Computació i Criptografia Quàntica

Lluís Ametller

Universitat Politècnica de Catalunya

7 de març de 2022

Resum

Apunts de l'assignatura Computació i Criptografia Quàntiques (CCQ), impartida a la Facultat d'informàtica de Barcelona (FIB). Es parteix d'una introducció a la Física Quàntica (FQ) per observar que el microcosmos no es comporta igual que el macrocosmos. L'existència d'estats quantificats dóna lloc al bit quàntic (qubit) que admet superposicions i entrellaçaments amb d'altres qubits. Aquestes propietats, inexistents als bits clàssics, donen lloc a la possibilitat d'encriptar missatges i, també, de fer operacions amb paral·lelisme (quàntic) massiu. Així s'arriba doncs a la Criptografia Quàntica i a la Computació Quàntica. S'analitzen els seus fonaments i els algorismes quàntics que suposen millores substancials respecte als seus equivalents clàssics.

Índex

1 Antecedents de la Física Quàntica

En aquesta secció anirem desgranant alguns dels antecedents de la Física Quàntica.

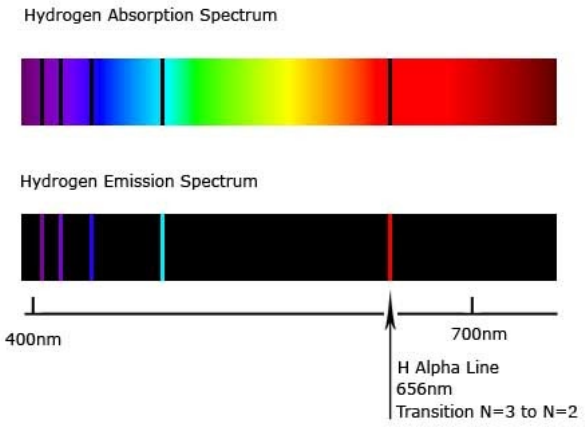
1.1 Espectres d'emissió i d'absorció

Quan un cos s'escalfa, emet llum. Si aquesta es fa passar per un prisma òptic, en dependre l'índex de refracció de la longitud d'ona, es separen les diferents components de la llum emesa. S'aprecien unes ratlles en la pantalla que corresponen a longituds d'ona ben definides, clarament separades entre si. És l'espectre d'emissió del cos. Si això es fa per diferents materials, l'espectre de cada un d'ells és únic i es pot considerar com la seva "empremta dactilar". La composició que es coneix dels estels, quins materials els componen i quin és el seu percentatge, està basat en el coneixement dels seus espectres d'emissió.

De manera anàloga, en cas que s'enviï llum blanca a un material, algunes de les longituds d'ona són absorbides, mentre que la majoria no. Les absorbides es corresponen a les emeses en radiar el mateix objecte.

Les característiques dels espectres d'emissió i absorció no eren enteses per la Física Clàssica, que no pot explicar l'existència de les línies espectrals, i esperaria una distribució contínua dels espectres.

A les figures es mostren el prisma òptic, descomponent llum blanca en els colors que la componen, i els espectres d'absorció i d'emissió de l'hidrogen.



1.2 Ones. Equació d'ones

Les ones són pertorbacions que s'estenen per un medi, transportant energia i quantitat de moviment, però sense transport de matèria. Poden ser ones unidimensionals, com les ones que es propaguen per una corda, bidimensionals, si ho fan en una superfície, com les ones produïdes en tirar una pedra a l'aigua calmada d'un estany, o tridimensionals, com les ones sonores que es propaguen a tot l'espai. Per altra banda, poden ser longitudinals i transversals. En el primer cas, les partícules del medi es

belluguen en la direcció de propagació de l'ona, com quan es comprimeix una molla, mentre que en el segon cas ho fan perpendicularment. Nosaltres ens restringirem només a les ones unidimensionals i estarem interessats en les ones transversals, degut a que les ones electromagnètiques –que poden viatjar en el buit, són camps elèctrics i camps magnètics oscil·lant perpendicularment a la direcció de propagació– ens serviran per tractar la llum.

Tota ona mecànica i també electromagnètica, viatjant en la direcció de l'eix x amb una velocitat v, pot expressar-se en termes d'una funció f que depèn de la posició x i del temps t, que satisfà una equació d'ones

$$\frac{\partial^2 f(x,t)}{\partial x^2} = \frac{1}{v^2}\frac{\partial^2 f(x,t)}{\partial t^2}.$$

Pot comprovar-se que tota funció

$$f(x,t) = f(x \pm vt)$$

és solució de l'equació d'ones. Les funcions $f(x - vt)$ ($f(x + vt)$) corresponen a pertorbacions desplaçant-se en la direcció i sentit positiu (negatiu) de l'eix x.

De totes les possibles solucions de l'equació d'ones, les més importants són les ones harmòniques simples. Si l'ona es desplaça amb velocitat v cap al sentit positiu de l'eix x, té l'expressió

$$f(x,t) = f_0 \cos(k(x - vt) + \varphi_0) = f_0 \sin(k(x - vt) + \varphi_0 + \pi/2),$$

on f_0 és l'amplitud de l'ona, k el número d'ones i φ_0 una fase inicial. Són ones periòdiques en l'espai, amb una longitud d'ona $\lambda = 2\pi/k$, i en el temps, amb $T = \frac{2\pi}{kv}$. Si definim la pulsació o velocitat angular $\omega = kv = 2\pi\nu = 2\pi/T$, moltes vegades l'ona s'expressa com

$$f(x,t) = f_0 \cos((kx - \omega t) + \varphi_0).$$

La importància d'aquest tipus de funcions rau en el fet que, combinant funcions de freqüències diferents, via Fourier, pot aconseguir-se qualsevol perfil d'ona i, especialment, polsos molt localitzats en l'espai i el temps. Això és interessant si es vol descriure objectes localitzats, com les partícules, amb una descripció via ones.

Una funció que tindrà rellevància en el nostre curs és la funció harmònica complexa:

$$\bar{f}(x,t) = f_0 e^{i(k(x-vt)+\varphi_0)},$$

de manera que la seva part real és l'ona harmònica $f(x,t) = f_0 \cos(k(x - vt) + \varphi_0)$ i la seva part imaginària també és una altra ona harmònica, $f(x,t) = f_0 \sin(k(x - vt) + \varphi_0) = f_0 \cos(k(x - vt) + \varphi_0 + \pi/2)$, desfasada $+\pi/2$ de l'anterior. Això és clar si un recorda que

$$e^{ix} = \cos x + i \sin x.$$

La direcció de propagació d'aquestes ones és $+x$, amb velocitat v. (Si es vol que viatgi en sentit oposat, només cal substituir $(x - vt)$ per $(x + vt)$.)

1.3 Interferència d'ones

Una de les característiques fonamentals de les ones és que poden interferir. Donada una ona, que suposarem harmònica, que viatja amb una velocitat v en la direcció $+x$, amb y_0 la seva amplitud i $k = 2\pi/\lambda$ el nombre d'ones, λ la seva longitud d'ona, $kv \equiv \omega = 2\pi/T$, ω la pulsació o velocitat angular, T el seu període, i φ una fase qualsevol, ve descrita per

$$y(x,t) = y_0 \sin(k(x - vt) + \varphi) = y_0 \sin(kx - \omega t + \varphi)).$$

Si aquesta ona arriba a un punt d'una pantalla x_p , la intensitat que s'observarà –definida com l'energia per unitat d'àrea– serà una mitjana temporal del quadrat de la funció,

$$\begin{aligned} I_p &= < y^2(x_p,t) > \equiv \frac{1}{T}\int_{t=0}^{t=T} y^2(x_p,t)dt = \frac{1}{T}\int_{t=0}^{t=T} y_0^2 \sin^2[k(x_p - vt) + \varphi]dt \\ &= \frac{1}{T}y_0^2 \int_{t=0}^{t=T} \left[\frac{1-\cos[2(kx_p - \omega t + \varphi)]}{2}\right] dt = \frac{1}{T}\frac{y_0^2}{2}\left[t + \frac{\sin[2(kx_p - \omega t + \varphi)]}{2\omega}\right]_{t=0}^{t=T} = \frac{y_0^2}{2}. \end{aligned}$$

La intensitat, així definida, és positiva o nul·la i és proporcional al quadrat de l'amplitud. A més, és independent de x_p, de la posició a la que mesurem la intensitat tampoc depèn de φ. Si ara al punt x_p arriben simultàniament dues ones amb la mateixa λ, mateixa ω i mateixa amplitud y_0, però desfasades entre si un angle $\Delta\varphi = \varphi 1 - \varphi 2$,

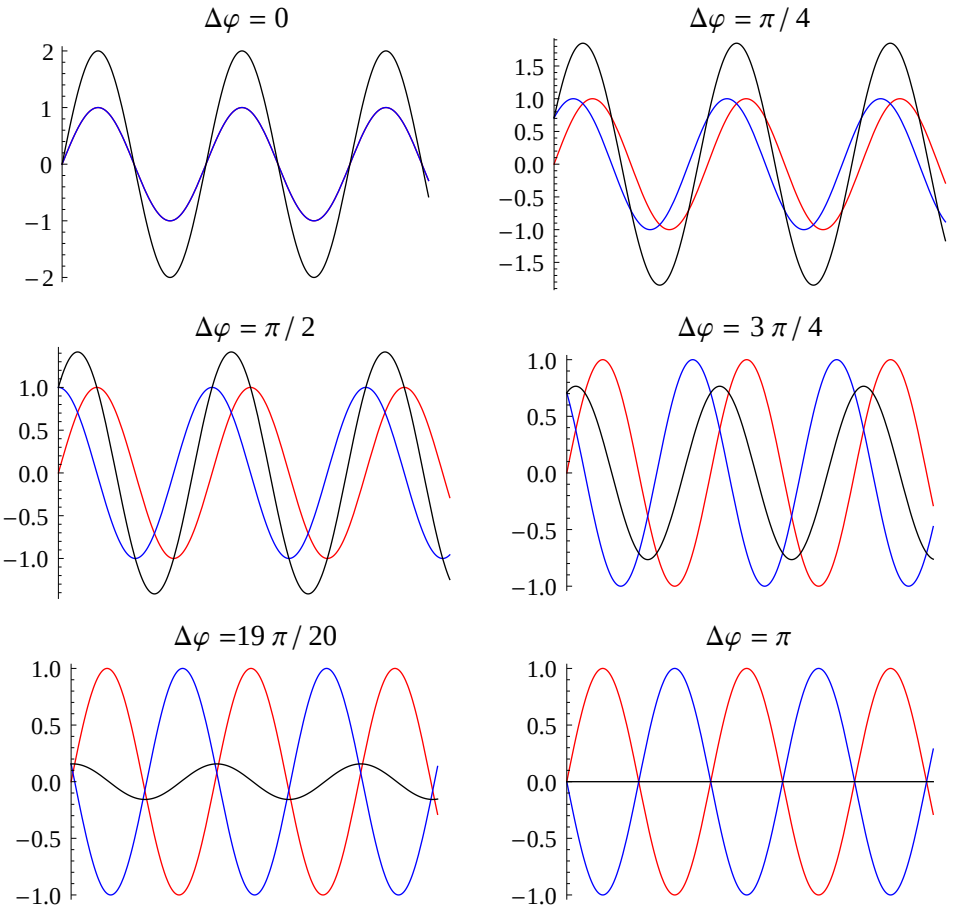
$$\begin{aligned} y_1(x,t) &= y_0 \sin(kx - \omega t + \varphi_1) \\ y_2(x,t) &= y_0 \sin(kx - \omega t + \varphi_2) \end{aligned}$$

la intensitat que registrarà el punt situat a x_p serà

$$\begin{aligned} I_p &= < (y_1(x_p,t) + y_2(x_p,t))^2 > \equiv \frac{1}{T}\int_{t=0}^{t=T} (y_1(x_p,t) + y_2(x_p,t))^2 dt = \\ &= \frac{1}{T}\int_{t=0}^{t=T} (y_0 \sin(kx_p - \omega t + \varphi_1) + y_0 \sin(kx_p - \omega t + \varphi_2))^2 dt \\ &= y_0^2(1 + \cos(\varphi_1 - \varphi_2)) = 2I_1(1 + \cos(\varphi_1 - \varphi_2)) = 2I_1(1 + \cos\Delta\varphi), \end{aligned}$$

on I_1 seria la intensitat recollida si només hi hagués l'ona 1. Observem que el resultat només depèn del desfasament relatiu entre les dues ones i adopta valors compresos entre 0 (interferència totalment destructiva, quan $\pm\Delta\varphi = \pi$) i $4I_1$ (interferència totalment constructiva, quan $\Delta\varphi = 0$, les ones estan en fase).

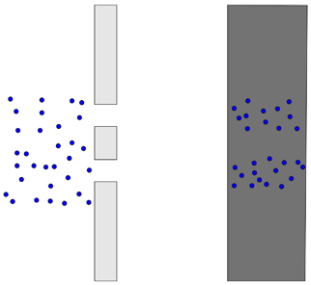
A la figura, representem dues ones com les descrites anteriorment, amb diferents desfasaments relatius, $\Delta\varphi = (\varphi_1 - \varphi_2)$, una en color vermell i l'altra en blau (a la primera figura, per $\Delta\varphi = 0$, la corba vermella coincideix exactament amb la blava), junt amb la seva suma, de color negre. S'entén que aquesta última depèn del desfasament entre les seves dues components i que la intensitat total oscil·li entre un valor mínim nul i un màxim que és $4I_1$ (recordem que les intensitats són proporcionals al quadrat de les amplituds).



Els fenòmens d'interferència són típics de les ones. Les partícules no interfereixen. La diferència fonamental és que la intensitat rebuda en un punt donat, quan s'envien partícules, és un còmput del nombre de partícules que hi arriben per unitat d'àrea. Així, si tenim un emissor de partícules, la intensitat rebuda per un detector serà el nombre de partícules rebut, $I_1 \geq 0$ Per un segon emissor, la intensitat corresponent serà $I_2 \geq 0$. Si ara les dues fonts emeten simultàniament, el detector comptarà el total de partícules, és a dir $I = I_1 + I_2$ i, com que tant I_1 com I_2 mai són negatives, la seva suma mai pot ser nul·la a no ser que ho siguin cada una d'elles.

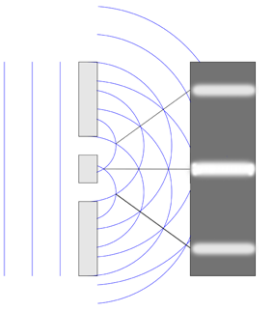
Tot això es pot veure en l'exemple de l'experiment de la doble escletxa.

Suposem que enviem un feix de partícules a un filtre sòlid que té dues escletxes i recollim les partícules que passen en una pantalla. La figura suggereix que la distribució de partícules rebudes a la pantalla serà concentrada en dues zones. De fet, la intensitat recollida obeirà la relació $I = I_1 + I_2$, essent I_1 (I_2) la intensitat que hi hauria si només l'escletxa 1 (2) estigués oberta.

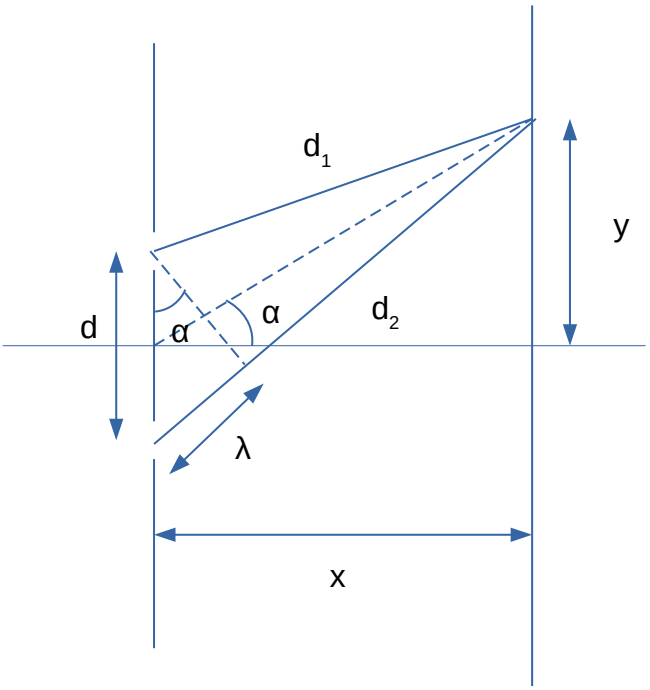


Si enviem llum monocromàtica (d'una única longitud d'ona), en canvi, resulta que la intensitat rebuda a la pantalla és completament diferent. Apareixen varies zones d'intensitat gran separades per zones fosques, del tipus indicat a la figura. La intensitat rebuda quan les dues escletxes són

obertes no és la suma de les intensitats individuals, quan només una de les dues escletxes és oberta, $I \neq I_1 + I_2$. Apareixen interferències que es poden explicar només recordant que la llum es comporta, en aquest experiment, com una ona.



Podem entendre aquest comportament recordant que, si la pantalla està situada a una distància x del pla on hi ha les dues escletxes, separades entre si una distància d, els punts de la pantalla on hi ha màxims satisfan que la diferència de camins que han realitzat els raigs, originats a cada una de les escletxes, $(d_2 - d_1)$ ha de ser un múltiple sencer de la longitud d'ona de la llum utilitzada.



Així, el punt central de la pantalla, a la mediatriu de les dues escletxes tindrà clarament un màxim d'intensitat. La figura d'intensitat serà simètrica respecte l'horitzontal i, el primer punt per sobre, y, que tindrà un màxim obeirà

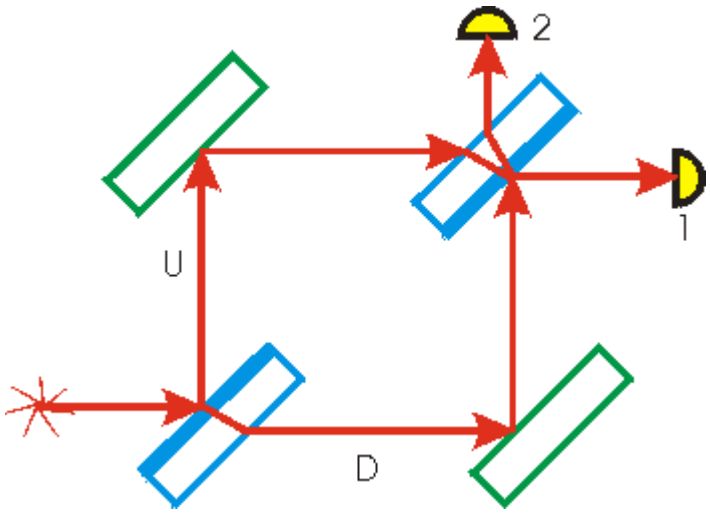
$$(d_2 - d_1) = \lambda = d \sin\alpha \simeq d \tan\alpha = d\ y/x; \qquad y = x\lambda/d,$$

on hem suposat que $x >> y$, la pantalla està lluny de les escletxes. Si volem que el màxim central i el primer màxim siguin clarament observables, la condició necessària és que λ/d no sigui excessivament petit, o sigui, d ha de ser de l'ordre de λ.

Per últim, es proposa com a exercici l'experiència de Mach-Zehnder:

EXERCICI DE COMPUTACIÓ QUÀNTICA

Aquest és un esquema del interferòmetre de Mach-Zenhder:



on els rectangles verds representen miralls, els blaus vidres semitransparents (que tenen una capa reflectant en un costat), i els semicercles 1 i 2 representen detectors.

Cal recordar:

- Quan la llum es reflecteix en un mitjà amb índex de refracció major que el del mitjà en el que està propagant-se, experimenta un canvi de fase de 180°.
- Quan la llum viatja per un medi, com per exemple el vidre, experimenta un canvi de fase que depen de de la longitud del camí recorregut (i de l'índex de refracció).

a) Descriviu el que passa als dos camins que arriben a cada detector (possibles canvis de fase de 180º, espai recorregut en el buit i a l'interior del vidre, etc.), de forma que es justifiqui el fet que no rebrem llum al detector 2 i tota es rebrà al detector 1.

b) Què opineu que passaria si cada un dels dos vidres semitransparents estigués girat 180º respecte un eix perpendicular al pla de la figura?

c) I si només en giréssim un i deixéssim l'altre sense girar?

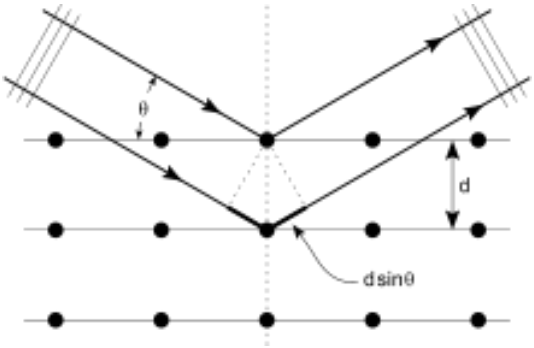
d) Si considerem que la llum es pot entendre com constituïda per partícules (fotons), quin percentatge n'arribarà a cada detector si fem la hipòtesi (aparentment molt raonable) de que cada fotó sols pot passar per un camí?

1.4 Difracció de Raigs X

Quan s'envien feixos de llum monocromàtica sobre cristalls, per certes direccions de rebot apareixen efectes d'interferència constructiva. Tenint en compte que els cristalls són estructures sòlides amb els àtoms regularment espaiats, podem considerar que formen capes regulars separades una distància d, de l'ordre de pocs d'Å, que actuen com a miralls. Així, algun raig del feix és reflectit per una capa d'àtoms, mentre que altres ho són per la següent. Apareixerà interferència totalment constructiva quan la diferència de camins viatjats pels dos raigs que arriben al detector sigui un múltiple sencer, n, de longituds d'ona, λ. El primer màxim d'interferència serà doncs per $n = 1$

$$2d \sin\theta = \lambda,$$

essent θ l'angle que formen els raigs amb la disposició en plans dels àtoms del cristall, tal com està indicat a la figura

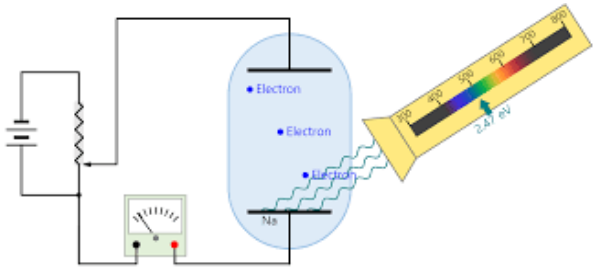


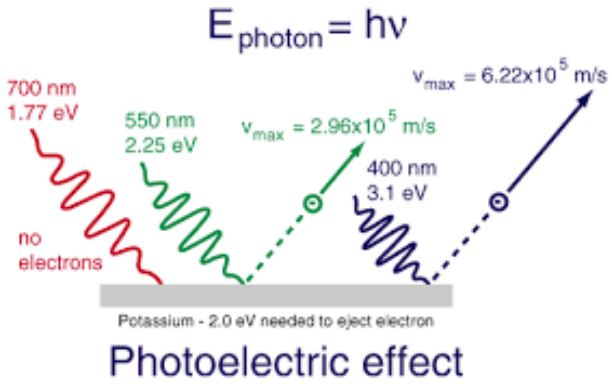
1.5 Efecte fotoelèctric

Quan s'il·lumina un metall pot ser que saltin electrons que surten de la seva superfície i poden donar lloc a corrents elèctrics. L'efecte té aquestes particularitats:

- Apareix només si la freqüència $f \equiv \nu$ de la llum incident és més gran que un valor llindar mínim, ν_0.
- Si hi ha efecte fotoelèctric, aquest és instantani i a més intensitat de llum, més electrons surten del metall. Com més gran és la freqüència, més gran és l'energia cinètica dels electrons emesos.
- Si no hi ha efecte, per més que s'augmenti la intensitat de la llum, no s'aconsegueix arrencar electrons del metall.

La física clàssica no pot explicar aquest comportament. De fet, entesa la llum com una ona electromagnètica, la seva acció sobre els electrons del metall és fer-los oscil·lar, de manera semblant a quan es gronxa un infant en un gronxador. Quan les oscil·lacions són grans, podem pensar que algun electró podrà escapar del metall, si l'energia assolida és suficient per vèncer l'energia de lligam al metall, ϕ. A més, l'energia de la llum és proporcional al quadrat del camp elèctric i independent de la longitud d'ona o freqüència de la llum, per tant no pot explicar que l'efecte depengui de la freqüència. Tampoc que l'efecte sigui instantani.





Einstein va considerar la hipòtesi de Planck de que la llum podia tenir un comportament tipus partícula i va pensar en termes del quantum de llum, o fotó. Un fotó γ seria un paquet de llum, l'energia del qual seria $E_\gamma = h\nu$, essent ν la seva freqüència i h la constant de Planck, amb un valor determinat experimentalment

$$h = 6.63 \cdot 10^{-34} Js$$

Quan s'il·lumina el metall, s'envien fotons de manera que col·lisionen contra els electrons. Si l'energia dels fotons és suficient per arrencar electrons, i això passa si

$$h\nu \geq \phi,$$

amb ϕ l'energia de lligam dels electrons al metall, hi haurà efecte fotoelèctric de manera que el sobrant d'energia serà energia cinètica de l'electró alliberat

$$h\nu = \phi + E_c.$$

Això explica cada una de les característiques esmentades de l'efecte fotoelèctric: Hi ha efecte només si $h\nu \geq \phi$, és a dir $\nu \geq \phi/h \equiv \nu_0$, essent ν_0 la freqüència llindar. Si hi ha efecte, aquest és instantani, i a més freqüència, més energia cinètica. Si no hi ha efecte, per molt que augmenti la intensitat de la llum –més nombre de fotons incidents– no apareixerà l'efecte fotoelèctric.

1.6 Dualitat ona - partícula. Hipòtesi de De Broglie

L'aparició del fotó com explicació de la llum comportant-se com a partícula en l'efecte fotoelèctric, però com a ona en els experiments d'interferència, li va donar un caràcter dual. També es va establir una relació entre la freqüència de la llum ν i l'energia del fotó E_γ, a través de la constant de Planck h.

$$E_\gamma = h\nu$$

Així, un fotó té una energia ben definida si es coneix la seva freqüència o, equivalentment, la seva longitud d'ona, i viatja a la velocitat de la llum, $c = 3 \cdot 10^8\ m/s$. En ser una partícula, ha de tenir una quantitat de moviment, o impuls, o moment lineal p. Per determinar-lo, recordem la famosa fórmula relativista d'Einstein que estableix l'equivalència entre massa i energia:

$$E = mc^2,$$

on m és la massa dinàmica d'una partícula i E la seva energia total equivalent. La massa dinàmica depèn de la velocitat de la partícula segons l'expressió

$$m = \frac{m_0}{\sqrt{1 - v^2/c^2}}, \quad E = mc^2 = \frac{m_0}{\sqrt{1 - v^2/c^2}} c^2,$$

on m_0 és la seva massa en repòs. Així, per un fotó, la seva velocitat és sempre $v = c$, per qualsevol sistema de referència inercial, pel que el denominador és zero i, per tant, sembla que la seva energia sigui infinita. Evidentment no ho és, per tant això ens porta a que la massa en repòs del fotó, $m_{\gamma 0}$ és nul·la. Això fa que no podem extreure el moment del fotó usant l'equivalència massa–energia, però sí extreure'n que la seva massa en repòs és zero. Per sort, el propi Einstein, va establir la relació entre energia E, moment p i massa en repòs m_0 d'una partícula relativista:

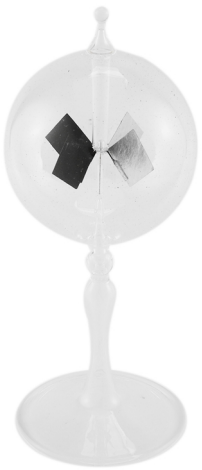
$$E = \sqrt{m_0^2 c^4 + p^2 c^2} = pc$$

on hem usat que, pels fotons, $m_0 = 0$. Així, el fotó el podem caracteritzar per un moment $p = \frac{E_\gamma}{c}$ i, si la seva freqüència és ν, aleshores

$$E_\gamma = h\nu; \quad p = \frac{E_\gamma}{c} = \frac{h\nu}{c} = \frac{h}{cT} = \frac{h}{\lambda},$$

on hem fet ús de que $\nu = 1/T$ i $\lambda = cT$, essent T el període i λ la longitud d'ona de la llum de freqüència ν.

En aquest punt, un es pot plantejar com detectar l'impuls dels fotons. Considerem una bombeta on al seu interior hi ha un molinet amb quatre veles, la superfície de les quals és rígida, de colors blanc per una banda i negre per l'altra, que poden girar respecte un eix comú. A l'interior s'hi ha fet el buit, de manera que la fricció sigui mínima. Il·luminem la bombeta, i per tant el molinet, amb llum de manera que els fotons que la componen tenen un impuls p. Volem veure quin efecte es produeix. Pensem què passa si un d'aquests fotons col·lisiona amb una de les veles del molinet, frontalment, quan l'impuls de la vela és P, si considerarem que en el xoc es conserva la quantitat de moviment total.



Si el fotó xoca sobre una superfície negra, el fotó quedarà absorbit per la superfície, i la quantitat de moviment abans i després del xoc satisfaran:

$$p + P = 0 + (P + p),$$

on el primer terme dels sumands és l'impuls del fotó i el segon el de la vela.

Si, en canvi, el fotó xoca contra una superfície blanca, el fotó surt rebotat de la vela i, per tant

$$p + P = (-p) + (P + 2p).$$

Veiem que l'impuls final de la vela és més gran quan el xoc es realitza contra la cara blanca, $(P+2p)$, que quan ho fa sobre la negra, $P + p$. Això implica que el molinet girarà de manera que les cares

blanques empenyen les cares negres. Cal tenir en compte que aquest efecte és molt difícil de realitzar, doncs en ser la constant de Planck tan petita, l'impuls dels fotons és molt petit. De fet, hi ha botigues de souvenirs que tenen aquest dispositiu bombeta-molinet. Si s'utilitza aquest dispositiu, es veu que el molinet gira... en sentit contrari al que nosaltres hem deduït. Això és degut a què la bombeta no té el buit a l'interior i les cares negres, on s'hi produeix un xoc inelàstic, s'escalfen més que les blanques, escalfen més l'aire que hi està en contacte i les molècules d'aire es mouen amb velocitat més gran, pressionant les parets negres més que les blanques. D'aquí que siguin les parets negres les que empenyen a les blanques.

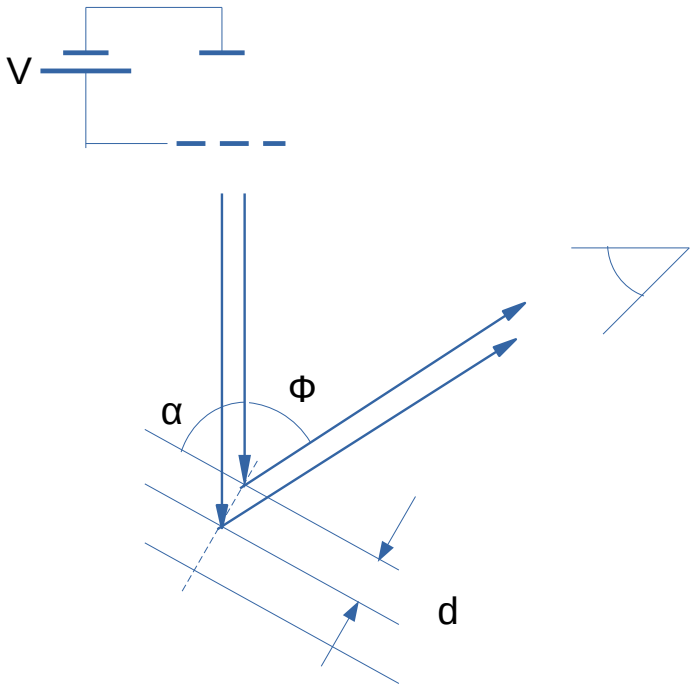
Donada la relació entre la longitud d'ona d'un fotó i el seu impuls, De Broglie va fer la hipòtesi de que aquesta relació aplica també a les partícules, de manera que aquestes, si tenen un impuls p, porten associada una ona tal que la seva longitud d'ona val:

$$\lambda = \frac{h}{p}$$

Podem veure de quin ordre de magnitud és aquesta quantitat per alguns objectes. Per exemple, per un protó, $m_p = 1,67 \cdot 10^{-27}$ kg, amb una velocitat $v = 1000$ m/s, $\lambda = \frac{h}{p} = \frac{h}{mv} = 4 \cdot 10^{-10}$ m $= 4$ Å. En canvi, per un balí de massa 5 g i velocitat 100 m/s, $\lambda = \frac{h}{p} = \frac{h}{mv} = 1,3 \cdot 10^{-33}$ m. Com que la distància típica interatòmica és de l'ordre de l'Å, això vol dir que serà possible veure fenòmens d'interferència per protons, però impossible per balins, doncs no tenim materials amb distàncies interatòmiques tan petites.

1.7 Difracció d'electrons

D'acord a la hipòtesi de De Broglie, als electrons els correspon una longitud d'ona depenent de la seva velocitat. Es podran veure doncs fenòmens d'interferència amb electrons? Considerem el següent muntatge.



Accelerem electrons des del repòs mitjançant una diferència de potencial V que podem variar. Els electrons es dirigeixen cap a un cristall del qual coneixem –a través de difracció de raigs X– que la

distància entre els seus plans d'ordenació dels seus àtoms és $d = 0.8$ Å. Quan l'angle que forma el feix dels electrons difractats respecte el feix incident val $\phi = 55^o$, s'observa que la quantitat d'electrons recollits en el detector presenta un màxim per $V = 75V$. Aquest màxim no té explicació si els electrons són i es comporten com a partícules.

En canvi, si pensem en termes d'ones, de manera similar al cas de difracció de raigs X, podem definir l'angle α que forma el feix incident amb el pla que actua com a mirall, de manera que $2\alpha + \phi = \pi$. La condició de màxim ondulatori és que

$$2d \sin \alpha = n\lambda,$$

amb n sencer. El primer màxim apareixerà per $n = 1$. Per tant,

$$2d \sin \alpha = 2d \cos \frac{\phi}{2} = 7,1 \text{ Å}.$$

Els electrons surten de la font amb una energia cinètica i un impuls

$$E_c = eV = \frac{p^2}{2m_e}; \qquad p = \sqrt{2m_e eV}$$

i, segons la hipòtesi de De Broglie, l'ona associada val

$$\lambda = \frac{h}{p} = \frac{h}{\sqrt{2m_e eV}} = \frac{12.3\text{Å}}{\sqrt{V(\text{Volts})}}$$

que, per $V = 75$ V resulta en $\lambda = 7,1$ Å. Així, es veu que quan $V = 75V$, la longitud de les ones associades als electrons és la que compleix la condició de màxim d'interferència.

