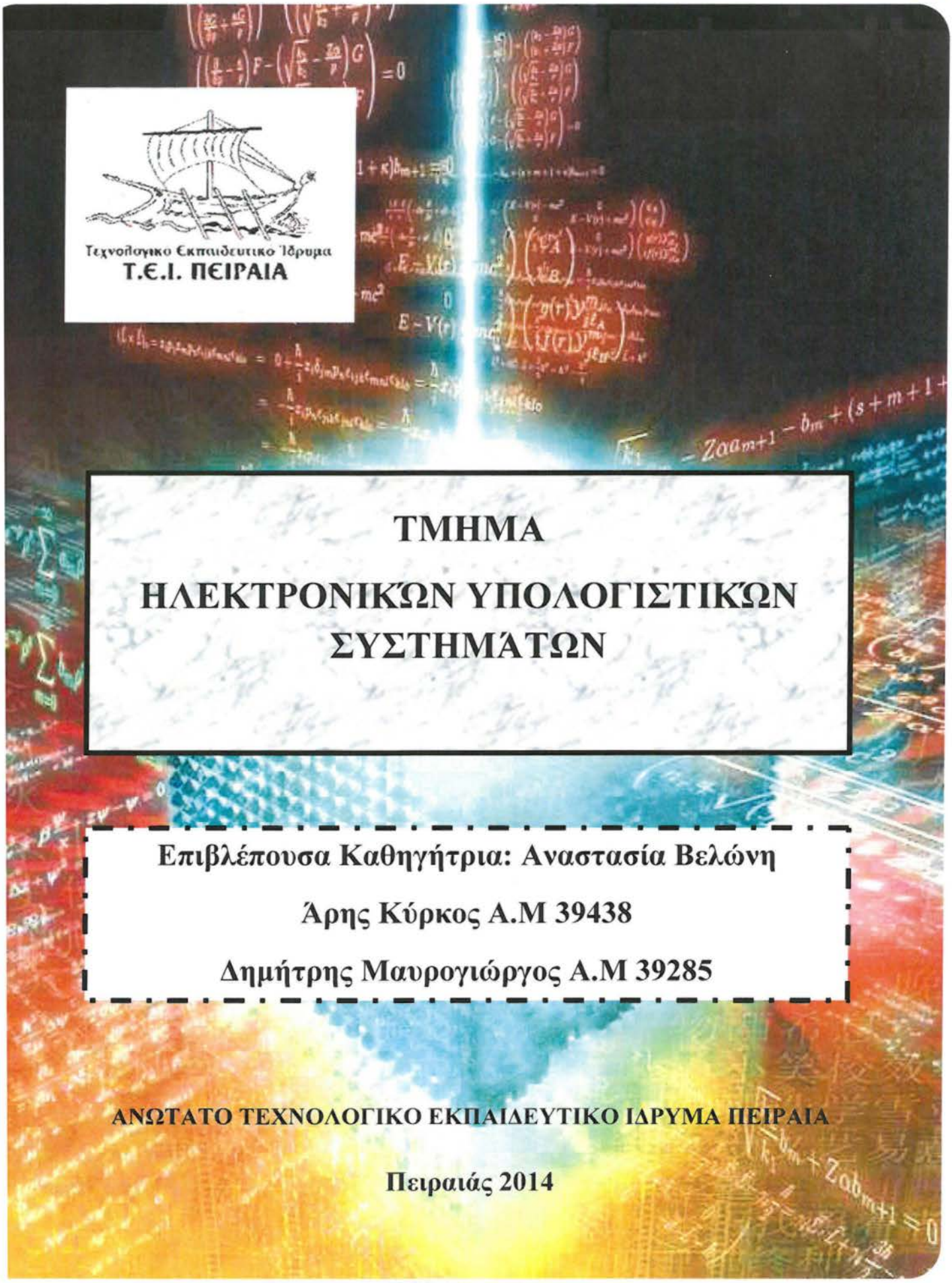


ΤΜΗΜΑ
ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Επιβλέπουσα Καθηγήτρια: Αναστασία Βελώνη

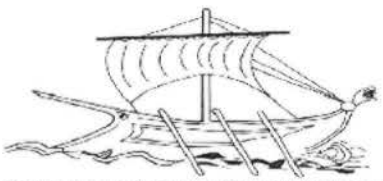
Άρης Κύρκος Α.Μ 39438

Δημήτρης Μαυρογιώργος Α.Μ 39285

ΑΝΩΤΑΤΟ ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΙΡΑΙΑ

Πειραιάς 2014

Department of Computer Systems
Technological Education Institute of Piraeus, Greece



Τμήμα Ηλεκτρονικών Υπολογιστικών Συστημάτων

Κβαντικοί Υπολογιστές

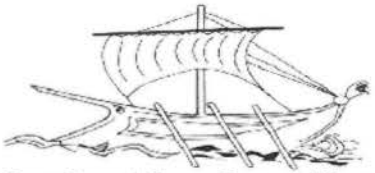
Πτυχιακή Εργασία

Άρης Κύρκος Α.Μ 39438

Δημήτρης Μαυρογιώργος Α.Μ 39285

Επιβλέπουσα Καθηγήτρια

Αναστασία Βελώνη



Department of Computer Systems.

Technological Educational Institute of Piraeus, Greece.

Quantum Computers.

Thesis

Aris Kirkos 39438

Dimitris Maurogiorgos 39285

Advisor Professor

Anastasia Beloni

Στην οικογένειά μας,

στους φίλους μας.

Ιδιαίτερες ευχαριστίες

στην καθηγήτριά μας Βελώνη Αναστασία.

Department of Computer Systems
Technological Education Institute of Piraeus, Greece

Άρης Κύρκος

Δημήτρης Μαυρογιώργος

Περίληψη

Αντικειμενικός σκοπός της παρούσας πτυχιακής εργασίας είναι η παρουσίαση των κβαντικών υπολογιστών μέσα από την τεχνολογία στους σημερινούς υπολογιστές, την θεωρία της πληροφορίας καθώς και την κβαντική θεωρία της φυσικής.

Πιο συγκεκριμένα, θα γίνει μια εισαγωγή πάνω στην κβαντική θεωρία της φυσικής , την θεωρίας της πληροφορίας και ο συνδυασμός τους για την δημιουργία ενός ακόμα τεχνολογικού επιτεύγματος τους κβαντικούς υπολογιστές.

Επίσης θα αναφερθούν τρόποι και μέθοδοι υλοποίησης αλγορίθμων που μπορούν να υλοποιηθούν πάνω στην λογική των κβαντικών υπολογιστών.

Λέξεις κλειδιά

Κβαντικός υπολογιστής, qubit, Κβαντική Φυσική, Θεωρεία της πληροφορίας, κβαντικά κυκλώματα.

Abstract

The objective of this thesis is the presentation of quantum computers through technology in today's computers, information theory and quantum theory of physics.

More specifically, it will be an introduction on the theory of quantum physics, the theory of information and the combination of them to create yet another technological achievement that is quantum computers.

Also the methods mentioned and procedures for implementation of algorithms that can be implemented on the logic of quantum computers.

Key words

Quantum computing, qubit, Quantum Physics, Information Theory, quantum circuits.

Πίνακας περιεχομένων

Κβαντικοί Υπολογιστές

Πτυχιακή Εργασία

Εισαγωγή

Αντικειμενικός σκοπός της παρούσας πτυχιακής εργασίας είναι η πλήρη κατανόηση ενίων των υπολογιστών, η κατανόηση της πληροφορίας (Κβαντικής και κλασικής) , τα μαθηματικά που κρύβονται πίσω από την τεχνολογία που μπορούμε να έχουμε στην διάθεση μας σήμερα και είναι σχεδόν σε όλα τα σπίτια του 21^{ου} αιώνα. Επίσης θα αναφερθούν τρόποι κωδικοποίησης πληροφορίας και κρυπτογράφησης. Θα αναλυθούν επίσης οι ιδέες της Κβαντομηχανικής πώς άλλαξαν τον κόσμο, καθώς και το πώς μπορούμε να σκεφτόμαστε στην σημερινή εποχή να υλοποιήσουμε μια μηχανή που να δουλεύει στον μικρόκοσμο με τους κανόνες της κβαντομηχανικής για την επίλυση πολύπλοκων υπολογισμών.

Η παρούσα πτυχιακή εργασία αποτελείται από τα ακόλουθα έξι κεφάλαια:

Κεφάλαιο 1^{ο} – Βασικές έννοιες Κβαντομηχανικής.

Στο πρώτο κεφάλαιο θα εξεταστούν οι έννοιες της κβαντομηχανικής, η ιστορία της κβαντομηχανικής (κβαντική φυσική), οι χρήσιμες έννοιες και καινούργιες ιδέες που εισήγαγε η ερμηνεία κάποιων φαινομένων από επιστήμονες που άλλαξαν την αντίληψη μας σε πολλά πράγματα που αφορούν το πώς δουλεύει ο κόσμος γύρω μας.

Κεφάλαιο 2^{ο} – Εισαγωγή στην θεωρία της πληροφορικής.

Στο δεύτερο κεφάλαιο θα γίνει μια εισαγωγή στην θεωρία της πληροφορίας στις βασικές της έννοιες καθώς επίσης θα αναλυθεί ιστορικά η πορεία της τεχνολογίας και της λογικής που διέπουν τους σημερινούς υπολογιστές.

Κεφάλαιο 3^{ο} –Βασικές έννοιες θεωρίας πληροφορίας.

Στο τρίτο κεφάλαιο θα γίνει μια ανάλυση των σημαντικότερων εννοιών της θεωρίας της πληροφορίας, τα επικοινωνιακά μοντέλα, την στατιστική ανάλυση

καθώς επίσης κάποιες έννοιες σχετικά με την κρυπτογραφία και την θεωρία κωδικοποίησης.

Κεφάλαιο 4°- Κβαντικοί Υπολογιστές.

Στο τέταρτο κεφάλαιο θα γίνει αναλυτική παρουσίαση των κβαντικών υπολογιστών θα αναλυθούν έννοιες όπως η κβαντική πληροφορία, κβαντικοί καταχωρητές, κβαντικά κυκλώματα, κβαντικοί αλγόριθμοι καθώς επίσης και κβαντική κρυπτογραφία.

Κεφάλαιο 5° – Από την θεωρία στην υλοποίηση Κβαντικών Υπολογιστών.

Στο πέμπτο κεφάλαιο θα παρουσιάσουμε τους ερευνητικούς κβαντικούς υπολογιστές όπως ένας από αυτους είναι ο υπολογιστής της google καθώς επίσης και κβαντικούς υπολογιστές της αγοράς όπως ο D-Wave.

Κεφάλαιο 6° – Συμπεράσματα.

Στο έκτο κεφάλαιο γίνεται μια αναφορά στα συμπεράσματα που έχουμε βγάλει από όλη την πορεία της πτυχιακής μας.

Κεφάλαιο 1°: Βασικές έννοιες Κβαντομηχανικής

1.1 Ιστορική Αναδρομή της Κβαντομηχανικής

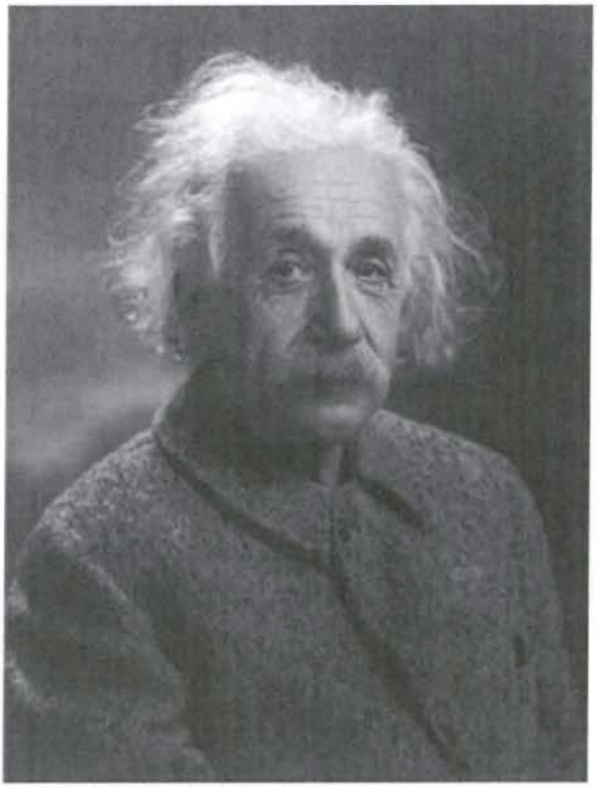
1. 1900 Max Planck

Ο Μαξ Πλανκ (Max Karl Ernst Ludwig Planck) ήταν Γερμανός φυσικός και κάτοχος Βραβείου Νόμπελ Φυσικής. Γεννήθηκε στις 23 Απριλίου 1858 στο Κίελο της Γερμανίας και πέθανε στις 4 Οκτωβρίου 1947 στο Γκέτινγκεν. Θεωρείται ως ο πατέρας της Κβαντικής Θεωρίας.

Εικόνα 1 Max Planck Πατέρας της Κβαντικής Θεωρίας.

2. **1905 Albert Einstein (φωτοηλεκτρικό φαινόμενο)**
3. **1908 Albert Einstein (κίνηση Brown)**

Ο Άλμπερτ Αϊνστάιν (γερμ.: Albert Einstein, Ουλμ 14 Μαρτίου 1879 - Πρίνστον 18 Απριλίου 1955) ήταν φυσικός γερμανοεβραϊκής καταγωγής, ο οποίος έχει βραβευθεί με το Νόμπελ Φυσικής. Είναι ο θεμελιωτής της Θεωρίας της Σχετικότητας και από πολλούς θεωρείται ο σημαντικότερος επιστήμονας του 20ού αιώνα.



Εικόνα 2 Albert Einstein .

4. 1911 Ernest Rutherford

Ο Έρνεστ Ράδερφορντ, 1ος Βαρώνος Ράδερφορντ του Νέλσον Μέλος του Τάγματος της Αξίας, Μέλος της Βασιλικής Εταιρείας (πήρε αργότερα τον τιμητικό τίτλο Βαρώνος Ράδερφορντ του Νέλσον) ήταν Νεοζηλανδός φυσικός και χημικός. Γεννήθηκε στις 30 Αυγούστου του 1871 και πέθανε στις 19 Οκτωβρίου του 1937. Ο Ράδερφορντ ανακάλυψε ότι το άτομο έχει συγκεντρωμένο το θετικό φορτίο στο κέντρο του και το αρνητικό

περιφερειακά και δημιούργησε το πλανητικό μοντέλο του ατόμου, που διαδέχτηκε το μοντέλο της "σταφίδας" του Τόμσον.

Εικόνα 3 Ernest Rutherford.

5. 1915 Niels Bohr

Ο Νιλς Μπορ (Niels Henrik David Bohr 7 Οκτωβρίου 1885 - 18 Νοεμβρίου 1962) ήταν Δανός φυσικός. Σπούδασε στο Πανεπιστήμιο της Κοπεγχάγης

και είχε θεμελιώδεις συνεισφορές στην κατανόηση της ατομικής δομής και της κβαντικής μηχανικής. Το 1911 δούλεψε με τον Έρνεστ Ράδερφορντ και το 1913 σκέφθηκε να συνδυάσει το μοντέλο του τελευταίου για τη δομή του ατόμου (όπου τα αρνητικά φορτισμένα και ελαφρά ηλεκτρόνια περιφέρονται γύρω από τον θετικά φορτισμένο και βαρύ πυρήνα) με τη Κβαντική Θεωρία του Μαξ Πλανκ. Ο Μπορ υπέθεσε στη θεωρία του ότι (α) το ηλεκτρόνιο μπορεί να ακολουθεί μόνον ορισμένες τροχιές, και όχι οποιεσδήποτε, και (β) το ηλεκτρόνιο ακτινοβολεί όχι συνεχώς, όπως ήταν η ως τότε κρατούσα άποψη, αλλά μόνο όταν αλλάζει τροχιά.

Εικόνα 4 Niels Bohr.

6. 1923 Louis de Broglie

Ο Λουί ντε Μπρολί (Louis De Broglie) ήταν γόνος μια αριστοκρατικής γαλλικής οικογένειας, που περιλάμβανε στρατηγούς, πρεσβευτές, υπουργούς εξωτερικών και τουλάχιστον ένα δούκα, τον μεγαλύτερο του αδελφό, Μορίς ντε Μπρολί. Ο Λουί ντε Μπρολί ασχολήθηκε μάλλον αργά με την θεωρητική φυσική, γιατί είχε σπουδάσει αρχικά ιστορία. Μόνον μετά τη θητεία του ως χειριστής ασυρμάτου στον Πρώτο Παγκόσμιο πόλεμο ακολούθησε το παράδειγμα του μεγάλου του αδερφού και άρχισε τις σπουδές του στην φυσική. Ο Μορίς ντε Μπρολί ήταν διακεκριμένος πειραματικός φυσικός και διεξήγαγε πειράματα στο οικογενειακό του μέγαρο στο Παρίσι.

Εικόνα 5 Louis de Broglie.

7. 1927 Werner Heisenberg

Ο Βέρνερ Χάιζενμπεργκ (Werner Heisenberg, Βύρτσμπουργκ 5 Δεκεμβρίου 1901 – Μόναχο 1 Φεβρουαρίου 1976), ήταν Γερμανός φυσικός, με σπουδαία συμβολή στη θεμελίωση της Κβαντομηχανικής, για την οποία τιμήθηκε με το Βραβείο Νόμπελ Φυσικής του 1932. Ο Χάιζενμπεργκ σπούδασε από το 1920 Θεωρητική Φυσική στο Πανεπιστήμιο του Μονάχου. Μπήκε στο πνεύμα της Κβαντικής Φυσικής — η οποία απαρτιζόταν τότε από ασύνδετα θεωρήματα — τόσο γρήγορα, ώστε μετά από μερικούς μήνες έδωσε λύσεις σε σημαντικά προβλήματα. Επειδή απαιτείτο μία ελάχιστη σπουδή έξι εξαμήνων, μόλις το 1923 μπόρεσε ο Χάιζενμπεργκ να ανακηρυχθεί διδάκτωρ. Το 1924 έγινε βοηθός του Μαξ Μπορν στο Γκέτινγκεν.

Εικόνα 6 Werner Heisenberg.

8. 1928 Erwin Schrodinger

Ο Έρβιν Σρέντινγκερ (Erwin Schrödinger, 12 Αυγούστου 1887- 4 Ιανουαρίου 1961) ήταν Αυστριακός φυσικός. Ασχολήθηκε με τη Στατιστική φυσική, τη Θερμοδυναμική, την Ηλεκτροδυναμική, την Κοσμολογία, τη Βιολογία, τη Φιλοσοφία, αλλά κυρίως με την Κβαντική φυσική, ανακαλύπτοντας την περίφημη κυματική εξίσωση που φέρει το όνομά του. Τιμήθηκε μαζί με τον Πολ Ντιράκ (Paul Dirac, 1902-1984) με το βραβείο Νόμπελ Φυσικής για τις εργασίες του πάνω στην ατομική θεωρία.

Εικόνα 7 Erwin Schrodinger .

9. 1928 Max Born

Ο Μαξ Μπορν (γερμανικά:Max Born, Μπρατισλάβα, 11 Δεκεμβρίου 1882 – Γκέτινγκεν 5 Ιανουαρίου 1970) ήταν Γερμανός μαθηματικός και φυσικός, εβραϊκής καταγωγής.

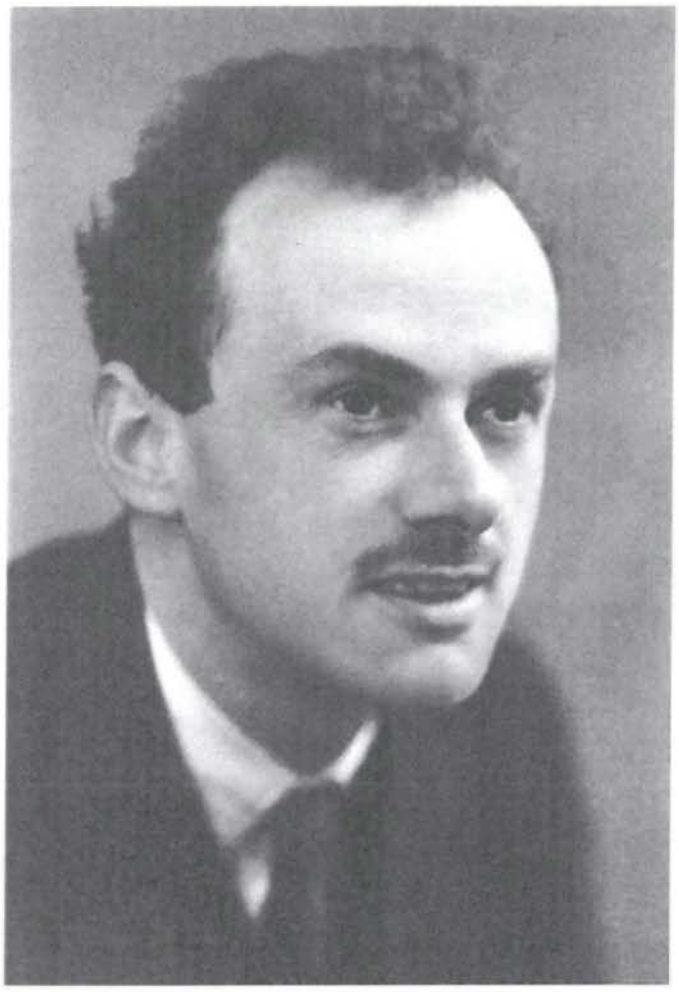
Συνέβαλε στην θεμελίωση της κβαντομηχανικής. Το 1954 του απονεμήθηκε το Βραβείο Νόμπελ Φυσικής, για την ερμηνεία που έδωσε στην κυματοσυνάρτηση του Έρβιν Σρέντιγκερ.

Εικόνα 8 Max Born.

10.1930 P.A.M. Dirac , J. von Neumann

Ο Πολ Άντριεν Μορίς Ντιράκ (αγγλ. Paul Dirac, 8 Αυγούστου 1902 - 20 Οκτωβρίου 1984), Μέλος του Τάγματος της Αξίας, Μέλος της Βρετανικής

Ακαδημίας ήταν Βρετανός θεωρητικός φυσικός. Η συμβολή του Ντιράκ στα αρχικά στάδια της Κβαντομηχανικής και της Κβαντικής Ηλεκτροδυναμικής θεωρείται πολύ σημαντική. Μεταξύ άλλων ανακαλύψεων, διατύπωσε την εξίσωση Ντιράκ, η οποία περιγράφει την συμπεριφορά των φερμιονίων, και προέβλεψε την ύπαρξη αντιύλης. Ο Ντιράκ μοιράστηκε το βραβείο Νόμπελ Φυσικής το 1933 με τον Έρβιν Σρέντινγκερ «για την ανακάλυψη νέων, παραγωγικών μορφών της ατομικής θεωρίας».



Εικόνα 9 Paul Dirac.

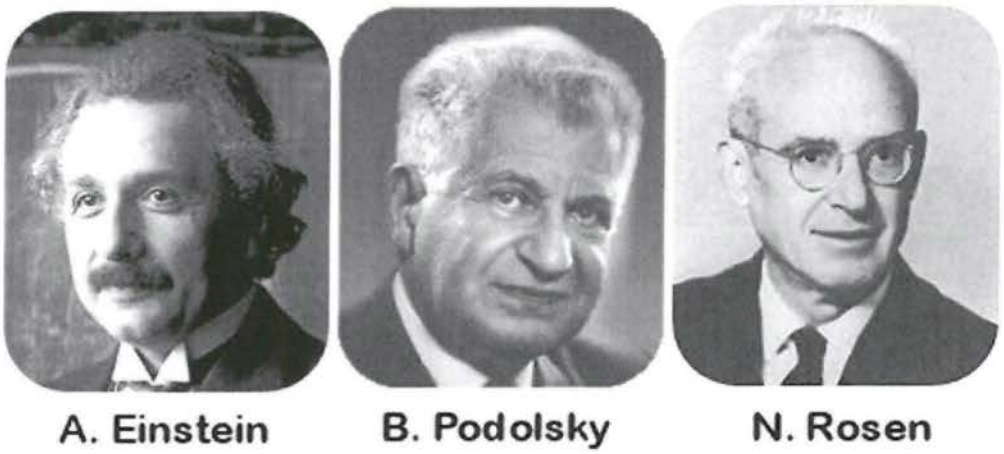
Ένας από τους σπουδαιότερους μαθηματικούς του εικοστού αιώνα, ο γεννημένος στην Ουγγαρία Γιάνος Νόιμαν (Janos Neumann, 28 Δεκεμβρίου 1903 – 8 Φεβρουαρίου 1957), (περισσότερο γνωστός ως Τζον φον Νόιμαν - τον

γερμανικό τίτλο φον τον αγόρασε ο πατέρας του), προσέφερε σε πάμπολλους κλάδους όπως μαθηματικά, φυσική, οικονομικά, πληροφορική. Από μικρό παιδί έδειξε τα μεγάλα του χαρίσματα, όταν σε ηλικία 6 ετών μπορούσε να διαιρέσει 8ψήφιους αριθμούς από μνήμης, και να απαγγέλλει από μνήμης αρχαίους κλασσικούς. Σε ηλικία 8 ετών ήξερε ήδη μαθηματική ανάλυση. Σε ηλικία 23 ετών δίδασκε στο Πανεπιστήμιο του Βερολίνου, όπου και ήταν ο νεότερος καθηγητής που υπήρξε ποτέ. Στην ίδια ηλικία απέκτησε το διδακτορικό του στα μαθηματικά από το Πανεπιστήμιο της Βουδαπέστης.

Εικόνα 10 John Von Neumann.

11.1935 EPR

Το Παράδοξο EPR (από τα αρχικά των ονομάτων των φυσικών που το διατύπωσαν το 1935: Einstein, Podolsky και Rosen) λέει πως: "Αν μπορούμε, χωρίς καθόλου να διαταράξουμε ένα σύστημα, να προβλέψουμε με βεβαιότητα την τιμή ενός φυσικού μεγέθους, τότε υπάρχει κάποιο στοιχείο φυσικής πραγματικότητας που αντιστοιχεί σ'αυτό το φυσικό μέγεθος". Το παράδοξο διατυπώθηκε σαν απόδειξη της ύπαρξης φυσικών πραγματικοτήτων, κάτι στο οποίο διαφωνούσε η κβαντική μηχανική.



Εικόνα 11 Einstein, Podolsky and Rosen.

12.1962 J. Bell

John Stewart Bell (28 Ιουνίου 1928-1 Οκτωβρίου 1990) ήταν ένας φυσικός της Βόρειας Ιρλανδίας και ο δημιουργός του θεωρήματος του Bell, ένα σημαντικό θεώρημα στην κβαντική φυσική για θεωρίες κρυφών μεταβλητών.

Εικόνα 12 John Stewart Bell.

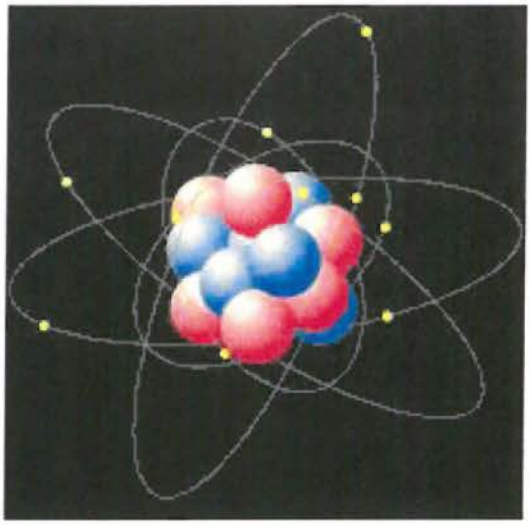
1.2.1 Βασικές έννοιες Κβαντομηχανικής

Στις αρχές του 20ού αιώνα, μερικά πειράματα παρήγαγαν αποτελέσματα που δεν θα μπορούσαν να εξηγηθούν από την κλασσική φυσική.

Ένα παράδειγμα είναι ότι εάν τα ηλεκτρόνια ήταν σε τροχιά γύρω από τον πυρήνα ενός ατόμου, με τρόπο που να έμοιαζε με τους πλανήτες που στρέφονται γύρω από τον ήλιο, η κλασσική φυσική προέβλεπε ότι τα ηλεκτρόνια θα κινούνταν σπειροειδώς συνεχώς προς τα μέσα και θα συντρίβονταν στον πυρήνα εντός εντός κλάσματος του δευτερολέπτου.

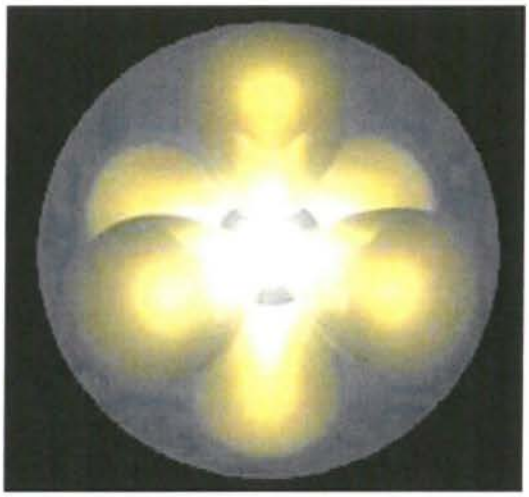
Εκείνη η λανθασμένη πρόβλεψη, μαζί με μερικά άλλα πειράματα όπως η ακτινοβολία μέλανος σώματος και το πείραμα των δύο σχισμών, έδειξε στους επιστήμονες ότι κάτι νέο απαιτείται για να εξηγήσει η επιστήμη τι συμβαίνει στο ατομικό επίπεδο.

Η παρακάτω εικόνα είναι η αντίληψη που είχαν τότε για το άτομο, με τα ηλεκτρόνια που περιστρέφονται γύρω από τον πυρήνα.



Εικόνα 13 Κλασσικό ατομικό πρότυπο.

Η νέα αντίληψη που έφερε η κβαντομηχανική για τη μορφή του ατόμου απεικονίζεται στο παρακάτω σχήμα. Η εικόνα εμφανίζει μερικά σχήματα στο χώρο, στις περιοχές των οποίων υπάρχει πιθανότατα να βρεθεί ένα ηλεκτρόνιο σε ένα άτομο υδρογόνου (ο πυρήνας είναι στο κέντρο κάθε σχήματος). Τα σχήματα αυτά ονομάζονται τροχιακά.



Εικόνα 14 Κβαντομηχανική μορφή ατόμου.

Αντί λοιπόν να έχουμε τροχιές έχουμε τροχιακά. Αντί να ξέρουμε με ακρίβεια την ακτίνα των τροχιών, γνωρίζουμε την πιθανότητα να βρούμε ένα ηλεκτρόνιο σε μια δεδομένη θέση και με δεδομένη ενέργεια.

Τα παρακάτω είναι μεταξύ των σημαντικότερων πραγμάτων που η κβαντομηχανική μπορεί να περιγράψει ενώ η κλασσική φυσική δεν μπορεί:

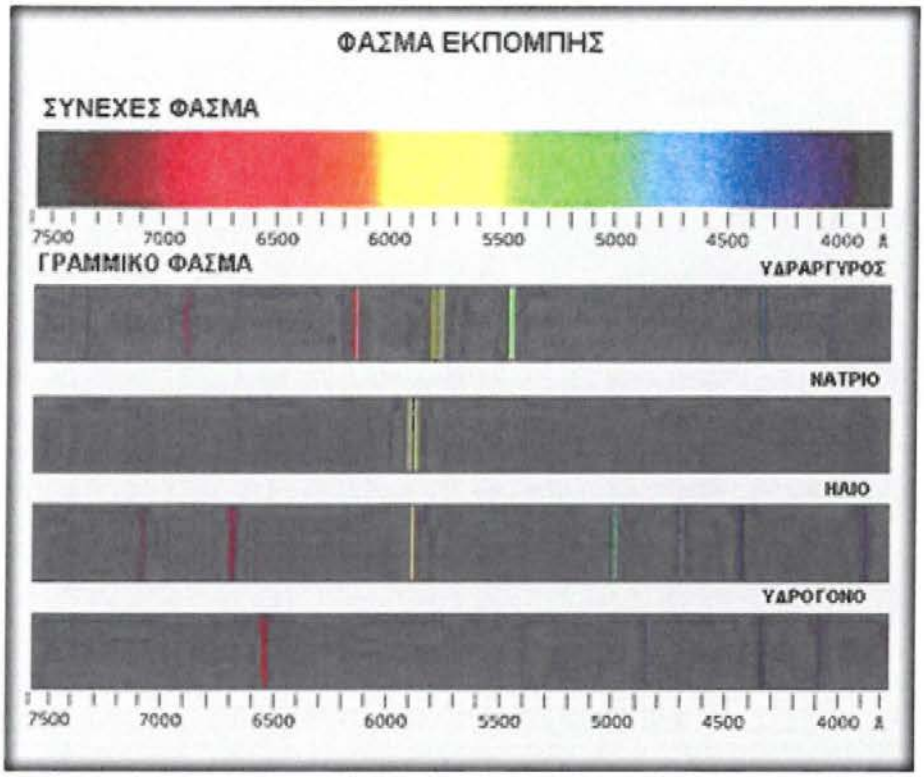
α) Διακριτότητα της ενέργειας.

β) Η δυαδικότητα του φωτός και της ύλης .

γ) Κβαντική σήραγγα.

α) Διακριτότητα της ενέργειας.

Εάν εξετάσουμε το φάσμα του φωτός που εκπέμπεται από ενεργητικά άτομα θα παρατηρήσουμε ότι αποτελείται από μεμονωμένες γραμμές διαφορετικών χρωμάτων. Αυτές οι γραμμές αντιπροσωπεύουν τα ιδιαίτερα ενεργειακά επίπεδα των ηλεκτρονίων σε εκείνα τα διεγερμένα άτομα.



Εικόνα 15 Φάσμα εκπομπής στοιχείων.

Όταν δηλαδή ένα ηλεκτρόνιο σε μια υψηλή ενεργειακή κατάσταση μεταπηδά σε μια χαμηλότερη ενεργειακή κατάσταση, το άτομο εκπέμπει ένα φωτόνιο φωτός που αντιστοιχεί στη ακριβή ενεργειακή διαφορά εκείνων των δύο επιπέδων. Όσο μεγαλύτερη είναι η ενεργειακή διαφορά, τόσο πιο ενεργητικό θα είναι το φωτόνιο, και εάν βρίσκεται στην περιοχή του ορατού φωτός, τόσο πιο κοντά θα είναι το χρώμα του στο ιώδες, στο τέλος του φάσματος. Εάν τα ηλεκτρόνια δεν ήταν περιορισμένα σε διακριτές ενεργειακές στάθμες, το φάσμα από ένα διεγερμένο άτομο θα είχε τη μορφή μιας συνεχούς διαδοχής χρωμάτων από το κόκκινο ως το ιώδες χωρίς μεμονωμένες - διακριτές γραμμές.

Τα ηλεκτρόνια μπορούν να υπάρξουν μόνο σε ιδιαίτερα ενεργειακά επίπεδα, γεγονός που τα αποτρέπει από το να κινηθούν σπειροειδώς προς τον πυρήνα, όπως προβλέπει η κλασσική φυσική. Και αυτή είναι η κβάντωση της ενέργειας, μαζί με μερικές άλλες ατομικές ιδιότητες που είναι κβαντισμένες, η οποία δίνει στην κβαντομηχανική το όνομά της.

β) Η δυαδικότητα κύματος - σωματιδίου του φωτός και της ύλης.

Το 1690 ο Christiaan Huygens πρότεινε τη θεωρία ότι το φως αποτελούνταν από κύματα, ενώ το 1704 ο Isaac Newton πρότεινε ότι το φως αποτελούνταν από μικροσκοπικά σωματίδια.

Εντούτοις, ούτε μια τέλεια θεωρία σωματιδίων, ούτε μια τέλεια κυματική θεωρία μπορούσε να εξηγήσει όλα τα φαινόμενα που συνδέονται με το φως. Δεν θα επεκταθούμε στην παρουσίαση π.χ. του πειράματος των δυο σχισμών το οποίο αναδεικνύει τις δύο αυτές όψεις, θεωρώντας το γνωστό. Θα εστιαστούμε περισσότερο στα συμπεράσματα στα οποία μας οδήγησαν τα πειράματα αυτά. Αξίζει να σημειωθεί ότι το 1923 ο Louis δε Broglie υπέθεσε ότι όχι μόνο τα κύματα έχουν σωματιδιακές ιδιότητες, αλλά και ένα υλικό σωματίδιο θα μπορούσε να έχει κυματοειδείς ιδιότητες. Και ότι 1927 αποδείχτηκε πειραματικά από τους Davisson και Germer ότι τα ηλεκτρόνια μπορούν πράγματι να συμπεριφερθούν όπως τα κύματα.

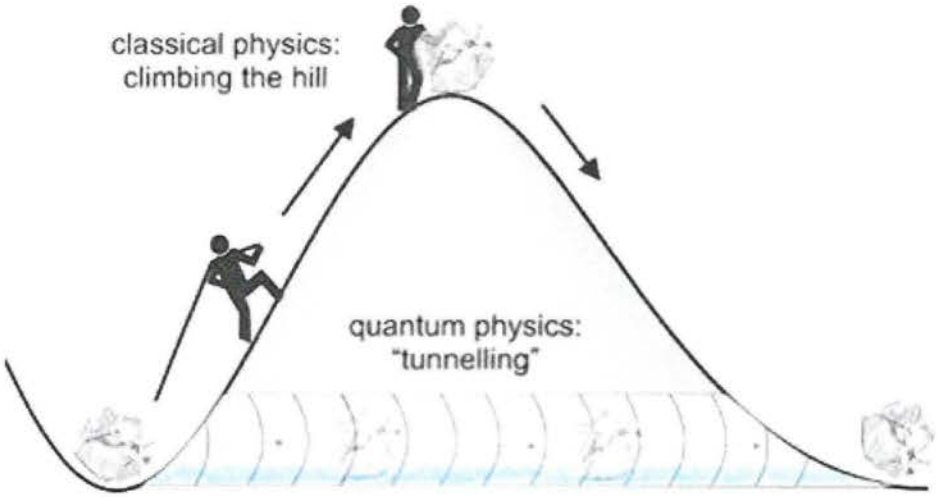
Για το πώς μπορεί κάτι να είναι και ένα σωματίδιο και ένα κύμα συγχρόνως, η απάντηση που δόθηκε σε πρώτο επίπεδο είναι η εξής: Το φως και η ύλη εντοπίζονται ως σωματίδια. Αυτό που συμπεριφέρεται σαν κύμα (εμφανίζοντας κυματικά χαρακτηριστικά όπως π.χ. η υπέρθεση, η συμβολή κ.τ.λ.), είναι η πιθανότητα να βρεθεί αυτό το σωματίδιο σε διάφορες θέσεις.

Το φως που εμφανίζεται μερικές φορές να ενεργεί όπως ένα κύμα, επειδή παρατηρούμε την συσσώρευση πολλών από τα σωματίδια του φωτός (κβάντα), κι έτσι διαμοιράζονται πάρα πολύ οι πιθανότητες για διαφορετικές θέσεις στις οποίες θα μπορούσε να είναι κάθε σωματίδιο.

γ) Κβαντική σήραγγα

Όπως αναφέρθηκε προηγουμένως, ένα κύμα καθορίζει την πιθανότητα για το πού θα βρίσκεται ένα σωματίδιο. Όταν αυτό το κύμα πιθανότητας του σωματιδίου αντιμετωπίσει ένα ενεργειακό φράγμα, το μεγαλύτερο μέρος του κύματος θα

ανακλαστεί προς τα πίσω, αλλά ένα μικρό μέρος από αυτό το κύμα "θα διαρρεύσει" μέσα στο φράγμα.



Εικόνα 16 Κβαντική Σήραγγα .

Εάν το φράγμα είναι αρκετά μικρού πάχους, το κύμα που διέρρευσε μέσα από αυτό, θα συνεχίσει την διάδοση του στη άλλη πλευρά του φράγματος. Ακόμα κι αν το σωματίδιο δεν έχει αρκετή ενέργεια να ξεπεράσει το φράγμα, υπάρχει ακόμα μια μικρή πιθανότητα, να μπορεί αυτό "να ανοίξει" μέσα στο φράγμα μια σήραγγα.

Για παράδειγμα, ας υποθέσουμε ότι ρίχνουμε μια λαστιχένια σφαίρα πάνω σε έναν τοίχο. Ξέρουμε ότι δεν έχουμε αρκετή ενέργεια για να περάσει μέσα από τον τοίχο κι έτσι αναμένουμε την σφαίρα να αναπηδά πάντα πίσω. Η κβαντομηχανική, εντούτοις, λέει ότι υπάρχει μια μικρή πιθανότητα η σφαίρα να περάσει διαμέσου του τοίχου (χωρίς την καταστροφή του) και να συνεχίσει την πορεία της από την άλλη πλευρά. Με ένα τόσο μεγάλο σώμα όσο μια λαστιχένια σφαίρα η πιθανότητα αυτή είναι τόσο μικρή ώστε και αν ακόμα ρίχναμε τη σφαίρα για δισεκατομμύρια χρόνια, δεν θα την βλέπαμε ποτέ να περνάει μέσα από τον τοίχο. Αλλά με ένα μικροσκοπικό σώμα όπως ένα ηλεκτρόνιο, το να ανοίξει μια "σήραγγα" είναι καθημερινό φαινόμενο.

1.2.2 Η κυματοσυνάρτηση και η εξίσωση Schrödinger

Τα μαθηματικά για την περιγραφή των κβαντικών φαινομένων μπορούν να διατυπωθούν με πολλούς τρόπους, αλλά ο πιο κλασικός είναι αυτός που στηρίζεται στην εξίσωσή του και στην κυματοσυνάρτηση ψ.

Η ακτινοβολία του μέλανος σώματος και το φωτοηλεκτρικό φαινόμενο οδήγησαν τον Bohr στην διατύπωση της αρχής της κβάντωσης της ενέργειας στον μικρόκοσμο. Ως κβαντωμένα μεγέθη ήδη ήταν γνωστές οι συχνότητες συντονισμού χορδών, όπως π.χ. των χορδών μιας κιθάρας με σταθερά άκρα, τα λεγόμενα στάσιμα κύματα, οπότε ο de Broglie διατύπωσε την άποψη της κυματικής φύσης της ύλης, και αυτός με την σειρά του οδήγησε τον Schrodinger στην διατύπωση της κυματικής εξίσωσης, πού περιγράφει την εξέλιξη ενός κβαντικού συστήματος.

Η εξίσωση του Schrodinger έχει την μορφή:

$$i\hbar\frac{\partial\Psi}{\partial t} = \frac{\hbar^2}{2m}\nabla^2\Psi + \nabla\Psi \qquad (1)$$

και είναι μια διαφορική εξίσωση δευτέρου βαθμού.

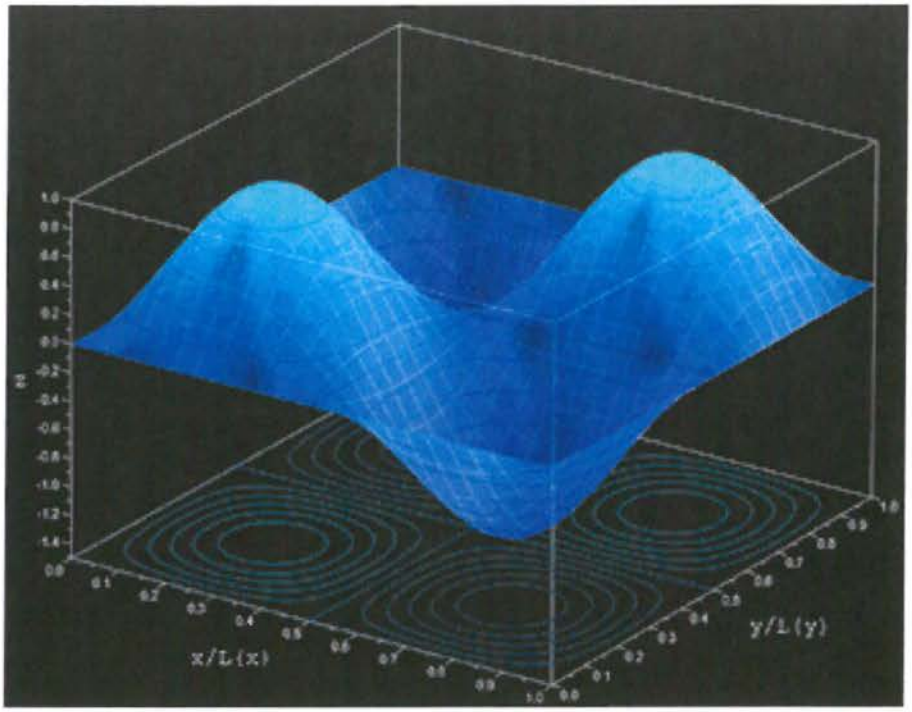
Η εξίσωση αυτή περιγράφει την εξάρτηση από την θέση και τηνεξέλιξη στον χρόνο της συνάρτησης ενός συστήματος και συμβολίζεται ως ψ(x,y,z,t). Η συνάρτηση που αντιστοιχεί σε ένα κβαντικό σύστημα ονομάζεται κυματοσυνάρτηση, επειδή είναι ανάλογη με τις συναρτήσεις που περιγράφουν την εξέλιξη των κυμάτων στην κλασική φυσική. Σε κάθε φυσικό σύστημα, μπορούμε να παρατηρήσουμε κάποια χαρακτηριστικά του φυσικά μεγέθη, π.χ. ταχύτητα, θέση, ορμή. Η ψ υπολογίζεται από την εξίσωση του Schrodinger και μας δίνει την δυνατότητα να τα υπολογίσουμε.

Υπάρχει μία ψ για κάθε κατάσταση του κβαντικού μας συστήματος και αντίστροφα για κάθε ψ αντιστοιχεί μία κατάσταση του συστήματος. Γνωρίζοντας την ψ ενός συστήματος μπορούμε να υπολογίσουμε όλα τα χαρακτηριστικά μεγέθη του συστήματος και τον τρόπο με τον όποιο αυτά εξελίσσονται στον

χρόνο. Η ψ περιλαμβάνει όλη την πληροφορία την οποία μπορούμε να ανακτήσουμε από το σύστημα μας.

Στην κλασική φυσική η αντίστοιχη εξίσωση με αυτήν του Schrodinger είναι η εξίσωση κίνησης του Νεύτωνα. Από αυτήν παίρνουμε αριθμητικές τιμές για την θέση και την ταχύτητα ενός σώματος, μέσα στην εξέλιξη του χρόνου, όταν αυτό κινείται πάνω σε συγκεκριμένες τροχιές. Δεν συμβαίνει όμως το ίδιο σε ένα κβαντικό σύστημα, το οποίο περιγράφει η εξίσωση του Schrödinger, γιατί η τελευταία είναι μιγαδική: Στο αριστερό της μέρος υπάρχει το i (οπού $i^2 = -1$). Οι μιγαδικές λύσεις δεν μπορούν να αντιστοιχούν σε φυσικά μεγέθη του κλασικού κόσμου. Στον κβαντικό κόσμο, λοιπόν, δεν μας φανερώνουν παράδοξα γεγονότα μόνο τα πειράματα, άλλα και ο μαθηματικός φορμαλισμός θέτει ερμηνευτικά προβλήματα. Γιατί το ερώτημα τι είδους οντότητα είναι ένα σωματίδιο μεταξύ της αρχής και του τέλους της διαδρομής, στην λεγόμενη κβαντική κατάσταση, είναι ισοδύναμο με το τι περιγράφει η κυματοσυνάρτηση, ποιο είναι το υποκείμενο της ψ.

Αν υποθέσουμε ότι έχουμε ένα τέτοιο κβαντικό σύστημα, π.χ. ένα ηλεκτρόνιο, το οποίο είναι απομονωμένο από το περιβάλλον του. Το σύστημα αυτό θα χαρακτηρίζεται από μια σειρά φυσικών μεγεθών, π.χ. ενέργεια, ταχύτητα, στροφορμή κ.τ.λ. Τα μεγέθη αυτά χαρακτηρίζουν την (αρχική) του κατάσταση. Όταν σε μια χρονική στιγμή ξέρουμε κάποια από αυτά τα μεγέθη, τότε με την βοήθεια της αντίστοιχης ψ μπορούμε να τα υπολογίσουμε σε μια επόμενη χρονική στιγμή και επομένως να γνωρίζουμε την κατάσταση του συστήματος μας. Για κάθε ένα από αυτά τα φυσικά μεγέθη υπάρχει ένας τελεστής, ο οποίος όταν εφαρμοσθεί στην ψ μάς δίδει έναν κανόνα αντιστοίχισης για το συγκεκριμένο φυσικό μέγεθος.



Εικόνα 17 Η εξίσωση Schrödinger.

Σε σχέση με ένα φυσικό μέγεθος a (στο οποίο αντιστοιχεί ένας τελεστής A), η ψ μπορεί να αναλυθεί σε ένα άθροισμα συναρτήσεων ψ_i που λέγονται ιδιοσυναρτήσεις του A, και έχουν την ιδιότητα, η δράση του A επί της ψ_i να έχει ως αποτέλεσμα απλά τον πολλαπλασιασμό της ψ_i επί ένα πραγματικό αριθμό α_i.

$$\sum_{n=1}^{\infty} C_n \Psi_n = C_1 \Psi_1 + C_2 \Psi_2 + \cdots \qquad (2)$$

(υπέρθεση, επαλληλία, ή γραμμικός συνδυασμός) και

$$A|\Psi_i> = a_i|\Psi_i> \qquad i=1,2,\ldots \qquad (3)$$

Η ψ_i είναι μια από τις ιδιοσυναρτήσεις του τελεστή A, που αντιστοιχούν στο φυσικό μέγεθος α. Ο αριθμός α_i καλείται ιδιοτιμή του τελεστή και είναι πραγματικός αριθμός, επειδή, αξιωματικά, οι τελεστές που περιγράφουν τα φυσικά μεγέθη είναι ερμιτιανοί τελεστές. Η φυσική σημασία των α_i είναι οι διάφορες τιμές που μπορεί να πάρει το φυσικό μέγεθος α του συστήματος μας όταν προσπαθήσουμε να το μετρήσουμε. Η γνώση λοιπόν του ψ μας δίνει την

δυνατότητα να γνωρίσουμε όλες τις δυνατές τιμές ενός φυσικού κβαντικού μεγέθους. Οι τιμές αυτές μπορεί να είναι άπειρες ή πεπερασμένες.

Η ψ είναι μια μιγαδική συνάρτηση και ως τέτοια, δεν έχει φυσικό νόημα. Το γινόμενο της όμως επί την συζυγή της, δηλαδή το τετράγωνο του μέτρου της, είναι πάντα πραγματικός αριθμός, ο $|\psi|^2$. Αυτό οδήγησε τον Born στην πιθανοκρατική ερμηνεία της ψ. Σύμφωνα με αυτήν η $|\psi|^2$ περιγράφει τις πιθανότητες που έχει να πάρει ένα μέγεθος μια συγκεκριμένη τιμή. Με άλλα λόγια η διαδικασία επίλυσης της εξίσωσης του Schrödinger δεν μας δίδει μόνο τις τιμές που μπορεί να πάρει ένα φυσικό μέγεθος ενός κβαντικού συστήματος, άλλα και το πόσο πιθανή είναι η κάθε τιμή.

Αν λοιπόν θελήσουμε να μετρήσουμε το φυσικό μέγεθος α, σε κάποια συγκεκριμένη χρονική στιγμή και σε συγκεκριμένη θέση, τότε στο μετρητικό μας όργανο θα πάρουμε, μία από τις τιμές αi που μας δίδουν οι εξισώσεις (1), (2) και (3), τις ιδιοτιμές δηλαδή του Α. Σε κάθε φυσικό μέγεθος μπορεί να αντιστοιχούν πολλές ιδιοσυναρτήσεις και επομένως ιδιοτιμές. Υπάρχουν μεγέθη, όπως η ιδιοστροφορμή (σπιν), που μπορεί να πάρει πεπερασμένο αριθμό τιμών, και επομένως ο τελεστής της ιδιοστροφορμής έχει πεπερασμένο αριθμό ιδιοσυναρτήσεων και ιδιοτιμών.

Όταν κάνουμε λοιπόν μια μέτρηση, η τιμή αi του φυσικού μεγέθους α έχει πιθανότητα $|\psi(\alpha i)|^2 = |ci|^2$ να εμφανισθεί στα όργανα μέτρησης. Αν κάνουμε ένα αρκετά μεγάλο αριθμό μετρήσεων, θα δούμε ότι η κάθε τιμή του μεγέθους που μετρούμε θα είναι μία από αυτές που μας λένε οι εξισώσεις (1) και (2) και στο τέλος θα εμφανισθούν όλες και με την συχνότητα που μας δίνει ο κανόνας του Born.

Έτσι η δράση ενός (ειδικού) τελεστή επί της ψ έχει ως αποτέλεσμα τον υπολογισμό όλων των δυνατών τιμών μιας μέτρησης καθώς και των πιθανοτήτων που αντιστοιχούν σε κάθε μια από αυτές (π.χ. της ταχύτητας, ή της ενέργειας, ή της θέσης ενός σωματιδίου), μετά από την παρέλευση ενός χρόνου t, εφόσον γνωρίζουμε την τιμή των αντίστοιχων μεγεθών στην αρχή του χρονικού διαστήματος. Η αφηρημένη αυτή μαθηματική περιγραφή, σε ειδικές περιπτώσεις μπορεί να υπολογισθεί αριθμητικά και να έχουμε συγκεκριμένα νούμερα. Αυτό

όμως είναι σπάνιο. Στην πραγματικότητα αυτή η μαθηματική περιγραφή έχει μάλλον ποιοτικό χαρακτήρα.

Ας κάνουμε όλα τα παραπάνω πιο σαφή. Ας υποθέσουμε ότι ένα κβαντικό μέγεθος μπορεί να πάρει δύο τιμές, α και β με αντίστοιχες ιδιοσυναρτήσεις ψ_α και ψ_β. Εάν ψ η κυματοσυνάρτηση του συστήματος τότε:

$$\Psi = C_\alpha \Psi_\alpha + C_\beta \Psi_\beta \qquad (4)$$

Επομένως τα $|c\alpha|^2$ και $|c\beta|^2$ μας δίνουν τις πιθανότητες που υπάρχουν ώστε κατά την μέτρηση μας να πάρει το μέγεθος αυτό μία από τις δύο αυτές τιμές, ας υποθέσουμε 30% για την α και 70% για τη β. Γράφουμε με βάση την (2),

$$\Psi = \sqrt{0.3}\Psi_\alpha + \sqrt{0.7}\Psi_\beta \qquad (5)$$

Αυτό δεν σημαίνει ότι σε κάθε μέτρηση έχουμε 30% α και 70% β, αλλά α ή β. Απλά, αν κάνουμε πάρα πολλές μετρήσεις σε άπειρα στον αριθμό πανομοιότυπα συστήματα, στο 30% του συνόλου των μετρήσεων θα μετρήσουμε την τιμή α και στο 70% θα βρούμε την τιμή β.

Όταν π.χ. ένα ηλεκτρόνιο φθάνει στο τέρμα της διαδρομής του, λέμε ότι δρα ο τελεστής που αντιστοιχεί στην φωτοευαίσθητη πλάκα και παίρνουμε την συγκεκριμένη κατανομή των κροσσών συμβολής. Αν π.χ. κάνουμε ενδιάμεση μέτρηση για να δούμε από ποια σχισμή περνά το ηλεκτρόνιο, πάλι λέμε ότι δρα ένας άλλος τελεστής και η δράση του μας δίνει τα αποτελέσματα πού βλέπουμε.

Η συσχέτιση της $|\psi|^2$, με την κατανομή των πιθανοτήτων να πάρει ένα μέγεθος μια συγκεκριμένη τιμή, ήταν και η πρώτη προσπάθεια να απαντηθεί το ερώτημα της προηγούμενης παραγράφου. Δηλαδή θεωρήθηκε ότι η ψ είναι ένα κύμα πιθανότητας. Έχουμε ένα κύμα πιθανότητας που, π.χ. στο πείραμα των δύο σχισμών, χωρίζεται στα δύο και περνώντας από τις σχισμές συμβάλλει με τον εαυτό του και παράγει τα φαινόμενα συμβολής. Μια τέτοια ερμηνεία όμως βασίζεται σιωπηρώς στο ότι οι πιθανότητες, π.χ., που έχει ένα σωματίδιο να βρεθεί σε μια συγκεκριμένη θέση στον χώρο, έχουν κάποιου είδους υπόσταση, σαν να είναι κάποιου είδους υλικό κύμα, πού πυκνώνει και αραιώνει και παράγει κυματισμούς. Κάτι τέτοιο, σαν γενική τάση, δεν γίνεται δεκτό και έτσι η

πιθανοκρατική ερμηνεία γίνεται συνήθως δεκτή μόνο στο υπολογιστικό μέρος της, όπου λειτουργεί εντυπωσιακά.

Μία άλλη σημαντική κβαντική ιδιότητα είναι το ότι η εξίσωση του Schrodinger είναι γραμμική:

Αν ψ_1, ψ_2,... είναι λύσεις της εξίσωσης Schrodinger, τότε και ο γραμμικός συνδυασμός τους:

$\psi = c_1\psi_1 + c_2\psi_2 + ...$ είναι επίσης λύση που ικανοποιεί τις ίδιες συνοριακές συνθήκες (υπέρθεση, επαλληλία).

Η φυσική σημασία της γραμμικότητας είναι πολύ σημαντική και μπορεί να νοηθεί με δύο τρόπους:

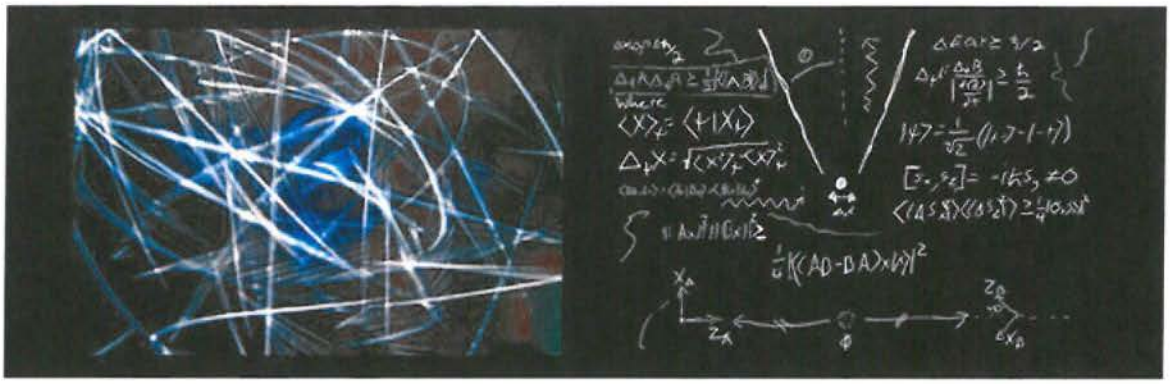
1) Ότι μια κβαντική οντότητα καθώς εξελίσσεται στον χρόνο αναλύεται σε αντίγραφα του εαυτού της και το καθένα ακολουθεί μία από τις διαδρομές που προβλέπει η ψ. Κάθε αντίγραφο εξελίσσεται εντελώς ανεξάρτητα από τα αλλά αντίγραφα. Αυτό εξηγεί πολλά από τα κβαντικά παράδοξα και είναι γνωστό στο ευρύ κοινό, ως το ότι ένα σωματίδιο μπορεί να είναι ταυτόχρονα σε περισσότερες της μιας θέσεις. Έτσι π.χ. λέμε ότι στο πείραμα των δύο σχισμών το σωματίδιο περνά κατά το ήμισυ από την μια σχισμή και κατά το ήμισυ από την άλλη.

2) Ότι μια σύνθετη οντότητα που αποτελείται από κβαντικές οντότητες θα είναι και αυτή κβαντική. Και αυτό έχει μεγάλη σημασία, όπως θα δούμε στην συνέχεια.

1.2.3 Η απροσδιοριστία

Ο δυισμός κύματος - σωματιδίου που προέκυψε από τα φαινόμενα κβάντωσης της ενέργειας και των φαινομένων συμβολής, γρήγορα συσχετίστηκε από τον Heisenberg με την απροσδιοριστία. Ο Heisenberg έκανε την συσχέτιση αυτή μέσα από μια σειρά αφηρημένων μαθηματικών συλλογισμών. Θεμέλιό τους ήταν η σκέψη ότι η κυματοσυνάρτηση ψ περιγράφει κάθε μια από τις υπερθέσεις, χωρίς να μπορούμε να διευκρινίσουμε ποια από όλες θα συναντήσουμε κατά την

εκτέλεση των πειραμάτων μας. Έτσι στο σημείο αυτό εισέρχεται η απροσδιοριστία.



Εικόνα 18 Εικόνα Απροσδιοριστίας.

Η βασική έκφραση της αρχής της απροσδιοριστίας είναι αυτή του 1927:

Εάν μετράμε τη θέση ενός σωματίου με αβεβαιότητα Δx και ταυτόχρονα μετράμε την ορμή του με αβεβαιότητα Δp, τότε το γινόμενο των δύο μεγεθών δεν μπορεί να είναι μικρότερο από έναν αριθμό της τάξης του ħ (όπου ħ= h/2π). Δηλαδή:

$$\Delta_x \Delta_p \geq \frac{\hbar}{2}$$

Οι αβεβαιότητες των μεγεθών θέσης και ορμής Δx και Δp ισούνται με τη διασπορά τους γύρω από τη μέση τους τιμή. Ο ίδιος ο Χάιζενμπεργκ εξήγησε ότι η ελάχιστη αβεβαιότητα στη μέτρηση των Δx και Δp δεν είναι πειραματικό σφάλμα, δεν οφείλεται δηλαδή στις ατέλειες των πειραματικών συσκευών, αλλά προκύπτει από τη δομή της ύλης κάθε αυτήν. Πιο συγκεκριμένα, η σχέση αβεβαιότητας είναι άμεση συνέπεια του κυματοσωματιδιακού δυϊσμού της ύλης. Σε θεωρητικό επίπεδο, είναι αποτέλεσμα των μεταθετικών σχέσεων ανάμεσα στους κβαντομηχανικούς τελεστές θέσης και ορμής.

Η σχέση αβεβαιότητας ισχύει για μεγέθη που μετρούνται στον ίδιο άξονα, για παράδειγμα για το ζευγάρι Δxx, Δpx. Όλα τα υπόλοιπα ζεύγη μεγεθών σε διαφορετικούς άξονες μπορούν να μετρηθούν ταυτόχρονα με απόλυτη ακρίβεια.

Υπάρχουν και άλλες εκφράσεις της αρχής της απροδιοριστίας. Μια από αυτές είναι η εξής:

$$\Delta_E \Delta_t \geq \frac{\hbar}{2}$$

Αυτό σημαίνει ότι υπάρχει όριο στην ακρίβεια που μπορούμε να μετρήσουμε την ενέργεια ΔΕ ενός συστήματος, αν το σύστημα παραμένει σε μια δεδομένη ενεργειακή κατάσταση για χρόνο Δt.

Η απροσδιοριστία αυτή είναι εγγενές χαρακτηριστικό του κβαντικού κόσμου. Το ερώτημα είναι αν η απροσδιοριστία είναι θέμα επιστημολογικό (δηλαδή αντανακλά τις γνωστικές δυνατότητες και περιορισμούς του ανθρώπου), αν είναι θέμα τεχνολογικό (και αντανακλά τεχνολογικές δυνατότητες και περιορισμούς του ανθρώπου), ή εντέλει είναι οντολογικής φύσης (δηλαδή ένα κβαντικό σωματίδιο «δεν μπορεί» να κατέχει ταυτόχρονα συγκεκριμένη θέση και ταχύτητα ώστε να μην έχει νόημα ο ακριβής προσδιορισμός τους ή ο ακριβής προσδιορισμός των άλλων μεγεθών).

Ακούμε συχνά να λέγεται ότι η θέση ενός σωματιδίου «παίζει», γιατί καθώς πάμε να το εντοπίσουμε, το ενοχλούμε λίγο. Αυτό υπονοεί ότι αν δεν πάμε να το εντοπίσουμε τότε αυτό θα έχει μια σαφή θέση. Αυτή η ερμηνεία προέρχεται από μια θετικιστική κοσμοθεωρητική στάση που έρχεται σε αντίθεση με φαινόμενα που μας υποδεικνύουν ότι η απροσδιοριστία δεν είναι τεχνικής φύσης, αλλά οντολογικής. Αν οι Bohr και Heisenberg κατανοούσαν την αρχή θετικιστικά ήταν λόγω της έλλειψης πειραματικών δεδομένων που υπάρχουν σήμερα και καθιστούν μια τέτοια προσέγγιση ανεπαρκή. Τα τσιπ πυριτίου λειτουργούν χάρις στην οντολογική διάσταση της απροσδιοριστίας και τα φαινόμενα σήραγγος που αυτή συνεπάγεται.

