Butlletí de la Societat Catalana de Matemàtiques
Vol. 28, núm. 2, 2013. Pàg. 183–231. DOI: 10.2436/20.2002.01.51

Introducció matemàtica a la computació quàntica

Juanjo Rué i Sebastià Xambó

Resum: El propòsit d'aquest article és exposar les nocions essencials de la computació quàntica en termes purament matemàtics. En particular, definim les nocions de q-computació, q-mesura, q-procediment, q-computador i q-algorisme, i cadascuna s'il·lustra amb diversos exemples. A més d'alguns q-algorismes de baix nivell, discutim en detall una bona mostra dels més rellevants que s'han descobert. Aquests inclouen un q-algorisme per a la transformada de Fourier discreta i els q-algorismes de Deutsch (que resol un problema de decisió per a certes funcions booleanes), de Grover (cerca en una base de dades), de Kitaev (per estimar la fase d'un valor propi d'un vector propi d'un operador unitari), i els celebrats q-algorismes de Shor (per trobar l'ordre multiplicatiu d'un enter mòdul un altre i per factoritzar nombres enters). Les possibles realitzacions físiques del model, i el seu ús potencial per a obtenir guanys respecte de la computació clàssica (en ocasions fins i tot guanys exponencials), s'analitzen en termes d'una formulació axiomàtica de la teoria quàntica per a espais hermítics de dimensió finita.

Paraules clau: computació quàntica, algorísmica, factorització de nombres enters.

Classificació MSC2010: 68Q12, 81P15, 81P68, 15A23.

Contingut

Una versió prèvia d'aquest article, en anglès i amb el títol «Mathematical essentials of quantum computing», es pot trobar a la pàgina web del segon autor, a l'adreça `http://www-ma2.upc.es/sxd/QC/qc.pdf`.

Introducció

El substrat matemàtic del «processament quàntic», que aquí en diem q-processament, serà presentat com un canvi de llenguatge en parlar de certes nocions matemàtiques, i molt prominentment de nocions d'àlgebra lineal complexa (sobre els nombres complexos) i de teoria elemental de probabilitats. El nostre propòsit és cobrir des dels conceptes més bàsics fins a l'expressió i anàlisi d'una bona mostra dels remarcables q-algorismes descoberts en els darrers vint-i-cinc anys.

Encara que del contingut físic no se'n parla fins a la secció 9, la significació física de la presentació serà manifesta per als físics, mentre que els matemàtics hi trobaran, si s'escau, una base per a apreciar més fàcilment algunes de les idees físiques de fons.

En els primers estadis, la raó més visible per a la robustesa del paradigma, i també per al seu interès, rau en l'estreta relació amb la cara matemàtica de la computació clàssica, és a dir, l'àlgebra de Boole. L'arrel d'aquesta relació és el fet que el terreny del q-processament és l'espai vectorial complex $\boldsymbol{H}^{(n)}$ generat pel conjunt $\boldsymbol{B}^n$ dels vectors binaris de longitud n, que és el marc en el qual es produeix la computació clàssica.

Posteriorment, quan la q de q-processament s'interpreta com una característica quàntica genuïna, l'esquema s'interpreta com un model matemàtic de fenòmens físics interessants que s'estan explorant intensament en laboratoris d'arreu del món. Amb un flux creixent de resultats publicats a revistes del més alt impacte, tot apunta a un ampli ventall de possibilitats científiques i tecnològiques per als anys a venir.

Si la computació amb bits clàssics s'ha manifestat com el que anomenem era digital (basada en la teoria de la computació de Turing, la teoria de la informació de Shannon i en els desenvolupaments teòrics, científics i tecnològics a què donaren lloc), pot tenir interès reflexionar que el desenvolupament del q-processament, fabulosament més ampli, possiblement serà tant o més extraordinari i sens dubte no menys interessant.

1 Preliminars

Comencem establint diversos símbols i convencions que usarem d'ara endavant.

- n, un nombre enter positiu. Diem que n és el *nombre de q-bits*.
- $j, k, \ldots$ nombres enters positius de l'interval $0, \ldots, 2^n - 1$.
- $j = j_1 j_2 \cdots j_n$, l'expressió binària de j (i anàlogament per a k). En altres paraules,

$$j_1, \ldots, j_n \in \{0,1\} \quad \text{i} \quad j = j_1 2^{n-1} + j_2 2^{n-2} + \cdots + j_{n-1} 2 + j_n 2^0.$$

Vectors binaris. Sigui $\boldsymbol{B} = \{0,1\}$, que és el conjunt de *dígits binaris* (*bits*). Llavors el conjunt dels vectors binaris de longitud n és $\boldsymbol{B}^n$. Els seus elements

s'escriuen usualment com a cadenes de bits. Per exemple,

$$\boldsymbol{B}^3 = \{000, 001, 010, 011, 100, 101, 110, 111\}.$$

Les cadenes constants $0 \overset{n)}{\cdots} 0$ i $1 \overset{n)}{\cdots} 1$ seran denotades per $\mathbf{0}_n$ i $\mathbf{1}_n$, respectivament.

La representació binària dels nombres enters ens permet *identificar els vectors binaris de longitud n amb els nombres enters de l'interval* $0, \ldots, 2^n - 1$:

$$j \leftrightarrow j_1 j_2 \cdots j_n.$$

Com que la informació (clàssica) es pot representar per elements de $\boldsymbol{B}^n$, per a algun n,[1] els conjunts $\boldsymbol{B}^n$ són el terreny en el qual tenen lloc les computacions clàssiques. De fet, una *computació clàssica* es pot entendre com una aplicació $f\colon \boldsymbol{B}^n \to \boldsymbol{B}^m$. Si aquesta aplicació és bijectiva (cosa que comporta $m = n$), es diu que la computació és *reversible*. Com que tota computació clàssica es pot incrustar en una computació reversible ($\triangleright$ **1**),[2] sempre suposarem que les computacions clàssiques són reversibles llevat que diguem explícitament el contrari. Adonem-nos que el nombre de computacions $B^n \to B^m$ és $(2^m)^{2^n}$ i que el nombre de computacions reversibles de n bits és $(2^n)!$.

q-vectors. Escrivim $\boldsymbol{H}^{(n)} = \mathbb{C}^{2^n}$ ($\mathbb{C}$ el cos dels nombres complexos), i diem que és l'espai dels *q-vectors d'ordre n*. Com veurem a la secció 3, els espais $\boldsymbol{H}^{(n)}$ són l'àmbit en el qual tenen lloc els q-procediments, d'una manera anàloga a com els conjunts $\boldsymbol{B}^n$ són l'àmbit en el qual tenen lloc les computacions clàssiques. En notació matemàtica usual, els elements $\boldsymbol{a} \in \boldsymbol{H}^{(n)}$ es presenten com vectors columna (amb components complexos) de *dimensió* (o *longitud*) 2^n:

$$\boldsymbol{a} = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{2^n-1} \end{bmatrix}, \quad a_j \in \mathbb{C}.$$

El q-vector $\boldsymbol{a}$ es pot escriure en la forma

$$\boldsymbol{a} = a_0 \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + a_{2^n-1} \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}.$$

1 Un text és una cadena de caràcters d'un determinat alfabet, i els caràcters es poden convertir en una cadena de bits mitjançant una codificació apropiada, com ara la utf-8. Una imatge es pot entendre com una cadena de píxels (diguem N), cada píxel es pot representar com una combinació de tres coloracions (vermell, verd i blau), i cada coloració es pot representar per l bits si el nombre de nivells considerats és 2^l. Un so es pot considerar com una cadena de N valors de pressió, i aquests valors es poden representar per l bits si el nombre de nivells de pressió considerats és 2^l. Així, doncs, texts, imatges i sons es poden representar mitjançant cadenes de bits (diem que es poden *digitalitzar*). En el cas d'imatges i sons, la digitalització és només una aproximació, però es poden escollir N i l de manera que la diferència amb el senyal real sigui imperceptible a la vista i l'oïda, respectivament.

2 $\triangleright n$ fa referència a la nota número n de la secció 10 (Remarques i demostracions), p. 224.

En forma comprimida, $\boldsymbol{a} = \sum_j a_j \boldsymbol{u}_j$, on $\boldsymbol{u}_j$ és el q-vector que té un 1 a la posició j i zeros en la resta de posicions.

Notació de Dirac. Consisteix a escriure $|j\rangle$ en lloc de $\boldsymbol{u}_j$. Així, doncs, $\boldsymbol{a} = \sum_j a_j|j\rangle$. Si considerem j com a un vector binari de longitud n, veiem que $\boldsymbol{H}^{(n)}$ és l'espai vectorial complex amb base $\boldsymbol{B}^n$.

EXEMPLE 1.1 ($n = 1$: Un q-bit).

$$\boldsymbol{a} = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = a_0|0\rangle + a_1|1\rangle = a_0 \begin{bmatrix} 1 \\ 0 \end{bmatrix} + a_1 \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

EXEMPLE 1.2 ($n = 2$: Dos q-bits).

$$\begin{aligned} \boldsymbol{a} &= a_0|0\rangle + a_1|1\rangle + a_2|2\rangle + a_3|3\rangle \\ &= a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \\ &= \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} a_{00} \\ a_{01} \\ a_{10} \\ a_{11} \end{bmatrix} = a_{00} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + a_{01} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + a_{10} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + a_{11} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \end{aligned}$$

Adonem-nos que el 0 de $|0\rangle$ és un enter, mentre que els de $|00\rangle$ són bits. Aquest abús de notació és acceptable, ja que el context ens permet inferir de quin ús es tracta. Fixem-nos també que $|1\rangle$ (1 enter) i $|01\rangle$ (0 i 1 bits) designen el mateix vector, i que és obligat escriure el bit 0 a l'esquerra.

EXEMPLE 1.3 (q-vector d'Hadamard d'ordre n). El *q-vector d'Hadamard d'ordre n* es defineix com

$$\boldsymbol{h}^{(n)} = \rho^n(|0\rangle + |1\rangle + \cdots + |2^n - 1\rangle),$$

on $\rho = 1/\sqrt{2}$ (usarem aquesta notació en tot l'article).

