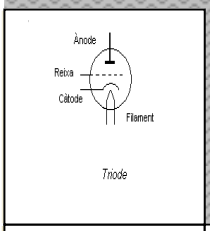
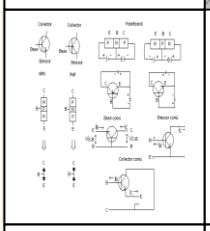
2011

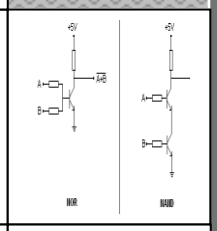
TFC

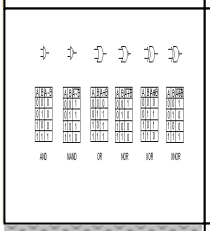
Computadors: del bit al qubit

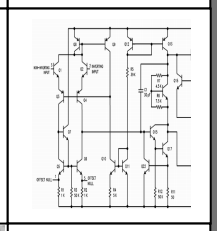
Desenvolupament dels computadors electrònics des dels seus orígens.

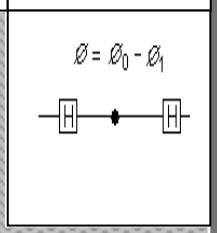


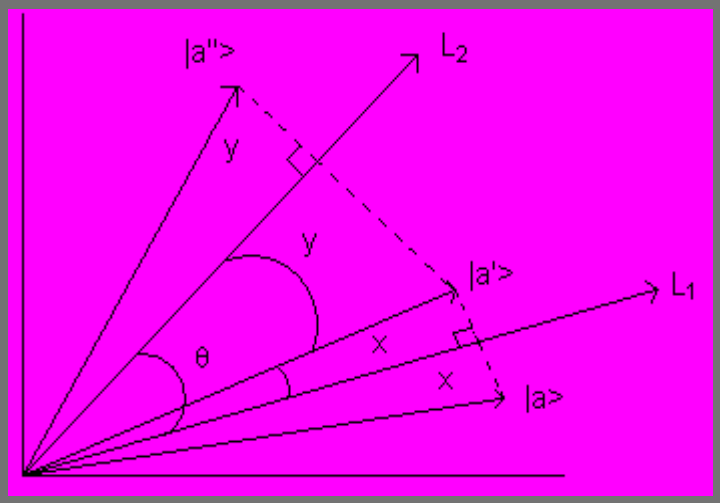












Francesc Guim Bernat (Tutor)
Josep Torras Font (ETIS)

04/04/2011

Índex

- Portada....1
- Índex....2

1. Motivació....5

2. Objectius....6

3. Resultats....7

4. Organització del document....7

5. Introducció....8

6. Desenvolupament dels computadors electrònics....9

7. Primera generació 10

7.1 Vàlvules, resistències i condensadors....10

7.1.1 Com funciona una vàlvula....11

7.1.2 Que és una resistència....13

7.1.3 Que és un condensador....14

7.2 Computadors de la primera generació....15

7.3 Fi de la primera generació....16

8. Segona generació....16

8.1 Que és un transistor....17

8.2 Que és la memòria de ferrita....19

8.3 Màquines a la segona generació....21

8.4 Fi de la segona generació....23

9. Tercera generació....23

9.1 Portes lògiques....24

9.1.2 Com funciona un circuit sumador i un multiplicador....25

9.2 Circuits Integrats....29

9.3 Visió d'aquesta generació....34

9.4 Fi de la tercera generació....35

10. Quarta generació....35

10.1 El microprocessador....35

10.2 Tipus de màquines....39

10.3 Final de la quarta generació....40

11. Cinquena generació....40

11.1 Tecnologia en aquesta generació....41

12. Sisena generació....42

12.1 Avanços de les dues últimes dècades....48

13. Visió general del desenvolupament dels sistemes operatius....48

14.1 Dispositius mòbils: evolució....50

14.2 Sistemes operatius que donen suport en els dispositius mòbils....52

15. Alternatives tecnològiques per a nous computadors....53

16. Breu introducció a la computació quàntica....54

16.1 Qubit, portes i xarxes....60

16.1.1 Qubit....60

16.1.2 Portes lògiques i xarxes....61

16.2 Aritmètica quàntica i avaluació de funcions....65

16.3 Algorismes i la seva complexitat....68

16.4 Des de interferòmetres a computadors....71

16.5 Els primers algorismes quàntics....75

16.6 Cerca quàntica....77

16.7 Estimació òptima de la fase....79

16.8 Periodicitat i factorització quàntica....80

16.9 La dinàmica quàntica condicional....82

16.10 Decoherència i recoherència.....83

- Annex I.....97
- Annex II.....104
- Annex III.....108
- Annex IV.....124
- Annex V.....125
- Annex VI.....127

1. Motivació

A principis de la dècada dels 50 del passat segle, es va construir el primer computador completament electrònic i que estava construït amb vàlvules de buit. La seva capacitat de càlcul, les seves dimensions i els costos tant de construcció com de manteniment varen ser enormes. Des d'aquella època fins els nostres dies, l'evolució dels computadors ha estat molt gran. De fet, ha estat en el transcurs de les dues últimes dècades quan aquesta evolució ha experimentat un avanç brutal i que ha originat un canvi en els hàbits de relació, treball, lleure, etc. de gran part de la societat. Aquesta evolució s'ha donat gràcies els avenços tecnològics en àrees tècniques de diverses branques de la física que han fet possible el desenvolupament de circuits cada cop més densos, és a dir han aconseguit introduir més circuits en una mateixa superfície. A mitjà termini però, ja s'entreveu que s'arribarà al límit del nivell de densitat d'integració degut a que les minses dimensions dels components integrats ja superaran la barrera de la física tradicional (o diguem-ne Newtoniana) per passar a obeir les lleis de la física quàntica. Com a conseqüència, els circuits deixen de funcionar amb la lògica preestablerta esdevenint inservibles. La única possibilitat de millorar les prestacions dels microprocessadors per tal d'aconseguir cotes més elevades d'execució d'instruccions en un temps més reduït consisteix en afegir nuclis. Això llògicament comporta un augment d'espai i de consum. De moment és la única sortida que actualment veiem quan arribi aquest moment però això pot canviar molt probablement en el transcurs aproximadament d'una dècada. En l'actualitat i encara a nivell experimental s'està avançant en un nou tipus de "processador" que està basat amb la mecànica quàntica. Primer i ja fa uns anys es va dissenyar a nivell teòric i més tard es va començar a experimentar a nivell de laboratori. És tracta d'un concepte completament nou, molt complex però amb una potència incomparable amb el circuits que estem usant actualment. Veritablement, en el moment que estigui enllestit i sigui possible extendre'l en el seu ús com ho són ara els actuals computadors, és previsible que generin un gran impacta social degut a que es podran accelerar molts processos en un ventall de camps multidisciplinaris ampli anticipant resultats previstos a anys vista. Això provocarà un canvi en la visió general del món que ens envolta. Per exemple podrem veure com es resolent problemes que fins ara es consideraven irresolubles degut a la seva complexitat exponencial, també en un altre ordre de coses veurem com els algorismes actuals de xifrat que es consideren segurs (RSA, ElGamal, etc.) deixaran de ser-ho, en el camp de la biologia, en desxiframent del codis genètics també es donarà un gran impuls, en astrofísica, etc.

En resum des del seu origen, els computadors han estat una eina clau per el desenvolupament multidisciplinari i la seva evolució sobretot en les dues últimes dècades ha estat vertiginosa. En el moment actual estem en una corba evolutiva pràcticament plana tot esperant la materialització d'un nou tipus que marcarà un abans i un després i que s'aventura com una veritable revolució social i tecnològica.

2. Objectius

Aquest treball pretén, en primer lloc, donar una visió clara de l'evolució dels computadors (merament electrònics) des dels orígens fins a l'actualitat aprofundint en la seva estructura interna per tal de fer-nos una idea de la seva complexitat actual. També veurem com una estructura de computador té aplicacions molt més especialitzades en el mon industrial i en el de les comunicacions i oci. De igual manera anirem veient com els sistemes operatius han anat evolucionant per tal d'aprofitar el màxim les potencialitats que el nou hardware en continua evolució anava aportant tan en el mon del PC com en els dispositius mòbils. Pensem que en el sector de la telefonia mòbil i de les tablets també hi ha hagut una gran evolució i que amb tota probabilitat són actualment productes de major consum i cada cop més van adquirint majors funcionalitats. Al darrera d'això també hi ha una evolució dels sistemes operatius i llenguatges de programació que permeten treure el màxim rendiment a aquesta tecnologia. Finalment mirarem el futur que ens espera i intentarem aprofundir al màxim en la vesant conceptual dels sistemes computacionals basats o regits per les lleis de la mecànica quàntica. Veurem la potencialitat que aquests nous sistemes seran capaços d'oferir i veurem com això afectarà a totes les coses de la nostra vida quotidiana. Entrarem en un terreny que possiblement ens pot arribar a canviar part de la nostra lògica i manera de veure i enfocar els problemes.
Per tant la llista d'objectius la podríem resumir de la següent manera:

1. Tenir una visió de l'evolució dels computadors així com dels sistemes operatius.
2. Conèixer i entendre el funcionament dels elements bàsics que forment els actuals microprocessadors i en general, tota la sèrie de circuits de suport dels computadors i també dispositius mòbils.
3. Entendre els límits del nivell d'integració actuals i conèixer les solucions que s'adopten per tal d'aconseguir més potència de computació.
4. Intuir quins seran els nous conceptes de la computació futura i quin tipus de tecnologia s'aplicarà. Explicar-la i entendre-la fins allà on la informació vigent ens permeti.

3. Resultats

La lectura del document ens permetrà tenir una idea una mica més profunda sobre la base de que es compon un microprocessador, així com en general la circuiteria electrònica que composa un computador. Veurem la seva evolució i el estat actual en el qual està i quins són els límits tecnològics i físics del moment. També veurem que ens depara el futur i amb quins conceptes nous ens tindrem que familiaritzar per entendre la nova tecnologia. Amb tot això, també ens actualitzarem amb l'estat que es troben en aquests moments els sistemes operatius relacionats amb els aparells tecnològics d'avantguarda. Tindrem una visió molt aproximada del concepte de còmput quàntic i haurem aprofundit en els conceptes teòrics que s'estan desenvolupant en l'assoliment de les màquines da càlcul en aquest nou entorn. Això també ens portarà a comprendre fonaments teòrics de la mecànica quàntica i també la lògica que regeix el món de les partícules subatòmiques. Podrem veure conceptes que en certa manera contradiuen la lògica del nostre mon quotidià.

4. Organització del document

En primer lloc farem un repàs per la història dels computadors electrònics des dels seus inicis. Veurem les diverses generacions fins els nostres dies. Entrarem a veure quins eren els seus principals components, com funcionaven i quines avantatges i inconvenients tenien. Això ens ajudarà a comprendre les seves funcionalitats i les seves limitacions. També ens permetrà veure la velocitat en que han anat evolucionant. Donarem un cop d'ull als dispositius mòbils actuals i veurem la seva potència ja que n'hi ha una gran varietat i estan en continua evolució al igual que els sistemes operatius específics per a ells. De fet veurem com tenen una potència de càlcul molt bona. Finalment entrarem a veure el que ens depara el futur pròxim amb el ja esmentat computador quàntic. Ens endinsarem tant com podrem en el seu principi de funcionament, el seu estat actual de desenvolupament i analitzarem la seva potència de càlcul juntament amb els problemes que serà capaç de resoldre.

5. Introducció

La història de la humanitat ha anat lligada sempre a avanços tècnics des dels seus inicis. Avui en dia i en una mirada retrospectiva n'hi ha de fa milers d'anys (i de no tan llunyans) que ens poden semblar simples i insignificants, però en realitat en el temps en que estan emmarcats varen suposar veritables revolucions i varen fer possible fins i tot la evolució de l'esser humà. Aquests avanços sempre han servit per a cobrir unes certes necessitats d'un col·lectiu, de manera que podrem dir que han resolt un problema quotidià, han millorat la manera de realitzar alguna cosa que s'estava fen de forma rudimentària. De totes les necessitats que ha tingut l'esser humà en el transcurs de la seva història, una de les que ha estat sempre present ha sigut la de contar. El fet de contar ha estat una necessitat que ha sorgit i ha anat augmentant en complexitat a mesura que la civilització s'ha anat desenvolupant i les comunitats s'han anat relacionant. D'aquesta manera, tenim constància de que fa ja uns 5000 anys es va materialitzar una solució per tal d'alleugerir la tasca de contar i fer operacions relacionades: es tracta d'un petit artefacte anomenat àbac[1]. Va ser molt efectiu i ha superat el pas del temps. Molt més propers en els nostres temps i degut a un notable desenvolupament del comerç, el inici incipient de tallers amb certa especialització, es desenvolupen autèntiques màquines per sumar. Així , a la primera meitat del segle XVII es dissenya la primera màquina per sumar feta mitjançant engranatges i rodes (l'autor n'és el matemàtic i filòsof francès Blaise Pascal [2] i la màquina rep el nom de Pascalina [3]). A l'any 75 del mateix segle el també filòsof i matemàtic Gottfried Wilhelm Leibniz [4] perfecciona la màquina d'en Pascal i n'inventa una que també pot multiplicar. No solsament en el camp matemàtic s'inventen màquines que realitzen càlculs, també se'n desenvolupen en la automatització industrial. L'inventor francès Joseph Marie Jacquard [5] dissenya un teler automàtic fen ús de plaques de fusta perforades (veurem com aquesta idea serà la base d'entrada i sortida de dades en les primeres computadores electròniques). Més tard, ben entrat el segle XIX, el matemàtic britànic Charles Babbage va elaborà els principis de la computadora digital moderna. Va dissenyar (encara que no va arribar a construir-la degut a que la tecnologia no estava prou evolucionada) la màquina diferencial [6] capaç de solucionar problemes matemàtics complexos. La màquina diferencial tractava de resoldre un problema operatiu d'aquells temps, que consistia en la dificultat i monotonia de la tabulació de funcions matemàtiques (com per exemple logaritmes o funcions trigonomètriques). En aquells temps aquestes tasques es feien de forma manual, sen lentes i poc eficients. El fonament matemàtic de la màquina diferencial és el mètode numèric d'interpolació de Lagrange segons polinomis basats en interpolacions finites, és a dir en notació newtoniana. El problema d'interpolació de Lagrange consisteix en cercar el polinomi d'un cert grau que passa per uns punts concrets i per tant donen solució de continuïtat a aquests. Bàsicament l'algorisme que implementa la màquina era el següent: el punt de partida eren uns valor coneguts per a l'ordenada del polinomi a tabular i corresponia a certs valors de l'abscissa. Aquests valors es podien calcular usant el mètode de Lagrange per diferències finites (mètode de newton), de forma manual

(amb llapis i paper). Un cop ingressats aquests valors a les corresponents columnes d'engranatges de la màquina, així com les diferències finites que els relacionen, en moure una maneta, anirà computant els valors d'ordenada per a abscisses consecutives a les d'entrada. Per a fer-ho la màquina diferencial només fa una única operació aritmètica: la resta. Amb aquesta operació simple ens podem moure per la taula de diferències finites associada al problema per anar calculant els valors de les diferències finites de cada ordre, així com els de les ordenades.
També cal destacar el seu disseny de la màquina analítica [7] que té moltes característiques d'un ordenador modern. En el disseny es pot apreciar ja un flux de dades d'entrada en forma de paquets de targes perforades, una memòria per guardar les dades, un processador per les operacions matemàtiques i una impressora per enregistrar els resultats. Aquesta màquina ja és de propòsit més general sent capaç de realitzar càlculs més generals. En el segle XX comencen a sortir els primers computadors analògics. Aquests estaven basats en eixos i engranatges. Eren capaços d'avaluar aproximacions numèriques d'equacions complexes. Més tard es van substituint parts mecàniques per elèctriques fins que sobre l'any 1943 està a punt la primera màquina de còmput completament electrònica. A partir d'aquest moment l'avanç tecnològic farà possible una evolució de les computadores i els sistemes d'emmagatzemar dades que avançarà d'una forma mes o menys pausada les següents quatre dècades però que a partir d'aquestes l'evolució és vertiginosa degut sobre tot al molt alt nivell d'integració de components per unitat de superfície. En l'actualitat i des de fa uns anys s'està experimentat en un altre concepte de computació: la computació quàntica. Veurem com quan aquesta tecnologia estigui consolidada suposarà un gran salt en la potència de càlcul que ajudarà a una acceleració en els processos en diversos camps de totes les ciències i ens permetrà una acceleració evolutiva considerable.

6. Desenvolupament dels computadors electrònics

Des de la creació del primer computador purament electrònic a l'any 1943 l'evolució d'aquests ha estat molt important. El desenvolupament de tecnologia en diversos camps de la física (òptica, electrònica, etc.) han permès de crear cada vegada computadors més sofisticats els quals en un espai molt reduït i amb un consum molt baix han anat multiplicant la seva capacitat de càlcul i per tant, la seva potència. Una altre diferència important és la de que en els seus inicis, els computadors estaven dedicats a una tasca exclusiva amb la particularitat de que si es volia canviar aquesta, es tenia que tornar a dissenyar fen importants modificacions a la pròpia màquina. Aquest inconvenient es va poder resoldre al cap d'uns pocs anys, a mesura que les noves tecnologies van permetre de crear computadors més sofisticats i versàtils. Disposen, el contrari de les primeres màquines, d'un sistema operatiu i per altre banda es disposa de llenguatges de programació mitjançant els quals podem programar a

voluntat les diferents tasques que volem que la nostra màquina executi. L'evolució d'aquestes màquines ha estat classificada com a generacions. Més o menys es coincideix en dividir aquesta evolució amb sis generacions.

7. Primera generació

Abans d'introduir-nos en el que va ser i representar aquesta primera generació de computadors farem un repàs a la tecnologia que va fer possible aquest esdeveniment i per tant, va ser clau per a fer un pas endavant en l'historia de la computació.

7.1 Vàlvules, resistències i condensadors

Com hem vist, els elements bàsics que formaven els computadors, completament electrònics, d'aquesta primera generació eren les vàlvules (com elements actius) i les resistències i condensadors (com a passius) a part de cables i soldadures. Però que són les vàlvules [15] de buit?
Les vàlvules de buit varen ser descobertes l'any 1904 per Sir Ambrose Flemig i varen ser denominades diodes. Aquestes, amb dos elèctrodes, nomes eren capaces de transformar el corrent altern amb corren continua. Una any més tard en Lee de Forest va afegir un elèctrode més en el diode i va aconseguir el denominat tríode que regulava el pas de corrent i per tant tenia la capacitat d'actuar com amplificador. Més tard es va anar afegint elèctrodes en aquestes vàlvules per aconseguir diferents regulacions i va ser com van aparèixer els tètrodes, pèntodes, hèxodes, hèptodes, i òctodes.

Diversos tipos de vàlvules

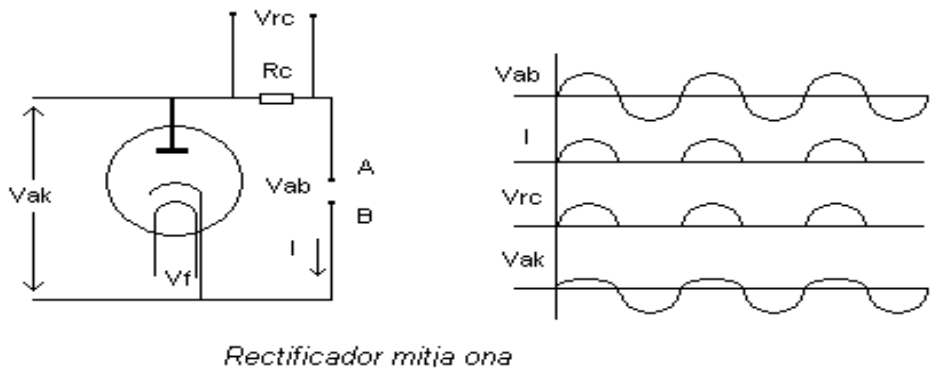
Vàlvules de buit de diferent tipus i mida [f2]

7.1.1 Com funciona una vàlvula

Una vàlvula diode consta de dos elèctrodes denominats ànode i càtode. El seu funcionament es basa en l'emissió d'electrons del càtode que son rebuts per l'ànode. Aquesta emissió pot ser generada per temperatura (emissió termoelèctrica), per camp elèctric, per efecte fotoelèctric, o per ionització d'un gas. El sistema més utilitzat és el termoelèctric, i que pot ser per escalfament directe o indirecte.

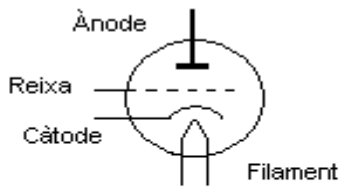
Representació esquemàtica del diode amb els dos sistemes d'escalfament [E1]

Un muntatge típic de diode com a rectificador de mitja ona és el següent:



Muntatge típic del diode com a rectificador de mitja ona [e2]

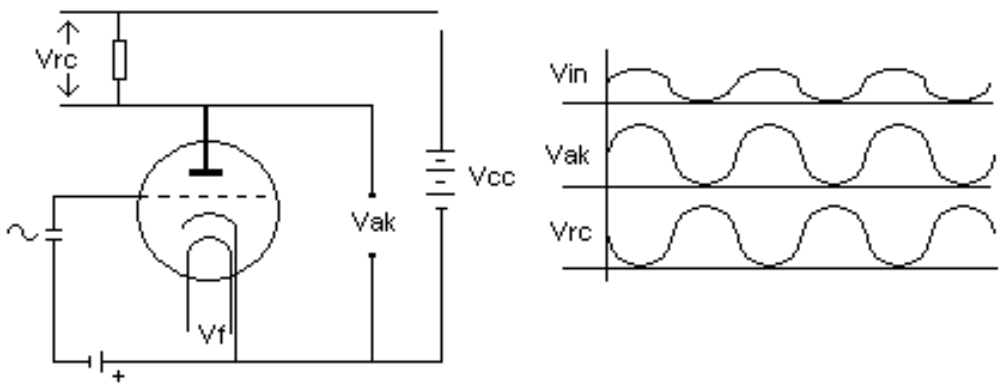
El tríode és el mateix concepte però amb un elèctrode que s'anomena reixa i que per dir-ho d'una forma planera actua com un regulador deixant circular més electrons cap el ànode depenent de la seva polaritat i nivell. La seva representació simbòlica és la següent:



Triode

Representació esquemàtica del tríode [e3]

Un muntatge típic del tríode com amplificador és el següent:



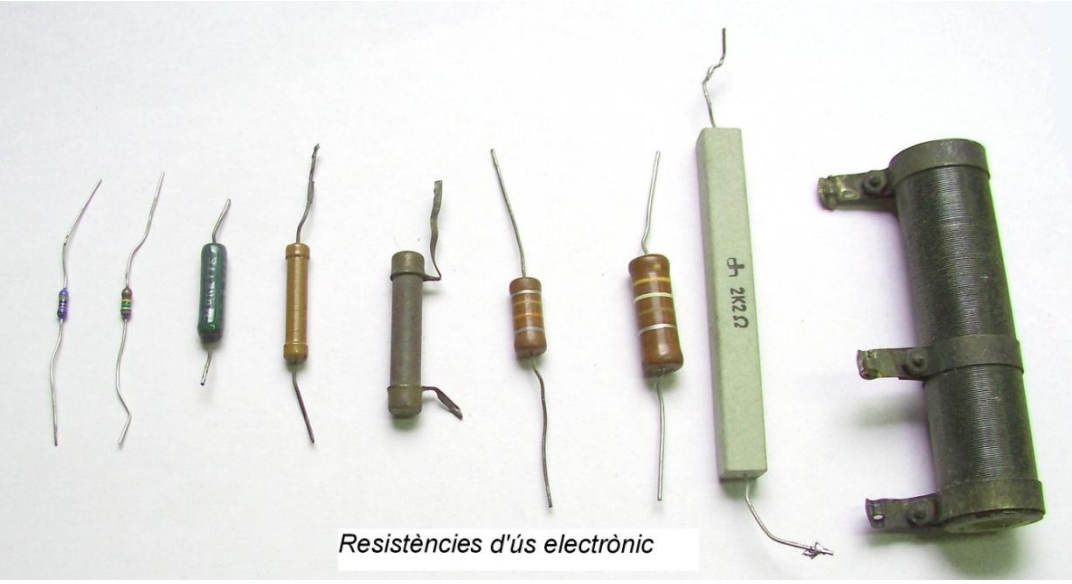
Circuit amplificador

Circuit típic amplificador amb tríode [e4]

De fet, és fàcil veure que es possible fer-lo treballar de forma digital. Nomes cal treballar amb dos nivells de tensió d'entrada: 0 volts o Vcc màxima de forma que no hi haurà circulació d'electrons cap el ànode en ser la reixa negativa o la circulació serà màxima en tenir la reixa a màxima tensió positiva. En aquestes condicions el tríode es comportarà com un circuit inversor.

7.1.2 Que és una resistència

Una resistència elèctrica és un element passiu que l'únic que fa és oposar-se el pas del corrent elèctric. Això ho fa d'una manera més accentuada o menys depenent dels seu valor òhmic. Hi ha diferents materials de construcció de resistències: carbó, Ni Crom, wolframi, etc. També estan dissenyades per aguantar més o menys potència depenent la seva funcionalitat. Els filaments de les vàlvules de buit que hem vist a l'apartat anterior estan construïdes amb wolframi. Les bombetes elèctriques tradicionals també. En els circuits electrònics normalment el seu ús es generalitza per crear divisors de tensió i sobre tot per a limitar la circulació de corrent. També les utilitzem molt sovint en la vida quotidiana a l'hora de elevar o reduir el volum de l'aparell de ràdio, en escalfar l'aigua a la rentadora, termos, etc. Les diverses formes que prenent depenent molt del ús per al qual han estat dissenyades i també per la potència que són capaces dissipar. En la següent imatge podem veure diferents tipus de resistències d'ús electrònic:

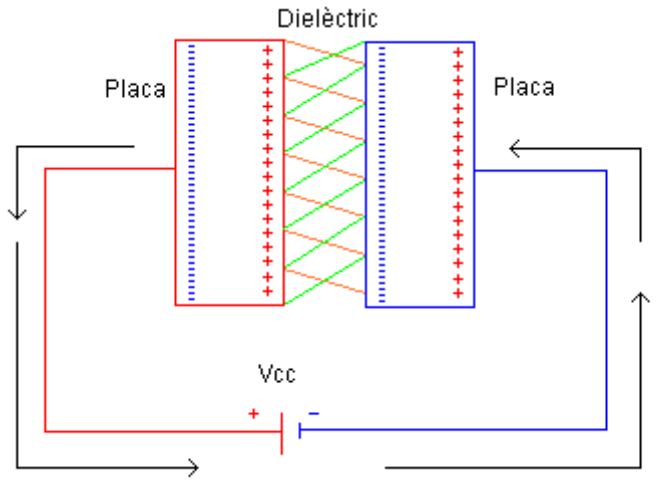


Imatge de diversos tipus i mides de resistències[f3]

7.1.3 Que és un condensador

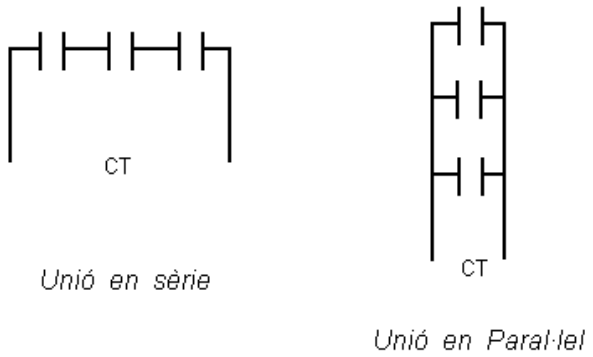
Un condensador és un aparell que està constituït per a dues plaques paral·leles amb un material dielèctric [16] al mig que les aïlla. Depenent de la superfície de les plaques i de la seva proximitat, el condensador tindrà més o menys capacitat. Al connectar el condensador a una font d'alimentació de corrent continua [17], la placa que està connectada al extrem positiu quedarà amb un excés de carga positiva degut a que els electrons s'hauran desplaçat cap el pol positiu de la bateria. A l'altre placa els electrons de la bateria es desplacen cap a ella i les partícules amb carga positiva d'aquesta, ho fan

cap el extrem negatiu de la bateria. Com a resultat tenim que aquesta placa es queda amb excés de cargues negatives. Baiem-ho gràficament:



Dibuix il·lustratiu del efecte condensador [d1]

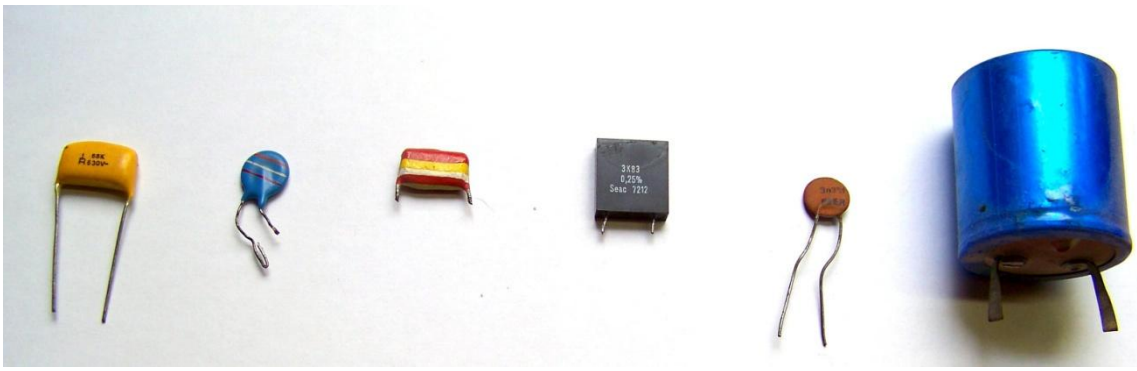
La carga elèctrica [18] que pot adquirir un condensador bé donada per el producte de la seva capacitat amb la diferència de potencial entre els seus extrems(plaques): Q = C * V. La capacitat d'un condensador és l'aptitud que posseeix per emmagatzemar cargues elèctriques. La unitat de capacitat és el Farad [19]. La capacitat d'un condensador és directament proporcional a la superfície de les plaques i inversament proporcional a la distància entre elles.
Els condensadors es poden connectar entre ells en sèrie i en paral·lel. Connectats en sèrie, la capacitat total del circuit és: $C_T = \frac{1}{\frac{1}{C_1}+\frac{1}{C_2}+\frac{1}{C_3}+\cdots\frac{1}{C_n}}$ i connectats en paral·lel la capacitat total bé donada per la fórmula $C_T = C_1 + C_2 + C_3 + \ldots C_n$.
Podem veure en el següent gràfic:



Esquema del tipus d'unió de condensadors [e5]

Els condensadors són molt utilitzats per diverses funcions dintre d'un circuit electrònic: per estabilitzar (fins un cert punt) la tensió continua rectificada, juntament

amb bobines i resistències constitueixen filtres per tal de deixar passar unes determinades freqüències, també junt amb una resistència formen un circuit bàsic temporització (la resistència limita la circulació de corrent i per tant rellentint-se la carga del condensador), actuen com a separadors del corrent continuo amb l'altern, etc. A la següent fotografia podem veure diversos tipus de condensadors:



Diferents tipus de condensadors [f4]

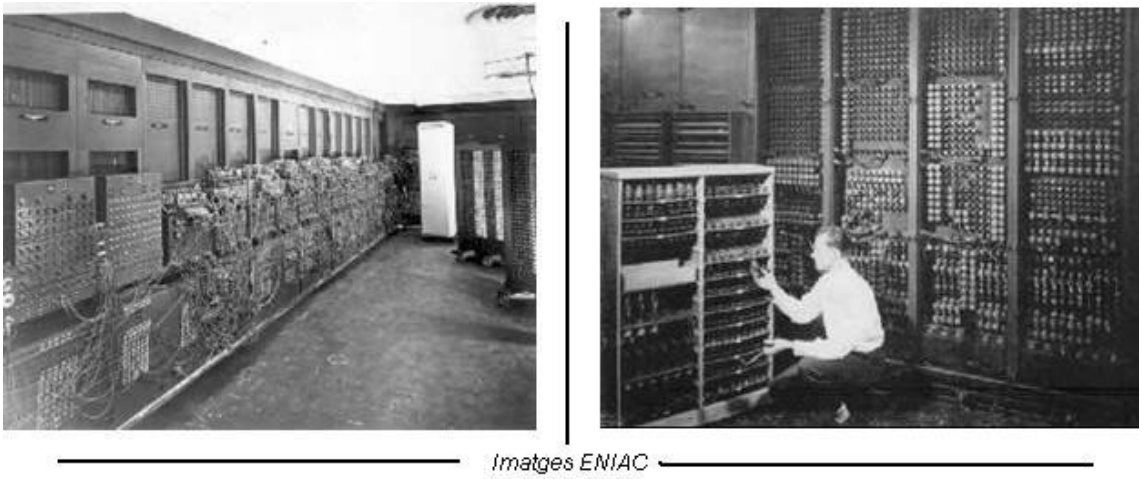
7.2 Computadors de la primera generació

La primera generació dels computadors es situa entre els anys 1946 i 1955. Les computadores d'aquesta generació eren computadores completament electròniques que usaven la tecnologia pionera d'aquells moments. L'element fonamental era la vàlvula de buit. A més, els circuits estaven formats per elements passius com resistències i també condensadors. Tot el demès eren cables per unir les diferents parts del circuit i soldadures. La vàlvula actuava com un interruptor: deixava passar el corrent o el tallava. Això era aprofitat per treballar amb representació numèrica binaria: el pas de corrent representava un 1, l'absència un 0. Amb aquesta filosofia, s'agrupaven conjunts de vàlvules formant diferents circuits lògics capaços de realitzar sumes, restes multiplicacions i divisions. No existien els programes com els entenem avui en dia i la programació es realitzava directament sobre la màquina.
La primera computadora d'aquesta generació va ser l'anomenada Colossus [8] i va ser construïda a Gran Bretanya. Tenia entrada per a cinta de paper perforat i era capaç de fer bifurcacions condicionals. La rèplica americana va ser la ENIAC [9] amb una potència de operacions del ordre de 100.000 càlculs simples per segon. Aquestes dues computadores la primera de elles anglesa i la segona americana, estaven dedicades a usos militars. La Colossus s'utilitzava per ajudar a desxifrar missatges alemanys interceptats per la ràdio. L ENIAC

s'usava per a càlculs balístics i trajectòries de míssils. Més tard es va fabricar a Manchester la Manchester Baby [10] i la Manchester Mark I [11]. Aquesta última va utilitzar el tub de William [12] per memòria i ja va introduir registres índex. A la universitat de Cambridge es va construir la EDSAC [13] que era capaç de resoldre ja problemes reals i de propòsit general. La successora de la ENIAC va ser la EDVAC [14] que utilitzava, a diferencia de la seva predecessora, una sola unitat de processament. Molts consideren la Mark I, la EDSAC i la EDVAC com les precursores de gairebé totes les computadores actuals que deriven de la seva arquitectura.

Els problemes principals d'aquestes màquines eren la seva mida, la quantitat d'energia que consumien i l'elevada temperatura que desprenien. El seu manteniment era costos degut a que les vàlvules s'anaven fonen i tenien que anar se'n substituïdes. Això originava que funcionessin amb continuïtat en intervals d'unes poques hores.

Com a curiositat, podem explicar que va ser en aquesta generació de computadors quan apareix per primera vegada el concepte o terme *bug* aplicat o fent referència a la incipient informàtica (en aquest cas concret un problema en el hardware). Va ser l'any 1947 i es va produir en el computador Mark II (successor del Mark I). El problema va ser una arna atrapada en els contactes d'un relé que va provocar que aquest quedés obert i origines un mal funcionament del computador. La causa d'aquest problema va ser descrit com *bug* (traduïda al català bitxo).



Vistes de la ENIAC [f1]

7.3 Fi de la primera generació

El 16 de desembre del 1947, en William Shockley, John Bardeen y Walter Brattain construïen el primer transistor. Aquest fet revolucionaria el mon de l'electrònica en

general i el dels computadors en particular. El transistor solucionarà molts dels inconvenients que presenten les vàlvules de buit. La seva implementació marcarà una nova generació de computadors molt més potents i eficients. Comença així la segona generació dels computadors.

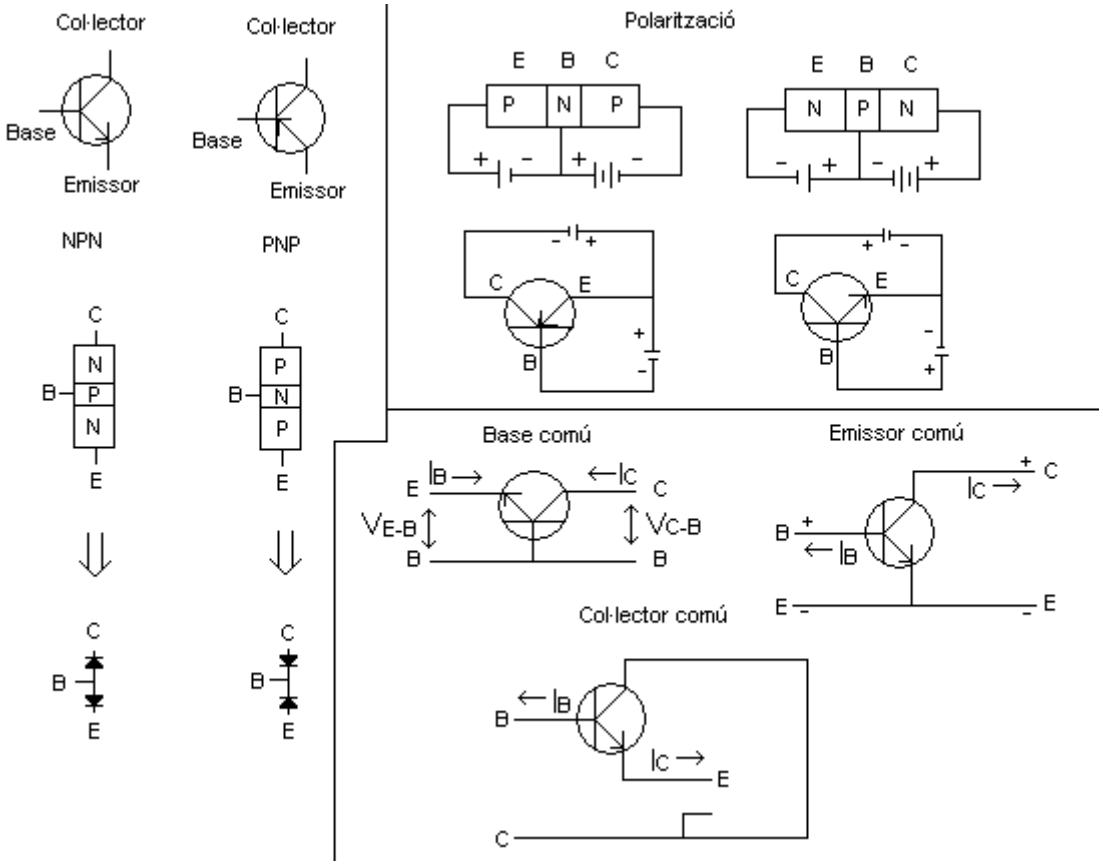
8. Segona generació

Aquesta segona generació vindrà marcada per l'aparició d'un nou component: el transistor. Això suposarà un avanç important en la construcció dels nous computadors ja que aquests ocuparan un espai molt més reduït, tindran molt menys consum i més potència i seran més econòmics tan de fabricació com de manteniment.

8.1 Que és un transistor

Com ja hem esmentat, el transistor passa a ser l'element actiu dels nous computadors d'aquesta segona generació. Substitueix a la vàlvula de buit amb totes les avantatges respecte a aquesta que hem esmentat.
Els transistors són dispositius semiconductors que estan construïts bàsicament amb dos materials: el germani i el silici. Consten de tres terminals, anomenats emissor, base i col·lector. Depenent de la seva construcció els podem classificar com a PNP o NPN [20]. Els transistors per el seu funcionament, es tenen que connectar a una font d'alimentació de corrent continu respectant segons el tipus (PNP, NPN), la polaritat. Per polaritat (o polarització del transistor) entenem aplicar a cada terminal el sentit o potencial del corrent que l'hi correspon (negatiu o positiu) per tal d'aconseguir variar les característiques internes seves. D'aquesta manera, la resistència interna del entre col·lector i emissor (entenem per resistència interna la oposició que presenta al pas del corrent) pot variar des de pràcticament zero fins a un elevat valor en el qual no hi ha circulació de corrent.
Perquè un transistor deixi circular corrent entre els seus terminals, la unió base – emissor es polaritza en sentit directa, és a dir, en un NPN en el terminal de base s'aplica el potencial positiu de la font d'alimentació i en el d'emissor el negatiu; en un PNP a la base s'aplica negatiu i en l'emissor positiu; la unió base – col·lector ho fa en sentit invers (en un NPN tan base com col·lector estan a potencial positiu però aquest últim a un potencial més eleva i amb un NPN el mateix però amb potencial negatiu) .
En un transistor, la intensitat del col·lector depèn sempre de la intensitat de la base. En circular un corrent d'emissor a base, hi ha electrons que s'escapen per els buits de la base i són atrets cap el col·lector,sent així com s'origina el corrent de col·lector.
Existeixen tres possibles muntatges del transistor en un circuit: base comú, emissor comú i col·lector comú o seguidor d'emissor. Cada modalitat confereix en el transistor unes característiques específiques de funcionament: en el muntatge de base comú

s'assoleix un guany en tensió però no en corrent. La impedància d'entrada és baixa i la de sortida alta. No hi ha inversió de fase entre entrada i sortida. En el muntatge en emissor comú les impedàncies d'entrada i sortida estan entre alta i baixa. Es produeix guany de tensió i corrent. El senyal a la sortida està invertit 180 graus respecte el senyal de l'entrada. Finalment, en el muntatge de seguidor d'emissor, la impedància d'entrada és molt elevada i la de sortida és baixa. No presenta guany de tensió però si de corrent. No es produeix inversió de fase entre el senyal d'entrada i el de sortida.
La següent imatge resumeix el que hem explicat sobre el transistor:

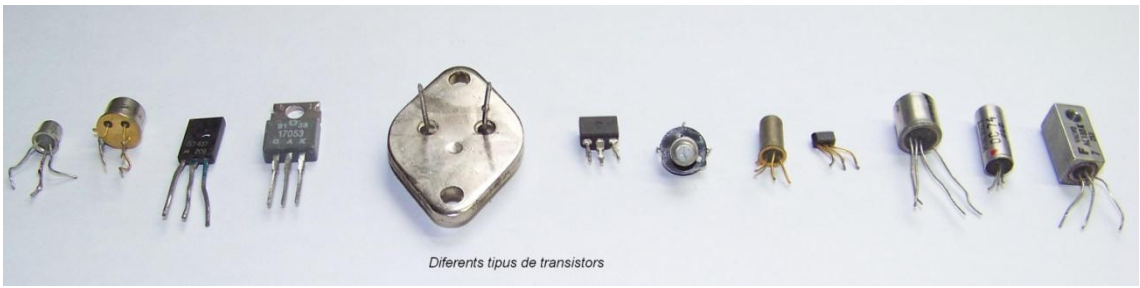


Esquema de tipus de transistors, polarització i muntatges típics [e6]

A la part esquerra de la imatge podem veure la representació simbòlica del transistor en les seves dues versions: PNP i NPN. Esquemàticament la diferència està en el sentit de la fletxa del emissor. En el NPN el sentit de la fletxa surt de la base mentre que en PNP entra en la base. Després tenim la representació per material de cada tipus de transistor: en el NPN tant l'emissor com el col·lector estan construïts en semiconductor de tipus N (el semiconductor s'ha dopat amb àtoms per augmentar el nombre de portadors de carga negativa o electrons) mentre que la base està feta de semiconductor tipus P (el semiconductor s'ha dopat amb àtoms per tal d'augmentar el nombre de portadors de carga positiva o buits). En el PNP la base és de semiconductor tipus N i tant l'emissor com el col·lector són de semiconductor tipus P. Finalment tenim l'esquema teòric (que no pràctic o real) del transistor com unió de semiconductors (en

aquest cas díodes).A la part dreta superior veiem com es polaritza un transistor PNP i NPN. Polaritzar significa quin signa del corrent continu s'aplica a cada un dels terminals per aconseguir que el transistor estigui en estat de conducció, és a dir, que circuli corrent per base – emissor, i aquesta indueixi una altre corrent per el col·lector – emissor. O podem veure tan en el transistor PNP com amb el NPN. Finalment, a la part inferior dreta podem veure les tres diferents formes de configurar un transistor respecta al senyal d'entrada i el de sortida. Cada una d'aquestes configuracions confereix en el circuit unes determinades característiques que el fan idoni per un tipus determinat d'aplicació.

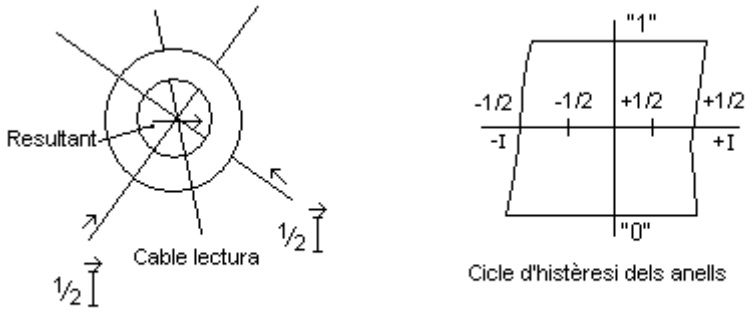
Els transistors tenen la capacitat de, donat un senyal dèbil d'entrada, amplificar-la en un factor que depèn del tipus i característiques del transistor però que sol ser força alt i si aquesta no és suficient a la seva sortida, es poden anar combinant fins obtindre el nivell desitjat. Una altre característica molt important que va obrir les portes a l'electrònica digital, i en ella, el desenvolupament dels computadors, va ser la que fa que pugui funcionar com un interruptor (treballant ens els dos extrems, tall / saturació, de la recta de carga [21]). Això significa que aplicant un nivell de tensió 0 a l'entrada (base), a la sortida (emissor o col·lector) podem tenir un nivell també baix (0) o alt (1) que representa la tensió d'alimentació. Això dona origen al desenvolupament de les portes lògiques i en definitiva al que hem esmentat, l'electrònica digital (funcionament en sistema binari).
El transistor té moltes facetes dins el món de l'electrònica i ha estat la base per desenvolupar tota classe de circuits que fan front a cobrir les necessitats en diversos camps tant domèstics com industrials. N'hi ha capaços de subministra grans potències mentre d'altres ho fan amb mitjanes i petites. També el rang de freqüències a les que són capaços de respondre és molt variat. Com a més freqüència és capaç de respondre un transistor a major velocitat pot commutar entre el seu estat de tall i saturació. Per últim, podem diferenciar entre tipus de transistors com el bipolar [22] (PNP, NPN), MOS [23] (canal N i canal P), FET [24] (transistor d'efecte de camp de canal N o canal P), UJT [25] (uniunió), PUT [26] (transistor uniunió programable), IGBT[27], etc.