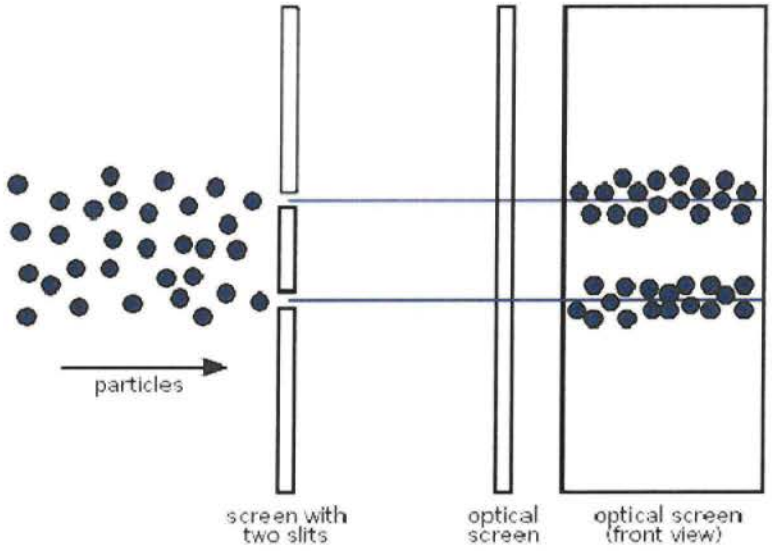
Η εξίσωση Schrödinger, όσον αφορά σε ένα μονωμένο σωματίδιο, είναι αρκετά απλή και μπορεί να επιλυθεί. Όταν δύο τέτοια σωματίδια συγκρούονται μεταξύ τους με αποτέλεσμα να συντίθενται, τότε το φαινόμενο μπορεί να μελετηθεί αριθμητικά (και σε μερικές περιπτώσεις αναλυτικά). Η γραμμικότητα της ψ δείχνει (αλλά και το πείραμα επιβεβαιώνει) ότι προκύπτει ένα σωματίδιο που περιγράφεται από μια κυματοσυνάρτηση που έχει τις ίδιες γραμμικές ιδιότητες με αυτές των αρχικών κυματοσυναρτήσεων. Το ίδιο ισχύει και για κάπως πιο συνθέτες περιπτώσεις.

Η λογική λοιπόν των μαθηματικών μας κάνει να πιστεύουμε ότι η ίδια διαδικασία μπορεί να συνεχίζεται επ' άπειρο και επομένως ότι και τα πλέον σύνθετα αντικείμενα θα περιγράφονται από μια κυματοσυνάρτηση που είναι σύνθεση των κυματοσυναρτήσεων στοιχείων που τα απαρτίζουν. Αυτό θα μπορούσε θεωρητικά να επεκταθεί για όλο το σύμπαν.

Ωστόσο η απαίτηση ώστε ένα απομονωμένο μεν, μακροσκοπικό δε, σύστημα να περιγράφεται από μια κυματοσυνάρτηση προϋποθέτει ότι το σύστημα παρουσιάζει πότε κάποια χαρακτηριστικά και πότε άλλα, κάτι το οποίο η παρατήρησή μας λέει ότι δεν συμβαίνει.

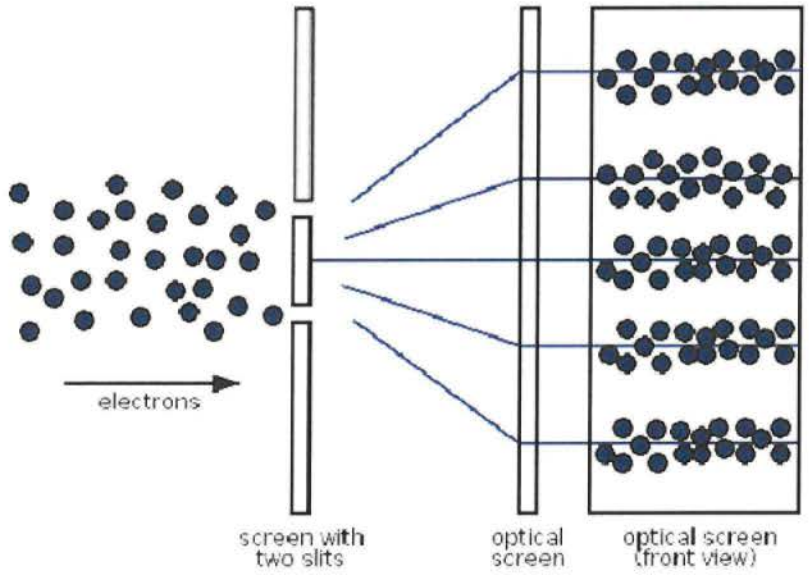
Αυτήν την συλλογιστική μπορούμε να εφαρμόσουμε και να επιβεβαιώσουμε για πολύ απλά συστήματα. Για έστω και λίγο πιο πολύπλοκα, όπως π.χ. το άτομο του ηλίου τα πράγματα γίνονται απαγορευτικά σύνθετα. Στην πραγματικότητα δεν μπορούμε να ξέρουμε ακριβώς τι συμβαίνει. Ωστόσο κόσμος στον οποίο ζούμε δεν εμφανίζει κβαντικά χαρακτηριστικά σε μακροσκοπικό επίπεδο. Αυτό οδηγεί στην ιδέα ύπαρξης ενός σημείου μετάβασης πέρα από το οποίο παύουν να υπάρχουν υπερθέσεις και τα συστήματα έχουν καλώς ορισμένες φυσικές ιδιότητες.

Το ότι η σύνθετη κυματοσυνάρτηση παύει να είναι κυματοσυνάρτηση με κβαντικά χαρακτηριστικά το ονομάζουμε κατάρρευση της κυματοσυνάρτησης και συμβαίνει κάποια στιγμή που δεν μας είναι φανερή. Το πότε, το γιατί και το πώς συμβαίνει αυτό είναι άγνωστο. Το ερώτημα αυτό προέκυψε ιστορικά όταν έγινε προσπάθεια να καταλάβουμε τι συμβαίνει κατά τη διάρκεια των μετρήσεων (και γι' αυτό ονομάστηκε μετρητικό πρόβλημα της κβαντομηχανικής). Π.χ. στο πείραμα των δύο σχισμών έχουμε την κατάρρευση της ψ είτε όταν παρατηρούμε το ηλεκτρόνιο είτε όταν φτάνει στην φωτογραφική πλάκα.



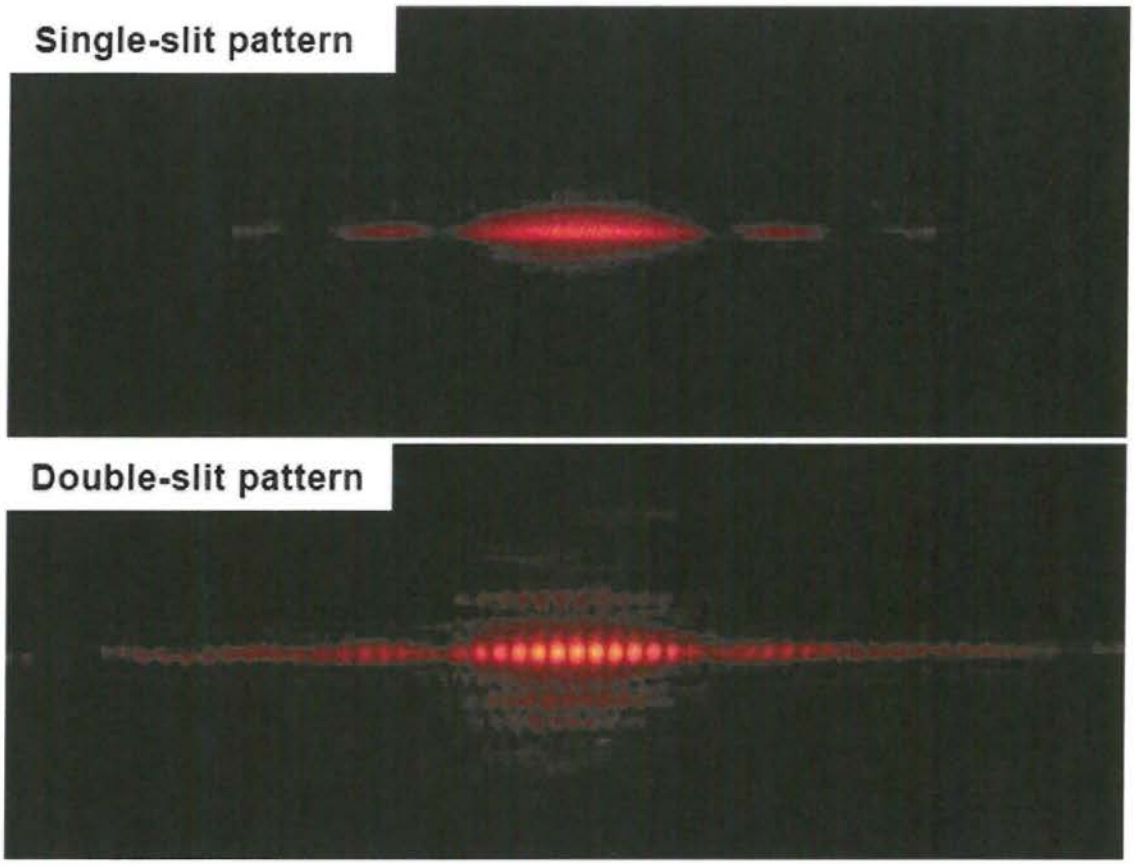
Εικόνα 19 Κλασσικά σωματίδια μέσα από σχισμή.

Συμβαίνει όμως όντως κατάρρευση της κυματοσυνάρτησης και αν ναι, τι την προκαλεί; Η αρχική πρόταση του von Newmann, να συνδέσει την κατάρρευση με την μέτρηση και τη μετρητική συσκευή, οδήγησε τον Eugene Wigner στην συσχέτιση της κατάρρευσης με την παρατήρηση, δηλαδή με την ύπαρξη μιας συνείδησης.



Εικόνα 20 Ηλεκρόνια μέσα από σχισμή. Συμπεριφορά κύματος.

Ένα άλλο σημαντικό ζήτημα που προκύπτει είναι αυτό της αιτιότητας. Η ίδια η κυματοσυνάρτηση είναι ντετερμινιστική. Ωστόσο η κυματοσυνάρτηση υπολογίζει όλες τις δυνατές υπερθέσεις και την πιθανότητα να συμβεί κάθε μια από αυτές. Δεν μας λέει τίποτα για το ποια από αυτές θα εμφανιστεί όταν κάνουμε τη μέτρηση. Κι εδώ εμφανίζεται ο μη ντετερμινιστικός παράγων.

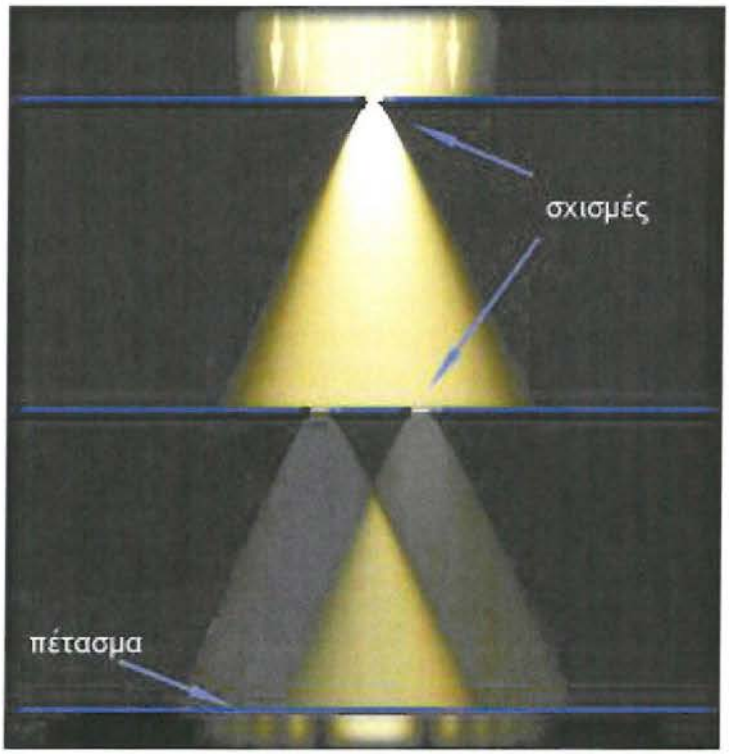


Εικόνα 21 Πείραμα Laser.

1.2.4 Τι είναι μια κβαντική οντότητα.

Το ερώτημα του τι είναι μια κβαντική οντότητα παραμένει ανοιχτό. Το πρόβλημα φαίνεται να προκύπτει από το ότι οι καθημερινές μας παραστάσεις δεν έχουν κάτι ανάλογο με μια κβαντική οντότητα. Έτσι υπάρχει η ανάγκη κατανόησης των κβαντικών οντοτήτων με μια περιγραφή που περιλαμβάνει κλασικές έννοιες. Αυτό επιχειρούν οι ερμηνείες της κβαντομηχανικής. Ο φορμαλισμός της κβαντομηχανικής δεν αρκεί για να μας εξηγήσει τι ακριβώς συμβαίνει.

Στο πείραμα των δύο σχισμών φανερώνεται ο δυϊσμός κύματος και σωματιδίου. Λέγοντας ότι το ηλεκτρόνιο στο πείραμα αυτό εμφανίζει κυματικά χαρακτηριστικά και περνά κατά το ήμισυ από την κάθε μια σχισμή, ναι μεν κάνουμε μια μαθηματική περιγραφή αλλά δεν εξηγούμε τι είναι το ηλεκτρόνιο. Τέτοια ερωτήματα φαίνεται πως δεν μπορούν να απαντηθούν χωρίς την αποδοχή κάποιων υποθέσεων που ενδέχεται να είναι μεν επιστημολογικά αυτοσυνεπείς, αλλά δεν παύουν να είναι υποθέσεις.



Εικόνα 22 Πείραμα Δύο Σχισμών.

1.2.5 Η ερμηνεία της Κοπεγχάγης

Σε γενικές γραμμές μπορούμε να διακρίνουμε δύο ερμηνευτικές τάσεις της Κβαντομηχανικής. Η μία ξεκίνησε ως ερμηνεία που συγγενεύει με τον λογικό θετικισμό και εκφράζεται από τη σχολή της Κοπεγχάγης και η άλλη με τον ρεαλισμό που είχε κύριο αρχικό εκφραστή τον Αϊνστάιν.

Σήμερα κυρίαρχη τάση θεωρείται η πρώτη, αν και φαίνεται να έχει αποδεσμευτεί από τον θετικισμό. Ο θετικισμός δίνει απόλυτη προτεραιότητα στα αισθητηριακά δεδομένα και στις έννοιες που προκύπτουν από αυτά και όχι στα όντα. Η φιλοσοφία αυτή παρακάμπτει τα ερμηνευτικά και οντολογικά προβλήματα της φυσικής. Έτσι απαλλάσσει την κβαντομηχανική από αυτά τα δύσκολα ερωτήματα ισχυριζόμενη ότι δεν έχουν νόημα. Π.χ. το ερώτημα για τη φύση του ηλεκτρονίου στερείται νοήματος και οι δυσχέρειες κατανόησης που έχουμε προέρχονται από την παραπλανητική μας επιθυμία να «δούμε πίσω» από τα πειραματικά δεδομένα και τις εξισώσεις που τα περιγράφουν.

Η θέση του θετικισμού έχει έναν αντιμεταφυσικό χαρακτήρα. Ο Καντ είχε δείξει ότι η γνώση που έχουμε για τον κόσμο δεν μπορεί να είναι άμεση, επομένως το ερώτημα για τα πράγματα καθ' εαυτά έχει μεταφυσικό χαρακτήρα. Ο θετικισμός ήταν η αντίδραση απέναντι στη μεταφυσική και τον ιδεαλισμό και γι' αυτό αρνείται οποιαδήποτε οντολογία. Από την άποψη αυτή, μόνο επιφανειακή ομοιότητα υπάρχει μεταξύ του θετικισμού και της σχολής της Κοπεγχάγης. Στον πυρήνα της ερμηνείας της υπάρχει η θέση ότι δεν έχει νόημα να συζητάμε για τη φύση του κβαντωμένου σωματιδίου. Αλλά όχι για λόγους αρχής, όπως στον θετικισμό, αλλά για το λόγο ότι η φύση αυτή δεν μπορεί να προσεγγιστεί με κλασικούς όρους. Η σχολή δεν αρνείται την ύπαρξη κβαντικής φύσης, αλλά θεωρεί ότι οι γνωστικές και λεκτικές δυνατότητες του ανθρώπου δεν επαρκούν για να την περιγράψουν. Απλά μπορούν να πουν κάποια πράγματα για αυτήν. Ο Bohr εισήγαγε την αρχή της συμπληρωματικότητας σύμφωνα με την οποία η φύση του σωματιδίου είναι τέτοια που μπορούμε να την περιγράψουμε με δύο διαφορετικούς αλλά αμοιβαία αποκλειόμενους τρόπους. Ισχυρίστηκε ότι οι δύο τρόποι συνιστούν την οντολογία του σωματιδίου και ότι η περιγραφή αυτή έχει νόημα αποκλειστικά στα πλαίσια του πειράματος. Το πείραμα είναι αυτό που

καθορίζει ποιος από τους δύο τρόπους περιγραφής της κατανόησης του σωματιδίου είναι ο κατάλληλος.

Εικόνα 23 Κβαντική οντότητα.

Οι συσκευές μετρούν μεγέθη κλασικής οντολογίας και αυτά τα φυσικά μεγέθη υπολογίζει ο μαθηματικός φορμαλισμός. Για παράδειγμα, η ταχύτητα ορίζεται στα πλαίσια των κλασικών περιγραφών. Μπορεί να οριστεί με τον ίδιο τρόπο και στον κβαντικό κόσμο; Ο Bohr λέει όχι ακριβώς αλλά υπάρχει κάποιο κβαντικό μέγεθος που είναι ανάλογο με την ταχύτητα (αρχή της αντιστοιχίας). Αυτό το μέγεθος μπορούμε να το ορίσουμε μόνο σε σχέση με το πείραμα που εκτελούμε. Δηλαδή κάθε σωματίδιο δείχνει διαφορετικό πρόσωπο ανάλογα με αυτό που θέλουμε να μετρήσουμε και με τον τρόπο που το κοιτάμε. Για παράδειγμα, στο πείραμα των δύο σχισμών, αν κοιτάξουμε το ηλεκτρόνιο, αυτό θα συμπεριφερθεί σαν σωματίδιο. Αν δεν το κοιτάξουμε θα συμπεριφερθεί σαν κύμα.

Έτσι δεν έχει νόημα να ψάχνουμε για την ενιαία φύση του της κβαντικής οντότητας. Η ερμηνεία της Κοπεγχάγης λέει ότι δεν έχει νόημα να συζητάμε για την ερμηνεία της ψ.

Η αρχή της συμπληρωματικότητας είναι ο οντολογικός πυρήνας της ερμηνείας της Κοπεγχάγης. Είναι ένα βήμα πέραν του θετικισμού αφού μιλά για το «είναι» των σωματιδίων. Αλλά μας αποτρέπει από να ζητούμε πλήρη ερμηνεία. Στην

πραγματικότητα αφήνει εκκρεμές ένα καίριο ερώτημα: Η συμπληρωματικότητα είναι αρχή οντολογικής ή επιστημολογικής φύσης; Μια κβαντική οντότητα είναι είτε κύμα είτε σωματίδιο ή μια κβαντική οντότητα μπορούμε να τη γνωρίσουμε είτε ως κύμα είτε ως σωματίδιο;

1.2.6 Η αντίδραση στη Σχολή της Κοπεγχάγης.

Ο φορμαλισμός της κβαντομηχανικής ακολουθεί πολλούς διαφορετικούς δρόμους που θεωρούνται ισοδύναμοι μεταξύ τους και οδηγούν στα ίδια αποτελέσματα. Οι περισσότεροι φυσικοί ασχολούνται με τις πρακτικές εφαρμογές του χωρίς να ενδιαφέρονται για το ερμηνευτικό κενό που υπάρχει. Τους ενδιαφέρουν τα φαινόμενα και όχι το τι «κρύβεται» από πίσω τους και τα προκαλεί.

Εικόνα 24 Μπορ - Αϊνστάιν.

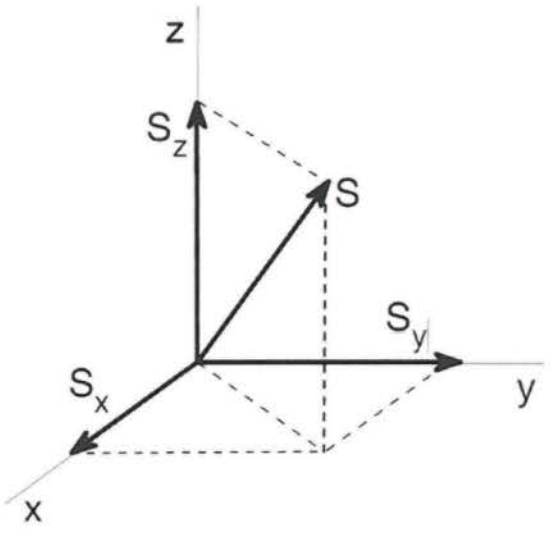
Σε ένα πρώτο επίπεδο, το οντολογικό ενδιαφέρον αφορά στην απόδοση συγκεκριμένων και σαφώς προσδιορισμένων ιδιοτήτων στην οντότητα (οι οποίες έχουν συγκεκριμένες τιμές). Αυτό για τους περισσότερους φυσικούς εξαντλεί τον οντολογικό ρεαλισμό. Για τους φιλοσόφους όμως το πρόβλημα δεν σταματά εδώ. Το πρόβλημα μετατίθεται στο τι σημαίνουν αυτές οι τιμές. Π.χ. τι μπορεί να σημαίνει η τιμή της ιδιοστροφορμής ενός ηλεκτρονίου, που εμφανίζει κυματική συμπεριφορά και έχει συγκεκριμένο μήκος κύματος; Ποιο είναι το διαισθητικό νόημα της περιστροφής ενός κύματος γύρω από τον εαυτό του; Αν δεν υπάρχει

τέτοιο νόημα, καταλήγουμε στο ότι ένα σωματίδιο είναι απλά μια σειρά από τιμές που αποδίδονται σε μη κατανοητά μεγέθη.

Αυτές οι λεπτές διευκρινήσεις δεν είναι πάντοτε ορατές στα έργα των θεωρητικών φυσικών. Κι αυτό γιατί το δεύτερο μέρος του οντολογικού ερωτήματος αποτελεί μεταφυσικό ερώτημα. Υπάρχουν, λοιπόν, ερμηνείες της κβαντομηχανικής που θεωρούν ότι λύνουν το ερμηνευτικό πρόβλημα της κβαντομηχανικής, ενώ ασχολούνται αποκλειστικά με το πρώτο επίπεδο, χωρίς να εξηγούν ποια είναι η φυσική σημασία αυτών που ερμηνεύουν. Από την άλλη υπάρχουν ερμηνείες που ασχολούνται και με το δεύτερο αλλά διακηρύσσουν ότι δεν κάνουν οντολογία ή μεταφυσική, λόγω του ότι οι λέξεις αυτές είναι κακόηχες για πολλούς φυσικούς.

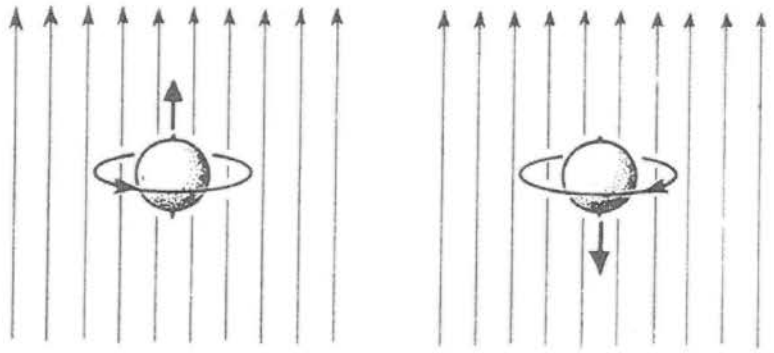
Όλα τα σωματίδια (άτομα, πυρήνες, ηλεκτρόνια, πρωτόνια, φωτόνια κλπ.) χαρακτηρίζονται από μια ιδιότητα που λέγεται σπιν ή ιδιοστροφορμή. Θα μπορούσαμε να παρομοιάσουμε αυτό το κβαντομηχανικό μέγεθος με τη στροφορμή που δημιουργεί τον 24-ώρο κύκλο της Γης.

Το σπιν των σωματιδίων είναι ένα διανυσματικό μέγεθος και επομένως μπορεί να παρασταθεί ως προς κάποιο σύστημα αξόνων Oxyz. Δηλαδή το σπιν καθορίζεται πλήρως αν γνωρίζουμε τις τρεις συνιστώσες Sx, Sy, Sz, που είναι οι προβολές του στους άξονες x, y και z.Σύμφωνα με τους κανόνες της Κβαντομηχανικής οι τρεις συνιστώσες της στροφορμής Sx, Sy, Sz δεν μπορούν να προσδιοριστούν συγχρόνως. Μόνο η μια μπορεί να προσδιοριστεί με ακρίβεια.



Εικόνα 25 Ανάλυση του διανύσματος του σπίν σε τρεις συνιστώσες.

Ας περιοριστούμε στην περίπτωση ενός πρωτονίου (ή ενός ηλεκτρονίου). Αν αυτό βρεθεί μέσα σ' ένα ομογενές μαγνητικό πεδίο το σπιν του μπορεί να προσανατολιστεί είτε παράλληλα είτε αντιπαράλληλα προς τις δυναμικές γραμμές. Στις δύο αυτές δυνατότητες προσανατολισμού μπορούμε να δώσουμε τις τιμές +1 και −1 (σε κάποιες μονάδες στροφορμής) ή όπως συχνά λέμε επάνω (↑) και κάτω (↓), αντίστοιχα.

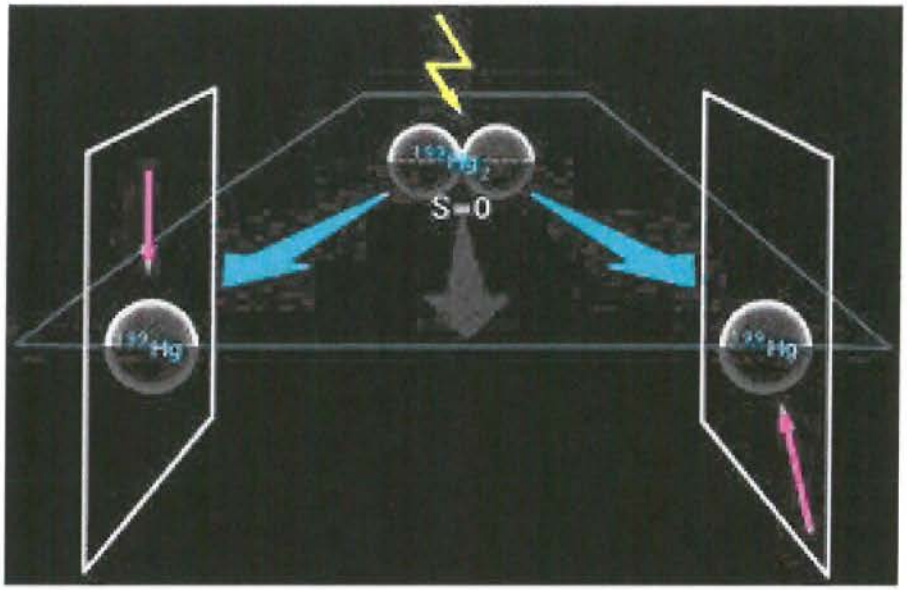


Εικόνα 26 Προσανατολισμός του σπίν σε ομογενές μαγνητικό πεδίο.

Ο θετικισμός διαπραγματεύεται την κβαντομηχανική αποκλειστικά στα όρια της επιστημολογίας και αγνοεί εντελώς το οντολογικό ερώτημα. Η ερμηνεία της Κοπεγχάγης, όπως είπαμε, κάνει ένα άνοιγμα προς το πρώτο επίπεδο οντολογίας με την αρχή της συμπληρωματικότητας και αποδίδει στις πιθανότητες των κβαντικών φαινομένων οντολογικό και όχι επιστημολογικό χαρακτήρα. Παραδέχεται την ύπαρξη οντοτήτων που συνιστούν τον μικρόκοσμο αλλά ασχολείται αποκλειστικά με το πρώτο επίπεδο του οντολογικού ερωτήματος. Και θεωρεί ότι τα σωματίδια έχουν σαφώς ορισμένες ιδιότητες που εξαρτώνται -σε επίπεδο οντολογίας- από τον τρόπο με τον οποίο γίνεται η μέτρηση. Όμως δεν εξετάζει το καθ' αυτό οντολογικό πρόβλημα της φύσης των οντοτήτων και παραμένει στα όρια των πειραμάτων και των μετρήσεων.

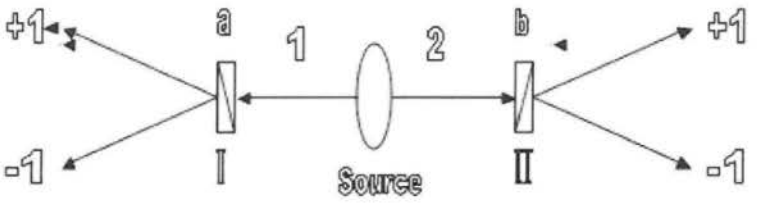
Η ιδέα ότι δεν μπορούμε να μελετήσουμε τα όντα καθ' αυτά κι ότι τα όντα του μικρόκοσμου έχουν ιδιότητες που εξαρτώνται από την παρατήρηση προκάλεσαν σοβαρές αντιδράσεις. Ο Einstein αντέδρασε πρώτος σε αυτή τη θετικιστική χροιά

της ερμηνείας αυτής. Ήταν ρεαλιστής, δηλαδή πίστευε ότι για κάθε φυσικό μέγεθος που προβλέπεται από κάθε θεωρία αντιστοιχεί και κάτι πραγματικό που πρέπει να περιγραφεί με ακρίβεια. Επομένως αν μια θεωρία δεν μπορεί να μας πει π.χ. τα χαρακτηριστικά του ηλεκτρονίου, αυτό δεν σημαίνει ότι το ηλεκτρόνιο δεν έχει σαφή χαρακτηριστικά, αλλά ότι έχει πρόβλημα η θεωρία.



Εικόνα 27 Πείραμα EPR.

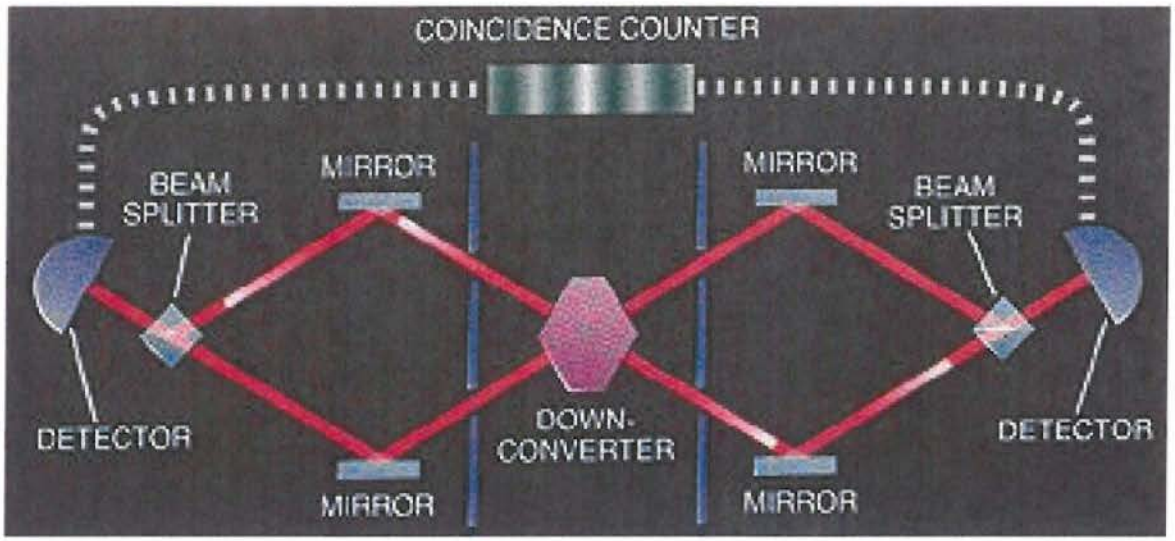
Για να δείξει λοιπόν την ανεπάρκεια της θεωρίας, παρουσίασε ένα τυπικό νοητικό πείραμα, μαζί με τους Poldosky και Rosen (πείραμα E.P.R.), στο οποίο αποδείκνυε ότι αν η κβαντική θεωρία είναι σωστή, τότε μπορούμε να παράγουμε δύο σωματίδια που να είναι συσχετισμένα μεταξύ τους ώστε να συμβαίνει το εξής: Κάνοντας μια μέτρηση στο ένα από τα δύο συζευγμένα σωματίδια (δηλαδή δύο σωματίδια που έχουν την ίδια κυματοσυνάρτηση), τότε κατά τη μέτρηση του ενός (κατά την οποία μια ιδιότητά του παίρνει συγκεκριμένη τιμή), και στο δεύτερο σωματίδιο η ιδιότητα αυτή αναγκάζεται να πάρει την συγκεκριμένη τιμή. Μάλιστα ο εξαναγκασμός αυτός γίνεται σε χρόνο μηδέν, όσο μεγάλη και να είναι η απόσταση που χωρίζει τα δύο σωματίδια (παραβιάζοντας την αρχή της θεωρίας της σχετικότητας για μέγιστη ταχύτητα c). Αν μπορεί να συμβεί αυτό, τότε μπορούμε στο πρώτο μεν σωματίδιο να μετρήσουμε την ορμή του και στο δεύτερο τη θέση του. Έτσι είναι δυνατόν να ξέρουμε και την θέση και την ορμή και των δύο σωματιδίων ταυτόχρονα, κάτι το οποίο δεν επιτρέπεται από τη θεωρία. Άρα η κβαντική θεωρία είναι λάθος.



Εικόνα 28 Θεωρία του Bell.

Η απάντηση του Bohr ήταν ότι η ύπαρξη ενός σωματιδίου και κατ' επέκταση μιας φυσικής ιδιότητας (όπως η θέση και η ορμή) είναι συνυφασμένη με μια πράξη μέτρησης. Εφ' όσον στο δεύτερο σωματίδιο δεν κάνουμε μέτρηση, το να λέμε ότι η ορμή του ή η θέση του είναι γνωστές, είναι κάτι που δεν έχει νόημα. Γιατί η θέση και η ορμή έχουν νόημα μόνο μέσα από την πράξη της μέτρησης. Στην πραγματικότητα όμως η κατάρριψη του επιχειρήματος του Einstein έγινε το 1982 όταν στο Aspect πραγματοποιήθηκε το περίφημο νοητικό πείραμα. Το πείραμα δικαίωσε πλήρως τις προβλέψεις της κβαντικής θεωρίας και επαληθεύτηκε πολλές φορές.

Το 1964 ο Bell απέδειξε το περίφημο θεώρημα του Bell, σύμφωνα με το οποίο για να είναι μια θεωρία τοπική (δηλαδή να μην επιτρέπει δράση από απόσταση και να υπακούει στον ρεαλισμό του Einstein) πρέπει να υπακούει σε μια σειρά ανισοτήτων. Στα κβαντικά φαινόμενα παραβιάζονται αυτές οι ανισότητες κι επομένως η κβαντική θεωρία που τα περιγράφει είναι μη τοπική. Τα πειράματα επιβεβαιώνουν την παραβίαση των ανισοτήτων του Bell. Όλα αυτά φαίνεται πως δείχνουν ότι η κλασική αντίληψη για τα πράγματα δεν μπορεί να εφαρμοστεί στον μικρόκοσμο. Ωστόσο υπήρξαν και θεωρίες που προσπάθησαν να εξαλείψουν τις «παραδοξότητες» και να επαναφέρουν την κλασική αντίληψη.



Εικόνα 29 Πείραμα Aspect πάνω στο θεώρημα Bell.

Σύμφωνα με τους de Broglie και Bohm τα παραπάνω παράξενα συμβαίνουν επειδή υπάρχουν κάποιες κρυμμένες μεταβλητές που περιγράφουν την πραγματικότητα και τις οποίες η θεωρία δεν τις λαμβάνει υπόψη και επομένως πρέπει να συμπληρωθεί για να είναι πλήρης. Η θεωρία αυτή έκανε πολλούς φυσικούς να πιστεύουν ότι υπάρχει μια πραγματικότητα στον μικρόκοσμο.

Ο Bell (1964) πρότεινε τη διεξαγωγή ενός πειράματος που θα αποδείκνυε την ύπαρξη αυτών των κρυμμένων μεταβλητών. Σύμφωνα με το Bell αν ισχύει η τοπικότητα και υπάρχουν οι κρυμμένες μεταβλητές πρέπει να ισχύουν κάποιες ανισότητες. Αν παραβιάζονται αυτές οι ανισότητες τότε οι μεταβλητές αυτές δεν υπάρχουν και ισχύει η μη τοπικότητα στο μικρόκοσμο.

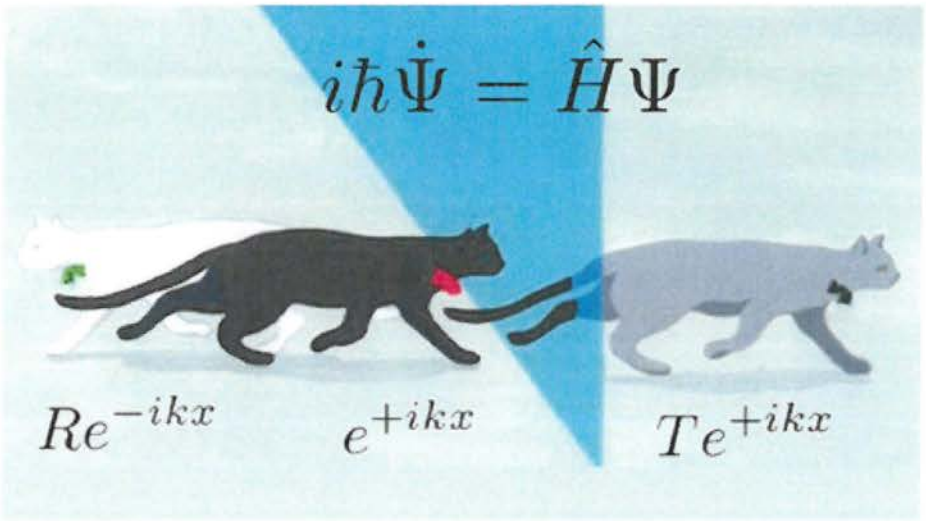
Το πείραμα του Aspect (1982) αποφάνθηκε υπέρ της επικρατούσας άποψης. Το πείραμα έγινε όχι με δύο πρωτόνια ολικού σπιν 0 αλλά με δύο φωτόνια και ελέγχοντας την πόλωση των φωτονίων σε μεγάλες αποστάσεις.

1.2.7 Εναλλακτικές ερμηνείες.

Μπορεί τελικά η ερμηνεία της Κοπεγχάγης να εξελίχθηκε σε κβαντομηχανική ορθοδοξία, αλλά το κεντρικό φιλοσοφικό κενό παρέμεινε. Η οντολογία των στοιχειωδών σωματιδίων δεν αντιστοιχεί σε κάποια οντολογία για την οποία μπορούμε να έχουμε άμεση εποπτεία. Αυτή η απουσία εποπτείας μοιάζει να

καθιστά αναγκαία κάποιου είδους μεταφυσική. Μάλιστα ορισμένες ακραίες εκδοχές της Κοπεγχάγης φτάνουν να αμφισβητούν ακόμη και την αυτόνομη ύπαρξη της πραγματικότητας, εξαρτώντας την από την παρουσία κάποιας συνείδησης (Wigner). Υπάρχει ένα ισχυρό επιστημονικό ρεύμα που επιδιώκει την άρση αυτού του επιστημονικού κενού. Το ρεύμα αυτό ενισχύεται από το ότι η απουσία εποπτείας συνδυάζεται από την έλλειψη ντετερμινισμού στην εξέλιξη των φυσικών φαινομένων.

Όλα αυτά ήταν ισχυρά κίνητρα για την ανάπτυξη εναλλακτικών προτάσεων. Και υπάρχει άφθονος τέτοιος χώρος. Τα μαθηματικά της κβαντομηχανικής είναι σαφή αλλά όταν θελήσει κανείς να τα εφαρμόσει σε πραγματικά συστήματα τα πράγματα δυσκολεύουν και γίνονται απαγορευτικά όταν τα συστήματα γίνουν συνθετότερα και αποκτήσουν μια κάπως περίπλοκη δομή (π.χ. ένα άτομο). Μόλις ξεφύγουμε από τα πολύ απλά συστήματα οι εξισώσεις της κβαντομηχανικής δεν λύνονται και επομένως δεν είναι επαληθεύσιμες και συνεπώς υπάρχει χώρος για διάφορες υποθέσεις που δεν είναι ελέγξιμες.



Εικόνα 30 Κβαντομηχανική.

Έτσι λοιπόν η κβαντομηχανική αφήνει ανοικτή την πόρτα σε διάφορα ερμηνευτικά συμπληρώματα που έχουν γραφτεί από φυσικούς και έχουν μαθηματική μορφή. Μπορεί να πει κανείς ότι υπάρχουν σε γενικές γραμμές τέσσερα είδη τέτοιων ερμηνευτικών συμπληρωμάτων.

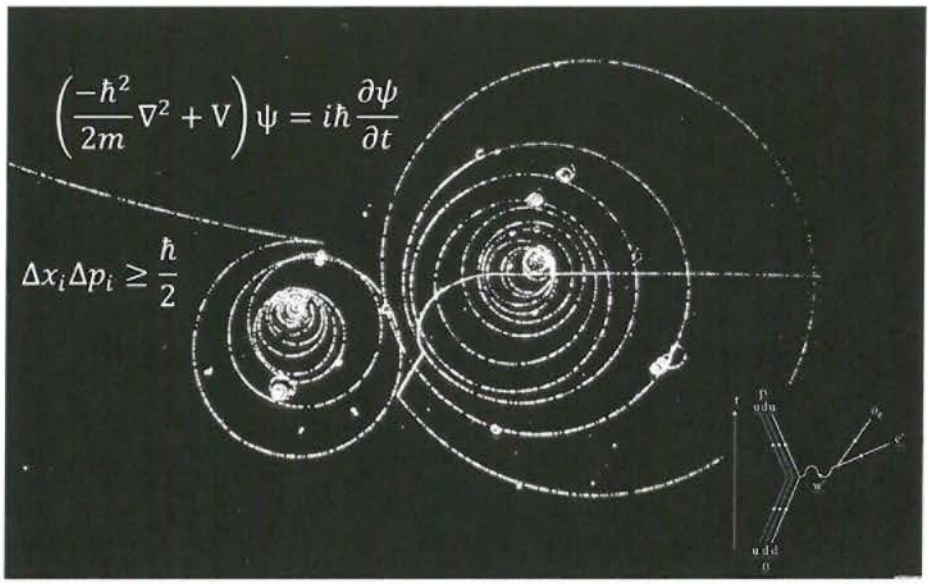
Η πρώτη αναφέρεται στον δυισμό κύματος - σωματιδίου και προκειμένου να τον εξηγήσει αναπτύσσει ναι νέα οντολογία όσον αφορά στην υφή των στοιχειωδών σωματιδίων.

Η δεύτερη έχει να κάνει με την μη τοπικότητα και αναφέρεται στο σύμπαν ολόκληρο ή στη γνώση που έχουμε γι' αυτό. Διατηρεί την κλασική οντολογία στην περιγραφή του μικρόκοσμου και αναπτύσσει μια νέα οντολογία σε συμπαντικό επίπεδο.

Η τρίτη αναφέρεται στο μετρητικό πρόβλημα και ουσιαστικά εισάγει νέα στοιχεία όσον αφορά στις φυσικές διεργασίες

Η κάθε μία από τις τρεις αυτές εκδοχές, αφού αντιμετωπίσει το κεντρικό κατά την άποψή της θέμα, συνήθως δίνει απαντήσεις και στα άλλα δύο.

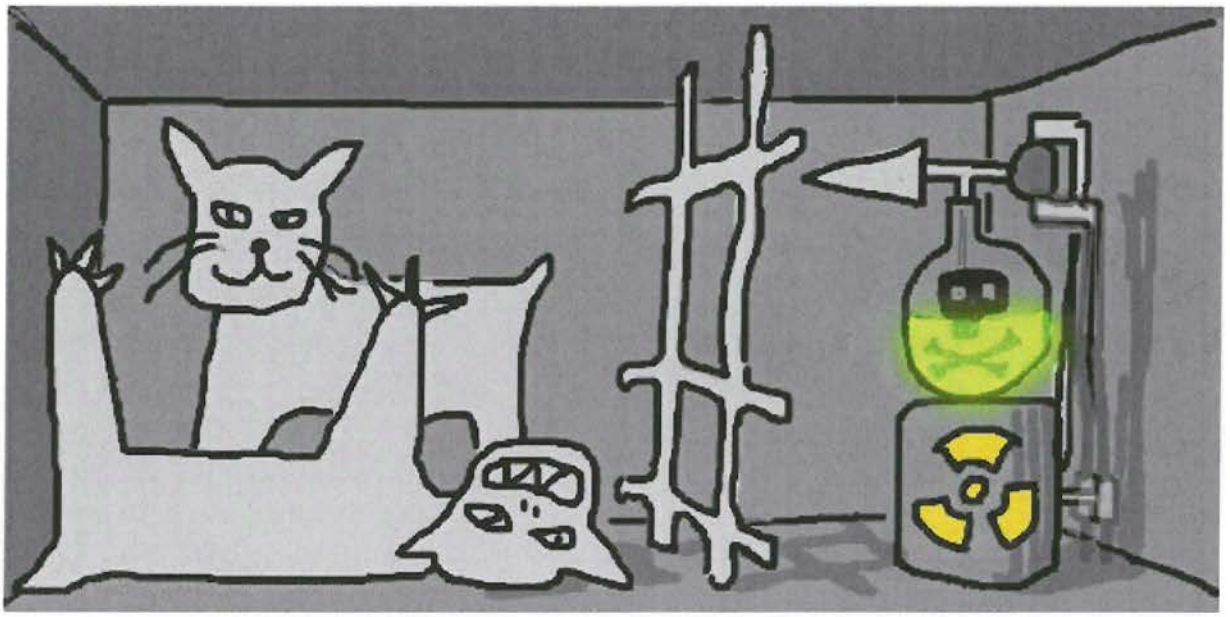
Το τέταρτο ρεύμα προσπαθεί να υπερβεί την ανάγκη για μεταφυσική προσθήκη με την ανάπτυξη είτε μιας διαφορετικής λογικής είτε μιας διαφορετικής μαθηματικής προσέγγισης, μένοντας αυστηρά στα όρια του πρώτου επιπέδου του οντολογικού ερωτήματος (δηλαδή στην απόδοση συγκεκριμένων τιμών για τα φυσικά μεγέθη) και αγνοώντας το δεύτερο (δηλαδή τη φυσική τους σημασία).



Εικόνα 31 Κβαντομηχανική.

Επισημαίνω ότι όλες αυτές οι ερμηνείες είναι διατυπωμένες έτσι ώστε να οδηγούν στα αποτελέσματα που παράγουν τα πειράματα. Δεν είναι όλες ισοδύναμες. Αλλά οι διαφορές τους δεν είναι ελέγξιμες με τις πειραματικές διατάξεις που διαθέτουμε.

Όλες οι ερμηνευτικές προτάσεις εμφανίζονται σε πάνω από μία παραλλαγές και υφίστανται διαρκή εξέλιξη. Πρόκειται για διατυπώσεις εξαιρετικά πολύπλοκες και λεπτές. Η απλή θεμελιακή άποψη της κάθε μιας επενδύεται με μαθηματικό φορμαλισμό και συμπληρώνεται με θεωρήματα που έχουν εξαιρετικά λεπτή λογική δομή. Το αποτέλεσμα είναι να μην υπάρξει κοινή αποδοχή μιας από τις ερμηνείες και όσοι δεν θέλουν να το ψάξουν παραπάνω να επανέρχονται στην γραμμή της Κοπεγχάγης.



Εικόνα 32 Το παράδοξο της γάτας του Schrödinger.

1.2.8 Οι προσθήκες των εναλλακτικών ερμηνειών.

1) Η πρώτη ομάδα ερμηνειών επικεντρώνεται στο πρόβλημα του δυισμού κύματος – σωματιδίου και ως επίλυσή του προβάλλει την άρνηση της πραγματικότητάς του. Για αυτήν υπάρχουν μόνο σωματίδια που έχουν πάντα καθορισμένη θέση και ταχύτητα. Είναι οι θεωρίες των «κρυφών μεταβλητών» (μηχανική του Bohm). Κύριο χαρακτηριστικό τους είναι ο ντετερμινιστικός και αντί-ιδεαλιστικός της χαρακτήρας. Η θεωρία του Bohm κάνει μια προσθήκη στην κλασική οντολογία προσπαθώντας να διατηρήσει την αιτιοκρατία. Κάθε σωματίδιο το εξαρτά από ένα κύμα με ιδιαίτερες ιδιότητες. (Η φυσική υφή του κύματος μένει απροσδιόριστη). Το κύμα αυτό καθοδηγεί την πορεία των σωματιδίων ενημερώνοντάς τα ακαριαία για το τι θα βρουν στο δρόμο τους.

Για αν εκφράσει και μαθηματικά την άποψή του ο Bohm, μετέγραψε την εξίσωση Schrödinger σε πολικές συντεταγμένες, οπότε εμφανίστηκε ένας όρος που δεν είναι δυνατόν να υπολογιστεί. Ο όρος αυτός θεωρήθηκε ότι εκφράζει ένα κβαντικό δυναμικό που περιγράφει το καθοδηγητικό κύμα (pilot wave). Την αδυναμία υπολογισμού την θεωρεί ο Bohm προσωρινή και την συσχετίζει με κάποιες κρυφές μεταβλητές τις οποίες, προς το παρόν, δεν γνωρίζουμε αλλά που ενδέχεται να υπολογίσουμε στο μέλλον. Το κύμα καθοδηγεί με ακρίβεια τις τροχιές των σωματιδίων, αλλά αυτές δεν μπορούν να υπολογιστούν με ακρίβεια γιατί εμφανίζουν μια στατιστική κατανομή που περιγράφεται από την εξίσωση Schrödinger. Η θεωρία λοιπόν μπορεί να είναι ντετερμινιστική, αλλά υπεισέρχεται η απροσδιοριστία (λόγω της αρχής της απροσδιοριστίας του Heisenberg) με

αποτέλεσμα οι μετρήσεις να εμφανίσουν μια στατιστική κατανομή (όπως και στην κλασική κβαντομηχανική).

Οι υποστηρικτές της θεωρίας διατείνουν ότι είναι η μόνη που δεν έχει μεταφυσικό χαρακτήρα και κρατά ακέραια την οντολογία της κλασικής φυσικής. Αλλά μήπως η υπόθεση της ύπαρξης του ιδιαίτερου αυτού κύματος δεν είναι μεταφυσική, αφού δεν μπορούμε να επιβεβαιώσουμε ή να διαψεύσουμε την ύπαρξή του; Πέραν αυτού, υπάρχουν θεωρήματα που αποκλείουν τη δυνατότητα ύπαρξης «κρυφών μεταβλητών».

2) Η δεύτερη ομάδα έχει πρώτο στόχο την αντιμετώπιση του προβλήματος της μέτρησης (της κατάρρευσης της κυματοσυνάρτησης). Η ομάδα αυτή στην πραγματικότητα αρνείται το γεγονός της κατάρρευσης και, για να αποφύγει την ανάγκη της, θεωρεί ότι όλες οι δυνατές καταστάσεις που περιγράφει η κυματοσυνάρτηση αποτελούν ανεξάρτητες μεταξύ τους φυσικές πραγματικότητες (ενώ στην κλασική κβαντομηχανική αποτελούν υπερθέσεις). Κατά συνέπεια κάθε φορά που συμβαίνει ένα κβαντικό γεγονός, έχουμε έναν πολλαπλασιασμό του φυσικού κόσμου (θεωρίες των πολλών κόσμων). Έτσι δεν μιλούμε για το σύμπαν αλλά για το πολυσύμπαν (Multiuniverse). Προς το παρόν, εφόσον δεν υπάρχει ενοποιητική θεωρία της βαρύτητας και της κβαντομηχανικής, το κβαντικό πολυσύμπαν είναι διαφορετικό από το πολυσύμπαν για το οποίο μας μιλά η κοσμολογία.

Η αρχική ιδέα ήταν του Everett. Η αρχική πρόταση δεν ήταν πολύ ξεκάθαρη και στη συνέχεια διάφοροι ερευνητές παρουσίασαν διάφορες εκδοχές της. Σε αυτές η υπόθεση των πολλών κόσμων αντικαταστάθηκε από την υπόθεση των πολλών ιστοριών του ίδιου κόσμου ή των πολλών καταστάσεων του μυαλού του παρατηρητή ή μιας relational quantum mechanics. Οι θεωρίες αυτές είναι παράξενες αλλά έχουν τα υποστηρικτικά τους επιχειρήματα που από μαθηματική και φυσική άποψη είναι ισάξια των άλλων θεωριών. Αλλά λόγω της αισθητικής τους και κάποιων αδυναμιών τους δεν έχουν πολλούς υποστηρικτές. Να σημειωθεί ότι σύμφωνα με αυτές δεν είναι δυνατή καμία επικοινωνία μεταξύ των διαφόρων συμπάντων του Multiuniverse. Ωστόσο η έννοια του Multiuniverse έρχεται και δένει με στοιχεία της κοσμολογίας και αποκτά βαρύτητα, για την οποία οι περισσότεροι δεν είμαστε προετοιμασμένοι.

3) Η επόμενη ομάδα θεωριών είναι αυτή που παραδέχεται την κατάρρευση της κυματοσυνάρτησης και γι' αυτό οι θεωρίες αυτές λέγονται collapse theories. Το κεντρικό πρόβλημα που επιχειρούν να αντιμετωπίσουν είναι το πρόβλημα της κβαντικής μέτρησης. Υποστηρίζουν ότι δεν υπάρχουν καθαρές κβαντικές καταστάσεις που κάποια στιγμή καταρρέουν, αλλά ότι η κατάρρευση είναι ένα διαρκές φαινόμενο που συμβαίνει με συγκεκριμένο ρυθμό στη μονάδα του χρόνου και του όγκου. Π.χ. ένα σωματίδιο που όταν είναι σε κβαντική κατάσταση δεν είναι σαφώς εντοπισμένο, έχει στην πραγματικότητα την αυθόρμητη τάση να χάσει την κβαντική του κατάσταση και να μεταπέσει σε μια σαφώς εντοπισμένη. Η τάση αυτή έχει στατιστικό χαρακτήρα, με μια κατανομή πιθανότητας τύπου καμπάνας. Ο ρυθμός των εντοπισμένων κτυπημάτων (hittings) είναι έτσι καθορισμένος ώστε για ένα μεμονωμένο σωματίδιο η πιθανότητα εντοπισμού να είναι πάρα πολύ μικρή. Αντιθέτως, για ένα μακροσκοπικό σώμα που αποτελείται από τεράστιο αριθμό σωματιδίων, ο ρυθμός αυτός είναι έτσι διαμορφωμένος ώστε πάντα το συντριπτικά μεγαλύτερο ποσοστό από αυτόν τον τεράστιο αριθμό να είναι εντοπισμένο. Γι' αυτό και τα μακροσκοπικά αντικείμενα τα βλέπουμε εντοπισμένα.

Οι θεωρίες αυτές μοιάζουν να διατηρούν την κλασική οντολογία. Ωστόσο προϋποθέτουν μη παρατηρήσιμες διεργασίες, εισάγουν δύο ή τρεις καινούριες παραμέτρους με αυθαίρετες και εκ των υστέρων καθορισμένες τιμές και δεν προτείνουν τίποτα για τα προβλήματα της μη τοπικότητας και του δυϊσμού. Επιπλέον δημιουργούνται καινούρια εννοιολογικά προβλήματα που τις οδηγούν στην άποψη ότι η ύλη που βλέπουμε αποτελείται από κάποιο άλλο υλικό που είναι ορατό κάτω από ορισμένες προϋποθέσεις και αόρατο κάτω από άλλες. Τελικά, προσπαθώντας να λύσουν ένα πρόβλημα δημιουργούν πλήθος άλλων... Αλλά αυτό συμβαίνει και με τις άλλες ερμηνείες.

4) Η τέταρτη ομάδα θεωριών ονομάζονται modal interpretations και κατά κάποιο τρόπο αποτελούν παραλλαγή της Κοπεγχάγης. Οι θεωρίες αυτές δεν θεωρούν την κατάρρευση της κυματοσυνάρτησης ως φυσικό γεγονός, αλλά ασχολούνται με τη μαθηματική διατύπωση της σχέσης των πειραματικών αποτελεσμάτων με τις προβλεπόμενες από την κβαντική θεωρία τιμές. Αυτή πρέπει να είναι τέτοια ώστε να μην υπάρχει ανάγκη για αλλαγή της μαθηματικής διατύπωσης κατά την μετάβαση από την κβαντική στην κλασική κατάσταση. Για τον σκοπό αυτόν

αναπτύσσονται νέα μαθηματικά, νέες άλγεβρες και νέα λογική. Ο πυρήνας των θεωριών έγκειται στη διάκριση ανάμεσα στα γεγονότα που όντως συμβαίνουν και στην περιγραφή των γεγονότων από την κβαντική θεωρία. Κατά την κβαντική θεωρία, για κάθε παρατηρίσιμο φυσικό μέγεθος υπάρχει μια αυστηρή αντιστοίχηση ανάμεσα στις τιμές που μπορεί να πάρει και τις ιδιοτιμές του τελεστή που τού αντιστοιχεί. Ο van Fraassen αμφισβητεί αυτήν την αυστηρή αντιστοίχηση και θεωρεί ότι οι πραγματικές φυσικές τιμές δεν περιορίζονται κατά έναν αναγκαστικό τρόπο μόνο στις ιδιοτιμές του τελεστή, αλλά μπορούν να πάρουν την οποιαδήποτε τιμή. Δηλαδή το ότι μια μετρητική συσκευή βρίσκει κατά τη μέτρηση ότι η ταχύτητα έχει μια συγκεκριμένη τιμή, δεν συνεπάγεται ότι η κβαντική οντότητα κατέχει μόνο αυτή την ταχύτητα. «Κατέχει» και όλες τις άλλες δυνατές, αλλά εμείς βλέπουμε μόνο αυτή που δείχνει η συσκευή. Έτσι αποφεύγεται η ανάγκη μιας αλλαγής της εξίσωσης που υπολογίζει την ταχύτητα, την κατάρρευση δηλαδή της κυματοσυνάρτησης.

Εικόνα 33 Κβαντική Μηχανική.

Οι θεωρίες αυτές αναπτύσσουν μια περιγραφή της σχέσης, ενός χάρτη, που συνδέει τις δύο αυτές ομάδες γεγονότων των ιδιοτιμών του τελεστή και των πραγματικών τιμών του συγκεκριμένου μεγέθους. Με άλλα λόγια αναπτύσσουν μια μαθηματική περιγραφή του επιστημολογικού ερωτήματος και του πρώτου τμήματος του οντολογικού ερωτήματος. Περιγράφουν ή συσχετίζουν αυτό που μπορούμε να γνωρίσουμε, με τις πραγματικές τιμές που μπορεί να πάρει ένα

παρατηρήσιμο μέγεθος. Αν και τραβούν το ενδιαφέρον πολλών ερευνητών, δεν δίνουν ουσιαστική απάντηση στα φιλοσοφικά ερωτήματα με τα οποία συνδέεται η κβαντική φυσική.Να σημειωθεί ότι εκτός από τις τέσσερεις αυτές ομάδες θεωριών, υπάρχουν και πολλές άλλες ερμηνευτικές εκδοχές που όμως δεν έχουν πολλούς οπαδούς.

Κεφάλαιο 2°: Εισαγωγή στην θεωρία της Πληροφορικής.

2.1.1 Ιστορική αναδρομή στην θεωρίας πληροφορικής.

Σύμφωνα με το λεξικό Oxford English Dictionary, η λέξη υπολογιστής καταγράφηκε για πρώτη φορά σαν λήμμα το 1613, και αναφερόταν στο άτομο που έκανε υπολογισμούς. Με το πέρασμα του χρόνου και κοντά στον 20° αιώνα η έννοια της λέξης εξελίχθηκε και αναφέρεται πια στις μηχανές και όχι στους ανθρώπους. Σήμερα η λέξη υπολογιστής αναφέρεται στη μηχανή η οποία έχει την ικανότητα, σύμφωνα με ένα σύνολο εντολών, να επεξεργάζεται δεδομένα και πληροφορίες και να παρέχει κάποιας μορφής αποτέλεσμα.

Μέσα σε αυτό το πλαίσιο, μια μηχανή είναι μία μηχανική διάταξη από συσχετιζόμενα μέρη τα οποία χρησιμοποιούν κάποιας μορφής ενέργεια για εκτελέσουν κάποια δραστηριότητα ή κάποιο έργο. Παρόλο που υπάρχουν πολλοί τύποι και πολλές ταξινομήσεις υπολογιστών εύκολη απάντηση στην ερώτηση «Πότε εφευρέθηκε ο πρώτος υπολογιστής;» δεν υπάρχει. Το ίδιο ισχύει και για την ερώτηση «Ποιος ανακάλυψε τον υπολογιστή;» διότι πολλοί άνθρωποι συνέβαλαν στην δημιουργία του και την εξέλιξή του.

Τα σημαντικότερα άτομα που συνέβαλαν στην εξέλιξη των υπολογιστών:

1. Τσαρλς Μπάμπατζ (1815 - 1871)

Ο Τσαρλς Μπάμπατζ (26 Δεκεμβρίου 1792 - 18 Οκτωβρίου 1871) ήταν Βρετανός μαθηματικός, φιλόσοφος, εφευρέτης και μηχανικός ο οποίος επινόησε τον

προγραμματίσιμο υπολογιστή. Θεωρείται ο «πατέρας του υπολογιστή». Του αποδίδεται η εφεύρεση του πρώτου μηχανικού υπολογιστή, ο οποίος σταδιακά οδήγησε σε πιο προχωρημένο σχεδιασμό. Τμήματα των μη ολοκληρωμένων μηχανών του εκτίθενται στο Μουσείο Επιστημών του Λονδίνου. Το 1991 κατασκευάστηκε μια πλήρως λειτουργική διαφορική μηχανή από τα αρχικά σχέδια του Μπάμπατζ, με μεθόδους κατασκευής που αντιστοιχούσαν στον 19ο αιώνα. Η επιτυχής κατασκευή της μηχανής έδειξε ότι η μηχανή θα μπορούσε να λειτουργήσει. Εννέα χρόνια αργότερα το Μουσείο Επιστημών ολοκλήρωσε τον εκτυπωτή που ο Μπάμπατζ είχε σχεδιάσει για την διαφορική μηχανή, μια εξαιρετικά πολύπλοκη συσκευή για τον 19ο αιώνα.

Εικόνα 34 Charles Babbage.

2. Άντα Λάβλεϊς (1815 - 1852)

Η Αυγούστα Άντα Κίνγκ, Κόμισσα του Λάβλεϊς (πατρικό Αυγούστα Άντα Μπάιρον) είναι γνωστή για το έργο που άφησε σχετικά με την Αναλυτική Μηχανή του Τσαρλς Μπάμπατζ. Η συνεισφορά της αυτή θεωρείται σήμερα από τους ιστορικούς ως το πρώτο πρόγραμμα για υπολογιστή.

Εικόνα 35 Ada Lovelace.

3. John Vincent Atanasoff (1903 - 1995)

John Vincent Atanasoff (4 Οκτ, 1903 - 15 Ιούνη του 1995) ήταν ένας Αμερικανός φυσικός και εφευρέτης, γνωστός για την επινόηση το πρώτο ηλεκτρονικού ψηφιακού υπολογιστή.

Ο Ατανάσοφ εφηύρε το πρώτο ηλεκτρονικό ψηφιακό υπολογιστή στη δεκαετία του 1930 στο Iowa State College. Προκλήσεις για την απαίτησή του επιλύθηκαν το 1973, όταν η Honeywell κατά Sperry Rand μήνυση έκρινε ότι Atanasoff ήταν ο εφευρέτης του υπολογιστή. Μηχανή ειδικού σκοπού του έχει έρθει να κληθεί Atanasoff-Berry Υπολογιστής.

Εικόνα 36 John Vincent Atanasoff.