Aplicacions lineals. Recordem que una *apliació $\mathbb{C}$-lineal* $T\colon \boldsymbol{H}^{(n)} \to \boldsymbol{H}^{(n)}$ (també en diem un *operador*) queda determinada per les 2^n imatges $\boldsymbol{t}_j = T|j\rangle$, ja que

$$T\left(\sum_j a_j|j\rangle\right) = \sum_j a_j T(|j\rangle) = \sum_j a_j \boldsymbol{t}_j.$$

A més, donat un conjunt de q-vectors $\{\boldsymbol{t}_j\}_{0\le j<2^n}$, existeix una única aplicació lineal $T\colon \boldsymbol{H}^{(n)} \to \boldsymbol{H}^{(n)}$ que compleix $T|j\rangle = \boldsymbol{t}_j$. Aquesta observació serà el mètode bàsic que usarem per definir operadors. Les propietats de T usualment es poden inferir de propietats dels vectors $\boldsymbol{t}_j$. Per exemple, l'aplicació T és bijectiva si i només si els vectors $\boldsymbol{t}_j$ són linealment independents.

Producte escalar i norma. Si $\boldsymbol{a}$ i $\boldsymbol{b}$ són q-vectors, el *producte escalar* de $\boldsymbol{a}$ i $\boldsymbol{b}$, $\langle \boldsymbol{a} | \boldsymbol{b} \rangle$, es defineix per la fórmula

$$\langle \boldsymbol{a} | \boldsymbol{b} \rangle = \sum_j \bar{a}_j b_j.$$

El producte escalar és lineal en $\boldsymbol{b}$ i lineal conjugat en $\boldsymbol{a}$. Si $\langle \boldsymbol{a} | \boldsymbol{b} \rangle = 0$, diem que $\boldsymbol{a}$ i $\boldsymbol{b}$ són *ortogonals*. Observem que $\langle \boldsymbol{a} | \boldsymbol{a} \rangle = |\boldsymbol{a}|^2$, on

$$|\boldsymbol{a}|^2 = |a_0|^2 + |a_1|^2 + \cdots + |a_{2^n-1}|^2$$

(la *norma* del vector $\boldsymbol{a}$ al quadrat). Si $|\boldsymbol{a}| = 1$, diem que $\boldsymbol{a}$ és un *vector unitari*. Donat un q-vector no nul $\boldsymbol{x}$, $\boldsymbol{x}/|\boldsymbol{x}|$ és un q-vector unitari que denotem per $\hat{\boldsymbol{x}}$ o $\boldsymbol{u}(\boldsymbol{x})$.

Per exemple, $\langle \boldsymbol{u}_j | \boldsymbol{u}_k \rangle = \delta_{jk}$ (o $\langle j | k \rangle = \delta_{jk}$ en la notació de Dirac). Això significa que els $\boldsymbol{u}_j$ són vectors unitaris ortogonals dos a dos, propietat que expressem dient que els vectors $\{\boldsymbol{u}_j\}$ formen una base *ortonormal*.

Producte tensorial. El *producte tensorial* dels vectors $\boldsymbol{a} \in \boldsymbol{H}^{(n)}$ i $\boldsymbol{a}' \in \boldsymbol{H}^{(n')}$, que denotem per $\boldsymbol{a} \hat{\otimes} \boldsymbol{a}'$, és el vector de $\boldsymbol{H}^{(n+n')}$ les components del qual són $a_j a'_{j'}$, amb (j, j') ordenats lexicogràficament.

Per exemple,

$$\begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \hat{\otimes} \begin{bmatrix} a'_0 \\ a'_1 \end{bmatrix} = \begin{bmatrix} a_0 a'_0 \\ a_0 a'_1 \\ a_1 a'_0 \\ a_1 a'_1 \end{bmatrix}.$$

PROPOSICIÓ 1.4. *Si* $\boldsymbol{a} = \sum_j a_j |j\rangle$ *i* $\boldsymbol{a}' = \sum_{j'} a'_{j'} |j'\rangle$, *llavors*

$$\boldsymbol{a} \hat{\otimes} \boldsymbol{a}' = \sum_{j,j'} a_j a'_{j'} |j \cdot 2^{n'} + j'\rangle.$$

PROVA. L'índex $j \in \{0, \ldots, 2^n - 1\}$ del component a_j del vector $\boldsymbol{a}$ és el nombre de components que el precedeixen (aquests components són $a_0, a_1, \ldots, a_{j-1}$). Si apliquem aquesta observació al component $a_j a'_{j'}$ de l'element $\boldsymbol{a} \hat{\otimes} \boldsymbol{a}'$, efectivament trobem que el nombre de components que el precedeixen és $j' + j \cdot 2^{n'}$. □

Fixem-nos que si j i j' són nombres binaris, llavors $j \cdot 2^{n'} + j'$ és el nombre binari obtingut concatenant les representacions binàries de j i j'. En la pràctica aquest nombre s'escriu simplement jj', de manera que obtenim la relació

$$\boldsymbol{a} \hat{\otimes} \boldsymbol{a}' = \sum_{j,j'} a_j a'_{j'} |jj'\rangle.$$

El producte tensorial $|j\rangle \hat{\otimes} |j'\rangle$ també es denota $|j\rangle|j'\rangle$, de manera que tenim

$$|j\rangle \hat{\otimes} |j'\rangle = |j\rangle|j'\rangle = |jj'\rangle.$$

En particular podem escriure

$$|j_1\rangle \hat{\otimes} |j_2\rangle \hat{\otimes} \cdots \hat{\otimes} |j_n\rangle = |j_1\rangle|j_2\rangle \cdots |j_n\rangle = |j_1 j_2 \cdots j_n\rangle.$$

EXEMPLE 1.5. Sigui $\boldsymbol{h}^{(n)}$ el q-vector d'Hadamard d'ordre n (vegeu l'exemple 1.3). Aleshores,

$$\boldsymbol{h}^{(n)} = \rho^n(|0\rangle + |1\rangle)\hat{\otimes}(l|0\rangle + |1\rangle)\hat{\otimes}\cdots\hat{\otimes}(|0\rangle + |1\rangle).$$

De fet, l'expressió del segon membre de la igualtat és igual a

$$\rho^n \sum_{j_1,\ldots,j_n\in\boldsymbol{B}} |j_1\rangle\cdots|j_n\rangle = \rho^n \sum_{j\in\boldsymbol{B}^n} |j\rangle = \boldsymbol{h}^{(n)}.$$

REMARCA 1.6. L'aplicació $\boldsymbol{H}^{(n)}\times\boldsymbol{H}^{(n')}\to\boldsymbol{H}^{(n+n')}$, $(\boldsymbol{a},\boldsymbol{a}')\mapsto\boldsymbol{a}\hat{\otimes}\boldsymbol{a}'$ és bilineal i, per tant, indueix una aplicació lineal

$$\boldsymbol{H}^{(n)}\otimes\boldsymbol{H}^{(n')}\to\boldsymbol{H}^{(n+n')},\quad \boldsymbol{a}\otimes\boldsymbol{a}'\mapsto\boldsymbol{a}\hat{\otimes}\boldsymbol{a}'.$$

Aquesta aplicació és un isomorfisme, ja que transforma la base $\{|j\rangle|j'\rangle\}_{j,j'}$ del primer espai en la base $\{|jj'\rangle\}_{j,j'}$ del segon. En particular, tenim un isomorfisme

$$\boldsymbol{H}^{(n)}\simeq\boldsymbol{H}^{(1)}\otimes\overset{n)}{\cdots}\otimes\boldsymbol{H}^{(1)}.$$

Podem, doncs, identificar $\boldsymbol{a}\otimes\boldsymbol{a}'$ i $\boldsymbol{a}\hat{\otimes}\boldsymbol{a}'$, de manera que en el que segueix només emprarem el símbol $\otimes$.

Com veurem a la secció 9, l'isomorfisme anterior estableix que els vectors no nuls de $\boldsymbol{H}^{(n)}$ representen estats quàntics d'un sistema format per n partícules d'espín $1/2$ (com ara electrons o protons). Aquí pot resultar escaient, per als qui desconeguin l'axiomàtica de la física quàntica, prendre un primer contacte amb les subseccions 1 i 4 de la secció 9.

REMARCA 1.7. D'un q-vector d'ordre n de la forma $\boldsymbol{a}_1\otimes\cdots\otimes\boldsymbol{a}_n$, $\boldsymbol{a}_l\in\boldsymbol{H}^{(1)}$, diem que és *descomponible*. Els vectors de la base $|j_1j_2\cdots j_n\rangle = |j_1\rangle|j_2\rangle\cdots|j_n\rangle$ són exemples de q-vectors descomponibles. Però, en general, els q-vectors no són descomponibles. És fàcil comprovar, per exemple, que $|00\rangle+|11\rangle\in\boldsymbol{H}^{(2)}$ no es pot escriure com un producte $(a_0|0\rangle+a_1|1\rangle)(b_0|0\rangle+b_1|1\rangle)$. Usant una terminologia originada en la física (vegeu la p. 220), dels q-vectors descomponibles (no descomponibles) també en diem q-vectors *compostos* (*entrellaçats*).

2 q-computacions

Si $U=[u_{jk}]$ és una matriu, la seva *transposada* és $U^T=[u_{kj}]$ i la seva *adjunta*,

$$U^\dagger=[\bar{u}_{kj}]=\overline{U^T}.$$

Una *q-computació d'ordre n* és una *matriu unitària* U de dimensió 2^n. Això significa que

$$U=[u_{jk}]_{0\le j,k<2^n},\quad u_{jk}\in\mathbb{C}\quad\text{i}\quad UU^\dagger=I_{2^n},$$

on I_{2^n} denota la matriu identitat de dimensió 2^n.

El conjunt de les matrius unitàries de dimensió 2^n, $\boldsymbol{U}(2^n)$, serà denotat per $\boldsymbol{U}^{(n)}$. Amb el producte ordinari de matrius, $\boldsymbol{U}^{(n)}$ és un grup. En detall, això significa el següent:

- (*Identitat*) $I_{2^n} \in \boldsymbol{U}^{(n)}$. En altres paraules, la matriu identitat de dimensió 2^n és una q-computació d'ordre n.
- (*Composició*) Si $U, V \in \boldsymbol{U}^{(n)}$, llavors $VU \in \boldsymbol{U}^{(n)}$. Així, doncs, la composició de dues q-computacions d'ordre n és una q-computació d'ordre n.
- (*Reversibilitat*) Si $U \in \boldsymbol{U}^{(n)}$, aleshores $U^{-1} \in \boldsymbol{U}^{(n)}$ (adonem-nos que $U^{-1} = U^\dagger$). La inversa d'una q-computació d'ordre n és una q-computació d'ordre n.

Si $\boldsymbol{a} \in \boldsymbol{H}^{(n)}$ és un vector unitari i U una q-computació, llavors $\boldsymbol{b} = U\boldsymbol{a}$ és també un vector unitari. Com en el cas de les computacions clàssiques, diem que $\boldsymbol{b}$ és el *q-output* de U amb *q-input* $\boldsymbol{a}$.