Fotografia que ens mostra diferents tipus de transistors [f6]

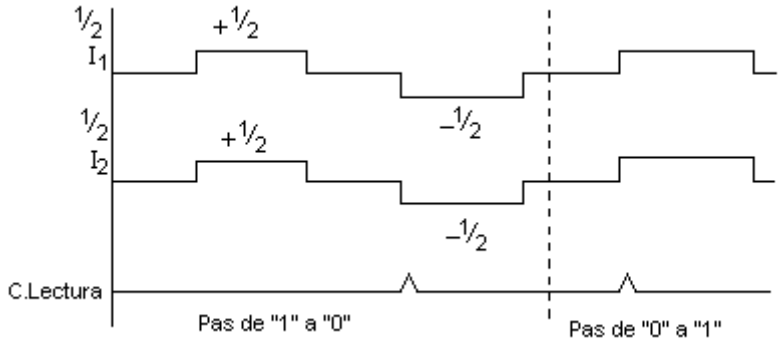
8.2 Que és la memòria de ferrita

Les memòries de ferrita varen ser un avanç important degut a la seva simplicitat, mida, molt baix consum i romanència de les dades. El problema era que aquestes memòries s'organitzaven en panels, es construïen a ma i normalment no superaven la xifra de 4k bytes. El seu principi de funcionament es basa amb anells de òxid de ferro [28] els quals són travessats per dos cables perpendiculars i un altre oblic. Els perpendiculars magnetitzen l'anell i estan configurats d'aquesta manera perquè el corrent que hi circula es sumi; el tercer porta la informació del resultat de la lectura.



Detall d'una cel·la de memòria de ferrita i gràfica del cicle d'histèresi del anell [d2]

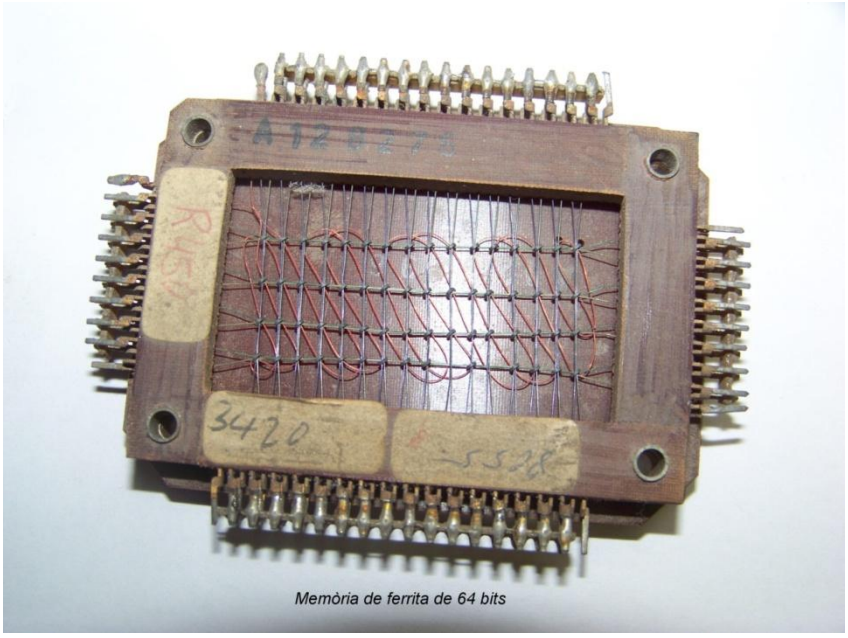
En aplicar a cada cable +½ I o -½ I es sumen obtenint la I total i varien el camp. Per tal d'escriure un 1 a la memòria s'aplica +½ I i per un 0 -½ I. En el següent gràfic podem veure la mecànica que segueix:



Cicle d'escriptura / lectura de la memòria de ferrita [g1]

En llegir la memòria de ferrita tenim possibilitats de perdre la informació. En el moment de fer la lectura apliquem un pas de corrent en els dos cables perpendiculars. Si és positiu i teníem escrit un "1" no perdrem la informació ja que no variem la

magnetització. Per el cable de lectura no tindrem cap pols i per això sabrem que teníem un "1". Si enlloc d'un "1" i havia emmagatzemat un "0", llavors canviem la informació en aquest procés de lectura ja que variem la magnetització. Per el cable de lectura obtindrem un pols amb la qual cosa sabrem que hi havia un zero. Un cop hem fet la lectura tindrem que tornar a escriure un zero en aquella posició (aplicant un pas de corrent negatiu) per tal de no adulterar la informació que tenia. Per tant cada cop que obtenim un pols en el cable de lectura en fer un accés per llegir, tindrem que restaurar la informació d'aquell bit.
Aquest tipus de memòria mante el contingut sense necessitat de mantenir alimentat el circuit. Com a curiositat cal assenyalar que aquestes memòries eren les que s'usaven en els míssils i tots els artefactes que sortien al espai ja que eren les úniques que no s'alteraven davant les radiacions còsmiques.



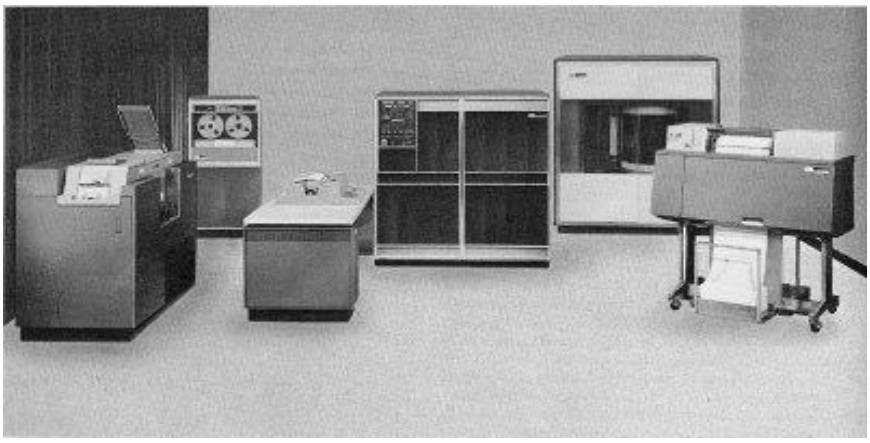
Detall de memòria de ferrita de 64bits [f7]

8.3 Màquines de la segona generació

La segona generació de computadors es considera que avarca des del 1956 fins el 1964 aproximadament. Bàsicament comença amb el descobriment i posterior implementació del transistor. Aquest va ser materialitzat per primera vegada l'any 1947 per John Bardeen, Walter Brattain y William Shockley. Comparat a les vàlvules, el transistor és molt més petit (uns pocs mil·límetres davant de uns quans centímetres de la vàlvula), el seu consum és molt més baix, la velocitat de transició entre estat de conducció i tall és molt més ràpida que el de les vàlvules (això té al final com a resultat més quantitat d'operacions per segon), i una altre característica molt important és la seva baixa temperatura de treball. Ara, amb els computadors fets a base de transistors, el seu funcionament és continu ja que no es produeixen averies constants com passava amb les vàlvules degut a que l'alta temperatura les fonia i es tenien d'anar substituint.

També el consum energètic cau en picat, doncs passem de les desenes de kilowatts hora a uns centenars de vats hora. L'espai també pateix un canvi impressionant: passem de molts metros cúbics a centímetre cúbic. La velocitat de procés també es multiplica per deu. Finalment dir que el preu de fabricació del transistor també és molt més econòmic que no pas el de la vàlvula. En quan el principi de funcionament dels circuits conserven la mateixa filosofia que el de les vàlvules (es treballa amb dos nivells: el de tensió = 1 i el d'absència de tensió = 0). Aquests es continuen agrupant per tal de formar circuits lògics així com sumadors, divisors, multiplicadors, etc. A la generació anterior, la major part dels computadors funcionen de forma analògica. També s'han construeixen de digitals amb ús d'àlgebra booleana però aquests resultaven més cars i també el fet dels analògics es justificava degut a que es dissenyaven per resoldre una sèrie de problemes força anàlegs. En aquesta generació, la construcció de computadors digitals amb l'ús de portes lògiques s'estén més degut a que els costos s'abarateixen, però no serà fins a la pròxima generació amb l'aparició del circuit integrat, que l'ús extensiu de la porta lògica no serà ja habitual, cosa que permetrà construir computadors de propòsit més general.
Els computadors analògics basen el seu funcionament amb la mesura dels temps de dades continues i usa una quantitat física com corrent, voltatges, mesures de distància, temps, etc. per a presentar dades i processar-les. L'exactitud dels càlculs està limitada per la mesura de les quantitats físiques que representen les dades. D'aquesta manera, aprofiten la similitud matemàtica entre les interrelacions físiques de determinats problemes i usen els circuits electrònics per a simular dits problemes. El computador digital presenta les dades amb termes de números discrets i els processa usant operacions aritmètiques normals. Opera basant-se en seqüències d'impulsos creats per a una combinació de dígits. Aquest tipus de computador és molt versàtil i és capaç de donar solucions a gran diversitat de problemes variant únicament el programa d'entrada sense necessitat de cap modificació de hardware.
Per altre banda cal destacar que els sistemes per emmagatzemar les dades han evolucionat. Per les dades temporals s'utilitza memòria de ferrita. Aquesta consta d'uns anells de material ferromagnètic els quals són travessats per tres cables que són els encarregats d'orientar el camp magnètic de l'anell per tal d'enregistrar un 0 o bé un 1 lògic. El tercer cable és el de lectura de la dada. També cauen ja en desús els tambors magnètics que són substituïts per discos magnètics que estan incorporats en el computador però que són fàcilment intercanviables. Es continuen utilitzant targetes perforades, però ara ja amb capacitat de llegir-les i perforar-les al mateix temps. També els computadors són ja capaços de prendre decisions lògiques, executar càlculs i fer lectures / escriptures en cintes magnètiques que també son usades per emmagatzemar dades. Apareixen les unitats terminals que transmeten les dades a la unitat de càlcul central que pot estar a molts kilòmetres de distància, mitjançant enllaços telefònics. Aquests computadors tenen un gran ús comercial en sistemes de control de trànsit aeri, reserva de bitllets, construcció i manteniment d'inventaris, gestió de nòmines, comptabilitat i fins i tot simulacions d'us general.
En aquesta segona generació s'incorporen els llenguatges de programació Cobol i Fortran (Fortran el desenvolupa IBM el 1957, i Cobol el 1961) i també a finals d'aquesta

generació neix Basic. Ara per canviar la tasca del computador ja no fa falta modificar el circuit, simplement es crea el programa a mida de la nova tasca i el computador el llegeix i l'executa. De fet, el llenguatge Cobol (COmmon Business Oriented Languaje) neix l'any 1952 i s'atorga l'honor de la seva creació (i com a mínim va ser una gran impulsora en el desenvolupament del compilador de la primera versió) a Grace Murray Hoper, una oficial de la marina dels EU. Aquest es capaç de traduir enunciats semblants a l'anglès amb codi binari comprensible per a la màquina. Les màquines que funcionen amb aquests llenguatges són màquines amb circuits digitals que usen àlgebra de bool i basen els seus càlculs amb operacions aritmètiques comuns, sent de propòsit general (amb l'estructura ja molt semblant a les màquines que coneixem en l'actualitat).
Imatge del equip de càlcul, emmagatzematge, computador, etc. en una empresa de la època:



Imatge d'un computador a transistors junt amb els seus perifèrics [f5]

8.4 Fi de la segona generació

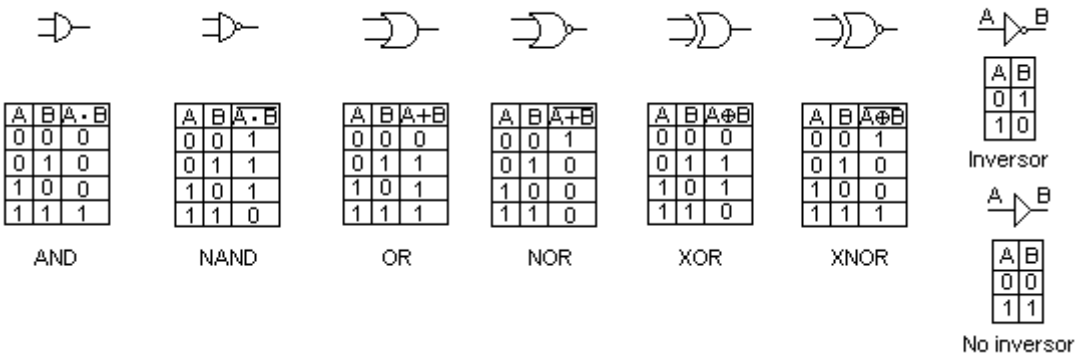
L'any 1958, el físic Jack Kilby desenvolupa el primer circuit integrat. Aquest consta de sis transistors integrats en una mateixa base semi conductora formant un circuit oscil·lador de rotació de fase. Aquest fet marca el inici d'una nova era de l'electrònica en la qual la mida dels components experimenten una reducció molt gran, junt amb un consum molt més baix, una fiabilitat i velocitat més alta i finalment, amb uns costos de producció també més reduïts. Això afecta evidentment la construcció dels computadors en els quals marcarà el que es considera el inici de la tercera generació

9. Tercera generació

En aquesta generació, els computadors experimenten un avanç important. Redueixen considerablement l'espai que ocupen, tornen a baixar el seu consum i augmenten la seva potència. Això és degut a que s' aconseguit reduir la mida dels circuits electrònics. Ha estat possible gràcies a l'aparició del circuit integrat.

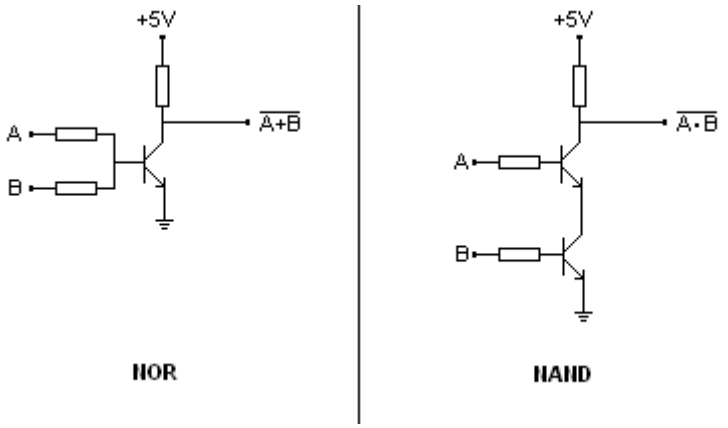
9.1 Portes lògiques

Podem considerar que hi ha 8 tipus de portes tot i que dues d'aquests 8 es pot considerar que ho són o no. Així, podem parlar de portes AND, NAND, OR, NOR, XOR, XNOR, i les que són més ambigües en aquesta consideració són l'inversor i el no inversor. Anem a veure com es representen esquemàticament i la seva taula de la veritat:



Esquema i taules de les diferents portes lògiques [e7]

En la figura, A i B representen les entrades de les portes. A aquestes entrades se'ls aplica un nivell de tensió . El nivell de tensió positiu representa un 1 lògic, el negatiu representa el nivell 0 lògic (depenent de la tecnologia de fabricació de la porta l'absència de tensió a l'entrada també representa un 0 lògic). El resultat de les diferents combinacions lògiques a les entrades queden registrades a la tercera columna de la taula i depèn del tipus de porta. Combinat aquestes portes es poden construir sumadors, restadors, divisors, multiplicadors, registres de desplaçament, bàscules, etc. De fet, la porta AND en sí ja és un multiplicador de un bit i la OR un sumador també d'un bit. En la següent imatge mostrem una de les moltes maneres en que s'implementa una porta mitjançant transistors. En concret es tracta d'una porta NOR i una altra de tipus NAND:



Esquema circuit amb transistors d'una porta NOR i una NAND [e8]

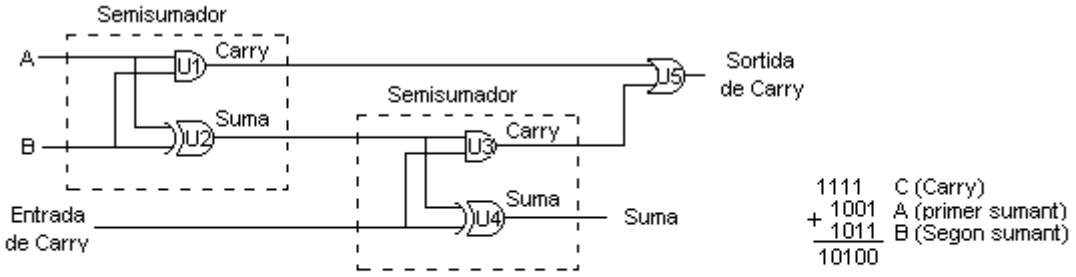
Depenent de la tecnologia i el tipus de porta, s'usen transistors multi emissor o multi col·lector que fan la funció d'entrada de la porta lògica.

9.1.2 Com funciona un circuit sumador i un multiplicador

Anirem a veure en aquest apartat (a tall d'exemple), com unint una sèrie de portes podem aconseguir un sumador i un multiplicador.
En primer lloc veiem l'algorisme de la suma binària:

0 + 0 = 0
0 + 1 = 1
1 + 0 = 1
1 + 1 = 0 i "em porto una" (ròssec, carry)

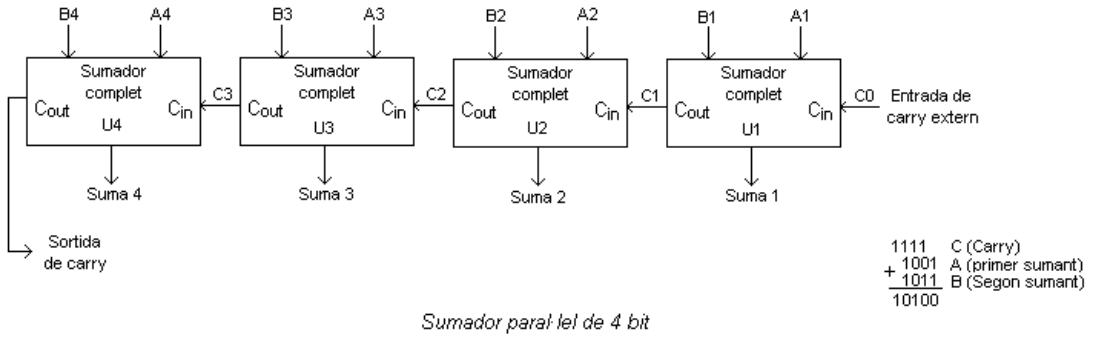
Podem observar que per cada bit necessitarem una entrada per el ròssec i una sortida per si s'han produeix. Per tant, el circuit lògic per dos bit el podem construir mitjançant cinc portes, dues XOR, dues AND i un OR:



Sumador complet de dos bit

Circuit sumador complert amb cinc portes i dos bit [e11]

Per tal de realitzar sumes de varis bits el que es fa és ajuntar sumadors com el de la figura, tants com resolució de bits necessitem. A la següent figura podrem veure un sumador de 4 bits:



Esquema en blocs d'un sumador de 4 bit de resolució [e12]

Ara anem a veure l'algorisme del producte:

L'algorisme fonamental de la multiplicació és el següent:

0 x 0 = 0
0 x 1 = 0
1 x 0 = 0
1 x 1 = 1

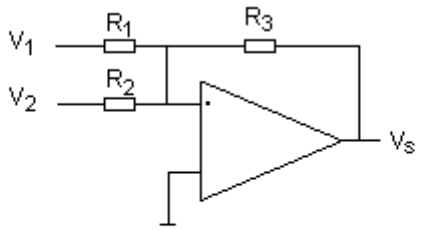
Per realitzar una multiplicació en binari usarem dues propietats del producte:

- El producte consisteix en la repetició d'una suma. Així, 4 x 10 = a sumar quatre vagades 10.
- Un desplaçament d'un dígit cap a l'esquerra en binari equival a multiplicar per 2. Així, 1010 (10 decimal) si el desplacem un dígit a l'esquerra queda 10100 donant com a resultat 20 en decimal (2 x 10).

Anem a fer la multiplicació en binari aplicant l'algorisme de, per exemple, 13 x 11 = 143:

```
      1101 (13)      Multiplicador
      1011 (11)      Multiplicant
     ----------
      1101     1 x 1101
     1101      fem el desplaçament a l'esquerra i 1 x 1101.
    0000       fem el desplaçament a l'esquerra i 0 x 1101.
   1101        fem el desplaçament a l'esquerra i 1 x 1101
  --------------
  10001111  (143)  Resultat
```

En l'exemple hem sumat tots els productes parcials al final i de cop però normalment, el que es fa és anar sumant els productes parcials així que es produeixen.
Els circuit multiplicadors són més complexes amb nombre de portes que els sumadors degut a que porten una lògica de control per tal de fer les operacions de desplaçament i de decidir si es suma 0 ó el valor del multiplicant. Cada operació la marca un pols de rellotge que obliga en els circuits a executar-la. La freqüència d'aquest rellotge és el que marca la velocitat en el nombre d'operacions per segon. Per tant podem veure que al final de cada pols, tenim un resultat numèric que pot ser parcial o total quan s'han completat el conjunt d'operacions (nombres de polsos necessaris) sent això vàlid per els circuits tant sumadors com divisors, multiplicadors, etc.
Això que hem explicat contrasta amb la forma de funcionament dels circuits analògics en els quals es basaven els computadors de les primeres generacions (i es basen els de les actuals generacions dissenyats analògicament). Com ja hem explicat, els computadors analògics tracten la informació d'una forma continua i treballen en magnituds siguin del tipus que siguin. Aquestes magnituds es tradueixen en un nivell de tensió o corrent proporcional que és introduïda en els circuits d'entrada i es té una resposta a la sortida, com a resultat del processament que els circuits de la màquina n'ha fet.
Ara, veurem a mode d'exemple com és un sumador i un restador analògic, usant un amplificador operacional, que és un tipus de circuit més o menys modern (avui en dia estan fabricats en un circuit integrat) però que el concepte és vàlid per fer-se una idea de com funcionaven amb transistors i fins i tot amb vàlvules. Veurem com és el circuit desenvolupat amb transistors i ens el podrem imaginar substituint aquests per vàlvules i fer-nos una idea aproximada de com devien ser.

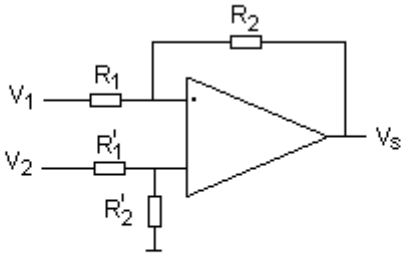


$$V_s = -\left(V_1 \frac{R_3}{R_1} + V_2 \frac{R_3}{R_2}\right)$$

Sumador analògic amb amplificador operacional [e13]

Aquest petit circuit suma els valors dels senyals que té presents a les entrades sempre que el valor de les resistències R_1, R_2, i R_3 siguin iguals. Veiem com això ens dona una potència molt gran amb versatilitat, doncs si volem fer sumes amb percentatges d'un senyal nomes ens cal variar el valor d'una resistència i podem aconseguir senyals proporcionals. També és molt fàcil multiplicar dites senyals o obtenir la suma dels dos senyals multiplicats per cert valor (o fins i tot el d'un sol senyal).

Veiem ara un circuit restador:



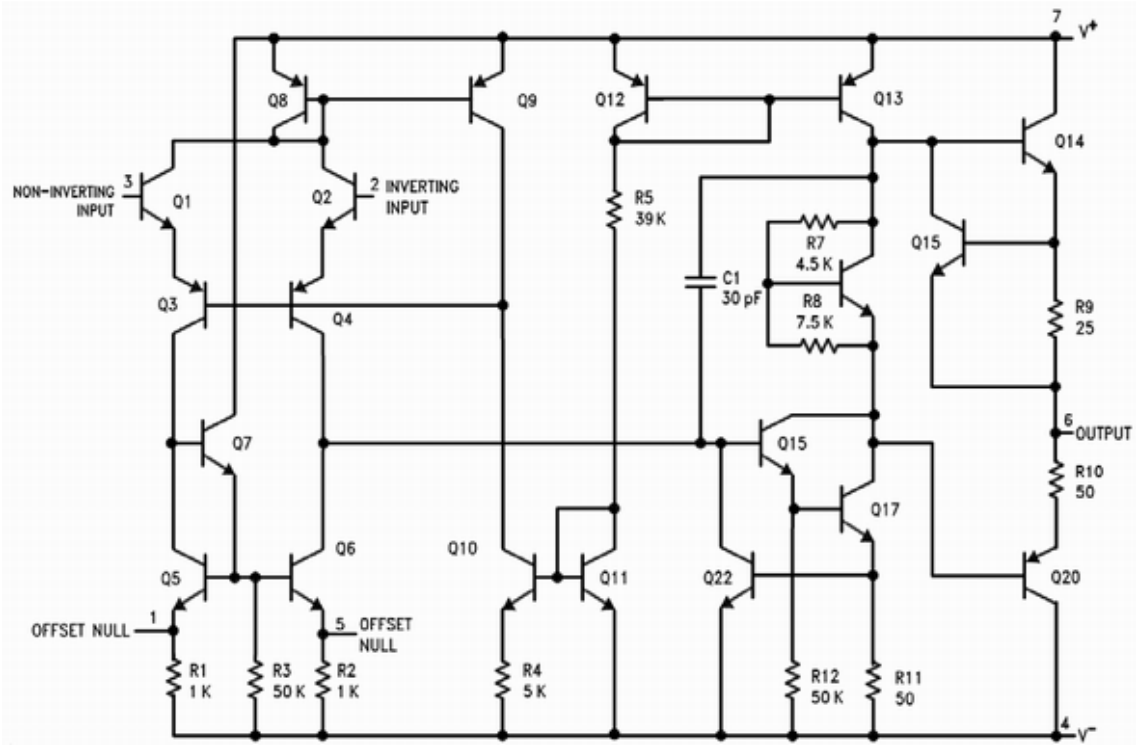
$$R_1 = R'_1$$
$$R_2 = R'_2$$

$$V_s = (V_2 - V_1)\frac{R_2}{R_1}$$

Restador analògic amb amplificador operacional [e14]

En aquest circuit, sempre que R_1 sigui igual que R_2 tindrem el senyal de sortida com la diferència dels senyals d'entrada $V_2 - V_1$. Si variem el valor d'aquestes resistències podrem obtenir senyals proporcionals de la diferència dels senyals d'entrada.

La següent figura ens mostrarà els components que conformen un amplificador operacional molt comú:



Amplificador operacional [e15]

A la figura podem veure el desenvolupament amb transistors, resistències i condensadors d'un amplificador operacional. Encapsulat en un circuit integrat normalment venent de 4 en 4 i ocupen uns pocs mil·límetres. Desenvolupat amb transistors, un de sol ocupa una superfície de varis centímetres quadrats. Fet amb vàlvules, la superfície és de molts centímetres quadrats. També els nivells de consum i temperatura són molt diferents segons la tecnologia de construcció.

9.2 Circuits integrats

Com ja hem explicat en el punt anterior els circuits integrats són circuits electrònics condensats en una petita superfície. Anem a veure en primer lloc quines avantatges presenten els circuits integrats sobre els circuits convencionals:

- El mateix circuit està integrat en un petit chip.
- El seu consum és menor. Això suposa una tassa d'averies menor, una major vida útil i en la majoria dels casos n'hi ha prou amb la refrigeració ambient.
- Menor cost. Simplement són repeticions d'un mateix patró.
- Major fiabilitat. Estalvien una gran quantitat de connexions. Facilitat de manteniment.
- Major velocitat. Això és així degut a que les connexions entre components són extremadament curtes.

S'entén per densitat en el context dels circuits integrats com el nombre de portes per unitat de superfície.

Les diferències físiques entre un circuit convencional i un circuit integrat es poden resumir de la següent manera:

- El suport d'un circuit convencional és de fibra de vidre o baquelita (els models més antics). El circuit integrat està dissenyat sobre una estructura de silici (o arseniür de gal·li).
- Les connexions entre components d'un circuit convencional solen ser llargues i de coure, mentre que les d'un circuit integrat són extremadament curtes i de semiconductor (excepte les que uneixen els punts interns amb els exteriors o terminals).
- Els circuits convencionals uneixen els seus components (transistors, resistències, bobines, etc) a les connexions de coure mitjançant soldadures (amb estany), en canvi, els circuits integrats no en tenen cosa que dona més fiabilitat en els circuits.
- El circuit integrat queda encapsulat i protegit mentre que el circuit convencional està tot exposat amb la qual cosa és més vulnerable.

Els circuits integrats es fabriquen majoritàriament de silici (Si) [35] però també d'arseniür de gal·li (Ga As) [36]. També en podem destacar dues famílies: els de tecnologia TTL i els CMOS. Les principal diferències entre les dues famílies són:

- Els TTL tenen un major consum que els CMOS.
- La tensió d'alimentació dels TTL és de 5V mentre que en els CMOS sol ser de 24V.
- La immunitat al soroll dels CMOS és superior que en els TTL.
- La rapidesa amb que commuta un TTL (passa del estat 0 a 1) és major a la de un CMOS. Per tant els TTL poden funcionar a velocitats més altes.
- Els circuits CMOS tenen un factor de carga més alt que els TTL.

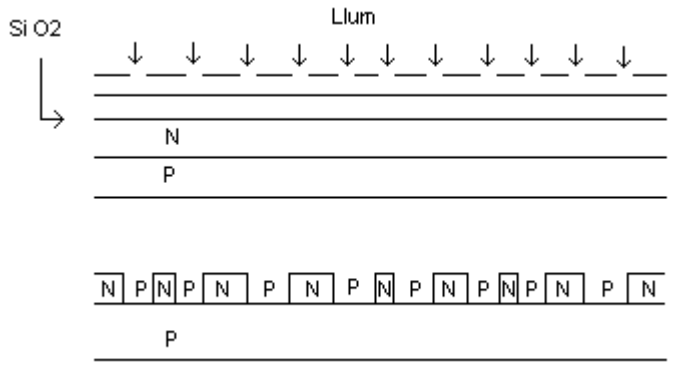
A vegades hi ha combinació d'aquests dos tipus de circuits integrats en un mateix circuit elèctric. En aquests casos s'ha de preveure adaptadors de nivell per tal de que ambdós circuits s'entenguin i per tant es puguin compatibilitzar.
Normalment els circuits CMOS s'usen en circuits digitals alimentats per bateries i en sistemes especials que tenen de funcionar llargs períodes de temps, amb baixos nivells de potència. També l'elevada immunitat al soroll és una gran avantatge per el seu ús en automatismes industrials. Els circuits TTL s'utilitzen en aplicacions en les quals es requereix d'una alta velocitat de treball

La tecnologia de fabricació d'un circuit integrat és la següent:

- 1. Obtenció del monocristall. Un monocristall és un cristall pur de silici o d'arseniür de gal·li. Podem distingir dos mètodes: el mètode de Chrozansky i el mètode d'eliminació d'impureses per alta freqüència. El cristall s'introdueix en una cubeta envoltada per una bobina en la qual circula un

corrent d'alta freqüència. El cristall s'hi introdueix lentament i aplicant-l'hi un gir constant. D'aquesta manera, les impureses es van dipositant a la part més baixa del cristall. Un cop finalitzat aquest procés, es torna a passar per una altre cubeta d'alta freqüència que acaba d'eliminar les impureses per evaporació. A aquest procés se'l denomina creixement epitaxial. Llavors es talla el cristall en oblees mitjançant un disc de diamant.

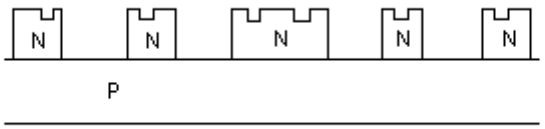
- 2. Primer procés foto litogràfic. Consta del aïllament del òxid de silici ($Si\ O_2$), foto sensibilitzat de la superfície, insolació amb màscara (reducció dels plans), revelat i atac amb àcids.



Dibuix esquemàtic del primer procés foto litogràfic [d3]

La figura mostra de forma esquemàtica el procés descrit. La finalitat és aïllar l'òxid de silici. Per això es col·loca la màscara creada amb la finalitat de que en els llocs que interessa eliminar el semiconductor N deixi passar la llum i els llocs on s'ha de preservar quedin tapats (línea de trass discontinu). Les fletxes indicant per on passa la llum en el procés d'insolació. A la part inferior tenim el resultat després del revelat i atac amb àcid (que elimina les parts insolades).

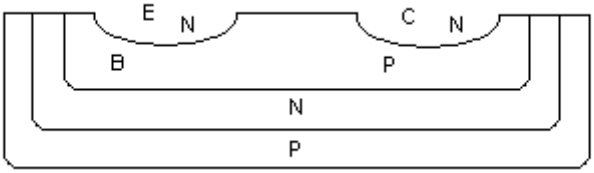
- 3. Difusió d'aïllament.
- 4. Procés foto litogràfic.



Esquema del resultat del segon procés foto litogràfic [d4]

En aquesta imatge es repeteix el procés anterior però aquest cop sobre el semiconductor N resultant per tal de crear els allotjaments per a les següents difusions.

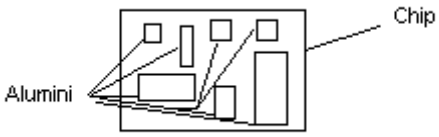
- 5. Difusió de base.
- 6. Procés foto litogràfic.
- 7. Difusió d'emissor.



Esquema del resultat de la difusió de base i emissor [d5]

En aquesta figura veiem de forma esquemàtica com s'han creat mitjançant un nou procés foto litogràfic (sensibilització de superfície, insolació i atac amb àcid) la base i l'emissor . També en aquest procés queda format el col·lector.

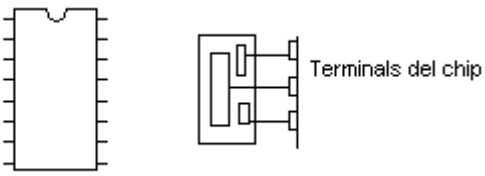
- 8. Procés foto litogràfic.
- 9. Aluminitzat.



Esquema del procés de difusió d'alumini [d6]

En aquest procés, es recobreixen las parts del circuit que tindran que sortir a l'exterior amb alumini. Posteriorment si soldaran els fins cables que aniran units en els terminals exteriors del encapsulat.

- 10. Plastificat.



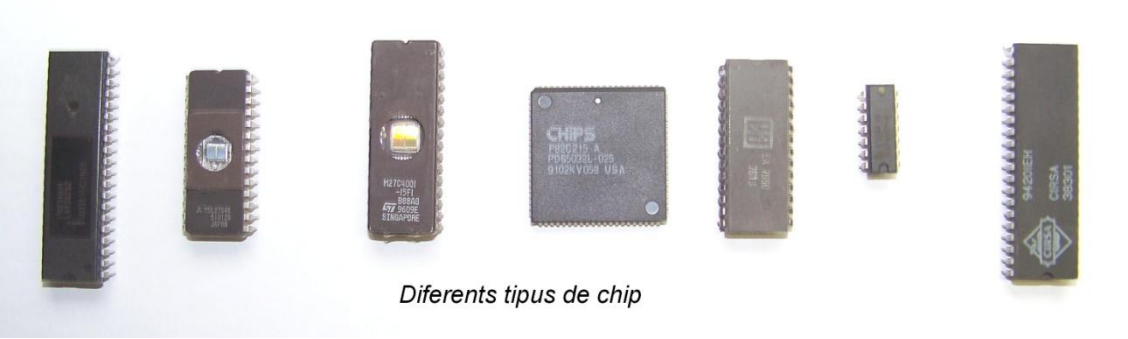
Recobriment de capa plàstica [d7]

Per últim, es recobreix el chip amb una capa que normalment és plàstica per tal de preservar-lo i donar-l'hi consistència per a la seva manipulació.

A mesura que la tecnologia en la construcció de circuits integrats avança, cada vegada es pot anar introduint més components per unitat de superfície dintre del monocristall de silici. Llavors, en la construcció dels circuits integrats es crea una classificació d'aquests segons el seu grau de densitat que s'anomena com escala d'integració. Per tant, podem definir les escales d'integració [37] com les tècniques, mides, i útils per a la consecució d'un determinat grau de densitat de circuits per unitat de superfície. La seva classificació és la següent:

- SSI(small scale integration): escala simple d'integració que encapsula fins a 10 portes per chip. Són chips de portes lògiques, inversors, buffers i amplificadors operacionals.
- MSI(medium scale integration):escala mitja d'integració amb capacitat per englobar fins a 100 portes. Aquests chips estan dedicats a descodificadors, contadors, multiplexors i demultiplexors.
- LSI(large scale integration): gran escala d'integració. Aquests chips acumulen en el seu interior fins a 1000 portes. Estan dedicats a microprocessadors de 8 bits, memòries de fins a 1kb i microcomputadors de 8 bits.
- VLSI(very large scale integration): molt alta escala d'integració. Integren fins a 10000 portes. Estan dedicats a microprocessadors de 16 bits, microcomputadors de 16 bits, memòries de 16kb i de 64kb.
- SVSLI(super very large scale integration): super molt alta escala d'integració. Integren fins a 100000 portes lògiques. En el seu abast inclouen els microprocessadors avançats i les memòries d'alta capacitat (mínim 1Mb).

En un futur no massa llunyà, es preveu que el nivell d'integració arribarà al límit degut a que ja no es podran miniaturitzar més els components (s'arribarà a nivells moleculars) i que les parets aïllants entre components seran tan petites que els electrons travessaran les parts aïllants amb la qual cosa es produiran efectes no desitjables que faran malt funcionar els circuits. Serà en aquest punt en el qual entraran en joc les lleis de la mecànica quàntica.



Imatge de diferents tipus de circuits integrats o chips [f8]

Detall d'un circuit integrat com és internament [f9]

9.3 Visió d'aquesta generació

La tercera generació es considera que comença el 1965 i englobarà els 10 següents anys, és a dir, finalitzarà el 1975. De fet en aquesta època hi ha un solapament en la fabricació de computadors ja que se'n produiran encara, amb tecnologia de la segona generació. El fet més rellevant d'aquesta generació és la introducció de circuits integrats [29]. Aquests estan compostos per nombrosos transistors, resistències i condensadors formant complexos circuits electrònics i amb la particularitat de que ocupen una superfície molt petita. Una altra avantatja és el seu baix consum i també s'augmenta la velocitat de còmput. Els circuits integrats substitueixen els transistors i se'n fabriquen amb moltes funcionalitats: des de chips que contenent varies portes lògiques de tot tipus, fins a d'altres capaços de realitzar operacions aritmètiques i lògiques. També surten les primeres memòries amb certa capacitat per l'època que ajuden amb l'emmagatzematge de dades de programa. Tot això fa que en un espai relativament reduït es pugui concentrar una considerable potència de càlcul. Ara els computadors ja no estaran nomes pensats per el càlcul matemàtic i negocis sinó que s'aplicaran a un ventall de camps molt més ampli. D'aquesta manera s'incrementa la flexibilitat dels programes i també s'estandarditzen els models. En aquesta època i degut a la velocitat que proporcionen els computadors fabricats amb circuits integrats, ja es dona la possibilitat de que en aquestes màquines pugui corre més d'un programa de forma simultània (multiprogramació).També destaca aquesta generació per el desenvolupament de sistemes operatius i de les comunicacions i interconnexions d'ordinadors en xarxa. IBM [30] és la marca que comença a desenvolupar les primeres

computadores amb circuits integrats. Es comença a popularitzar la sèrie 360 [31]. També adquireixen fama les PDP-8 [32] i PDP 11 [33] creades per Digital Equipment Corporation [34].

9.4 Fi de la tercera generació

Aquesta tercera generació va representar el inici d'una cursa cap el augment de densitat en la construcció dels chips, de manera que cada vegada aquests eren capaços de contenir circuit més complexes. Això va tenir un efecte determinant tan en la construcció com en la comercialització dels computadors. Cada vegada el cost de fabricació, potència, consum i espai que ocupaven estaven més optimitzats. El desenvolupament dels perifèrics tal com els bussos d'expansió, les memòries, els elements per emmagatzemar les dades, dispositius d'entrada de dades,etc. També es desenvolupaven a bon ritme. En aquesta pròxima generació veurem l'important avanç que experimenta el món de la computació i com comença a popularitzar-se.

10. Quarta generació

Aquesta generació bé marcada per l'avanç tecnològic en la fabricació de circuits integrats. Cada cop es redueix més la mida del component electrònic i cada cop més, se'n poden integrar quantitativament per unitat de superfície. Apareix així el microprocessador que es convertirà en el cor del computador.

10.1 El microprocessador

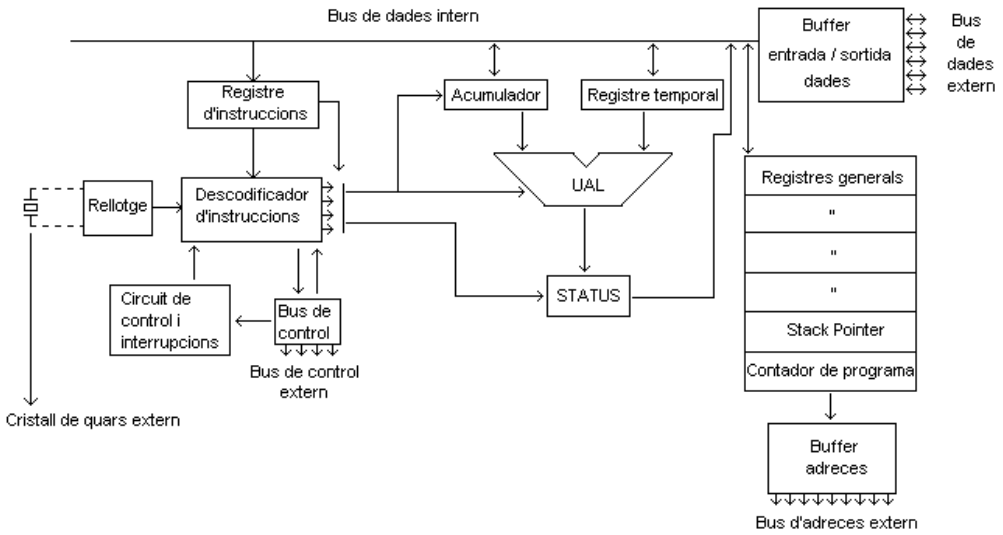
Un microprocessador o CPU (unitat central de procés) és un circuit electrònic complex i integrat en un chip, que proporciona totes les funcions de control de càlcul. La seva utilitat no es limita a ordinadors sinó que tenen un ampli camp d'aplicació: impressores, reproductors de DVD, telèfons mòbils, automoció, etc. Aquests són capaços de realitzar diverses operacions aritmètiques (sumes, restes, multiplicacions i divisions) i lògiques (funcions AND, OR, rotacions de bits, desplaçaments, etc.) entre moltes d'altres (veure referència instruccions [207]). Aquestes operacions que és capaç

de realitzar, venent classificades amb uns codis binaris que el microprocessador és capaç d'interpretar i executar. Aquests codis són el que anomenem instruccions.
El microprocessador consta de varies seccions o blocs: una unitat lògica – aritmètica anomenada UAL [46] on tenen lloc aquests tipus d'operacions; un bloc estatus que passa balanç del estat de les operacions; un(o varis) registres acumuladors [47] que contenent dades temporals que han d'intervenir en un càlcul imminent o que s'han dipositat com a resultat d'un càlcul realitzat ; registres temporals [48] que guarden resultats de càlculs entremitjos; registre d'instruccions [49] que guarda les instruccions a executar de forma immediat; un descodificador d'instruccions [50] que interpreta que ha de fer o quines operacions s'han d'executar; un bloc de registres de propòsit general [51], els quals guarden dades que s'han d'utilitzar en operacions aritmètiques o lògiques i també guarden adreces de memòria a les quals s'ha d'accedir; un registre comptador de programa [52] que guarda l'adreça de la pròxima instrucció a executar; un registre de pila (stack pointer) [53] que guarda l'adreça pròxima de la memòria de pila on es guarden dades i adreces que està utilitzant el procés en execució; un rellotge que marca el ritme en que s'executa cada operació; un bus de control [54] associat en el circuit de control i interrupcions que activa i desactiva els blocs per tal de preparar-los per executar una determinada instrucció; dos buffers: un d'adreces i un altre de dades que estan connectats en els seus respectius busos externs (de adreces [56] i dades [55]) i que són els encarregats de comunicar-se amb l'exterior i per tant, amb tots els perifèrics (memòria, controlador de teclat, controladora de vídeo, controlador de ratolí, controladores de disc dur, ports de comunicació (USB, sèrie), etc.).
En la següent taula podem veure un resum de l'estructura que guarda un microprocessador de l'època com pot ser el 8080 de Intel:

Part	**Descripció**
Buffer de dades	Memòria d'ús temporal on es guarden dades per a ser transferides cap el interior o exterior del microprocessador.
Registre d'instruccions	Registre de memòria on es guarda la instrucció pròxima a executar.
Descodificador d'instruccions	Unitat que rep les instruccions a executar i les descodifica per tal de poder portar a terme el que la instrucció sol·licita.
Seqüenciador / controlador	Bloc que porta la lògica de control per tal de preparar els senyals encaminats a l'execució de les instruccions.
Multiplexor	És un circuit lògic de control que s'encarrega de posar un registre en el bus.
ALU	Unitat aritmètica i lògica. Consta d'una sèrie de circuits combinacionals, de dues entrades de dades i una sortida. Efectua operacions aritmètiques com sumes, restes,comparacions, increment, etc. i lògiques com AND, OR, etc. També actualitza un registre especial de flags.
Acumulador	Registre que guarda resultats de la ALU i que l'hi proporciona una dada per fer l'operació pertinent.
Registre TMP	Registre que proporciona (en cas necessari) una altre dada a la

	ALU.
Registre ACT	Registre acumulador temporal en el qual l'acumulador i transfereix dades perquè les guardi mentre ell té de carregar una altra dada necessària per una operació de la ALU.
Registre de Flags	Registre especial de 8 bits en el qual es senyalitzen, activant els diferents bits, situacions que s'han produït en l'execució de l'última operació.
Registres de dades de propòsit general B,C, D, E, H, L	Són registres de 8 bits per emmagatzemar dades necessàries en l'execució de instruccions i altres propòsits.
Registre SP (Punter de Pila)	Registre que compte l'adreça de la posició alta de la pila. La pila és una part de la memòria on es guarden dades necessàries i de temporals en el transcurs de l'execució del programa.
Registre PC (comptador de programa)	Registre de 16 bit que guarda l'adreça de memòria on hi ha la següent instrucció a carregar.