4. Konrad Zuse (1910 - 1995)

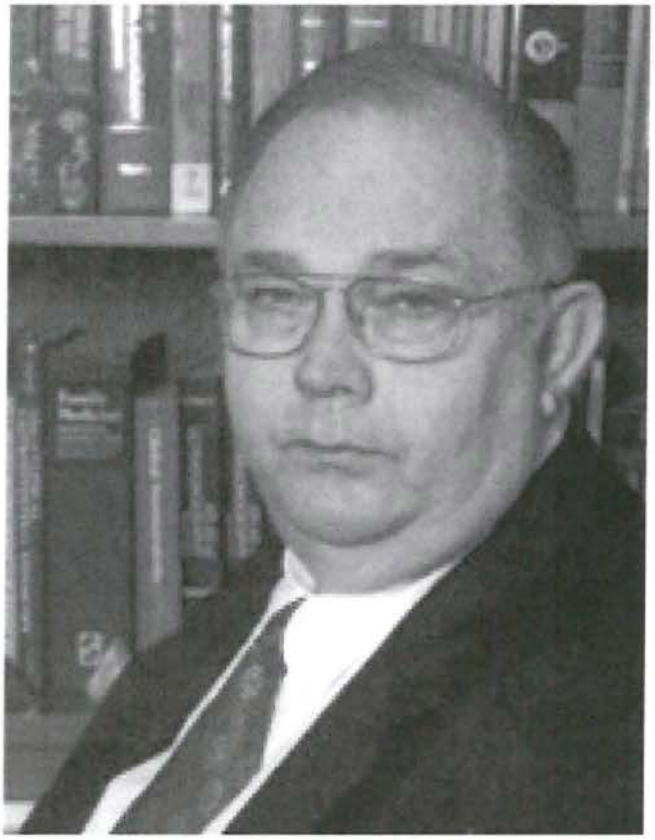
Ο Κόνραντ Τσούζε (γερμ. Konrad Zuse, 22 Ιουνίου 1910 – 18 Δεκεμβρίου 1995) ήταν Γερμανός μηχανικός και πρωτοπόρος των υπολογιστών. Το μεγαλύτερό του επίτευγμα ήταν η ολοκλήρωση του πρώτου λειτουργικού προγραμματιζόμενου υπολογιστή, του Z3, το 1941.

Εικόνα 37 Konrad Zuse.

5. Henry Edward Roberts (1941 - 2010)

Ο αμερικανός Henry Edward Roberts κατασκεύασε το 1974 τον Altair 8800 που βασιζόταν στον επεξεργαστή Intel 8008. Για πρώτη φορά όλα τα εξαρτήματα συναρμολόγησης περιέχονται μέσα σε ένα κουτί. Την εποχή αυτή δεν υπήρχαν μαγαζιά ώστε να μπορεί κάποιος να αγοράζει υπολογιστή.

Η μόνη επιλογή που είχε για να κατασκευάσει το δικό του σύστημα ήταν από σχέδια που δημοσιεύονταν ή πουλιόταν σε περιοδικά και άλλες πηγές και η ευθύνη για το ποια τμήματα χρειαζόταν να βρει ή να ζητήσει ήταν αποκλειστικά δική του. Το 1975 το Altair 8800 δημοσιεύτηκε στο εξώφυλλο του περιοδικού Popular Electronics και έγινε αμέσως μεγάλη εμπορική επιτυχία.



Εικόνα 38 Henry Edward Roberts.

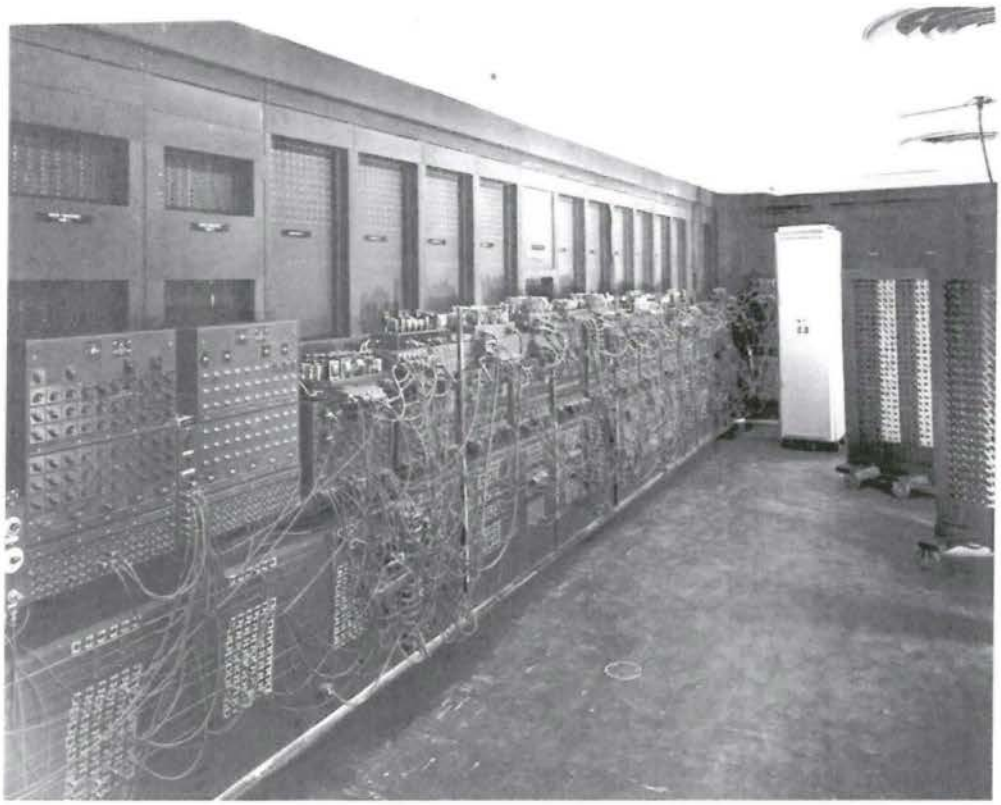
2.1.2 Υπολογιστές ιστορικής σημασίας.

1. ENIAC - Ο πρώτος γενικός ψηφιακός υπολογιστής

Δύο αμερικανοί επιστήμονες του University of Pennsylvania στη Philadelphia, ο John Mauchly (φυσικός) και ο J. Presper Eckert (μηχανικός), πρότειναν έναν ηλεκτρονικό ψηφιακό υπολογιστή που τον αποκάλεσαν «Ηλεκτρονικός Αριθμητικός Ολοκληρωτής και Υπολογιστής» (Electronic Numerical Integrator And Computer - ENIAC). Ο ENIAC ολοκληρώθηκε το 1945, τέθηκε σε λειτουργία τον Φεβρουάριο του 1946 και θεωρείται ο πρώτος επιτυχών γενικός ψηφιακός υπολογιστής, δηλαδή ο υπολογιστής που μπορούσε να προγραμματιστεί για να λύσει ένα οποιοδήποτε πρόβλημα.

Προγραμματιζόταν με την τοποθέτηση καλωδίων σε μια διάτρητη επιφάνεια. Προοριζόταν για την επίλυση προβλημάτων βαλλιστικής (υπολογισμός πινάκων βολών). Ο ENIAC κατασκευάστηκε πριν εφευρεθεί το πρώτο τρανζίστορ για' αυτό και χρησιμοποιήθηκαν οι λυχνίες κενού. Αποτελείτο από βαθμίδες (panels) χωρίς κινούμενα μέρη. Το πιο αξιοθαύμαστο στον ENIAC είναι η πολυπλοκότητά του.

Ο ENIAC ζύγιζε 27 τόνους, καταλάμβανε 63 τετραγωνικά μέτρα (μόνο το υλικό, χωρίς τους διαδρόμους), περιείχε δέκα διαφορετικών τύπων λυχνίες κενού (περίπου 18.000). Μπορούσε να κάνει 5.000 αριθμητικές πράξεις (προσθέσεις ή αφαιρέσεις) το δευτερόλεπτο. Τα ψηφία της κάθε πράξης μπορούσαν να είναι μέχρι 10. Μπορούσε επίσης να κάνει μέχρι 385 πολλαπλασιασμούς το δευτερόλεπτο, 10 διαιρέσεις ή να βρίσκει 3 τετραγωνικές ρίζες το δευτερόλεπτο. Η ταχύτητά του επεξεργαστή του ήταν κοντά στα 5KHz. Η κατανάλωσή ρεύματος ήταν 150 KWatt. Μόνιμη μονάδα αποθήκευσης (μνήμη) δεν είχε. Φυσικά δεν είχε ούτε οθόνη και για την εμφάνιση των αποτελεσμάτων είχε μία συσκευή που έκανε τρύπες σε κάρτες.



Εικόνα 39 ENIAC 1946.

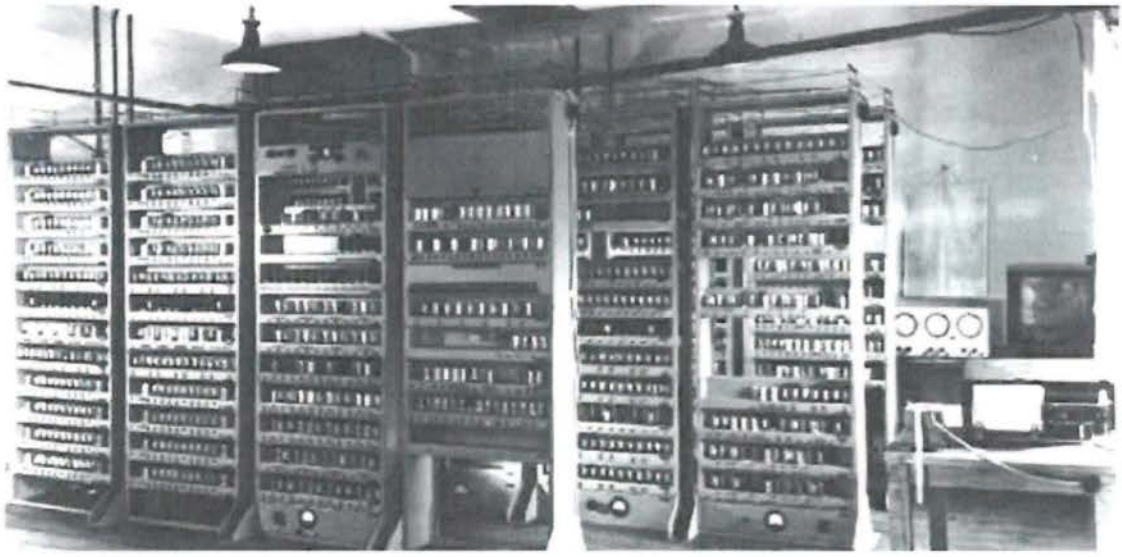
2. EDSAC - Ο πρώτος εσωτερικά προγραμματιζόμενος υπολογιστής

Ο EDSAC (Electronic Delay Storage Automatic Calculator) ήταν ένας βρετανικός υπολογιστής που κατασκευάστηκε στο University of Cambridge. Το Μάιο του 1946 ο υπολογιστής έτρεξε το πρώτο του πρόγραμμα το οποίο υπολόγισε τα τετράγωνα των ακέραιων αριθμών από το 0 έως και το 99 και μια λίστα πρώτων αριθμών.

Χρησιμοποιούσε 3.000 λυχνίες, κατανάλωνε 12 κιλοβάτ (kW) ενέργειας και καταλάμβανε ένα δωμάτιο 20 τ.μ. Πρόσφερε 1.024 θέσεις μνήμης 17 δυαδικών ψηφίων, ενώ επέτρεπε το συνδυασμό δύο γειτονικών θέσεων μνήμης, προκειμένου να αποθηκευτούν μεγάλοι αριθμοί. Η «αποθήκευση προγράμματος» γίνονταν σε επίπεδο μνήμης, όλα τα δεδομένα και οι εντολές αναπαρίστανται μέσω δυαδικού κώδικα και αποθηκεύονται στην μνήμη του υπολογιστή και δεν υπάρχει διάκριση μεταξύ δεδομένων και εντολών.

Για τον προγραμματισμό του EDSAC δημιουργήθηκε μία βιβλιοθήκη από μικρά προγράμματα που αποκαλούντο υπορουτίνες και ήταν αποθηκευμένα σε διάτρητες χάρτινες ταινίες. Τα προγράμματα εισάγονταν μέσω ενός αναγνώστη διάτρητης χαρτοταινίας, ενώ τα αποτελέσματα εκτυπώνονταν σε ένα τηλέτυπο. Η συχνότητα λειτουργίας του ήταν 500KHz δηλαδή μπορούσε να εκτελεί 714 εντολές ανά δευτερόλεπτο), η Μνήμη του ήταν 1.024 λέξεις των 17bit και τύπου υδραργύρου γραμμής καθυστέρησης. Το λειτουργικό του σύστημα αποτελείτο από 31 εντολές (Initial Orders 1) που μετέφραζαν τα προγράμματα, τα αποθήκευαν στην κεντρική μνήμη και τα εκτελούσαν.

Το βασικό πλεονέκτημά του ήταν ότι μπορούσε να αποθηκεύει λίστες εντολών και στη συνέχεια να εκτελεί τους απαραίτητους υπολογισμούς αυτόματα. Έτσι, αξιοποιήθηκε άμεσα για πρακτικούς σκοπούς, όπως για την επίλυση μετεωρολογικών προβλημάτων, χρησιμοποιώντας τη διαφορική εξίσωση του Airy. Το 1951 χρησιμοποιήθηκε για τον υπολογισμό ενός πρώτου αριθμού 79 ψηφίων, που ήταν ο μεγαλύτερος της εποχής.



Εικόνα 40 EDSAC 1949

3. Apple I - Ο πρώτος οικιακός υπολογιστής

Το 1976, μετά την παρουσίαση του υπολογιστή Altair, η εταιρία Apple παρουσίασε τον δικό της υπολογιστή τον Apple I τον πρώτο με μονή κάρτα ολοκληρωμένων κυκλωμάτων. Στόχος της εταιρείας ήταν ο Apple I γίνει ο πρώτος

χρήσιμος οικιακός υπολογιστής. Αυτός ήταν σε ξύλινη θήκη και στην αρχή πουλήθηκε σαν κιτ υπολογιστή για χόμπι. Το κιτ περιείχε: θήκη, μετατροπείς ηλεκτρικού ρεύματος, την κάρτα ολοκληρωμένων κυκλωμάτων, διακόπτη ηλεκτρικού ρεύματος και πληκτρολόγιο αλλά δεν περιείχε οθόνη.

Ο επεξεργαστής του Apple I ήταν MOS 6502 8-bit στα 1MHz, η μνήμη του ήταν στα 4KB με δυνατότητες επέκτασης στα 8K ή 48K χρησιμοποιώντας κάρτες επέκτασης, για την αποθήκευση των δεδομένων υπήρχε διεπαφή κασέτας και η τιμή του ήταν 666.66$ US. Το 2010 σε δημοπρασία πουλήθηκε ο Apple I προς £150,000. Η παραγωγή του σταμάτησε το 1977 όταν η εταιρία Apple ανακοίνωσε τον Apple II τον διάδοχο του Apple I, ο οποίος για πολλά έτη παρέμεινε βασικός παράγοντας της οικονομικής ευημερίας της εταιρίας. Ο Apple II κατέκτησε εκατομμύρια χρηστών που μέχρι τότε δεν είχαν πρόσβαση σε ηλεκτρονικούς υπολογιστές με πρωτοποριακά για την εποχή προγράμματα όπως το VisiCalc το οποίο ήταν και το πρώτο πρόγραμμα υπολογιστικού φύλλου (spreadsheet). Το VisiCalc αποτέλεσε τον σημαντικότερο λόγο αγοράς του εν λόγω υπολογιστή.

Εικόνα 41 Apple I 1976.

4. Osborne I - Ο πρώτος φορητός υπολογιστής

Το 1981 η εταιρία Osborne Computer Corporation παρουσίασε τον πρώτο επιτυχημένο εμπορικά φορητό μικροϋπολογιστή ή laptop που κόστιζε περίπου 1.795$ US. Το Osborne I είχε: 64K μνήμη, έναν οδηγό εύκαμπτου δίσκου και μόντεμ. Ο υπολογιστής έκλεινε για προστασία και είχε ένα χερούλι για την μεταφορά του. Επιπλέον είχε και μία προαιρετική μπαταρία για να μπορεί να δουλέψει ανεξάρτητα από τη σύνδεση με το ηλεκτρικό ρεύμα. Διέθετε κεντρική μονάδα επεξεργασίας Zilog Z80 στα 4 MHz, δύο οδηγούς για μονής όψης εύκαμπτες δισκέτες και 5" οθόνη σωλήνα καθοδικών ακτινών (CRT- Cathode Ray Tube) μονόχρωμη, ενώ παρόλο που ήταν πολύ επαναστατικός τύπος υπολογιστή είχε αρκετούς περιορισμούς όπως τη μικρή οθόνη των 5"και το ότι δεν μπορούσε να εμφανίσει στην οθόνη περισσότερους από 52 χαρακτήρες ανά γραμμή κειμένου. Περισσότεροι χαρακτήρες μέχρι 128 μπορούσαν να γίνουν ορατοί με την κίνηση των πλήκτρων του δρομέα.

Εικόνα 42 Osborne I.

5. IBM PC - Προσωπικός Υπολογιστής (Personal Computer)

Το 1981 η εταιρία IBM ανακοίνωσε τον πρώτο προσωπικό υπολογιστή IBM PC 5150, στην τιμή των 1.565$ US. Ο υπολογιστής είχε μικροεπεξεργαστή Intel 8088 στα 4.77 MHz, μνήμη επεκτάσιμη στα 256KB, οδηγούς ευκάμπτων δίσκων, μονόχρωμη οθόνη (σωλήνα καθοδικών ακτινών) με πράσινα γράμματα και ένα στοιχειώδες λειτουργικό σύστημα DOS 1.0 (DOS = Disk Operating System) που έφτιαξε στα γρήγορα μια ομάδα υπό τον Bill Gates.

Οι χαρακτήρες PC ήταν τα αρχικά των αγγλικών όρων Personal Computer (Προσωπικός Υπολογιστής) και λόγω της επιτυχίας της IBM και της συμβατότητας σε υλικό των άλλων εταιριών υπολογιστών ως προς την IBM επικράτησε για τους προσωπικούς υπολογιστές ο όρος PC. Η σημαντικότερη κίνηση της IBM, ήταν πως δημοσίευσε τις προδιαγραφές του υπολογιστικού της συστήματος και έτσι άνοιξε ο δρόμος για την κατασκευή των λεγόμενων IBM-συμβατών.

Εικόνα 43 IBM PC.

2.1.3 Σημαντικότερα άτομα που συνέβαλαν στην εξέλιξη των υπολογιστών.

1. Alan Turing (1912-1954)

Ο βρετανός Alan Turing θεωρείται ένας από τους πιο διάσημους μαθηματικούς του 20ου αιώνα. Αλγόριθμοι, Κρυπτογραφία – Κρυπτανάλυση, Τεχνητή Νοημοσύνη χρωστούν τη θεμελίωσή τους στον μεγάλο αυτό Άγγλο επιστήμονα. Σχετικά με τη Τεχνητή Νοημοσύνη έθεσε ένα απλό τεστ για το κατά πόσο ένα πρόγραμμα μπορεί τελικά να σκέφτεται. Το λογισμικό λοιπόν έπρεπε να καταφέρει να ξεγελάσει ανθρώπους και να θεωρήσουν πως συνομιλούσαν με έναν άνθρωπο και όχι με μία μηχανή. Με τις μελέτες του πάνω στην έννοια του αλγορίθμου αλλά και της μηχανής ο Turing έθεσε τις βάσεις της μοντέρνας επιστήμης των υπολογιστών. Εξελίσσοντας την ιδέα του αλγορίθμου, δημιούργησε και τα πρώτα προγράμματα τα οποία ήταν κατάλληλα για να λειτουργήσουν από μια μηχανή, χρησιμοποιώντας διάτρητες κάρτες. Η λειτουργία ήταν η εξής: Εισαγωγή των προγραμμάτων μέσω διάτρητων καρτών, ανάγνωση σειριακά από τον αναγνώστη καρτών και εκτελέσιμες ενέργειες σύμφωνα με τις εντολές που ήταν στις κάρτες. Η μηχανή αυτή αντιπροσωπεύει τον σημερινό υπολογιστή και, παρά την εξέλιξή τους, η αρχή παραμένει η ίδια.

Εικόνα 44 Alan Turing.

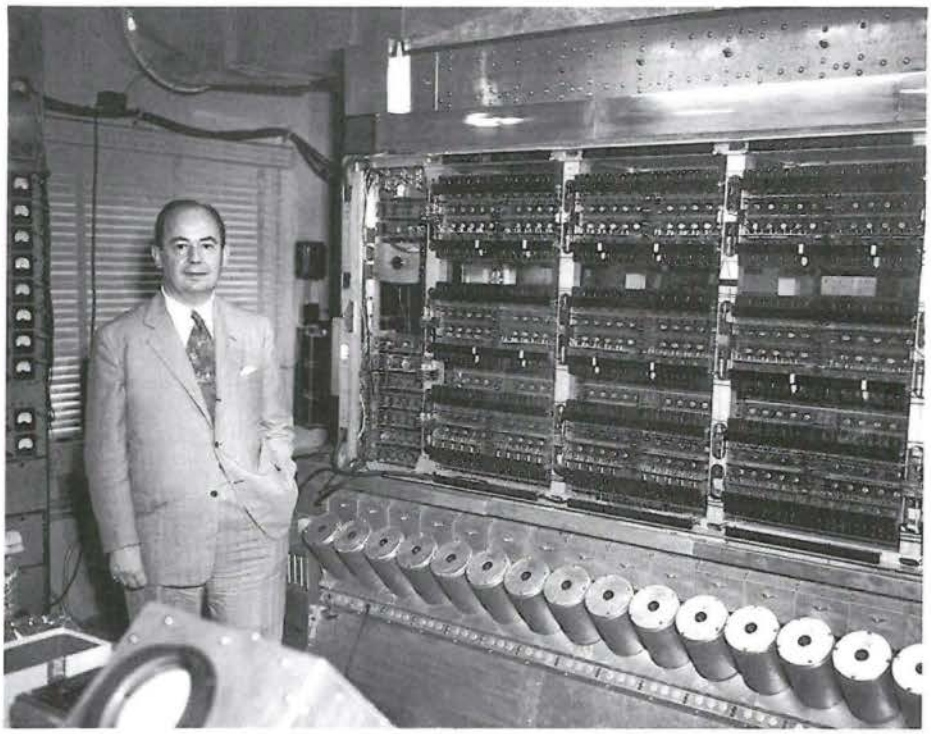
2. John Louis von Neumann (1903 - 1957)

Ο ουγγρο-αμερικανός ο Von Neumann είναι γνωστός για την προσφορά του στις θετικές επιστήμες και ιδιαίτερα στην επιστήμη των υπολογιστών όπου ξεφεύγει από τη λογική του μηχανικού υπολογισμού και αντιμετωπίζει το ζήτημα σαν κλάδο της λογικής και των μαθηματικών.

Το 1946 ο Von Neumann και οι συνεργάτες του άρχισαν το σχεδιασμό ενός υπολογιστή με αποθηκευμένο πρόγραμμα, που είχε την ονομασία IAS. Ο υπολογιστής αυτός ολοκληρώθηκε το 1952. Ο IAS αποτελεί το πρωτότυπο όλων των επόμενων υπολογιστών γενικής χρήσης διότι σε αυτόν προστέθηκε ένα νέο στοιχείο που πήρε το όνομα «μονάδα μνήμης». Η μονάδα μνήμης ήταν μία επιπλέον μονάδα η οποία μπορούσε να αποθηκεύει τις τιμές εισόδου και εξόδου.

Η αρχιτεκτονική του μοντέλου von Neumann χαρακτηρίζεται από τις από 5 διακριτές μονάδες: 1) τη μονάδα αριθμητικής λογικής (ALU), 2) τη μονάδα

ελέγχου για ρύθμιση λειτουργιών, 3) τη μνήμη, 4) τη μονάδα εισόδου δεδομένων και 5)τη μονάδα εξόδου αποτελεσμάτων. Υποστήριξε επίσης ότι ένα τέτοιο σύστημα θα έπρεπε: α) να χειρίζεται δυαδικούς αριθμούς, β) να λειτουργεί ηλεκτρονικά και γ) να εκτελεί τις λειτουργίες του μία-μία (σειριακά). Στη μνήμη του υπολογιστή υπάρχουν 1000 θέσεις αποθήκευσης που ονομάζονται λέξεις. Η κάθε θέση αποθήκευσης είναι με 40 δυαδικά ψηφία (binary digits ή bits). Στις θέσεις αυτές αποθηκεύονται και τα δεδομένα και οι εντολές. Συνεπώς οι αριθμοί αναπαρίστανται σε δυαδική μορφή και οι εντολές δυαδικοί κωδικοί. Ο κάθε αριθμός αναπαρίσταται από ένα bit προσήμου και από μια τιμή 39bit.



Εικόνα 45 John Louis von Neumann.

2.2.1 Εισαγωγικές έννοιες υπολογιστή.

Οι βασικές έννοιες που πρέπει κανείς να εξετάσει για να μπορεί να σκεφθεί λογικά και να μιλήσει με νόημα για τους υπολογιστές είναι:

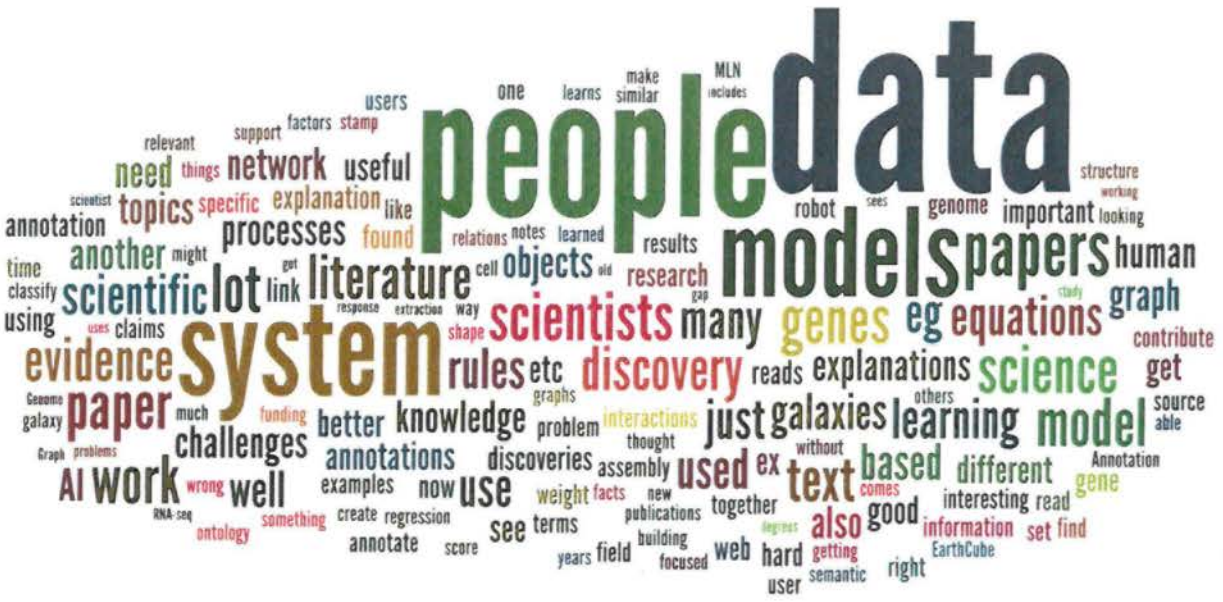
Τι είναι υπολογιστές;

Τι μπορούν να κάνουν οι υπολογιστές;

Πώς μπορούμε να επικοινωνούμε με τους υπολογιστές;

Στο συνοπτικό λεξικό της Οξφόρδης (Concise Oxford Dictionary, 1964) η λέξη υπολογιστής (Computer) ορίζεται απλά ως «ηλεκτρονική υπολογιστική μηχανή». Ο αρχικός αντικειμενικός στόχος για την ανακάλυψη του υπολογιστή ήταν να δημιουργηθεί μία γρήγορη υπολογιστική μηχανή. Σήμερα διαπιστώνεται ότι ένα μεγάλο ποσοστό των υπολογισμών αφορά εφαρμογές που είναι μη μαθηματικής ή μη αριθμητικής φύσης. Σημειώνουμε το βασικό γεγονός ότι ο υπολογιστής ενεργεί με βάση τις πληροφορίες που δέχεται. Οι πληροφορίες αυτές, που στην υπολογιστική ορολογία καλούνται «δεδομένα» (data), δίνονται με μορφή διάφορων σχημάτων και μεγεθών, από μαθηματικές εξισώσεις έως λεπτομέρειες για το εργατικό δυναμικό μιας εταιρείας που απαιτείται για την παραγωγή του μισθολογίου ή ακόμα μεγάλου όγκου δεδομένων που χρειάζονται σε επιστημονικές εφαρμογές.

Η επεξεργασία πληροφοριών από τους υπολογιστές θεωρείται θεμελιώδης και εκφράζεται με τη λέξη ΠΛΗΡΟΦΟΡΙΚΗ (Informatics). Η Πληροφορική είναι η επιστήμη της επεξεργασίας πληροφοριών, δηλαδή των μεθόδων καταγραφής, χειρισμού και ανάκτησης πληροφοριών και θεωρείται από πολλούς επιστήμονες ότι είναι η ουσία των υπολογισμών. Ο όρος Πληροφορική χρησιμοποιείται κύρια στις κεντρικές ευρωπαϊκές χώρες, ενώ στις αγγλοσαξονικές χώρες και στις Η.Π.Α. χρησιμοποιείται περίπου ισοδύναμα ο όρος «επιστήμη υπολογισμών» (computing science ή computing). Στις χώρες της πρώην Σοβιετικής Ένωσης χρησιμοποιείται με την ίδια σημασία ο όρος «κυβερνητική» (cybernetics).



Εικόνα 46 Informatics.

Στις αρχές του 18ου αιώνα, όπως προαναφέρθηκε, ο C. Babbage παρουσίασε την αναλυτική μηχανή του, που ήταν σχεδιασμένη να λειτουργεί εντελώς αυτόματα και να εκτελεί βασικές αριθμητικές λειτουργίες για κάθε μαθηματικό πρόβλημα. Η μηχανή αυτή αποτελείτο από τα ακόλουθα πέντε μέρη:

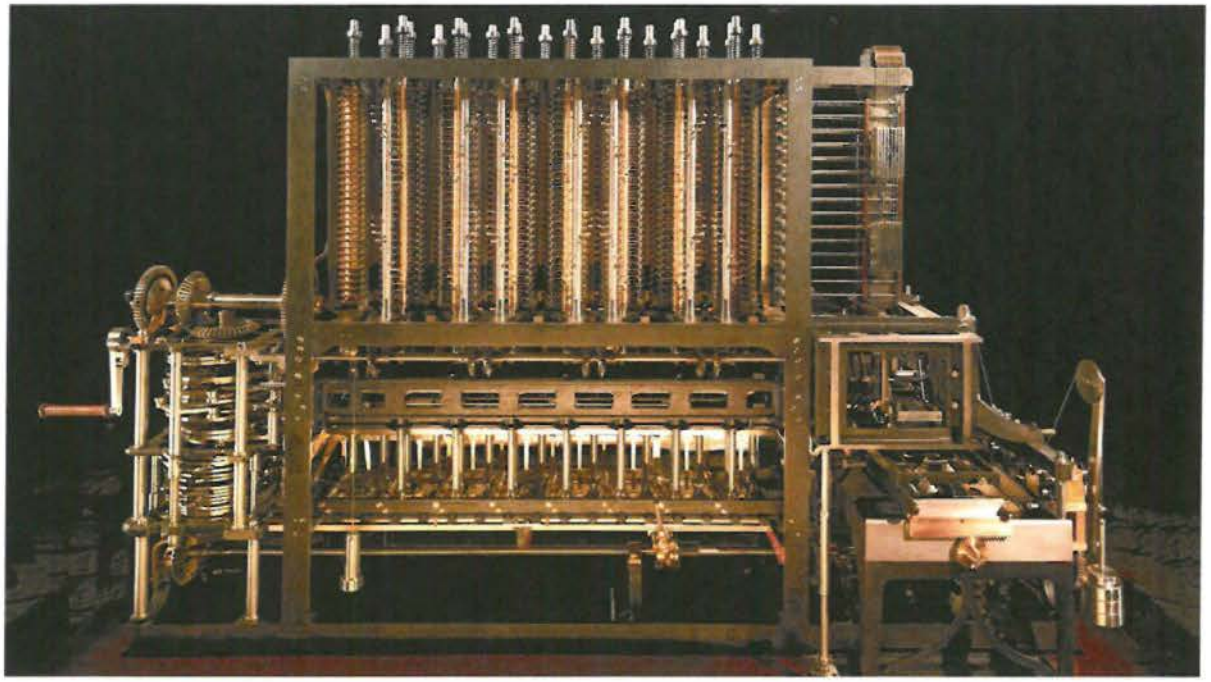
(i) Μία μνήμη που κρατούσε αριθμούς, δηλαδή εκείνους που έδιναν πληροφορίες (δεδομένα) για τα προβλήματα και εκείνους που επρόκειτο να δημιουργηθούν στην πορεία των υπολογισμών.

(ii) Μία αριθμητική μονάδα (ο Babbage την ονόμασε mill), που ήταν ένα μηχάνημα για την εκτέλεση αριθμητικών πράξεων στους αριθμούς που είχαν αποθηκευτεί. Όλες οι λειτουργίες εκτελούνταν αυτόματα μέσω περιστρεφόμενων οδοντωτών τροχών.

(iii) Μία μονάδα ελέγχου, για την πιστοποίηση ότι η μηχανή εκτελούσε τις λειτουργίες με τη σωστή σειρά και για τη μεταφορά δεδομένων μεταξύ αριθμητικής μονάδας και μνήμης (με μία σειρά οδοντωτών τροχών).

(iv) Μία μονάδα εισόδου για να δίνονται στη μηχανή δεδομένα και οδηγίες ποιες αριθμητικές λειτουργίες θα εκτελεστούν.

(v) Μία μονάδα εξόδου για να δίνονται τα αποτελέσματα. Τα τρία μέρη της αναλυτικής μηχανής που αποτελούν τη μνήμη, τον έλεγχο και την αριθμητική μονάδα είναι συλλογικά γνωστά, στην τρέχουσα ορολογία, ως Κεντρική Μονάδα Επεξεργασίας [Central Processing Unit (CPU)].

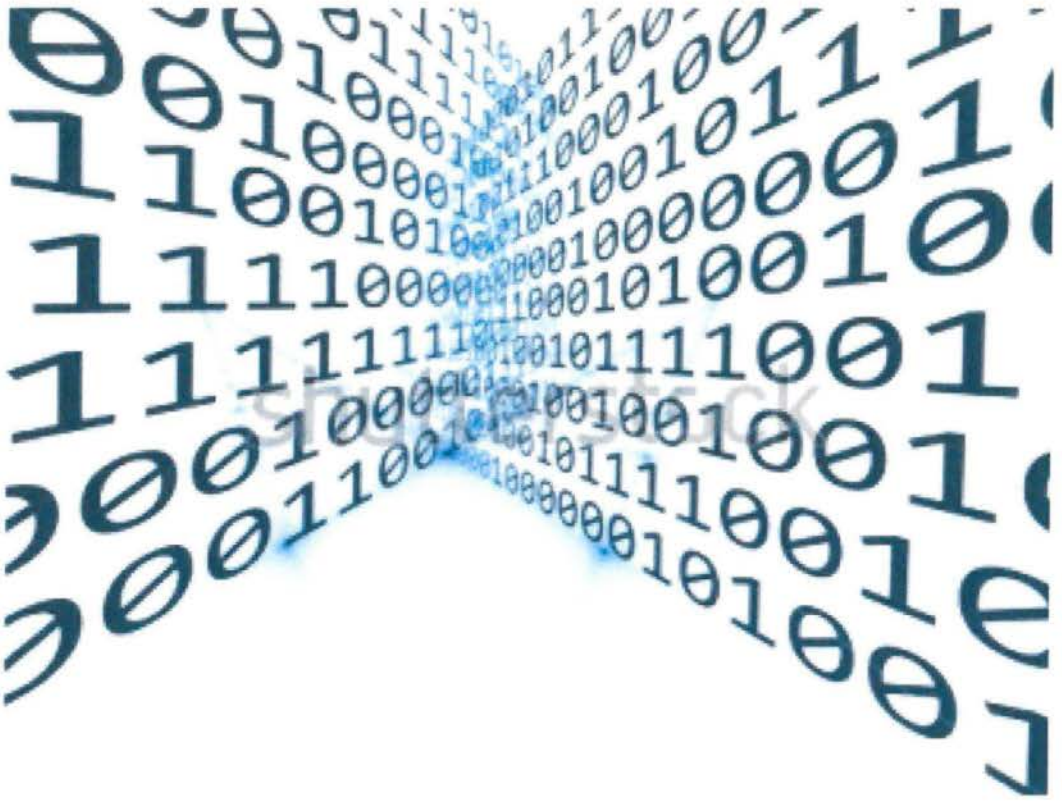


Εικόνα 47 Μηχανή Babbage.

Ενώ η αναλυτική μηχανή του Babbage ήταν μηχανική, οι σημερινοί υπολογιστές χαρακτηρίζονται ως «ηλεκτρονικοί». Ο όρος «ηλεκτρονικός» αναφέρεται σε μία ψηφιακή υπολογιστική μηχανή που είναι κατασκευασμένη από ηλεκτρονικά στοιχεία. Σημειώνεται ότι οι περισσότεροι σύγχρονοι υπολογιστές είναι ηλεκτρονικοί, ενώ υπάρχουν και ορισμένες άλλες κατηγορίες μη ηλεκτρονικών υπολογιστών, π.χ. οπτικοί υπολογιστές. Σε έναν η/υ οι πληροφορίες δηλώνονται χρησιμοποιώντας τη δυαδική κατάσταση.

Τα δεδομένα μετατρέπονται από τη μονάδα εισόδου σε ηλεκτρικούς παλμούς που μεταδίδονται στη CPU για επεξεργασία. Για να μπορεί ένας η/υ να αποθηκεύει γραπτούς χαρακτήρες, θα πρέπει να τους αναγνωρίζει ως διατεταγμένο σύνολο ηλεκτρικών παλμών. Αν η παρουσία ενός τέτοιου παλμού δηλώνεται με 1 (ένα) και η απουσία με 0 (μηδέν) και αν 000 σημαίνει S, ενώ 111 σημαίνει O (όμικρον),

τότε το γνωστό σήμα SOS θα εμφανισθεί ως 000111000. Τα στοιχεία 1 και 0 είναι γνωστά ως δυαδικά ψηφία (binary digits) ή bits.



Εικόνα 48 Binary Digit (Bit).

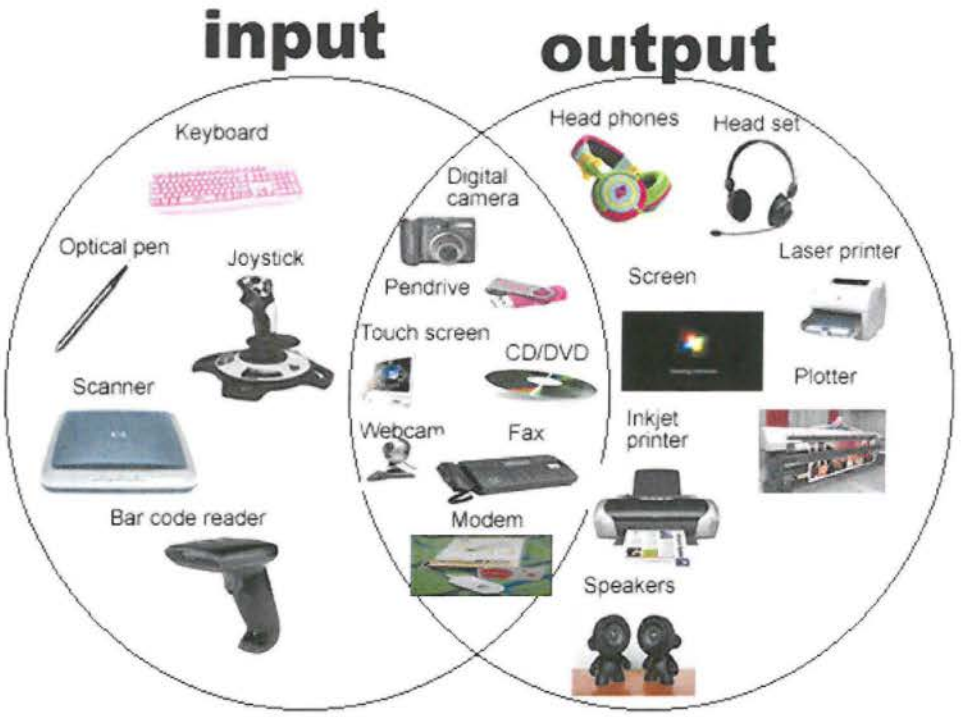
Θα θεωρήσουμε τώρα τη φύση αυτών των πληροφοριών. Οι υπολογιστές μπορούν να επεξεργασθούν τις πληροφορίες που δέχονται με έναν προκαθορισμένο λογικό τρόπο. Αν ένα δεδομένο υπολογιστικό πρόβλημα μπορεί να αναχθεί σε μια σειρά απλών, διαδοχικών λογικών λειτουργιών, τότε μπορεί να εκτελεστεί από τον υπολογιστή πολύ πιο γρήγορα απ' ότι θα μπορούσε να το επιλύσει ο άνθρωπος. Οι περισσότερες υπολογιστικές εργασίες που εκτελούνται από τους ανθρώπους είναι λογικής φύσης και συνήθως χαρακτηρίζονται από μια σειρά διαδοχικών, διακεκριμένων, λογικών βημάτων. Οι προγραμματιστές, που είναι υπεύθυνοι για τις οδηγίες που δίνονται στους υπολογιστές, χρησιμοποιούν λογικές μάλλον παρά μαθηματικές ικανότητες. Ο υπολογιστής λοιπόν μπορεί να χαρακτηριστεί ως μία λογική μηχανή.

Σημειώνεται ότι, όταν δοθούν πληροφορίες στον υπολογιστή, είναι πάντα δυνατή η ανάκληση και χρήση τους σε οποιαδήποτε χρονική στιγμή. Με αυτή την έννοια ο υπολογιστής είναι κατά πολύ ανώτερος από τον ανθρώπινο εγκέφαλο, που αν και δέχεται πλήθος πληροφοριών καθημερινά, έχει σχετική δυσκολία στην ανάκληση ορισμένων λεπτομερειών, όταν τις χρειασθεί. Ο υπολογιστής όμως μπορεί πάντοτε να έχει προσπέλαση σε πληροφορίες που έχει στη μνήμη του και αυτά τα δεδομένα μπορούν να αναπαραχθούν ακριβώς στον πρωτότυπο τύπο τους βραχυπρόθεσμα ή μετά από πολύ μεγάλα χρονικά διαστήματα, υπό την προϋπόθεση ότι δεν έχουν αλλαχθεί σκόπιμα.

Μηχανήματα Εισόδου Εξόδου.

Η λειτουργία των μηχανημάτων Εισόδου/Εξόδου [Input/Output (I/O)] είναι να δώσουν πληροφορίες στη CPU και να αποδώσουν πληροφορίες από τη CPU αντίστοιχα. Στην αρχική φάση ανάπτυξης των Υπολογιστών τα μηχανήματα εισόδου ήταν πολύ απλές μηχανές, που χρησιμοποιούσαν δυαδικά ψηφία για την ενεργοποίησή τους. Στη συνέχεια οι εξελίξεις οδήγησαν σε πολυπλοκότερα μηχανήματα, που μπορούν να μεταφράσουν χαρακτήρες και σύμβολα σε αντίστοιχες δυαδικές παραστάσεις. Ευνόητο είναι ότι το υλικό εξόδου του υπολογιστή πρέπει να είναι σε αναγνώσιμη μορφή για τον άνθρωπο. Τα μηχανήματα εισόδου μεταφράζουν κωδικοποιούν τους χαρακτήρες που εισάγουν οι χειριστές σε δυαδικές παραστάσεις, ώστε να είναι κατανοητοί από αυτά. Αντίθετα, τα μηχανήματα εξόδου αποκωδικοποιούν τις δυαδικές παραστάσεις σε αναγνωρίσιμους από τους ανθρώπους χαρακτήρες.

Ο σκοπός των μηχανημάτων εισόδου/εξόδου είναι γενικά να ενεργήσουν ως μεταφραστικά μηχανήματα μεταξύ του εξωτερικού κόσμου και του εσωτερικού κόσμου της Κεντρικής Μονάδας Επεξεργασίας (CPU), δηλαδή να ενεργήσουν ως ένα μέσο επικοινωνίας (interface) μεταξύ ανθρώπου και μηχανής.



Εικόνα 49 Input - Output.

Κύρια χαρακτηριστικά των υπολογιστών αποτελούν οι ακόλουθοι πέντε βασικοί παράγοντες:

(i) Ταχύτητα: Ο υπολογιστής κατασκευάσθηκε και χρησιμοποιήθηκε ως μία μηχανή με υψηλές υπολογιστικές ταχύτητες. Η υψηλή ταχύτητα επεξεργασίας του υπολογιστή είναι ο κύριος βασικός παράγων που οδήγησε στη λύση πολύπλοκων επιστημονικών προβλημάτων που ήταν προηγούμενα αδύνατον να επιλυθούν. Για παράδειγμα, οι διαδικασίες προσσελήνωσης και διαστημικών ταξιδιών δεν θα ήταν πραγματοποιήσιμες χωρίς τους ταχύτατους σύγχρονους υπολογιστές, όπως επίσης η συχνή και αναγκαία πληροφόρηση για την πρόγνωση του καιρού.

Για τη μεσοπρόθεσμη και μακροπρόθεσμη πρόγνωση του καιρού οι μετεωρολόγοι χρησιμοποιούν σύγχρονα υπολογιστικά συστήματα για την ταχύτατη εκτέλεση των αναγκαίων υπολογισμών και αναλύσεων. Η ικανότητα της λήψης απαντήσεων αρκετά γρήγορα από τον υπολογιστή, έτσι ώστε ο χρήστης να έχει τον

απαιτούμενο χρόνο για να ενεργήσει κατάλληλα, επιτρέπει τους υπολογισμούς σε «πραγματικό χρόνο» (real time).

Οι ηλεκτρικοί παλμοί ταξιδεύουν (μάλλον παρά κινούνται) με πολύ μεγάλες ταχύτητες και, επειδή οι υπολογιστές είναι ηλεκτρονικοί (χωρίς μηχανικές κινήσεις), η εσωτερική ταχύτητά τους αναφέρεται σε χρόνους της τάξης μικρό δευτερολέπτων (1 microsec = 10^{-6} sec), νανο-δευτερολέπτων (1 nanosec = 10^{-9} sec) και τελευταία πικο-δευτερολέπτων (1 picosec = 10^{-12} sec).

(ii) Μνήμη: Είναι γνωστό ότι ο ανθρώπινος εγκέφαλος από τις νέες γνώσεις που δέχεται επιλέγει ότι θεωρεί σπουδαίο και άξιο να κρατηθεί στη μνήμη του, ενώ οι ασήμαντες λεπτομέρειες καταχωρούνται σε «δευτερεύουσες» περιοχές της μνήμης.

Στους υπολογιστές η εσωτερική μνήμη της CPU είναι αρκετά μεγάλη, ώστε να χωρέσει ένα ορισμένο ποσό πληροφοριών, δηλαδή έχει καθορισμένα όρια. Όλα τα υπόλοιπα απαιτούμενα δεδομένα αποθηκεύονται έξω από τη μνήμη της CPU σε βοηθητικές ή δευτερεύουσες μονάδες μνήμης (auxiliary or secondary storage devices). Μικρά τμήματα από το σύνολο των δεδομένων μπορούν να μεταφερθούν στην κύρια εσωτερική μνήμη, όπως και όταν απαιτηθεί για την επεξεργασία. Η εσωτερική μνήμη (στην CPU) είναι εγκατεστημένη σε K-δομημένες μονάδες μνήμης, όπου K ισοδυναμεί με 1024 θέσεις μνήμης, π.χ. ο υπολογιστής CDC CYBER 73 είχε μνήμη 128 K (δηλ. 128 x 1024 θέσεις μνήμης).,

Εικόνα 50 CPU's.

(iii) Ακρίβεια: Μηχανικά σφάλματα στους υπολογιστές είναι δυνατόν να συμβούν, αλλά λόγω της αυξανόμενης αποδοτικότητας στις τεχνικές που ανιχνεύουν σφάλματα, αυτά σπάνια οδηγούν σε λανθασμένα αποτελέσματα. Τα σφάλματα στους υπολογισμούς σε πολύ μεγάλο ποσοστό οφείλονται σε ανθρώπινες μάλλον παρά τεχνολογικές αδυναμίες, π.χ. ανακριβή λογική στον προγραμματισμό, ανακριβή δεδομένα ή ακατάλληλα σχεδιασμένα συστήματα.

(iv) Λειτουργικότητα: Οι υπολογιστές μπορούν να εκτελέσουν σχεδόν κάθε υπολογιστικό έργο, με την προϋπόθεση ότι το έργο μπορεί να ελαττωθεί σε μία σειρά από λογικά βήματα. Για παράδειγμα, ένα έργο όπως η προετοιμασία ενός μισθολογίου ή ο έλεγχος της ροής κίνησης μπορεί να χωρισθεί σε μία λογική ακολουθία από λειτουργίες. Σημειώνεται ότι ο υπολογιστής έχει σχετικά περιορισμένη λειτουργική ικανότητα και σε τελευταία ανάλυση εκτελεί μόνον τέσσερις βασικές λειτουργίες:

α) ανταλλάσσει πληροφορίες με τον εξωτερικό χώρο μέσω των μηχανών εισόδου/εξόδου,

β) μετακινεί δεδομένα εσωτερικά στη CPU,

γ) εκτελεί βασικές αριθμητικές λειτουργίες,

δ) εκτελεί λειτουργίες σύγκρισης.

Κατά μία έννοια λοιπόν ο υπολογιστής έχει περιορισμένη λειτουργικότητα, γιατί περιορίζεται στις παραπάνω τέσσερις βασικές λειτουργίες. Επειδή όμως ένα πολύ μεγάλο μέρος δραστηριοτήτων μπορεί να θεωρηθεί ότι καλύπτεται από αυτές τις λειτουργίες, ο υπολογιστής εμφανίζεται ότι λειτουργεί πάρα πολύ έξυπνα προγραμματισμός μπορεί να θεωρηθεί ως η τέχνη που ελαττώνει ένα δεδομένο πρόβλημα σε μία κατανεμημένη συνεργασία των παραπάνω βασικών λειτουργιών.

(v) Αυτοματισμός: Όταν ένα πρόγραμμα είναι στη μνήμη του υπολογιστή, οι ατομικές οδηγίες μεταφέρονται η μία μετά από την άλλη για εκτέλεση στην μονάδα ελέγχου. Η CPU ακολουθεί αυτές τις οδηγίες, μέχρι να συναντήσει μία τελευταία οδηγία που αναφέρεται στον τερματισμό της εκτέλεσης. Στην αναλυτική μηχανή του Babbage ο όρος «αυτόματη μηχανή» σήμαινε ότι όταν η επεξεργασία ενός προγράμματος είχε αρχίσει, θα συνεχιζόταν μέχρις ότου συμπληρωθεί, χωρίς την ανάγκη ανθρώπινης παρέμβασης. Σημειώνεται ότι ο υπολογιστής εκτελεί εξαιρετικά μεγάλους αριθμούς υπολογισμών με ακριβώς την ίδια ακρίβεια και ταχύτητα όπως εκτελεί τον πρώτο υπολογισμό. Οι υπολογιστές έχουν ήδη αποδείξει σήμερα ότι είναι ένα από τα καλύτερα εργαλεία του ανθρώπου και αναμένεται ότι οι δυναμικές ωφέλειές τους στις αρχές της τρίτης χιλιετίας θα είναι πολύ μεγάλες για το ανθρώπινο γένος. Οι ωφέλειες όμως αυτές δεν θα αποδοθούν χωρίς την κατάλληλη προεργασία, που απαιτεί εντατική και επίπονη προσπάθεια και μελέτη για την πληρέστερη κατανόηση των ευεργετημάτων από τους υπολογιστές. Θα πρέπει επίσης να μελετηθεί προσεκτικά η αποφυγή των κινδύνων που τυχόν συνοδεύουν την «ανεξέλεγκτη» πρόοδο.

2.2.2 Κατηγορίες Υπολογιστών.

Οι υπολογιστές μπορούν να ταξινομηθούν με διάφορους τρόπους:

(i) Ανάλογα με τον τρόπο παράστασης πληροφοριών σε ψηφιακούς (digital), αναλογικούς (analogue) και υβριδικούς (hybrid). Οι ψηφιακοί υπολογιστές επεξεργάζονται διακεκριμένα (ψηφιακά) μεγέθη και μπορούν να εκτελέσουν αριθμητικές και λογικές πράξεις με την επιθυμητή ακρίβεια και σε μικρό χρονικό διάστημα. Οι αναλογικοί λειτουργούν με συνεχή (αναλογικά) μεγέθη, π.χ. θερμοκρασίες, και αποτελούν μία συλλογή παράλληλων υπολογιστικών στοιχείων που μπορούν εύκολα να επεκταθούν, ενώ οι υβριδικοί αποτελούν έναν συνδυασμό των δύο προηγούμενων κατηγοριών.

(ii) Ανάλογα με τη χρήση τους σε γενικού σκοπού και ειδικού σκοπού.

(iii) Ανάλογα με το είδος εφαρμογών σε υπολογιστές επιστημονικών εφαρμογών και υπολογιστές διαχειριστικών εφαρμογών. Στην πρώτη κατηγορία η έμφαση δίνεται στην ταχύτητα επεξεργασίας, ενώ στη δεύτερη κατηγορία ο φόρτος επικεντρώνεται στην είσοδο-έξοδο στοιχείων.

(iv) Ανάλογα με τα κριτήρια προδιαγραφών κατηγοριοποίησης, που αναφέρονται σε παράγοντες όπως: τρόπος εργασίας και τυπικές προδιαγραφές (floating point, specs κτλ.), κεντρική μνήμη, «ρυθμό απόδοση» (throughput) κτλ. Αντιπροσωπευτικές τάξεις αποτελούν οι προσωπικοί υπολογιστές, οι σταθμοί εργασίας και οι «εξυπηρετητές».

Εικόνα 51 Τύποι Υπολογιστών.

Οι προσωπικοί υπολογιστές [Personal Computers (PC)] είναι μικρού μεγέθους οικονομικά μικροϋπολογιστικά συστήματα (πρωτοχρησιμοποιήθηκαν στα μέσα της δεκαετίας 1970 80) διαθέσιμα για κάθε εργαζόμενο, που μπορεί να πάρει πληροφορίες από μεγαλύτερα συστήματα και να αυξήσει σημαντικά την προσωπική του παραγωγικότητα.

«εξυπηρετητής» (server) είναι ένας ειδικός υπολογιστής που συντονίζει και προωθεί προγράμματα ή δεδομένα σε άλλους υπολογιστές μέλη (κόμβους) ενός δικτύου υπολογιστών. Οι σταθμοί εργασίας (workstations) είναι μικροϋπολογιστές μεγάλης υπολογιστικής ισχύος, που χρησιμοποιούνται συχνά είτε αυτόνομα για παραγωγή γραφικών ή ως «εξυπηρετητές» σε ένα μικρό δίκτυο υπολογιστών. Σημειώνεται ότι τα όρια της παλαιότερης κατηγορίας «μεγέθους» [μεγάλοι ή κεντρικοί (large mainframe), μεσαίοι (medium), μίνι (mini), μικροϋπολογιστές (microcomputers)] δεν ήταν σαφώς καθορισμένα και υπήρχε επικάλυψη του κριτηρίου αυτού σε διάφορες περιπτώσεις, όπως π.χ. υπέρ μικροϋπολογιστές (supermicro), όπου έπρεπε να χρησιμοποιούνται άλλα κριτήρια διάκρισης, όπως π.χ. υπολογιστική ισχύς, ταχύτητα επεξεργασίας, κόστος κτλ. Οι φορητοί μικροϋπολογιστές είναι συμπαγείς, ελαφριοί και περιλαμβάνουν διάφορους τύπους, όπως π.χ. laptop computers, μεγέθους χαρτοφύλακα και βάρους περίπου 5 kg, notebook computers, μεγέθους σημειωματάριου περίπου 3 kg, και palmtop computers, μεγέθους ανθρώπινης παλάμης με βάρος λιγότερο από 1 kg. Ο κύριος σκοπός κατασκευής των φορητών μικροϋπολογιστών είναι να παρέχουν τη μεγαλύτερη δυνατή υπολογιστική ισχύ στη μικρότερη δυνατή επιφάνεια. Αναφέρονται επίσης τύποι υπολογιστών, όπως π.χ. υπερυπολογιστές, υπολογιστές 5ης και 6ης γενιάς, προσωπικοί υπολογιστές, δικτυακοί υπολογιστές [network computers (NC)], οικιακοί υπολογιστές, προηγμένοι σταθμοί εργασίας, παράλληλοι υπολογιστές, οπτικοί και νευρωνικοί υπολογιστές, βιοϋπολογιστές κτλ.

Πρόσφατες παρατηρήσεις σε διάφορα συστήματα σωματιδίων του μικρόκοσμου που υπακούουν στους νόμους της Κβαντομηχανικής έδειξαν ότι αυτά έχουν πολύ μεγαλύτερες δυνατότητες επεξεργασίας δεδομένων απ' ότι τα κλασικά που χρησιμοποιούνται σήμερα. Το γεγονός αυτό έχει οδηγήσει σε θεωρητικές μελέτες για την κατασκευή ενός «κβαντικού» υπολογιστή.

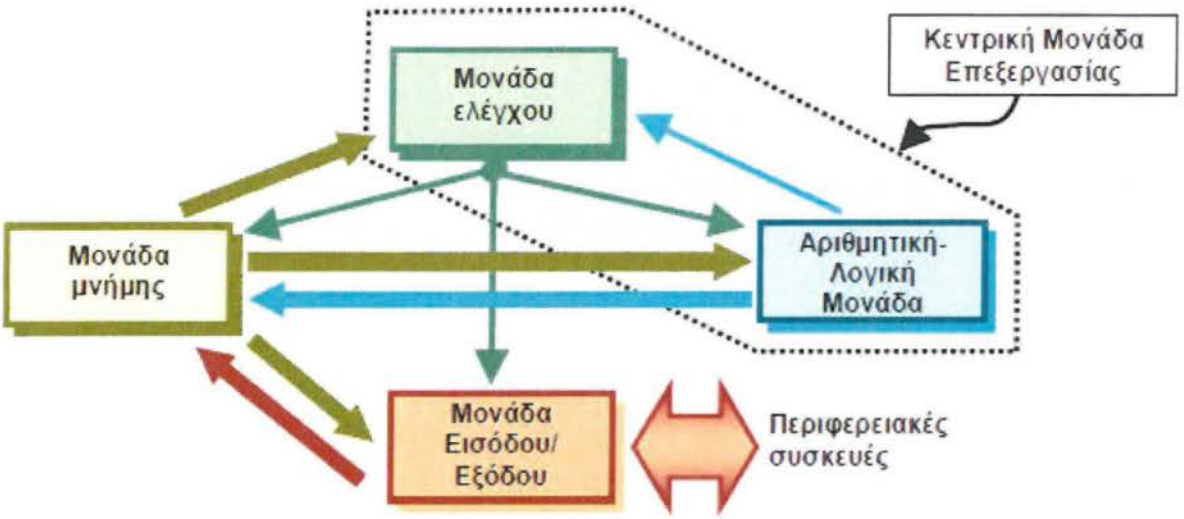
2.2.3 Δομή Υπολογιστή.

Ο υπολογιστής γενικά λαμβάνει πληροφορίες (input), επεξεργάζεται τις πληροφορίες αυτές σύμφωνα με ένα σύνολο εντολών (στη CPU) και στη συνέχεια παρουσιάζει τα αποτελέσματα σε χρήσιμη μορφή (output). Η κεντρική μονάδα επεξεργασίας (CPU) αποθηκεύει τις πληροφορίες στη μνήμη πριν εκτελεστούν οι λειτουργίες επεξεργασίας. Με τον όρο μνήμη σε ένα υπολογιστικό σύστημα εννοούμε κάθε μέσο αποθήκευσης πληροφοριών, όπως π.χ. οι μαγνητικοί και οπτικοί δίσκοι, οι μαγνητικές δισκέτες, η κύρια μνήμη κ.ά. Πληροφορίες εισόδου αποτελούν το πρόγραμμα και τα δεδομένα. Το πρόγραμμα είναι το σύνολο των εντολών (instructions) που εκτελεί ο υπολογιστής και τα δεδομένα είναι οι πληροφορίες στις οποίες εφαρμόζονται οι παραπάνω εντολές.

Για παράδειγμα, αν το πρόβλημα είναι η αλφαβητική ταξινόμηση ενός καταλόγου συνδρομητών τηλεφώνου, τότε η ακολουθία εντολών ή η διαδικασία που ακολουθείται από τον υπολογιστή για τη λειτουργία αυτή είναι το πρόγραμμα, ενώ ο κατάλογος με τα ονόματα που θα ταξινομηθούν είναι τα δεδομένα. Όλες οι πληροφορίες, πρόγραμμα και δεδομένα, παριστάνονται με αριθμητική μορφή. Εκτός από τις αριθμητικές πράξεις (+, -, *, /), εκτελούνται επίσης λογικού τύπου πράξεις και γίνονται συγκρίσεις. Για το λόγο αυτό η μονάδα αναφέρεται ως Αριθμητική και Λογική Μονάδα [Arithmetic and Logic Unit (ALU)]. Για τον έλεγχο της σωστής τοποθέτησης πληροφοριών στη μνήμη, της κατάλληλης σειράς των οδηγιών προγράμματος και επιλογής δεδομένων από τη μνήμη, απαιτείται μία Μονάδα Ελέγχου (Control Unit).Η μονάδα ελέγχου με την ALU και τη μονάδα μνήμης σχηματίζουν την Κεντρική Μονάδα Επεξεργασίας [Central Processing Unit (CPU)].

Η βασική δομή μίας απλοποιημένης μορφής ενός υπολογιστή (μοντέλο von Neumann), όπου οι διακεκομμένες γραμμές δηλώνουν έλεγχο γεγονότων, ενώ οι πλήρεις γραμμές δηλώνουν ροή πληροφοριών. Ένα υπολογιστικό σύστημα διαθέτει συνήθως πολλούς τύπους μνήμης. Η μνήμη, που είναι απ' ευθείας προσπελάσιμη από την CPU, ονομάζεται κύρια μνήμη (main memory) ή κεντρική μνήμη. Η κεντρική μνήμη έχει τη δυνατότητα άμεσης επικοινωνίας με τις άλλες μονάδες μνήμης (ROM, PROM, RAM κ.ά.). Σημειώνουμε ότι σε κλασικούς υπολογιστές με αποθηκευμένα προγράμματα, που συχνά αναφέρονται ως μηχανές

von Neumann, οι εντολές και τα δεδομένα αποθηκεύονται χωρίς διάκριση στην κύρια μνήμη.



Εικόνα 52 Δομή Υπολογιστή.

Ένα υπολογιστικό σύστημα μπορεί να χρησιμοποιεί πολλά είδη μονάδων μνήμης. Κάθε είδος μνήμης έχει ορισμένα ιδιαίτερα χαρακτηριστικά τα οποία επιβάλλουν τη χρησιμοποίησή του. Η μονάδα μνήμης αναφέρεται σε ένα σύνολο καταχωρητών υψηλής ταχύτητας. Ο υπολογιστής,, το κυριότερο τμήμα ενός υπολογιστικού συστήματος, αποτελείται από την CPU και την κύρια μνήμη, που τοποθετούνται συνήθως στο ίδιο κατασκευαστικό συγκρότημα. Οι οδηγίες προγράμματος και τα δεδομένα μεταφέρονται από την είσοδο στη μνήμη, με την εποπτεία της μονάδας ελέγχου. Κατά τη διάρκεια της εκτέλεσης του προγράμματος κάθε οδηγία ανακτάται από τη μνήμη και ερμηνεύεται κατάλληλα. Ο έλεγχος πληροφορεί την ALU για την ακριβή πράξη που πρέπει να εκτελεσθεί και κατευθύνει τη μεταφορά στην ALU κάθε ομάδας δεδομένων που χρειάζονται για την πράξη. Η ALU εκτελεί τότε όλους τους υπολογισμούς και συγκρίσεις. Τα αποτελέσματα κατευθύνονται στη μνήμη, όπου κρατούνται προσωρινά πριν από την παρουσίασή τους στην έξοδο. Η διαδικασία αυτή γίνεται με την εποπτεία της μονάδας ελέγχου. Όλες οι λειτουργίες του υπολογιστή εκτελούνται υπό τον έλεγχο της CPU, που αποτελεί την «καρδιά» του συστήματος, και διαθέτει τρία βασικά χαρακτηριστικά:

(i) Επικοινωνεί με την κύρια μνήμη για αποθήκευση δεδομένων και προγραμμάτων,

(ii) ελέγχει κάθε λειτουργία με τη μονάδα ελέγχου, και

(iii) εκτελεί αριθμητικές και συγκριτικές πράξεις με την αριθμητική/λογική μονάδα.