S'observa que la dualitat ona–partícula no és específica de la llum, sinó que els electrons també presenten aquesta dualitat, comportant-se com a ones en els experiments de difracció. Cal dir que experiments similars ens diuen que els protons també experimenten difracció. Macromolècules com els ful·lerens (C60) i fluoro ful·lerens també es difracten.

1.8 Postulats Física Quàntica

Un cop establerta la dualitat ona–partícula, calia trobar un formalisme que la incorporés. Està clar que l'única possibilitat és utilitzar una funció d'ona a tal fi, doncs sabem que podem empaquetar les ones per obligar-les a viure en llocs confinats, com les partícules, mentre que usant el llenguatge de partícules no som capaços d'entendre o descriure els fenòmens ondulatoris d'interferència. Ara bé, quina mena d'ona descriu les partícules del món quàntic? De quin tipus és? Quina equació d'ones verifica?

Aquestes preguntes les responen els postulats de la Física Quàntica, és a dir, un conjunt d'afirmacions que no es poden demostrar, i que sobre ells s'edifica tota la teoria quàntica. La seva versemblança està basada en la comparació de les conseqüències dels postulats i l'experiment. A dia d'avui, els postulats són majoritàriament acceptats per la comunitat científica.

En aquesta assignatura no enunciarem de manera formal els postulats, sinó que intentarem destil·lar les parts que ens seran aplicables i útils en el camp de la Computació i Criptografia Quàntiques. També intentarem "justificar-los" en la mesura del possible, recordant però que són postulats i, per tant, indemostrables. Ens centrarem en:

- Funció d'ona
- Equació de Schrödinger
- La mesura en Física Quàntica: Principi d'incertesa i Col·lapse en la mesura.

1.8.1 Funció d'ona

Si una partícula ve descrita per una funció d'ona, què representa aquesta funció i quina equació verifica? Intentarem justificar la resposta tot i que, com hem dit, no podrem fer-ho totalment.

Considerem una partícula lliure que es pot moure per tots els punts de l'eix x i que té una energia total E, tota d'origen cinètic (la seva energia potencial serà constant, que prendrem igual a zero). Sabem que

$$E = \frac{p^2}{2m}.$$

Si aquesta partícula ha de venir descrita per una ona, sabem que

$$\begin{aligned} E &= h\nu = \frac{h}{2\pi}\omega = \hbar\omega \\ p &= \frac{h}{\lambda} = \frac{h}{2\pi}\frac{2\pi}{\lambda} = \hbar k, \end{aligned}$$

on hem introduït la constant de Planck reduïda, $\hbar \equiv \frac{h}{2\pi}$, essent ω la velocitat angular o pulsació i k el número d'ones. Així, en termes de ω i k, el balanç d'energia s'escriu

$$\hbar\omega = \frac{\hbar^2 k^2}{2m}.$$

Provem si una funció harmònica harmònica pot descriure la partícula lliure. Prenem

$$\psi(x,t) = A\cos(kx - \omega t).$$

Si ara considerem les derivades parcials, en primer lloc respecte el temps

$$\frac{\partial\psi(x,t)}{\partial t} = \omega A\sin(kx - \omega t),$$

i, en segon lloc, respecte la posició x

$$\frac{\partial\psi(x,t)}{\partial x} = -kA\sin(kx - \omega t); \quad \frac{\partial^2\psi(x,t)}{\partial x^2} = -k^2 A\cos(kx - \omega t) = -k^2\psi(x,t).$$

Observem que podem tenir informació de l'energia E i del moment p a partir de les derivades parcials de la funció d'ona respecte al temps i a la posició, respectivament. De totes maneres, és impossible que es compleixi una equació diferencial del tipus

$$\alpha\frac{\partial\psi(x,t)}{\partial t} = \beta\frac{\partial^2\psi(x,t)}{\partial x^2},$$

degut a que no apareix la mateixa dependència funcional als dos termes: a l'esquerra apareix una funció sinus i a la dreta una cosinus, de manera que no es pot factoritzar la funció d'ona.

Anem a provar amb la funció harmònica complexa,

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

Les seves derivades parcials són

$$\frac{\partial\bar{\psi}(x,t)}{\partial x} = ikAe^{i(kx-\omega t)} = ik\bar{\psi}(x,t); \quad \frac{\partial^2\bar{\psi}(x,t)}{\partial x^2} = -k^2 Ae^{i(kx-\omega t)} = -k^2\bar{\psi}(x,t),$$

$$\frac{\partial\bar{\psi}(x,t)}{\partial t} = -i\omega Ae^{i(kx-\omega t)} = -i\omega\bar{\psi}(x,t),$$

de manera que

$$\alpha\frac{\partial\bar{\psi}(x,t)}{\partial t}=\beta\frac{\partial^2\bar{\psi}(x,t)}{\partial x^2},$$

es redueix a una equació algebraica:

$$\alpha(-i\omega)\bar{\psi}=\beta(-k^2)\bar{\psi}\longrightarrow\alpha(-i\omega)=\beta(-k^2).$$

Els valors α i β els obtenim quan imposem que es compleixi el balanç energètic

$$\hbar\omega=\frac{\hbar^2k^2}{2m},$$

i resulta que

$$\alpha=i\hbar;\quad\beta=-\frac{\hbar^2}{2m}.$$

Així arribem a que la partícula lliure ve descrita per la funció $\bar{\psi}(x,t)=Ae^{i(kx-\omega t)}$ i verifica l'equació d'ones

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

De fet, aquesta equació d'ones que hem trobat és igual a l'equació de Schrödinger per la partícula lliure, quan la seva energia potencial és zero per a qualsevol posició i qualsevol instant, $V(x,t)=0$. Per un potencial (en realitat, energia potencial) qualsevol, l'equació de Schrödinger completa és:

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

que podem interpretar com: l'energia total de la partícula descrita per la funció $\bar{\psi}(x,t)$ és la suma de la seva energia cinètica més la seva energia potencial.

Curiosament, la funció d'ona trobada és complexa i la mateixa equació de Schrödinger que verifica incorpora el nombre imaginari i de manera explícita. La interpretació que podem fer de la funció d'ona és atribuir-li probabilitat de trobar la partícula, però en ser la funció complexa, no és possible. La solució rau en dir que la densitat de probabilitat de trobar la partícula en un punt x i a l'instant t és

$$\left|\bar{\psi}(x,t)\right|^2.$$

Així, la probabilitat de trobar la partícula en un interval infinitesimal dx centrat a x a l'instant t és

$$\left|\bar{\psi}(x,t)\right|^2dx.$$

Veurem que aquí ens apareix un problema. Si calculem quina és la probabilitat de trobar la partícula lliure a qualsevol lloc de l'eix x, tindríem

$$Prob=\int_{-\infty}^{\infty}\left|\bar{\psi}(x,t)\right|^2dx=|A|^2\int_{-\infty}^{\infty}\left|e^{i(kx-\omega t)}\right|^2dx=|A|^2\int_{-\infty}^{\infty}dx,$$

on hem usat que $\left|e^{i(kx-\omega t)}\right|^2=1$, que implica que la densitat de probabilitat de trobar la partícula és constant, la mateixa per totes les posicions i temps. Aquesta probabilitat, $Prob$, hauria de ser 1 però la integral de la dreta és infinit (vegades $|A|^2$). Tenim doncs una contradicció. Volíem justificar la funció d'ones i l'equació de Schrödinger per la partícula lliure amb arguments plausibles i trobem contradiccions. Ja havíem avançat que no ens en sortiríem.

Aquest intent ha servit però per interpretar la manera de llegir l'equació de Schrödinger, atribuir a la funció d'ona un caràcter probabilístic i obrir camí per trobar solucions a problemes amb potencials més realistes.

1.8.2 Equació de Schrödinger

Per una partícula que visqui en un món unidimensional, l'equació de Schrödinger és

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

És l'equació d'ones que descriu quines funcions d'ona poden representar la partícula quan està en presència d'un cert potencial $V(x,t)$. La seva interpretació és en termes de balanç energètic: la seva energia total és la suma de la seva energia cinètica més la seva energia potencial (els termes potencial i energia potencial, en quàntica, s'usen indistintament).

En un món realista, les partícules viuen en un espai tridimensional. L'equació en aquest cas és

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

1.8.3 La mesura en Física Quàntica: Principi d'incertesa de Heisenberg i Col·lapse en la mesura

La mesura en el món quàntic, en el microcosmos, es diferencia de la mesura en el món macroscòpic. En el segon, la precisió depèn de la qualitat o resolució de l'aparell de mesura. En el primer, el principi d'incertesa de Heisenberg estableix que és impossible mesurar amb precisió infinita i de manera simultània la posició i el moment d'una partícula (o qualsevol parell de variables conjugades). Concretament, de manera més específica, si la incertesa en la mesura de la posició la denotem per Δx i la incertesa en el seu moment Δp, el seu producte

$$\Delta x\Delta p \geq \frac{\hbar}{2}.$$

Com afecta aquest principi en el cas que hem tractat de la partícula lliure? Si la funció d'ona que la descriu és

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

el seu moment és $p = \hbar k$ amb certesa, per tant $\Delta p = 0$. Sembla que el principi no apliqui en aquest cas. Ara bé, recordem que tots els punts de l'eix x tenen la mateixa densitat de probabilitat de trobar la partícula. Això implica que la incertesa en la seva posició és $\Delta x = \infty$, de manera que es compleix el principi d'incertesa de Heisenberg.

Una manera de justificar el principi és recordant com mesurem. Si volem mesurar la posició d'un cotxe, per exemple, enviem llum que toca el cotxe i, en rebotar, arriba al detector. El rebot de la llum contra el cotxe no afecta a la seva posició. Pel seu moment, coneguda la massa es redueix a conèixer la seva velocitat, que es determina de manera similar, il·luminant-lo amb llum que rebota i es processa. Si ara fem el mateix procés per determinar la posició i moment d'un electró, hem de pensar que la llum que enviem és un feix de fotons. Els fotons duen un impuls i energia que ara no són menyspreables i alteren la posició i velocitat de l'electró. D'aquí que no podem saber amb precisió infinita les dues mesures simultàniament.

Un altre aspecte important és el que se'n diu col·lapse en la mesura. Hem vist que la funció d'ona -el seu mòdul al quadrat, més precisament- representa la densitat de probabilitat de trobar la partícula en un lloc i en un instant. Ara bé, si mesurem la posició, per exemple, la funció que descriu la partícula deixa de ser la inicial i canvia de manera que s'adapta al coneixement que hem adquirit en la seva mesura prèvia. Es diu que la mesura ha col·lapsat la seva funció d'ona. De nou, la mesura afecta a l'estat/objecte mesurat. Ho veurem més clar a mesura que avancem durant el transcurs del curs.

2 Equació de Schrödinger. Pou unidimensional infinit

Considerem l'equació de Schrödinger

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

i analitzem-la pel cas del pou unidimensional infinit:

$$V(x) = \begin{cases} 0, & si \quad 0 \leq x \leq l \\ \infty, & si \quad |x| > l \end{cases}$$

Aquest potencial és nul entre els valors $0 < x < l$, per tant la partícula es pot moure lliurement entre aquests valors. Pels punts $x = 0$ i $x = l$ apareix una força infinita que retorna la partícula a la zona permesa. (Recordem que $F = -\frac{dV}{dx}$. La força que actuarà sobre la partícula quan s'apropi a $x = 0^+$ la podem extreure de $V(x) = x\tan\alpha \Rightarrow F = -\frac{dV}{dx} = -\tan\alpha \to -\infty$, quan $\alpha = \pi/2 - \epsilon$ i $\epsilon \to 0$. De manera similar, quan la partícula s'apropi a $x = l^-$, $V(x) = (x-l)\tan\beta \Rightarrow F = -\frac{dV}{dx} = -\tan\beta \to \infty$, quan $\beta = \pi/2 + \epsilon$ i $\epsilon \to 0$.)

Volem trobar les solucions a l'equació donat aquest potencial. Per això, provem de trobar solucions amb separació de variables, del tipus:

$$\psi(x,t) = \psi(x)\phi(t)$$

$$i\hbar\psi(x)\frac{d\phi(t)}{dt} = -\frac{\hbar^2}{2m}\phi(t)\frac{d^2\psi(x)}{dx^2} + V(x)\psi(x)\phi(t) = E\psi(x)\phi(t)$$

on ara les derivades són totals. Dividim tota l'equació per $\psi(x)\phi(t)$,

$$i\hbar\frac{1}{\phi(t)}\frac{d\phi(t)}{dt} = -\frac{\hbar^2}{2m}\frac{1}{\psi(x)}\frac{d^2\psi(x)}{dx^2} + V(x) = E$$

Obtenim una equació que només depèn del temps, i una altra que només depèn de la posició. L'equació temporal és

$$i\hbar\frac{1}{\phi(t)}\frac{d\phi(t)}{dt} = E$$

$$\frac{d\phi(t)}{\phi(t)} = -i\frac{E}{\hbar}dt; \qquad \ln\phi(t) = -i\frac{E}{\hbar}t; \quad \phi(t) = e^{-i\frac{E}{\hbar}t}.$$

L'equació espacial

$$-\frac{\hbar^2}{2m}\frac{1}{\psi(x)}\frac{d^2\psi(x)}{dx^2} + V(x) = E,$$

per la zona interior al pou de potencial ($V(x) = 0$)

$$-\frac{\hbar^2}{2m}\frac{1}{\psi(x)}\frac{d^2\psi(x)}{dx^2} = E,$$

$$\frac{d^2\psi(x)}{dx^2} = -\frac{2mE}{\hbar^2}\psi(x)$$

Apart d'una constant, resoldre l'equació anterior és cercar una funció que, derivada dos cops respecte x, doni la mateixa funció canviada de signe. Una solució serà:

$$\psi(x) = A\sin(kx), \quad \frac{d^2\psi(x)}{dx^2} = -k^2 A\sin(kx) = -k^2\psi(x),$$

amb $k^2 = \frac{2mE}{\hbar^2}$

Ara hem de tenir en compte les condicions de contorn:

$$\psi(x=0) = 0; \quad \psi(x=l) = 0$$

La primera es compleix automàticament. La segona, cal que

$$kl = n\pi; \quad n = 1, 2, 3, ...,$$

(amb $n = 0$ prohibit, doncs la funció seria nul·la a tot l'espai). Això implica que les energies E han de verificar:

$$E = \frac{\hbar^2 k^2}{2m} = \frac{n^2\hbar^2\pi^2}{2ml^2},$$

és a dir: estan quantificades! Per això escriurem:

$$E_n = \frac{n^2\hbar^2\pi^2}{2ml^2}, \quad n = 1, 2, 3, ...$$

$$\psi_n(x) = A_n \sin(n\pi x/l),$$

Recopilant:

$$\psi_n(x,t) = A_n \sin(n\pi x/l)e^{-i\frac{E_n}{\hbar}t}; \quad E_n = \frac{n^2\hbar^2\pi^2}{2ml^2}, n = 1, 2, 3, ...$$

2.1 Estats estacionaris

Hem trobat els que se'n diuen estats propis de l'energia, doncs tenen un valor ben definit de la seva energia. També s'anomenen estats estacionaris. Perquè? anem a justificar-ho veient quina és la densitat de probabilitat de trobar una partícula descrita per un d'aquests estats en funció del temps.

$$\rho_n(x,t) = \psi_n^*(x,t)\psi_n(x,t) = |A_n|^2 \sin(n\pi x/l)e^{+i\frac{E_n}{\hbar}t}\sin(n\pi x/l)e^{-i\frac{E_n}{\hbar}t} = |A_n|^2\sin^2(n\pi x/l),$$

que és independent del temps.

Les constants A_n son constants d'integració que no estan fixades. Quan un imposa la condició que la funció d'ona estigui normalitzada, que equival a dir que la probabilitat de trobar la partícula entre 0 i l ha de ser 1, aleshores obté:

$$\int_0^l \psi_n(x,t)^*\psi_n(x,t)dx = |A_n|^2 \int_0^l \sin^2(k_n x)dx = |A_n|^2 \frac{l}{2} = 1; \quad |A_n| = \sqrt{\frac{2}{l}},$$

valor que és el mateix per tots els valors de n.

L'estat d'energia més baixa $E_1 = \frac{\hbar^2\pi^2}{2ml^2}$ correspon a $n = 1$ i s'anomena estat fonamental. Tota la resta són estats excitats. Les energies possibles estan quantificades i expliquen clarament l'existència dels espectres d'emissió i absorció dels diferents materials, que són com les seves empremtes digitals.

2.2 Estats superposició. Evolució temporal

L'equació de Schrödinger és lineal. Això implica que si tenim dues solucions - o més - per un determinat potencial, aleshores una combinació lineal d'elles també és solució. Així, considerem per exemple

$$\psi(x,t) = a_n\psi_n(x,t) + b_m\psi_m(x,t)$$

i calculem la seva densitat de probabilitat

$$\begin{aligned}\rho(x,t) = \psi^*(x,t)\psi(x,t) &= (a_n^*\psi_n^*(x,t) + b_m^*\psi_m^*(x,t))(a_n\psi_n(x,t) + b_m\psi_m(x,t)) \\ &= |a_n|^2\rho_n(x,t) + |b_m|^2\rho_m(x,t) \\ &+ \frac{2}{l}a_n^*b_m e^{i\frac{(E_n-E_m)t}{\hbar}}\sin(n\pi x/l)\sin(m\pi x/l) + \frac{2}{l}a_n b_m^* e^{-i\frac{(E_n-E_m)t}{\hbar}}\sin(n\pi x/l)\sin(m\pi x/l).\end{aligned}$$

Si les constants de la combinació lineal a_n, b_n són nombres reals, aleshores l'expressió anterior simplifica a

$$\begin{aligned}\rho(x,t) &= a_n^2\rho_n(x,t) + b_m^2\rho_m(x,t) + \frac{2}{l}2a_nb_m\cos\frac{(E_n-E_m)t}{\hbar}\sin(n\pi x/l)\sin(m\pi x/l) \\ &= \frac{2}{l}\left(a_n^2\sin^2(n\pi x/l) + b_m^2\sin^2(m\pi x/l) + 2a_nb_m\cos\frac{(E_n-E_m)t}{\hbar}\sin(n\pi x/l)\sin(m\pi x/l)\right)\end{aligned}$$

on ara el temps apareix explícitament a la densitat de probabilitat i, per tant, s'observa que la funció d'ona evoluciona en el temps, de manera periòdica, amb una freqüència angular $\omega = \frac{E_n-E_m}{\hbar}$ i un període $T = \frac{2\pi}{\omega} = \frac{2\pi\hbar}{E_n-E_m} = \frac{h}{E_n-E_m}$.

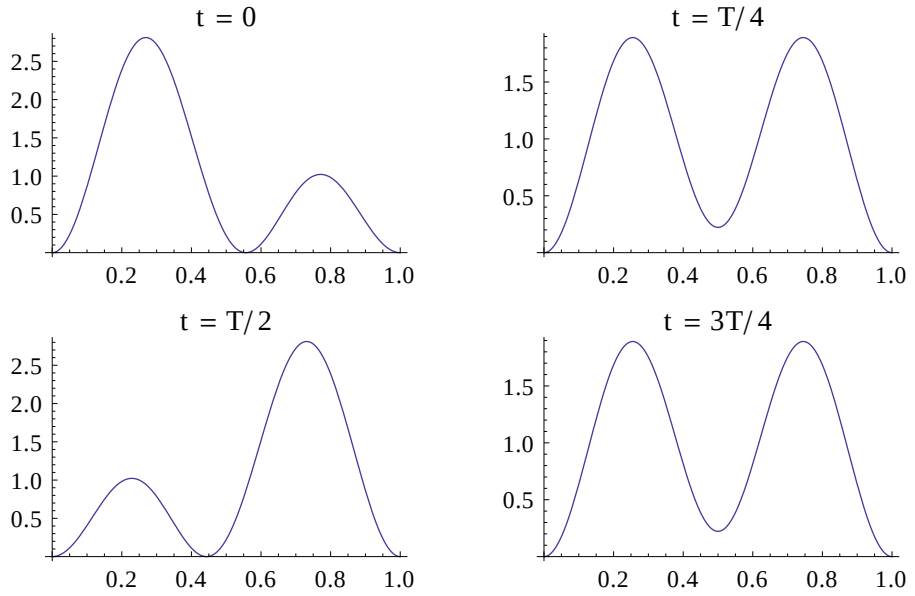
Com exemple, si tenim l'estat

$$\psi(x,t) = \frac{1}{3}\psi_1(x,t) + \frac{2\sqrt{2}}{3}\psi_2(x,t),$$

la seva densitat de probabilitat és

$$\rho(x,t) = \frac{1}{9}\rho_1(x,t) + \frac{8}{9}\rho_2(x,t) + \frac{2}{l}\frac{4\sqrt{2}}{9}\cos\frac{(E_2-E_1)t}{\hbar}\sin(\pi x/l)\sin(2\pi x/l)$$
$$= \frac{2}{l}\left(\frac{1}{9}\sin^2(\pi x/l) + \frac{8}{9}\sin^2(2\pi x/l) + \frac{4\sqrt{2}}{9}\cos\frac{(E_2-E_1)t}{\hbar}\sin(\pi x/l)\sin(2\pi x/l)\right),$$

que podem visualitzar qualitativament, per $l = 1$ i $\frac{m}{\hbar}$ tal que $T = 1$, representant-la en funció de x per diferents instants de temps:



2.3 Estats estacionaris: Base

Els estats estacionaris, independents del temps, formen una base si definim un producte escalar de la manera següent:

$$\langle\psi_n(x,t)|\psi_m(x,t)\rangle = \int_0^l \psi_n^*(x,t)\psi_m(x,t)dx = \frac{2}{l}\int_0^l \sin(n\pi x)\sin(m\pi x)dx = \delta_{n,m} = \begin{cases} 1, & m = n \\ 0, & m \neq m \end{cases}$$

Diem que, segons aquest producte, són funcions ortonormals i generen una base a partir de la qual, amb combinacions lineals, podem construir qualsevol funció que sigui solució de l'equació de Schrödinger. Generem el que en diem un espai de Hilbert, semblant a un espai vectorial de dimensió infinita, amb coeficients complexos.

Si un es restringeix només a dos estats, el fonamental i el primer excitat, per exemple, de manera que els altres són inaccessibles, aleshores la nostra partícula en el pou només pot estar en un dels dos estats i/o en una combinació lineal dels dos. Aquest sistema pot descriure un qubit.

En aquesta situació, convé introduir una notació més senzilla i pràctica: els kets -i els bras- ideats per Dirac. Així, els dos estats base els definim com els "kets"

$$|0\rangle = \psi_1(x,t); \quad |1\rangle = \psi_2(x,t),$$

essent els "bras":

$$\langle 0| = \psi_1^*(x,t); \quad \langle 1| = \psi_2^*(x,t),$$

i els productes escalars vénen representats pels brackets:

$$\langle n-1|m-1\rangle = \int_0^l \psi_n^*(x,t)\psi_m(x,t)dx = \frac{2}{l}\int_0^l \sin(n\pi x)\sin(m\pi x)dx = \delta_{n,m},$$

és a dir

$$\langle 0|0\rangle = \langle 1|1\rangle = 1; \quad \langle 0|1\rangle = \langle 1|0\rangle = 0.$$

Un estat qualsevol per un qubit, pot estar en una superposició:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,,$$

amb els coeficients a i b valors complexos en general. Tot i que aparentment es necessiten quatre nombres reals per descriure els coeficients d'un qubit general, veurem que, en realitat, dos són suficients.

2.4 Exercicis

A continuació teniu un exercici sobre el principi d'incertesa de Heisenberg, que estableix que no es pot mesurar amb precisió infinita la posició i el moment d'una partícula.

EXERCICI COMPUTACIÓ QUÀNTICA

INCERTESA

En Física Quàntica es verifica el Principi d'Incertesa de Heisenberg: És impossible mesurar amb precisió infinita la posició i el moment d'una partícula. Més concretament, si Δx i Δp són les incerteses en la posició i el moment, respectivament, es verifica

$$\Delta x \Delta p \geq \hbar/2.$$

Ara sabem també que les partícules venen descrites per funcions d'ona $\psi(x,t)$ que obeeixen l'equació de Schrödinger. La forma d'avaluar les incerteses, coneguda la funció d'ona $|\psi>$, és:

$$\Delta x_{|\psi>} = \sqrt{< x^2 >_{|\psi>} - < x >^2_{|\psi>}},$$

$$\Delta p_{|\psi>} = \sqrt{< p^2 >_{|\psi>} - < p >^2_{|\psi>}},$$

on $< x >_{|\psi>}$ s'anomena valor esperat en la mesura de x, en sentit estadístic: Seria el valor mitjà obtingut en fer moltes mesures de x si disposéssim de moltes còpies idèntiques de l'estat $|\psi>$. De manera anàloga, s'interpreten $< x^2 >_{|\psi>}$,$< p >_{|\psi>}$ i $< p^2 >_{|\psi>}$. La manera explícita de calcular els valors esperats és:

$$< x >_{|\psi>} = \int dx \psi^*(x,t) x \psi(x,t); \qquad < x^2 >_{|\psi>} = \int dx \psi^*(x,t) x^2 \psi(x,t),$$

$$< p >_{|\psi>} = \int dx \psi^*(x,t)(-i)\hbar \frac{\partial}{\partial x}\psi(x,t); \qquad < p^2 >_{|\psi>} = \int dx \psi^*(x,t)(-\hbar^2)\frac{\partial^2}{\partial x^2}\psi(x,t).$$

1) Quin seria el "valor esperat" (valor mitjà estadístic) que obtindriem si tiréssim un dau de sis cares moltes vegades? I quina la seva incertesa?

2) Justifiqueu quant val $< x >_{|\varphi_1>}$ i $< p >_{|\varphi_1>}$, essent $|\varphi_1>$ l'estat fonamental del pou unidimensional infinit, d'amplada L. (A classe varem considerar que la partícula podia trobar-se a l'interval $0 \leq x \leq L$.)

3) Els resultats de l'apartat anterior, són també vàlids per qualsevol dels estats propis de l'energia $|\varphi_n>$?

4) De manera analítica o bé usant un programa de manipulació algebraic (Mathematica, Maple,...), calculeu els resultats dels dos apartats anteriors i, també: $< x^2 >_{|\varphi_n>}$ i $< p^2 >_{|\varphi_n>}$.

5) Comproveu per tot n que es compleix el principi d'incertesa de Heisenberg:

$$\Delta x_{|\varphi_n>} \Delta p_{|\varphi_n>} \geq \hbar/2$$

3 Qubits

Considerem el següent qubit:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,.$$

Els nombres complexos a i b els podem escriure en forma polar,

$$a = r_0 e^{i\varphi_0}; \quad b = r_1 e^{i\varphi_1},$$

de manera que

$$|\psi\rangle = r_0 e^{i\varphi_0}\,|0\rangle + r_1 e^{i\varphi_1}\,|1\rangle = e^{i\varphi_0}(r_0\,|0\rangle + r_1 e^{i(\varphi_1-\varphi_0)}\,|1\rangle).$$

La fase $e^{i\varphi_0}$ inicial és immesurable. Si mesurem la probabilitat de trobar el qubit en un dels estats de la base, veurem que no depèn d'aquesta fase. Es diu que és una fase global no mesurable i s'adopta el conveni de menystenir-la, de manera que el coeficient de l'estat $|0>$ s'agafa real. A més, l'altra fase es reescriu en termes només d'un únic angle, que serà φ. Així, tenim ara tres paràmetres per descriure l'estat:

$$|\psi\rangle = r_0\,|0\rangle + r_1 e^{i\varphi}\,|1\rangle\,.$$

Si ens adonem que l'estat ha d'estar normalitzat, això implica que

$$\langle\psi|\psi\rangle = r_0^2 + r_1^2 = 1,$$

que ens relaciona els dos valors r_0 i r_1. De fet, els podem escriure en termes d'un angle, identificant $r_0 = \cos\alpha$ i $r_1 = \sin\alpha$. Així

$$|\psi\rangle = \cos\alpha\,|0\rangle + \sin\alpha e^{i\varphi}\,|1\rangle\,.$$

Ja tenim doncs que, la normalització de l'estat i el fet que la fase global sigui no mesurable, fan que el qubit més general sigui expressable en termes de dos nombres reals. Anem a veure quina descripció geomètrica podem donar als angles α i φ.

Bloch va adonar-se que usant l'esfera de radi 1, amb la convenció habitual d'angles zenital i azimutal, si identificava α amb el zenital θ i φ amb l'azimutal, podia identificar el "pol nord" de l'esfera amb l'estat $|0>$, quan $\alpha = 0$ i φ qualsevol ($|0\rangle = |+\rangle_{\alpha=0,\varphi}$). Si es vol identificar el "pol sud" amb l'estat $|1\rangle$, s'arriba a contradicció, doncs aquest hauria de ser $|\,|+\rangle_{\alpha=\pi,\varphi} = -\,|0\rangle \neq |1\rangle$.

La solució és identificar $\alpha = \frac{\theta}{2}$, aleshores

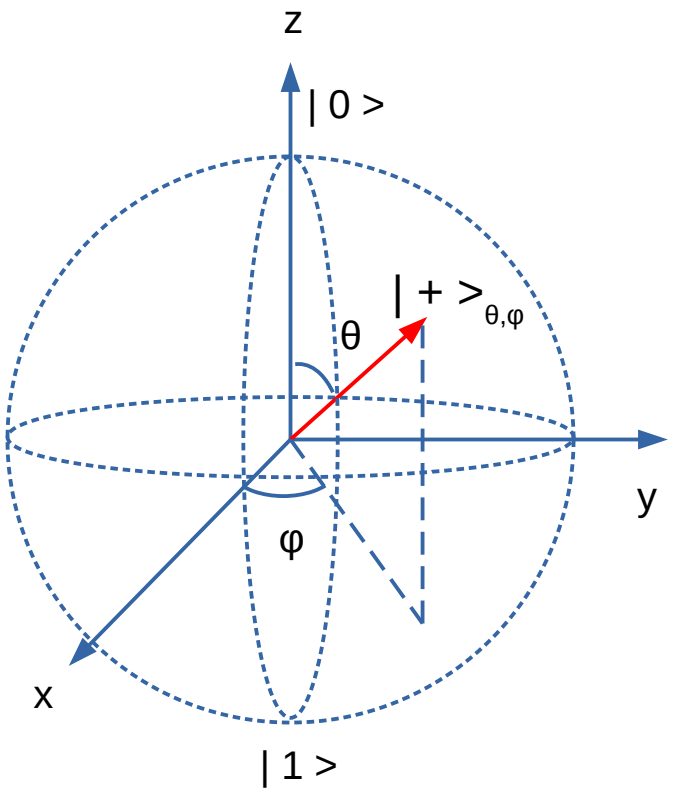
$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}\,|1\rangle\,.$$

Normalment s'usa la notació indicant la direcció en la que punxa el qubit a l'esfera de Bloch

$$|+\rangle_{\theta,\varphi} = \cos\frac{\theta}{2}\,|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}\,|1\rangle\,,$$
$$|-\rangle_{\theta,\varphi} = -\sin\frac{\theta}{2}\,|0\rangle + \cos\frac{\theta}{2}e^{i\varphi}\,|1\rangle = |+>_{\theta+\pi,\varphi}$$

amb

$$|0\rangle = |+\rangle_{\theta=0,\varphi} = |+\rangle_z\,; \quad |1\rangle = |-\rangle_{\theta=0,\varphi=0} = |+\rangle_{\theta=\pi,\varphi=0} = |-\rangle_z\,.$$



3.1 Qubit: Bases

L'expressió més general d'un qubit, a l'esfera de Bloch:

$$|+\rangle_{\theta,\varphi} = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}|1\rangle$$

Els qubits $|0\rangle, |1\rangle$ són base, és a dir, verifiquen que

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

Anem a veure que, definint

$$|-\rangle_{\theta,\varphi} = |+\rangle_{\theta+\pi,\varphi} = -\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}e^{i\varphi}|1\rangle,$$

aleshores els estats $|+\rangle_{\theta,\varphi}$ i $|-\rangle_{\theta,\varphi}$, també son base.

$${}_{\theta,\varphi}\langle +|+\rangle_{\theta,\varphi} = (\langle 0|\cos\frac{\theta}{2} + \langle 1|\sin\frac{\theta}{2}e^{-i\varphi})(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}|1\rangle) = \cos^2\frac{\theta}{2} + \sin^2\frac{\theta}{2} = 1$$

$${}_{\theta,\varphi}\langle +|-\rangle_{\theta,\varphi} = (\langle 0|\cos\frac{\theta}{2} + \langle 1|\sin\frac{\theta}{2}e^{-i\varphi})(-\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}e^{i\varphi}|1\rangle) = -\cos\frac{\theta}{2}\sin\frac{\theta}{2} + \sin\frac{\theta}{2}\cos\frac{\theta}{2} = 0$$

Els altres casos es comproven de manera anàloga:

$$_{\theta,\varphi}\langle -|-\rangle_{\theta,\varphi} = (-\langle 0|\sin\frac{\theta}{2} + \langle 1|\cos\frac{\theta}{2}e^{i\varphi})(-\sin\frac{\theta}{2}|0\rangle + \cos\frac{\theta}{2}e^{i\varphi}|1\rangle) = \sin^2\frac{\theta}{2} + \cos^2\frac{\theta}{2} = 1$$

$$_{\theta,\varphi}\langle -|+\rangle_{\theta,\varphi} = (-\langle 0|\sin\frac{\theta}{2} + \langle 1|\cos\frac{\theta}{2}e^{-i\varphi})(\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}|1\rangle) = -\cos\frac{\theta}{2}\sin\frac{\theta}{2} + \sin\frac{\theta}{2}\cos\frac{\theta}{2} = 0$$

Casos particulars:

$$\begin{aligned}
\{|+\rangle_x &= |+>_{\pi/2,0} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |-\rangle_x = |-\rangle_{\pi/2,0} = -\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\} \\
\{|+\rangle_y &= |+\rangle_{\pi/2,\pi/2} = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \quad |-\rangle_y = |-\rangle_{\pi/2,\pi/2} = -\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}
\end{aligned}$$

3.2 Notació alternativa

Degut a la similitud de l'espai de Hilbert amb un espai vectorial, els estats que descriuen un qubit poden descriure's també fent ús de vectors de dues components. De fet, la base canònica pot representar-se com

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

i un estat superposició qualsevol es representa com el "ket":

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

essent el seu "bra" corresponent

$$\langle\psi| = a^*\langle 0| + b^*\langle 1| = (a^*, b^*).$$

Per últim, donats dos estats

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}; \quad |\phi\rangle = c|0\rangle + d|1\rangle = \begin{pmatrix} c \\ d \end{pmatrix},$$

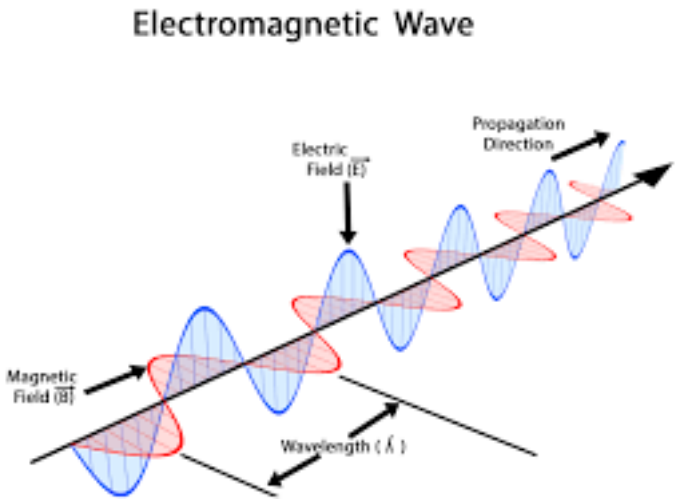
el seu producte escalar

$$\langle\psi|\phi\rangle = (a^*\langle 0| + b^*\langle 1|)(c|0\rangle + d|1\rangle) = (a^*, b^*)\begin{pmatrix} c \\ d \end{pmatrix} = a^*c + b^*d$$

3.3 Qubits: Implementació física

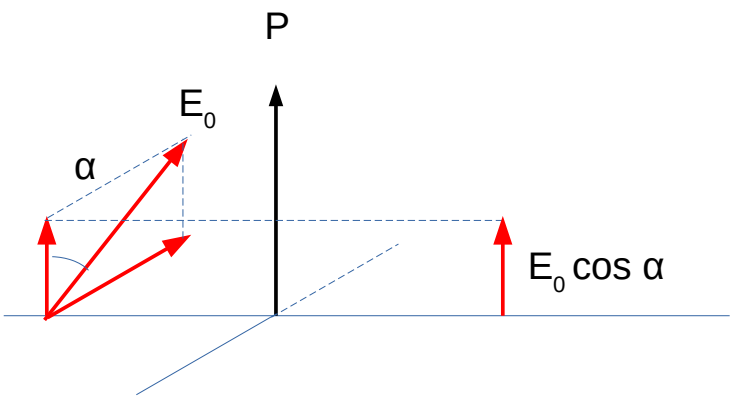
Un qubit podrà ser implementat per qualsevol estat quàntic que es manifesti en dos estats possibles. Nosaltres hem introduït els dos estats d'energia més baixa del potencial unidimensional del pou infinit. Altres exemples són l'espín de l'electró, que pot adoptar només dos valors possibles. A la introducció varem parlar de l'experiment de Stern-Gerlach, que usava l'espín dels àtoms de plata. Hi ha una gamma molt àmplia de sistemes físics que poden usar-se. Entre ells, nosaltres descriurem només els fotons, ja que tindran un paper rellevant en un dels protocols més famosos, el BB84. Els qubits fotònics s'implementen en la polarització del fotó.