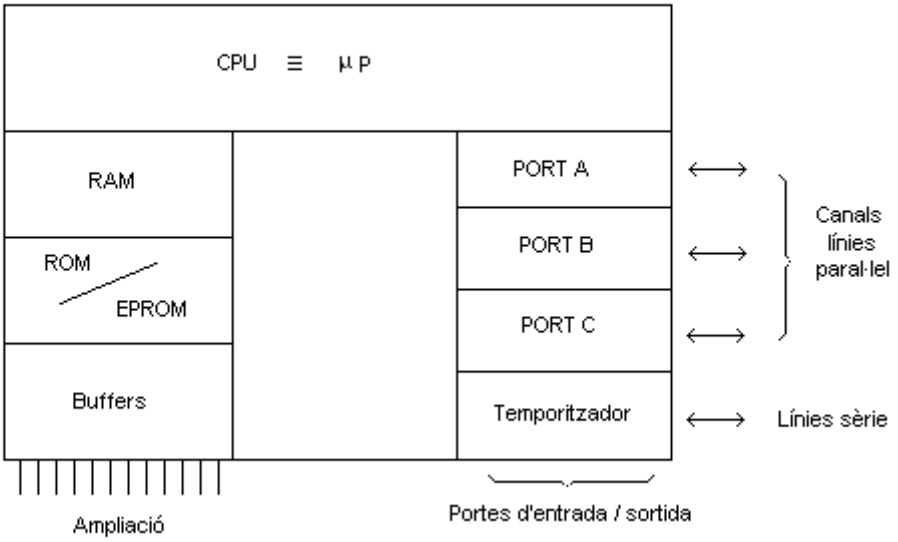
La figura següent mostra de forma esquemàtica els blocs que formen el microprocessador i que són els que acabem d'esmentar:



Esquema bàsic d'un microprocessador [e9]

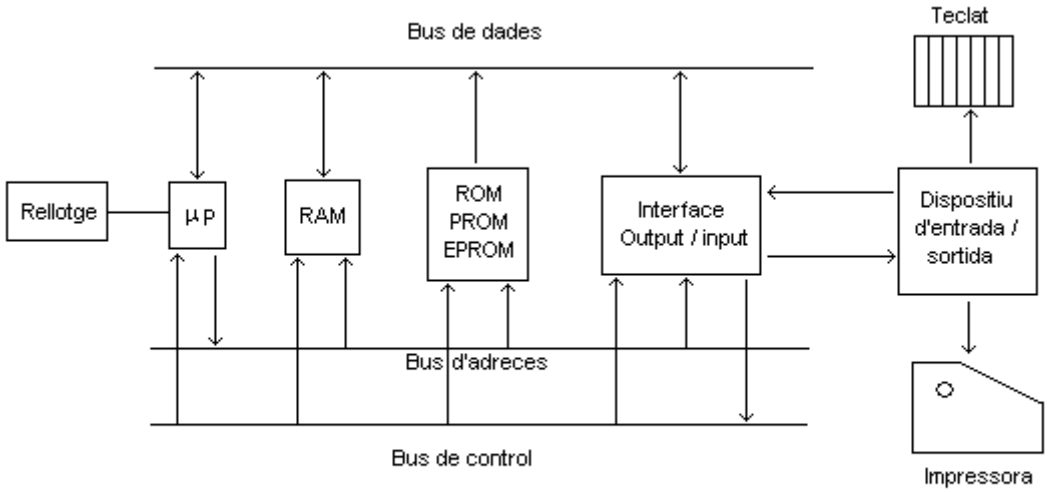
Els microprocessadors aniran evolucionant en les dècades dels 80 i 90 d'una forma vertiginosa. Aniran incrementant l'ample (amb nombre de bits) dels busos tan de dades com d'adreces la qual cosa els permetrà direccionar molta més quantitat de

memòria i transporta dades més grans, repercutint amb una reducció en els accessos de lectura / escriptura a memòria i el fet de poder realitzar operacions més amplies. També la quantitat i amplada dels registres s'incrementaran i el nombre d'instruccions augmentarà (el que revertirà en una diversificació més amplia de les operacions). La velocitat de treball també creix (la freqüència del rellotge que, recordem, marca el ritma de les operacions per segon) i també implementaran memòria interna (cau) per tal de guardar instruccions pendents d'executar de forma que es reduiran les esperes per lectures externes de codi.
De l'evolució del microprocessador arribaran els microcomputadors els quals implementen en un chip tot un computador. En la següent imatge veiem l'estructura d'aquests tipus de chip:



Dibuix esquemàtic dels microcomputadors [d8]

Aquests nous microchips tenen tota la potència d'un computador integrant a part del microprocessador, la memòria RAM on allotjar el programa i les dades, la memòria EPROM on es pot emmagatzemar el sistema operatiu i les funcions de la BIOS, els ports d'entrada / sortida de comunicació amb els perifèrics externs, buffers per ampliacions de memòria i les comunicacions sèrie via temporitzador de sincronisme.
Una manera més funcional, la podem veure a la següent imatge:



Esquema del sistema lògic usat per el µc [e10]

10.2 Tipus de màquines

La quarta generació la podem considerar o ubicar entre els anys 1975 i 1981. Els inicis d'aquesta nova generació la marquen dos fets tecnològics importants: la substitució de la memòria amb nucli de ferrita per memòria de silici integrada dintre d'un chip i la ubicació de molts més components a l'interior de un circuit integrat. S'arriba així, a un nivell de miniaturització considerable. Serà en aquesta generació que apareix el concepte de computador personal (PC). Ja el 1971, la companyia Intel[38] fabrica el primer microprocessador de 4 bits que en un espai de 4 x 5mm integra 2.250 transistors. Aquest microprocessador va ser batejat com 4004. El 1972 la mateixa companyia fabrica un microprocessador de 8 bits que bateja com a 8008. Aquest ja contenia 3.300 transistors i el seu ús és està dedicat a terminals informàtics. El 1974, fabrica un nou microprocessador, el 8080, de propòsit general, de 8 bits, que contenia 4500 transistors i era capaç d'executar un total de 200.000 instruccions per segon. El 1977 apareixen els primers microcomputadors fabricats per Apple Computer[40] i Commodore Business Machines [41]. IBM s'integra en el mercat dels microcomputadors amb el seu Personal Computer i que d'aquí ha quedat el nom de PC. Una altre de les coses importants d'aquesta generació es que per primera vegada s'inclou ja un sistema operatiu estandarditzat: el MS-DOS[42] (MicroSoft Disk Operating System). Serà ja en els finals d'aquesta generació quan els PC comencen a arribar en el gran públic i a popularitzar-se. A part de les oficines i els centres docents, aquests ja comencen a entrar a les cases particulars. Les estadístiques diuen que el 1981 estaven en actiu 2.000.000 de PCs i a finals del 1982 la xifra era de 5,5 milions. Els àmbits d'aplicació són diversos: fulls de càlcul, bases de dades amb accés a elles, editors de text, etc. i afecten a tots els camps: disseny, administració, medecina, comerç, educació, enginyeria, etc.
Apareix el disquet com a dispositiu t'emmagatzemen i també són d'ús habitual les xarxes. Aquests ordenadors, bàsicament estan formats per el microprocessador amb la placa de control, 256 kb de memòria RAM [43], 40 kb de memòria ROM[44], 1 ó 2

unitats de disquet de 5 ¼" amb capacitat de 360 kb, 5 plaques d'expansió i un monitor CGA [45] monocrom.
Cal remarcar que l'aparició del microprocessador integrat en un sol chip dotarà d'una gran potència els computadors, doncs en un espai reduït es concentra tota la unitat i potència de càlcul que amb anterioritat estava dispersa en forma de diferents circuits, amb la qual cosa es tenia d'invertir molt més temps amb traslladar dades d'un costat a l'altre, i amb la preparació dels chips que intervenien en els càlculs per a poder-los realitzar de forma coherent i ordenada.

10.3 Final de la quarta generació

Amb l'arribada dels primers microprocessadors s'inicialitzava aquesta quarta generació que ha permès reduir la mida dels computadors i augmentar la seva potència de còmput. Els costos de producció s'han decrementat molt i això els ha començat a popularitzar. Ara ja els podem trobar tant a les empreses i oficines com a les escoles, administració i s'han anat introduint a les llars. Les tasques que resolent engloben un ampli ventall i són molt diverses: fulls de càlcul, processadors de text, assistència a disseny gràfic, comptabilitat, bases de dades, etc. També en aquests anys apareixen els primers microcomputadors els quals tenen una immediata aplicació en el món dels electrodomèstics, automoció i en altre camps. És doncs en aquesta generació que comença una cursa vertiginosa en el desenvolupament de chips cada cop més sofisticats i que aniran integrat cada cop més nombre de components conferint-los així de molta més potència. Això donarà pas a una nova generació de computadors a uns preus molt assequibles, cada cop més versàtils i amb unes prestacions enormes.

11. Cinquena generació

Aquesta generació podem considerar que s'inicia el 1982 i s'estén fins el 1990. Hi ha qui considera que és la última i la limita fins els nostres dies. De fet, nosaltres fem aquesta distinció ja no tant per la diferència tecnològica (que en certa manera hi és) sinó més aviat per la manera en que s'usaran les màquines. En aquesta quinta generació, tenim que destacar les interconnexions entre tot tipus de computadores, dispositius i xarxes (xarxes integrades). Es comencen a crear esquemes o tipus de funcionament en paral·lel, és a dir, coexisteixen dins una mateixa computadora varis microprocessadors, el que obliga a desenvolupar software per tal d'aprofitar el màxim el seu ús. El nivell d'integració en aquesta generació és el VLSI (molt alta escala d'integració). També es desenvolupa la intel·ligència artificial, la robòtica i els sistemes experts. Neixen els entorns multimèdia en els quals s'integra la veu, imatge junt amb les dades. De fet, els microprocessadors d'aquesta generació i la següent, disposen d'instruccions especialitzades per operar en aquests entorns.
Dos dels computadors que varen marcar un exemple clar del còmput amb estructura paral·lela varen ser el DEC VAX-180 i el Sequent valance 8000 [57]. Aquestes màquines disposaven de 20 processadors i tenien cada un la seva memòria cau local. Cada

processador executava un treball d'usuari però Sequent venia equipat amb una llibreria de subrutines que permetia desenvolupar programes que usaven més d'un processador. Aquesta màquina va ser molt utilitzada per a explorar tècniques de programació i algorismes paral·lels. El 1985 Intel va treure el iPSC-1 [58] amb el pseudònim d'hipercub. Aquest dotava a cada processador de la seva memòria i disposava d'una interfície de xarxa per a connectar els diferents processadors. Aquesta arquitectura de memòria distribuïda significava que la memòria ja no era una limitació i es podien construir sistemes amb molts processadors. El model més gran contenia 128 processadors. Als finals d'aquesta generació es va desenvolupar un tercer tipus de processador paral·lel denominat paral·lel – dades o SIMD [59] en els quals podien existir varis milers de processadors molt simples treballant coordinadament sota una mateixa unitat de control. Tots els processadors treballen en una mateixa tasca amb variables locals. Dues de les computadores més representatives són la Connection Machine [60] de Thinking Machines i la MP-1 [61] de MasPar.
En quan a les xarxes es produeix un gran desenvolupament en tots aquests anys i van néixer els conceptes de xarxes d'àrea ample (Wide, Area network, Wan) [62] complementant a les xarxes d'àrea local (Local Area Network, LAN) [63], estimulant així la transició del esquema tradicional de Marcs Principals (Mainframes) [64] cap a la computació distribuïda, on cada usuari disposa de la seva pròpia estació de treball per a tasques personals poc complexes, compartint els recursos més costosos del servidor principal.
Els microprocessadors han experimentat un gran avanç. S'han pogut integrar molts més components en una mateixa superfície i això dota a aquests d'una potència molt més gran. Els busos de dades i adreces s'han eixamplat lo qual permet no tant sols gestionar una més gran quantitat de memòria sinó fer operacions amb números més grans amb la consegüent acceleració en els càlculs. També la freqüència a la que treballen és més alta, cosa que influeix positivament amb la velocitat a l'hora de fer les operacions. Els circuits auxiliars de control també experimenten millores ja que es van sintetitzant amb lo qual s'optimitza amb velocitat i funcionalitat. Les memòries de silici també han avançat considerablement i estalvien molt de temps d'accés a altres mitjans de emmagatzematge de dades molt més lents. Ara els programes ja poden quedar carregats a la memòria de silici d'accés ràpid des don s'executen d'una forma continua.

11.1 Tecnologia en aquesta generació

En aquesta generació la tecnologia està en constant expansió. Cada any i fins i tot cada pocs mesos s'anuncien nous productes en el mercat en una carrera entre les diverses companyies per tal d'aportar l'o últim tan en hardware com en software. Neixen noves companyies, altres es fusionen o són absorbides. La millor manera de veure aquesta evolució és fer un repàs cronològic del que don de sí tots aquests anys. Això ho podem veure per a fer-nos una idea en aquest annex II.

12. Sisena generació

Aquesta generació s'inicia el 1991 i perdura fins els nostres dies. Com s'ha comentat en anterioritat, aquests anys vindran marcats per una carrera cap a la minimització dels components lo qual ens portarà a circuits cada cop amb més components i per tant, amb una potència més gran. En el camp de les comunicacions també es produeix un gran desenvolupament degut a que l'ús de les xarxes cada cop és més habitual. Els computadors s'interconnecten entre si per treball cooperatiu i per intercanvi d'informació. Internet, el paradigma de les xarxes, s'acaba de desenvolupar i pren un protagonisme indiscutible. Ja seran milions d'usuaris arreu del mon els que en faran ús. Avui en dia, s'ha convertit en una eina fonamental per a moltes persones i avarca diferents àmbits: comunicació, videoconferència, negocis, televisió, ràdio, etc. Els computadors, a més de un gran augment de potència de càlcul, han reduït la seva mida fins el punt que els equips portàtils s'han estandarditzat i fins i tot n'han sorgit de butxaca. Els telèfons mòbils també s'han posat a l'ordre del dia i són assequibles per el gran públic, fins al punt que han començat a desplaçar la telefonia fixa en moltes llars. També és destacable el fet que el PC ha entrat a la industria però no ja a les oficines per a tasques contables i de base de dades sinó a l'automatització de la maquinaria. Els enormes armaris elèctrics plens de components, que eren els responsables de les maniobres de funcionament de les màquines s'han vist reduïts enormement en substituir la major part dels components per veritables computador els quals ocupen un espai molt reduït, tenen un baix consum, són molt més ràpids i precisos, no tenen desgast mecànic i permeten readaptacions de maniobres a baix cost ja que aquestes es basen en una modificació del programa. També en el món de l'automoció el microprocessador hi és present, exercint un control en tota la mecànica del cotxe i interactua amb l'usuari mitjançant interfícies gràfiques presentades en pantalles tàctils. Ens seria bastant difícil de trobar avui en dia electrodomèstics on no hi hagués un controlador que gestiones el seu funcionament. També els edificis disposen de tecnologia controlada per microprocessadors: gestió de persianes, aparell de calefacció, alarmes i fins i tot n'hi ha connectats en xarxa, els quals es pot gestionar la seva administració, supervisió i control remot de diversos electrodomèstics des de qualsevol punt, simplement amb un PC i connexió de xarxa.

En aquests anys doncs, la tecnologia a evolucionat però no com hem vist en altres generacions en les quals han aparegut nous components, (per exemple quan es va passar de la vàlvula al transistor o del transistor al integrat) sinó que aquesta evolució es deu a la capacitat de reduir progressivament la mida dels components cosa que ha permès minimitzar els circuits, baixar el consum, augmentar la potència i reduir l'espai. Això a afectat en els diversos àmbits de la societat i ha fomentat una veritable revolució social. Estem en l'actualitat en el que es denomina la era de les comunicacions.

En el camp dels microprocessadors, el desenvolupament de les tècniques òptiques que han permès reduir la mida dels components en la fabricació dels circuits integrats i entre ells dels microprocessadors permeten construir-los en una sol circuit i amb doble nucli (dos processadors independents en el mateix circuit integrat). És a l'any 2004 quan la firma AMD treu el primer microprocessador dual core (doble nucli). A partir d'aquest moment, altres empreses treuen també els seus microprocessadors de dos nuclis i a l'actualitat, ja en podem trobar en el mercat de fins a sis nuclis. Aquest avenç és superior al de l'increment de la freqüència a la qual funcionen (recordem que fins aquests moments es desenvolupaven microprocessadors que cada cop anaven més ràpids) degut a que un processadors en varis nuclis és capaç d'executar més instruccions a l'hora (multiprocessament o CMP (Chip – level multiprocessing)), ja que aquests, treballen en paral·lel o de forma cooperativa. Per tant la potència de còmput es veu incrementada de forma indiscutible. En aquests anys també es construeixen súper computadores (de fet, en totes les generacions se n'han construït amb la potència que la tecnologia de l'època a permès) que estan fetes amb una gran quantitat de microprocessadors treballant en paral·lel i la seva capacitat operativa és de centenars de teraflops (bilions d'operacions per segon). Així a l'any 2007 podem trobar les computadores Blue Gene/ L [208] a California amb capacitat de 280,6 teraflops, 73728 GB de memòria i amb un total de 65556 processadors; la Jaguar (Cray XT5 QC 2.3 GHz) [209] amb capacitat d'operacions de 20,2 Teraflops; l'any 2008 la Pleiades (SGI Altix ICE 8200 EX, Xeon QC 3.0/ 2,66 GHz) [210] amb 51200 GB de memòria i 63,4 Teraflops de capacitat operativa; actualment la súper computadora més ràpida està fabricada a la China. Es tracta de la Tianhe – 1A [211] amb una capacitat de còmput de 2507 Petaflops (un Petaflop equival a un trillo d'operacions per segon). Està construïda amb 14336 microprocessadors Intel Xeon. Aquestes són un reduït model de súper computadores d'aquesta última dècada dels molts models amb diferents capacitats operatives que hi ha. Per tenir-ne una visió més amplia i detallada es poden visitar els següents enllaços: súper computadores 1 [212] i súper computadores 2 [213].

Un altre aspecte a tenir en compte d'aquesta generació és la tecnologia de fabricació dels circuits integrats. A la segona generació, amb l' invenció del transistor, n'hem vist de moltes mides: des de uns que ocupaven uns pocs centímetres (amb càpsula metàl·lica de refrigeració) fins a d'altres d'uns pocs mil·límetres. Actualment , a nivell de component individual, es fabriquen transistors de fins a 1 mil·límetre, amb la tecnologia anomenada SMD (Surface Mount Technology) [214]. A nivell d'integració a gran escala, els transistors també han anat reduint la seva mida a mesura que anaven passant els anys. Així, avui en dia, podem trobar microprocessadors construïts amb tecnologia de 45 nm (milionèsima part d'un metre), 32 nm, 22 nm i Intel, l'any passat, va enunciar la fabricació d'un microprocessador (l'Atom) amb tecnologia ja de 15nm. Perquè ens fem una idea, 15 nm equivalen a la mida que ocupen 8 molècules de ADN o 60 àtoms. Això vol dir que el dia que es pugui reduir la mida a 1 nm que equivaldrà a 4 àtoms probablement estarem parlant de que hem arribat al límit. Fins ara s'anava complint la Llei de Moore [215] que diu que cada 18 mesos és duplica el nombre de transistors dintre d'un circuit integrat.

A mesura que han anat evolucionant els microprocessador i en general, els circuits integrats, també ha anat evolucionant tota la part perifèrica del computador. Així podem destacar la memòria RAM, component clau en l'execució de processos i per emmagatzemar dades, ha anat experimentant una evolució notable. De memòria Ram n'hi ha bàsicament de dos tipus: DRAM

i SRAM. La primera és dinàmica, això vol dir que per conservar el seu contingut s'ha d'anar refrescant uns centenars de vegades per segon. La segona és estàtica i, encara que també es te d'anar refrescant, no es té que fer amb la freqüència de la primera. Per tant, la segona és millor que la primera degut a que ens estalvia molts cicles de refresc i el consum és menor. L'inconvenient és el seu cost més elevat. En els seus orígens, la memòria anava col·locada en sòcols en forma de chip individual però a mesura que els computadors varen anar avançant el model de memòria va evolucionar cap a petits circuits impresos que contenien els chips de memòria i s'inserien a la placa base. Els primers que van sortir eren els denominats SIMM (Single In Line Memory Module) amb topologia primer de 30 i després de 72 pins, a unes freqüències de 66, 100 i 133 MHz i unes capacitats de 4, 16, 32, 64, 128 i 256 MB. Després surten els denominats DIMM (Dual In Line Memory) amb topologia de 168 i 184 pins, freqüències de 200, 265 i 400 MHz, amb alimentació de 3,3V i capacitats de fins a 1024 MB. D'aquest tipus de memòria en surt una denominada EDO (Extended Data Output) que es tracta d'una DRAM que millora el rendiment de mode de memòria Fast Page (memòria en mode paginat) fins a un 10%. Aquesta memòria es presenta en format DIMM de 184 pins, a 2,5V i 400MHz. Actualment estan funcionant les memòries DDR (Double Data Rate) que són mòduls compostos de memòria sincrònica SDRAM. El seu encapsulat és tipus DIMM i permet la transferència de dades per dos canals diferents de forma simultània en un mateix cicle de rellotge. Tenen 184 pins i funcionen amb una alimentació de 2,5V. En al següent taula fem un resum d'aquestes memòries:

Memòria	Nom	Temps entre senyals	Velocitat del rellotge d'E/S	Dades transferides per segon	Nom del mòdul	Màxima capacitat de transferència
DDR	DDR 200 DDR 533	10 ns 3,7 ns	100 MHz 266 MHz	200 milions 533 milions	PC 1600 PC 4300	1600 MiB/s 4264 MiB/s
DDR 2	DDR 2400 DDR21.200	10 ns 7 ns	200 MHz 600 MHz	400 milions 1200 milions	PC 23200 PC 29600	3200 MiB/s 9600 MiB/s
DDR 3	DDR 31.066 DDR 32.000	7,5 ns 3 ns	533 MHz 1000 MHz	1066 milions 2000 milions	PC 38500 PC 316000	8530 MiB/s 16000 MiB/s

El terme MiB/s equival a Mebibyte i són 1024^2. Com podem apreciar, tan les freqüències com les tasses de transferència de dades són força elevades, encara que per sota de les velocitats a les quals funcionen els microprocessadors.

Des del 1980 que s'anuncia el primer disc dur de 10 MB, aquests han anat evolucionat en aquestes dues últimes dècades de forma vertiginosa. En uns anys es passa ja a discs durs de 20, 40 i 80MB. Aquests eren d'una mida de 5,25". A la dècada dels 90, disminueix la mida d'aquests a 3,5" i augmenta la capacitat a 250 MB als principis i van evolucionant cap a capacitats majors: 1GB, 10GB, 20GB, 40GB, 140GB, etc. fins arribar els nostres dies amb capacitats de més de 2 TB. Les mides també van disminuint i en surten de 2,5", 1,8", 1" i 0,85". Aquests més petits estan destinats a dispositius mòbils i videocàmeres. També la tassa de transferència es va incrementant a mida que es van desenvolupant. Els primers tenien una tassa al voltant dels 1 – 5 MB/s i giraven a 3600 rpm. Com més ràpid giren els discs menys tarden en

localitzar els sectors i més ràpid poden llegir o escriure dades. La velocitat de gir va evolucionant i així els estàndards es queden amb 4500, 5400, 7200 i 10000 rpm. A la següent taula podrem veure un resum dels modes de transferència junt amb la seva tassa:

Modes de transferència	Tassa de transferència
PIO 0	2-3 MB/s
PIO 1, 2	4 MB/s
PIO 3	11 MB/s
PIO4	16 MB/s
MultiWord DMA 1	13 MB/s
MultiWord DMA 2	16,6 MB/s
Ultra DMA 33	33 MB/s
Ultra DMA 66	66 MB/s
SCSI-1 bus 8 bits	3 MB/s
SCSI-2 bus 8 bits	5 MB/s
Fast SCSI-2 bus 8 bits	10 MB/s
Fast Wide SCSI-2 bus 16 bits	20 MB/s
Ultra SCSI bus 8/16 bits	20/40 MB/s
Ultra2 SCSI LVD bus 8/16 bits	40/80 MB/s
IDE	33 MB/s
EIDE	66 MB/s
Ultra ATA	100 – 133 MB/s
SATA I	150 MB/s
SATA II	300 MB/s

També apareixen els malt dits discs d'estat sòlid amb capacitats que avui en dia arriben a 250 GB i fins i tot més. En realitat no es tracta de discs ja que estan construïts amb memòria i generalment, tenen tasses més baixes. També surten al mercat les memòries Flash amb capacitats avui en dia de fins a 64 GB i amb una mida molt petita (de butxaca), molt versàtils i d'un ús força estès.

Tot seguit podrem veure un petit resum evolutiu dels diferents microprocessadors amb ordre cronològic:

Any	Companyia	Processador	Bus	Freqüència	Informació
1971	Intel	4004	4 bits	740 KHZ	Arquitectura Hardvard. 2300 transistors
1972	Intel	8008	8 bits	500-800 KHZ	Tecnologia MOS
1974	National Semiconductor	SC/MP	8 bits	1-2 MHZ	Tecnologia nMOS i pMOS
1974	Intel	8080	8 bits	2 MHZ	Tecnologia nMOS
1975	Motorola	6800	8 bits	1 MHZ	Tecnologia MOS. 6800 transistors

1976	Zilog	Z80	8 bits	2,5-3,58 MHZ	Tecnologia nMOS
1978	Intel	8086/8088	16 bits	4,77-10 MHZ	Tecnologia Depletion-load nMOS
1982	Intel	80286	16 bits	6, 8, 25 MHZ	Tecnologia de 1,5 µm
1985	Intel	80386	32 bits	16, 40 MHZ	275000 transistors. Tecnologia de 1,5-1µm. Instruccions CISC
1985	Digital Equipment Corporation	VAX 78032	32 bits	5 MHZ	125000 transistors; tecnologia 3,0µm i zMOS
1989	Intel	80486	32 bits	25-100 MHZ	Tecnologia de 0,8µm
1991	AMD	AMx86	32 bits	40 MHZ	
1993	AIM	Power PC 601	32 bits	50-66 MHZ	Set instruccions RISC
1993	Intel	Pentium	64 bits	166, 200, 233, 300 MHZ	Instrucions MMX; tecnologia de 0,8-0,25µm
1994	AIM	Power PC 620	64 bits	133 MHZ	7 milions de transistors
1995	Intel	Pentium Pro	32 bits	150-200 MHZ	5,5 milions de transistors; tecnologia 0,5-0,35µm
1996	AMD	K5		50-100 MHZ	4300000 transistors;Tecnologia 0,5-0,35µm; instruccions RISC
1996	AMD	K6/K6-2	32 bits	166-500 MHZ	8,8 milions de transistors; tecnologia de 350-250nm i SIMD
1997	Intel	Pentium II	32 bits	166-450 MHZ	7,5 milions de transistors; tecnologia 0,35-0,25µm; instruccions MMX
1998	Intel	Pentium II Xeon	32 bits	450 MHZ	Tecnologia de 0,5µm
1999	Intel	Celeron	32 bits	266-600 MHZ	Tecnologia de 0,25-0,13µm
1999	AMD	Athlon K7	32/64 bits	500-650 MHZ	22 milions de transistors; tecnologia de0,23-0,13µm

1999	Intel	Pentium III	32 bits	450, 500, 733 MHZ	9,5 milions de transistors; tecnologia de 250nm; i SIMD + instruccions MMX
1999	Intel	Pentium III Xeon	32 bits	100-550 MHZ	9,5 milions de transistors; tecnologia 0,25µm
2000	Intel	Pentium 4	64 bits	1,7 GHZ	Tecnologia de 0,18µm i NetBurst
2001	AMD	Athlon XP	64 bits	500-1,4 GHZ	Tecnologia de 0,25µm
2004	Intel	Pentium 4 Prescatt	64 bits	1,8 GHZ	Tecnologia de 90-65nm
2004	AMD	Athlon 64	64 bits	1-3,2 GHZ	Tecnologia de 0,13µm – 65nm; Instruccions MMX, SSE,SSE2,SSE3,X86-64, 3D Now
2006	Intel	Core Duo	64 bits	1,06-2,5 GHZ	Doble nucli, micro arquitectura Core, tecnologia de 65-45nm; instruccions MMX, x86, SSE, SSE2, SSE3
2007	AMD	Phenom	64 bits	2,4-2,8 GHZ	3-4 nuclis, tecnologia HiperTransport i 65nm
2008	Intel	Core Nehalem i3, i5, i7	64 bits, bus amb anell 256 bits	2,66-3,33 GHZ	4 nuclis, micro arquitectura Nehalem; tecnologia de 45-32nm i 731 milions de transistors; instruccions x-86, x86-64, MMX, SSE, SSE2, SSSE3, SSE4.1, SSE4.2
2008	AMD	Phenom II / Athlon II	64 bits	2,8-3,2 GHZ	2, 3, 4, 6 nuclis; tecnologia de 45nm; instruccions 3D Now, SSE, SSE2, SSE3, SSE4a, AMD 64
2011	Intel	Core Sandy Bridge i3, i5, i7	64 bits, bus amb anell 256 bits	2,2-3,4 GHZ	Instruccions de 256 bits; tecnologia de 22nm; instruccions AVX i GPV integrada

2011	AMD	Fusion (Ontaro, Zacate, Llano, Brazos, Bulldozer)	64 bits	1,5-2,5 GHZ	GPU (processador gràfic); tecnologia de 40-28nm; instruccions SSE, SSE2, SSE3, SSSE3, SSE4a, NXbit, AMD64, Power now, AMD-V

Aquesta és una taula amb un resum cronològic representatiu de l'evolució dels microprocessadors des del seu origen. Dins cada any i família, hi ha diversos models que aquí no es presenten. Per ampliar la informació sobre aquests microprocessadors i poder veure els diferents models de cada família, en el següent enllaç es pot trobar aquesta classificació junt amb tot el complement informatiu: evolució dels microprocessadors [216].

En el següent apartat, farem una petita síntesi cronològica d'aquesta evolució en els últims anys.

12.1 Avanços de les dues últimes dècades

En aquestes dues últimes dècades s'experimenta una ràpida evolució dels computadors juntament amb les comunicacions. La clau de tot plegat està, tal com hem dit amb anterioritat, els avanços tecnològics en els diferents camps de la física que permeten dissenyar i portar a la pràctica circuit cada cop més petits i sofisticats. Farem un breu repàs de com es produeix aquesta evolució, doncs potser és la millor manera de veure aquest progrés. Això ho podem veure en el següent apartat: annex III.

13. Visió general del desenvolupament dels sistemes operatius

En el transcurs d'aquests anys, s'han anat desenvolupant junt amb els diferents computadors, un software espacial anomenat sistema operatiu, que la seva funció bàsica consisteix amb ajudà a desenvolupar els programes d'una manera estàndard, carregar-los en les màquines i facilitant la seva execució, també s'encarreguen d'administrar els recursos de la màquina. Amb això, generen una capa entre aquests i el hardware, de manera que aquest es fa transparent per el programador i usuari final.
En la primera generació i les primeres màquines, realment això no existia i els programes consistien en un cablejat que s'interconnectaba a la pròpia computadora.

Més tard, i per optimitzar el temps, aquest cablejat es substitueix per targetes perforades existint dispositius d'entrada capaços de llegir-les, i dispositius de sortida que hi deixen els resultats del còmput. En un tercer pas, aquestes targes es substitueixen per cinta magnètica on s'hi emmagatzemen els programes per tal de carregar-se un darrera l'altre tot seguit que van finalitzen la seva execució. Finalment a voltants del 1960 surten els primer sistemes operatius en format ja software. Això pràcticament succeeix amb l'aparició del transistor. A partir d'aquest punt, els sistemes operatius evolucionen a ritme del nou hardware, i cada vegada es van optimitzant més i van augmentant les seves prestacions i la seva complexitat. A mesura que la potència dels computadors augmenta, el sistemes operatius nous, s'escriuen per tal d'explotar el màxim els recursos de les màquines. Així, en el pas de les dècades, els sistemes operatius ja són capaços de gestionar la multi tasca donant així servei a molts usuaris amb temps compartit però en sensació d'exclusivitat.
Ara farem una enumeració dels principals sistemes operatius al llarg d'aquestes sis generacions de computadors:

- Any 1960: IBYS i FMS.
- Any 1961: CTSS.
- Any 1965: Multics.
- Any 1969: UNICS.
- Any 1970: BATCH,-11 (PDP-11).
- Any 1971: OS/8, UNIX.
- Any 1972: MFT, MVT, RDOS, SVS, VM/CMS.
- Any 1973: Alto OS, BS2000.
- Any 1976: CP/M, TOPS – 20.
- Any 1978: Apple DOS 3.1, TripOS, VMS, Lisp Machine (CADR).
- Any 1979: POS, NLTSS.
- Any 1980: OS-9, QDOS, SOS, XDE (Tajo), Xenix.
- Any 1981: MS-DOS.
- Any 1982: Commodore DOS, SunOS (1.0), Ultrix.
- Any 1983: Lisa OS, Coherent, Novell Netware, ProDOS.
- Any 1984: Macintosh OS (System 1.0), MSX-DOS, QNX, UniCOS.
- Any 1985: AmigaOS, Atari TOS, MIPS OS.
- Any 1986: AIX, GS-OS, HP-UX.
- Any 1987: Arthur, IRIX (3.0), Minix, OS/2 (1.0).
- Any 1988: A / UX (Apple), LynxOS, MVS/ESA, OS/400.
- Any 1989: NeXTSTEP (1.0), RISC OS, SCO Unix (Release 3).
- Any 1990: Amiga OS 2.0, BeOS (v1), OSF/1.
- Any 1991: Linux.
- Any 1992: 386 BSD 0.1, Amiga OS 3.0, Solaris 2.0.
- Any 1993: Linux Debian, Linux Slackware, Plan 9 (v1), Free BSD, Net BSD.
- Any 1994: Linux RedHat.
- Any 1995: Digital Unix (aka Tru64), Open BSD, OS / 390, Windows 95, Plan 9 (v2).

- Any 1996: Windows NT 4.0.
- Any 1997: Inferno, MAC OS 7.6, SkyOS.
- Any 1998: Mandrake Linux, (Conegut com Mandriva Linux), Solaris 7 (64 bits), Windows 98, React OS 0.0.13.
- Any 1999: AROS, MAC OS 8, React OS 0.0.14.
- Any 2000: Athe OS, Mac OS 9, MorphOS, Windows 2000, Windows ME, React OS 0.0.16, Plan 9 v3.
- Any 2001: Amiga OS 4.0, MAC OS X 10.1, Windows XP, Z / OS, React OS 0.0.18.
- Any 2002: Syllable, Mac OS X 10.2, React OS 0.0.21, Plan 9 v4, gnulinex.
- Any 2003: Windows Server 2003, Mac OS X 10.3, React OS 0.1.5.
- Any 2004: Ubuntu Linux, React OS 0.2.4.
- Any 2005: Mac OS X 10.4, React OS 0.2.9.
- Any 2006: Windows Vista, React OS 0.3.0.
- Any 2007: Mac OS X v10.5, React OS 0.3.2, iPhone OS 1.0.
- Any 2008: React OS 0.3.7, Windows Server 2008, iPhone OS 2.0.
- Any 2009: JNode 0.2.8, Mac OS X v10.6, Windows 7, React OS 0.3.10, iPhone OS 3.0, Palm webOS, Android.
- Any 2010: Windows Home 7, Android 2.1, iOS 4, Ubuntu 10.04, Windows Mobile 7.1 iOS.

En el següent enllaç, podem trobar aquesta llista de sistemes operatius junt amb informació detallada sobre les seves característiques: sistemes operatius [192].

14.1 Dispositius mòbils: evolució

A mesura que la tecnologia avançava i cada vegada els circuits es feien més petits, cada cop sortien el mercat nous productes més reduïts i amb més potència. Es en aquests context quan comencen a sorgir les primeres màquines amb capacitat de còmput, una mida reduïda i un molt baix consum: són les calculadores de butxaca i estem en els anys 70. Ja en el 1965, la companyia Texas Instruments [193] està desenvolupant un projecta de calculadores de butxaca. Serà però a l'any 1970 que des de Japó i de la mà de Sanyo [151], Sharp [194] i Canon [195] ens arribaran les primeres calculadores. Estan equipades amb display de vàlvula de buit i són capaces d'efectuar les operacions bàsiques de suma, resta, divisió i multiplicació. El 1972 HP [82] entra en el mercat de la calculadora amb un model que ja és programable i dos anys més tard un nou model capaç de llegir targes magnètiques on s'hi emmagatzemen els programes. En el 1979 les calculadores ja surten preparades per a ser connectades a perifèrics com impressores tèrmiques, unitats de disquet, ampliacions de memòria, etc. En el 1985, Casio [158], treu la primera calculadora gràfica i dos anys més tard les calculadores ja tenen potència de càlcul per a resoldre equacions quadràtiques. A la dècada dels 90 ja resolen

càlculs amb derivades, integrals, representació gràfica de funcions, etc. Arriba un punt, però, que l'ordenador portàtil guanya molt terreny i les companyes dedicades al desenvolupament de calculadores perden interès per treure nous models. És així que a l'any 2003 HP[82], una de les companyies amb més fama amb el desenvolupament de calculadores (junt amb Texas Instruments [193]), anuncia que deixa de fabricar-ne.
A l'any 1992 surt al mercat un nou aparell (presentat per Apple [80]) que neix com un assistent personal per emmagatzemar informació de tot tipus, un organitzador, amb capacitats per a reconeixement d'escriptura, pantalla tàctil, connectivitat via mòdem, sincronització amb un ordinador, i que rebrà el nom de PDA[143]. Dos any abans ja havia sortit un aparell semblant però que encara no havia estat catalogat amb aquests termes. No va ser per això fins el 1995, amb el naixement de la companyia Palm [159], dedicada a la creació de PDAs [143], que aquestes es popularitzen i experimenten un gran desenvolupament. Amb l'arribada de la telefonia mòbil, les PDAs [143] es veuen dotades de connectivitat a xarxa de telefonia amb la qual cosa, augmenten les seves prestacions amb possibilitat de connexió a Internet de forma independent. Els telèfons mòbils, que al principi no disposaven de masses recursos, cada cop es sofistiquen més fins que arriben a un punt que adquireixen moltes funcionalitats de les PDAs [143]. Podem parlar ja d'uns híbrids entre telèfon mòbil i PDA [143].
A la dècada del 2000, surt un nou element al mercat que avui en dia a rebut un impuls de desenvolupament important: es tracta de les Tablet PC [196]. En realitat, la idea del Tablet [196] és antiga, doncs ja va ser concebuda a nivell teòric a l'any 1968 per Alan Kay [197]. L'any 1982 es crea el primer prototipus anomenat GRiDpad Pen Computer de la firma GRiD Systems [198] i es llença al mercat l'any 1989. En el 2001 Microsoft torna a llançar les Tablets PC amb un model amb pantalla tàctil, amb reconeixement d'escriptura i que pot funcionar amb bolígraf. Altres companyies com HP [82], Apple [80], Nokia [122], Toshiba [169], etc. treuen models amb un nivell semblant de prestacions, amb diferents mides de pantalla, resolucions, amb funcions de telèfon cel·lular (on es pot incerta la tarja del telèfon mòbil i es possible tant de rebre i fer trucades com de connectar-se a Internet de forma autònoma), amb gran varietat de capacitats de memòria d'emmagatzematge, i interconnexió amb perifèrics. També en els finals d'aquesta dècada surten models de més baix cost destinats al oci. Estan pensats per a reproduir música, vídeos, connectar a Internet i amb serveis de missatgeria. També però contenent aplicacions per tal de crear i reproduir arxius de text amb diferents format i fulls de càlcul. Una altre aplicació que es posa a l'ordre del dia és la del llibre virtual. Tots aquestes Tablets són capaces de reproduir llibres però per això surten en el marcat i procedents de diversos fabricants els ebooks [178] que són aparells de format divers i semblant en les Tablets però específics per a la lectura de llibres amb format electrònic. Tenen capacitat per emmagatzemar milers de llibres que es poden comprar i descarregar directament de la xarxa. Funcionen amb bateries i tenen moltes hores d'autonomia doncs molts d'aquests models funcionen amb la tecnologia de tinta electrònica que optimitza el màxim el consum i està pensada per una lectura còmoda que no cansi la vista.
Com hem comentat, aquestes PDA [143] tenen diverses aplicacions depenent per el que han estat dissenyades. Normalment, les de mides més grans de pantalla (a partir de

10″) disposen de sistemes operatius com Windows [101] o Linux [107] i tenen les funcionalitats d'un portàtil amb certes limitacions tan de velocitat com d'ergonomia. També les de 7″ es poden trobar amb aquests sistemes operatius. Dins aquestes mateixes mides (principalment 7″) i per sota, són les que estan orientades a la multimèdia i al oci, amb uns sistemes operatius més lleugers, molt gràfiques i intuïtives però també amb més limitacions que les altres, tot i que tenen un ampli ventall de funcionalitats. En el següent capítol farem un repàs dels sistemes operatius que donen cobertura en aquests tipus de màquines.

14.2 Sistemes operatius que donen suport en els dispositius mòbils

Aquests dispositius mòbils que acabem de veure a l'apartat anterior tenien suport de diferents sistemes operatius que estaven dissenyats força a mida del hardware que contenien, i per tal d'aprofitar el màxim tots els seus recursos. Així podem veure que per a les PDA [143] per exemple la plataforma més utilitzada és Windows Mobile [101]. Aquesta plataforma està desenvolupada per Microsoft [84], que posa a disposició dels desenvolupadors d'aplicacions per aquest sistema operatiu, Visual Studio [199] amb els llenguatges adients com C++ [200] o .net Compact Framework [201]. Han anat surtin diverses versions que responen a la necessitat d'actualització degudes al desenvolupament del hardware. Per a la telefonia mòbil exclusiva, un dels sistemes més usat és el Symbian [202]. Aquesta plataforma ofereix un suport prou versàtil tan per a la gestió de les funcions pròpies del telèfon amb una interfície gràfica molt funcional, com també per aplicacions. Aquest sistema operatiu està basat en Java [120] i és en aquest llenguatge que es desenvolupen aplicacions. Un altre plataforma usada també en telefonia mòbil és Flash lite [203]. Està basat amb el llenguatge Flash [203] i les aplicacions també és programen en aquest llenguatge. El sistema va evolucionant amb versions a mesura que evolucionen les versions de Flash [203]. És molt utilitzat a Asia. Per el dispositius de Apple [80], el sistema operatiu utilitzat és una versió lleugera de MAC OS X [204]. Les aplicacions es desenvolupen amb llenguatge Objetive – C [205]. Tot això és made in Apple [80]. Per a les Tablet PC [196] podem destacar dos nivells de sistemes operatius o plataformes. La primera és per el tipus de màquina amb funcionalitat complerta de PC. Aquest utilitzen plataforma Windows [101](tan XP com 7 dels quals hi ha versions especials que donen suport a aquestes màquines) i també poden utilitzar plataforma Linux [107]. Le segones són les orientades al oci amb

funcionalitats més limitades que les primeres i per aquestes va sortir una plataforma basada en Linux [107] i que s'anomena Android [206] que n'han sortit ja varies versions En resum aquest és el panorama actual de les principals plataformes que donen suport al que són els dispositius mòbils de més ús d'aquest moment en vigència.

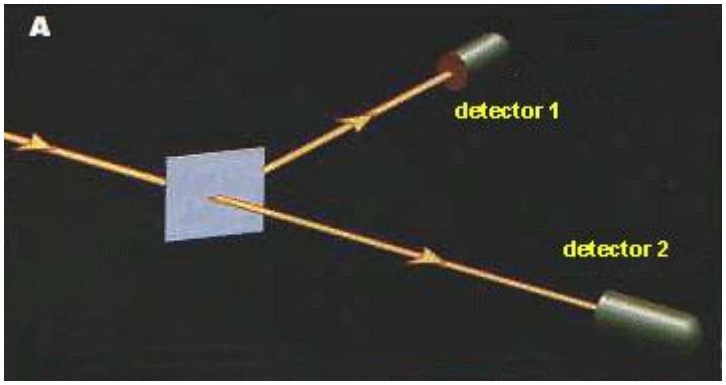
15. Alternatives tecnològiques per a nous computadors

L'augment de la densitat dels circuit electrònics no serà infinita i els seu límit no tardarà massa temps en arribar. La tendència actual en la construcció dels microprocessadors és la d'anar augmentant el nombre de nuclis per tal de dotar-los de més potència de còmput en el sentit de que sigui possible efectuar més operacions de forma simultània. Amb això s'aconsegueix una major velocitat d'operacions per unitat de temps. Malgrat la complexitat en la fabricació d'aquests circuits i els avantatges que suposen en la seva potència, els investigadors fa ja uns anys, estan cercant noves alternatives. S'han realitzat proves amb components nous com els nanotubs de carboni, circuits amb transmissió òptica, etc. que obren noves perspectives de fabricació de microprocessadors i circuits en general, que poden funcionar de forma més ràpida. Però a on molts investigadors concentren els seus esforços i molts recursos per tal d'aconseguir crear computadors de molta més potència que els actuals és amb substituir el silici per àtoms i/o molècules. Així, el nou nivell de computadores que es vol desenvolupar estan basades amb la computació quàntica i la molecular. Les primeres, aprofiten les característiques del àtom i la seva capacitat per a poder emmagatzemar informació no solsament de dos estats (0 ó 1) sinó una barreja dels dos (estats múltiples). Això permet de fer molts càlculs de forma simultània amb un molt gran estalvi de temps. També té l'avantatge de que la mida d'un àtom és extremadament petita. Els segons, estan basats en el processament d'informació amb molècules orgàniques i fer-les reaccionar en un tub d'assaig per tal de resoldre problemes. El 1994 ja es va aconseguir resoldre d'aquesta forma, un problema matemàtic mitjanament complex. Es van utilitzar una estructura de molècules de ADN per emmagatzemar la informació de sortida del problema i es van estudiar les molècules resultants de la reacció química per tal d'obtenir la solució. Si comparem un computador molecular amb un supercomputador actual, el primer té una velocitat de càlcul de 1 milió de vagades més que el segon i és capaç d'emmagatzemar 1 bilió de vagades més informació que el primer. Això és degut bàsicament a la mida de la molècula. En un espai de 1 centímetre quadrat hi podríem emmagatzemar el contingut d'informació que hi ha en un bilió de CDs. Aquestes molècules en les q1uals s'han fet

probes han estat polímers i la informació es guarda en forma de carga elèctrica. També la potència de càlcul és deguda al fet de que les molècules es poden fer reaccionar de forma simultània la qual cosa és equivalen a fer operacions en paral·lel. Si a això l'hi sumem la seva reduïda mida ens dona com a resultat una enorme quantitat de càlculs en un espai molt reduït.
Per tant, sembla que el futur ens depara una nova revolució en la fabricació de computadors i sobre tot, amb la tecnologia en que es basaran. Serà comparable amb l'aparició de la vàlvula, transistor i circuit integrat que varen marcar les pautes d'un desenvolupament que van afectar múltiples disciplines i varen tenir un gran impacte a la vida quotidiana.
En els següents capítols, anirem a profunditzar conceptualment en les bases dels computadors quàntics.

