c_{I2} c_{I1} t_I\rangle = 011\rangle$	$ c_{o2} c_{o1} t_o\rangle = 011\rangle$
	$ c_{I2} c_{I1} t_I\rangle = 100\rangle$	$ c_{o2} c_{o1} t_o\rangle = 100\rangle$
	$ c_{I2} c_{I1} t_I\rangle = 101\rangle$	$ c_{o2} c_{o1} t_o\rangle = 101\rangle$
	$ c_{I2} c_{I1} t_I\rangle = 110\rangle$	$ c_{o2} c_{o1} t_o\rangle = 111\rangle$
	$ c_{I2} c_{I1} t_I\rangle = 111\rangle$	$ c_{o2} c_{o1} t_o\rangle = 110\rangle$

Σχήμα 6.10

■ Τα χαρακτηριστικά του πίνακα του προηγούμενου σχήματος προκύπτουν εύκολα μετά από τις ανάλογες πράξεις. Πράγματι είναι

$$|000\rangle \cdot \text{CCNOT} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |000\rangle$$

Ομοίως για τις καταστάσεις $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, η δράση της CCNOT δεν τις επηρεάζει και μετά τις πράξεις τις αφήνει αναλλοίωτες κάτι που δεν συμβαίνει για τις επόμενες δύο καταστάσεις $|110\rangle$ και $|111\rangle$ καθώς μετά τις πράξεις προκύπτει ότι

$$|110\rangle \cdot \text{CCNOT} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |111\rangle$$

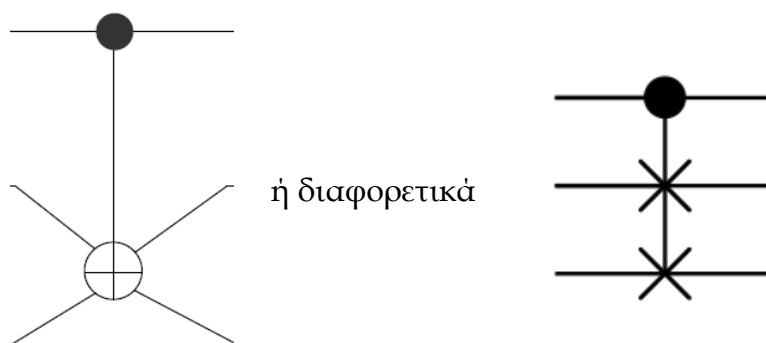
$$|111\rangle \cdot \text{CCNOT} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |110\rangle$$

6.10 ΚΒΑΝΤΙΚΗ ΠΥΛΗ FREDKIN Ή ΠΥΛΗ ΕΛΕΓΧΟΜΕΝΗΣ ΕΝΑΛΛΑΓΗΣ

Η **κβαντική πύλη Fredkin**⁵ ή πύλη ελεγχόμενης εναλλαγής δρα σε τρία qubit. Ο συμβολισμός της είναι το **F**. Το ένα από τα τρία qubit ονομάζεται qubit ελέγχου (c) και τα άλλα δύο ονομάζονται qubits στόχοι (t₁ και t₂). Η πύλη F εναλλάσσει τις καταστάσεις των qubits στόχων, όταν το qubit ελέγχου βρίσκεται στην κατάσταση 1, ενώ όταν το qubit ελέγχου βρίσκονται στην κατάσταση 0 οι καταστάσεις των qubits στόχων δεν αλλάζουν. Η κατάσταση του qubit ελέγχου c_i δε μεταβάλλεται, δηλαδή ισχύει πάντα c_i=c₀. Η κβαντική πύλη Fredkin μπορεί να χρησιμοποιηθεί για προσομοίωση κλασσικών ψηφιακών πυλών (NOT και AND). Ο συμβολισμός⁶ για δίκτυα της πύλης Fredkin είναι ο εξής:

⁵ Επικρατεί συνήθως η ονομασία κβαντική πύλη Fredkin.

⁶ Η πύλη Fredkin, στην βιβλιογραφία χρησιμοποιείται κυρίως με τον πρώτο (εκ των δύο), σχεδιαστικό συμβολισμό για κυκλωματικά δίκτυα.



Η κβαντική πύλη Fredkin περιγράφεται από τον ακόλουθο πίνακα:

$$F = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad 6.10$$

Ο συμβολισμός και ο πίνακας αληθείας που αποδίδει τις χαρακτηριστικές ιδιότητες της πύλης μετατόπισης φάσης φαίνεται στο επόμενο σχήμα 6.11.

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»	
Πύλη FREDKIN	Input ($ c_I t_{2I} t_{1I}\rangle$)	Output ($ c_o t_{o2} t_{o1}\rangle$)
	$ c_I t_{2I} t_{1I}\rangle = 000\rangle$	$ c_o t_{o2} t_{o1}\rangle = 000\rangle$
	$ c_I t_{2I} t_{1I}\rangle = 001\rangle$	$ c_o t_{o2} t_{o1}\rangle = 001\rangle$
	$ c_I t_{2I} t_{1I}\rangle = 010\rangle$	$ c_o t_{o2} t_{o1}\rangle = 010\rangle$
	$ c_I t_{2I} t_{1I}\rangle = 011\rangle$	$ c_o t_{o2} t_{o1}\rangle = 011\rangle$
	$ c_I t_{2I} t_{1I}\rangle = 100\rangle$	$ c_o t_{o2} t_{o1}\rangle = 100\rangle$
	$ c_I t_{2I} t_{1I}\rangle = 101\rangle$	$ c_o t_{o2} t_{o1}\rangle = 110\rangle$
	$ c_I t_{2I} t_{1I}\rangle = 110\rangle$	$ c_o t_{o2} t_{o1}\rangle = 101\rangle$
	$ c_I t_{2I} t_{1I}\rangle = 111\rangle$	$ c_o t_{o2} t_{o1}\rangle = 111\rangle$

Σχήμα 6.11

■ Τα χαρακτηριστικά του πίνακα του προηγούμενου σχήματος προκύπτουν εύκολα μετά από τις ανάλογες πράξεις. Πράγματι είναι

$$|000\rangle \cdot F = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = |000\rangle$$

Ομοίως για τις καταστάσεις $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, και $|111\rangle$ η δράση της F δεν τις επηρεάζει και μετά τις πράξεις τις αφήνει αναλλοίωτες κάτι που δεν συμβαίνει για τις επόμενες δύο καταστάσεις $|110\rangle$ και $|101\rangle$ καθώς μετά τις πράξεις προκύπτει ότι

$$|101\rangle \cdot F = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = |110\rangle$$

και τέλος

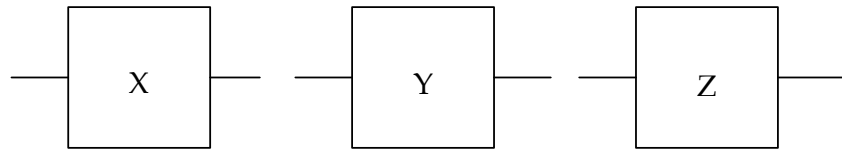
$$|110\rangle \cdot F = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = |101\rangle$$

6.11 ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ ΚΑΙ ΠΙΝΑΚΕΣ PAULI

Σύμφωνα με όσα ειπώθηκαν στο Α' μέρος, § 2.20, οι πίνακες του Pauli είναι πίνακες 2x2 και δίνονται από τις

$$X = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \text{ και} \quad Z = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Σε δίκτυα ο συμβολισμός των πυλών Pauli για κάθε μία εκ των X , Y , Z είναι αντίστοιχα:



Σχήμα 6.12

Επίσης μπορούμε μέσω των πινάκων Pauli να εκφράσουμε και επιπλέον κβαντικές πύλες. Πράγματι

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

Όμως η κβαντική πύλη Hadamard είναι η

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

οπότε συμπεραίνουμε ότι

$$H = \frac{1}{\sqrt{2}} (X + Z)$$

Επίσης και η πύλη NOT μπορεί να εκφραστεί με βάση τους πίνακες του Pauli.

Πράγματι η πύλη NOT δίνεται από τον πίνακα

$$\text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

ή διαφορετικά ισοδύναμα η NOT είναι η πύλη X , ώστε

$$\text{NOT} = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

ΚΕΦΑΛΑΙΟ 7^ο

ΚΒΑΝΤΙΚΑ ΚΥΚΛΩΜΑΤΑ

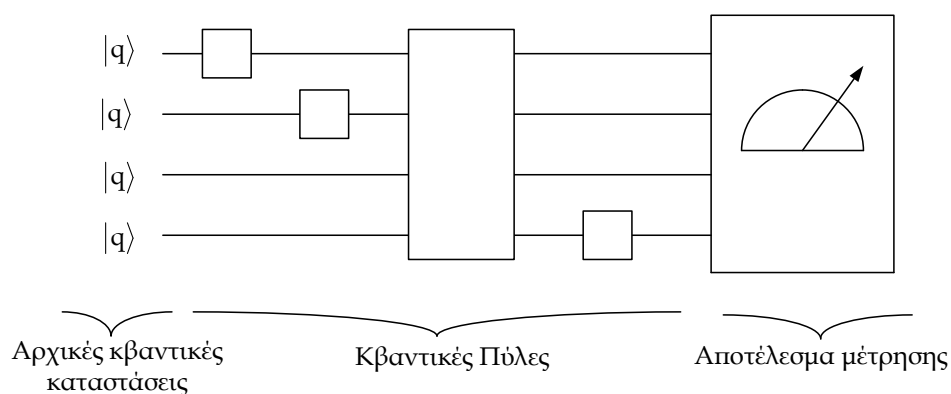
7.1 ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ

Οι βασικές αρχές λειτουργίας των κβαντικών υπολογιστών με όσα μελετήθηκαν μέχρι τώρα μπορούν να οριοθετηθούν στις εξής επιγραμματικές αναφορές: Στους κβαντικούς υπολογιστές η πληροφορία βρίσκεται αποθηκευμένη σε κβαντικούς καταχωρητές ή σε qubits. Οι καταστάσεις των κβαντικών καταχωρητών και των qubits είναι διανύσματα στον χώρο Hilbert. Επίσης οι κβαντικές πύλες είναι τελεστές (ορθομοναδιαίοι πίνακες) που δρουν πάνω σε κβαντικούς καταχωρητές και σε qubits περιστρέφοντας ουσιαστικά την κατάσταση των διανυσμάτων ώστε να αλλάζουν την κατάστασή τους. Στους κβαντικούς υπολογιστές δεν μπορούμε να αντιγράψουμε την κατάσταση ενός qubit, δηλαδή δεν έχει βρεθεί (ακόμα τουλάχιστον) μια πύλη που να αντιγράφει την κατάσταση του qubit.

Κάθε κβαντικό κύκλωμα, είναι ουσιαστικά κβαντικοί υπολογισμοί και αποτελούνται από qubits, κβαντικούς καταχωρητές και φυσικά κβαντικές πύλες. Βασική αρχή στα κβαντικά κυκλώματα είναι ότι δεν μεταφέρεται η πληροφορία από μια κβαντική πύλη σε κάποια άλλη (όπως στους κλασσικούς υπολογιστές) αλλά η πληροφορία παραμένει στους κβαντικούς καταχωρητές και στα qubits. Ο σχεδιασμός των κβαντικών κυκλωμάτων γίνεται με τους γνωστούς συμβολισμούς των κβαντικών πυλών που είδαμε στο προηγούμενο κεφάλαιο και δείχνει την σειρά με την οποία δρουν οι κβαντικές πύλες στις κβαντικές καταστάσεις. Επίσης σε αντίθεση με τα κυκλώματα των κλασσικών ηλεκτρονικών διατάξεων, στα κβαντικά κυκλώματα δεν έχουμε διακλαδώσεις και βρόγχους. Το αποτέλεσμα ενός κβαντικού υπολογισμού που προκύπτει από το υπό περίπτωση μελέτης κβαντικό κύκλωμα θα είναι η τελική κατάσταση του κβαντικού καταχωρητή [1, 4, 5, 7, 8].

Για την μελέτη κβαντικών υπολογισμών μέσω qubits καταχωρητών και πυλών, υπάρχουν στην βιβλιογραφία δύο κύρια μοντέλα, το κυκλωματικό μοντέλο – Quantum circuit model- (αυτό που θα αναπτυχθεί στο συγκεκριμένο κεφάλαιο και έχει ως κύρια αρχή την διαδοχική δράση κβαντικών πυλών σε καταχωρητές όπου είναι αποθηκευμένη η πληροφορία και με την δυνατότητα που παρέχει με το να μπορεί κάθε πύλη να αναλυθεί σε οποιοδήποτε σύνολο από πύλες -εξ' ου και η ονομασία καθολικές πύλες-) και το μοντέλο της κβαντικής μηχανής Turing [8] (Quantum turing model).

Στο επόμενο σχήμα απεικονίζεται ένα τυχαίο κβαντικό κύκλωμα που αποτελείται από κβαντικές πύλες συνδεδεμένες μεταξύ τους με ορθή διάταξη χωρίς ανάδραση και συνδέονται με κβαντικά σύρματα δηλαδή με αυτό που είναι ο δρόμος των qubit, τα οποία περιγράφουν τις κβαντικές καταστάσεις των διανυσμάτων $|q\rangle$ στον χώρο του Hilbert.



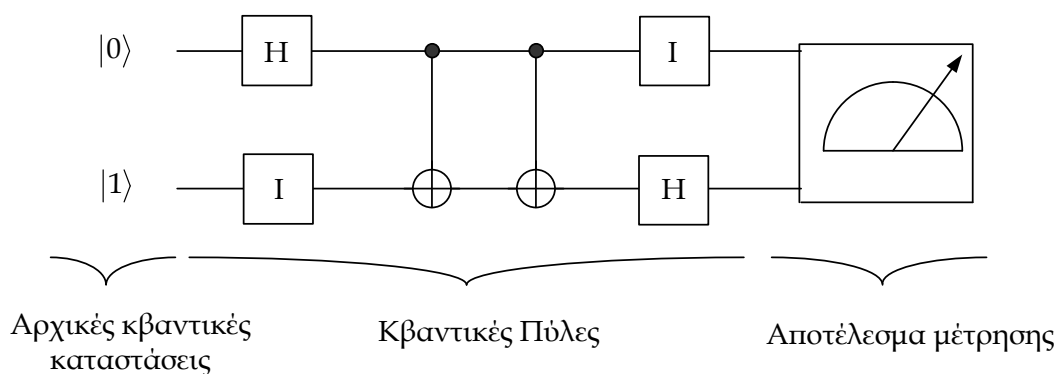
Σχήμα 7.1

7.2 ΚΒΑΝΤΙΚΑ ΚΥΚΛΩΜΑΤΑ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΔΙΑΔΙΚΑΣΙΑ

Κάθε κβαντικό κύκλωμα υπόκειται σε δράσεις υπολογισμού μεταξύ των πυλών που δρουν στις καταστάσεις των qubits προκειμένου μετά από την υπολογιστική διαδικασία να προκύψει το αποτέλεσμα την πιθανότητας να βρεθεί ο κβαντικός καταχωρητής σε μια κβαντική κατάσταση. Αυτό στηρίζεται σε μια δράση επιμέρους βημάτων των κβαντικών πυλών που καθορίζεται από την δομή του κβαντικού κυκλώματος. Θα εξετάσουμε στην συνέχεια την υπολογιστική διαδικασία κάποιων χαρακτηριστικών κβαντικών κυκλωμάτων. Σε κυκλώματα ιδιαίτερης πολυπλοκότητας έχουν αναπτυχθεί και σχεδιαστεί ερευνητικά προσομοιωτές που εκτελούν ένα αρκετά μεγάλο αριθμό κβαντικών πράξεων σε μικρό χρονικό διάστημα.

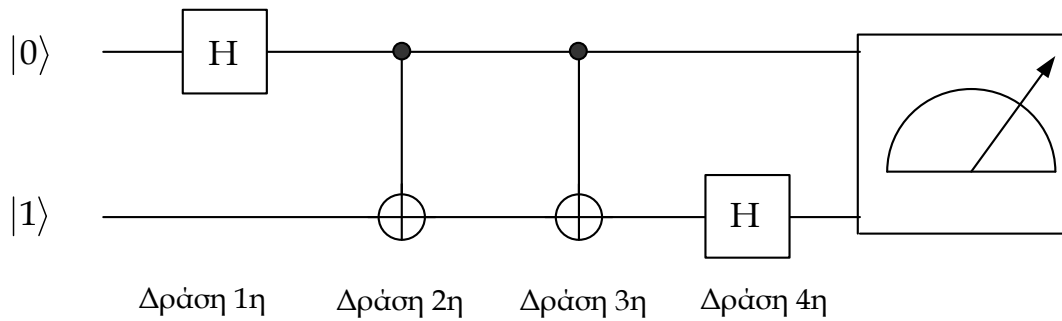
■ Παράδειγμα Υπολογισμού Κβαντικού Κυκλώματος

Δίνεται το επόμενο κβαντικό κύκλωμα του σχήματος 7.2 το οποίο θα επεξεργαστούμε δράση-δράση μεταξύ των πυλών προκειμένου να υπολογίσουμε το αποτέλεσμα της κατάστασης.



Σχήμα 7.2

Το κύκλωμα περιλαμβάνει τις πύλες: Hadamard, αδρανείας και CNOT. Η πύλη αδρανείας επειδή δεν αλλάζει με την δράση της την κβαντική κατάσταση μπορούμε να την παραλείψουμε και να φαίνεται στο σχήμα η συνεχόμενη γραμμή του κβαντικού σύρματος. Επομένως μπορούμε ισοδύναμα να γράψουμε το κύκλωμα του προηγούμενου σχήματος 7.2, απλοποιημένο με την μορφή του επόμενου:



Σχήμα 7.3

Ο κβαντικός υπολογισμός του κβαντικού κυκλώματος, θα προκύψει από τα βήματα όλων των δράσεων. Κατ' αρχήν ο κβαντικός καταχωρητής του κυκλώματος αποτελείται από δύο qubits και η κατάσταση του είναι η $|q\rangle$, δηλαδή η

$$|01\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

ή διαφορετικά

$$|01\rangle = 0|00\rangle + |01\rangle + 0|10\rangle + 0|11\rangle$$

(κάτι που προφανώς υποδηλώνει ότι η πιθανότητα να μετρήσουμε την κατάσταση $|01\rangle$, είναι 1).

Στην συνέχεια το βήμα της 1^{ης} δράσης θα δώσει το τανυστικό γινόμενο των πινάκων των πυλών $H \otimes I$ πάνω στην κατάσταση $|01\rangle$. Οπότε προκύπτει

$$(H \otimes I)|01\rangle = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

ή διαφορετικά

$$(H \otimes I)|01\rangle = 0|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + 0|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Στην συνέχεια στο βήμα της 2^{ης} δράσης, στην $(H \otimes I)|01\rangle$ δρά η πύλη CNOT ώστε

$$\text{CNOT} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Ομοίως στο επόμενο βήμα της 3^{ης} δράσης μια πύλη CNOT δρα στην $\frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$ οπότε

προκύπτει ότι

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 0|00\rangle + \frac{1}{\sqrt{2}}|01\rangle + 0|10\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

(κάτι που προφανώς υποδηλώνει ότι η πιθανότητα να μετρήσουμε την κατάσταση $|01\rangle$, είναι 0,5 και την κατάσταση $|11\rangle$ είναι επίσης 0,5).

Τέλος στο επόμενο βήμα της 4^{ης} δράσης, με την πύλη αδρανείας και Hadamard $I \otimes H$

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

η οποία θα δράση στην $\frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$ θα έχει ως αποτέλεσμα να προκύψει ότι

$$(I \otimes H) \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}$$

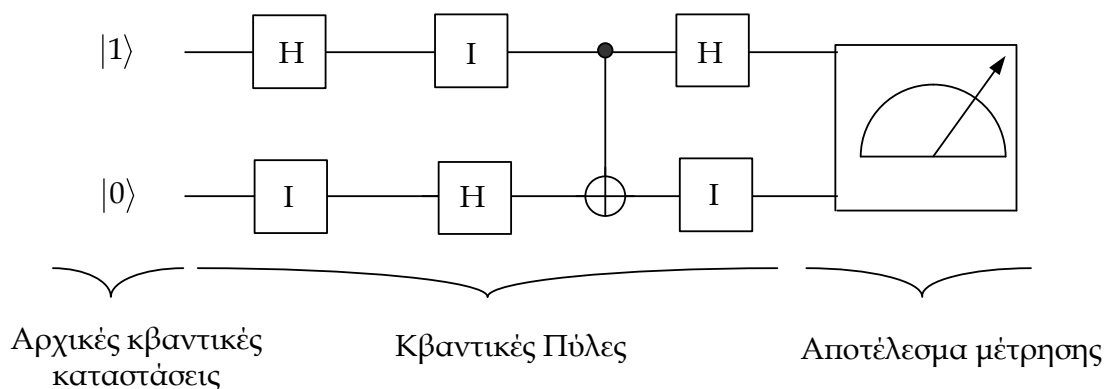
ή διαφορετικά

$$(I \otimes H) \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{2} |00\rangle - \frac{1}{2} |01\rangle + \frac{1}{2} |10\rangle - \frac{1}{2} |11\rangle$$

Επομένως το κβαντικό αποτέλεσμα του υπολογισμού του κβαντικού κυκλώματος του σχήματος 7.2, θα δώσει πιθανότητα να βρεθεί ο κβαντικός καταχωρητής σε όλες τις καταστάσεις $|00\rangle |01\rangle |10\rangle |11\rangle$, ίση με 0,25 ή 25% για κάθε μια από αυτές.

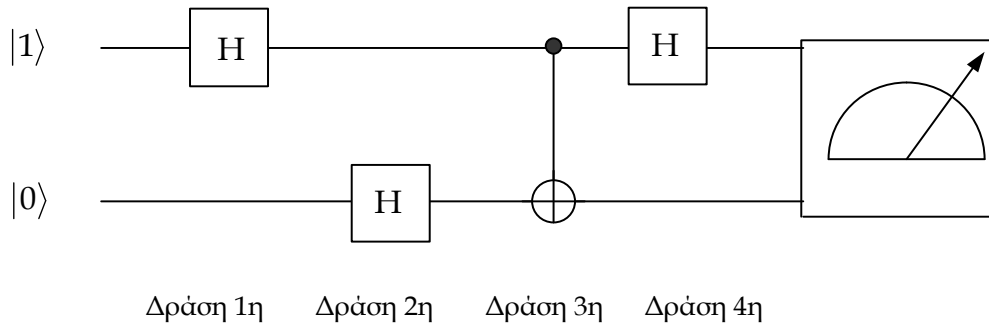
■ Παράδειγμα Υπολογισμού Κβαντικού Κυκλώματος

Δίνεται το επόμενο κβαντικό κύκλωμα του σχήματος 7.4 το οποίο θα επεξεργαστούμε δράση-δράση μεταξύ των πυλών προκειμένου να υπολογίσουμε το αποτέλεσμα της κατάστασης.