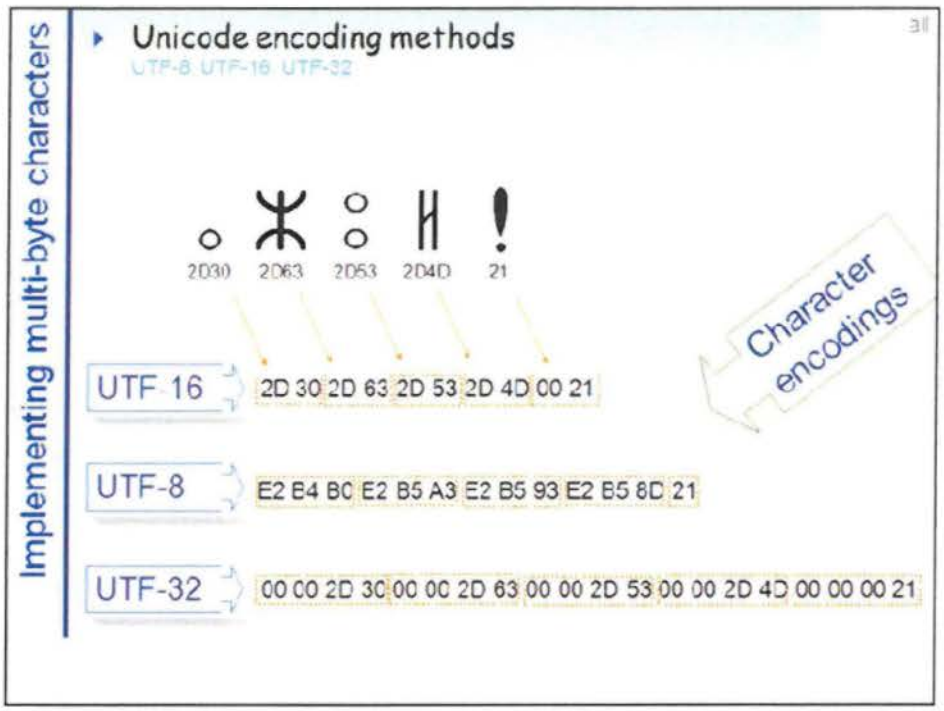
Οι βασικές λειτουργίες της CPU είναι λοιπόν ο έλεγχος μετάδοσης προγραμμάτων και αρχείων από τη βοηθητική μνήμη στην κύρια μνήμη, και η επεξεργασία δεδομένων σύμφωνα με τις οδηγίες του προγράμματος. Άλλες βασικές λειτουργίες της CPU είναι (α) η ενεργοποίηση μονάδων εισόδου για εισαγωγή δεδομένων (αρχείων) και προγραμμάτων και (β) ο έλεγχος δημιουργίας αποτελεσμάτων (εξόδου). Η CPU ενεργοποιεί τις μονάδες εξόδου και ελέγχει τη μετάδοση πληροφοριών προς τις μονάδες εξόδου. Οι περισσότεροι υπολογιστές χρησιμοποιούν ολοκληρωμένα κυκλώματα (chips) για τη CPU και την κύρια μνήμη. Η CPU και η κύρια μνήμη ενός μικροϋπολογιστή συνήθως τοποθετούνται σε μία απλή κάρτα που είναι γνωστή ως μικροεπεξεργαστής (microprocessor).

2.2.4 Δεδομένα υπολογιστή.

Οι πληροφορίες χρησιμοποιούνται από τον υπολογιστή μέσω ηλεκτρικών εξαρτημάτων, όπως τρανζίστορς και ολοκληρωμένα κυκλώματα (integrated circuits), μαγνητικοί πυρήνες (magnetic cores) και ημιαγωγοί (semi conductors) κτλ., που όμως μπορούν να δηλώσουν μόνο δύο καταστάσεις ή συνθήκες. Οι πληροφορίες στο σύνολό τους αντιπροσωπεύονται μέσα στον υπολογιστή με την παρουσία ή απουσία διάφορων σημάτων, ενώ το δυαδικό αριθμητικό σύστημα (με στοιχεία 0 και 1) χρησιμοποιείται για να εκφράσει τις δύο πιθανές καταστάσεις. Όλα τα συνήθη σύμβολα που χρησιμοποιούνται σε γραπτές πληροφορίες αντιπροσωπεύονται στον υπολογιστή από συνδυασμούς διάφορων δυαδικών ψηφίων [binary digits (bits)], με ένα μοναδικό συνδυασμό για κάθε σύμβολο. Ένα σύνολο τέτοιων συνδυασμών από bits μπορεί να περιλαμβάνει τα γράμματα του αλφαβήτου, τα ψηφία 0-9 και ορισμένους ειδικούς χαρακτήρες.

Ένα τέτοιο σύνολο χαρακτήρων καλείται Αλφαριθμητικό (Alphanumeric ή Alphameric). Μία κοινή μέθοδος κωδικοποίησης χρησιμοποιεί ένα συνδυασμό από έξι bits για κάθε χαρακτήρα, που μπορούν να διαταχθούν κατά $2^6 = 64$ διαφορετικούς τρόπους, δηλαδή επιτρέποντας τη χρήση ενός συνόλου 64 χαρακτήρων. Σημειώνεται ότι η χρήση πέντε bits για κάθε σύμβολο θα δώσει 32 δυνατούς συνδυασμούς και ο αριθμός χαρακτήρων για αντιπροσώπευση στην περίπτωση αυτή θεωρείται ανεπαρκής. Οι πληροφορίες εκφράζονται σε λέξεις (words) υπολογιστή. Κάθε τέτοια λέξη είναι μία ομάδα από bits και το μήκος της διαφέρει από υπολογιστή σε υπολογιστή, είναι όμως σαφώς προκαθορισμένο για κάθε υπολογιστή. Το μήκος μιας λέξης υπολογιστή μπορεί να είναι από 8 bits έως 64 bits. Σε μερικούς υπολογιστές η θεμελιώδης ομαδοποίηση των bits καλείται ψηφιολέξη (byte), είναι συνήθως μικρότερη από μία λέξη και αποτελείται τυπικά από 8 bits.

Μία ψηφιολέξη, που αποτελείται από 8 bits, μπορεί να χρησιμοποιηθεί για αντιπροσώπευση ενός αλφαριθμητικού χαρακτήρα ή δύο δεκαδικών ψηφίων. Σε άλλους υπολογιστές η ομαδοποίηση των bits, ψηφιολέξεων ή λέξεων είναι ευέλικτη στον σχεδιασμό, έτσι ώστε να συμφωνεί στις διαφορετικές απαιτήσεις αποθήκευσης των αριθμών, αλφαριθμητικών χαρακτήρων και οδηγιών. Ανάλογα με τον τύπο της πληροφορίας (αλφαριθμητικά δεδομένα, αριθμητικά δεδομένα ή οδηγίες μηχανής) που θα αποθηκευτεί, η λέξη του υπολογιστή τακτοποιείται διαφορετικά. Μία λέξη π.χ. από 21 bits με αλφαριθμητική κωδικοποίηση και ομαδοποίηση από 7 bits [σε κώδικα ASCII (American Standard Code for Information Interchange) που ορίζει 128 διαφορετικούς χαρακτήρες]



Εικόνα 53 Unicode Encoding Methods.

Οι ειδικοί κώδικες που χρησιμοποιούνται για την παράσταση χαρακτήρων κατά τη λειτουργία αποθήκευσής τους, την εισαγωγή εξαγωγή και μετάδοσή τους καλούνται κώδικες χαρακτήρων. Οι κώδικες αυτοί διακρίνονται σε «κώδικες εσωτερικής παράστασης», που χρησιμοποιούνται για την παράσταση πληροφοριών στη μνήμη του υπολογιστή, και σε «κώδικες επικοινωνίας», που αναφέρονται σε λειτουργίες εισόδου-εξόδου. Οι κώδικες χαρακτήρων που χρησιμοποιούνται περισσότερο στους υπολογιστές είναι οι εξής:

(i) Ο κώδικας ASCII (American Standard Code for Information Interchange) ή κώδικας λατινικών χαρακτήρων, που μπορεί να χρησιμοποιεί 7 ή 8 bits δεδομένων για κάθε θέση αποθήκευσης ή «ψηφιολέξη». Στον 8 ψήφιο κώδικα ASCII, τα 4 bits (ζώνης) δηλώνουν αν ένας χαρακτήρας είναι γράμμα, αριθμός (θετικός, αρνητικός ή χωρίς πρόσημο) ή ειδικό σύμβολο, ενώ τα υπόλοιπα 4 bits (ψηφίου) χρησιμοποιούνται για την παράσταση των αριθμών 0 9. Για παράδειγμα, η ύπαρξη 1111 στα 4 bits ζώνης δηλώνει ένα χαρακτήρα ως αριθμό χωρίς πρόσημο, ενώ το 0100 στα 4 bits ψηφίου παριστάνει τον αριθμό 4.

(ii) Ο κώδικας EBCDIC (Extended Binary Coded Decimal Interchange Code) που χρησιμοποιεί 8 bits δεδομένων για κάθε ψηφιολέξη. Ο κώδικας EBCDIC, που

χρησιμοποιείται από πολλούς υπολογιστές, ειδικά από κεντρικούς υπολογιστές IBM και αντίστοιχους συμβατούς, ορίζει ένα σύνολο $2^8 = 256$ διαφορετικούς χαρακτήρες, ενώ ο κώδικας ASCII με 7 bits χρησιμοποιείται κύρια από μικρο υπολογιστές και ορίζει $2^7 = 128$ συνολικά διαφορετικούς χαρακτήρες. Ο παγκόσμιος κώδικας (universal code) περιέχει ένα σύνολο χιλιάδων διαφορετικών χαρακτήρων και χρησιμοποιείται ιδιαίτερα σε παραστάσεις γραμμάτων από τα αλφάβητα διάφορων γλωσσών, όπως, Ιαπωνική, Κινέζικη, Εβραϊκή, Πολωνική κτλ., και ειδικών συμβόλων και ιδεογραμμάτων.

2.2.5 Συστήματα αρίθμησης - Λογικές Πύλες.

Ένας αριθμός αποτελείται από ξεχωριστά ψηφία. Η τιμή κάθε ψηφίου σε ένα αριθμό καθορίζεται από τα ακόλουθα:

(i) Το ίδιο το ψηφίο,

(ii) τη θέση του ψηφίου στον αριθμό,

(iii) τη βάση του συστήματος αρίθμησης, όπου η βάση ορίζεται ως ο αριθμός των ψηφίων που προσφέρονται σε κάθε θέση.

Στο δεκαδικό σύστημα η βάση είναι ίση με 10, επειδή κάθε θέση μπορεί να περιέχει ένα από τα δέκα ψηφία 0-9. Το σύστημα λοιπόν έχει έναν παράγοντα «μεταφοράς» 10 και κάθε ψηφίο δηλώνει μία τιμή που εξαρτάται από τη θέση την οποία κατέχει, π.χ. στον αριθμό 2475 το ψηφίο 2 σημαίνει 2 x 10, ενώ στον αριθμό 4527 το ίδιο ψηφίο 2 x 10 κτλ. Στο δυαδικό σύστημα η βάση είναι 2 και τα δύο ψηφία είναι 0 και 1. Ο χειρισμός πληροφοριών σε ένα υπολογιστή γίνεται με ηλεκτρικές συνιστώσες, π.χ. ολοκληρωμένα κυκλώματα, ημιαγωγοί, μαγνητικοί πυρήνες, σύρματα, οι οποίες μπορούν να εμφανίσουν μόνο δύο πιθανές καταστάσεις ή συνθήκες. Για παράδειγμα τα μαγνητικά υλικά είναι μαγνητισμένα ή όχι μαγνητισμένα, ή μαγνητισμένα προς μία διεύθυνση ή προς την αντίθετη διεύθυνση. Οι πληροφορίες παριστάνονται στον υπολογιστή με την παρουσία ή απουσία διαφόρων σημάτων. Το δυαδικό σύστημα, που έχει μόνο δύο ψηφία (0 και 1), χρησιμοποιείται κατάλληλα για να εκφράσει τις δυο πιθανές καταστάσεις.

Binary	Hex	Decimal
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

Εικόνα 54 Πίνακας με αριθμούς στη δυαδική, δεκαεξαδική και δεκαδική αναπαράσταση τους.

Οι δυαδικές πληροφορίες αντιπροσωπεύονται στους ψηφιακούς υπολογιστές με φυσικές ποσότητες που καλούνται σήματα (signals). Τα ηλεκτρικά σήματα, π.χ. τάση, υπάρχουν στον υπολογιστή σε δύο αναγνωρίσιμες καταστάσεις μιας δυαδικής μεταβλητής, που μπορεί να είναι ίση με 0 ή 1. Ο χειρισμός των δυαδικών πληροφοριών γίνεται με λογικά κυκλώματα (πύλες). Κάθε πύλη έχει ένα διακεκριμένο γραφικό σύμβολο, καθορισμένη λειτουργία (αλγεβρική έκφραση), και η σχέση εισόδου εξόδου των δυαδικών μεταβλητών μπορεί να παρασταθεί με έναν αντίστοιχο λογικό πίνακα ή πίνακα αλήθειας (truth table).

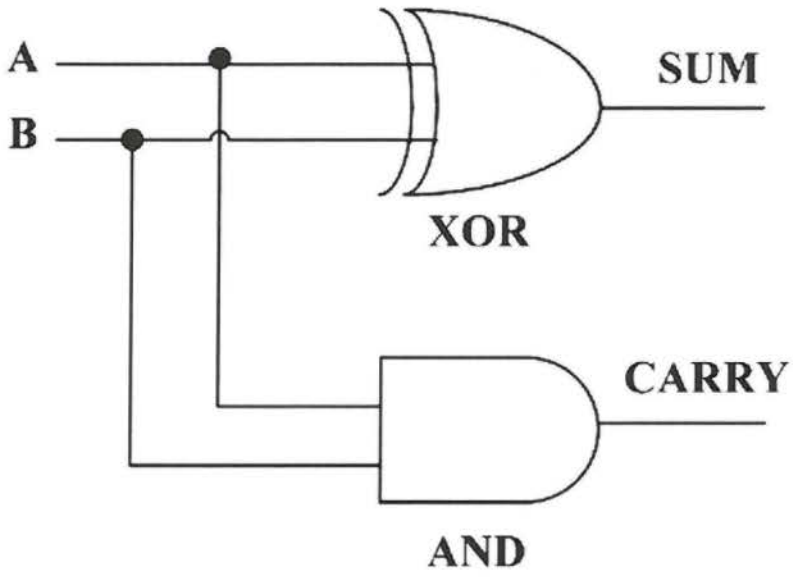
Λογικές πύλες: Τα κυκλώματα είναι κατασκευασμένα χρησιμοποιώντας συνδυασμούς διάφορων τύπων πυλών για την εκτέλεση αριθμητικών πράξεων. Υπάρχουν διάφοροι τύποι πυλών (gates), από τις οποίες οι γνωστότερες στοιχειώδεις λογικές πύλες είναι AND, OR και NOT. Η χρήση αυτών των λογικών πυλών είναι ικανή για να δείξει την έννοια του σχεδιασμού κυκλωμάτων.

(i) Μία πύλη AND δημιουργεί ως σήμα εξόδου 1, μόνο αν όλα τα σήματα εισόδου είναι επίσης 1.

(ii) Μία πύλη OR δημιουργεί ως σήμα εξόδου 1, αν ένα από τα σήματα εισόδου είναι επίσης 1.

(iii) Μία πύλη NOT δημιουργεί ως σήμα εξόδου το αντίστροφο του αρχικού σήματος.

Χρησιμοποιώντας την έξοδο από μία πύλη ως μέρος της εισόδου σε άλλη πύλη και χρησιμοποιώντας μία ποικιλία από πύλες τακτοποιημένες σε διαφορετικές ακολουθίες, μπορούμε να κατασκευάσουμε κυκλώματα που εκτελούν αριθμητική με 1 και 0. Είναι δυνατή επίσης η παραγωγή μίας σειράς από λογικές πύλες που μπορούν να επιλύσουν σωστά τις τέσσερις δυνατές περιπτώσεις πρόσθεσης, έτσι ώστε όποια και αν είναι τα δύο σήματα εισόδου, να σχηματίζεται πάντοτε το σωστό άθροισμα και το σωστό ψηφίο μεταφοράς.



Εικόνα 55 Δυαδικός προσθέτης.

Σημειώνουμε ότι η ύπαρξη της πύλης NOT είναι απλά ενδεικτική του τρόπου λειτουργίας αυτής της λογικής πύλης. Συνδέοντας σχεδιασμούς όπως οι παραπάνω και χρησιμοποιώντας άλλους τύπους πυλών και πύλες που έχουν περισσότερες από δύο εισόδους, είναι δυνατή η κατασκευή πλήρων κυκλωμάτων που εκτελούν

όλες τις απαραίτητες αριθμητικές λειτουργίες του υπολογιστή καθώς επίσης και η χρήση μεγάλων σειρών από bits, αντί να χρησιμοποιούνται δύο bits κάθε φορά.

Άλλοι τύποι λογικών πυλών είναι οι πύλες NAND και NOR. Η πύλη NAND (ο όρος προέρχεται από συντόμευση των όρων NOT-AND) χρησιμοποιεί το γραφικό σύμβολο της πύλης AND ακολουθούμενο από ένα μικρό κύκλο, και η λειτουργία της είναι συμπληρωματική της λειτουργίας της πύλης AND. Η πύλη NOR είναι αντίστοιχα το συμπλήρωμα της πύλης OR και χρησιμοποιεί το γραφικό σύμβολο της OR ακολουθούμενο από ένα μικρό κύκλο. Οι πύλες NAND και NOR μπορούν να έχουν περισσότερα από δύο στοιχεία εισόδου, και το αποτέλεσμα στην έξοδο είναι πάντοτε το συμπλήρωμα των λειτουργιών AND ή OR αντίστοιχα. Η «αποκλειστική» πύλη OR [exclusive OR (XOR) gate] δίνει στην έξοδο αποτέλεσμα 1, όταν υπάρχει στην είσοδο στοιχείο 1, εκτός από την περίπτωση όπου και τα δύο στοιχεία εισόδου είναι 1. Η πύλη XOR παριστάνεται με το ίδιο σύμβολο της πύλης OR, αλλά με την προσθήκη μιας καμπύλης γραμμής στην πλευρά της εισόδου.

Λογική Πύλη	Σύμβολο	Αλγεβρική Πράξη	Πίνακας Αλήθειας
AND		C = A · B	A 0 1 0 1 B 0 0 1 1 C 0 0 0 1
OR		C = A + B	A 0 1 0 1 B 0 0 1 1 C 0 1 1 1
NOT		C = A'	A 0 1 C 1 0
NAND		C = (AB)'	A 0 1 0 1 B 0 0 1 1 C 1 1 1 0
NOR		C = (A + B)'	A 0 1 0 1 B 0 0 1 1 C 1 0 0 0
XOR		C = A'B + AB'	A 0 1 0 1 B 0 0 1 1 C 0 1 1 0
XNOR		C = A'B' + AB	A 0 1 0 1 B 0 0 1 1 C 1 0 0 1

Εικόνα 56 Λογικές Πύλες και πίνακες αληθείας.

Η «αποκλειστική» πύλη NOR [exclusive NOR (XNOR) gate] είναι το συμπλήρωμα της πύλης XOR. Η έξοδος της πύλης XNOR είναι 1, μόνον εάν και τα δύο στοιχεία εισόδου είναι 1 ή και τα δύο στοιχεία εισόδου είναι 0. Στη συνέχεια δίνεται ένας ενδεικτικός κατάλογος ψηφιακών λογικών πυλών με εναλλακτικούς γραφικούς συμβολισμούς, αντίστοιχες αλγεβρικές πράξεις και πίνακες «αλήθειας».

Οι λογικές πύλες της ALU που επιτρέπουν να εκτελεστούν οι αριθμητικές πράξεις δεν πρέπει να συγχέονται με την ικανότητα του υπολογιστή να δοκιμάζει διάφορες συνθήκες που προκύπτουν κατά τη διάρκεια εκτέλεσης του προγράμματος και να εκτελεί τις κατάλληλες ενέργειες που βασίζονται στις οδηγίες που δίνονται από τον προγραμματιστή. Η λογική περιοχή της ALU εκτελεί όλες τις αναγκαίες λογικές ενέργειες.

2.2.6 Μνήμη και Αρχιτεκτονική υπολογιστή.

Τα δεδομένα και οι οδηγίες που χρειάζεται η ALU παίρνονται από τη Μονάδα Μνήμης (memory unit), που είναι κατασκευασμένη από έναν αριθμό θέσεων ή κελιών (cells). Σε καθεμία από τις θέσεις αυτές μπορεί να αποθηκευθεί μία λέξη, διατηρώντας μία οδηγία ή στοιχεία δεδομένων. Ο αριθμός και το μέγεθος των θέσεων σε μία περιοχή μνήμης ποικίλλει από υπολογιστή σε υπολογιστή. Κάθε τέτοια περιοχή αριθμείται σειριακά για να δώσει μία μοναδική αναφορά για κάθε στοιχείο πληροφορίας που κρατείται στη μνήμη. Η αναφορά αυτή είναι γνωστή ως διεύθυνση θέσης (location address).

Η σκοπιμότητα της διεύθυνσης θέσης στη μνήμη του υπολογιστή είναι η εξακρίβωση κάθε θέσης, έτσι ώστε κάθε στοιχείο πληροφορίας να μπορεί να τοποθετηθεί στη μνήμη και στη συνέχεια να προσδιορίζεται με αναφορά στη διεύθυνση θέσης, που ο υπολογιστής «θυμάται». Αυτό σημαίνει ότι τα περιεχόμενα μιας θέσης αποθήκευσης μπορούν να μεταβληθούν και οι νέες πληροφορίες μπορούν να ανακτηθούν χωρίς να είναι γνωστά τα πραγματικά περιεχόμενά της. Μία οδηγία που προέρχεται από μία λέξη μνήμης (χρησιμοποιώντας τη μονάδα ελέγχου) αποτελείται κανονικά από τον κώδικα λειτουργίας (operation code), που δηλώνει τι πρέπει να γίνει, και από τη διεύθυνση (θέσης), που δηλώνει την ακριβή θέση μνήμης που περιέχει τις πληροφορίες που χρησιμοποιούνται όταν εκτελείται η λειτουργία. Η κύρια μνήμη ενός υπολογιστή που χρησιμοποιεί ολοκληρωμένα κυκλώματα είναι δυνατόν να απολέσει όλα τα περιεχόμενά της αν χαθεί η (ηλεκτρική) ενέργεια λειτουργίας του (volatile memory), ενώ οι βοηθητικές μνήμες, π.χ. δίσκοι, για την αποθήκευση δεδομένων και προγραμμάτων δεν παρουσιάζουν την παραπάνω συμπεριφορά (non volatile memory).

Υπάρχουν δύο τύποι κύριας μνήμης: Η μνήμη τυχαίας προσπέλασης [Random Access Memory, (RAM)], που είναι μέρος της πρωτεύουσας αποθήκευσης και δέχεται δεδομένα και προγράμματα κατά τη διάρκεια επεξεργασίας, και η μνήμη ανάγνωσης [Read Only Memory (ROM)] ή υλικολογισμικό (firmware), που αναφέρεται σε κυκλώματα μνήμης που περιέχουν σταθερές οδηγίες προγραμματισμένες εκ των προτέρων. Οι μνήμες ανάγνωσης ROM διακρίνονται στις ακόλουθες κατηγορίες:

Προγραμματισμένες μνήμες ανάγνωσης [Programmable Read Only Memory (PROM)],

Προγραμματισμένες μνήμες ανάγνωσης με δυνατότητα απόσβεσης [Erasable PROM (EPROM)], και

Προγραμματισμένες μνήμες ανάγνωσης με δυνατότητα ηλεκτρονικής απόσβεσης [Electronically EPROM (EEPROM)].

Η γρήγορη μνήμη (cache memory) ή «κρυφή μνήμη» είναι ένας τύπος μνήμης που μπορεί να αυξήσει σημαντικά την ταχύτητα ενός υπολογιστή, και βασίζεται σε τεχνικές αποθήκευσης και ανάκτησης δεδομένων, που χρησιμοποιούνται πολύ συχνά, με έναν εύκολο, προσπελάσιμο τρόπο. Στη θέση των ολοκληρωμένων κυκλωμάτων ή επιπρόσθετα με αυτά μπορεί να χρησιμοποιηθεί η μνήμη μαγνητικών φυσαλίδων (magnetic bubble memory).

Η Μονάδα Ελέγχου (Control Unit), όταν πάρει μία οδηγία που περιέχει έναν υπολογισμό ή σύγκριση, ελέγχει την κίνηση των δεδομένων στην ALU και μετακινεί το αποτέλεσμα σε μία προκαθορισμένη θέση αποθήκευσης, όταν συμπληρωθεί η διαδικασία. Συνοψίζοντας την υπολογιστική επεξεργασία σημειώνεται ότι η μονάδα ελέγχου είναι σχεδιασμένη για να συντονίζει την παράσταση, αποθήκευση και εσωτερική κίνηση οδηγιών και δεδομένων, καθώς επίσης την ερμηνεία και κατάλληλη εκτέλεση αυτών των οδηγιών και στη συνέχεια να διαβιβάζει τα αποτελέσματα. Το βασικό στοιχείο για την εκτέλεση διάφορων λειτουργιών σε έναν υπολογιστή είναι το κύκλωμα υπολογιστή (computer circuitry) ή υπολογιστικό κύκλωμα. Η ταχύτατη εξέλιξη της τεχνολογίας έχει επιτρέψει την κατασκευή πολύπλοκων υπολογιστικών κυκλωμάτων, που αποτελούνται από εκατομμύρια συνιστώσες (τρανζίστορς) μέσα σε μία «ψηφίδα» (chip) ολοκληρωμένου κυκλώματος (τέταρτη γενιά υπολογιστών). Τα υπολογιστικά συστήματα χρησιμοποιούν διάφορα βασικά ηλεκτρονικά κυκλώματα, όπως π.χ. κυκλώματα πυλών, ολοκληρωμένα κυκλώματα, συνδυαστικά κυκλώματα και ακολουθιακά κυκλώματα.

Τα κυκλώματα πυλών είναι ηλεκτρονικά ψηφιακά κυκλώματα που εκτελούν βασικές λογικές πράξεις της άλγεβρας Boole και είναι γνωστά ως «λογικές πύλες» (logical gates). Η ραγδαία τεχνολογική εξέλιξη έχει επιτρέψει την κατασκευή λογικών πυλών και πολύπλοκων ψηφιακών κυκλωμάτων σε ένα πολύ μικρό

τεμάχιο ημιαγωγού, στο οποίο με κατάλληλες τεχνικές σχηματίζονται διάφορα στοιχεία (δίοδοι, πυκνωτές, τρανζίστορς κτλ.), καθώς και συνδέσεις τους. Το σύνολο της κατασκευής σχηματίζει ένα ολοκληρωμένο κύκλωμα (integrated circuit) και συνήθως τοποθετείται σε μεταλλική, κεραμική ή πλαστική συσκευασία που αποτελεί την ψηφίδα (chip). Τα ολοκληρωμένα κυκλώματα, ανάλογα με τον τρόπο κατασκευής του βασικού δομικού κυκλώματος, διακρίνονται στις ακόλουθες οικογένειες:

TTL (Transistor Transistor Logic) με μεγάλη χρήση,

ECL (Emitter Coupled Logic) για κυκλώματα υψηλών ταχυτήτων,

MOS (Metal Oxide Semiconductor), και

I2L (Integrated Injection Logic) για κυκλώματα με μεγάλη πυκνότητα συσκευασίας, CMOS (Complementary Metal Oxide Semiconductor) με μικρή κατανάλωση ισχύος, GaAs (Gallium Arsenide) με πολύ υψηλές ταχύτητες λειτουργίας.

Είναι γνωστό ότι η κίνηση πληροφοριών μέσα στη CPU, καθώς ερμηνεύεται και εκτελείται κάθε εντολή, μπορεί να ρυθμισθεί ικανοποιητικά διατηρώντας ορισμένες πληροφορίες σε σταθερή βάση. Για το σκοπό αυτό ο υπολογιστής χρησιμοποιεί ειδικές μονάδες μνήμης που καλούνται καταχωρητές (registers). Οι καταχωρητές δεν θεωρούνται μέρος της κύριας μνήμης και υπάρχουν διάφοροι τύποι σχεδιασμένοι για την εκτέλεση ειδικών λειτουργιών. Κοινό χαρακτηριστικό των καταχωρητών είναι η ικανότητα λήψης πληροφοριών, η προσωρινή κράτηση και η μετάδοσή τους με

τρόπο που καθορίζει η μονάδα ελέγχου. Παρακάτω δίνεται συνοπτική περιγραφή διάφορων καταχωρητών:

- Ο καταχωρητής αποθήκευσης [Storage Data Register DR (16 bits)] περιέχει πληροφορίες που κατευθύνονται ή προέρχονται από τη μνήμη.
- Ο καταχωρητής οδηγιών [Instructions Register IR (16 bits)] ή καταχωρητής εντολών περιέχει οδηγίες ενώ αυτές εκτελούνται.

- Ο καταχωρητής διεύθυνσης [Address Register AR (12 bits)] περιέχει μία διεύθυνση θέσης αποθήκευσης μέχρις ότου αυτή χρειασθεί.
- Ο καταχωρητής συσσώρευσης [Accumulator Register AC (16bits)] συσσωρεύει αποτελέσματα.
- Ο καταχωρητής προγράμματος [Program Counter PC (12 bits)] ή μετρητής προγράμματος περιέχει τη διεύθυνση των οδηγιών.
- Ο προσωρινός καταχωρητής [Temporary Register TR (16 bits)] περιέχει προσωρινά δεδομένα.
- Ο καταχωρητής εισόδου [Input Register INPR (8 bits)] περιέχει χαρακτήρες εισόδου.
- Ο καταχωρητής εξόδου [Output Register OUTR (8 bits)] περιέχει χαρακτήρες εξόδου.

Σημειώνουμε ότι ο μετρητής προγράμματος περιέχει κάθε στιγμή τη διεύθυνση της εντολής που πρόκειται να εκτελεσθεί από τη CPU, ενώ ο καταχωρητής εντολής περιέχει τον κώδικα της εντολής που εκτελείται στη CPU.

Οι στοιχειώδεις λειτουργίες που εκτελούνται με τα δεδομένα που είναι αποθηκευμένα στους καταχωρητές καλούνται μικρολειτουργίες (micro operations). Οι μικρολειτουργίες ταξινομούνται στις ακόλουθες κατηγορίες:

(i) Μικρολειτουργίες μεταφοράς καταχωρητών, που μεταφέρουν δυαδικές πληροφορίες από έναν καταχωρητή σε άλλο.

(ii) Αριθμητικές μικρολειτουργίες, που εκτελούν αριθμητικές λειτουργίες σε αριθμητικά δεδομένα που είναι αποθηκευμένα σε καταχωρητές.

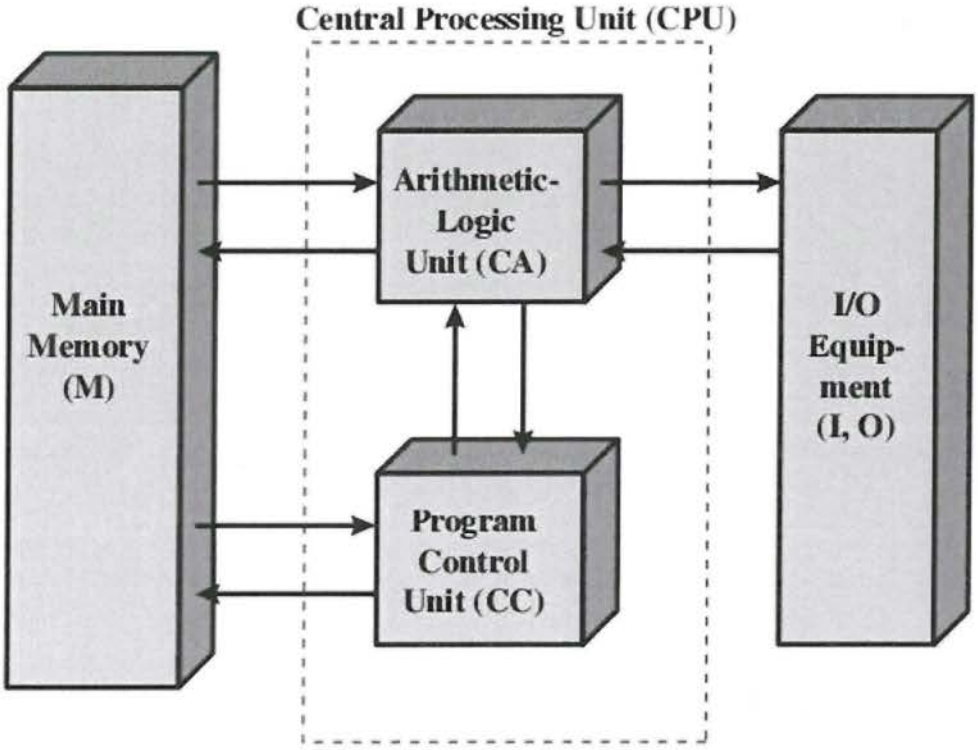
(iii) Λογικές μικρολειτουργίες, που εκτελούν λειτουργίες χειρισμών δυαδικών ψηφίων σε μη αριθμητικά δεδομένα που είναι αποθηκευμένα στους καταχωρητές.

(iv) Μικρολειτουργίες «μετατόπισης», που εκτελούν λειτουργίες μετατόπισης σε δεδομένα αποθηκευμένα στους καταχωρητές.

Ο όρος αρχιτεκτονική εδώ αναφέρεται γενικά στην τεχνολογία που χρησιμοποιείται για την επεξεργασία δεδομένων. Το μέγεθος μιας λέξης (word)

υπολογιστή, που δηλώνει τον αριθμό bits που επεξεργάζεται η CPU σε μία χρονική στιγμή, σχετίζεται αναλογικά με την ταχύτητα επεξεργασίας, δηλαδή μεγαλύτερη λέξη αντιστοιχεί σε ταχύτερο υπολογιστή. Η απόδοση της CPU ενός μικροϋπολογιστή μετριέται με την ταχύτητα ρολογιού (clock speed) σε MegaHertz (MHz), ενώ εναλλακτικό μέσο μέτρησης ταχύτητας αποτελούν τα «εκατομμύρια εντολών ανά δευτερόλεπτο» [Millions of Instructions Per Second (MIPS)], π.χ. ένας υπολογιστής που έχει ταχύτητα 600 MIPS μπορεί να επεξεργασθεί 600 εκατομμύρια εντολές ανά δευτερόλεπτο.

Ένα MHz αντιστοιχεί σε ένα εκατομμύριο κτυπήματα (ticks) ενός ρολογιού του συστήματος ανά δευτερόλεπτο. Οι κατασκευαστές μικροϋπολογιστών αναφέρονται συνήθως σε υπολογιστές με μεγαλύτερες ταχύτητες ρολογιού με τον όρο «turbo systems». Σημειώνεται ότι η ταχύτητα ρολογιού αναφέρεται στο χρόνο επεξεργασίας και όχι στη συνολική ταχύτητα του υπολογιστικού συστήματος.



Εικόνα 57 Βασική Αρχιτεκτονική Επεξεργαστή.

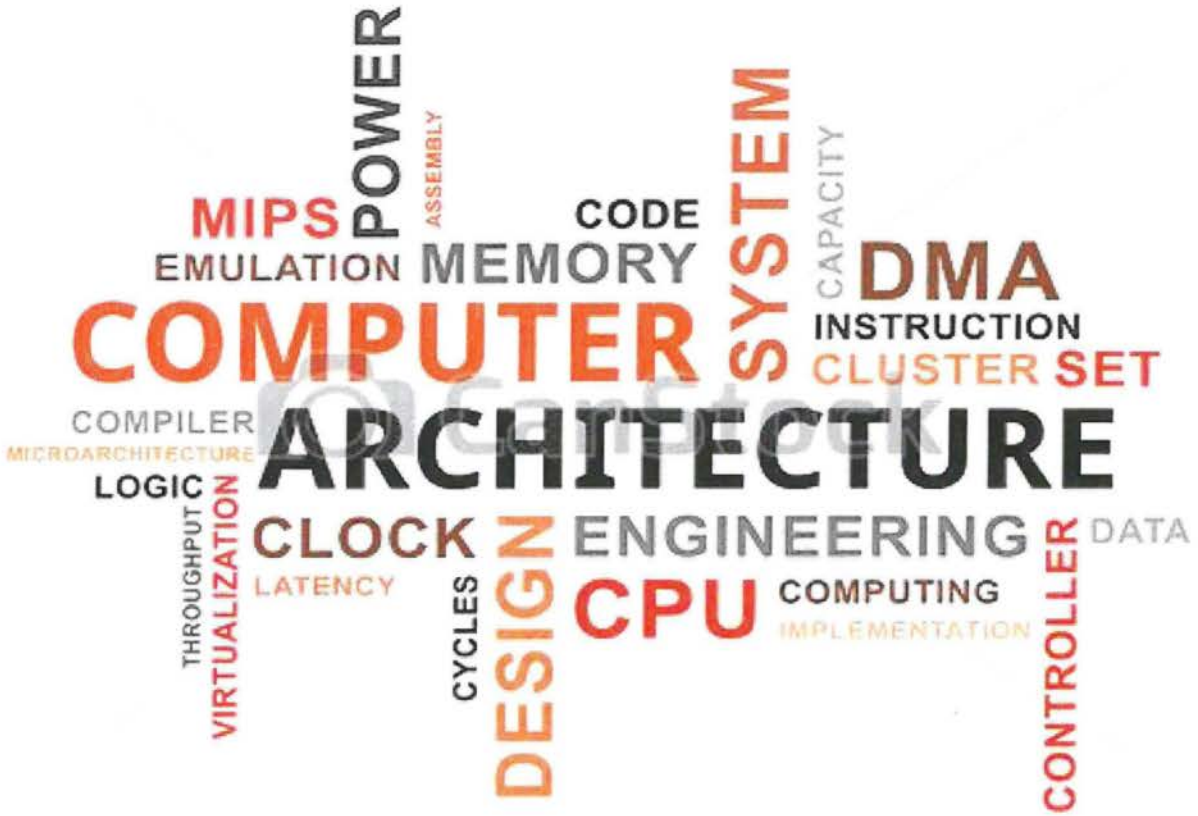
Η κύρια κάρτα κυκλωμάτων ενός υπολογιστή, που περιέχει τους μικροεπεξεργαστές, ενδοσυνδεδεμένα κυκλώματα, τον ωρολογιακό μηχανισμό

μπαταρίας κτλ., καλείται συνήθως κύρια κάρτα (motherboard). Ο όρος ανοικτή αρχιτεκτονική σε έναν μικροϋπολογιστή σημαίνει ότι ο χρήστης μπορεί να ανοίξει την υπολογιστική συσκευή και να προσθέσει επιλεκτικά συνιστώσες σε κάρτες κυκλωμάτων ή στην κύρια κάρτα, που διαθέτει μία σειρά ειδικών υποδοχών (slots) επέκτασης για την εισαγωγή επιπρόσθετων μονάδων.

Ο όρος υπολογιστικό σύστημα (computer system) χρησιμοποιείται γενικά για να χαρακτηρίσει ένα σύνολο υλικού λογισμικού που λειτουργεί με καθορισμένες διαδικασίες. Σημειώνουμε ότι η αρχιτεκτονική υπολογιστικών συστημάτων αναφέρεται γενικά στη μελέτη της δομής, συμπεριφοράς και στη σχεδίαση υπολογιστικών συστημάτων, τα οποία χαρακτηρίζονται από πολυπλοκότητα και ιεραρχική οργάνωση.

Η πολυπλοκότητα αναφέρεται στην ύπαρξη πολλών μερών του συστήματος, τα οποία αλληλεπιδρούν μεταξύ τους με σύνθετο τρόπο. Η ιεραρχική οργάνωση εμφανίζεται στα πολύπλοκα υπολογιστικά συστήματα, που αποτελούνται από διάφορα επίπεδα ιεραρχίας. Οι λειτουργίες κάθε επιπέδου στηρίζονται σε λειτουργίες χαμηλότερων επιπέδων. Η έννοια της αρχιτεκτονικής μπορεί να χρησιμοποιηθεί ανεξάρτητα για κάθε επίπεδο, π.χ. αρχιτεκτονική γλωσσών προγραμματισμού, αρχιτεκτονική λειτουργικών συστημάτων. Η αρχιτεκτονική υπολογιστικών συστημάτων ορίζεται ως μία έννοια που ενοποιεί συλλογικά βασικούς παράγοντες, όπως υλικό, λογισμικό, γλώσσες προγραμματισμού και αλγορίθμους για την εκτέλεση υπολογισμών μεγάλης κλίμακας. Εναλλακτικά, η αρχιτεκτονική υπολογιστών μπορεί να ορισθεί ως ένα σύνολο χαρακτηριστικών, τα οποία είναι ανεξάρτητα από συγκεκριμένο υπολογιστή και συγκεκριμένη υλοποίηση, π.χ. η αναφορά στην κύρια μνήμη ενός υπολογιστή είναι αρχιτεκτονικό χαρακτηριστικό.

Τα υπολογιστικά συστήματα μπορούν να ταξινομηθούν σε γενιές ανάλογα με την τεχνολογία, αρχιτεκτονική, είδος επεξεργασίας και γλώσσες προγραμματισμού που χρησιμοποιούν. Περισσότερες λεπτομέρειες για την αρχιτεκτονική υπολογιστών θα παρουσιασθούν στην αντίστοιχη θεματική ενότητα της Πληροφορικής.



Εικόνα 58 Computer Architecture.

Κεφάλαιο 3°: Βασικές έννοιες Θεωρίας Πληροφορίας

3.1.1 Εισαγωγή στην Θεωρία της πληροφορίας

Θεωρία Πληροφορίας είναι το πεδίο εκείνο που ασχολείται με την έννοια της «πληροφορίας», τα μέτρα και τις εφαρμογές της. Πιο συγκεκριμένα, στα θέματα που απασχολούν τη Θεωρία Πληροφορίας συγκαταλέγονται η ποσότητα συντακτικής πληροφορίας (ή εντροπία) και οι μονάδες μέτρησης αυτής, η ροή πληροφορίας σε κανάλια και τα θεμελιώδη όρια της ποσότητας πληροφορίας που μπορούν να μεταδοθούν, δηλαδή η χωρητικότητα καναλιών, που αποτελεί το μέγιστο δυνατό ρυθμό μετάδοσης. Ακόμα, θέματα που απασχολούν είναι η κατασκευή συστημάτων επεξεργασίας και επικοινωνίας πληροφορίας που μπορούν να προσεγγίσουν αυτά τα ανωτέρω όρια κ.ά.

Η συντακτική πληροφορία σχετίζεται με τα σύμβολα και τις σχέσεις μεταξύ αυτών, από τα οποία αποτελούνται τα μηνύματα. Η σημασιολογική πληροφορία σχετίζεται με τη σημασία και η πραγματική με τη χρήση και τη δυνατή επίπτωση των μηνυμάτων. Έτσι, ενώ ο συντακτικός τύπος της πληροφορίας αναφέρεται στη μορφή, ο σημασιολογικός και ο πραγματικός αναφέρονται στο περιεχόμενο. Ας εξετάσουμε, στη συνέχεια, τις ακόλουθες προτάσεις για να αποσαφηνίσουμε αυτές τις έννοιες.

1. Η Άννα πήγε με ψαρόβαρκα από το λιμάνι της Πάργας στο Χρυσογυάλι.

2. Η ψαρόβαρκα μετέφερε την Άννα από το λιμάνι της Πάργας στο Χρυσογυάλι.

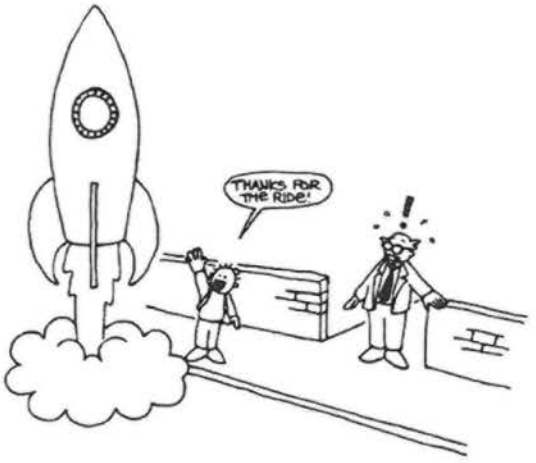
3. Στα ελληνικά πελάγη πνέουν άνεμοι ισχύος 5 - 9 μποφόρ.

4. Στο Ιόνιο πέλαγος πνέουν άνεμοι ισχύος 5 - 6 μποφόρ, στο ΒΑ Αιγαίο 6 - 7 μποφόρ, στο Ν. Αιγαίο 8 - 9 μποφόρ και στο Κρητικό πέλαγος 7 - 8 μποφόρ.

Οι δύο πρώτες προτάσεις διαφοροποιούνται ως προς τη σύνταξη και είναι ταυτόσημες ως προς τη σημασία, προσφέρουν δηλαδή την ίδια πληροφόρηση. Αντίθετα, οι δύο τελευταίες προτάσεις διαφέρουν όχι μόνο ως προς τη σύνταξη αλλά και ως προς το περιεχόμενο. Η τέταρτη πρόταση είναι πιο ακριβής από την

τρίτη, προσφέρει επομένως περισσότερη πληροφόρηση. Η πραγματική διάσταση της πληροφορίας εξαρτάται κυρίως από το δεδομένο γενικό πλαίσιο.

Δηλαδή, η σημασία της τρίτης και της τέταρτης πρότασης είναι σημαντική και ενδιαφέρουσα για όσους βρίσκονται στην Ελλάδα και όχι για κάποιους που βρίσκονται στην Αυστραλία. Ιδιαίτερα, η ακρίβεια της τέταρτης πρότασης μπορεί να καθορίσει επιλογές των ναυτιλλομένων στα ελληνικά πελάγη.



Εικόνα 59 Αστείο σκίτσο στην θεωρία πληροφορίας.

Όπως θα δούμε στη συνέχεια, η Θεωρία Πληροφορίας αναφέρεται στη συντακτική πληροφορία, δηλαδή η πληροφορία εξαρτάται από την πιθανότητα εμφάνισης των μηνυμάτων και όχι από τη σημασία τους.

3.1.2 Μέτρο ποσότητας πληροφορίας του Harley.

Καθοριστική συμβολή στην ανάπτυξη της Θεωρίας Πληροφορίας είχαν οι Shannon και Wiener. Ιδιαίτερα ο πρώτος θεωρείται ως ο πατέρας αυτής, θέτοντας τις βάσεις της με το επιστημονικό του άρθρο «A mathematical theory of communication», το 1948. Του άρθρου του Shannon προηγήθηκε η προσπάθεια του Hartley να ορίσει ένα «μέτρο ποσότητας πληροφορίας».

Σύμφωνα με την πρόταση του Hartley, η «ποσότητα πληροφορίας» διαμορφώνεται από τη διαδοχική επιλογή συμβόλων ή λέξεων από ένα δεδομένο σύνολο. Ας υποθέσουμε ότι σχηματίζουμε λέξεις ή μηνύματα αποτελούμενα από ν σύμβολα

από ένα αλφάβητο N συμβόλων. Τότε μπορούμε να επιλέξουμε N^v διαφορετικές λέξεις.

Ποσότητα πληροφορίας Ο Hartley όρισε την ποσότητα πληροφορίας (ή πληροφορικό περιεχόμενο) ως το δεκαδικό λογάριθμο του πλήθους των διαφορετικών λέξεων που μπορούν να σχηματιστούν, αποτελούμενες από ένα δεδομένο πλήθος συμβόλων. Στην περίπτωση μηνυμάτων μήκους κ συμβόλων από ένα αλφάβητο με N σύμβολα, η ποσότητα πληροφορίας είναι ίση με:

$$H(N^k) = \log(N^k) = k\,logN$$

Για μηνύματα μήκους 1 συμβόλου, από το ανωτέρω αλφάβητο, η ποσότητα πληροφορίας είναι :

$$H(N^1) = \log(N)$$

Οι ανωτέρω σχέσεις ανταποκρίνονται στη διαίσθησή μας ότι η ποσότητα πληροφορίας ενός μηνύματος αποτελούμενου από κ σύμβολα θα πρέπει να είναι κ φορές μεγαλύτερη από αυτή ενός μηνύματος που αποτελείται από 1 σύμβολο. Αυτός είναι, άλλωστε, ο λόγος που επελέγη η λογαριθμική συνάρτηση στον ορισμό της ποσότητας πληροφορίας, αφού πληροί τη σχέση :

$$f(x^y) = yf(x)$$

Με βάση του λογάριθμου το 10, η μονάδα της ποσότητας πληροφορίας είναι η decit (decimal unit) ή Hartley. Αν χρησιμοποιήσουμε φυσικό λογάριθμο, η μονάδα είναι το nat (natural unit). Εξετάζοντας ως παράδειγμα το σχηματισμό μηνυμάτων μήκους ενός συμβόλου από ένα αλφάβητο αποτελούμενο από 10 σύμβολα, η ποσότητα πληροφορίας κάθε μηνύματος είναι ίση με :

$$H(N^1) = \log_{10} 10 = 1\ decit.$$

Με βάση του λογάριθμου το 2, η μονάδα της ποσότητας πληροφορίας καλείται bit (binary unit). Αν τώρα εξετάσουμε ως παράδειγμα το σχηματισμό μηνυμάτων μήκους ενός συμβόλου από ένα αλφάβητο αποτελούμενο από δύο σύμβολα, τότε η ποσότητα πληροφορίας είναι :

$$H(N^1) = \log_2 N = \log_2 2 = 1\ bit.$$

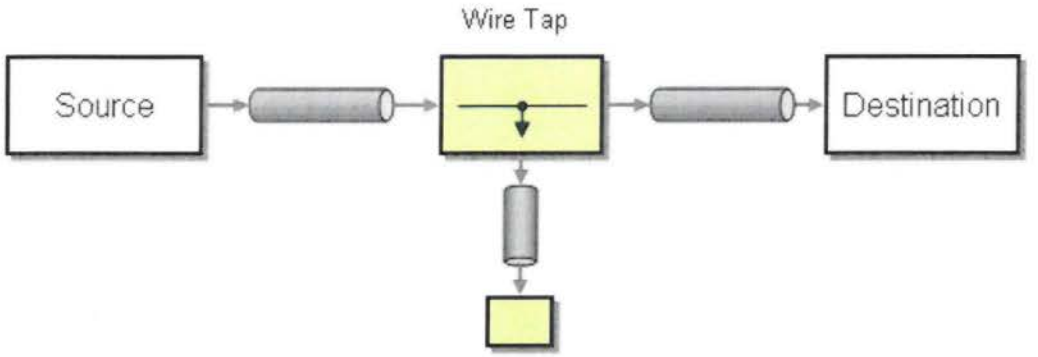
Ο Hartley επηρεάστηκε από το νόμο που, σχεδόν ταυτόχρονα, είχαν διατυπώσει ο Nyquist στις Ηνωμένες Πολιτείες της Αμερικής και ο Kupfmuller στη Γερμανία, το 1924. Σύμφωνα με αυτό το νόμο, η μετάδοση σημάτων τηλεγράφου σ' ένα δεδομένο ρυθμό απαιτεί ένα καθορισμένο εύρος συχνοτήτων. Ο Hartley στον ορισμό του δε διακρίνει διαφορετικές πιθανότητες για τα σύμβολα που απαρτίζουν το αλφάβητο, θεωρεί την επιλογή καθενός εξ αυτών κατά το σχηματισμό ενός μηνύματος ως ίσης πιθανότητας γεγονός.

Αντίθετα, ο Shannon εισήγαγε την έννοια της πιθανότητας στον ορισμό της ποσότητας πληροφορίας και έθεσε τις βάσεις της σύγχρονης Θεωρίας Πληροφορίας. Η επιλογή κάθε συμβόλου συνδέεται με κάποια, στη γενική περίπτωση, διαφορετική πιθανότητα. Έτσι, ο ορισμός του Hartley είναι μια ειδική περίπτωση του ορισμού του Shannon για την ποσότητα πληροφορίας.

3.1.3 Επικοινωνιακό Μοντέλο.

Σε κάθε επικοινωνιακή διεργασία λαμβάνει χώρα ροή πληροφορίας μεταξύ ενός αποστολέα και ενός αποδέκτη. Η πληροφορία αυτή μπορεί να έχει διάφορες μορφές, όπως ηλεκτρισμού, μουσικής, λέξεων ή εικόνων. Η μεταφορά της πληροφορίας επιτυγχάνεται, στη γενική περίπτωση, με τη βοήθεια ενός δικτύου μετάδοσης. Έτσι, τα βασικά μέρη ενός επικοινωνιακού μοντέλου είναι ο αποστολέας ή πηγή πληροφορίας, το κανάλι ή δίκτυο μετάδοσης και ο παραλήπτης ή προορισμός αυτής.

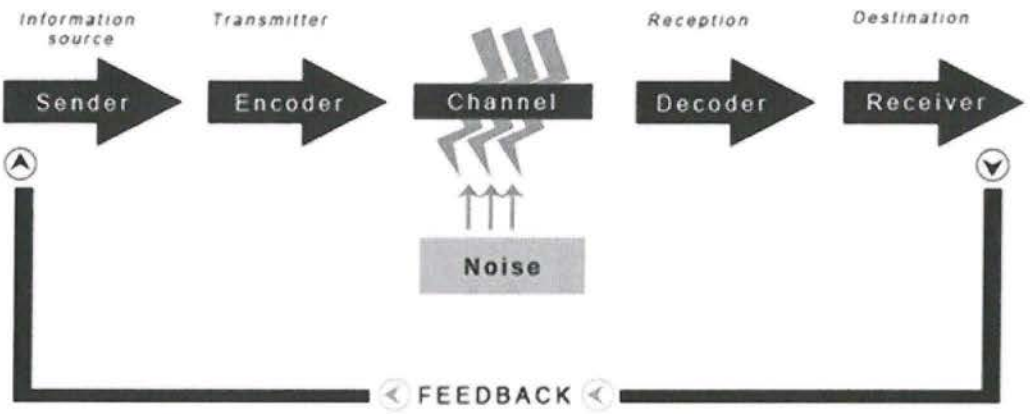
Η αποθήκευση της πληροφορίας παίζει σήμερα σημαντικό ρόλο. Αν και κατά κανόνα δεν είναι ζήτημα μετάδοσης, μπορεί ωστόσο να περιγραφεί ως μέρος του καναλιού ή δικτύου μετάδοσης. Η πληροφορία κατά τη μετάδοσή της μπορεί να αλλοιωθεί από την επενέργεια του θορύβου πάνω στο κανάλι.



Εικόνα 60 Απλό Επικοινωνιακό μοντέλο.

Η μεταφορά της πληροφορίας θα πρέπει να είναι, ως ένα βαθμό, χωρίς σφάλματα. Γι' αυτό πρέπει να είναι δυνατή η διόρθωση σφαλμάτων ή η μεταφορά να είναι τόσο καλή, ώστε να μην υπεισέρχονται παρά μόνο ασήμαντα σφάλματα που είναι ανεκτά. Μια τέλεια, δηλαδή χωρίς σφάλματα, μεταφορά δεν είναι δυνατή για σήματα ομιλίας, μουσικής ή video. Μπορούν μόνο να τεθούν απαιτήσεις ως προς το μέγεθος της απόκλισης του σήματος που λαμβάνει ο αποδέκτης από το σήμα που έχει αποστείλει ο μεταδότης.

Η απαιτούμενη ποιότητα μεταφοράς της πληροφορίας οδηγεί στην επιλογή κατάλληλου μέσου μεταφοράς ή καναλιού και επιβάλλει οριακές συνθήκες προσαρμογής του καναλιού στον αποστολέα και τον παραλήπτη. Μια από τις σημαντικές επιδιώξεις σχεδιαστών επικοινωνιακών συστημάτων είναι η ελαχιστοποίηση των απωλειών πληροφορίας στο κανάλι και η βέλτιστη επανάκτηση πληροφορίας που έχει προσβληθεί από θόρυβο. Για την επίτευξη της επιδίωξης αυτής χρησιμοποιούνται τεχνικές κωδικοποίησης στην πλευρά του αποστολέα και αντίστοιχες τεχνικές αποκωδικοποίησης στην πλευρά του αποδέκτη.



SHANNON-WEAVER'S MODEL OF COMMUNICATION

Εικόνα 61 Γενική Δομή επικοινωνιακού μοντέλου.

Στη συνέχεια θα επιχειρήσουμε πιο λεπτομερή περιγραφή των λειτουργιών του αποστολέα και του παραλήπτη. Καταρχήν θεωρούμε ως δεδομένα την πηγή πληροφορίας, τον προορισμό, το κανάλι με τα φυσικά χαρακτηριστικά του και την πηγή του θορύβου που επενεργεί στο επικοινωνιακό κανάλι. Σκοπός της πηγής πληροφορίας ή του αποστολέα είναι να καταστήσει την πληροφορία κατάλληλη για μετάδοση μέσω του δεδομένου καναλιού.

Από την άλλη πλευρά, ο αποδέκτης έχει ως σκοπό τη διόρθωση σφαλμάτων τα οποία προέκυψαν κατά τη μεταφορά της πληροφορίας στο επικοινωνιακό κανάλι εξαιτίας του θορύβου και, επίσης, τη μετατροπή της πληροφορίας σε τέτοια μορφή που να είναι κατάλληλη για τον παραλήπτη. Έτσι, μπορούμε να διακρίνουμε στην πλευρά του μεταδότη ή αποστολέα τέσσερις λειτουργίες:

1. Εφόσον δεν είναι σημαντικό για τον παραλήπτη το σύνολο της πληροφορίας που έχει δημιουργηθεί από την πηγή, θα πρέπει να αφαιρεθεί το μη χρήσιμο μέρος από την προς μεταφορά πληροφορία. Αυτή η λειτουργία καλείται απαλοιφή δεδομένων (data reduction). Η πληροφορία που απομένει για μεταφορά καλείται αποτελεσματική (ή ουσιαστική) πληροφορία.

2. Πολλές φορές, η ουσιαστική πληροφορία μπορεί να αποτελέσει αντικείμενο περαιτέρω επεξεργασίας για την αναπαράστασή της με όσο το δυνατόν πιο

συμπυκνωμένο τρόπο. Σ' αυτό στοχεύει μια δεύτερη λειτουργία, αυτή της συμπίεσης.

3. Η τρίτη λειτουργία, αυτή της κρυπτογράφησης, εφαρμόζεται όταν επιδιώκεται η προστασία του περιεχομένου από υποκλοπή ή σκόπιμη παραποίηση.

4. Η τελευταία λειτουργία, στην πλευρά του αποστολέα, στοχεύει στην προστασία από σφάλματα που δημιουργούνται κατά τη μεταφορά της πληροφορίας στο επικοινωνιακό κανάλι εξαιτίας της επενέργειας του θορύβου σ' αυτό. Για το λόγο αυτό προστίθεται ειδική πληροφορία και μεταφέρεται από το κανάλι μαζί με την ουσιαστική πληροφορία για την ανίχνευση και, πολλές φορές, διόρθωση σφαλμάτων. Αυτή η τέταρτη λειτουργία καλείται κωδικοποίηση καναλιού.

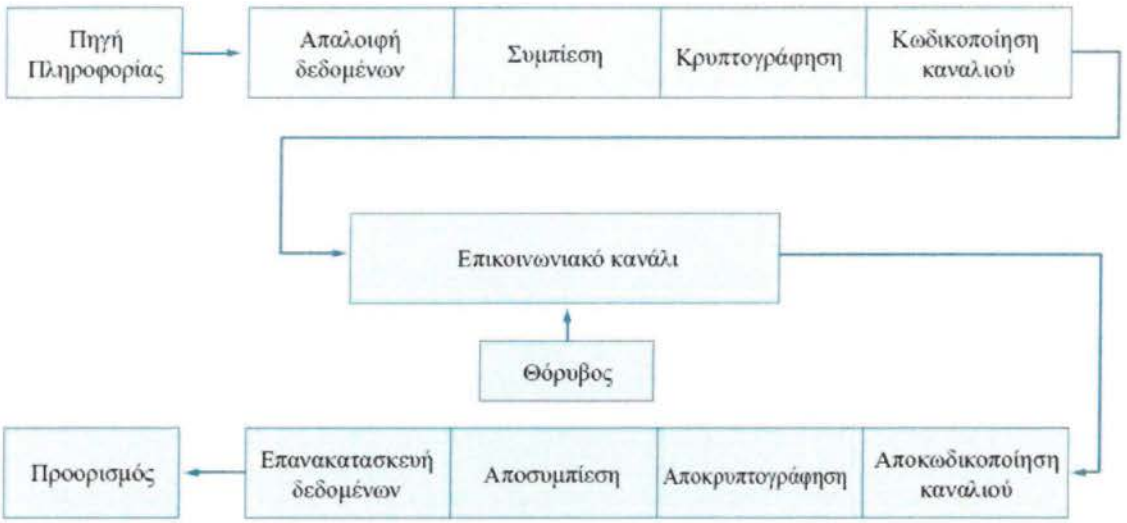
Το επικοινωνιακό κανάλι μεταφέρει και αποδίδει την πληροφορία, ενδεχομένως με σφάλματα στον αποδέκτη. Στην πλευρά του αποδέκτη, οι λειτουργίες εκτελούνται με αντίστροφη σειρά.

1. Η πρώτη λειτουργία, η αποκωδικοποίηση καναλιού, επιτρέπει τον έλεγχο ύπαρξης σφαλμάτων και, ενδεχομένως, διόρθωσης αυτών.

2. Η δεύτερη λειτουργία, η αποκρυπτογράφηση, επαναφέρει την πληροφορία σε τέτοιον τρόπο αναπαράστασης, που επιτρέπει την αποκάλυψη της σημασίας και, ενδεχομένως, επιτρέπει τον έλεγχο ύπαρξης παραποίησης (μη επιτρεπτής τροποποίησης).

3. Στην περίπτωση συμπίεσης της πληροφορίας στην πλευρά του μεταδότη, η λειτουργία της αποσυμπίεσης εκτελείται στον αποδέκτη.

4. Τέλος, η τέταρτη λειτουργία, αυτή της ανακατασκευής των δεδομένων (data reconstruction), φέρει την πληροφορία σε μορφή κατάλληλη για τον παραλήπτη.



Εικόνα 62 Λεπτομερές Επικοινωνιακό Μοντέλο.

3.2.1 Έννοιες Πιθανότητας.

Το αποτέλεσμα ενός τυχαίου πειράματος, όπως, παραδείγματος χάρη, της ρίψης ενός ζαριού ή κέρματος, δεν είναι εκ των προτέρων βέβαιο. Τα ατομικά αδιαίρετα αποτελέσματα, όπως στην περίπτωση του ζαριού το 1, 2, 3, 4, 5 και 6, λέγονται εκβάσεις ή στοιχειώδη ή απλώς ενδεχόμενα ή δειγματικά σημεία. Έτσι και η επιλογή από την πηγή πληροφορίας των συμβόλων ενός μηνύματος είναι ένα τυχαίο πείραμα και τα σύμβολα τα δειγματικά σημεία. Το σύνολο των στοιχειωδών ενδεχομένων ενός τυχαίου πειράματος λέγεται δειγματικός χώρος. Στην περίπτωση της ρίψης του ζαριού ο δειγματικός χώρος είναι το σύνολο $S = \{1, 2, 3, 4, 5, 6\}$ και στην περίπτωση επιλογής ενός συμβόλου κατά το σχηματισμό μηνύματος από πηγή πληροφορίας είναι το αλφάβητο που χρησιμοποιείται.

Ένα υποσύνολο του δειγματικού χώρου, δηλαδή μια συλλογή εκβάσεων ή απλών ενδεχομένων ή δειγματικών σημείων, στην περίπτωση του ζαριού το $S_1 = \{1, 4\}$, ή μια λέξη στην περίπτωση της πηγής, λέγεται γεγονός ή συμβάν. Υποθέτουμε ότι μπορούν να προσδιοριστούν όλα τα ενδεχόμενα που ενδιαφέρουν. Αν θεωρήσουμε

ότι ένα γεγονός Ε αποτελείται από ν δειγματικά σημεία και ότι όλα τα σημεία του δειγματικού χώρου είναι Ν και ισοπίθανα, τότε ορίζουμε ως πιθανότητα του Ε το λόγο ν/Ν.