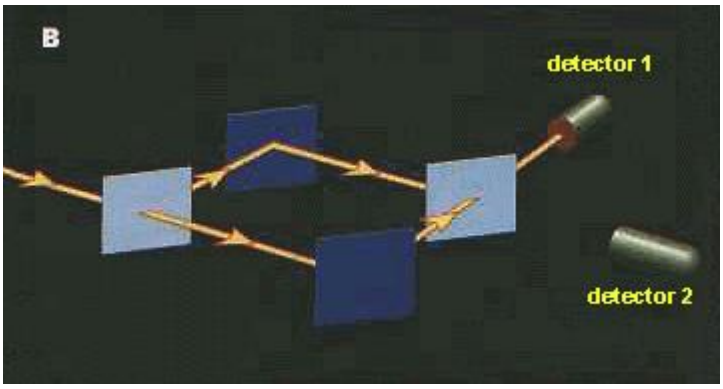
16. Breu introducció a la computació quàntica

Amb tot el que hem vist fins aquest moment sobre la lògica amb la qual treballen els actuals computadors, som conscients que aquestos operen amb bits que poden tenir dos estats o nivells lògics, i aquestos són *0* ó *1*, nivell alt o baix, veritable o fals (tres maneres de dir la mateixa cosa). Els circuits lògics, responent a unes combinacions d'aquests estats a les seves entrades amb un resultat de la mateixa naturalesa a la sortida. El que tots som conscients és que aquests estats estan presents en un determinat moment de forma concreta i inequívoca: o tenim un nivell *1* o bé un nivell *0*. Doncs bé, a partir d'ara entrem en un món diferent, el món de l'àtom. Nosaltres assignarem també en aquests un valor de *1* o bé de *0* en dos estats diferents (que veurem més endavant) però la gran novetat aquí és que podrem preparar l'àtom en el que s'anomena una *superposició coherent dels dos estats*, és a dir, l'àtom, estarà en l'estat *0* i *1* al mateix temps. Per tal de que ens anem acostumant a aquest nou concepte, serà útil considerà el següent experiment:



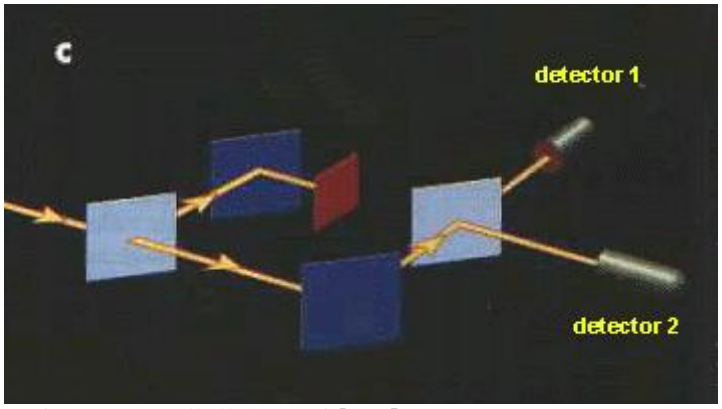
Incidència del fotó en un mirall semi platejat [d9]

Com mostra la figura, anem a mirar de fer topar un fotó en un mirall semi platejat (és un semi mirall, un tros transparent i l'altre mirall), és a dir un mirall que reflexa la meitat de la llum que incideix sobre ell, mentre que la restant, la transmetem a través d'ell. On pensem que estarà el fotó després d'haver trobat el mirall? S'ha reflectit o bé s'ha transmès a través d'ell? Seria lògic afirmar que el fotó ha tingut la mateixa probabilitat de ser transmès a través del mirall que de haver sigut reflectit per aquest. Podríem pensar que el fotó a seguit un dels dos camins a l'atzar. En efecte, si col·loquem dos fotodetectors, un el darrere del mirall i l'altre perpendicular en la direcció del feix reflectit, el fotó es registrarà amb la mateixa probabilitat , ja sigui en el detector *1* o *2*. Vol dir això que, després del mirall semitransparent, el fotó que viatge ja sigui en la direcció reflectida o transmesa ho farà amb la mateixa probabilitat del *50%*? Doncs no. De fet el fotó segueix els dos camins al mateix temps. Això es pot demostrar mitjançant la recombinació dels dos feixos amb ajuda de dos miralls totalment platejats (mirall 100%), i col·locant un altre mirall semi platejat (meitat mirall meitat transparent) en el seu punt de trobada, amb dos fotodetectors en línia directa en els dos feixos (com mostra la següent figura):



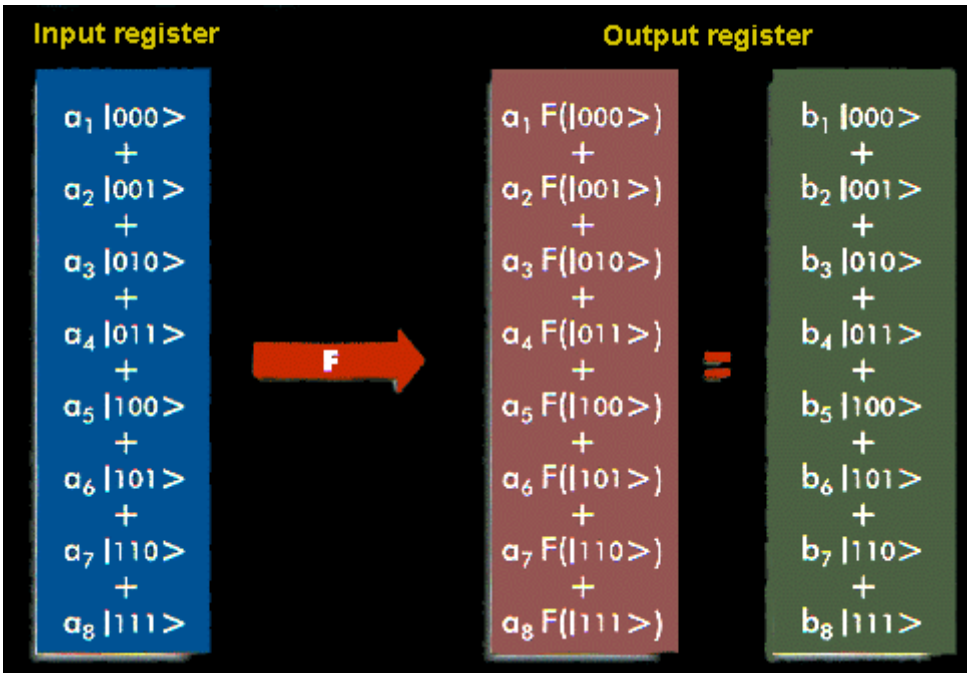
Fotó en una trampa de miralls [d10]

Amb aquesta configuració es pot observar un fenomen d'interferència quàntica realment sorprenent.
Si es donés el cas de que existís un *50%* de probabilitats que un fotó seguís un camí, i un *50%* de que seguis l'altre, llavors tindríem de tenir un 50% de probabilitats que un detector ens donés un registre de detecció i un altre 50% que ens en donés l'altre. No obstant, això no és el que succeeix. Si els dos camins són exactament igual de llargs, llavors resulta que hi ha una probabilitat del *100%* de que el fotó arribi al detector *1*, i una probabilitat del *0%* que arribi al *2*. Per tant, és segur que el fotó arriba al detector *1*. Sembla inevitable, en cert sentit, que el fotó ha tingut de recorre les dues rutes a la vegada, perquè si col·loquem una pantalla absorbidora en el camí de qualsevol de les dues rutes, llavors és igualment probable que arribi a qualsevol dels dos detectors, com podem veure en el següent dibuix:



Fotó en un mirall d'absorció [d11]

El bloqueig de un dels dos camins permet en el fotó d'arribar al fotodetector *2*; amb les dues rutes obertes, el fotó sap d'alguna manera que no se l'hi permet arribar en el fotodetector 2. Per tant podem dir que entre els dos miralls semi platejats, el fotó pren tant el camí resultat de la reflexió com el camí de la transmissió, o, en llenguatge més tècnic, podem dir que el fotó es troba en una superposició coherent del feix transmès i reflectit. Per aquesta mateixa raó, un àtom es pot preparar en una superposició de dos estats electrònics diferents, i en general un sistema quàntic de dos estats, denominat bit quàntic o qubit, es pot preparar en una superposició dels seus dos estats lògics *1* i *0*. Així doncs, un qubit pot codificar en un moment donat de temps *0* i *1*.
Anem ara a extendre la idea de la superposició dins el camp numèric. Considerem en primer lloc un registre típic de tres bits. Un registre d'aquest tipus només pot emmagatzemar en un moment donat una de les buit possibles combinacions *(000, 001, 010, 011, 100, 101, 110,111)*. Un registre quàntic format per tres qubit pot emmagatzemar en un moment donat totes les buit combinacions en una superposició quàntica. Això es mostra en el següent dibuix de forma esquemàtica on veiem el registre d'entrada, la funció i un registre de control i finalment el de sortida amb els resultats:



Registre quàntic [d12]

És remarcable que tots els buit números estan físicament en el registre, però no ens té que sorprendre que estigui al mateix temps a *0* i a *1*. Si continuem afegint qubit en el registre augmentem la seva capacitat de forma exponencial, és a dir, tres qubit poden emmagatzemar *8* números diferents a la vegada, quatre en poden emmagatzemar *16* i així successivament. En general, *L* qubit poden emmagatzemar 2^L números a la vegada. Un cop el registre està preparat en una superposició de diferents números, és possible realitzar operacions entre tots ells i tindrem tots els possibles resultats al mateix temps. Per exemple, si els qubit són àtoms, sintonitzant convenientment impulsos làser,afecten l'estat electrònic d'aquests i evoluciona cap a una superposició inicial de números codificats en diferents superposicions. En el transcurs d'aquesta evolució cada número en la superposició es veu afectat, i com a resultat es genera una computació paral·lela massiva. Això significa que un computador quàntic realitza la mateixa operació matemàtica en 2^L números d'entrada diferents codificats en superposició coherent de *L* qubit. Per a realitzar la mateixa feina en un computador convencional, es tindria que repetir el càlcul 2^L vegades o es tindria d'usar 2^L processadors treballant en paral·lel. En resum, el computador quàntic ofereix un enorme guany en temps i memòria a l'hora de realitzar càlculs.

Però tot això, desprès de tot, sona com un pur avanç purament tecnològic. Dona la impressió de que els computadors clàssics poden fer el mateix que els quàntics simplement usant més temps i més memòria. El problema és que els computadors clàssics o actuals necessiten una quantitat de temps i memòria de creixement exponencial per equipara'ls a la potència d'un computador quàntic. No disposem d'aquest temps ni d'aquesta memòria.

Per a resoldre un problema particular, les computadores d'avui dia executen un seguit d'instruccions les quals es poden anar aplicant per tal de resoldre o trobar la solució a un determinat problema. A l'especificació d'aquest conjunt d'instruccions se l'anomena algorisme. Exemples d'algorismes són els procediments elementals que s'ensenyen a les escoles per tal de fer sumes, restes, multiplicacions, etc. de nombres. Aplicant aquests procediments mecànics, sempre s'obtenen els resultats correctes per a qualsevol parell de números. Alguns algorismes són ràpids (per exemple la multiplicació), altres són molt lents (per exemple, la factorització, jugar a escacs, etc.). Considerem per exemple, el següent problema de factorització: *? x ? = 29083*

Quan temps necessitaríem per a trobar la solució, és a dir els dos números (la solució és única) usant llapis i paper? Probablement una hora. Resolem el problema invers: *127 x 129 =?* Segur que amb paper i llapis invertiríem menys d'un minut. Això és així perquè coneixem un algorisme ràpid per a la multiplicació, però el que coneixem per a la factorització no és tant ràpid. El que realment compta perquè un algorisme sigui ràpid o usable, d'acord amb la seva definició, és que aquest sigui igualment eficaç i viable tant per a números petits com grans. El mètode de la multiplicació no requereix de molt més esforç quan passem de dos números de tres xifres a dos números de trenta. Pel contrari, factoritzar un número de trenta xifres usant el mètode més simple de proba per divisió(annex 4), consumeix aproximadament 10^{13} vagades més de temps o memòria que amb números de tres xifres. La necessitat de recursos és enorme a mesura que augmentem el nombre de xifres. En número més gran que ha estat factoritzat com un desafiament va ser de *129* xifres. Ningú pot concebre com es podria en aquest moment factoritzar un número de mil dígits. Per el càlcul, s'invertiria un temps més gran que l'edat estimada de l'univers. Els informàtics tenen una forma rigorosa de definició del que és un algorisme ràpid (i útil) o lent (i inútil). Un algorisme, per a ser ràpid, el temps que es tarda per executar-lo no pot augmentar més ràpid que una funció polinòmica de la mida de l'entrada. Informalment, pensem amb la mida de l'entrada com el nombre total de bits necessaris per a especificar l'entrada del

problema, per exemple, el nombre de bits necessaris per codificar el número que es vol factoritzar. Si el millor algorisme que coneixem per a resoldre un problema té un temps d'execució (vist com una funció de la mida com la de l'entrada) delimitat per un polinomi llavors diem que el problema pertany a la *classe P [222]*. Els problemes fora de la *classe P* [222] es coneixen com a problemes difícils. Així diem, per exemple, que la multiplicació és un problema de *tipus P* [222], metres que la factorització no està a P i per això és un problema difícil. Difícil no significa impossible de resoldre o no computable. La factorització és perfectament calculable usant un computador clàssic, però els recursos físics per tal de factoritzar un número gran són de tal magnitud que a la pràctica pot resultar intractable (annex 4). Hem de senyalar que els científics informàtics han definit el que són algorismes eficients i ineficients sense fer cap referència a la part del hardware. D'acord amb això la factorització és un problema difícil per a qualsevol equip sense importar el tipus d'equip i la velocitat de rellotge a la qual pugui funcionar. Comparem el model que va dissenyar el segle *XIX* en *Babbage* [7] amb un computador d'ara. La diferència tecnològica és evident i no obstant, el model de Babbage pot realitzar els mateixos càlculs que la computadora digital moderna. La factorització és tan difícil per el model de Babbage com per les màquines actuals; el temps d'execució creix exponencialment amb la mida del número en ambdós casos. El progrés tecnològic pot augmentar la velocitat de càlcul por un factor multiplicador fix que no ajuda, però, a canviar la dependència exponencial entre la mida de l'entrada i el temps d'execució. Aquest canvi requeriria inventar nous algorismes millors. Malgrat que la computació quàntica aporta nova tecnologia, el seu poder real radica amb la creació de nous algorismes quàntics que permeten explotar la superposició quàntica i que pot contenir un nombre exponencial dels termes. Els computadors quàntics es poden programar d'una forma qualitativament nova. Per exemple, un programa quàntic pot incorporar tot una sèrie indefinida d'operacions i obtindre una superposició de tots el números de les operacions anteriors. Això no té sentit per qualsevol dispositiu de processament de dades clàssic però en té molt per un computador quàntic. Com a resultat podem construir nous algorismes per a resoldre problemes considerats difícils (com la factorització de números grans) i passar així a ser classificats com a fàcils.

La historia de la computació quàntica va començar l'any 1982 quan el físic Richard *Feynman* [226] té en consideració la simulació dels objectes de la mecànica quàntica de sistemes quàntics. Però en realitat el poder de la computació quàntica no es posa de manifest o no s'han pren realment consciència fins el 1985 quan David Deutsch [228] de l' universitat de *Oxford* publica un article teòric fonamental en el qual descriu un computador quàntics universal. A partir de llavors, el interès està en la seva realització. En aquells moments però, tot el que es va poder fer va ser plantejà una sèrie de problemes matemàtics i poca cosa més. La computació quàntica semblava una simple curiositat acadèmica. Tot això va canviar de cop el 1994 quan *Peter Shor* [225] dels laboratoris *AT & T Bell* a *Nova Jersey* va idear l'algorisme quàntic que en principi, podia realitza de manera eficient la factorització. Això es va convertir en una aplicació molt útil que nomes una computadora quàntica podia realitzar. La dificultat de factorització és que sustenta molts algorismes de xifrat com *RSA, & dash*, etc. El més popular sistema de xifrat basat en clau pública que s'usa normalment per a protegir els comptes bancaris electrònics obté la seguretat amb la dificultat de la factorització de números grans. Aquesta possibilitat de l'ús de la computació quàntica per a trencar els xifratges ha plantejat una pregunta obvia: que passa amb la construcció d'un computador quàntic?

En principi sabem com construir un computador quàntic, podem començar amb una simple porta lògica quàntica i després tractar d'integrar-la amb d'altres circuits

quàntics. Una porta lògica quàntica, com un porta clàssica, és un dispositiu lògic molt simple que realitza una operació quàntica elemental, generalment amb dos qubit, en un període determinat de temps. Òbviament, les portes lògiques quàntiques són diferents de les seves homòlogues clàssiques, degut a que poden crear i realitzar operacions de superposició quàntica (annex 5).No obstant, si seguim afegint portes quàntiques, junt a altres circuits d'aquestes característiques, ens trobarem ràpidament amb problemes pràctics molt importants. Els qubit involucrats interactuen més de l'esperat mostrant una interferència quàntica. A part de les dificultats tècniques que suposa treballar a escales d'un sol fotó -àtom, un dels problemes més importants és el de prevenir de no ser afectat per les interaccions que generen superposició quàntica. El temor és la probabilitat de que la computació quàntica s'estengui fora de l' unitat de còmput i de forma irreversible es dissipi informació útil cap el exterior. Aquest procés s'anomena decoherència. Així, el problema a resoldre per els enginyers de sistemes submicroscòpics és el d'aconseguir que els qubit interactuïn amb ells mateixos però no amb l'entorn extern.

Alguns físics són bastant pessimistes sobre les perspectives de cara a importants avenços en aquest camp. Uns científics creuen que la decoherència, a la pràctica, mai es reduirà fins el punt d'aconseguir realitzar uns pocs passos consecutius de càlcul quàntic. D'altres, els més optimistes, creuen que els computadors quàntics seran una realitat en qüestió d'anys (no de dècades). Això pot ser una pura il·lusió, però a vegades l'optimisme fa que les coses succeeixin. Després de tot, una de les veritats científiques deia que una màquina més pesada que el aire mai no podria volar.

El repte actual no està en construir immediatament un computador quàntic, sinó en passar de fer experiments en els quals ens limitem a observar els fenòmens quàntics, a poder controlar dits fenòmens. Aquest és un primer pas cap a les portes lògiques quàntiques i senzilles xarxes també quàntiques.

Llavors, podrem controlar la naturalesa a nivell d'àtoms i fotons individuals? Si, fins a cert punt es pot. Per exemple, en l'anomenada cavitat de l'electrodinàmica quàntica, experiments realitzats per *Sergio Haroche*, *Raimond*, *Jean Michel* i els seus col·legues en la *École Normale Superieure* de *París*, els àtoms poden ser controlats per els fotons individuals, atrapats en petites cavitats superconductores. Un altre enfocament defensat per *Christopher Monroe*, *Wineland David* i els seus companys de treball del *NIST* a *Boulder*. *EU*, utilitzen ions situats en una trampa de radio freqüència. Els ions interactuen entre sí excitant-los amb vibracions i l'intercanvi de cada ió pot ser controlat per separat per un raig làser enfocat adequadament i polaritzat.

Els experiments i la investigació teòrica en la computació quàntica s'estan accelerant a tot el mon. S'estan proposant noves tecnologies per a la realització de computadors quàntics i nous tipus de computació quàntica amb moltes avantatges sobre la computació convencional s'estan descobrint i analitzant i tot fa pensar que alguns d'ells donaran els seus fruits tecnològics. No importa molt el temps que es tardi en realitzar la primera computadora quàntica. La teoria de la computació quàntica en tot cas, és una part integral de la visió del mon de qualsevol persona que cerca una comprensió fonamental de la teoria quàntica i el tractament de la informació.

Els següents apartats ens parlaran del qubit, portes i xarxes quàntiques, aritmètica quàntica, algorismes quàntics, etc. No es tracta de temes senzills i per comprendre'ls es necessita una base de coneixements matemàtics i físics que probablement se'ns escapen a la majoria de nosaltres. La notació matemàtica que veurem és molt abstracta conceptualment i esta escrita amb un llenguatge de "alt nivell" (fent una analogia amb la informàtica). Però si volguéssim traduir-la a la seva essència , a "baix nivell" ens endinsaríem encara més en un terreny del tot impracticable sens tenir uns coneixements matemàtics i físics com he dit abans, molt profunds. De tota manera,

abans d'entrar-hi, es recomanable llegir-se el següent annex VI, dons s'expliquen conceptes sens matemàtiques però que pot servir d'ajut en aquesta posterior lectura.

16.1 Qubit, portes i xarxes

16.1.1 Qubit

Considerem les dues xifres binaries *011* i *111*. La primera és el número *3* en decimal i la segona el *7*. En general, amb tres bits podem aconseguir 2^3 combinacions i per tan, representar *8* números *(0 – 7)*. Un registre convencional pot guardar en un determinat moment un de qualsevol d'aquests números.
Un qubit és un sistema quàntic en el qual els estats *0* i *1* estan representats per un parell d'estats quàntics preestablerts, normalitzats i mútuament ortogonals etiquetats com $\{|0>, |1>\}$. Aquests dos estats formen la base computacional i qualsevol altre estat del qubit pot ser escrit com una superposició $a|0> + \beta|1>$ per a qualsevol a i β tals que $|a|^2 + |\beta|^2 = 1$. El qubit és típic dels sistemes microscòpics com un àtom, un spin nuclear, o un fotó polaritzat. Una col·lecció de n qubit s'anomena registre quàntic de mida n. Nosaltres assumim que la informació esta guardada en registres de format binari. Per exemple, el número *6* esta representat en un registre quàntic en l'estat $|1> \otimes|1> \otimes|0>$. En notació més compacta: $|a>$ representada per el producte tensorial [217] $|a_{n-1}> \otimes|a_{n-2}> \otimes... |a_1> \otimes |a_0>$, amb $a_i \in \{0, 1\}$ i representa un registre quàntic amb el valor $a= 2^0a_0 + 2^1a_1 + ... 2^{n-1}a_{n-1}$. Hi ha 2^n estats d'aquests tipus, que representen totes les cadenes binàries de longitud n o números de *0* fins a 2^n-1, i forment la base computacional. Quan escrivim $a\in \{0, 1\}^n$ (a és una cadena binària de longitud n) implica que $|a>$ pertany a la base computacional.
Per tant, un registre quàntic de mida 3 pot guardar individualment números com *3* i *7*:

$$|0> \otimes |1> \otimes |1> \equiv |011> \equiv |3>$$
$$|1>\otimes |1> \otimes |1> \equiv |111> \equiv |7>$$

Però també pot guardar els dos números de forma simultània. Si prenem el primer qubit i en lloc de posar-lo a *0* ó *1* preparem la superposició $\frac{1}{\sqrt{2}}(|0> + |1>)$ obtindrem:

$$\frac{1}{\sqrt{2}}(|0> + |1>) \otimes |1> \otimes |1> \equiv \frac{1}{\sqrt{2}}(|011> + |111>) \equiv \frac{1}{\sqrt{2}}(|3> + |7>)$$

De fet, podem preparar aquest registre en una superposició de tots els 8 números, per això és suficient:

$$\frac{1}{\sqrt{2}}(|0> + |1>) \otimes \frac{1}{\sqrt{2}}(|0> + |1>) \otimes \frac{1}{\sqrt{2}}(|0> + |1>)$$

Que també es pot escriure en binari (ignorant la constant de normalització $2^{-2/3}$), $|000> + |001> + |010> + |011> + |100> + |101> + |110> + |111>$ ó en notació decimal $|0> + |1> + |2> + |3> + |4> + |5> + |6> + |7>$ ó simplement $\sum_{x=0}^{7} |x>$

Per tal de realitzar operacions unitàries, cal preparar els qubit en alguna d'aquestes formes.

16.1.2 Portes lògiques quàntiques i xarxes

La porta lògica quàntica és un dispositiu que realitza una operació unitària fixa en qubit seleccionats en un període determinat de temps. Una xarxa quàntica consisteix en un dispositiu format per a portes lògiques quàntiques en les quals, els passos de càlcul es sincronitzen en el temps. Les sortides d'algunes d'aquestes portes estan connectades a les entrades d'altres. La mida de la xarxa depèn del nombre de portes que conté.
La més comú de les portes quàntiques és la porta *Hadamard*, feta d'un sol qubit que realitza la transformació unitària coneguda com la transformació de *Hadamard*. Aquesta està definida com:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad |x\rangle \;-\boxed{H}-\; (-1)^x\,|x\rangle + |1-x\rangle$$

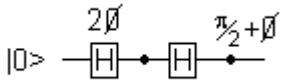
La matriu esta escrita en la base computacional $\{|0\rangle, |1\rangle\}$ i el diagrama de dalt representa la porta *H* que actua sobre un qubit en estat $|x\rangle$, amb $x = 0, 1$. Aquí és una xarxa de mida tres la qual cosa significa que afecta, la transformació de *Hadamard* en tres qubit. Si inicialment estan en l'estat $|000\rangle$ llavors la sortida és una superposició de tots els *8* números *(0 a 7)*.

$$\begin{array}{lll} |0\rangle \;-\boxed{H}-\; \frac{|0\rangle+|1\rangle}{\sqrt{2}} & | & = \frac{1}{\sqrt{2^3}}\;\{\,|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + \\ |0\rangle \;-\boxed{H}-\; \frac{|0\rangle+|1\rangle}{\sqrt{2}} & | & \qquad |101\rangle + |110\rangle + |111\rangle\;\} \\ |0\rangle \;-\boxed{H}-\; \frac{|0\rangle+|1\rangle}{\sqrt{2}} & | & = \frac{1}{\sqrt{2^3}}\;\{\,|0\rangle + |1\rangle + |2\rangle + |3\rangle + |4\rangle + |5\rangle + |6\rangle + |7\rangle\} \end{array}$$

Si els tres qubit estan inicialment en un altre estat de la base computacional, el resultat és una superposició de tots els números de *0 a 7* però exactament la meitat d'ells apareixen a la superposició amb el signe -. Per exemple:

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

En general, si comencem amb un registre de mida n en algun estat $y \in \{0, 1\}^n$ llavors $|y\rangle \rightarrow 2^{-n/2} \sum_{x\in\{0,1\}} n\,(-1)^{y*x}|x\rangle$ on el producte $y = (y_{n-1}, \ldots y_0)$ i $x = (x_{n-1}, \ldots x_0)$ és pres bit a bit és $y * x = (y_{n-1}\,x_{n-1} + \ldots y_1\,x_1 + y_0\,x_0)$.
Una altre porta és la de desplaçament de fase d'un qubit $\varnothing$ definida com $|0\rangle \rightarrow i\,|1\rangle \rightarrow e^{i\varnothing}\,|1\rangle$ o en notació matricial: $\emptyset = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\emptyset} \end{pmatrix}$ $|x\rangle$ ----•----- $e^{ix\varnothing}\,|x\rangle$
La porta *Hadamard* i la porta de fase poden combinar-se per a construir la següent xarxa de mida 4, que genera l'estat general més pur amb un simple qubit (fins a una fase global):



Portes Hadamard i de fase combinades [e16]

$$\cos \varnothing \, |0\rangle + e^{i\varnothing} \sin \varnothing \, |1\rangle$$

Com a conseqüència les portes Hadamard i les de fase són suficients per a construir qualsevol operació unitària amb un qubit simple. Par tant, aquestes portes es poden usar per a transformar estats d'entrada $|0\rangle \; |0\rangle \; ... |0\rangle$ de registres d'un qubit en qualsevol estat de tipus $|\Psi_1\rangle \; |\Psi_2\rangle \; ... |\Psi_n\rangle$ on $|\Psi_i\rangle$ és un superposició arbitrària de $|0\rangle$ *i* $|1\rangle$. Aquests són més aviat estats especials de n – qubit anomenats estats de producte o estats separables. En general, els registres quàntics de mida $n > 1$ es poden preparar en estats que no són separables i que se'ls coneix per estats entrellaçats. Per exemple per 2 qubit $(n = 2)$, l'estat:

$$a \, |00\rangle + \beta \, |11\rangle = |0\rangle \otimes (a \, |0\rangle + \beta \, |1\rangle)$$

és separable,

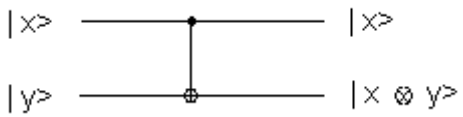
$$|\Psi_1\rangle = |0\rangle \;\; i \;\; |\Psi_2\rangle = a \, |0\rangle + \beta \, |1\rangle$$

mentre que l'estat

$$a \, |00\rangle + \beta \, |11\rangle \neq |\Psi_1\rangle \otimes |\Psi_2\rangle$$

s'entrellaça $(a, \beta \neq 0)$ perquè no es pot escriure com un producte tensorial [217].
Així, l'entrellaçament de 2 ó més qubit fa ampliable tot aquest repertori a les portes quàntiques de dos qubit. Les més populars són les *NOT Controlades (C – NOT)*, també coneguda com porta de mesurament *XOR*. El que fa és invertir el segon qubit (objectiu) si el primer (de control) és *1* i no fa res en cas de que sigui *0*. La porta es representa amb una matriu unitària:

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



Porta C – NOT [e17]

on $x, y = 0$ ò 1 i $\oplus$ denota *XOR* o *suma mòdul 2*. Si apliquem la *C – NOT* amb dades booleanes en la que el qubit objectiu és $|0\rangle$ i el control és o bé $|0\rangle$ *o* $|1\rangle$ llavors el que passa és que el control no experimenta cap canvi mentre que l'objectiu esdevé una còpia del control:

$$|x\rangle\ |0\rangle \rightarrow |x\rangle\ |x\rangle \qquad x = 0, 1$$

Podríem arribar a suposar que aquesta porta també pot ser usada per copiar superposicions del tipus:

$$|\Psi\rangle\ |0\rangle \rightarrow |\Psi\rangle\ |\Psi\rangle$$

per a qualsevol $|\Psi\rangle$. Doncs bé, això no és així. La unicitat de la porta *C – NOT* requereix canvis a superposicions en el qubit de control en l'entrellaçament de control i del objectiu. Si el qubit de control esta en l'estat de superposició $|\Psi\rangle = a\ |0\rangle + \beta\ |1\rangle$, $(a, \beta \neq 0)$, i l'objectiu a $|0\rangle$, llavors la *C – NOT* genera un estat entrellaçat: $(a\ |0\rangle + \beta\ |1\rangle)\ |0\rangle \rightarrow a\ |00\rangle + \beta\ |11\rangle$.

Diem de passada que és impossible de construir una màquina de clonació quàntica universal que realitzi la transformació de l'equació $|\Psi\rangle\ |0\rangle \rightarrow |\Psi\rangle\ |\Psi\rangle$ o inclús de manera més general: $|\Psi\rangle\ |0\rangle\ |w\rangle \rightarrow |\Psi\rangle\ |\Psi\rangle\ |w'\rangle$ on $|w\rangle$ fa referència al estat general i $|\Psi\rangle$ és qualsevol estat quàntic. Per a veure això agafem dos estats normalitzats qualsevol $|\Psi\rangle$ i $|\Phi\rangle$ els quals no són idèntics $(|\langle\Phi\ |\ \Psi\rangle\ | \neq 1)$ i no ortogonals $(\langle\Phi\ |\ \Psi\rangle \neq 0)$ i engeguem la màquina de clonar:

$$|\Psi\rangle\ |0\rangle\ |w\rangle \rightarrow |\Psi\rangle\ |\Psi\rangle\ |w'\rangle$$
$$|\Phi\rangle\ |0\rangle\ |w\rangle \rightarrow |\Phi\rangle\ |\Phi\rangle\ |w''\rangle$$

Ja que aquesta ha de ser una transformació unitària la qual preserva el contingut intern, tenim que exigir que:

$$\langle\Phi|\ \Psi\rangle = \langle\Phi\ |\ \Psi\rangle^2 \langle w'\ |w''\rangle$$

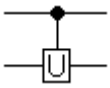
i això nomes es pot satisfer si $|\langle\Phi\ |\ \Psi\rangle| = 0$ ó 1 que contradiu els nostre supòsits. Així, els estats dels qubit, a diferència dels clàssics, no poden ser fidelment clonats. Això condueix a aplicacions interessants se'n la criptografia quàntica una de elles.

Una altre porta quàntica molt comú és la de canvi de fase controlada $B(\varnothing)$ definida com:

$$B(\emptyset) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\emptyset} \end{pmatrix}$$

Porta de canvi de fase controlada [e18]

Una altra vegada, la matriu està escrita en base computacional *{|00>, |01>, |10>, |11>}* i la figura de d'alt mostra l'estructura de la porta.
De forma més general, aquestes diverses portes controlades de *2* qubit tenen totes la forma de control *U* per algunes transformacions unitàries de tipus *U* de qubit simple. Les portes de control *U* apliquen la transformació d'identitat al qubit auxiliar quan el qubit de control esta en estat *|0>* i aplica una d'arbitrària preestablerta quan el bit de control està en estat *|1>*. Els mapes de les portes *|0> |y> a |0> |y> i |1> |y> a |1> < U |y>)* estan representades gràficament:



Porta de control U [e19]

La porta *Hadamard*, totes les portes de fase, i la *C – NOT*, formen un infinit set de portes universals. Combinant aquestes portes es possible simular qualsevol operació unitària de n qubit amb una complexitat *O(T(n))* acotada superiorment amb *cT(n)* per alguna constant *c>0* per a una n suficientment gran. Aquestes no són solsament tot el set de portes universals. De fet, qualsevol tipus de porta capaç de generar un entrellaçament de dos qubit pot ser usada com una porta universal. Matemàticament, una elecció elegant és la combinació de dues portes *Hadamard* amb la controlada *V (C – V)* on *V* es descriu amb la matriu unitària:

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

Les dues portes formen un set finit de portes universals. La xarxa conté nomes un nombre finit d'aquestes portes que poden aproximar qualsevol transformació unitària amb *2* o més qubit. De forma més precisa, si *U* és qualsevol porta de *2* qubit i $\varepsilon > 0$ llavors hi ha una xarxa quàntica de mida $O(\log^d (1/\varepsilon))$ (on d és una constant), consistent nomes amb portes *H* i *C – V* que computen una operació unitària *U'* que es troba dintre d'una distància ε de *U*. La mètrica és induïda per la norma *Euclidiana* (diem que *U'* està dins la distància ε de *U* si existeix un número complexa λ (factor de fase) tal que $|| U - \lambda U' || \leq \varepsilon$). Per tan, si substituïm *U'* per *U* a la xarxa quàntica llavors el seu estat final $\Sigma_x a'_x |x>$ aproxima l'estat final al de la xarxa original $\Sigma_x a_x |x>$ de la forma següent: $\sqrt{\Sigma_x |\lambda\alpha'_x - \alpha_x|^2} \leq \varepsilon$. La probabilitat de qualsevol resultat de medició específic sobre l'estat final, es veu afectat per un màxim de λ. Una computadora quàntica, es pot veure aquí com una xarxa quàntica (o família de xarxes quàntiques) i la computació quàntica esta definida com l'evolució unitària de la xarxa que pren el seu estat inicial (input) cap algun estat final (output). Hem triat el model de xarxa de computació en lloc d'una màquina de Turing perquè és relativament simple i fàcil de treballar-hi i perquè és molt més rellevant quan es tracta de l' implementació física de computació quàntica.

16.2 Aritmètica quàntica i avaluació de funcions

Ara descriurem com els computadors quàntics realment calculen, com sumen i multipliquen números, i com calculen les funcions booleanes mitjançant operacions unitàries. D'aquí en endavant, usarem l'aritmètica modular. Així $a \bmod b$ denota el residu de la divisió de a per b. El resultat és sempre un número més petit que b. Bàsicament $a = b \bmod n$ si $a = b + kn$ per a qualsevol enter k. Això s'expressa dient que a és congruent amb b *mòdul* n o que b és el residu de a *mòdul* n. Per exemple, $1 \bmod 7 = 8 \bmod 7 = 15 \bmod 7 = 50 \bmod 7 = 1$. L'aritmètica modular és commutativa, associativa i distributiva:

$$(a \pm b) \bmod n = ((a \bmod n) \pm (b \bmod n)) \bmod n$$
$$(a \times b) \bmod n = ((a \bmod n) \times (b \bmod n)) \bmod n$$
$$(a \times (b + c) \bmod n = (((ab) \bmod n + ((ac) \bmod n)) \bmod n$$

Per tan, si necessitem calcular per exemple, 3^8 mod 7 no usarem la forma més ingènua que consisteix en 7 productes i una enorme reducció modular. En lloc d'això farem tres petites multiplicacions i tres petites reduccions:

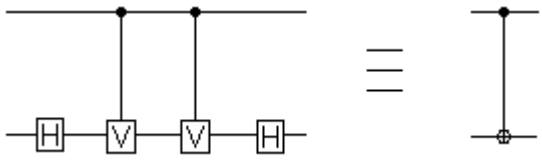
$$((3^2 \bmod 7)^2 \bmod 7)^2 \bmod 7 = (2^2 \bmod 7)^2 \bmod 7 = 16 \bmod 7 = 2$$

Aquest tipus d'aritmètica és ideal per els computadors ja que restringeix la mida dels resultats entremitjos. Per $L - bit \bmod n$, els resultats entremitjos per a qualsevol suma, resta o multiplicació no seran més grans que $2L$ bit. En els registres quàntics de mida n, la suma de mòdul 2^n és una suma de les operacions més comuns; per a tot $x \in \{0, 1\}^n$ i per a qualsevol $a \in \{0, 1\}^n$, $|x\rangle\ |(x + a) \bmod 2^n\rangle$ és una transformació unitària ben definida. La clau en aritmètica modular és l'operació inversa, i aquesta necessita la teoria bàsica de números. Un enter $a \geq 2$ és sabut que és primer si nomes és divisible per 1 i per a (considerant nomes els divisors positius). D'altre manera, a es considera compost. El màxim comú divisor de dos enters a i b és el major enter positiu d anomenat $d = mcd\ (a, b)$ que divideix tan a com b. Els dos enters a i b es diu que són primers entre si es pot demostrar que existeix un enter únic $d \in \{0, \ldots n-1\}$ tal que $ad = 1 \bmod n$. L'enter d s'anomena mòdul invers n de a i s'escriu a^{-1}. Per exemple, *mod 7* ens trobem que $3^{-1} = 5 \bmod n$ ja que $3 \times 5 = 15 = 2 \times 7 + 1 = 1 \bmod 7$. Aquesta estranya aritmètica és deguda a Karl Friedrich Gauss *[218]*. Va ser el primer a introduir-la en la seva obra *Disquistiones Arithmeticae*.

En els computadors quàntics la suma, multiplicació i qualsevol altre operació aritmètica té de ser integrada en l'evolució unitària. Ens centrarem en les portes *Hadamard* i *V controlades (c – V)* i les usarem per a construir blocs per a totes les demes portes i eventualment per a sumadors i multiplicadors quàntics.

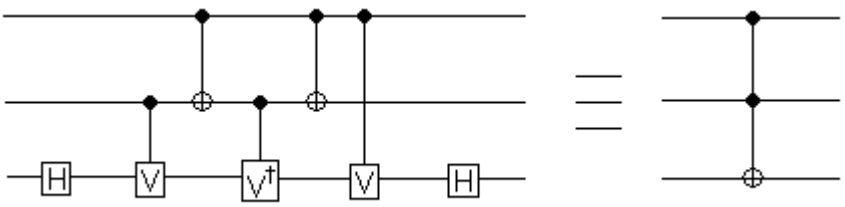
Si apliquem $c - V$ cinc vegades obtenim la identitat. Per a qualsevol de les tres sol·licituds posteriors de $c - V$ dona l'inversa de $c - V$ que s'anomena $c\text{-}V^{\dagger}$. Ara, si

tenim dues portes *c – V* i dues *Hadamard* podem construir una *C – NOT* de la següent manera:



Porta C – NOT amb 2 c – V i 2 Hadamard [e20]

Amb una porta *C – NOT* podem fer una simple operació *NOT* amb un sol qubit si el bit de control es posa a *|1>* (i és vist com un qubit auxiliar). Això però, no vol dir que ho vulguem fer a la pràctica. Una porta *C –NOT* és molt més difícil de construir que una *NOT* d'un qubit. En aquest moment estem cercant en l'estructura matemàtica de la física quàntica booleana xarxes i no importen els aspectes pràctics. Les nostres dues portes elementals també permeten de construir portes molt útils anomenades controlades - controlades *NOT* (C^2 *– NOT)* o de *Toffoli*. La seva construcció s'aprecia en la següent xarxa:

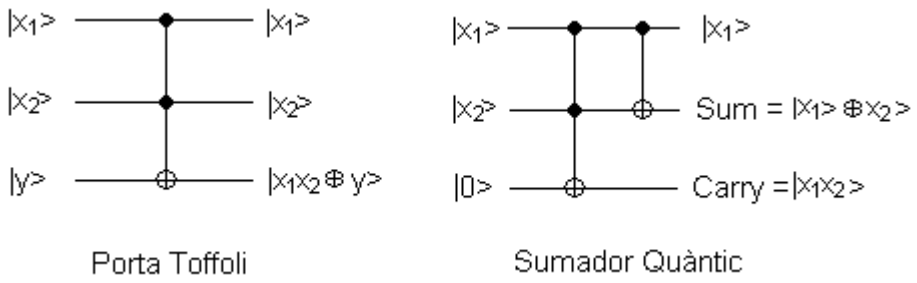


Estructura de la porta de Toffoli [e21]

Aquesta porta té dos qubit de control (els dos cables superiors del diagrama) i un objectiu qubit el qual està negat només quan els dos controls estan en l'estat *|1> |1>*. La porta C^2 -. *NOT* ens dona les connexions lògiques que necessitem per l'aritmètica. Si l'objectiu el posem inicialment a *|0>* la porta actua com a reversible *AND* (després de l'operació de la porta objectiu es torna a la lògica *AND* amb els dos qubit de control).

$$|x_1, x_2\rangle\ |0\rangle \rightarrow |x_1, x_2\rangle\ |x_1 \wedge x_2\rangle$$

Nosaltres tenim un repertori d'operacions com *NOT*, *AND*, i *C – NOT*, totes implementades com operacions unitàries. Amb principi podem avaluar una funció booleana $\{0, 1\}^n \rightarrow \{0, 1\}^m$ amb *n* bits d'entrada i en *m* bits de sortida. Una simple concatenació amb portes *Toffoli* i *C – NOT* poden simplificar els sumadors quàntics, sen un bon punt de partida per a construir sumadors complets, multiplicadors i xarxes més elaborades.



Sumador quàntic [e22]

Podem veure la porta *Toffoli* i la seva implementació quàntica per a la funció booleana $f: \{0, 1\}^2 \rightarrow \{0, 1\}$ definida per $f(x_1, x_2) = x_1 \wedge x_2$. La operació *AND* no és reversible així que l'hem hagut d'integrar en l'operació reversible C^2 – *NOT*. Si el primer bit el posem inicialment a *1* en lloc de *0* llavors el valor de $x_1 \wedge x_2$ queda negat. En general, podem escriure la funció de la porta *Toffoli* com l'avaluació de la funció:

$$|x_1, x_2\rangle\ |y\rangle \rightarrow |x_1, x_2\rangle\ |\ (y + (x_1 \wedge x_2))\ mod\ 2\rangle$$

Així és com es computa una funció booleana $\{0, 1\}^n \rightarrow \{0, 1\}^m$ en un computador quàntic. Necessitem al menys dos registres quàntics. El primer de mida *n* emmagatzema els arguments de *f* i el segon de mida *m* emmagatzema els valors de *f*. L'avaluació de la funció és una evolució unitària dels dos registres:

$$|x, y\rangle \rightarrow |x, (y + f(x))\ mod\ 2^m\rangle$$

Per tan $y\ \varepsilon\ \{0, 1\}^m$ (d'ara en endavant simplificarem la notació prescindint del sufix *mod*). Per exemple, una xarxa computacional $f: \{0, 1\}^2 \rightarrow \{0, 1\}^3$ de tal manera que $f(x) = x^2$ actua de la següent manera:

$$|00\rangle\ |000\rangle \rightarrow |00\rangle\ 000\rangle, \quad |10\rangle\ |000\rangle \rightarrow |10\rangle\ |100\rangle$$
$$|01\rangle\ |000\rangle \rightarrow |01\rangle\ 001\rangle, \quad |11\rangle\ |000\rangle \rightarrow |11\rangle\ |001\rangle$$

que es pot escriure com $|x, 0\rangle \rightarrow |x, x^2\ mod\ 8\rangle$
Exemple: $3^2\ mod\ 2^2 = 1$ que s'explica com $|11\rangle\ |000\rangle \rightarrow |11\rangle\ 001\rangle$.
De fet, per aquest tipus d'operacions necessitem un tercer registre denominat bit de treball que hem posat a zero a l'entrada i retorna zero a la sortida però que poden prendre valors diferents a *0* en el transcurs de la computació. El que fa interessant realment la funció quàntica d'avaluació és la seva acció de superposició per a diferents *x* d'entrada, per exemple:

$$\Sigma_x\ |x, 0\rangle \rightarrow \Sigma_x\ |x, f(x)\rangle$$

Produeix totes les *f(x)* per a totes les x en una sola maniobra. La desgràcia és que nosaltres no podem aconseguir tot això en l'estat entrellaçat $\Sigma_x\ |x, f(x)\rangle$ perquè

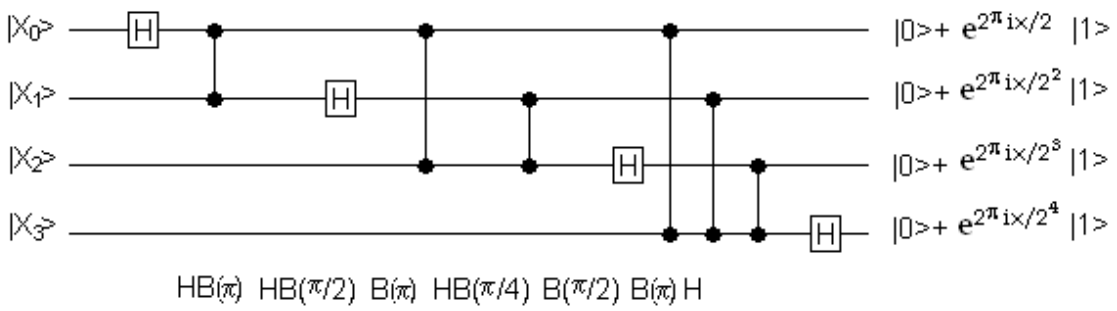
qualsevol bit amb bit de mesurament en el primer registre passarà un valor particular $x' \in \{0, 1\}^n$ i el segon registre, a continuació, es trobarà amb el valor $f(x') \in \{0, 1\}^m$.