Σχήμα 7.4

Το κύκλωμα περιλαμβάνει τις πύλες: Hadamard, αδρανείας και CNOT. Η πύλη αδρανείας επειδή δεν αλλάζει με την δράση της την κβαντική κατάσταση μπορούμε να την παραλείψουμε και να φαίνεται στο σχήμα η συνεχόμενη γραμμή του κβαντικού σύρματος. Επομένως μπορούμε ισοδύναμα να γράψουμε το κύκλωμα του προηγούμενου σχήματος 7.4, με την μορφή του επόμενου:



Σχήμα 7.5

Ο κβαντικός υπολογισμός του κβαντικού κυκλώματος, θα προκύψει από τα βήματα όλων των δράσεων. Κατ' αρχήν ο κβαντικός καταχωρητής του κυκλώματος αποτελείται από δύο qubits και η κατάσταση του είναι η $|q\rangle$, δηλαδή η

$$|10\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad \text{ή} \quad |10\rangle = 0|00\rangle + 0|01\rangle + 1|10\rangle + 0|11\rangle$$

Στην συνέχεια το βήμα της 1ης δράσης θα δώσει το τανυστικό γινόμενο των πινάκων των πυλών $H \otimes I$ πάνω στην δράση $|01\rangle$. Οπότε προκύπτει

$$(H \otimes I)|10\rangle = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix}$$

ή διαφορετικά

$$(H \otimes I)|10\rangle = \frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle - \frac{1}{\sqrt{2}}|10\rangle + 0|11\rangle$$

Στην συνέχεια στο βήμα της 2ης δράσης στην $(H \otimes I)|01\rangle$ δρά μια νέα πύλη αδράνειας με δράση Hadamard $I \otimes H$, όπου θα είναι

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

οπότε ισοδύναμα θα γίνει

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix} = \frac{1}{2} \cdot \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}$$

Ομοίως στο επόμενο βήμα της 3ης δράσης, μια πύλη CNOT δρα στην $\frac{1}{2} \cdot \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}$ οπότε

προκύπτει

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

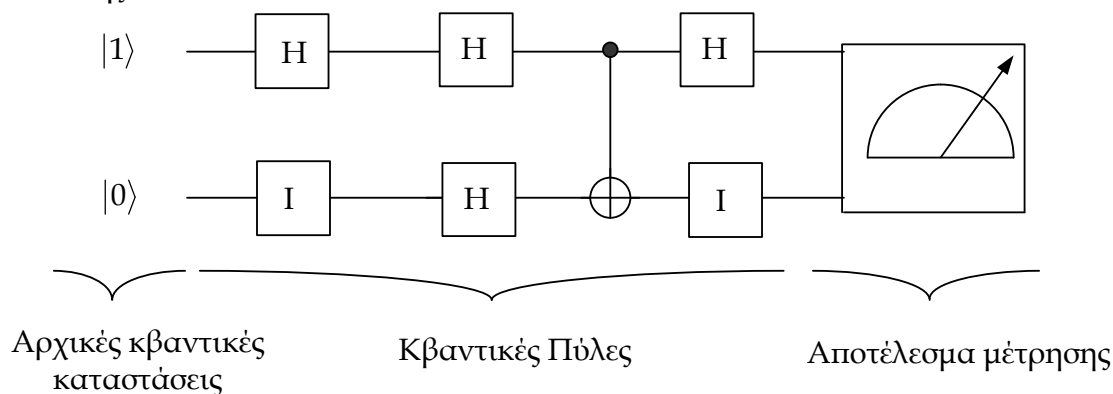
Τέλος το επόμενο βήμα της 4ης δράσης θα δώσει υπό την δράση της πύλης Hadamard και αδρανείας $H \otimes I$, ότι

$$\begin{aligned} (H \otimes I) \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} &= \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ 2 \\ 2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \\ &= 0|00\rangle + 0|01\rangle + \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle \end{aligned}$$

Επομένως το κβαντικό αποτέλεσμα του υπολογισμού του κβαντικού κυκλώματος του σχήματος 7.5, θα δώσει πιθανότητα να βρεθεί ο κβαντικός καταχωρητής στην κατάσταση $|10\rangle$ και $|11\rangle$ ίση με 0,5 ή 50% για κάθε μια περίπτωση αντίστοιχα.

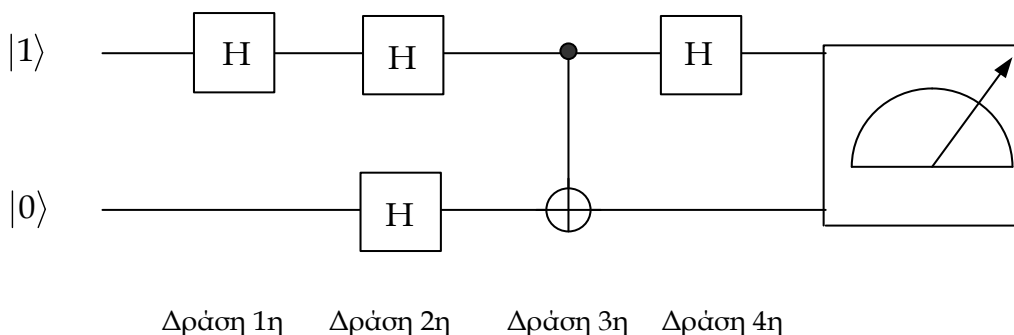
■ Παράδειγμα Υπολογισμού Κβαντικού Κυκλώματος

Δίνεται το επόμενο κβαντικό κύκλωμα του σχήματος 7.6 το οποίο θα επεξεργαστούμε δράση-δράση μεταξύ των πυλών προκειμένου να υπολογίσουμε το αποτέλεσμα της κατάστασης.



Σχήμα 7.6

Το κύκλωμα περιλαμβάνει τις πύλες: Hadamard, αδρανείας και CNOT. Η πύλη αδρανείας επειδή δεν αλλάζει με την δράση της την κβαντική κατάσταση μπορούμε να την παραλείψουμε και να φαίνεται στο σχήμα η συνεχόμενη γραμμή του κβαντικού σύρματος. Επομένως μπορούμε ισοδύναμα να γράψουμε το κύκλωμα του προηγούμενου σχήματος 7.6, με την μορφή του επόμενου:



Σχήμα 7.7

Ο κβαντικός υπολογισμός του κβαντικού κυκλώματος, θα προκύψει από τα βήματα όλων των δράσεων. Κατ' αρχήν ο κβαντικός καταχωρητής του κυκλώματος αποτελείται από δύο qubits και η κατάσταση του είναι η $|q\rangle$, δηλαδή η

$$|10\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \quad \text{ή} \quad |10\rangle = 0|00\rangle + 0|01\rangle + 1|10\rangle + 0|11\rangle$$

Στην συνέχεια το βήμα της 1ης δράσης θα δώσει το τανυστικό γινόμενο των πινάκων των πυλών $H \otimes I$ πάνω στην δράση $|01\rangle$. Οπότε προκύπτει

$$(H \otimes I)|10\rangle = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix}$$

ή διαφορετικά

$$(H \otimes I)|10\rangle = \frac{1}{\sqrt{2}}|00\rangle + 0|01\rangle - \frac{1}{\sqrt{2}}|10\rangle + 0|11\rangle$$

Στην συνέχεια στο βήμα της 2ης δράσης στην $(H \otimes I)|01\rangle$ δρα η πύλη Hadamard $H \otimes H$ ώστε

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

Επομένως θα προκύψει

$$(H \otimes H) \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix} = \frac{1}{2\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ 2 \\ 2 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

Ομοίως στο επόμενο βήμα της 3ης δράσης μια πύλη CNOT δρα στην $\frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$ οπότε

προκύπτει ότι

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Τέλος το επόμενο βήμα της 4^{ης} δράσης θα δώσει υπό την δράση του τανυστικού

γινομένου $H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$, ότι

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 0 \\ 2 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = |01\rangle$$

Επομένως το κβαντικό αποτέλεσμα του υπολογισμού του κβαντικού κυκλώματος του σχήματος 7.7, θα δώσει πιθανότητα να βρεθεί ο κβαντικός καταχωρητής στην κατάσταση $|01\rangle$ ίση με 1.

7.3 ΚΒΑΝΤΙΚΟ ΚΥΚΛΩΜΑ ΚΒΑΝΤΙΚΗΣ ΔΙΕΜΠΛΟΚΗΣ

Σύμφωνα με όσα ειπώθηκαν (§ 3.6 και § 4.4) σε **κβαντική διεμπλοκή** είναι δύο κβαντικά συστήματα των οποίων η κατάσταση δεν μπορεί να γραφεί ως τανυστικό γινόμενο των βασικών τους καταστάσεων.

Μια γενική κβαντική κατάσταση n qubits, η

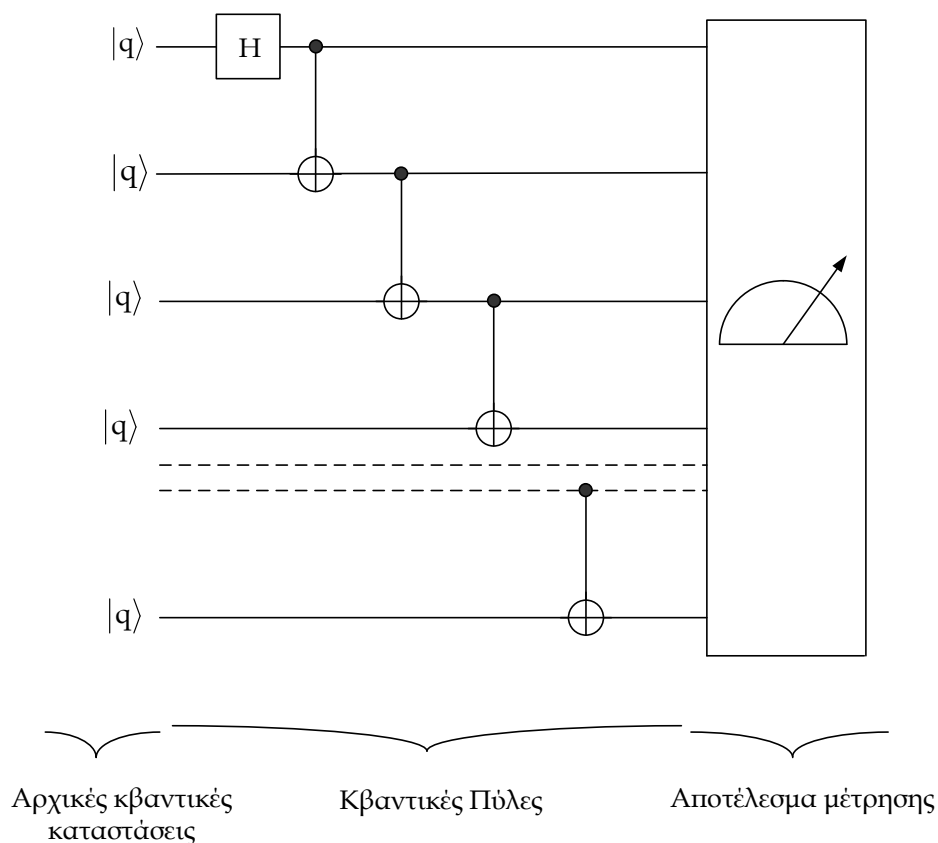
$$\alpha_0 |000000\rangle + \alpha_1 |000001\rangle + \dots + \alpha_{2^n-1} |111111\rangle$$

μπορεί να αναλυθεί σε μεμονωμένα bits ανάλογα με την κρατούσα κατάσταση όπως π.χ. στην

$$\frac{1}{2} (|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle).$$

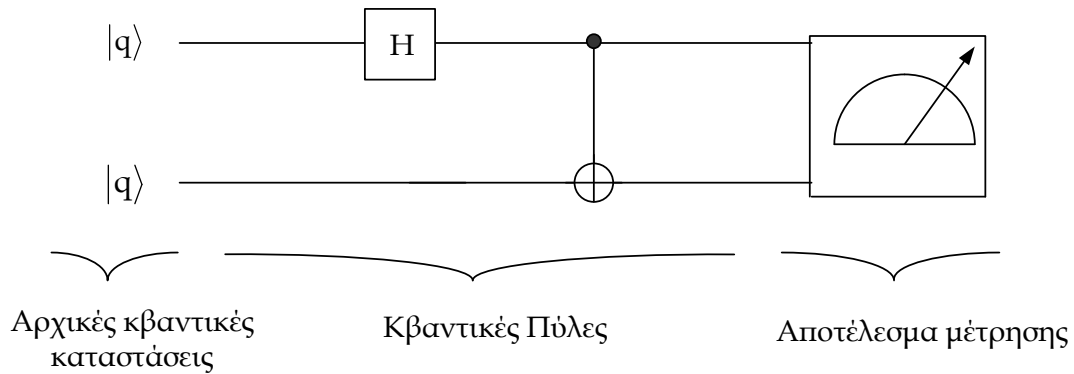
Συγκρίνοντας δύο καταστάσεις τις $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ και $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ παρατηρούμε σημαντικές διαφορές. Συγκεκριμένα για την μέτρηση της πρώτης κατάστασης $\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ παρατηρούμε πως η πιθανότητα να βρούμε $|0\rangle$ είναι 1 (100%) και η κατάσταση παραμένει αμετάβλητη. Στη δεύτερη περίπτωση της κβαντικής κατάστασης $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, η πιθανότητα να πάρουμε $|0\rangle$ ή $|1\rangle$ είναι η ίδια με αποτέλεσμα η πιθανότητα του πρώτου να καθορίζει και του δεύτερου. Αυτό ακριβώς χαρακτηρίζει την κβαντική διεμπλοκή [1, 40]. Επομένως δύο qubits όταν βρίσκονται σε κβαντική διεμπλοκή, τότε η μέτρηση της κατάστασης του ενός θα επηρεάζει και την κατάσταση του άλλου.

Το κβαντικό κύκλωμα κβαντικής διεμπλοκής αποτελείται από κβαντικές πύλες CNOT και την πύλη Hadamard. Για n qubits το κβαντικό κύκλωμα της κβαντικής διεμπλοκής είναι το ακόλουθο του σχήματος 7.8:



Σχήμα 7.8

Το κβαντικό κύκλωμα του σχήματος 7.8 αφορά n qubits. Για δύο qubits το κβαντικό κύκλωμα που αποδίδει την κβαντική διεμπλοκή περιλαμβάνει μια πύλη Hadamard και μια CNOT σύμφωνα με το επόμενο σχήμα 7.9 :



Σχήμα 7.9

Στην συνέχεια θα υπολογίσουμε τις δράσεις των κβαντικών πυλών που περιλαμβάνονται στο κβαντικό κύκλωμα της κβαντικής διεμπλοκής, πάνω στις αρχικές καταστάσεις $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

■ Το κύκλωμα του σχήματος 7.9, για την αρχική κατάσταση $|00\rangle$ με την επίδραση του τανυστικού γινομένου $H \otimes I$ και με βάση την μελέτη της προηγούμενης παραγράφου, θα δώσει τα εξής:

$$(H \otimes I)|00\rangle = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$$

Επομένως με την δράση της CNOT στην $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix}$ θα προκύψει ότι

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} (|00\rangle + 0|01\rangle + 0|10\rangle + |11\rangle) = \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle)$$

Παρατηρούμε για την κατάσταση $|00\rangle$, από το αποτέλεσμα μετά την δράση των πυλών του κυκλώματος πως δημιουργείται μια κατάσταση κβαντικής διεμπλοκής η $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

■ Με τον ίδιο τρόπο για την αρχική κατάσταση $|01\rangle$ του σχήματος 7.9, με την επίδραση του τανυστικού γινομένου $H \otimes I$ και της δράσης της CNOT θα έχουμε ότι:

$$(H \otimes I)|01\rangle = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$$

Επομένως με την δράση της CNOT στην $\frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$ θα προκύψει ότι

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}} (|01\rangle + |10\rangle)$$

Παρατηρούμε για την κατάσταση $|01\rangle$, από το αποτέλεσμα μετά την δράση των πυλών του κυκλώματος πως δημιουργείται μια κατάσταση κβαντικής διεμπλοκής η $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$.

■ Επίσης για την αρχική κατάσταση $|10\rangle$ του σχήματος 7.9, με την επίδραση του τανυστικού γινομένου $H \otimes I$ και της δράσης της CNOT θα έχουμε ότι:

$$(H \otimes I)|10\rangle = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix}$$

Επομένως με την δράση της CNOT στην $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix}$ θα προκύψει ότι

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ -1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} (|00\rangle + 0|01\rangle + 0|10\rangle - |11\rangle) = \frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$$

Παρατηρούμε για την κατάσταση $|01\rangle$, από το αποτέλεσμα μετά την δράση των πυλών του κυκλώματος, πως δημιουργείται μια κατάσταση κβαντικής διεμπλοκής η $\frac{1}{\sqrt{2}} (|00\rangle - |11\rangle)$.

■ Τέλος για την αρχική κατάσταση $|11\rangle$ του σχήματος 7.9, με την επίδραση του τανυστικού γινομένου $H \otimes I$ και της δράσης της CNOT θα έχουμε ότι:

$$(H \otimes I)|11\rangle = \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ -1 \end{bmatrix}$$

Επομένως με την δράση της CNOT στην $\frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ -1 \end{bmatrix}$ θα προκύψει ότι

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 1 \\ 0 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 0 \\ 1 \\ -1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} (0|00\rangle + |01\rangle - |10\rangle + 0|11\rangle) = \frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$$

Παρατηρούμε για την κατάσταση $|01\rangle$, από το αποτέλεσμα μετά την δράση των πυλών του κυκλώματος πως δημιουργείται μια κατάσταση κβαντικής διεμπλοκής η $\frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$.

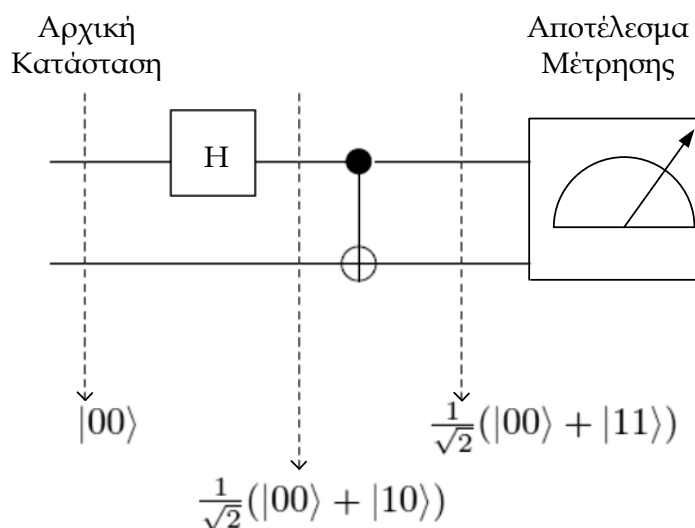
► Αυτές οι καταστάσεις κβαντικής διεμπλοκής (που δημιουργήθηκαν μετά την δράση των πυλών, από τις αρχικές καταστάσεις $|00\rangle, |01\rangle, |10\rangle$ και $|11\rangle$) ονομάζονται αντίστοιχα, καταστάσεις BELL [1, 11, 40] και αποτυπώνονται στον πίνακα του επόμενου σχήματος 7.10.

A/A	Κβαντικές καταστάσεις	Δράση πυλών	Αποτέλεσμα κβαντικής διεμπλοκής
1)	$ 00\rangle$	$\text{CNOT} \cdot ((H \otimes I) \cdot 00\rangle)$	$\frac{1}{\sqrt{2}}(00\rangle + 11\rangle)$
2)	$ 01\rangle$	$\text{CNOT} \cdot ((H \otimes I) \cdot 01\rangle)$	$\frac{1}{\sqrt{2}}(01\rangle + 10\rangle)$
3)	$ 10\rangle$	$\text{CNOT} \cdot ((H \otimes I) \cdot 10\rangle)$	$\frac{1}{\sqrt{2}}(00\rangle - 11\rangle)$
4)	$ 11\rangle$	$\text{CNOT} \cdot ((H \otimes I) \cdot 11\rangle)$	$\frac{1}{\sqrt{2}}(01\rangle - 10\rangle)$

Σχήμα 7.10

Στον πίνακα απεικονίζονται οι καταστάσεις Bell

Στο επόμενο κβαντικό κύκλωμα αποτυπώνεται η δράση των κβαντικών πυλών της 1^{ης} από τις τέσσερις καταστάσεις Bell:



Σχήμα 7.11

ΚΕΦΑΛΑΙΟ 8^ο

ΚΒΑΝΤΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ

8.1 ΕΙΣΑΓΩΓΗ ΣΤΟΥΣ ΚΒΑΝΤΙΚΟΥΣ ΑΛΓΟΡΙΘΜΟΥΣ

Η δομή των κβαντικών αλγορίθμων είναι διαφορετική από αυτή των κλασσικών υπολογιστών. Η είσοδος ενός κβαντικού αλγορίθμου δέχεται n qubits, και κατόπιν δημιουργείται κβαντική υπέρθεση των καταστάσεων ώστε το αποτέλεσμα θα είναι να πάρουμε τα ανάλογα qubits εξόδου δηλαδή την πιθανότητα να συμβούν οι τελικές καταστάσεις.

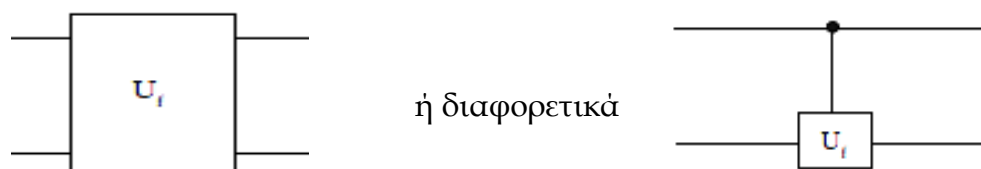
Η χρήση των κβαντικών αλγορίθμων γίνεται με την κατάλληλη χρήση κβαντικών πυλών. Το αποτέλεσμα της χρήσης των αλγορίθμων αποτυπώνει την πιθανότητα των καταστάσεων της μέτρησης δηλαδή η χρήση των κβαντικών

αλγορίθμων έχει να κάνει με την αξιολόγηση των πιθανοτήτων και των νόμων που τους διέπουν. Επίσης η χρήση των αλγορίθμων προσβλέπει και στην ελαχιστοποίηση της πιθανότητας σφάλματος του αποτελέσματος που προκύπτει μετά την δράση τους.

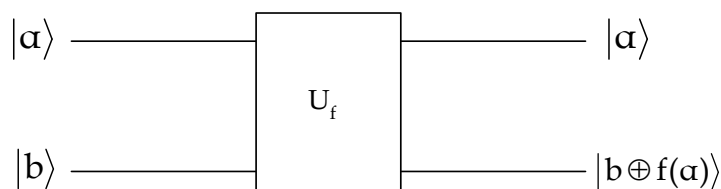
Ο πρώτος κβαντικός αλγόριθμος που αναπτύχθηκε είναι ο αλγόριθμος του Deutsch το καλοκαίρι του 1984. Ο συγκεκριμένος αλγόριθμος αφορά μόνο τους κβαντικούς υπολογιστές και δεν εφαρμόζεται στους κλασσικούς υπολογιστές.

8.2 ΚΒΑΝΤΙΚΟΣ ΑΛΓΟΡΙΘΜΟΣ ΤΟΥ DEUTSCH

Στον κβαντικό αλγόριθμο του Deutsch ⁷ γίνεται αξιοποίηση της κβαντικής υπέρθεσης των κβαντικών καταστάσεων. Ο αλγόριθμος αξιοποιεί τις κβαντικές πύλες ώστε μέσω των δράσεών τους να δωθεί το αποτέλεσμα της πιθανότητας να βρεθεί η κβαντική κατάσταση, σύμφωνα πάντα με την διαδικασία των δράσεων που αναλύθηκαν στο προηγούμενο κεφάλαιο των κβαντικών κυκλωμάτων. Το κβαντικό κύκλωμα του αλγορίθμου του Deutsch περιλαμβάνει κβαντικές πύλες Hadamard και την συνδυαστική πύλη κβαντικών πυλών που συμβολίζεται -καλείται μαύρο κουτί- με U_f και δρά στις κβαντικές αρχικές καταστάσεις $|0\rangle$ ή $|1\rangle$. Ο συμβολισμός της σε δίκτυα θα είναι ο εξής



Το ενδιαφέρον της δομής της πύλης σύμφωνα με τον Deutsch είναι ότι αφήνει την μια από τις δύο κβαντικές αρχικές καταστάσεις qubits, του κβαντικού καταχωρητή αναλλοίωτη ενώ την δεύτερη την μετασχηματίζει, σύμφωνα με το επόμενο σχήμα



Σχήμα 8.1

⁷ Ο αλγόριθμος στην βιβλιογραφία καλείται και Deutsch - Jozsa αλγόριθμος

Παρατηρούμε ότι η κατάσταση $|b\rangle$ μετά την δράση της U_f αλλάζει και γίνεται $|b \oplus f(a)\rangle$.