Sabem que la llum es comporta com una ona electromagnètica, oscil·lacions elèctriques i oscil·lacions magnètiques que es produeixen perpendiculars entre si i perpendiculars a la direcció de propagació de l'ona.



Quan les oscil·lacions elèctriques es produeixen sempre en el mateix pla es diu que l'ona està linealment polaritzada.

La llum produïda per bombetes, la llum del sol, etc, són exemples de llum no polaritzada. Si llum no polaritzada passa per una làmina polaritzadora, polaritzador d'ara endavant, amb un eix donat, la llum que en surt està linealment polaritzada en la direcció de l'eix del polaritzador. La intensitat de la llum transmesa (i, per tant, polaritzada) és el 50% de la llum -no polaritzada- incident. A més, quan llum linealment polaritzada paral·lelament a l'eix d'un polaritzador incideix sobre ell, la llum transmesa ho és en la direcció del polaritzador i amb el 100% d'intensitat. En canvi, si llum linealment polaritzada incideix de manera que el seu pla de polarització forma un angle de 90° amb l'eix del polaritzador,



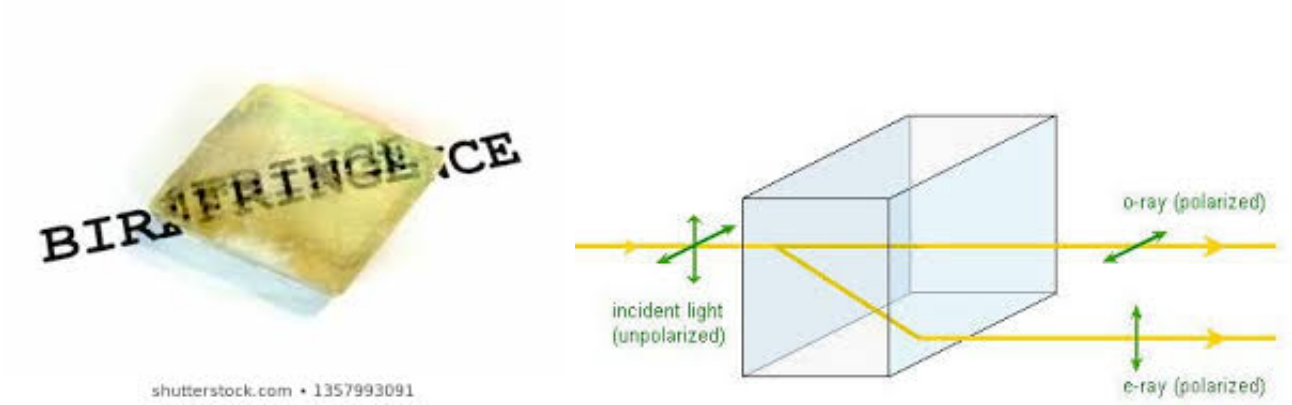
la intensitat transmesa és nul·la. Quan la polarització de la llum i l'eix del polaritzador formen un angle α, aleshores es pot descompondre el vector amplitud $\vec{E}_0$ en una component paral·lela, $\vec{E}_0 \cos\alpha$, i una altra perpendicular, $\vec{E}_0 \sin\alpha$, al polaritzador P, de manera que només la component paral·lela es transmet. La llum emergeix polaritzada, paral·lelament al polaritzador, i la seva intensitat –proporcional al quadrat de l'amplitud– ve donada per

$$I_s = (E_0 \cos\alpha)^2 = E_0^2 \cos^2\alpha = I_e \cos^2\alpha,$$

amb I_s la intensitat de la llum transmesa o sortint, i I_e la intensitat de la llum incident o d'entrada. $\vec{E}_0 \cos\alpha$

Quan un pensa en termes de fotons individuals, polaritzats linealment, incidint sobre un polaritzador ideal (sense pèrdues d'absorció, per exemple), amb α l'angle que forma la polarització del fotó amb l'eix del polaritzador, $\cos^2\alpha$ és la probabilitat que el fotó travessi el polaritzador i adopti la seva polarització. $\sin^2\alpha$ és la probabilitat que el fotó sigui absorbit al polaritzador.

Existeixen els materials birefringents que tenen també un eix que els caracteritza. Difereixen dels polaritzadors en que, quan els arriba llum amb una polarització lineal que forma un angle α amb el seu eix, apareixen dos feixos de llum: el raig ordinari, polaritzat paral·lelament a l'eix del material birefringent amb una intensitat proporcional a $\cos^2\alpha$, i el raig extraordinari, polaritzat perpendicularment amb una intensitat proporcional a $\sin^2\alpha$. Si, en canvi, és un fotó qui incideix, aleshores $\cos^2\alpha$ ($\sin^2\alpha$) és la probabilitat de que el fotó surti amb polarització paral·lela (perpendicular) a l'eix. Es pot considerar un aparell que mesura la polarització dels fotons en una base paral·lela/perpendicular a l'eix del material birefringent.



3.4 Mesures. Probabilitats i Col·lapse de la mesura

Imaginem que tenim un qubit en l'estat $|0\rangle$ -que correspon a trobar-se en la funció d'ona $\phi_1(x,t)$ en el model que hem estudiat-. Si mesurem el seu estat usant la base canònica $\{|0\rangle, |1\rangle\}$, amb probabilitat 1 trobarem l'estat $|0>$ (la seva energia, E_1, la de l'estat fonamental). Pensem ara que, en canvi, partim d'un estat que és una combinació lineal (superposició):

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,.$$

Si el mesurem en la base canònica, la probabilitat de trobar-lo en $|0\rangle$ és $|a|^2$ i la de trobar-lo en $|1\rangle$ és $|b|^2$. Podem expressar-ho com

$$p_0 = |\,\langle 0|\psi\rangle\,|^2 = |a|^2; \quad p_1 = |\,\langle 1|\psi\rangle\,|^2 = |a|^2.$$

Si volem saber quines són les probabilitats que tindríem si mesuréssim en una altra base, el procediment seria anàleg. Per exemple, Si mesuréssim el mateix estat $|\psi\rangle$ en la base $\{|+\rangle_x, |-\rangle_x\}$,

$$p_{+x} = |_x\langle +|\psi\rangle|^2 = |\frac{1}{\sqrt{2}}(\langle 0| + \langle 1|)|\psi\rangle|^2 = |\frac{a+b}{\sqrt{2}}|^2$$
$$p_{-x} = |_x\langle -|\psi\rangle|^2 = |\frac{1}{\sqrt{2}}(\langle 0| - \langle 1|)|\psi\rangle|^2 = |\frac{a-b}{\sqrt{2}}|^2.$$

Amb més generalitat, podem usar una base parametritzada pels angles θ, φ, la donada per $\{|+>_{\theta,\varphi}, |->_{\theta,\varphi}$,

$$p_{+\{\theta,\varphi\}} = |_{\theta,\varphi}\langle +|\psi\rangle|^2 = |\left(\cos\frac{\theta}{2}\langle 0| + \sin\frac{\theta}{2}e^{-i\varphi}\langle 1|\right)|\psi\rangle|^2 = |a\cos\frac{\theta}{2} + b\sin\frac{\theta}{2}e^{-i\varphi}|^2$$

$$p_{-\{\theta,\varphi\}} = |_{\theta,\varphi}\langle -|\psi\rangle|^2 = |\left(-\sin\frac{\theta}{2}\langle 0| + \cos\frac{\theta}{2}e^{-i\varphi}\langle 1|\right)|\psi\rangle|^2 = |-a\sin\frac{\theta}{2} + b\cos\frac{\theta}{2}e^{-i\varphi}|^2$$

Es pot comprovar que les dues probabilitats obtingudes sumen 1.

Col.lapse en la mesura:

Pensem novament que tenim un estat inicial $|\psi\rangle$ i el mesurem en la base canònica. Un cop realitzada la mesura, l'estat deixa de ser l'inicial, col·lapsa i es transforma en l'estat mesurat: ja sigui $|0\rangle$ o $|1\rangle$. Suposem que hem trobat l'estat $|0\rangle$. Si insistíssim en seguir mesurant-lo en la mateixa base, trobaríem novament $|0\rangle$: l'estat inicial $|\psi\rangle$ ha col·lapsat en l'estat $|0\rangle$.

Això es veu en l'exemple dels fotons. Si la polarització vertical (horitzontal) correspon a l'estat$|0\rangle$ ($|1\rangle$), quan es mesura quina polarització té un estat combinació lineal que forma un angle α amb l'eix vertical, fent-lo passar a través d'un material birefringent amb eix vertical, el fotó sortirà o bé amb polarització vertical (amb probabilitat a priori $\cos^2\alpha$), o en polarització horitzontal (amb probabilitat a priori $\sin^2\alpha$). La mesura de la seva polarització col·lapsa l'estat en una de les dues polaritzacions de la base.

3.5 Estats de dos qubits

Un sistema de dos qubits el designem com un producte tensorial. Per exemple, si tenim dos qubits cadascun en l'estat $|0\rangle$, descrivim el sistema dels dos com

$$|0\rangle \otimes |0\rangle$$

Com que un qubit pot estar en superposició, podem tenir estats del tipus

$$|\psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}; \quad |\phi\rangle = c|0\rangle + d|1\rangle = \begin{pmatrix} c \\ d \end{pmatrix},$$

$$
\begin{aligned}
|\psi\rangle \otimes |\phi\rangle &= (a\,|0\rangle + b\,|1\rangle) \otimes (c\,|0\rangle + d\,|1\rangle) \\
&= ac\,|0\rangle \otimes |0\rangle + ad\,|0\rangle \otimes |1\rangle + bc\,|1\rangle \otimes |0\rangle + bd\,|1\rangle \otimes |1\rangle \\
&= ac\,|0\rangle\,|0\rangle + ad\,|0\rangle\,|1\rangle + bc\,|1\rangle\,|0\rangle + bd\,|1\rangle\,|1\rangle \\
&= ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle \\
&= \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix},
\end{aligned}
$$

on hem anat simplificant la notació, obviant el símbol del producte tensorial, reagrupant els "kets" i, finalment, usant la notació matemàtica amb vectors, que ens ha permès definir el seu producte tensorial.

Aquest exercici ens fa adonar que el sistema de dos qubits també té una base (canònica) que és:

$$
\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}.
$$

Això implica que tota combinació lineal dels elements de la base d'estats de dos qubits, és un estat possible per aquests dos qubits. En l'exemple anterior, l'estat

$$
|\psi\rangle \otimes |\phi\rangle
$$

és un estat separable, doncs es pot expressar com el producte tensorial dels dos qubits individuals. No sempre tindrem aquest tipus de comportament. Per exemple, l'estat següent és possible però no és separable:

$$
|\beta_{00}\rangle = \frac{1}{\sqrt{2}} (|0\rangle\,|0\rangle + |1\rangle\,|1\rangle)
$$

doncs no es pot separar en dos qubits. És un exemple del que se'n diu estat entrellaçat (entangled).

3.6 Estats de múltiples qubits

La generalització a estats de més qubits és clara. Per n qubits:

$$
|\psi\rangle_n = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle.
$$

La dimensionalitat de l'espai de Hilbert en el que viu és 2^n. Si el volguéssim representar en la base matemàtica, hauríem de fer-ho amb un vector de 2^n components. Està clar que la representació en termes de "kets" és més convenient, sobretot per n grans.

3.7 Exercicis

A continuació trobareu una sèrie d'exercicis sobre qubits i sistemes de qubits:

EXERCICI COMPUTACIÓ QUÀNTICA

QUANTITZACIÓ

En l'exemple del pou quadrat infinit, amb $V(x) = 0$, per $0 \leq x \leq L$, i $V(x) = \infty$ si $x < 0$ o $x > L$, hem vist que les **funcions d'ona** que obtenim al resoldre l'equació de Schrödinger són

$$\psi_i(x,t) = \varphi_i(x) e^{-i\frac{E_i}{\hbar}t}, \tag{1}$$

on les parts que depenen de x s'anomenen **estats propis de l'energia**

$$\varphi_1(x) = \sqrt{\frac{2}{L}} \sin(\frac{\pi}{L}x)$$

$$\varphi_2(x) = \sqrt{\frac{2}{L}} \sin(2\frac{\pi}{L}x)$$

$$\varphi_3(x) = \sqrt{\frac{2}{L}} \sin(3\frac{\pi}{L}x)$$

$$\dots$$

Les transicions entre aquests estats d'energia donada són les que es detecten en experiments d'espectroscòpia. Doneu l'expressió de la freqüència del fotó que s'emet quan el sistema passa del primer estat excitat (ψ_2) a l'estat fonalmental (ψ_1)

Resposta 1

PROBABILITAT

Escriviu la densitat de **probabilitat** ($p_i(x) = \psi_i \cdot \psi_i^*$) per l'estat ψ_4

Resposta 2

Si la funció d'ona que descriu la partícula és $\psi_4(x,t)$, quina és la probabilitat de que al mesurar la seva posició la trobem a $x = L/2$?

Resposta 3

SUPERPOSICIÓ

Qualsevol **superposició** de funcions d'ona també serà solució

$$\psi(x,t) = a_1 \cdot \psi_1 + a_2 \cdot \psi_2 + \dots$$

i, per tant, també és un estat possible de la partícula. Els $\{a_i\}$ són nombres complexos qualsevol amb la condició que es compleixi

$$\int \psi^* \cdot \psi dx = 1. \tag{2}$$

Insertant l'expressió 1

$$\psi(x,t) = a_1 \cdot e^{-i\frac{E_1}{\hbar}t}\varphi_1(x) + a_2 \cdot e^{-i\frac{E_2}{\hbar}t}\varphi_2(x) + \dots$$

que es pot simplificar englobant totes les constants numèriques en els coeficients $\{c_i(t)\}$

$$\psi(x,t) = c_1(t) \cdot \varphi_1(x) + c_2(t) \cdot \varphi_2(x) + \dots \tag{3}$$

BASE

Aquesta expressió ens indica que les funcions φ_i constitueixen una *base* de les funcions. Compleixen ademés les següents condicions d'*ortonormalitat*

$$\int \varphi_i \varphi_j^* dx = 0 \qquad\qquad i \neq j$$

$$\int \varphi_i \varphi_i^* dx = 1$$

comproveu que el valor de la següent integral és 0
$\int_0^L \varphi_1(x)\varphi_2(x)dx = \frac{2}{L}\int_0^L sin(\frac{\pi}{L}x)sin(2\frac{\pi}{L}x)dx = \dots$
Resposta 4

tingueu en compte que es compleix per la integral indefinida:

$$\int sin(ax)sin(bx)dx = \frac{sin[(a-b)x]}{2(a-b)} - \frac{sin[(a+b)x]}{2(a+b)}$$

PROBABILITATS D'OCUPACIÓ

Aquestes propietats ens permeten interpretar els coeficients $\{c_i\}$. Si apliquem la condició de normalització 2, la majoria de termes són nuls i resulta

$$1 = \int \psi^* \cdot \psi dx = c_1^* \cdot c_1 + c_2^* \cdot c_2 + \dots \tag{4}$$

per tant podem interpretar $c_i^* \cdot c_i$ com la probabilitat de que al fer una mesura de l'energia trobem que el sistema es trobi en l'estat descrit per φ_i.

Donada la següent superposició, quina és la probabilitat de cada un dels estats?

$$\psi = \frac{\sqrt{6}}{\pi}\{\varphi_1(x) + \frac{1}{2} \cdot \varphi_2(x) + \frac{1}{3} \cdot \varphi_3(x) + \dots\}$$

Resposta 5

Donat el següent estat, quin valor de N fa que estigui normalitzat correctament?

$$\psi = \frac{1}{N}\{5 \cdot \varphi_1(x) + 8 \cdot \varphi_2(x)\}$$

Resposta 6

KETs i BRAs

En lloc d'aquesta notació tant feixuga, adoptem la notació de Dirac en termes de símbols anomenats *kets*: utilitzem $\mid 0 >$ en lloc de $\varphi_1(x)$, etc. Així, en lloc d'utilitzar (3), diem que el sistema es troba en un cert estat $\mid a >$ que es pot expressar com

$$\mid a >= c_1 \mid 0 > + c_2 \mid 1 > + \ldots \tag{5}$$

En termes d'aquesta notació, les integrals s'expressen com

$$\int \phi^*(x) \cdot \varphi(x) dx \equiv < \phi \mid \varphi > \tag{6}$$

Una forma alternativa de pensar en aquesta mena d'integrals consisteix en definir per cada *ket* un altre vector anomenat *bra* i representat $< a \mid$, de forma que la integral es pot entendre com el *producte escalar* (*braket*) d'aquestes dos vectors

$$< \phi \mid \varphi >= (< \phi \mid) \cdot (\mid \varphi >) \tag{7}$$

QUBIT

Per les aplicacions de Computació i Criptografia Quàntica en tenim prou amb dos estats, per exemple amb els dos estats de menor energia del pou infinit (altres sistemes directament sols tenen dos estats, com per exemple l'spin de l'electró). Per tant sols ens ocuparem d'aquells estats que es poden expressar com combinació lineal d'aquests dos

$$\mid a >= \alpha \mid 0 > + \beta \mid 1 >, \tag{8}$$

on els coeficients han de satisfer

$$\alpha^* \cdot \alpha + \beta^* \cdot \beta = 1. \tag{9}$$

Es pot deduir que la forma més general per un qubit involucra dos paràmetres (θ, ϕ)

$$\mid a >= \cos(\theta/2) \mid 0 > + e^{i\phi} \sin(\theta/2) \mid 1 > \tag{10}$$

Escriviu quatre estats possibles *diferents* d'un qubit pels quals la probabilitat de trobar-lo en cada estat sigui la mateixa

Resposta 7

representeu-los gràficament sobre l'esfera de Bloch

Resposta 8

SISTEMES AMB MÉS D'UN QUBIT

Si tenim més d'un qubit, escrivim l'estat del sistema com un producte. Així si el primer qubit es troba en l'estat $\mid 0 >$ i el segon en l'estat $\mid 1 >$, llavors tindrem l'estat

$$\mid 0 >\mid 1 > \equiv \mid 01 > \equiv \mid 1 >_2 \equiv \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \tag{11}$$

que com veieu es pot expressar en un cert nombre de notacions.

Donat el següent estat de dos qubits

$$\frac{1}{\sqrt{2}}(\mid 0 > + \mid 1 >) \cdot \frac{\mid}{\sqrt{2}}(\mid 0 > + \mid 1 >)$$

expresseu-lo en les diferents notacions.

Resposta 9

Idem per l'estat d'un sistema de 3 qubits que s'expressi com el producte

$$\frac{1}{\sqrt{5}}(\mid 0 > +2 \mid 1 >) \cdot \frac{1}{\sqrt{2}}(\mid 0 > - \mid 1 >) \cdot \mid 1 >$$

Resposta 10

ENTANGLEMENT

Els dos exercicis anteriors tracten amb estats que resulten del producte d'estats ben definits per cada qubit, però aquest no és el cas general. Hi ha estats (*entangled*) pels quals no podem dir que cada qubit individual estigui caracteritzat per un estat deslligat dels altres qubits.

Més en detall, un estat qualsevol de dos qubits es pot escriure

$$\phi >= \alpha \mid 00 > + \beta \mid 01 > + \gamma \mid 10 > + \delta \mid 11 > \tag{12}$$

on els coeficients sols han de satisfer la condició de normalització (2).

En contraposició un estat factoritzable s'escriu

$$\begin{aligned} \mid \phi >\mid \varphi > &= (a(\mid 0 > + b \mid 1 >) \cdot (c \mid 0 > + d \mid 1 >) \\ &= ac \mid 00 > + ad \mid 01 > + bc \mid 10 > + bd \mid 11 > \end{aligned} \tag{13}$$

de forma que, com veiem, els coeficients satisfan la condició addicional

$$\alpha\delta = \beta\gamma \tag{14}$$

Digueu si $\mid \phi >= \frac{1}{\sqrt{2}}(\mid 00 > + \mid 11 >)$ és entangled
Resposta 11

Si definim una nova base $\{\mid + >, \mid - >\}$ per un qubit individual com

$$\mid 0 > \equiv \frac{1}{\sqrt{2}}(\mid + > + \mid - >)$$

$$\mid 1 > \equiv \frac{1}{\sqrt{2}}(\mid + > - \mid - >)$$

com s'expressa l'estat $\mid \phi >$ en aquesta base?
Resposta 12

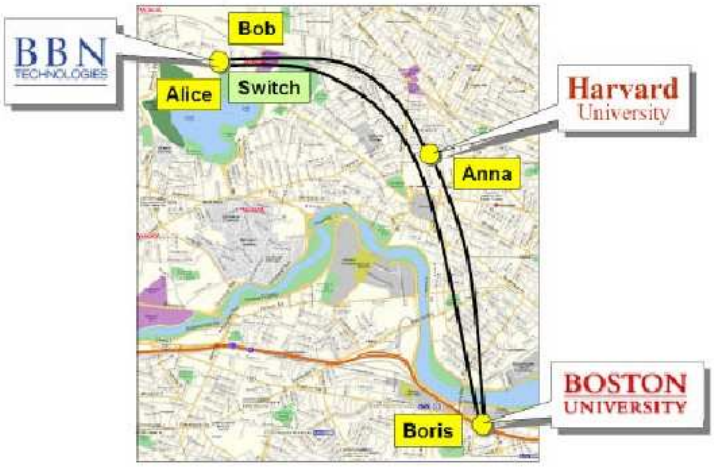
4 Criptografia Quàntica

Una vegada hem descrit el col·lapse en la mesura i el teorema de no-clonació, podem entendre com construir claus criptogràfiques compartides per una persona emissora, Alice, i un receptor, Bob.

Criptografia Quàntica:

Protocols d’Eckert i BB84

Criptografia Quàntica: Precedents



- DARPA Quantum Network
- Operacional al Juny del 2004
- Link per aire al Juny del 2005

BBN Technologies va ser la companyia que va montar el precursor de l'actual INTERNET a l'any 1969 (ARPANET)

…és tecnologia comercial!

Quantum Key Server

Toshiba's Quantum Key Server delivers digital keys for cryptographic applications on fibre optic based computer networks. Based on quantum cryptography it provides a failsafe method of distributing verifiably secret digital keys, with significant cost and key management advantages.

The system provides world-leading performance. In particular, it allows key distribution over standard telecom fibre links exceeding 100km in length and bit rates sufficient to generate up to 100 256-bit keys per second.

Toshiba's system uses a simple architecture, in which the photons travel from sender to receiver. This is the only design that has been rigorously proven as secure from all types of eavesdropping attack. This ensures that the Toshiba design will be secure not only today, but also in the future.

Toshiba have pioneered active stabilisation technology that allows the system to distribute key material continuously, in even the most challenging operating conditions, without any user intervention. This avoids the need for recalibration of the system due to temperature-induced changes in the fibre lengths. Initiation of the system is also managed automatically, allowing simple turn-key operation.

The system can be used for a wide range of cryptographic applications, eg encryption or authentication of sensitive documents, messages or transactions. A programming interface gives the user access to the key material.

Einstein-Podolsky-Rosen (EPR)

Van fer notar que estats com aquest

$$|0\rangle\,|0\rangle + |1\rangle\,|1\rangle$$

tenen propietats aparentment paradoxals, que actualment s'anomenen

ENTRELLAÇAMENT

(**ENTANGLEMENT**)

“Li estires la cua a Nova York, i el cap miola a Los Angeles” A. Einstein

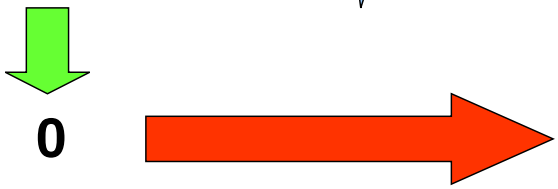
Generem dos qubits en el següent estat

$$|0\rangle\,|0\rangle + |1\rangle\,|1\rangle$$

Probabilitat del 50% de que mesurem alguna d’aquestes dues configuracions

I ara els separem un de l’altre … tant com vulguem

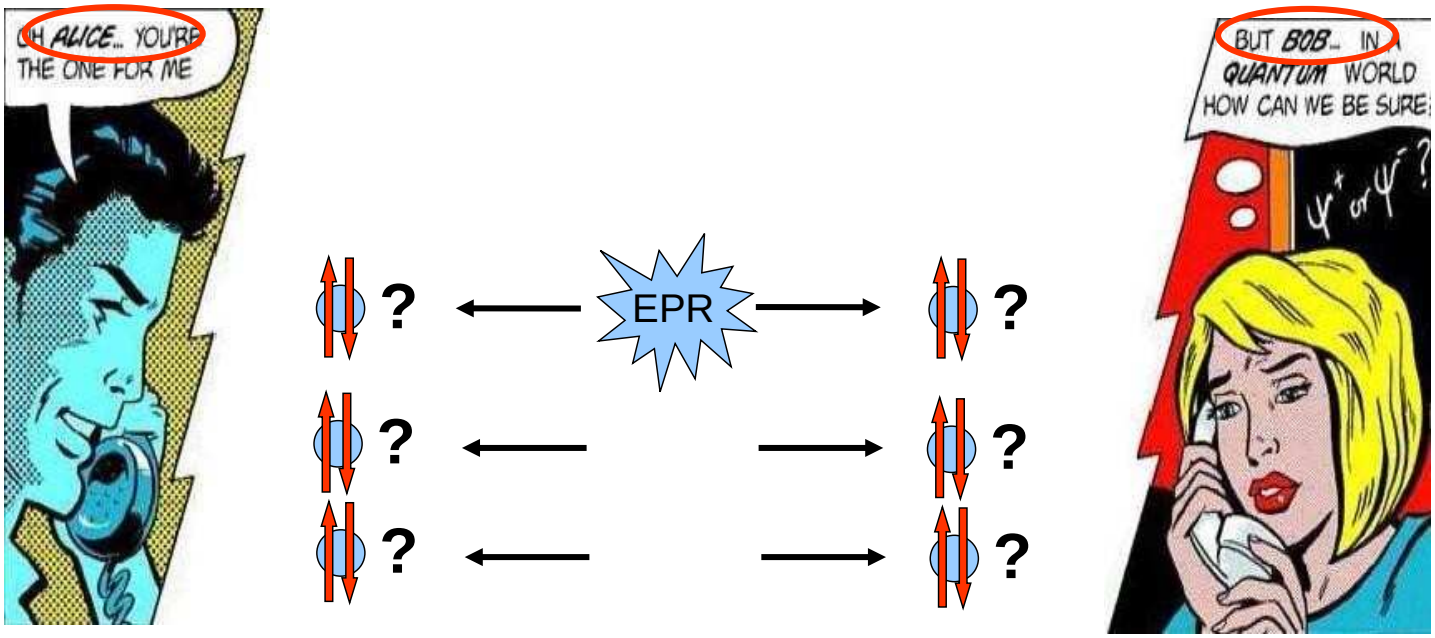
Mesurem aquest qubit



Sabem que quan aquest es mesuri obtindrem també un 0

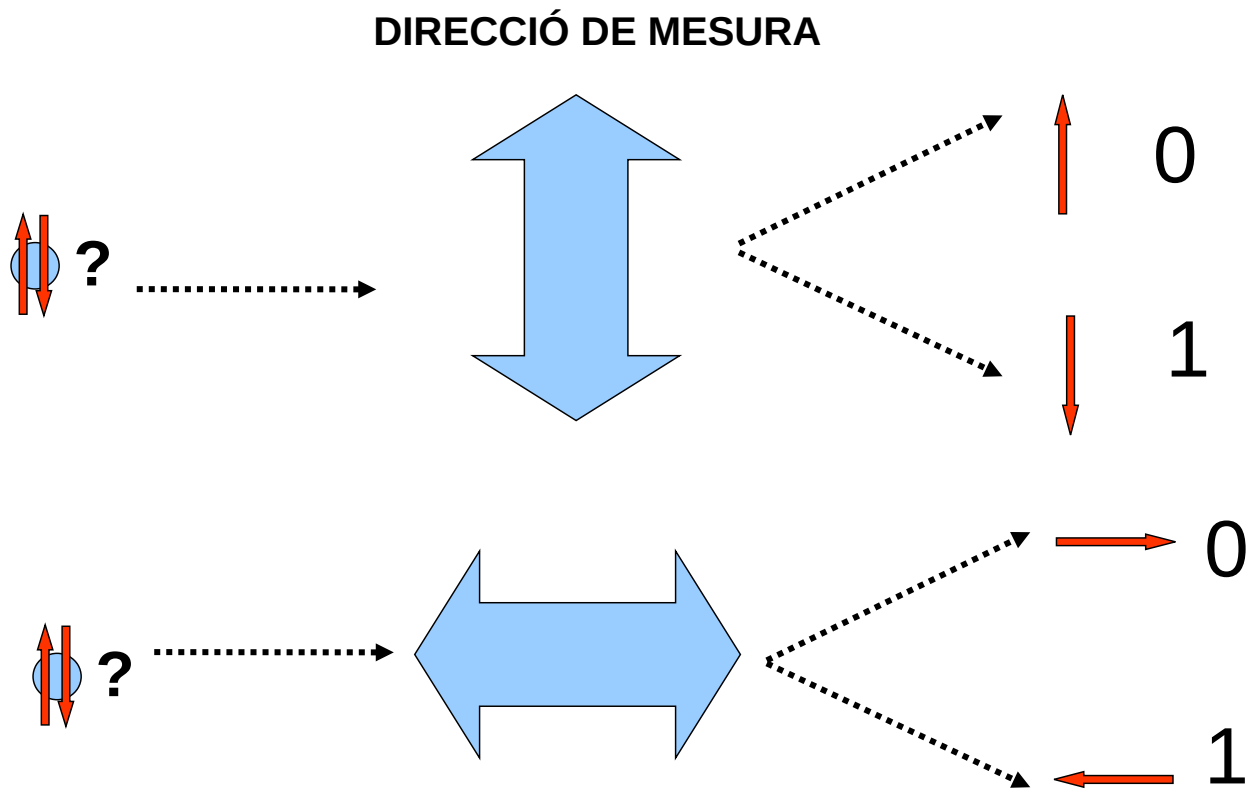
Protocol d'Ekert (no és el més popular)