16.3 Algorismes i la seva complexitat

Per tal de resoldre un problema concret, els computadors, siguin clàssics o quàntics, necessiten un precís set d'instruccions que pot ser aplicat de forma mecanitzada i dona solució a qualsevol instància del mateix tipus de problema. L'especificació dels set d'instruccions a realitzar s'anomena algorisme. Exemples d'algorismes són els procediments que s'ensenyen per sumar, multiplicar etc. Aquests algorismes ben aplicats sempre donen el resultat correcta per a l'operació determinada. Qualsevol algorisme pot representar-se amb una família de xarxes booleanes $(N_1, N_2, N3, ...)$ on la xarxa N_n actua per a totes les possibles instàncies d'entrada de mida n bits. Qualsevol algorisme útil ha de tenir una família específica mitjançant una xarxa com l'exemple N_n i una regla simple que expliqui com construir la xarxa N_{n+1} a partir de la N_n. Això s'anomena família uniforme de xarxes. La porta quàntica *Hadamard* té una família uniforme de xarxes d'una mida cada cop més gran a mesura que n creix segons el número de qubit d'entrada. Un altre exemple de família uniforme de xarxes és la transformada quàntica de *Fourier (QFT)[219]* definida en base computacional com una operació unitària:

$$|y\rangle \rightarrow 2^{-n/2} \Sigma_x e^{i2\pi/2n\, yx} \, |x\rangle$$

Suposem que la volem construir com una evolució unitària de n qubit usant el nostre repertori de portes lògiques quàntiques. Podem començar amb un simple qubit i observem que en aquest cas la *QFT[219]* es redueix a aplicar una porta *Hadamard*. Després podem agafar dos qubit i observem que la *QFT[219]* pot ser implementada amb dues *Hadamard* i la de control de canvi de fase $B(\pi)$ al mig. Progressant per el mateix camí podem construir tres qubit i quatre, la xarxa de les quals podem veure tot seguit:



Implementació de la QFT amb una xarxa de portes [e23]

Hi ha tres diferents tipus de portes $B(\varnothing)$ a la xarxa i són: $B(\pi)$, $B(\pi/2)$ i $B(\pi/4)$.
El cas general per a n qubit requereix una extensió trivial de xarxes seguint la mateixa seqüència patró de portes H i B. Les xarxes que operen en la QFT [219]de n qubit contenen n portes H i $n(n-1)/2$ portes de canvi de fase B, en total $n(n+1)/2$ portes elementals.
El gran problema en el disseny d'algorismes o de les seves corresponents famílies de xarxes, és l'òptim ús de recursos físics que requereix per resoldre el problema. La teoria de la complexitat fa esment de l'inherent cost de la computació en termes de designar operacions elementals, ús de memòria i mida de la xarxa. És sabut que un algorisme per a ser ràpid o eficient el nombre d'operacions elementals adoptades per executar és més ràpid que una funció polinòmica de la mida de l'entrada. Nosaltres, generalment, prenem la mida de l'entrada com el nombre total de bits necessaris que especifica l'entrada(per exemple un número N requereix log_2N bits d'emmagatzemen binari en el computador). En el llenguatge de complexitat de xarxes un algorisme se sap que és eficient si és uniforme i de mida polinòmica $(O(n^d))$ per alguna d constant. Per exemple la QFT[219] pot ser construïda d'una manera eficient perquè té una família de xarxes uniforme la mida de la qual creix nomes com una funció quadràtica amb mida d'entrada $O(n^2)$. Canviant un tipus de portes per unes altres en la seva construcció, per exemple construint-les amb *Hadamard* i $c-V$ amb una precisió prescrita ε, nomes pot afectar la mida de la xarxa amb una constant multiplicativa que no afecta l'escala quadràtica de n. Per tant la complexitat de la QFT[219] és $O(n^2)$ sens importar el tipus de portes que usem. Els problemes que no tenen algorismes eficients són els problemes catalogats com a difícils.
Les operacions aritmètiques elementals que ensenyen a les escoles com sumes llargues, multiplicacions o divisions de números de n bits necessiten $O(n^2)$ operacions. Per exemple, per multiplicar $x=(x_{n-1} \ldots x_1\ x_0)$ i $y=(y_{n-1} \ldots y_1\ y_0)$ multipliquem de forma successiva y per x_0, x_1, etc. canviem i després sumem el resultat. Cada multiplicació Y per x_k prenem operacions sobre n bits simples, sumem els n productes fen del ordre de n^2 operacions de bit, i amb les sumes, fem un total de $O(n^2)$ operacions. Coneixen la complexitat de les operacions aritmètiques elementals podem avaluar sovint la complexitat d'altres algorismes. Per exemple, el *mcd* de dos enters x i y amb $y < x$ es pot trobar usant l'algorisme d' Euclides [220]. El més vell no trivial algorisme ve ser conegut i usat el 300 A.C. Primer divideix x per y obtenint el resta r_1. Ara, dividim y per r_1 i obtenim el resta r_2, llavors dividim r_1 per r_2 i obtenim el resta r_3, etc. Al final obtindrem un resta 0. L'últim resta que no és 0 és el $mcd(x, y)$ perquè divideix a tots els restes anteriors i per tant també x i y. Per exemple, aquesta és una seqüència de restes (r_j, r_{j+1}) resultant d'aplicar l'algorisme de Euclides {[220]per cercar el *mcd* de $(12378, 3054) = 6$:
$(12378, 3054)$, $(3054, 162)$, $(162, 138)$, $(138, 24)$, $(24, 18)$, $(18, 6)$, $(6, 0)$. Quina és la complexitat d'aquest algorisme? És fàcil de veure que la longitud d'aquets dos números és al menys, la meitat cada dos passos així que cada dos passos es necessita un bit menys per a representar el número, per la qual cosa, el número de passos es troba o és al menys $2n$, on n és el número de bits en els dos números. Cada divisió es pot fer amb menys de $O(n^2)$ operacions, per tant el nombre total d'operacions és $O(n^3)$.

Hi ha bàsicament tres tipus de xarxes booleanes: *clàssiques deterministes, clàssiques probabilístiques* [221] i algorismes quàntics. Les primeres estan basades amb connectives lògiques tals com *AND*, *OR*, i *NOT* i estan sempre obligades a donar una resposta correcta. Si un problema admet xarxes uniformes deterministes de mida polinòmica, sabem que el problema és de *classe P* [222]. Les xarxes probabilístiques tenen portes sumadores "*coin flip*" (cara o creu) que no tenen cap entrada i emeten una distribució uniforme de bit aleatori en el transcurs de l'execució de l'operació. Malgrat que les xarxes probabilístiques poden generar respostes errònies, poden ser més poderoses que les deterministes. Un bon exemple és la proba de números primers, que donat un número x de n bits decideix si aquest és o no primer. La més petita xarxa determinista coneguda resol el problema amb $O(n^{d \log \log n})$ que no és un temps polinòmic. No obstant hi ha un algorisme probabilístic, el de *Solovay i Strassen* [223], que pot resoldre el mateix problema mitjançant una xarxa uniforme probabilística de mida o complexitat $O(n^3 \log(1/\varepsilon))$, on ε és la probabilitat d'error i no depèn de n poden ser triat tan petit com vulguem i tot i així tindrem un algorisme eficient. El $\log(1/\varepsilon)$ l'expliquem a continuació. Imaginem una xarxa probabilística que resol un problema de decisió i amb una probabilitat d'error menor a $\frac{1}{2} + \delta$ per $\delta > 0$. Si nosaltres posem en marxa r d'aquestes xarxes en paral·lel (de manera que la mida de la xarxa s'incrementa en un factor r) i usa el vot per majoria per a la resposta final de *si* o *no*, la nostra probabilitat general d'error es limita a $\varepsilon = \exp(-\delta^2 r)$ (això es dedueix directament de *Chernoff* [224]). Per tan, r és del l'ordre de $\log(1/\varepsilon)$. Si el problema admet aquesta família de xarxes sabem que el problema és de la classe *BPP* (és sinònim de "*error acotat polinòmic probabilístic*").

Per últim però no menys important, tenim algorismes quàntics, o famílies de xarxes quàntiques que són més potents que les homòlogues probabilístiques. Un exemple d'això és el problema de la factorització. Prenem un número x de n bits i busquem la llista de factors primers de x. La família de xarxes uniformes probabilístiques resolent el problema amb mida $O(2^{d\sqrt{n \log n}})$. Una de les raons per les quals la computació quàntica està de moda avui és per el descobriment per part de *Peter Shor*[225] de la família uniforme de xarxes quàntiques de $O(n^2 \log \log n \log(1/\varepsilon))$de mida, que resol el problema de la factorització. Si el problema admet aquests tipus de xarxes de mida polinòmica que per a qualsevol entrada dona la resposta correcta amb probabilitat superior a $\frac{1}{2} + \delta$ per $\delta > 0$ llavors sabem que el problema està inclòs a la classe *BQP* (error delimitat probabilístic polinòmic) i tenim que $P \subseteq BPP \subseteq BQP$.

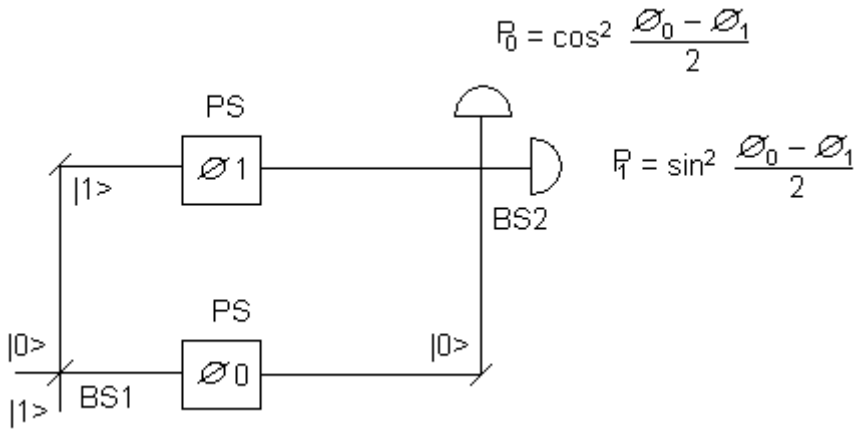
Les xarxes quàntiques són potencialment més poderoses perquè la interferència de les multi partícules quàntiques (un fenomen intrínsecament quàntic) fa que la teoria quàntica sigui radicalment diferent de la teoria estadística clàssica.

Richard Feynman [226] va ser el primer en anticipar la gran potència dels computadors quàntics. Va observar que és impossible de simular l'evolució quàntica en un computador probabilístic quàntic d'una forma eficient, és a dir, qualsevol simulació de l'evolució quàntica sembla implicar una desacceleració exponencial de temps comparada en l'evolució natural ja que la quantitat de informació necessària per descriure l'estat d'evolució quàntica en termes clàssics generalment creix exponencialment en el temps. No obstant, en lloc de veure això com un obstacle, *Feynman* [226] ho va veure com una oportunitat. A continuació seguirem el seu

exemple i tractarem de construir un computador usant els efectes inherents de la mecànica quàntica.

16.4 Des de interferòmetres a computadors

Una interferència de partícules individuals en el *Mach Zehnder* [227] (interferòmetre) treballa de la següent manera. La partícula, en aquest cas un fotó, incideix sobre una paret divisòria *(BS1)* i les seves possibles amplituds es propaguen a traves de diferents camins a una altre paret divisòria *(BS2)* que dirigeix la partícula cap a un dels dos detectors. Al llarg de cada ruta cap a una de les dues parets divisòries hi ha un modulador de fase *(PS)*.



Dibuix esquemàtic d'un interferòmetre [e24]

Si el camí inferior és posat al nivell d'estat |*0*> i el superior a l'estat |*1*> llavors la partícula, inicialment en el camí |*0*>, es sotmet a la següent seqüència de transformació:

$$|0> \xrightarrow{BS1} \frac{1}{\sqrt{2}}(|0> + |1>) \xrightarrow{PS} \frac{1}{\sqrt{2}}\left(e^{i\phi_0}|0> + e^{i\phi_1}|1>\right) =$$

$$= e^{i\,\frac{\phi_0+\phi_1}{2}}\,\frac{1}{\sqrt{2}}\,(e^{i\,\frac{\phi_0-\phi_1}{2}}\,|0> + e^{i\,\frac{-\phi_0+\phi_1}{2}}\,|1> \xrightarrow{BS2}$$

$$\xrightarrow{BS2} e^{i\,\frac{\phi_0+\phi_1}{2}}\,(\cos\frac{1}{2}\,(\phi_0 - \phi_1)|0> + i\sin\frac{1}{2}\,(\phi_0 - \phi_1\,|1>)$$

on $\varnothing_0$ i $\varnothing_1$ són els valors resultants dels moduladors de fase i l'acció de les parets divisòries es defineix com:

$|0\rangle \rightarrow \frac{1}{\sqrt{2}}\ (\ |0\rangle + |1\rangle),\quad |1\rangle \rightarrow \frac{1}{\sqrt{2}}\ (\ |0\rangle - |1\rangle).$

(Hem ignorat el desplaçament de fase en el feix reflectit). El canvi de fase global $e^{i\,\frac{\phi_0+\phi_1}{2}}$ és irrellevant ja que el patró d'interferència depèn de la diferència entre els canvis de fase en les diferents branques del interferòmetre. El canvi de fase en els dos camins es pot ajustar per efectuar qualsevol canvi de fase relativa prevista $\varnothing = \varnothing_0 - \varnothing_1$ i per dirigir la partícula amb probabilitats:

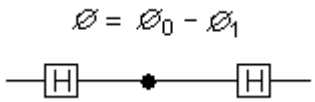
$$P_0 = cos^2\left(\frac{\phi}{2}\right) = \frac{1}{2}\ (1 + cos\phi)$$

$$P_1 = sin^2\left(\frac{\phi}{2}\right) = \frac{1}{2}\ (1 - cos\phi)$$

respectivament cap els detectors *0* i *1*.

Les funcions dels tres ingredients claus en aquest experiment són clares. La primera paret separadora prepara la superposició dels possibles camins, els canviadors de fase modifiquen les fases quàntiques en els diferents camins i la segona paret separadora combina tots els camins i també esborra tota la informació sobre els camins que han seguit o pres les partícules entre les dues parets separadores. Aquesta supressió o esborrat és molt important com veurem tot seguit.

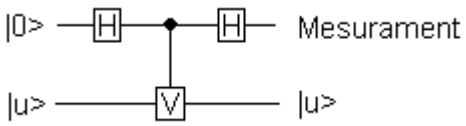
No cal dir que els experiments d'interferència de partícula simple no estan restringits a fotons. Es pot agafar diferents hardware i repetir l'experiment amb electrons, neutrons, àtoms o inclús molècules. Quan es tracta d'àtoms i molècules es poden usar graus de llibertat tan interns com externs. Encara que els experiments d'interferència de partícula simple val la pena de discutir-los, nomes estem interessats simplement en les seves característiques genèriques perquè totes elles són "*isomòrfiques*" i un cop coneixem i comprenem una d'elles al menys per els nostres propòsits, les comprenem totes (mòdul de detalls experimentals, per suposat). Anem a descriure qualsevol experiment de interferència de partícula simple amb els termes més generals. Les parets separadores es diran ara porta *Hadamard* i els canviadors de fase (desfasadors) portes desfasadores. En particular, qualsevol interferència quàntica de partícula simple es pot representar com la següent xarxa simple:



Interferència quàntica de partícula simple [e24]

Amb la finalitat de connectar amb una avaluació de la funció quàntica anem a descriure una construcció alternativa que simula l'acció de la porta desfasadora.

Aquesta construcció introdueix un factor de fase $\varnothing$ fen ús d'una porta de control U. El desfasador $\varnothing$ està controlat amb l'ajut d'un qubit auxiliar en l'estat preestablert $|u>$ tal que $U|u> = e^{i\varnothing}\,|u>$.



Simulador de porta desfasadora [e26]

En el nostre exemple obtenim la següent seqüència de transformacions en els dos qubit:

$$|0>\ |u> \xrightarrow{H} \frac{1}{\sqrt{2}}\ (|0> + |1>)\ |u> \xrightarrow{CV} \frac{1}{\sqrt{2}}\left(|0> + e^{i\phi}\,|1>\right)|u> \xrightarrow{H} cos\frac{\phi}{2}\,|0> + i\,sin\frac{\phi}{2}\,|1>|u>)$$

Podem veure que l'estat del qubit auxiliar $|u>$ és un estat propi de U, no s'altera al llarg de la xarxa, però el seu valor propi $e^{i\varnothing}$ és "*rebotat*" davant de $|1>$ component en el primer qubit. La seqüència és una simulació exacta del interferòmetre de *Mach – Zehnder* [227] i, com veurem més endavant, el nucli dels algorismes quàntics.
Algunes operacions de les portes *control – U* són especials i representen funcions d'avaluació quàntica. De fet, una evolució unitària que calcula $f: \{0, 1\}^n \rightarrow \{0, 1\}^m$

$$|x>\ |y> \rightarrow\ |x>\ |(y + f(x))\ mod\ 2^m>$$

es de tipus de *control – U*. La transformació unitària del segon registre especificada com $|y> \rightarrow\ |(y + f(x))\ mod\ 2^m>$ depèn de x (del estat del primer registre). Si el estat inicial del segon registre s'estableix a:

$$|u> = \frac{1}{2^{\frac{m}{2}}}\ \sum_{y=0}^{2^m-1} exp\left(-\frac{2\pi i}{2^m}y\right)|y>$$

mitjançant l'aplicació de *QFT* [219] al estat $|111...1>$, llavors la funció d'avaluació general és:

$$|x>|u> = \frac{1}{2^{m/2}}\ |x> \ \sum_{y=0}^{2^m-1} exp\left(-\frac{2\pi i}{2^m}y\right)|y> \rightarrow \frac{1}{2^{\frac{m}{2}}}\ |x> \ \sum_{y=0}^{2^m-1} exp\left(-\frac{2\pi i}{2^m}y\right)|f(x)+y>$$

$$= \frac{e^{\frac{2\pi i}{2m}\ f(x)}}{2^{m/2}}\ |x> \sum_{y=0}^{2^m-1} exp\left(-\frac{2\pi i}{2^m}(f(x)+y)\right)|f(x)+y> = \frac{e^{\frac{2\pi i}{2m}\ f(x)}}{2^{m/2}}\ |x>$$

$$\sum_{y=0}^{2^m-1} exp\left(-\frac{2\pi i}{2^m}y\right)\Big|y> = \ e^{\frac{2\pi i}{2m}} f(x)\Big|x>|u>$$

on tenim l'índex del sumatori que conté la suma de 2^m termes:

$$\sum_{y=0}^{2^m-1} exp\left(-\frac{2\pi i}{2^m}\ (f(x)+\ y)\right)\ |f(x)+\ y> = \ \sum_{y=0}^{2^m-1} exp\left(-\frac{2\pi i}{2^m}\ y\right)\ |y>$$

Un cop més, la funció d'avaluació introdueix factors de fase davant de termes $|x>$ en el primer registre:

$$|x>|u> \rightarrow exp\left(\frac{2\pi i}{2^m}\ f(x)\right)\ |x>|u>$$

Notis que la resolució a $\emptyset(x) = \frac{2\pi}{2^m}\ f(x)$ esta determinada per la mida de m en el segon registre. Per $m = 1$ obtenim $\emptyset(x) = \pi f(x)$, és adir, el factor de fase és $(-1)^{f(x)}$. Veurem com aquest enfocament explica el funcionament intern dels algorismes quàntics.

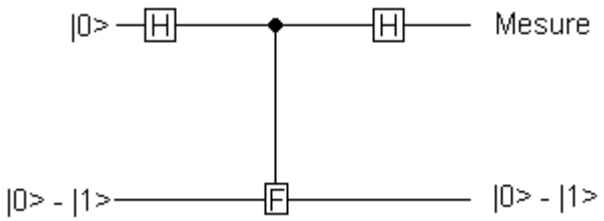
16.5 Els primers algorismes quàntics

Els primers algorismes quàntics van mostrar els avantatges de la computació quàntica en lo que és refereix a la mesura de la complexitat computacional amb les propietats de l'escala de la mida de les xarxes. La potència computacional de la interferència quàntica va ser descoberta en contar quantes vegades certes funcions booleanes tenen de ser avaluades amb la finalitat de trobar la resposta a un determinat problema. Imaginem una *caixa negre* anomenada "*oracle*" que computa una funció booleana i un escenari en que nosaltres volem aprendre sobre alguna propietat de dita funció però tenim que pegar per cada cop que usem la caixa negre. L'objectiu és el de minimitzar el número de usos.

Considerem per exemple, que la *caixa negre* computa la funció booleana $f: \{0, 1\} \rightarrow \{0, 1\}$. Hi ha 4 d'aquestes funcions: 2 de constants $f(0) = f(1) = 0$ i $f(0) = f(1) = 1$ i dues altres de balancejades: $f(0) = 0$, $f(1) = 1$ i $f(0) = 1$ i $f(1) = 0$. La feina consisteix en deduir mitjançant l'ús de la *caixa negre* quines *f* són balancejades i quines constants (quines $f(0)$ i $f(1)$ són iguals i quines diferents).

La intuïció clàssica ens diu que tenim d'avaluar tan $f(0)$ i $f(1)$, el que implica avaluar *f* dues vegades (dos accessos a la *caixa negre*). Veurem que això no és tant, amb l'entorn de la informació quàntica, doncs podrem resoldre el problema amb una simple avaluació usant un algorisme que té la mateixa estructura matemàtica que el interferòmetre de *Mach – Zehnder* [225]. L'algorisme quàntic que resolt aquest problema

queda més ben representat amb una xarxa quàntica que mostrem a continuació, on l'operació del mig representa la caixa negre que avalua la funció:

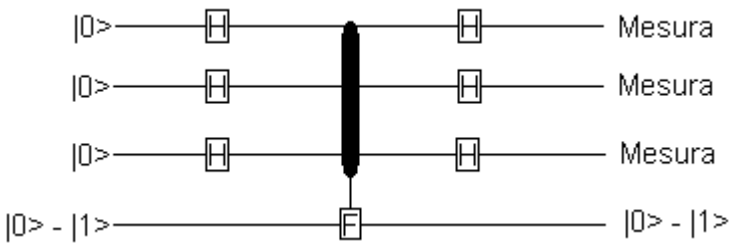


Algorisme quàntic representat amb portes [e27]

L'estat inicial dels qubit a les xarxes quàntiques és $|0\rangle\ (|0\rangle - |1\rangle)$ després de la primera transformació de la porta *Hadamard* l'estat dels dos qubit tenen la forma $(|0\rangle + |1\rangle), (|0\rangle - |1\rangle)$. Això, determina l'efecte de l'avaluació de la funció en aquest estat. Recordar primer que per cada $x \in \{0, 1\}$, $|x\rangle\ (|0\rangle - |1\rangle)\ f \rightarrow (-1)^{f(x)}\ |x\rangle\ (|0\rangle - |1\rangle)$
Per tan, l'estat després de l'avaluació de la funció és:

$$[(-1)^{f(0)}\ |0\rangle + (-1)^{f(1)}\ |1\rangle]\ (|0\rangle - |1\rangle)$$

Per a cada x, el terme $|x\rangle$ adquireix un factor de fase $(-1)^{f(x)}$, que correspon a l'autovalor de l'estat del qubit auxiliar sota l'acció de l'operador que envia $|y\rangle$ de $|y + f(x)\rangle$. El segon qubit no és d'interès per nosaltres, però l'estat del primer qubit: $(-1)^{f(0)}\ |0\rangle + (-1)^{f(1)}\ |1\rangle$ és igual ja sigui per $\pm\ (|0\rangle + |1\rangle)$ quan $f(0) = f(1)$ o $\pm\ (|0\rangle - |1\rangle)$ quan $f(0) \neq f(1)$. Llavors, desprès d'aplicar la segona porta *Hadamard* l'estat del primer qubit es converteix $|0\rangle$ si f és constant i $|1\rangle$ si és balancejada. El mesurament del valor del bit en aquest qubit distingeix aquests casos amb certesa.
Aquest exemple és una versió millorada del primer algorisme quàntic proposat per Deutsch [228] (que donava una probabilitat de certesa en la resposta del *50%*). El resultat de Deutsch [228] va posar les bases per el nou camp de la computació quàntica, i va ser seguit per a altres algorismes quàntics. El problema original de Deutsch [228] va ser posteriorment generalitzat per tal de cobrir la computació de funcions booleanes $f: \{0, 1\}^n \rightarrow \{0, 1\}$. Assumint això per a una o més funcions d'aquestes, ens assegura que és constant o balancejada (té el mateix nombre de sortides *0* que *1*), i l'objectiu està determinat per dues propietats que la funció actual té. Quantes consultes a f han calgut per això? Qualsevol algorisme clàssic, per aquest problema necessitaria, en el pitjor dels casos, $2^{n-1} + 1$ consultes per tal de determinar la resposta de forma segura. Amb l'algorisme quàntic resolem el problema amb una sola consulta a f.
Il·lustrem aquest algorisme de forma gràfica:

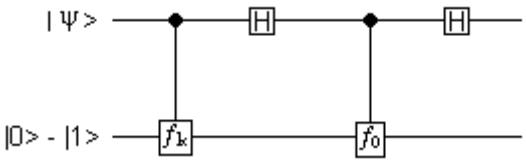


Algorisme de Deutsch millorat amb portes quàntiques [e28]

El registre de control, ara integrat en n qubit ($n = 3$ en el diagrama) està inicialitzat en l'estat $|00...0>$ i un qubit auxiliar en el segon registre s'inicialitza i es manté en l'estat $|0> - |1>$. Pas a pas a través de l'execució de la xarxa, l'estat després de la transformació de la porta *Hadamard* del primer qubit un cop aplicat és: $\Sigma_x\ |x>\ (|0> - |1>)$, i després d'avaluar la funció: $\Sigma_x\ (-1)^{f(x)}\ |X>\ (|0> - |1>)$. Finalment, després de l'última transformació de la porta *Hadamard*, l'estat és: $\Sigma_{x,y}\ (-1)^{f(x) + (x*y)}\ |y>\ (|0> - |1>)$.
L'amplitud de $|00...0>$ és $\Sigma_x \frac{(-1)^{f(x)}}{2^n}$ que és $(-1)^{f(0)}$ quan f és constant i 0 quan f és balancejada. Per tan, mitjançant el mesurament dels primers n qubit, podem determinar amb seguretat si f és constant o balancejada. L'algorisme segueix el mateix patró que l'algorisme de Deutsch *[228]*: la transformació de la porta *Hadamard*, la funció d'avaluació, i l'altre transformació de la porta *Hadamard* (la seqüència *H-F-H*). Reconeixem que es tracta d'un patró de interferència genèric.

16.6 Cerca quàntica

La seqüència genèrica *H-f-H* es pot repetir vàries vegades. Això bé il·lustrat per exemple, amb la base de dades de Grover [229] de recerca d'algorismes. Suposem que se'ns dona , com un oracle, una funció booleana f_k que amb domini $[0, 1\}^n$ a $\{0, 1\}$ de tal manera que $f_k(x) = \delta_{xk}$ per algunes k. Tenim de trobar k. Per tan, en un conjunt de números de 0 a $2^n - 1$ un element ha estat "*etiquetat*" avaluar f_k i el tenim de trobar. Amb la finalitat de trobar-lo amb probabilitat del 50% un algorisme clàssic, sigui determinista o probabilístic, necessita avaluar f_k un mínim de vegades 2^{n-1}. Contràriament un algorisme clàssic necessita nomes $O(2^{n/2})$ avaluacions. A diferència dels algorismes estudiats fins aquest moment, l'algorisme de Grover [229] consisteix a repetir aplicacions de la mateixa transformació unitària $(O(2^{n/2}))$ vegades. L'estat inicial es tria per ser el que té la mateixa superposició amb cada un dels estats de la base de càlcul: $|S> = 2^{-n/2} \sum_{i=0}^{2^n} |i>$. L'operació aplicada a cada iteració individual, referida com iteració de Grover *[229]*, pot ser representada millor amb la següent xarxa:

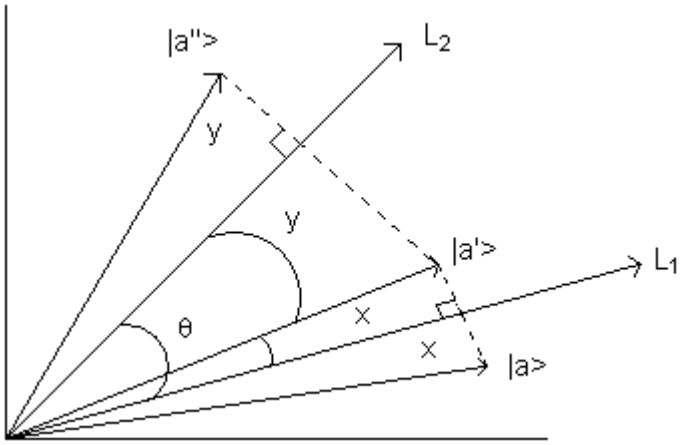


Algorisme de Grover amb portes quàntiques [e29]

Els components de la xarxa ens resulten familiars: transformació *Hadamard* i portes *control – F*. És important notar que en el dibuix de la xarxa hem usat notació taquigràfica: el primer registre (amb entrada $|\psi>$) consta ara de n qubit. La transformació *Hadamard* s'aplica a cada un d'aquests qubit i les portes *control – f* actuen en tots de forma simultània. També l'entrada del segon registre és sempre $|0>$ - $|1>$ però l'entrada del primer registre, denotada com $|\psi>$ canvia d'iteració en iteració, a mesura que el càlcul avança. Com de costum, el segon registre l'ignorem, doncs es manté constant en el transcurs de la computació. Per començar, considerem nomes la porta controlada - f_x. En particular, la transformació no fa res per a qualsevol dels elements de la base excepte per $|k>$ que transforma a - $|k>$. Geomètricament, és un simple reflex al hiper pla perpendicular a $|k>$ així que l'anomenem R_k. De forma similar, en respecta nomes al primer registre, la operació amb la control - f_0 envia $|0>$ en - $|0>$ i fixa tots els altres elements de la base, per lo que es pot escriure R_0. Ara considerem la seqüència d'operacions HR_0H. Com $H^2 = I$, podem reescriure la terna com HR_0H^{-1} que és simplement R_0 interpretat o escrit en una base diferent. Més concretament, és la reflexió sobre la perpendicular a d'hiperplà:

$$H\,|0> = \frac{1}{2^{\frac{n}{2}}} \sum_{x=0}^{2^n-1} |x> = |S>$$

Per lo qual simplement escrivim la triple com R_s.
Podem reescriure la iteració de Grover [229] en la forma simple com $G = R_s\, R_k$. Ara, ja que cada reflexió és una transformació ortogonal amb determinant unitat, en altres paraules, una rotació. Per trobar la resposta n'hi ha prou amb considerar les rotacions en el pla definit per $|k>$ i $|S>$ ja que tots els altres vectors s'han fixat amb la iteració de Grover *[229]*. La situació geomètrica genèrica s'il·lustra en el diagrama següent:



Representació geomètrica de les iteracions del algorisme de Grover [e30]

Si el vector $|a>$ és reflexa a través de la línia L_1 això genera el vector $|a'>$ i aquest es reflecteix per segona vagada a través de la línia L_2 i genera el vector $|a''>$, així, l'efecte net és una rotació per l'angle total subtendit entre $|a>$ *i* $|a''>$, que és $2x + 2y = 2(x + y) = 2\theta$. Per tan, escrivim $|k^{\perp}>$ i $|S^{\perp}>$. Posem $sin\theta = \frac{1}{2^{n/2}}$, això és fàcil de veure que es tracta d'una rotació:

$$2\left(3\frac{\pi}{2} - \emptyset\right) = \pi - 2\emptyset \; mod \; 2\pi$$

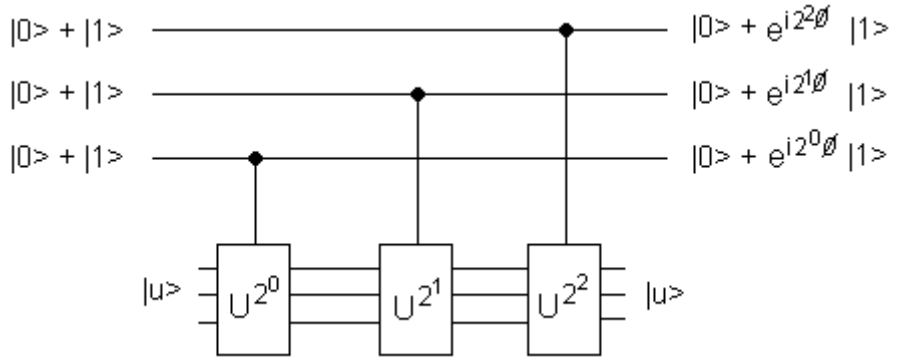
Per tan, fins a les fases, la iteració de Grover [229] provoca una rotació del vector amb un angle de $2\varnothing$ cap a la solució desitjada $|k>$. Normalment, l'estat inicial del primer registre es tria per $|S>$. Ja que l'estat inicial de $|S>$ ja es troba en un angle $\varnothing$ respecta $|k>$, la iteració es té de repetir m vegades, on:

$$(2m+1)\,\varnothing \approx \pi/2, \quad \text{amb resultat} \quad m \approx \pi/4\varnothing - 1/4$$

Per tal d'obtenir una probabilitat d'èxit limitada inferiorment $cos^2\,(2\varnothing)$, que tendeix a 1 quan $n \rightarrow \infty$. Per a una n gran $\frac{1}{2^{n/2}} = \sin\emptyset$, per tan $m \approx \frac{\pi}{4}\frac{1}{2^{n/2}}$.
Aquest és un resultat sorprenent: qualsevol cerca en una base de dades no estructurada es pot realitzar en un temps proporcional a l'arrel quadrada del número d'entrades de la base de dades. El treball posterior va ampliar el resultat de la cerca de varis elements, la cerca a bases de dades estructurades i moltes altres situacions. També, Zalka [230], Boyer [231] i d'altres, van demostrar que l'algorisme de Grover [229] és òptim, en el sentit de que cap altre algorisme quàntic per a cerca a una base de dades desestructurada consumeix un temps per sota de $O(2^{n/2})$.

16.7 Estimació òptima de la fase

Els models de consulta de computació quàntica proporcionen una configuració natural de productes per el descobriment posterior d'algorismes quàntics. L'exemple més notable és l'algorisme de factorització quàntic *Shor* [225] que va evolucionar amb la finalitat de resoldre el problema que es va formular originalment en el llenguatge de les consultes quàntiques. En base al nostre enfocament d'interferometria descriurem aquest algorisme en termes d'interferometria multi partícula quàntica.
Suposem que U és qualsevol transformació unitària de un qubit i $|u>$ és un autovector de U amb valor propi $e^{i\varnothing}$ i considerem el següent escenari: nosaltres no coneixem explícitament U o ,$|u>$ o $e^{i\varnothing}$, però en el seu lloc se'ns faciliten els dispositius que realitzen les funcions de les portes control – U, control - u^{2^1}, control - U^{2^2} i així successivament fins arribar a control - $U^{2^{n-1}}$. També, assumim que disposem d'una preparació simple del estat $|u>$. El nostre objectiu és el d'obtenir una estimació de n - bit de $\varnothing$. Comencem construint la següent xarxa:



Funcions amb portes de control U [e31]

El segon registre de m qubit esta preparat inicialment en l'estat $|u>$ i segueix en aquest estat després del còmput, mentre que el primer registre amb n qubit evoluciona cap el estat:

$$(|0> + e^{i\emptyset 2^{n-1}}|1>)\left(|0> + e^{i\emptyset 2^{n-2}}|1>\right)\ldots\left(|0> + e^{i\emptyset}|1>\right) = \sum_{y=0}^{2^n-1} e^{2\pi i\frac{\emptyset y}{2^n}}|y> \quad [e1]$$

Considerem el cas especial $\varnothing = 2\pi x/2^n$ per a $x = \sum_{i=0}^{n-1} 2^i xi$, i recordem la transformada quàntica de *Fourier (QFT)* *[219]*. L'estat que queda amb representació binària de x a saber, $|x_{n-1}\ldots x_0>$ (per tan, $\varnothing$) es pot obtenir aplicant la *QFT* [219] mitjançant l'execució de la xarxa per la *QFT* [219] en direcció inversa. Si x és un nombre de n – bit això ens donarà el valor exacta de $\varnothing$. No obstant, $\varnothing$ no té perquè ser una fracció de una potència de 2 (ni tan sols té perquè ser un número racional). Per aquest tipus de $\varnothing$ resulta que l'aplicació de la *QFT* [219] inversa la millor n – bit aproximació de $\varnothing$ amb probabilitat per lo menys de $4/\pi^2 \approx 0.405$.

Per veure el perquè això és així, escriurem $\varnothing = 2\pi(a/2^n + \delta)$, on $a=(a_{n-1}...a_0)$ en la millor n – bit estimació de $\varnothing/2\pi$ i $0 < |\delta| \leq 1/2^{n+1}$. Aplicant la QFT [219] inversa la equació que hem vist a dalt *[e1]* evoluciona al següent estat:

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^{n-1}} e^{\frac{2\pi i}{2^n}(a-x)^y} \; e^{2\pi i\delta y} \, |x>$$

i el coeficient davant $|x = a>$ és la sèrie geomètrica:

$$\frac{1}{2^n} \sum_{y=0}^{2^n-1} \left(e^{2\pi i\delta}\right)^y = \frac{1}{2^n}\left(\frac{1-\left(e^{2\pi i\delta}\right)^{2^n}}{1-e^{2\pi i\delta}}\right)$$

Des de $|\delta| \leq 1/2^{n+1}$, es dedueix que $2^n\,|\delta| \leq ½$, i fen ús de la desigualtat $2z \leq \sin \pi z \leq \pi z$ tenint que $z \in [0, ½]$, obtenim $\left|1 - e^{2\pi i\delta 2^n}\right| = 2|\sin(\pi\delta 2^n)| \geq 4|\delta|2^n$. També, $\left|1 - e^{2\pi i\delta}\right| = 2|\sin \pi\delta| \leq 2\pi\delta$. Per tan, la probabilitat d'observar $a_{n-1}...a_0$ a l'hora de mesurar l'estat és:

$$\left|\frac{1}{2^n}\left(\frac{1-\left(e^{2\pi i\delta}\right)^{2^n}}{1-e^{2\pi i\delta}}\right)\right|^2 \geq \left(\frac{1}{2^n}\left(\frac{4\delta 2^n}{2\pi\delta}\right)\right)^2 = \frac{4}{\pi^2}$$

el que prova la nostra afirmació. De fet, la probabilitat d'obtenir la millor estimació es pot expressar amb $1 - \delta$ per a qualsevol $0 < \delta < 1$, a l'estat en el qual evoluciona la eq1uació *[e1]* però amb $n + O(\log(1/\delta))$ qubit.

16.8 Periodicitat i factorització quàntica

Sorprenentment l'aplicació de l'estimació de la fase òptima per a un operador unitari molt particular, ens permetrà factoritzar números enters de forma molt eficient. De fet, ens permet resoldre una classe més general de problemes relacionats amb la periodicitat per a certes funcions amb enters.
Sigui N un nombre enter de m – bits i a un enter més petit que N i coprimer de N. Definim un operador unitari que actuï en m qubit tal que per a tot $y < N$

$$|y> \rightarrow U_a \; |y> = |ay \bmod N>$$

Aquesta operació unitària la podem anomenar multiplicació de *a mòdul N*. Això significa que existeix estrictament al menys un r positiu de tal manera que $a^r = 1 \bmod N$. Aquesta r s'anomena de ordre de *a mòdul N*. De forma equivalen r és el període de la funció $f(x) = a^x \bmod N$, per exemple, $r > 0$ de tal forma que $f(x) = f(x + r)$ per a totes les x. Ara anem als vectors $|u_k>$ $(k \in \{1,...,r\})$ definits per $|u_k> = r^{-1/2} \sum_{j=0}^{r-1} e - \frac{2\pi ikj}{r} \, |a^j \bmod N>$ $k \in \{1,...,r\}$, $|u_k>$ és un autovector amb autovalor $e^{2\pi i\frac{k}{r}}$ de l'operador de la

multiplicació modular U_a anteriorment definida. És important observar que es pot construir de forma eficient una xarxa quàntica per a la multiplicació modular controlada de un número N. Per altre banda, per qualsevol j, és possible la implementació eficient d'una porta control - U_a^{2j}. Per tan, podem aplicar tècniques per l'estimació òptima de la fase. Per qualsevol $k \in \{1,...,r\}$, donat un estat $|u_k>$ podem obtenir la millor aproximació de n – bit per a k/r. Això equival a determinar per sí mateix r. Malauradament això és una complicació.

La nostra feina és: prenem un número N de longitud m – bit i escollim de forma aleatòria un $a < N$ coprimer (primers entre sí) de N i cerquem l'ordre a mòdul N. El problema amb aquest mètode és que som conscients que no coneixem un forma senzilla i eficient per preparar qualsevol dels estats $|u_k>$. No obstant $|1> = r^{1/2} \sum_{k=1}^{r} |u^k>$ és un estat fàcil de preparar.

Si comencem amb $|1>$ en lloc del autovector $|u_k>$, aplicant la xarxa d'estimació de fase i mesurant el primer registre bit a bit podem obtenir n dígits binaris de x de tal manera que amb una probabilitat per sobre de $\frac{4}{\pi^2}$, $\frac{x}{2^n}$ és la millor estimació de n – bit de k/r per k entre $\{0, ..., r\}$ triat aleatòriament. La pregunta ara és: donada x, com calculem r? Anem a fer algunes observacions:

· Donada una x, k/r és única.

El valor de $\frac{x}{2^n}$ sen una estimació de n – bit, no defineix amb més de $\frac{1}{2^n}$ k/r. Per tant, sempre que $n > 2m$, l'estimació de n – bit de x determina un valor únic de k/r ja que r és un número de m – bit.

· Els valors candidats per k/r són tots convergents a $\frac{x}{2^m}$.

Per a qualsevol número real θ, hi ha una seqüència única de racionals especials $\frac{p_n}{q_n}$ $n \in N$ $(mcd\ (p_n, q_n) = 1)$ anomenats convergents a θ que tendeixen a 0 quan n creix. El teorema dels estats estableix que si p i q són enters que $\left|\theta - \frac{p}{q}\right| < \frac{1}{2q^2}$ llavors p/q convergeix a θ. Des de que tenim que $\frac{1}{2^n} \leq \frac{1}{2(2^m)^2} \leq \frac{1}{2r^2}$, això implica que $\frac{x}{2^n} - \frac{k}{r} < \frac{1}{2r^2}$ i $k/2$ convergeix a $x/2^n$.

· Nomes es pot triar una convergència.

És fàcil demostrar que hi ha més d'una fracció a/b que satisfà tan $b \leq r$ com $\left|\frac{x}{2^n} - \frac{a}{b}\right| < \frac{1}{2r^2}$.

Les convergència es poden trobar de manera eficient usant el conegut mètode de les fraccions continues. Per tan, usem les fraccions continues i les nostres observacions a fi de trobar una fracció a/b de tal manera que $b \leq 2^m$ i $\left|\frac{x}{2^n} - \frac{a}{b}\right| < \frac{1}{2^n}$. Obtenim el número racional k/r, i $k = a$, $r = b$, amb k i r coprimers. Escollint k al atzar, això passa amb una probabilitat $\geq 1/ln(r)$. Finalment, demostrem com l'ordre descobert pot ser usat per factoritzar un número compost N. Sigui a un enter positiu petit de N triat al atzar tal que $mcd(a, N) = 1$. Llavors l'ordre de a *mòdul* N esta definit i el podem trobar de manera eficient amb l'anterior algorisme. Si r és parell, llavors tenim que:

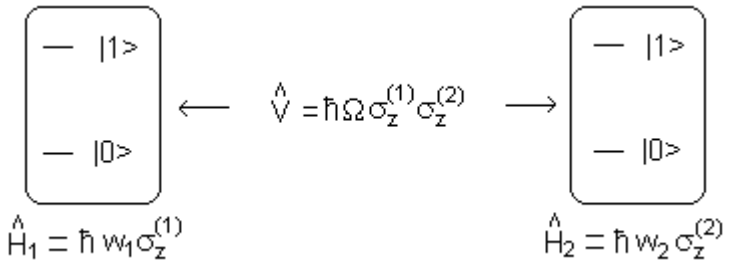
$A^r = 1 \bmod N \Leftrightarrow (a^{r/2})^2 - 1^2 = 0 \bmod N \Leftrightarrow (a^{r/2} - 1)\ (a^{r/2} + 1) = 0 \bmod N.$

El producte $(a^{r/2} -1)(a^{r/2} +1)$ té de ser un múltiple de N, i el menys $a^{r/2} = \pm 1 \bmod N$ té de complir la condició mínima de tenir un factor no trivial en comú amb N. Calculant el *mcd* d'aquest terme i N, s'obté un factor no trivial de N.
Per altre banda, si N és senar amb factors primers: $N = P_1^{\alpha_1} P_2^{\alpha_2} \dots P_s^{\alpha_s}$, llavors es pot demostrar que si $a < N$ que es tria a l'atzar de tal manera que $mcd\ (a, N) = 1$ llavors la probabilitat de que l'ordre del mòdul N sigui uniforme i que $a^{r/2} \neq \pm 1 \bmod N$ és: P_r (r és uniforme i $a^{r/2} \neq \pm 1 \bmod N$) $\geq 1 - \frac{1}{2^{s-1}}$.
Així, la combinació de les nostres estimacions d'èxit a cada pas, amb probabilitat igual o major a: $\frac{4}{\pi^2} \frac{1}{Ln(r)} \left(1 - \frac{1}{2^{s-1}}\right) \geq \frac{2}{\pi^2} \frac{1}{Ln(N)}$ la trobem en un factor de N^4 (amb N compost i $r < N$). Si N és $Log(N) = n$ bits de longitud, mitjançant la repetició de tot el procés amb temps $O(n)$ o per $O(n)$ computacions en paral·lel, per una extensió adequada d'una xarxa de factorització quàntica, es pot garantir que trobarem un factor de N amb una probabilitat fixada superior a ½. Això i el fet que la família de xarxa quàntica per el control del producte modular d'alguns números és uniforme i de mida $O(n^2)$, ens diu que la factorització esta inclosa dintre la classe de complexitat *BQP*(error delimitat probabilístic polinòmic).

16.9 La dinàmica quàntica condicional

Les portes quàntiques i les xarxes quàntiques proporcionen un llenguatge molt convenient per construir qualsevol computador quàntic o (que és bàsicament el mateix) interferòmetre quàntics. Però, podem construir portes lògiques quàntiques? Les portes quàntiques d'un simple qubit són considerades relativament fàcils d'implementar. Per exemple, un construcció típica en òptica quàntica usa àtoms com a qubit i controla els seus estats amb polsos de llum làser de una selecció curosa de freqüència, intensitat i durada. Qualsevol superposició prescrita de dos estats atòmics seleccionats es poden preparar d'aquesta manera. Les portes de *2* qubit són molt més difícils de construir.
Amb la finalitat d'implementar portes lògiques quàntiques de *2* qubit és suficient, des del punt de vista experimental , per induir una dinàmica condicional de bits físics, és a dir, per a realitzar una transformació unitària en un subsistema físic al estat quàntic d'un altre subsistema,
$U = |0\rangle\langle 0| \otimes U_0 + |1\rangle\langle 1| \otimes U_1 + \dots + |k\rangle\langle k| \otimes U_k$,
On els projectors es refereixen a estats quàntics del subsistema de control i les operacions unitàries U_i es realitzen en el subsistema objectiu. L'operació més simple no trivial d'aquesta classe és, probablement, un canvi de fase condicional, com $B(\varnothing)$ que hem usat en implementar la QFT [219] i amb la porta quàntica *control – NOT (o XOR)*.