Ο συμβολισμός $\oplus$ ⁸ σημαίνει πρόσθεση με βάση το 2 (δηλαδή mod 2⁹). Η $f(a)$ είναι μια συνάρτηση που μπορεί να πάρει τιμές 0 ή 1 και ισχύει $f: \{0,1\} \rightarrow \{0,1\}$ (δηλαδή $a, b, f(x) \in \{0,1\}$) και χαρακτηρίζεται ως constant (σταθερή) ή balanced (ισορροπημένη) όταν αντίστοιχα είναι $f(0)=f(1)$ ή $f(0) \neq f(1)$. Ισχύουν ότι:

— Η συνάρτηση f είναι σταθερή όταν

$$\alpha) f(0)=f(1)=0 \text{ και } \beta) f(0)=f(1)=1$$

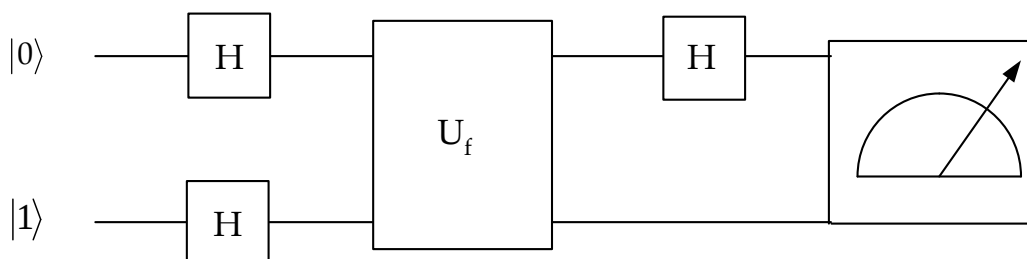
— Η συνάρτηση f είναι ισορροπημένη όταν

$$\alpha) f(0)=0, f(1)=1 \text{ και } \beta) f(1)=0, f(0)=1$$

Η δράση λοιπόν της κβαντικής πύλης U_f θα είναι αποτέλεσμα του κβαντικού κυκλώματος του προηγούμενου σχήματος 8.1 και θα δίνεται από την

$$U_f |ab\rangle = |a\rangle |b \oplus f(a)\rangle \quad 8.1$$

Το κβαντικό κύκλωμα του αλγορίθμου Deutsch φαίνεται στο επόμενο σχήμα 8.2, στο οποίο οι αρχικές καταστάσεις εισόδου του κβαντικού καταχωρητή είναι οι $|0\rangle$ και η $|1\rangle$:



Σχήμα 8.2

⁸ Ισχύουν $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0, 2 \oplus 3 = 1$ κ.ο.κ.

⁹ Μοδιακή αριθμητική ή modular arithmetic (περισσότερα στην παράγραφο §9.1).

■ Μαθηματική επεξεργασία του αλγορίθμου Deutsch

Δράση 1^η

Η είσοδος είναι η κατάσταση $|01\rangle$, στην οποία δρα η $H \otimes H$ που όπως είδαμε στο προηγούμενο κεφάλαιο των κβαντικών κυκλωμάτων, θα ισοδυναμεί με

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

Οπότε η κατάσταση που είναι η είσοδος στην πύλη U_f θα είναι η $H|0\rangle \otimes H|1\rangle = (H \otimes H)|01\rangle$. Αντικαθιστώντας προκύπτει ότι

$$(H \otimes H)|01\rangle = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}$$

Δράση 2^η

Η δράση της U_f θα δώσει με χρήση της σχέσης 8.1, την

$$\begin{aligned} U_f(H \otimes H)|01\rangle &= U_f \cdot \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = U_f \frac{1}{2} (|00\rangle - |01\rangle + |10\rangle - |11\rangle) \stackrel{U_f|ab\rangle = |a\rangle|b \oplus f(a)\rangle}{=} \\ &= \frac{1}{2} |0\rangle |0 \oplus f(0)\rangle - \frac{1}{2} |0\rangle |1 \oplus f(0)\rangle + \frac{1}{2} |1\rangle |0 \oplus f(1)\rangle - \frac{1}{2} |1\rangle |1 \oplus f(1)\rangle \end{aligned}$$

Δράση 3^η

Στην συνέχεια δρα η $H \otimes I$ η οποία είναι ίση με

$$H \otimes I = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

Τότε θα προκύψει το αποτέλεσμα της συνολικής δράσης του κβαντικού κυκλώματος που θα είναι ίση με

$$\begin{aligned}
& (H \otimes I)(U_f(H \otimes H)|01\rangle) = \\
& = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \left(\frac{1}{2}|0\rangle|0 \oplus f(0)\rangle - \frac{1}{2}|0\rangle|1 \oplus f(0)\rangle + \frac{1}{2}|1\rangle|0 \oplus f(1)\rangle - \frac{1}{2}|1\rangle|1 \oplus f(1)\rangle \right)
\end{aligned}$$

Διακρίνουμε τις περιπτώσεις:

1.α Όταν η συνάρτηση f είναι σταθερή με $f(0)=f(1)=0$ και

1.β Όταν η συνάρτηση f είναι σταθερή με $f(0)=f(1)=1$

και

2.α Όταν η συνάρτηση f είναι ισορροπημένη με $f(0)=0, f(1)=1$

2.β Όταν η συνάρτηση f είναι ισορροπημένη με $f(1)=0, f(0)=1$

Οπότε θα προκύψει με γνωστά τα $0 \oplus 0=0, 0 \oplus 1=1, 1 \oplus 0=1, 1 \oplus 1=0$ ότι

$$\begin{aligned}
& (H \otimes I)(U_f(H \otimes H)|01\rangle) = \\
& \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|0\rangle|0 \oplus f(0)\rangle - \frac{1}{2}|0\rangle|1 \oplus f(0)\rangle + \frac{1}{2}|1\rangle|0 \oplus f(1)\rangle - \frac{1}{2}|1\rangle|1 \oplus f(1)\rangle \right) = \\
& \left\{ \begin{aligned} & = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|0\rangle|0 \oplus 0\rangle - \frac{1}{2}|0\rangle|1 \oplus 0\rangle + \frac{1}{2}|1\rangle|0 \oplus 0\rangle - \frac{1}{2}|1\rangle|1 \oplus 0\rangle \right) = \\ & \stackrel{1.α}{=} \stackrel{f(0)=f(1)=0}{=} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle \right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix} = \\ & = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|01\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle) = \frac{1}{\sqrt{2}}|0\rangle(|0\rangle - |1\rangle) \end{aligned} \right.
\end{aligned}$$

Ομοίως για την περίπτωση 1.β (με γνωστά τα $0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0$) προκύπτει

$$\begin{aligned}
 (H \otimes I)(U_f(H \otimes H)|01\rangle) &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|0\rangle|0 \oplus f(0)\rangle - \frac{1}{2}|0\rangle|1 \oplus f(0)\rangle + \frac{1}{2}|1\rangle|0 \oplus f(1)\rangle - \frac{1}{2}|1\rangle|1 \oplus f(1)\rangle \right) = \\
 &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|0\rangle|0 \oplus 1\rangle - \frac{1}{2}|0\rangle|1 \oplus 1\rangle + \frac{1}{2}|1\rangle|0 \oplus 1\rangle - \frac{1}{2}|1\rangle|1 \oplus 1\rangle \right) = \\
 \stackrel{1.\beta}{\overline{f(0)=f(1)=1}}} &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|01\rangle - \frac{1}{2}|00\rangle + \frac{1}{2}|11\rangle - \frac{1}{2}|10\rangle \right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \\
 &= \frac{1}{\sqrt{2}} \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = -\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|01\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |00\rangle) = \frac{1}{\sqrt{2}}|0\rangle(|1\rangle - |0\rangle)
 \end{aligned}$$

Επίσης για την περίπτωση 2.α είναι

$$\begin{aligned}
 (H \otimes I)(U_f(H \otimes H)|01\rangle) &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|0\rangle|0 \oplus f(0)\rangle - \frac{1}{2}|0\rangle|1 \oplus f(0)\rangle + \frac{1}{2}|1\rangle|0 \oplus f(1)\rangle - \frac{1}{2}|1\rangle|1 \oplus f(1)\rangle \right) = \\
 &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|0\rangle|0 \oplus 0\rangle - \frac{1}{2}|0\rangle|1 \oplus 0\rangle + \frac{1}{2}|1\rangle|0 \oplus 1\rangle - \frac{1}{2}|1\rangle|1 \oplus 1\rangle \right) = \\
 \stackrel{2.\alpha}{\overline{f(0) \neq f(1) \\ f(0)=0, f(1)=1}}} &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|11\rangle - \frac{1}{2}|10\rangle \right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \frac{1}{2} \begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix} = \\
 &= \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle) = \frac{1}{\sqrt{2}}|1\rangle(|0\rangle - |1\rangle)
 \end{aligned}$$

Και τέλος

$$\begin{aligned}
 (H \otimes I)(U_f(H \otimes H)|01\rangle) &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|0\rangle|0 \oplus f(0)\rangle - \frac{1}{2}|0\rangle|1 \oplus f(0)\rangle + \frac{1}{2}|1\rangle|0 \oplus f(1)\rangle - \frac{1}{2}|1\rangle|1 \oplus f(1)\rangle \right) = \\
 &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|0\rangle|0 \oplus 1\rangle - \frac{1}{2}|0\rangle|1 \oplus 1\rangle + \frac{1}{2}|1\rangle|0 \oplus 0\rangle - \frac{1}{2}|1\rangle|1 \oplus 0\rangle \right) = \\
 &\stackrel{\substack{2\beta \\ f(0) \neq f(1) \\ f(0)=1, f(1)=0}}{=} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \left(\frac{1}{2}|01\rangle - \frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle \right) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} \cdot \frac{1}{2} \begin{bmatrix} -1 \\ 1 \\ 1 \\ -1 \end{bmatrix} = \\
 &= \frac{1}{\sqrt{2}} \begin{bmatrix} 0 \\ 0 \\ -1 \\ 1 \end{bmatrix} = -\frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{\sqrt{2}}(-|10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}|1\rangle(|1\rangle - |0\rangle)
 \end{aligned}$$

Σχόλια - Παρατηρήσεις:

■ Από τα αποτελέσματα των μετρήσεων βλέπουμε πως όταν η συνάρτηση f είναι σταθερή, τότε το αποτέλεσμα θα είναι ανάλογο της κατάστασης $|0\rangle$ και όταν η συνάρτηση f είναι ισορροπημένη, τότε το αποτέλεσμα, θα είναι ανάλογο της κβαντικής κατάστασης $|1\rangle$.

■ Η σχέση 8.1: $U_f|x\rangle|b\rangle = |x\rangle|b \oplus f(x)\rangle$, μπορεί να γραφεί και με τον εξής τρόπο :

$$U_f|x\rangle|b\rangle = (-1)^{f(x)}|x\rangle|b\rangle = \begin{cases} = |xb\rangle & f(x)=0 \\ = -|xb\rangle & f(x)=1 \end{cases} \quad 8.2$$

Οπότε αν γίνει επεξεργασία των δεδομένων με $|b\rangle=|1\rangle$ και $|b\rangle=|0\rangle$ γίνεται ισοδύναμα

$$U_f |x\rangle |b\rangle = (-1)^{f(x)} |x\rangle |b\rangle = \begin{cases} = |xb\rangle & b=0 \\ = -|xb\rangle & b=1 \end{cases} \xrightarrow{b=0, b=1} \begin{cases} U_f |x\rangle |0\rangle = (-1)^{f(x)} |x\rangle |0\rangle = \begin{cases} = |x\rangle |0\rangle & f(x)=0 \\ = |x\rangle |1\rangle & f(x)=1 \end{cases} \\ U_f |x\rangle |1\rangle = (-1)^{f(x)} |x\rangle |1\rangle = \begin{cases} = |x\rangle |1\rangle & f(x)=0 \\ = |x\rangle |0\rangle & f(x)=1 \end{cases} \end{cases} \xrightarrow{\text{αφαιρούμε κατά μέλη}} \Rightarrow$$

Αφαιρώντας κατά μέλη τις δύο προηγούμενες σχέσεις προκύπτει ότι

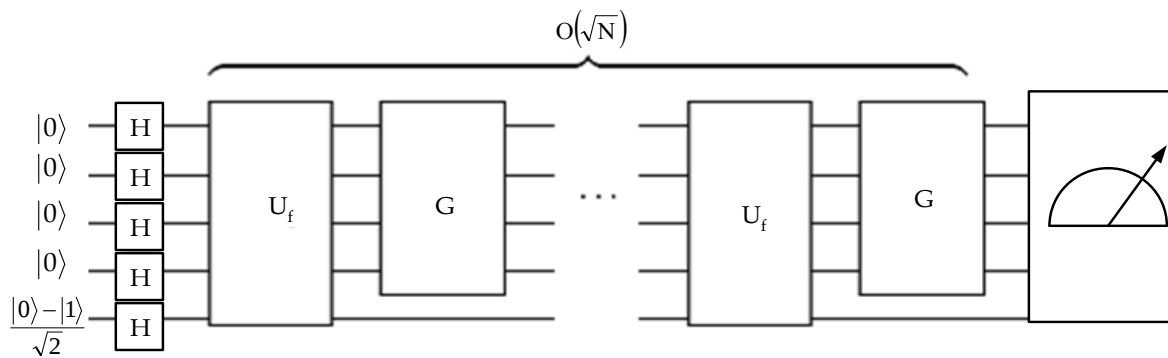
$$U_f |x\rangle |0\rangle - U_f |x\rangle |1\rangle = \begin{cases} = |x\rangle |0\rangle - |x\rangle |1\rangle = |x\rangle (|0\rangle - |1\rangle) & f(x)=0 \\ = -|x\rangle |0\rangle + |x\rangle |1\rangle = -|x\rangle (|0\rangle - |1\rangle) & f(x)=1 \end{cases} \Rightarrow$$

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

Παρατηρούμε πως η σχέση που καταλήξαμε καθορίζεται άμεσα από το αν η συνάρτηση $f(x)$ είναι σταθερή ή ισορροπημένη για $x=0$ ή $x=1$.

8.3 ΚΒΑΝΤΙΚΟΣ ΑΛΓΟΡΙΘΜΟΣ ΤΟΥ GROVER

Ο Λον Grover έδειξε ότι με έναν κβαντικό υπολογιστή μπορούμε σε αταξινόμητες (ή αλλιώς μη δομημένες) βάσεις δεδομένων να βρούμε ένα ζητούμενο (ένα άγνωστο στοιχείο από τα γνωστά δεδομένα) αν γίνει έλεγχος $\sqrt{N}$ φορές στην βάση δεδομένων. Αυτό συγκριτικά είναι πολύ λιγότερο από τον έλεγχο του κλασσικού υπολογιστή, ο οποίος είναι ίσος περίπου με $N/2$. Αυτό λοιπόν πετυχαίνεται με τον κβαντικό αλγόριθμο που ανέπτυξε ο Grover ο οποίος αποτυπώνεται στο επόμενο σχήμα και ο οποίος θα αναπτυχθεί στην συνέχεια της παραγράφου.

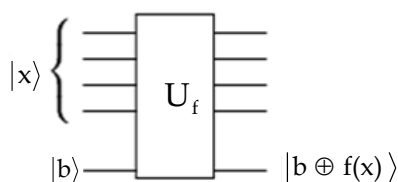


Σχήμα 8.3

Όσο μεγαλύτερη είναι η αταξινόμητη βάση δεδομένων τόσο πιο αποτελεσματικός είναι ο κβαντικός υπολογιστής συγκριτικά με τον κλασσικό, καθώς ο έλεγχος γίνεται σε υπολογιστικό χρόνο τάξεως $O(\sqrt{N})$, όπως φαίνεται στο σχήμα. Ο αριθμός των επαναλήψεων για την εύρεση ενός στοιχείου μιας μη δομημένης βάσης δεδομένων έχει αποδειχθεί ότι είναι $\frac{1}{2}(\frac{\pi}{2}\sqrt{N} - 1)$. Ο αλγόριθμος Grover επίσης μπορεί να χρησιμοποιηθεί και για την εύρεση k στοιχείων από N αντικείμενα μιας μη δομημένης βάσης δεδομένων σε $\frac{\pi}{4}\sqrt{\frac{N}{k}}$ δοκιμές.

— Το **κβαντικό Oracle** ουσιαστικά είναι μια συνάρτηση f η οποία παίρνει τιμές 0 ή 1, δηλαδή $f:N \rightarrow \{0,1\}$, με $N=2^n-1$ ($n=1,2,3,4,\dots$) στοιχεία και η συνάρτηση έχει n qubits, δηλαδή για $1,2,3,4,5,\dots$ οι κβαντικές καταστάσεις αντίστοιχα, θα είναι οι $|000\dots00000\rangle, |000\dots00001\rangle, |000\dots00011\rangle, |000\dots00100\rangle, |000\dots00101\rangle, |000\dots00110\rangle, |000\dots00111\rangle, \dots$

Το σύστημα που μας λέει αν ένα στοιχείο είναι το ζητούμενο ή όχι λέγεται **μαύρο κουτί ή oracle** U_f και αποτυπώνεται από το επόμενο κβαντικό κύκλωμα



Σχήμα 8.4

Η συνάρτηση f για το ζητούμενο στοιχείο α (ή η βασική κατάσταση, από την μη δομημένη βάση δεδομένων) παίρνει τιμές $f(x=\alpha)=1$, ενώ για άλλες τιμές x ($x \neq \alpha$) είναι $f(x \neq \alpha)=0$, δηλαδή

$$\begin{cases} f(x)=0, & x \neq a \\ f(x)=1, & x = a \end{cases}$$

Επομένως η δράση του oracle όταν ο κβαντικός καταχωρητής έχει δύο αρχικές καταστάσεις έστω τις $|x\rangle, |b\rangle$, θα αφήνει αναλλοίωτη την $|x\rangle$ και θα επηρεάζει την δεύτερη, και θα δίνεται από την

$$U_f |xb\rangle = |x\rangle |b \oplus f(x)\rangle. \quad 8.3$$

όπου όπως είδαμε και στον αλγόριθμο του Deutsch το $\oplus$ είναι η πρόσθεση με βάση το 2 (mod 2¹⁰).

Το αποτέλεσμα της δράσης του oracle που δρα στην αρχική βασική κατάσταση του κβαντικού καταχωρητή θα είναι

$$U_f |x\rangle = (-1)^{f(x)} |x\rangle = \begin{cases} (-1)^0 |x\rangle = |x\rangle & f(x)=0 \\ (-1)^1 |x\rangle = -|x\rangle & f(x)=1 \end{cases} \quad 8.4$$

Η $f(x)$ παίρνει την τιμή $|x\rangle$ αν το στοιχείο x είναι το ζητούμενο και την τιμή $-|x\rangle$ αν δεν είναι και αλλάζει έτσι το πρόσημο της κβαντικής κατάστασης. Το κβαντικό oracle με την δράση του πάνω στα qubits μπορεί να γραφεί, ως τελεστής, δηλαδή θα δρα με την εξής σχέση (όπου I η κβαντική πύλη αδρανείας και $|a\rangle$ το ζητούμενο στοιχείο ή κατάσταση):

$$U_f = I - 2|a\rangle\langle a| \quad 8.5$$

— Ο αλγόριθμος του Grover (που αποδίδεται από το κβαντικό κύκλωμα του σχήματος 8.3) μας δίνει αποτέλεσμα μέτρησης θεωρώντας δεδομένα εισόδου τις καταστάσεις που προκύπτουν από τον τρόπο υπολογισμού του oracle (ή μαύρου κουτιού) U_f . Ο Grover όρισε την δράση της κβαντικής πύλης μέσω του τελεστή G , στον χώρο του Hilbert και η δράση θα δίνεται από την σχέση

$$G = -I + 2|\psi\rangle\langle\psi| \quad 8.6$$

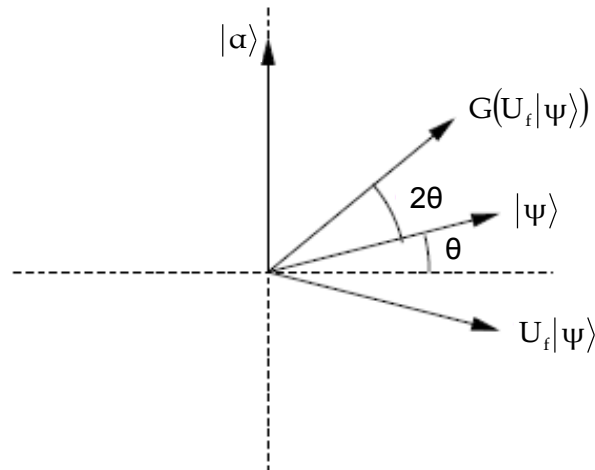
όπου $|\psi\rangle$ είναι η υπέρθεση όλων των κβαντικών αρχικών καταστάσεων δηλαδή,

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{v=1}^{N-1} |x_v\rangle$$

¹⁰ Αναλυτικότερα στοιχεία και υπολογισμός πράξεων στην §9.1.

ή πιο συγκεκριμένα (για υπέρθεση κβαντικών καταστάσεων με σταθερό πλάτος για κάθε κατάσταση $\sqrt{N}^{-1}$) $|\psi\rangle = \frac{1}{\sqrt{N}}(|0\rangle + |1\rangle + \dots + |N-1\rangle)$.

Επίσης μπορούμε να δώσουμε μια **γεωμετρική εικόνα των δράσεων** των κβαντικών $U = I - 2|\alpha\rangle\langle\alpha|$ και $G = -I + 2|\psi\rangle\langle\psi|$ μέσω των καταστάσεων $|\alpha\rangle$ και $|\psi\rangle$. Αυτή φαίνεται στο επόμενο σχήμα.



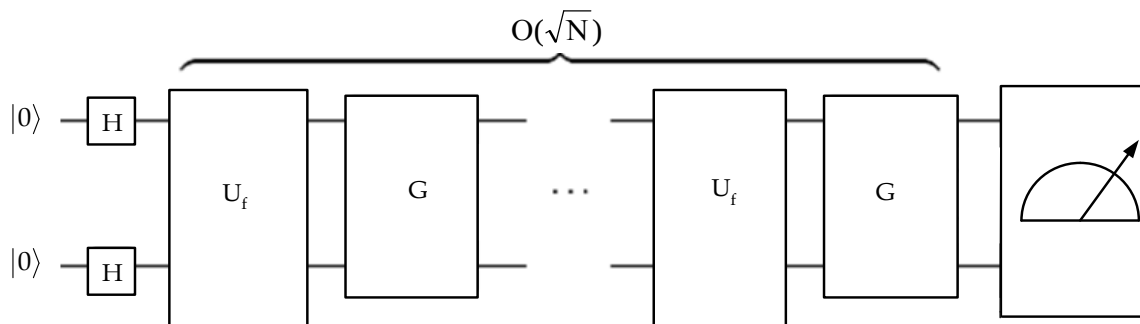
Σχήμα 8.5

Το U_f είναι μια αντανάκλαση της σχετικής κάθετης γραμμής του διανύσματος κατάστασης $|\alpha\rangle$. Το G είναι η αντανάκλαση αντίστοιχα της κατάστασης $U_f|\psi\rangle$ όπως αποτυπώνεται στο σχήμα. Η σύνθεση των δύο αντανάκλασεων του πλάνου των διανυσμάτων και των δράσεων είναι πάντα μια περιστροφή. Η δράση της U_f περιστρέφει την $|\psi\rangle$. Η δράση της G περιστρέφει την $U_f|\psi\rangle$. Η δράση των τελεστών G και U_f πάνω στην $|\psi\rangle$ περιστρέφει την κατάσταση της κατά γωνία θ ως προς την ζητούμενη αρχική κατάσταση $|\alpha\rangle$. Κάθε επανάληψη του κβαντικού αλγορίθμου Grover περιστρέφει την κατάσταση κατά $|\psi\rangle$ γωνία θ ως προς την κατάσταση $|\alpha\rangle$. Στο σχήμα 8.5 φαίνεται ότι $\sin\theta = \cos(90^\circ - \theta) = \langle\alpha|\psi\rangle = \frac{1}{\sqrt{N}}$ και για μεγάλες τιμές N η γωνία είναι $\theta \approx \frac{1}{\sqrt{N}}$. Περαιτέρω επαναλήψεις πέρα από χρόνο t θα μειώσει την πιθανότητα εύρεσης της κατάστασης $|\alpha\rangle$. Ο χρόνος υπολογισμού του στοιχείου έχει υπολογιστεί ότι είναι $t \approx \frac{90^\circ}{2\theta} \approx \frac{\pi}{4} \sqrt{N}$ και μετά από επαναλήψεις του

αλγορίθμου Grover ίση με $\frac{\pi}{4}\sqrt{N} - \frac{1}{2}$, έχει αποδειχθεί ότι το πλάτος της κβαντικής κατάστασης γίνεται 1.