Tenim dues persones que es volen comunicar secretament

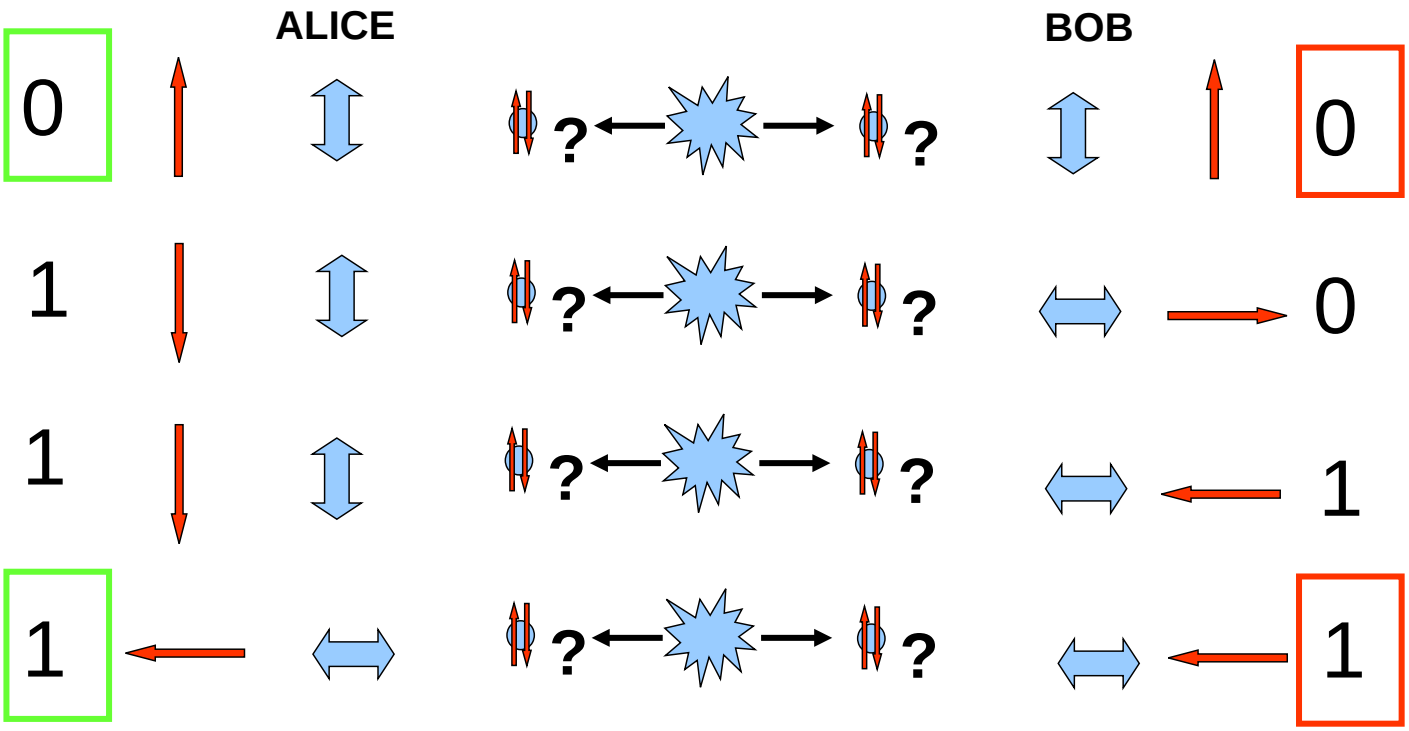


Amb aquests parells generaran una **CLAU**

Poden mesurar en dues direccions



Direccions de mesura a l'atzar



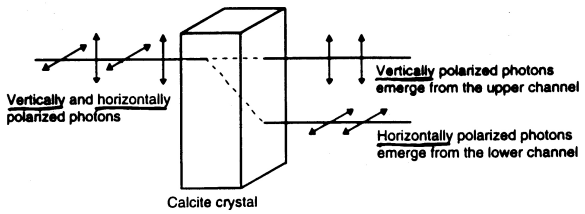
Anuncien les bases públicament i descarten les no coincidències

CLAU NUMÈRICA: **0 1**

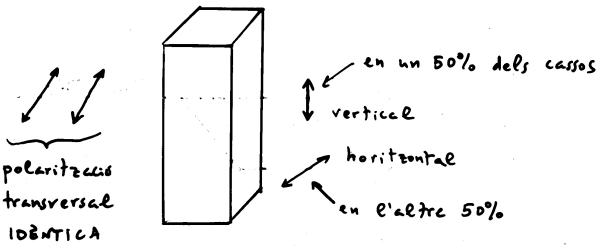
Criptografia Quàntica

Protocol BB84

Els estats de polarització es poden mesurar amb un cristall orientat convenientment

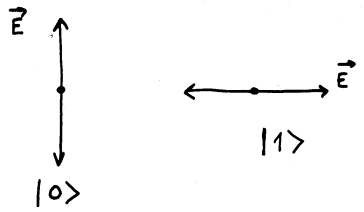


Ara bé, si no està orientat correctament obtenim cada una de les polaritzacions amb una probabilitat del 50%

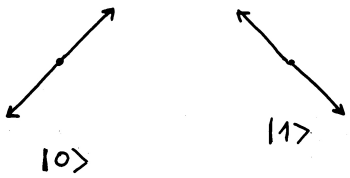


EXEMPLE DE MÈTODE PER ENVIAR CLAUS

Hem vist que podem codificar els 0s i 1s en les polaritzacions verticals/horitzontals dels fotons

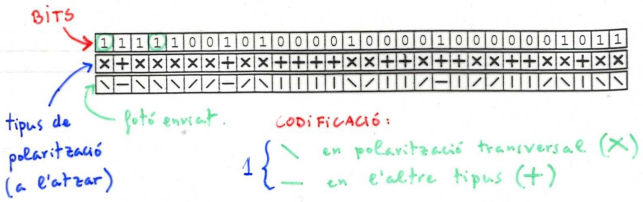


Podem fer exactament el mateix respecte a uns eixos orientats 45° respecte dels anteriors

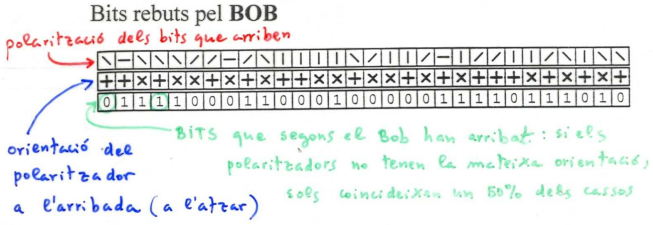


Polarització transversal

Bits enviats per **ALICE**



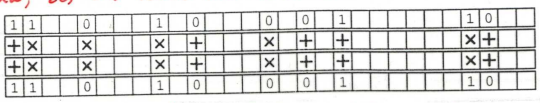
Bits rebuts pel **BOB**



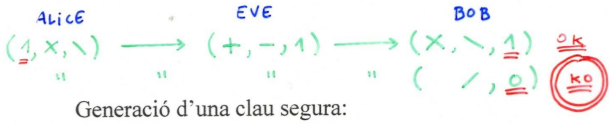
Ara es comuniquen per un canal insegur:

- Alice li diu a Bob quina era l'orientació per un **subconjunt** de bits
- Bob li diu l'orientació que ell ha fet servir en cada cas.
- Alice li diu els bits que hauria mesurat: **si el canal no està intervingut haurien de coincidir.**

En tots els casos que l'orientació dels polaritzadors és la mateixa, els bits rebuts han de coincidir

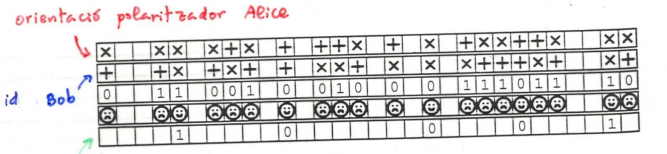


Si hi ha algú observant els fotons, els bits NO COINCIDIRAN EN ALGUNS CASOS



Generació d'una clau segura:

- Alice li diu a Bob l'orientació per tots els bits, però no el valor d'aquests bits
- Bob dedueix una seqüència de bits a partir dels cassos en que han utilitzat la mateixa orientació



quan són la mateixa, prenem aquests bits per generar una CLAU SEGURA que podem utilitzar per enviar informació encriptada de la forma habitual

"SIFTED" KEY

Teorema de No-Clonació

Potser és possible clonar ovelles, però no ho és clonar estats quàntics

5 Evolució unitària

Nosaltres estem enfocats en fer ús dels qubits per computació, apart de criptografia. Això vol dir que hem de ser capaços de fer canvis en els qubits, és a dir, de fer-los evolucionar. Si recordem novament el nostre exemple dels dos estats d'energia més baixa del pou infinit, ja varem veure que una combinació lineal dels dos no és estacionària, sinó que presenta una variació temporal,

$$\psi(x,t) = a\psi_1(x)e^{-iE_1t/\hbar} + b\psi_2(x)e^{-iE_2t/\hbar} = e^{-iE_1t/\hbar}\left(a\psi_1(x) + b\psi_2(x)e^{-i(E_2-E_1)t/\hbar}\right),$$

on suposem que l'estat està correctament normalitzat ($|a|^2+|b|^2=1$), prenem a i b reals, i hem posat de manera explícita una fase global que és, com sabem, prescindible. Per tant, apart d'aquesta fase global, definint $\omega = -(E_2-E_1)/\hbar$, i usant la notació de Dirac ($\psi_1(x) = |0\rangle\,; \psi_2(x) = |1\rangle$, el nostre estat varia en el temps com

$$|\psi(t)\rangle = a\,|0\rangle + be^{i\omega t}\,|1\rangle\,.$$

Si comparem aquesta expressió amb el qubit més general possible,

$$|+\rangle_{\theta,\varphi} = \cos\frac{\theta}{2}\,|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}\,|1\rangle$$

veiem que

$$a = \cos\frac{\theta}{2}; b = \sin\frac{\theta}{2}; \varphi = \omega t,$$

és a dir, que el nostre estat "punxa" segons la direcció donada per θ i $\varphi(t)$ a l'esfera de Bloch, amb

$$\theta = 2\arccos(a) = 2\arcsin(b); \quad \varphi(t) = \omega t,$$

un angle zenital fixat i l'azimutal que augmenta en el temps: el qubit precessa en el pla azimutal i la fase relativa del ket $|1\rangle$ respecte de $|0\rangle$ augmenta en el temps a raó de $\varphi(t) = \omega t$: En llenguatge computacional, l'efecte d'esperar un temps t equival a aplicar una porta quàntica: la Porta phase-shift $\Phi(\varphi(t) = \omega t)$ (canvi de fase relatiu).

Tot i aquesta dependència en el temps, si mesurem el qubit en la base canònica, les probabilitats de trobar el qubit en els estats $|0\rangle$ i $|1\rangle$, respectivament són

$$p_0 = |\,\langle 0|+\rangle_{\theta,\varphi}\,|^2 = \cos^2\frac{\theta}{2} = a^2; \quad p_1 = |\,\langle 1|+\rangle_{\theta,\varphi}\,|^2 = \sin^2\frac{\theta}{2} = b^2,$$

que no varien en el temps. Això vol dir que, per molt que esperem, el nostre estat no canvia les probabilitats. Canviar les probabilitats vol dir canviar l'angle zenital θ i això el nostre model no ho fa. Necessitem fer alguna cosa més que esperar perquè el nostre qubit sigui útil per computació.

El problema se soluciona pertorbant el sistema, afegint un potencial que depèn del temps, com pot ser un pols d'una ona electromagnètica. Quan això passa, la solució (al pou infinit en el nostre cas) es pot seguir expressant com una combinació lineal dels elements de la base del sistema no pertorbat, però on ara els coeficients depenen del temps, de forma no trivial i no són només fases temporals, sinó que els mòduls depenen de t. Així poden canviar doncs les probabilitats.

Fem una pinzellada de com es poden fer aquests polsos amb un exemple senzill. Considerem dues càrregues puntuals de valors q i $-q$, situades en els punts A i B, respectivament, separades una distància d i orientades segons el vector $\vec{d}$. Si connectem un camp elèctric uniforme $\vec{E}$ que forma un angle α amb $\vec{d}$, l'augment d'energia potencial que adquirirà el sistema serà

$$qV_A - qV_B = q(V_A - V_B),$$

amb

$$V_A - V_B = -Ed\cos\alpha = -\vec{E}\cdot\vec{d}.$$

Si ara pensem que el camp elèctric és variable en el temps, de manera que

$$\vec{E} = \vec{E}_0\cos(\omega t)$$

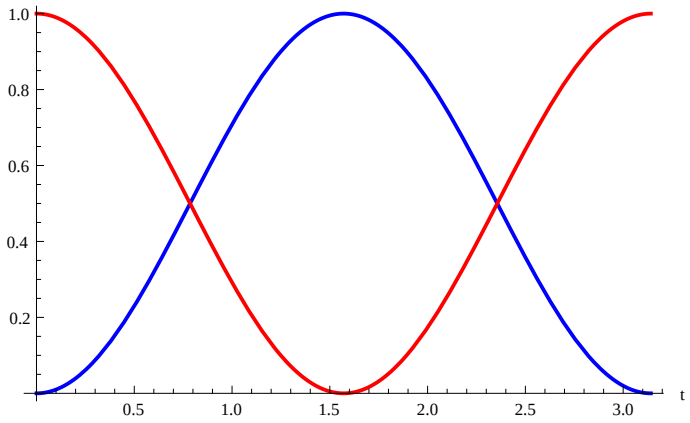
aleshores

$$(V_A - V_B)(t) = -\vec{E}\cdot\vec{d}\cos(\omega t).$$

Es pot demostrar que si la freqüència angular del camp aplicat coincideix amb la de l'evolució del sistema,

$$\omega = -\frac{E_2 - E_1}{\hbar}$$

aleshores és quan apareixen els efectes més espectaculars, que vénen resumits en aquesta gràfica: on



a l'escala horitzontal hi ha el temps i a l'escala vertical la probabilitat de trobar la partícula en l'estat $|0\rangle$, en vermell, o en l'estat $|1\rangle$, en blau. Aquestes probabilitats són periòdiques, amb un període $T = \frac{2\pi}{\omega}$. Així, partint a l'instant inicial de $|0\rangle$ aquest es transforma, amb probabilitat 1 en l'estat $|1\rangle$ quan $t = T/2$. Hauríem implementat la porta NOT (esperant el temps $t = T/2$). El que es pot fer amb un bit es pot fer doncs amb un qubit.

Un cas que ens serà d'interès és l'estat que s'obté a l'instant $t = T/4$, on les probabilitats de trobar-lo en $|0\rangle$ i $|1\rangle$ són les mateixes i iguals a $1/2$. L'estat és la superposició

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Aquesta transformació es defineix com la Porta Hadamard (H):

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

Aquesta porta ens permet generar superposicions dels estats de la base, superposicions de 0 i 1, inexistents pels bits clàssics. La porta Hadamard és una porta quàntica que no té cap anàleg en la computació clàssica.

6 Evolució temporal

Si retornem al que coneixem de l'equació de Schrödinger, la combinació de varis estats estacionaris té una dependència temporal. De fet, si ens restringim a només dos estats possibles -recordem que estem interessats en qubits- l'expressió d'una superposició d'ells dos representa un qubit.

$$\begin{aligned}\psi(x,t) &= a\psi_1(x,t) + b\psi_2(x,t) \\ &= a\psi_1(x)e^{-iE_1t/\hbar} + b\psi_2(x)e^{-iE_2t/\hbar} \\ &= a(t)\psi_1(x) + b(t)\psi_2(x)\end{aligned}$$

on a la darrera línea usem la notació $a(t) = ae^{-iE_1t/\hbar}; \quad b(t) = be^{-iE_2t/\hbar}$.

L'expressió anterior ens permet parlar de l'operador d'evolució temporal, $U(t)$, per qualsevol sistema quàntic que vingui descrit per una equació de Schrödinger: Si a l'instant inicial, $t = 0$, l'estat ve descrit per $\Psi(x, 0)$, al cap d'un temps t estarà descrit per $\Psi(x, t)$

$$\Psi(x,0) \longrightarrow \Psi(x,t) = U(t)\Psi(x,0)$$

que representa que canvien els coeficients de la superposició en el temps.

La transformació és lineal -perquè ve descrita per l'eq. de Schrödinger, que és lineal- i suposa passar dels valors a l'instant inicial als de l'estat final. Una transformació lineal quan els estats vénen descrits per vectors de dimensió 2 ve descrita per una matriu 2×2. Podem definir doncs una matriu 2×2, $U(t)$ que ens descriu l'evolució temporal:

$$\begin{pmatrix} a(t) \\ b(t) \end{pmatrix} = U(t) \begin{pmatrix} a(0) \\ b(0) \end{pmatrix}$$

Què vol dir que l'operador, a més de lineal, sigui unitari? Vol dir que es conservi la norma (la normalització de l'estat). Si l'estat inicial -obviem la dependència en x, doncs estem interessats en la dependència en t- el representem per un "ket" $|\psi(0)\rangle$, normalitzat, això implica que

$$\langle\psi(0)|\psi(0)\rangle = 1$$

En passar un temps t,

$$\begin{aligned}|\Psi(0)\rangle \quad &\longrightarrow |\Psi(x,t)\rangle = U(t)\,|\Psi(x,0)\rangle \\ \langle\Psi(0)| \quad &\longrightarrow \langle\Psi(x,t)| = \langle\Psi(x,0)|\,U(t)^\dagger\end{aligned}$$

on $U(t)^\dagger$ és l'operador transposat i complex conjugat de $U(t)$. Que es conservi la norma implica que

$$\langle\psi(t)|\psi(t)\rangle = 1,$$

que implica

$$\langle\psi(t)|\psi(t)\rangle = \langle\psi(0)|\,U(t)^\dagger U(t)\,|\psi(0)\rangle = \langle\psi(0)|\psi(0)\rangle = 1,$$

és a dir, que l'operador evolució temporal, a més de lineal, ha de verificar que sigui unitari, és a dir

$$U(t)^\dagger U(t) = \mathbb{1}$$

Ens preguntem ara quina és l'expressió més general possible per descriure l'evolució temporal d'un qubit. Sabem que ha de ser un operador lineal i unitari. Si el representem en la notació que el qubit ve descrit per un vector de dues components, l'operador vindrà descrit per una matriu 2×2 i, aquesta ha de ser unitària. Així, podem escriure la matriu com

$$U(t) = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix}$$

essent

$$U^\dagger(t) = \begin{pmatrix} u_{11}^* & u_{21}^* \\ u_{12}^* & u_{22}^* \end{pmatrix}$$

la seva transposada i complex conjugada (no hem escrit la dependència del temps dels seus termes, per alleugerir la notació). Que la matriu sigui unitària vol dir que hem d'imposar que $U^\dagger(t)U(t) = \mathbb{1}$.

Una altra manera d'enfocar el problema és que la matriu que busquem ha de ser capaç de transformar l'estat $|0\rangle$ en el ket més general possible, és a dir

$$U|0\rangle = |+\rangle_{\theta,\varphi} = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}|1\rangle,$$

que, simplificant encara més la notació de la matriu:

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}; \quad U^\dagger = \begin{pmatrix} \alpha^* & \gamma^* \\ \beta^* & \delta^* \end{pmatrix}$$

en notació vectorial s'escriu

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos\frac{\theta}{2} \\ \sin\frac{\theta}{2}e^{i\varphi} \end{pmatrix}.$$

De la igualtat anterior es desprèn que

$$\alpha = \cos\frac{\theta}{2}; \quad \gamma = \sin\frac{\theta}{2}e^{i\varphi}$$

Falta encara aplicar la relació d'unitarietat, $U^\dagger U = \mathbb{1}$. Aquesta implica

$$U^\dagger U = \begin{pmatrix} \alpha^* & \gamma^* \\ \beta^* & \delta^* \end{pmatrix}\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = \begin{pmatrix} |\alpha|^2 + |\gamma|^2 & \alpha^*\beta + \gamma^*\delta \\ \beta^*\alpha + \delta^*\gamma & |\beta|^2 + |\delta|^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

La primera condició, $|\alpha|^2 + |\gamma|^2 = 1$ es satisfà automàticament en ser $\alpha = \cos\frac{\theta}{2}$ i $\gamma = \sin\frac{\theta}{2}e^{i\varphi}$. Falta només trobar β i δ, amb les condicions que

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

i

$$\alpha^*\beta + \gamma^*\delta = \beta\cos\frac{\theta}{2} + \delta\sin\frac{\theta}{2}e^{-i\varphi} = 0.$$

Les dues equacions se satisfan si:

$$\beta = -\sin\frac{\theta}{2}e^{i\phi}$$

i

$$\delta = \cos\frac{\theta}{2}e^{i\varphi}e^{i\phi},$$

on ϕ és una fase arbitraria. Així, recopilant tot, trobem que la matriu unitària més general la podem escriure com:

$$U = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2}e^{i\phi} \\ \sin\frac{\theta}{2}e^{i\varphi} & \cos\frac{\theta}{2}e^{i\varphi}e^{i\phi} \end{pmatrix} e^{i\chi},$$

on θ, ϕ són els dos angles referits a l'esfera de Bloch i ϕ, χ dues fases. Normalment prendrem $\Phi = 0$.

Si un qubit és la versió quàntica d'un bit, veiem doncs que el qubit és molt diferent que un bit. De fet, si disposem d'un bit només podem fer-li dues coses: Deixar-lo com està (aplicar-li la identitat) o canviar-lo d'estat (aplicar-li la porta NOT). En canvi, si disposem d'un qubit podem aplicar-li la porta general que acabem de trobar, on els dos angles i les dues fases varien de manera contínua. Podem aconseguir que el nostre qubit "punxi" en qualsevol direcció de l'esfera de Bloch i no, només, cap al pol Nord o el pol Sud, com fa el bit clàssic. Es desprèn que podrem fer moltes més coses amb qubits que amb bits.

7 Portes quàntiques

Enfocats cap a la Computació Quàntica, els operadors que actuïn sobre estats quàntics els anomenarem portes quàntiques.

7.1 Portes quàntiques d'un qubit

Les portes quàntiques per un qubit les hem "trobat" en l'apartat anterior, en el context de l'exemple del pou de potencial. De fet, tot sistema físic, del microcosmos, que tingui dos estats possibles és candidat a ser un qubit. A partir d'ara, deixarem ja la notació en termes de funcions d'ona i ens centrarem en la notació en termes d'estats quàntics, de kets. La implementació física quedarà obviada.

Les portes (manera de descriure els operadors en llenguatge computacional) d'un qubit que considerarem són (i estan definides sobre els estats de la base canònica $\{|x\rangle, x = 0, 1\}$):

- Identitat: $\mathbb{1}|x\rangle = |x\rangle$
- NOT $= X$: $X|x\rangle = |1 - x\rangle$
- Phase shift: $\Phi(\varphi)|x\rangle = e^{ix\varphi}|x\rangle$
- Hadamard: $H|x\rangle = \frac{1}{\sqrt{2}}((-1)^x|x\rangle + |1 - x\rangle)$

Moltes vegades, la base canònica s'escriu en llenguatge matemàtic i en lloc d'escriure-la en termes de kets $\{|0\rangle, |1\rangle\}$ es fa en termes de vectors:

$$\left\{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\right\}.$$

En aquesta notació, les portes anteriors s'expressen en termes de matrius 2×2:

- Identitat: $\mathbb{1} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$
- NOT $= X = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$
- Phase shift: $\Phi(\varphi) = \begin{pmatrix}1 & 0\\0 & e^{i\varphi}\end{pmatrix}$
- Hadamard: $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$

Recordem que els operadors quàntics U (portes quàntiques) han de ser unitaris: $U^\dagger U = 1$. En el cas de les portes anteriors és fàcil verificar que efectivament, ho són:

- Identitat: $U = \mathbb{1} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}; U^\dagger = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = \mathbb{1}; U^\dagger U = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = \mathbb{1}$

- NOT : $U = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}; U^\dagger = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = X; U^\dagger U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{1}$
- Phase shift: $U = \Phi(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{pmatrix}; U^\dagger = \Phi^\dagger(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\varphi} \end{pmatrix}; U^\dagger U = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{1}$
- Hadamard: $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}; U^\dagger = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H; U^\dagger U = HH = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathbb{1}.$

Una manera alternativa seria veure que són casos particulars de la matriu unitària més general.

És interessant que, només amb les portes Hadamard i la Phase-Shift, podem generar qualsevol estat d'un qubit a partir de l'estat inicial $|0\rangle$. Recordem que l'estat més general és, apart d'una fase global que no és mesurable

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}|1\rangle .$$

Anem a aplicar la seqüència de portes: H, seguida de $\Phi(\theta)$, a continuació una altra H i finalment $\Phi(\varphi + \pi/2)$. L'estat anirà canviant de la manera següent

$$|0\rangle \xrightarrow{\text{H}} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \xrightarrow{\Phi(\theta)} \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle) \xrightarrow{H} \frac{1}{2}\left[|0\rangle + |1\rangle + e^{i\theta}(|0\rangle - |1\rangle)\right] \equiv |\text{tmp}\rangle$$

Falta encara aplicar la darrera porta, $\Phi(\varphi + \pi/2)$. Abans convé reescriure el resultat que tenim, $|\text{tmp}\rangle$ de manera més senzilla:

$$|\text{tmp}\rangle = \frac{1}{2}(1 + e^{i\theta})|0\rangle + (1 - e^{i\theta})|1\rangle = e^{i\frac{\theta}{2}}\left[\frac{(e^{i\frac{\theta}{2}} + e^{-i\frac{\theta}{2}})}{2}|0\rangle + \frac{(e^{-i\frac{\theta}{2}} - e^{i\frac{\theta}{2}})}{2}|1\rangle\right]$$

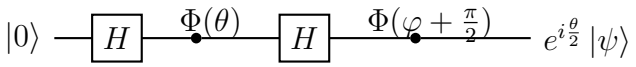
$$|\text{tmp}\rangle = e^{i\frac{\theta}{2}}\left[\cos\frac{\theta}{2}|0\rangle - i\sin\frac{\theta}{2}|1\rangle\right]$$

Si apliquem finalment la darrera porta, obtenim

$$|\text{tmp}\rangle \xrightarrow{\Phi(\varphi+\frac{\pi}{2})} e^{i\frac{\theta}{2}}\left[\cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}e^{i\varphi}|1\rangle\right] = e^{i\frac{\theta}{2}}|\psi\rangle ,$$

és a dir, l'estat més general vegades la fase global, $e^{i\frac{\theta}{2}}$, que no és mesurable.

És habitual expressar la seqüència de portes en termes diagramàtics. Al llarg d'una línia per cada qubit, es col·loca l'ordre temporal en que s'apliquen les portes, d'esquerra a dreta. En el nostre cas, seria



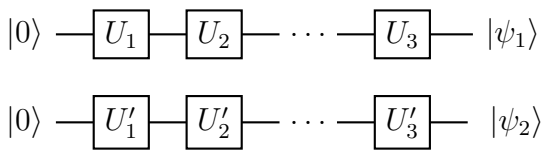
Per últim, el mateix resultat el podem obtenir fent ús de les matrius 2×2 que representen els operadors en la base matemàtica. Aleshores, la seqüència que hem aplicat correspon a aplicar la seqüència de matrius, escrita en ordre invers a l'ordre temporal, a l'estat inicial,

$$\Phi(\varphi + \frac{\pi}{2}) \cdot H \cdot \Phi(\theta) \cdot H \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

on els punts representen el producte de matrius habitual. Notar que ara la seqüència s'escriu amb l'ordre invertit respecte a l'ordre temporal, doncs la primera matriu que actua sobre el vector és la més propera i així successivament.

7.2 Portes quàntiques de dos qubits

Treballar amb un únic qubit no dona gaire joc. Es necessiten varis qubits per poder fer computació. El diagrama següent mostra una seqüència de varies portes d'un qubit, aplicada a dos qubits, inicialitzats a l'estat $|0\rangle \otimes |0\rangle$ i amb les línies horitzontals indicant l'evolució de cada qubit:



on cada una de les portes U_i, U_i' pot ser, per exemple, $H, \Phi(\theta), X, \cdots$. Amb aquest tipus de portes els estats evolucionaran a un estat final que, de ben segur, serà un estat separable, $|\psi_1\rangle \otimes |\psi_2\rangle$. Està clar que no podrem aconseguir estats entrellaçats si només disposem de porte d'un qubit. Calen doncs portes de dos qubits.

- Porta C-NOT = CNOT = C-X = CX:

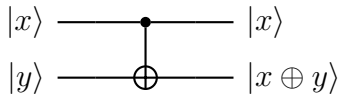
  Considerem la porta següent, que anomenarem Control Not i la representarem per C-NOT, CNOT o C-X i actua en dos qubits. Un d'ells actua com a qubit de control i l'altre de target. Si el qubit de control està en 0, el target no es modifica. Si, en canvi, el control està en 1, la porta NOT=X actua sobre el target. La seva taula de veritat és

CNOT			
Abans		Després	
Control	Target	Control	Target
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

  que es pot resumir, usant $x, y = 0, 1$, amb el primer qubit actuant de control i el segon de target, en

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

  La descripció gràfica de la porta CNOT és

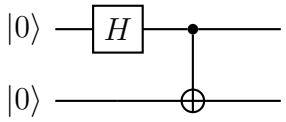


  on, de nou, $x, y = 0, 1$ i $\oplus$ significa la suma mòdul 2.

  També la podem expressar, en la notació matemàtica, com una matriu 4×4:

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

  Anem a veure ara que, usant la porta CNOT es pot aconseguir entrellaçar dos qubits. Considerem el següent diagrama:



L'evolució dels dos qubits serà (el qubit de control, dalt del diagrama, correspon al de l'esquerra en l'expresió següent):

$$|0\rangle \otimes |0\rangle \xrightarrow{H\otimes\mathbb{1}} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle),$$

on a la darrera expressió ometem els productes tensorials per alleugerir la notació, i veiem que apareix l'estat entrellaçat de dos qubits que anomenem $|\beta_{00}\rangle$

- Porta C-U:

  Si U és una porta d'un qubit, amb U unitària, la porta C-U es defineix de manera similar, és a dir, només s'aplica la porta U al qubit target si el qubit de control és 1

C-U			
Abans		Després	
Control	Target	Control	Target
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	U $\|0\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	U $\|1\rangle$

  Veiem que la porta CNOT és un cas particular de la porta C-U. Podem comprovar que, amb U unitària, la C-U de dos qubits també és unitària i, per tant, factible de ser implementada. Només cal veure que $(\text{C-U})^\dagger = \text{C-U}^\dagger$ i, en aplicar $(\text{C-U})^\dagger \cdot \text{C-U}$ als elements de la base (veure taula de veritat) aquests no canvien gràcies a que $\text{U}^\dagger \cdot \text{U} = \mathbb{1}$.

Totes les portes de dos qubits, matemàticament, poden representar-se amb matrius 4×4. Veiem alguns exemples:

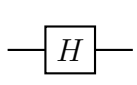
- La matriu Control Phase-shift, C-$\Phi(\varphi)$, seria:

$$\text{C-}\Phi(\varphi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\varphi} \end{pmatrix}.$$

- Un cas particular de l'anterior seria la porta C-V, amb $V = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \equiv \Phi(\varphi = \pi/2)$ que seria

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

- La matriu $\mathbb{1} \otimes H$, corresponent a aquest diagrama



on $\mathbb{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ és la matriu identitat per un qubit i H és la matriu Hadamard, també per un qubit, $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, la trobarem de dues maneres

- 1. Apliquem-la a cada un dels estats de la base:

$$\begin{aligned} \mathbb{1} \otimes H \, |0\rangle \, |0\rangle &= \frac{1}{\sqrt{2}} \, |0\rangle \, (|0\rangle + |1\rangle) \\ \mathbb{1} \otimes H \, |0\rangle \, |1\rangle &= \frac{1}{\sqrt{2}} \, |0\rangle \, (|0\rangle - |1\rangle) \\ \mathbb{1} \otimes H \, |1\rangle \, |0\rangle &= \frac{1}{\sqrt{2}} \, |1\rangle \, (|0\rangle + |1\rangle) \\ \mathbb{1} \otimes H \, |1\rangle \, |1\rangle &= \frac{1}{\sqrt{2}} \, |1\rangle \, (|0\rangle - |1\rangle), \end{aligned}$$

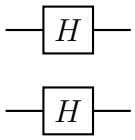
  i si ara ho expressem amb la base en notació matemàtica, tenim

$$\mathbb{1} \otimes H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

  Aquest resultat ens permet entendre com es fa el producte tensorial de dos matrius. Si les dues matrius són de dimensió 2×2, el resultat és una matriu 4×4 que s'obté prenent cada component de la primera matriu i multiplicant-la per la matriu 2×2 de la segona.
- 2. Fent el producte tensorial directament (definit segons el comentari final de l'apartat anterior:

$$\mathbb{1} \otimes H = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

- La matriu $H \otimes H$, corresponent al diagrama



  la calculem directament fent el producte tensorial

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

Com a complement, anem a veure com es pot implementar la porta CNOT en el cas que els qubits vinguin descrits pels dos estats d'energia més baixa del pou de potencial infinit. Cal tenir present que, quan dos àtoms estan propers, els seus nivells d'energia venen modificats per la proximitat de l'altre i depenen de en quin estat es troba l'àtom veí. Així, si la freqüència angular de rotació respecte l'angle azimutal –a l'esfera de Bloch– del qubit target depèn de l'estat del qubit de control, de manera que quan aquest es troba en l'estat $|1\rangle$ és 2ω i quan es troba en $|0\rangle$ és ω, anomenant $T = \frac{2\pi}{\omega}$, resulta que si apliquem pertorbacions al qubit target amb durades corresponents a $T/4$ i esperem temps $T/2$ segons està descrit en la taula següent (on usem $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$)

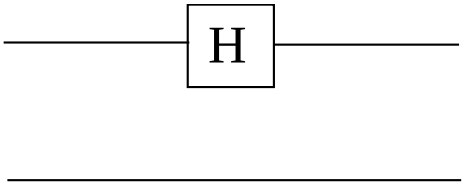
	Control		Target			Control		Target	
Inici	$\|0\rangle$	$\uparrow$	$\uparrow$	$\|0\rangle$	Inici	$\|1\rangle$	$\downarrow$	$\uparrow$	$\|0\rangle$
Pert. $T/4$ sobre target	$\|0\rangle$	$\uparrow$	$\rightarrow$	$\|+\rangle$	Pert. $T/4$ sobre target	$\|1\rangle$	$\downarrow$	$\rightarrow$	$\|+\rangle$
Esperar $T/2$	$\|0\rangle$	$\uparrow$	$\leftarrow$	$\|-\rangle$	Esperar $T/2$	$\|1\rangle$	$\downarrow$	$\rightarrow$	$\|+\rangle$
Pert. $T/4$ sobre target	$\|0\rangle$	$\uparrow$	$\uparrow$	$\|0\rangle$	Pert. $T/4$ sobre target	$\|1\rangle$	$\downarrow$	$\downarrow$	$\|1\rangle$

veiem que s'aconsegueix, efectivament, realitzar la porta CNOT

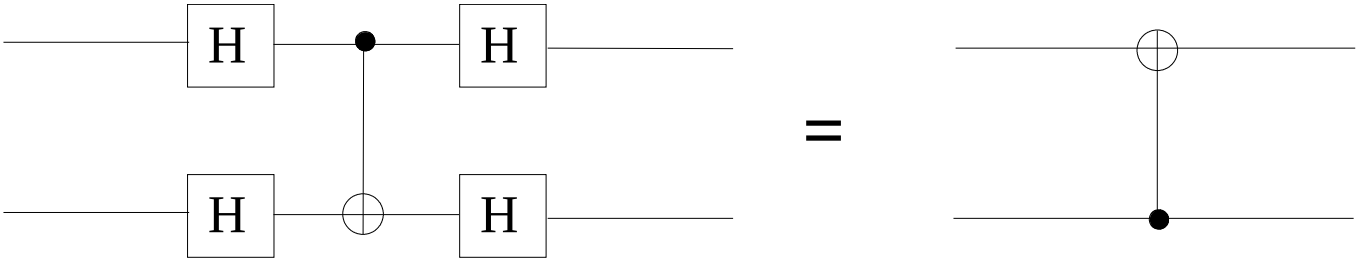
A continuació trobareu una sèrie d'exercicis sobre portes quàntiques d'un i/o dos qubits.