Αυτός είναι ο κλασικός ορισμός της πιθανότητας. Σε οποιοδήποτε εισαγωγικό βιβλίο στη Θεωρία Πιθανοτήτων μπορείτε να βρείτε και τον εμπειρικό και τον αξιωματικό ορισμό. Τυχαία μεταβλητή είναι μια μονοσήμαντη συνάρτηση με πεδίο ορισμού ένα δειγματικό χώρο S και πεδίο τιμών ένα υποσύνολο των πραγματικών αριθμών. Μια τυχαία μεταβλητή λέγεται διακριτή αν το σύνολο των τιμών της είναι πεπερασμένο ή απείρως αριθμήσιμο. (Απείρως αριθμήσιμο σημαίνει πως το σύνολο των δυνατών τιμών μπορεί να τεθεί σε μία προς μία αντιστοιχία με το σύνολο των ακέραιων αριθμών.) Οι συνεχείς τυχαίες μεταβλητές αντιστοιχούν σε συνεχείς δειγματικούς χώρους. Έστω ένα τυχαίο πείραμα S με δειγματοχώρο $S = \{s_1, s_2, \ldots, s_n\}$ και η διακριτή τυχαία μεταβλητή X με πεδίο τιμών $X = \{x_1, x_2, \ldots, x_n\}$. Κάθε γεγονός s_i μπορεί να συμβεί με πιθανότητα $P(S = s_i) = P(X = x_i) = p_i$. Η $P(X = x_i) = p_i$ λέγεται συνάρτηση πιθανότητας μάζας και το σύνολο των πιθανοτήτων αυτών είναι $P = \{p_1, p_2, \ldots, p_n\}$. Η συνάρτηση πιθανότητας μάζας πληροί τις ακόλουθες θεμελιώδεις απαιτήσεις:

1. $p(x_i) \geq 0$, για κάθε i

2. $\sum_{x_i \leq x} p(x_i) = 1$.

Η συνάρτηση κατανομής αθροιστικής πιθανότητας μιας διακριτής τυχαίας μεταβλητής X δίνεται από τη σχέση :

$$F(X \leq x) = \sum_{x_i \leq x} p(x_i) \text{ , για κάθε } x \in (-\infty, \infty).$$

Αντίστοιχα, η συνάρτηση κατανομής μιας συνεχούς τυχαίας μεταβλητής δίνεται από τη σχέση :

$$F(X \leq x) = P[X \in (-\infty, x)] = \int_{-\infty}^{x} f(y)dy \text{ , για κάθε } x \in (-\infty, \infty).$$

Η μη αρνητική συνάρτηση f(x) καλείται συνάρτηση πυκνότητας πιθανότητας της συνεχούς τυχαίας μεταβλητής X. Για τη συνάρτηση πυκνότητας πιθανότητας ισχύουν τα εξής:

$$\int_B f(x)dx = P(X \in B) \text{ και } \int_{-\infty}^{+\infty} f(x)dx = 1 .$$

Η συνάρτηση κατανομής της συνεχούς τυχαίας μεταβλητής έχει τις ακόλουθες ιδιότητες:

1. $0 \leq F(X \leq x) \leq 1$, για κάθε x

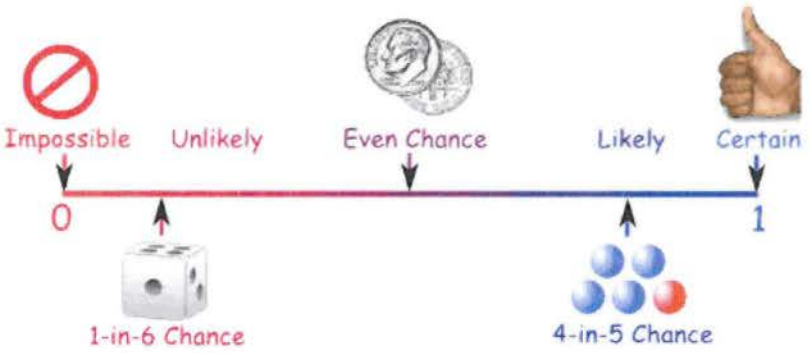
2. Η συνάρτηση κατανομής είναι μη φθίνουσα, δηλαδή αν $x_i \leq x_k$, τότε

$$F(X \leq x_i) \leq F(X \leq x_k)$$

3. $\lim_{x \to -\infty} F(X \leq x) = 1$ και $\lim_{x \to \infty} F(X \leq x) = 0$

Μερικές φορές συνδυάζουμε n τυχαία πειράματα σε ένα σύνθετο ή ενδιαφερόμαστε για n τυχαίες μεταβλητές ταυτόχρονα. Στη συνέχεια θα περιορίσουμε τη συζήτηση σε δύο πειράματα ή τυχαίες μεταβλητές. Σ' αυτή την περίπτωση έχουμε δύο δειγματικούς χώρους, έστω X και Y, όπου ο δειγματικός χώρος Y αναφέρεται στο αντίστοιχο πείραμα ή στην αντίστοιχη διακριτή τυχαία μεταβλητή, $Y = \{y_1, y_2, ..., y_m\}$.Η κατανομή πιθανότητας της Y είναι $P(Y) = [p(y_1), p(y_2), ..., p(y_m)]$, δηλαδή $p(y_i) = P(Y=y_i)$. Ας εξετάσουμε τώρα το πείραμα (X, Y) με δειγματικό χώρο το σύνολο των συνδυασμών (x, y). Ορίζουμε ως συνάρτηση συνδυασμένης πιθανότητας μάζας την $p_{ij} = P(X=x_i , Y=y_i)$, που δίνει την πιθανότητα να ισχύει: $X = x_i$ και $Y = y_j$. Από τη συνάρτηση συνδυασμένης πιθανότητας μάζας p_{ij} μπορούν να υπολογιστούν οι συναρτήσεις ακραίας πιθανότητας $p(x_i)$ μάζας και $p(y_i)$:

$$p(x_i) = \sum_{j=1}^{m} p_{ij} \text{ και } p(y_j) = \sum_{i=1}^{n} p_{ij}$$



Εικόνα 63 Σκίτσο εξήγησης πιθανότητας.

3.2.2 Το Μέτρο πληροφορίας του Shannon.

Το μέτρο ποσότητας πληροφορίας του Hartley, δε λαμβάνει υπόψη διαφορετικές πιθανότητες για την επιλογή των συμβόλων που απαρτίζουν ένα μήνυμα. Η εισαγωγή, από τον Shannon, της έννοιας της πιθανότητας στον ορισμό του μέτρου ποσότητας πληροφορίας, που πραγματεύεται αυτή η ενότητα, έθεσε τις βάσεις για την ανάπτυξη της σύγχρονης Θεωρίας Πληροφορίας.

Ο Shannon γενίκευσε, λοιπόν, τον ορισμό της ποσότητας πληροφορίας του Hartley, επιτρέποντας διαφορετικές πιθανότητες εμφάνισης των συμβόλων σε μηνύματα και κατ΄επέκταση και των διαφόρων μηνυμάτων.

Η συσχέτιση της έννοιας της πιθανότητας με τον ορισμό του μέτρου ποσότητας πληροφορίας είναι εύλογη. Αν θεωρήσουμε ένα τυχαίο πείραμα με δειγματοχώρο του οποίου τα γεγονότα είναι ισοπίθανα, τότε υπάρχει μεγάλη αβεβαιότητα για το αποτέλεσμα. Αντίθετα, αν ο δειγματοχώρος έχει ένα στοιχείο με πολύ μεγάλη πιθανότητα, τότε το να συμβεί αυτό το γεγονός προσφέρει πολύ λιγότερη πληροφορία απ' ότι το να συμβεί ένα από τ' άλλα γεγονότα.

Εικόνα 64 Claude Elwood Shannon (1916 - 2001).

Μέση ποσότητα πληροφορίας ή μέση πληροφορία ή μέσο πληροφορικό περιεχόμενο Αν X είναι μια διακριτή τυχαία μεταβλητή με δειγματοχώρο $X = \{x_1, x_2, \ldots, x_n\}$ και συνάρτηση πιθανότητας μάζας $p(x_i)$, τότε η μέση ποσότητα πληροφορίας (ή μέση πληροφορία ή μέσο πληροφορικό περιεχόμενο) της X , H(X), δίνεται από τη σχέση :

$$H(x) = -\sum_{i=1}^{n} p(x_i)\log_b p(x_i).$$

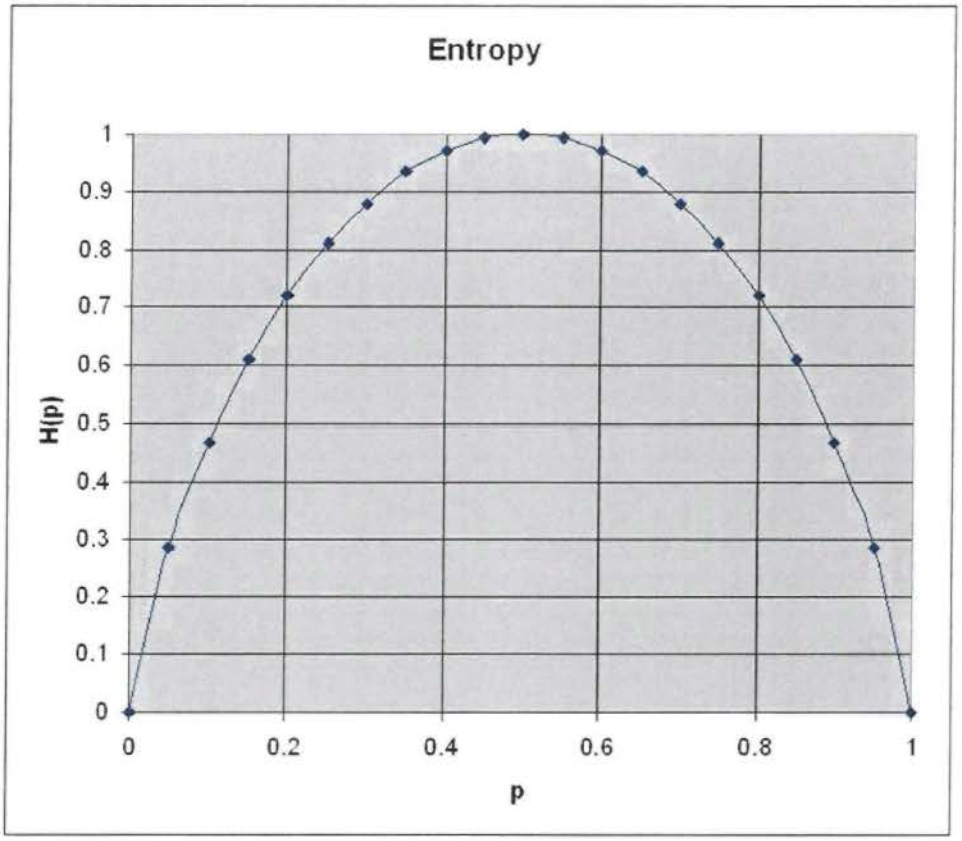
Η μέση πληροφορία ονομάζεται και εντροπία.

Στην περίπτωση μιας διακριτής τυχαίας μεταβλητής X με δύο ενδεχόμενα, π.χ. εκπομπή ενός από δύο δυνατά μηνύματα και πιθανότητες αυτών p και (1–p), αντίστοιχα, η εντροπία είναι :

$$H(X) = -p\log_b p - (1-p)\log_b(1-p).$$

Όπως μπορούμε να συνάγουμε από τον ορισμό της εντροπίας, η ποσότητα πληροφορίας (ή το πληροφορικό περιεχόμενο) ενός γεγονότος xi της τυχαίας μεταβλητής X είναι ίσο με τον αρνητικό λογάριθμο της πιθανότητας εμφάνισής

του $p(x_i)$, δηλαδή ίσο με $(- \log p(x_i))$. Επομένως, η ποσότητα πληροφορίας ενός γεγονότος είναι αντιστρόφως ανάλογη της πιθανότητας εμφάνισής του.



Εικόνα 65 Shannon's Entropy.

Παρατηρούμε στη γραφική παράσταση του παραπάνω σχήματος ότι η μέση πληροφορία παίρνει τη μέγιστη τιμή, που ισούται με ένα, όταν τα δύο γεγονότα μπορούν να συμβούν με την ίδια πιθανότητα, δηλαδή $p=1/2$. Από την άλλη πλευρά, αν $p = 1$ ή $p = 0$, τότε η εντροπία είναι 0, αφού το τελικό αποτέλεσμα (η έκβαση του πειράματος) είναι βέβαιο.

Οι ιδιότητες της μέσης (ποσότητας) πληροφορίας, που έχουν τεθεί και ως απαιτήσεις κατά τον ορισμό της, δηλαδή κατά την αναζήτηση από τον Shannon και άλλους ερευνητές της κατάλληλης συνάρτησης, διακρίνονται στις ακόλουθες:

1. Η μέση πληροφορία $H(X)$ είναι συνεχής στο p.

2. Η μέση πληροφορία H(X) είναι συμμετρική, δηλαδή η διάταξη των πιθανοτήτων δεν την επηρεάζει. Έτσι, διαφορετικές τυχαίες μεταβλητές με κατανομές πιθανοτήτων που προέρχονται από μεταθέσεις της ίδιας κατανομής πιθανοτήτων έχουν ίση εντροπία. Σε ορισμένες περιπτώσεις, ακόμα και διαφορετικές κατανομές πιθανοτήτων οδηγούν στην ίδια μέση ποσότητα πληροφορίας.

3. Η εντροπία H(X) παίρνει τη μέγιστη τιμή όταν όλα τα ενδεχόμενα είναι ισοπίθανα. Τότε, η αβεβαιότητα είναι η μέγιστη δυνατή και, κατά συνέπεια, η επιλογή ενός μηνύματος προσφέρει τη μέγιστη δυνατή μέση πληροφορία.

4. Η εντροπία είναι προσθετική (additive). Η ιδιότητα αυτή αναφέρεται στην περίπτωση κατά την οποία δύο ανεξάρτητες τυχαίες μεταβλητές X και Y συνδυάζονται. Τότε, για τη συνδυασμένη ποσότητα πληροφορίας ισχύει :

$$H(X,Y) = H(X) + H(Y).$$

Η σχέση H(X,Y) = H(X) + H(Y) μπορεί να δειχθεί αν χρησιμοποιήσουμε τον ορισμό της μέσης πληροφορίας. Σύμφωνα με τον ορισμό ισχύει :

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p_{ij}\log p_{ij} .$$

Αφού οι δύο τυχαίες μεταβλητές είναι ανεξάρτητες, ισχύει και έτσι έχουμε :

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p_{ij}\log p_{ij}$$

$$= -\sum_{i=1}^{n} p_i \sum_{j=1}^{m} p_j(\log p_i + \log p_j)$$

$$= -\sum_{i=1}^{n} p_i \sum_{j=1}^{m} p_j(\log p_i) - \sum_{i=1}^{n} p_i \sum_{j=1}^{m} p_j(\log p_j)$$

$$= -\sum_{i=1}^{n} p_i \log p_i \sum_{j=1}^{m} p_j - \sum_{i=1}^{n} p_i \sum_{j=1}^{m} p_j \log p_j$$

$$= -\sum_{i=1}^{n} p_i \log p_i - \sum_{j=1}^{m} p_j \log p_j$$

3.2.3 Η Πληροφορία.

Πολλές φορές μάς ενδιαφέρει να εξετάσουμε την ποσότητα πληροφορίας ενός συνδυασμού δύο τυχαίων μεταβλητών, δηλαδή ενός πειράματος που αποτελείται από δύο υπό-πειράματα. Ένα τυχαίο πείραμα (X, Y) έχει ως δυνατά αποτελέσματα όλους του συνδυασμούς των αποτελεσμάτων των $X=\{x_1,x_2,\ldots,x_n\}$ και $Y=\{y_1,y_2,\ldots,y_m\}$, επομένως το δειγματοχώρο:

$$(X,Y) = \{(x_1,y_1),(x_1,y_2),\ldots,(x_1,y_m),\ldots,(x_n,y_1),(x_n,y_2),\ldots,(x_n,y_m)\}$$

Η κατανομή πιθανοτήτων δίνεται από :

$$P = \{p(x_1,y_1),\ldots,p(x_1,y_m),\ldots,p(x_n,y_1),\ldots,p(x_n,y_n)\}.$$

Συνδυασμένη ποσότητα πληροφορίας (ή συνδυασμένη πληροφορία) Αν (X, Y) είναι ένα τυχαίο πείραμα με δισδιάστατο δειγματοχώρο και κατανομή πιθανοτήτων όπως ανωτέρω, τότε η συνδυασμένη πληροφορία H(X, Y) ορίζεται ως η μέση τιμή :

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i,y_j)\log p(x_i,y_j).$$

Αν είναι γνωστές όλες οι συνδυασμένες πιθανότητες $p(x_i, y_j)$, τότε μπορούν να υπολογιστούν οι ακραίες πιθανότητες $p(x_i)$ και $p(y_j)$, και επομένως οι ακραίες ποσότητες πληροφορίας H(X) και H(Y).

Ο ορισμός της μέσης ποσότητας πληροφορίας μπορεί να επεκταθεί και για περισσότερες από δύο διαστάσεις. Σε κάθε περίπτωση λαμβάνουμε υπόψη όλους τους δυνατούς συνδυασμούς αποτελεσμάτων και, εφόσον γνωρίζουμε τις πιθανότητες αυτών, μπορούμε να υπολογίσουμε τη συνδυασμένη ποσότητα πληροφορίας. Για τρεις τυχαίες μεταβλητές (X, Y, Z) με συνδυασμένες

πιθανότητες $p(x_i, y_j, z_k)$ η συνδυασμένη ποσότητα πληροφορίας δίνεται από τη σχέση

$$H(X,Y,Z) = -\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{l} p(x_i,y_j,z_k)\log p(x_i,y_j,z_k) .$$

Εναλλακτικά, μπορούμε να θεωρήσουμε ότι τα ενδεχόμενα, v, του τρισδιάστατου πειράματος είναι όλοι οι δυνατοί συνδυασμοί των τριών τυχαίων μεταβλητών και επομένως το πλήθος αυτών είναι ίσο με lmn. Οι αντίστοιχες πιθανότητες είναι $p(v_1), p(v_2), \ldots, p(v_{lmn})$ και η συνδυασμένη πληροφορία δίνεται από τη σχέση :

$$H(X,Y,Z) = -\sum_{i=1}^{lmn} p(v_i)\log p(v_i)$$

Το τελευταίο άθροισμα είναι ίσο με το άθροισμα που προκύπτει από τον προηγούμενο τύπο, αφού κάθε $p(v_h)$ ισούται με κάποια $p(x_i, y_j, z_k)$.

Επίσης, μας ενδιαφέρει, αρκετές φορές, να υπολογίσουμε την ποσότητα πληροφορίας μιας τυχαίας μεταβλητής, X, όταν δίνεται το αποτέλεσμα μιας άλλης τυχαίας μεταβλητής, Y. Αυτή καλείται υπό συνθήκη ποσότητα πληροφορίας της X ως προς την Y. Η υπό συνθήκη ποσότητα πληροφορίας του αποτελέσματος xi αν είναι γνωστό ότι έχει λάβει χώρα το αποτέλεσμα y_j δίνεται από :

$$H\left(\frac{x_i}{y_j}\right) = -\log p(x_i,y_i) .$$

Η μέση τιμή της υπό συνθήκη ποσότητας πληροφορίας της τυχαίας μεταβλητής X, δεδομένου του αποτελέσματος y_j, δίνεται από :

$$H\left(\frac{X}{y_j}\right) = -\sum_{i=1}^{n} \mathbf{p}\left(\frac{\mathbf{x_i}}{\mathbf{y_j}}\right)\log p\left(\frac{x_i}{y_j}\right).$$

Λαμβάνοντας υπόψη όλα τα δυνατά αποτελέσματα της Y, μπορούμε να υπολογίσουμε τη μέση τιμή της υπό συνθήκη ποσότητας πληροφορίας της X, με δεδομένο το αποτέλεσμα της Y, ως ακολούθως:

$$H\left(\frac{X}{Y}\right) = \sum_{j=1}^{m} p(y_j) H\left(\frac{X}{y_j}\right) = -\sum_{j=1}^{m} p(y_j) \sum_{i=1}^{n} p\left(\frac{x_i}{y_j}\right) \log p\left(\frac{x_i}{y_j}\right)$$

$$= -\sum_{i=1}^{n}\sum_{j=1}^{m} p(y_j) p\left(\frac{x_i}{y_j}\right) \log p\left(\frac{x_i}{y_j}\right)$$

Λαμβάνοντας ακόμα υπόψη τη σχέση p(a/b) = p(a,b)/p(b) , η οποία αναφέρεται στη συνδυασμένη πιθανότητα δύο τυχαίων μεταβλητών και τις υπό συνθήκη και τις ακραίες πιθανότητες αυτών, μπορούμε να οδηγηθούμε στον ακόλουθο ορισμό :

Η υπό συνθήκη ποσότητα πληροφορίας (ή υπό συνθήκη πληροφορία) Η (μέση) υπό συνθήκη ποσότητα πληροφορίας του τυχαίου πειράματος X, με δεδομένο το αποτέλεσμα του πειράματος Y, δίνεται από :

$$H\left(\frac{X}{Y}\right) = -\sum_{i=1}^{n}\sum_{j=1}^{m} p(x_i, y_j) \log p\left(\frac{x_i}{y_j}\right).$$

Αντίστοιχα, η υπό συνθήκη ποσότητα πληροφορίας του τυχαίου πειράματος Y, με δεδομένο το αποτέλεσμα του πειράματος X, δίνεται από :

$$H\left(\frac{Y}{X}\right) = -\sum_{j=1}^{m}\sum_{i=1}^{n} p(x_i, y_j) \log p\left(\frac{y_j}{x_i}\right).$$

Το τελευταίο ζήτημα αυτής της ενότητας αφορά στον ορισμό ενός μέτρου αμοιβαίας πληροφορίας δύο τυχαίων μεταβλητών X, Y. Η αμοιβαία πληροφορία είναι ένα μέτρο της ποσότητας πληροφορίας που μια τυχαία μεταβλητή περιέχει για μια άλλη τυχαία μεταβλητή ή ένα μέτρο της εξάρτησης μεταξύ δύο τυχαίων μεταβλητών.

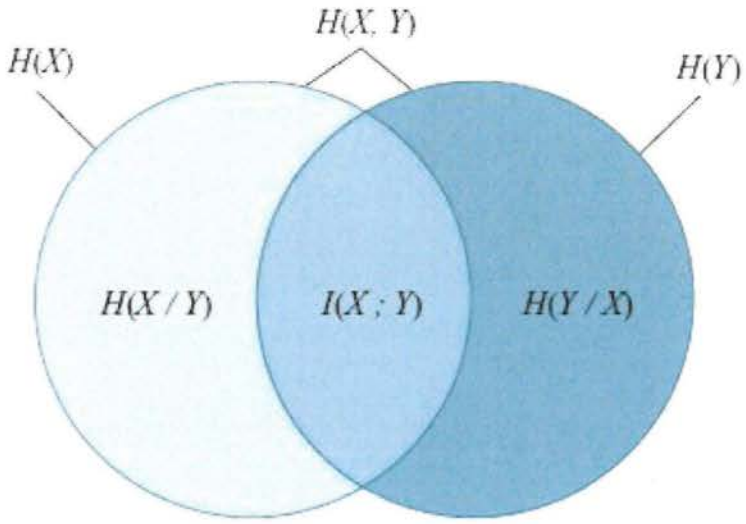
Η αμοιβαία ποσότητα πληροφορίας (ή αμοιβαία πληροφορία) Η αμοιβαία πληροφορία δύο τυχαίων μεταβλητών X και Y ορίζεται από τη σχέση :

$$I(X;Y) = H(Y) - H\left(\frac{Y}{X}\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} \frac{p(x_i, y_i) \log p(x_i, y_j)}{p(x_i) p(y_j)}.$$

Από τον ορισμό της αμοιβαίας πληροφορίας έχουμε :

$I(X;Y) = H(X) + H(Y) - H(X,Y) = H(X) - H(X/Y) = H(Y) - H(X/Y)$.

Παρατηρούμε πως η αμοιβαία ποσότητα πληροφορίας δύο ανεξάρτητων τυχαίων μεταβλητών είναι $I(X;Y) = 0$. Από την άλλη πλευρά, αν η X είναι πλήρως εξαρτημένη από την Y, δηλαδή $H(X/Y) = 0$,τότε $I(X;Y) = H(X) = H(Y)$.



Εικόνα 66 Ιδιότητες πιθανοτήτων.

3.3.1 Θεωρία Κωδικοποίησης.

Η Θεωρία Κωδικοποίησης είναι η μελέτη μεθόδων για την αποτελεσματική και ορθή μεταφορά της πληροφορίας από την πηγή στον προορισμό. Η ανάπτυξη της θεωρίας οφείλεται στις σχετικές απαιτήσεις εφαρμογών, όπως της μεταφοράς οικονομικών πληροφοριών μέσω τηλεφωνικών γραμμών, μεταφοράς δεδομένων από έναν ηλεκτρονικό υπολογιστή σε άλλο ή από τη μνήμη στην κεντρική μονάδα επεξεργασίας και μεταφοράς δεδομένων από δορυφόρους ή διαστημικά σκάφη στη Γη.

Το φυσικό μέσο, δια του οποίου μεταδίδεται η πληροφορία, ονομάζεται κανάλι επικοινωνίας. Παραδείγματα καναλιών είναι οι τηλεφωνικές γραμμές και η ατμόσφαιρα. Δυστυχώς, στα κανάλια επικοινωνίας επενεργεί θόρυβος, ο οποίος

προκαλεί αλλοίωση της μεταδιδόμενης πληροφορίας. Η Θεωρία Κωδικοποίησης ασχολείται με το πρόβλημα της ανίχνευσης και της διόρθωσης σφαλμάτων μετάδοσης, τα οποία προκαλούνται από το θόρυβο στα επικοινωνιακά κανάλια.

Οι κωδικές λέξεις είναι ακολουθίες δυαδικών ψηφίων. Για παράδειγμα, ο κώδικας που απαρτίζεται από όλες τις λέξεις μήκους δύο ψηφίων είναι C = {00, 10, 01, 11}. Ένας κώδικας ονομάζεται ισομήκης κώδικας (ή κώδικας μπλοκ) αν όλες οι κωδικές λέξεις έχουν το ίδιο μήκος. Στο κεφάλαιο αυτό θα μας απασχολήσουν μόνο κώδικες μπλοκ. Το πλήθος των κωδικών λέξεων ενός κώδικα C συμβολίζεται με |C|.

Σχετικά με το κανάλι κάνουμε δύο παραδοχές, καθοριστικές για την ανάπτυξη της θεωρίας κωδικοποίησης. Σύμφωνα με την πρώτη παραδοχή, μια κωδική λέξη μήκους n δυαδικών ψηφίων, που εισέρχεται στο κανάλι, λαμβάνεται στην έξοδό του ως λέξη μήκους και πάλι n δυαδικών ψηφίων, αν και η ακολουθία εισόδου του καναλιού μπορεί να διαφέρει από αυτή της εξόδου του καναλιού. Επίσης, χωρίς δυσκολία διαπιστώνεται, από το δέκτη, η αρχή της πρώτης λέξης μιας ακολουθίας κωδικών λέξεων που μεταδίδεται μέσω του καναλιού. Για παράδειγμα, αν στο κανάλι μεταδίδεται η δυαδική ακολουθία 010011, τότε στην έξοδό του λαμβάνεται η ακολουθία 010011 ή κάποια άλλη του ιδίου μήκους, όχι όμως η ακολουθία 10011 ή κάποια άλλη μικρότερου μήκους, επειδή χάθηκε το 1ο ψηφίο (το «0») της 1ης λέξης της ακολουθίας. Επομένως, η πρώτη παραδοχή αναφέρεται στη δυνατότητα του δέκτη να λάβει όλες τις λέξεις που μεταδόθηκαν, με ή χωρίς σφάλματα.

Εικόνα 67 Κύκλος Ζωής Πληροφορίας.

Η δεύτερη παραδοχή αναφέρεται στο ότι τα σφάλματα, δηλαδή ο θόρυβος, εμφανίζονται διασκορπισμένα κατά τυχαίο τρόπο και όχι σε συστάδες (ή καταιγισμούς, bursts). Με άλλα λόγια, η πιθανότητα να αλλοιωθεί ένα bit κατά τη μετάδοση εξαιτίας του θορύβου είναι η ίδια με αυτή οποιουδήποτε άλλου bit και δεν επηρεάζεται από σφάλματα σε γειτονικά δυαδικά ψηφία. Αυτή η παραδοχή δεν είναι ιδιαίτερα ρεαλιστική, αν λάβουμε υπόψη φυσικά φαινόμενα όπως αστραπές ή ακόμα και «γρατσουνιές» δίσκων, που οδηγούν σε καταιγισμούς σφαλμάτων.

Η αξιοπιστία του καναλιού είναι ο πραγματικός αριθμός p, $0 \leq p \leq 1$, όπου p είναι η πιθανότητα της ορθής μεταφοράς ενός δυαδικού ψηφίου μέσω του καναλιού. Ένα κανάλι χαρακτηρίζεται πιο αξιόπιστο από ένα άλλο αν η πιθανότητα p, δηλαδή η αξιοπιστία του, είναι πιο υψηλή. Ωστόσο, αν $p = 1$ (ή $p = 0$) τότε δεν υπάρχει περίπτωση σφάλματος (ή πάντοτε υπεισέρχεται σφάλμα) και επομένως το κανάλι αυτό δε θα μας απασχολήσει. Επειδή κάθε κανάλι αξιοπιστίας p, $0 < p \leq 1/2$, μπορεί να μετατραπεί σε ένα κανάλι με $1/2 \leq p < 1$, στο κεφάλαιο αυτό θα

ασχοληθούμε με δυαδικά συμμετρικά κανάλια με $1/2 < p < 1$. (Η περίπτωση $p = 1/2$ δεν επιτρέπει την εξαγωγή οποιουδήποτε αξιοποιήσιμου αποτελέσματος.)

Ο ρυθμός πληροφορίας ενός κώδικα είναι το ποσοστό της κωδικής λέξης που μεταφέρει το μήνυμα. Ο ρυθμός πληροφορίας ενός δυαδικού κώδικα C μήκους n είναι ίσος με $(1/n)\log_2|C|$. Αφού $1 \leq |C| \leq 2^n$, ο ρυθμός πληροφορίας παίρνει τιμές μεταξύ 0 και 1, την τιμή 1 αν $|C| = 2^n$ δηλαδή κάθε λέξη n δυαδικών ψηφίων είναι κωδική λέξη και την τιμή 0 αν $|C| = 1$.

Ας προσπαθήσουμε τώρα να αποκτήσουμε μια πρώτη, διαισθητική, εικόνα της ανίχνευσης και της διόρθωσης σφαλμάτων. Ας υποθέσουμε πρώτα ότι χρησιμοποιούμε για τη μετάδοση τον κώδικα $C1 = \{00, 10, 01, 11\}$. Αν τώρα κατά τη μετάδοση της ακολουθίας 0010, ο παραλήπτης λαμβάνει στην έξοδο του καναλιού την ακολουθία 0111, δεν μπορεί να ξέρει αν έχει υπεισέλθει κάποιο σφάλμα, αφού «01» και «11» είναι κωδικές λέξεις που θα μπορούσαν να είχαν σταλεί από τον αποστολέα. Δεν μπορεί, επομένως, να επιτευχθεί η ανίχνευση, πόσο μάλλον η διόρθωση σφαλμάτων. Αν σε κάθε κωδική λέξη του κώδικα C_1 προσθέσουμε ακόμα ένα ψηφίο ελέγχου ισοτιμίας, δηλαδή το ψηφίο εκείνο για το οποίο προκύπτει άρτιο πλήθος του «1» στην κωδική λέξη, λαμβάνουμε τον κώδικα $C_2 = \{000, 101, 011, 110\}$.

Η χρήση του κώδικα C_2 επιτρέπει, σε ορισμένες περιπτώσεις, την ανίχνευση σφαλμάτων. Για παράδειγμα, αν αποστέλλεται η κωδική λέξη «000» και ο παραλήπτης λαμβάνει τη λέξη «001», η οποία δεν είναι κωδική λέξη, τότε ανιχνεύει το σφάλμα. Η διόρθωση όμως του σφάλματος δεν είναι εύκολη, αφού η λέξη «001» μπορεί να προκύψει με αλλαγή ενός ψηφίου από τις κωδικές λέξεις «000», «011» και «101».

Αλλά και η ανίχνευση σφαλμάτων δεν είναι πάντοτε δυνατή με τη χρήση του κώδικα C_2, για παράδειγμα, αν αποστέλλεται και πάλι η κωδική λέξη «000» και λαμβάνεται στην έξοδο η κωδική λέξη «011» ή οποιαδήποτε άλλη κωδική λέξη. Η ανίχνευση του σφάλματος (ή των σφαλμάτων) είναι μόνο δυνατή αν στην έξοδο του καναλιού λαμβάνεται κάποια λέξη, η οποία όμως δεν είναι και κωδική λέξη.

Αν τώρα κάνουμε χρήση του κώδικα $C_3 = \{000000, 101010, 010101, 111111\}$, ο οποίος προκύπτει από τον κώδικα C_1 , με τριπλή επανάληψη κάθε κωδικής λέξης, είναι δυνατή και η ανίχνευση και η διόρθωση σφαλμάτων. Για παράδειγμα, αν

αποστέλλεται η κωδική λέξη «000000» και λαμβάνεται στην έξοδο η λέξη «000010», αφού η τελευταία δεν είναι κωδική λέξη, ανιχνεύουμε την ύπαρξη τουλάχιστον ενός σφάλματος. Αλλάζοντας μόνο ένα δυαδικό ψηφίο της λέξης «000010» μπορούμε να λάβουμε την κωδική λέξη «000000», αλλά θα πρέπει να αλλάξουμε περισσότερα ψηφία για να λάβουμε οποιαδήποτε από τις άλλες κωδικές λέξεις. Για το λόγο αυτό θεωρούμε ότι η πιο πιθανή κωδική λέξη που μεταδόθηκε είναι η «000000» και διορθώνουμε επομένως τη λέξη «000010» στην κωδική λέξη «000000». Διαπιστώνουμε λοιπόν ότι εφόσον κατά τη μετάδοση οποιασδήποτε από τις κωδικές λέξεις του κώδικα C_3 υπεισέλθει ένα μόνο σφάλμα, ο παραλήπτης μπορεί να ανιχνεύσει και να διορθώσει το σφάλμα. Αν υπεισέλθουν περισσότερα σφάλματα, τότε η διόρθωση και σε ορισμένες περιπτώσεις και η ανίχνευση δεν είναι δυνατή και με τον κώδικα C_3.

Βάρος Hamming ή απλά βάρος, *wt(x)*, μιας λέξης x μήκους n ψηφίων ονομάζεται το πλήθος των ψηφίων της λέξης, τα οποία είναι ίσα με το «1». Το βάρος παίρνει τιμές από 0 έως n.

Απόσταση Hamming ή απλά απόσταση, d(x, y), μεταξύ δύο λέξεων x και y του ιδίου μήκους n ονομάζεται το πλήθος των θέσεων, στις οποίες οι δύο λέξεις εμφανίζουν ασυμφωνία του δυαδικού ψηφίου. Η απόσταση παίρνει τιμές από 0 έως n.

3.3.2 Κωδικοποίηση - Αποκωδικοποίηση.

Τα δεδομένα των σχεδιαστών επικοινωνιακών καναλιών είναι η αξιοπιστία του καναλιού, δηλαδή η πιθανότητα ένα δυαδικό ψηφίο να μεταδίδεται χωρίς σφάλμα και το πλήθος των δυνατών διαφορετικών μηνυμάτων που μπορεί να μεταδοθούν. Τα δύο βασικά προβλήματα που απασχολούν τους σχεδιαστές στη Θεωρία Κωδικοποίησης είναι η κωδικοποίηση και η αποκωδικοποίηση. Η κωδικοποίηση συνίσταται στον προσδιορισμό ενός κώδικα, ο οποίος θα χρησιμοποιηθεί για την αποστολή των μηνυμάτων. Πρώτα επιλέγεται ένας θετικός ακέραιος k, το μήκος κάθε δυαδικής λέξης που αντιστοιχεί σε ένα μήνυμα.

Το μήκος των λέξεων επιλέγεται κατά τέτοιον τρόπο ώστε το πλήθος των δυνατών λέξεων να είναι μεγαλύτερο ή ίσο του πλήθους των δυνατών μηνυμάτων, δηλαδή $2k \geq |M|$, όπου $|M|$ είναι το πλήθος των δυνατών μηνυμάτων. Στη συνέχεια, επιλέγεται το πλήθος των δυαδικών ψηφίων που θα προστεθούν σε κάθε λέξη (πλεονασμός) έτσι ώστε να μπορεί να ανιχνεύεται ή και να διορθώνεται το επιθυμητό πλήθος σφαλμάτων. Έτσι προκύπτουν οι κωδικές λέξεις που αντιστοιχούν στα δυνατά μηνύματα, μήκους n ψηφίων, εκ των οποίων τα n – k bits είναι ο πλεονασμός. Επομένως, για τη μετάδοση ενός συγκεκριμένου μηνύματος, ο μεταδότης βρίσκει την κωδική λέξη που αντιστοιχεί σε αυτό το μήνυμα.

Αναφορικά με το δεύτερο πρόβλημα, την αποκωδικοποίηση, αν ο αποδέκτης (παραλήπτης) λάβει μία λέξη y, μήκους n ψηφίων, η οποία είναι κωδική λέξη, τότε εξάγει το αντίστοιχο μήνυμα. Αν όμως η λέξη y δεν είναι κωδική λέξη (ανίχνευση σφαλμάτων), ο παραλήπτης μπορεί να χρησιμοποιήσει μια διαδικασία, η οποία ονομάζεται αποκωδικοποίηση μέγιστης πιθανότητας, για την επιλογή της κωδικής λέξης που μεταδόθηκε (διόρθωση σφαλμάτων). Η διαδικασία αυτή διακρίνεται σε δύο εκδοχές:

1. Πλήρης αποκωδικοποίηση μέγιστης πιθανότητας (ΠΑΜΠ)

Αν υπάρχει μόνο μία κωδική λέξη x, η οποία εμφανίζει τη μικρότερη απόσταση από τη λέξη y, σε σύγκριση με τις αποστάσεις όλων των άλλων κωδικών λέξεων από τη λέξη y, τότε ο αποδέκτης αποκωδικοποιεί την y ως x. Αν όμως υπάρχουν περισσότερες κωδικές λέξεις που εμφανίζουν την ίδια απόσταση από τη λέξη y, τότε ο αποδέκτης αποκωδικοποιεί αυθαίρετα τη ληφθείσα λέξη ως μία από αυτές τις κωδικές λέξεις.

2. Ατελής αποκωδικοποίηση μέγιστης πιθανότητας (ΑΑΜΠ)

Όπως προηγουμένως, αν υπάρχει μία μοναδική κωδική λέξη x πλησιέστερη στη λέξη y, τότε ο αποδέκτης αποκωδικοποιεί την y ως x. Αν όμως υπάρχουν περισσότερες κωδικές λέξεις με την ίδια απόσταση στη λέξη y, τότε ο αποδέκτης ζητά από τον αποστολέα επανάληψη της μετάδοσης. Επανάληψη της μετάδοσης μπορεί να ζητηθεί και στις περιπτώσεις που, ενώ υπάρχει μια μόνο κωδική λέξη εγγύτερη στη ληφθείσα λέξη, η απόστασή τους είναι πολύ μεγάλη.

Ονομάζουμε το άθροισμα της κωδικής λέξης x που μεταδόθηκε με τη λέξη y που ελήφθη στον αποδέκτη, δηλαδή ε = x + y. Επίσης, ας ορίσουμε και την απόσταση κώδικα C. Η απόσταση ενός κώδικα C είναι η μικρότερη από τις αποστάσεις όλων των δυνατών ζευγών κωδικών λέξεων του κώδικα. Επειδή d(x, y) = wt(x + y), η απόσταση του κώδικα C είναι ίση με την ελάχιστη τιμή του βάρους wt(x + y), όπου x, y $\in$ C και x $\neq$y.

Όπως ήδη είπαμε, ο αποδέκτης μπορεί να ανιχνεύσει σφάλματα κατά τη μετάδοση, αν λάβει λέξεις που δεν ανήκουν στον κώδικα που χρησιμοποιείται, δεν είναι δηλαδή και κωδικές λέξεις. Έτσι, λέμε ότι ο κώδικας ανιχνεύει το πρότυπο σφάλματος ε, αν και μόνο αν x + ε = y δεν είναι κωδική λέξη, (για κάθε) $\forall$ x $\in$ C.

Ένας κώδικας C απόστασης d ανιχνεύει όλα τα μη μηδενικά πρότυπα σφάλματος βάρους μικρότερου ή ίσου του d – 1. Επίσης, υπάρχει τουλάχιστον ένα πρότυπο σφάλματος βάρους d που δεν ανιχνεύει ο κώδικας C.

Απόδειξη

Θεωρούμε ένα μη μηδενικό πρότυπο σφάλματος ε βάρους wt(ε) £ d – 1 και την κωδική λέξη x. Τότε

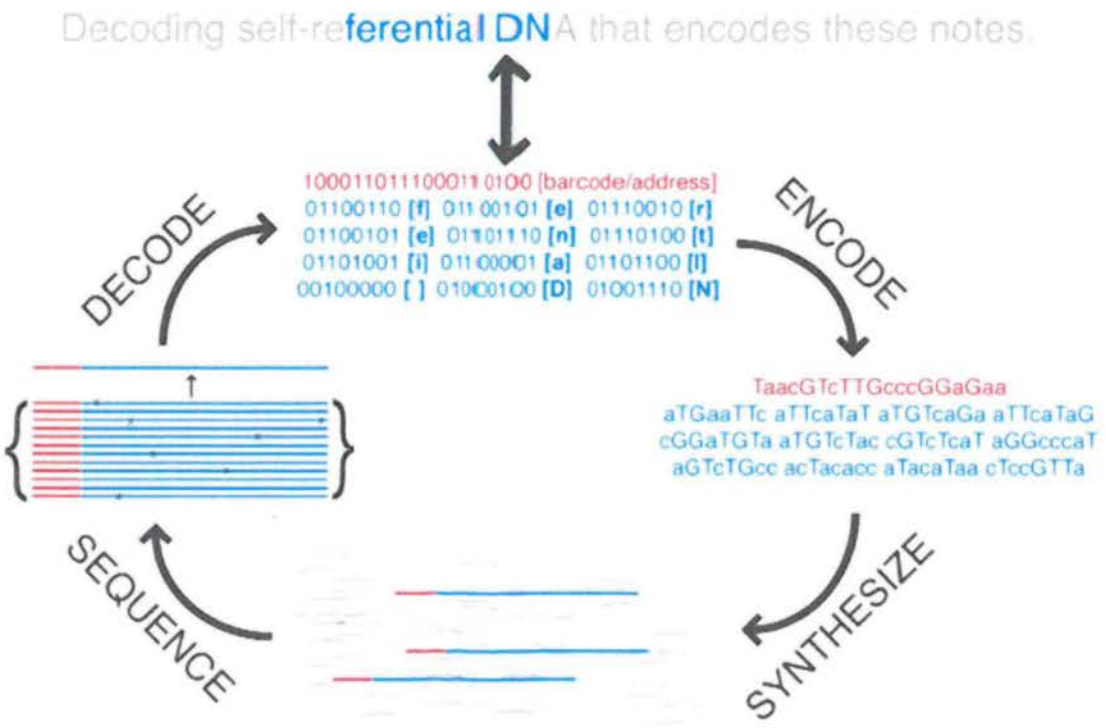
$$d(x, x + \varepsilon) = wt(x, x + \varepsilon) = wt(\varepsilon) \leq d - 1 < d .$$

Αφού πρόκειται για κώδικα απόστασης d, η λέξη x + ε = y που ελήφθη από τον αποδέκτη δεν ανήκει στον κώδικα C και επομένως ο κώδικας ανιχνεύει το πρότυπο σφάλματος ε. Αν τώρα εξετάσουμε το πρότυπο σφάλματος ε = x + y βάρους d με y = x + ε $\in$ C, τότε ο κώδικας C δεν ανιχνεύει το πρότυπο σφάλματος ε βάρους d.

Αν μεταδίδεται η κωδική λέξη x ενός κώδικα C και λαμβάνεται η λέξη y (με πρότυπο σφάλματος ε = x + y), τότε συμπεραίνεται από τον αποδέκτη, στη βάση της ατελούς αποκωδικοποίησης μέγιστης πιθανότητας, ότι μεταδόθηκε η x εφόσον η ληφθείσα λέξη y είναι πλησιέστερα στη x από ότι σε οποιαδήποτε άλλη κωδική λέξη του κώδικα C. Αν αυτό συμβαίνει κάθε φορά που εμφανίζεται το πρότυπο σφάλματος ε ανεξαρτήτως της κωδικής λέξης που μεταδόθηκε, τότε λέμε ότι ο κώδικας C διορθώνει το πρότυπο σφάλματος ε. Δηλαδή, ένας κώδικας C διορθώνει το πρότυπο σφάλματος ε αν $\forall$ x $\in$ C, τότε x + ε = y είναι εγγύτερα στη

x από ότι σε οποιαδήποτε άλλη κωδική λέξη του κώδικα C. Επίσης, χαρακτηρίζουμε έναν κώδικα C ως κώδικα β-διόρθωσης, αν διορθώνει όλα τα πρότυπα σφάλματος βάρους μικρότερου ή ίσου του β και δεν διορθώνει τουλάχιστον ένα πρότυπο σφάλματος βάρους β + 1.

Ένας κώδικας C απόστασης d διορθώνει όλα τα πρότυπα σφάλματος βάρους μικρότερου ή ίσου του $\lfloor \frac{d-1}{2} \rfloor$. (Υπενθυμίζεται ότι $\lfloor z \rfloor$ συμβολίζει το μεγαλύτερο ακέραιο αριθμό i που ικανοποιεί τη σχέση $i \leq z$.) Επίσης, υπάρχει τουλάχιστον ένα πρότυπο σφάλματος βάρους $1 + \lfloor (d-1)/2 \rfloor$ που δε διορθώνει ο κώδικας C.

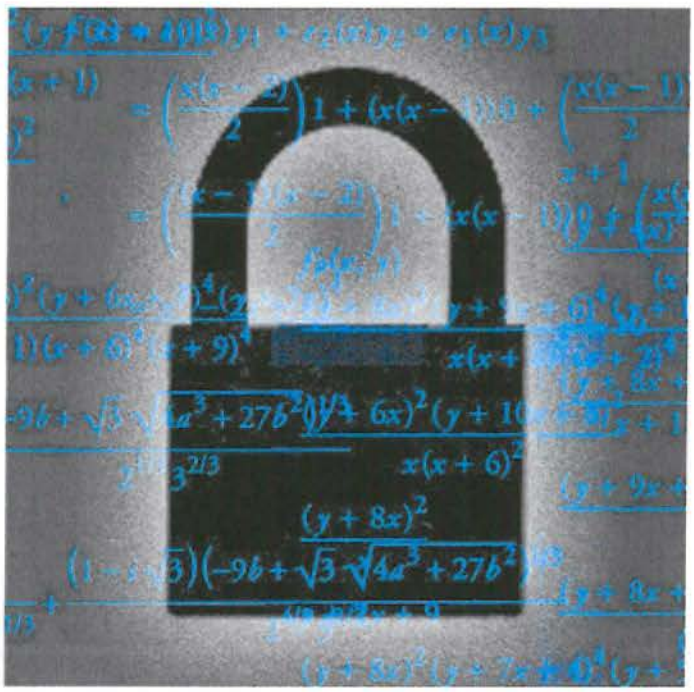


Εικόνα 68 Παράδειγμα Κωδικοποίησης - Αποκωδικοποίησης.

3.3.3 Κρυπτογραφία.

Κρυπτογραφία είναι ο επιστημονικός κλάδος που πραγματεύεται τη μελέτη και σχεδίαση κρυπτογραφικών τεχνικών, συστημάτων και πρωτοκόλλων. Μαζί με τον κλάδο της Κρυπτανάλυσης, που ασχολείται με τη μελέτη τρόπων παραβίασης αυτών, απαρτίζουν την Επιστήμη της Κρυπτολογίας. Κρυπτολογία είναι, επομένως, η επιστήμη της απόκρυψης από τη μία πλευρά και, από την άλλη, της αποκάλυψης του περιεχομένου κωδικοποιημένων μηνυμάτων ή δεδομένων.

Η επιθυμία προστασίας του περιεχομένου μηνυμάτων οδήγησε στην επινόηση και χρήση κρυπτογραφικών τεχνικών και συστημάτων, τα οποία επιτρέπουν το μετασχηματισμό μηνυμάτων ή δεδομένων κατά τέτοιο τρόπο ώστε να είναι αδύνατη η υποκλοπή του περιεχομένου τους κατά τη μετάδοσή ή αποθήκευσή τους και, βεβαίως, την αντιστροφή του μετασχηματισμού. Η διαδικασία μετασχηματισμού καλείται κρυπτογράφηση και η αντίστροφή της αποκρυπτογράφηση.



Εικόνα 69 Κρυπτογραφία.

Η συνάρτηση ή το σύνολο των κανόνων, στοιχείων και βημάτων που καθορίζουν την κρυπτογράφηση και την αποκρυπτογράφηση ονομάζεται κρυπτογραφικός αλγόριθμος ή κρυπτογραφικό σύστημα. (Σε μερικές περιπτώσεις, στη βιβλιογραφία, διαφοροποιείται μεταξύ αλγόριθμου και συστήματος, όπου ως σύστημα εννοείται η πραγματοποίηση του αλγόριθμου.) Ο κρυπτογραφικός αλγόριθμος καλείται και κωδικοποιητής (cipher). Πρωτόκολλα που χρησιμοποιούν κρυπτογραφικούς αλγόριθμους καλούνται κρυπτογραφικά πρωτόκολλα. Οι κρυπτογραφικοί αλγόριθμοι χρησιμοποιούν, κατά κανόνα, κρυπτογραφικά κλειδιά (keys), η τιμή των οποίων επηρεάζει την κρυπτογράφηση και την αποκρυπτογράφηση.

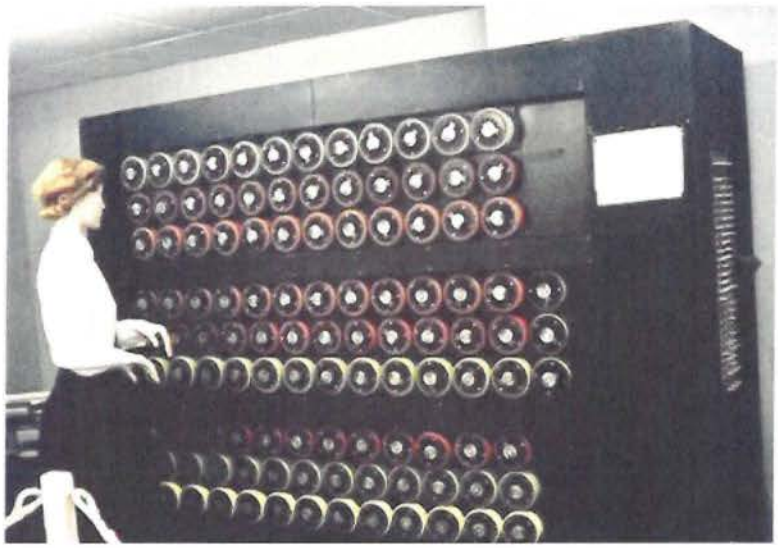
Υπάρχουν δύο κατηγορίες κρυπτογραφικών αλγορίθμων και επομένως και συστημάτων: οι συμμετρικοί και οι ασύμμετροι αλγόριθμοι. Οι συμμετρικοί αλγόριθμοι χρησιμοποιούν το ίδιο κλειδί για την κρυπτογράφηση και την αποκρυπτογράφηση και για το λόγο αυτό καλούνται, επίσης, αλγόριθμοι μυστικού κλειδιού ή αλγόριθμοι μονού κλειδιού. Οι ασύμμετροι αλγόριθμοι χρησιμοποιούν ένα ζεύγος κρυπτογραφικών κλειδιών, το δημόσιο κλειδί για την κρυπτογράφηση και το ιδιωτικό κλειδί για την αποκρυπτογράφηση. Έτσι, ο κάθε χρήστης ενός ασύμμετρου συστήματος έχει δύο κλειδιά, το δημόσιο και το ιδιωτικό. Το πρώτο το κοινοποιεί σε όλους που επιθυμούν να επικοινωνήσουν μαζί του. Όμως, δεν είναι δυνατό από το δημόσιο να υπολογίσουμε το ιδιωτικό κλειδί ενός χρήστη. Οι ασύμμετροι αλγόριθμοι ονομάζονται και αλγόριθμοι δημόσιου κλειδιού.

Οι συμμετρικοί αλγόριθμοι χωρίζονται, με τη σειρά τους, σε δύο κατηγορίες: στους κωδικοποιητές ροής (stream ciphers) και στους κωδικοποιητές τμημάτων (block ciphers). Οι πρώτοι εφαρμόζονται σε κάθε bit ή χαρακτήρα ενός μηνύματος, ενώ οι δεύτεροι σε τμήματα (blocks) του μηνύματος σταθερού μήκους. Συνήθως, το μήκος αυτό ανέρχεται σε 64 ή 128 bits.

Θα συμβολίζουμε το καθαρό (ή μη κρυπτογραφημένο) μήνυμα ή κείμενο (plaintext) με M, το κρυπτογραφημένο μήνυμα ή κείμενο (ciphertext) με C και το κλειδί με K.

Η Κρυπτανάλυση έχει ως σκοπό την ανάπτυξη τεχνικών και μεθόδων για την παραβίαση κρυπτογραφημένων μηνυμάτων ή κρυπτογραφικών συστημάτων. Μία επιτυχής κρυπτανάλυση μπορεί να αποκαλύψει το καθαρό από το

κρυπτογραφημένο μήνυμα. Μπορεί, ακόμα, να εντοπίσει αδυναμίες σε ένα κρυπτογραφικό σύστημα, οι οποίες οδηγούν τελικά στα παραπάνω αποτελέσματα. Αντίθετα, η Κρυπτογραφία επιδιώκει την ανάπτυξη ισχυρών κρυπτογραφικών συστημάτων, τα οποία να είναι σε θέση να ανταπεξέλθουν σε απόπειρες παραβίασης από τους κρυπταναλυτές.



Εικόνα 70 Μηχανή κρυπτανάλυσης Turing.

Μία επιχειρούμενη κρυπτανάλυση χαρακτηρίζεται και επίθεση (attack). Οι κρυπταναλυτές μπορεί να έχουν στη διάθεσή τους κρυπτογραφημένα μηνύματα, τα αντίστοιχα καθαρά μηνύματα, τους αλγόριθμους κρυπτογράφησης που χρησιμοποιήθηκαν, στατιστικά εργαλεία και τεχνικές, κτλ. Επίσης, υποθέτουμε ότι ο κρυπταναλυτής γνωρίζει τις λεπτομέρειες του κρυπτογραφικού αλγόριθμου, αν και αυτό δε συμβαίνει πάντα στην πράξη. Η υπόθεση αυτή είναι εύλογη, γιατί, όπως αναφέρεται συχνά στη βιβλιογραφία, αν η ασφάλεια των κρυπτογραφικών συστημάτων στηρίζεται στη μυστικότητά τους, τότε αυτή δεν μπορεί να είναι επαρκής.

Αν στηρίζεται εκτός των άλλων και στη μυστικότητα των αλγορίθμων, κάτι το οποίο δεν συνιστάται, τότε πρόκειται κατά κανόνα για συστήματα με περιορισμένο πεδίο εφαρμογής. Οι τύποι κρυπταναλυτικών επιθέσεων διαφοροποιούνται σύμφωνα με το τι έχει στη διάθεσή του ο επιτιθέμενος. Όλοι οι τύποι επιθέσεων προϋποθέτουν ότι ο κρυπταναλυτής γνωρίζει πλήρως τον χρησιμοποιούμενο αλγόριθμο κρυπτογράφησης. Στη συνέχεια, παρατίθενται βασικοί τύποι

επιθέσεων, οι οποίοι αποτελούν τη βάση αξιολόγησης κρυπτογραφικών συστημάτων.

- Επίθεση κρυπτογραφημένου κειμένου (Ciphertext – only attack). Ο κρυπταναλυτής έχει στη διάθεσή του αρκετά κρυπτογραφημένα, με τον ίδιο αλγόριθμο και το ίδιο κλειδί, μηνύματα και επιδιώκει να αποκρυπτογραφήσει όσο πιο πολλά μηνύματα μπορεί ή και να προσδιορίσει το κρυπτογραφικό κλειδί που χρησιμοποιήθηκε ή ακόμα και να επινοήσει έναν αλγόριθμο που θα του επιτρέπει να υπολογίζει το καθαρό από το κρυπτογραφημένο μήνυμα.

- Επίθεση γνωστού καθαρού κειμένου (Known – plaintext attack). Ο κρυπταναλυτής έχει στη διάθεσή του όχι μόνο κρυπτογραφημένα μηνύματα αλλά και τα αντίστοιχα καθαρά μηνύματα και επιδιώκει να προσδιορίσει το κλειδί που χρησιμοποιήθηκε για την κρυπτογράφηση των μηνυμάτων ή κάποιον αλγόριθμο που θα του επιτρέπει να υπολογίζει από το κρυπτογραφημένο μήνυμα το αντίστοιχο καθαρό που πλέον δεν γνωρίζει.

- Επίθεση επιλεγμένων καθαρών κειμένων (Chosen – plaintext attack). Οι κρυπταναλυτές έχουν στη διάθεσή τους τα κρυπτογράμματα επιλεγμένων από τους ίδιους καθαρών μηνυμάτων. Ο στόχος είναι να βρεθεί το κλειδί που χρησιμοποιείται για την κρυπτογράφηση των μηνυμάτων, ή να επινοηθεί ένας αλγόριθμος για την αποκρυπτογράφηση των νέων μηνυμάτων, τα οποία κρυπτογραφούνται με το ίδιο κλειδί.

- Επίθεση επιλεγμένων κρυπτογραφημένων κειμένων (Chosen – ciphertext attack). Οι κρυπταναλυτές μπορούν να επιλέξουν διάφορα κρυπτογραφημένα μηνύματα και διαθέτουν ακόμα τα αντίστοιχα καθαρά μηνύματα, επιδιώκουν δε τον προσδιορισμό του κλειδιού που μπορεί να χρησιμοποιηθεί για την αποκρυπτογράφηση.

Όπως αναφέρθηκε προηγουμένως, τα κρυπτογραφικά συστήματα που χρησιμοποιούνται για την προστασία του περιεχομένου μηνυμάτων διακρίνονται στα συμμετρικά και τα ασύμμετρα. Στους κρυπτογραφικούς αλγόριθμους συγκαταλέγονται ωστόσο και αλγόριθμοι που χρησιμοποιούνται σε σχήματα ψηφιακών υπογραφών (digital signature schemes), σε συναρτήσεις

κατακερματισμού (one-way hash functions), για την ανταλλαγή κλειδιών (key exchange mechanisms) κ.ά.

Η κλασική κρυπτογραφία διακρίνει τις τεχνικές της αντικατάστασης και της μετάθεσης. Η μέθοδος του Καίσαρα αποτελεί μια από τις πιο παλιές τεχνικές μόνο-αλφαβητικής αντικατάστασης. Σύμφωνα με τη μέθοδο αυτή, κάθε γράμμα του απλού μηνύματος αντικαθίσταται από το γράμμα που βρίσκεται τρεις θέσεις δεξιά του στο αλφάβητο. Δηλαδή το «Α» αντικαθίσταται από το «Δ», το «Β» από το «Ε», το «Γ» από το «Ζ», κοκ. Η μέθοδος του Καίσαρα μπορεί να γενικευθεί, αν στη θέση του 3 (κλειδιού) χρησιμοποιήσουμε έναν οποιοδήποτε αριθμό k, μικρότερο του 24 και μεγαλύτερο του μηδενός. Με τη βοήθεια μιας αντιστοιχίας των γραμμάτων του αλφαβήτου με αριθμούς από το 1 έως το 24, μπορούμε να εκφράσουμε την κρυπτογράφηση και την αποκρυπτογράφηση της μονοαλφαβητικής αντικατάστασης με τις ακόλουθες σχέσεις (όπου M συμβολίζει ένα οποιοδήποτε γράμμα του μηνύματος και C το σύμβολο – γράμμα από το οποίο αντικαθίσταται):

Κρυπτογράφηση: $C = (M + k) \bmod 24$ (για το ελληνικό αλφάβητο)

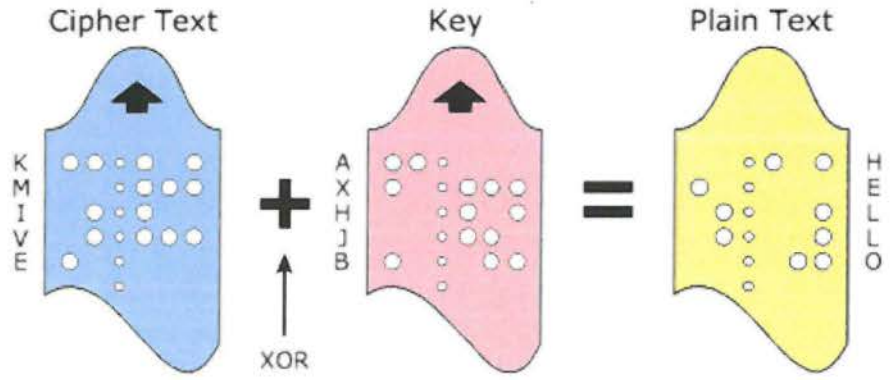
Αποκρυπτογράφηση: $M = (C - k) \bmod 24$

Αν το αποτέλεσμα της αφαίρεσης (C – k) είναι αρνητικός αριθμός, προσθέτουμε σε αυτόν το 24 και έτσι παίρνουμε τον επιθυμητό μη αρνητικό αριθμό. Στην περίπτωση του αγγλικού αλφαβήτου αντί του mod 24 χρησιμοποιούμε mod 26. Αν χρησιμοποιήσουμε για την κρυπτογράφηση τη σχέση $C = (aM + k) \bmod 26$ (αγγλικό αλφάβητο), όπου a μεγαλύτερος ή ίσος του 1 και σχετικά πρώτος του 26, έχουμε τον επονομαζόμενο Affine Κωδικοποιητή. Η αποκρυπτογράφηση επιτυγχάνεται με τη σχέση $M = b(C - k) \bmod 26$, όπου b είναι ο αντίστροφος του a mod26, δηλαδή $ab = m\ 26 + 1$ (m οποιοσδήποτε ακέραιος).

Στην πολυαλφαβητική αντικατάσταση, το κλειδί δεν είναι μόνο ένας αριθμός k, αλλά μια ακολουθία αριθμών $k_1k_2\ldots k_n$. Ο αριθμός k1 χρησιμοποιείται για την αντικατάσταση του 1ου, του (n + 1) – οστού, του (2n + 1) – οστού γράμματος του μηνύματος κοκ., ο αριθμός k2 χρησιμοποιείται για την αντικατάσταση του 2ου, του (n + 2) – οστού, του (2n + 2) – οστού γράμματος του μηνύματος κοκ. και ο αριθμός kn για την αντικατάσταση του n – οστού, του 2n – οστού γράμματος του μηνύματος κοκ.

Ο κωδικοποιητής του Vernam βασίζεται στην πολυαλφαβητική αντικατάσταση και προβλέπει μήκος κλειδιού ίσο με αυτό του μηνύματος καθώς και τυχαία δημιουργία των αριθμών (ή αντίστοιχων γραμμάτων ή συμβόλων) του κλειδιού. Η μέθοδος αυτή κρυπτογράφησης λέγεται μπλοκ μιας χρήσης (one – time pad). Η ανακάλυψη του Vernam χρησιμοποιούσε διάτρητες ταινίες χαρτιού με τυχαίους αριθμούς, τους οποίους συνδύαζε με τα γράμματα του καθαρού μηνύματος που τροφοδοτούσε σε συσκευή τηλετύπου. Η ακολουθία των τυχαίων αριθμών ήταν μη επαναλαμβανόμενη και κάθε ταινία χρησιμοποιείτο μία φορά.

Ο δυαδικός κωδικοποιητής του Vernam χρησιμοποιεί, αντί γραμμάτων και αριθμών, δυαδικά ψηφία. Δηλαδή τόσο οι τυχαίοι αριθμοί που απαρτίζουν το κλειδί όσο και το μήνυμα είναι σε δυαδική μορφή. Για τον υπολογισμό του κρυπτογραφημένου, δυαδικού, μηνύματος, κάθε bit αυτού συσχετίζεται με το αντίστοιχο bit του κλειδιού μέσω της πράξης XOR, το αποτέλεσμα δε αυτής είναι το bit του κρυπτογραφημένου μηνύματος. Στη συνέχεια μπορούμε να δούμε ένα σχετικό παράδειγμα. Τόσο ο αποστολέας όσο και ο παραλήπτης έχουν την ίδια τυχαία ακολουθία δυαδικών ψηφίων. Ο αποστολέας υπολογίζει το κρυπτογραφημένο μήνυμα και το αποστέλλει στον παραλήπτη. Ο παραλήπτης, από την πλευρά του, από την τυχαία ακολουθία και το κρυπτογραφημένο μήνυμα υπολογίζει το καθαρό μήνυμα (το αποτέλεσμα της πράξης XOR).



Εικόνα 71 Αλγόριθμος του Vernam.

3.3.4 Το ασύμμετρο κρυπτογραφικό σύστημα RSA.