EXEMPLE 2.1. Si $U \in \boldsymbol{U}^{(n)}$ i $U' \in \boldsymbol{U}^{(n')}$, considerem l'aplicació lineal

$$U \otimes U' \colon \boldsymbol{H}^{(n+n')} \to \boldsymbol{H}^{(n+n')}$$

tal que $|jj'\rangle = |j\rangle|j'\rangle \mapsto U|j\rangle\, U'|j'\rangle$. És fàcil comprovar que $U \otimes U' \in \boldsymbol{U}^{(n+n')}$ i que de fet es compleix la relació $|\boldsymbol{a}\rangle|\boldsymbol{a}'\rangle \mapsto U|\boldsymbol{a}\rangle\, U'|\boldsymbol{a}'\rangle$ qualssevol que siguin $\boldsymbol{a} \in \boldsymbol{H}^{(n)}$ i $\boldsymbol{a}' \in \boldsymbol{H}^{(n')}$.

Similarment, si $U \in \boldsymbol{U}^{(1)}$, podem definir $U^{\otimes n} \in \boldsymbol{U}^{(n)}$ per la relació

$$U^{\otimes n}|j\rangle = U|j_1\rangle\, U|j_2\rangle \cdots U|j_n\rangle.$$

EXEMPLE 2.2 (Computacions clàssiques reversibles). Si $f \colon \boldsymbol{B}^n \to \boldsymbol{B}^n$ és una *computació clàssica d'ordre n*, podem definir l'aplicació lineal $U_f \colon \boldsymbol{H}^{(n)} \to \boldsymbol{H}^{(n)}$ per les relacions

$$U_f|j\rangle = |f(j)\rangle.$$

Si f és reversible, llavors U_f és una q-computació, ja que transforma la base ortonormal $\{|j\rangle\}$ en la base ortonormal $\{|f(j)\rangle\}$ (és una simple permutació de la primera). Diem que U_f és la q-computació associada a la computació clàssica reversible f.

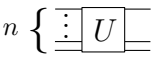
Alguns dels exemples que segueixen són casos especials de l'exemple general anterior.

REMARCA 2.3. Les q-computacions d'ordre n són molt més abundants que les computacions clàssiques reversibles d'ordre n. Això ja és manifest quan $n = 1$, ja que en aquest cas NOT[3] (la negació) és, fora de la identitat, l'única computació clàssica reversible d'ordre 1, mentre que les q-computacions d'ordre 1 depenen, com veurem, de quatre paràmetres reals continus (*cf.* l'exemple 2.4).

3 Per als operadors lògics mantenim la notació estàndard dels texts en anglès: NOT, AND, NAND, OR, XOR, SWAP…

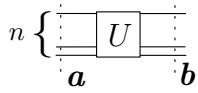
Representació gràfica

Una q-computació U d'ordre n se sol representar per un diagrama de l'estil següent:

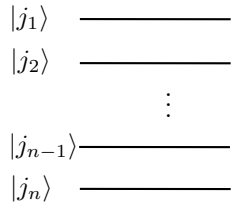


Les n línies horitzontals s'anomenen *q-fils*.

Si hom vol representar el q-input $\boldsymbol{a}$ i el q-output $\boldsymbol{b}$, el diagrama es modifica com segueix:



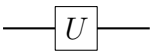
En el cas en què $\boldsymbol{a} = |j_1\rangle \cdots |j_n\rangle$, el q-input es representa com en l'esquema que segueix:



EXEMPLE 2.4 ($n = 1$). És fàcil comprovar que la matriu

$$U = e^{i\alpha}\begin{bmatrix} u_0 & u_1 \\ -\bar{u}_1 & \bar{u}_0 \end{bmatrix}, \quad \alpha \in \mathbb{R}, \quad u_0, u_1 \in \mathbb{C}, \quad u_0\bar{u}_0 + u_1\bar{u}_1 = 1$$

és una q-computació d'ordre 1. De fet, qualsevol $U \in \boldsymbol{U}^{(1)}$ té aquesta forma, ja que podem posar $U = e^{i\alpha}U'$ amb $\det(U') = 1$ (això segueix de la relació $UU^\dagger = I_2$, de la qual es dedueix que $\det(U)$ és un nombre complex unitari), i aleshores $U' \in \boldsymbol{U}^{(1)}$ té necessàriament la forma $\left[\begin{smallmatrix} u_0 & u_1 \\ -\bar{u}_1 & \bar{u}_0 \end{smallmatrix}\right]$ si la seva inversa ha de coincidir amb la seva adjunta.



REMARCA 2.5. Per a ulteriors usos, considerem una construcció més explícita de les q-computacions d'ordre 1.[4] Amb les notacions de l'exemple precedent, la relació $u_0\bar{u}_0 + u_1\bar{u}_1 = 1$ implica que existeix un únic $\theta \in [0, \pi]$ que compleix $|u_0| = \cos\frac{\theta}{2}$ i $|u_1| = \sin\frac{\theta}{2}$. D'això se segueix que $u_0 = e^{-i\lambda}\cos\frac{\theta}{2}$ i $u_1 = -e^{i\mu}\sin\frac{\theta}{2}$, $\lambda, \mu \in \mathbb{R}$ (l'elecció de signes obeeix a conveniències de càlculs posteriors), i així

$$\begin{bmatrix} u_0 & u_1 \\ -\bar{u}_1 & \bar{u}_0 \end{bmatrix} = \begin{bmatrix} e^{-i\lambda}\cos\frac{\theta}{2} & -e^{i\mu}\sin\frac{\theta}{2} \\ e^{-i\mu}\sin\frac{\theta}{2} & e^{i\lambda}\cos\frac{\theta}{2} \end{bmatrix}.$$

4 Aquí, i en el que resta de la secció, seguim molt de prop la secció 4.2 de [16].

Si fem les substitucions $\lambda = (\beta + \gamma)/2$, $\mu = (\gamma - \beta)/2$ ($\beta, \gamma \in \mathbb{R}$), llavors podem escriure

$$\begin{bmatrix} e^{-i\lambda}\cos\frac{\theta}{2} & -e^{i\mu}\sin\frac{\theta}{2} \\ e^{-i\mu}\sin\frac{\theta}{2} & e^{i\lambda}\cos\frac{\theta}{2} \end{bmatrix} = R_z(\beta)R_y(\theta)R_z(\gamma),$$

on definim

$$R_z(\varphi) = \begin{bmatrix} e^{-i\varphi/2} & 0 \\ 0 & e^{i\varphi/2} \end{bmatrix}, \quad R_y(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}.$$

Podem, doncs, concloure que l'element general del grup $S\boldsymbol{U}^{(1)}$ (és el subgrup del grup $\boldsymbol{U}^{(1)}$ format pels elements de determinant 1) té la forma

$$U(\theta, \beta, \gamma) = R_z(\beta)R_y(\theta)R_z(\gamma).$$

El significat geomètric d'aquest enunciat, molt estretament relacionat amb les rotacions de l'espai euclidià, el considerem a la secció 9.

Casos especials

a) Matrius de Pauli

$$I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad X = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

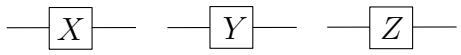
Les matrius de Pauli són autoadjuntes i unitàries: $X^2 = Y^2 = Z^2 = \mathbf{1}$.
La matriu X es pot definir per les relacions

$$X|0\rangle = |1\rangle, X|1\rangle = |0\rangle.$$

Això significa que X és la q-computació corresponent a l'operador booleà clàssic NOT:

$$X|j\rangle = |\text{NOT}(j)\rangle.$$

En termes de la suma booleana de bits, $\text{NOT}(j) = 1 + j$, ja que $1 + 0 = 1$ i $1 + 1 = 0$. Breument, $X|j\rangle = |1 + j\rangle$.



REMARCA 2.6. Amb les notacions de la remarca 2.5, tenim

$$R_z(\varphi) = \cos\tfrac{\varphi}{2} I_2 - i\sin\tfrac{\varphi}{2} Z = e^{-i\frac{\varphi}{2}Z}$$

$$R_y(\theta) = \cos\tfrac{\theta}{2} I_2 - i\sin\tfrac{\theta}{2} Y = e^{-i\frac{\theta}{2}Y}.$$

Això suggereix definir

$$R_X(\psi) = \cos\tfrac{\psi}{2} I_2 - i \sin\tfrac{\psi}{2} X = e^{-i\frac{\psi}{2}X} = \begin{bmatrix} \cos\frac{\psi}{2} & -i\sin\frac{\psi}{2} \\ -i\sin\frac{\psi}{2} & \cos\frac{\psi}{2} \end{bmatrix}.$$

Una altra observació és que cada $U \in \boldsymbol{U}^{(1)}$ es pot expressar com

$$U = e^{i\alpha} AXBXC,$$

amb $A, B, C \in S\boldsymbol{U}^{(1)}$ i $ABC = I_2$ (d'aquesta relació en diem *descomposició d'Euler* de U). En efecte, si $U = e^{i\alpha} R_z(\beta) R_y(\theta) R_z(\gamma)$, basta posar (▷ **2**)

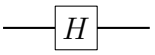
$$\begin{aligned} A &= R_z(\beta) R_y(\tfrac{\theta}{2}) \\ B &= R_y(-\tfrac{\theta}{2}) R_z(-\tfrac{\beta+\gamma}{2}) \\ C &= R_z(\tfrac{\gamma-\beta}{2}). \end{aligned}$$

b) La matriu d'Hadamard H

La matriu $\left[\begin{smallmatrix} 1 & -1 \\ 1 & -1 \end{smallmatrix}\right]$ és autoadjunta i $\left[\begin{smallmatrix} 1 & -1 \\ 1 & -1 \end{smallmatrix}\right]^2 = 2\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. En resulta que la matriu

$$H = \rho \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \begin{cases} |0\rangle \mapsto \rho(|0\rangle + |1\rangle) \\ |1\rangle \mapsto \rho(|0\rangle - |1\rangle) \end{cases}$$

és una q-computació d'ordre 1. Per a escriure H en la forma de l'exemple 2.4, notem que $H = (-i)(iH)$ i que iH té la forma $\left[\begin{smallmatrix} u_0 & u_1 \\ -\bar{u}_1 & \bar{u}_0 \end{smallmatrix}\right]$ amb $u_0 = u_1 = i$.