EXERCICI DE COMPUTACIÓ QUÀNTICA

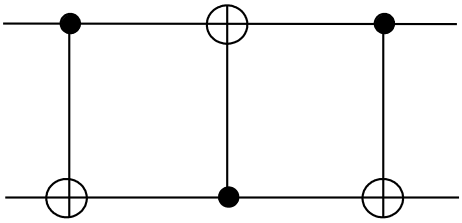
1.- Quina és la matriu corresponent a la porta de 2 qubits següent?



2.- Demostreu la següent equivalència entre portes:



3.- Demostreu que la següent porta implementa la funció *swap* (intercanvia els valors dels qubits), i donar la matriu associada.



4.- Dissenyeu una matriu U $\sqrt{NOT}$ que representi una porta $\sqrt{NOT}$ sobre un qubit, definint l'operació $\sqrt{NOT}$ de tal manera que

$(\sqrt{NOT}) (\sqrt{NOT}) | x > = | 1 - x >$, $x = 0, 1.$

Expresseu la matriu en la base $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$

5. Comproveu que la matriu que heu dissenyat sigui unitària, i que

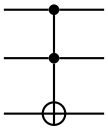
$$U\sqrt{NOT} \cdot U\sqrt{NOT} = U\,NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

7.3 Portes quàntiques de tres qubits

Considerem ara el cas de portes amb més qubits. La porta Toffoli n'és un exemple. És una generalització de la porta CNOT de dos qubits, en que ara dos qubits, amb valors lògics a i b, actuen com a controls i el tercer, c, com a target, se li aplica la NOT només quan els dos controls són 1. En podem dir també CCNOT. La seva taula de veritat seria:

Toffoli = CCNOT					
Abans			Després		
a	b	c	a'	b'	c'
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

La seva representació en el diagrama de portes,



i la seva expressió matricial seria

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

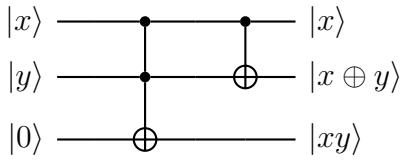
on les entrades en blanc són nul·les.

La porta de Toffoli és universal (qualsevol computació es pot fer en termes exclusivament d'aquesta porta). Una de les característiques dels circuits formats per portes quàntiques és que són reversibles, és a dir, que es pot reconstruir l'entrada a partir del coneixement de la sortida (penseu com això no és possible per exemple en una porta OR). Aquesta característica, que en principi permet fer computació sense consum d'energia, no és exclusiva, però, de la computació quàntica. Tot i que en l'actualitat s'utilitzen conjunts universals no reversibles (per exemple NAND amb FANOUT), també és possible fer computació clàssica reversible, encara que això implica l'ús de portes amb tres entrades/sortides.

La reversibilitat quàntica és deguda a que les portes quàntiques són unitàries. La porta de Toffoli és unitària ja que ella és la seva pròpia inversa, en ser simètrica i de coeficients reals. A més, és molt versàtil, doncs amb ella es poden generar les portes:

- NOT: Escollint $a = b = 1$, l'output $c' = NOTc$
- NAND: Escollint $c = 1$, l'output $c' = aNANDb$
- CNOT: Escollint $a = 1$, l'output $c' = bCNOTc$
- Còpia de c: Escollint $a = 1, c = 0$, l'output $c' = b$

Com a expemple, veiem que podem usar la porta de Toffoli, combinada amb la porta CNOT per fer la suma de dos bits:



on el primer qubit manté el valor, el segon la suma mòdul 2 de $x + y$ i el tercer és el carry. Està clar que la porta és reversible, doncs a partir de l'output podem recuperar l'input.

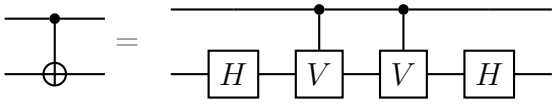
7.4 Conjunt universal de portes

Pot demostrar-se que per fer computació amb un nombre gran de qubits és suficient usar només portes d'un i de dos qubits. No calen portes específiques de més qubits, doncs aquestes poden ser implementades a partir de les anteriors.

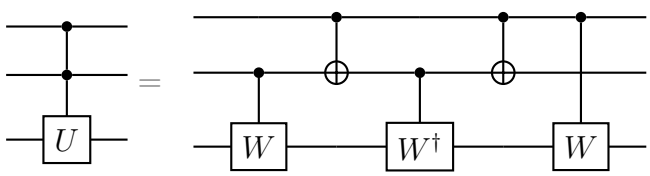
- El conjunt de portes {Hadamard, totes les portes phase-shift $\Phi(\varphi)$, C-NOT}, és un conjunt infinit universal: Qualsevol porta de n qubits pot ser implementada a partir d'aquestes. Noteu que la segona depèn d'un paràmetre continu, φ.
- Les portes {Hadamard, C-V}, amb V la phase-shift de $\pi/2$ per un qubit, és un conjunt finit universal de portes: A partir d'elles podem aproximar amb la precisió que vulguem qualsevol porta de n qubits.

Com exemples/exercicis, considerem:

- La porta C-NOT pot construir-se de la manera següent:

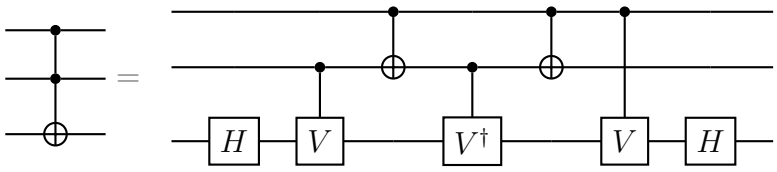


- La porta de tres qubits CC-U, on dos qubits controlen l'aplicació d'una porta unitària U sobre un tercer, amb $W^2 = U$:



Fixem-nos que, si U = NOT, aleshores la porta es redueix a la porta Toffoli, amb $W = \sqrt{NOT}$, que, a la vegada, sabem que és universal.

- Per últim, la porta de Toffoli també pot implementar-se així:



8 Teorema de no-clonació

El fet del col·lapse de la funció d'ona en la mesura porta al teorema de no-clonació. De manera senzilla, estableix que és impossible fer una còpia idèntica d'un estat quàntic que no sigui un estat de la base en què es mesura (altrament dit, només es poden fer còpies dels estats base).

De fet, si ens fixem en la porta CNOT, sembla que sigui possible clonar estats. En efecte, si tenim dos qubits, el primer el fem servir de control i el target l'inicialitzem a $|0\rangle$, aleshores

$$CNOT\,|0\rangle\,|0\rangle = |0\rangle\,|0\rangle\,; \quad CNOT\,|1\rangle\,|0\rangle = |1\rangle\,|1\rangle$$

de manera que l'estat final del target és una còpia del control. Però això ho hem fet per estats de la base! Què passa si ho fem de manera que el control sigui una combinació lineal qualsevol? Considerem com a control el qubit

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle$$
$$CNOT\,|\psi\rangle\,|0\rangle = CNOT\,(a\,|0\rangle + b\,|1\rangle)\,|0\rangle = a\,|0\rangle\,|0\rangle + b\,|1\rangle\,|1\rangle \neq |\psi\rangle\,|\psi\rangle\,,$$

doncs

$$|\psi\rangle\,|\psi\rangle = (a\,|0\rangle + b\,|1\rangle)\,(a\,|0\rangle + b\,|1\rangle) = a^2\,|0\rangle\,|0\rangle + ab\,|0\rangle\,|1\rangle + ab\,|1\rangle\,|0\rangle + b^2\,|1\rangle\,|1\rangle$$

Ara bé, veiem que la porta CNOT no pot clonar estats superposició, però això no exclou que alguna altra porta pugui fer-ho. Qui ho exclou és el teorema de no-clonació:

Demostració:

Demostrarem el teorema de no-clonació per reducció a l'absurd: Donats dos estats d'un qubit, $|\psi\rangle\,, |\phi\rangle$ tals que $\langle\psi|\phi\rangle \neq \{0, 1\}$ (no son ortonormals: no són el mateix tret d'una fase global, ni són elements de la base d'estats), suposem que existeix una porta clonació, U_C, unitària, tal que:

$$U_C\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle\,; \quad U_C\,|\phi\rangle\,|0\rangle = |\phi\rangle\,|\phi\rangle\,,$$

aleshores, calculem la projecció de l'estats final d'un sobre l'altra,

$$\langle\psi|\,\langle\psi|\phi\rangle\,|\phi\rangle = \langle 0|\,\langle\psi|\,U_C^\dagger U_C\,|\phi\rangle\,|0\rangle = \langle 0|\,\langle\psi|\phi\rangle\,|0\rangle\,,$$

i recordant que un bracket és un valor numèric (complex, en general), l'equació anterior implica que

$$\langle\psi|\phi\rangle\,\langle\psi|\phi\rangle = \langle\psi|\phi\rangle\,\langle 0|0\rangle\,,$$

és a dir,

$$\langle\psi|\phi\rangle^2 = \langle\psi|\phi\rangle\,,$$

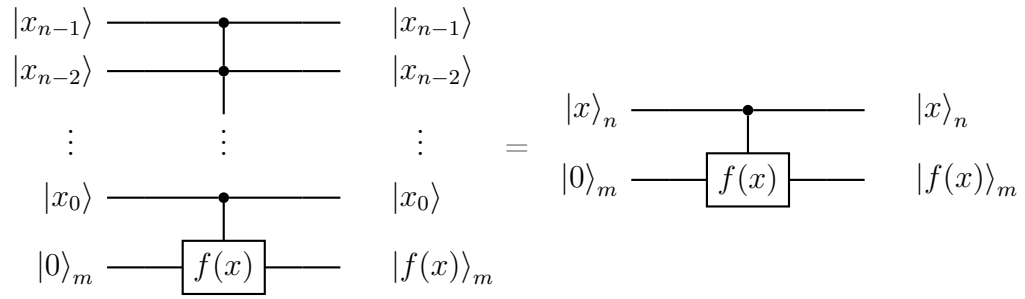
cosa que només és certa si $\langle\psi|\phi\rangle = \{0, 1\}$, és a dir, que haurien de ser ortonormals, contrariament a la hipòtesi de que no ho eren. Ho hem reduït a l'absurd, per tant no existeix cap porta que pugui clonar estats superposició.

9 Avaluació de funcions

En computació quàntica voldrem avaluar funcions usant portes unitàries reversibles. La computació serà doncs reversible. La manera pràctica de fer-ho és dedicar els qubits necessaris per encabir l'input i, separadament, uns altres per l'ouput. Parlarem dels registres d'input i d'output, respectivament. Així, si volem avaluar una funció de 2^n inputs possibles i que el resultat sigui un output de 2^m valors possibles

$$f : \{0,1\}^n \longrightarrow \{0,1\}^m.$$

Si un valor de l'input x el representem en la seva notació binària, $x = x_{n-1}2^{n-1} + x_{n-2}2^{n-2} + \cdots x_1 2^1 + x_0 2^0$, amb $x_i = \{0,1\}, i = 1, n-1$ podem prendre n qubits en el registre input, i, de manera anàloga, m qubits per l'output (aquest l'inicialitzarem a zero).



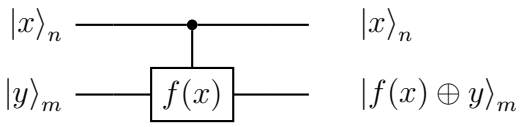
on a la figura de l'esquerra hem explicitat els n qubit de l'input i, en canvi, els m qubits d'ouput els denotem tots junts com un ket de m qubits. A la dreta usem la notació completament condensada. La idea és que els qubits d'input actuen com a controls que afecten als de l'output, on apareix el resultat de la funció de l'input, quan tots els qubits de l'output han estat inicialitzats prèviament a zeros. En termes d'operadors quàntics, l'operació que avalua la funció en direm U_f i la seva acció sobre els qubits d'input i output la definim com

$$U_f \left|x\right\rangle_n \left|0\right\rangle_m = \left|x\right\rangle_n \left|f(x)\right\rangle_m$$

Però l'operador U_f cal que estigui definit també per altres inicialitzacions de l'output. La manera estandard de fer-ho és:

$$U_f \left|x\right\rangle_n \left|y\right\rangle_m = \left|x\right\rangle_n \left|f(x) \oplus y\right\rangle_m ,$$

amb $f(x) \oplus y$ la suma mòdul dos, bit a bit, de l'expressió binària de $f(x)$ i y. El diagrama de portes és



Per últim, es pot veure que l'operador U_f definit d'aquesta manera és físicament factible, és a dir, que és unitari, $U_f^\dagger U_f = \mathbb{1}$. Per demostrar-ho veiem que

- U_f és la seva pròpia inversa:

$$\begin{aligned} U_f \left|x\right\rangle \left|y\right\rangle &= \left|x\right\rangle \left|f(x) \oplus y\right\rangle \\ U_f U_f \left|x\right\rangle \left|y\right\rangle &= U_f \left|x\right\rangle \left|f(x) \oplus y\right\rangle = \left|x\right\rangle \left|f(x) \oplus f(x) \oplus y\right\rangle = \left|x\right\rangle \left|y\right\rangle , \end{aligned}$$

  per tant

$$U_f U_f = \mathbb{1}.$$

- U_f és simètric: Les components de U_f les podem trobar fent el bracket

$$\begin{aligned}\langle y'|\langle x'|U_f|x\rangle|y\rangle &= \langle y'|\langle x'|x\rangle|f(x)\oplus y\rangle \\ &= \delta_{x,x'}\langle y'|f(x)\oplus y\rangle = \delta_{x,x'}\delta_{y',f(x)\oplus y} \\ &= \delta_{x,x'}\delta_{y\oplus y',f(x)},\end{aligned}$$

on a la delta de Kronecker de la darrera igualtat hem fet un shift de y als seus valors, de manera que la simetria en x i en y queda patent.

Així, l'operador matricial que implementa U_f, amb elements 0 o 1, és simètric, per tant igual al seu trasposat: $U_f^T = U_f$ el que implica que $U_f^\dagger = U_f$ i, per tant, queda demostrat que $U_f^\dagger U_f = \mathbb{1}$. U_f és per tant un operador unitari.

9.1 Paral·lelisme quàntic

Fins ara hem descrit com avaluar funcions i no s'aprecia cap diferència substancial amb el cas clàssic. La diferència arriba quan recordem que els estats quàntics poden estar en superposició dels elements de la base. Així, si a un qubit inicialitzat en $|0\rangle$ o $|1\rangle$ li apliquem la porta Hadamard, obtenim les superposicions

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

Si tenim n qubits d'input, tots inicialitzats a zero, i apliquem una Hadamard a cada un d'ells, aleshores tindrem

$$\begin{aligned}H^{\otimes n}|0\rangle_n &= H|0\rangle_{n-1}\otimes H|0\rangle_{n-2}\otimes\cdots\otimes H|0\rangle_0 \\ &= \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\cdots\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \\ &= \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_n,\end{aligned}$$

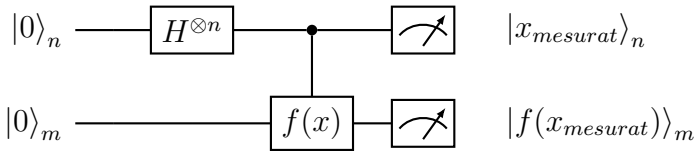
és a dir, obtenim una superposició de tots els 2^n estats de la base (del sistema de n qubits) equiprobable, amb els mateixos coeficients. Si alimentem la funció amb aquesta superposició d'estats, aleshores és quan apareix el paral·lelisme quàntic:

$$U_f H^{\otimes n}|0\rangle_n|y\rangle_m = U_f\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_n|y\rangle_m = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_n|f(x)\oplus y\rangle_m.$$

Si s'inicialitza l'output a zeros, aleshores l'estat final obtingut és un estat entrellaçat de tots els possibles inputs amb els seus corresponents outputs. L'aplicació de la funció a tots els inputs superposats conté informació de tots els valors de la funció:

$$U_f H^{\otimes n}|0\rangle_n|0\rangle_m = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle_n|f(x)\rangle_m.$$

Ara bé, és possible extreure'n tots els valors de la funció? Si realitzem una mesura de l'estat entrellaçat, trobarem només, i amb probabilitat $\frac{1}{2^n}$, un dels 2^n valors de l'input, $|x_{mesurat}\rangle$ i el seu corresponent valor de la funció al registre output, $|f(x_{mesurat})\rangle$. De fet, haurem trobat de manera aleatòria, random, probabilística, un dels valors de la funció. (Clàssicament, triem nosaltres quin output volem conèixer triant l'input.)



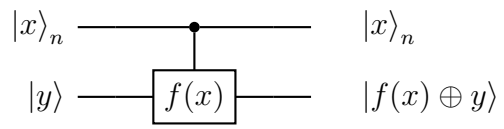
Això vol dir que si volem aprofitar el paral·lelisme quàntic haurem de fer alguna cosa, prèvia a la mesura, que ens permeti obtenir més informació. Abans, però, veurem tot seguit que, quan l'output és binari, podem alleugerir la notació.

9.2 Truc quan l'output és binari

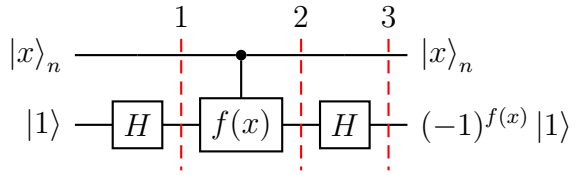
Anem a veure un cas particular que ens anirem trobant al llarg del curs: si l'output de la funció és binari, és a dir, per funcions del tipus:

$$f : \{0,1\}^n \longrightarrow \{0,1\},$$

en què la representació és



considerem què passa si inicialitzem el qubit d'output a l'estat $|1\rangle$ i apliquem la seqüència:



on cal justificar l'estat final. Fem-ho en termes equivalents: Partint de l'estat inicial

$$|x\rangle_n \otimes |1\rangle ,$$

analitzem què passa a cada pas.

- Pas 1: En aplicar $\mathbb{1} \otimes H$ obtenim:

$$\mathbb{1} \otimes H\,|1\rangle = |x\rangle_n \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

- Pas 2: En avaluar la funció al resultat del Pas 1:

$$\begin{aligned} |x\rangle_n \frac{1}{\sqrt{2}}\left(|f(x)\rangle - |f(x)\oplus 1\rangle\right) &= |x\rangle_n \left\{ \begin{array}{cccc} \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & if & f(x)=0 \\ -\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & if & f(x)=1 \end{array} \right\} \\ &= (-1)^{f(x)}\,|x\rangle_n \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

- Pas 3: En aplicar $H^{\otimes n} \otimes H$ al resultat del Pas 2:

$$(-1)^{f(x)} |x\rangle_n \otimes |1\rangle .$$

Així, tot el procés ens ha portat de

$$|x\rangle_n \otimes |1\rangle \longrightarrow (-1)^{f(x)} |x\rangle_n \otimes |1\rangle$$

ens ha afegit un possible canvi de signe depenent del valor de $f(x)$ que, si en lloc de pensar-lo en el qubit d'output, l'incloguem a l'input, podem pensar que l'output no ha canviat i juga només el paper de qubit auxiliar (ancilla, en anglès). Així, podem pensar que, de manera efectiva, podem definir la porta unitària de la funció en termes només de l'input, de manera que

$$U_f |x\rangle_n = (-1)^{f(x)} |x\rangle_n ,$$

diagramàticament

$$|x\rangle_n \text{ ——} \boxed{U_f} \text{——} (-1)^{f(x)} |x\rangle_n$$

però recordant que, experimentalment, sí cal usar el qubit auxiliar.

10 Algorismes quàntics senzills

En aquesta secció analitzarem diferents algorismes quàntics senzills, en el sentit que la majoria són d'interès acadèmic. Veurem que són capaços de millorar les seves versions clàssiques, especialment quan es tracta de trobar propietats col·lectives, gràcies a fer ús de la superposició quàntica.

10.1 Generador de nombres random

Si un vol generar un nombre aleatori pot fer ús del caràcter probabilístic de la física quàntica. Considerem per exemple 3 qubits inicialitzats a $|0\rangle$. Si apliquem una matriu Hadamard a cada un d'ells, l'estat que es genera serà:

$$\begin{aligned} H|0\rangle H|0\rangle H|0\rangle &= \frac{1}{2^{3/2}}(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)(|0\rangle + |1\rangle) \\ &= \frac{1}{2^{3/2}}(|0\rangle|0\rangle|0\rangle + |0\rangle|0\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |0\rangle|1\rangle|1\rangle + |1\rangle|0\rangle|0\rangle + |1\rangle|0\rangle|1\rangle \\ &\quad + |1\rangle|1\rangle|0\rangle + |1\rangle|1\rangle|1\rangle) \\ &= \frac{1}{\sqrt{8}}(|0\rangle_3 + |1\rangle_3 + |2\rangle_3 + |3\rangle_3 + |4\rangle_3 + |5\rangle_3 + |6\rangle_3 + |7\rangle_3) \end{aligned}$$

on, a la darrera igualtat, hem escrit els estats amb els valors que els correspon quan es llegeixen en base 2. S'obté una superposició de 8 estats/valors possibles cada un d'ells amb la mateixa probabilitat, $p = 1/8$.

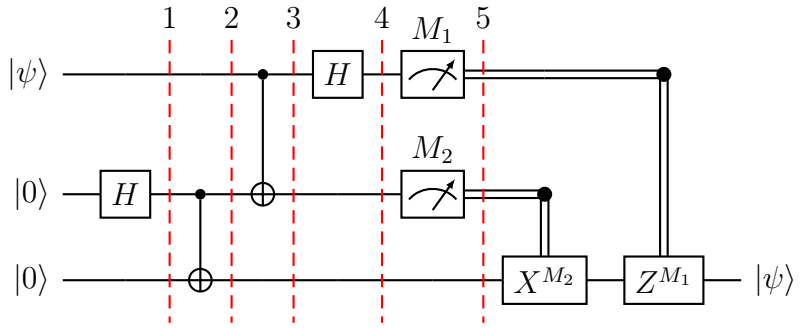
Per un nombre n de qubits, s'obté

$$|x\rangle_n \text{ ——} \boxed{H^{\otimes n}} \text{——} \tfrac{1}{2^{n/2}} \textstyle\sum_{x=0}^{2^n-1} |x\rangle_n$$

que és una superposició de 2^n estats amb probabilitat $\frac{1}{2^n}$, tenim un generador de 2^n valors random.

10.2 Teleportació

És un dels algorismes més famosos: Com tele-portar un qubit sense transport de matèria. Està descrit pel conjunt de portes de la figura.



La idea és que Alice vol tele-transportar un qubit $|\psi\rangle$ a Bob. Per això necessitaran compartir un estat entrellaçat, cosa que s'aconsegueix amb les dues primeres portes de la figura, H i CNOT, aplicades al segon i tercer qubit. Un cop disposen d'aquest estat entrellaçat, Alice se'n queda la seva part i Bob l'altra. L'algorisme complet, a partir de l'estat inicial $|\psi\rangle\,|0\rangle\,|0\rangle$, amb $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ seria:

- Pas 1: Després d'aplicar $\mathbb{1} \otimes H \otimes \mathbb{1}$

$$|\psi\rangle\,\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|0\rangle$$

- Pas 2: En aplicar $\mathbb{1} \otimes CNOT$ es genera l'estat entrellaçat entre els qubits 2 i 3. Alice se'n queda el 2 i Bob, el 3. A partir d'ara usarem que l'estat que es vol tele-transportar és $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$

$$|\psi\rangle\,\frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) = (a\,|0\rangle + b\,|1\rangle)\frac{1}{\sqrt{2}}(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle)$$

- Pas 3: S'aplica ara $CNOT \otimes \mathbb{1}$ i s'obté

$$\frac{1}{\sqrt{2}}\left\{a\,|0\rangle\,(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) + b\,|1\rangle\,(|1\rangle\,|0\rangle + |0\rangle\,|1\rangle)\right\}$$

- Pas 4: Després d'aplicar $H \otimes \mathbb{1} \otimes \mathbb{1}$

$$\begin{gathered}\tfrac{1}{2}\left\{a(|0\rangle + |1\rangle)(|0\rangle\,|0\rangle + |1\rangle\,|1\rangle) + b(|0\rangle - |1\rangle)(|1\rangle\,|0\rangle + |0\rangle\,|1\rangle)\right\} \\ = \tfrac{1}{2}\left\{|0\rangle\,|0\rangle\,(a\,|0\rangle + b\,|1\rangle) + |0\rangle\,|1\rangle\,(a\,|1\rangle + b\,|0\rangle) + |1\rangle\,|0\rangle\,(a\,|0\rangle - b\,|1\rangle) + |1\rangle\,|1\rangle\,(a\,|1\rangle - b\,|0\rangle)\right\}\end{gathered}$$

  on recordem que els dos primers qubits pertanyen a Alice (els escrivim junts) i el tercer a Bob.

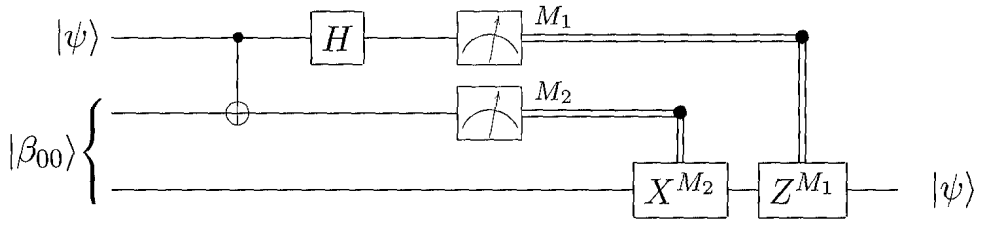
  - Si ens fixem en el primer terme, quan els qubits d'Alice són $|0\rangle\,|0\rangle$, el de BoB és $a\,|0\rangle + b\,|1\rangle = |\psi\rangle$, ja s'ha tele-transportat l'estat $|\psi\rangle$ d'Alice a Bob. Però això passa amb una probabilitat $1/4$.
  - En el segon terme, Alice té $|0\rangle\,|1\rangle$ i Bob $a\,|1\rangle + b\,|0\rangle$ que no és l'estat $|\psi\rangle$ però s'hi transforma si se li aplica una porta NOT=X $= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.
  - En el tercer terme, Alice té $|1\rangle\,|0\rangle$ i Bob $a\,|0\rangle - b\,|1\rangle$ que es pot transformar amb $|\psi\rangle$ si Bob aplica una porta Z $= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

  - Per últim, quan els qubits d'Alice són $|1\rangle\,|1\rangle$ el de Bob és $a\,|1\rangle - b\,|0\rangle$ que es transforma en $|\psi\rangle$ si s'aplica la porta X i seguidament la Z.

- Pas 5: Alice mesura els seus qubits 1 i 2, obtenint valors M_1 i M_2 que només poden ser 0 o 1. Un cop coneguts, truca a Bob dient-li que apliqui les portes X^{M_2} i després Z^{M_1}. Si Bob ho fa, l'estat final que li queda és $|\psi\rangle$. L'estat ha estat correctament tele-transportat, no físicament, sinó la informació inclosa en els coeficient a i b. Per això ha calgut la trucada d'Alice a Bob

EXERCICI DE COMPUTACIÓ QUÀNTICA

Hem vist que la teleportació permet que Alice pugui transferir l'estat $|\psi\rangle$ d'un qubit cap a Bob, si tots dos comparteixen inicialment un parell entrellaçat. En el procés Alice deixa de tenir l'estat inicial (en cas contrari hauríem fet una còpia) i també deixen de compartir el parell entrellaçat, segons el següent esquema



Cal notar que Bob recupera l'estat inicial que tenia Alice després d'aplicar (si és necessari) les portes X i/o Z, segons quins resultats li ha comunicat Alice al mesurar els seus dos qubits (el que assegura que no hi ha una transferència instantània de l'estat). Recordeu que

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle] \,,\; X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\; Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

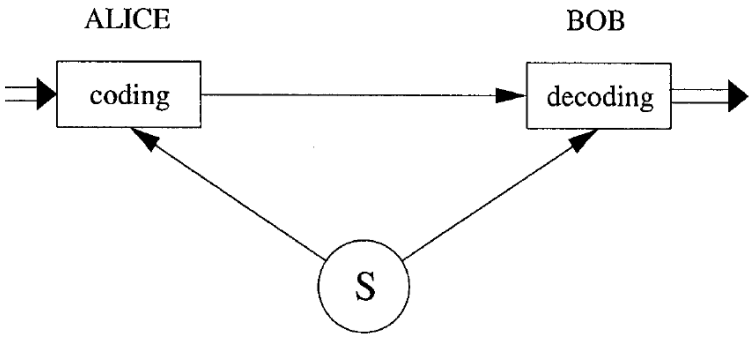
Una generalització directa permet transferir l'entrellaçament entre dos punts, de forma que al final dos punts allunyats comparteixin dos qubits entrellaçats sense que hagin estat en contacte (poden fer servir posteriorment els parells generats per construir claus segures com hem vist en el protocol d'Ekert). Aquesta possibilitat es coneix com "entanglement swapping" i consisteix en:

1. Alice i Bob comparteixen un parell entrellaçat.
2. Bob i Carol també comparteixen una altre parell entrellaçat.
3. Bob aplica les mateixes portes (C-NOT i H) als seus dos qubits (com en l'esquema de teleportació).
4. Bob mesura els seus dos qubits (ídem).
5. Depenent dels resultats que anuncia Bob, Carol aplica les portes adequades per tal que finalment ella i Alice comparteixin un parell entrellaçat (en el procés s'han destruït els parells entrellaçats de partida).

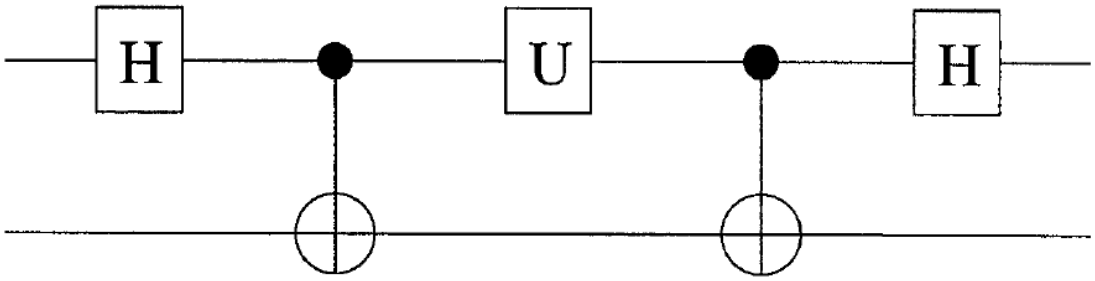
A) Dibuixeu l'esquema corresponent pels 4 qubits involucrats
B) Escriviu l'estat total d'entrada (cada un dels parells entrellaçats inicials és del tipus $|\beta_{00}\rangle$).
C) Com canvia al passar per les portes que aplica Bob (abans de fer cap mesura)? Factoritzar-lo en termes dels possibles estats que pot mesurar en Bob.
D) Quines portes ha d'aplicar Carol (segons les mesures que anuncia Bob) per tal que finalment ella i Alice comparteixin un parell entrellaçat?

EXERCICI DE COMPUTACIÓ QUÀNTICA

La **codificació densa** és un exemple de l'aplicació de l'entrellaçament a la comunicació. Permet a l'Alice enviar dos bits d'informació clàssica enviant un sol qubit. L'esquema del protocol es dibuixa a continuació, on S indica una font de qubits entrellaçats, les línies dobles bits clàssics i les rectes qubits individuals.



El circuit que l'implementa en termes de portes quàntiques és el següent, on el qubit superior és la part que té l'Alice i l'inferior la meitat en possessió del Bob.



1) Demostreu com l'aplicació de les dues primeres portes (que es faria a la font S) sobre el parell |0>|0> resulta en l'estat entrellaçat habitual

2) Segons el parell de bits clàssics que vol enviar l'Alice (00,01,10,11) aplica (representat per l'operador U a l'esquema) una de les portes (I, σ_x, σ_y, σ_z) al seu qubit, on I indica la identitat i la resta són les anomenades matrius de Pauli. Quin és l'estat que s'obté en cada cas?

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

3) Finalment l'Alice envia el qubit resultant a en Bob, i aquest aplica les dos últimes portes de l'esquema. A continuació mesura l'estat dels dos qubits que estan en el seu poder. Demostreu com en cada cas, i amb probabilitat 1, obté els dos bits clàssics que ha codificat l'Alice.

10.3 Algorisme de Deutsch (Problema de la moneda)

Aquest va ser el primer algorisme que permet veure la millora quàntica respecte la clàssica.

Plantejament:

Donada una moneda, pot ser vertadera (cara/creu) o falsa (cara/cara o creu/creu). Quantes vegades cal mirar la moneda per esbrinar de quin tipus és?