Ας δούμε τώρα και το ευρέως χρησιμοποιούμενο, σύγχρονο κρυπτογραφικό σύστημα, το RSA, το οποίο βασίζεται στο δύσκολο πρόβλημα της ανάλυσης πολύ μεγάλων αριθμών σε γινόμενο πρώτων παραγόντων και το οποίο εντάσσεται στην κατηγορία των ασύμμετρων συστημάτων. Πιο συγκεκριμένα, στον αλγόριθμο RSA χρησιμοποιούνται υπολογισμοί μεγάλων δυνάμεων ως προς μέτρο ισοτιμίας ένα φυσικό αριθμό n, ο οποίος είναι το γινόμενο δύο πολύ μεγάλων πρώτων αριθμών. Για τον λόγο αυτό, πρώτα επιλέγονται δύο πολύ μεγάλοι πρώτοι αριθμοί p και q και στη συνέχεια υπολογίζεται το γινόμενό τους, $n = p\,q$. Στη συνέχεια επιλέγονται το δημόσιο e και το μυστικό κλειδί d. Ο αριθμός e επιλέγεται έτσι ώστε να είναι σχετικά πρώτος ως προς το $\varphi(n)$ και να ικανοποιεί την ακόλουθη σχέση: $3 < e < \varphi(n) = (p - 1)(q - 1)$. (Υπόμνηση: $\varphi(n)$ είναι η συνάρτηση του Euler, η οποία υποδηλώνει το πλήθος των φυσικών, μικρότερων ή ίσων του n, οι οποίοι είναι σχετικά πρώτοι με αυτόν.) Αναφορικά με το φυσικό αριθμό d, αυτός είναι αντίστροφος του e, δηλαδή προσδιορίζεται έτσι ώστε να πληροί την ακόλουθη σχέση ισοτιμίας: $d\,e \equiv 1 \bmod \varphi(n)$ ή $d \equiv e^{-1} \bmod \varphi(n)$.

Η κρυπτογράφηση ενός μηνύματος M, το οποίο χωρίζεται σε τμήματα M1, M2, …,Mk που αναπαριστώνται από αριθμούς μικρότερους του n καθώς και η αποκρυπτογράφηση επιτυγχάνονται ως εξής:

$C_1 = M_1^{\,e} \bmod n,$

$C_2 = M_2^{\,e} \bmod n,$

…,

$C_k = M_k^{\,e} \bmod n,$

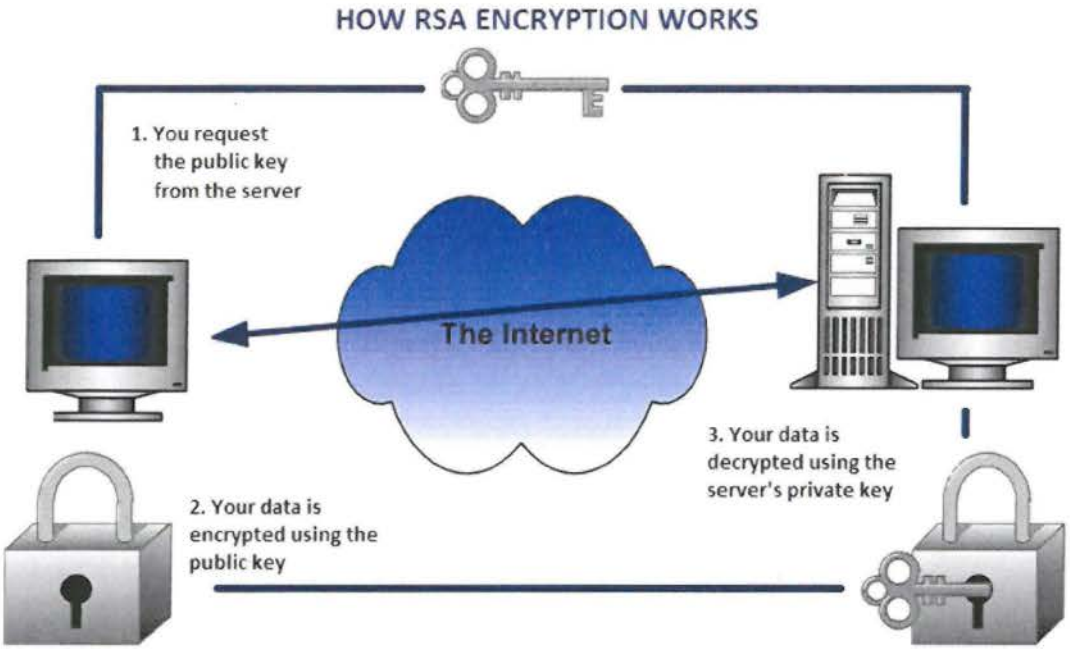
$M_1 = C_1^{\,d} \bmod n = M_1^{\,ed} \bmod n,$

$M_2 = C_2^{\,d} \bmod n, \ldots, M_k = C_k^{\,d} \bmod n.$

Ο αποστολέας του μηνύματος χρησιμοποιεί για την κρυπτογράφηση το δημόσιο κλειδί του παραλήπτη, το οποίο αποτελείται από τους αριθμούς e και n, δηλαδή {e, n}. Ο παραλήπτης αποκρυπτογραφεί το κρυπτογραφημένο μήνυμα με το ιδιωτικό

του κλειδί, το οποίο αποτελείται από τους αριθμούς d και n, δηλαδή {d, n). Η ασφάλεια του RSA στηρίζεται στο ότι είναι μη εφικτό να υπολογιστεί το ιδιωτικό από το δημόσιο κλειδί. Για την εύρεση του d, από τα δημοσιοποιημένα e και n, απαιτείται η ανάλυση του n σε γινόμενο πρώτων παραγόντων, δηλαδή στα p και q. Η ανάλυση πολύ μεγάλων αριθμών, μήκους μεγαλύτερου των 1024 bits, σε γινόμενο πρώτων παραγόντων είναι ανέφικτη σε πρακτικά χρήσιμους χρόνους με τις τωρινές δυνατότητες υπολογιστικών πόρων.

Η ασφάλεια των κρυπτογραφικών συστημάτων, δηλαδή η ανθεκτικότητά τους σε απόπειρες παραβίασης, είναι ένα από τα πρώτα ερωτήματα που θέτουμε πριν αποφασίσουμε να τα χρησιμοποιήσουμε σε πρακτικές εφαρμογές. Τα κρυπτογραφικά συστήματα εμφανίζουν διάφορα επίπεδα ασφαλείας, ανάλογα με το πόσο δύσκολα παραβιάζονται. Μερικοί όμως αλγόριθμοι απαιτούν εκατομμύρια χρόνια ή απεριόριστους υπολογιστικούς πόρους για να παραβιαστούν. Αυτοί οι αλγόριθμοι είναι θεωρητικά παραβιάσιμοι, αλλά όχι πρακτικά. Ένας αλγόριθμος που δεν παραβιάζεται στην πράξη θεωρείται ασφαλής (secure). Ένας αλγόριθμος είναι απόλυτα ασφαλής (unconditionally secure), αν, ανεξαρτήτως του μεγέθους του κρυπτογραφημένου μηνύματος, των υπολογιστικών πόρων και του χρόνου που μπορεί να διαθέτει ο κρυπταναλυτής, δεν υπάρχει δυνατότητα να παραβιαστεί, δηλαδή να αποκαλυφθεί το καθαρό μήνυμα. Τα one-time pads, όπως θα αποδείξουμε στην Υποενότητα 5.2.1, δεν μπορούν να παραβιασθούν, ακόμα και αν ο κρυπταναλυτής έχει στη διάθεσή του άπειρους υπολογιστικούς και αποθηκευτικούς πόρους.



Εικόνα 72 RSA Εξήγηση αλγορίθμου.

Ωστόσο, η μοντέρνα κρυπτογραφία ασχολείται κυρίως με κρυπτογραφικά συστήματα, τα οποία δεν μπορούν να παραβιαστούν με τις δεδομένες υπολογιστικές δυνατότητες. Ένας αλγόριθμος λέγεται υπολογιστικά ασφαλής (computationally secure), ή δυνατός (strong), αν είναι αδύνατη η παραβίασή του με τους διαθέσιμους (τωρινούς ή μελλοντικούς) πόρους. Με τη βοήθεια της Θεωρίας Πληροφορίας, μπορούμε να δώσουμε κάποιες απαντήσεις στο ερώτημα της ασφαλείας κρυπτογραφικών συστημάτων, καθώς επίσης και στο ερώτημα του «πόσο σημαντικό είναι το μήκος του κρυπτογραφημένου μηνύματος» το οποίο έχει στη διάθεσή του ένας κρυπταναλυτής για την παραβίασή του, θεωρώντας ωστόσο ότι ο κρυπταναλυτής έχει στη διάθεσή του απεριόριστους υπολογιστικούς και αποθηκευτικούς πόρους.

Από την άλλη πλευρά, στη σύγχρονη Κρυπτογραφία θεωρούμε κατά κανόνα ότι ο κρυπταναλυτής έχει στη διάθεσή του μόνο περιορισμένους πόρους και ανατρέχουμε πλέον στη Θεωρία Πολυπλοκότητας για να απαντήσουμε στο ερώτημα της ασφαλείας κρυπτογραφικών συστημάτων, αφού αυτά βασίζονται κυρίως σε υπολογιστικά δύσκολα προβλήματα.

Κεφάλαιο 4°: Κβαντικοί Υπολογιστές.

4.1.1 Ιστορική αναδρομή Κβαντικής Θεωρίας Υπολογισμού.

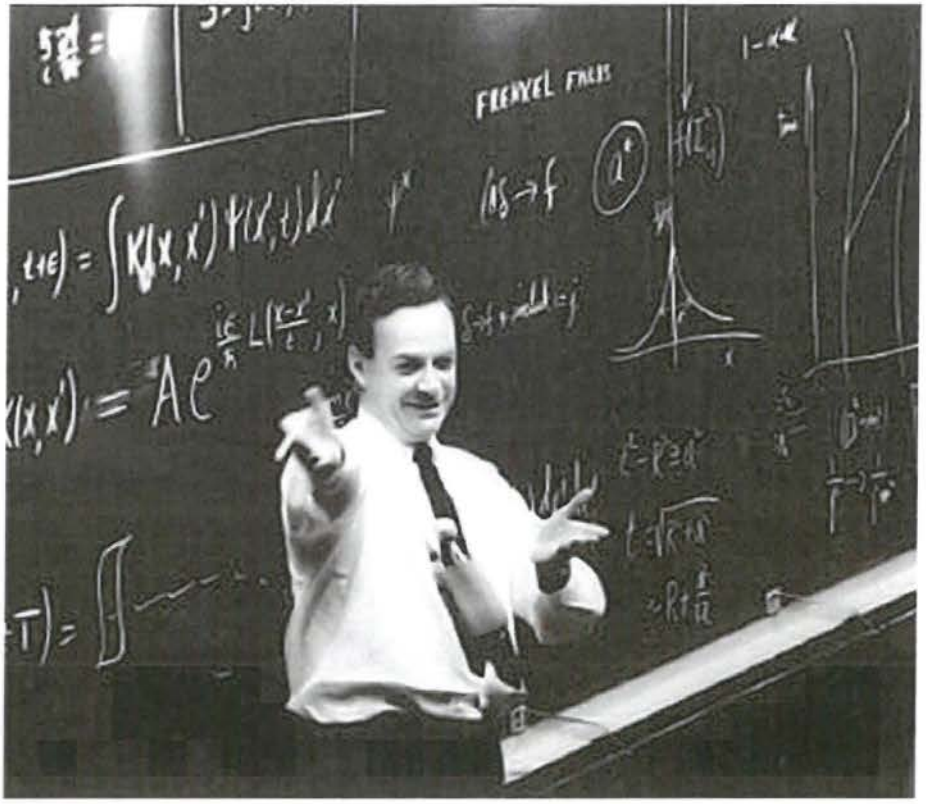
Τα πρώτα δημοσιεύματα που προετοίμασαν το έδαφος για την ανάπτυξη κβαντικών αλγορίθμων έγιναν τη δεκαετία του 1970. Κάποια από αυτά ήταν η διατύπωση του θεωρήματος του Holevo (1973) ότι n qubits δεν μπορούν να μεταφέρουν περισσότερα από n κλασικά bits πληροφορίας, μια απόδειξη της μη αποδοτικής προσομοίωσης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

Όμως το ουσιαστικό βήμα που έστρεψε το ενδιαφέρον της ερευνητικής κοινότητας προς τους κβαντικούς υπολογιστές έγινε το 1981 με τη διάλεξη του διάσημου φυσικού και νομπελίστα Richard Feynman στο First Conference on the Physics of Computation που έγινε στο MIT και τη δημοσίευση που ακολούθησε το 1982 από τον ίδιο. Στο άρθρο αυτό επισήμανε ότι ένα κβαντομηχανικό σύστημα R σωματιδίων δεν μπορεί να προσομοιωθεί αποδοτικά με ένα συνηθισμένο υπολογιστή χωρίς εκθετική επιβράδυνση στην αποδοτικότητα της προσομοίωσης. Παρ' όλα αυτά ένα σύστημα R σωματιδίων στην κλασική φυσική είναι δυνατόν να προσομοιωθεί αρκετά καλά με μόνο πολυωνυμική επιβράδυνση.

Ο κύριος λόγος για τον οποίο συμβαίνει αυτό είναι ότι το μέγεθος της περιγραφής ενός συστήματος σωματιδίων είναι γραμμικό ως προς R στην κλασική φυσική (αρκεί να δοθούν οι συντεταγμένες και οι ορμές των σωματιδίων με την απαιτούμενη ακρίβεια), ενώ στην κβαντική φυσική είναι εκθετικό. Ο ίδιος ο Feynman γράφει:

Αλλά η πλήρης κβαντομηχανική περιγραφή για ένα μεγάλο σύστημα με R σωματίδια δίνεται από μια συνάρτηση $\Psi(x_1,x_2,...,x_R,t)$ της οποίας λαμβάνουμε το πλάτος για να βρούμε τα σωματίδια $x_1,x_2,...,x_R$ και συνεπώς επειδή έχει τόσες πολλές μεταβλητές δεν είναι δυνατόν να προσομοιωθεί με ένα κανονικό υπολογιστή με αριθμό στοιχείων ανάλογο του ή του N. επειδή έχει τόσες πολλές μεταβλητές δεν είναι

δυνατόν να προσομοιωθεί με ένα κανονικό υπολογιστή με αριθμό στοιχείων ανάλογο του R ή του N.



Εικόνα 73 Richard Feynman

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

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

Εικόνα 74 David Deutsch.

Η μεγάλη έκρηξη στο ενδιαφέρον της επιστημονικής κοινότητας έγινε το 1994 με την ανακάλυψη του αλγορίθμου παραγοντοποίησης του Shor . Ο αλγόριθμος

αυτός καταφέρνει να λύσει το πρόβλημα της παραγοντοποίησης μεγάλων αριθμών, όπως και το πρόβλημα του διακριτού λογάριθμου, σε πολυωνυμικό χρόνο. Τα δύο αυτά προβλήματα δεν έχει αποδειχθεί ότι δεν λύνονται σε πολυωνυμικό χρόνο με κλασικούς αλγόριθμους αλλά αυτή είναι η κοινή πεποίθηση των επιστημόνων μέχρι στιγμής. Η μεγάλη σημασία του αλγορίθμου του Shor προκύπτει από το γεγονός ότι η αξιοπιστία του διάσημου κρυπτοσυστήματος RSA (δημοσίου κλειδιού) το οποίο έχει σχεδιαστεί για μυστικές επικοινωνίες βασίζεται στην υπόθεση ότι η παραγοντοποίηση μεγάλων ακεραίων αποτελεί ένα δυσεπίλυτο (intractable) πρόβλημα. Ο Shor έδειξε ότι αυτό δεν ισχύει αν κάποιος καταφέρει να κατασκευάσει ένα κβαντικό υπολογιστή.

Εικόνα 75 Peter Shor.

Επομένως μυστικές υπηρεσίες, κυβερνήσεις και οποιοσδήποτε που ασχολείται με την κρυπτογραφία έχει συμφέρον να εφευρεθούν λειτουργικοί κβαντικοί υπολογιστές - κβαντικοί υπολογιστές μεγάλης κλίμακας. Επόμενος σημαντικός σταθμός ήταν το 1996 που ανακαλύφθηκε ο αλγόριθμος κβαντικής αναζήτησης του Lov Grover. Με αυτό τον αλγόριθμο είναι δυνατόν να βρεθεί ένα στοιχείο σε μια αταξινόμητη λίστα μήκους n σε χρόνο $O(\sqrt{n})$. Αντίθετα για τους κλασικούς αλγόριθμους το κάτω όριο είναι O(n). Επομένως παρ' όλο που δεν παρουσιάζει αυτός ο αλγόριθμος εκθετική επιτάχυνση όπως ο αλγόριθμος παραγοντοποίησης

παρουσιάζει την απόδειξη ότι οι κβαντικοί υπολογιστές είναι ισχυρότεροι σε ορισμένες περιπτώσεις από τους κλασικούς.

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

Από τότε μέχρι σήμερα εκατοντάδες ερευνητικά κέντρα προσπαθούν να κατασκευάσουν αξιόπιστους κβαντικούς υπολογιστές χρησιμοποιώντας διαφορετικά υλικά. Η μεγαλύτερη δυσκολία ανακύπτει από δύο αντικρουόμενες προϋποθέσεις. Από τη μία η μνήμη ενός υπολογιστή η οποία αποτελείται από μικροσκοπικά κβαντικά συστήματα πρέπει να απομονωθεί όσο τέλεια γίνεται για να προστατευθεί από καταστροφική αλληλεπίδραση με το περιβάλλον.

Από την άλλη η «κβαντική κεντρική μονάδα επεξεργασίας» δεν πρέπει να είναι εντελώς απομονωμένη, αφού οι υπολογισμοί πρέπει να είναι συνεχείς, και ένας «ελεγκτής» πρέπει να ελέγχει ότι το κβαντικό σύστημα εξελίσσεται με το ζητούμενο τρόπο. Μάλιστα το πρόβλημα ότι ανεξέλεγκτα σφάλματα είναι δυνατόν να προκύψουν κατά τη διάρκεια των υπολογισμών δεν είναι καινούριο: στην κλασική θεωρία πληροφορίας θεωρούμε συχνά ένα θορυβώδες κανάλι το οποίο μπορεί να αλλοιώσει τα μηνύματα. Η δουλειά του παραλήπτη είναι να εξάγει την σωστή πληροφορία από το παραμορφωμένο μήνυμα χωρίς επιπλέον μετάδοση πληροφορίας. Η κλασική θεωρία πληροφορίας ασχολείται με αυτό το πρόβλημα και το συμπέρασμα που προκύπτει χάρη στην εργασία του Claude Shannon είναι το εξής:

Για ένα σχετικά θορυβώδες κανάλι υπάρχει ένα σύστημα κωδικοποίησης των μηνυμάτων το οποίο μας επιτρέπει να μειώσουμε την πιθανότητα σφάλματος στη μετάδοση όσο θέλουμε. Αρχικά ήταν κοινή η άποψη ότι ένα αντίστοιχο μοντέλο ήταν αδύνατο για τους κβαντικούς υπολογισμούς ακόμη και σε θεωρητικό επίπεδο, κυρίως εξαιτίας του θεωρήματος «Μη Αντιγραφής», το οποίο έλεγε ότι η

κβαντική πληροφορία είναι αδύνατον να διπλασιαστεί με ακρίβεια. Παρ' όλα αυτά το 1995 ο Shor έδειξε ότι μπορούμε να κατασκευάσουμε σχήματα διόρθωσης λαθών για τους κβαντικούς υπολογιστές, και άρα θεμελίωσε την θεωρία των κβαντικών κωδικών διόρθωσης σφαλμάτων. Αυτή η θεωρία είναι ακόμα αντικείμενο μελετών και ίσως οδηγήσει μια μέρα στην κατασκευή κβαντικών υπολογιστών μεγάλης κλίμακας.

4.1.2 Ιστορική αναδρομή γλωσσών κβαντικού προγραμματισμού.

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

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

Χωρίζονται όμως σε διάφορες κατηγορίες. Μια πρώτη κατηγοριοποίησή τους είναι σε τρία υποσύνολα παρόμοια με τα αντίστοιχα των συμβατικών γλωσσών. Αυτά είναι οι προστακτικές γλώσσες κβαντικού προγραμματισμού, οι συναρτησιακές γλώσσες και όλες οι υπόλοιπες. Αρχικά αναπτύχθηκαν οι προστακτικές γλώσσες των οποίων τα προγράμματα αποτελούνται από μια ακολουθία εντολών

προστακτικής φύσεως κατ' αναλογία με τις αντίστοιχες γλώσσες του συμβατικού υπολογισμού. Ακόμη και σήμερα βέβαια οι περισσότεροι αλγόριθμοι ακολουθούν υποσυνείδητα αυτό το μοντέλο και συνεχίζεται η ανάπτυξη τους.

Αργότερα εμφανίστηκε η μεγάλη τάση των συναρτησιακών γλωσσών οι οποίες ταιριάζουν αρκετά καλά στο κβαντικό μοντέλο καθώς κάθε αλγόριθμος πρόκειται ουσιαστικά για συνεχείς μετασχηματισμούς πάνω σε μια ποσότητα κβαντικής πληροφορίας. Τέλος στην τρίτη κατηγορία ανήκουν γλώσσες διαφορετικών μορφών. Εκτός από αυτήν την κατηγοριοποίηση υπάρχει και ο χωρισμός των κβαντικών γλωσσών σε δύο τάξεις: αυτές που επιτρέπουν μόνο κλασική ροή ελέγχου και αυτές που επιτρέπουν και κβαντική ροή ελέγχου. Η πρώτη και απλούστερη αποτελείται από γλώσσες οι οποίες επιτρέπουν την κβαντική υπέρθεση μόνο στην κατάσταση των qubits (κβαντικά bit).

Εικόνα 76 Γελοιογραφία Κβαντικού προγραμματιστή.

Αντίθετα ο έλεγχος του προγράμματος γίνεται με κλασικό τρόπο. Συνοπτικά η υπέρθεση είναι η ικανότητα των κβαντικών συστημάτων να βρίσκονται σε περισσότερες από μία καταστάσεις ταυτόχρονα. Στο πρώτο είδος γλωσσών οι οποίες αναφέρονται ως "quantum data, classical control paradigm" τα προγράμματα ακολουθούν μια συγκεκριμένη ροή και απλώς επεξεργάζονται κβαντικά bits.

Η δεύτερη κατηγορία είναι οι γλώσσες που επιτρέπουν και κβαντικό έλεγχο: "quantum data and control paradigm". Σε αυτές το πρόγραμμα μπορεί να

βρίσκεται σε υπέρθεση δύο δυνατών μονοπατιών υπολογισμού. Φυσικά και τα δεδομένα που χειρίζονται μπορούν να είναι σε υπέρθεση. Η κβαντική μηχανή Turing του Deutsch λειτουργούσε σύμφωνα με αυτό το μοντέλο.

Προστακτικές γλώσσες

Όπως είδαμε η κβαντική μηχανή Turing (QTM) του Deutsch εφευρέθηκε το 1985. Αυτή είχε μια στοιχειώδη ψευδογλώσσα - οδηγίες προστακτικής μορφής. Το 1993 οι Bernstein και Vazirani εκτός από την βελτίωση της μηχανής πρότειναν και κάποια προγραμματιστικά δομικά στοιχεία. Πιθανότατα όμως η πρώτη πρόταση για μια σαφώς ορισμένη κβαντική γλώσσα προγραμματισμού, σε αντίθεση με τις περιγραφές QTM μηχανών, ήρθε το 1996 με την εργασία του Knill. Αυτός ορίζει έναν προστακτικό ψευδοκώδικα ο οποίος έτρεχε σε ένα μοντέλο κβαντικής μηχανής τυχαίας πρόσβασης (Quantum Random Access Machine – QRAM) αντίστοιχο με το κλασικό μοντέλο RAM. Ο Knill κατανοεί ότι ο κβαντικός ψευδοκώδικας δεν αποτελεί από μόνος του μια υλοποιήσιμη κβαντική γλώσσα αλλά είναι ένα σημαντικό βήμα εμπρός σε σχέση με τις εκ των υστέρων περιγραφές του πως πρέπει να υλοποιούνται οι κβαντικοί υπολογισμοί. Κατά τη διάρκεια μιας περιόδου αρκετών χρόνων (1998, 2000, 2001, 2002, 2003) ο Ömer ανέπτυξε την QCL, την πρώτη πραγματική κβαντική γλώσσα προγραμματισμού, με σύνταξη αρκετά παρόμοια της C.

Μάλιστα υλοποίησε και ένα λειτουργικό προσομοιωτή της γλώσσας. Η QCL περιέχει μία πλήρη κλασική γλώσσα προγραμματισμού ως υποσύνολο και παρέχει ένα σύνολο χρήσιμων κβαντικών δομών υψηλού επιπέδου όπως διαχείριση μνήμης και αυτόματη παραγωγή ελεγχόμενων εκδόσεων τελεστών. Οι Sanders&Zuliani (2000) και Zuliani (2001) ορίζουν την προστακτική γλώσσα qQCL, η οποία βασίζεται σε μια αυστηρή γλώσσα εντολών (guarded-command language).

Συναρτησιακές γλώσσες

Ο Maymin (1996) ορίζει δύο επεκτάσεις του λ-λογισμού. Η πρώτη, ένας πιθανοτικός λ-λογισμός (λ^p-λογισμός) ενσωματώνει κατανομές όρων επιτρέποντας σε συναρτήσεις να επιστρέφουν τυχαία αποτελέσματα. Η δεύτερη, ένας κβαντικός λ-λογισμός (λ^q -λογισμός), επεκτείνει την έννοια αυτή επιτρέποντας στους όρους να αντιπροσωπεύονται και από αρνητικές κατανομές. Επομένως υπάρχει η δυνατότητα αφαιρετικής συμβολής δύο όρων όταν δύο κατανομές συνδυάζονται.

Κάτι παρόμοιο είναι δυνατό και στο μοντέλο κβαντικού υπολογισμού όπως θα δούμε σε επόμενες ενότητες. Βέβαια αυτό περιορίζει τους όρους σε διαφορές φάσεων μόνο 180°, όμως ο Maymin αποδεικνύει ότι ο λ^q -λογισμός μπορεί να λύσει με αποδοτικό τρόπο NP-πλήρη προβλήματα. Τελικά όμως φαίνεται ότι ο λογισμός αυτός είναι αυστηρά πιο εκφραστικός από το μοντέλο κβαντικού προγραμματισμού το οποίο μπορεί να υλοποιηθεί φυσικά.

Ο Van Tonder (2004) όρισε επίσης ένα κβαντικό λ-λογισμό, λ_q ,ο οποίος είναι μια γλώσσα αγνού κβαντικού προγραμματισμού, δηλαδή δεν επιτρέπονται μετρήσεις. Οι Valiron (2004a,b) και οι Valiron & Selinger (2005; 2006) ορίζουν μια συναρτησιακή γλώσσα υψηλού επιπέδου, την QPL, η οποία ακολουθεί το σχήμα «κβαντικών δεδομένων και κλασικού ελέγχου». Η γλώσσα βασίζεται στο λ-λογισμό κλήσης κατά τιμή και περιλαμβάνει τόσο κλασικά όσο και κβαντικά δεδομένα. Υπάρχει ένα γραμμικό σύστημα τύπων και αποδεικνύονται ιδιότητες διατήρησης και ασφάλειας τύπων.

Οι Altenkirch και Grattage (2005a; 2005b) μία πρώτης-τάξεως συναρτησιακή γλώσσα, την QML, στην οποία η ροή του ελέγχου όπως και τα δεδομένα μπορούν να είναι κβαντικά. Η σημασιολογία της QML ακολουθεί το παράδειγμα του Selinger (2004c) με όρους υπερτελεστών και πινάκων πυκνότητας και μία μετάφραση σε κβαντικά κυκλώματα. Ακολουθεί και αυτή γραμμικό σύστημα τύπων. Μετεξέλιξη της QML αποτελεί η γλώσσα nQML των Lampis, Ginis, Papakyriakou, Papaspyrou (2006) και η οποία είναι αυτή με την οποία θα ασχοληθούμε στην εργασία. Επιτρέπει νέες δομές ελέγχου και είναι απλούστερη χωρίς να χάνει σε εκφραστικότητα. Η σημασιολογία της μέχρι στιγμής αποτελείται μόνο από τελεστές σε πίνακες πυκνότητας και όχι από κβαντικά κυκλώματα.

Άλλες κατηγορίες γλωσσών

Πρόκειται για γλώσσες που ενσωματώνουν στοιχεία ξένα προς τις δύο προηγούμενες κατηγορίες και είναι σχετικά νέες. Για παράδειγμα οι Gay & Nagarajan (2005; 2006) ορίζουν το λογισμό διαδικασιών CQP (Communicating Quantum Processes) και οι Jorand & Larire (2004) την QPAlg (Quantum Process Algebra). Και οι δύο γλώσσες μπορούν να περιγράψουν συστήματα τα οποία συνδυάζουν κλασικό και κβαντικό υπολογισμό και επικοινωνία και ο στόχος τους

είναι να υποστηρίξουν τον φορμαλισμό του ορισμού και της επαλήθευσης κβαντικών κρυπτογραφικών πρωτοκόλλων. Ο Παπανικολάου (2004) περιγράφει συνοπτικά τον ορισμό της γλώσσας QSPEC, η οποία υποστηρίζει τις δηλώσεις ταυτόχρονων διαδικασιών, με επικοινωνία, με ένα προστακτικό στυλ βασισμένο στις γλώσσες Promela και Probmela.

4.2.1 Εισαγωγικές έννοιες.

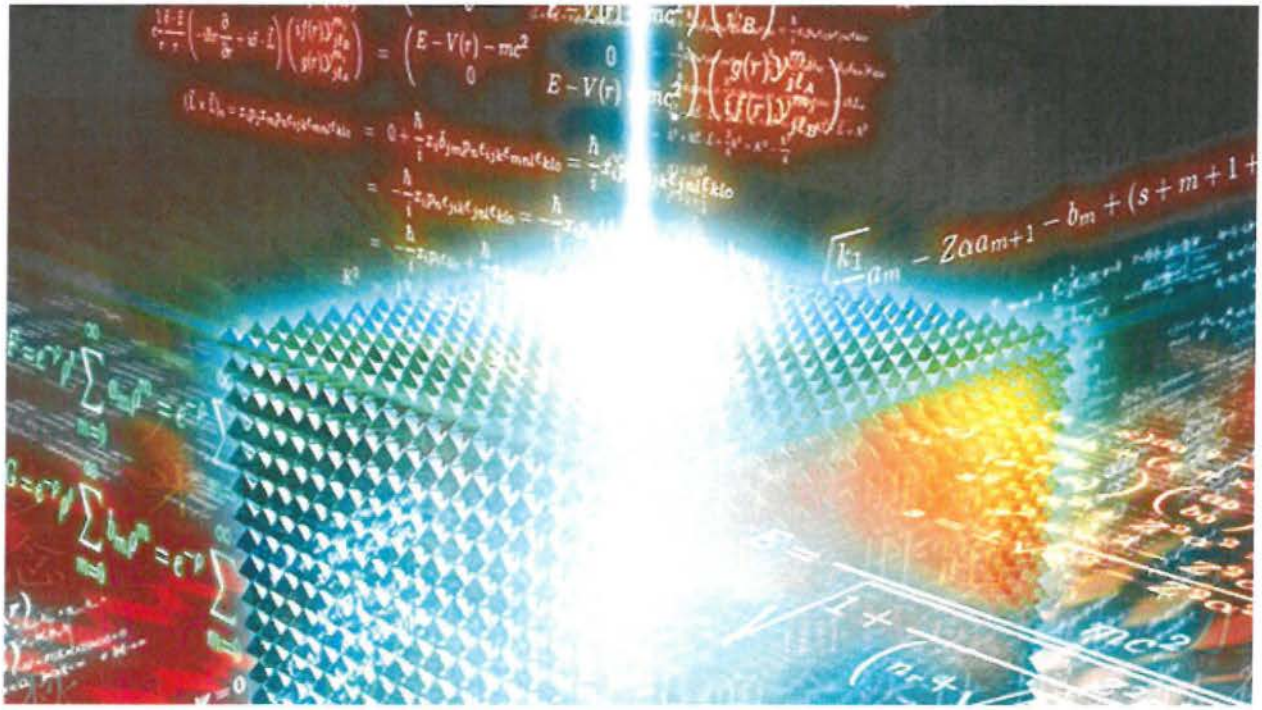
Οι κβαντικοί υπολογισμοί βασίζονται στις αρχές της κβαντομηχανικής οι οποίες είναι αντίθετες προς την κοινή λογική και εμπειρία. Εδώ θα αναφερθούμε επιγραμματικά στις αρχές οι οποίες είναι σημαντικές για τους κβαντικούς υπολογισμούς.

Η πρώτη είναι η αρχή της υπέρθεσης η οποία λέει ότι ένα κβαντικό σύστημα μπορεί να βρίσκεται σε 2 ή περισσότερες καταστάσεις ταυτόχρονα. Στο παράδειγμα των υπολογιστών ενώ ένα bit μπορεί να είναι κάθε στιγμή σε μία από τις καταστάσεις 0 ή 1, ένα κβαντικό bit (ή qubit) μπορεί να βρίσκεται και στις δύο καταστάσεις ταυτόχρονα. Αυτή η εξωτική κατάσταση εκφράζεται στη φυσική πλήρως από την κυματοσυνάρτηση του σωματιδίου, το οποίο παριστάνει το qubit. Αυτό το σωματίδιο βρίσκεται τότε σε μια υπέρθεση καταστάσεων. Η κυματοσυνάρτηση του καθορίζει πλήρως τη συμπεριφορά του.

Επομένως και ο τρόπος υπέρθεσης στην οποία βρίσκεται ένα qubit καθορίζει την μετέπειτα εξέλιξη του όπως θα δούμε παρακάτω. Σημειώνω ότι η υπέρθεση δεν είναι χαρακτηριστικό μόνο σωματιδίων αλλά και ολόκληρων συστημάτων (άλλωστε και τα σωματίδια δεν είναι στοιχειώδη). Επομένως είναι δυνατόν ένα σύστημα από qubits να βρίσκεται σε περισσότερες καταστάσεις από δύο σε αντίθεση με το μονό qubit. Για παράδειγμα μια συστοιχία n qubits μπορεί να είναι σε οποιεσδήποτε από τις καταστάσεις $\{0,1,\ldots,2^n-1\}$ ταυτόχρονα.

Η δεύτερη αρχή είναι η αρχή της κβαντικής μέτρησης. Σύμφωνα με αυτή την αρχή κατά την μέτρηση ενός κβαντικού συστήματος η κυματοσυνάρτηση «καταρρέει» και το σύστημα μεταβαίνει σε μία συγκεκριμένη κατάσταση η οποία είναι και το αποτέλεσμα της μέτρησης. Οποιεσδήποτε άλλες μετρήσεις του ίδιου μεγέθους στο

σύστημα θα δώσουν το ίδιο αποτέλεσμα. Ουσιαστικά δηλαδή από τη μέτρηση και μετά το qubit συμπεριφέρεται κλασικά. Φυσικά εδώ πρέπει να επισημάνω ότι το qubit δεν σταμάτησε να είναι κβαντικό σύστημα, απλώς το συγκεκριμένο μέγεθος του απέκτησε μια ορισμένη τιμή. Σύμφωνα με την αρχή της απροσδιοριστίας του Heisenberg άλλες ιδιότητες του παραμένουν απροσδιόριστες ή αλλιώς σε υπέρθεση.



Εικόνα 77 Quantum Art.

Οι δύο παραπάνω αρχές έχουν ελεγχθεί πειραματικά και κανένα πείραμα δεν τις έχει θέσει υπό αμφισβήτηση. Από την πρώτη πηγάζουν τα πλεονεκτήματα των κβαντικών υπολογιστών. Ένας υπολογιστής που βρίσκεται σε πολλές καταστάσεις ταυτόχρονα αυξάνει το δυνατό παραλληλισμό και μάλιστα στην περίπτωση των κβαντικών υπολογισμών έχουμε εκθετική αύξηση. Ένα qubit το οποίο είναι ταυτόχρονα 0 και 1 θα μας δώσει στο τέλος των υπολογισμών ένα αποτέλεσμα το οποίο είναι υπέρθεση των αποτελεσμάτων που θα είχαμε πάρει αν το qubit ήταν 0 ή 1. Ομοίως η πραγματοποίηση ενός υπολογισμού qubit θα μας δώσει υπέρθεση 2^n αποτελεσμάτων.

Η δεύτερη αρχή όμως μειώνει κατά πολύ την αξία αυτού του παραλληλισμού και προκαλεί τις δυσκολίες στο σχεδιασμό κβαντικών αλγορίθμων. Σύμφωνα με αυτή είναι αδύνατο να μετρήσουμε όλες τις καταστάσεις στις οποίες βρίσκεται ο υπολογιστής μας αλλά μόνο μία. Όλες οι υπόλοιπες καταστρέφονται. Τέλος όπως θα δούμε παρακάτω οι νόμοι της κβαντομηχανικής εμπεριέχουν επιπλέον περιορισμούς, όπως η αντιστρεψιμότητα, οι οποίοι δυσκολεύουν περισσότερο το σχεδιασμό των κβαντικών αλγορίθμων.

4.2.2 Κβαντικό bit (qubit).

Η πρωταρχική μονάδα δεδομένων ενός κβαντικού υπολογιστή είναι το qubit. Το κλασικό bit μπορεί να βρίσκεται όπως ξέρουμε στην κατάσταση 0 ή 1. Αντίθετα το κβαντικό bit μπορεί να βρίσκεται σε οποιαδήποτε κατάσταση της μορφής $q = a0 + b1$ όπου $a,b \in C$ και δεν είναι ταυτόχρονα 0. Δύο καταστάσεις q και q' για τις οποίες ισχύει $q = \gamma q'$ με $\gamma \in C$ είναι ισοδύναμες. Συνήθως θεωρούμε την κανονικοποίηση $|a|^2 + |b|^2 = 1$ οπότε όλες οι ισοδύναμες καταστάσεις αντιπροσωπεύονται από μία μόνο.

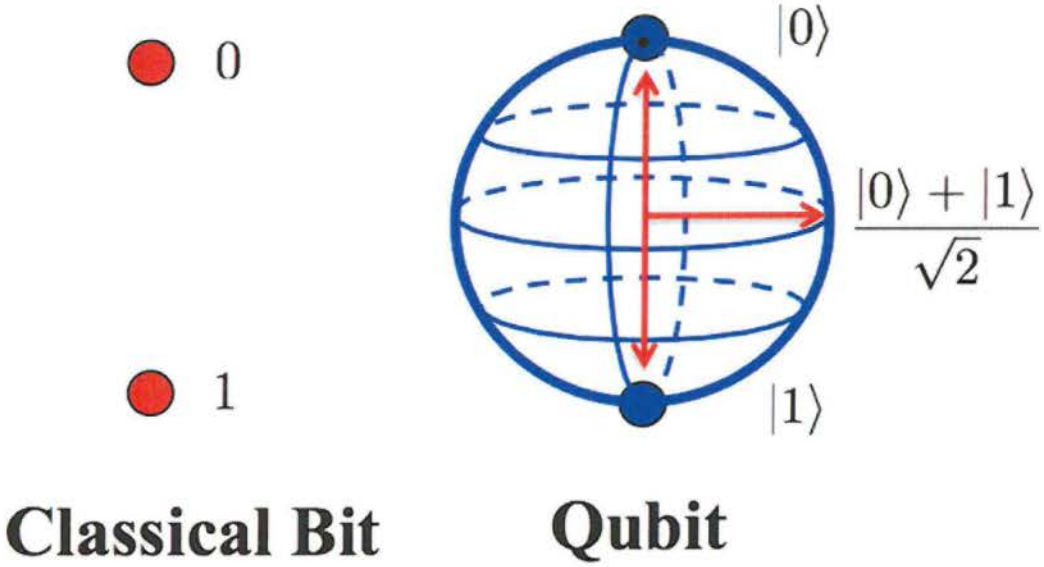
Τα a, b είναι μιγαδικοί αριθμοί και φυσικά δεν έχουν άμεση φυσική σημασία. Με την κανονικοποίηση όμως το τετράγωνο του μέτρου τους μας δίνει την πιθανότητα να μετρήσουμε την αντίστοιχη κατάσταση. Δηλαδή σε μία μέτρηση έχουμε $|a|^2$ πιθανότητα να μετρήσουμε 1 και $|b|^2$ να μετρήσουμε 0.

Σημειώνω σε αυτό το σημείο ότι ενώ δύο καταστάσεις μπορούν να δίνουν ακριβώς τα ίδια μετρήσιμα αποτελέσματα (ίδια με την έννοια της ίδιας κατανομής μετρήσεων) μπορεί να μην είναι ισοδύναμες. Για παράδειγμα οι καταστάσεις και . Μόνο με περαιτέρω επεξεργασία τους μπορούμε να ξεχωρίσουμε την μία κατάσταση από την άλλη και όχι με μετρήσεις. Μάλιστα η πρώτη μέτρηση στην κάθε κατάσταση θα καταστρέψει την υπέρθεση και όλη η πληροφορία για τα a, b θα χαθεί.

Επομένως κάθε κατάσταση ενός qubit ορίζεται μονοσήμαντα από ένα ζεύγος μιγαδικών αριθμών και άρα πρόκειται για διανύσματα στο χώρο $C \times C$. Η βάση

αυτού του χώρου είναι τα διανύσματα $\binom{1}{0}$ και $\binom{0}{1}$ τα οποία συμβολίζουν τις καταστάσεις 0 και 1 αντίστοιχα. Αυτές οι καταστάσεις ονομάζονται κλασικές καταστάσεις καθώς ένα κλασικό bit βρίσκεται σε μία από τις δύο.

Στη βιβλιογραφία οι καταστάσεις των qubits συμβολίζονται ως |q› και οι δύο σταθερές καταστάσεις που αποτελούν και την βάση του χώρου ως |1› και |0› . Όλες οι υπόλοιπες καταστάσεις αποτελούν υπέρθεση αυτών των δύο. Ο παραπάνω συμβολισμός ονομάζεται bracket notation ή Dirac notation και τα παραπάνω διανύσματα ονομάζονται ket. Υπάρχουν και bra τα οποία συμβολίζονται ως ‹q| και είναι τα αναστροφοσυζυγή των προηγουμένων.



Εικόνα 78 Qubit vs Bit

Στην περίπτωση του κβαντικού υπολογιστή λοιπόν, το bit ως φυσικό αντικείμενο είναι ένα κβαντικό σύστημα, ένα quantum bit, και κατά σύντμηση qubit. Ελληνική απόδοση κβαντικό-δυφίο ή, απλούστερα, κβαντο-δυφίο. Η μνήμη του υπολογιστή του κβαντικού στην περίπτωσή μας θα αποτελείται, βέβαια, όχι μόνο από ένα qubit ένα κβαντο-δυφίο αλλά από έναν επαρκή αριθμό από αυτά, τοποθετημένα σχετικά κοντά, αλλά όχι πολύ κοντά, ώστε να είναι δυνατός ο ανεξάρτητος «έλεγχός» τους με κατάλληλα εξωτερικά πεδία. Στην απλή περίπτωση ενός κβαντικού υπολογιστή με δύο κβαντο-δυφία οι δυνατές καταστάσεις του συστήματος θα είναι, προφανώς, οι

$$|00> \equiv |0>|0> \quad , \qquad |01> \equiv |0>|1>>$$

$$|10> \equiv |1>|0> \quad , \qquad |11> \equiv |1>|1>>$$

και θα αποτελούν μια πλήρη βάση στον τετραδιάστατο πλέον χώρο των δύο κβαντοδυφίων. Η γενική κατάσταση της μνήμης ή του καταχωρητή (register) όπως επίσης λέγεται θα περιγράφεται από την επαλληλία

όπου, βέβαια, η τετραγωνισμένη απόλυτη τιμή καθενός από τους παραπάνω συντελεστές θα δίνει την πιθανότητα να βρούμε τον καταχωρητή στην αντίστοιχη κβαντική κατάσταση. Και θα είναι, βεβαίως,

$$\sum_{\alpha,\beta} |c_{\alpha,\beta}|^2 = 1 \quad \alpha,\beta \in \{0,1\},$$

όπου {0, 1} το (διμελές) σύνολο των δύο ψηφίων 0 και 1.

Για έναν κβαντικό υπολογιστή με N θέσεις μνήμης το τυχόν στοιχείο της υπολογιστικής βάσης έτσι αποκαλούνται τα βασικά διανύσματα της μορφής |011 ... > ≡ |0>|1>|1> ... κ.λπ. θα γράφεται ως

όπου $x_1, x_2, \ldots, x_N$ είναι οι δυαδικές μεταβλητές για την κάθε θέση μνήμης το

κάθε κβαντοδυφίο και το x ένας πυκνός συμβολισμός για τη νιάδα $x_1, \ldots, x_N$.

Δηλαδή $x \equiv x_1, \ldots, x_N$. Η γενική κβαντική κατάσταση της μνήμης (ή του καταχωρητή) θα γράφεται λοιπόν ως

με συνθήκη κανονικοποίησης την

$$\sum_x |c_x|^2 = 1.$$

Ως προς τη διάσταση αυτού του χώρου, δηλαδή το πλήθος των βασικών του διανυσμάτων

$$, |x_i 1, \ldots, x_i N> \equiv |x_i 1> \; |x_i 2>, \ldots, |x_i N> ,$$

αυτή θα ισούται, προφανώς, με

$$D = 2^N,$$

αφού τόσοι είναι οι συνδυασμοί δύο βασικών διανυσμάτων από το πρώτο κβαντοδυφίο με δύο από το δεύτερο, δύο από το τρίτο κ.ο.κ. Ακόμα και με έναν πολύ μικρό αριθμό κβαντοδυφίων (π.χ. N = 200) ασήμαντο με τα μέτρα ενός κλασικού υπολογιστή η διάσταση αυτού του χώρου είναι εξωφρενική. Δεδομένου ότι $2^n \approx 10^{n/2,3}$ θα είναι

$$D = 2^{200} \approx 10^{200/2,3} \approx 10^{87},$$

που είναι ένας αριθμός μεγαλύτερος από τον αριθμό των υλικών σωματιδίων όλου του ορατού σύμπαντος! Πρόκειται, βέβαια, για τον ίδιο εκθετικό νόμο που επισημάναμε και στην εισαγωγή, αλλά με d = 2, αφού τώρα τα σωματίδιά μας (≡ τα κβαντοδυφία) θεωρούνται ως δικαταστασιακά συστήματα και άρα ο χώρος Hilbert του καθενός έχει διάσταση δύο.

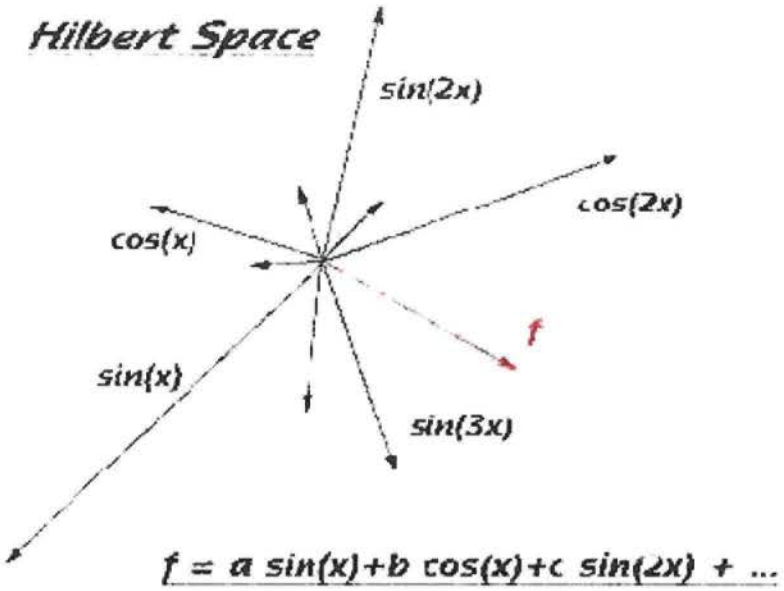
Βρισκόμαστε έτσι ξανά μπροστά στις εκπληκτικές σχεδόν αδιανόητες δυνατότητες του κβαντικού υπολογιστή. Πάνω σε έναν υπολογιστή με διακόσιες μόνο θέσεις μνήμης μπορεί να «φορτωθεί» και να γίνει αντικείμενο επεξεργασίας πληροφορία 2^{200} bit≡ 2^{200} δυφίων. Σαφώς περισσότερη από ότι σε όλα τα υλικά σωματίδια του σύμπαντος, αν θεωρηθούν ως κλασικές θέσεις μνήμης ως κλασικά δυφία.

Και ο λόγος γι' αυτό αξίζει να αναλυθεί και από μια διαφορετική γωνία, που φωτίζει πολύ καλύτερα τη βασική αρχή λειτουργίας του κβαντικού υπολογιστή. Το βασικό γεγονός είναι η δυνατότητα των κβαντικών δυφίων να υπάρχουν σε καταστάσεις επαλληλίας της μορφής ($|\psi> = \alpha|0> + \beta|1>$) και επομένως να είναι και «πάνω» και «κάτω» ταυτόχρονα. Δηλαδή να μπορούν να καταχωρούν και να διαχειρίζονται και το 0 και το 1 ταυτόχρονα. Αφού όμως η χωρητικότητα του κάθε κβαντοδυφίου είναι ίση με δύο, η χωρητικότητα των δύο κβαντοδυφίων θα είναι ίση με $2^2 = 4$ όσοι είναι οι συνδυασμοί ενός ψηφίου (0 ή 1) από το πρώτο κβαντοδυφίο και ενός από το δεύτερο και, βέβαια, ίση με 2N για N κβαντοδυφία. Η προέλευση του εκθετικού νόμου είναι τώρα τελείως φανερή και πολύ αποκαλυπτική για τις δυνατότητες του κβαντικού υπολογιστή.

Πώς μπορεί ένα κβαντοδυφίο, στην κατάσταση επαλληλίας $\alpha|0> + \beta|1>$, να κρατάει και να διαχειρίζεται ταυτόχρονα και το $|0>$ και το $|1>$, αφού σε μια μέτρηση μόνο η μία από τις δύο καταστάσεις θα βρεθεί ότι υπάρχει; Και η απάντηση είναι βέβαια γνωστή. Πράγματι με τη μέτρηση το κβαντοδυφίο θα καταρρεύσει στη μία ή την άλλη από τις καταστάσεις $|0>$ ή $|1>$.

Όμως ουδεμία τέτοια μέτρηση πραγματοποιείται στη διάρκεια ενός υπολογισμού. Έτσι το κβαντοδυφίο όλα τα κβαντοδυφία παραμένουν συνεχώς σε διάφορες καταστάσεις επαλληλίας, οπότε το υπολογιστικό πρόγραμμα εκτελείται ταυτόχρονα ή «παράλληλα» και για τις δύο τιμές της δυαδικής μεταβλητής του κάθε κβαντοδυφίου. Το φαινόμενο αυτό δηλαδή η παράλληλη εκτέλεση του προγράμματος για όλες τις ενδεχόμενες καταστάσεις των κβαντοδυφίων είναι γνωστό ως μαζικός κβαντικός παραλληλισμός και αποτελεί τον θεμελιώδη μηχανισμό λειτουργίας ενός κβαντικού υπολογιστή. Και σε αυτόν τον, καθαρά κβαντικό, μηχανισμό οφείλεται βέβαια η τερατώδης υπολογιστική ικανότητα αυτής της μοναδικής μηχανής!

Υπάρχει όμως και μια άλλη απορία που πρέπει να απαντηθεί πριν ο αναγνώστης αισθανθεί ότι αρχίζει να καταλαβαίνει κάπως το πώς μπορεί να δουλεύει και να δίνει απαντήσεις ένας κβαντικός υπολογιστής. Η απορία είναι πολύ στοιχειώδης. Στον κλασικό υπολογιστή η απάντηση είναι γραμμένη στον καταχωρητή ως μια αλυσίδα 0 και 1 πάνω στα διαδοχικά δυφία του. Δηλαδή ως ένα ψηφιακό μήνυμα που μπορεί να είναι ένας αριθμός, ένα ψηφιοποιημένο κείμενο ή οτιδήποτε άλλο. Τι γίνεται όμως με τον κβαντικό υπολογιστή του οποίου οι θέσεις μνήμης μπορεί να βρίσκονται και συνήθως βρίσκονται σε καταστάσεις επαλληλίας με κάποια πιθανότητα να είναι μηδέν ή να είναι ένα; Οπότε το πλήθος των δυνατών μηνυμάτων θα είναι επίσης 2^N, όπως πριν. Τι κάνουμε τότε; Θα μετρήσουμε μια φορά όλα τα κβαντοδυφία και. . . ότι προκύψει; Ή θα μετράμε συνέχεια έως το. . . τέλος του κόσμου; Και όταν. . . τελειώσουμε, ποια απ' όλες τις 2^N αλυσίδες ψηφίων 0 και 1 θα θεωρήσουμε ότι αποτελεί την απάντηση στο πρόβλημά μας;



Εικόνα 79 Χώρος Hilbert.

Αντιλαμβάνεστε, βεβαίως, ότι αν δεν δώσουμε μια ικανοποιητική απάντηση στο ερώτημα αυτό, τότε η όλη ιδέα του κβαντικού υπολογιστή δεν θα είναι απλώς μια χίμαιρα αλλά μια καθαρή ανοησία. Ένα υπέροχο μηχάνημα που θα μας κάνει εκθετικά γρήγορα τις πράξεις αλλά θα απαιτεί μετά εκθετικά μεγάλο χρόνο για να διαβαστεί το αποτέλεσμα· αν διαβαστεί ποτέ!

Ευτυχώς τα πράγματα δεν είναι ακριβώς έτσι. Πρώτα απ' όλα η απάντηση δεν χρειάζεται να είναι τόσο μακροσκελής όσο η μνήμη του υπολογιστή. Σε πολλά προβλήματα η απάντηση που ζητάμε μπορεί να είναι μόνο ένα ΝΑΙ ή ένα ΟΧΙ. Όπως, παραδείγματος χάριν, όταν θέλουμε απλώς να μάθουμε αν ένας δεδομένος μεγάλος αριθμός είναι πρώτος ή όχι. Το πρόβλημα αυτό είναι αφάνταστα δύσκολο στην πραγματικότητα άλυτο με τους κλασικούς υπολογιστές και σίγουρα θα απαιτεί όλες τις δυνατότητες της μνήμης ενός κβαντικού υπολογιστή. Όμως το αποτέλεσμα είναι ένα ΝΑΙ ή ένα ΟΧΙ που μπορεί να καταχωρηθεί μόνο στο πρώτο κβαντοδυφίο της μνήμης: Αν η απάντηση είναι ΝΑΙ το κβαντοδυφίο να βγαίνει ως μέρος της αλγοριθμικής διαδικασίας στην κατάσταση |0> και αν είναι ΟΧΙ, στην κατάσταση |1>.

Οπότε δεν έχουμε παρά να μετρήσουμε αυτό μόνο το κβαντοδυφίο και να πάρουμε αμέσως την απάντηση που ζητάμε. Και αν δεν είμαστε βέβαιοι λόγω

συσσώρευσης σφαλμάτων ότι το κβαντοδυφίο εξόδου ήταν πράγματι στην κατάσταση που μετρήσαμε, δεν έχουμε παρά να «ξανατρέξουμε» το πρόγραμμα όσες φορές χρειαστεί και να επαναλάβουμε τη μέτρηση ώστε να περιορίσουμε το ενδεχόμενο σφάλματος κάτω από ένα ανεκτό επίπεδο. Και συνειδητοποιούμε έτσι, με αυτή την ευκαιρία, κάτι που ίσως θα έπρεπε να μας είναι προφανές από την αρχή. Ότι δηλαδή ο κβαντικός υπολογιστής δεν είναι μια ντετερμινιστική μηχανή. Εμπεριέχει ένα στοιχείο τυχαιότητας που όμως μπορεί να τεθεί υπό έλεγχο ώστε το αποτέλεσμα να πλησιάζει την πρακτική βεβαιότητα.

Θα κλείσουμε τούτη την παράγραφο με μια σύντομη αναφορά στις λεγόμενες καταστάσεις Bell που ορίζονται μέσω των σχέσεων

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

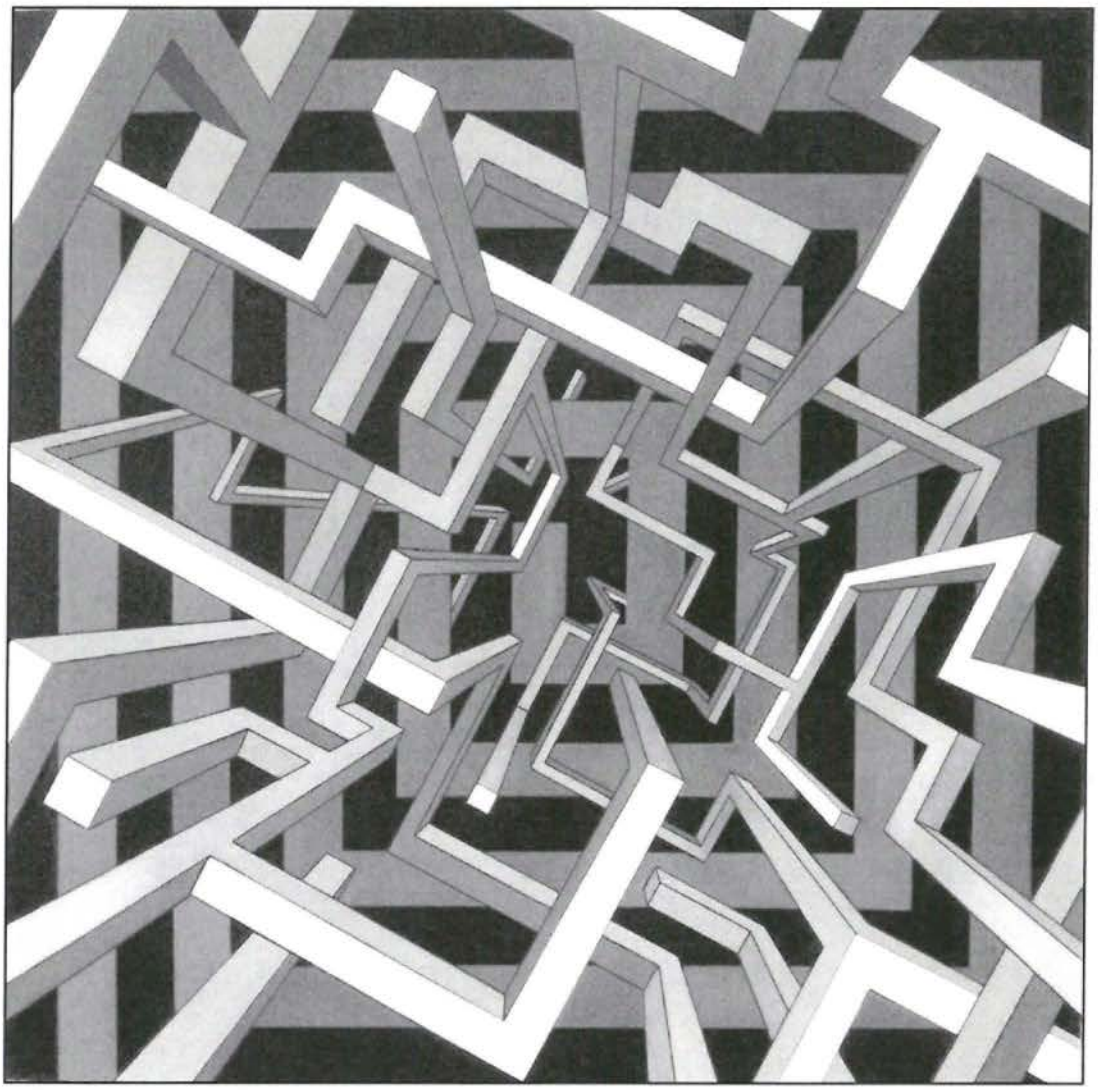
$$|B_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \qquad |B_{11}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

Εικόνα 80 Καταστάσεις Bell

από όπου είναι προφανές ότι: α) Πρόκειται για καταστάσεις δύο κβαντοδυφίων και επειδή ο χώρος αυτός είναι τετραδιάστατος μπορούν να θεωρηθούν και ως μια διαφορετική εκλογή βάσης σε αυτό τον χώρο έναντι της τετράδας |00>, |01>, |10>, |11>. Επιπλέον όπως είναι εύκολο να δείτε οι καταστάσεις, είναι αμοιβαία ορθογώνιες (και βεβαίως κανονικοποιημένες), οπότε μπορούν να θεωρηθούν ως μια άλλη ορθοκανονική βάση σε αυτό τον χώρο. β) Από φυσικής πλευράς είναι επίσης φανερό ότι οι καταστάσεις (15.2) είναι σύμπλεκτες καταστάσεις και σ' αυτό, βέβαια, οφείλεται η ονομασία τους, αφού ο Bell είναι εκείνος που ανέδειξε τη θεμελιώδη σημασία των καταστάσεων αυτού του τύπου. Σημειώστε ειδικότερα ότι για κβαντοδυφία που πραγματώνονται μέσω των δύο καταστάσεων σπιν $|\uparrow\rangle$ και $|\downarrow\rangle$ σπιν πάνω και σπιν κάτω αντίστοιχα θα είναι $|0\rangle \equiv |\uparrow\rangle$, $|1\rangle \equiv |\downarrow\rangle$

οπότε η κατάσταση Bell $|B_{10}\rangle$ θα γράφεται ως

και σε αυτή τη μορφή αναγνωρίζεται αμέσως ως η περίφημη κατάσταση EPR. Όπως θα δούμε στη συνέχεια του κεφαλαίου η κβαντική σύμπλεξη θα αποτελέσει συστατικό στοιχείο της λειτουργίας ενός κβαντικού υπολογιστή και ειδικότερα των τηλεπικοινωνιακών εφαρμογών του και της κβαντικής κρυπτογραφίας. Και σε αυτό το πλαίσιο οι καταστάσεις Bell θα αναδειχτούν σε ένα θεμελιώδες εργαλείο.



Εικόνα 81 Παράδειγμα χώρου Hilbert.

4.2.3 Βασικές αρχές.

Τέσσερις είναι οι βασικές αρχές που διέπουν την κβαντική θεωρία :

1. Η κβαντική κατάσταση ενός κλειστού κβαντικού συστήματος (π.χ. στοιχειώδες σωμάτιο όπως το ηλεκτρόνιο) περιγράφεται από ένα διάνυσμα μέσα σε διανυσματικό χώρο Η στο σύνολο των μιγαδικών αριθμών C. Στο χώρο αυτό, που ονομάζεται χώρος Hilbert, ορίζεται το εσωτερικό γινόμενο μεταξύ δύο διανυσμάτων $|\psi\rangle$, $|x\rangle$ ως συνάρτηση από το HxH→C:

Όπου το t σημαίνει ερμιτιανό ανάστροφο.

2.Σε κάθε φυσικό μέγεθος αντιστοιχεί και ένας γραμμικός μετασχηματισμός στο χώρο Hilbert. Συμβολίζεται συνήθως με κεφαλαίο γράμμα και <<καπέλο>> (π.χ. $\hat{A}$). Ο γραμμικός τελεστής που αντιστοιχεί σε φυσικά μεγέθη πρέπει να είναι Ερμιτιανός τελεστής, δηλ. να ισχύει:

$$\hat{A}^t=\hat{A}.$$

Ο λόγος γι' αυτό είναι ότι μόνο οι ερμιτιανοί τελεστές έχουν πραγματικές ιδιοτιμές κάτι που είναι απαραίτητη προϋπόθεση για ένα φυσικό μέγεθος.

3. Το αποτέλεσμα μίας μοναδικής μέτρησης ενός φυσικού μεγέθους Α σε ένα κβαντικό σύστημα που βρίσκεται σε μία κατάσταση $|\psi\rangle$ μπορεί να είναι μόνο μία από τις ιδιοτιμές του αντίστοιχου γραμμικού τελεστή Α του φυσικού μεγέθους. Αμέσως μετά τη μέτρηση το κβαντικό σύστημα καταρρέει σε μία νέα κατάσταση η οποία είναι το αντίστοιχο ιδιοδιάνυσμα του γραμμικού τελεστή. Για να βρούμε τις ιδιοτιμές και τα ιδιοδιανύσματα του Α λύνουμε την εξίσωση:

$$A|\psi\rangle = \lambda|\psi\rangle.$$

Όπου λ οι ιδιοτιμές και ψ το αντίστοιχο ιδιοδιάνυσμα.

4.Η πιθανότητα να ληφθεί μία από τις ιδιοτιμές λ_i ενός τελεστή ως αποτέλεσμα μίας μοναδικής μέτρησης πάνω σε κβαντικό σύστημα που βρίσκεται σε μία γενική κατάσταση ψ δίνεται από το τετράγωνο του μέτρου της προβολής της ψ πάνω στο αντίστοιχο ιδιοδιάνυσμα $|e_i\rangle$ του τελεστή:

$$P(\lambda_i) = |\langle ei\ |\psi\rangle|^2.$$

4.2.4 Κβαντικές Πύλες.