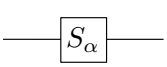
La q-computació $H^{\otimes n}$ (vegeu la segona part de l'exemple 2.1) apareixerà sovint en el que segueix. Convé adonar-se que, usant la notació de l'exemple 1.3, es compleix la identitat

$$H^{\otimes n}(|\mathbf{0}_n\rangle) = \boldsymbol{h}^{(n)}.$$

c) Matrius de canvi de fase

Són les matrius que tenen la forma

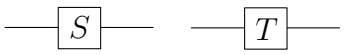
$$S_\alpha = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{bmatrix} = e^{i\frac{\alpha}{2}} \begin{bmatrix} e^{-i\frac{\alpha}{2}} & 0 \\ 0 & e^{i\frac{\alpha}{2}} \end{bmatrix}$$



En particular, definim

$$S = S_{\pi/2} = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} \quad \text{i} \quad T = S_{\pi/4} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}.$$

Adonem-nos que $T^4 = S^2 = X$, que hom podria escriure, si tingués algun propòsit més enllà de l'acudit, $S = \sqrt{\text{NOT}}$.



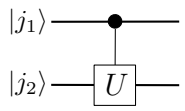
EXEMPLE 2.7 ($n = 2$). Sigui $U \in \boldsymbol{U}^{(1)}$. Definim $C_{12}(U) \in \boldsymbol{U}^{(2)}$ per les relacions

$$C_{12}(U)|0j_2\rangle = |0j_2\rangle, \quad C_{12}(U)|1j_2\rangle = |1\rangle U|j_2\rangle.$$

En forma de matriu tenim, si $U = \left[\begin{smallmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{smallmatrix}\right]$,

$$C_{12}(U) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}.$$

Es tracta, doncs, d'un U controlat, o C-U, atès que U actua sobre $|j_2\rangle$ només quan $j_1 = 1$.



En particular posem $N_{12} = C_{12}(X)$ (NOT controlat, o CNOT):

$$N_{12}|0j_2\rangle = |0j_2\rangle, \quad N_{12}|1j_2\rangle = |1\rangle|1 + j_2\rangle,$$

que es pot escriure d'una manera més compacta com

$$N_{12}|j_1j_2\rangle = |j_1\rangle|j_1 + j_2\rangle.$$

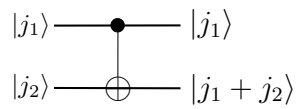
Això mostra que $N_{12}\colon \boldsymbol{H}^{(2)} \to \boldsymbol{H}^{(2)}$ és la q-computació corresponent a la computació clàssica CNOT: $\boldsymbol{B}^2 \to \boldsymbol{B}^2$ tal que

$$00 \mapsto 00, \quad 01 \mapsto 01, \quad 10 \mapsto 11, \quad 11 \mapsto 10$$

o $\text{CNOT}(j_1, j_2) = (j_1, j_1 + j_2)$. Com que això equival a negar el segon q-bit si i només si el primer q-bit és 1, es tracta d'un NOT sobre el segon q-bit «controlat» pel primer q-bit, i això explica la notació.

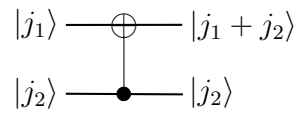
En forma de matriu,

$$N_{12} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$



La q-computació $C_{21}(U)$ es defineix d'una manera anàloga. Per exemple, la matriu de $N_{21} = C_{21}(X)$ és

$$N_{21} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



Més generalment, en el cas d'ordre n, podem definir les q-computacions $C_{r,s}(U)$, on $r, s \in \{1, \ldots, n\}$ són dos índexs diferents, d'una manera similar. Aquesta q-computació actua com U sobre el q-bit s-èsim quan el q-bit r-èsim és 1, i altrament és la identitat. En el cas especial $U = X$, posem $N_{r,s} = C_{r,s}(X)$, que nega el q-bit s-èsim si i només si el q-bit r-èsim és 1. Vegem-ne alguns exemples:

$$N_{4,1}|10101\rangle = |10101\rangle, \quad C_{4,1}(U)|10101\rangle = |10101\rangle$$
$$N_{4,1}|10111\rangle = |00111\rangle, \quad C_{4,1}(U)|10111\rangle = (U|1\rangle)|0111\rangle.$$

EXEMPLE 2.8. La q-computació $C_{12}(U)$ és diferent de $I_2 \otimes U$. De fet, la matriu d'aquesta darrera és

$$\begin{bmatrix} u_{00} & u_{01} & 0 & 0 \\ u_{10} & u_{11} & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}.$$

Així, $(I_2 \otimes U)|00\rangle = |0\rangle\, U|0\rangle = u_{00}|0\rangle|0\rangle + u_{10}|0\rangle|1\rangle$, mentre que $C_{12}(U)|00\rangle = |00\rangle$.

EXEMPLE 2.9 (La q-clonació no és possible). En la seva forma bàsica, el teorema de no-clonació és l'afirmació que no existeix cap q-computació U d'ordre 2 que satisfaci

$$U(|b\rangle|0\rangle) = |b\rangle|b\rangle,$$

$b \in \{0,1\}$. En efecte, considerem $|x\rangle = \rho(|b\rangle + |b'\rangle)$, amb $b' = 1 + b$. Aleshores tenim

$$U(|x\rangle|0\rangle) = \begin{cases} |x\rangle|x\rangle = \rho^2(|b\rangle|b\rangle + |b\rangle|b'\rangle + |b'\rangle|b\rangle + |b'\rangle|b'\rangle), \\ \rho U(|b\rangle|0\rangle + |b'\rangle|0\rangle) = \rho(|b\rangle|b\rangle + |b'\rangle|b'\rangle), \end{cases}$$

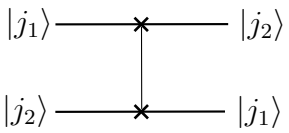
que és una contradicció.

EXEMPLE 2.10. La *porta transposició* («swap» en anglès) és la q-computació d'ordre 2 corresponent a la transposició clàssica $j_1 j_2 \mapsto j_2 j_1$:

$$|j_1 j_2\rangle \mapsto |j_2 j_1\rangle.$$

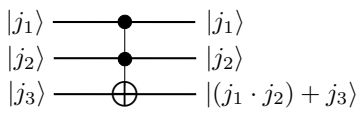
Atès que la porta anterior deixa $|00\rangle$ i $|11\rangle$ fixos i intercanvia $|01\rangle$ i $|10\rangle$, la seva matriu és

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$



EXEMPLE 2.11. La *porta de Toffoli* és la q-computació d'ordre 3 corresponent a la computació clàssica $j_1 j_2 j_3 \mapsto (j_1 \cdot j_2) + j_3$, la qual nega el q-bit j_3 exactament quan $j_1 = j_2 = 1$, de manera que és una negació doblement controlada. Intercanvia $|110\rangle$ i $|111\rangle$ ensems que deixa fixos tots els altres q-vectors de la base. La seva matriu és

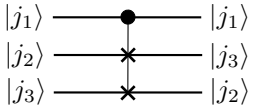
$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$



La porta de Toffoli coincideix amb la q-computació d'ordre 3 corresponent a una versió reversible de la computació clàssica d'ordre 3 NAND (▷ **1**).

EXEMPLE 2.12. La *porta de Fredkin* és la q-computació d'ordre 3 corresponent a la computació clàssica $0j_2j_3 \mapsto 0j_2j_3$ i $1j_2j_3 \mapsto 1j_3j_2$. En altres paraules, és un SWAP controlat. Intercanvia $|110\rangle$ i $|101\rangle$, i deixa tots els altres vectors de la base fixos. Per tant, la seva matriu és

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$



Si $j_3 = 0$, llavors $j_3' = \text{AND}(j_1, j_2)$. Si a més $j_2 = 1$, aleshores $j_2' = \text{NOT}(j_1)$. Així, doncs, la porta de Fredkin també es pot usar per a implementar una versió reversible de la computació clàssica.

3 q-mesures i q-procediments

A més de q-computacions, a fi de produir un model matemàtic de la computació quàntica, ens cal incloure una prescripció per a l'operació de mesurar (també en diem observar) un conjunt $L = \{l_1, \ldots, l_r\} \subseteq \{1, \ldots, n\}$ de q-bits. En el que segueix, $\boldsymbol{a} \in \boldsymbol{H}^{(n)}$ denota un q-vector unitari que representa l'estat corrent d'un *q-registre* de longitud n (la *q-memòria*).

q-mesures. Per a tot vector binari de longitud r, diguem $M = m_1 \cdots m_r \in \boldsymbol{B}^n$, podem formar el subespai vectorial $E_M \subseteq \boldsymbol{H}^{(n)}$ generat pels vectors $|j\rangle$ tals que $j_L = M$, on $j_L = j_{l_1} \cdots j_{l_r}$. La dimensió de E_M és 2^{n-r} i la projecció ortogonal de $\boldsymbol{a}$ sobre E_M és el vector

$$\boldsymbol{a}_L^M = \sum_{j_L = M} a_j |j\rangle.$$

Com que els espais E_M, $M \in \boldsymbol{B}^n$, són ortogonals dos a dos i $\oplus_M E_M = \boldsymbol{H}^{(n)}$, es compleix que

$$\boldsymbol{a} = \sum_{M \in \boldsymbol{B}^n} \boldsymbol{a}_L^M \quad \text{i} \quad 1 = |\boldsymbol{a}|^2 = \sum_M \left| \boldsymbol{a}_L^M \right|^2.$$

Això significa que els nombres $p_M = \left| \boldsymbol{a}_L^M \right|^2$ defineixen una distribució de probabilitat sobre $\{M\} = \boldsymbol{B}^r$ i ens porta a definir la *q-mesura*, o *q-observació*,

dels q-bits de les posicions $l_1, \ldots, l_r$, com l'operació $M_L(\boldsymbol{a})$ que produeix els dos efectes següents:

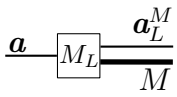
(*i*) Extreure un vector $M \in \boldsymbol{B}^n$ aleatòriament segons la distribució p_M.

(*ii*) Canviar l'estat $\boldsymbol{a}$ de la q-memòria en $\boldsymbol{u}(\boldsymbol{a}_L^M)$, on $\boldsymbol{u}(\boldsymbol{x}) = \hat{\boldsymbol{x}}$ denota el vector unitari definit pel q-vector no nul $\boldsymbol{x}$.

Fixem-nos que si M és un resultat observat, llavors $p_M \neq 0$ i, per tant, $\boldsymbol{a}_L^M \neq 0$.

Dels q-vectors $\boldsymbol{a}_L^M$ en diem que són els *col·lapses* de $\boldsymbol{a}$ respecte de les posicions L.