Anem a il·lustrar el concepte de la dinàmica quàntica condicional amb un exemple simple. Considerem 2 qubit, per exemple 2 spins, àtoms, un electró, que s'ajunten via $\sigma_z^{(1)}\ \sigma_z^{(2)}$ interacció (per exemple una interacció dipol – dipol):



Exemple de dinàmica quàntica condicional [e32]

El primer qubit amb freqüència de ressonància w_1, actua de qubit de control i el segon, amb freqüència de ressonància w_2, és el qubit objectiu. Degut al acoblament $\hat{V}$ la freqüència de ressonància de la transició entre l'estat $|0\rangle$ *i* $|1\rangle$ d'un qubit depèn de l'estat del "*vei*". La freqüència de ressonància per el primer qubit es converteix amb $w_1 \pm \Omega$ depenent de si el segon qubit està en l'estat $|0\rangle$ o $|1\rangle$. De forma similar, la freqüència de ressonància del segon qubit es converteix en $w_2 \pm \Omega$, depenent de l'estat del primer qubit. Per tant, a π polsos a freqüència $w_2 + \Omega$ provoca la transició $|0\rangle \leftrightarrow |1\rangle$ en el segon qubit nomes si el primer qubit és a l'estat $|1\rangle$. D'aquesta manera podem implementar la porta quàntica *control – NOT*.

16.10 Decoherència i recoherència

En principi, sabem com construir un computador quàntic. Podem començar amb simples portes lògiques quàntiques i intentar integrar-les amb xarxes quàntiques. No obstant, si continuem posant portes dintre la xarxa, de seguida ens trobarem amb problemes greus. La interacció dels qubit involucrats pot mostrar interferències quàntiques no desitjades. A més de les dificultats tècniques de treballar a escala de simple àtom i simple fotó, un altre dels problemes més importants és el de prevenir de l'entorn el còmput dintre l' interferòmetre multi partícula.
Considerem la següent interacció qubit - entorn:
$|0, m\rangle \rightarrow |0, m_0\rangle$, $|1, m\rangle \rightarrow 1, m_1\rangle$,
On $|m\rangle$ és l'estat inicial i $|m_0\rangle$, $m_1\rangle$ són els estats finals de l'entorn. Aquesta és bàsicament la mesura presa per l'entorn d'un qubit. Suposem que en el nostre experiment de interferència de qubit simple, el qubit entre dues transformacions per porta *Hadamard* és "*vist*" per l'entorn com un "*aprenentatge*" de si el qubit està en estat

$|0>$, o $|1>$. L'evolució del qubit i l'entorn després de la primera porta *Hadamard* i de la porta de *fase* es descriu amb la següent transformació:

$$|0>|m> \xrightarrow{H} \frac{1}{\sqrt{2}}(|0> +|1>)|m> \xrightarrow{\varnothing} \frac{1}{\sqrt{2}}(e^{\frac{i\emptyset}{2}}|0> + e^{\frac{-i\emptyset}{2}}|1>)\,|m>$$

Podem escriure l'acció de la decoherència com:

$$\frac{1}{\sqrt{2}}(e^{\frac{i\emptyset}{2}}|0> + e^{\frac{-i\emptyset}{2}}|1>)\,|m> \rightarrow \frac{1}{\sqrt{2}}(e^{\frac{i\emptyset}{2}}|0>|m_0 + e^{\frac{-i\emptyset}{2}}|1>|m_1>)$$

La porta *Hadamard* final genera l'estat de sortida:

$$\frac{1}{\sqrt{2}}(e^{\frac{i\emptyset}{2}}|0>|m_0 + e^{\frac{-i\emptyset}{2}}|1>|m_1>) \xrightarrow{H} \frac{1}{2}|0>(e^{\frac{i\emptyset}{2}}|m_0> + e^{\frac{-i\emptyset}{2}}|m_1>) + \frac{1}{2}|1>(e^{\frac{i\emptyset}{2}}|m_0> - e^{\frac{-i\emptyset}{2}}|m_1>)$$

Tenint $|m_0>$ i $|m_1>$ normalitzats i $<m_0|\ m_1>$ real obtenim les probabilitats P_0 i P_1:

$$P_0 = \frac{1}{2}(1+< m_0|m_1 > cos\emptyset), \qquad P_1 = \frac{1}{2}(1-< m_0|m_1 > cos\emptyset)$$

És instructiu veure l'efecte de la decoherència en el qubit només quan el seu estat és escrit en termes d'operador de densitat. La decoherència de interacció de qubit enredats amb l'entorn és: $(\alpha\,|0> + \beta\,|1>)\,|m> \rightarrow \alpha\,|0>\,m_0> + \beta\,|1>\,|m_1>$

Reescrivint els operadors en termes de densitat i rastrejant l'entorn del *espai de Hilbert* [232] en ambdós costats, obtenim:

$$\begin{pmatrix} |\alpha|^2 & \alpha\beta^* \\ \alpha^*\beta & |\beta|^2 \end{pmatrix} \rightarrow \begin{pmatrix} |\alpha|^2 & \alpha\beta^* < m_0|m_1 > \\ \alpha^*\beta < m_1|m_0 > & |\beta|^2 \end{pmatrix}$$

Els elements de "*fora de la diagonal*", originalment anomenat per els físics de coherències atòmiques, desapareixen com $<m_1|m_0> \rightarrow 0$, i és per això que aquesta interacció particular amb l'entorn s'anomena decoherència.

Com afecten els efectes de la decoherència, per exemple, al algorisme de *Deutsch*[228]? Substituint 0 o π per $\varnothing$ en la primera equació obtenim la resposta correcta només amb certa probabilitat que és: $\frac{1+<m_0|m_1>}{2}$.

Si $<m_0|m_1> = 0$, cas de perfecta decoherència, les sortides de la xarxa (0 ó 1) tenen les mateixes probabilitats, és a dir, és inútil com a dispositiu de computació. Està clar que volem evitar la decoherència o per lo menys disminuir el seu impacte en el nostre dispositiu de computació. En general, quan analitzem computacions físicament realitzables tenim que considerar errors causats per la interacció del computador amb l'entorn i des del punt de la complexitat computacional, és necessari avaluar l'escala d'aquests errors amb la mida de l'entrada. Si la probabilitat d'un error en una proba única, δ(n), creix exponencialment amb n, és a dir, si $\delta(n) = 1 - A\,exp(-\alpha n)$, on A i α són constants positives, llavors l'algorisme aleatori tècnicament és pot considerar que no és

eficient independentment de lo dèbil que la interacció amb l'entorn pugui ser. Per desgràcia, la interacció del computador amb l'entorn només condueix a un augment exponencial no desitjable de la tassa d'error amb la mida de l'entrada. Per a veure això, considerem un registre de mida n i assumim que cada qubit té decoherència per separat:
$|x\rangle\ |M\rangle = |x_{n-1},...x_1x_0\rangle\ |m\rangle...|m\rangle|m\rangle \rightarrow |x_{n-1},...x_1x_0\rangle\ |m_{x1>|m}x2\rangle = |x\rangle\ |M_x\rangle$, *on* $x_i \in \{0, 1\}$. A continuació la superposició $\alpha\ |x\rangle + \beta\ |y\rangle$ cobreix:

$(\alpha\ |x\rangle + \beta\ |y\rangle)\ |M\rangle \rightarrow \alpha\ |x\rangle\ |M_x\rangle + \beta\ |y\rangle\ |M_y\rangle$,

Però ara, el producte escalar $\langle M_x|M_y\rangle$ que redueix els elements de "*fora la diagonal*" de l'operador de densitat del registre general i que els efectes de probabilitats del experiment d'interferència bé donat per:
$\langle M_x|M_y\rangle = \langle m_{x0}|m_{y1}\rangle \langle m_{x1}|m_{y2}\rangle ... \langle m_{xn-1}|m_{yn-1}\rangle$

que és de l'ordre de $\langle M_x|M_y\rangle = \langle m_0|m_1\rangle^{H(x,y)}$ on $H(x,y)$ és la distància de *Hamming* entre x i y, és a dir, el número de llocs binaris en que x i y difereixen (exemple: la distància de *Hamming* entre *101101* i *111101* és *1* perquè els dos *strings* binaris són diferents només en el bit de la segona posició). Per tan, hi ha algunes coherències que desapareixen com $\langle m_0|m_1\rangle^n$ i per tant, en alguns experiments de interferència la probabilitat d'error pot créixer exponencialment amb n.
Està clar que per la computació quàntica de qualsevol longitud raonable, en ser físicament possible es fa necessari incorporar algun esquema d'estabilització eficient i possible per combatre els efectes de la decoherència. Deutsch [228] va ser el primer en discutir aquest problema. El 1993 va proposar la recoherència basada en un procediment de simetrització. La idea bàsica l'expliquem a continuació. Suposem que disposem d'un sistema quàntic i el preparem en el seu estat inicial $|\Psi_i\rangle$ i volem posar-lo en pràctica amb una evolució unitària prescrita $|\Psi(t)\rangle$ o simplement mantenir $|\Psi_i\rangle$ per algun període de temps t. Ara suposem que en lloc d'un sistema simple podem preparar R còpies de $|\Psi_i\rangle$ i posteriorment podem projectar l'estat del sistema combinant en el interior d'un subespai simètric, és a dir, un subespai que conté tots els estats que són invariants sota qualsevol permutació dels subsistemes. La finalitat és que les projeccions freqüents en el subespai simètric reduiran els errors induïts per el entorn.
La intuïció darrere aquest concepte esta basada amb l'observació que en la prescripció d'emmagatzemen lliure d'errors o evolució de les R còpies independents comença en el subespai simètric i té que mantenir-se contingut en aquest subespai. Per tant, el component lliure d'errors en qualsevol estat sempre es proba en el subespai simètric, en la projecció que ha tingut èxit i que per tant, no es modificarà, i part de l'error s'eliminarà. Hem de tenir en compte no obstant, que l'estat de projecció generalment, no esta lliure d'errors i des del subespai simètric conté els estats que no són de simple producte de $|\Psi\rangle|\Psi\rangle...|\Psi\rangle$. S'ha demostrat però que la probabilitat d'error es reduirà en un factor de $1/R$. Més recents projeccions en el subespai simètric es substituiran per a projeccions més complexes en una selecció curosa de subespais. Aquestes projeccions

proposades per Shor, Calderbank, Steane [233] i d'altres estan construïdes sobre la base dels mètodes clàssics de correcció d'errors però representen intrínsecament una nova correcció quàntica i esquemes d'estabilització que són objecta d'estudi.
Anem a il·lustrar la idea principal de recoherència descrivint un mètode simple per protegir un estat desconegut d'un simple qubit en registre quàntic pertorbat. Considerem el següent escenari: emmagatzemem a la memòria d'un computador un qubit en un estat quàntic desconegut amb forma $|\varnothing = \alpha\ |0> + \beta\ |1>$ i sabem que qualsevol simple qubit que s'emmagatzema en un registre es sotmet a decoherència del tipus d'entrellaçament amb l'entorn com ja s'ha descrit anteriorment. Es pot veure com l'estat del qubit esta afectat pel entorn. Calculem la fidelitat del estat de decoherència en el temps t respecta l'estat inicial $|\varnothing>$: $F(t) = <\varnothing|\ p(t)\ |\varnothing>$. Es dedueix que:

$$F(t) = |\alpha|^4 + |\beta|^4 + 2|\alpha|^2\ |\beta|^2\ Re[<m_0(t)|m_1(t)>].$$

L'expressió depèn de l'estat inicial $|\varnothing>$ i clarament indica que alguns estats són més vulnerables a la decoherència que d'altres.
Amb la finalitat d'obtenir o eliminar la dependència considerem la fidelitat promig calculada sota l'assumpció de que qualsevol estat inicial $|\varnothing>$ és igualment probable. Tenint en compte la restricció de la normalització la fidelitat promig bé donada per:

$$\bar{F}(t) = \int_0^1 F(t)d|\alpha|^2 = \frac{1}{3}(2 + Re[< m_0(t)|m_1(t) >].$$

Si assumim un tipus exponencial de decoherència, on $<m_0(t)|m_1(t)>= e^{-\gamma t}$, la fidelitat promig pren la següent forma: $\bar{F}(t) = \frac{1}{3}(2 + e^{-\gamma t})$. En particular, per a temps més curs que el temps de decoherència $t_d = 1/\gamma$, la fidelitat pot aproximar-se per sobre de:

$$\bar{F}(t) \cong 1 - \frac{1}{3}\gamma t + O(\gamma^2 t^2).$$

Ara mostrarem la forma de millorar la fidelitat promig mitjançant la codificació quàntica. Abans de col·locar el qubit en el registre de memòria el codificarem: podem afegir dos qubit inicialment tant en l'estat $|0>$ com en el original i realitzar una transformació unitària codificada:

$$|000> \rightarrow |\bar{0}\bar{0}\bar{0}> = (|0> + |1>)\ (|0> + |1>)\ (|0> + |1>),$$
$$|100> \rightarrow |\bar{1}\bar{1}\bar{1}> = (|0> - |1>)\ (|0> - |1>)\ (|0> - |1>),$$

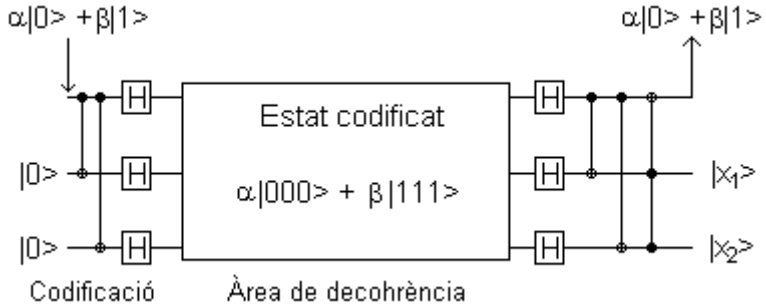
Generem l'estat $\alpha\ |\ \bar{0}\bar{0}\bar{0}\ > + \beta\ |\ \bar{1}\bar{1}\bar{1}\ >$, *on* $|\bar{0}> = |0> + |1>$ *i* $|\bar{1}> = |0> - |1>$. Hara suposem que nomes el segon qubit guardat esta afectat per la decoherència i etrellaçat en l'entorn i es converteix amb:

$$\alpha(|0> + |1>)\ (|0>\ |m_0> + |1>\ |m_1>)\ (|0> + |1>) + \beta(|0> - |1>)\ (|0>\ |m_0> - |1>\ |m_1>)\ (|0> - |1>),$$

que es pot escriure com:

$(\alpha|\ \bar{0}\bar{0}\bar{0}> + \beta\ |\bar{1}\bar{1}\bar{1}>)\ (|m_0> +\ |m_1>) + (\alpha|\ \bar{0}\bar{0}\bar{0}> + \beta\ |\bar{1}\bar{1}\bar{1}>)\ (|m_0> -\ |m_1>)$.

La transformació unitària codificada es pot construir amb una parella de portes quàntiques *control – NOT* i una porta *Toffoli*, per tal de completar la xarxa de correcció d'error:



Xarxa de correcció d'error [e33]

Una curosa inspecció de la xarxa mostra que qualsevol fase simple $|\bar{0}> \leftrightarrow |\bar{1}>$ queda corregida i l'entorn queda desenredat dels qubit. En el nostre cas particular obtenim:

$(\alpha|0> + \beta\ |1>)\ [|00>(|m_0> +\ |m_1>) +\ |10>\ (|m_0> -\ |m_1>)]$

Les dues sortides auxiliars porten la informació sobre l'estat d'error (*00* significa que no hi ha error, *01* significa que l'eliminació s'ha produit en el tercer bit, i *11* senyals de fase erroni en el tercer bit).
La decoherència és de només *1* qubit en la triple, podem recuperar l'estat original. En realitat, tots tres qubits reflecteixen decoherència de forma simultània i com a resultat només és posible una recuperació parcial. En aquest cas, els càlculs són llargs però és sencill demostrar que la fidelitat promig del estat reconstruit després de l'operació de decodificació per un tipus exponencial de decoherència és:

$\bar{F}_{ec}(t) = \frac{1}{6}[4 + 3e^{-\gamma t} - e^{-3\gamma t}]$.
Per un temps curt, podem escriure:

$\bar{F}_{ec}(t) \cong 1 - \frac{1}{2}\gamma^2 t^2 + O(\gamma^3 t^3)$.

Per tots els temps t, $\bar{F}_{ec}(t) \geq \bar{F}(t)$.

Aquesta és l'essència de la recoherència via codificació i descodificació. Hi ha molt més a dir sobre codis quàntics i, en general, tota aquesta tecnologia que esta en plena recerca i avança dia a dia.

Reflexió final sobre la computació quàntica

Tota aquesta sèrie d'articles que hem vist ens expliquen d'una manera general i resumida una mica de teoria quàntica aplicada a la computació. Això és una aproximació que ens pot donar una idea dels treballs que s'han fet i que segueixen evolucionant dia a dia en aquest terreny. Tota aquesta nomenclatura que hem vist i que està basada amb la notació de la mecànica quàntica moderna, introduïda per Dirac, és abstracta i fen una analogia amb els llenguatges informàtics és d'alt nivell. Però al darrera, en el seu baix nivell, la complexitat augmenta molt més. Per entendre bé i en profunditat el que hem anat llegint en aquests apartats, es necessària una base de coneixements matemàtics i físics molt especialitzats (que jo i probablement molts de nosaltres no tenim). Necessitaríem uns estudis específics per a poder-nos submergir en aquests temes amb comoditat i aconseguir una comprensió absoluta. De tota manera, el propòsit d'aquests apartats en aquesta memòria no és el pedagògic en el sentit formatiu en aquesta especialitat sinó que l'objectiu és simplement el de donar una visió aproximada del tema i sobre tot, de la seva complexitat, així com un testimoniatge de la realitat que envolta l'estudi cap a la computació quàntica, intentant esborrar aquella imatge que en podíem tenir a vegades com una cosa d'aquelles que sen parla molt però que no se sap ben bé que és, en que es basa, com es desenvolupa, etc. Finalment només dir que podem trobar força material que parla sobre aquesta temàtica i publicacions de tot tipus que va surtin. Deixo el següent enllaç que és el lloc de on he tret tota aquesta informació i on podem trobar-ne molta més de tan o més interessant en el cas que tinguem algun interès amb ampliar els coneixements en aquesta temàtica: http://theory.caltech.edu/~preskill/ph229/#prereq

Índex gràfic

[f1]Fotografies ENIAC....8
[f2]Fotografies vàlvules 9
[e1]Vàlvula diode....9
[e2]Rectificador mitja ona 9
[e3]Vàlvula tríode....10
[e4]Amplificador tríode 10
[f3]Fotografia resistències 11
[d1]Dibuix condensador 12
[e5]Unió condensadors 12
[f4]Tipus de condensadors 13
[f5]Computador a transistors 14
[e6]Tipus transistors, polarització, muntatge típic 15
[f6]Diferents tipus de transistors 16
[d2]Cel·la memòria ferrita i cicle d'histèresi del anell 17
[g1]Cicle d'escriptura / lectura de la memòria de ferrita....17
[f7]Detall de memòria de ferrita de 64bits....18
[d3] Dibuix esquemàtic del primer procés foto litogràfic 20
[d4]Esquema del resultat del segon procés foto litogràfic 21
[d5]Difusió de base i emissor....21
[d6]Esquema de difusió d'alumini 21
[d7]Recobriment de capa plàstica 22
[f8]Imatge de diferents tipus de circuits integrats o chips 23
[f9]Detall d'un circuit integrat com és internament 23
[e7] Esquema i taules de les diferents portes lògiques 24
[e8]Esquema circuit amb transistors d'una porta NOR i una NAND....26
[e9]Esquema bàsic d'un microprocessador 29
[d8]Dibuix esquemàtic dels microcomputadors 30
[e10]Esquema del sistema lògic usat per el µc 30
[e11]Circuit sumador complet amb cinc portes i dos bit....25
[e12]Esquema en blocs de sumador de 4 bit de resolució....25
[e13]Sumador amb amplificador operacional....27
[e14]Restador analògic amb amplificador operacional....27
[e15]Amplificador operacional....28
[d9]Incidència del fotó en un mirall semi platejat....54
[d10]Fotó en una trampa de miralls....55
[d11]Fotó en un mirall d'absorció....55
[d12]Registre quàntic....56
[e16]Portes Hadamard i de fase combinades....63
[e17]Porta C – NOT....64
[e18]Porta de canvi de fase controlada....65

[e19]Porta de control U....65
[e20]Porta C – NOT amb 2 c – V i 2 Hadamard....67
[e21]Estructura de la porta de Toffoli....68
[e22]Sumador quàntic....68
[e23]Implementació de la QFT amb una xarxa de portes....70
[e24]Dibuix esquemàtic d'un interferòmetre....73
[e25]Interferència quàntica de partícula simple....74
[e26]Simulador de porta desfasadora....74
[e27]Algorisme quàntic representat amb portes....76
[e28]Algorisme millorat de Deutsch amb portes quàntiques....77
[e29]Algorisme de Grover amb portes quàntiques....78
[e30]Representació geomètrica de les iteracions de l'algorisme de Grover 79
[e31]Funcions amb portes de control U....80
[e32]Exemple de dinàmica quàntica condicional....84
[e33]Xarxa de correcció d'error....88

Fonts

[1]Àbac.....http://es.wikipedia.org/wiki/%C3%81baco
[3]Simulació Pascalina.....http://www.amolasmates.es/flash/pascaline.html
[2]Blaise Pascal..... http://es.wikipedia.org/wiki/Blaise_Pascal
[4]Gottfried Wilhelm Leibniz..... http://es.wikipedia.org/wiki/Gottfried_Leibniz
[5]Joseph Marie Jacquard.....http://es.wikipedia.org/wiki/Joseph_Marie_Jacquard
[6]Màquina diferencial ..... http://es.wikipedia.org/wiki/M%C3%A1quina_diferencial
[7]Màquina analítica.....http://www.neoteo.com/la-maquina-analitica-de-babbage
[8]Colossus.....http://www.dma.eui.upm.es/historia_informatica/Doc/Maquinas/Colossus.htm
[9]ENIAC.....http://www.dma.eui.upm.es/historia_informatica/Doc/Maquinas/ENIAC.htm
[10]Manchester Baby.....http://www.computer50.org/mark1/new.baby.html
[11]Manchester Mark I.....http://www.computer50.org/mark1/MM1.html
[12]Tub Williams.....http://es.wikipedia.org/wiki/Tubo_Williams
[13]EDSAC.....http://www.tecnotopia.com.mx/computadoras/edsac.htm
[14]EDVAC.....http://www.tecnotopia.com.mx/computadoras/edvac.htm
[15]Vàlvula.....http://es.wikipedia.org/wiki/V%C3%A1lvula_termoi%C3%B3nica
[16]Dielèctric..... http://es.wikipedia.org/wiki/Diel%C3%A9ctrico
[17]Corrent C http://centros5.pntic.mec.es/ies.victoria.kent/Rincon-C/pregunta/p-19/p-19.htm
[18]Carga elèctrica..... http://es.wikipedia.org/wiki/Carga_el%C3%A9ctrica
[19]Farad..... http://en.wikipedia.org/wiki/Farad
[20]NPN_PNP..... http://es.wikipedia.org/wiki/Transistor_de_uni%C3%B3n_bipolar
[21]Recta de carga .....
http://www.unicrom.com/Tut_recta_carga_estatica_transistor_bipolar.asp
[22]Bipolar.....http://www.unicrom.com/Tut_transistor_bipolar.asp
[23]MOS.....http://tamarisco.datsi.fi.upm.es/ASIGNATURAS/FFI/apuntes/Tema_6_2_Trans_MOS.pdf
[24]FET..... http://www.electronicafacil.net/tutoriales/TRANSISTOR-FET.php
[25]UJT.....http://www.angelfire.com/electronic2/electronicaanalogica/ujt.html
[26]PUT.....http://www.reocities.com/SiliconValley/Orchard/2753/put/put.html
[27]IGBT.....http://ccpot.galeon.com/enlaces1737117.html
[28]Òxid de ferro.....http://es.wikipedia.org/wiki/%C3%93xidos_de_hierro
[29]Circuit integrat..http://www.terra.es/personal/lermon/cat/articles/evin0086.htm
[30]IBM.....http://es.wikipedia.org/wiki/IBM
[31]IBM360.....http://es.wikipedia.org/wiki/IBM_S/360
[32]PDP-8.....http://es.wikipedia.org/wiki/PDP-8
[33]PDP-11.....http://es.wikipedia.org/wiki/PDP-11
[34]DEC.....http://es.wikipedia.org/wiki/Digital_Equipment_Corporation
[35]Silici.....http://es.wikipedia.org/wiki/Silicio

[36]Ga As.....http://es.wikipedia.org/wiki/Arseniuro_de_galio
[37]Escales integració.....http://www.electronicafacil.net/tutoriales/ESCALAS-INTEGRACION-CIRCUITOS-LOGICOS-SSI-MSI-LSI.php
[38]Intel..... http://www.intel.com/?es_ES_01
[40]Apple..... http://www.apple.com/
[41] Commodore..... http://www.commodore.ca/
[42]MS_DOS.....http://www.hispazone.com/Articulo/97/MS-DOS-(I):-La-historia-del-sistema-operativo.html
[43]RAM.....http://www.monografias.com/trabajos11/memoram/memoram.shtml
[44]ROM..... http://es.wikipedia.org/wiki/Memoria_de_s%C3%B3lo_lectura
[45]CGA..... http://es.wikipedia.org/wiki/Color_Graphics_Adapter
[46]UAL.....http://es.wikipedia.org/wiki/Unidad_aritm%C3%A9tico_l%C3%B3gica
[47]Acumulador..... http://es.wikipedia.org/wiki/Acumulador_(inform%C3%A1tica)
[48]Registres.....http://es.wikipedia.org/wiki/Registro_(hardware)
[49]Registre instrucció...http://es.wikipedia.org/wiki/Registro_de_instrucci%C3%B3n
[50]Descodificador d'instruccions..... http://www.zator.com/Hardware/H3_2.htm
[51]Registres generals.....http://www.monografias.com/trabajos7/regi/regi.shtml
[52]Registre PC..... http://es.wikipedia.org/wiki/Contador_de_programa
[53]Stack Pointer..... http://es.wikipedia.org/wiki/Registro_de_pila
[54]Bus de control..... http://es.wikipedia.org/wiki/Bus_de_control
[55]Bus de dades.....http://es.wikipedia.org/wiki/Bus_de_datos#Clases_de_buses
[56]Bus d'adreces..... http://es.wikipedia.org/wiki/Bus_de_direcciones
[57]Sequent valance.....http://en.wikipedia.org/wiki/Sequent_Computer_Systems
[58] iPSC-1.....http://atc2.aut.uah.es/~acebron/cap6mcomp.pdf
[59]SIM-D..... http://es.wikipedia.org/wiki/SIMD
[60]Connection Machine.....http://en.wikipedia.org/wiki/Connection_Machine
[61]MP-1..... http://nvl.nist.gov/pub/nistpubs/jres/101/2/j2anut.pdf
[62]Xarxa àrea ampla..... http://www.masadelante.com/faqs/lan
[63]Xarxa d'àrea local..... http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local
[64]Marcs principals..... http://es.wikipedia.org/wiki/Computadora_central
[65]Commodore.....http://www.commodorecorp.com/
[66]Rockwell.....http://www.rockwellautomation.com/
[67] Zilog..... http://www.zilog.com/
[68]Micres....http://es.wikipedia.org/wiki/Micr%C3%B3metro_(unidad_de_longitud)
[69]Memòria virtual.....http://es.wikipedia.org/wiki/Memoria_virtual
[70]Non-Linear Systems.....http://www.nonlinearsystems.com/
[71] MS-DOS..... http://es.wikipedia.org/wiki/MS-DOS
[72]Epson Amèrica..... http://pe.linkedin.com/company/epson-america-inc.
[73]Lotus Devolopment Corporation.....
.....http://ecommerce.hostip.info/pages/686/Lotus-Development-Corp.html
[74]Sony..... http://www.sony.com/index.php
[75]Philips..... http://www.philips.es/
[76] DNS..... http://es.wikipedia.org/wiki/Domain_Name_System
[77] C++..... http://es.wikipedia.org/wiki/C%2B%2B

[78] OOP..... http://www.monografias.com/trabajos/objetos/objetos.shtml
[79] UNIX System V..... http://www.unix.org/what_is_unix/history_timeline.html
[80] Apple..... http://www.apple.com/
[81] Motorola.....http://www.motorola.com/staticfiles/Consumers/CLP/ES-ES/index_ES-ES.html
[82] Hewlett – Packard.. .....http://www8.hp.com/es/es/home.html
[83]Compaq..... http://www.compaq.com/country/index.html
[84]Microsoft..... http://www.microsoft.com/en-us/default.aspx
[85]Murray Turoff..... http://web.njit.edu/~turoff/
[86]Token Ring..... http://es.wikipedia.org/wiki/Token_Ring
[87]Institut Courant.....http://www.cims.nyu.edu/
[88]IEEE 802.3..... http://es.wikipedia.org/wiki/IEEE_802.3
[89]10 base 5..... http://es.wikipedia.org/wiki/10Base5
[90]10 base 2..... http://es.wikipedia.org/wiki/10Base2
[91]Bell Labs..... http://www.alcatel-lucent.com/wps/portal/BellLabs
[92]4ESS..... http://en.wikipedia.org/wiki/4ESS_switch
[93]SCSI..... http://es.kioskea.net/contents/pc/scsi.php3
[94]PS/2..... http://es.wikipedia.org/wiki/IBM_Personal_System/2
[95]OS/2..... http://es.wikipedia.org/wiki/OS/2
[96]SCO XENIX 386..... http://en.wikipedia.org/wiki/Xenix
[97]TCP / IP..... http://www4.uji.es/~al019803/tcpip/paginas/introduccion.htm
[98]SiGe..... http://www.dr-zippie.net/IMB20021106
[99] Macintosh..... http://es.wikipedia.org/wiki/Macintosh
[100]Pixel..... http://es.wikipedia.org/wiki/P%C3%ADxel
[101]Windows..... http://windows.microsoft.com/es-ES/windows/home
[102]Internet..... http://es.wikipedia.org/wiki/Internet
[103]Wireless..... http://www.configurarequipos.com/wireless.php
[104]PCMCIA..... http://es.wikipedia.org/wiki/PCMCIA
[105]HTML..... http://es.wikipedia.org/wiki/HTML
[106]Linus Torvalds..... http://www.laflecha.net/perfiles/tecnologia/linus_torvalds
[107]Linux..... http://es.wikipedia.org/wiki/GNU/Linux
[108]Seagate.....http://www.seagate.com/www/en-us/
[109]W3C.....http://www.w3c.es/Consorcio/
[110]Western Digital Corporation.....http://www.wdc.com/en/
[111]Honda.....http://world.honda.com/ASIMO/
[112]Netscape Communications Corporation.. http://en.wikipedia.org/wiki/Netscape
[113]EMV.....http://es.wikipedia.org/wiki/EMV
[114]Intranet..... http://es.wikipedia.org/wiki/Intranet
[115]Sun Microsystems..... http://www.thesun.co.uk/sol/homepage/
[116]Dig. Equip. Cor.... http://es.wikipedia.org/wiki/Digital_Equipment_Corporation
[117]AltaVista.....http://es.altavista.com/
[118]TCL/TK..... http://www.tcl.tk/
[119]EIDE..... http://es.wikipedia.org/wiki/EIDE
[120]JavaSoft.....http://javasoft-softwares.com/javasoft.htm

[121]Hotmail.....http://es.wikipedia.org/wiki/Hotmail
[122]Nokia..... http://www.nokia.com/
[123]GSM.....http://www.gsmspain.com/glosario/?palabra=GSM
[124]Mirabilis Ltd..... http://mirabilis-ltd.software.informer.com/
[125]DVD.....http://es.wikipedia.org/wiki/DVD
[126]AMD..... http://www.amd.com/es/Pages/AMDHomePage.aspx
[127]G.T.. http://in.kompass.com/profile_IN720845_es/global-telesystems-ltd-gi.html
[128]3Dlabs..... http://www.3dlabs.com/content/legacy/
[129]ATI..... http://es.wikipedia.org/wiki/ATI_Technologies
[130]Cirrus Lògic.....http://www.cirrus.com/en/
[131]NVIDIA.....http://www.nvidia.es/page/home.html
[132]AGP... .....http://es.wikipedia.org/wiki/Accelerated_Graphics_Port
[133]Ericsson.....http://www.ericsson.com/
[134]Unwired Planet..... http://www.unwired-planet.com/
[135]WAP.....http://es.wikipedia.org/wiki/Wireless_Application_Protocol
[136]CardBus PC card.....http://es.wikipedia.org/wiki/PC_Card
[137]Hitachi Amèrica.....http://www.hitachi.us/
[138]LCD.....http://en.wikipedia.org/wiki/Liquid_crystal_display
[139]RISC.....http://es.wikipedia.org/wiki/RISC
[140]VGA.....http://www.alegsa.com.ar/Dic/VGA.php
[141]IrDA.....http://en.wikipedia.org/wiki/IRDA
[142]Bluetooth.....http://www.bluetooth.com/Pages/Bluetooth-Home.aspx
[143]PDA.....http://es.wikipedia.org/wiki/PDA
[144]USB.....http://es.wikipedia.org/wiki/Universal_Serial_Bus
[145]DVD-Ram.....http://es.wikipedia.org/wiki/DVD-RAM
[146]DVD-ROM.....http://es.wikipedia.org/wiki/DVD-ROM
[147]DVD-Video / ROM..... http://www.monografias.com/trabajos16/dvd-video-digital/dvd-video-digital.shtml
[148]EEE.....http://es.wikipedia.org/wiki/Adoptar,_extender_y_extinguir
[149]LAN.....http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local
[150]WLAN.....http://es.kioskea.net/contents/wireless/wlan.php3
[151]Sanyo Electronic.....http://us.sanyo.com/Electronic-Devices-Components
[152]Eastman Kodak Company.....http://www.kodak.com/
[153]IrWW.....http://www.ttc.or.jp/jp/document_list/sum/sumE_JF-IR008.10v1.pdf
[154]JetSend....http://h10025.www1.hp.com/ewfrf/wc/document?cc=es&lc=es&dlc=es&docname=bsy20235
[155]CMOS.....http://en.wikipedia.org/wiki/CMOS
[156]LED.....http://es.wikipedia.org/wiki/Led
[157]iPAQ.....http://es.wikipedia.org/wiki/IPAQ
[158]Casio Computer.....http://world.casio.com/
[159]Palm.....http://www.palm.com/es/es/index.html
[160]Palm OS versió 5.0.....http://es.wikipedia.org/wiki/Palm_OS
[161]Kingston Technology Company.....http://www.kingston.com/
[162]Memòria ovònica..... http://es.wikipedia.org/wiki/PRAM

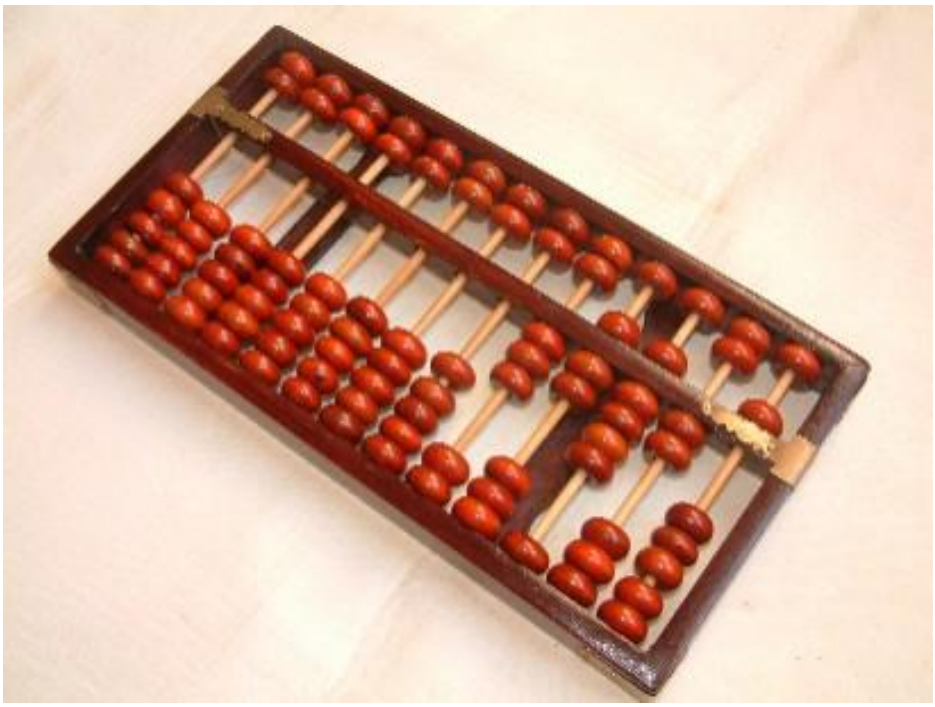
[163]DRAM.....http://es.wikipedia.org/wiki/DRAM
[164]SRAM.....http://es.wikipedia.org/wiki/SRAM
[165]MRAM.....http://www.neoteo.com/mram-la-memoria-ram-del-futuro-13733
[166]FRAM.....http://www.museo8bits.com/wiki/index.php?title=FRAM
[167]Sol_Med....http://www.businesswire.com/news/home/20030717_es_1002608_generatedID/es/
[168]IEEE.....http://es.wikipedia.org/wiki/IEEE
[169]Toshiba.....http://www.toshiba.com/tai/
[170]WUSB.....http://www.usb.org/developers/wusb/
[171]ADSL.....http://es.wikipedia.org/wiki/Asymmetric_Digital_Subscriber_Line
[172]UIT....http://es.wikipedia.org/wiki/Uni%C3%B3n_Internacional_de_Telecomunicaciones
[173]iPod.....http://www.apple.com/es/itunes/
[174]HD-DVD.....http://www.alegsa.com.ar/Dic/hd-dvd.php
[175] Blu-Ray Disc.....http://es.wikipedia.org/wiki/Blu-ray_Disc
[176]Samsung..... http://www.samsung.com/es/
[177]Cheoptics 360..... http://www.xataka.com/otros/cheoptics360-el-futuro-del-3d
[178]e-book.....http://es.wikipedia.org/wiki/Libro_electr%C3%B3nico
[179]CPU.....http://www.masadelante.com/faqs/cpu
[180]Làser.....http://ca.wikipedia.org/wiki/L%C3%A0ser
[181]LG...http://www.lg.com/es/index.jsp?gclid=CKuLofXyq6gCFcUMfAodDhkLew
[182]Graphics Lab.....http://www.graphicslab.com/
[183]Roadrunner..... http://es.wikipedia.org/wiki/IBM_Roadrunner
[184]Ubuntu.....http://www.ubuntu-es.org/
[185]Debian.....http://www.debian.org/index.es.html
[186]GFLOPS.....http://en.wikipedia.org/wiki/FLOPS
[187]Nanotubs.....http://www.euroresidentes.com/futuro/nanotecnologia/diccionario/nanotubos.htm
[188]Grafè.....http://es.wikipedia.org/wiki/Grafeno
[189]Robotics Institute.....http://www.ri.cmu.edu/
[190]Acualux 3D.....http://www.tendencias21.net/Un-novedoso-sistema-genera-imagenes-3D-sobre-pantallas-de-agua_a4647.html
[191]CSIC....http://www.csic.es/web/guest/home;jsessionid=79C524C6410834CBB9D6888058F6A3F3
[192]S.O....http://es.wikipedia.org/wiki/Anexo:Cronolog%C3%ADa_de_los_sistemas_operativos
[193]Texas Instruments..... http://www.ti.com/
[194]Sharp..... http://www.sharp.eu/es/
[195]Canon.....http://www.canon.es/
[196]Tablet PC.....http://es.wikipedia.org/wiki/Tablet_PC
[197]Alan Kay.....http://es.wikipedia.org/wiki/Alan_Kay
[198]GRiD Systems.....http://www.gridsystems.com/
[199]Visual Studio.....http://www.microsoft.com/spain/visualstudio
[200]C++.....http://msdn.microsoft.com/en-us/visualc/aa336395

[201].net Compact F...http://microsoft-net-compact-framework.softonic.com/pocketpc
[202]Symbian.....http://www.todosymbian.com/
[203]Flash lite.....http://www.adobe.com/products/flashplatformruntimes/
[204]MAC OS X.....http://www.apple.com/es/macosx/
[205]Objetive – C..... http://dymas.ii.uam.es/~flh/macprog/LenguajeObjective-C.pdf
[206]Android.....http://www.android.com/
[207]Instruccions x86.....http://www.buenastareas.com/ensayos/Instrucciones-En-Ensamblador/774598.html
[208]Blue Gene/L..http://www.abadiadigital.com/articulo/blue-genel-bate-el-record-de-supercomputacion/
[209]Cray XT5..... http://www.cray.com/Products/XT5/Product/Specifications.aspx
[210]Pleiades..... http://www.top500.org/connfam/8
[211]Tianhe 1-A..... http://www.eweekeurope.es/etiqueta/tianhe-1a
[212]Súper computadores 1.....http://listiki.com/my-favorite-supercomputers
[213]Súper computadores 2.....http://www.top500.org/connfam/8
[214]SMD..http://es.wikipedia.org/wiki/Tecnolog%C3%ADa_de_montaje_superficial
[215]Llei de Moore.....http://es.wikipedia.org/wiki/Ley_de_Moore
[216]Evolució dels microprocessadors..http://es.wikipedia.org/wiki/Microprocesador
[217]Producte tensorial.....http://es.wikipedia.org/wiki/Tensor
[218]Karl Friedrich Gauss.....http://www.ecured.cu/index.php/Karl_Friedrich_Gauss
[219]QFT.....http://www.ic-itcr.ac.cr/~jcastro/libro/libro/node40.html
[220]Algorisme d' Euclides.....http://www.vitutor.com/di/di/a_8.html
[221]Models probabilístics...http://home.ubalt.edu/ntsbarsh/opre640s/spanishp.htm
[222]Problemes classe P.....http://es.scribd.com/doc/56396824/23/Complejidad-computacional
[223]Solovay i Strassen..... http://es-la.facebook.com/pages/Solovay-Strassen-algorithm/143368819013295?sk=wiki
[224]Chernoff..... http://es.wikipedia.org/wiki/Herman_Chernoff
[225]Peter Shor.....http://es.wikipedia.org/wiki/Peter_Shor
[226]Richaard Feynman.....http://es.wikipedia.org/wiki/Richard_Feynman
[227]Mach Zehnder.....http://www.gruascastelao.com/java/MZI.htm
[228]Deutsch.....http://www.worldlingo.com/ma/enwiki/es/Deutsch-Jozsa_algorithm/1
[229]Algorisme de Grover.....http://es.wikipedia.org/wiki/Algoritmo_de_Grover
[230]Zalka....http://biblioteca.universia.net/html_bura/ficha/params/id/466026.html
[231]Boyer.. http://diccionario.sensagent.com/CARL%20BENJAMIN%20BOYER/en-en/
[232]Espai de Hilbert.....http://138.100.110.67/t3.pdf
[233]Calderbank_Shor_Steane...http://journal.info.unlp.edu.ar/journal/journal26/papers/JCST-Oct09-2.pdf

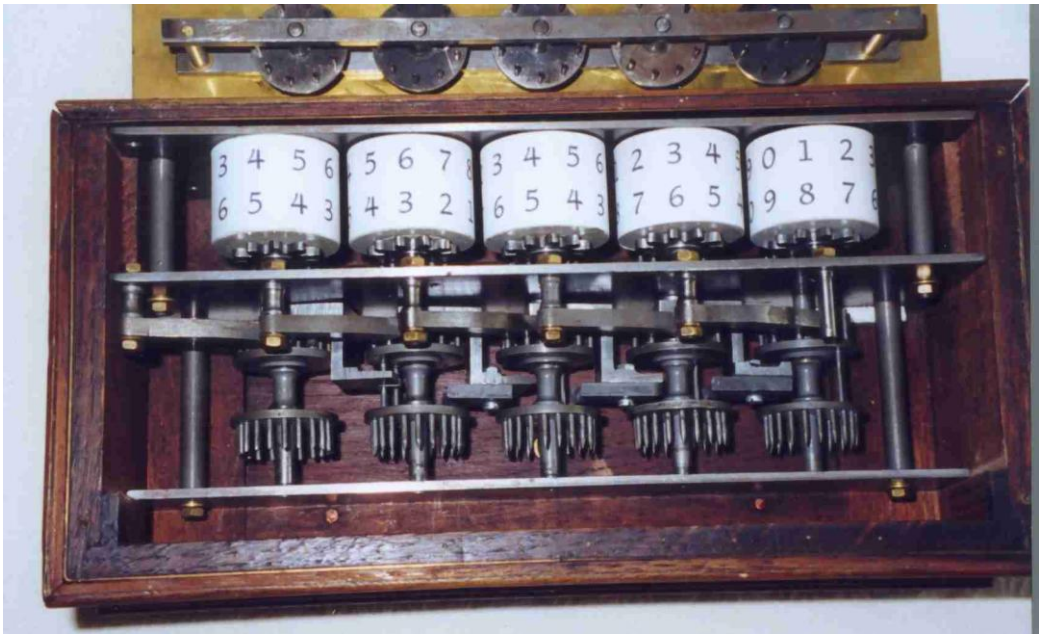
Annex I

Aquest apartat pretén donar una visió gràfica de les diferents màquines que hem anat mencionant a les diferents generacions per tal de poder veure com evolucionen amb mida i materials.