■ Μαθηματική επεξεργασία του αλγορίθμου Grover

Δίνεται το κύκλωμα του κβαντικού αλγορίθμου Grover του επόμενου σχήματος. Θα υπολογίσουμε την πιθανότητα του στοιχείου που αντιστοιχεί στην κατάσταση $|10\rangle$. Για την επίλυση θεωρούμε $N=4$ και 2 qubits .



Σχήμα 8.6

Δράση 1^η

Η είσοδος είναι η κατάσταση $|00\rangle$ και δρα η $H \otimes H$, η οποία θα ισοδυναμεί με

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

Οπότε η κατάσταση που είναι η είσοδος στην πύλη U_f θα είναι

$$H|0\rangle \otimes H|0\rangle = (H \otimes H)|00\rangle.$$

Αντικαθιστώντας προκύπτει ότι

$$(H \otimes H)|00\rangle = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Δράση 2^η

Η δράση της U_f θα δώσει (με χρήση της σχέσης 8.5, $U = I - 2|a\rangle\langle a|$ όπου I ο μοναδιαίος

πίνακας και $|a\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}$ η ζητούμενη κατάσταση), τα εξής

$$U_f = I - 2|a\rangle\langle a| = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} - 2 \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} - 2 \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Τότε η δράση του oracle (ελέγχει το αν η κατάσταση μπορεί να αλλάξει το πρόσημο σύμφωνα με την σχέση 8.4) θα δώσει ότι

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \cdot \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{2} (|00\rangle + |01\rangle - |10\rangle + |11\rangle)$$

Παρατηρούμε ότι το πρόσημο της κατάστασης $|10\rangle$ έχει αλλάξει.

Δράση 3^η

Η δράση της σχέσης 8.6, $G = -I + 2|\psi\rangle\langle\psi|$ (με την κατάσταση να είναι αυτή που

υπολογίστηκε στο βήμα της 1^{ης} δράσης $\frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$ στην προκύπτουσα $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$) θα

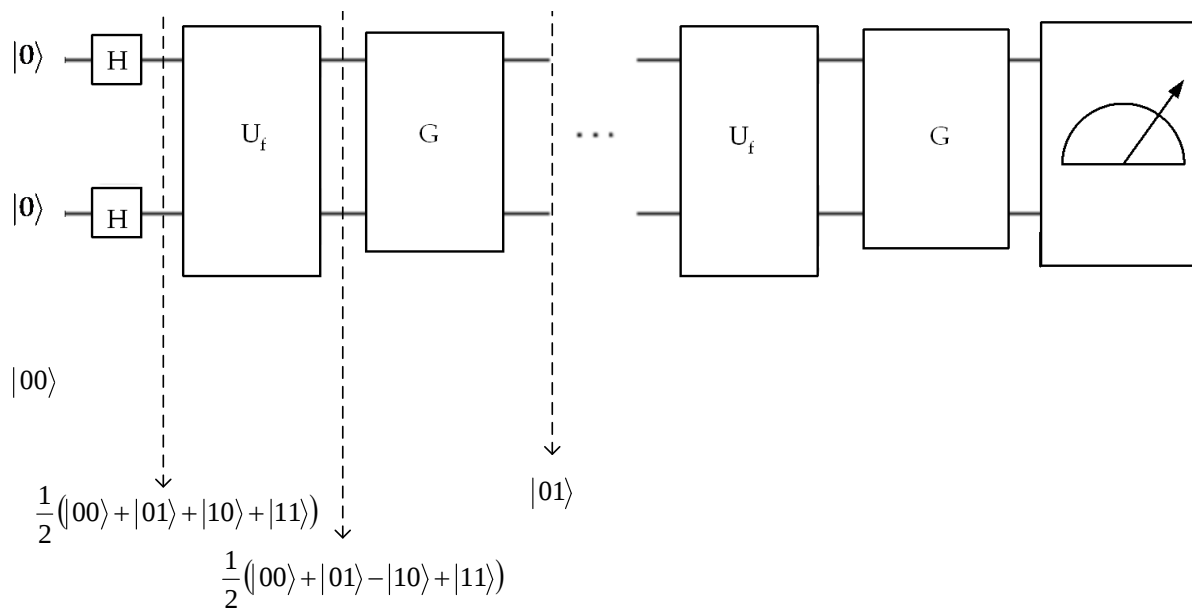
δώσει τα εξής:

$$G = -I + 2|\psi\rangle\langle\psi| = -\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} + 2 \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} = -\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \frac{1}{2} = \frac{1}{2} \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix}$$

Οπότε η δράση της κβαντικής πύλης του αλγορίθμου του Grover θα δράσει πάνω στην κατάσταση εισόδου της

$$\frac{1}{2} \begin{bmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{bmatrix} \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ -1 \\ 1 \end{bmatrix} = \frac{1}{4} \begin{bmatrix} 0 \\ 0 \\ 4 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 0|00\rangle + 0|01\rangle + |10\rangle + 0|11\rangle = |10\rangle .$$

Τα βήματα των δράσεων που υπολογίστηκαν, απεικονίζονται στο επόμενο σχήμα :



Δράση 4^η

Επανάληψη δράσεων ακόμα μια φορά . Δίνεται από τα δεδομένα (με $N=4$), ότι τα βήματα των επαναλήψεων είναι $O(\sqrt{N}) = 2$. Οπότε μετά από μια ακόμα επανάληψη (γιατί $\frac{1}{2}(\frac{\pi}{2}\sqrt{N} - 1) = \frac{1}{2}(\frac{\pi}{2}\sqrt{4} - 1) = 1,07 \approx 1$) των ιδίων υπολογισμών που μόλις έγιναν θα υπολογίσουμε όντως ότι η ζητούμενη κατάσταση θα είναι η $|10\rangle$.

Οπότε χωρίς να επαναλάβουμε ξανά τις πράξεις με τους τελεστές των δράσεων θα έχουμε με δράση της oracle και της Grover ότι:

$$G\left(U_f\left(\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |10\rangle + |11\rangle)\right)\right) = |10\rangle .$$

ΚΕΦΑΛΑΙΟ 9^ο

ΚΒΑΝΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

9.1 ΣΤΟΙΧΕΙΑ ΚΡΥΠΤΟΓΡΑΦΙΑΣ

Η λέξη **κρυπτογραφία** προέρχεται από τα συνθετικά «κρυπτός και γράφω» και είναι ένας επιστημονικός κλάδος που ασχολείται με την μελέτη, την ανάπτυξη και την χρήση τεχνικών κρυπτογράφησης και αποκρυπτογράφησης με σκοπό την απόκρυψη του περιεχομένου των μηνυμάτων. Ο κύριος στόχος της είναι να παρέχει μηχανισμούς για 2 ή περισσότερα μέλη να επικοινωνήσουν χωρίς κάποιος άλλος να είναι ικανός να διαβάσει την πληροφορία εκτός από τα μέλη. Η κρυπτογραφία έχει 4 βασικές λειτουργίες:

- **Confidentiality** (εμπιστευτικότητα): Η προς μετάδοση πληροφορία είναι προσβάσιμη μόνο στα εξουσιοδοτημένα, επιλεγμένα μέλη (παραλήπτης-αποστολέας). Η πληροφορία είναι ακατανόητη σε κάποιον τρίτο (υποκλοπέας).
- **Integrity** (ακεραιότητα): Η πληροφορία μπορεί να αλλοιωθεί μόνο από τα εξουσιοδοτημένα μέλη (παραλήπτης-αποστολέας) και δεν μπορεί να αλλοιώνεται χωρίς την ανίχνευση της αλλοίωσης. Ένας εισβολέας δεν μπορεί να τροποποιήσει τα δεδομένα.
- **Non repudiation** (μη απάρνηση-αποποίηση): Ο αποστολέας (ή ο παραλήπτης) της πληροφορίας δεν μπορεί να αρνηθεί την αυθεντικότητα της μετάδοσης της.
- **Authentication** (πιστοποίηση-αυθεντικοποίηση): Ο αποστολέας και ο παραλήπτης μπορούν να εξακριβώνουν τις ταυτότητές τους καθώς και την πηγή και τον προορισμό της πληροφορίας με διαβεβαίωση ότι οι ταυτότητές τους δεν είναι αλλοιωμένες ή πλαστές. Ένας εισβολέας δεν μπορεί να μεταμφιεστεί σε κάποιον άλλο.

Η κρυπτογραφία μπορεί να χωριστεί στην διάρκεια εξέλιξης του ανθρώπου σε τρεις μεγάλες περιόδους. Η πρώτη είναι μέχρι το 1900, η δεύτερη από τις αρχές του προηγούμενου αιώνα μέχρι το 1950 και η τρίτη και σημαντικότερη περίοδος εξέλιξης της κρυπτογραφίας είναι από τα μέσα του προηγούμενου αιώνα μέχρι σήμερα. Ουσιαστικά οι σημαντικές χρονιές ορόσημο για την δημιουργία της είναι το 1976 με την ανάπτυξη του DES (data encryption standard), το 1976 με τις New Directions in Cryptography και το 1978 με την ανάπτυξη του RSA algorithm που επινόησαν οι Rivest – Shamir – Adleman. Στα μέσα της δεκαετίας του '70 έγινε η δημοσίευση του σχεδίου προτύπου κρυπτογράφησης DES στον ομοσπονδιακό κατάλογο της Αμερικής (στις 17 Μαρτίου 1975). Ο DES αντικαταστάθηκε επίσημα από τον AES (advanced encryption standard) το 2001. Επίσης στα τέλη της δεκαετίας του 70 έγινε η ανάπτυξη του RSA δηλαδή, το κρυπτογραφικό σύστημα το οποίο χρησιμοποιείται ακόμα και σήμερα σε πύστες εφαρμογές, σημαντικότερη ίσως, εκ των οποίων είναι και η αξιοποίηση του στις τραπεζικές συναλλαγές. Η εξέλιξη και χρησιμοποίηση της κρυπτογραφίας αυξάνεται με την εξέλιξη των πληροφοριακών συστημάτων και καθίσταται πολύ σημαντική στις μέρες μας καθώς χρησιμοποιείται για σκοπούς όπως η ασφάλεια συναλλαγών σε τραπεζικά δίκτυα και Α.Τ.Μ., στην σταθερή και κινητή τηλεφωνία, σε στρατιωτικά δίκτυα, σε συστήματα συναγερμών, σε συστήματα βιομετρικής αναγνώρισης, σε συστήματα τηλεϊατρικών δεδομένων και εφαρμογών κ.α. πολλά.

Διακρίνουμε δύο είδη κρυπτογραφίας της συμμετρική και την ασύμμετρη κρυπτογραφία [43]. Η βασική διαφορά μεταξύ τους είναι ότι στην συμμετρική οι δύο οντότητες (αποστολέας και παραλήπτης) συνομιλούν και έχουν το ίδιο κλειδί ενώ

στην ασύμμετρη οι δύο οντότητες είναι «άνισες» δηλαδή η μια έχει ιδιωτικό κλειδί και η άλλη δημόσιο. Η ασύμμετρη επίσης είναι πιο αργή από την συμμετρική.

Ίσως το πιο επιτυχημένο κρυπτογραφικό σύστημα για τους κλασσικούς υπολογιστές να είναι το RSA (ασύμμετρη κρυπτογραφία), το οποίο είναι ένα σύστημα με χρήση δημόσιου κλειδιού και δεν μπορεί να σπάσει εύκολα με την χρήση των συμβατικών υπολογιστών καθώς όπως αποδείχθηκε ένας ακέραιος αριθμός 129 ψηφίων χρειάστηκε 17 χρόνια να αναλυθεί σε γινόμενο δύο πρώτων αριθμών, όπως θα δούμε στην βασική του δομή στην συνέχεια. Προφανώς για νούμερα με 4 ψηφία αυτό θα ήταν σχεδόν αδύνατο να αναλυθεί σε εύλογο χρονικό διάστημα. Αυτό το αδιέξοδο καλείται να αντιμετωπίσει η κβαντική κρυπτογραφία καθώς με χρήση της μέσω του κβαντικού αλγορίθμου του Shor που θα αναλύσουμε σε επόμενη παράγραφο, μπορεί να βρεθεί γρήγορα το γινόμενο δύο μεγάλων πρώτων ακεραίων αριθμών.

Η δομή του κρυπτογραφικού συστήματος RSA αποτελείται από τα ακόλουθα βήματα [1, 8, 43, 45] :

- 1) Επιλέγονται δύο πρώτοι ακέραιοι αριθμοί p, q (μεγάλοι).
- 2) Υπολογίζουμε το γινόμενό τους $n=p \cdot q$ και την $\phi(n)=(p-1) \cdot (q-1)$ (συνάρτηση Euler¹¹).
- 3) Επιλέγεται ένας τυχαίος αριθμός d , που είναι ο πρώτος ως προς τους $p-1$ και $q-1$, όπου το 1 είναι ο ΜΚΔ (μέγιστος κοινός διαιρέτης) των d και $p-1, q-1$.
- 4) Υπολογίζεται ο αριθμός e (με $1 < e < \phi(n)$), όπου $e \cdot d = 1 \pmod{\phi(n)}$. Ο e είναι ο αντίστροφος του d (ή δηλαδή $d = e^{-1} \pmod{\phi(n)}$) (ο $d \cdot e^{-1}$ διαιρείται από τον $(p-1)(q-1)$).
- 5) Το δημόσιο κλειδί είναι το ζεύγος των (e, n) .
- 6) Το ιδιωτικό κλειδί είναι το ζεύγος (d, n) .
- 7) Ο αποστολέας στέλνει ένα μήνυμα m στον παραλήπτη, δηλαδή στέλνει $c = m^e \pmod{n}$. Ο Παραλήπτης λαμβάνει μήνυμα $m = c^d \pmod{n}$.

■ Συνήθως, στα βιβλία κρυπτογραφίας κατά σύμβαση αναφέρεται το όνομα του αποστολέας ως **Alice**, το όνομα του παραλήπτη ως **Bob** και το όνομα του υποκλοπέα ή «ωτακουστή» ως **Eve**.

¹¹ Η συνάρτηση Euler $\phi(n)$ αφορά το πλήθος των θετικών ακεραίων που δεν υπερβαίνουν τον θετικό ακέραιο n και είναι σχετικά πρώτοι προς αυτόν.

— ΣΧΟΛΙΟ —

Η **modular arithmetic** **-mod-** αφορά την μοδιακή αριθμητική σύμφωνα με την οποία, στα μαθηματικά εξετάζουμε μια πεπερασμένη ομάδα αριθμών με κυκλική διάταξη. Χαρακτηριστικά κατά μέτρο $9 \bmod 9$ το άθροισμα $2+8=1 \pmod{9}$ (όπου $\bmod 9$ είναι αριθμοί από το 0 μέχρι και το 8) ή επίσης $2+6=8 \pmod{9}$ ή επίσης $2+3=5 \pmod{9}$ ή $5+7=5 \pmod{9}$ ή αν έχουμε $16 \pmod{10}=6$ (γιατί $2+2+2+2+2+6=16$), ή αν έχουμε $128 \pmod{15}=8$ (γιατί $15+15+15+15+15+15+15+8=128$), κ.ο.κ..

■ Παράδειγμα κρυπτογραφικού συστήματος RSA:

- Η Alice (αποστολέας) επιλέγει δύο πρώτους αριθμούς $p=23$, $q=41$.
- Η Alice πολλαπλασιάζει τους p , q : $p \cdot q=23 \cdot 41=943=n$, που αυτό είναι το δημόσιο κλειδί δηλαδή $n=943$ και η Alice το στέλνει στον Bob (παραλήπτης).
- Η Alice επιλέγει έναν άλλο αριθμό e ο οποίος είναι πρώτος ως προς τον $(p-1)(q-1)=22 \cdot 40=880$, έστω $e=7$.
- Το e επίσης είναι μέρος του δημόσιου κλειδιού και ο Bob το ξέρει.
- Έστω ότι η Alice στέλνει ένα μήνυμα στον Bob, $M=35$.
- Η Alice υπολογίζει την $c=m^e \pmod{n}$, δηλαδή $c=35^7 \pmod{943}=64339296875 \pmod{943}=545$. Οπότε $c=545$ το κρυπτογραφημένο μήνυμα που στέλνει η Alice στον Bob.
- Ο Bob στην συνέχεια αποκωδικοποιεί το c . Βρίσκει ένα d ώστε $e \cdot d=1 \pmod{(p-1)(q-1)}$, δηλαδή $e \cdot d=1 \pmod{22 \cdot 40}=1 \pmod{880}$. Άρα $7d=1 \pmod{880}$. Επειδή $7 \cdot 503=3521=4 \cdot 880+1=1 \pmod{880}$, συμπεραίνουμε ότι μια λύση είναι η $d=503$.
- Η Alice για να βρει την αποκωδικοποίηση υπολογίζει το $c=m^e \pmod{n}$. Οπότε $c=545^{503} \pmod{943}=\dots=35$

Οι περισσότεροι αλγόριθμοι κρυπτογράφησης (όπως ο RSA), βασίζονται στην δυσκολία που παρουσιάζει η παραγοντοποίηση μεγάλων πρώτων αριθμών [1, 6, 8, 11, 44]. Στη συνέχεια θα περιγράψουμε κλασσικά, τον αλγόριθμο παραγοντοποίησης για την ανάλυση ενός αριθμού σε γινόμενο δύο πρώτων αριθμών. Διαθέτουμε τον ακέραιο αριθμό τον οποίο θέλουμε να αναλύσουμε σε γινόμενο δύο πρώτων αριθμών και υπολογίζουμε την περίοδο τ , της περιοδικής συνάρτησης $\varphi(x)=a^x \pmod{n}$, όπου a τυχαίος ακέραιος, πρώτος ως προς τον n ($x=0,1,2,\dots$).

Τα βήματα που ακολουθούμε αναλυτικά θα είναι :

1. Επιλογή τυχαίου αριθμού a (με $a < n$)
2. Υπολογισμός του $\text{ΜΚΔ}(a, n)$
3. Αν $\text{ΜΚΔ}(a, n) \neq 1$, τότε έχουμε βρει το ζητούμενο, αλλιώς προχωράμε στο επόμενο βήμα 4
4. Χρησιμοποιούμε την ρουτίνα εύρεσης περιόδου, για να υπολογίσουμε την περίοδο τ της συνάρτησης $\varphi(x) = a^x \pmod{n}$
5. Αν ο τ είναι περιττός, τότε επιστρέφουμε στο βήμα 1.
6. Αν $a^{\tau/2} \equiv -1 \pmod{n}$, τότε επιστρέφουμε στο βήμα 1
7. Ο $\text{ΜΚΔ}(a^{\tau/2} + 1, n)$ και ο $\text{ΜΚΔ}(a^{\tau/2} - 1, n)$ είναι μη τετριμμένος παράγοντας του n .
8. Αν τ ζυγός αριθμός τότε ένας τουλάχιστον από τους αριθμούς $a^{\tau/2} + 1$ και $a^{\tau/2} - 1$, έχει κοινό παράγοντα με τον αριθμό n .

Επομένως το θέμα του προβλήματος ανάγεται στο να υπολογίσουμε την περίοδο τ , μιας περιοδικής συνάρτησης προκειμένου να βρούμε το πρόβλημα της ανάλυσης ενός αριθμού σε γινόμενο δύο πρώτων αριθμών.

■ Παράδειγμα παραγοντοποίησης:

Θα αναλυθεί ο αριθμός 35 σε γινόμενο δύο πρώτων αριθμών. Καταρχήν επιλέγουμε τυχαία τον αριθμό $a=13$, με $\text{ΜΚΔ}(13, 35)=1$. Η περιοδική συνάρτηση $\varphi(x) = a^x \pmod{n}$, θα δώσει

$$\Phi(1) = 13^1 \pmod{35} = 13$$

$$\Phi(2) = 13^2 \pmod{35} = 169 \pmod{35} = 29 \quad (\text{γιατί είναι } 35+35+35+35+29=169)$$

$$\Phi(3) = 13^3 \pmod{35} = 2197 \pmod{35} = 27$$

$$\Phi(4) = 13^4 \pmod{35} = 28561 \pmod{35} = 1$$

$$\Phi(5) = 13^5 \pmod{35} = 371293 \pmod{35} = 13$$

$$\Phi(6) = 13^6 \pmod{35} = 4826809 \pmod{35} = 29$$

$$\Phi(7) = 13^7 \pmod{35} = 162748517 \pmod{35} = 27$$

$$\Phi(8) = 13^8 \pmod{35} = 815730721 \pmod{35} = 1$$

$$\Phi(9) = 13^9 \pmod{35} = 10604499373 \pmod{35} = 13 \quad \text{κ.ο.κ}$$

Παρατηρούμε λοιπόν πως η συνάρτηση έχει περίοδο $\tau=4$. Οπότε ο $\text{ΜΚΔ}(a^{\tau/2} + 1, n)$ και ο $\text{ΜΚΔ}(a^{\tau/2} - 1, n)$ θα είναι:

$$\text{ΜΚΔ}(13^{4/2} + 1, 35) = \text{ΜΚΔ}(170, 35) = 5 \quad \text{και} \quad \text{ΜΚΔ}(13^{4/2} - 1, 35) = \text{ΜΚΔ}(168, 35) = 7$$

Τελικά οι δύο πρώτοι αριθμοί είναι οι $5 \cdot 7 = 35$.

Η συνεχής έρευνα πάντως τα τελευταία χρόνια, πάνω στους κβαντικούς υπολογιστές έχει δείξει ότι είναι δυνατόν να παραγοντοποιήσει κανείς μεγάλους πρώτους αριθμούς σε πολυωνυμικό χρόνο με την χρήση κβαντικών πιθανοτικών αλγορίθμων. Ένας τέτοιος αλγόριθμος είναι και ο αλγόριθμος του Shor που θα αναλυθεί στην συνέχεια του κεφαλαίου.

9.2 ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΚΒΑΝΤΙΚΗ ΜΗΧΑΝΙΚΗ

Το κβαντικό σύστημα κρυπτογραφίας είναι μια επέκταση της κβαντικής επικοινωνίας δεδομένου ότι «στέλνονται» τα σωματίδια χρησιμοποιώντας την κβαντική τηλεμεταφορά¹². Τα σωματίδια κωδικοποιούνται σε κβαντικές καταστάσεις και στέλνονται στο δέκτη όπως στην κλασσική επικοινωνία. Οι καταστάσεις αντιπροσωπεύουν τις κωδικοποιημένες πληροφορίες που μπορούν να υποβληθούν σε επεξεργασία και να γίνουν κατανοητές μόνο από αυτόν που τις λαμβάνει στο τέλος. Εάν ένας άλλος παρατηρητής προσπαθήσει να εξετάσει τις πληροφορίες που στέλνονται, πρέπει να ξέρει το σχέδιο κωδικοποίησης, επειδή η μετάδοση καταστρέφεται μόλις παρατηρηθεί [6, 44].