Com que una q-mesura produeix un vector binari clàssic M i un nou estat de la q-memòria, M_L es representa gràficament amb un fil que porta M (línia gruixuda) i un q-fil que porta l'estat definit pel corresponent col·lapse:



EXEMPLE 3.1. Com a il·lustració, mirem un parell de casos especials. Considerem el cas $n = 3$. Si mesurem el tercer q-bit, $M_3(\boldsymbol{a})$, llavors hi ha dos valors possibles, 0 i 1, el col·lapse corresponent a $m \in \boldsymbol{B}$ és $\boldsymbol{a}_3^m = \sum_{jk} a_{jkm}|jkm\rangle$ i la probabilitat de m és $p_m = |\boldsymbol{a}_3^m|^2$. Similarment, els resultats possibles de $M_{13}(\boldsymbol{a})$ són $rs \in \boldsymbol{B}^2$ i el col·lapse de rs és $\boldsymbol{a}_{13}^{rs} = a_{r0s}|r0s\rangle + a_{r1s}|r1s\rangle$, amb probabilitat $p_{rs} = |\boldsymbol{a}_{13}^{rs}|^2$.

En el cas en què $L = \{1, \ldots, n\}$, escrivim simplement $M(\boldsymbol{a})$. Els resultats possibles són els $j \in \boldsymbol{B}^n$ i el col·lapse de j és $a_j|j\rangle$ amb probabilitat $|a_j|^2$. En aquest context, usualment el coeficient a_j es coneix com a *amplitud* (de probabilitat) de $|j\rangle$, i la probabilitat del resultat j és $p_j = |a_j|^2$: *la probabilitat és el quadrat de la norma de l'amplitud*. Si $n = 3$, per exemple, els $2^3 = 8$ resultats possibles per a $M(\boldsymbol{a}) = M_{123}(\boldsymbol{a})$ són $rst \in \boldsymbol{B}^3$ i el col·lapses de rst és $\boldsymbol{a}_{123}^{rst} = a_{rst}|rst\rangle$ amb probabilitat $p_{rst} = |a_{rst}|^2$.

Un *q-procediment* és una seqüència d'accions que són o bé una q-computació o bé una q-mesura. L'execució del q-procediment consisteix a aplicar successivament les accions de què consta a $|0 \cdots 0\rangle$ (d'aquest q-vector en diem *estat inicial per defecte* de la q-memòria). Atès que la funció última dels q-procediments és produir resultats, la darrera acció sol ser una q-mesura.

EXEMPLE 3.2 (Generador de nombres aleatoris). El q-procediment que segueix produeix nombres aleatoris de n bits amb distribució de probabilitat uniforme:

RANDOM

$$\boldsymbol{a} = H^{\otimes n}|0\cdots 0\rangle = H|0\rangle\cdots H|0\rangle, \quad M(\boldsymbol{a})\ \blacksquare$$

En efecte, des de l'exemple 1.3 sabem que $\boldsymbol{a}$ és el q-vector d'Hadamard $\boldsymbol{h}^{(n)}$. Per tant, l'amplitud de qualsevol vector binari de longitud n és $1/\rho^n$ i la seva probabilitat és $(1/\rho^n)^2 = 1/(\rho^2)^n = 1/2^n$.

4 q-computadors i q-algorismes

Un *q-computador d'ordre n* és un sistema equipat amb implementacions dels quatre elements següents:

1. q-memòria. Capacitat per a contenir qualsevol q-vector unitari $\boldsymbol{a} \in \boldsymbol{H}^{(n)}$. Diem que $\boldsymbol{a}$ és l'*estat* de la q-memòria o simplement l'estat.

De les operacions 2, 3 i 4 que descrivim a continuació en diem *q-procediments elementals*. Els q-procediments elementals són els ingredients bàsics dels q-algorismes que presentem a la secció següent.

2. Rotacions d'un q-bit, $R_l(U)$. Aquesta acció consisteix a aplicar $U \in \boldsymbol{U}^{(1)}$ al q-bit l-èsim, i això ha de ser possible per a qualssevol U i l. Més precisament, $R_l(U)$ és la q-computació definida per

$$|\cdots j_l \cdots\rangle = |\cdots\rangle\,|j_l\rangle\,|\cdots\rangle \mapsto |\cdots\rangle\,U|j_l\rangle\,|\cdots\rangle.$$

Per a $n = 2$, per exemple, $R_2(U) = I_2 \otimes U$ (*cf.* exemple 2.8).

Ens referim als q-procediments elementals $R_l(U)$ com a U-portes. També diem que una U-porta és *restringida* quan U és una de les tres matrius següents: H (Hadamard), $S = S_{\pi/2}$ o $T = S_{\pi/4}$.

3. Negacions controlades $N_{r,s}$. Aquest acció nega el q-bit s-èsim si i només si el q-bit r-èsim és $|1\rangle$, i això ha de ser possible per a qualsevol parell d'índexs diferents r i s. És, doncs, una implementació de l'aplicació lineal que és la identitat sobre els q-vectors de la base que tenen la forma $|\cdots 0_r \cdots\rangle$ i que a més compleix

$$|\cdots 1_r \cdots 0_s \cdots\rangle \mapsto |\cdots 1_r \cdots 1_s \cdots\rangle$$
$$|\cdots 1_r \cdots 1_s \cdots\rangle \mapsto |\cdots 1_r \cdots 0_s \cdots\rangle.$$

D'aquesta mena de q-procediments elementals, en diem *portes* CNOT.

4. Mesura $M_L(\boldsymbol{a})$, $L = \{l_1 < \cdots < l_r\} \subseteq \{1, \ldots, n\}$. Aquest q-procediment elemental s'ha explicat detalladament a la secció anterior.

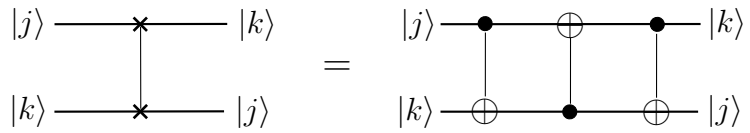
q-algorismes

Un *q-algorisme* és un q-procediment en el qual només s'usen q-procediments elementals. Diem que un q-algorisme és *intern* si no conté q-mesures. Un q-algorisme (intern o no) es diu *restringit* si totes les U-portes que empra són U-portes restringides.

Com a mesura de la *complexitat* d'un q-algorisme prenem el nombre de portes elementals que conté. Un q-algorisme és *polinòmic* si la seva complexitat es pot fitar per una funció polinòmica de n.

EXEMPLE 4.1 (SWAP$[r,s]$). Aquest q-algorisme intern es pot descriure com segueix:

SWAP$[r,s]$
  $N_{r,s}, N_{s,r}, N_{r,s}$ ∎



La q-computació que produeix aquest q-algorisme intercanvia els q-bits r-èsim i s-èsim, la qual cosa significa que implementa l'aplicació lineal definida per

$$|\cdots j_r \cdots j_s \cdots\rangle \mapsto |\cdots j_s \cdots j_r \cdots\rangle.$$

Aquesta afirmació és una conseqüència directa del fet que es compleix per a computacions clàssiques: per a qualsevol parell de bits, (x,y), tenim:

$$\begin{aligned} &N_{1,2}(x,y) = (x, x+y),\\ &N_{2,1}(x, x+y) = (x+x+y, x+y) = (y, x+y),\\ &N_{1,2}(y, x+y) = (y, y+x+y) = (y,x). \end{aligned}$$

EXEMPLE 4.2 (H múltiple). Consisteix a aplicar la porta d'Hadamard H a qualsevol índex d'una llista de posicions diferents $L \subseteq \{1,\ldots,n\}$:

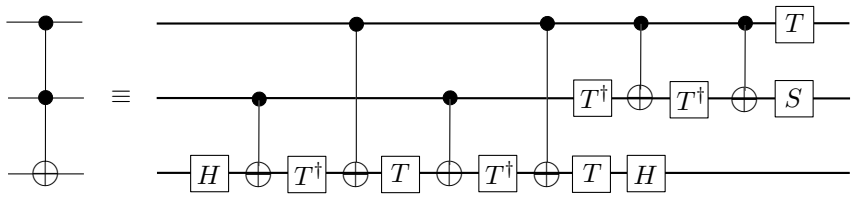
HADAMARD$[L]$
  for $l \in L$ do $R_l(H)$ ∎

Adonem-nos que si $m \in \{1,\ldots,n\}$, HADAMARD$[\{1,\ldots,m\}]$ proporciona un q-algorisme per al q-procediment $|j\rangle \mapsto (H^{\otimes m}|j_1 \cdots j_m\rangle)|j_{m+1} \cdots j_n\rangle$. Aquest algorisme serà denotat per HADAMARD$[m]$. En el cas $m = n$, és un q-algorisme per a $H^{\otimes n}$ i en lloc de HADAMARD$[n]$ simplement escriurem HADAMARD.

Es pot procedir anàlogament per a obtenir q-algorismes en els quals en lloc de H usem qualsevol $U \in \boldsymbol{U}^{(1)}$. Per exemple, $U^{\otimes n}$ es pot calcular pel q-algorisme següent:

  for $l \in \{1,\ldots,n\}$ do $R_l(U)$ ∎

EXEMPLE 4.3 (q-algorisme associat a un algorisme clàssic). Si $f\colon \boldsymbol{B}^n \to \boldsymbol{B}^n$ és una computació reversible, llavors existeix un algorisme clàssic que computa f. Aquest algorisme és una seqüència de portes lògiques NOT o NAND. Afegint bits si és necessari, podem a més suposar que les NAND són reversibles, amb la qual cosa podem traduir l'algorisme en un q-procediment format amb q-portes que són o bé la X de Pauli o bé la q-porta de Toffoli. Aquest q-procediment esdevindrà un q-algorisme si podem trobar un q-algorisme per a la q-porta de Toffoli. Una solució a aquesta qüestió es pot expressar en el diagrama següent (*cf.* [16, exercici 4.24]):



TOFFOLI

$R_3(H)$, $N_{2,3}$, $R_3(T^\dagger)$, $N_{1,3}$, $R_3(T)$, $N_{2,3}$, $R_3(T^\dagger)$, $N_{1,3}$, $R_3(T)$, $R_3(H)$, $R_2(T^\dagger)$, $N_{2,3}$, $R_2(T^\dagger)$, $N_{1,2}$, $R_2(S)$, $R_1(T)$ ∎

EXEMPLE 4.4. Un algorisme per al q-procediment $C_{r,s}(U)$, $U \in \boldsymbol{U}^{(1)}$, $r, s \in \{1, \dots, n\}$ índexs diferents (vegeu l'exemple 2.7 per a la definició). Usarem una descomposició d'Euler de U (vegeu la remarca 2.6):

$$U = e^{i\alpha} AXBXC, \quad ABC = I_2.$$

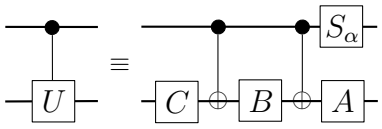
Amb aquestes notacions, el q-algorisme és com segueix:

CONTROL$[r, s, U]$

$R_s(C), N_{r,s}, R_s(B), N_{r,s}, R_s(A), R_r(S_\alpha)$ ∎

Suposarem que $r = 1$ i $s = 2$, ja que l'argument es pot adaptar fàcilment al cas general. Fixem-nos que si $j_1 = 0$, llavors $N_{1,2}$ i $R_1(S_\alpha)$ actuen com la identitat i, atès que $ABC = I_2$, CONTROL també actua com la identitat. Si $j_1 = 1$, aleshores l'acció sobre $|j_2\rangle$ és $AXBXC|j_2\rangle$ i $|j_1\rangle = |1\rangle$ queda multiplicat per $e^{i\alpha}$:

$$|1\rangle|j_2\rangle \mapsto e^{i\alpha}|1\rangle\, AXBXC|j_2\rangle = |1\rangle\, U|j_2\rangle.$$



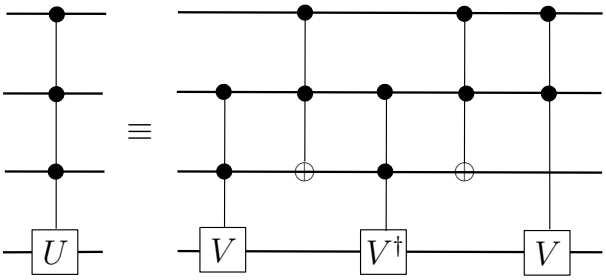
EXEMPLE 4.5 (U-portes multicontrolades). En aquest exemple indiquem com obtenir un q-algorisme per al q-procediment $C_{\{1,\dots,n\},n+1}(U)$ definit per les relacions

$$|j\rangle|j_{n+1} \mapsto \begin{cases} |\mathbf{1}_n\rangle|1 + j_{n+1}\rangle & \text{si } j = \mathbf{1}_n, \\ |j\rangle|j_{n+1}\rangle & \text{altrament.} \end{cases}$$

Si prenem $V \in \boldsymbol{U}^{(1)}$ tal que $U = V^2$, llavors l'algorisme es basa en el procediment recursiu següent:

$$\begin{aligned}
&\textsc{Control}[\{1,\dots,n\}, n+1, U]\\
&\textsc{Control}[\{2,\dots,n\}, n+1, V]\\
&\textsc{Control}[\{1,\dots,n-1\}, n, X]\\
&\textsc{Control}[\{2,\dots,n\}, n+1, V^\dagger]\\
&\textsc{Control}[\{1,\dots,n-1\}, n, X]\\
&\textsc{Control}[\{1,\dots,n-1\}, n+1, V]\ \blacksquare
\end{aligned}$$

En altres paraules, una U-porta n-controlada es redueix a cinc U-portes $(n-1)$-controlades. Aquesta prescripció es copsa més ràpidament amb un gràfic, que dibuixem per al cas $n = 3$:



Si el primer q-bit és $|0\rangle$, aleshores l'acció sobre el tercer q-bit és $VV^\dagger = I_2$. Si el segon q-bit és $|0\rangle$, llavors l'acció sobre el tercer q-bit és I_2. Si el tercer q-bit és $|0\rangle$, i el primer i el segon són $|1\rangle$, aleshores l'acció del tercer q-bit és $V^\dagger V = I_2$. Finalment, si els tres q-bits són $|1\rangle$, l'acció sobre el tercer q-bit és $V^2 = U$.

EXEMPLE 4.6 (Acció d'un $U \in S\boldsymbol{U}^{(1)}$ sobre un pla). Sigui $P = [|j\rangle, |k\rangle]$ el pla generat per dos vectors de la base diferents $|j\rangle$ i $|k\rangle$. Aleshores podem fer actuar $U = [[a,b],[c,d]] \in S\boldsymbol{U}^{(1)}$ sobre P de la manera òbvia: $U|j\rangle = a|j\rangle + b|k\rangle$ i $U|k\rangle = c|j\rangle + d|k\rangle$. A més, podem estendre aquesta acció a tot $\boldsymbol{H}^{(n)}$ de manera que $U|l\rangle = |l\rangle$ per a tot $l \neq j,k$. Com que $|l\rangle$ és ortogonal a P, aquesta acció és una q-computació, i escrivim $U_{j,k}$ per a denotar-la. Per exemple, si $j = 1$ i $k = 2$, llavors la matriu de la q-computació $U_{1,2}$ és $U \oplus I_{2^n-2}$.

L'objecte d'aquest exemple és indicar com obtenir un q-algorisme per a $U_{j,k}$. De fet, és suficient veure, per l'exemple anterior, com resoldre $U_{j,k}$ mitjançant U-portes simples i multicontrol. El cas més simple és quan $|j\rangle$ i $|k\rangle$ tenen la forma

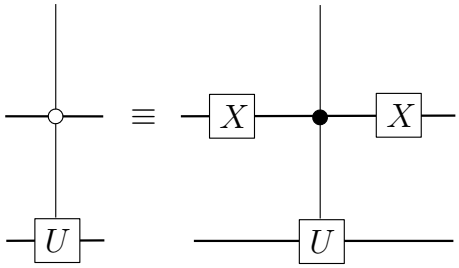
$$|j\rangle = |x\rangle|0\rangle|y\rangle, \quad |k\rangle = |x\rangle|1\rangle|y\rangle.$$

En efecte, en aquest cas es compleix

$$U|j\rangle = a|j\rangle + b|k\rangle = |x\rangle(a|0\rangle + b|1\rangle)|y\rangle = |x\rangle(U|0\rangle)|y\rangle,$$

i $U|k\rangle = |x\rangle(U|1\rangle)|y\rangle$ (un càlcul similar). Per tant, $U_{j,k}$ és una U-porta multicontrol, en el sentit que si $|l\rangle = |x'\rangle|b\rangle|y'\rangle$, llavors $U_{j,k}|l\rangle = |l\rangle$ si $x \neq x'$ o $y \neq y'$, i

altrament és igual a $|x\rangle(U|b\rangle)|y\rangle$. Notem que si el valor del bit controlador és 0, llavors el podem reduir al valor 1 del bit de control i dues portes X, com ho mostra la il·lustració (el cercle blanc és per indicar que el valor de control és 0):



Si j i k difereixen en $r \geq 2$ posicions, escollim $j' \in \boldsymbol{B}^n$ tal que j' difereix de j en una posició i de k en $r-1$ posicions. Per inducció, podem suposar que existeix un q-algorisme per a calcular $U_{j',k}$, donat que el cas $r = 1$ ja s'ha establert, i aleshores es pot obtenir un q-algorisme per a $U_{j,k}$ observant que coincideix amb $X_{j,j'}U_{j',k}X_{j,j'}$, on $X_{j,j'}$ es defineix de manera que $X_{j,j'}|j\rangle = |j'\rangle$, $X_{j,j'}|j'\rangle = |j\rangle$ i $X_{j,j'}|l\rangle = |l\rangle$ si $l \neq j, j'$. Atès que $X_{j,j'}$ és una (mena de) NOT multicontrolat, es pot calcular mitjançant un q-algorisme i, per tant, el mateix es pot fer amb $U_{j,k}$.

EXEMPLE 4.7 (Transformada de Fourier). La *transformada de Fourier* (TF) de $\boldsymbol{H}^{(n)}$ és l'operador lineal

$$F\colon \boldsymbol{H}^{(n)} \to \boldsymbol{H}^{(n)},\ |j\rangle \mapsto \boldsymbol{f}_j = \rho^n \sum_k \xi^{jk}|k\rangle,$$

on $\xi = \xi_n = e^{i\frac{2\pi}{2^n}} = e^{i\frac{\pi}{2^{n-1}}}$ (una arrel primitiva 2^n-èsima de la unitat).

Observem que $F \in \boldsymbol{U}^{(n)}$:

$$\langle \boldsymbol{f}_j|\boldsymbol{f}_{j'}\rangle = \frac{1}{2^n}\sum_k \xi^{(j'-j)k} = \delta_{jj'},$$

ja que, si $l \neq 0$,

$$\sum_{k=0}^{2^n-1} \xi^{lk} = \frac{(\xi^l)^{2^n}-1}{(\xi^l-1)} = 0.$$

Vegem com es pot obtenir un q-algorisme intern per a calcular F. Tenim, posant $\rho = 1/\sqrt{2}$,

$$\begin{aligned}
F|j\rangle &= \rho^n \sum_{k=0}^{2^n-1} e^{\frac{2\pi ijk}{2^n}}|k\rangle \\
&= \rho^n \sum_{k_1,\dots,k_n\in\boldsymbol{B}} e^{2\pi ij\left(\frac{k_1}{2^1}+\frac{k_2}{2^2}+\cdots+\frac{k_n}{2^n}\right)}|k_1\cdots k_n\rangle \\
&= \rho^n \sum_{k_1,\dots,k_n\in\boldsymbol{B}} \bigotimes_{l=1}^{n} e^{\frac{2\pi ijk_l}{2^l}}|k_l\rangle \\
&= \rho^n \bigotimes_{l=1}^{n}\left(|0\rangle + e^{\frac{2\pi ij}{2^l}}|1\rangle\right).
\end{aligned}$$

Però

$$\frac{j}{2^l} = \frac{j_n}{2^l} + \frac{j_{n-1}}{2^{l-1}} + \cdots + \frac{j_{n-(l-1)}}{2} + \left(j_l + \cdots + j_1 2^{n-l-1}\right).$$

Atès que la part entre parèntesis és un enter, el factor tensorial l-èsim de l'expressió anterior és igual a

$$|0\rangle + e^{i\pi \frac{j_n}{2^{l-1}}} \cdots e^{i\pi j_{n-(l-1)}}|1\rangle.$$

Com a conseqüència,

$$F|j\rangle = \rho^n \left(|0\rangle + e^{i\pi j_n}|1\rangle\right)\left(|0\rangle + e^{i\pi \frac{j_n}{2}} e^{i\pi j_{n-1}}|1\rangle\right)\cdots \\ \cdots \left(|0\rangle + e^{i\pi \frac{j_n}{2^{n-1}}} \cdots e^{i\pi \frac{j_2}{2}} e^{i\pi j_1}|1\rangle\right). \quad (*)$$

Si aquest producte tensorial l'escrivim en ordre invers, amb un ρ per a cada factor,

$$\rho\left(|0\rangle + e^{i\pi \frac{j_n}{2^{n-1}}} \cdots e^{i\pi \frac{j_2}{2}} e^{i\pi j_1}|1\rangle\right)\rho\left(|0\rangle + e^{i\pi \frac{j_n}{2^{n-2}}} \cdots e^{i\pi j_2}|1\rangle\right)\cdots \\ \cdots \rho\left(|0\rangle + e^{i\pi j_n/2} e^{i\pi j_{n-1}}|1\rangle\right)\rho\left(|0\rangle + e^{i\pi j_n}|1\rangle\right),$$