La nostra intuïció diu que l'hem de mirar dues vegades, primer una cara i després l'altra.

Equivalent matemàtic:

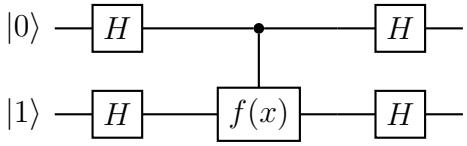
Sigui una funció binària, $f(x) : \{0,1\} \to \{0,1\}$, una de les quatre funcions binàries que hi ha,

$$\begin{aligned} f_1(0) &= 0; \quad f_1(1) = 0, \\ f_2(0) &= 0; \quad f_2(1) = 1, \\ f_3(0) &= 1; \quad f_3(1) = 0, \\ f_4(0) &= 1; \quad f_4(1) = 1, \end{aligned}$$

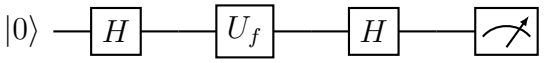
on $f_1(x)$ i $f_4(x)$ són funcions constants mentre que $f_2(x)$ i $f_3(x)$ són balancejades. Només hi tenim accés donant-li un valor d'input i ella ens retorna el seu output. Ens reten a esbrinar si la funció és constant ($f(0) = f(1)$) o balancejada ($f(0) \neq f(1)$) fent el mínim nombre de crides a la funció.

La nostra experiència ens diu que necessitarem fer dues crides. La primera no ens dona informació suficient per saber de quin tipus és la funció, tal com passa amb el problema de la moneda. És un problema equivalent. Ara bé, si tenim accés a la funció la en un ordinador quàntic, podrem posar com a input una superposició de les dues entrades possibles. Això pot permetre millorar l'eficiència.

Plantegem el circuit quàntic per respondre al repte.



De fet, com que la funció és binària, podem usar el truc que ens permet prescindir del qubit auxiliar i simplificar l'anàlisi en termes de



on recordem que $U_f |x\rangle = (-1)^{f(x)} |x\rangle$. Així tindrem

$$\begin{aligned} |0\rangle \quad & \xrightarrow{H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ & \xrightarrow{U_f} \frac{1}{\sqrt{2}}((-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle) \\ & \xrightarrow{H} \frac{1}{2}\{\left[(-1)^{f(0)} + (-1)^{f(1)}\right] |0\rangle + \left[(-1)^{f(0)} - (-1)^{f(1)}\right] |1\rangle\}. \end{aligned}$$

Observem que:

Si la funció és constant, l'estat final és $\pm|0\rangle$.

Si la funció és balancejada, l'estat final és $\pm|1\rangle$.

Per tant, en mesurar, si trobem el valor 0 (1) voldrà dir que, amb seguretat, la funció és constant (balancejada) i només haurem fet una crida a la funció. Fixem-nos que estem avaluant una propietat col·lectiva de la funció. Som capaços de dir de quin tipus és la funció: constant o balancejada, només fent una crida a la funció. En canvi, no sabem quina de les quatre funcions possibles hi ha dins la caixa negra. Si volguéssim saber quina és, hauríem de fer una segona crida i, per tant, no tindríem cap millora respecte l'algorisme clàssic.

10.4 Algorisme de Deutsch-Jozsa generalitzat

És una generalització de l'algorisme de Deutsch. Ara tenim una funció amb 2^n inputs possibles i un output binari.

$$f(x) : \{0,1\}^n \to \{0,1\}$$

Ens diuen que la funció és constant o balancejada, i amb la promesa de que és cert, ens reten a determinar de quin dels dos tipus és. Només podem, com abans, esbrinar-ho entrant-li inputs i usar l'output corresponent.

Fixem-nos que clàssicament, aniríem entrant-li valors i en llegiríem el seu output. Suposem que obtenim una seqüència d'outputs del tipus $0, 1$. Ja podríem assegurar -gràcies a la promesa- que la funció és balancejada, havent fet només dues úniques crides a la funció. Ara bé, si la seqüencia és $0, 0, 0, 0, ...$ i així fins l'entrada $2^n/2$, no podrem dir res fins que, a l'entrada següent, la número $2^n/2 + 1$ obtinguem ja sigui 0 o 1. En el primer cas podem assegurar que la funció és constant. En el segon, que és balancejada. Necessitem en aquest cas $2^n/2 + 1$ crides a la funció.

Està clar que els casos esmentats són el més optimista, 2 crides, i el més pessimista $2^n/2 + 1$ crides. Entremig hi haurà moltes altres possibilitats.

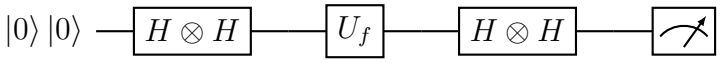
Anem a veure com ho faríem si la funció estigués implementada quànticament i hi tinguéssim accés amb un ordinador quàntic. L'algorisme l'implementarem similarment al cas de Deutsch. Per fer-ho, començarem suposant que $n = 2$ i després passarem al cas n general.

10.4.1 Cas n=2

La funció:

$$f(x) : \{0,1\}^2 \to \{0,1\}$$

El procediment simplificat (output binari: fem servir el truc):



L'evolució de l'estat en aplicar les portes serà

$$
\begin{aligned}
|0\rangle|0\rangle = |0\rangle_2 &\xrightarrow{H\otimes H} \frac{1}{2}\sum_{x=0}^{3}|x\rangle_2 \xrightarrow{U_f} \frac{1}{2}\left\{(-1)^{f(0)}|0\rangle_2 + (-1)^{f(1)}|1\rangle_2 + (-1)^{f(2)}|2\rangle_2 + (-1)^{f(3)}|3\rangle_2\right\} \\
&\xrightarrow{H\otimes H} \frac{1}{4}\{ \left[(-1)^{f(0)} + (-1)^{f(1)} + (-1)^{f(2)} + (-1)^{f(3)}\right]|0\rangle_2 \\
&\quad + \left[(-1)^{f(0)} - (-1)^{f(1)} + (-1)^{f(2)} - (-1)^{f(3)}\right]|1\rangle_2 \\
&\quad + \left[(-1)^{f(0)} + (-1)^{f(1)} - (-1)^{f(2)} - (-1)^{f(3)}\right]|2\rangle_2 \\
&\quad + \left[(-1)^{f(0)} - (-1)^{f(1)} - (-1)^{f(2)} + (-1)^{f(3)}\right]|3\rangle_2\} .
\end{aligned}
$$

Finalment, abans de mesurar, veiem que si la funció és constant, l'estat es redueix a $\pm|0\rangle$. En aquest cas, la probabilitat de trobar el valor 0 és 1. Si, en canvi, la funció és balancejada, la probabilitat de trobar el valor 0 és 0. Així, quan mesurem, trobarem o bé 0, amb el que sabrem que la funció és constant; o bé trobarem $1, 2$ o 3, el qual garantirà que la funció no és constant, per tant, balancejada. Fixem-nos que, en aquest cas, la millora també s'obté en avaluar una propietat col·lectiva: quin tipus de funció és, i no quina funció és. Quan la mesura dona 0 sabem que la funció és constant, però no sabem si la constant és 0 o 1. Si la mesura és 1, la funció és balancejada i, a més, sabem que $f(0) = f(2)$, $f(1) = f(3)$ i $f(0) \neq f(1)$, però no sabem els valors concrets corresponents.

Nota Al darrer pas hem usat:

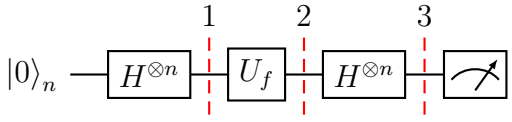
$$
\begin{aligned}
H\otimes H\,|0\rangle_2 &= H|0\rangle\,H|0\rangle = \frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle+|1\rangle) = \frac{1}{2}(|0\rangle_2+|1\rangle_2+|2\rangle_2+|3\rangle_2) \\
H\otimes H\,|1\rangle_2 &= H|0\rangle\,H|1\rangle = \frac{1}{2}(|0\rangle+|1\rangle)(|0\rangle-|1\rangle) = \frac{1}{2}(|0\rangle_2-|1\rangle_2+|2\rangle_2-|3\rangle_2) \\
H\otimes H\,|2\rangle_2 &= H|1\rangle\,H|0\rangle = \frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle+|1\rangle) = \frac{1}{2}(|0\rangle_2+|1\rangle_2-|2\rangle_2-|3\rangle_2) \\
H\otimes H\,|3\rangle_2 &= H|1\rangle\,H|1\rangle = \frac{1}{2}(|0\rangle-|1\rangle)(|0\rangle-|1\rangle) = \frac{1}{2}(|0\rangle_2-|1\rangle_2-|2\rangle_2+|3\rangle_2)
\end{aligned}
$$

10.4.2 Cas n

Considerem ara una funció definida com

$$f(x) : \{0,1\}^n \to \{0,1\}$$

amb n un valor sencer qualsevol. Com abans, ens diuen que la funció és constant o balancejada, i amb la promesa de que és cert, ens reten a determinar de quin dels dos tipus és. Només podem esbrinar-ho entrant-li inputs i usar l'output corresponent. El procediment simplificat segueix essent vàlid (output binari: fem servir el truc). Partim de n qubits inicialitzats a 0 i apliquem la seqüència de portes:



Veiem que hem de conèixer l'acció de les portes Hadamard, no només sobre els n qubits inicials que estan tots en l'estat 0, sinó també sobre els finals, que hauran canviat. O sigui, necessitem saber com actuen les n Hadamards sobre qualsevol estat. Veiem com fer-ho, recordant que sobre un únic qubit

$$H|x\rangle = \frac{1}{\sqrt{2}}\left[(-1)^x|x\rangle + |1-x\rangle\right]; \quad x = 0, 1,$$

l'acció múltiple serà una expressió d'una suma de molts termes, del tipus

$$H^{\otimes n}\left|x\right\rangle_n = \frac{1}{2^{n/2}}\left[\cdots(-1)^{x_2}(-1)^{x_0}\cdots\left|x_2\right\rangle\left|1-x_1\right\rangle\left|x_0\right\rangle+\cdots\right], \quad x_i=0,1, \quad i=0,n-1.$$

Ara, farem dos canvis.

- En primer lloc, pels termes en què els kets siguin $|x_i\rangle$, $y_i = x_i$, i pels que siguin $|1-x_i\rangle$, $y_i = 1-x_i$. En el nostre exemple:

$$y_0 = x_0; y_1 = 1-x_1; y_2 = x_2; \cdots$$

- En segon lloc, el signe global que apareix a l'exemple es pot reescriure com

$$(-1)^{x0+x2+\cdots} = (-1)^{x_0y_0+x_1y_1+x_2y_2+\cdots},$$

  doncs es compleix que:

$$x_0 = x_0y_0; \quad x_1y_1 = 0; \quad x_2 = x_2y_2, \cdots,$$

Per tant, obtenim l'expressió compacte

$$H^{\otimes n}\left|x\right\rangle_n = \frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}\left|y\right\rangle_n$$

que, quan actua sobre el $|0\rangle_n$, es redueix a la ja coneguda superposició

$$H^{\otimes n}\left|0\right\rangle_n = \frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}\left|y\right\rangle_n.$$

Ara estem en disposició de trobar l'evolució de l'algorisme

- Pas 1:

$$H^{\otimes n}\left|0\right\rangle_n = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}\left|x\right\rangle_n$$

- Pas 2:

$$U_fH^{\otimes n}\left|0\right\rangle_n = \frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\left|x\right\rangle_n$$

- pas 3:

$$\begin{aligned} H^{\otimes n}U_fH^{\otimes n}\left|0\right\rangle_n &= \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot y}\left|y\right\rangle_n \\ &= \sum_{y=0}^{2^n-1}\left\{\frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot y}\right\}\left|y\right\rangle_n \end{aligned}$$

  que és un sumatori de tots els estats possibles amb uns coeficients dins de la clau. Pensem per un moment quin és el coeficient de $|0\rangle$, amb $y=0$, quan la funció sigui constant, $f(x)=0,1$. Veiem que, en aquest cas, el terme dins de la clau es redueix a ±1, l'estat final esdevé $\pm\left|0\right\rangle_n$ i la probabilitat de mesurar i trobar tots el n qubits iguals a 0, és 1.

  En conclusió, mesurem l'estat final. Si trobem el valor 0 sabem amb certesa que la funció és constant. Si trobem qualsevol dels valors restants, $1,2,3,\cdots,2^n-1$, la funció és balancejada. Amb una única crida a la funció superem el repte.

10.5 Algorisme de Bernstein-Vazirani

Sigui una funció en el domini

$$f_a(x) : \{0,1\}^n \to \{0,1\}, \quad a \in \{0,1\}^n$$

tal que

$$f_a(x) = x \cdot a = x_0 a_0 \oplus x_1 a_1 \cdots \oplus x_{n-1} a_{n-1}.$$

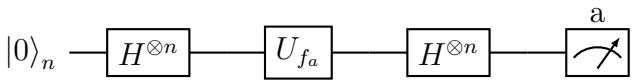
Ens repten a determinar quin és el valor de a fent el menor nombre de crides a la funció.

Clàssicament, la millor estratègia és entrar n inputs x de la forma

$$\begin{aligned} f_a(100\cdots 0_{n-1}) &= a_0, \\ f_a(010\cdots 0_{n-1}) &= a_1, \\ f_a(001\cdots 0_{n-1}) &= a_2, \\ &\vdots \\ f_a(000\cdots 1_{n-1}) &= a_{n-1}. \end{aligned}$$

Trobem el valor de a fent n crides a la funció.

Quànticament podem fer-ho millor amb l'algorisme següent



Veiem-ho:

$$\begin{aligned} |0\rangle_n \xrightarrow{H^{\otimes n}} & \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n \\ \xrightarrow{U_{f_a}} & \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f_a(x)} |x\rangle_n \\ \xrightarrow{H^{\otimes n}} & \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f_a(x)} (-1)^{x\cdot y} |y\rangle_n \\ = & \sum_{y=0}^{2^n-1} \left\{ \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f_a(x)+x\cdot y} \right\} |y\rangle_n \\ = & \sum_{y=0}^{2^n-1} \left\{ \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{(a+y)\cdot x} \right\} |y\rangle_n \\ = & |a\rangle_n . \end{aligned}$$

El darrer pas es justifica cercant quin és el coeficient de l'estat $|a\rangle$ dins de la suma de tots els estats $|y\rangle$ i adonat-se que el terme $(-1)^{(a+y)\cdot x} = (-1)^{2a\cdot x} = 1$ per tots els termes de la suma sobre x, que conté 2^n termes. Per tant el terme dins la clau és 1, és a dir, ens diu que la probabilitat de trobar el ket $|a\rangle$ és 1. Això implica que la probabilitat de trobar qualsevol altre ket és zero. En mesurar, finalment, trobarem el valor que es cercava, a, amb certesa (probabilitat 1) havent preguntat a la funció una única vegada. Representa una millora significativa respecte la millor alternativa clàssica.

Fixem-nos en tres aspectes: i) no hem justificat matemàticament la darrera igualtat, tot i que hem trobat la justificació dins del context quàntic. ii) hem fet novament ús del truc, simplificant la descripció de l'algorisme i iii) s'agrairia entendre una mica millor l'eficàcia de l'algorisme.

Comencem pel punt 1) justificant que el coeficient d'un estat $|y\rangle_n$ amb $y \neq a$ val zero. El coeficient de l'estat $|y\rangle_n$ és

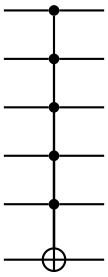
$$c_y = \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{(a+y)\cdot x} = \frac{1}{2^n} \prod_{j=0}^{n-1} \left[\sum_{x_j=0,1} (-1)^{(a_j+y_j)x_j} \right].$$

Si $y = a$ tots els termes dell productori donen 2 i, per tant, $c_{y=a} = 1$. En canvi, si $y \neq a$ vol dir que en la seva expressió binària, al menys un dels seus bits ha de ser diferent del de a. Sigui $y_k \neq a_k$, El terme que li correspon al productori és

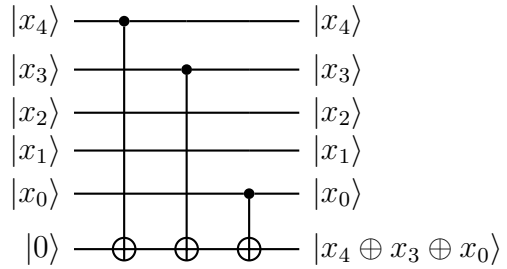
$$\sum_{x_k=0,1} (-1)^{(a_k+y_k)x_k} = (-1)^0 + (-1)^1 = 0,$$

i per tant el productori serà zero: $c_{y\neq a} = 0$.

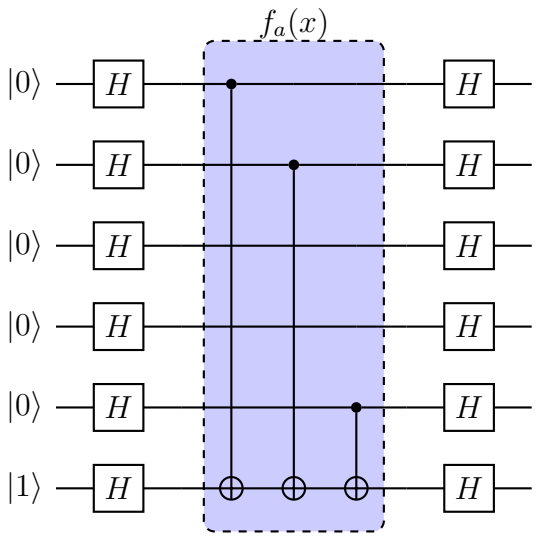
Els punts ii) i iii) els tractarem junts. Recordem com és el circuit quàntic per l'avaluació d'una funció, U_f. Farem un exemple suposant que tenim $n = 5$ qubits d'input i un qubit d'output:



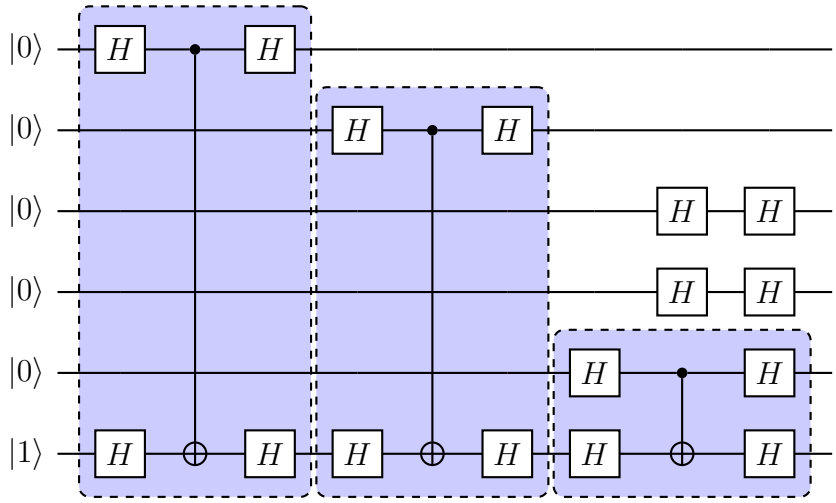
Com seria la funció $f_a(x) = x \cdot a$? Suposem un exemple amb $a = 25 = 2^4 + 2^3 + 2^0 = 11001$. En aquest cas $f_a(x) = x_4 \oplus x_3 \oplus x_0$ i s'obté amb el circuit:



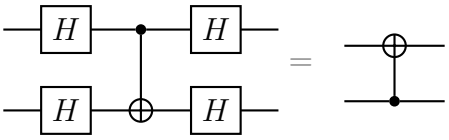
Pensem ara que algú ha programat aquesta funció en una caixa negra i només ens deixa entrar-hi inputs, retornant la caixa el seu output. Aleshores nosaltres consideraríem el següent circuit quàntic, amb els qubits d'input inicialitzats a $|0\rangle$ mentre que el d'output, inicialitzat a $|1\rangle$.



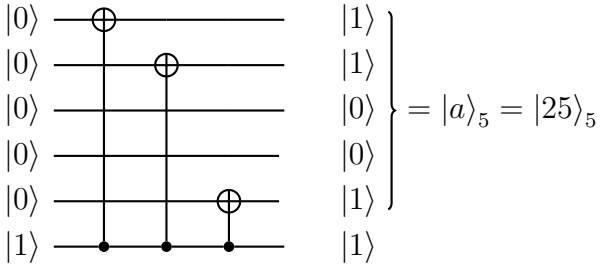
Per entendre com funciona el circuit, podem fer les següents manipulacions: Apropem els operadors H entre sí. A més, a la línia de l'output, hem insertat la identitat $HH = \mathbb{1}$ entre les portes CNOT. Finalment, destaquem en color blau reagrupaments de portes que tenen un equivalent molt senzill:



on sabem que el grup de color té l'equivalent



que quan es substitueix al circuit original, i es té en compte que $HH = \mathbb{1}$, aquest queda simplificat a



on es veu clarament que l'estat final de l'input és el ket $|a\rangle_5$, havent cridat la funció una única vegada. A més, es veu el paper auxiliar del qubit output, doncs ha estat necessari per la implementació del

circuit però finalment queda inalterat. Està fent el seu paper d'ancilla. Per això es pot fer l'anàlisi usant el truc i prescindint d'ell, tal com hem fet cada vegada que l'output és binari.

10.6 Distribució de Claus Quàntiques via Algorisme de Bernstein-Vazirani

Anem a veure una possible aplicació de l'algorisme de Bernstein-Vazirani per implementar un sistema quàntic de distribució de claus per criptografia. Farà ús de sistemes de qubits entrellaçats com l'algorisme d'Ecker, del tipus

$$|\beta_{00}\rangle \equiv \left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right),$$

on el subíndex A (B) indica que el qubit estarà en possessió d'Alice (de BoB). De fet, aquests qubits poden haver estat generats per una font S independent d'Alice i Bob, a qui els ha enviat la seva part. A més, en lloc d'un d'aquests estats, se'n disposa de varis, n, de manera que els estats compartits els podem escriure com

$$\left|\phi^+\right\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle_A|x\rangle_B$$

Si tant Alice com Bob disposen d'un nombre secret de n bits s_A i s_B respectivament, i avaluen cada un d'ells la funció $f_A(x) = x\cdot s_A$ i $f_B(x) = x\cdot s_B$ aleshores s'obté l'estat

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f_A(s_A)}(-1)^{f_B(s_B)}|x\rangle_A|x\rangle_B,$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot s_A}(-1)^{x\cdot s_B}|x\rangle_A|x\rangle_B,$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot(s_A\oplus s_B)}|x\rangle_A|x\rangle_B.$$

A continuació, Alice i Bob apliquen al seu input la porta $H^{\otimes n,}$ obtenint

$$|\psi_2\rangle = \frac{1}{(\sqrt{2^n})^3}\sum_{x\in\{0,1\}^n}\sum_{y\in\{0,1\}^n}\sum_{z\in\{0,1\}^n}(-1)^{x\cdot(s_A\oplus s_B\oplus y\oplus z)}|y\rangle_A|z\rangle_B,$$

$$|\psi_2\rangle = \frac{1}{(\sqrt{2^n})^3}\sum_{y\in\{0,1\}^n}\sum_{z\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}(-1)^{x\cdot(s_A\oplus s_B\oplus y\oplus z)}|y\rangle_A|z\rangle_B.$$

D'acord amb el que hem trobat quan hem analitzat l'algorisme de Bernstein-Vazirani, el sumatori

$$\sum_{x\in\{0,1\}^n}(-1)^{x\cdot(s_A\oplus s_B\oplus y\oplus z)} = 2^n\delta_{y\oplus z,s_a\oplus s_b},$$

i, per tant

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}}\delta_{y\oplus z,s_a\oplus s_b}\sum_{y\in\{0,1\}^n}\sum_{z\in\{0,1\}^n}(-1)^{x\cdot(s_A\oplus s_B\oplus y\oplus z)}|y\rangle_A|z\rangle_B,$$

que es pot escriure de dues maneres:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} |y\rangle_A \, |s_a \oplus s_b \oplus y\rangle_B$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{z\in\{0,1\}^n} |s_a \oplus s_b \oplus z\rangle_A \, |z\rangle_B \, .$$

Si ara Alice i Bob mesuren el seu input, l'estat col.lapsarà a

$$|\psi_3\rangle = |y_0\rangle_A \, |s_a \oplus s_b \oplus y_0\rangle_B = |s_a \oplus s_b \oplus z_0\rangle_A \, |z_0\rangle_B \, ,$$

amb $y_0, z_0 \in \{0,1\}^n$. En general $y_0 \neq z_0$. La clau secreta és $z_0 = s_a \oplus s_b \oplus y_0$ i és coneguda per Bob. Ara Bob truca a Alice per un canal clàssic insegur i li comunica la seva clau inicial s_B. Com que Alice coneix s_A, y_0 i ara s_B, pot avaluar $y_0 \oplus s_A \oplus s_B = z_0$ i per tant conèixer la clau secreta compartida amb Bob. En cas que Eva escolti la clau s_B enviada pel canal insegur, no disposa de prou informació per reconstruir la clau final, z_0.

A més, aquest algorisme és simètric en el rol d'Alice i Bob.

Hi ha una variant que perd aquesta simetria. És la següent: Bob no fa ús de la seva funció, mentre que Alice sí: $s_a \neq 0$ i $s_B = 0$. Seguint el mateix procediment que abans, l'estat després de mesurar és:

$$|\psi_3\rangle = |y_0\rangle_A \, |s_a \oplus y_0\rangle_B = |s_a \oplus z_0\rangle_A \, |z_0\rangle_B \, ,$$

amb $y_0, z_0 \in \{0,1\}^n$, on, en general $y_0 \neq z_0$. Ara hi ha dues maneres de determinar la clau secreta. La primera és, com abans, la mesura que fa Bob del seu input $z_0 = s_a \oplus y_0$, sense comunicar res de Bob a Alice pel canal insegur. Alice pot obtenir-la ja que coneix s_A i y_0, de manera que la calcula fent $s_A \oplus y_0 = z_0$.

L'altra opció és que s_A sigui la clau secreta, coneguda evidentment per Alice. Truca a Bob pel canal insegur i li diu quin valor y_0 ha mesurat ella. Com que la mesura de Bob és $z_0 = s_A \oplus y_0$, només li caldrà calcular $z_0 \oplus y_0 = s_a \oplus y_0 \oplus y_0 = s_a$ i, per tant, coneixerà la clau que comparteix amb Alice. Com que pel canal insegur només es transmet y_0, l'Eva no té manera de conèixer la clau secreta.

10.7 Algorisme de Simon

Sigui una funció en el domini

$$f(x) : \{0,1\}^n \to \{0,1\}^n,$$

tal que, per un valor $s \in \{0,1\}^n$ no nul, i per tot $x, y \in \{0,1\}^n$, ens prometen que verifica la propietat que

$$f(x) = f(y) \iff x \oplus y = s \in \{0,1\}^n,$$

o, el que és el mateix, f és una funció dos a un (quan $s \neq 0$), tal que

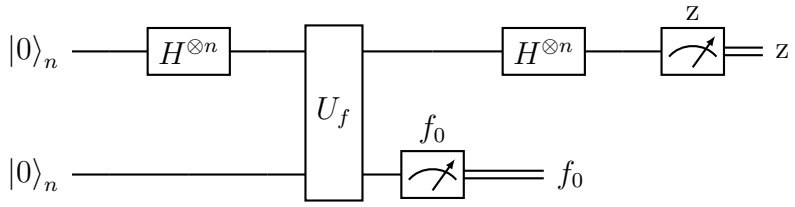
$$f(x) = f(x \oplus s); \quad x \in \{0,1\}^n; \quad s \in \{0,1\}^n$$

amb s desconegut. El problema és trobar s.

Per exemple, si $n = 3$ i la funció és

x	000	001	010	011	100	101	110	111
f(x)	101	010	000	110	000	110	101	010

per inspecció veiem que $s = 110$. La funció és efectivament del tipus dos a un i quan els outputs són iguals, els inputs verifiquen que $x \oplus y = s = 110$. El problema clàssicament és difícil doncs hem d'anar provant diferents inputs fins que l'output coincideixi. Això vol dir que s'han de provar de l'ordre de $O(\sqrt{2^n})$ inputs per tenir assegurat obtenir outputs repetits. Volem veure com ho pot gestionar l'algorisme quàntic, on la funció estarà implementada en un operador U_f. L'estructura de l'algorisme serà la del circuit



La seva evolució vindrà donada per

$$\begin{aligned} |0\rangle_n \otimes |0\rangle_n \xrightarrow{H^{\otimes n}\otimes \mathbb{1}^{\otimes n}} & \quad \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n \otimes |0\rangle_n \\ \xrightarrow{U_f} & \quad \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n \otimes |f(x)\rangle_n \end{aligned}$$

Si ara mesurem el registre output, trobarem algun valor f_0. Això implica que el registre input, que està entrellaçat amb ell, col·lapsarà en inputs x, y tals que $f(x) = f(y) = f_0$, amb $y = x \oplus s$

$$\frac{1}{\sqrt{2}}(|x\rangle + |y\rangle) = \frac{1}{\sqrt{2}}(|x\rangle + |x \oplus s\rangle)$$

Apliquem ara les portes Hadamard a l'input,

$$\begin{aligned} \xrightarrow{H^{\otimes n}\otimes \mathbb{1}^{\otimes n}} & \quad \frac{1}{\sqrt{2}}\frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} \left((-1)^{x\cdot z} + (-1)^{y\cdot z}\right) |z\rangle_n \\ = & \quad \frac{1}{\sqrt{2}}\frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} \left((-1)^{x\cdot z} + (-1)^{(x\oplus s)\cdot z}\right) |z\rangle_n \\ = & \quad \frac{1}{\sqrt{2}}\frac{1}{2^{n/2}} \sum_{z=0}^{2^n-1} (-1)^{x\cdot z} \left(1 + (-1)^{s\cdot z}\right) |z\rangle_n \end{aligned}$$

Si mesurem, obtindrem un estat $|z\rangle_n$ tal que

$$(-1)^{x\cdot z} = (-1)^{y\cdot z} \Rightarrow x \cdot z = y \cdot z = (x \oplus s) \cdot z \Rightarrow z \cdot s = 0,$$

doncs en cas que $z \cdot s = 1$, la probabilitat d'obtenir-lo és nul·la.

Si recordem que

$$z \cdot s = z_0 s_0 \oplus z_1 s_1 \oplus \cdots \oplus z_n s_n,$$

l'algorisme ens subministra una string $z = \{z_0, z_1, \cdots z_n\}$ que verifica $z \cdot s = 0$. Per determinar s (n valors) necessitem tenir n equacions com aquesta, que corresponen a diferents z i que siguin linealment independents (el valor $z = 0$ sempre és una solució). Això vol dir que haurem de córrer l'algorisme complet $(n-1)$ vegades de manera que s'obtinguin $(n-1)$ strings z que verifiquin:

$$\begin{aligned} z^{(1)} \cdot s &= 0 \\ z^{(2)} \cdot s &= 0 \\ &\vdots \\ z^{(n-1)} \cdot s &= 0 \end{aligned}$$

Si són independents, podem solucionar el sistema, trobar un candidat a la solució, $s' \neq 0^n$ i comprovar si $f(0^n) = f(s')$. Si es verifica, sabem que $s' = s$ i hem resolt el problema. En canvi, si $f(0^n) \neq f(s')$, aleshores la solució ha de ser $s = 0^n$. Sigui com sigui, un cop tenim la independència lineal, podem resoldre el problema.

Cal veure ara amb quina probabilitat aquestes equacions seran linealment independents. Imaginem que trobem la primera $z^{(1)}$, que serà independent i útil si és diferent que 0^n, hi ha doncs una única possibilitat que falli, amb probabilitat $\dfrac{1}{2^{n-1}}$ i, per tant, la probabilitat que sigui independent i no fallar és $1 - \dfrac{1}{2^{n-1}}$. De manera similar podem analitzar el segon cas i els següents, tal com recull la següent taula

z mesurat	Falla si surt	Probabilitat de fallar	Probabilitat independent
$z^{(1)}$	$\{0^n\} = 1$	$\frac{1}{2^{n-1}}$	$1 - \frac{1}{2^{n-1}}$
$z^{(2)}$	$\{0^n, z^{(1)}\} = 2$	$\frac{2}{2^{n-1}}$	$1 - \frac{1}{2^{n-2}}$
$z^{(3)}$	$\{0^n, z^{(1)}, z^{(2)}, z^{(1)} + z^{(2)}\} = 4$	$\frac{4}{2^{n-1}}$	$1 - \frac{1}{2^{n-3}}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$z^{(n-1)}$	$\{0^n, z^{(1)}, z^{(2)}, z^{(1)} + z^{(2)}, \cdots, z^{(n-2)}\} = 2^{n-2}$	$\frac{2^{n-2}}{2^{n-1}} = \frac{1}{2}$	$1 - \frac{1}{2} = \frac{1}{2}$

La probabilitat de que els $(n-1)$ valors mesurats donin $(n-1)$ equacions independents serà

$$\prod_{k=1}^{n-1} \left(1 - \frac{1}{2^k}\right) > \prod_{k=1}^{\infty} \left(1 - \frac{1}{2^k}\right) = 0,288788\cdots$$

Per tant, amb $O(n)$ crides a la funció, tenim una probabilitat més gran d'un 28% de trobar el valor s i resoldre el repte.

La cota anterior prové del resultat de la q-serie, que no és fàcil d'obtenir. En canvi, es pot fer una cota menys restrictiva amb un argument senzill.