En primer lloc veiem com és un àbac:

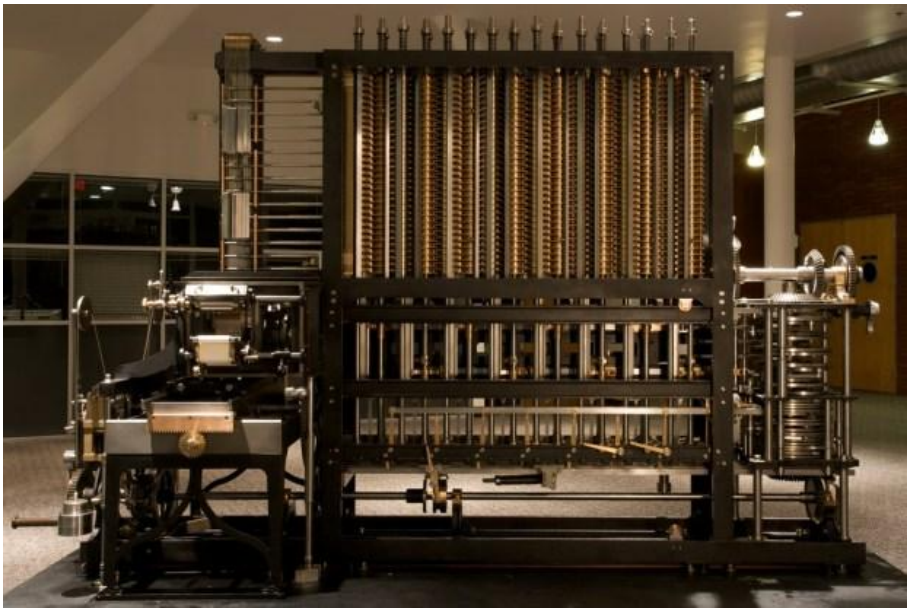


En aquesta pròxima imatge podrem veure la Pascalina de Blaise Pascal:

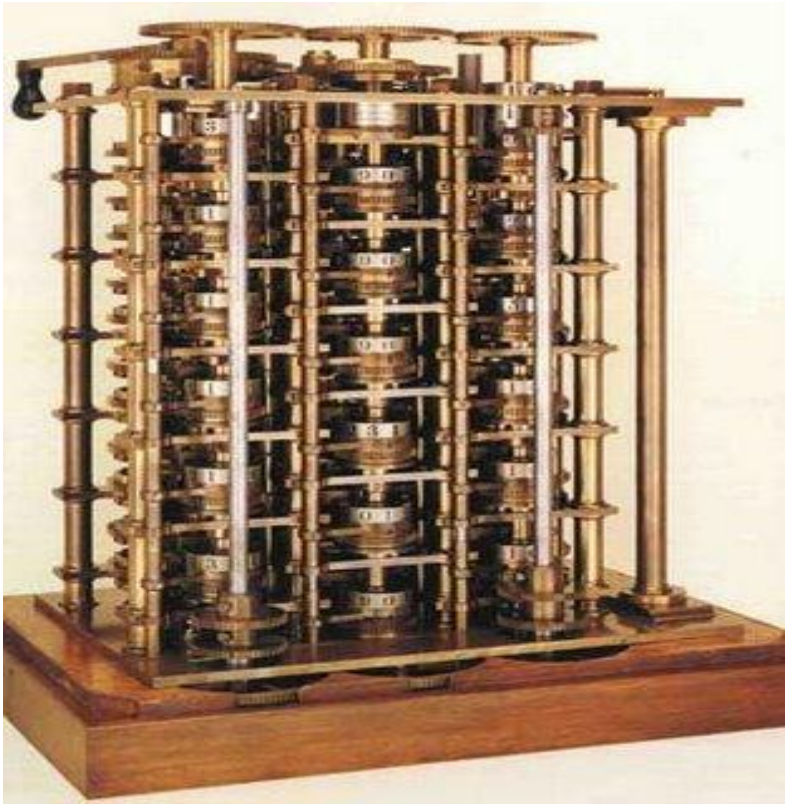


En la següent imatge podem veure el taler de Joseph Marie Jacquard:

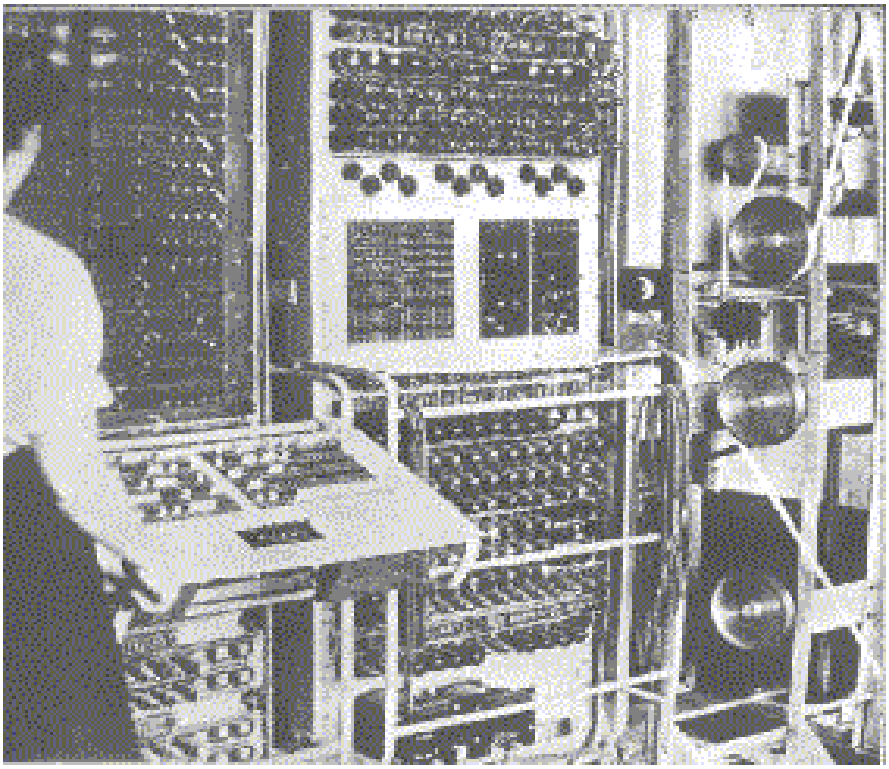
La pròxima imatge mostra la màquina diferencial de Charles Babbage:



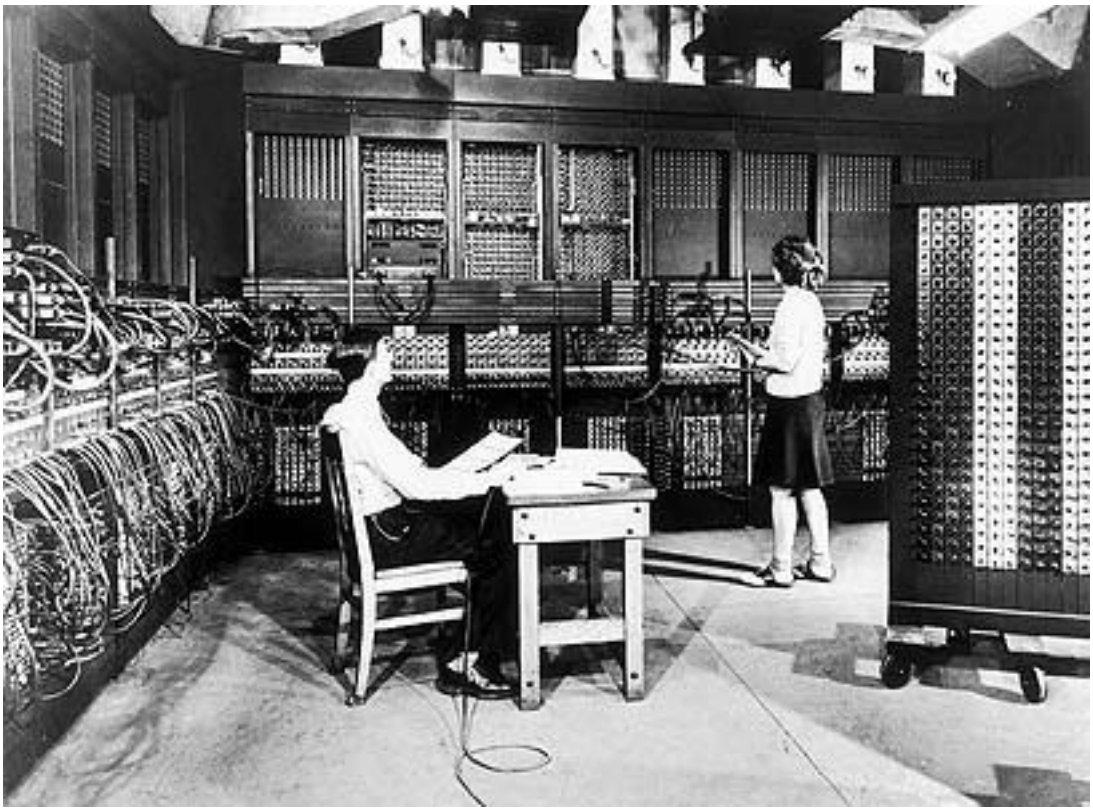
A continuació podem veure la màquina analítica del mateix autor que la màquina diferencial:



Passem al primer computador electrònic i podem veure una imatge de la Colossus:

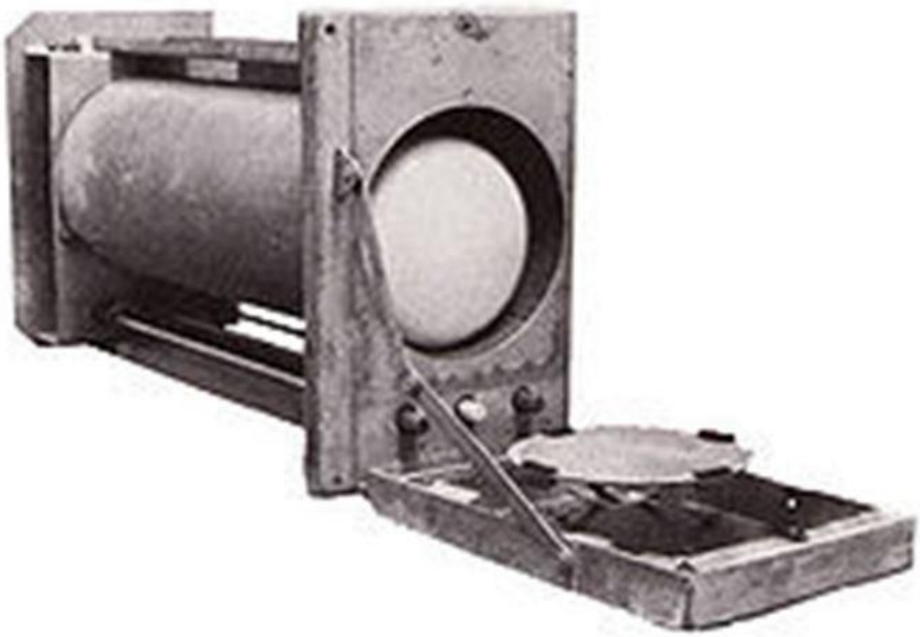


La fotografia següent ens mostra com era la ENIAC:

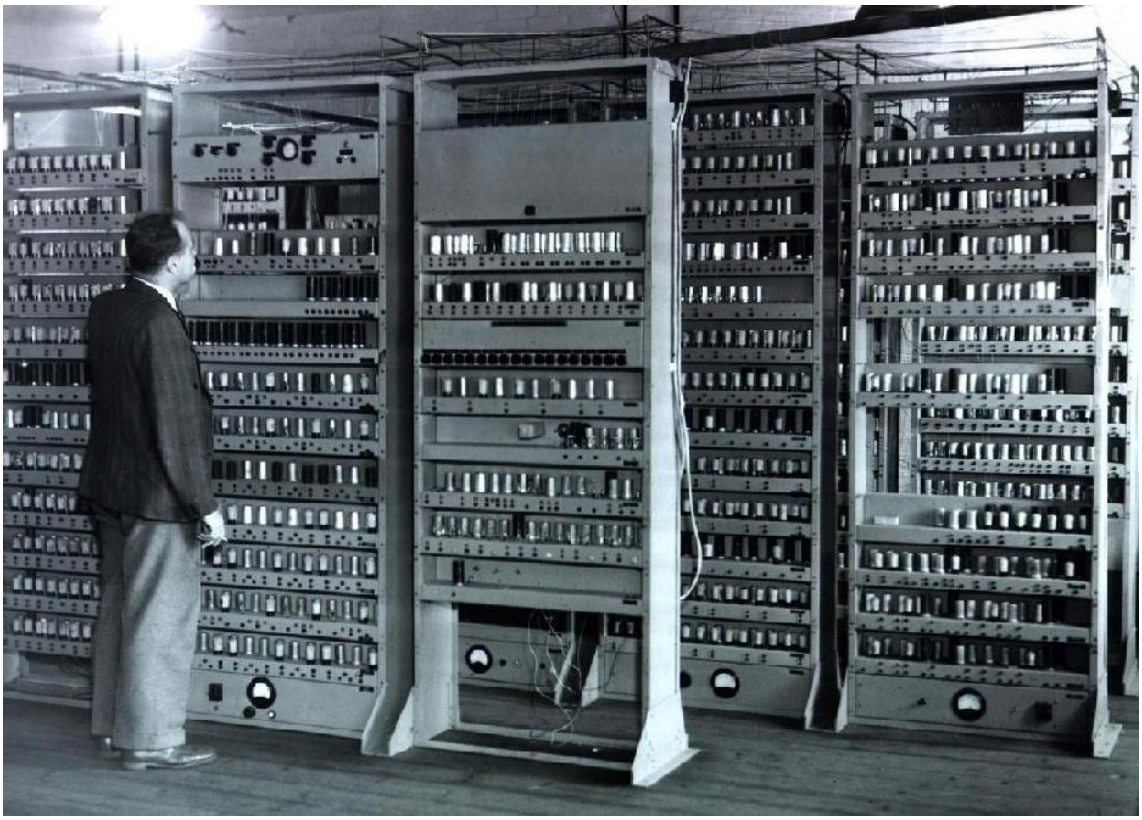


La Manchester Baby tenia l'aspecte següent:

La següent és una imatge del tub de Williams per guardar dades de forma temporal:



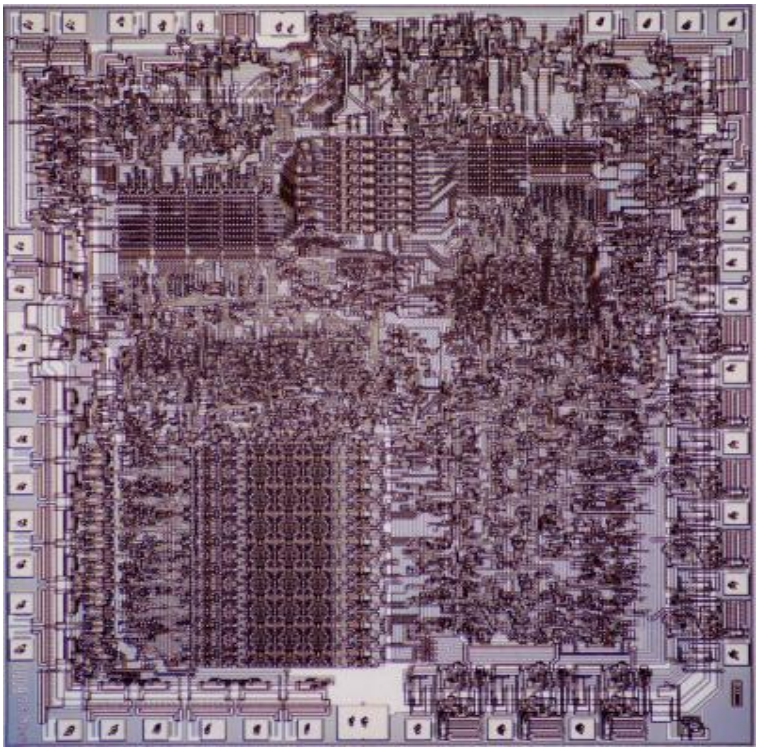
Ara un detall de com era la computadora EDSAC:



Ara podrem veure una sala amb dos computadors a transistors que són de les primeres generacions. Eren d'una mida considerable però molt més reduïts que els de la generació anterior de vàlvules:

La següent fotografia ens mostra un dels primers computadors amb integrats. Es tracta del IBM sèrie 360:

La imatge següent ens mostra el microprocessador 8080 de Intel desencapsulat:



Annex II

En aquest annex farem un repàs del que va donar de si aquesta generació en quan a l'aparició de computadors personals, en quina tecnologia sortien equipats i com van evolucionar. També veurem com evolucionen les comunicacions i els sistemes operatius.

Any 1982

- Commodore [51] treu el Commodore 64 amb un processador 6510 de Rockwell [66], 64 KB de RAM, 20 KB de memòria ROM, amb so, gràfics amb color i amb el software Microsoft BASIC instal·lat. Surt a un preu inicial de 600$ i a l'any sobre cau el seu preu a 200$. Se'n venent entre 17 i 22 milions d'unitats. És la primera computadora personal que compta amb un circuit sintetitzador de so.
- Toshiba Amèrica treu el seu primer PC, el model T-100 equipat amb un microprocessador Z80A de Zilog [67], una pantalla LCD, 32 KB de RAM, 32 KB de ROM en format de cartutxos.
- Sharp introdueix la PC-1500 amb 16 KB de ROM i amb 3.5 KB de RAM a un preu de 300$. També treu una microimpresora a color per 250$.
- Radio Shack treu el TRS-80 model 16 amb un microprocessador MC68000 de Motorola, un Z80 de Zilog, platines de floppy de 8" i de forma opcional, un disc dur de 8 MB.
- Intel (fabricant de microprocessadors) treu al mercat el microprocessador 80286 a 6 MHz. El seu bus de dades és de 16 bits, incorpora 134000 transistors, amb tecnologia de 1.5 micres [68], oferint un mode d'operació protegit. El seu preu és de 360 $ cadascun comprats en quantitats de 100 unitats. Pot accedir a 16 MB de memòria RAM i 1 GB de memòria virtual [69]. Té una velocitat de 0.9 MIPS (milions d'instruccions per segon). En posterior versions s'augmenta la velocitat i el nombre de MIPS (10MHz / 1.5 MIPS i 12 MHz / 2.66 MIPS).
- Non-Linear Systems [70], introdueix la Kaycom II per 1800$. Està equipada amb dues platines de floppy de 5.25", processador Z-80 de Zilog, CP/M i una pantalla de 9" amb 80 columnes monocromàtica.
- Microsoft allibera el sistema operatiu MS-DOS 1.1 [71] a IBM, per a la IBM PC. Suporta platines i discs floppy de doble cara amb 320 KB de capacitat. També allibera MS-DOS 1.25 per a les computadores compatibles amb IBM.
- Epson Amèrica [72] treu la HX-20, HC-20. Es tracta d'una computadora de mida com una llibreta que pesa 1.5 Kg i funciona amb bateries amb una autonomia de fins a 50 hores.
- Commodore Business Machines introdueix la microcomputadora professional multiprocessador a 16 bits. És la BX256 amb 256 KB de RAM, un microprocessador 8088 de Intel per CP / M 86, un microprocessador 6509 de Rockwell, un monitor monocrom de 80 columnes, platines de disket integrades, so i to per 3000$.

- Lotus Devolopment Corporation [73] treu en el mercat el full de càlcul Lotus 1-2-3. Sony [74] i Philips [75] tenen ja productes de disc compacte a punt per a la seva sortida al mercat.
- Els CD es comencen a fabricar en massa.

Any 1983

- Es publiquen les especificacions per el Sistema de Nom de Domini (DNS) [76] de Internet desenvolupades a la universitat de Wisconsin.
- Microsoft anuncia el Windows 1.0.
- Bjarne Stroustrup desenvolupa la primera versió de C++ [77] que combina la programació orientada a objectes (OOP) [78] amb l'eficiència que ofereix la mida reduïda i flexibilitat de C.
- S'allibera comercialment el sistema operatiu UNIX System V [79], Release 1.
- Apple [80] treu el Macintosh basat en el microprocessador MC 68000 de Motorola [81] a 8MHz, de 16 bits, amb 64 KB de ROM, 128 KB de RAM, unitat de disc de 3.5" i 400 KB, monitor gràfic integrat monocrom de 9" i de 512 x 342 de resolució so de 8 bits de resolució a un preu de 2495 $.
- Motorola treu el MC68020 que és el primer microprocessador de 32 bits reals i que integra un total de 200000 transistors en una pastilla de silici de 10 x 10 mm.
- S'inicia la distribució i implementació de DNS.
- Hewlett – Packard [82] entra en el negoci de l'impressora amb la seva línea d'impressores d'injecció de tinta (InkJet) i làser (LaserJet). La resolució d'impressió és de 96dpi per a equips portàtils i d'escriptori.
- IBM treu el seu primer portàtil considerat una còpia del Compaq [83], i la computadora personal AT amb processador de 16 bits, el 80286 de Intel, disc dur de 20 o 30 MB, monitor a color amb capacitat gràfica per 6700 $.
- Microsoft [84] treu la versió 3:0 de MS-DOS per a la IBM AT i el MS-DOS 3.1 per a xarxes.

Any 1985

- Intel treu el microprocessador 386DX que funciona a una freqüència de rellotge de 33MHz, amb un bus de 32 bits, integra 275000 transistors i amb capacitat per direccionar 4GB de memòria RAM.
- Commodore treu en el mercat la Amiga 1000. Es tracta de la primera computadora multimèdia. Funciona amb un 68000 de Motorola i era capaç de manegar gràfics, so i vídeo. És capaç de suportar 4096 colors i produeix so de alta qualitat a 4 canals. Usa un sistema operatiu multi tasca basat en finestres.
- En aquest any, Internet ja connecta a 2000 amfitrions.
- El grup de Murray Turoff [85] en el NJIT estrena el concepte d'aula virtual oferint cursos a distància a través de la xarxa.

- La companyia IBM introdueix els elements i accessoris per a xarxes Token Ring [86], per a compartir recursos de còmput a través d'edificis, iniciant així un estàndard per a les xarxes d'àrea local.
- L' institut Courant [87] de Ciencies Matemàtiques, de la universitat de New York, comença el disseny del RP3, una computadora experimental amb 512 processadors en paral·lel i una memòria principal de 2GB.
- Es presenta la norma estàndard IEEE 802.3 [88] per a xarxes Ethernet, oferint especificacions per a les xarxes amb cable coaxial gruixut (10 base 5 [89]) i prim (10 base 2 [90]).
- Arriben les primeres unitats de CD reproductores en els PC. Bell Labs [91] desenvolupa els equips d'accés i procediments de senyalització per a permetre la transmissió commutada de dades a 56Kbps a través del commutador de tarificació 4ESS [92], que permet en els usuaris transmetre dades en una connexió d'accés telefònic a xarxes sens haver d'utilitzar línies privades dedicades entre elles.
- En el Japó finalitza la instal·lació de la primera xarxa de fibra òptica.

Any 1986

- Canon inventa la fotocopiadora làser a color.
- Microsoft allibera el MS-DOS 3.2 i el Windows 1.03.

Any 1987

- Internet ja compta amb 30000 amfitrions.
- Apareix el model de computador Apple Mac II amb un processador MC68020 de Motorola a 16MHz i 32 bits, una unitat de coma flotant 68881 de Motorola, 256 KB de ROM, fins a 20MB de RAM, port SCSI [93], unitat de disquet de 800KB i 3.5", disc dur opcional de 40 o 80MB, i so estèreo de 8 bits, monitor de color extern i a un preu de 3898 $.
- IBM treu el Personal System / 2 (PS/2) [94], usant el sistema operatiu OS/2 [95], que busca substituir el MS-DOS. El model 30 estava equipat amb un processador Intel de 8MHz, amb una o dos unitats de disquet de 3.5" i 720KB, i un disc dur de 20MB. El model 80 era un model a 16MHz, 1MB de RAM i un disc dur de 44MB. Els preus variaven de 1695 $ a 10995 $.
- Microsoft allibera MS-DOS 3.3 i Windows 2.0. Arriba en el mercat SCO XENIX 386 [96], el primer sistema operatiu de 32 bits, i el primer UNIX per equips amb processador Intel 386.

Any 1988

- S'introdueix en el computador la unitat de CD gravable (CD-R, CD Recordable).

- S'instal·la el cable telefònic transatlàntic amb fibra òptica. Suporta 8000 trucades telefòniques simultànies a 280Mbps. Es comença a adoptar en aquest any i per alguns països el protocol TCP / IP [97].

Any 1989

- Internet ja compta amb 160000 amfitrions.
- Surten en el mercat els processadors de Intel 486DX i 486SX. El primer integra un coprocessador matemàtic, funciona a 50 MHz, conté 1.2 milions de transistors i pot direccionar 4GB de RAM. El segon funciona a 33MHz, amb bus de 32 bits i integra 1185000 transistors. També té capacitat per direccionar 4GB de memòria.
- IBM inventa el transistor de silici – germani (SiGe) [98], que substitueix els de Arseniür de Gali (molt més costosos) en el que són semiconductors d'alta velocitat de commutació (canvi d'estat).

Com veiem, en aquesta dècada el computador experimenta una constant evolució juntament amb els perifèrics i també les comunicacions experimenten una expansió. Cada cop surten al mercat circuits integrats més densos la qual cosa augmenta la potència dels equips que els incorporen. També el preu cada vegada és més baix i això provoca un augment en el número de vendes d'aquests equips i una popularització dels mateixos. Els sistemes d'emmagatzematge de dades evolucionen i creixent. Veiem que surt en el mercat el CD de lectura i poc després ho fa el de lectura / escriptura. També en aquesta dècada la telefonia mòbil es comença a desenvolupar i a comercialitzar encara que ho fa d'una forma incipient. Per el que fa a Internet podem veure com el nombre d'usuaris es va multiplicant cada any. La revolució de les comunicacions ha començat.
En la següent generació podrem veure com tots aquests camps continuen avançant de forma frenètica i cada any que passa l'evolució és considerable.

Annex III

Any 1991

- Surt la Power Book 100 de Macintosh [99]. Es tracta del primer ordenador portàtil d'aquesta firma comercial. Té un processador de 16 bits MC68HC00 de Motorola [81] a 16MHz, 256KB de ROM [44], 2MB de RAM [43] expansible a 8, mòdem opcional, disc dur de 20 – 40 MB, pantalla monocroma de matriu passiva i 640 x 400 píxels [100] de resolució, so de 8 bits monofònic i tot a un preu de 2500 $.
- Microsoft [84] allibera el seu sistema operatiu MS-DOS 5.0 [42] i Windows 3.0 [101].
- Internet [102] connecta a 600000 amfitrions a més de 100 països.
- Finalitza la instal·lació del cable telefònic transatlàntic TAT-9. Pot suportar 80000 trucades simultànies o 560Mbps. També s'instal·la el cable del pacífic nord per Cable & Wireless [103], capaç de suportar 85000 trucades simultànies.
- L'associació Internacional de Targetes de Memòria per a Computador Personal (Personal Computer Memory Card International Association, PCMCIA [104]), allibera la primera versió del seu estàndard per a targetes d'ampliació de memòria per a equips portàtils amb factor de forma de targeta.
- Motorola Computer Group[81] desenvolupa i presenta el VME64 que és una evolució del VMEBus elevant la velocitat teòrica de 40MBps a 80MBps.
- Es comencen a presentar les primeres bases de dades amb llenguatge HTML [105].
- Linus Torvalds [106] anuncia a Internet [102]la creació de Linux [107], un sistema operatiu tipus UNIX [79] per a PC. Es troba en fase de desenvolupament però el seu autor l'ofereix lliure i proposa a d'altres programadors compartir millores i correccions. Tres anys després, aquest sistema operatiu tindria més de 100000 usuaris i contaria amb la col·laboració per el seu desenvolupament de centenars de programadors.

Any 1992

- Microsoft [84] allibera el Windows 3.1[101]. Se'n venen més d'un milió de còpies.
- La firma comercial Seagate [108], introdueix en el mercat la primera platina de disc dur de 7200 RPM, i també la tecnologia amb sensor de cop per a discs de 2.5".
- El cable Trans - Pacífic TPC-4 s'acaba d'instal·lar entre Japó, Canada i Estats Units. Té una capacitat de 2 x 256Mbps. També el cable Transatlàntic TAT-10 és instal·lat, entre Green Hill, Rhode Island, Norden, Alemania, Terschelling, Països Baixos, i Alkmaar. Cobreix una distància total de 7354Km. Té un ample de banda de 560Mbps.
- Internet [102] ja connecta a un milió d'amfitrions.

Any 1993

- La companyia Intel [38] treu al mercat el microprocessador Pentium que funciona a 66MHz, amb un bus de 64 bits. Té capacitat per a direccionar 4GB de memòria.
- Apple Computer [40] allibera en el mercat la Apple Newton, la primera computadora de ma capaç d'identificar escriptura manual i que pot ser usada com un bloc de notes.
- Microsoft [84] treu Windows NT 3.1[101].
- Compaq [83] treu al mercat les primeres famílies PC en format mini torre. Es tracte dels models Presario i ProLinea.
- Segons un estudi fet a finals d'aquest any (1993), un 81% dels ordinadors estan basats en arquitectura Intel.
- S'estableix el World Wide Web Consortium, o W3C [109]. La seva principal missió serà el desenvolupament del concepte Web.
- El cable Atlàntic sud SAT-2 s'acaba d'instal·lar entre Melkbosstrand, (Àfrica del sud), El Medano, (a l'illa de Tenerife) i Funchal, (illa de Madeira, Portugal) amb una distància total de 9500Km i un ample de banda de 2 x 260Mbps. També s'acaba d'instal·lar el cable transatlàntic TAT-11 entre Manahawkin (New Jersey), Oxwich Bay (Inglaterra) i St. Hilaire de Riez (France), amb una longitud total de 7162Km. Suporta un ample de banda de 560Mbps.
- Western Digital Corporation [110] fabrica el primer disc dur amb dos plats i 3.5" amb capacitat de 340MB.
- Honda [111] presenta el primer prototip de robot amb una alçada de 1915mm i 175Kg. Tenia la font d'alimentació i la computadora ubicada a l'esquena. Era capaç d'activar un commutador, girar la balda d'una porta i carregar objectes.

Any 1994

- El desenvolupament del WWW [109] passa del CERN al consorci W3 establert per Tim Berners-Lee i amb base a Europa i Estats Units.
- Microsoft [84] treu el seu Windows NT 3.5 [101].
- Netscape Communications Corporation [112] treu el seu navegador Netscape (TM) Network Navigator, versió Beta, gratuït a través de Internet. Aquest navegador dona suport natiu al format d'imatges JPEG i permet accessos múltiples i simultanis a la xarxa, aspectes aquests que es convertiran en estàndard en els navegadors de Internet.
- L'Associació Internacional de Targetes de Memòria per a Computadora Personal (PCMCIA) [104] treu la versió 3.0 dels seu estàndard amb el nom de

PC-Card 95. El propòsit d'aquesta nova versió és el de reduir la confusió creada amb els estàndards tipus I, II i III.

- Netscape Communications Corporation [112], associats amb First Data Card Services Group, el processador de pagaments amb targeta de crèdit més gran del mon en aquests moments, anuncia un acord que permet en els bancs a proveir de serveis de comerç electrònic a través de Internet.
- El cable transatlàntic Canadenc CANTAT-3 és instal·lat entre Pennant Point (Nova Escòcia, Canadà), Vestmannaevjar (Islàndia), Tjornivik (Illes Faroe), Redcar (Regne Unit), Blaabjerg (Dinamarca), i Sylt (Alemanya) amb una longitud total de 7104Km. Té un ample de banda de 2,5 Gbps.
- S'instal·la el cable Columbus-II entre Palerm (Sicília, Itàlia), Funchal (Illa Madeira, Portugal), Sardina (Gran Canàries), St. Thomas (Illes Verges, Estats Units), Palm Beach del oest (Florida, estats Units), i Cancún (Mèxic). Té una longitud total de 12300 Km i un ample de banda de 3 x 560Mbps. El tram de les Illes Verges a Florida l'ample de banda és de 2 x 2.5Gbps.
- S'instal·la el cable SEA-ME-WE 2 entre France, Itàlia, Indonèsia i Singapur, amb un ample de banda de 2 x 560 Mbps.
- Europay, Màster Card, i VISA (EMV) [113] crea'n especificacions per els diners electrònics.
- Motorola [81] treu el sistema comercial de ràdio iDen dissenyat per a integrar cerca persones, comunicacions de dades, veu, i telefonia mòbil en una mateixa xarxa de ràdio i un mateix dispositiu de mà.
- Apareix per primer cop el terme Intranet [114] per a un servidor web de servei intern dintre d'una companyia. L'ha creat Steven L. Telleen a Amdahal Corporation.
- Western Digital Corporation [110] fabrica el primer disc dur EIDE [119] de 1 GB amb tres discs integrats.

Any 1995

- Sun Microsystems [115] treu el llenguatge de programació Java i el navegador de Internet Hotjava.
- Netscape [112] llicencia Java.
- Microsoft [84] treu Windows NT 3.51 [101]. També treu Windows 4.0 amb el nom comercial de Windows 95.
- PCMCIA [104] forma un grup de treball, dintre el comitè tècnic de PCMCIA, dedicat a la estandardització i promoció de la PC Card com a dispositiu de seguretat.
- Intel [38] treu el microprocessador Intel Pentium a 200MHz, amb un bus de 64 bits, 5.5 milions de transistors i capaç de direccionar 64GB de memòria.
- Els laboratoris d'investigació de Palo Alto a Califòrnia, de Digital Equipment Corporation [116] presenta AltaVista [117], el primer motor de cerca a Internet, que funciona en base de dades, emmagatzemant cada paraula de les pàgines i permet cercar en base a criteris. El software s'ha elaborat amb llenguatge de

programació C sota Digital UNIX [79], en un Alpha Server 8400s. El cercador Web és una aranya denominada Scooter, que suporta 1500 fils (threads) i revisa al voltant de 6 milions de pàgines al dia. Respecte arxius d'exclusió de robot i usa una algorisme per tal d'evitar sobrecarregar en els servidors.

- Sun Microsystems [115] introdueix el TCL/TK [118], una plataforma múltiple per a donar suport per execució segura de programes de xarxa i aplicacions GUI independents de la plataforma en que es treballi.
- S'introdueixen els mòdems per cable, que ofereixen connexió digital a xarxes de dades a alta velocitat a través de marxes de televisió per cables. Són normalment usats per a tenir connectivitat a Internet.
- Western Digital Corporation [110] fabrica el primer disc dur EIDE [119] de 1.6GB de capacitat.
- Bell Labs [91] treu Plan 9. Es tracte d'un sistema operatiu per a computació distribuïda junt amb les seves eines associades creades per el Centre d'Investigació de Ciencies de la Computació (Computing Science Research Center).

Any 1996

- Sun Microsystems [115] treu el conjunt d'eines per a desenvolupadors de Java, Java Developers Kit (JDK) v 1.0.
- Aquest any, Internet [102] ja compta amb 30 milions d'usuaris.
- JavaSoft [120], una companyia de Sun Microsystems [115], anuncia JavaOS, el sistema operatiu per a executar aplicacions Java directament en microprocessadors en qualsevol tipus de dispositiu, des de computadores de xarxa fins a cerca persones.
- Apareix Hotmail [121] , el primer servei gratuït de correu electrònic de Internet, creant amb aquest concepte més relacionat amb el Internet, web mail.
- Nokia [122] comença a vendre el seu comunicador Nokia 9000, integrant per primer cop un telèfon cel·lular GSM [123] amb un organitzador personal.
- S'instal·la el cable telefònic transatlàntic TAT-12/13. Es tracte d'un anell de segments de cable submarí interconnectant estacions de cable a Green Hill (Rhode Island), Lands End (Anglaterra), Penmarch (France) i Shirley (New York), cobrint una distància de 6321Km. Utilitza tecnologia d'amplificació òptica i té un ample de banda de 10Gbps amb 300000 circuits de veu.
- Microsoft [84] treu el Windows NT 4.0 [101].
- Sun Microsystems [115] allibera la tecnologia Targeta Java 1.0. Es tracte d'una targeta intel·ligent que incorpora un microprocessador Java dintre de la mateixa targeta.
- Intel Corporation [38] anuncia un nou factor de formes per a plaques base anomenat NLX, que millora els actuals de baix perfil.
- Mirabilis Ltd [124], una empresa virtual, treu la primera versió de ICQ (I Seek You). És el primer software de comunicació instantània persona a persona, creant una nova categoria de termes a Internet: el missatger instantani.

- Microsoft [84] treu Windows CE 1.0 [101]. És la primera versió de Windows per a dispositius portàtils. CE són les sigles de Compact Edition.
- S'instal·la el cable Trans – Pacífic TPC-5CN entre San Lluis Bisbe (Califòrnia), Guam (Hawai), Japó i Bandom (Oregon), amb un ample de banda de 2 x 5Gbps.
- En promig, en el mon hi ha 12,8 línies principals i 2,4 cel·lulars per a cada 100 habitants, amb un creixement anual del 7% i 62% respectivament. Asia i Nord-americà tenen cadascun 46 milions de subscriptors a telefonia cel·lular, però el creixement anual estimat és del 106% i 30% respectivament.
- Es presenta la tecnologia per el Vídeo Disc Digital, que eventualment canviarà el seu nom per el de Disc Versàtil Digital o DVD [125].

Any 1997

- AMD [126] anuncia el processadors AMD-K5 a 166MHz i el AMD-K5-PR166.
- Global Telesystems Ltd [127] anuncia la signatura d'un acord per a instal·lar el cablejat de xarxa Atlàntic Crossing 1 (AC-1), una xarxa anular de fibra òptica autor regenerable d'alta capacitat, amb quatre brins, i Jerarquia Sincrònica Digital (SDH), connectant Estats Units amb el Regne Unit i Alemanya. Serà la xarxa més avançada amb Multiplexació per Divisió de Longitud d'Ona (WDM) i tecnologia d'Amplificació per aliatge de Fibra amb Erbi. Tindrà una longitud de 14000 kilòmetres i un ampla de banda de 40 Gbps bidireccional. Estarà enllestida a finals de 1998.
- A San José (Califòrnia) Intel [38] es posa en marxa amb una iniciativa dirigida a l'entrega de noves capacitats visuals més potents en computació. Sota el nom d'Iniciativa de Computació Visual, 3Dlabs [128], ATI [129], Cirrus Lògic[130], Evans & Sutherland, NVIDIA [131], S3 i Trident donen suport al Port Accelerat per a Gràfics (AGP [132]). També anuncia que inicia el desenvolupament de les futures versions d'aquest port que arribaran en els 512Mbps (2x) i 1Gbps (4x).
- AMD [126] anuncia els nous processadors AMD-K6 a 166MHz, a 200MHz, i a 233MHz per a sòcol 7 CPGA. Contenent 8,8 milions de transistors i estan fabricats amb tecnologia de 0,35 micres.
- Intel [38] treu el microprocessador Pentium II a 300MHz amb bus de 64 bits i que conté 7,5 milions de transistors. Té capacitat per a direccionar 64GB de memòria.
- Ericsson [133], Motorola [81], Nokia [122] i Unwired Planet [134] s'uneixen per a crear en protocol per aplicacions sense fils (Wireless Applications Protocol, WAP [135]), d'arquitectura oberta.
- Compaq [83] llença al mercat el monitor de pantalla plana TFT 500.
- Intel Corporation [38] anuncia la disponibilitat del primer adaptador de xarxa que permet en els administradors de sistemes engegar, arrancar i donar servei remotament a computadores personals. Aquest desenvolupament es part de la Iniciativa cablejada per a Administració (Wired for Management Initiative) per a permetre un control centralitzat de computadores sens sacrificar agilitat. El nou adaptador és un membre de la família EtherEpress de Intel i compta amb

capacitats avançades d'administració, utilitzant l'Agent de Serveis LANDesk de Intel i la tecnologia Activació en Xarxa (Wake on LAN WOL) de IBM [30].

- A Santa Clara (Califòrnia) Intel [38] anuncia el seu conjunt de circuits 440LX AGP [132], que incorpora el primer port accelerat per a gràfics, així com un disseny arquitectural innovador denominat Quad Port Acceleration (QPA) que inclou AGP [132] de connexió directa, accés de multi flux a memòria i arbitratge distribuït dinàmic.
- Intel [38] treu el processador Mobile Pentium que treballa a 200 i 233 MHz, amb 4,5 milions de transistors, construït amb tecnologia de 0,25 micres, bus de 64 bits, amb càpsula de 320 pins i dissenyat per ús en computadores portàtils.
- Es crea el estàndard CardBus PC card [135]. Defineix dispositius amb format targeta a 32 bits i 3.3v, que s'integra en el bus PCI amb totes les millores que pot heretar, neixen la possibilitat de crear targes per a xarxa a 100Mbps, SCSI II, vídeo conferència, etc., I superant-ho amb les característiques d'intercanvi en calent i connectar i usar, que ja eren part del estàndard anterior. Inclou un esquema de osques per a prevenir la inserció de targes CardBus en els slots de 16 bits que no suporten aquestes noves tecnologies.
- S'instal·la el cable Fiber Link Across/Around the Globe (FLAG) passant per a 12 països incloent-hi Shangai (China) entre el regne Unit i Japó cobrint una distància de 27000 Km i un ample de banda de 2 x 5Gbps.
- Es crea l'estàndard per el DVD [125] gravable, el DVD-Recordable (DVD-R) a 3,9GB.

Any 1998

- AMD [126] anuncia la disponibilitat dels primers microprocessadors AMD-K6 fabricats amb tecnologia de 0,25 micres. Funcionen a 266 i 233 MHz.
- S'instal·la el cable Gemini per Gemini Submarine Cable System Ltd, entre Manasquan (Nova Jersey), Charlestown (Estats Units), Abadia de Oxwich (Regne Unit) i Porthcurno (Regna Unit), cobrint una distància total de 12600 Km i amb un ample de banda de 2 x 15Gbps en un anell SDH.
- Intel [38] anuncia el AGP Pro [132], part de la seva futura especificació v2.0 de la interfície. Arriba els 512MBps en 2x i 1Gbps en 4x, i inclou les especificacions per a un connector i sistema de refredament millorat, així com especificacions de factor de forma i distribució.
- Hitachi Amèrica Ltd. I Hitachi Home Electronics (Amèrica) [137], anuncien dos models de computadores de ma optimitzades per a Microsoft Windows CE 2.0 [101]. La HPW-200EC és la primera del seu tipus amb pantalla LCD [138] a color, processador RISC [139] a 32 bits Hitachi Super HTM SH3 a 100MHz, 16 MB de RAM [43], expandible a 48, 128 MB de ROM [44], mòdem per software a 33,6 Kbps, port de sortida VGA [140], interfície IrDA [141], bateria recarregable de Lithium-Ion i una pantalla LCD [138] a color de 8,1" de diagonal amb resolució de 640 x 240 píxels i una mida de punt de 0.30mm. També disposa d'un teclat de 74 tecles gairebé de mida completa, una ranura de PCMCIA [104]

tipus II, una ranura per a targeta compacta tipus Flash, tecles d'accés ràpid, micròfon, altaveu integrat i també capacitat de gravar veu.

- Nokia [122] presenta el Nokia 9110 Communicator, dit de segona generació. Pesa 149 grams i compta amb les característiques del model 9000 a més de la capacitat d'ampliar la memòria a 4MB. Nokia és el segon fabricant mundial de telèfons mòbils.
- Seagate [108] produeix un bilió de capçals magnètics per a disc dur.
- Intel [38] llença el microprocessador de 64 bits Intel Celeron, operand a 266MHz amb bus de sistema a 66MHz. Incorpora 7,5 milions de transistors i es fabrica amb tecnologia de 0,25 micres. Està dissenyat per ordinadors de baix cost.
- AMD [126] anuncia 3DNow, una tecnologia propietària que incorpora 21 instruccions noves dintre de l'arquitectura del processador x86 que millora les funcions 3D.
- Es fa el primer anunci de la tecnologia sense fils Bluetooth [142] per a xarxes d'àrea personal. Opera en banda gratuïta de 2,4GHz i promet velocitats de 1Mbps en distàncies de fins a 10 metres.
- S'instal·la el cable ACI per la companyia Global Crossing entre Brookhaven (Regne Unit), Whitesands (Regne Unit), Beverwyjk (Països Baixos), Sylt (Alemanya) i Brookhaven (Estats Units), amb una distància total de 14000 Km i amb un ample de banda de 4 x 10Gbps.
- PCMCIA [104] anuncia la introducció d'un nou estàndard per a PC Card petita, que és un 42% més petita, a 16 bits i totes les demes característiques que el seu estàndard de mida complerta. Està enfocat a cobrir el mercat de les càmeres digitals, computadores portàtils i PDAs [143]. Es presenten en tres formats: Tipus I (45mm x 42,8mm x 3,3mm), Tipus II (45,00mm x 42,8mm x 5,0mm) i Tipus III (45,0mm x 42,8mm x 10,5mm).
- Surt en el mercat el microprocessador Intel [38] Pentium II Xenon, a 400MHz, amb bus de 100MHz i 64 bits, per a ús en servidors i estacions de treball de rang mitjà i superior.
- Surten al mercat Microsoft [84] Windows 98 i CE 2.1 [101].
- Apple [40] presenta una nova línia de computadors, la iMAC, amb una aparença que suposa una revolució en el disseny de computadors. Estan equipats amb un processador de 64 bits Power PC 750 a 233MHz, 1 MB de ROM [44], RAM [43] expandible a 256MB, sens unitat de disc, 4GB de disc dur, CD-ROM 24x, monitor a color de 15" i 1024 x 768 píxels [100] de resolució, so estèreo de 16 bits, Ethernet de 10/100Mbps i tot a un preu de 1299 $.
- Apareix i es promociona el Bus Sèrie Universal (USB) [144].
- AMD [126] presenta les versions del processador AMD-K6-2 a 366MHz, 380MHz i 400MHz amb 3DNow!.
- Compaq [83] desenvolupa junt amb Panasonic el primer sintonitzador de televisió d'alta definició per a PCs.
- S'instal·len els segments 8 i 9 del cables EL SEA-ME-WE 3 (South-East Asia – Middel East – Western Europe 3). El segment 9 té un ample de banda de 2 x

20GHz amb 1600Km a Penmarch (France) i Sesimbra (Portugal). El segment 8 té un ample de banda de 2 x 20Gbps i 5300Km entre Sesimbra (Portugal), Tetuan (Marroc), Mazara (Itàlia), Chania (Grècia), Marmaris (Turquia), Yeroskipos (Xipre), i Alexandria (Egipte).

- Arriba al marcat l'equipament per a DVD-Ram [145] i DVD-R [146] . També s'alliberen les eines de creació per DVD- vídeo / ROM [147].

Any 1999

- En una presentació del Fòrum de desenvolupament de Intel, es mostra el prototip d'un processador que funciona a 1GHz i està fabricat amb tecnologia de 0,25 micres. També ve acompanyat de tècniques noves de refredament.
- Intel [38] treu el microprocessador Pentium III, que treballa a 450 i 500 MHz. Disposa en el seu interior de 9,5 milions de transistors, basat en tecnologia de 0,25 micres, bus de 64 bits a 100MHz. Té 70 instruccions noves específiques per millorar i ajudar en el disseny d'aplicacions de flux d'àudio, vídeo 3D i aplicacions de reconeixement de veu. Aquestes instruccions es coneixen com a Extensions de flux SIMD.
- Finalitza la instal·lació del cable SEA-ME-WE 3 (South – East Asia – Middle East – Western Europe 3) que passa per a 34 paisos i 40 punts de d'Alemanya, Bèlgica, Regna Unit, el Mediterrani, India, Indonèsia, Austràlia fins a Japó. Té una longitud total de 39000Km. Porta 20Gbps a través de WDM (Wavelength – Division Multiplex) de 4 vies, en dos parells de fibra òptica.
- Intel [38] anuncia la sortida del microprocessador Celeron a 466MHz i el conjunt de circuits Intel 810 integra innovacions com la integració d'àudio, mòdem i DVD [125] per software, juntament amb gràfics AGP 3D [132] amb qualitat AGP 2x [132].
- Microsoft [84] treu el nou Windows 98 SE (segona edició) [101].
- Surt al mercat el processador Intel [38] Mobile Pentium II a 400MHz, amb tecnologia de 0.25 o 0,18 micres, tots dos amb 7,4 milions de transistors, destinats al mercat del portàtil.
- Compaq [83] treu el seu projector portàtil MP1600.
- Surt al mercat el processador Intel [38] Mobile Pentium III, a 400, 450, o 500 MHz, amb 28 milions de transistors, Basats en tecnologia de 0.18 micres, bus a 100 ó 133 MHz i de 64 bits. També es presenta el nou Pentium estàndard a freqüències de 500, 533, 550, 600, 650, 667, 700 i 733 MHz.
- EEE [148] presenta l'estàndard 802.11b per a xarxes d'àrea sense fils (Wireless [103] LAN[149], WLAN [150]),de 11Mbps a la banda ISM a 2,4GHz, amb 12 cm de longitud d'ona, la freqüència de ressonància de la molècula d'aigua, també utilitzada en forns microones. Apareixen el mercat molts productes per equip d'oficina i també no tarden amb aparèixer productes WLAN [150].
- Motorola [81] presenta el dispositiu de ma i1000plus, el primer que integra un telèfon digital, radio de dues vies, cerca persones alfanumèric, un micro

navegador de Internet, correu electrònic, fax i capacitat de missatges de dues vies. Usa tecnologia digital de comunicacions iDEN de Motorola.