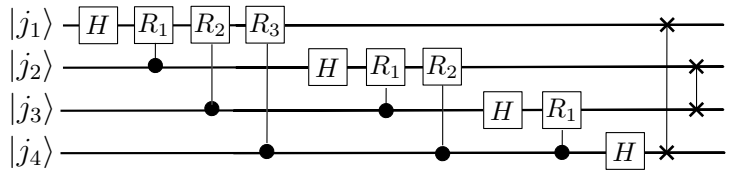
aleshores per al factor l-èsim tenim

$$\rho\left(|0\rangle + e^{i\pi \frac{j_n}{2^{n-l}}} \cdots e^{i\pi \frac{j_{l+1}}{2}} e^{i\pi j_l}|1\rangle\right) = R_{n-l} \cdots R_1 H|j_l\rangle,$$

on R_s significa, per al q-bit l-èsim, $C_{l+s,l}(S_{i\pi/2^s})$. Per tant, tenim l'algorisme següent:

QFT
  for $l \in \{1, \ldots, n\}$ do
    $R_l(H)$
    for $s \in \{1, \ldots, n-l\}$ do $C_{l+s,l}(S_{i\pi/2^s})$
  for $l \in \{1, \ldots, \lfloor n/2 \rfloor\}$ do SWAP$[l, n-l+1]$ ∎

Això mostra que QFT computa F amb complexitat $O(n^2)$. La funció dels SWAPS és restaurar l'ordre original. En el diagrama que segueix il·lustrem el cas $n = 4$.



REMARCA 4.8. Assenyalem, per a ulterior referència, que la fórmula $(*)$ es pot escriure en la forma

$$F.|j\rangle = \rho^n(|0\rangle + e^{2\pi i\, 0.j_n}|1\rangle)(|0\rangle + e^{2\pi i\, 0.j_{n-1}j_n}|1\rangle)\cdots(|0\rangle + e^{2\pi i\, 0.j_1 j_1\cdots j_n}|1\rangle),$$

on, donats els bits $b_1, b_2, \ldots$, és

$$0.b_1b_2\cdots = \frac{b_1}{2} + \frac{b_2}{2^2} + \cdots$$

Els q-algorismes que hem presentat fins ara il·lustren bé el resultat general següent:

TEOREMA 4.9 (Universalitat de les portes U i CNOT).

1) *Qualsevol q-computació es pot realitzar mitjançant un q-algorisme.*
2) *Per a qualsevol q-computació U, i qualsevol $\varepsilon > 0$, existeix un q-algorisme intern restringit que aproxima U amb un error inferior a ε.*

PROVA. $\triangleright$ **3** per a 1) i $\triangleright$ **4** per a 2). □

5 q-algorismes de Deutsch i Grover

En aquesta secció presentem dos q-algorismes arquetípics. El primer, degut a Deutsch-Jozsa [5], decideix, donada una funció booleana $f\colon \boldsymbol{B}^n \to \boldsymbol{B}$ de la qual se sap que és constant o equilibrada, quina de les dues possibilitats és la correcta. Aquest q-algorisme és remarcable per almenys dues raons: d'una banda, és *categòric* (també es diu que és *exacte*), en el sentit que el resultat de la decisió és segur, quan en general els q-algorismes són intrínsecament probabilístics, i de l'altra, la seva complexitat és $O(n)$, en contrast amb el fet que la decisió clàssica pot menester, com veurem tot seguit, fins a $2^{n-1}+1$ passos.

El segon q-algorisme, degut a Grover [7], cerca un element en una llista no ordenada de longitud N en $O(\sqrt{N})$ passos. En aquest cas, la reducció de la complexitat també és significativa, encara que no sigui una reducció exponencial, ja que la complexitat de l'algorisme clàssic és $O(N)$. Cal dir, però, que la solució pot ser incorrecta amb una petita probabilitat, un fet que és menys problemàtic del que pugui semblar a primera vista, ja que es pot repetir la cerca si l'element retornat no és el que cercàvem.

El problema de Deutsch

Sigui $f\colon \boldsymbol{B}^n \to \boldsymbol{B}$ una aplicació de la qual sabem que és *constant* o *equilibrada* (això significa que els conjunts $f^{-1}(0)$ i $f^{-1}(1)$ tenen el mateix cardinal). El *problema de Deutsch* consisteix a decidir a quina de les dues categories pertany f.

La solució clàssica es basa en avaluar f en successius elements de $\boldsymbol{B}^n$. Aquest procés s'atura tan aviat com trobem un valor diferent de l'anterior, cas en el

qual f és equilibrada, o, altrament, quan el nombre d'avaluacions és superior a 2^{n-1}, en el qual cas f és constant. D'això es desprèn que la complexitat del procediment és d'ordre exponencial en n.

El q-procediment de Deutsch. El q-procediment que segueix, dit de Deutsch-Jozsa, resol el problema de Deutsch:

1. Inicialitzem un q-computador d'ordre $n+1$ amb $|\boldsymbol{u}_1\rangle = |0\rangle\overset{n)}{\ldots}|0\rangle|1\rangle$.

2. Usem l'exemple 4.2 per a obtenir

$$|\boldsymbol{u}_2\rangle = H^{\otimes(n+1)}|\boldsymbol{u}_1\rangle = \rho^{n+1}\sum_{j=0}^{2^n-1}|j\rangle(|0\rangle - |1\rangle).$$

3. Sigui $U_{\tilde{f}}$ la q-computació corresponent a la computació clàssica (reversible) $\boldsymbol{B}^n \times \boldsymbol{B} \to \boldsymbol{B}^n \times \boldsymbol{B}$, $(x, b) \mapsto (x, b + f(x))$, i sigui $|\boldsymbol{u}_3\rangle = U_{\tilde{f}}|\boldsymbol{u}_2\rangle$. Atès que

$$U(|j\rangle|b\rangle) = |j\rangle|b + f(j)\rangle$$

obtenim

$$|\boldsymbol{u}_3\rangle = \rho^{n+1}\sum_{j=0}^{2^n-1}|j\rangle(|f(j)\rangle - |1 + f(j)\rangle),$$

que es pot escriure com

$$\rho^{n+1}\sum_{j=0}^{2^n-1}(-1)^{f(j)}|j\rangle(|0\rangle - |1\rangle) = \rho^{n+1}\sum_{j_r\in\boldsymbol{B}}(-1)^{f(j_1\cdots j_n)}|j_1\cdots j_n\rangle(|0\rangle - |1\rangle).$$

4. Calculem $|\boldsymbol{u}_4\rangle = (H^{\otimes n}\otimes I_2)\,|\boldsymbol{u}_3\rangle$. Com que

$$\begin{aligned}(H^{\otimes n}\otimes I_2)|j_1\cdots j_n\rangle(|0\rangle - |1\rangle) &= (H|j_1\rangle)\cdots(H|j_n\rangle)(|0\rangle - |1\rangle)\\ &= \rho^n\prod_{r=1}^{n}(|0\rangle + (-1)^{j_r}|1\rangle)(|0\rangle - |1\rangle)\\ &= \rho^n\sum_{k_s\in\boldsymbol{B}}(-1)^{j\cdot k}|k_1\cdots k_n\rangle(|0\rangle - |1\rangle),\end{aligned}$$

on $j\cdot k = j_1k_1 + \cdots + j_nk_n$ és el producte escalar dels vectors binaris j i k, trobem

$$|\boldsymbol{u}_4\rangle = \rho^{2n+1}\sum_{k_s\in\boldsymbol{B}}\sum_{j_r\in\boldsymbol{B}}(-1)^{j\cdot k+f(j_1\cdots j_n)}|k_1\cdots k_n\rangle(|0 - |1\rangle),$$

que es pot expressar com

$$\rho^{2n+1}\sum_{j,k}(-1)^{j\cdot k+f(j)}|k\rangle(|0\rangle - |1\rangle).$$

Mirem ara, en aquesta expressió, el coeficient $a_k = \rho^{2n+1}\sum_j (-1)^{j\cdot k+f(j)}$ de $|k\rangle(|0\rangle - |1\rangle)$. Si f és constant, $a_k = \rho^{2n+1}(-1)^{f(0)}\sum_j (-1)^{j\cdot k}$, de manera que $a_0 = (-1)^{f(0)}\rho$ i $a_k = 0$ per a $k \neq 0$. Si f és equilibrada, llavors $a_0 = \rho^{2n+1}\sum_j (-1)^{f(j)} = 0$, i és clar que $a_k \neq 0$ per a algun $k \neq 0$. Aquestes conclusions es poden resumir com segueix:

$$|\boldsymbol{u}_4\rangle = \begin{cases} \rho|0\rangle\,(|0\rangle - |1\rangle) & \text{si } f \text{ és constant,} \\ \sum_{k\neq 0} a_k|k\rangle\,(|0\rangle - |1\rangle) & \text{si } f \text{ és equilibrada.} \end{cases}$$

5. El darrer pas consisteix a mesurar els n primers q-bits. El resultat és 0 amb certesa si f és constant i diferent de zero, també amb certesa, si f és equilibrada. Per tant, l'algorisme decideix *categòricament* si f és constant o equilibrada.

***q*-algorisme de Deutsch.** Donada una aplicació $f\colon \boldsymbol{B}^n \to \boldsymbol{B}$ que és constant o equilibrada, aquest q-algorisme retorna 0 si i només si f és constant. Treballem amb $n+1$ bits i posem $\widetilde{f}$ per a denotar la computació clàssica reversible definida per $(x,b) \mapsto (x, b+f(x))$, $x \in \boldsymbol{B}^n$, $b \in \boldsymbol{B}$.

DEUTSCH$[f]$

$$\begin{aligned} & \to |\mathbf{0}_n\rangle|0\rangle \\ R_{n+1}(X) \quad & \to |0\cdots 0\rangle|1\rangle \\ \text{HADAMARD}[n] \quad & \to \rho^{n+1}\textstyle\sum_{j=0}^{2^n-1}|j\rangle(|0\rangle - |1\rangle) \\ U_{\widetilde{f}} \quad & \to \rho^{n+1}\textstyle\sum_{j=0}^{2^n-1}(-1)^{f(j)}|j\rangle(|0\rangle - |1\rangle) \\ \text{HADAMARD}[n] \quad & \to \rho^{2n+1}\textstyle\sum_k\sum_j(-1)^{j\cdot k+f(j)}|k\rangle(|0\rangle - |1\rangle) \end{aligned}$$

$//\rho|\mathbf{0}_n\rangle(|0\rangle - |1\rangle)$ si f és constant, i
$//\sum_{j\neq 0} a_j|j\rangle(|0\rangle - |1\rangle)$ si f és equilibrada.