Η κβαντική κρυπτογραφία ουσιαστικά αξιοποιεί ορισμένες ιδιότητες ενός φυσικού συστήματος σύμφωνα με την κβαντική μηχανική, έτσι ώστε να δημιουργηθεί ένα κλειδί κρυπτογράφησης μέσω του οποίου θα εξασφαλίζεται ένα ασφαλές κανάλι επικοινωνίας μεταξύ των κατόχων του (αποστολέα και παραλήπτη). Το σημαντικότερο χαρακτηριστικό της κβαντικής κρυπτογραφίας, που την διαφοροποιεί από τις κλασσικές μεθόδους κρυπτογράφησης έγκειται στο ότι οι μετέχοντες (παρατηρητής και αποστολέας), στο ασφαλές κανάλι επικοινωνίας έχουν την δυνατότητα να καταλάβουν πότε και αν κάποιος υποκλέπτει την μεταξύ τους επικοινωνία. Αυτό συμβαίνει γιατί η διαδικασία της μέτρησης (εμφάνιση υποκλοπής) διαταράσσει το κβαντικό σύστημα που στην προκειμένη περίπτωση είναι το κλειδί κρυπτογραφίας και έτσι αυτό υφίσταται αλλοιώσεις τις οποίες είναι σε θέση να τις αναγνωρίσουν οι συμμετέχοντες στο κανάλι επικοινωνίας, με την βοήθεια κάποιων αλγοριθμικών διαδικασιών, να τις διορθώσουν και εξασφαλίσουν έτσι μία απολύτως ασφαλή επικοινωνία μεταξύ τους χωρίς υπολοπές από κάποιον «ωτακουστή».

¹² Η **κβαντική τηλεμεταφορά** είναι η μεταφορά μιας κβαντικής κατάστασης από ένα σημείο σε ένα άλλο με την μορφή πληροφορίας. Εργαστηριακά κβαντική τηλεμεταφορά πραγματοποιήθηκε με χρήση φωτονίων και παγίδες ιόντων δηλαδή έγινε μεταφορά και επικόλληση πληροφοριών από ένα σημείο σε άλλο. Στην κβαντική τηλεμεταφορά ουσιαστικά εφαρμόζεται η κβαντική διεμπλοκή (§ 3.5 και § 7.3).



Σχήμα 9.1

Μια κεντρική πηγή εκπέμπει σωματίδια προς δύο παρατηρητές οι οποίοι κάνουν μετρήσεις στο *spin* (ή και σε οποιοδήποτε άλλο παρατηρήσιμο φυσικό μέγεθος όπως θέση, ορμή κ.α.). Όπως αναφέρθηκε και στο 3^ο κεφάλαιο (§ 3.3) αν το ένα σωματίδιο έχει *spin* +1, τότε το άλλο σωματίδιο θα πρέπει να έχει *spin* -1 (αρχή διατήρησης στροφορμής). Όμως η ερμηνεία της σχολής της Κοπεγχάγης (§2.2) αλλά και η αρχή της αβεβαιότητας (§1.4), θα δώσουν την κατάσταση του *spin* για κάθε ένα εκ των δύο φωτονίων να έχει 50% πιθανότητα να είναι είτε + είτε -. Με το πείραμα **EPR** (§3.3) αποδείχθηκε ότι αν ο παρατηρητής Α κάνει μια μέτρηση π.χ. του σπίν του φωτονίου που λαμβάνει, τότε ο παρατηρητής Β δεν θα ξέρει ακριβώς την τιμή που θα πάρει το σπίν του δικού του φωτονίου, οπότε η αμοιβαία κατάρρευση της κυματοσυνάρτησης φαίνεται να λαμβάνει χώρα στιγμιαία (η ανταλλαγή πληροφοριών γίνεται με την ταχύτητα του φωτός). Επομένως οι μετέχοντες έχουν την δυνατότητα να καταλάβουν πότε και αν κάποιος υποκλέπτει την επικοινωνία τους και έτσι το κανάλι καθίσταται ασφαλές καθώς ενδεχόμενη διαδικασία μέτρησης, διαταράσσει το κβαντικό σύστημα δηλαδή το κλειδί της κρυπτογράφησης και έτσι αυτό υφίσταται αλλοιώσεις, τις οποίες μπορούν να τις αναγνωρίσουν οι μετέχοντες, με την βοήθεια κάποιων αλγοριθμικών διαδικασιών, να τις διορθώσουν και εξασφαλίσουν έτσι μία απολύτως ασφαλή επικοινωνία [44]. Στο σχήμα απεικονίζονται οι δύο παρατηρητές ως Bob A και B, η Alice, το κλειδί κρυπτογράφησης και ο υπολοπέας ως Eve.

Σε αντίθεση λοιπόν, με την κλασσική κρυπτογραφία που βασίζεται πάνω σε ιδιότητες υπολογιστικής πολυπλοκότητας κάποιων συγκεκριμένων μαθηματικών συναρτήσεων, οι οποίες δεν προσφέρουν καμία εγγύηση καθώς εξαρτώνται μεταξύ άλλων και από την υπάρχουσα τεχνολογία, η κβαντική κρυπτογραφία βασίζεται πάνω στα καλά ελεγμένα θεμέλια της κβαντικής μηχανικής.

Η κβαντική κρυπτογραφία έχει δύο βασικές μεθόδους που αντιπροσωπεύονται από δύο βασικά πρωτόκολλα κρυπτογραφίας που έχουν να κάνουν με την διαχείριση του κβαντικού κλειδιού. Αυτές είναι η μέθοδος των πολωμένων φωτονίων και η μέθοδος των πρωτοκόλλων κβαντικής κρυπτογραφίας διεμπλεγμένων φωτονίων.

Η μέθοδος των **πολωμένων φωτονίων** [44] (διατυπώθηκε το 1984, από τους Charles Bennett και Gilles Brassard) χρησιμοποιεί ένα κβαντικό κανάλι για την ανταλλαγή του κλειδιού και ένα κλασσικό κανάλι για την ανταλλαγή της πραγματικής πληροφορίας. Υποθέτουμε ότι ο «ωτακουστής» ή υπολοπέας, ονόματι Eve μπορεί να δει την πληροφορία που αποστέλλεται στα δύο κανάλια. Αρχικά ο αποστολέας ονόματι Alice αποστέλλει στον παραλήπτη ονόματι Bob, μέσω του κβαντικού καναλιού μία αλληλουχία από κωδικοποιημένα qubits, τα οποία είναι κωδικοποιημένα με τυχαία επιλογή βάσης κάθε φορά, και έστω οι κβαντικές καταστάσεις ότι είναι οι $|q_1\rangle = |01\rangle$ και $|q_2\rangle = (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$. Κάθε φωτόνιο που λαμβάνει ο Bob, το μετράει βάσει τυχαίας επιλογής βάσης μεταξύ των $|q_1\rangle$ και $|q_2\rangle$ και κρατεί τα αποτελέσματα των μετρήσεων κρυφά. Μετά την ολοκλήρωση των μετρήσεων, επικοινωνεί με την Alice και στέλνει τις βάσεις δεδομένων που χρησιμοποίησε για να κάνει την κάθε μέτρηση μέσω του κλασσικού καναλιού. Από το ίδιο κανάλι, η Alice του απαντά ποιες από αυτές τις βάσεις ήταν επιλεγμένες σωστά και κρατούν μόνο αυτά τα qubits, για να σχηματίσουν το κλειδί. Έτσι και οι δύο έχουν μια «αλληλουχία» από ισοάριθμα qubits που συμφωνούν ένα προς ένα στις τιμές τους. Βάσει πιθανοτήτων, περίπου τα μισά qubits θα είναι ίσα, δηλαδή οι μισές μετρήσεις θα έχουν γίνει με την σωστή βάση. Αν υποθέσουμε επίσης ότι η Eve υπολέπει ακούγοντας το κβαντικό κανάλι επικοινωνίας, τότε το πλήθος των σωστών qubits που θα βρεί ο Bob θα είναι μικρότερο από το κανονικό. Για την ακρίβεια, όπως και με τον Bob, κάθε μέτρηση που κάνει η Eve έχει 50% πιθανότητα να είναι λάθος. Από τον πολλαπλασιαστικό νόμο των πιθανοτήτων, αυτό σημαίνει ότι ο Bob έχει 25% πιθανότητα να κάνει σωστή μέτρηση για κάθε qubit που υπέκλεψε η Eve. Έτσι, από την κατανομή των σωστών τιμών, η Alice και ο Bob μπορούν να καταλάβουν αν κάποιος τους παρακολουθούσε, αλλά ακόμη και το ποσοστό της πληροφορίας που υπέκλεψε η Eve.

Η δεύτερη μέθοδος καλείται **πρωτόκολλα κβαντικής κρυπτογραφίας διεπλεγμένων σωματιδίων** [44] (ανακαλύφθηκε το 1991, από τον Artur Ekert), χρησιμοποιεί ένα κβαντικό κανάλι για την μετάδοση του δημόσιου κλειδιού και ένα κλασσικό κανάλι για την μεταφορά της πληροφορίας, και τα qubits που στέλνονται μεταξύ της Alice και του Bob είναι αποτελούμενα από φωτόνια (ζεύγη διεμπλεκόμενων φωτονίων) ώστε έκαστος να λαμβάνει ένα φωτόνιο, όπως παρόμοια είδαμε στο σχήμα 9.1. Τα φωτόνια που έχουν η Alice και ο Bob είναι συμπληρωματικά μεταξύ τους σύμφωνα με την πύλη κβαντική πύλη NOT (§ 6.4) και μπορούν έτσι να έχουν ένα κοινό κλειδί, στο οποίο όμως τυχόν αλλοιώσεις στις μετρήσεις τους και τις σχέσεις μεταξύ ακολουθιών qubits θα έχει ως αποτέλεσμα να μην είναι ακριβείας με βάση την πύλη NOT. Με βάση την κβαντική διεπλοκή, η Alice θα έχει πιθανότητα μεγαλύτερη του 50% να πάρει σωστά την ακολουθία του Bob οπότε με βάση τα κλασσικά μοντέλα κρυπτογραφίας θα έχει και μικρότερη πιθανότητα υποκλοπής.

9.3 ΚΒΑΝΤΙΚΟΣ ΜΕΤΑΣΧΗΜΑΤΙΣΜΟΣ FOURIER

Ο κλασσικός διακριτός μετασχηματισμός Fourier (Discrete Fourier Transform – DFT-) δίνεται από την σχέση

$$X(k) = \sum_{n=0}^{N-1} x(n) e^{-j \frac{2\pi}{N} kn} \quad , \text{ με } k=0,1,2,\dots,N-1 \quad 9.1$$

Η αντιστοιχία συμβολίζεται μεταξύ μιας x (π.χ. σήμα πεπερασμένης έκτασης με διάρκεια N) και μιας X (σήμα πεπερασμένης έκτασης) ως εξής:

$$x(n) \xleftrightarrow{\text{DFT}} X(k)$$

Ο κβαντικός μετασχηματισμός Fourier (Quantum Fourier Transform – QFT-) είναι σημαντικός γιατί δρά σε κβαντικούς αλγόριθμους και θα τον συναντήσουμε στον κβαντικό αλγόριθμο του Shor, στην συνέχεια. **Ο QFT είναι ένας τελεστής του χώρου Hilbert και μετασχηματίζει τυχαίες αρχικές βασικές καταστάσεις κβαντικών καταχωρητών.** Επομένως προκαλεί αλληλεπιδράσεις μεταξύ των qubits και των κβαντικών καταχωρητών. Δρα σε μια αρχική κατάσταση, π.χ. την $|a\rangle$ (όπου $|a\rangle = |N-1, N-2, N-3, \dots, 3, 2, 1, 0\rangle$) και δίνει ότι

$$|a\rangle \cdot U_{\text{QFT}} \rightarrow \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} e^{j \frac{2\pi}{N} ab} |b\rangle \quad 9.2$$

— Η δράση του QFT, στην κατάσταση του κβαντικού καταχωρητή $|1\rangle$, ως απλή εφαρμογή, θα είναι

$$|1\rangle \cdot U_{\text{QFT}} \rightarrow \frac{1}{\sqrt{2}} \sum_{b=0}^1 e^{j\frac{2\pi}{N}1b} |b\rangle = \frac{1}{\sqrt{2}} \sum_{b=0}^1 e^{j\frac{2\pi}{2}b} |b\rangle = \frac{1}{\sqrt{2}} (e^0|0\rangle + e^{j\pi}|1\rangle) = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Εάν η αρχική κατάσταση ενός κβαντικού καταχωρητή, είναι υπέρθεση βασικών καταστάσεων $|q\rangle = \sum_{m=0}^{N-1} x_m |c\rangle$, τότε ο QFT θα δράσει στην υπέρθεση και θα δώσει τον μετασχηματισμό

$$|q\rangle \cdot U_{\text{QFT}} \rightarrow \frac{1}{\sqrt{N}} \sum_{m=0}^{N-1} \sum_{b=0}^{N-1} x_m e^{j\frac{2\pi}{N}mb} |b\rangle \quad 9.3$$

Οπότε η σχέση 9.3, με χρήση της 9.1 θα δώσει

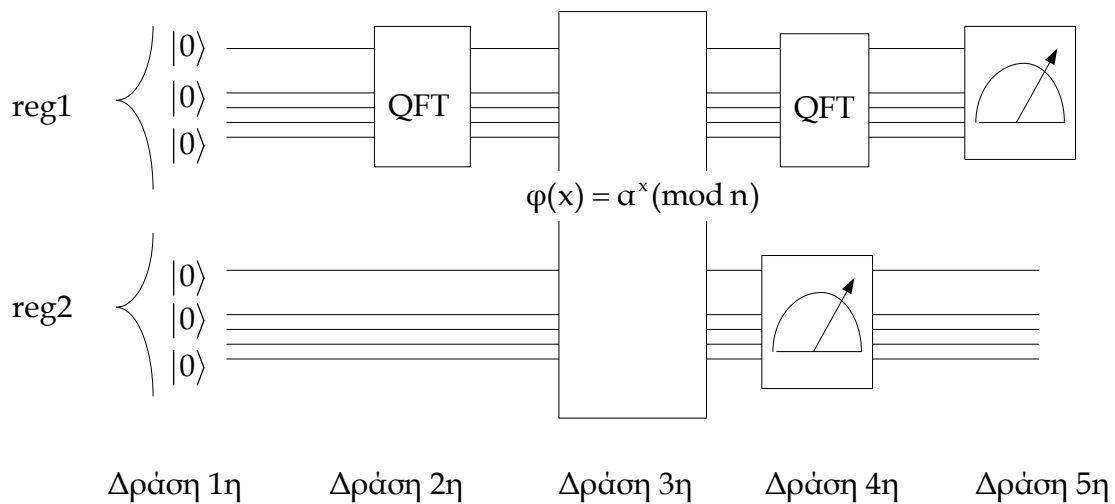
$$|q\rangle \cdot U_{\text{QFT}} \rightarrow \frac{1}{\sqrt{N}} \sum_{b=0}^{N-1} X(b) |b\rangle \quad 9.4$$

9.4 ΚΒΑΝΤΙΚΟΣ ΑΛΓΟΡΙΘΜΟΣ ΤΟΥ SHOR

Εκτός από τις μεθόδους κβαντικής κρυπτογραφίας που προαναφέρθηκαν με χρήση πρωτοκόλλου ανταλλαγής κλειδιού, η επικοινωνία γίνεται μέσω κλειδιού και με την επιλογή ενός αλγορίθμου κρυπτογράφησης (εκτός από την RSA μέθοδο που προαναφέρθηκε και η οποία δεν είναι αποτελεσματική για παραγοντοποίηση μεγάλων πρώτων αριθμών) όπου, είναι δυνατόν να χρησιμοποιήσουμε κβαντικούς αλγορίθμους για να παραγοντοποιήσουμε μεγάλους πρώτους αριθμούς σε πολυωνυμικό χρόνο και αυτό μπορεί να υλοποιηθεί αποτελεσματικά με την χρήση του αλγόριθμου του Shor. Ο αλγόριθμος (που διατυπώθηκε από τον Shor το 1994) εκτελεί μια αναγωγή του προβλήματος της παραγοντοποίησης στο πρόβλημα εύρεσης μια ρουτίνας περιόδου της συνάρτησης $\varphi(x) = a^x \pmod{n}$ (όπου a τυχαίος ακέραιος αριθμός πρώτος ως προς τον n αριθμό) και έπειτα επιλύεται το πρόβλημα με έναν κβαντικό αλγόριθμο (συνήθως χρήση του κβαντικού μετασχηματισμού Fourier).

Η δομή [1, 8, 44] του αλγορίθμου του Shor αφορά την εύρεση της περιόδου τ της συνάρτησης $\varphi(x) = a^x \pmod{n}$. Μπορούμε με χρήση του αλγορίθμου να αναλύσουμε έναν αριθμό σε γινόμενο δύο πρώτων αριθμών, να υπολογίσουμε την περίοδο μιας συνάρτησης και γενικά να κάνουμε ότι υλοποιείται με έναν κλασσικό

αλγόριθμο αλλά σε πολύ μικρότερο χρόνο επίλυσης του προβλήματος, όταν αυτό είναι αδύνατον να γίνει σε εύλογο χρονικό διάστημα καθώς σε κλασσικούς υπολογιστές η ανάλυση ενός μεγάλου αριθμού με πολλά ψηφία μπορεί να κρατήσει και πάνω από 100 χρόνια. Στο επόμενο κύκλωμα φαίνεται η δομή του κβαντικού αλγορίθμου του Shor.



Σχήμα 9.2

Για την επίλυσή του ακολουθούμε κάποια βήματα δράσεων, όπως φαίνεται στο σχήμα. Ο κβαντικός καταχωρητής αποτελείται από δύο επιμέρους καταχωρητές τους reg1 και reg2, οι οποίοι βρίσκονται σε κβαντική διεμπλοκή. **Ακολουθούμε λοιπόν τα βήματα των εξής 5 δράσεων :**

- Κατ' αρχήν επιλέγουμε έναν ακέραιο αριθμό Q για τον οποίο ισχύει ότι $n^2 \leq Q \leq 2n^2$, με $Q=s^2$, όπου το s είναι ανάλογο της $s = 2\log_2 n$. Στην συνέχεια επιλέγουμε έναν ακέραιο αριθμό a , ο οποίος είναι πρώτος ως προς τον n και για τον οποίο ισχύει $1 < a < n-1$. Επίσης θα είναι ο $\text{ΜΚΔ}(a,n)=1$. Οι δύο κβαντικοί καταχωρητές reg1 και reg2 βρίσκονται στην κατάσταση $|0\rangle$. Η κατάσταση του κβαντικού καταχωρητή που αποτελείται από τους reg 1, reg2 θα είναι $|\psi\rangle = |\psi_1\rangle |\psi_2\rangle = |0\rangle |0\rangle$.

- Στην συνέχεια αρχικοποιούμε μια ακολουθία από qubits που είναι η προκύπτουσα κβαντική κατάσταση επαλληλίας των καταστάσεων του reg1, η $|\psi\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |0\rangle$.

Δεν γίνεται δράση στον reg2 όπως αποτυπώνεται και στο σχήμα, το οποίο περιλαμβάνει μια πύλη δράσης κβαντικού μετασχηματιστή Fourier και η οποία

ισοδύναμα μπορεί να αντικατασταθεί από ένα μετασχηματισμό μιας σειράς πυλών Hadamard για κάθε μια από τις $|0\rangle$, καταλήγοντας στο ίδιο αποτέλεσμα δράσης $|\psi\rangle$ στον reg1 .

- Στην συνέχεια λόγω της δράσης της $\varphi(x)=a^x \pmod n$ στην κατάσταση του καταχωρητή reg2 , προκύπτει το αποτέλεσμα που μετράται από τον μετρητή της προκύπτουσας κατάστασης (λόγω υπέρθεσης των $\varphi(x)$), που θα είναι η $|\psi\rangle = Q^{-0,5} \sum_{x=0}^{Q-1} |x\rangle |\varphi(x)\rangle$. Επισημαίνεται ότι οι δύο καταχωρητές reg1 , reg2 βρίσκονται σε κατάσταση κβαντικής διεμπλοκής, δηλαδή η μέτρηση της κατάστασης του reg2 επηρεάζει την κατάσταση του reg1 η οποία είναι η $|\psi\rangle = (Q')^{-\frac{1}{2}} \sum_{x=0}^{Q'-1} |x'\rangle |\varphi(x')\rangle$.

- Δρά έπειτα ο μετασχηματισμός QFT (σχέση 9.4, $|a\rangle \cdot U_{\text{QFT}} \rightarrow \frac{1}{N} \sum_{b=0}^{N-1} e^{j\frac{2\pi}{N}ab} |b\rangle$) στον reg1 και προκύπτει η νέα κατάσταση του κβαντικού καταχωρητή που θα δίνεται από την σχέση (λόγω νέας υπέρθεσης)

$$|\psi\rangle = \frac{1}{\sqrt{Q}} \sum_{b=0}^{N-1} e^{j\frac{2\pi}{Q}xb} |b\rangle \frac{1}{\sqrt{Q'}} \sum_{x=0}^{Q'-1} |x'\rangle |\varphi(x')\rangle \quad \text{ή}$$

$$|\psi\rangle = \frac{1}{\sqrt{QQ'}} \sum_b e^{j\frac{2\pi}{Q}xb} |b\rangle \sum_{x'} |x'\rangle |\varphi(x')\rangle .$$

- Προκύπτει αποτέλεσμα την πιθανότητα του οποίου μετράμε και τελικά η τιμή της περιόδου τ θα είναι ανάλογη της μέτρησης M , $\tau \approx Q/M$. Επίσης μπορεί να υπάρξει επανάληψη των βημάτων η οποία είναι ανάλογη του $\log_2(Q)$. Με γνωστή την περίοδο υπολογίζεται ο ΜΚΔ($a^{\tau/2}+1, n$) και ο ΜΚΔ($a^{\tau/2}-1, n$), από την προκύπτουσα τιμή των οποίων προσδιορίζεται η παραγοντοποίηση και το γινόμενο των δύο πρώτων αριθμών που δίνει την ανάλυση ενός αριθμού.

■ Παράδειγμα παραγοντοποίησης με τον αλγόριθμο του Shor :

Θα αναλυθεί ο αριθμός 15 σε γινόμενο δύο πρώτων αριθμών με την δράση του αλγόριθμου του Shor .

- Καταρχήν επιλέγουμε τυχαία τον αριθμό $Q=16$ και η οποία είναι μεταξύ των $n^2 \leq Q \leq 2n^2$ ή με $n=15$, $15^2 \leq Q \leq 215^2 \Rightarrow 225 \leq Q \leq 450$, με $\text{ΜΚΔ}(16,15)=1$. Στην συνέχεια επιλέγουμε τον αριθμό $a=7$, και είναι $\text{ΜΚΔ}(7,15)=1$.