Όπως θα έπρεπε να το περιμένουμε, η λειτουργία ενός κβαντικού υπολογιστή δηλαδή η εκτέλεση ενός υπολογιστικού προγράμματος για έναν συγκεκριμένο σκοπό θα γίνεται με κατάλληλους χειρισμούς πάνω στα κβαντοδυφία που συγκροτούν τη μνήμη του ή τον καταχωρητή του όπως έχει επίσης καθιερωθεί να λέγεται.

Και επειδή τα κβαντοδυφία είναι, βεβαίως, κβαντικά αντικείμενα, ο χειρισμός τους δηλαδή η πρόκληση των επιθυμητών αλλαγών στην κατάστασή τους θα γίνεται με τις δύο μόνες διαδικασίες που προβλέπει η κβαντική θεωρία. Τη μοναδιαία εξέλιξη μέσω της εξισώσεως Schrödinger που προκαλείται κυρίως με τη δράση κατάλληλων ηλεκτρομαγνητικών παλμών καθώς και τη διαδικασία της μέτρησης που δεν είναι μοναδιαία όπως γνωρίζουμε, αλλά διέπεται από την αρχή της κατάρρευσης του καταστασιακού διανύσματος.

Επειδή όμως, πλην ειδικών εξαιρέσεων, η μέτρηση εκτελείται στο τέλος της υπολογιστικής διαδικασίας (και αποσκοπεί κυρίως στην ανάγνωση του αποτελέσματος) οι δυνατοί χειρισμοί επί των κβαντοδυφίων θα πρέπει να είναι υποχρεωτικά μοναδιαίοι και σε αυτούς πράγματι θα περιορίσουμε τις επιλογές μας στη συνέχεια.

Ως προς την ορολογία, ο καθιερωμένος όρος γι' αυτές τις μοναδιαίες «πράξεις» είναι κβαντικές πύλες ή απλώς πύλες, όπως και στους κλασικούς υπολογιστές. Και είναι σημαντικό να υπογραμμίσουμε από την αρχή ένα βασικό γεγονός πάνω στο οποίο βασίζεται όλο το κυκλωματικό μοντέλο (circuit model) των υπολογιστών, κλασικών και μη. Ότι αρκεί ένας μικρός αριθμός στοιχειωδών πυλών δηλαδή απλών μοναδιαίων τελεστών για να υλοποιηθεί μέσω αυτών (έστω προσεγγιστικά)

κάθε δυνατός μοναδιαίος μετασχηματισμός επί του συνόλου των κβαντοδυφίων του καταχωρητή.

Ακόμα πιο συγκεκριμένα: Αρκεί ένας μικρός αριθμός πυλών που δρουν μόνο πάνω σε ένα κβαντοδυφίο, σε συνδυασμό με μία μόνο πύλη που δρα σε δύο κβαντοδυφία. Οπότε, βεβαίως, οι πρώτες πύλες θα αναπαρίστανται από μοναδιαίες μήτρες διαστάσεως 2 × 2 και η δεύτερη (με τις γενικεύσεις της) από μια αντίστοιχη μήτρα διαστάσεως 4 × 4. Θα αρχίσουμε τη μελέτη μας με την πρώτη κατηγορία πυλών.

Όπως είπαμε πριν οι πύλες αυτού του τύπου δρουν πάνω στις καταστάσεις ενός μόνο κβαντοδυφίου, δηλαδή στον δισδιάστατο χώρο των διανυσμάτων $\alpha|0> + \beta|1>$, και επομένως θα αναπαρίστανται από μοναδιαίες μήτρες της ίδιας διάστασης δηλαδή 2 × 2 όπως στον κατάλογο που ακολουθεί. Όπου παρατίθεται επίσης το όνομα και το κυκλωματικό σύμβολο της κάθε πύλης.

Οι βασικές μονοδυφιακές πύλες

Μονάδα	I	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Hadamard	H	$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
Pauli X	X	$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Pauli Y	Y	$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$
Pauli Z	Z	$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Φάση S	S	$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$

Εικόνα 82 Βασικές μονοδυφιακές πύλες.

Σημειώστε κατ' αρχάς ως πρώτη παρατήρηση πάνω στον κατάλογο αυτό ότι οι τρεις πύλες X, Y και Z και οι αντίστοιχες μήτρες δεν είναι παρά οι γνωστές μας

μήτρες του Pauli σ_x, σ_y και σ_z που είναι ταυτόχρονα ερμιτιανές και μοναδιαίες λόγω της γνωστής τους ιδιότητας να είναι

$\sigma^2_x = \sigma^2_y = \sigma^2_z = 1$. Ερμιτιανή και μοναδιαία είναι επίσης και η πύλη Hadamard αφού ισχύει και γι' αυτήν ότι H2 = 1. Μεταξύ άλλων αυτό συνεπάγεται ότι η διπλή δράση αυτών των πυλών επαναφέρει το κβαντοδυφίο στην αρχική του κατάσταση. Ως προς το αποτέλεσμα της «μονής» δράσης των παραπάνω πυλών είναι χρήσιμο να σημειώσουμε τα εξής:

- Για την πύλη Hadamard: Με βάση τη δεδομένη μήτρα θα έχουμε:

$$H|0> = 1/\sqrt{2}(|0> + |1>) \equiv |+>$$

$$H|1> = 1/\sqrt{2}(|0> - |1>) \equiv |->$$

από όπου είναι φανερός και ο ρόλος αυτής της πύλης: Δημιουργεί ισοβαρείς επαλληλίες των βασικών καταστάσεων |0> και |1>, οι οποίες είναι αναγκαίες για την αποτελεσματική αξιοποίηση των δυνατοτήτων ενός κβαντικού υπολογιστή, όπως θα δούμε σε λίγο.

- Για την πύλη X: Εδώ θα έχουμε:

$$X|0> = |1> , X|1> = |0>$$

που σημαίνει ότι η πύλη αυτή αναστρέφει την κατάσταση του κβαντοδυφίου μετατρέποντας το 0 σε 1 και το 1 σε 0. Κάνει δηλαδή ότι και η κλασική πύλη NOT που οφείλει το όνομά της ακριβώς στο γεγονός ότι λέει «ΟΧΙ» στην εκάστοτε κατάσταση του δυφίου μετασχηματίζοντάς την στην αντίθετή της. Ένας συμπαγής συμβολισμός γι' αυτή τη δράση είναι ο

$$X|x> = |\bar{x}> ,$$

όπου, x = (0, 1) η συνήθης δυαδική μεταβλητή και x = (1, 0) το ανεστραμμένο είδωλό της όπου η παύλα πάνω από το x παραπέμπει εύλογα στο καθιερωμένο σύμβολο για το αντισωματίδιο. Ανάλογα απλή είναι και η δράση των άλλων πυλών πάνω στα κβαντοδυφία και περιοριζόμαστε στην απλή καταγραφή της:

- Πύλη Y

$$Y|0> = i|1>, Y|1> = -i|0>.$$

❖ Πύλη Z

$$Z|0> = |0>, Y|1> = -|1>.$$

❖ Πύλη S

$$S|0> = |0>, S|1> = i|1>.$$

ενώ, βέβαια, για την τυχούσα κατάσταση υπέρθεσης θα έχουμε:

$$X(a|0> + \beta|1>) = \beta|0> + \alpha|1>$$

$$Y(a|0> + \beta|1>) = -i\beta|0> + i\alpha|1>$$

$$Z(a|0> + \beta|1>) = \alpha|0> - \beta|1>$$

$$S(a|0> + \beta|1>) = \alpha|0> + \iota\beta|1>$$

και για την πύλη Hadamard

$$H(\alpha|0> + \beta|1>) = \frac{1}{\sqrt{2}}((\alpha + \beta)|0> + (\alpha - \beta)|1>).$$

4.2.5 Πύλη CNOT.

Πύλες που δρουν σε δύο κβαντοδυφία

Η βασική πύλη αυτού του είδους είναι γνωστή ως

$$\text{Controlled-NOT} \equiv \text{CNOT}$$

και η δράση της πάνω σε μια τυχούσα κατάσταση $|x, y> \equiv |x> |y>$ περιγράφεται από τις σχέσεις

$$\text{CNOT } |0|y> = |0|y>, \text{ CNOT } |1|y> = |1|\bar{y}>$$

που γράφονται επίσης ως

$$|0\rangle|y\rangle \xrightarrow{\text{CNOT}} |0\rangle|y\rangle, \qquad |1\rangle|y\rangle \xrightarrow{\text{CNOT}} |1\rangle|\overline{y}\rangle$$

και μας λένε το εξής απλό. Ότι αν το πρώτο κβαντοδυφίο είναι στην κατάσταση |0 η πύλη CNOT δεν κάνει τίποτε στο δεύτερο, ενώ αν το πρώτο είναι στην κατάσταση |1 η πύλη CNOT αναστρέφει το δεύτερο. Το πρώτο κβαντοδυφίο είναι επομένως το κβαντοδυφίο ελέγχου (control qubit) ενώ το δεύτερο είναι το κβαντοδυφίο-στόχος (target qubit) και σε αυτόν τον τρόπο δράσης οφείλεται, βεβαίως, η ονομασία αυτής της πολύ σημαντικής πύλης. Ως προς την αναπαράστασή της υπό μορφήν μήτρας, δείξτε μόνοι σας ότι θα είναι:

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

όπου στην πάνω αριστερή γωνία υπάρχει η 2 × 2 ταυτοτική μήτρα που αντιπροσωπεύει, βεβαίως, τη δράση της CNOT στο πρώτο κβαντοδυφίο ενώ στην κάτω δεξιά γωνία είναι η μήτρα X ≡ NOT που αντιπροσωπεύει επίσης τον τρόπο δράσης της CNOT πάνω στο δεύτερο κβαντοδυφίο. Σημειώστε ακόμα ότι η δράση της πύλης CNOTπάνω στην τυχούσα κατάσταση |x, y> μπορεί να γραφεί στη συμπαγή μορφή :

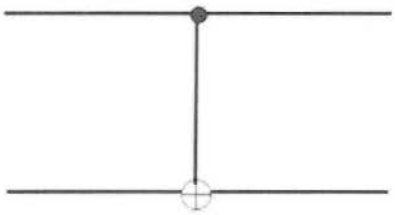
$$\text{CNOT}\,|x, y\rangle = |x, y \oplus x\rangle,$$

όπου το σύμβολο ⊕ δηλώνει την πρόσθεση modulo 2, που δεν είναι παρά η συνήθης πρόσθεση ακεραίων αλλά με «αφαίρεση» από το άθροισμα των πολλαπλασίων του δύο. Έτσι το αποτέλεσμα είναι πάντα 0 ή 1 και άρα πρόκειται για το είδος της πρόσθεσης που ταιριάζει σε ένα δυαδικό σύστημα όπου μόνο τα ψηφία 0 και 1 είναι δεκτά. Τρία απλά παραδείγματα είναι τα εξής:

$$1 \oplus 1 = 0, 3 \oplus 2 = 1, 2 \oplus 2 = 0.$$

Ως προς τον κυκλωματικό συμβολισμό της, η πύλη CNOT θα διαφέρει βεβαίως από τις πύλες που εξετάσαμε προηγουμένως που δηλώνονταν με ένα ευθύγραμμο τμήμα και το σύμβολο της πύλης στο μέσον του εφόσον τώρα τα εμπλεκόμενα κβαντοδυφία είναι δύο και άρα θα απαιτούνται δύο ευθείες γραμμές. Πράγματι το καθιερωμένο κυκλωματικό σύμβολο για την CNOT είναι το:

CNOT



όπου η βαρεία τελεία δηλώνει το κβαντοδυφίο ελέγχου και το «σταυρωμένο» κυκλάκι το κβαντοδυφίο-στόχο. Μια θεμελιώδης νέα δυνατότητα που μας παρέχει η πύλη CNOT είναι η σύμπλεξη καταστάσεων που ήταν ασύμπλεκτες πριν τη δράση της. Ένα απλό σχετικό παράδειγμα παρέχεται από την (εμφανώς ασύμπλεκτη) αρχική κατάσταση:

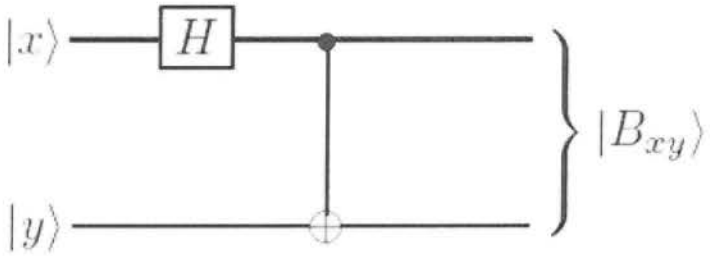
$$|\Psi_{IN}> = (\alpha|0> + \beta|1>)\,|1>$$

στην οποία το πρώτο κβαντοδυφίο είναι στην κατάσταση επαλληλίας $\alpha|0> + \beta|1>$ ενώ το δεύτερο στην κατάσταση βάσης $|1>$. Δρώντας τώρα με την CNOT στην παραπάνω σχέση παίρνουμε :

$$\text{CNOT}\,|\Psi_{IN}> = \alpha|0>|1> + \beta|1>\,|0>$$

που είναι τώρα μια σύμπλεκτη κατάσταση αφού δεν μπορεί πλέον να γραφεί ως γινόμενο καταστάσεων των δύο κβαντοδυφίων αλλά μόνο ως γραμμικός συνδυασμός τέτοιων γινομένων. Ειδικότερα για $\alpha = \beta =$ γράφεται παραπάνω πρόταση γράφεται ως :

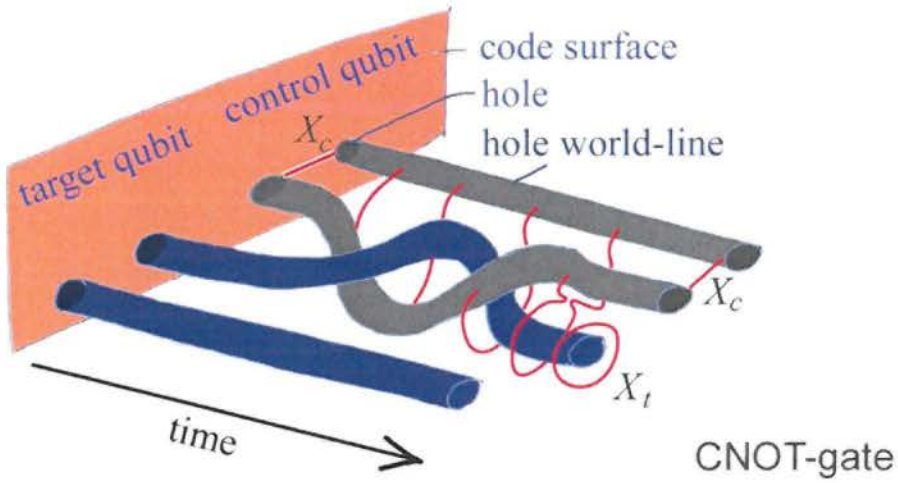
και δεν είναι παρά η κατάσταση Bell $|B_{01}>$ στην οποία είχαμε αναφερθεί λίγο νωρίτερα. Σημειώστε ακόμα ότι όχι μόνο η $|B_{01}>$ αλλά και οι άλλες καταστάσεις Bell $|B_{xy}>$ μπορούν να δημιουργηθούν με τον ίδιο τρόπο και η σχετική «κατασκευή» φαίνεται στο κύκλωμα που ακολουθεί.



Έτσι, παραδείγματος χάριν, με κατάσταση εισόδου $|0|0 \equiv |00$ προκύπτει ως έξοδος η κατάσταση Bell

και παρόμοια για τις άλλες καταστάσεις.

Όπως θα το περίμενε κανείς η Controlled-NOT ≡ CNOT είναι το αρχέτυπο μιας κατηγορίας πυλών του τύπου Controlled-U ≡ C-U ≡ CU, όπου τη θέση του NOT ≡ X την παίρνει μια οποιαδήποτε άλλη πύλη U που δρα πάνω στο κβαντοδυφίο-στόχο. Και βέβαια το κυκλωματικό σύμβολο θα είναι:



Εικόνα 83 Πύλη CNOT.

4.2.6 Κβαντική διεμπλοκή (entanglement).

Κβαντική διεμπλοκή (entanglement), ονομάζεται το φαινόμενο κατά το οποίο η κατάσταση δύο ή περισσοτέρων κβαντικών bit δεν μπορεί να περιγραφεί σαν συνδυασμός των καταστάσεων του κάθε bit ξεχωριστά. Διεμπλοκή μπορεί να δημιουργηθεί από διάφορους κβαντικούς μετασχηματισμούς που διενεργούνται σε περισσότερα του ενός bit.

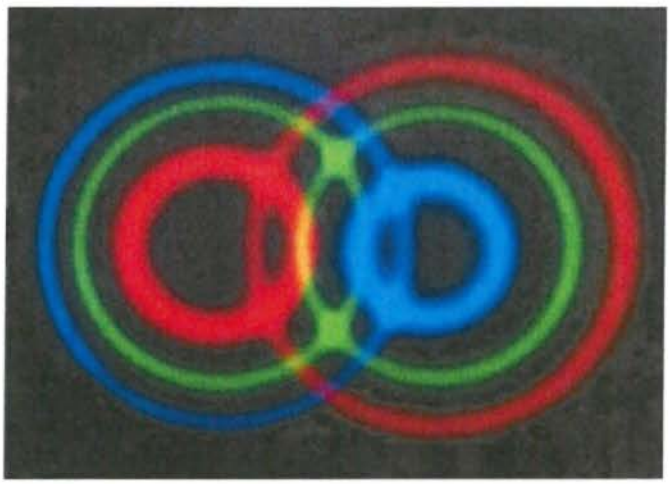
Όταν τα bit p και q είναι συμπλεγμένα ο προσδιορισμός της τιμής του ενός μας δίνει πληροφορία για την κατάσταση του άλλου. Όταν δύο κβαντικά bit δεν είναι συμπλεγμένα λέγονται ανεξάρτητα. Σε αυτή την περίπτωση η κατάσταση ενός καταχωρητή που τα περιέχει μπορεί να δοθεί αν πολλαπλασιάσουμε τους αντίστοιχους συντελεστές των δύο qubit. Μαθηματικά δηλαδή λέμε ότι δύο συστήματα βρίσκονται σε κβαντική διεμπλοκή, όταν η κατάστασή τους δεν μπορεί να γραφεί σαν τανυστικό γινόμενο των βασικών τους καταστάσεων. Αυτή η μαθηματική πρόταση αναλύεται παρακάτω με ένα παράδειγμα:

Ας θεωρήσουμε ότι έχουμε δύο qubits το $|q_{e0}>$ και το $|q_{e1}>$ τα οποία βρίσκονται στην κατάσταση $|q_e>$ που δίνεται από:

Η $|q_e>$ δεν μπορεί, όπως φαίνεται εύκολα, να γραφεί σαν τανυστικό γινόμενο των καταστάσεων των δύο qubits, οπότε τα $|q_{e0}>$ και $|q_{e1}>$ βρίσκονται σε κβαντική διεμπλοκή. Αυτό σημαίνει πως αν μετρήσουμε την κατάσταση του qubit $|q_{e1}>$ της κατάστασης $|q_e>$, θα βρούμε με πιθανότητα 0,5 ότι βρίσκεται στην κατάσταση 0 και με πιθανότητα 0,5 ότι βρίσκεται στην κατάσταση 1 . Αν το βρούμε στην κατάσταση $|0>$, τότε, αν μετρήσουμε την κατάσταση του qubit $|q_{e0}>$, θα βρούμε σίγουρα ότι βρίσκεται και αυτό στην κατάσταση $|0>$.

Αν το βρούμε στην κατάσταση $|1>$, τότε, αν μετρήσουμε την κατάσταση του qubit $|q_{e0}>$, θα βρούμε σίγουρα ότι βρίσκεται και αυτό στην κατάσταση $|1>$. Δηλαδή, αφού τα δύο qubits, βρίσκονται σε διεμπλοκή, η μέτρηση της κατάστασης του ενός qubit καθορίζει την κατάσταση του άλλου. Αυτή η απόλυτη συσχέτιση ισχύει πάντα ανεξάρτητα με τον τρόπο που γίνεται η μέτρηση (π.χ. εάν τα qubit υλοποιούνται μέσω συστήματος σπιν ½, τότε ανεξάρτητα από τον άξονα μέτρησης

του σπιν για τα δύο σωματίδια θα παίρνουμε πάντα συσχετισμένα αποτελέσματα). Η συσχέτιση ισχύει ανεξάρτητα και από την χωρική απόσταση των δύο qubits.



Εικόνα 84 Quantum Entanglement.

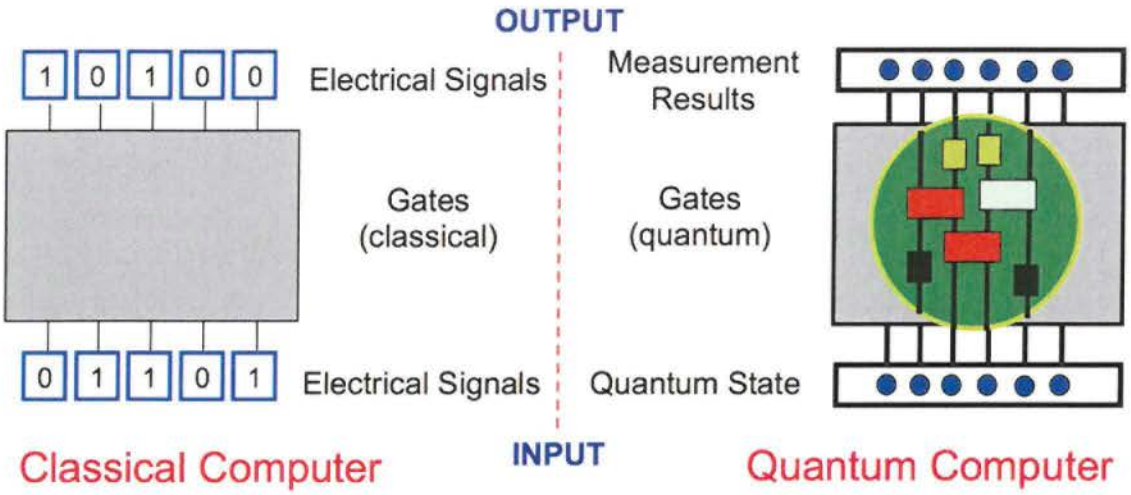
4.3.1 Προβλήματα Υλοποίησης Κβαντικού Υπολογιστή.

Τα πλεονεκτήματα των κβαντικών υπολογιστών σε σχέση με τους κλασικούς είναι τα εξής :

1. Μεγαλύτερη ταχύτητα

2. Τεράστια μνήμη

3. Δυνατότητα επίλυσης ορισμένων «υπολογιστικά δύσκολων» κλασικών προβλημάτων (προβλήματα NP) σε πολυωνυμικό χρόνο.



Εικόνα 85 Quantum vs Classical Computer.

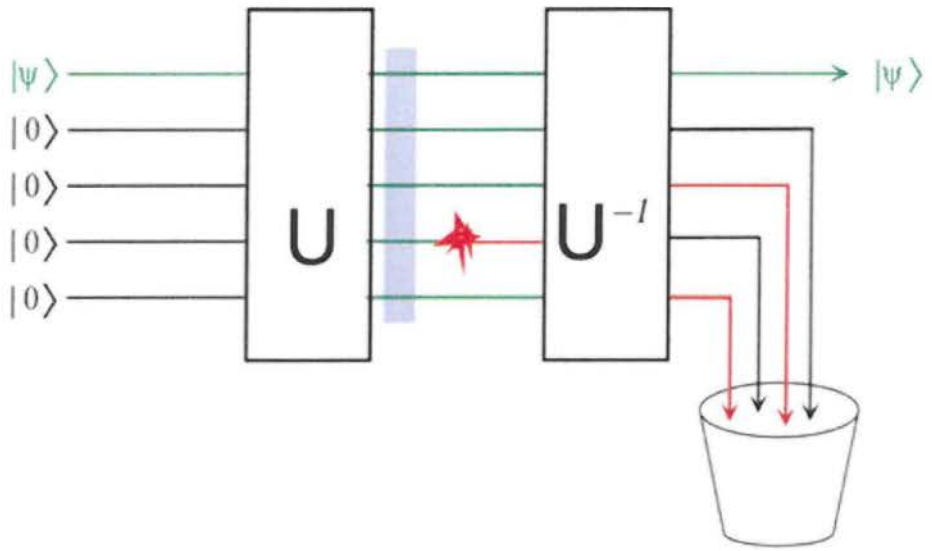
Ο πρώτος που επινόησε έναν κβαντικό υπολογιστικό αλγόριθμο ήταν ο Peter Shor που μπόρεσε εκμεταλλευόμενος την κβαντική δύναμη να παραγοντοποιήσει πολύ μεγάλους αριθμούς σε κλάσματα δευτερολέπτου. Αν και έχει σημειωθεί σημαντική πρόοδος από τη σύλληψη της ιδέας του κβαντικού υπολογιστή μέχρι σήμερα, ωστόσο υπάρχουν πολλά εμπόδια στην υλοποίησή του. Το κυριότερο πρόβλημα στη δημιουργία κβαντικών υπολογιστών είναι η ύπαρξη σφαλμάτων και η αντιμετώπισή τους.

Το πρόβλημα που προκύπτει στη διόρθωση σφάλματος είναι ποια λάθη χρειάζονται διόρθωση (στην επόμενη παράγραφο περιγράφονται κώδικες διόρθωσης σφαλμάτων) . Η απάντηση είναι πρώτιστα εκείνα τα λάθη που προκύπτουν ως άμεσο αποτέλεσμα αποσυσχετισμού (decoherence) ή από την τάση ενός κβαντικού υπολογιστή να αποσυντεθεί από μία δεδομένη κβαντική κατάσταση σε μία ασυνάρτητη κατάσταση καθώς αλληλεπιδρά με το περιβάλλον. Αυτές οι αλληλεπιδράσεις μεταξύ του περιβάλλοντος και των qubits είναι αναπόφευκτες και προκαλούν τη διακοπή των πληροφοριών που αποθηκεύονται στον κβαντικό υπολογιστή, και έτσι τα λάθη στον υπολογισμό.

Η διόρθωση σφαλμάτων είναι απαραίτητη στην υλοποίηση των κβαντικών υπολογιστών γιατί τα κβαντικά συστήματα αλληλεπιδρούν με το περιβάλλον. Αυτή η αλληλεπίδραση, όπως ειπώθηκε, μπορεί να οδηγήσει σε κατάρρευση του συστήματος και η ύπαρξη μηχανισμών για τη διόρθωση των λαθών είναι απαραίτητη.

Υπάρχουν δύο είδη λαθών που μπορεί να εισάγει το περιβάλλον στο σύστημα. Αυτά είναι :

- Δυαδική αντιστροφή
- Αποσυσχετισμός



Εικόνα 86 Quantum Error Correction.

Δυαδική αντιστροφή (Bit flip)

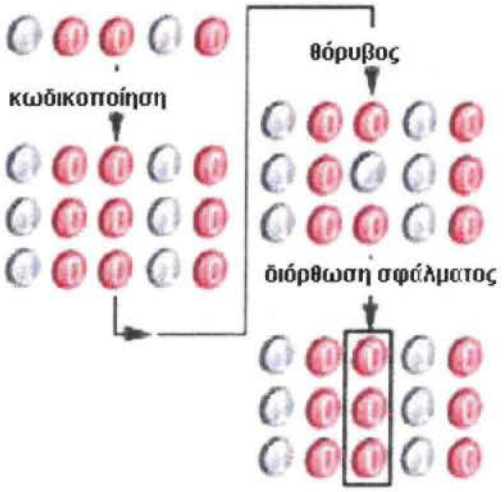
Αρχικά υποθέτουμε ότι το σύστημά μας αποτελείται από ένα qubit. Ένα σφάλμα που μπορεί να προκύψει είναι όμοιο με αυτό σε έναν κλασικό υπολογιστή, είναι το σφάλμα της δυαδικής αντιστροφής.

Αυτό το λάθος μετατρέπει την αρχική κατάσταση από π.χ. α|0> + b|1> σε α|1> + b|0> . Μπορεί να διορθωθεί αυτό το λάθος χρησιμοποιώντας κλασικούς κώδικες διόρθωσης. Μπορούμε να εφαρμόσουμε έναν κλασικό κώδικα επανάληψης και να το αποφύγουμε. Είναι σημαντικό να τονίσουμε ότι η δυαδική αντιστροφή είναι μία αντιστρεπτή πράξη πάνω στα qubits και για αυτό το λόγο μπορεί εύκολα να διορθωθεί.

Αποσυσχετισμός

Ένα άλλο σφάλμα που ενδεχομένως να προκύψει σε έναν κβαντικό υπολογιστή είναι λόγω του φαινόμενου του αποσυσχετισμού (decoherence) των κβαντικών καταστάσεων. Σε αυτή την περίπτωση ανεπιθύμητες όσο και τυχαίες αλληλεπιδράσεις των κβαντικών καταχωρητών με το περιβάλλον οδηγούν στην κατάρρευση της κατάστασης του συστήματος. Αυτό ισοδυναμεί με «μέτρηση» του καταχωρητή η οποία είναι μία μη αντιστρεπτή διεργασία. Αν το σύστημα βρίσκεται σε μια αρχική κατάσταση και ένα δεύτερο qubit μετρηθεί η κατάσταση του συστήματος καταρρέει και κατά συνέπεια χάνεται με μη αναστρέψιμο τρόπο η αποθηκευμένη πληροφορία. Η επίλυση αυτού του προβλήματος είναι εξαιρετικά δύσκολη και η επαναφορά του συστήματος μετά από τέτοια λάθη είναι σχεδόν αδύνατη.

Στους κλασικούς υπολογιστές για τον περιορισμό των σφαλμάτων, κωδικοποιείται κάθε bit ως μια τριπλέτα από όμοια bits. Αν κάποιος θόρυβος αντιστρέψει ένα bit, το σφάλμα μπορεί να αποκατασταθεί επιδιορθώνοντας το μεμονωμένο bit της τριπλέτας.



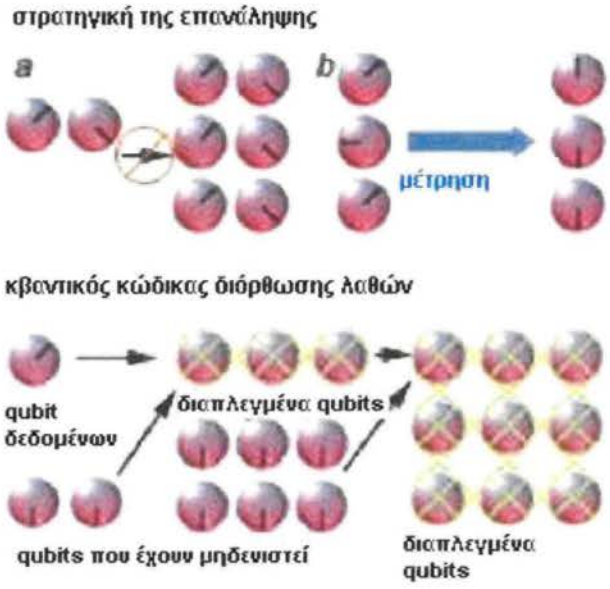
Εικόνα 87 Διόρθωση σφαλμάτων σε κλασσικούς υπολογιστές.

Όσον αφορά τους κβαντικούς υπολογιστές, αρχικά φάνηκε ότι είναι αδύνατον να αναπτύξουμε κώδικες για την διόρθωση κβαντικών σφαλμάτων, διότι η κβαντομηχανική μας απαγορεύει να μάθουμε με βεβαιότητα την άγνωστη κατάσταση ενός κβαντικού αντικειμένου .

Ο κώδικας της απλής κλασικής τριπλέτας συνεπώς αποτυγχάνει διότι δεν μπορούμε να εξετάσουμε κάθε αντίγραφο ενός qubit χωρίς να καταστρέψουμε όλα τα αντίγραφα κατά την διαδικασία αυτή. Ακόμη χειρότερα, το να φτιάξουμε αντίγραφα στην αρχική κατάσταση δεν είναι απλό. Η κβαντομηχανική μας απαγορεύει να πάρουμε ένα άγνωστο qubit και να φτιάξουμε με αξιοπιστία ένα αντίγραφό του. Το αποτέλεσμα αυτό είναι γνωστό ως θεώρημα της αδυναμίας κλωνοποίησης.

Όμως στις αρχές 1990 ερευνητές της IBM υποστήριξαν ότι η κβαντική διόρθωση σφαλμάτων θα ήταν αναγκαία για τους κβαντικούς υπολογιστές, αλλά οι κλασικοί κώδικες δεν μπορούσαν να χρησιμοποιηθούν στον κβαντικό κόσμο. Απέδειξαν πως μπορούμε να κάνουμε κβαντική διόρθωση σφαλμάτων, χωρίς να μάθουμε ποτέ τις καταστάσεις των qubits.

Όπως και με τον κώδικα της τριπλέτας, κάθε τιμή παριστάνεται με ένα σύνολο από qubits. Τα qubits αυτά περνάνε μέσα από ένα κύκλωμα (το κβαντικό ανάλογο των λογικών πυλών) το οποίο βρίσκει με επιτυχία ένα σφάλμα στα qubits χωρίς να "διαβάσει" πραγματικά ποιες είναι οι ξεχωριστές καταστάσεις.



Εικόνα 88 Διόρθωση σφαλμάτων σε κβαντικούς υπολογιστές.

Η προστασία των κβαντικών καταστάσεων από τον θόρυβο επιτεύχθηκε με τη χρήση ενός συνδυασμού ιδεών από την επιστήμη της πληροφορίας και από τη

βασική κβαντομηχανική. Η κβαντική διόρθωση σφαλμάτων έχει δημιουργήσει επίσης πολλές ενδιαφέρουσες νέες ιδέες.

Για παράδειγμα μερικά φυσικά συστήματα μπορεί να έχουν ένα τύπο φυσικής ανοχής στο θόρυβο. Αυτά τα συστήματα θα χρησιμοποιούν κβαντική διόρθωση σφαλμάτων, χωρίς την ανθρώπινη επέμβαση και θα μπορούν να επιδείξουν εξαιρετική αντίσταση στην καταστροφή της υπέρθεσης των καταστάσεων.

4.3.2 Κβαντικά Κυκλώματα.

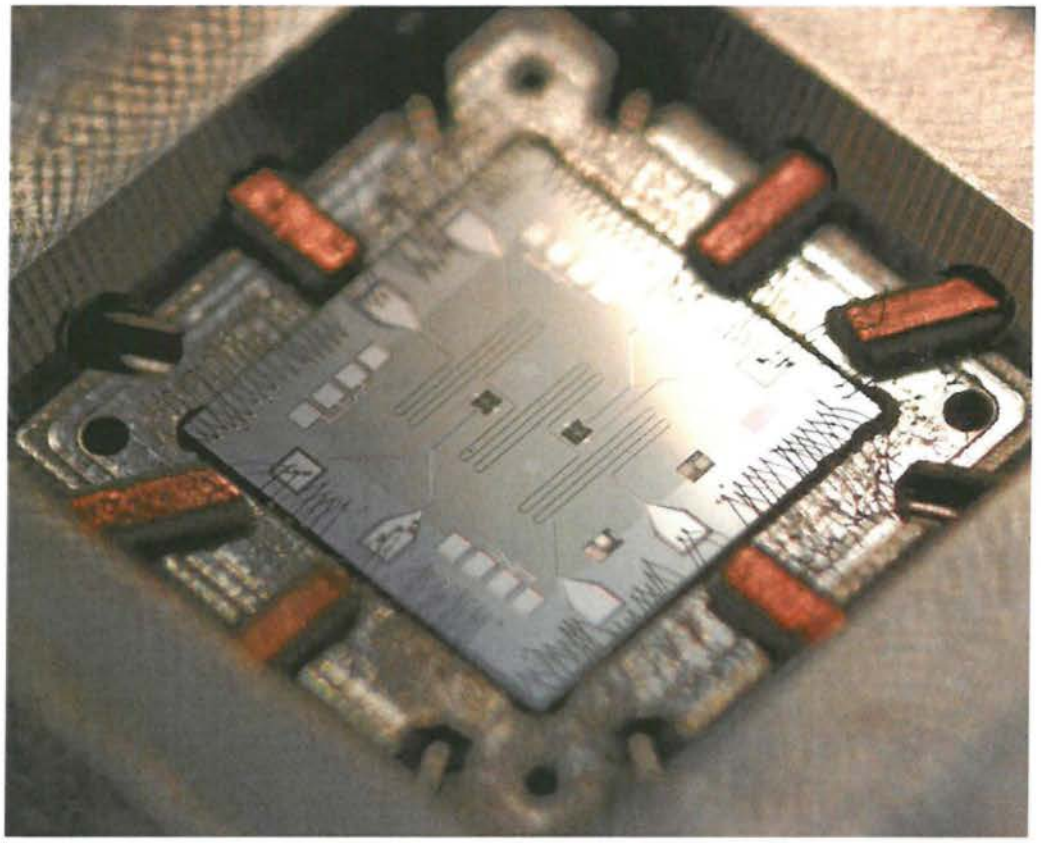
Τα κβαντικά κυκλώματα υλοποιούν κβαντικές πύλες, δηλαδή μετασχηματίζουν κβαντικές καταστάσεις. Η βάση για την ανάπτυξη των τελικών κβαντικών κυκλωμάτων υπήρξε το πρώτο κβαντικό κύκλωμα (κβαντικός αθροιστής) που ήταν ικανό να εκτελεί κβαντικούς υπολογισμούς.

Προτάθηκε από τον Barenco και μπορούσε να εκτελεί προσθέσεις, χρησιμοποιώντας τη μνήμη των καταχωρητών και μπορούσε να αποθηκεύει δεδομένα. Επίσης ο κβαντικός πολλαπλασιαστής που εκτελούσε πολλαπλασιασμούς, βοήθησε στην εξέλιξη των κβαντικών κυκλωμάτων. Έγιναν πολλές ερευνητικές προσπάθειες για την κατασκευή κβαντικών κυκλωμάτων και κυρίως για την κατασκευή βέλτιστων κυκλωμάτων που θα μειώνουν τον υπολογιστικό χρόνο και τα λάθη. Από τις πρώτες έρευνες που έγιναν κατέληξαν στο συμπέρασμα ότι οι κβαντικές πύλες των ενός και δύο qubit θα μπορούσαν να αποτελέσουν τη βάση για την κατασκευή οποιουδήποτε κυκλώματος.

Αρχικά έγιναν έρευνες για την αναπαράσταση πολυπλοκότερων κβαντικών πυλών από απλούστερες. Οι Chau και Wilczek ανακάλυψαν ότι η πύλη Fredkin (που είναι μία καθολική πύλη 3-qubit) μπορεί να αναπαρασταθεί από 6 πύλες 2-qubit. Αυτό

το αποτέλεσμα βελτιώθηκε από τους Smolin και DiVincenzo με την παραδοχή ότι χρειάζονται μόνο 5 πύλες.

Πολλές από τις μεθόδους που προτάθηκαν κατά καιρούς βασίζονται στις καθολικές πύλες. Καθολικές πύλες είναι ένα σύνολο από στοιχειώδεις πύλες του ενός και δύο qubits οι οποίες συνδέονται μέσω κβαντικών συνδέσεων και μπορούν να υλοποιήσουν οποιοδήποτε κβαντικό αλγόριθμο.



Εικόνα 89 Κβαντικό κύκλωμα.

4.3.2.1 Πρότυπο Κυκλωματικό Μοντέλο

Το Πρότυπο Κυκλωματικό Μοντέλο είναι ένα μοντέλο που ακολουθείται για την κατασκευή κβαντικών κυκλωμάτων. Σ' αυτό το μοντέλο είναι σημαντική η έννοια των καθολικών πυλών. Μία οποιαδήποτε κβαντική πύλη, μπορεί να αναλυθεί χρησιμοποιώντας ένα σύνολο από βασικές πύλες, γνωστές σαν καθολικές πύλες. Η

επιλογή του συνόλου των καθολικών πυλών δεν είναι μοναδική. Πύλες του ενός qubit μπορούν να αναλυθούν χρησιμοποιώντας μόνο πύλες Hadamard και πύλες μετατόπισης φάσης. Πύλες των δύο qubit μπορούν να αναλυθούν χρησιμοποιώντας πύλες Hadamard, CNOT και μετατόπισης φάσης και αυτό μπορεί να γενικευτεί στην περίπτωση των πυλών N-qubits, καθώς μπορεί να υποτεθεί ότι οι πύλες των N-qubits μπορούν να προσεγγιστούν από $O(4^N)$ πύλες μετατόπισης φάσης, CNOT και Hadamard.

Στο Πρότυπο Κυκλωματικό Μοντέλο κάθε πύλη μπορεί να αναλυθεί σε ένα οποιοδήποτε σύνολο καθολικών πυλών. Αυτή η ανάλυση όμως μπορεί να οδηγήσει σε συστήματα που δεν μπορούν να λειτουργήσουν σωστά επειδή ίσως δεν μπορούν να εκτελέσουν κάποια καθολική πύλη στην οποία έχουν αναλυθεί. Επίσης ούτε ο αριθμός των υπολογιστικών βημάτων ούτε ο συνολικός χρόνος για τον υπολογισμό είναι βέλτιστα. Παρόλα τα προβλήματα του μοντέλου, πολλά κυκλώματα κατασκευάζονται σύμφωνα με αυτό.

4.3.2.2 Μέθοδος κωδικοποιημένης παγκοσμιότητας (Encoded universality)

Εκτός από το Πρότυπο Κυκλωματικό Μοντέλο, η μέθοδος κωδικοποιημένης παγκοσμιότητας, είναι μία μέθοδος που παρέχει ένα πρότυπο για την κατασκευή βέλτιστων κβαντικών κυκλωμάτων με χρήση των ελάχιστων δυνατών Χαμιλτονιανών. Με αυτή τη μέθοδο ελαχιστοποιούνται οι φυσικοί πόροι που απαιτούνται για να εκτελεστούν οι κβαντικοί υπολογισμοί και η όλη υπολογιστική διαδικασία. Σ' αυτό το μοντέλο δεν γίνεται χρήση των καθολικών πυλών για την κατασκευή κυκλωμάτων, το σύστημα δεν ωθείται να λειτουργήσει σαν ένα προκαθορισμένο σύνολο από καθολικές πύλες που συνδέονται μέσω κβαντικών συνδέσεων (όπως στο Πρότυπο Κυκλωματικό Μοντέλο), αλλά εκμεταλλευόμαστε τις εγγενείς ικανότητες του να εκτελεί κβαντικούς υπολογισμούς που υιοθετεί από την φυσική διαθέσιμη αλληλεπίδραση.

Πιο συγκεκριμένα, δύο όμοιες συνδέσεις Josephson που συνδέονται μέσω ενός αμοιβαίου πηνίου, μπορούν να εκφράσουν πύλες των ενός και δύο qubit. Αυτό μπορεί να πραγματοποιηθεί από έναν πεπερασμένο αριθμό από χρονικά βήματα που εξελίσσονται σύμφωνα με μία περιορισμένη συλλογή από βασικές

Χαμιλτονιανές. Σύμφωνα με αυτή την άποψη μπορούν να κατασκευαστούν πύλες ενός και δύο qubit δεν γενικεύεται όμως για πύλες των N-qubit.

Παρακάτω περιγράφεται αναλυτικά η μέθοδος μέσω δύο παραδειγμάτων σε συσκευές 1 και 2-qubit .

i) Συσκευές 1-qubit.

Αυτή η συσκευή αποτελείται από ένα μικρό "κουτί" με n εντολές που συνδέονται μέσω ενός συνδέσμου με χωρητικότητα πυκνωτή C κα μία ενέργεια E σε ένα υπεραγώγιμο ηλεκτρόδιο. Μία πύλη για τον έλεγχο της τάσης (V) συνδέεται στο σύστημα μέσω μίας πύλης πυκνωτή Cg . η επιλεγμένη συσκευή είναι τέτοια ώστε το υπεραγώγιμο ενεργειακό κενό να είναι το μεγαλύτερο δυνατό. Η τάση παίρνει δύο τιμές 0 ή 1. Επίσης στη συσκευή υπάρχει ένας διακόπτης που παίρνει τιμές 0 ή 1 ανάλογα αν είναι κλειστός (OFF) ή ανοιχτός (ON). Αυτός ο διακόπτης ελέγχει την τάση που μπορεί να είναι είτε Vid είτε Vdeg.

Ειδικότερα, το σύστημα βρίσκεται στην OFF κατάσταση (ή 0) ανταποκρινόμενο στην Vdeg σε μία χρονική διάρκεια t_1. Έπειτα το σύστημα μεταβαίνει στην κατάσταση ON (ή 1) που ανταποκρίνεται στην Vid σε μία χρονική στιγμή t_2. Στη συνέχεια επανέρχεται στην αρχική Χαμιλτονιανή Vdeg στη διάρκεια της στιγμής t_3. Η γενική μορφή της λειτουργίας της συσκευής περιγράφεται από τον παρακάτω τύπο:

$$U = e^{-it_3 H deg}\, e^{-it_2 H deg}\, e^{-it_1 H deg}$$

Αυτό σημαίνει ότι ο συνδυασμός τριών όρων που περιλαμβάνει ο παραπάνω τύπος καλύπτει όλους τους 2x2 πίνακες και μπορεί να υλοποιηθεί από την συσκευή αυτή. Από τον παραπάνω τύπο προκύπτει και ο πίνακας που περιγράφει την κατάσταση του συστήματος τις στιγμές t_1, t_2, t_3 και είναι ο ακόλουθος:

U
$\{0,t_1\}$
$\{1,t_2\}$
$\{0,t_3\}$

Οι πύλες λοιπόν των 1-qubit υπακούουν στον πίνακα.

i) Συσκευές 2-qubit

Για να υλοποιηθούν χειρισμοί πυλών ενός και δύο qubit, πρέπει να συνδυαστούν ζεύγη από qubits μαζί και να ελεγχθούν οι μεταξύ τους αλληλεπιδράσεις. Γι' αυτό και στη μέθοδο encoded universality προτείνεται μία συσκευή 2-qubits. Το σύστημα θα μπορεί να είναι στην κατάσταση ON εφαρμόζοντας μία εισαγωγή μέσω ενός πυκνωτή L και έχοντας ζευγαρωμένα διαφορετικά qubits και σε κατάσταση OFF όταν ο πυκνωτής είναι ο δηλαδή όταν L=0 και δεν υπάρχουν σε ζευγάρια τα qubits. όπου E_{c1}, E_{c2}, E_L είναι διακόπτες. Οι πρώτοι δύο ελέγχονται από τις τάσεις V_{g1} , V_{g2} και ο τελευταίος σχετίζεται με τον πυκνωτή L. Οι παράμετροι E_{c1}, E_{c2} μπορούν να έχουν δύο τιμές 0 ή E_c.

Τώρα οι χαμιλτονινές είναι 4 και όχι 2 όπως πριν (V_{id} ,V_{deg}) και είναι οι ακόλουθες:

H1: όταν και οι δύο σύνδεσμοι είναι σε ιδανική κατάσταση ($E_{c1} = E_{c2} = E_c$). Αυτή η κατάσταση αντιστοιχεί στην κατάσταση του διακόπτη (E_{c1}, E_{c2} , E_L) → (1, 1, 0).

H2: όταν οι σύνδεσμοι είναι στην κατάσταση ($E_{c1} = E_{c2} = 0$) και δύο qubits είναι ζευγαρωμένα και αντιστοιχεί στο διακόπτη (0, 0, 1).

H3: όταν για την πρώτη σύνδεση ισχύει ($E_{c1} = 0$), για τη δεύτερη ($E_{c1} = E_c$) και βρίσκεται στην ιδανική κατάσταση και είναι μη ζευγαρωμένα τα qubits. Αυτή η χαμιλτονιανή αντιστοιχεί στις επιλογές διακόπτη (0, 1, 0).

H4: όταν η πρώτη σύνδεση είναι στην ιδανική κατάσταση ($E_{c1} = E_c$) , η δεύτερη στην εκφυλισμένη ($E_{c2}= 0$) και είναι πάλι μη ζευγαρωμένα τα qubits ($E_L = 0$).

Οι 4 Χαμιλτονιανές αντιπροσωπεύουν κάθε πίνακα 4x4 και ακολουθούν τον παρακάτω τύπο:

$$U = e^{-iH_{21s}t_{15}} e^{-iH_{21}t_{14}} \dots e^{-iH_{21}t_{6}} \dots e^{-iH_{15}t_{5}} e^{-iH_{4}t_{4}} e^{-iH_{23}t_{3}} e^{-iH_{21}t_{2}} e^{-iH_{15}t_{1}}$$

Έτσι από τον τύπο βγαίνει το συμπέρασμα ότι οποιαδήποτε κβαντική πύλη 2-qubit μπορεί να υλοποιηθεί μέσα σε 15 χρονικά βήματα που φαίνονται και από τον πίνακα:

U
$\{1,1,0,t_1\}$
$\{0,0,1,t_2\}$
$\{0,1,0,t_3\}$
$\{1,0,0,t_4\}$
$\{1,1,0,t_5\}$
$\{0,0,1,t_6\}$
$\{0,1,0,t_7\}$
$\{1,0,0,t_8\}$
$\{1,1,0,t_9\}$
$\{0,0,1,t_{10}\}$
$\{0,1,0,t_{11}\}$
$\{1,0,0,t_{12}\}$
$\{1,1,0,t_{13}\}$
$\{0,0,1,t_{14}\}$
$\{0,1,0,t_{15}\}$

Τέλος η διαδοχή των βημάτων του διακόπτη ακολουθεί κυκλική πορεία και διευκολύνει τον χειρισμό των συσκευών με ζεύγη qubit.

Συμπερασματικά η μέθοδος αποτελείται από κάποια βασικά μέρη που συνοψίζονται στα παρακάτω:

1) Αντί να καταναγκάζει ένα φυσικό σύστημα να ενεργήσει σαν προκαθορισμένο σύνολο καθολικών πυλών, δίνεται έμφαση στη δυνατότητα του φυσικού συστήματος να ενεργήσει σαν κβαντικός υπολογιστής χρησιμοποιώντας μόνο τις φυσικές διαθέσιμες αλληλεπιδράσεις του.

2) Οποιαδήποτε πύλη και αλγόριθμος κατασκευάζεται από την άποψη μίας ελάχιστης διαμόρφωσης και υπολογιστικής διαδικασίας.

3) Ελαχιστοποιημένος πεπερασμένος αριθμός βημάτων, που εξελίσσεται εγκαίρως, σύμφωνα με έναν πεπερασμένο αριθμό από βασικές Χαμιλτονιανές που ελέγχονται από έναν ελάχιστο πεπερασμένο αριθμό από κλασικούς διακόπτες που ανοίγουν για συγκεκριμένα χρονικά διαστήματα (η επιλογή των διακοπτών δεν είναι μοναδική).

4) Ανεξαρτησία του φυσικού συστήματος που χρησιμοποιείται για την εφαρμογή.

4.3.2.3 Μέθοδος Shende, Bullock και Markov

Το 2003 οι ερευνητές Shende, Bullock και Markov πρότειναν έναν αλγόριθμο για τη σύνθεση κυκλωμάτων δύο qubit με τον βέλτιστο αριθμό από πύλες CNOT. Παρουσίασαν μία μέθοδο, χρησιμοποιώντας στοιχεία πίνακα, για τη δημιουργία κβαντικών κυκλωμάτων που υπάρχουν σε επεξεργαστές με ακριβώς 0 ή 1 ή και 2 πύλες CNOT και με όλες τις άλλες πύλες να είναι πύλες ενός qubit.

Δημιούργησαν έναν αλγόριθμο για τη σύνθεση 2-qubit κβαντικών κυκλωμάτων με το βέλτιστο αριθμό CNOT και τον εφάρμοσαν σε επεξεργαστές που εκτελούν τους γνωστούς βασικούς κβαντικούς αλγορίθμους(Shor, Grover, Deutch). Οι ερευνητές κατέληξαν σε μαθηματικούς τύπους για την περίπτωση που ο επεξεργαστής αποτελείται από 0, 1 ή 2 CNOT. Σε κάθε περίπτωση εξετάζεται η συνθήκη που ισχύει και εφαρμόζονται οι αντίστοιχοι τύποι.

Αυτό που πέτυχαν τελικά ήταν να μειώσουν τον πιθανό αριθμό CNOT και να καταλήξουν σε βέλτιστα πλην μικρά κυκλώματα.

4.3.2.4 Μέθοδος CSD(Cosine-sine).

Η πολυπλοκότητα μίας εφαρμογής υπολογίζεται με βάση τον αριθμό των στοιχειωδών πυλών που απαιτούνται. Το να επιτυγχάνεται μία σειρά από πύλες κατώτερης πολυπλοκότητας είναι σημαντικό γιατί οδηγεί σε γρηγορότερη εκτέλεση υπολογισμών αλλά και σε λιγότερα λάθη. Σύμφωνα με τη μέθοδο CSD,

ένα κβαντικό κύκλωμα δίνεται από έναν ελάχιστο αριθμό από στοιχειώδεις πύλες και έναν ελάχιστο αριθμό από πύλες CNOT.

Σε σύγκριση με τη μέθοδο των Shende, Bullock και Markov, η CSD απαιτεί επιπλέον 5 CNOT. Για μία 3-qubit πύλη η CSD απαιτεί 48 πύλες CNOT και 64 στοιχειώδεις πύλες 1-qubit. Όμως για μία 4-qubit πύλη που περιγράφεται από αυτή τη μέθοδο η CSD χρησιμοποιεί 256 στοιχειώδεις 1-qubit πύλες και 224 CNOT's. Αυτή είναι και η μικρότερη σειρά πυλών για να εφαρμοστεί σε μία τέτοιου είδους πύλη. Επίσης αυτή η μέθοδος για μία nqubit πύλη όπου n>4 , παρέχει το πιο αποτελεσματικό κβαντικό κύκλωμα για να εφαρμοστεί σε μία τέτοια πύλη.

4.3.2.5 Μέθοδος KGD(Khaneja-Glaser)

Μία μέθοδος για την κατασκευή βέλτιστου κβαντικού κυκλώματος για την επίτευξη 2-qubit κβαντικού υπολογισμού, απαιτεί το πολύ τρεις πύλες CNOT και 15 στοιχειώδεις πύλες του ενός qubit. Αυτή η μέθοδος αποδεικνύεται ότι οδηγεί στην κατασκευή βέλτιστου κυκλώματος, υπό την έννοια, ότι δεν υπάρχει μικρότερο κύκλωμα που να χρησιμοποιεί την ίδια οικογένεια πυλών και επιτυγχάνει την ίδια λειτουργία. Επιπλέον αν ο ενωτικός πίνακας ανταποκρίνεται στην επιθυμητή πύλη, τότε το βέλτιστο κύκλωμα μπορεί να επιτευχθεί με δύο CNOT και 12 άλλες στοιχειώδεις πύλες. Είναι γνωστό ότι ένας γενικότερος n-qubit κβαντικός υπολογισμός μπορεί να έρθει εις πέρας χρησιμοποιώντας O (2^{2n}) κβαντικές πύλες 2-qubit. Αυτή η γνώση έγινε πιο ακριβής στην περίπτωση των 2-qubit κβαντικών χειρισμών όπως αναφέρθηκε.

Παρόλο που έχει κατασκευαστεί ένα βέλτιστο κύκλωμα για επίτευξη 2-qubit κβαντικού υπολογισμού, δεν υπάρχει η ίδια πρόοδος και για τα κυκλώματα που εκτελούν κβαντικούς υπολογισμούς 3-qubit γιατί το φαινόμενο της διεμπλοκής είναι πολύ ισχυρό σε τέτοιου είδους υπολογισμούς. Μία πρόσφατη έρευνα έδειξε ότι κβαντικοί υπολογισμοί 3-qubit μπορούν να αναλυθούν χρησιμοποιώντας 136 1-qubit πύλες και 64 CNOT πύλες. Η τελευταία όμως εργασία πάνω στους κβαντικούς υπολογισμούς 3-qubit βελτίωσε την παραπάνω υπόθεση, αποδεικνύοντας ότι μπορούν να χρησιμοποιηθούν 98 1-qubit πύλες και 40 CNOT πύλες σε αντιδιαστολή με την CSD που απαιτεί 48 πύλες CNOT και 64 στοιχειώδεις πύλες 1-qubit.

4.3.2.6 Τεχνική "Carry-Save".

Υπάρχουν επίσης διάφορες τεχνικές που χρησιμοποιούν μεθόδους carry-save που δανείζονται από τη σχεδίαση των κλασικών υπολογιστών και μπορούν να σχεδιάζουν αποτελεσματικά αριθμητικά στοιχεία των κβαντικών πυλών. Σύμφωνα με αυτή την τεχνική, επιτρέπεται η αξιολόγηση των παράλληλων bit όλων των αριθμητικών στοιχείων που απαιτούνται για τον αλγόριθμο του Shor, αναβάλλοντας ταυτόχρονα τη διάδοση του bit για το τέλος της υπολογιστικής διαδικασίας. Σε μία τεχνική που αναπτύχθηκε από τον Gossett η μέθοδος carry-save χρησιμοποιείται και μειώνει την καθυστέρηση στην κβαντική πύλη από $O(N^3)$ σε $O(NlogN)$ με κόστος την αύξηση του αριθμού των qubits που απαιτούνται και συγκεκριμένα από $O(N)$ σε $O(N^2)$. Σύμφωνα με τον Gossett αυτή η τεχνική μπορεί να εφαρμοστεί και να βελτιώσει και τον αλγόριθμο του Shor και πιο συγκεκριμένα για N=1000 ο αλγόριθμος επιταχύνεται με τεχνικές carry-save κατά ένα παράγοντα 10^5 με κόστος την αύξηση των qubits σε 10^2.

4.3.2.7 Μέθοδος των Levitin, Toffoli, Zachary.

Το 2002 οι Levitin, Toffoli, Zachary κατέδειξαν ποιος είναι ο ελάχιστος χρόνος λειτουργίας των κβαντικών πυλών όταν λειτουργούν πάνω σε qubits. Ήταν ήδη γνωστό από το 1998 , ότι ο χρόνος που χρειάζεται ένα κβαντικό σύστημα να μεταβεί από μία κατάσταση σε μία κάθετη σε αυτή είναι :

$$\tau=h/4^{E}$$

όπου h η σταθερά του Planck και E ο μέσος όρος ενέργειας του κβαντικού συστήματος. Υπολόγισαν ότι ο ελάχιστος χρόνος επεξεργασίας μίας κβαντικής πύλης είναι:

$$\tau= h/2|E2-E1|$$

Από τον τύπο θα μπορούσε κανείς να υποθέσει ότι ο χρόνος μπορεί να γίνει εξαιρετικά μικρός αν η διαφορά E_2-E_1 είναι μεγάλη(όπου E_2, E_1 είναι αξίες των Χαμιλτονιανών). Κάτι τέτοιο όμως δεν ισχύει σε μία πραγματική κβαντική κατάσταση. Αυτή η απόδειξη αποτέλεσε και μία βάση για μετέπειτα έρευνες στην ελαχιστοποίηση του κβαντικού υπολογιστικού χρόνου.

4.3.2.8 Μέθοδος Zhang, Vala, Sastry και Whaley.

Μία άλλη μέθοδος για την κατασκευή βέλτιστων κβαντικών κυκλωμάτων προτάθηκε από τους Zhang, Vala, Sastry και Whaley. Οι τρεις ερευνητές έλαβαν υπόψη τους προηγούμενες μελέτες που αποδείκνυαν ότι 3 εφαρμογές της CNOT και πύλες του ενός qubit είναι καθολικές.

Επίσης κατανοώντας την γεωμετρική αναπαράσταση των πυλών 2-qubit κατέληξαν σε ένα ανώτατο όριο για την κατασκευή κβαντικών κυκλωμάτων από κβαντικές πύλες που δρουν σε περισσότερα από ένα qubit σε συνδυασμό με τοπικές πύλες. Το ανώτατο αυτό όριο για την κατασκευή κβαντικών κυκλωμάτων είναι :

$$U = e^{\frac{\frac{\gamma_i}{2\sigma_1}}{2\sigma_2 2}}$$

Κατέληξαν επίσης στο συμπέρασμα ότι από τις κβαντικές πύλες που δρουν σε περισσότερα από ένα qubit, η πύλη CNOT είναι η πιο αποτελεσματική και οδηγεί σε βέλτιστα κβαντικά κυκλώματα και στο παραπάνω ανώτερο όριο. Μια εφαρμογή της CNOT τέσσερις φορές μπορεί να οδηγήσει στη σύνθεση

οποιασδήποτε πύλης 2-qubit, σε αντίθεση με τις προηγούμενες μεθόδους που χρησιμοποιούσαν καθολικές πύλες για τη σύνθεση όλων των υπόλοιπων πυλών.

4.3.2.9 Μέθοδος Maslov και Dueck.

Πολλοί από τους ερευνητές στην προσπάθειά τους να βελτιώσουν τα κβαντικά κυκλώματα εστίασαν την προσοχή τους στην αντικατάσταση πολύπλοκων κβαντικών πυλών με απλούστερες ώστε να επιταχυνθούν οι λειτουργίες του τελικού κβαντικού κυκλώματος. Οι Maslov και Dueck επικεντρώθηκαν στις πύλες Toffoli οι οποίες είναι ιδιαίτερα δημοφιλείς έναντι των υπόλοιπων πυλών, εξαιτίας της απλότητάς τους. Για το λόγο αυτό η απαίτηση για δημιουργία πυλών Toffoli που θα οδηγούν σε χαμηλού κόστους κβαντικό κύκλωμα ήταν απαραίτητη.

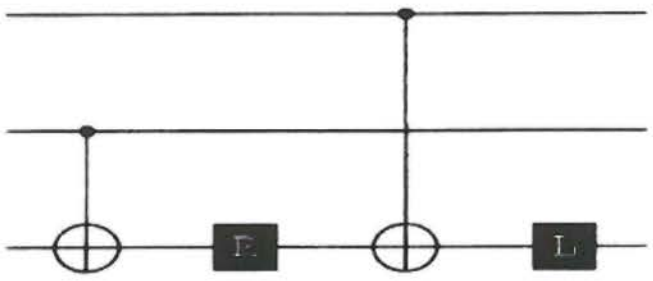
Έτσι βελτίωσαν το κβαντικό κύκλωμα που είχε προταθεί από τον Barenco και το οποίο βασίζονταν σε πύλες Toffoli. Ο τελευταίος είχε προτείνει ένα κβαντικό κύκλωμα, όπου κάποιες από τις πύλες Toffoli αντικαταστάθηκαν με πύλες Peres (οι πύλες Peres οδηγούν σε ισοδύναμο μετασχηματισμό με αυτό που παράγουν μία πύλη Toffoli ακολουθούμενη από μία CNOT) και κατέληξε σε κύκλωμα με μειωμένο κόστος. Διατύπωσε ότι μία (m+1) bit πύλη Toffoli μπορεί να προσομοιωθεί με κόστος 48m-116 βασικές λειτουργίες (πράξεις σε ένα και δύο qubits), δηλαδή, σε ένα κβαντικό κύκλωμα που αποτελείται από n bits όπου $n>=5$ και $m \in \{3,\ldots,[n/2]\}$, τότε μία πύλη Toffoli των (m+1)bits μπορεί να υλοποιηθεί από ένα δίκτυο αποτελούμενο από 4(m-2) πύλες Toffoli.

Όμως οι δύο ερευνητές βελτίωσαν το κβαντικό κύκλωμα που προσομοιώνει πύλες Toffoli των (m+1) bits χρησιμοποιώντας 32m-96 βασικές λειτουργίες. Τελικά

βελτίωσαν το κόστος και το χρόνο για τη δημιουργία κβαντικών κυκλωμάτων χρησιμοποιώντας και οι ίδιοι τις πύλες Peres.

4.3.2.10 Κβαντικά κυκλώματα με γενετικό προγραμματισμό.

Ένας ακόμη τρόπος για τη σχεδίαση αποτελεσματικών κβαντικών κυκλωμάτων είναι με τη χρήση ευρηστικών αλγορίθμων που βασίζονται στον γενετικό προγραμματισμό. Η μέθοδος αυτή οδηγεί σε καινούργια κυκλώματα ανώτερα από τα προηγούμενα. Χαρακτηριστικό της μεθόδου είναι ότι το πρόβλημα της σύνθεσης κυκλώματος, χαρακτηρίζεται σαν πρόβλημα εύρεσης κι ένας αλγόριθμος βρίσκει τη λύση σε βέλτιστο χρόνο. Η μέθοδος μπορεί να βρει κυκλώματα όταν ο αριθμός των πυλών που απαιτούνται είναι πολύ μικρός, όπως φαίνεται και στο κύκλωμα.



Εικόνα 90 Κύκλωμα που εφαρμόζεται γενετικός προγραμματισμός.

Περιληπτικά η μέθοδος, αφού αρχικοποιηθεί ένα πλήθος από τυχαίες λύσεις: μέχρι να ικανοποιηθεί το κριτήριο που απαιτείται επαναλαμβάνονται τα βήματα:

- Αποτίμηση της ποιότητας της κάθε λύσης που προκύπτει
- Υπολογίζεται η ποιότητα της λύσης, δειγματιζόμαστε από το πλήθος
- Για κάθε μέλος του πλήθους , επιλέγουμε ένα για να εξασκήσουμε σε αυτό:
  - α) Μεταλλαγή
  - β) Διασταύρωση

4.3.3 Τεχνολογίες Κβαντικών Υπολογιστών.