La probabilitat de fallar en els primers $(n-2)$ intents (excepte el darrer, que té probabilitat 1/2) és, en el pitjor cas (com a màxim)

$$p^{fallar}_{\text{primers } (n-2)} = \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^{n-1}}$$

que es pot expressar com

$$p^{fallar}_{\text{primers }(n-2)} = \frac{1}{4}\left(1+\frac{1}{2}+\frac{1}{4}+\cdots+\frac{1}{2^{n-3}}\right) \leq \frac{1}{4}\left(1+\frac{1}{2}+\frac{1}{4}+\cdots\right) = \frac{1}{2}$$

on hem acotat la suma pel resultat d'una sèrie geomètrica d'infinits termes. Així, la probabilitat d'èxit, d'obtenir els primers $(n-2)$ $z's$ linealment independents,

$$p^{\text{èxit}}_{\text{primers }(n-2)} \geq \frac{1}{2}$$

Així, quan considerem el darrer $z^{(n-1)}$, la probabilitat final de tenir èxit (independència lineal) serà la probabilitat d'haver-ne tingut en els $(n-2)$ anteriors $(\geq 1/2)$ multiplicada per la probabilitat de tenir-ne en el darrer $(1/2)$, obtenint finalment

$$\text{Probabilitat d'èxit } = p^{\text{èxit}}_{\text{primers }(n-2)} \cdot p^{\text{èxit}}_{\text{darrer}} \geq \frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}.$$

11 Algorisme de Grover

L'algorisme de Grover és un algorisme quàntic per cercar un element d'una base de dades desordenada. L'exemple típic és imaginar que es cerca el propietari d'un número de telèfon. Com que la guia telefònica està ordenada per noms però no per números, el procés pot comportar molts intents.

Si la base de dades consta de N_{BD} elements, un pot tenir molta sort i trobar el número correcte al primer intent. També pot tenir molta mala sort i trobar-lo a l'últim. Podem dir que, amb probabilitat 50% el trobarà fent $O(N_{BD}/2)$ intents. Aquest seria la manera standard, clàssica, de fer-ho. Veurem que quànticament es pot fer millor amb l'algorisme de Grover.

Suposem que cada element de la base de dades el tenim etiquetat. Considerem un número de qubits n, el mínim sencer tal que

$$N = 2^n \geq N_{BD}.$$

Podem usar els estats quàntics generats pels n qubits per encabir tots els elements de la base de dades,

$$\{|i>_n; i = 0, \quad \cdots, 2^n - 1\}.$$

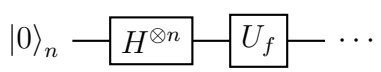
Denotem per $|i_0\rangle_n$ l'element que cerquem. Necessitarem un Oracle que ens confirmi si l'element que estem considerant (mirant) és o no l'element que cerquem. Això ho fa la funció d'output binari,

$$f(i) = \begin{cases} 1 & \text{si } i = i_0 \\ 0 & \text{si } i \neq i_0 \end{cases}$$

que la podrem implementar, dins de l'esquema habitual del truc, amb l'operador unitari

$$U_f\,|i\rangle_n = (-1)^{f(i)}\,|i\rangle_n$$

Ja sabem que, per aprofitar el paral·lelisme quàntic, hem d'entrar a la funció una combinació lineal de tots els 2^n elements de la base. Així, començarem l'algorisme quàntic com és habitual



L'evolució de l'estat inicial seria

$$|0\rangle_n \xrightarrow{H^{\otimes n}} |\psi\rangle_n = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle_n$$

$$\xrightarrow{U_f} |\psi_1\rangle_n = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{f(i)} |i\rangle_n = \frac{1}{\sqrt{N}} \left[\sum_{\substack{i=0 \\ i \neq i_0}}^{N-1} |i\rangle_n - |i_0\rangle_n \right] = |\psi\rangle_n - \frac{2}{\sqrt{N}} |i_0\rangle_n$$

Veiem que trobem una combinació lineal de tots els termes tal que el signe de l'element cercat ha canviat respecte al de tota la resta d'elements, gràcies a l'oracle. De totes maneres, si ara féssim la mesura de l'estat, la probabilitat d'obtenir cada un de tots els diferents valors és la mateixa. Amb la funció oracle, no en tenim prou perquè l'element cercat tingui una probabilitat més alta que la resta. Cal fer alguna cosa més.

Grover va pensar en l'operador inversió respecte la mitjana (Inversion Around de Mean) definit com:

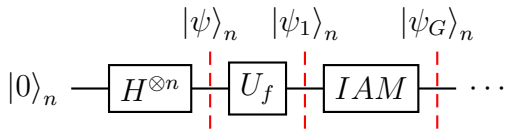
$$IAM = 2 |\psi\rangle_{n\,n}\langle\psi| - \mathbb{1}$$

Aquest és un operador que actua de la manera següent

$$\begin{aligned} IAM\,|\psi\rangle_n &= [2\,|\psi\rangle_{n\,n}\langle\psi| - \mathbb{1}]\,|\psi\rangle_n = 2\,|\psi\rangle_{n\,n}\langle\psi|\psi\rangle_n - |\psi\rangle_n = |\psi\rangle_n \\ IAM\,|i_0\rangle_n &= [2\,|\psi\rangle_{n\,n}\langle\psi| - \mathbb{1}]\,|i_0\rangle_n = 2\,|\psi\rangle_{n\,n}\langle\psi|i_0\rangle_n - |i_0\rangle_n = \frac{2}{\sqrt{N}}\,|\psi\rangle_n - |i_0\rangle_n \end{aligned}$$

on hem fet ús que ${}_n\langle\psi|\psi\rangle_n = 1$ i que ${}_n\langle\psi|i_0\rangle_n = \frac{1}{\sqrt{N}}$.

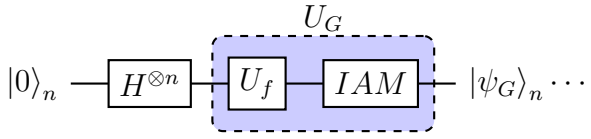
Si apliquem l'operador IAM sobre l'estat $|\psi_1\rangle_n$, ampliem la seqüència de portes



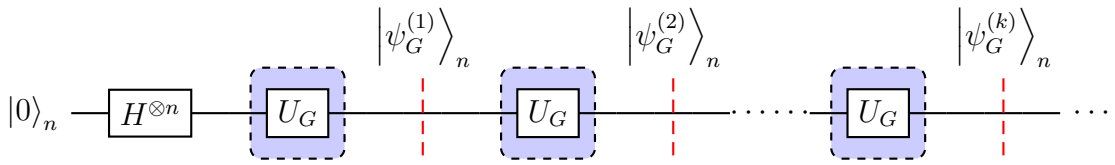
i n'obtenim el resultat

$$|\psi_G\rangle_n = IAM\,|\psi_1\rangle_n = IAM\left[|\psi\rangle_n - \frac{2}{\sqrt{N}}|i_0\rangle_n\right] = |\psi\rangle_n - \frac{4}{N}|\psi\rangle_n + \frac{2}{\sqrt{N}}|i_0\rangle = \left(1 - \frac{4}{N}\right)|\psi\rangle_n + \frac{2}{\sqrt{N}}|i_0\rangle_n$$

és a dir, una superposició de tots els estats on el coeficient de l'estat que cerquem és $\left[\left(1 - \frac{4}{N}\right)\frac{1}{\sqrt{N}} + \frac{2}{\sqrt{N}}\right]$, que és més gran que el de qualsevol altre $\left(1 - \frac{4}{N}\right)\frac{1}{\sqrt{N}}$. Ara ja hi ha una probabilitat més gran de trobar el que cerquem que qualsevol altre, tot i que quan N és molt gran, l'augment és molt petit. A la combinació de la porta U_f i IAM se l'anomena U_G, porta de Grover.



Què passa si, un cop aplicada la porta de Grover i, abans de mesurar, es torna a aplicar de nou vàries vegades?



Si ens fixem, l'estat $|\psi_G\rangle_n$ és una combinació lineal dels estats $|\psi\rangle_n$ i $|i_0\rangle_n$ i sabem com actua cada un dels components de l'operador de Grover sobre cada un d'ells. Concretament

$$\begin{aligned} U_f\,|\psi\rangle_n &= |\psi\rangle_n - \frac{2}{\sqrt{N}}\,|i_0\rangle_n \\ U_f\,|i_0\rangle_n &= -\,|i_0\rangle_n \\ IAM\,|\psi\rangle_n &= |\psi\rangle_n \\ IAM\,|i_0\rangle_n &= \frac{2}{\sqrt{N}}\,|\psi\rangle_n - |i_0\rangle_n \end{aligned}$$

per tant, successives aplicacions de l'operador de Grover donaran sempre combinacions lineals dels mateixos estats, amb coeficients reals, que es podran representar en un pla, en termes de vectors. Els brackets poden interpretar-se com projeccions d'un vector unitari sobre un altre, també unitari (el seu producte escalar). La projecció de l'estat $|\psi\rangle_n$ sobre $|i_0\rangle_n$ és

$${}_n\langle i_0|\psi\rangle_n = \frac{1}{\sqrt{N}} \equiv \cos\alpha \equiv \sin\frac{\theta}{2}$$

on α és l'angle que formen els dos vectors i $\theta/2$ el seu complementari. Observem que el seu producte escalar, quan N és molt gran, és un valor molt petit, però no nul, indicant que els dos vectors no són estrictament perpendiculars. Anem a definir un vector $|u\rangle_n$ que sigui perpendicular a $|i_0\rangle_n$ i els podem usar com a vectors ortonormals del nostre espai vectorial.

$$|\psi\rangle_n = \frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle_n = \frac{1}{\sqrt{N}}\left[\sum_{\substack{i=0\\ i\neq i_0}}^{N-1}|i\rangle_n + |i_0\rangle_n\right] = \frac{\sqrt{N-1}}{\sqrt{N}}\,|u\rangle_n + \frac{1}{\sqrt{N}}\,|i_0\rangle_n$$

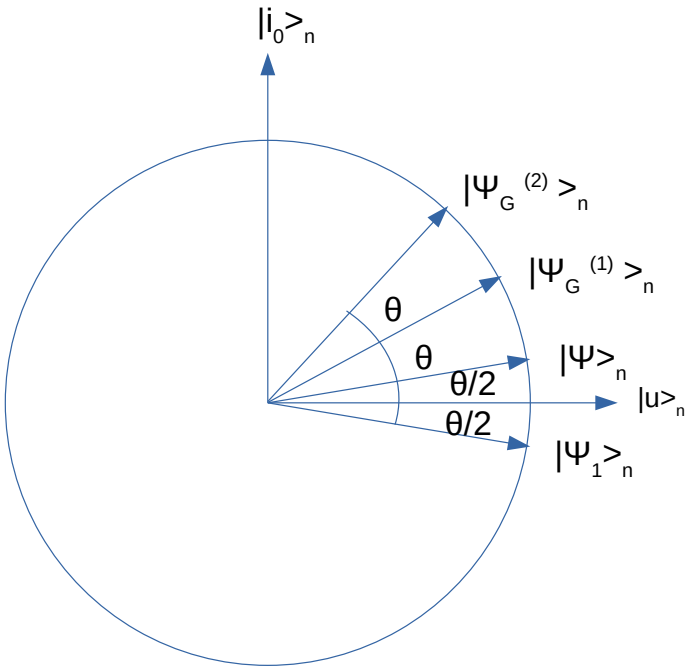
on hem definit el vector unitari $|u\rangle_n$

$$|u\rangle_n \equiv \frac{1}{\sqrt{N-1}}\sum_{\substack{i=0\\ i\neq i_0}}^{N-1}|i\rangle_n$$

que és perpendicular al $|i_0\rangle$, ja que ${}_n\langle i_0|u\rangle_n = 0$ perquè els vectors de la base que intervenen dins del $|u\rangle_n$ no hi ha el $|i_0\rangle$. Els kets $\{|u\rangle_n, |i_0\rangle\}$ són ortonormals i formen una base de l'espai bidimensional on viuen els estats generats per les aplicacions successives de l'operador de Grover. A la figura es mostra la base i els diferents estats que s'obtenen durant la realització de l'algorisme, en un cercle de radi la unitat. Ja hem vist que $|\psi\rangle_n$ forma un angle α amb el $|i_0\rangle_n$ i, equivalentment, un angle $\theta/2$ amb el $|u\rangle_n$.

Veiem ara on hem de situar el ket $|\psi_1\rangle_n$. Recordant que $|\psi_1\rangle_n = |\psi\rangle_n - \frac{2}{\sqrt{N}}\,|i_0\rangle$, podem expressar

$$\begin{aligned} |\psi\rangle_n &= \frac{\sqrt{N-1}}{\sqrt{N}}\,|u\rangle_n + \frac{1}{\sqrt{N}}\,|i_0\rangle_n \\ |\psi_1\rangle_n &= \frac{\sqrt{N-1}}{\sqrt{N}}\,|u\rangle_n - \frac{1}{\sqrt{N}}\,|i_0\rangle_n \end{aligned}$$



i les projeccions sobre l'estat $|u\rangle_n$ són

$$ {}_n\langle u|\psi\rangle_n = {}_n\langle u|\psi_1\rangle_n \quad = \quad \sqrt{\frac{N-1}{N}} = \cos\frac{\theta}{2} $$

amb la diferència que $|\psi\rangle_n$ està per sobre de l'eix horitzontal, mentre que $|\psi_1\rangle_n$ està per sota. Això es pot veure notant que $|\psi_1\rangle_n$ i $|\psi\rangle_n$ difereixen només en el signe de $|i_0\rangle_n$ en les seves expressions. L'efecte del primer operador de Grover, U_f és passar de $|\psi\rangle_n$ a $|\psi_1\rangle_n = U_f\,|\psi\rangle_n$, és a dir, fer una reflexió especular del primer respecte l'eix $|u\rangle_n$. Per consistència, calculem quina seria la projecció de $|\psi_1\rangle_n$ sobre $|\psi\rangle_n$,

$$ {}_n\langle\psi|\psi_1\rangle_n = {}_n\langle\psi|\left\{|\psi\rangle_n - \frac{2}{\sqrt{N}}\,|i_0\rangle_n\right\} = 1 - \frac{2}{N} = \cos\theta, $$

on la darrera igualtat es dedueix a partir de $\sin\theta/2 = 1/\sqrt{N}$ i $\cos\theta = \cos^2(\theta/2) - \sin^2(\theta/2)$.

Per veure l'efecte del segon operador, IAM, hem de veure on està situat l'estat $|\psi_G\rangle_n$. Calculem la projecció

$$ {}_n\langle\psi|\psi_G\rangle_n = {}_n\langle\psi|\left\{\left(1 - \frac{4}{N}\right)|\psi\rangle_n + \frac{2}{\sqrt{N}}\,|i_0\rangle_n\right\} = (1 - \frac{4}{N}) + \frac{2}{N} = 1 - \frac{2}{N} = \cos\theta, $$

i trobem que l'angle que formen $|\psi_G\rangle_n$ i $|\psi\rangle_n$ és θ, situat al primer quadrant de manera que $|\psi_G\rangle_n$ i $|u\rangle_n$) formen un angle $\frac{\theta}{2}+\theta$. Com que IAM actua sobre $|\psi_1\rangle_n$ per transformar-lo en $|\psi_G\rangle_n$, veiem que l'efecte de l'operador IAM és una reflexió especular respecte l'estat $|\psi\rangle_n$. D'aquí el seu nom, inversió respecte la mitjana. Així, en aquesta visió geomètrica podem veure que l'acció final de l'operador de Grover és

$$ |\psi_G\rangle_n = \cos\left(\frac{\theta}{2}+\theta\right)|u\rangle_n + \sin\left(\frac{\theta}{2}+\theta\right)|i_0\rangle_n\,. $$

Si ara iterem l'operador de Grover un nombre de vegades k, la seva acció sempre serà partir d'un estat i aplicar-li una reflexió respecte l'eix horitzontal, $|u\rangle_n$, deguda a U_f, seguida d'una reflexió respecte l'estat $|\psi\rangle_n$, deguda a l'operador IAM. Això implica que, a cada iteració, l'angle augmenta un valor θ constant, com un pas de rosca, sempre en el sentit de gir antihorari. Així, l'estat a la iteració k serà

$$\left|\psi_G^{(k)}\right\rangle_n = \cos\left(\frac{\theta}{2}+k\theta\right)|u\rangle_n + \sin\left(\frac{\theta}{2}+k\theta\right)|i_0\rangle_n\,.$$

Cal recordar que els coeficients dels kets son, elevats al quadrat, la probabilitat que tenim de mesurar-los. Veiem que la probabilitat de mesurar l'element cercat, $|i_0\rangle_n$ a la iteració k és

$$p_k(i_0) = \sin^2\left(\frac{\theta}{2}+k\theta\right).$$

Aquí es veu que és important saber en quin moment hem de parar. Si mesurem massa aviat, o massa tard, pot ser que tinguem molt poca probabilitat d'èxit. Cal trobar doncs quina és la iteració òptima, k_o, per maximitzar la probabilitat de tenir èxit. Per això, volem

$$p_k \;=\; \sin^2\left(\frac{\theta}{2}+k\theta\right)=1 \quad\rightarrow\quad \frac{\theta}{2}+k_o\theta=\frac{\pi}{2};\quad k_o=\left[\frac{\pi-\theta}{2\theta}\right],$$

on el parèntesi final indica que s'ha de prendre la part sencera més propera al número del seu interior. Podem trobar una expressió aproximada, vàlida per N molt gran, recordant que $\sin\frac{\theta}{2}=\frac{1}{\sqrt{N}}\simeq\frac{\theta}{2}$ i, per tant $\theta\simeq\frac{2}{\sqrt{N}}$, on hem fet ús que N serà molt gran, $\sin\theta$ molt petit i, per tant, aproximadament igual a θ. Tot plegat, el nombre òptim d'iteracions k_o quan N és molt gran, aproximadament serà

$$k_o=\left[\frac{\pi-\theta}{2\theta}\right]\simeq\left[\frac{\pi-2/\sqrt{N}}{4/\sqrt{N}}\right]\simeq\left[\frac{\pi}{4}\sqrt{N}\right]$$

que és un número de l'orde de $\sqrt{N}$. L'avantatge quàntic és palès, recordant que clàssicament necessitem un nombre de l'ordre $N/2$ per trobar l'element, amb una probabilitat del 50%. Ara només cal valorar quina és la probabilitat d'encertar a la iteració k_o de l'algorisme quàntic. La iteració serà òptima quan el vector que descriu l'estat $\left|\psi_G^{(k)}\right\rangle$ amb el $|i_0\rangle$ formi un angle β tal que $\beta<\theta/2$. aleshores

$$p_{k_o}=\cos^2\beta\geq\cos^2\frac{\theta}{2}=1-\frac{1}{N},$$

una probabilitat molt propera a 1 i que, de fet, tendeix a 1 quan N tendeix a infinit.

12 Algorisme de Shor

L'algorisme de Shor és un algorisme de factorització. Pretén trobar quins són els factors p i q d'un nombre N, tal que $N=pq$.

Aquest és un procés difícil de realitzar.

És un procés interessant, doncs el sistema d'encriptació actual està basat en RSA, que es pot trencar si es coneixen els dos factors d'un número molt gran.

L'algorisme de Shor té varies parts. Algunes són clàssiques i una quàntica. Esquemàticament:

1. Donat N, volem trobar els seus factors p i q.
2. Escollim y coprimer amb N, $g.c.d.(N,y)=1$. Si no és coprimer, ja tenim un factor.
3. Cerquem el període, r, de la funció $f(x)=y^x \bmod N$ ($f(0)=f(r)=1$).
4. Si r és imparell, retornem al punt 2.

5. Si r és parell, calculem $g.c.d(y^{r/2} \pm 1, N)$. Almenys un dels dos és un factor de N

Totes les parts excepte la 3^a són completament clàssiques. La 3^a té una component quàntica i una de clàssica. Abans de descriure la 3^a fase, justifiquem el punt 5.

Considerem l'equació:

$$x^2 - 1 = 0 \text{ mod } N \rightarrow (x+1)(x-1) = 0 \text{ mod } N = mN; \quad m > 0 \text{ enter}$$

i cerquem solucions no trivials ($x \neq 1; x \neq -1$). Això vol dir que, o bé $(x+1)$ i/o $(x-1)$ és un divisor de N o, equivalentment, que almenys un de

$$g.c.d(x \pm 1, N)$$

és un factor de N. Si considerem ara que r és parell i el període de la nostra funció,

$$y^r = 1 \text{ mod } N \rightarrow (y^{r/2}+1)(y^{r/2}-1) = 0 \text{ mod } N,$$

i per tant, almenys un dels valors

$$g.c.d.(y^{r/2} \pm 1, N)$$

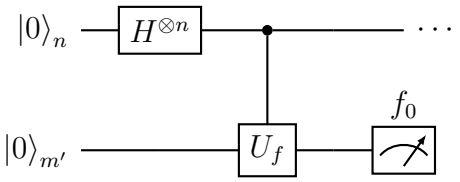
és un factor de N.

Per trobar el període de la funció entra en joc la part quàntica (tot i que no trobarà el període directament, sinó que ens donarà una informació, que podrem tractar després en un ordinador clàssic i extreure'n, ara sí, el període cercat).

Volem trobar el període de la funció $f(x) = y^x \text{ mod } N$. Per això considerarem un registre input de n qubits, essent n l'enter més petit tal que

$$2^n \geq N^2$$

(n ha de ser suficientment gran per poder trobar el període r. Justificarem més endavant aquesta elecció.) Tindrem també un registre output de m' qubits, amb m' el menor enter tal que $2^{m'} \geq N$ (l'output ha d'encabir fins a N valors. El nostre algorisme l'anirem discutint pas a pas. Està clar que, en prime lloc, hem de fer ús del paral·lelisme quàntic i aplicarem una Hadamard a cada un dels qubits de l'input, seguides de l'operador unitari que implementa la funció:



$$\begin{aligned}
|0\rangle_n |0\rangle_{m'} \quad &\xrightarrow{H^{\otimes n} \otimes \mathbb{1}^{\otimes m'}} \quad H^{\otimes n} |0\rangle_n |0\rangle_{m'} = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |0\rangle_{m'} \\
&\xrightarrow{U_f} \qquad \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |f(x)\rangle_{m'} \\
&\xrightarrow{\mathbb{1} \otimes \text{Mesura } f_0} \quad \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n |f_0\rangle_{m'}
\end{aligned}$$

on hem mesurat el registre output, trobant el valor f_0, amb $x_0 + kr$ tots els valors d'input que tenen f_0 com output. Recordem que la funció té període r, desconegut i que volem trobar. m és el nombre d'inputs que tenen el mateix valor d'output i que podem acotar-lo veient:

$$x_0 + (m-1)r \leq 2^n; x_0 + mr > 2^n; x_0 < r \rightarrow m \geq \frac{2^n}{r}$$

L'estat input, després de la mesura de l'output, queda:

$$|\psi\rangle_n = \quad \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n$$

Pensem què passaria si mesuréssim el registre d'input:

Quan el mesuréssim, trobaríem algun dels m valors possibles (amb output f_0). Però a partir del seu coneixement no en podem extreure el període.

Si el tornéssim mesurar, degut al col·lapse en la mesura quàntica, el valor no canviaria.

Si el poguéssim clonar abans de fer la mesura, ens permetria fer varies mesures als clons que ens donarien altres valors. Fent diferències entre ells, podríem extreure'n el període o múltiples d'ell i, finalment aconseguiríem trobar-lo. Però el teorema de no-clonació ens diu que això no es pot fer.

L'única opció que ens quedaria seria reiniciar l'algorisme. Mesuraríem de nou el registre output i trobaríem f_1 que, amb probabilitat molt alta seria diferent de la primera mesura, f_0. Quan mesuréssim el registre input trobaríem algun valor de la seqüència $x_1 + kr$ que no ens permetria, fent diferències, trobar el període ja que $x_0, x_1 < r$.

Cal fer doncs alguna cosa més abans de mesurar l'input.

La nostra expertesa ens porta a pensar que potser caldria aplicar Hadamards a l'input i, després, mesurar-lo. Veiem què passaria:

$$\begin{aligned}
H^{\otimes n} |\psi\rangle_n &= \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} H^{\otimes n} |x_0 + kr\rangle_n = \frac{1}{\sqrt{2^n m}} \sum_{k=0}^{m-1} \sum_{l=0}^{2^n-1} (-1)^{l\cdot(x_0+kr)} |l\rangle_n \\
&= \sum_{l=0}^{2^n-1} \left[\frac{1}{\sqrt{2^n m}} \sum_{k=0}^{m-1} (-1)^{l\cdot(x_0+kr)} \right] |l\rangle_n = \sum_{l=0}^{2^n-1} \left[\frac{1}{\sqrt{2^n m}} (-1)^{l\cdot x_0} \sum_{k=0}^{m-1} (-1)^{l\cdot kr} \right] |l\rangle_n \\
&= \sum_{l=0}^{2^n-1} a_l |l\rangle_n ; \\
a_l &= \frac{1}{\sqrt{2^n m}} (-1)^{l\cdot x_0} \sum_{k=0}^{m-1} (-1)^{l\cdot kr}
\end{aligned}$$

on es veu que apareix una suma de tots els estats possibles amb uns coeficients a_l. La probabilitat de trobar -si mesuréssim ara- el valor l corresponent al ket $|l\rangle$ és:

$$p_l = |a_l|^2 = \frac{1}{2^n m} \left| \sum_{k=0}^{m-1} (-1)^{l\cdot kr} \right|^2$$

on x_0 ha desaparegut de la probabilitat. Aparentment sembla que es va pel bon camí, la probabilitat no depèn de x_0 ni de f_0. De totes maneres, veiem en un exemple que això no és suficient per trobar el període.

Suposem que disposem de $n = 3$ qubits i que el període de la funció sigui $r = 2$. Està clar que $2^n = 2^3 = 8$ i $m = \frac{2^n}{r} = 4$. Tenint en compte que $l \cdot kr$ és la suma mòdul 2 del producte bit a bit, i que $2k = \{(0,0,0),(0,1,0),(1,0,0),(1,1,0); k = 0,1,2,3\}$, tindrem

$$\begin{aligned}
p_0 &= \frac{1}{32}|1+1+1+1|^2 = 1/2; \quad \text{doncs } l = 0 = (0,0,0) \text{ en binari} \\
p_1 &= \frac{1}{32}|1+1+1+1|^2 = 1/2; \quad \text{doncs } l = 1 = (0,0,1) \text{ en binari} \\
p_2 &= \frac{1}{32}|1-1+1-1|^2 = 0; \quad \text{doncs } l = 2 = (0,1,0) \text{ en binari} \\
&\vdots \\
p_7 &= \frac{1}{32}|1-1-1+1|^2 = 0; \quad \text{doncs } l = 7 = (1,1,1) \text{ en binari.}
\end{aligned}$$

De fet, un cop hem vist que $p_0 = p_1 = 1/2$, la resta de valors han de tenir probabilitat 0, cosa que es pot comprovar fent l'anàlisi similar als casos explicitats per p_2 i p_7.

Així, només podem trobar, quan mesurem l'input, els nombres 0 i 1, que no donen cap informació sobre el període r que busquem.

Shor va pensar una alternativa a la porta Hadamard: La transformada de Fourier quàntica, F, definida de manera que actuant sobre un ket $|x\rangle_n$ el transforma en:

$$F|x\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{i\frac{2\pi xy}{2^n}} |y\rangle_n ,$$

és a dir, una nova combinació lineal amb pesos complexos, on el producte que apareix a l'exponent, xy, és el producte normal dels valors x vegades y.

Al final d'aquesta secció veurem una manera d'expressar l'operador F en termes de bras i kets, i demostrarem que l'operador és unitari. Ens interessa saber quina és l'acció de la transformada de Fourier quàntica sobre l'estat $|\psi\rangle_n$. Veiem-ho:

$$\begin{aligned}
F|\psi\rangle_n &= F\frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_n = \frac{1}{\sqrt{m}} \frac{1}{2^{n/2}} \sum_{k=0}^{m-1} \sum_{l=0}^{2^n-1} e^{i\frac{2\pi(x_0+kr)l}{2^n}} |l\rangle_n \\
&= \sum_{l=0}^{2^n-1} \left[\frac{1}{2^{n/2}\sqrt{m}} \sum_{k=0}^{m-1} e^{i\frac{2\pi(x_0+kr)l}{2^n}} \right] |l\rangle_n \\
&= \sum_{l=0}^{2^n-1} \left[\frac{1}{2^{n/2}\sqrt{m}} e^{i\frac{2\pi x_0 l}{2^n}} \sum_{k=0}^{m-1} e^{i\frac{2\pi krl}{2^n}} \right] |l\rangle_n = \sum_{l=0}^{2^n-1} a_l |l\rangle_n ,
\end{aligned}$$

una superposició de tots els estats, de manera que el ket $|l\rangle_n$ té un coeficient, a_l, donat per

$$a_l = \frac{1}{2^{n/2}\sqrt{m}} e^{i\frac{2\pi x_0 l}{2^n}} \sum_{k=0}^{m-1} e^{i\frac{2\pi}{2^n}krl}.$$

La probabilitat de mesurar el valor l és

$$p_l = |a_l|^2 = \frac{1}{2^n m} \left| \sum_{k=0}^{m-1} e^{i\frac{2\pi}{2^n}krl} \right|^2 = \frac{1}{2^n m} |S|^2$$

Fixem-nos que no apareix x_0, i que el sumatori es redueix a una sèrie geomètrica del tipus

$$S = a_0 + a_1 + a_2 \cdots + a_{m-1}$$

on cada terme és igual a l'anterior multiplicat per la raó R, $a_1 = a_0 R, a_2 = a_1 R, \cdots$ La seva suma S, val

$$S = a_0 \frac{1 - R^m}{1 - R}.$$

Abans d'avaluar aquesta suma, pensem què passaria en un cas particular. Suposem que prenem un valor l_j que sigui un múltiple de $2^n/r$, $l_j = j2^n/r$ (suposem que $2^n/r$ és sencer, per tant). Aleshores la fase que apareix a l'exponencial és $i2\pi jk$, amb $k = 0, 1, 2, \cdots (m-1)$. Això implica que $e^{i2\pi jk} = 1$ a tots els sumands: la seva suma serà m i, per tant,

$$p_{l_j} = \frac{m}{2^n}; \quad \text{si } \frac{2^n}{r} \text{ és sencer i } l_j = j\frac{2^n}{r}$$

Ara bé, la restricció anterior, que $2^n/r$ sigui sencer, és molt severa. De fet, és molt improbable que $2^n/r$ sigui sencer. Quan valen les probabilitats en aquest cas, més general?

Fixem-nos que, quan mesurem, trobarem un nombre sencer, l_j, que sempre es podrà escriure com

$$l_j = j\frac{2^n}{r} + \Delta_j,$$

amb j sencer, i volem saber la probabilitat $p_{l_j} = p(l_j)$ que tenim de mesurar-lo. En l'expressió anterior, Δ_j és la mínima quantitat, generalment no sencera, que indica quant difereix l_j de $j\frac{2^n}{r}$.

En el nostre cas, la sèrie geomètrica té els paràmetres

$$a_0 = 1, \quad R = e^{i\frac{2\pi}{2^n} r l_j} = e^{i\frac{2\pi}{2^n} r (j\frac{2^n}{r} + \Delta_j)} = e^{i\frac{2\pi}{2^n} r \Delta_j}$$

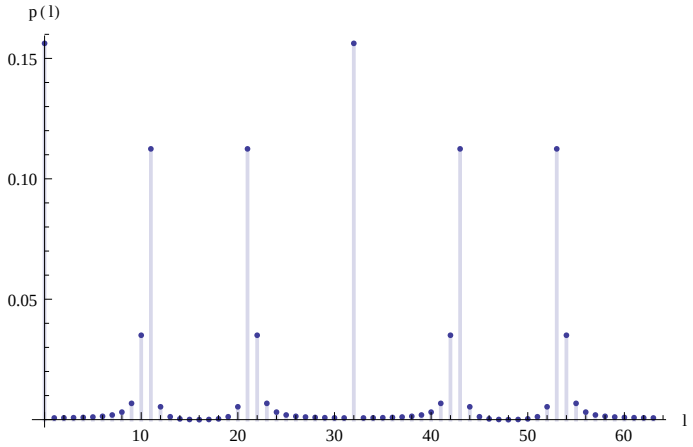
i, per tant, la suma només depèn de Δ_j, de quan es desvia l_j d'un múltiple sencer de $\frac{2^n}{r}$. Per això l'expressarem com $S_{\Delta_j} \equiv S(\Delta_j)$ i valdrà

$$\begin{aligned}
S(\Delta_j) &= \frac{1 - e^{i\frac{2\pi}{2^n} r \Delta_j m}}{1 - e^{i\frac{2\pi}{2^n} r \Delta_j}} \\
&= \frac{e^{i\frac{\pi}{2^n} r \Delta_j m}}{e^{i\frac{\pi}{2^n} r \Delta_j}} \frac{e^{-i\frac{\pi}{2^n} r \Delta_j m} - e^{i\frac{\pi}{2^n} r \Delta_j m}}{e^{-i\frac{\pi}{2^n} r \Delta_j} - e^{i\frac{\pi}{2^n} r \Delta_j}} \\
&= \frac{e^{i\frac{\pi}{2^n} r \Delta_j m}}{e^{i\frac{\pi}{2^n} r \Delta_j}} \frac{-2i \sin\left(\frac{\pi}{2^n} r \Delta_j m\right)}{-2i \sin\left(\frac{\pi}{2^n} r \Delta_j\right)} \\
|S(\Delta_j)|^2 &= \frac{\sin^2\left(\frac{\pi}{2^n} r \Delta_j m\right)}{\sin^2\left(\frac{\pi}{2^n} r \Delta_j\right)}
\end{aligned}$$

Per tant, recopilant,

$$p(l_j) = \frac{1}{2^n m} |S(\Delta_j)|^2 = \frac{1}{2^n m} \frac{\sin^2\left(\frac{\pi}{2^n} r \Delta_j m\right)}{\sin^2\left(\frac{\pi}{2^n} r \Delta_j\right)} \equiv p(\Delta_j)$$

és a dir, tots els valors que distin el mateix $\pm\Delta_j$ d'un nombre sencer tenen la mateixa probabilitat de ser mesurats. Cal dir que aquesta expressió, quan $\Delta_j = 0$ es comporta com hem trobat prèviament, $p(\Delta_j = 0) = \frac{m}{2^n}$. En la figura següent, representem la probabilitat pel cas en què $n = 6, r = 6, m = 10$ on es veu que els valors amb probabilitat més alta són aquells que poden escriure's com $j2^n/r = j64/6 = j32/3$ amb j sencers, és a dir, $0, 32, \cdots$, pels quals el seu $\Delta_j = 0$. També es pot veure que,



com més gran és Δ_j la probabilitat es fa molt més petita. La part quàntica de l'algorisme de Shor, que cerca el període r de la funció, no ens dona r sinó que ens dona valors del tipus $j2^n/r + \Delta_j$, amb j sencer i amb probabilitats que depenen fortament de Δ_j, essent les probabilitats més grans per Δ_j propers a 0.