- Sanyo Electronic [151] i Eastman Kodak Company [152], treuen la primera pantalla OLED de matriu activa a color de 2,4".

Any 2000

- Comencen les operacions en una part de la xarxa de cable China – Estats Units, la primera xarxa de fibra òptica submarina que transferirà veu, dades i vídeo directament entre aquests dos països. La xarxa té dos punts terrestres a China (Chongming i Shantou), dos en els Estats Units (Bandon a Oregon i Sant Luis Bisbe a Califòrnia), dos a Japó, un a Guam (Corea) i un a Taiwan. L'ample de banda és de 80Gbps. El creuament del Pacífic 1 és de 640Gbps, i el tram de Japó a Estats Units és també de 640Gbps.
- IrDA [141] publica les especificacions i perfils per a rellotges de polsera IrDA (IrDA Infrared Wrist Watch, IrWW [153]). També publica l'especificació de l' interfície Serial per el control de transceptors. També publica el perfil d'aplicació d'apuntar i disparar JetSend [154] i la nota d'aplicació de fotografia digital JetSend.
- S'instal·la el cable Atlantis-2 entre Las Toninas (Argentina), Rio de Janeiro (Brasil), Fortaleza (Brasil), Dakar (Senegal),n Praga (Illes Cap Verd), El Medano (Illes Canàries), Funchal, Illa Madeira (Portugal), Conil (Espanya) i Lisboa (Portugal), cubrintn una distància de 13000Km i amb un ample de banda de 2 x 20Gbps.
- Seagate [108] introdueix en el mercat el primer disc dur a 15000 RPM, el Cheetah x 15.
- Peter Thiel i Max Levchin funden PayPal Incorporated a Mountain View, Califòrnia. Inicien treballs de pagament electrònic a través de Internet.
- Microsoft [84] treu el Windows 2000 [101].
- Intel [38] treu al mercat el Pentium III a 1GHz.
- Una companyia Israelita anuncia la creació d'una càmera de vídeo de la mida d'una píndola. De 1 x 0,5 polsades, porta en el seu interior un LED [156] de llum blanca, un transmissor de ràdio, una pastilla d'imatge CMOS [155] i bateries. Té l'habilitat de retransmetre imatges mentre viatge a través del tracte digestiu.
- Surt al mercat el microprocessador mòbil de baix voltatge Celeron, que opera a 500MHz, construït amb tecnologia de 0,18 micres i funciona a 1,35v i un consum menor de 2 watts. També es presenta el Pentim III mòbil de baix consum a 600MHz.
- Surt al mercat Microsoft Windows ME [101].

- Motorola Computer Group [81] treu l'arquitectura de IP commutat que permet solucions d'infraestructura punt final a punt final (End – to – End).
- Compaq [83] expandeix la seva línia iPAQ [157] amb cinc nous productes, incloent el dispositiu de Internet a casa i el reproductor personal d'àudio.
- S'inicia la instal·lació del cable Cruce Sur que connecta Austràlia, Nova Zelanda, Fiji, Hawaii i la costa oest dels Estats Units, cobrint una distància de 30500 Km i amb un ample de banda de 120Gbps a Austràlia i 160Gbps de Hawaii a Califòrnia.
- Surt al mercat el microprocessador Intel [38] Pentium – 4 que treballa a 1400 ó 1500 MHz, fabricat amb tecnologia de 0,18 micres i CMOS [155]. La mida del troquel és de 217 mm^2 i té un consum de 50w. Entrega un rendiment de 535 SPECint2000 i 558 SPECfp2000.
- Seagate [108] treu al mercat el disc dur Barracuda de 180GB.
- S'instal·la el cable PAC per Global Crossing entre Grover Beach (EEUU), Tijuana (Mèxic), Mazatlàn (Mèxic), Fuerte Amadour (Panamà), Puerto Viejo (Veneçuela), St. Croix (EEUU) i Illes Verges cobrint una distància total de 9500 Km i amb un ample de banda de 2 x 10Gbps.

Any 2001

- AMD [126] presenta el microprocessador Duron a 850MHz. Suporta l'arquitectura de memòria unificada (UMA), està encapsulat per a suport A i té bus de 200MHz.
- Surt al mercat el processador de Intel [38] Pentium III de consum energètic ultra baix: 1 Watt i funciona a 1,1v i 500MHz. En mode d'optimització de bateria és capaç de funcionar a 1v i consumir 0,5 watts.
- A Tokio, Hitachi [137] anuncia el desenvolupament del circuit integrat per a identificador per radio freqüència més petit del mon, sota el nom de Mu. Retransmet en el rang dels 2,45Ghz, té 128 bits de ROM [44], i les seves mides són de 0,4mm de costat per 0,15mm de gruix. És resistent a factors climàtics i es pot incrustar en un paper.
- Advanced Micro Devices (AMD) [126] treu la seva família de processadors Athlon XP. Els models van de 1,33GHz a 1,53MHz i els anomena com Athlon XP 1500+, 1600+, 1700+ i 1800+. Estan construïts amb arquitectura QuantiSpeed.1.53GHz. AMD valora més el rendiment total que la velocitat de rellotge a la que funcionen.
- Microsoft [84] treu el nou sistema operatiu Windows XP.
- Surt la versió del Nou Testament més petita del mon. Té de mides 5 mil·límetres quadrats. Està fet amb un pastilla de silici cristal·lí i lletres amb or de 24 quirats. Cada lletra mesura 4 micres d'alçada, el mateix que una cèl·lula vermella de la sang, i en total hi ha 180568 paraules.

Any 2002

- Casio Computer [158] anuncia que ha tingut èxit en el desenvolupament de cel·les d'energia petites i alt rendiment, amb un mètode que pot ser utilitzat en equips portàtils. El dispositiu és un micro reactor format de silici que provoca una reacció química que obté hidrogen a partir de metanol en presència d'un catalitzador amb un rendiment de més del 98%.
- Palm [159] treu la versió beta del seu sistema operatiu Palm OS versió 5.0 [160], que integra noves funcions per a multimèdia, comunicacions i seguretat. També dona suport per a connexions sense fils 802.11b i millora la qualitat del so i resolució de pantalla a 320 x 320. Dona suport per a l'arquitectura de processadors ARM.
- Intel [38] anuncia el Pentium 4 a 2,53GHz, amb bus a 533MHz mitjançant un rellotge a 133MHz i un quadriplicador màster. Els circuits de suport per aquest microprocessador és el nou model 850e. En aquests moments , l'únic problema està en que no hi ha encara memòria disponible per aquesta nova tecnologia.
- Kingston Technology Company [161], anuncia la disponibilitat de mòduls de memòria RIMM a 1066MHz per tal de donar suport en els nous microprocessadors.
- Microsoft [84]treu la primera versió del paquet Service pack 1 per a Windows XP. Compte amb modificacions per eficiència amb seguretat, compatibilitat i actualitzacions. També compta amb elements que permeten amagar el Internet Explorer, el reproductor multimèdia, el Messenger i l'Outlook Express.
- Nvidia [131], fabricant de tecnologia de vídeo 3D, presenta Cg, el primer llenguatge de programació per a desenvolupadors de 3D.
- Western Digital [110] presenta el disc dur Caviar a 200GB i 7200 RPM. Està format per discs de 60GB cadascun
- A la universitat de Princenton, el Dr. Stephen Y. Chou, director del laboratori de Nanoestructures anuncia ena alternativa a la nanotecnologia, mecànica, per a substituir la fotografia utilitzada per a la construcció de circuit integrats. Aquesta nova tecnologia consisteix en passar un raig làser ultraviolat a través d'un cristall de quars amb el motlle del circuit. El cristall és transparent al raig ultraviolat però fon la superfície de silici lo suficient per a imprimir el circuit. Amb aquesta tecnologia es pot arribar amb un detall de nivell de 10 nanòmetres.
- La memòria Ovònica [162] unificada es considera una alternativa a la memòria Flash, utilitzada en dispositius sense fils, que es desgasta amb el seu ús. També es pensa que pot desplaçar a la memòria DRAM [163] i SRAM [164]. També entren en consideració altres tecnologies com la RAM magnètica, MRAM [165] i la ferro – elèctrica FRAM [166] o FeRAM.
- AMD treu al mercat el seu primer microprocessadore amb tecnologia de 0,13 micres per a servidors i estacions de treball. Es tracta del Atrhlon MP 2200+.

Any 2003

- Intel [38] anuncia la seva nova marca Intel Centrino, per a nova tecnologia mòbil sense fils. Està basada en un microprocessador de nom Banias. Disposa de capacitat per a connectivitat a xarxes 802.11 (Wi-Fi).
- Casio Computer [158] presenta una cel·la d'energia per a computadores portàtils que anomena Micro – reformadora. Té la mida d'un segell i pot generar electricitat per a 20 hores d'ús d'una computadora portàtil, comparat amb les 4 a 6 hores per a una bateria de ió – liti.
- Nokia [122] anuncia el naixement de Java Multimèdia Mòbil [120], junt amb la introducció al mercat del seu telèfon mòbil Nokia 3650. El desenvolupament de les API estàndard per a Media Mòbil és fan a través del Procés de la Comunitat Java (JCP) i dirigida per Nokia. Ofereix per el desenvolupador de software, noves capacitats per a àudio i vídeo.
- A Ciutat de Mèxic, Solucions Aplicades i Solucat Mèdica [167] presenten el VeriChip [167]. Es tracte d'una micropastille de silici de la mida d'un gra d'arròs que és capaç d'emmagatzemar i transmetre informació. El dispositiu serà usat per la identificació de persones. Als Estats Units s'utilitza per identificació de mascotes.

Any 2004

- S'acaba l'estàndard 802.11i i és ratificat en una reunió del comitè d'estàndards IEEE [168] preparant el camí per a millorar la seguretat en xarxes sense fils.
- Intel [38]Corporation anuncia una nova família de processadors basats en la tecnologia XScale de Intel, que pot manegar múltiples formes d'accés de banda ample sense fils, amb suficient poder de còmput per a proveir a telèfons cel·lulars amb capacitats de videoconferència amb moviment complet i a les PDAs [143] amb reproducció de vídeo amb qualitat DVD [125].
- La divisió de dispositius d'emmagatzematge de Toshiba [169] anuncia el desenvolupament d'un disc dur de 0,85 polsades, el primer en oferir capacitat de varis gigabytes en un dispositiu de factor de forma per sota de la polsada. Pot ser de gran utilitat en els mercats telefònics, reproductors de àudio digital, PDAs [143] i càmeres digitals.

Any 2005

- S'aproven les especificacions del estàndard WUSB [170], que obre les portes a una nova era en la qual es podran eliminar els cables per a les connexions dels perifèrics. Aquest estàndard (WUSB 802.11n) anuncien velocitats de fins a 135Mbps. Manté el mateix ús i arquitectura que el USB amb cables amb una connexió d'alta velocitat del amfitrió al dispositiu.
- AMD [126] presenta els seus nous microprocessadors amb dos nuclis. Aquesta nova tecnologia permet col·locar en un sol processador el doble de capacitat de treball que en els processadors estàndards. Segons AMD, tenen un 80% més de

capacitat de procés que els models amb un sol nucli. Els anomena Athlon64 x2. Segons la companyia, aquest processador donarà a les computadores la capacitat de true multi – tasking, amb lo qual , cada aplicació pot corre en un processador amb independència de l'altre, sense que es produeixin caigudes generals de rendiment.

- Intel [38] anuncia el Pentium D amb dos nuclis.
- Les connexions de Internet [102] a través de banda ampla (ADSL [171]) per via telefònica podran multiplicar per deu la seva velocitat de connexió i oferir per la mateixa xarxa serveis de vídeo i veu a partir de una definició de normes tècniques decidida per la Unió Internacional de Telecomunicacions (UIT[172]). La de coure, on avui circula la telefonia i Internet de banda ample, televisió d'alta definició, vídeo a la carta, videoconferència, accés a Internet d'alta velocitat i veu IP entre d'altres serveis. Aquesta tecnologia compres una velocitat de fins a 100Mbps.
- Nvidia [131] presenta la targeta de vídeo GeForce 7800 Pro, per a molts, la molts potent del mercat. Aquesta placa ja nomes ocupa un slot dintre del PC. Amb total, els chips que la integren, contenen 302 milions de transistors (per exemple, el processador Athlon x 2 té 233 milions de transistors). Tota la targeta corre a 430MHz i suporta 512MB de memòria a 1,2GHz. L'slot és l'estàndard PCI Express x 16.
- Microsoft [84] anuncia la sortida en dates pròximes d'un nou sistema operatiu que l'anomenaran Longhorn.
- Apple [40] treu una nova versió de iPod [173] que serà capaç de reproduir arxius de vídeo digital, des de programes de televisió fins a vídeos musicals.
- Microsoft i Intel recolzen el desenvolupament del format HD-DVD [174] , un dels suports que intentarà desplaçar als DVDs [125] actuals. Abandonen així a Sony [74] en el desenvolupament del seu Blu-Ray Disc [175].
- Microsoft [84] anuncia que llançarà al mercat varies versions del nou sistema operatiu Vista (abans amb el nom de Longhort).
- Samsung [176] desenvolupa un nou chip flash de memòria que arribarà fins a 32GB.
- Internet [102] enregistra més de 82 milions de dominis.
- L'enciclopèdia en línia Wikipedia aspira a convertir-se en els pròxims 10 anys en una xarxa mundial i en qualsevol idioma.

Any 2006

- Microsoft [84] anuncia que deixarà de donar suport a Windows 98 i Windows ME. També treu la primera versió beta pública de Windows Vista.
- A l'estat espanyol es posa en marxa el DNI electrònic.
- Investigadors de la Universitat de Califòrnia i de Intel desenvolupen un nou chip de transmissió de dades làser. Pot arribar a tasses de transferència de fins a 40Gbps i a distàncies de varis metres.

- Intel [38] , junt amb altres empreses està treballant amb nanotubs de carbono i a aconseguit desenvolupar un prototip que interconnecta transistors. Aquests tubs microscòpics poden transmetre l'electricitat molt millor que els metalls i els electrons no es dispersen ni boqueixen. L'únic problema és que són molt complicats de construir en massa. També un cop creats, n'hi ha que tenen un bon comportament mentre que d'altres no.
- S'han fet importants progressos amb el vídeo en 3D. El producte desenvolupat s'anomena Cheoptics 360 [177]. Es tracta d'imatges gravades a través d'una especia de piràmide transparent de 4 costats, desenvolupada per enginyers i dissenyadors danesos. Això sembla ser substituirà les pantalles 3D lenticulars, hologrames i projectors 3D "reals".
- Sony treu el seu e-book [178] amb llibreria online pròpia.
- S'està investigant a l'escola de medicina de Harvard amb unes proteïnes anomenades bacteriodopsines que són excitables amb llum i que es troben a les membranes d'un microbi de les salines. Aquestes proteïnes canvien a molècules intermèdies amb el contacte amb la llum. A la pràctica tenen tendència a tornar al seu estat original passades unes hores. Les probes que fan estan orientades a modificar-l'hi el seu ADN per tal de que siguin capaces de conservar el seu estat entremig en el transcurs de forces anys. Es podrien aconseguir capacitats de 50 terabytes.

Any 2007

- Un equip internacional de científics aconsegueix realitzar el primer càlcul matemàtic, consistent en una factorització d'un número petit, utilitzant un computador quàntic.
- Enginyers de IBM [30] han inventat una nova forma de CPU [179]que utilitza impulsos de llum en lloc de impulsos elèctrics per a moure la informació entre els nuclis d'un chip. La tecnologia és cent cops més ràpida que l'actual. Ha estat bategada amb el nom de Silicon Nanophotonics i un cop implementada podrà reduir la mida de les súper computadores a més o menys la mida d'un Laptop.
- Per primer cop s'ha aconseguit demostrar la viabilitat de realitzar una connexió via làser [180] a través de 1,5 milions de kilòmetres.
- LG [181] ha desenvolupat la primera pantalla flexible del mercat a color. Té 14,1 polsades (A4). Es pot veure amb claredat en angles de fins 180º. El número de colors és de 4096.
- Intel [38] treu en el mercat aquest any el processadors Core 2 Extreme QX6850. Funciona a 3GHz, el bus a 1333MHz i 8MB de memòria cau L2. El Core 2 Quad Q6700. Funciona a 2,66GHz, 1066MHz el bus, 8MB de memòria cau L2. El Core 2 Duo E6850 de doble nucli a 3GHz, bus a 1333MHz, memòria cau L2 de 4MB. El Core 2 Duo E6750 amb doble nucli a 2,66GHz, 1333MHz de freqüència de bus i 4MB de memòria cau. Finalment el Core Duo E6550. És el menys potent. Té doble nucli a 2,33GHz, bus a 1333MHz i memòria cau de 4MB.

Any 2008

- Graphics Lab [182] a La universitat de Southern Califòrnia construeix un projector 3D amb 360 graus de visualització que no necessita ulleres per a veure imatges interactives.
- El Roadrunner [183] és el computador més potent del moment, construït per enginyers de IBM [30] i el Laboratori Nacional dels Àlamos. Està equipat amb 12000 processadors tipus Cell, que són el dissenyats originalment per la consola de Sony [74] PlayStation 3, i acaba de batre la marca del petaflop (mil bilions) d'operacions per segon.
- Científics del grup IBM [30] han desenvolupat un nou chip de memòria flash que permet guardar en aparells com telèfons mòbils i reproductors de mp3 centenars de vegades més informació que en l'actualitat.
- Surt la versió 8.04 de Ubuntu [184], un sistema operatiu basat en Debian [185] de Linux [107] que ha tingut una gran acceptació en els usuaris de PC. Windows vista no ha tingut massa èxit i es veu superada en el seu ús per el Windows XP Service Pack 3.
- Intel [38] llença al mercat una nova gama de processadors que anomena Intel Atom. Són molt petits i estan dissenyats per equips MID i netbooks. Estan també disponibles també sota la plataforma Intel Centrino Atom. Funcionen a una freqüència de fins a 1,73GHz i poden arribar a 3300 MIPS i 2,1 GFLOPS [186].

Any 2009

- Intel [38] té previst de vendre cables de baix cost i del calibre de la fibra òptica per a interconnecta un PC amb els perifèrics. La companyia va anunciar aquest nou cable que espera que sigui el suficient ment econòmic, ràpid i prim per que es converteixi amb el substitut del cable de coure.
- IBM [30] està cercant diverses fórmules en les que el ADN podria organitzar-se en diferents patrons a la superfície d'un chip per així, actuar com a plataformes en les que podrien dipositar-se milions de diminuts nanotubs de carboni i nanopartícules. Tota aquesta xarxa de nanotubs [187] i nanopartícules podrien actuar com a transistors en els futurs processadors.
- Els científics europeus estan utilitzant les tècniques convencionals de producció de chips per crear circuits que imiten l'estructura i funció del cervell humà. Aquest prototipus té nomes 384 neurones i 100000 sinapsis, però la última versió ja conté 200000 neurones i 50 milions de sinapsis.
- LG Electronics [181] ha desenvolupat un rellotge que és també un telèfon mòbil amb vídeo. El seu nom comercial és LG-GD910.
- AMD [126] presenta el seu nou microprocessador de 6 nuclis. Els denomina Opteron i també són coneguts com Istanbul. Estan pensats per els servidors i

cloud computing. El model Six – Core Opteron EE 2419, que funciona a 1.8Ghz, té un consum de 40 watts. Estan construït amb tecnologia de 45nm.

- Intel [38] treu al mercat la família Xeon 5500 amb Micro arquitectura Nehalem. Estan construïts amb tecnologia de 45nm. El seu ús està orientat a servidors . Un exemple d'aquests models és el Intel Core i7.
- Microsoft [84] treu al mercat el nou sistema operatiu Windows 7 [101].

Any 2010

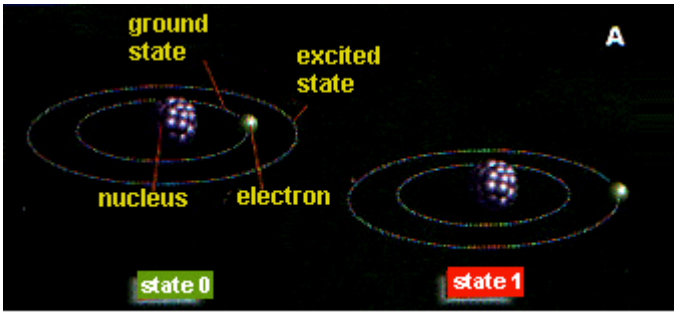
- Una investigació de la Universitat Rice que aprofita les amplies capacitats del grafè podria conduir a aplicacions de circuits molt més compactes i versàtils que el que és avui en dia factible amb les tecnologies a base de silici. Els amplificadors de triple mode amb un sol transistor basats amb grafè [188], la forma del carboni d'un àtom de gruix, podrien convertir-se amb elements clau en els futurs circuits electrònica.
- Científics del Robotics Institute [189] de la universitat de Carnegie Mellon, en el Estats Units, han desenvolupat una tecnologia de projecció que permet generar imatges mòbils 3D sobre capes d'aigua, amb alta resolució. Denominat Acualux 3D [190], el sistema consisteix en generar línies coordinades de gotes, sobre les que incideixen de forma alternada la llum d'un projector.
- Un grup d'investigadors del CSIC [191] ha demostrat, en una sèrie d'experiments, el resultat dels quals s'han publicat a la revista Small, que l'actual tecnologia ja permet crear chips de silici, més petits que cèl·lules vives i introduir-les en elles. Les aplicacions que poden derivar-se encara, però, són llunyanes.
- En aquest any podem destacar els microprocessadors de quatre nuclis de AMD [126] com el Athlon II X4 645 que funciona a 3,1GHz, usa una tensió de 0,875 – 1,425 volts, amb un consum de 95 Watts i té memòria cau L2 4 x 512KB. La tecnologia de construcció és de 45nm. Aquest seria un exemple de model més avançat encara que se'n fabricant molts d'altres amb igual o menys nuclis per a cobrir diferents prestacions.
- Intel Corporation [38] també desenvolupa microprocessadors molt potents i de diversos nuclis. Un dels millors és el model Core i7 980X que funciona a una freqüència de 3,3GHz, disposa de 6 nuclis, té memòria cau L2 6 x 256KB i L3 12MB, una tensió d'alimentació de 0,8 – 1,375 volts i un consum de 130 watts.
- Cal destacar per últim, que en el transcurs d'aquests últims anys, es produeixen inversions amb el desenvolupament de intel·ligència artificial i es construeixen robots que cada vagada tenen més autonomia i són capaços de desenvolupar tasques quotidianes pròpies del esser humà.

Annex IV

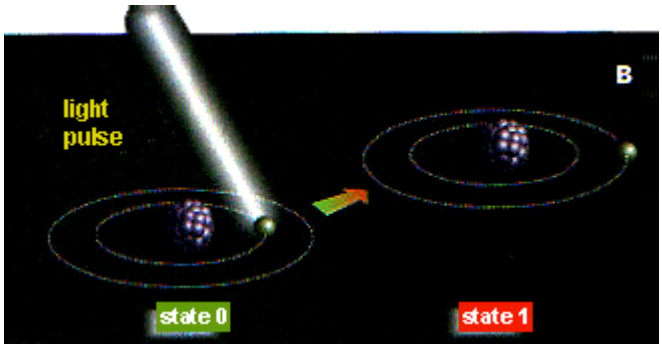
Una manera simple de factoritzar un número enter N es basa en comprovar el resta de la divisió de *N* per alguns números *P* menors que l'arrel quadrada de *N*. Si el resta és 0 arribem a la conclusió que *P* és un factor. Aquest mètode de fet, és molt ineficient: amb un equip capaç de provar amb *10 ^ 10 P* números per segon, el temps mitjà per trobar el factor en un número llarg de 60 xifres supera l'edat del univers. En lloc d'aquest mètode de la divisió, els ordenadors quàntics es basen en una tècnica diferent per tal de realitzar la factorització de forma eficient. De fet, és possible demostrar que factoritzar un número es pot relacionar amb el problema d'avaluar el període d'una funció. Per tal d'explicar com funciona aquest mètode, usem un exemple simple i imaginem que volem trobar els factors primers de *N = 15*. Per això, prenem un número al atzar més petit que *N*, per exemple *a = 7*, i definim una funció *F(x) = 7 ^ x mod 15*. Aquesta funció eleva 7 els enters *x* i pren el resta de dividir el resultat per 15. Per exemple, si *x = 3, f(x) = 13*, perquè *7 ^ 3 = 343 = (15 x 22) + 13*. Les matemàtiques demostren que *f(x)* és periòdica i el seu període *r* pot estar relacionat amb els factors de 15. Amb aquesta informació, la computació dels factors de *N* nomes requereix avaluar el màxim comú divisor de *N* i *a ^ r/2 +-1*.En el nostre exemple, el càlcul del màxim comú divisor de 15 és: 50 = 7 ^ 4/2 + 1 (o 48 = 7 ^ 4/2 -1) retorna de fet, els valors 5 (o 3), que son els factors de 15.
És evident que els computadors clàssics no poden usar aquest mètode ja que trobar el període de f(x) requereix avaluar la funció moltes vegades. De fet els matemàtics ens diuen que el promig de la avaluació necessària per a trobar el període és del mateix ordre del nombre de divisions necessàries amb el mètode simple que hem explicat al principi. Amb un computador quàntic, la situació és completament diferent: mitjançant l'establiment d'un registre quàntic en una superposició d'estats que representen 0, 1, 2, 3, 4, ... és possible calcular de forma simultània o de cop els valors f(0), f(1), f(2), ... Aquests valors es codifiquen en els estats superposats d'un registre quàntic, i el període de recuperació d'aquestos es fa en un pas (conegut com Transformada Quàntica de Fourier), que també es pot realitzar d'una manera molt eficient en un computador quàntic.

Annex V

Qualsevol sistema quàntic amb per lo menys dos nivells discrets d'energia i prou separats , és un candidat adequat per a ser un qubit. Fins ara, els qubit més populars entre els investigadors experimentals són àtoms de rubidi (experiments ENS) o de beril·li (experiments del NST). En un àtom, els nivells d'energia dels electrons són discrets. Dos d'ells poden ser seleccionats i etiquetats com 0 i 1 lògics. Aquets nivells es corresponent als estats d'excitació específica dels electrons en el àtom. Per a veure com és possible controlar els dos valors lògics, simplificarem la situació i considerem un àtom idealitzat, amb un sol electró i dos nivells d'energia, un estat fonamental (identificat amb el valor 0) i un estat excitat (identificat amb el valor 1). Es mostra a la següent figura:

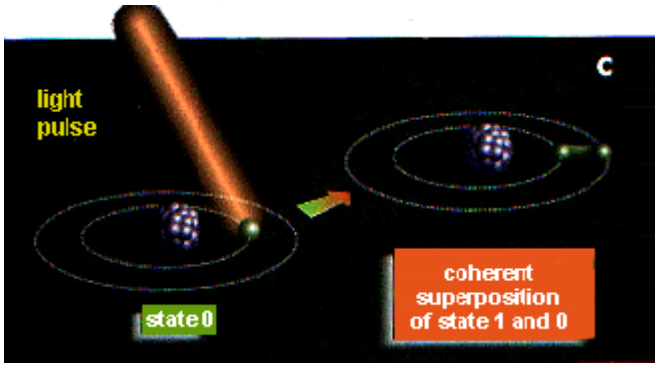


Imaginem que el àtom es troba en el estat inicial 0 i volem efectuar l'operació lògic NOT. L'operació lògica NOT només nega el valor lògic inicial de manera que converteix un 0 en un 1 i un 1 en un 0. Això es realitza fàcilment amb els àtoms. Al incidir sobre l'àtom amb un pols de llum d'intensitat, longitud d'ona i temps adequat (la longitud d'ona té de coincidir amb la diferència d'energia entre els dos nivells d'energia del àtom), és possible obligar en els electrons a canviar de nivell energètic. En el nostre cas, l'electró inicialment en l'estat fonamental absorbirà part de l'energia del pols de llum i canviarà de nivell energètic passant el nivell d'excitació i per tant estat lògic 1. Si l'electró inicialment s'hagués trobat en l'estat 1, el pols de llum el portaria cap el nivell energètic corresponent a l'estat 0. Ho podem veure a la següent figura:



La imatge ens mostra com en viant un pols de longitud d'ona apropiada a l'àtom, es pot induir una transferència d'un electró, d'una òrbita a una altre. Si l' intensitat i durada del pols han estat calculats curosament, aquest circuit actua com una porta lògica quàntica amb la funció NOT: l'electró es transfereix d'una òrbita a una altre,

seguint la lògica d'aquesta porta 0 <---> 1.
La lògica NOT, descrita anteriorment, es pot entendre amb termes completament clàssics, però no obstant, també es poden realitzar operacions lògiques purament quàntiques sens analogia amb les clàssiques. Per exemple, usant un impuls de llum de la meitat de durada de la necessària per a realitzar la funció lògica NOT, l'electró es queda a mig camí entre els dos estats lògica. Que significa això? En essència, això significa que l'operació 0 ----> 1 s'ha realitzat de forma parcial i l'estat del àtom després del mig impuls no és ni 0 ni 1, sinó una superposició quàntica coherent de ambdós estats (figura c). Al igual que el fotó que viatge a través de les rutes A i B, l'electró de l'àtom està tant en l'estat 0 com 1. Actuen sobre l'àtom que es troba en aquest estat aplicant un altre mig impuls de llum es completa l'operació NOT, i l'acaba de posar en l'estat 1. Aquesta operació que s'obté com a resultat d'aplicar aquests dos mitjos impulsos i que és purament quàntica, normalment es denomina arrel quadrada de NOT. Amb l'ús d'aquests tipus de mitjos impulsos és possible crear superposicions d'estats en la memòria d'una computadora quàntica (la memòria està formada òbviament per àtoms), obrint així noves vies per a realitzar càlculs. Altres operacions lògiques, per un general, impliquen operacions físiques més complexes en més d'un qubit.



A la figura podem veure gràficament el concepte del mig impuls. Aplicant el mig impuls (meitat d'intensitat o meitat de duració) necessari per a l'operació NOT, és possible implementar un nou tipus de porta quàntica: l'operació nomes s'executa a la meitat i l'electró inicialment en l'estat 0 es transfereix a una superposició coherent d'estats 1 i 0. L'electró està en ambdós estats. L'aplicació d'un segon mig impuls completa l'operació i posa l'electró a l'estat 1. A aquesta operació se la denomina arrel quadrada de NOT degut a la consecució de les dues meitats del impuls necessàries per a completar el total de l'operació. Aquest tipus de portes són purament quàntiques ja que no tenen equivalent amb les clàssiques.

Annex VI

L'objectiu d'aquest annex és el d'aportar una mica de llum a una sèrie de conceptes, que ens poden ajudar a digerir una mica més bé la secció que explica en formalismes matemàtics els diferents aspectes de la base de la computació quàntica. Aquí no veurem pràcticament matemàtiques però si una sèrie de conceptes que ens ajudaran a entendre una mica certes expressions d'aquelles seccions.

Estat quàntic

Una definició d'estat quàntic el descriu com un objecte matemàtic contenidor de tota la informació disponible sobre un sistema físic. Si un sistema es troba en un determinat estat E ho denotarem com |E>. Per tant si diem que una cosa X es troba en l'estat |A> estem afirmant que coneixem o tenim tota la informació sobre X com a sistema. Aquest tipus de definició suposa un grau d'abstracció molt alt, però quan el definim, significa que som capaços o partim de la base que podem definir |A> amb molt més detall. En física quàntica, conèixer l'estat dels sistemes no significa predir perfectament el que mesurarem o observarem sinó que la única cosa que podrem predir serà la probabilitat de mesurar un valor determinat de les magnituds observables en el sistema. Amb un exemple ho podrem veure més clar:
Imaginem el nostre sistema com una moneda, i el motiu de mesura és veure, en el moment que la mirem, si és cara o bé és creu. La moneda la tenim tancada dintre d'una caixa. Podríem pensar equivocadament que el sistema es pot trobar nomes en dos estats: |cara> i |creu>. Amb això estem confonent la moneda amb l'estat. L'estat no és la moneda sinó la informació que tenim sobre la moneda. Tenim que veure que l'estat de la moneda ja no és el mateix després d'haver-la mirat que abans de mira-la. L'estat depèn de la informació que tenim del sistema i per tant, després d'haver mirat la moneda aquesta informació ha canviat. L'estat de la moneda esta definit en tot moment per nosaltres i és el que ens permet predir el que observarem si mirem la moneda. Si per exemple, prenem la caixa que conté la moneda, la remenem i la tronem a deixar sobre la taula, ara el sistema ha canviat perquè tenim més informació sobre ell i podem definir els estats de |cara>, |creu> i |remenat>, i així, podem tenir molts més estats depenent de la situació inicial del experiment i del que coneixem sobre la moneda. Així podem arribar a concloure que els estats de la moneda poden arribar a ser infinits.

Estats i valors propis

En primer lloc anem a definir que és un observable. Un observable és cada variable que podem mesurar sobre un sistema quàntic. En el cas de la moneda explicat en el capítol anterior, l'observable seria el costat de la moneda. Aquest pot tenir dos valors: o bé cara o bé creu. Per tant, observar la moneda és observar el valor de l'únic observable, el costat de la moneda. Recordem que en observar la moneda el seu estat canvia i de fet, aquesta ja nomes es pot trobar en un dels dos estats |cara> o |creu>, que es corresponent en els dos únics valors possibles del únic observable del sistema, el costat que mostra la moneda. En el món real i han dues raons per les quals l'estat quàntic canvia en observar el sistema:

. El primer és el ja esmentat: Com la informació canvia, el sistema canvia, dons l'estat representa la informació que tenim del sistema.

. El segon és que l'observador del sistema requereix d'una interacció amb aquest i això provoca una modificació (en el cas de la moneda aquesta raó no es manifesta).

Els estats $|cara>$ i $|creu>$ que es corresponent en els possibles valors de l'observable "*costat*" són especials: no canvien en mesurar l'observable i com hem dit, són valors concrets de l'observable. Aquests valors es denominen valors propis o autovalors, i els estats corresponents, auto estats o estats propis.

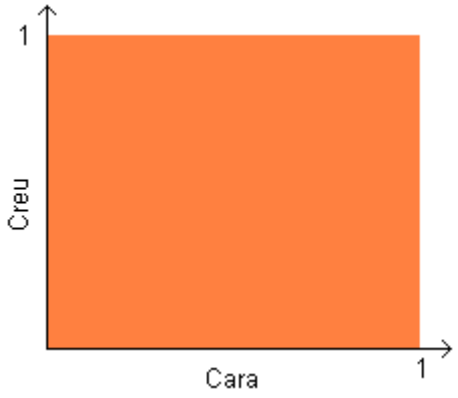
Els auto estats són incompatibles entre sí després de la mesura. La compatibilitat de dos estats $|a>$ i $|b>$ pot expressar-se com $<a|b>$. Els estats $|a>$, $|b>$, etc. es denominen *kets* i els $<a|$, $<b|$, etc. es denominen *bra*. El *bra – ket* $<a|b>$ és un número i el valor d'aquest número ens indica el nivell de compatibilitat dels dos estats. Si $<a|b> = 0$ significa que els dos estats són incompatibles. Si $<a|b> = 1$ són realment el mateix estat. Per tant, *1* representa el *100%* i *0* el *0%*. En general es tractarà d'un número complex i aquesta mesura de *1* ó *0* farà referència en el seu mòdul.

Els estats quàntics poden expressar-se com vectors unitaris i el *bra – ket* $<a|b>$ és el producte intern o escalar d'ambdós. Si el producte escalar és nul, els dos vectors són perpendiculars (per el nostre cas incompatibles); si el producte és *1* és que tenen la mateixa direcció i sentit, és a dir, són el mateix vector (perquè són unitaris). Si no són ni *0* ni *1* seran més compatibles com més petit sigui l'angle que formen.

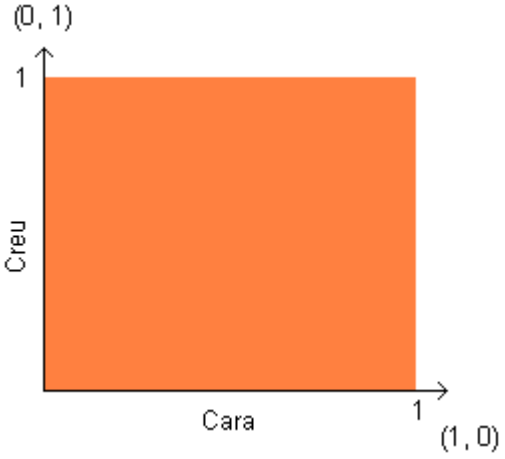
Per tant, el valor de $<a|b>$ és de gran utilitat per veure quant tenen que veure dos estats entre sí. Si $|a>$ i $|b>$ són auto estats del sistema és segur que $<a|b> = 0$: els auto estats són incompatibles, són perpendiculars entre sí.

Superposicions quàntiques

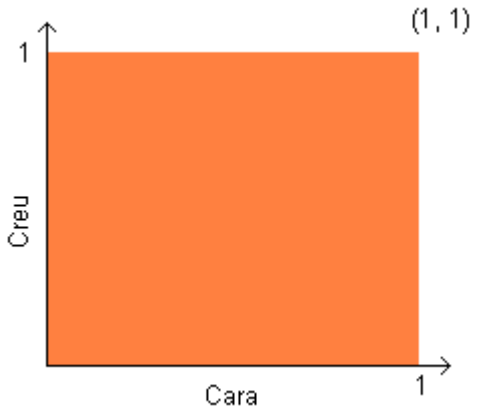
Seguin amb l'exemple de la moneda, direm que els dos auto estats d'aquesta |cara> i |creu>, estableixen les úniques dues possibilitats que poden mesurar-se del observable "costat". Qualsevol altre estat "col·lapsa" cap a un d'aquests dos. Cada un dels altres estats és una mesura de la probabilitat de que, en observar la moneda, aquesta presenti un dels seus dos auto estats. Això ens porta a pensar en els estats de la moneda com superposicions dels altres estats. Per tal de visualitzar aquest fet, usarem un sistema cartesià no euclidià que ens serà d'utilitat gràfica.
Tenint en compta que els estats estan normalitzats, és a dir, que 1 = 100% i 0 = 0% tenim gràficament:



En el quadrat podem representar diferents estats de la moneda.
L'estat |cara> l'hem situat en l'eix horitzontal i el |creu> en el vertical. Les seves coordenades les podem veure a la següent imatge:

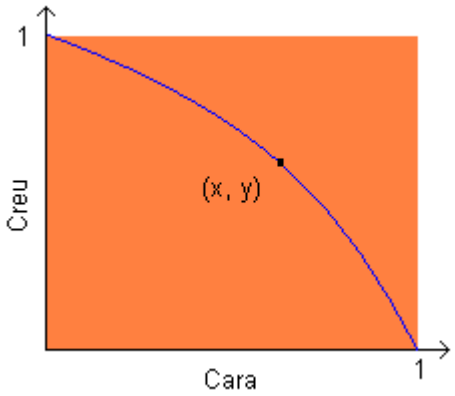


Ara la clau es adonar-se que tots els possibles estats són dintre el quadrat però que no tots els punts del quadrat són possibles estats.

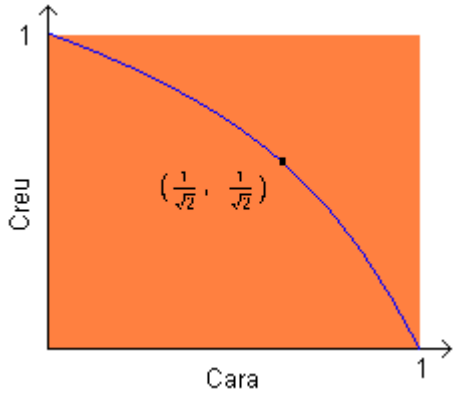


Aquest punt que hem marcat no pot ser un estat possible ja que sinó significaria que aquest estat seria un 100% cara i un 100% creu cosa impossible. Per tant, els possibles estats es limiten al fet que dits estats disten de l'origen de coordenades 1 unitat. Per tant, els possibles estats vàlids tindran d'estar sobre l'arc de la següent figura:

Podem veure que |cara> = 1|cara> + 0|creu>, i |creu> = 0|cara> + 1|creu>. Cualsevol altre estat possible de la moneda es pot expresar com un punt (x, y) d'aquest quadrat. x, y ens indica quanta de |cara> i quant de |creu> té. Per tant, (x, y) representen un estat que podem escriure com: |estat> = x|cara> + y|creu>.



Per tant, el punt que té el mateix de cara que de creu seria: |estat mig> = $\frac{1}{\sqrt{2}}$ |cara> + $\frac{1}{\sqrt{2}}$ |creu>. Qualsevol altre estat es pot escriure com una convinació ponderada dels auto estats.



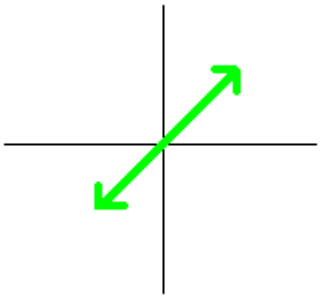
Si tot això ho traslladesim, per exemple, a un dau tindriem que els sis auto valors serien: |1>, |2>, |3>, |4>, |5>, |6>. Tindriem per tant un espai de 6 dimensions. Aquí, qualsevol estat es podria escriure com un punt (x, y, z, p, q, r) que són les coordenades del punt a l'espai de 6 dimensions i aquests punts tindrien que distar 1 del origen. Així, els infinits estats possibles del dau constitueixen una hiper esfera de 6 dimensions formats pels seus auto estats. El punt mig en el qual tots els auto estats tenent la mateixa probabilitat seria ($\frac{1}{\sqrt{6}}$, $\frac{1}{\sqrt{6}}$, $\frac{1}{\sqrt{6}}$, $\frac{1}{\sqrt{6}}$, $\frac{1}{\sqrt{6}}$, $\frac{1}{\sqrt{6}}$). Si avans de llençar el dau (anomenem aquest estat com |previ>) tenim que |previ> = $\frac{1}{\sqrt{6}}$ |1> + $\frac{1}{\sqrt{6}}$ |2> + $\frac{1}{\sqrt{6}}$ |3> + $\frac{1}{\sqrt{6}}$ |4> + $\frac{1}{\sqrt{6}}$ |5> + $\frac{1}{\sqrt{6}}$ |6>.

Si tot això ho traslladem en els infinit esgraons d'energia en l'estat de l'electrò, usan els auto vectors de l'electrò i al construir l'espai conceptual trovem que hi han infinites dimensions, una per a cada un dels seus auto estats. Parlem llavors d'una hiper esfera d'infinites dimensions. Qualsevol estat de l'electrò es pot escriure com |E> = a|E_0> +

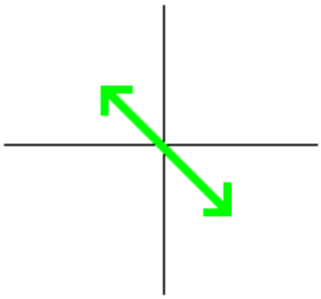
$b|E_0> + c|E_1> + d|E_2>+ \ldots$ Com exemple, si l'electrò es troba a miyges entre els estats $|E_0>$, $|E_1>$, $|E_2>$ el seu estat serà: $\frac{1}{\sqrt{3}}|E_0> + \frac{1}{\sqrt{3}}|E_1> + \frac{1}{\sqrt{3}}|E_2>$.
En general, un estat quàntic es correspon amb un punt qualsevol d'una hiper esfera d'infinites dimensions. Aquests espais conceptuals reben el nom d'espais de Hilbert en honior a la persona que va desenvolupar l'eina matemàtica que els descriu (David Hilbert).

Entrellaçament quàntic

L'entrellaçament quàntic no és un concepta trivial i fàcil d'explicar. A grans trets el podem definir com el fet de que dues partícules que s'han generat en un mateix instant i en una mateixa font, és a dir, que són "bessones" comparteixen informació estiguin a la distància que estiguin, i el fet d'observar l'estat d'una d'elles condiciona un canvi instantani en l'altre. Això significa que podrem predir en un 100% de probabilitat en quin auto estat es trobarà l'altre pertícula. Un exemple que ens pot ajudar a aclarir el concepta el describim a continuació i que de fet, és una de les formes d'aconseguir entrellaçar dues partícules actualment. Certs cristalls, quan reben llum (fotons), alguna vegade absorbeiexen un fotó i a continuació n'emeten dos, la suma de les seves energies és igual a l'energia inicial del fotó que ha absorbit. Aquest procés rep el nom de conversió peramètrica a la baixa. En aquest fenòmen, existeix una propietat molt curiosa, deguda a la conservació del moment lineal, els dos fotons que surten estan polaritzats perpendicularment l'un respecta l'altre, es adir, si la ona electromagnètica que transporta el primer fotó oscila verticalment llavors és segur que la del altre ho farà horitzontalment, i per a qualsevol altre direcció d'oscilació, ho faran perpendicularment l'un de l'altre. Per tant podem dir que els dos fotons apareixent de forma simultània, són idèntics un i altre fins que es realitza una observació sobre algun d'ells. Com els fotons s'allunyent l'un de l'altre pot ser que nomes tingui accés a un d'ells per tal d'observar-lo. Però el que és segur és que si el que observo vec el següent:



llavors l'estat del nostre fotó ha canviat, com també ho ha fet de forma instantànea, l'altre fotó que mai hem vist i podem estar segus de que quan algú l'observi veurà el següent:



Els estats entrellaçats generats d'aquesta manera tenen l'inconvenient de que és mol difícil mantenir-los en aquest estat.

Aquesta informació està extreta i resumida d'uns articles de tota una sèrie que expliquen d'un manera senzilla, sense entrar en formulismes, les bases de la mecànica quàntica. Són molt didàctics i penso de gran utilitat per tenir una bona base conceptual d'aquesta disciplina. Si algun lector sen curiositat per aquet tipus de temàtica l'hi recomano la lectura completa de tots els articles que composen la publicació i que podeu trobar en el següent enllaç: http://eltamiz.com/cuantica-sin-formulas/