- Έπειτα στον καταχωρητή reg1 θα έχουμε $\log_2 16 = \log_2 2^4 = 4$ qubits. Επίσης ο καταχωρητής reg2 (θα κρατά τις τιμές) θα αποτελείται από 4 qubits. Η κατάσταση του καταχωρητή θα είναι

$$|\psi\rangle = Q^{-0.5} \sum_{x=0}^{Q-1} |x\rangle |\varphi(x)\rangle \Rightarrow |\psi\rangle = 16^{-\frac{1}{2}} \sum_{x=0}^{15} |x\rangle |\varphi(x)\rangle \Rightarrow |\psi\rangle = \frac{1}{4} \sum_{x=0}^{15} |0\dots 0, x\rangle \Rightarrow$$

$$|\psi\rangle = \frac{1}{4} (|0,0\rangle + |1,0\rangle + |2,0\rangle + |3,0\rangle + |4,0\rangle + |5,0\rangle + \dots + |14,0\rangle + |15,0\rangle)$$

- Η συνάρτηση $\varphi(x) = x^7 \pmod{15}$, θα είναι ίση με $\varphi(x) = 7^x \pmod{15}$ (με $x=0,1,2,\dots,15$). Τότε η κατάσταση του καταχωρητή λόγω κβαντικής διεμπλοκής των reg1, reg2 θα γίνει

$$|\psi\rangle = Q^{-0.5} \sum_{x=0}^{Q-1} |x\rangle |\varphi(x)\rangle \Rightarrow$$

$$|\psi\rangle = \frac{1}{4} \sum_{x=0}^{15} |x, \varphi(x)\rangle = \frac{1}{4} (|0, \varphi(0)\rangle + |1, \varphi(1)\rangle + |2, \varphi(2)\rangle + \dots + |15, \varphi(15)\rangle) \Rightarrow$$

$$|\psi\rangle = \frac{1}{4} (|0,1\rangle + |1,7\rangle + |2,4\rangle + |3,13\rangle + |5,7\rangle + |6,4\rangle + |7,13\rangle + |8,1\rangle +$$

$$+ |9,7\rangle + |10,4\rangle + |11,13\rangle + |12,1\rangle + |13,7\rangle + |14,4\rangle + |15,13\rangle)$$

- Η κατάσταση του reg2 (έστω η $|1\rangle$) επηρεάζει την κατάσταση του reg1 λόγω κβαντικής διεμπλοκής και θα βρίσκονται μόνο οι αριθμοί x' για τους οποίους ισχύει ότι $\varphi(x)=1$, δηλαδή οι $x'=0, 4, 8, 12$. Οπότε η κατάσταση του κβαντικού καταχωρητή θα είναι η

$$|\psi\rangle = (4)^{-\frac{1}{2}} \sum_{x=0}^{Q'-1} |x'\rangle |\varphi(x')\rangle \Rightarrow |\psi\rangle = \frac{1}{\sqrt{4}} \sum_{x'} |x'\rangle |\varphi(x')\rangle \Rightarrow |\psi\rangle = \frac{1}{2} (|0,1\rangle + |4,1\rangle + |8,1\rangle + |12,1\rangle)$$

- Στην συνέχεια δρά ο QFT στον reg1 (αναλλοίωτος ο reg2) και η κατάσταση γίνεται

$$|\psi\rangle = \frac{1}{\sqrt{QQ'}} \sum_{x'} e^{j\frac{2\pi}{Q} x'b} |b\rangle \sum_{x=0}^{Q'-1} |x'\rangle |\varphi(x')\rangle \Rightarrow |\psi\rangle = \frac{1}{2} \frac{1}{\sqrt{16}} \sum_{x'} e^{j\frac{2\pi}{16} x'b} |b\rangle \sum_{x=0}^{16'-1} |x', \varphi(x')\rangle \Rightarrow$$

$$|\psi\rangle = \frac{1}{2} \frac{1}{4} \sum_{b=0}^{15} \sum_{x'} e^{j\frac{2\pi}{16} x'b} |b,1\rangle \Rightarrow |\psi\rangle = \frac{1}{8} \sum_{b=0}^{15} \sum_{x'} e^{j\frac{2\pi}{16} x'b} |b,1\rangle \Rightarrow$$

$$\begin{cases} x'=0 \\ x'=4 \\ x'=8 \\ x'=12 \end{cases}$$

$$\begin{aligned}
|\psi\rangle = & \frac{1}{8} (|0,1\rangle + |1,1\rangle + |2,1\rangle + |3,1\rangle + |4,1\rangle + |5,1\rangle + |6,1\rangle + |7,1\rangle + |8,1\rangle + |9,1\rangle + \\
& |10,1\rangle + |11,1\rangle + |12,1\rangle + |13,1\rangle + |14,1\rangle + |15,1\rangle + \\
& + |0,1\rangle + e^{j\frac{\pi}{2}} |1,1\rangle + e^{j\pi} |2,1\rangle + e^{j\frac{3\pi}{2}} |3,1\rangle + e^{j2\pi} |4,1\rangle + e^{j\frac{5\pi}{2}} |5,1\rangle + e^{j3\pi} |6,1\rangle + e^{j\frac{7\pi}{2}} |7,1\rangle + e^{j4\pi} |8,1\rangle + e^{j\frac{9\pi}{2}} |9,1\rangle + \\
& e^{j10\pi} |10,1\rangle + e^{j\frac{11\pi}{2}} |11,1\rangle + e^{j12\pi} |12,1\rangle + e^{j\frac{13\pi}{2}} |13,1\rangle + e^{j7\pi} |14,1\rangle + e^{j\frac{15\pi}{2}} |15,1\rangle + \\
& + |0,1\rangle + e^{j\pi} |1,1\rangle + e^{j2\pi} |2,1\rangle + e^{j3\pi} |3,1\rangle + e^{j4\pi} |4,1\rangle + e^{j5\pi} |5,1\rangle + e^{j6\pi} |6,1\rangle + e^{j7\pi} |7,1\rangle + e^{j8\pi} |8,1\rangle + e^{j9\pi} |9,1\rangle + \\
& e^{j10\pi} |10,1\rangle + e^{j11\pi} |11,1\rangle + e^{j12\pi} |12,1\rangle + e^{j13\pi} |13,1\rangle + e^{j14\pi} |14,1\rangle + e^{j15\pi} |15,1\rangle + \\
& + |0,1\rangle + e^{j\frac{3\pi}{2}} |1,1\rangle + e^{j3\pi} |2,1\rangle + e^{j\frac{9\pi}{2}} |3,1\rangle + e^{j6\pi} |4,1\rangle + e^{j\frac{15\pi}{2}} |5,1\rangle + e^{j\frac{18\pi}{2}} |6,1\rangle + e^{j21\frac{\pi}{2}} |7,1\rangle + e^{j12\pi} |8,1\rangle + e^{j\frac{27\pi}{2}} |9,1\rangle + \\
& e^{j15\pi} |10,1\rangle + e^{j\frac{33\pi}{2}} |11,1\rangle + e^{j18\pi} |12,1\rangle + e^{j\frac{39\pi}{2}} |13,1\rangle + e^{j21\pi} |14,1\rangle + e^{j\frac{44\pi}{2}} |15,1\rangle)
\end{aligned}$$

Παρατηρούμε με προσοχή πως από την πιο πάνω κατάσταση μόνο οι καταστάσεις $|0,1\rangle, |4,1\rangle, |8,1\rangle, |12,1\rangle$ δεν επηρεάζονται από συμβολές καταστάσεων μεταξύ των πλατών πιθανότητας που έχουν η κάθε μια από όλες τις προηγούμενες, ώστε να μένουν ανέπαφες. Δηλαδή η κατάσταση θα είναι τελικά η

$$\begin{aligned}
|\psi\rangle = & \frac{1}{8} [(|0,1\rangle + |0,1\rangle + |0,1\rangle + |0,1\rangle) + (|4,1\rangle + e^{j2\pi} |4,1\rangle + e^{j4\pi} |4,1\rangle + e^{j6\pi} |4,1\rangle) + \\
& (|8,1\rangle + e^{j4\pi} |8,1\rangle + e^{j8\pi} |8,1\rangle + e^{j12\pi} |8,1\rangle) + (|12,1\rangle + e^{j12\pi} |12,1\rangle + e^{j12\pi} |12,1\rangle + e^{j18\pi} |12,1\rangle)]
\end{aligned}$$

Επομένως θα επαναλάβουμε 4 φορές την μέτρηση των προηγούμενων δράσεων καθότι με $Q=16$, είναι $\log_2 16 = \log_2 2^4 = 4$, οπότε η περίοδος της συνάρτησης $\varphi(x)$ θα είναι $\tau \approx Q/M \approx 16/4 = 4$. Άρα $\tau=4$.

Με γνωστή την περίοδο υπολογίζεται ο $MKD(\alpha^{\tau/2} + 1, n)$ και ο $MKD(\alpha^{\tau/2} - 1, n)$, από την προκύπτουσα τιμή των οποίων προσδιορίζεται το γινόμενο των δύο πρώτων αριθμών, θα είναι δηλαδή

$$MKD(\alpha^{\tau/2} + 1, n) = MKD(7^2 + 1, 15) = MKD(48, 15) = 3 \quad \text{και}$$

$$MKD(\alpha^{\tau/2} - 1, n) = MKD(7^2 - 1, 15) = MKD(50, 15) = 5$$

Τελικά θα είναι $5 \cdot 3 = 15$.

► Παρατήρηση

Θα λύσουμε το ίδιο πρόβλημα με την χρήση ενός κλασσικού τρόπου που εκτελεί ένας συμβατικός υπολογιστής, σύμφωνα με το παράδειγμα που αναλύθηκε στην §9.1. Έχουμε λοιπόν, προκειμένου να αναλύσουμε το 15 σε γινόμενο δύο πρώτων αριθμών και να βρούμε την περίοδο του τα εξής βήματα δράσεων.

Επιλέγουμε καταρχήν τυχαίο αριθμό $a=2$ με $\text{ΜΚΔ}(2,15)=1$. Η περιοδική συνάρτηση $\phi(x)=a^x(\text{mod } x)$, θα δώσει

$$\Phi(0)=2^0(\text{mod } 15)=1$$

$$\Phi(1)=2^1(\text{mod } 15)=2$$

$$\Phi(2)=2^2(\text{mod } 15)=4(\text{mod } 15)=4$$

$$\Phi(3)=2^3(\text{mod } 15)=8(\text{mod } 15)=8$$

$$\Phi(4)=2^4(\text{mod } 15)=16(\text{mod } 15)=1$$

$$\Phi(5)=2^5(\text{mod } 15)=32(\text{mod } 15)=2$$

$$\Phi(6)=2^6(\text{mod } 15)=64(\text{mod } 15)=4$$

$$\Phi(7)=2^7(\text{mod } 15)=128(\text{mod } 15)=8$$

$$\Phi(8)=2^8(\text{mod } 15)=256(\text{mod } 15)=1$$

$$\Phi(9)=2^9(\text{mod } 15)=512(\text{mod } 15)=2 \text{ κ.ο.κ}$$

Παρατηρούμε λοιπόν πως η συνάρτηση έχει περίοδο $\tau=4$. Οπότε ο $\text{ΜΚΔ}(a^{\tau/2} + 1, n)$ και ο $\text{ΜΚΔ}(a^{\tau/2} - 1, n)$ θα είναι:

$$\text{ΜΚΔ}(2^{4/2} + 1, 15) = \text{ΜΚΔ}(5, 15) = 5 \text{ και ο } \text{ΜΚΔ}(2^{4/2} - 1, 15) = \text{ΜΚΔ}(3, 15) = 3.$$

Τελικά οι δύο πρώτοι αριθμοί είναι οι $5 \cdot 3 = 15$.

Κατά την σύγκριση της δράσης του κβαντικού αλγορίθμου του Shor με αυτή του κλασσικού τρόπου υπολογισμού (κρυπτογραφικό σύστημα της RSA όπως αναφέρθηκε στην §9.1), παρατηρούμε πως στον κλασσικό τρόπο δράσης είναι εύκολο να βρούμε το γινόμενο δύο πρώτων αριθμών ενός μικρού αριθμού, αλλά για τριψήφιο ακέραιο (ή πόσο μάλλον μεγαλύτερο 4 και 5 ψηφίων) είναι υπερβολικά δύσκολο να γίνει η ανάλυση, καθώς απαιτείται ένα σύστημα υπολογιστικών δικτύων με χιλιάδες ή και εκατοντάδες υπολογιστές προκειμένου μετά από δεκαετίες (ή και πολύ περισσότερο) να βρεθεί η λύση. Αυτό το πρόβλημα με την χρήση των

κβαντικών υπολογιστών και του αλγορίθμου που μόλις αναπτύχθηκε μπορεί να παραγκωνιστεί και έτσι ελπίζουμε ότι με τις έρευνες που γίνονται εντατικά τα τελευταία χρόνια, να έχει ανοίξει ένα πεδίο ταχύτατων υπολογισμών που προστατεύει αποτελεσματικά κάθε σύστημα.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η έρευνα και τα αποτελέσματα που έχουν γίνει στον τομέα ανάπτυξης των κβαντικών υπολογιστών είναι ιδιαίτερα αξιοσημείωτα και τα τελευταία χρόνια ιδίως, παρατηρούνται επιτεύγματα πολύ ελπιδοφόρα (όπως το βραβείο νόμπελ του 2012) . Η εδραίωση και η αξιοποίηση των κβαντικών υπολογιστών είναι πιο κοντά από ποτέ.

Οι κβαντικοί υπολογιστές προς το παρόν δεν προσφέρουν λύσεις για κάθε υπολογιστική διεργασία (όπως επεξεργασία κειμένου ή φωτογραφίας). Στο άμεσο μέλλον, μάλλον θα πρέπει γίνει, μια «υβριδική» χρήση κβαντικών και κλασσικών υπολογιστών ώστε για εφαρμογές απλών διαδικασιών να γίνεται αξιοποίηση των κλασσικών υπολογιστών ενώ για υπολογισμό μεγάλων δεδομένων ή για απόλυτη προστασία δεδομένων από κακόβουλες επιθέσεις να χρησιμοποιούνται οι κβαντικοί υπολογιστές.

Υπάρχουν διάφορες τεχνολογίες για την υλοποίηση κβαντικών υπολογιστών οι κυριότερες εκ των οποίων αναπτύχθηκαν στην μεταπτυχιακή εργασία και έχουν αξιοποιηθεί για την κατασκευή τους από εταιρείες κολοσσούς στον κλάδο των υπολογιστών (όπως η IBM η οποία στα τέλη του περασμένου αιώνα παρουσίασε έναν κβαντικό υπολογιστή 2, 3, 5, και 7 qubits με δυνατότητα κβαντικής διόρθωσης σφαλμάτων). Επίσης σημαντικό γεγονός είναι η αγορά από την εταιρεία Lockheed Martin (δραστηριοποιείται σε έρευνα και προμήθεια υλικών σε τομείς υψηλών τεχνολογιών όπως αεροδιαστημική) του πρώτου κβαντικού υπολογιστή που τον εμπορεύτηκε η Καναδική εταιρία D-Wave Ins.

Όλες οι ενδείξεις οδηγούν στον δρόμο της κβαντικής εποχής για τους υπολογιστές. Αναμένεται να προσφέρουν ώθηση σε κάθε τεχνολογία αιχμής σε ένα ευρύ φάσμα επιστημών όπως της φυσικής, της πληροφορικής, της βιολογίας, της ιατρικής κ.α.. Προς το παρόν, και μέχρι να οδηγηθεί η κατασκευή των κβαντικών υπολογιστών σε επίπεδο πληρότητας, η επιστημονική και κοινή γνώμη θα είναι σε εγρήγορση και σε αναμονή τυχόν σημαντικών εξελίξεων στην παραγωγή την διακίνηση και χρήση των κβαντικών υπολογιστών.

*«Everything should be made as simple as possible,
but not simpler»*
Albert Einstein

ΠΑΡΑΡΤΗΜΑ Α΄

ΜΑΘΗΜΑΤΙΚΑ ΕΡΓΑΛΕΙΑ

1. ΠΡΟΘΕΜΑΤΑ ΜΟΝΑΔΩΝ ΣΤΟ S.I.

ΠΟΛΛΑΠΛΑΣΙΑ		ΥΠΟΠΟΛΛΑΠΛΑΣΙΑ	
Deka	1da = 10^1	Deci	1d = 10^{-1}
Hecto	1h = 10^2	Centi	1c = 10^{-2}
Kilo	1K = 10^3	Mili	1m = 10^{-3}
Mega	1M = 10^6	Micro	1μ = 10^{-6}
Giga	1G = 10^9	Nano	1n = 10^{-9}
Tera	1T = 10^{12}	Pico	1p = 10^{-12}
Peta	1P = 10^{15}	Femto	1f = 10^{-15}
Exa	1E = 10^{18}	Atto	1a = 10^{-18}
Zetta	1Z = 10^{21}	Zepto	1z = 10^{-21}

2. ΑΛΓΕΒΡΑ ΠΙΝΑΚΩΝ

— Μια διάταξη $m \times n$ το πλήθος αριθμών σε μορφή ορθογωνίου σχήματος με m γραμμές και n στήλες λέγεται **πίνακας** τύπου $m \times n$. Ο πίνακας θα συμβολίζεται με

$$A_{m \times n} = \begin{bmatrix} A_{11} & A_{12} & A_{13} & \dots & A_{1n} \\ A_{21} & A_{22} & A_{23} & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ A_{m1} & A_{m2} & \dots & \dots & A_{mn} \end{bmatrix}$$

— **Άθροισμα** δύο $m \times n$ πινάκων A και B λέγεται ο $m \times n$ πίνακας του οποίου κάθε στοιχείο είναι το άθροισμα των αντιστοιχών στοιχείων των A και B . Ο πίνακας αυτός συμβολίζεται με $A+B$.

Ιδιότητες πρόσθεσης πινάκων:

- $A+B=B+A$
- $A+(B+Γ)=(A+B)+Γ$
- $A+O=O+A=A$
- $A+(-A)=(-A)+A=O$
- $A-B=A+(-B)$

— **Γινόμενο** ενός πραγματικού αριθμού κ με ένα πίνακα A , καλείται ο πίνακας που προκύπτει αν πολλαπλασιάσουμε κάθε στοιχείο με του πίνακα A με το κ , δηλαδή $\kappa \cdot A$.

Ιδιότητες πολλαπλασιασμού αριθμού με πίνακα

- $(\kappa+\lambda)A=\kappa A+\lambda A$
- $\kappa(A+B)=\kappa A+\kappa B$
- $\kappa(\lambda A)=(\kappa\lambda)A$
- $1 A=A$

— Έστω A $m \times n$ πίνακας και B ένας $n \times r$ πίνακας, τότε ορίζουμε ως **γινόμενο** του πίνακα A με τον πίνακα B και το συμβολίζουμε με AB $m \times r$ πίνακα του οποίου κάθε στοιχείο είναι το άθροισμα των γινομένων των n στοιχείων της $i=1,2,\dots,m$ γραμμής του A πίνακα με τα αντίστοιχα n στοιχεία του $j=1,2,\dots,r$ στήλης του πίνακα B .

Ιδιότητες πολλαπλασιασμού πινάκων

- $A(BΓ)=(AB)Γ$
- $A(A+Γ)=AB+AΓ$
- $(B+Γ)A=BA+ΓA$
- $(\kappa A)(\lambda B)=(\kappa\lambda)AB$

— **Αντιστρέψιμοι πίνακες:** Έστω πίνακας τετραγωνικός τύπου $n \times n$. Αν υπάρχει ένας τετραγωνικός πίνακας τύπου Υ $n \times n$ τέτοιος ώστε να ισχύει $A\Upsilon=I=\Upsilon A$, τότε ο πίνακας A λέγεται αντιστρέψιμος πίνακας και ο Υ λέγεται αντίστροφος του A .

— Αν ένας τετραγωνικός πίνακας A είναι **αντιστρέψιμος**, τότε ο αντίστροφός του είναι **μοναδικός**. Ισχύει η κεντρική ιδιότητα:

$$A \cdot A^{-1}=A^{-1} \cdot A=I$$

— Τανυστικό γινόμενο δύο πινάκων $A \otimes B$ διαστάσεων 2×2 ο καθένας, με

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \text{ και } B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix}$$

θα είναι

$$A \otimes B = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix} \otimes \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix} = \begin{bmatrix} A_{11}B_{11} & A_{11}B_{12} & A_{12}B_{11} & A_{12}B_{12} \\ A_{11}B_{21} & A_{11}B_{22} & A_{12}B_{21} & A_{12}B_{22} \\ A_{21}B_{11} & A_{21}B_{12} & A_{22}B_{11} & A_{22}B_{12} \\ A_{21}B_{21} & A_{21}B_{22} & A_{22}B_{21} & A_{22}B_{22} \end{bmatrix}$$

— **Ανάστροφος πίνακας** είναι ο πίνακας ο οποίος έχει την πρώτη γραμμή ίδια με την πρώτη στήλη του κανονικού πίνακα, την δεύτερη γραμμή ίδια με την δεύτερη στήλη κ.ο.κ. Θα ισχύει λοιπόν ότι εάν ο κανονικός πίνακας είναι ο A (μηκ διαστάσεων)

$$A = \begin{bmatrix} A_{11} & A_{12} & A_{13} & \dots & A_{1n} \\ A_{21} & A_{22} & A_{23} & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ A_{m1} & A_{m2} & \dots & \dots & A_{mn} \end{bmatrix}$$

τότε ο ανάστροφος πίνακας θα είναι ο

$$A^T = \begin{bmatrix} A_{11} & A_{21} & A_{31} & \dots & A_{m1} \\ A_{12} & A_{22} & \dots & \dots & A_{m2} \\ A_{13} & A_{23} & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & \dots & A_{nm} \end{bmatrix}$$

3. ΜΙΓΑΔΙΚΟΙ ΑΡΙΘΜΟΙ

— Μιγαδικός αριθμός με $i^2 = -1$: $Z = x + yi$

— Πραγματικό μέρος του Z : $x = \text{Re}(z)$

— Φανταστικό μέρος του Z : $y = \text{Im}(z)$

— Συζυγής μιγαδικός

$$Z^* : Z^* = (x + yi)^* = (x - yi)(x + yi) = 1$$

— Μέτρο μιγαδικού αριθμού: $|Z| = \sqrt{x^2 + y^2} = |Z^*|$

— Η εκθετική και πολική μορφή του μιγαδικού με $\begin{cases} x = r \cos \phi, \\ y = r \sin \phi, \end{cases}$ είναι

$$Z = x + yi = r(\cos \phi + i \sin \phi) = r e^{i\phi} = \sqrt{x^2 + y^2} e^{i\phi}$$

— Η γωνία του μιγαδικού είναι $\phi = \arctan \frac{y}{x}$

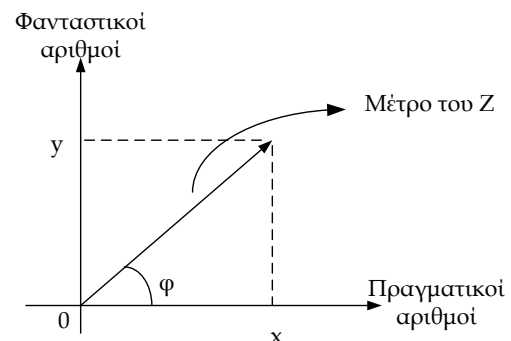
— Ο μιγαδικός αριθμός έχει τις εξής μορφές:

Τριγωνομετρική $Z = |z|(\cos \phi + i \sin \phi)$

Καρτεσιανή $Z = x + yi$

Εκθετική $Z = |z|e^{i\phi}$

Πολική $Z = |z| \angle \phi$



— Τύπος του Euler: $\cos \phi + i \sin \phi = e^{i\phi}$, όπου είναι $\cos \phi = \frac{e^{i\phi} + e^{-i\phi}}{2}$ και $\sin \phi = \frac{e^{i\phi} - e^{-i\phi}}{2i}$

— Αν $z_1 = r_1(\cos \theta_1 + i \sin \theta_1)$ και $z_2 = r_2(\cos \theta_2 + i \sin \theta_2)$ τότε ισχύουν οι πράξεις:

$$z_1 z_2 = r_1 r_2 \cos(\theta_1 + \theta_2) + i r_1 r_2 \sin(\theta_1 + \theta_2) \text{ και } \frac{z_1}{z_2} = \frac{r_1}{r_2} (\cos(\theta_1 - \theta_2) + i \sin(\theta_1 - \theta_2)).$$

4. ΔΙΑΝΥΣΜΑΤΑ

— Το μέτρο [2] ενός διανύσματος $\vec{A} = (A_x, A_y, A_z)$ είναι $A = \|\vec{A}\| = \sqrt{A_x^2 + A_y^2 + A_z^2}$

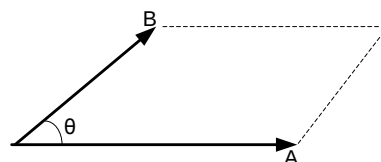
— Για τα μοναδιαία διανύσματα $\vec{i}, \vec{j}, \vec{k}$ που είναι κάθετα το ένα με το άλλο κατά τις διευθύνσεις x, y, z , ισχύουν τα εξής [2]:

$$\vec{i}\vec{i} = \vec{j}\vec{j} = \vec{k}\vec{k} = 1 \text{ και } \vec{i}\vec{j} = \vec{j}\vec{k} = \vec{i}\vec{k} = 0$$

$$\vec{i}\vec{x}\vec{i} = \vec{j}\vec{x}\vec{j} = \vec{k}\vec{x}\vec{k} = 0, \vec{i}\vec{x}\vec{j} = -\vec{j}\vec{x}\vec{i} = \vec{k}, \vec{j}\vec{x}\vec{k} = -\vec{k}\vec{x}\vec{j} = \vec{i} \text{ και } \vec{k}\vec{x}\vec{i} = -\vec{i}\vec{x}\vec{k} = \vec{j}$$