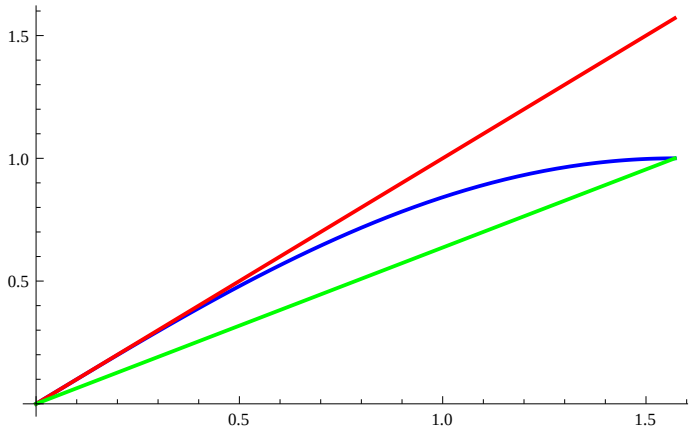
Anem a centrar-nos en acotar quina és la probabilitat de trobar algun

$$l_j = j2^n/r + \Delta_j; \quad j \text{ sencer i tal que } |\Delta_j| \leq 1/2.$$

Partim de

$$p(l_j) = \frac{1}{2^n m}|S(\Delta_j)|^2 = \frac{1}{2^n m}\frac{\sin^2\left(\frac{\pi}{2^n} r\Delta_j m\right)}{\sin^2\left(\frac{\pi}{2^n} r\Delta_j\right)} \equiv p(\Delta_j)$$

i dibuixem a la figura la funció $y_1 = \sin x$ (línia blava) , junt a les funcions $y_2 = x$ (línia vermella) i $y_3 = \frac{x}{\pi/2}$ (línia verda) a l'interval $[0, \pi/2]$.



Veiem que la funció sinus es comporta com

$$\frac{x}{\pi/2} \leq \sin x \leq x,$$

Això vol dir que podem escriure

$$p(l_j) = \frac{1}{2^n m}|S(\Delta_j)|^2 > \frac{1}{2^n m}\left|\frac{\frac{2}{2^n} r\Delta_j m}{\frac{\pi}{2^n} r\Delta_j}\right|^2 = \frac{1}{2^n m}\left|\frac{2}{\pi} m\right|^2 = \frac{4}{\pi^2}\frac{m}{2^n} > \frac{4}{\pi^2}\frac{1}{r}$$

on a l'últim pas hem usat que $m \geq 2^n/r$, és a dir, $m/2^n \geq 1/r$. Si ara tenim en compte que hi haurà r valors propers a $2^n/r$ en l'interval $[0, 2^n - 1]$, la probabilitat de trobar-ne algun d'ells (que no sigui

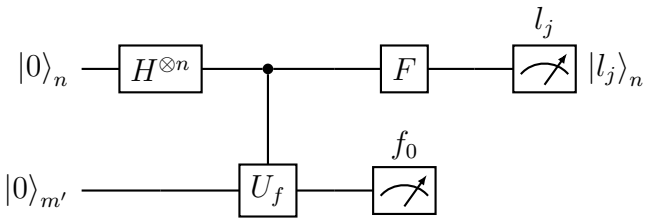
el 0, que no donaria informació) serà

$$p(\text{algun } l_j \text{ útil }) \geq \frac{4}{\pi^2}\frac{r-1}{r} > 0,4; \quad \text{quan } r >> 1.$$

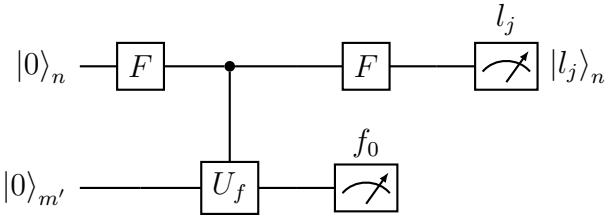
Aquí s'acaba la part quàntica de l'algorisme de Shor. Amb probabilitat més gran d'un 40% trobarem un valor del tipus [1]

$$l_j = j\frac{2^n}{r} + \Delta_j \text{ amb } |\Delta_j| < 1/2.$$

L'esquema de l'algorisme quàntic complet seria:



amb F la transformada de Fourier quàntica per n qubits. Cal precisar que la porta $H^{\otimes n}$ pot ser substituïda per F ja que, quan actuen sobre l'estat inicial, $|0\rangle_n$, es comporten idènticament. Així obtenim la versió final, més simètrica, de la part quàntica de l'algorisme de Shor:



El problema es concentra ara en com determinar el període r quan es coneix algun

$$l_j = j\frac{2^n}{r} + \Delta_j; \quad |\Delta_j| \leq \frac{1}{2},$$

amb j sencer, o equivalentment

$$\left| l_j - j\frac{2^n}{r} \right| = |\Delta_j| \leq \frac{1}{2},$$

$$\left| \frac{l_j}{2^n} - \frac{j}{r} \right| \leq \frac{1}{2 \cdot 2^n} < \frac{1}{2N^2} < \frac{1}{2r^2}$$

on hem fet ús de que $2^n > N^2$ i que $r < N$. Ara podem aclarir perquè el nombre n de qubits del registre input el varem triar de manera que $2^n > N^2$. El motiu és per poder arribar a l'equació anterior, la qual ens permet assegurar que j/r és un convergent de $l_j/2^n$. Trobar r és ara un procés que es podrà fer amb un ordinador clàssic utilitzant les propietats de les fraccions contínues, els convergents d'un nombre racional i el teorema general dels convergents.

[1] En el nostre exemple numèric, els valors l_j són 0, 11, 21, 32, 43, 53, que corresponen a $j = 0, 1, 2, 3, 4, 5$ amb $\Delta_j = 0, +1/3, -1/3, 0, +1/3, -1/3$, respectivament, essent $p(\Delta_j = 0) = 0,156$ i $p(|\Delta_j| = 1/3) = 0,112$. La $p(\text{algun } l_j \text{ útil }) = 0,156 + 4 \times 0,112 = 0,606$ que, efectivament, és més gran que $0,4$.

12.1 Fraccions contínues

Donat un nombre racional x sempre es pot escriure com una fracció contínua finita del tipus

$$x = [a_0, a_1, \cdots, a_N]$$

on a_0 és sencer, a_i son enters positius amb $i = 1, \cdots, N$ i N és sencer no negatiu. La seva relació és

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + a_N}}}$$

Veiem un exemple. Suposem que $x = 77/65$ i cerquem la seva fracció contínua.

$$\begin{aligned}\frac{77}{65} &= 1 + \frac{12}{65} = 1 + \frac{1}{\frac{65}{12}} = 1 + \frac{1}{5 + \frac{5}{12}} = 1 + \frac{1}{5 + \frac{1}{\frac{12}{5}}} \\ &= 1 + \frac{1}{5 + \frac{1}{2 + \frac{2}{5}}} = 1 + \frac{1}{5 + \frac{1}{2 + \frac{1}{\frac{5}{2}}}} = 1 + \frac{1}{5 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}}\end{aligned}$$

d'on es desprèn que

$$\frac{77}{65} = [1, 5, 2, 2, 2].$$

Els valors a_i s'obtenen, en general, segons la regla

$$a_0 = [x]; \chi_0 = x - a_0; \quad a_n = [1/\chi_{n-1}]; \chi_n = 1/\chi_{n-1} - a_n, \quad 0 < n \leq N$$

on $[x]$ indica la part entera de x.

El convergent n d'una fracció contínua $x = [a_0, a_1, \cdots, a_N]$ és

$$x_n = [a_0, a_1, \cdots, a_n], \quad n \leq N$$

que representa, per cada n, diferents aproximacions al valor x, recuperant aquest quan $n = N$. Cada un dels convergents, x_n, es pot escriure com un nombre racional, $x_n = p_n/q_n$, que es pot trobar amb el següent algorisme:

$$\begin{array}{lll} p_0 = a_0 & p_1 = a_0 a_1 + 1 & p_n = a_n p_{n-1} + p_{n-2}; \quad n \geq 2 \\ q_0 = 1 & q_1 = a_1 & q_n = a_n q_{n-1} + q_{n-2}; \quad n \geq 2 \end{array}$$

De fet convindrà avaluar els convergents junt amb el seu valor racional, cosa que es pot fer amb la següent taula, fent la fracció contínua del racional x :

n	0	1	n ≥ 2
a_n	$[x]$	$[1/\chi_0]$	$[1/\chi_{n-1}]$
χ_n	$x - a_0$	$1/\chi_0 - a_1$	$1/\chi_{n-1} - a_n$
p_n	a_0	$a_0a_1 + 1$	$a_np_{n-1}+p_{n-2}$
q_n	1	a_1	$a_nq_{n-1}+q_{n-2}$

La comprovem en l'exemple en que $x = 77/65$

n	0	1	2	3	4
a_n	$[x] = \left[\frac{77}{65}\right] = 1$	$\left[\frac{1}{\chi_0}\right] = \left[\frac{65}{12}\right] = 5$	$\left[\frac{1}{\chi_1}\right] = \left[\frac{12}{5}\right] = 2$	$\left[\frac{1}{\chi_2}\right] = \left[\frac{5}{2}\right] = 2$	$\left[\frac{1}{\chi_3}\right] = [2] = 2$
χ_n	$x - a_0 = \frac{12}{65}$	$1/\chi_0 - a_1 = \frac{5}{12}$	$1/\chi_1 - a_2 = \frac{2}{5}$	$1/\chi_2 - a_3 = \frac{1}{2}$	$1/\chi_3 - a_4 = 0$
p_n	$a_0 = 1$	$a_0a_1 + 1 = 6$	$a_2p_1 + p_0 = 13$	$a_3p_2 + p_1 = 32$	$a_4p_3 + p_3 = 77$
q_n	1	$a_1 = 5$	$a_2q_1 + q_0 = 11$	$a_3q_2 + q_1 = 27$	$a_4q_3 + q_2 = 65$

així, fent la fracció contínua de $x = \dfrac{77}{65}$ hem trobat, a la vegada, tots els seus convergents $\dfrac{p_n}{q_n}$, $n = 0, \cdots 4$.

12.1.1 Teorema general dels convergents

El teorema general dels convergents estableix que, donat un nombre racional x i dos enters p i q tals que

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q^2}$$

aleshores $\frac{p}{q}$ és un convergent de la sèrie de la fracció contínua de x.

No demostrarem el teorema, però comprovem que funciona en el mostre exemple, prenent $x = 77/65$. Un dels seus convergents és 13/11

$$\left| \frac{77}{65} - \frac{13}{11} \right| = 0.002797 < \frac{1}{2 \cdot 11^2} = 0.004132$$

12.2 Extracció del període

Acabàvem la part quàntica de l'algorisme de Shor dient:

El problema es concentra ara en com determinar el període r quan es coneix algun

$$l_j = j\frac{2^n}{r} + \Delta_j; \quad |\Delta_j| \leq \frac{1}{2},$$

amb j sencer, o equivalentment

$$\left| l_j - j\frac{2^n}{r} \right| = |\Delta_j| \leq \frac{1}{2},$$

$$\left| \frac{l_j}{2^n} - \frac{j}{r} \right| \leq \frac{1}{2 \cdot 2^n} < \frac{1}{2N^2} < \frac{1}{2r^2}$$

on hem fet ús de que $2^n > N^2$ i que $r < N$. Ara podem aclarir perquè el nombre n de qubits del registre input el varem triar de manera que $2^n > N^2$. El motiu és per poder arribar a l'equació anterior, la qual ens permet assegurar que j/r és un convergent de $l_j/2^n$. Trobar r és ara un procés que es podrà fer amb un ordinador clàssic utilitzant les propietats de les fraccions contínues, els convergents d'un nombre racional i el teorema general dels convergents.

Un cop mesurat l_j, conegut 2^n, el seu quocient $l_j/2^n$ és un nombre racional conegut i, en fer la seva fracció contínua, j/r serà un dels seus convergents. Podrem trobar per tant j i r, el període que cercàvem. A partir d'ell, tal com hem explicat a l'inici d'aquesta secció, podrem trobar quins són els factors del nombre N que volíem factoritzar.

12.3 Exemple complet

Anem a seguir la seqüència de l'algorisme, tal com es descriu a l'inici d'aquesta secció.

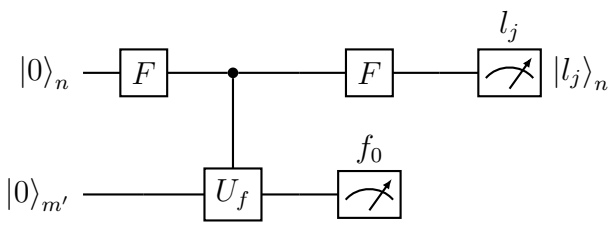
1. Sigui $N = 91$ el nombre que volem factoritzar, usant l'algorisme de Shor.
2. Escollim $y = 3$, que ha de ser coprimer amb $N = 91$. Per això calculem $g.c.d.(91, 3) = 1$. Són coprimers.
3. Implementem la funció $f(x) = y^x \bmod N = 3^x \bmod 91$ en un ordinador quàntic. Per això necessitem un registre input de n qubits, amb el menor n sencer tal que

   $$2^n > N^2; \quad 2^n > 91^2; \quad 2^n > 8281 \Longrightarrow n = 14; \quad 2^{13} = 8192 < 8281 < 2^{14} = 16384$$

   Necessitem també un registre output de m' qubits, amb m' el menor sencer tal que

   $$2^{m'} > N; \quad 2^{m'} > 91 \Longrightarrow m' = 7; \quad 2^6 = 64 < 91 < 2^7 = 128.$$

   Aquesta funció és periòdica i n'hem de trobar el seu període, r. Considerem el circuit



De fet, de moment, més que seguir tota l'evolució pas a pas, recordem que els valors obtinguts per x_0 i $f_0 = f(x_0)$ són irrellevants ja que, quan es mesura l'estat final de l'input es troba algun valor que és

$$l_j = j\frac{2^n}{r} + \Delta_j.$$

Suposem doncs que mesurem l'input i trobem $l_j = 13653$ (després justificarem perquè aquest valor, de moment suposem que tenim un ordinador quàntic i ens l'ha proporcionat). Comprovem que $l_j = 13653$ i $2^n = 16384$ són coprimers, amb l'algorisme d'Euclides, per tant podem aplicar la teoria de les fraccions contínues. Així, podem extreure el valor del període recordant que

$$\left|\frac{l_j}{2^n} - \frac{j}{r}\right| \leq \frac{1}{2r^2},$$

per tant, $\dfrac{j}{r}$ és un dels convergents de la fracció contínua de $\dfrac{l_j}{2^n} = \dfrac{13653}{16384}$. Fem la taula de la fracció contínua de $x = \frac{13653}{16384}$ incloent els convergents i afegim una entrada més que serà el valor de la funció $f(q_n) = 3^{q_n} \bmod 91$ per a cada candidat a ser el període r, és a dir, per cada q_n

n	0	1	2	3	4	5
a_n	$[x] = \left[\frac{13653}{16384}\right] = 0$	$\left[\frac{1}{\chi_0}\right] = \left[\frac{16384}{13653}\right] = 1$	$\left[\frac{1}{\chi_1}\right] = \left[\frac{13653}{2731}\right] = 4$	$\left[\frac{1}{\chi_2}\right] = \left[\frac{2731}{2729}\right] = 1$	$\left[\frac{1}{\chi_3}\right] = \left[\frac{2729}{2}\right] = 1364$	$\left[\frac{1}{\chi_4}\right] = [1] = 1$
χ_n	$x - a_0 = \frac{13653}{16384}$	$1/\chi_0 - a_1 = \frac{2731}{13653}$	$1/\chi_1 - a_2 = \frac{2729}{2731}$	$1/\chi_2 - a_3 = \frac{2}{2729}$	$1/\chi_3 - a_4 = \frac{1}{2}$	$1/\chi_4 - a_5 = 0$
p_n	$a_0 = 0$	$a_0a_1 + 1 = 1$	$a_2p_1 + p_0 = 4$	$a_3p_2 + p_1 = 5$	$a_4p_3 + p_2 = 6824$	$a_5p_4 + p_3 = 13653$
q_n	1	$a_1 = 1$	$a_2q_1 + q_0 = 5$	$a_3q_2 + q_1 = 6$	$a_4q_3 + q_2 = 8189$	$a_5q_4 + q_3 = 16384$
$f(q_n)$	3	3	61	1		

Podem veure que, per $n = 3$, trobem que $f(q_3 = 6) = 3^6 \bmod 91 = 1$, per tant hem trobat el període $r = 6$. De fet, no cal fer tota la sèrie completa per trobar la fracció contínua (tot i que la mostrem a la taula, per comprovar que s'obté correctament): ja tenim el resultat que cercàvem.

4. Hem trobat el període $r = 6$ que és parell.

5. Així podem cercar finalment els factors de $N = 91$, calculant

$$g.c.d(N, y^{r/2} \pm 1) = g.c.d(91, 3^3 \pm 1) = \begin{cases} g.c.d(91, 28) = 7 \\ g.c.d(91, 26) = 13 \end{cases}$$

on tant el 7 com el 13 són factors de 91.

12.4 Anàlisi de l'exemple complet

Anem a veure quins són els valors de l'input més probables de ser mesurats. Sabem que són aquells que

$$l_j = j\frac{2^n}{r} + \Delta_j; \quad |\Delta_j| \leq \frac{1}{2},$$

amb j sencer. Ara sabem que

$$n = 14; 2^n = 2^{14} = 16384; r = 6; m \geq 2^n/r = 2730,667 \longrightarrow m = 2731,$$

i que la probabilitat d'un valor l_j val

$$p(l_j) = \frac{1}{2^n m} \frac{\sin^2\left(\frac{\pi}{2^n} r\Delta_j m\right)}{\sin^2\left(\frac{\pi}{2^n} r\Delta_j\right)} \equiv p(\Delta_j),$$

podem trobar tots els valors amb probabilitat més alta (compte, cal posar els angles en radians a l'hora d'avaluar les funcions sinus):

j	0	1	2	3	4	5
l_j	0	2731	5461	8192	10923	13653
Δ_j	0	-1/3	1/3	0	-1/3	1/3
$p(l_j)$	0,166	0,114	0,114	0,166	0,114	0,114

Si prenem un valor lleugerament diferent a algun d'ells, per exemple $l_j = 13652$, trobarem

$$p(13652) = p(\Delta = 4/3) = 0,0071$$

que és molt més baixa que els valors de la taula.

Veiem que el valor 13653, que hem usat a l'exemple, és un dels valors possibles amb $\Delta_j = 1/3 < 1/2$ i, per tant, té una probabilitat alta de ser mesurat i se'n pot inferir el període r gràcies al teorema general dels convergents.

Per últim, la probabilitat *a priori* de mesurar algun valor útil, és a dir, algun dels que apareixen a la taula anterior, tret del zero, satisfà la cota teòrica del 40%

$$p(l_{\text{algun valor útil}}) = 1 \cdot 0,166 + 4 \cdot 0,114 = 0,572 > 0,4.$$

Què hagués passat si la mesura hagués donat algun valor no-útil? Doncs que no hauríem trobat el període i hauríem de tornar a córrer l'algorisme des del punt 3, que conté tota la part quàntica.

12.5 Consideracions addicionals

- Pot donar-se el cas que j i r no siguin coprimers, tinguin per tant algun factor en comú, aleshores el convergent $\frac{j}{r}$ no donaria r, sinó que r en seria un múltiple.
- Què passa si $\frac{l_j}{2^n}$ no són coprimers?
- La TFQ és un operador unitari.
- Com s'implementa la transformada de Fourier quàntica?

12.5.1 La Transformada de Fourier Quàntica és un operador unitari

L'operador que implementa la transformada de Fourier Quàntica es pot expressar en la notació de kets i bras de la manera següent (simplifiquem la notació ometent el subíndex n als bras i kets,

denotant, per exemple, $|x\rangle_n \equiv |x\rangle$)

$$F = \frac{1}{2^{n/2}} \sum_{y,y'=0}^{2^n-1} e^{i\frac{2\pi}{2^n}yy'} |y\rangle \langle y'|$$

Comprovem que actua correctament sobre un ket de n qubits

$$F|x\rangle = \frac{1}{2^{n/2}} \sum_{y,y'=0}^{2^n-1} e^{i\frac{2\pi}{2^n}yy'} |y\rangle \langle y'|x\rangle = \frac{1}{2^{n/2}} \sum_{y,y'=0}^{2^n-1} e^{i\frac{2\pi}{2^n}yy'} |y\rangle \delta_{xy'} = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{i\frac{2\pi}{2^n}yx} |y\rangle$$

que, efectivament, dona el resultat correcte.

El seu hermític conjugat (transposat i complex conjugat) és

$$F^\dagger = \frac{1}{2^{n/2}} \sum_{y,y'=0}^{2^n-1} e^{-i\frac{2\pi}{2^n}yy'} |y'\rangle \langle y|$$

Hem de comprovar, per ser unitari, que $F^\dagger F = \mathbb{1}$.

$$\begin{aligned}
F^\dagger F &= \frac{1}{2^n} \sum_{z,z'=0}^{2^n-1} e^{-i\frac{2\pi}{2^n}zz'} |z'\rangle \langle z| \sum_{y,y'=0}^{2^n-1} e^{i\frac{2\pi}{2^n}yy'} |y\rangle \langle y'| \\
&= \frac{1}{2^n} \sum_{z,z'=0}^{2^n-1} \sum_{y,y'=0}^{2^n-1} e^{i\frac{2\pi}{2^n}(yy'-zz')} |z'\rangle \langle z|y\rangle \langle y'| \\
&= \frac{1}{2^n} \sum_{z,z',y,y'=0}^{2^n-1} e^{i\frac{2\pi}{2^n}(yy'-zz')} |z'\rangle \langle y'| \delta_{zy} \\
&= \sum_{z',y'=0}^{2^n-1} \left(\frac{1}{2^n} \sum_{y=0}^{2^n-1} e^{i\frac{2\pi}{2^n}y(y'-z')} \right) |z'\rangle \langle y'| \\
&= \sum_{z'y'=0}^{2^n-1} |z'\rangle \langle y'| \delta_{y'z'} \\
&= \sum_{z'=0}^{2^n-1} |z'\rangle \langle z'| = \mathbb{1}
\end{aligned}$$

La darrera igualtat es verifica, doncs si l'apliquem a un estat $|x\rangle$ retrobem el mateix estat:

$$\sum_{z'=0}^{2^n-1} |z'\rangle \langle z'|x\rangle = \sum_{z'=0}^{2^n-1} |z'\rangle \delta_{z',x} = |x\rangle .$$

Queda només justificar el pas intermedi

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

Per $y' = z'$, la suma és clarament 1, doncs cada un dels 2^n sumands val 1. Per avaluar la suma quan $y' \neq z'$, és suficient adonar-se que el sumatori és el d'una sèrie geomètrica de raó $R = e^{i\frac{2\pi}{2^n}(y'-z')}$, amb el primer terme $a_0 = 1$ i el darrer $a_{2^n-1} = e^{i\frac{2\pi}{2^n}(y'-z')(2^n-1)}$. La suma és

$$S = a_0 \frac{1-R^{2^n}}{1-R} = \frac{1-e^{i2\pi(y'-z')}}{1-e^{i\frac{2\pi}{2^n}(y'-z')}} = 0$$

on el numerador és zero ja que y' i z' són nombres enters i, per tant, $e^{i2\pi(y'-z')}=1$.

Una expressió alternativa a la transformada de Fourier Quàntica és la matricial. Per n qubits, serà una matriu $2^n\times 2^n$ que la podem construir recordant com actua sobre cada un dels 2^n estats de la base, $\{|0\rangle,|1\rangle,\cdots,|2^n-1\rangle\}$

$$F_n\,|x\rangle_n=\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}e^{i\frac{2\pi}{2^n}xy}\,|y\rangle_n$$

Així,

$$F_n\,|0\rangle_n=\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}|y\rangle_n\,;\quad F_n\begin{pmatrix}1\\0\\0\\\vdots\\0\end{pmatrix}=\frac{1}{2^{n/2}}\begin{pmatrix}1\\1\\1\\\vdots\\1\end{pmatrix}$$

$$F_n\,|1\rangle_n=\frac{1}{2^{n/2}}\sum_{y=0}^{2^n-1}e^{i\frac{2\pi}{2^n}y}\,|y\rangle_n\,;\quad F_n\begin{pmatrix}0\\1\\0\\\vdots\\0\end{pmatrix}=\frac{1}{2^{n/2}}\begin{pmatrix}1\\\omega\\\omega^2\\\vdots\\\omega^{2^n-1}\end{pmatrix}$$

on hem introduït la notació $\omega=e^{i\frac{2\pi}{2^n}}$ Així, és fàcil convèncer-se que

$$F_n=\frac{1}{2^{n/2}}\begin{pmatrix}1&1&1&\cdots&1\\1&\omega&\omega^2&\cdots&\omega^{2^n-1}\\1&\omega^2&\omega^4&\cdots&\omega^{2(2^n-1)}\\\vdots&\vdots&\vdots&&\vdots\\1&\omega^{2^n-1}&\omega^{2(2^n-1)}&\cdots&\omega^{(2^n-1)(2^n-1)}\end{pmatrix}$$

Per exemple, per $n=2$, $\omega=e^{i\frac{2\pi}{2^n}}=i$, i la matriu F_2 és

$$F_2=\tfrac{1}{2}\begin{pmatrix}1&1&1&1\\1&i&-1&-i\\1&-1&1&-1\\1&-i&-1&i\end{pmatrix}$$

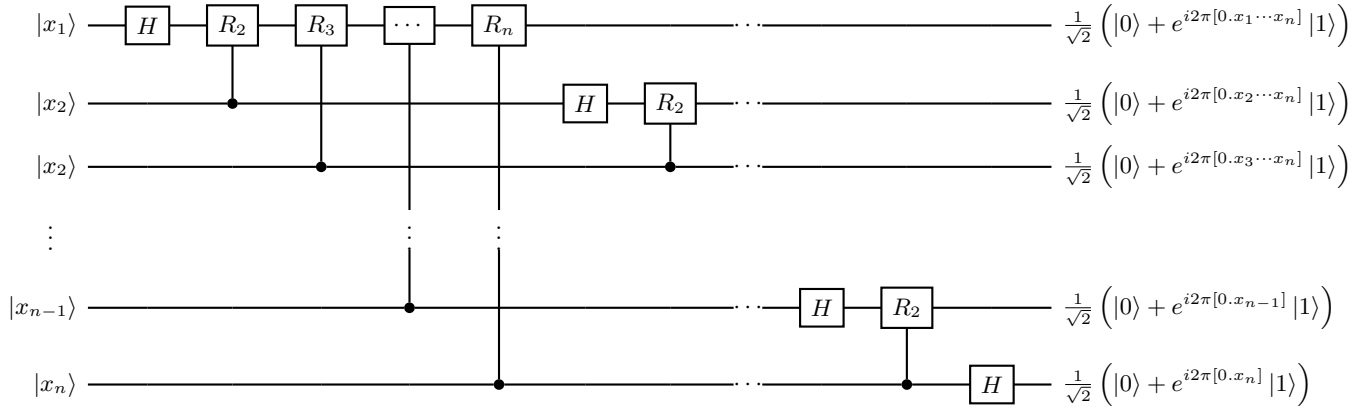
12.5.2 Implementació de la Transformada de Fourier Quàntica

Aquesta part està extreta i adaptada de la Wikipedia.

Anem a veure que la Transformada de Fourier Quàntica es pot implementar només amb portes Hadamard, d'un qubit, i portes control phase shfit de dos qubits, amb diferents valors dels phase shifts, que per alleugerir la notació les anomenarem R_m:

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix};\qquad R_m=\begin{pmatrix}1&0\\0&e^{i\frac{2\pi}{2^m}}\end{pmatrix}.$$

Fixem-nos que R_m és l'arrel 2^m de la identitat, ja que $R_m^{2^m} = \mathbb{1}$, amb m sencer positiu. El circuit quàntic que l'implementa és



Veiem que el circuit calcula la transformada de Fourier quàntica. Usem notació binària, definint

$$x = x_1 2^{n-1} + x_2 2^{n-2} + \cdots + x_n 2^0$$

i utilitzant $\omega = e^{i\frac{2\pi}{2^n}}$

Notació fraccional binària:

$$[0.x_1 x_2 \cdots x_m] = \sum_{k=1}^{m} x_k 2^{-k}$$

Per exemple

$$[0.x_1] = \frac{x_1}{2}; \quad [0.x_1 x_2] = \frac{x_1}{2} + \frac{x_2}{2^2}$$

$$\begin{aligned}
F_n |x\rangle_n &= \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} \omega^{xy} |y\rangle_n = \frac{1}{2^{n/2}} \sum_{y_1\in\{0,1\}} \sum_{y_2\in\{0,1\}} \cdots \sum_{y_n\in\{0,1\}} \omega^{x\sum_{j=1}^n y_j 2^{n-j}} |y_1 y_2 \cdots y_n\rangle \\
&= \frac{1}{2^{n/2}} \sum_{y_1\in\{0,1\}} \sum_{y_2\in\{0,1\}} \cdots \sum_{y_n\in\{0,1\}} \bigotimes_{j=1}^{n} \omega^{xy_j 2^{n-j}} |y_j\rangle \\
&= \frac{1}{2^{n/2}} \sum_{y_1\in\{0,1\}} \sum_{y_2\in\{0,1\}} \cdots \sum_{y_n\in\{0,1\}} \omega^{xy_1 2^{n-j}} |y_1\rangle \otimes \bigotimes_{j=2}^{n} \omega^{xy_j 2^{n-j}} |y_j\rangle \\
&= \frac{1}{2^{n/2}} \left(\sum_{y_1\in\{0,1\}} \omega^{xy_1 2^{n-1}} |y_1\rangle \right) \otimes \sum_{y_2\in\{0,1\}} \cdots \sum_{y_n\in\{0,1\}} \omega^{xy_j 2^{n-2}} |y_2\rangle \otimes \bigotimes_{j=3}^{n} \omega^{xy_j 2^{n-j}} |y_j\rangle \\
&= \frac{1}{2^{n/2}} \left(\sum_{y_1\in\{0,1\}} \omega^{xy_1 2^{n-1}} |y_1\rangle \right) \otimes \left(\sum_{y_2\in\{0,1\}} \omega^{xy_2 2^{n-2}} |y_2\rangle \right) \otimes \sum_{y_3\in\{0,1\}} \\
&\quad \cdots \sum_{y_n\in\{0,1\}} \omega^{xy_3 2^{n-3}} |y_3\rangle \otimes \bigotimes_{j=4}^{n} \omega^{xy_j 2^{n-j}} |y_j\rangle \\
&= \frac{1}{2^{n/2}} \bigotimes_{j=1}^{n} \sum_{y_j\in\{0,1\}} \omega^{xy_j 2^{n-j}} |y_j\rangle = \frac{1}{2^{n/2}} \bigotimes_{j=1}^{n} \left(|0\rangle + \omega^{x2^{n-j}} |1\rangle \right) \\
&= \frac{1}{2^{n/2}} \left(|0\rangle + e^{i2\pi[0.x_n]} |1\rangle \right) \otimes \left(|0\rangle + e^{i2\pi[0.x_{n-1}x_n]} |1\rangle \right) \otimes \cdots \otimes \left(|0\rangle + e^{i2\pi[0.x_1 x_2 \cdots x_n]} |1\rangle \right)
\end{aligned}$$

El darrer pas es justifica

$$\omega^{x2^{n-j}} = e^{\frac{i2\pi}{2^n}x2^{n-j}} = e^{i2\pi(x2^{-j})}$$

Sigui

$$f(j) = x2^{-j} = 2^{-j}\sum_{r=1}^{n} x_r 2^{n-r} = \sum_{r=1}^{n} x_r 2^{n-r-j} = \sum_{r=1}^{n-j} x_r 2^{n-r-j} + \sum_{r=n-j+1}^{n} x_r 2^{n-r-j} = a(j) + b(j)$$

El terme $a(j)$ és un nombre natural (sencer no negatiu) perquè $2^{n-r-j} \geq 0$ per $n-r-j \geq 0$. En canvi, $b(j) = [0.x_{n-j+1}x_{n-j+2}\cdots x_n]$. Així

$$\omega^{x2^{n-j}} = e^{i2\pi(x2^{-j})} = e^{i2\pi f(j)} = e^{i2\pi(a(j)+b(j))} = e^{i2\pi a(j)} \cdot e^{i2\pi b(j)} = e^{i2\pi[0.x_{n-j+1}x_{n-j+2}\cdots x_n]},$$

ja que $e^{i2\pi a(j)} = 1$ i $e^{i2\pi b(j)} = e^{i2\pi[0.x_{n-j+1}x_{n-j+2}\cdots x_n]}$. Recopilant

$$\begin{aligned} F_n \left|x_1x_2\cdots x_n\right\rangle &= \frac{1}{2^{n/2}}\bigotimes_{j=1}^{n}\left(\left|0\right\rangle + \omega^{x2^{n-j}}\left|1\right\rangle\right) \\ &= \frac{1}{2^{n/2}}\left(\left|0\right\rangle + e^{i2\pi[0.x_n]}\left|1\right\rangle\right)\otimes\left(\left|0\right\rangle + e^{i2\pi[0.x_{n-1}x_n]}\left|1\right\rangle\right)\otimes\cdots\otimes\left(\left|0\right\rangle + e^{i2\pi[0.x_1x_2\cdots x_n]}\left|1\right\rangle\right). \end{aligned}$$

Si ens fixem, el circuit proposat dona aquest resultat en l'ordre invers. Poden aplicar-se operacions swap. Es necessiten com a màxim $n/2$ portes swap (essent cada una d'elles tres portes CNOT). L'altra solució és llegir l'output en sentit invers.

La transformada de Fourier quàntica sobre n qubits factoritza en el producte tensorial de n operacions sobre qubits individuals. Si no considerem la reordenació del resultat, cada una d'elles es pot implementar usant una Hadamard i portes phase shift controlades. El primer qubit necessita una Hadamard i $(n-1)$ control phase shifts. El segon, una Hadamard i $(n-2)$ control phase shifts; el següent una control phase shift menys, etc. Si es sumen totes les portes que es necessiten (excepte la reordenació final) es troba $n + (n-1) + \cdots + 1 = n(n+1)/2 = O(n^2)$ portes, que és quadràtic en el nombre de qubits.