Στην προσπάθειά τους να αναζητήσουν τον τρόπο κατασκευής ενός υπολογιστή που θα εκμεταλλευόταν τις αρχές της κβαντομηχανικής, πολλοί ερευνητές ακολουθούν διάφορες ετερόκλητες τεχνολογίες, συμπεριλαμβανομένων των κβαντικών υπολογιστών στερεάς κατάστασης, όπως δηλαδή και οι κλασικοί, των παγίδων ιόντων (ion-traps), υπολογιστών κοιλότητας κβαντικής ηλεκτροδυναμικής (cavity QED) καθώς και του πυρηνικού μαγνητικού συντονισμού (NMR).

4.3.3.1 Μοριακοί υπολογιστές.

Τελευταία έχει αναπτυχθεί ένα νέο είδος υπολογιστικής διαδικασίας, η οποία στηρίζεται στην κίνηση των μορίων. Ερευνητές στην IBM έχουν καταφέρει να επιδείξουν λογικές πύλες χρησιμοποιώντας μία στοιβάδα μορίων μονοξειδίου του άνθρακα για να μεταφέρει δεδομένα. Οι συσκευές που γίνονται κατ' αυτό τον τρόπο έχουν διαστάσεις στην κλίμακα των νανομέτρων (10-9), μεγέθους αρκετές τάξεις μικρότερες από τεχνολογία πυριτίου των σημερινών συμβατικών υπολογιστών.

Η πυκνότητα των συστατικών στα μικροτσίπ πυριτίου έχει αυξηθεί εκθετικά τα τελευταία σαράντα χρόνια. Οι ερευνητές της IBM έχουν υπερνικήσει αυτό το πρόβλημα, σε γενικές γραμμές, με τη χρησιμοποίηση ενός ζεύγους, χαμηλής θερμοκρασίας, ηλεκτρονικών μικροσκοπίων σάρωσης, για να διευθετήσουν ζεύγη μορίων μονοξειδίου του άνθρακα σε μια επιφάνεια του χαλκού. Μετακίνησαν ένα απλό μόριο μονοξειδίου του άνθρακα παράλληλα με ένα από αυτά τα ζεύγη, έτσι ώστε τα τρία μόρια σχημάτισαν ένα σχήμα σαν την κεφαλή ενός βέλους. Εντούτοις, ο σχηματισμός αυτός ήταν ασταθής επειδή αύξησε την ενέργεια του συστήματος.

Οι ερευνητές της IBM χρησιμοποίησαν την αρχή αυτή για να κάνουν την πύλη AND. Τοποθέτησαν τρεις σειρές ζευγών μορίων σε μια μορφή Y, με ένα απλό μόριο στο κεντρικό σημείο, όπου συναντώνται οι σειρές. Δύο σειρές ενέργησαν ως είσοδοι και η τρίτη ενεργεί ως έξοδος. Εάν υπάρχει ένας καταρράκτης και στις δύο σειρές - δηλ. εάν υπάρχει ένα "1" και στις δύο εισόδους-μόρια θα πεταχτούν κατά μήκος των σειρών για να διαμορφώσουν την κεφαλή του βέλους με το απλό μόριο, που είναι ήδη στο σημείο όπου συναντώνται οι τρεις σειρές. Αυτή η κεφαλή έπειτα θα αποσυντεθεί, παράγοντας έναν καταρράκτη (δηλ. ένα σήμα) στην έξοδο. Οι ερευνητές χρησιμοποίησαν μια παρόμοια ρύθμιση που κάνει την πύλη OR.

Δυστυχώς οι μοριακές συσκευές καταρρακτών που έγιναν από τους ερευνητές της IBM ήταν πολύ αργές και θα μπορούσαν μόνο να χρησιμοποιηθούν για να εκτελέσουν μια απλή λειτουργία. Για να επαναχρησιμοποιήσουν τις συσκευές αυτές οι ερευνητές έπρεπε να τοποθετήσουν τα μόρια πίσω στην αρχική θέση τους χρησιμοποιώντας ένα από τα ηλεκτρονικά μικροσκόπια σάρωσης. Για να είναι χρήσιμοι, οι μοριακοί υπολογιστές καταρρακτών θα χρειάζονταν έναν αυτόματο μηχανισμό που θα επαναρρύθμιζε μερικά από τα μόρια και θα άφηνε τα άλλα άθικτα για να ενεργήσουν ως καταχωρητές δεδομένων.

4.3.3.2 Παγίδες ιόντων.

Μία νέα τεχνική για τη δημιουργία κβαντικών υπολογιστών είναι αυτή με τις παγίδες ιόντων. Ένας κβαντικός υπολογιστής, όπως έχουμε αναφέρει, λειτουργεί με κβαντικά bit (qubits), αντί των συνηθισμένων bit. Ένα qubit μπορεί να είναι όχι

μόνο 0 ή 1 αλλά και μία υπέρθεση των δύο τιμών, στην οποία οι δύο προηγούμενες τιμές συνδυάζονται σε μια ενιαία κατάσταση.

Μια σημαντική κατηγορία υπερθέσεων πολλών qubit είναι οι διαπλεγμένες καταστάσεις. Σε αυτό τις διαμορφώσεις, η κατάσταση του κάθε qubit διασυνδέεται με έναν λεπτό τρόπο με την κατάσταση του γειτονικού του. Πειράματα με τα ατομικά ιόντα περιλαμβάνουν τεράστιες ηλεκτρομαγνητικές παγίδες για να συγκρατηθούν τα ιόντα στη σειρά μέσα σε κενό. Αν και είναι καλό για τα πειράματα να γίνονται με έναν μικρό αριθμός ιόντων, είναι εντελώς αδύνατον για τα μεγάλης κλίμακας συστήματα όπως ένας κβαντικός υπολογιστής, αν θέλουμε να έχει σημαντική χρήση.

Τελευταία όμως ερευνητές έχουν δείξει μια ιοντική παγίδα μεγέθους 100 μικρών μέσα σε ένα τσιπ ημιαγωγών. Χρησιμοποίησαν το τσιπ για να παγιδέψουν ένα μόνο ιόν καδμίου και το μετακίνησαν προς διαφορετικές θέσεις στην παγίδα εφαρμόζοντας ηλεκτρικά σήματα στα ηλεκτρόδια. Η παγίδα φτιάχτηκε με τη βοήθεια της καθιερωμένης μεθόδου της λιθογραφίας. Μια ηλεκτρομαγνητική παγίδα είναι αυτή που κρατά τα ιόντα σε σειρά μέσα σε κενό, ενώ λέιζερ χειρίζονται τις καταστάσεις τους.

Σε γενικές γραμμές οι τεχνικές μπορούν να ενσωματώσουν μεγαλύτερους αριθμούς ιόντων. Ένα εμπόδιο όμως ήταν ότι η ποιότητα της πεπλεγμένης κατάστασης μειώθηκε καθώς αυξανόταν ο αριθμός των ιόντων. Για να μειώσουν αυτό το λάθος, οι ερευνητές θα μπορούσαν να ρυθμίσουν τις λεπτομέρειες των παλμών του λέιζερ, χρησιμοποιώντας διαφορετικές καταστάσεις ιόντων για την αναπαράσταση του 0 και του 1, ή να δουλέψουν με ένα διαφορετικό είδος ιόντων συνολικά.

Για να είναι χρήσιμος ένας κβαντικός υπολογιστής πρέπει όχι μόνο να μπορούμε να δημιουργούμε ειδικές καταστάσεις qubit αλλά και να τις χειριζόμαστε με τρόπο που να διατηρούνται τα κβαντικά χαρακτηριστικά τους. Δηλαδή κάποιος να μπορεί να εκτελέσει κβαντικούς αλγορίθμους στον υπολογιστή. Ένας γνωστός αλγόριθμος είναι ο κβαντικός αλγόριθμος του Grover σε ένα σύστημα από δύο παγιδευμένα ιόντα καδμίου. Ο αλγόριθμος κάνει αναζήτηση μέσα σε μια βάση δεδομένων, όπου οι καταχωρήσεις έγιναν με έναν τυχαίο τρόπο. Η έρευνα ενός τυχαίου στοιχείου απαιτεί συνήθως την εξέταση κάθε καταχώρησης και άρα ο

αντίστοιχος αλγόριθμος είναι τάξεως n, όπου n το μέγεθος της λίστας καταχωρήσεων. Ο κβαντικός αλγόριθμος αναζήτησης καταφέρνει το ίδιο σε αριθμό βημάτων που είναι τάξεως $n^{1/2}$.

4.3.3.3 Cavity QED.

Μία τρίτη ερευνητική κατεύθυνση για την υλοποίηση κβαντικών υπολογιστών είναι αυτή με τη χρήση κοιλότητας κβαντικής ηλεκτροδυναμικής (cavity QED).

Πιο συγκεκριμένα, η κβαντική ηλεκτροδυναμική (QED) είναι μια κβαντική θεωρία του ηλεκτρομαγνητισμού που περιγράφει τις αλληλεπιδράσεις της ακτινοβολίας με την φορτισμένη ύλη. Η QED είναι μια σχετικιστική θεωρία από τις εξισώσεις της οποίας προκύπτουν οι εξισώσεις της ειδικής θεωρίας της σχετικότητας. Η κβαντική ηλεκτροδυναμική (που είναι βασικός κορμός των κβαντικών θεωριών πεδίου) θεωρεί ότι η ανάπτυξη των ηλεκτρομαγνητικών δυνάμεων αποδίδεται στην εκπομπή και την απορρόφηση φωτονίων ως σωματιδίων ανταλλαγής, τα οποία αντιπροσωπεύουν διαταραχές των ηλεκτρομαγνητικών πεδίων. Κατά τρόπο ανάλογο και τα ηλεκτρόνια μπορούν να θεωρηθούν ως διαταραχές αντίστοιχων κβαντισμένων πεδίων.

Αυτά όμως τα φωτόνια είναι εικονικά (virtual) δηλαδή δεν μπορούν να φανερωθούν ή να ανιχνευθούν με κανένα τρόπο επειδή η ύπαρξή τους παραβιάζει την διατήρηση της ενέργειας και της ορμής. Η ανταλλαγή σωματιδίων είναι όμοια με τη "δύναμη" της αλληλεπίδρασης, επειδή τα αλληλεπιδρώντας σωματίδια αλλάζουν την ταχύτητα και την κατεύθυνση της κίνησης τους καθώς αυτά ελευθερώνουν ή απορροφούν την ενέργεια ενός φωτονίου.Τα φωτόνια μπορούν

επίσης να εκπεμφθούν σε μια ελεύθερη κατάσταση, οπότε μόνο σ' αυτή την περίπτωση μπορούν να παρατηρηθούν. Η αλληλεπίδραση των δύο φορτισμένων σωματιδίων συμβαίνει σε μια σειρά διαδικασιών αυξανόμενης πολυπλοκότητας. Στον απλούστερο τρόπο, μόνο ένα εικονικό φωτόνιο μπορεί να περιληφθεί. Σε μια διαδικασία δεύτερης τάξης, υπάρχουν δύο φωτόνια και ούτω καθ' εξής.

Οι διαδικασίες αντιστοιχούν σε όλους τους πιθανούς τρόπους στους οποίους μπορούν να αλληλεπιδράσουν τα σωματίδια κάνοντας ανταλλαγή εικονικών φωτονίων. Η κατασκευή των κβαντικών υπολογιστών με αυτή τη μέθοδο, συνίσταται στην παγίδευση ουδέτερων ατόμων και στην πόλωση φωτονίων, όπως περιγράφηκε παραπάνω. Η κβαντική πληροφορία αποθηκεύεται σε εσωτερικές καταστάσεις των ατόμων και είναι εύκολο να δημιουργηθούν αλληλεπιδράσεις με τα qubits.

4.3.3.4 Τεχνολογία NMR.

Ο Πυρηνικός μαγνητικός Συντονισμός (NMR) είναι ένα φαινόμενο που έχει χρησιμοποιηθεί για τη δημιουργία κβαντικών υπολογιστών. Η τεχνολογία NMR έχει χρησιμοποιηθεί παλιότερα σε ιατρικές εφαρμογές και μία νέα προοπτική είναι και η χρήση της στους κβαντικούς υπολογιστές. Η τεχνολογία αυτή έχει το πλεονέκτημα ότι μπορεί να χρησιμοποιηθεί σε θερμοκρασία δωματίου και έχει αποδειχθεί ότι είναι εύκολο να κατασκευαστεί με αυτή ένας κβαντικός υπολογιστής των 2 ή 3 qubits. Η βασική ιδέα είναι ότι 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 NMR κβαντικού υπολογιστή είναι ίσος με τον αριθμό των ατόμων σε κάθε μόριο.

Εκμεταλλευόμενοι τις ιδιότητες του φαινομένου ερευνητές κατάφεραν μέσω NMR πειραμάτων να αναπτύξουν θεμελιώδη εργαλεία που μπορούν να χρησιμοποιηθούν σε πολλούς μελλοντικούς τύπους κβαντικών υπολογιστών. Αυτή η τεχνολογία έχει αποδειχθεί ότι εύκολα μπορεί να σχεδιάσει 2 ή 3 qubits NMR κβαντικά συστήματα. Όμως τελευταία προσομοιώθηκε ένας υπολογιστής των 7-qubit με τη 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. Βέβαια το φαινόμενο έχει κάποιες δυσκολίες όπως το γεγονός ότι είναι δύσκολο να διαχωριστούν τα qubits σε ένα μόριο από τις χημικές τους ιδιότητες στην περίπτωση μεγάλων μορίων. Επίσης είναι δύσκολο να αποσαφηνιστεί με ακρίβεια η αρχική κατάσταση. Είναι λοιπόν δύσκολο έως αδύνατο η τεχνολογία αυτή να χρησιμοποιηθεί σε υπολογιστές με περισσότερα από 12 qubits.

4.3.3.5 Μελλοντική Προοπτική.

Οι κβαντικοί υπολογιστές δεν είναι κατάλληλοι για όλες τις υπολογιστικές διεργασίες. Παραδείγματος χάριν δεν μπορούν να επιταχύνουν την επεξεργασία κειμένου ή την πλοήγηση στο διαδίκτυο. Το πιθανότερο είναι να χρησιμοποιηθούν υβρίδια κλασικών και κβαντικών υπολογιστών στο μέλλον. Η βασική μελλοντική τους εφαρμογή θα είναι η χρήση τους για την προστασία απόρρητων και προσωπικών δεδομένων γιατί θα είναι αδύνατο να μπορούν να εισέρχονται σε e-mails και τραπεζικούς λογαριασμούς χρηστών του διαδικτύου, λόγω της ασφάλειας που θα παρέχουν. Επίσης, η αναζήτηση πληροφορίας στο διαδίκτυο θα διεξάγεται πολύ πιο γρήγορα, εφόσον υπάρχει κβαντικός αλγόριθμος αναζήτησης δεδομένων σε λίστα ο οποίος είναι μικρότερης τάξεως από τον αντίστοιχο κλασικό.

Τέλος μία άλλη εφαρμογή που έχει χρήση και στην καθημερινή ζωή είναι η βελτίωση στη χρήση GPS δηλαδή συστημάτων που χρησιμοποιούνται σε αυτοκίνητα για να ανιχνεύεται μία θέση προς αναζήτηση. Αυτά τα συστήματα βασίζονται σε ρολόγια που λειτουργούν με βάση τις αρχές της κβαντομηχανικής. Οι κβαντικοί υπολογιστές θα μπορούν να βελτιώσουν αυτές τις ρυθμίσεις και η αναζήτηση με τα μηχανήματα να δίνει καλύτερα και πιο έγκυρα αποτελέσματα.

Όπως αναφέρθηκε υπάρχουν διάφορες τεχνολογίες για την υλοποίηση κβαντικών υπολογιστών. Μέχρι στιγμής ο πρώτος κβαντικός υπολογιστής 2 qubits παρουσιάστηκε το 1998 από την IBM, η οποία το 1999 παρουσίασε κβαντικό υπολογιστή τριών qubits με δυνατότητα κβαντικής διόρθωσης σφαλμάτων ενώ από την ίδια εταιρεία το 2000 παρουσιάστηκε κβαντικός υπολογιστής των πέντε qubits. Ο τελευταίος υπολογιστής που έχει κατασκευαστεί είναι 7 qubits από τους Vandersypen, Steffen, Breyta, Yannoni,Sherwood, και Chuang το 2001.

4.3.4 Κβαντικοί Αλγόριθμοι.

Οι κλασικοί υπολογιστές αποτελούνται από αγωγούς και λογικές πύλες, οι οποίες συγκροτούν κυκλώματα και επεξεργαστές. Οι αγωγοί μεταφέρουν την πληροφορία από πύλη σε πύλη όπου γίνεται η επεξεργασία της. Οι πύλες των κλασικών υπολογιστών είναι φυσικά συστήματα και η πληροφορία διέρχεται μέσα από αυτές. Στους κβαντικούς υπολογιστές η πληροφορία βρίσκεται αποθηκευμένη σε qubits ή σε κβαντικούς καταχωρητές και παραμένει εκεί. Οι κβαντικές πύλες δεν είναι φυσικά συστήματα, αλλά αντιπροσωπεύουν μετασχηματισμούς (εφαρμογή γραμμικών τελεστών) που ασκούνται σε μεμονωμένα qubits ή σε κβαντικούς καταχωρητές (ομάδες από qubits).

Οι κβαντικοί υπολογισμοί είναι δράσεις τελεστών που έχουν σαν αποτέλεσμα την περιστροφή διανυσμάτων στο χώρο Hilbert. Τα διανύσματα αυτά παριστάνουν τις κβαντικές καταστάσεις των κβαντικών καταχωρητών. Έχουν γίνει αρκετές προσπάθειες για να αναπαρασταθούν οι κβαντικοί υπολογισμοί με κάποιο μοντέλο. Το πιο επιτυχημένο μοντέλο, που σήμερα χρησιμοποιείται σχεδόν αποκλειστικά, είναι το κυκλωματικό μοντέλο των κβαντικών υπολογισμών.

Σύμφωνα με αυτό, κάθε κβαντικός υπολογισμός, απλός ή πολύπλοκος, μπορεί να αναπαρασταθεί με ένα κύκλωμα. Τα κυκλώματα που αναπαριστούν κβαντικούς υπολογισμούς ονομάζονται κβαντικά κυκλώματα και αποτελούνται από qubits, κβαντικούς καταχωρητές και κβαντικές πύλες. Στα κβαντικά κυκλώματα δεν

υπάρχει ροή πληροφορίας από πύλη σε πύλη, αλλά διαδοχικές δράσεις κβαντικών πυλών σε κβαντικούς καταχωρητές στους οποίους βρίσκεται αποθηκευμένη η πληροφορία. Τα κβαντικά κυκλώματα αναπαριστούν τη χρονική σειρά και τον τρόπο με τον οποίο δρουν οι κβαντικές πύλες στους κβαντικούς καταχωρητές.

4.3.4.1 Κβαντικοί υπολογισμοί.

Όλοι οι κβαντικοί υπολογισμοί που βασίζονται στο κυκλωματικό μοντέλο εκτελούνται με την παρακάτω διαδικασία:

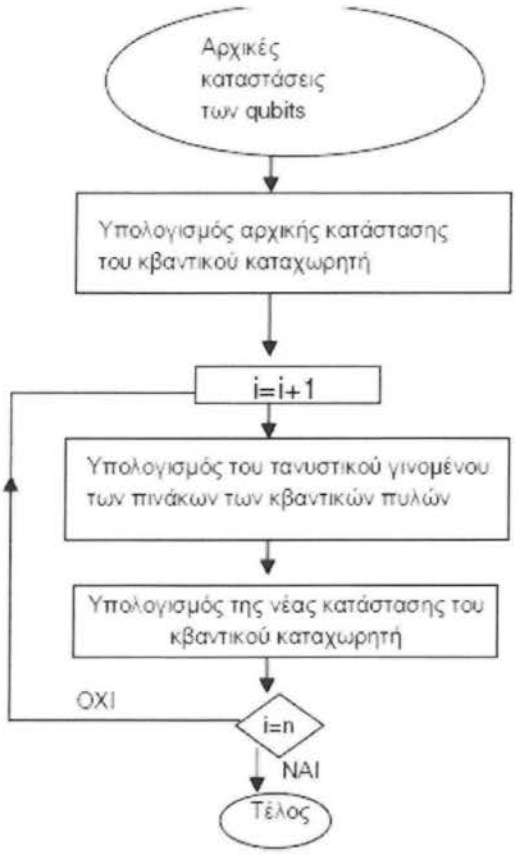
1. Δίνεται η αρχική κατάσταση των qubits που αποτελούν τον κβαντικό καταχωρητή. Υπολογίζεται το τανυστικό γινόμενο των πινάκων των καταστάσεων των qubits. Ο πίνακας που προκύπτει είναι η αρχική κατάσταση του κβαντικού καταχωρητή.

2. Υπολογίζεται το τανυστικό γινόμενο των πινάκων που περιγράφουν τις κβαντικές πύλες που δρουν στο επόμενο βήμα του κβαντικού υπολογισμού.

3. Ο πίνακας που προκύπτει από το τανυστικό γινόμενο των πινάκων των κβαντικών πυλών πολλαπλασιάζεται με τον πίνακα της νέας κατάστασης του κβαντικού καταχωρητή.

4. Τα 2 και 3 επαναλαμβάνονται τόσες φορές όσα και τα βήματα του κβαντικού υπολογισμού.

5. Η τελική κατάσταση του κβαντικού καταχωρητή είναι το αποτέλεσμα του κβαντικού υπολογισμού.



Εικόνα 91 Διάγραμμα Κβαντικών Υπολογισμών.

4.3.4.2 Κβαντικός Επεξεργαστής.

Μέχρι σήμερα δεν υπάρχει ένας προγραμματιζόμενος κβαντικός επεξεργαστής που να μπορεί να εκτελεί υπολογιστικά καθήκοντα. Για κάθε κβαντικό υπολογισμό συντίθεται και ένας κβαντικός επεξεργαστής, ο οποίος αποτελείται από έναν ή περισσότερους κβαντικούς καταχωρητές και από ένα σύνολο κβαντικών πυλών. Στους κβαντικούς υπολογιστές δεν υπάρχει σαφής διάκριση ανάμεσα στο υλικό και το λογισμικό όπως στους κλασικούς υπολογιστές. Σήμερα γίνεται έρευνα για να βρεθεί προγραμματιζόμενη αρχιτεκτονική για τους κβαντικούς υπολογιστές χωρίς ενθαρρυντικά αποτελέσματα.

4.3.4.3 Ο κβαντικός αλγόριθμος του Deutsch.

Ο πρώτος κβαντικός αλγόριθμος, δηλαδή ένας αλγόριθμος που να μπορεί να τρέξει σε έναν κβαντικό υπολογιστή, αναπτύχθηκε από τον Deutsch. Στον αλγόριθμο αυτό χρησιμοποιείται η κβαντική παραλληλία, δηλαδή η υπέρθεση των βασικών καταστάσεων των qubits και για πρώτη φορά ένας κβαντικός υπολογιστής μπορεί να εκτελέσει υπολογισμούς που είναι αδύνατο να εκτελεστούν από έναν κλασικό υπολογιστή.

Το πρόβλημα που έθεσε ο Deutsch είναι το εξής:

Δίνεται μία συνάρτηση f(x) τέτοια ώστε:

$$f(x): \{0,1\} \rightarrow \{0,1\}$$

Δηλαδή η μεταβλητή x και η συνάρτηση f(x) μπορούν να πάρουν μόνο τις τιμές 0 ή 1.

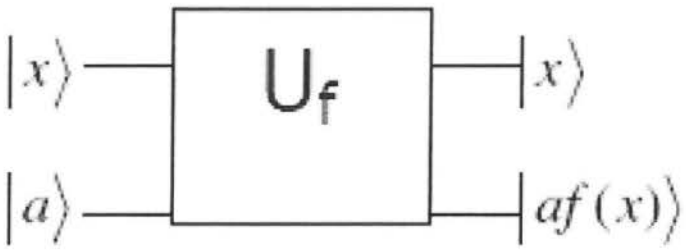
Για κάθε τέτοια συνάρτηση υπάρχουν δύο περιπτώσεις:

α) $f(0) = f(1)$, οπότε η συνάρτηση ονομάζεται σταθερή

β) $f(0) \neq f(1)$, οπότε η συνάρτηση ονομάζεται ισορροπημένη.

Αν για παράδειγμα δοθεί μία συνάρτηση f(x) και θέλουμε να δούμε αν είναι σταθερή ή ισορροπημένη κάνουμε τα εξής:

Αν χρησιμοποιήσουμε έναν κλασικό υπολογιστή θα πρέπει να υπολογίσουμε την τιμή f(0), στη συνέχεια να υπολογίσουμε την τιμή f(1) και να συγκρίνουμε τα αποτελέσματα. Αν είναι ίδια, τότε η συνάρτηση είναι ισορροπημένη. Δεν είναι δυνατό να αποφασιστεί τι είναι η συνάρτηση με έναν μόνο υπολογισμό. Αυτό όμως είναι δυνατόν αν χρησιμοποιήσουμε έναν κβαντικό υπολογιστή, σύμφωνα με τον αλγόριθμο του Deutsch.

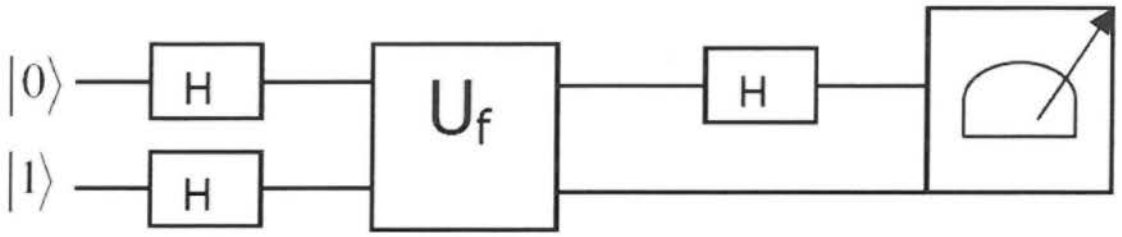


Εικόνα 92 Κβαντικό κύκλωμα που υπολογίζει το άθροισμα με βάση το 2.

Το κβαντικό αυτό κύκλωμα υπολογίζει το άθροισμα με βάση το 2 του πρώτου qubit με τη συνάρτηση f(x), όπου x το δεύτερο qubit .

Το παραπάνω αποτελείται από έναν κβαντικό καταχωρητή των δύο qubits όπου το πρώτο είναι το |a> και το δεύτερο το |x> , και από έναν συνδυασμό κβαντικών πυλών που παριστάνεται από το ορθογώνιο U_f. Για κάθε διαφορετική συνάρτηση f(x) χρειάζεται ένας διαφορετικός συνδυασμός κβαντικών πυλών. Ο συνδυασμός των κβαντικών πυλών U_f δρα στα δύο qubits και αφήνει το δεύτερο αμετάβλητο, ενώ φέρνει το πρώτο στην κατάσταση που αντιστοιχεί με το άθροισμα με βάση το 2 του πρώτου qubit |a> με τη συνάρτηση f(x), όπου x είναι το δεύτερο qubit.

Ο αλγόριθμος του Deutsch είναι και αυτός ένας κβαντικός υπολογισμός και περιγράφεται από το παρακάτω κύκλωμα. Η αρχική κατάσταση του πρώτου qubit είναι |1> και του δεύτερου |0> . Στο πρώτο βήμα του αλγορίθμου του Deutsch η κατάσταση του κβαντικού καταχωρητή είναι |01>. Στο δεύτερο βήμα δρουν δύο κβαντικές πύλες H. Στο τρίτο δρα ο συνδυασμός κβαντικών πυλών U_f και στο τέταρτο δρα η κβαντική πύλη H στο δεύτερο qubit. Στο τέλος του τέταρτου βήματος μετράται η κατάσταση του δεύτερου qubit. Αν το qubit αυτό βρεθεί στην κατάσταση |0>, τότε η συνάρτηση f(x) είναι σταθερή και αν βρεθεί στην κατάσταση |1>, τότε είναι ισορροπημένη.



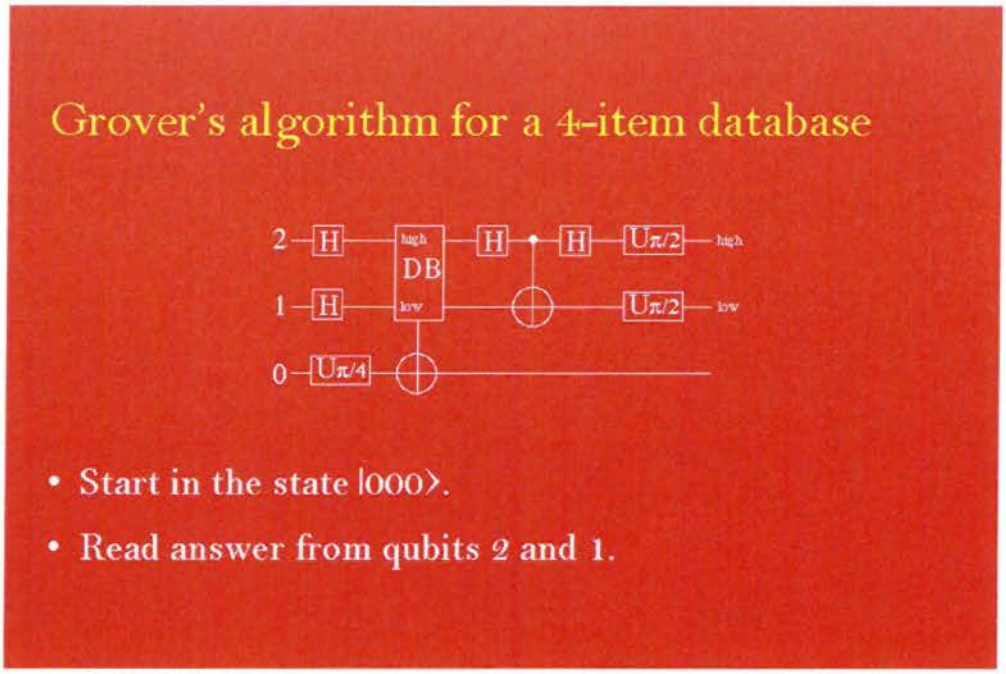
Εικόνα 93 Κβαντικός υπολογισμός με τον αλγόριθμο του Deutsch.

4.3.4.4 Ο κβαντικός αλγόριθμος του Grover.

Ο αλγόριθμος του Grover ερευνά μία δομημένη βάση δεδομένων που περιέχει N στοιχεία. Κάθε στοιχείο της βάσης έχει αριθμηθεί από 0 έως N-1. Το σύστημα που διαθέτουμε μπορεί να αναγνωρίσει αν κάποιο στοιχείο είναι αυτό που αναζητάμε ή όχι. Σε έναν κλασικό υπολογιστή το σύστημα αυτό είναι ένας καταχωρητής όπου έχουμε αποθηκεύσει τον αριθμό που ψάχνουμε να βρούμε και ένα κύκλωμα λογικών πυλών. Το κύκλωμα συγκρίνει κάθε αριθμό στην είσοδό του με τον αποθηκευμένο αριθμό. Το σύστημα αυτό ονομάζεται oracle.

Ο Grover επινόησε έναν κβαντικό αλγόριθμο ο οποίος μπορεί να ψάξει μία αταξινόμητη βάση δεδομένων και να την ταξινομήσει πολύ γρηγορότερα από ότι θα έκανε ένας κλασικός υπολογιστής. Κανονικά μία βάση δεδομένων με n στοιχεία θα έπαιρνε N/2 αριθμό αναζητήσεων για να βρεθεί το στοιχείο που αναζητείται αλλά σε έναν κβαντικό υπολογιστή ο αριθμός αναζητήσεων είναι της τάξεως $N^{1/2}$.

Μία άλλη εφαρμογή του αλγορίθμου είναι στον τομέα των κρυπτογραφημένων στοιχείων. Υποθέτουμε ότι έχουμε μία εικονική βάση δεδομένων που είναι τόσο μεγάλη που δεν θα ταίριαζε στις μνήμες των κλασικών υπολογιστών. Αυτό επιτρέπει στους κβαντικούς υπολογιστές να χρησιμοποιήσουν ένα ευρέως γνωστό σύστημα για την προστασία των δεδομένων. Αυτό είναι το σύστημα DES (Data Encryption Standard). Το σύστημα αυτό στηρίζεται σε έναν αριθμό 56 bits. Μία εξαντλητική αναζήτηση με τα συμβατικά μέσα θα απαιτούσε 2^{55} αναζητήσεις πριν βρεθεί το σωστό κλειδί. Ο αλγόριθμος του Grover θα μπορούσε να βρει το κλειδί μόνο μετά από 185 αναζητήσεις.



Εικόνα 94 Grovers Algorithm.

4.3.4.5 Ο αλγόριθμος του Shor.

Το 1994 ο Peter Shor απέδειξε ότι με τη χρήση κβαντικών υπολογιστών μπορεί εύκολα και γρήγορα να αναλυθούν σε γινόμενο δύο πρώτων αριθμών μεγάλοι ακέραιοι αριθμοί. Με έναν κβαντικό υπολογιστή απαιτείται πολυωνυμική αύξηση του χρόνου υπολογισμού για γραμμική αύξηση του μεγέθους n, δηλαδή του αριθμού των ψηφίων του αριθμού που έχει δύο πρώτους παράγοντες. Οι γρηγορότεροι κλασικοί αλγόριθμοι για το ίδιο πρόβλημα είναι υπερ-πολυωνυμικοί σε συνάρτηση με τον αριθμό ψηφίων n. Η μέθοδος που πρότεινε ο Shor είναι γνωστή ως κβαντικός αλγόριθμος του Shor.

Το πρόβλημα που λύνει ο κβαντικός αλγόριθμος του Shor είναι το εξής:

Αν δοθεί ένας ακέραιος αριθμός n, να βρεθεί η περίοδος της συνάρτησης $f_{n,a}(x)=a^x(\text{mod } n)$, όπου a είναι ένας τυχαίος ακέραιος που είναι πρώτος ως προς τον n. Εάν βρεθεί η περίοδος της συνάρτησης και εφόσον είναι άρτια (αυτό μπορεί

να κανονιστεί με κατάλληλη επιλογή του a), τότε οι πρώτοι παράγοντες του n είναι gcd(n, $a^{r/2}$ -1) και gcd(n, $a^{r/2}$ +1), όπου gcd(...) υποδηλώνει μέγιστο κοινό διαιρέτη.

Ο κβαντικός αλγόριθμος του Shor αρχίζει με δύο κβαντικούς καταχωρητές. Ο πρώτος ονομάζεται Reg1 και ο δεύτερος Reg2. Οι δύο κβαντικοί καταχωρητές αποτελούν έναν κβαντικό καταχωρητή που ονομάζεται Reg. Αν η κατάσταση του Reg1 είναι $|\psi_1\rangle$ και η κατάσταση του Reg2 είναι $|\psi_2\rangle$, η κατάσταση του Reg είναι η $|\psi\rangle$ που δίνεται από:

$$|\psi\rangle = |\psi_1\rangle\,|\psi_2\rangle = |\psi_1\psi_2\rangle = |\psi_1,\psi_2\rangle$$

Η αρχική κατάσταση του Reg είναι :

$$\psi\rangle = 0,0$$

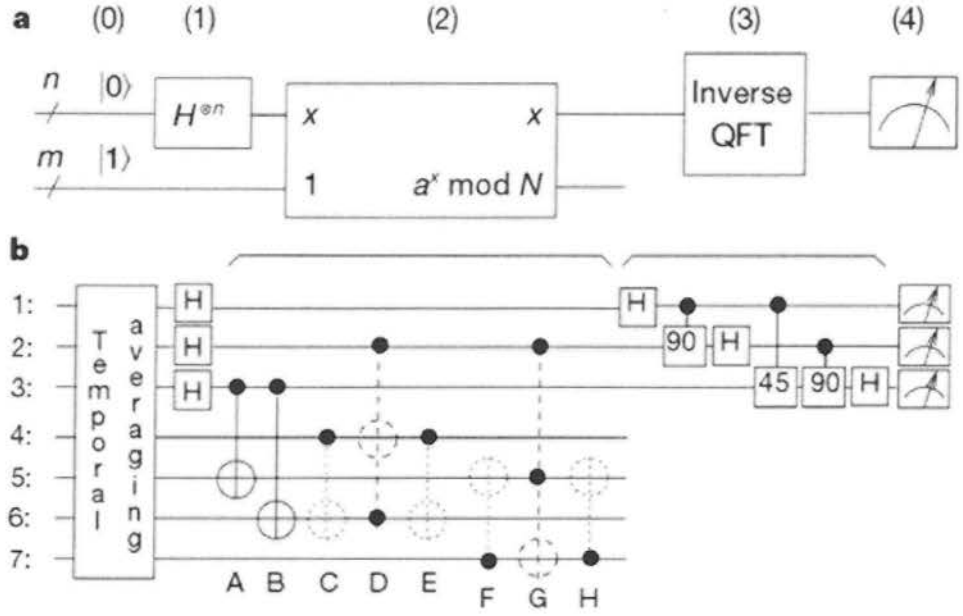
Φέρνουμε τον Reg1 σε κατάσταση υπέρθεσης όλων των βασικών καταστάσεων από 0 έως q-1. Ο Reg1 αποτελείται από τον κατάλληλο αριθμό από qubits. Στη συνέχεια υπολογίζεται η τιμή της f n,a(x) για κάθε x και τα αποτελέσματα καταγράφονται στον Reg2 ο οποίος κρατά την υπέρθεση όλων των τιμών της $f_{n,a}(x)$.

Κατόπιν γίνεται μέτρηση της κατάστασης του Reg2. ο Reg2 βρίσκεται σε υπέρθεση όλων των τιμών της $f_{n,a}(x)$, όμως το αποτέλεσμα της μέτρησης θα δώσει μόνο μία τιμή της συνάρτησης για παράδειγμα την k. Δηλαδή μετά τη μέτρηση ο Reg2 βρίσκεται στην κατάσταση $|k\rangle$.

Αφού λοιπόν ο Reg2 βρίσκεται στην κατάσταση $|k\rangle$, εξαιτίας της κβαντικής διεμπλοκής στον Reg1 θα βρίσκονται πια μόνο οι αριθμοί x για τους οποίους ισχύει:

$$f_{n,a}(x)=a^x(\text{mod } n)=k$$

Τα πλάτη πιθανότητας όλων των καταστάσεων είναι ίσα μεταξύ τους, όπου r είναι η ζητούμενη περίοδος της συνάρτησης.



Εικόνα 95 Shor's Algorithm.

Κεφάλαιο 5°: Από την θεωρία στην υλοποίηση Κβαντικών Υπολογιστών.

5.1 Κβαντικός υπολογιστής της Google.

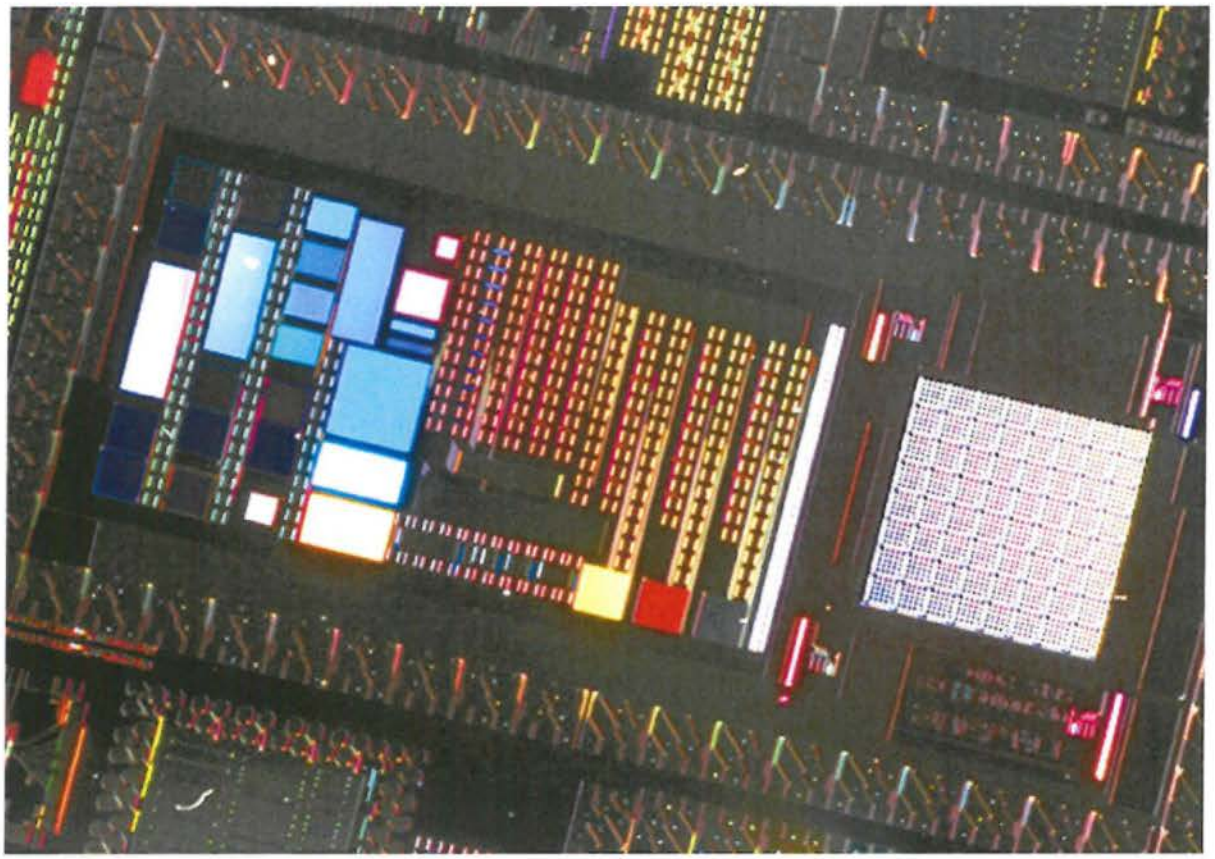
Πέρυσι, Google και NASA συνεργάστηκαν για τη δημιουργία ενός εργαστηρίου τεχνητής νοημοσύνης, στο οποίο θα χρησιμοποιείται ένας κβαντικός υπολογιστής D-Wave Two. Ο στόχος ήταν να μελετήσουν πως μαθαίνουν οι μηχανές, πως δουλεύουν με πρότυπα πληροφορίας και πως βελτιώνουν τις εξόδους τους. Παρά το γεγονός πως ο κβαντικός υπολογιστής βοήθησε την Google σε λειτουργίες του Google Glass, αυτός απέτυχε στο πρώτο benchmark speed test χρησιμοποιώντας τον αλγόριθμο της Google.

Θεωρητικά, οι κβαντικοί υπολογιστές είναι πιο γρήγοροι. Αντίθετα με τους ηλεκτρονικούς υπολογιστές που γνωρίζουμε, οι οποίοι χειρίζονται υπολογισμούς σειρών από 0 και 1 (bit) , οι κβαντικοί υπολογιστές μπορούν να "στριμώξουν" τα 0 και 1 στον ίδιο χρόνο (qubit aka κουμπίτ' :P). Η βασική ιδέα είναι πως ο κβαντικός υπολογιστής μπορεί να κάνει πολλούς υπολογισμούς ταυτόχρονα, κάνοντας τον έτσι πολύ πιο γρήγορο από τον ηλεκτρονικό υπολογιστή. Δυστυχώς όμως, αυτή τη φορά δεν συνέβη κάτι τέτοιο στον συγκεκριμένο αλγόριθμο της Google.

Στο τεστ ταχύτητας, ο D-Wave Two κοντραρίστηκε με ένα συνηθισμένο PC. Υπήρχαν στιγμές όπου ο D-Wave αποδείχθηκε ελαφρώς γρηγορότερος στη λύση προβλημάτων, όμως σε άλλες ήταν πιο αργός από το PC. Ακόμη και για τα σημεία όπου ήταν πιο γρήγορος όμως, εάν υπολογίσουμε τον χρόνο που απαιτείται για την διαμόρφωση του D-Wave έτσι ώστε να τρέξει τον αλγόριθμο (κάτι που δε χρειάζεται στο PC), το PC φαίνεται πάλι ταχύτερο. Το ίδιο απογοητευτικά ήταν και τα αποτελέσματα από την χρήση του πάνω σε δεδομένα της NASA για την αποστολή Kepler, που αφορά την αναζήτηση για εξωπλανήτες. Οι επιστήμονες ήλπιζαν πως ο κβαντικός υπολογιστής θα μπορούσε να ανακαλύψει πλανήτες που αυτοί δεν μπόρεσαν, όμως ο D-Wave δεν έβγαλε κανένα νέο συμπέρασμα.

Ωστόσο, η Google φαίνεται πως δεν ενδιαφέρεται τόσο πολύ για την ταχύτητα, καθώς θεωρεί τις δυνατότητες του D-Wave πάνω στην εκπαίδευση μηχανών πολύ σημαντικότερες. Η εταιρεία έτρεξε επιτυχώς τον αλγόριθμο εντοπισμού blink στο

Google Glass στον κβαντικό υπολογιστή προτού αυτή η δυνατότητα δόθηκε στο κοινό μέσω των τελευταίων ενημερώσεων.



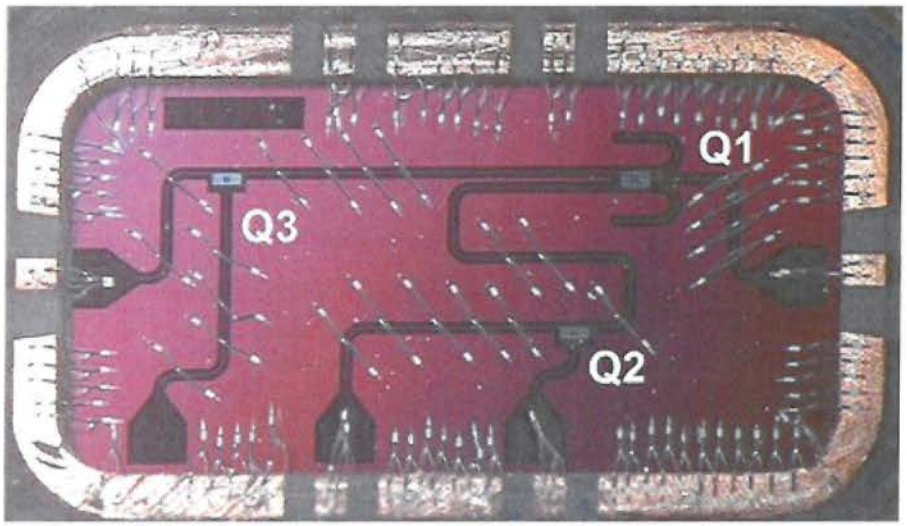
Εικόνα 96 Google Quantum computer.

Αυτή η επιστημονική περιοχή είναι σχετικά νέα, και όπως πάντα, υπάρχουν ακόμη πολλά πράγματα που δεν κατανοούμε. Η D-Wave πάντως δεν αγχώνεται: μέσα στον χρόνο θα κυκλοφορήσει νέος κβαντικός υπολογιστής 1.000 qubit (ο D-Wave Two είναι 512 qubit) και πιστεύουν πως αυτός θα μπορέσει να κατατροπώσει έναν κλασικό υπολογιστή.

5.2 Κβαντικός Υπολογιστής IBM.

Τεχνολογία που αναπτύσσει η IBM μας φέρνει ένα βήμα πιο κοντά στους κβαντικούς υπολογιστές, οι οποίοι πρόκειται να είναι πιο γρήγοροι από οποιονδήποτε υπε-ρυπολογιστή κυκλοφορεί σήμερα στη Γη. Οι κβαντικοί υπολογιστές χρησιμοποιούν το κβαντικό bit (qubit) ως μονάδα πληροφορίας, το οποίο μπορεί να πάρει τις τιμές 0 και 1 ταυτόχρονα, σε αντίθεση με τους σημερινούς υπολογιστές όπου το bit μπορεί να αναπαρασταθεί με μόνο μία από τις δύο τιμές σε κάθε χρονική στιγμή.

Οι επιστήμονες της IBM υποστηρίζουν ότι έχουνε βρει ένα νέο τρόπο να επεκτείνουν το χρόνο τον οποίο τα qubits διατηρούν την κβαντική τους κατάσταση, μειώνοντας με τον τρόπο αυτό τα λάθη στους υπολογισμούς. "Στο παρελθόν πιστεύαμε ότι ήταν θέμα 50 χρόνων η κατασκευή ολοκληρωμένων κβαντικών συστημάτων. Σήμερα πιστεύω ότι απέχουμε 15 χρόνια ή και λιγότερο από κάτι τέτοιο" αναφέρει στην New York Times ο Watson, υπεύθυνος στο τμήμα Φυσικής της IBM.



Εικόνα 97 Κβαντικό Κύκλωμα από την IBM.

Ο χρόνος στον οποίο οι επιστήμονες της IBM κατάφεραν τα qubit να κρατήσουν την κατάστασή τους είναι τα 100μs, αρκετά μικρός αν το σκεφτεί κανείς αλλά είναι ο διπλάσιος ή ακόμη και τετραπλάσιος χρόνος από τις προηγούμενες καταγραφές. Η εταιρεία αναφέρει ότι βρίσκεται πολύ κοντά στις ελάχιστες

απαιτήσεις που χρειάζονται για την κατασκευή ενός κβαντικού συστήματος, όπως αυτές ορίζονται από την επιστημονική κοινότητα, ενώ το επόμενο βήμα είναι η κατασκευή κβαντικών συστημάτων βασιζόμενα στην υπάρχουσα τεχνολογία.

5.3 Κβαντικός Υπολογιστής D-Wave.

Ο D Wave II είναι ένας υπολογιστής αλλά όχι ένας απλώς γρήγορος πολύπλοκος υπολογιστής, είναι ένας κβαντικός υπολογιστής. Από τη στιγμή που η λέξη κβαντικό έρχεται στο προσκήνιο είναι επόμενο το όλο θέμα να περνά στη χώρα της ομίχλης και του μυστηρίου, μιας και κάθε τι που είναι σχετικό με τη κβαντική επιστήμη φαντάζει D WAVE QUANTOM COMPUTERπερισσότερο ως ταινία επιστημονικής φαντασίας παρά ως μια εφαρμοσμένη πραγματικότητα. Ο D Wave II είναι ο διάδοχος του D Wave I κατασκευασμένος στο Καναδά από την ομώνυμη εταιρεία και ανακοινώθηκε επίσημα το 2011. Αμέσως ο το μεγαθήριο της παγκόσμιας αγοράς οπλικών συστημάτων Lockeed Martin έσπευσε να τον αποκτήσει. Ο διάδοχος του κατασκευάστηκε με την οικονομική συνδρομή του Τζεφ Μπέζος, και αυτή τη στιγμή η Google τον «μοιράζεται» με τη NASA στα εργαστήρια της οποίας έχει εγκατασταθεί το όλο σύστημα.

Ο D Wave είναι της τάξης των 512 qubits και σαν καλός κβαντικός υπολογιστής που σέβεται τον εαυτό του, οι δυνητικές ικανότητες του είναι αστρονομικές σε σχέση με τις αντίστοιχες των κοινών θνητών pc κάθε είδους. Οι τελευταίοι λειτουργούν με τα κοινά bits που μπορούν να πάρουν τη τιμή 0 ή 1 κάθε φορά. Αντίθετα το qubit ακολουθώντας τους νόμους του μικρόκοσμου μπορεί να βρεθεί σε κατάσταση 1 ή 0, ή και τα δύο συγχρόνως. Αποτέλεσμα να μπορεί να πραγματοποιεί κάθε είδους πράξης μερικές χιλιάδες φορές πιο γρήγορα από το ταχύτερο συμβατικό υπολογιστή. Η ύπαρξη ενός τέτοιου μεγαθηρίου ξεκλειδώνει μια σειρά από πιθανότητες που έχουν σεβαστό ποσοστό να γίνουν πραγματικότητες.

Εικόνα 98 Κβαντικός Υπολογιστης D-Wave II.

Απλούστερα μόνο η φαντασία μπορεί θέσει όρια στα επιτεύγματα που μπορούν να πραγματοποιηθούν με την υπολογιστική ισχύ κβαντικού πλέον τύπου. Φυσικά οι επικοινωνιολόγοι της Google έχουν αρχίσει την εκστρατεία τους για την ενημέρωση του κοινού για το τι και πως σχετικά με τις δυνάμεις του D Wave II, για τα πεδία έρευνας στα οποία έχουν σκοπό να προσανατολιστούν όπως τα αναμενόμενα, υγεία, επιστημονική πρόοδο για την κατανόηση και πρόβλεψη πιθανοτήτων κλπ. Αυτό είναι η μια πλευρά του θέματος. Η άλλη είναι πως ο καθένας με την απλή λογική του μπορεί να σκεφθεί ότι οι προτεραιότητες δεν θα είναι τουλάχιστον μόνο αυτές. Τι πιο λογικό από το να χρησιμοποιηθεί ο D Wave II για να «γεννηθεί» ο D Wave III, των 1024 qubits και πάει λέγοντας. Παράλληλα η AI του ίδιου του υπολογιστή αναμένεται να εκτιναχθεί με ότι συνεπάγεται αυτό. Και συνεπάγεται σίγουρα πολλά, πολύ περισσότερα τουλάχιστον από ότι η Google ανακοινώνει στην επικοινωνιακή εκστρατεία «ενημέρωσης» της.

Η επίσημη παραδοχή της ύπαρξης ενός τέτοιου συστήματος, σηματοδοτεί αυτόματα μια νέα εποχή στο τομέα της εξέλιξης καθώς χρήση συνεπάγεται την

αναβάθμιση του και παράλληλα αυτό που γρήγορα θα διαπιστώσουμε όλοι μας σε καταναλωτικό επίπεδο, και φυσικά όχι μόνο, την εμφάνιση νέων τεχνολογιών κάθε είδους. Το τι μπορεί να καταφέρει ένας κβαντικός υπολογιστής είναι θολό και αρκετά δυσνόητο όπως η ίδια η κβαντική φυσικά. Πέρα από όλα αυτά όμως για μια ακόμη φορά τα σημάδια των καιρών δείχνουν το αυτονόητο. Το μέλλον είναι ήδη εδώ και είναι πιο παράξενο από ότι το φανταζόμασταν.

Κεφάλαιο 6°: Συμπεράσματα.

Στην εργασία αυτή επιχειρήθηκε μία σύντομη εισαγωγή στο χώρο των κβαντικών υπολογιστών και των κβαντικών κυκλωμάτων. Αρχικά παρουσιάστηκε η ιστορία της κβαντικής θεωρίας, οι αρχές της στη συνέχεια η Θεωρία πληροφορικής, οι αρχές της καθώς επίσης και η Θεωρία Πληροφορίας και οι αρχές της.

Στη συνέχεια σε μια προσπάθεια σύνθεσης όλων των Θεωριών μπορούμε να πούμε οι συντέλεσε στην δημιουργία της Κβαντικής Θεωρίας Πληροφορίας.

Περιγράφηκε η πορεία προς την ανακάλυψη και σύνθεση των κβαντικών υπολογιστών και των κβαντικών αλγορίθμων. Παρουσιάστηκαν οι κβαντικές πύλες και η λειτουργία τους. Η μελέτη πολλών ερευνητικών εργασιών με βοήθησε στη σύνθεση του τελευταίου κεφαλαίου του άρθρου.

Παρατέθηκαν αναλυτικά ή και περιληπτικά μέθοδοι για τη δημιουργία κβαντικών κυκλωμάτων και παρουσιάστηκαν οι βελτιώσεις που έχουν σημειωθεί στη σύνθεσή τους.

Γενικά, η δημιουργία βέλτιστων κυκλωμάτων είναι στόχος και πεδίο έρευνας πολλών ερευνητών, καθόσον είναι κρίσιμης σημασίας για την υλοποίηση κβαντικών υπολογισμών στο μέλλον.

Πίνακας Εικόνων

Βιβλιογραφία

[1] Abbas Edalat (2003), Quantum Computing, Journal of Experimental and Theoretical Physics 102 (3), pp. 466-474.

[2] Adriano Barenco, et al. (1995), Elementary gates for quantum computation, European Physical Journal D 38 (2), pp. 375-379.

[3] Ahn C., Wiseman H.M., Milburn G.J.(2003) ,Quantum error correction for continuously detected errors, Physical Review A - Atomic, Molecular, and Optical Physics 67 (5), pp. 523101-5231011.

[4] Alber G., Delgado A., Mussinger M. (2002), Quantum error correction and quantum computation, Laser Physics 12 (4), pp. 742-750.

[5] Bennett C.H. (2003), Quantum Information: Qubits and Quantum Error Correction, International Journal of Theoretical Physics 42 (2), pp. 153-176.

[6] Bennett C.H., Bernstein E., Brassard G., Vazirani U. (1997), Strengths and weaknesses of quantum computing, SIAM Journal on Computing 26 (5), pp.1510-1523.

[7] Boykin, et al. (2002) , Algorithmic cooling and scalable NMR quantum computers, Proceedings of the National Academy of Sciences of the United States of America 99 (6), pp. 3388-3393.

[8] Chiaverini J., et al. (2004),Realization of quantum error correction, Nature 432 (7017), pp. 602-605.

[9] Colin P. Williams and Alexander G. Gray , Automated design of quantum circuits, Lecture notes in Computer Science 60(4), pp. 113-120.

[10] Daniel Neuenschwander (2001), Factorization with Quantum Computers: Shor s Algorithm, Applied Mathematics and Computation (New York) 174 (2),pp. 1363-1369.

[11] David P. DiVincenzo (1994), Two-bit gates are universal for quantum computation, Physical Review A, 51, pp. 1015-1022.

[12] DiVincenzo D.P.,et al. (2000), Universal quantum computation with the exchange interaction , Nature (London) 408, 339-342,quant-ph/0005116.

[13] Dmitri Maslov , Gerhard W. Dueck (2004), Improved Quantum Cost for n-bit Toffoli Gates, Electronics Letters 39 (25), pp. 1790-1791.

[14] E. Knill (1995), Approximation by quantum circuits, Superconductor Scienceand Technology 19 (5), pp. S350-S353 .

[15] Farrokh Vatan , Colin P. Williams (2004), Realization of a General Three - Qubit Quantum Gate, Journal of Applied Polymer Science 100 (4), pp. 3111-3115.

[16] G. Kato (2005), Grover like Operator Using Only Single-Qubit Gates, Nuclear Physics B - Proceedings Supplements 157 (1), pp. 162-166.

[17] G. Vidal and C. M. Dawson (2003), quant-ph/0307177.

[18] Goto A., et al. (2004) , Efficiency of the optical pumping qubit initializer for solid-state NMR quantum computers, Journal of Magnetism and Magnetic Materials 272-276 (SUPPL. 1), pp. e1669-e1670.

[19] Grassl, Markus (2000), Methods of quantum error correction, Proceedings - IEEE International Symposium on Circuits and Systems 1, pp. I-740-I-743.

[20] Grover, L.K. (1998), Quantum computers can search rapidly by using almost any transformation, Physical Review Letters 80 (19), pp. 4329-4332.

[21] http://dimitris.webgalaxy.gr/science-quantum-mechanics-ennoies.php

[22] http://el.wikipedia.org/

[23] Josef Gruska (1999), Quantum Computing, Cambridge, McGraw-Hill Publishing Company.

[24] Jun Zhang1, Jiri Vala, Shankar Sastry, Birgitta Whaley (2003), Optimal quantum circuit synthesis from Controlled-U gates, Journal of Computational Physics 215 (1), pp. 384.

[25] Levitin, Toffoli, Walton (2002), Operation Time Of Quantum Gates, Physical Review A - Atomic, Molecular, and Optical Physics 72 (3), pp. 1-8.

[26] Levitin, Toffoli,Walton (2002), Operation Time Of Quantum Gates, Physical Review A - Atomic, Molecular, and Optical Physics 72 (3), pp. 1-8.

[27] Makhlin, Shnirman (1999), Josephson-junction qubits with controlled couplings, Nature 398 (6725), pp. 305-307.

[28] Mikko M¨ott¨onen, Vartiainen, Bergholm, Salomaa (2004), Quantum circuits for general multi-qubit gates, Journal of the Mechanics and Physics of Solids 54 (6), pp. 1276-1303.

[29] Milburn G.J., Sarovar M., Ahn C.(2005),Quantum control and quantum error correction, 5th Asian Control Conference 1, pp. 33-41.

[30] Myers, Fahmy, Glaser, Marx (2001), Rapid solution of problems by nuclearmagnetic - resonance quantum computation, Physical Review A. Atomic, Molecular, and Optical Physics 63 (3), pp. 323021-323028.

[31] Norman Margolus and Lev Levitin (1998), "The maximum speed of dynamical evolution," Physica D 120, 188-195.

[32] Pesic, P. (2000), Identity and the foundations of quantum theory, Foundations of Physics Letters 13 (1), pp. 55-67

[33] Peter Shor (1994), algorithms for quantum computation, In Proceedings of 35th IEEE FOCS, pp. 124-134.

[34] Peter Shor (2002), introduction to quantum algorithms, Quantum Information Processing 5 (1), pp. 31-41.

[35] Peter W. Shor (2004), Progress in Quantum Algorithms, Quantum Information Processing 3 (1-5), pp. 5-13.

[36] Phil Gossett (1998), Quantum Carry-Save Arithmetic, Journal of Luminescence 119-120 (SPEC. ISS.), pp. 193-197.

[37] Physics4u.gr/articles/quantuminfo.html.

[38] Pollatsek H. (2001), Quantum error correction: Classic group theory meets a quantum challenge, American Mathematical Monthly 108 (10), pp. 932-962.

[39] Poyatos J.F., Cirac J.I., Zoller P. (2000), From Classical to Quantum Computers. Quantum Computations with Trapped Ions, Physica Scripta T 86, pp. 72-75.

[40] Rohit Khandekar (2004), Quantum error correction, Physical Review B - Condensed Matter and Materials Physics 71 (11), pp. 1-12.

[41] S. Gulde, et al. (2002), Quantum information processing and cavity QED experiments with trapped Ca+ ions, SIAM Journal on Computing 26 (5), pp.1484-1509.

[42] Sarovar M., Milburn G.J. (2005),Continuous quantum error correction, Proceedings of SPIE - The International Society for Optical Engineering 5842, pp.158-166.

[43] Shende V.V., Bullock S.S., Markov I.L (2004), Recognizing small-circuit structure in two-qubit operators, Physical Review A - Atomic, Molecular, andOptical Physics 70 (1), pp. 012310-1-012310-5.

[44] Simon D.R. (1997), On the power of quantum computation, SIAM Journal on Computing 30(4), pp. 1203-1218.

[45] Sloyd S., (1993) , A realizable quantum computer, Science 261 (5128), pp.1569-1571.

[46] Stephen S. Bullock(2006), Note on the Khaneja Glaser Decomposition, Quantum Information and Computation 4 (5), pp. 396-400.

[47] Tamulis A., Tamuliene J., Tamulis V., Ziriakoviene A. (2003), Quantum mechanical design of logic elements of NMR molecular quantum computers, Nonlinear Optics Quantum Optics 30 (3-4), pp. 285-300.

[48] V. V. Shende, et al. (2003), quant-ph/0308033.

[49] Valiev K.A., Kokin A.A. (1999), Semiconductor NMR Quantum Computers with Access to Individual Qubits and to an Ensemble of Qubits, Russian Microelectronics 28 (5), pp. 277-286.

[50] Vatan, F., Williams, C. (2004), Optimal quantum circuits for general twoqubit gates, Physical Review A - Atomic, Molecular, and Optical Physics 69 (3),pp. 032315-1.

[51] Y.-S. Lee, et al. (1999), Quantum Correlations and Intraband Coherences in Semiconductor Cavity QED, Physical Review Letters 83 (25), pp. 5338-5341.

[52] Zalka, (1999), Grover's quantum searching algorithm is optimal, Physical Review A - Atomic, Molecular, and Optical Physics 60 (4), pp. 2746-2751.

[53] Αντωνιάδης Ιωάννης, Σημειώσεις Μαθήματος Κβαντικών Υπολογιστών και Κβαντικής Κρυπτογραφίας, Τμήμα Πληροφορικής ΑΠΘ.

[54] Βασίλειος Ζορκάδης, Θεωρία Πληροφορίας και κωδικοποίησης, Ελληνικό Ανοιχτό Πανεπιστήμιο, Πάτρα 2002.

[55] Ηλίας Λυπιτάκης, Εισαγωγή στην επιστήμη των Υπολογιστών, Ελληνικό Ανοιχτό Πανεπιστήμιο, Πάτρα 2000.

[56] Καραφυλλίδης Ιωάννης (2005), Κβαντικοί Υπολογιστές, Αθήνα,Κλειδάριθμος.

[57] Κροντήρης Ιωάννης (2000), Κβαντική Θεωρία της Πληροφορίας,Διδακτορική Διατριβή, Πανεπιστήμιο Ηρακλείου.