— Το εσωτερικό γινόμενο [2] διανυσμάτων $\vec{A}\vec{B}$ με $\vec{A} = (A_x, A_y, A_z)$ και $\vec{B} = (B_x, B_y, B_z)$ είναι:

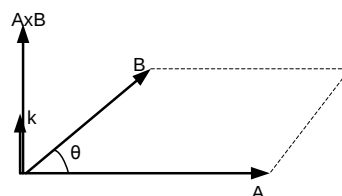
$$\vec{A}\vec{B} = A_x B_x + A_y B_y + A_z B_z = \|\vec{A}\| \|\vec{B}\| \cos \theta$$



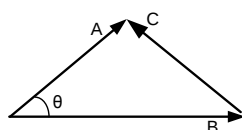
— Το εξωτερικό γινόμενο [2] διανυσμάτων $\vec{A} \times \vec{B}$ με $\vec{A} = (A_x, A_y, A_z)$ και $\vec{B} = (B_x, B_y, B_z)$ είναι:

$$\vec{A} \times \vec{B} = \begin{vmatrix} \vec{x} & \vec{y} & \vec{z} \\ A_x & A_y & A_z \\ B_x & B_y & B_z \end{vmatrix} = (A_y B_z - A_z B_y) \vec{x} - (A_x B_z - A_z B_x) \vec{y} + (A_x B_y - A_y B_x) \vec{z}$$

$$\text{ή } \vec{A} \times \vec{B} = \|\vec{A}\| \|\vec{B}\| \sin \theta \vec{k}$$



— Ο νόμος των συνημίτονων [2] είναι $C^2 = A^2 + B^2 - 2AB \cos \theta$



5. ΔΙΑΝΥΣΜΑΤΙΚΕΣ ΠΑΡΑΓΩΓΟΙ

I/

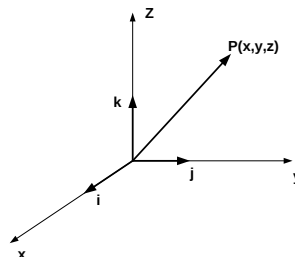
ΚΑΡΤΕΣΙΑΝΕΣ ΣΥΝΤΕΤΑΓΜΕΝΕΣ (x,y,z) [2]

Διάνυσμα θέσης $\vec{r} = x\vec{i} + y\vec{j} + z\vec{k}$

Μήκος $dl = dx\vec{i} + dy\vec{j} + dz\vec{k}$

Όγκος $dV = dxdydz$

Επιφάνεια $dA = dxdy$



Κλίση	$\vec{\nabla}f = \left(\frac{\partial}{\partial x}\vec{i} + \frac{\partial}{\partial y}\vec{j} + \frac{\partial}{\partial z}\vec{k}\right)f = \frac{\partial f}{\partial x}\vec{i} + \frac{\partial f}{\partial y}\vec{j} + \frac{\partial f}{\partial z}\vec{k}$
Απόκλιση	$\text{div}\vec{A} = \vec{\nabla}\cdot\vec{A} = \left(\frac{\partial}{\partial x}\vec{i} + \frac{\partial}{\partial y}\vec{j} + \frac{\partial}{\partial z}\vec{k}\right)(A_x\vec{i} + A_y\vec{j} + A_z\vec{k}) = \frac{\partial A_x}{\partial x} + \frac{\partial A_y}{\partial y} + \frac{\partial A_z}{\partial z}$
Στροβιλισμός	$\text{rot}\vec{A} = \vec{\nabla} \times \vec{A} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ \frac{\partial}{\partial x} & \frac{\partial}{\partial y} & \frac{\partial}{\partial z} \\ A_x & A_y & A_z \end{vmatrix} = \left(\frac{\partial A_z}{\partial y} - \frac{\partial A_y}{\partial z}\right)\vec{i} + \left(\frac{\partial A_x}{\partial z} - \frac{\partial A_z}{\partial x}\right)\vec{j} + \left(\frac{\partial A_y}{\partial x} - \frac{\partial A_x}{\partial y}\right)\vec{k}$

II/

ΣΕ ΣΦΑΙΡΙΚΕΣ ΣΥΝΤΕΤΑΓΜΕΝΕΣ (r,θ,φ) [2]

Διάνυσμα θέσης $\vec{r} = r \sin\theta \cos\phi\vec{i} + r \sin\theta \sin\phi\vec{j} + r \cos\theta\vec{k}$

Μήκος $dl = dr\vec{r} + r d\theta\vec{\theta} + r \sin\theta d\phi\vec{\phi}$

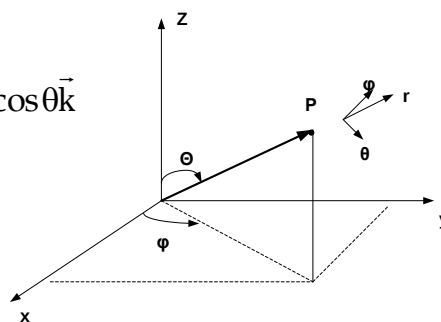
Όγκος $dV = r^2 \sin\theta dr d\theta d\phi$

Επιφάνεια $dA = r^2 \sin\theta d\theta d\phi$

Σχέση με καρτεσιανές συντεταγμένες

$\{x = r \sin\theta \cos\phi, y = r \sin\theta \sin\phi, z = r \cos\theta\}$

όπου $0 \leq r < \infty, 0 \leq \theta \leq \pi, 0 \leq \phi \leq 2\pi$



Κλίση	$\vec{\nabla}f = \frac{\partial f}{\partial r} \vec{r} + \frac{1}{r} \frac{\partial f}{\partial \theta} \vec{\theta} + \frac{1}{r \sin \theta} \frac{\partial f}{\partial \phi} \vec{\phi}$
Απόκλιση	$\text{div} \vec{A} = \vec{\nabla} \cdot \vec{A} = \frac{1}{r^2} \frac{\partial}{\partial r} (r^2 A_r) + \frac{1}{r \sin \theta} \frac{\partial}{\partial \theta} (\sin \theta A_\theta) + \frac{1}{r \sin \theta} \frac{\partial A_\phi}{\partial \phi}$
Στροβιλισμός	$\text{rot} \vec{A} = \vec{\nabla} \times \vec{A} =$ $\frac{1}{r \sin \theta} \left[\frac{\partial}{\partial \theta} (\sin \theta A_\phi) - \frac{\partial A_\theta}{\partial \phi} \right] \vec{r} + \frac{1}{r} \left[\frac{1}{\sin \theta} \frac{\partial A_r}{\partial \phi} - \frac{\partial}{\partial r} (r A_\phi) \right] \vec{\theta} +$ $+ \frac{1}{r} \left[\frac{\partial}{\partial r} (r A_\theta) - \frac{\partial A_r}{\partial \theta} \right] \vec{\phi}$

III/

ΣΕ ΚΥΛΙΝΔΡΙΚΕΣ ΣΥΝΤΕΤΑΓΜΕΝΕΣ (r,φ,z) [2]

Διάνυσμα θέσης $\vec{r} = r \cos \phi \vec{i} + r \sin \phi \vec{j} + z \vec{k}$

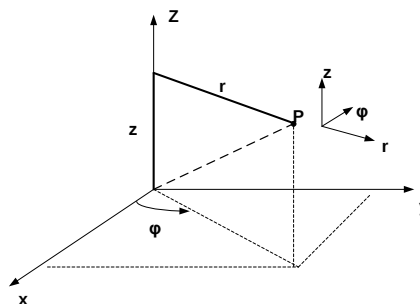
Μήκος $d\vec{l} = dr \vec{r} + r d\phi \vec{\phi} + dz \vec{z}$

Όγκος $dV = r dr d\phi dz$

Επιφάνεια $dA = r d\phi dz$

Σχέση με καρτεσιανές συντεταγμένες: $\{x = r \cos \phi, y = r \sin \phi, z = z\}$

όπου $0 \leq r < \infty, 0 \leq \phi \leq \pi, -\infty < z < +\infty$



Κλίση	$\vec{\nabla}f = \frac{\partial f}{\partial r} \vec{r} + \frac{1}{r} \frac{\partial f}{\partial \phi} \vec{\phi} + \frac{\partial f}{\partial z} \vec{z}$
Απόκλιση	$\text{div} \vec{A} = \vec{\nabla} \cdot \vec{A} = \frac{1}{r} \frac{\partial}{\partial r} (r A_r) + \frac{1}{r} \frac{\partial A_\phi}{\partial \phi} + \frac{\partial A_z}{\partial z}$
Στροβιλισμός	$\text{rot} \vec{A} = \vec{\nabla} \times \vec{A} = \begin{vmatrix} \frac{1}{r} \vec{r} & \vec{\phi} & \frac{1}{r} \vec{z} \\ \frac{\partial}{\partial r} & \frac{\partial}{\partial \phi} & \frac{\partial}{\partial z} \\ A_r & r A_\phi & A_z \end{vmatrix} =$ $\frac{1}{r} \left[\frac{\partial A_z}{\partial \phi} - \frac{\partial A_\phi}{\partial z} \right] \vec{r} + \left[\frac{\partial A_r}{\partial z} - \frac{\partial A_z}{\partial r} \right] \vec{\phi} + \frac{1}{r} \left[\frac{\partial}{\partial r} (r A_\phi) - \frac{\partial A_r}{\partial \phi} \right] \vec{z}$

IV/

Η μετατροπή των σφαιρικών συντεταγμένων (r, θ, ϕ) σε καρτεσιανές συντεταγμένες (x, y, z) είναι ισοδύναμα ανάλογη των σχέσεων [2]:

$$\begin{cases} x = r \sin \theta \cos \phi, \\ y = r \sin \theta \sin \phi, \\ z = r \cos \theta \end{cases} \text{ και } \begin{cases} \vec{i} = \sin \theta \cos \phi \vec{r} + \cos \theta \cos \phi \vec{\theta} - \sin \phi \vec{\phi} \\ \vec{j} = \sin \theta \sin \phi \vec{r} + \cos \theta \sin \phi \vec{\theta} + \cos \phi \vec{\phi} \\ \vec{k} = \cos \theta \vec{r} - \sin \theta \vec{\theta} \end{cases}$$

επίσης

$$\begin{cases} r = \sqrt{x^2 + y^2 + z^2} \\ \theta = \tan^{-1} \frac{\sqrt{x^2 + y^2}}{z} \\ \phi = \arctan \frac{y}{x} \end{cases} \text{ και } \begin{cases} \vec{r} = \sin \theta \cos \phi \vec{i} + \sin \theta \sin \phi \vec{j} + \cos \theta \vec{k} \\ \vec{\theta} = \cos \theta \cos \phi \vec{i} + \cos \theta \sin \phi \vec{j} - \sin \theta \vec{k} \\ \vec{\phi} = -\sin \phi \vec{i} + \cos \phi \vec{j} \end{cases}$$

*Αντί να ανησυχούμε γι' αυτό που συνέβει εχθές,
ας επινοήσουμε καλύτερα το αύριο"*

Steve Jobs

ΠΑΡΑΡΤΗΜΑ Β΄

ΘΕΜΕΛΙΩΔΕΙΣ ΣΤΑΘΕΡΕΣ

ΘΕΜΕΛΙΩΔΕΙΣ ΣΤΑΘΕΡΕΣ ΦΥΣΙΚΩΝ ΜΕΓΕΘΩΝ

ΟΝΟΜΑΣΙΑ ΣΤΑΘΕΡΑΣ	ΤΙΜΗ
Μάζα ηρεμίας ηλεκτρονίου	$m_e = 9,10939 \cdot 10^{-31} \text{ kg}$
Μάζα ηρεμίας πρωτονίου	$m_p = 1,67263 \cdot 10^{-27} \text{ kg}$
Μάζα ηρεμίας νετρονίου	$m_n = 1,67493 \cdot 10^{-27} \text{ kg}$
Ειδικό φορτίο ηλεκτρονίου	$\frac{e}{m} = 1,76 \cdot 10^{-11} \frac{\text{C}}{\text{kg}}$
Ατομική Μονάδα μάζας	$1u = 1,66054 \cdot 10^{-27} \text{ kg}$
Ακτίνα του Bohr	$a_o = \frac{\hbar^2}{m_e e^2} = 0,52917715 \cdot 10^{-10} \text{ m}$
Μαγνητόνη του Bohr	$\mu_B = \frac{e\hbar}{2m_p} = 0,9273 \cdot 10^{-23}$
Πυρηνική μαγνητόνη	$\mu_N = \frac{e\hbar}{2m_p} = 0,5050 \cdot 10^{-10}$
Μαγνητική διπολική ροπή ηλεκτρονίου	$\mu_e = -1,00115 \cdot \mu_B$
Μαγνητική διπολική ροπή πρωτονίου	$\mu_p = 2,79285 \cdot \mu_N$
Μαγνητική διπολική ροπή νετρονίου	$\mu_n = -1,913 \cdot \mu_N$
Ταχύτητα του φωτός	$c = 3 \cdot 10^8 \frac{\text{m}}{\text{s}}$
Σταθερά του Planck	$h = 6,626 \cdot 10^{-34} \text{ J} \cdot \text{sec}$
Σταθερά της λεπτής υφής α	$\alpha = \frac{1}{137}$
Φορτίο ηλεκτρονίου	$e = 1,602 \cdot 10^{-19} \text{ C}$
Ανηγγμένη σταθερά του Planck	$\hbar = 1,055 \cdot 10^{-34} \text{ J} \cdot \text{sec}$
Σταθερά ηλεκτρικής αλληλεπίδρασης στο κενό (νόμου Coulomb)	$\kappa = \frac{1}{4\pi\epsilon_0} = 9 \cdot 10^9 \frac{\text{Nm}^2}{\text{C}^2}$
Απόλυτο Μηδέν	$0^\circ \text{K} = -273,15^\circ \text{C}$
Ηλεκτρονιοβόλτ	$1\text{eV} = 1,6 \cdot 10^{-19} \text{ J}$

ΠΑΡΑΡΤΗΜΑ Γ'

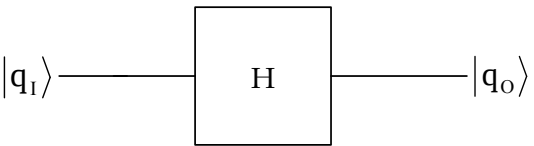
ΠΙΝΑΚΑΣ ΠΥΛΩΝ

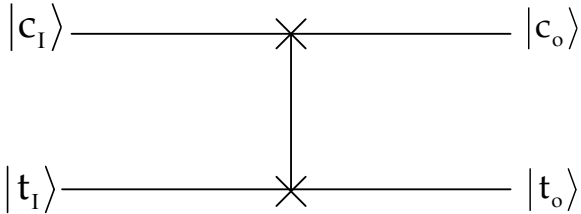
ΚΒΑΝΤΙΚΕΣ ΛΟΓΙΚΕΣ ΠΥΛΕΣ ΚΒΑΝΤΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

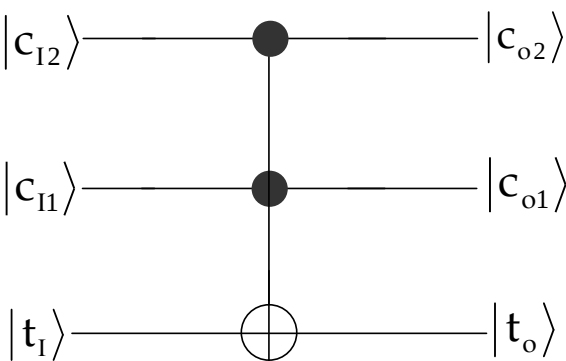
Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»								
$ q_I\rangle$ ——— I ——— $ q_O\rangle$ Πύλη Αδρανείας	<table> <tr> <th>Input ($q_I\rangle$)</th><th>Output ($q_O\rangle$)</th></tr> <tr> <td>$q_I\rangle = 0\rangle$</td><td>$q_O\rangle = 0\rangle$</td></tr> <tr> <td>$q_I\rangle = 1\rangle$</td><td>$q_O\rangle = 1\rangle$</td></tr> <tr> <td>$q_I\rangle = q\rangle$</td><td>$q_O\rangle = q\rangle$</td></tr> </table>	Input ($ q_I\rangle$)	Output ($ q_O\rangle$)	$ q_I\rangle = 0\rangle$	$ q_O\rangle = 0\rangle$	$ q_I\rangle = 1\rangle$	$ q_O\rangle = 1\rangle$	$ q_I\rangle = q\rangle$	$ q_O\rangle = q\rangle$
Input ($ q_I\rangle$)	Output ($ q_O\rangle$)								
$ q_I\rangle = 0\rangle$	$ q_O\rangle = 0\rangle$								
$ q_I\rangle = 1\rangle$	$ q_O\rangle = 1\rangle$								
$ q_I\rangle = q\rangle$	$ q_O\rangle = q\rangle$								

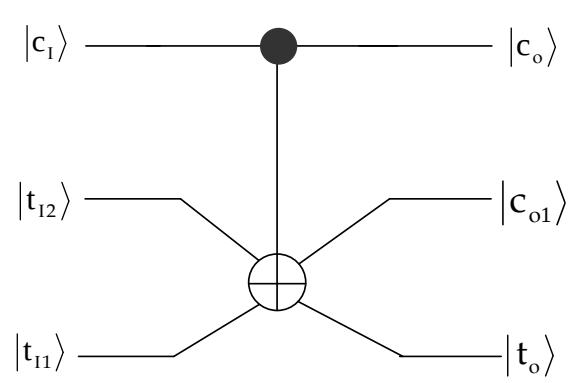
Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»								
$ q_I\rangle$ ——— Φ ——— $ q_O\rangle$ Πύλη Μετατόπισης Φάσης	<table> <tr> <th>Input ($q_I\rangle$)</th><th>Output ($q_O\rangle$)</th></tr> <tr> <td>$q_I\rangle = 0\rangle$</td><td>$q_O\rangle = 0\rangle$</td></tr> <tr> <td>$q_I\rangle = 1\rangle$</td><td>$q_O\rangle = e^{i\varphi} 1\rangle$</td></tr> <tr> <td>$q_I\rangle = \alpha 0\rangle + \beta 1\rangle$</td><td>$q_O\rangle = \alpha 0\rangle + \beta e^{i\varphi} 1\rangle$</td></tr> </table>	Input ($ q_I\rangle$)	Output ($ q_O\rangle$)	$ q_I\rangle = 0\rangle$	$ q_O\rangle = 0\rangle$	$ q_I\rangle = 1\rangle$	$ q_O\rangle = e^{i\varphi} 1\rangle$	$ q_I\rangle = \alpha 0\rangle + \beta 1\rangle$	$ q_O\rangle = \alpha 0\rangle + \beta e^{i\varphi} 1\rangle$
Input ($ q_I\rangle$)	Output ($ q_O\rangle$)								
$ q_I\rangle = 0\rangle$	$ q_O\rangle = 0\rangle$								
$ q_I\rangle = 1\rangle$	$ q_O\rangle = e^{i\varphi} 1\rangle$								
$ q_I\rangle = \alpha 0\rangle + \beta 1\rangle$	$ q_O\rangle = \alpha 0\rangle + \beta e^{i\varphi} 1\rangle$								

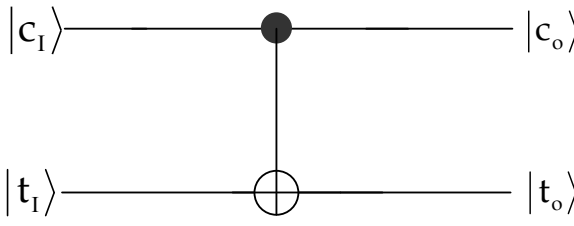
Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»								
$ q_I\rangle$ ——— NOT ——— $ q_O\rangle$ Πύλη NOT	<table> <tr> <th>Input ($q_I\rangle$)</th><th>Output ($q_O\rangle$)</th></tr> <tr> <td>$q_I\rangle = 0\rangle$</td><td>$q_O\rangle = 1\rangle$</td></tr> <tr> <td>$q_I\rangle = 1\rangle$</td><td>$q_O\rangle = 0\rangle$</td></tr> <tr> <td>$q_I\rangle = \alpha 0\rangle + \beta 1\rangle$</td><td>$q_O\rangle = \alpha 1\rangle + \beta 0\rangle$</td></tr> </table>	Input ($ q_I\rangle$)	Output ($ q_O\rangle$)	$ q_I\rangle = 0\rangle$	$ q_O\rangle = 1\rangle$	$ q_I\rangle = 1\rangle$	$ q_O\rangle = 0\rangle$	$ q_I\rangle = \alpha 0\rangle + \beta 1\rangle$	$ q_O\rangle = \alpha 1\rangle + \beta 0\rangle$
Input ($ q_I\rangle$)	Output ($ q_O\rangle$)								
$ q_I\rangle = 0\rangle$	$ q_O\rangle = 1\rangle$								
$ q_I\rangle = 1\rangle$	$ q_O\rangle = 0\rangle$								
$ q_I\rangle = \alpha 0\rangle + \beta 1\rangle$	$ q_O\rangle = \alpha 1\rangle + \beta 0\rangle$								

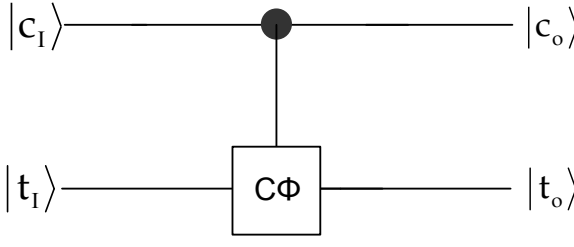
Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»										
 Πύλη HADAMARD	<table> <tr> <th>Input ($q_I\rangle$)</th><th>Output ($q_O\rangle$)</th></tr> <tr> <td>$q_I\rangle = 0\rangle$</td><td>$q_O\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$</td></tr> <tr> <td>$q_I\rangle = 1\rangle$</td><td>$q_O\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$</td></tr> <tr> <td>$q_I\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$</td><td>$q_O\rangle = 0\rangle$</td></tr> <tr> <td>$q_I\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$</td><td>$q_O\rangle = 1\rangle$</td></tr> </table>	Input ($ q_I\rangle$)	Output ($ q_O\rangle$)	$ q_I\rangle = 0\rangle$	$ q_O\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$	$ q_I\rangle = 1\rangle$	$ q_O\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$	$ q_I\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$	$ q_O\rangle = 0\rangle$	$ q_I\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$	$ q_O\rangle = 1\rangle$
Input ($ q_I\rangle$)	Output ($ q_O\rangle$)										
$ q_I\rangle = 0\rangle$	$ q_O\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$										
$ q_I\rangle = 1\rangle$	$ q_O\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$										
$ q_I\rangle = \frac{1}{\sqrt{2}}(0\rangle + 1\rangle)$	$ q_O\rangle = 0\rangle$										
$ q_I\rangle = \frac{1}{\sqrt{2}}(0\rangle - 1\rangle)$	$ q_O\rangle = 1\rangle$										

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»										
 Πύλη Εναλλαγής	<table> <tr> <th>Input ($c_I t_I\rangle$)</th><th>Output ($c_O t_O\rangle$)</th></tr> <tr> <td>$c_I t_I\rangle = 00\rangle$</td><td>$c_O t_O\rangle = 00\rangle$</td></tr> <tr> <td>$c_I t_I\rangle = 01\rangle$</td><td>$c_O t_O\rangle = 10\rangle$</td></tr> <tr> <td>$c_I t_I\rangle = 10\rangle$</td><td>$c_O t_O\rangle = 01\rangle$</td></tr> <tr> <td>$c_I t_I\rangle = 11\rangle$</td><td>$c_O t_O\rangle = 11\rangle$</td></tr> </table>	Input ($ c_I t_I\rangle$)	Output ($ c_O t_O\rangle$)	$ c_I t_I\rangle = 00\rangle$	$ c_O t_O\rangle = 00\rangle$	$ c_I t_I\rangle = 01\rangle$	$ c_O t_O\rangle = 10\rangle$	$ c_I t_I\rangle = 10\rangle$	$ c_O t_O\rangle = 01\rangle$	$ c_I t_I\rangle = 11\rangle$	$ c_O t_O\rangle = 11\rangle$
Input ($ c_I t_I\rangle$)	Output ($ c_O t_O\rangle$)										
$ c_I t_I\rangle = 00\rangle$	$ c_O t_O\rangle = 00\rangle$										
$ c_I t_I\rangle = 01\rangle$	$ c_O t_O\rangle = 10\rangle$										
$ c_I t_I\rangle = 10\rangle$	$ c_O t_O\rangle = 01\rangle$										
$ c_I t_I\rangle = 11\rangle$	$ c_O t_O\rangle = 11\rangle$										

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»																		
 Πύλη Διπλά Ελεγχόμενου ΟΧΙ	<table> <tr> <th>Input ($c_{I2} c_{I1} t_I\rangle$)</th><th>Output ($c_{O2} c_{O1} t_O\rangle$)</th></tr> <tr> <td>$c_{I2} c_{I1} t_I\rangle = 000\rangle$</td><td>$c_{O2} c_{O1} t_O\rangle = 000\rangle$</td></tr> <tr> <td>$c_{I2} c_{I1} t_I\rangle = 001\rangle$</td><td>$c_{O2} c_{O1} t_O\rangle = 001\rangle$</td></tr> <tr> <td>$c_{I2} c_{I1} t_I\rangle = 010\rangle$</td><td>$c_{O2} c_{O1} t_O\rangle = 010\rangle$</td></tr> <tr> <td>$c_{I2} c_{I1} t_I\rangle = 011\rangle$</td><td>$c_{O2} c_{O1} t_O\rangle = 011\rangle$</td></tr> <tr> <td>$c_{I2} c_{I1} t_I\rangle = 100\rangle$</td><td>$c_{O2} c_{O1} t_O\rangle = 100\rangle$</td></tr> <tr> <td>$c_{I2} c_{I1} t_I\rangle = 101\rangle$</td><td>$c_{O2} c_{O1} t_O\rangle = 101\rangle$</td></tr> <tr> <td>$c_{I2} c_{I1} t_I\rangle = 110\rangle$</td><td>$c_{O2} c_{O1} t_O\rangle = 111\rangle$</td></tr> <tr> <td>$c_{I2} c_{I1} t_I\rangle = 111\rangle$</td><td>$c_{O2} c_{O1} t_O\rangle = 110\rangle$</td></tr> </table>	Input ($ c_{I2} c_{I1} t_I\rangle$)	Output ($ c_{O2} c_{O1} t_O\rangle$)	$ c_{I2} c_{I1} t_I\rangle = 000\rangle$	$ c_{O2} c_{O1} t_O\rangle = 000\rangle$	$ c_{I2} c_{I1} t_I\rangle = 001\rangle$	$ c_{O2} c_{O1} t_O\rangle = 001\rangle$	$ c_{I2} c_{I1} t_I\rangle = 010\rangle$	$ c_{O2} c_{O1} t_O\rangle = 010\rangle$	$ c_{I2} c_{I1} t_I\rangle = 011\rangle$	$ c_{O2} c_{O1} t_O\rangle = 011\rangle$	$ c_{I2} c_{I1} t_I\rangle = 100\rangle$	$ c_{O2} c_{O1} t_O\rangle = 100\rangle$	$ c_{I2} c_{I1} t_I\rangle = 101\rangle$	$ c_{O2} c_{O1} t_O\rangle = 101\rangle$	$ c_{I2} c_{I1} t_I\rangle = 110\rangle$	$ c_{O2} c_{O1} t_O\rangle = 111\rangle$	$ c_{I2} c_{I1} t_I\rangle = 111\rangle$	$ c_{O2} c_{O1} t_O\rangle = 110\rangle$
Input ($ c_{I2} c_{I1} t_I\rangle$)	Output ($ c_{O2} c_{O1} t_O\rangle$)																		
$ c_{I2} c_{I1} t_I\rangle = 000\rangle$	$ c_{O2} c_{O1} t_O\rangle = 000\rangle$																		
$ c_{I2} c_{I1} t_I\rangle = 001\rangle$	$ c_{O2} c_{O1} t_O\rangle = 001\rangle$																		
$ c_{I2} c_{I1} t_I\rangle = 010\rangle$	$ c_{O2} c_{O1} t_O\rangle = 010\rangle$																		
$ c_{I2} c_{I1} t_I\rangle = 011\rangle$	$ c_{O2} c_{O1} t_O\rangle = 011\rangle$																		
$ c_{I2} c_{I1} t_I\rangle = 100\rangle$	$ c_{O2} c_{O1} t_O\rangle = 100\rangle$																		
$ c_{I2} c_{I1} t_I\rangle = 101\rangle$	$ c_{O2} c_{O1} t_O\rangle = 101\rangle$																		
$ c_{I2} c_{I1} t_I\rangle = 110\rangle$	$ c_{O2} c_{O1} t_O\rangle = 111\rangle$																		
$ c_{I2} c_{I1} t_I\rangle = 111\rangle$	$ c_{O2} c_{O1} t_O\rangle = 110\rangle$																		

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»																		
 Πύλη FREDKIN	<table> <tr> <th>Input ($c_I t_{21} t_{11}\rangle$)</th><th>Output ($c_o t_{o2} t_{o1}\rangle$)</th></tr> <tr> <td>$c_I t_{21} t_{11}\rangle = 000\rangle$</td><td>$c_o t_{o2} t_{o1}\rangle = 000\rangle$</td></tr> <tr> <td>$c_I t_{21} t_{11}\rangle = 001\rangle$</td><td>$c_o t_{o2} t_{o1}\rangle = 001\rangle$</td></tr> <tr> <td>$c_I t_{21} t_{11}\rangle = 010\rangle$</td><td>$c_o t_{o2} t_{o1}\rangle = 010\rangle$</td></tr> <tr> <td>$c_I t_{21} t_{11}\rangle = 011\rangle$</td><td>$c_o t_{o2} t_{o1}\rangle = 011\rangle$</td></tr> <tr> <td>$c_I t_{21} t_{11}\rangle = 100\rangle$</td><td>$c_o t_{o2} t_{o1}\rangle = 100\rangle$</td></tr> <tr> <td>$c_I t_{21} t_{11}\rangle = 101\rangle$</td><td>$c_o t_{o2} t_{o1}\rangle = 110\rangle$</td></tr> <tr> <td>$c_I t_{21} t_{11}\rangle = 110\rangle$</td><td>$c_o t_{o2} t_{o1}\rangle = 101\rangle$</td></tr> <tr> <td>$c_I t_{21} t_{11}\rangle = 111\rangle$</td><td>$c_o t_{o2} t_{o1}\rangle = 111\rangle$</td></tr> </table>	Input ($ c_I t_{21} t_{11}\rangle$)	Output ($ c_o t_{o2} t_{o1}\rangle$)	$ c_I t_{21} t_{11}\rangle = 000\rangle$	$ c_o t_{o2} t_{o1}\rangle = 000\rangle$	$ c_I t_{21} t_{11}\rangle = 001\rangle$	$ c_o t_{o2} t_{o1}\rangle = 001\rangle$	$ c_I t_{21} t_{11}\rangle = 010\rangle$	$ c_o t_{o2} t_{o1}\rangle = 010\rangle$	$ c_I t_{21} t_{11}\rangle = 011\rangle$	$ c_o t_{o2} t_{o1}\rangle = 011\rangle$	$ c_I t_{21} t_{11}\rangle = 100\rangle$	$ c_o t_{o2} t_{o1}\rangle = 100\rangle$	$ c_I t_{21} t_{11}\rangle = 101\rangle$	$ c_o t_{o2} t_{o1}\rangle = 110\rangle$	$ c_I t_{21} t_{11}\rangle = 110\rangle$	$ c_o t_{o2} t_{o1}\rangle = 101\rangle$	$ c_I t_{21} t_{11}\rangle = 111\rangle$	$ c_o t_{o2} t_{o1}\rangle = 111\rangle$
Input ($ c_I t_{21} t_{11}\rangle$)	Output ($ c_o t_{o2} t_{o1}\rangle$)																		
$ c_I t_{21} t_{11}\rangle = 000\rangle$	$ c_o t_{o2} t_{o1}\rangle = 000\rangle$																		
$ c_I t_{21} t_{11}\rangle = 001\rangle$	$ c_o t_{o2} t_{o1}\rangle = 001\rangle$																		
$ c_I t_{21} t_{11}\rangle = 010\rangle$	$ c_o t_{o2} t_{o1}\rangle = 010\rangle$																		
$ c_I t_{21} t_{11}\rangle = 011\rangle$	$ c_o t_{o2} t_{o1}\rangle = 011\rangle$																		
$ c_I t_{21} t_{11}\rangle = 100\rangle$	$ c_o t_{o2} t_{o1}\rangle = 100\rangle$																		
$ c_I t_{21} t_{11}\rangle = 101\rangle$	$ c_o t_{o2} t_{o1}\rangle = 110\rangle$																		
$ c_I t_{21} t_{11}\rangle = 110\rangle$	$ c_o t_{o2} t_{o1}\rangle = 101\rangle$																		
$ c_I t_{21} t_{11}\rangle = 111\rangle$	$ c_o t_{o2} t_{o1}\rangle = 111\rangle$																		

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»										
 Πύλη Ελεγχόμενου ΟΧΙ	<table> <tr> <th>Input ($c_I t_I\rangle$)</th><th>Output ($c_o t_o\rangle$)</th></tr> <tr> <td>$c_I t_I\rangle = 00\rangle$</td><td>$c_o t_o\rangle = 00\rangle$</td></tr> <tr> <td>$c_I t_I\rangle = 01\rangle$</td><td>$c_o t_o\rangle = 01\rangle$</td></tr> <tr> <td>$c_I t_I\rangle = 10\rangle$</td><td>$c_o t_o\rangle = 11\rangle$</td></tr> <tr> <td>$c_I t_I\rangle = 11\rangle$</td><td>$c_o t_o\rangle = 10\rangle$</td></tr> </table>	Input ($ c_I t_I\rangle$)	Output ($ c_o t_o\rangle$)	$ c_I t_I\rangle = 00\rangle$	$ c_o t_o\rangle = 00\rangle$	$ c_I t_I\rangle = 01\rangle$	$ c_o t_o\rangle = 01\rangle$	$ c_I t_I\rangle = 10\rangle$	$ c_o t_o\rangle = 11\rangle$	$ c_I t_I\rangle = 11\rangle$	$ c_o t_o\rangle = 10\rangle$
Input ($ c_I t_I\rangle$)	Output ($ c_o t_o\rangle$)										
$ c_I t_I\rangle = 00\rangle$	$ c_o t_o\rangle = 00\rangle$										
$ c_I t_I\rangle = 01\rangle$	$ c_o t_o\rangle = 01\rangle$										
$ c_I t_I\rangle = 10\rangle$	$ c_o t_o\rangle = 11\rangle$										
$ c_I t_I\rangle = 11\rangle$	$ c_o t_o\rangle = 10\rangle$										

Σχεδιαστικός Συμβολισμός (Είσοδος - Δράση πύλης - Έξοδος)	«Πίνακας Αληθείας»										
 Πύλη Ελεγχόμενης Μετατόπισης Φάσης	<table> <tr> <th>Input ($c_I t_I\rangle$)</th><th>Output ($c_o t_o\rangle$)</th></tr> <tr> <td>$c_I t_I\rangle = 00\rangle$</td><td>$c_o t_o\rangle = 00\rangle$</td></tr> <tr> <td>$c_I t_I\rangle = 01\rangle$</td><td>$c_o t_o\rangle = 01\rangle$</td></tr> <tr> <td>$c_I t_I\rangle = 10\rangle$</td><td>$c_o t_o\rangle = 10\rangle$</td></tr> <tr> <td>$c_I t_I\rangle = 11\rangle$</td><td>$c_o t_o\rangle = e^{i\varphi} 11\rangle$</td></tr> </table>	Input ($ c_I t_I\rangle$)	Output ($ c_o t_o\rangle$)	$ c_I t_I\rangle = 00\rangle$	$ c_o t_o\rangle = 00\rangle$	$ c_I t_I\rangle = 01\rangle$	$ c_o t_o\rangle = 01\rangle$	$ c_I t_I\rangle = 10\rangle$	$ c_o t_o\rangle = 10\rangle$	$ c_I t_I\rangle = 11\rangle$	$ c_o t_o\rangle = e^{i\varphi} 11\rangle$
Input ($ c_I t_I\rangle$)	Output ($ c_o t_o\rangle$)										
$ c_I t_I\rangle = 00\rangle$	$ c_o t_o\rangle = 00\rangle$										
$ c_I t_I\rangle = 01\rangle$	$ c_o t_o\rangle = 01\rangle$										
$ c_I t_I\rangle = 10\rangle$	$ c_o t_o\rangle = 10\rangle$										
$ c_I t_I\rangle = 11\rangle$	$ c_o t_o\rangle = e^{i\varphi} 11\rangle$										

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Κβαντικοί Υπολογιστές (Βασικές έννοιες) - Ιωάννης Καραφυλλίδης, ΗΜΜΥ ΔΠΘ, 2005 εκδόσεις Κλειδάριθμος, ISBN: 960- 209- 816-3
2. Κβαντική μηχανική (θεωρία και Προβλήματα) -Γιώργος Ασημάκης, Αθήνα 2012 εκδόσεις Συμμετρία, ISBN 978-960-266-362-2
3. Ξενοφών Ραφίος – Διπλωματική εργασία «Κβαντική φυσική και Υπολογιστές: Αλγόριθμοι, πολυπλοκότητα και θεωρία παιγνίων», Αθήνα 2006. ΔΠΜΣ ΕΚΠΑ
4. Κωνσταντίνος Ραμπαλάκος – Διπλωματική εργασία «Κβαντικοί Υπολογισμοί» Κρήτη 2004, ΠΜΣ Τμήματος Μαθηματικού - Πανεπιστήμιο Κρήτης
5. Γούσια Πολυξένη – Διπλωματική εργασία «Κβαντικοί υπολογιστές: Μέθοδοι υλοποίησης κβαντικών πυλών» Τμήμα Πληροφορικής ΑΠΘ
6. Τσετσιλα Μέλανι – Βασιλική – Διπλωματική εργασία: «Κρυπτογραφία και κβαντικοί Υπολογιστές», ΣΕΜΦΕ – ΕΜΠ
7. Πετρούλα Μαυρίδη- Διπλωματική Εργασία «Ανάπτυξη βιβλιοθήκης και Περιβάλλοντος Εξομοίωσης Κβαντικών Υπολογισμών σε γλώσσα Python», Πάτρα 2010, ΗΜΜΥ Πανεπιστήμιο Πατρών

8. Κουρτελής Αλέξιος – Διπλωματική εργασία «Κβαντικοί αλγόριθμοι , Κβαντικοί Υπολογιστές», Θεσσαλονίκη 2008, ΠΜΣ εφ. Πληροφορικής Πανεπιστήμιο Μακεδονίας
9. http://el.wikipedia.org/wiki/%CE%93%CE%AC%CF%84%CE%B1_%CF%84%CE%BF%CF%85_%CE%A3%CF%81%CE%AD%CE%BD%CF%84%CE%B9%CE%B3%CE%BA%CE%B5%CF%81
10. http://el.wikipedia.org/wiki/%CE%A7%CF%8E%CF%81%CE%BF%CF%82_%CE%A7%CE%AF%CE%BB%CE%BC%CF%80%CE%B5%CF%81%CF%84
11. Κβαντομηχανική II – Στέφανος Τραχανάς Κρήτη 2008- ΙΤΕ, εκδόσεις ΠΕΚ, ISBN: 978-960-524-267-1
12. http://el.wikipedia.org/wiki/%CE%91%CF%81%CF%87%CE%AE_%CF%84%CE%B7%CF%82_%CE%B5%CF%80%CE%B1%CE%BB%CE%BB%CE%B7%CE%BB%CE%AF%CE%B1%CF%82
13. Jim Al-Khalili - Quantika Παράδοξα, Εκδόσεις Τραυλός, Αθήνα 2005
14. <http://physics4u.wordpress.com/2010/02/22/%CF%8D-%CF%8E-%CF%8E%CF%8E%CF%8E/>
15. <http://arxiv.org/ftp/arxiv/papers/0712/0712.3466.pdf>
16. <http://www.digitallife.gr/how-quantum-computers-work-68054>
17. <http://technolnews.blogspot.gr/2012/04/quantum-computing-videos.html>
18. <http://el.wikipedia.org/wiki/Qubit>
19. http://el.wikipedia.org/wiki/%CE%A3%CF%86%CE%B1%CE%AF%CF%81%CE%B1_%CE%9C%CF%80%CE%BB%CE%BF%CF%87
20. <http://www.tovima.gr/science/article/?aid=275839>

21. <http://www.nature.com/nature/journal/vaop/ncurrent/abs/nature08121.html>
22. <http://plato.stanford.edu/entries/qt-quantcomp/>
23. <http://www.org.chemie.tu-muenchen.de/glaser/qcomp.html>
24. <https://sites.google.com/site/icsdkvantikoitypologistes/home/kephalaio-e/e2-kbantike-diemploke-kai-kbantikoi-katachoretas>
25. http://domino.research.ibm.com/comm/pr.nsf/pages/news.20011219_quantum.html
26. Quantum-Mechanical Computers, by Seth Lloyd. Scientific America October 1995: «Quantum-mechanical computers, if they can be constructed, will do things no ordinary computer can».
27. <https://sites.google.com/site/icsdkvantikoitypologistes/home>
28. http://en.wikipedia.org/wiki/Quantum_gate
29. <http://www.infogenesis.gr/modules.php?name=News&file=article&sid=126>.
Περιοδικό Science Daily Αύγουστος 24, 2008.
30. [http://www.news-medical.net/health/Quantum-Dots-What-are-Quantum-Dots- 28Greek%29.aspx](http://www.news-medical.net/health/Quantum-Dots-What-are-Quantum-Dots-28Greek%29.aspx):
31. Ευαγγελία Μαράτου. Πάτρα Ιούνιος 2010. Μεταπτυχιακή εργασία ειδίκευσης του τμήματος επιστήμης υλικών: «Σύνθεση και χαρακτηρισμός χαμηλοδιάστατων ημιαγωγών αλογονιδίων του μολύβδου και χαλκογενιδίων».
32. Μαθηματικά Γ' Λυκείου – ΟΕΔΒ. Άλγεβρα, αναλυτική γεωμετρία και πιθανότητες.

- 33.** Μυστηρίδου Εμμανουέλλα, Πάτρα 2010, 3^η εργασία για το μάθημα «Άμορφα κράματα και νανοδομημένα υλικά», με τίτλο Κβαντικές τελείες. Τμήμα επιστήμης υλικών πανεπιστημίου Πατρών.
- 34.** <http://tadeefi.wordpress.com/2013/05/20/k%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CF%8C%CF%82CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AE%CF%82-d-wave-two/>
- 35.** <http://techmaniacs.gr/google-test-performance-of-quantum-computers/>
- 36.** <http://www.dwavessys.com>
- 37.** http://en.wikipedia.org/wiki/D-Wave_Systems
- 38.** <http://www.kathimerini.gr/77465/article/tehnologia/computers/erxetai-to-neo-kvantiko-tsip>
- 39.** <http://www.naftemporiki.gr/story/694957/qcloud-enas-kbantikos-upologistis-sto-diadiktuo>
- 40.** Anuj Dawar - Quantum Computing: Lecture 1 «Bits and Qubit» University of Cambridge , διαλέξεις ακαδημαϊκού έτους 2007-2008.
- 41.** John Preskill-Lecture Notes for Physic «Quantum Information and Computation» California Institute of Technology, September 1998
- 42.** Quantum Mechanics Helps in Searching for a Needle in a Haystack- Lov K. Grover-3C-404A Bell Labs, 600 Mountain Avenue, Murray Hill, New Jersey 07974 (Received 4 December 1996)
- 43.** Παναγιώτης Ριζομιλιώτης, Ακ. έτος 2013-14 – ΠΜΣ Πληροφορικής και Τηλεματικής, διάλεξη 1^η -2^η : Ασφάλεια πληροφοριών και συστημάτων.

44. Καραγεωργός Βασίλειος, Ακ. έτος 2006-2007, Εργασία : Κβαντική κρυπτογραφία, διδασκων Ε. Ράπτης.
45. Βασιλική Ανδρονίκου, Ακ. έτος 2011-12. Διάλεξη 1^η – 3^η : Ασφάλεια πληροφοριακών συστημάτων, τμήμα Πληροφορικής και Τηλεματικής.
46. <http://www.skai.gr/news/technology/article/246002/to-neo-rekor-kvadikis-mnimis-mas-fernei-pio-koda-stous-kvadikous-upologistes/>.
47. Γιώργος Ασημάκης, 2010-2011, Διδακτικές σημειώσεις του εργαστηριακού μαθήματος «Αυτοματισμοί και Συστήματα Ελέγχου».
48. Μ. Βαμβακάρη, Ακ. Έτος 2013-14, Διαφάνειες διαλέξεων ΠΜΣ Πληροφορικής και Τηλεματικής στο μάθημα «Στατιστική και Διαδίκτυο» . Διάλεξη 1^η – 6^η .
49. Michael A. Nielsen. Νοέμβριος 2002 (Scientific America Ins.) Τίτλος άρθρου: «Rules for a Complex Quantum World. An exciting new fundamental discipline of research combines information science and quantum mechanics ».
50. Σημειώσεις διαλέξεων-παραδόσεων Κβαντομηχανικής I και II (2005-2006). Τμήμα Φυσικής της σχολής θετικών επιστημών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.
51. Σουηδική Ακαδημία επιστημών, Οκτώβριος 2012, Βραβείο Νόμπελ Φυσικής με τίτλο « Measuring and manipulating individual quantum systems». Το βραβείο Νόμπελ απονεμήθηκε στους Serge Haroche and David J. Wineland.
52. Ioannis G. Karafyllidis - September 2003. Visualization of the Quantum Fourier Transform Using a Quantum Computer Simulator
53. Ioannis G. Karafyllidis - August 2005. IEEE transactions on circuits and systems. Quantum Computer Simulator Based on the Circuit Model of Quantum Computation

54. John Preskill California Institute of Technology September 1998 Lecture Notes for Physics Quantum Information and Computation.
55. David Deutsch Appeared in Proceedings of the Royal Society of London A - 1985 Quantum theory, the Church-Turing principle and the universal quantum computer - (Communicated by R. Penrose, F.R.S. — Received 13 July 1984)
56. Ioannis G. Karafyllidis - November 2003. Cellular quantum computer architecture. Department of Electrical and Computer Engineering, Democritus University of Thrace, 671 00 Xanthi, Greece
57. Noboru KUNIHITO (The University of Electro-communications, Tokyo) and Shigeru YAMASHITA (Nara Institute of Science and Technology, Japan) August 2002. Efficient Algorithms for NMR Quantum Computers with Small Qubits
58. http://users.auth.gr/paloura/opto_3quant_confinment.pdf
59. Διδακτικές Σημειώσεις , Ιωάννης Καραφυλλίδης - Μάθημα 9ου Εξαμήνου Κβαντικοί Υπολογιστές. Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών Δ.Π.Θ., Τομέας Ηλεκτρονικής και Τεχνολογίας Συστημάτων Πληροφορικής
60. Lov K. Grover - December 1996. Quantum Mechanics Helps in Searching for a Needle in a Haystack.

Copyright - © Γιώργος Π. Ασημάκης

Απαγορεύεται η ανατύπωση ή η αναδημοσίευση ή η φωτοτύπωση ή η ηλεκτρονική αποθήκευση, ολικώς, μερικώς ή κατά παράφραση του περιεχομένου του παρόντος κειμένου χωρίς την έγγραφη άδεια του συγγραφέα.

Αθήνα, Ιανουάριος 2015