$M_{\{1,\ldots,n\}} \quad \to M$

si $M = 0$ llavors Constant altrament Equilibrada ∎

Cerca de Grover

Suposem que $\{j \to x_j \mid j = 0,\ldots,N-1\}$ és una base de dades amb $N = 2^n$ ítems. Si hem de cercar el j tal que x_j satisfà una certa condició, com ara trobar la posició d'un nombre de telèfon en una llista aleatòria, en el pitjor dels casos haurem d'examinar N ítems. De mitjana, el nombre d'elements que cal examinar per a trobar un ítem escollit a l'atzar és $N/2$.

El remarcable descobriment de Grover [7, 8] és que existeix un q-algorisme que troba un x satisfent la condició amb complexitat $O(\sqrt{N/M})$, on M és el nombre de solucions possibles a la cerca.[5]

5 El q-algorisme de Grover és probabilístic, en el sentit que existeix una petita probabilitat p d'obtenir un resultat que no satisfaci la condició. Com és costum en aquests casos, l'execució de l'algorisme un nombre fixat de vegades, diguem-ne k (la qual cosa no canvia l'ordre de la

***q*-procediment de Grover.** Sigui J_1 (J_0) el subconjunt de $\{0,1,\ldots,N-1\}$ format pels j tals que x_j satisfà (no satisfà) la condició en qüestió. Considerem l'aplicació tal que

$$f(j) = \begin{cases} 0 & \text{si } j \in J_0, \\ 1 & \text{si } j \in J_1. \end{cases}$$

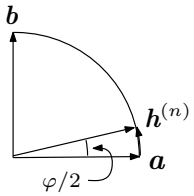
Definim els q-vectors unitaris

$$\boldsymbol{a} = \frac{1}{\sqrt{N-M}} \sum_{j\in J_0} |j\rangle \quad \text{i} \quad \boldsymbol{b} = \frac{1}{\sqrt{M}} \sum_{j\in J_1} |j\rangle.$$

Els sumands no nuls de $\boldsymbol{b}$ (respectivament $\boldsymbol{a}$) són els vectors de la base corresponents a les solucions (no solucions) de la cerca. Notem també que

$$\boldsymbol{h}^{(n)} = \sqrt{\frac{N-M}{N}}\boldsymbol{a} + \sqrt{\frac{M}{N}}\boldsymbol{b} = \cos\left(\frac{\varphi}{2}\right)\boldsymbol{a} + \sin\left(\frac{\varphi}{2}\right)\boldsymbol{b},$$

on la darrera igualtat defineix $\varphi \in (0,\pi)$ unívocament: $\varphi = 2\arcsin(\sqrt{M/N})$.



REMARCA 5.1. Usant les fórmules trigonomètriques de l'angle doble, obtenim

$$\sin(\varphi) = \frac{2\sqrt{M}\sqrt{N-M}}{N}, \quad \cos(\varphi) = \frac{N-2M}{N}. \qquad \square$$

Per a explicar com funciona el q-procediment de Grover, ens cal introduir dues q-computacions d'ordre n, que denotem per G_f i K. La definició de G_f és com segueix ($j \in \boldsymbol{B}^n$):

$$G_f(|j\rangle) = \begin{cases} -|j\rangle & \text{si } j \in J_1, \\ |j\rangle & \text{si } j \in J_0. \end{cases}$$

En altres paraules, G_f és la simetria respecte de l'espai generat per les no-solucions. En particular, $G_f(\boldsymbol{a}) = \boldsymbol{a}$ i $G_f(\boldsymbol{b}) = -\boldsymbol{b}$. Per tant, també tenim

$$G_f(\boldsymbol{h}^{(n)}) = G_f\left(\cos\left(\frac{\varphi}{2}\right)\boldsymbol{a} + \sin\left(\frac{\varphi}{2}\right)\boldsymbol{b}\right) = \cos\left(\frac{\varphi}{2}\right)\boldsymbol{a} - \sin\left(\frac{\varphi}{2}\right)\boldsymbol{b}.$$

La q-computació K, que no depèn de f, es defineix com

$$K(\boldsymbol{x}) = \sum_j (2x - x_j)|j\rangle,$$

---

complexitat), produirà una resposta incorrecta en tots els casos amb probabilitat p^k, un valor que usualment és negligible fins i tot per a valors petits de k, amb la qual cosa la probabilitat d'obtenir la resposta buscada en algun dels passos és $1 - p^k \simeq 1$.

on $x = \frac{1}{N}\sum_j x_j$, la mitjana de les amplituds x_j de $\boldsymbol{x}$ (diem que K és la *inversió respecte de la mitjana*). Aquesta aplicació lineal és realment una q-computació, ja que preserva la norma:

$$\begin{aligned}|K(\boldsymbol{x})|^2 &= \sum_j (2x - x_j)(2\bar{x} - \bar{x}_j)\\ &= 4Nx\bar{x} - 2\bar{x}\sum_j x_j - 2x\sum_j \bar{x}_j + \sum_j x_j\bar{x}_j\\ &= 4Nx\bar{x} - 2N\bar{x}x - 2Nx\bar{x} + |\boldsymbol{x}|^2\\ &= |\boldsymbol{x}|^2.\end{aligned}$$

Ara el q-procediment de Grover es pot descriure així:

1. Sigui $\boldsymbol{u}_0 = \boldsymbol{h}^{(n)} = \cos\left(\frac{\varphi}{2}\right)\boldsymbol{a} + \sin\left(\frac{\varphi}{2}\right)\boldsymbol{b}$.

2. Per a $j = 1, \ldots, m = \left\lfloor \dfrac{\pi}{2\varphi} \right\rfloor$, poseu $\boldsymbol{u}_j = K(G_f(\boldsymbol{u}_{j-1}))$.

3. Retorneu $M(\boldsymbol{u}_m)$.

La raó principal per a provar que aquest procediment és correcte és que *en el pla generat per $\boldsymbol{a}$ i $\boldsymbol{b}$ l'aplicació KG_f és una rotació d'amplitud φ*. De fet, és suficient mostrar que

$$K\boldsymbol{a} = \cos(\varphi)\boldsymbol{a} + \sin(\varphi)\boldsymbol{b}$$

i

$$K(-\boldsymbol{b}) = -\sin(\varphi)\boldsymbol{a} + \cos(\varphi)\boldsymbol{b}.$$

Però aquestes relacions són una conseqüència immediata de la definició de K i de la fórmula usada a la remarca 5.1 (▷ **5**). En particular,

$$\boldsymbol{u}_j = \boldsymbol{a}\cos\left(\frac{2j+1}{2}\varphi\right) + \boldsymbol{b}\sin\left(\frac{2j+1}{2}\varphi\right).$$

Això mostra que l'elecció òptima del nombre m d'iteracions en el pas 2 és el més petit enter positiu que minimitza la distància de $\boldsymbol{u}_m$ a $\boldsymbol{b}$, i això es compleix quan m és el nombre enter més proper a

$$\left(\frac{\pi}{2} - \frac{\varphi}{2}\right)\Big/\varphi = \frac{\pi}{2\varphi} - 1/2,$$

això és, quan $m = \lfloor \frac{\pi}{2\varphi} \rfloor = \left\lfloor \frac{\pi}{4\arcsin(\sqrt{M/N})} \right\rfloor$. [6]

REMARCA 5.2. Atès que $\arcsin(x) > x$ per a $x \in (0, \frac{\pi}{2})$, tenim

$$m \le \frac{\pi}{4\arcsin\sqrt{M/N}} \le \frac{\pi}{4}\sqrt{N/M}.$$

6 Usem que el nombre enter més proper a $x - \frac{1}{2}$ és $\lfloor x \rfloor$.

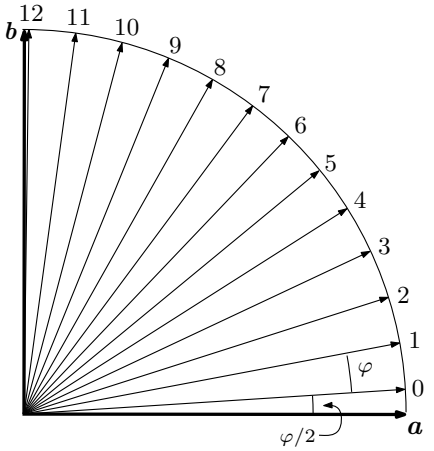
Per tant, també es compleix $m \le \left\lfloor \frac{\pi}{4}\sqrt{N/M} \right\rfloor$, i com que $\frac{\pi}{4x} - \frac{\pi}{4\arcsin(x)} < 1$ per a tot $x \in (0,1)$, $\left\lfloor \frac{\pi}{4}\sqrt{N/M} \right\rfloor \le m+1$. Un estudi més detallat mostra que quan $x \to 0$, els intervals en els quals $\left\lfloor \frac{\pi}{4x} \right\rfloor = \left\lfloor \frac{\pi}{4\arcsin(x)} \right\rfloor + 1$ esdevenen negligibles en comparació amb els intervals en els quals $\left\lfloor \frac{\pi}{4x} \right\rfloor = \left\lfloor \frac{\pi}{4\arcsin(x)} \right\rfloor$. Així, doncs, si iterem $\left\lfloor \frac{\pi}{4}\sqrt{N/M} \right\rfloor$ vegades el bucle del pas 2 del q-procediment de Grover, obtenim el nombre correcte de rotacions gairebé sempre, i altrament anem un pas enllà de l'òptim, que a la pràctica dóna un q-vector que és quasi tan bo com el precedent.

La probabilitat d'obtenir la resposta correcta en una passada del q-procediment de Grover és $p = \sin^2(\frac{2m+1}{2}\varphi)$, ja que $\sin(\frac{2m+1}{2}\varphi)\frac{1}{\sqrt{M}}$ és l'amplitud a $\boldsymbol{u}_m$ de qualsevol de les M solucions. Similarment, la probabilitat d'obtenir una resposta errònia és $q = \cos^2(\frac{2m+1}{2}\varphi)$. Com que l'especificació de m comporta que $\frac{2m+1}{2}\varphi = \frac{\pi}{2} + \varepsilon$, amb $|\varepsilon| \le \varphi/2$, veiem que

$$\begin{aligned} p &= \sin^2(\frac{\pi}{2} + \varepsilon) = \cos^2(\varepsilon) = \cos^2(|\varepsilon|) \\ &\ge \cos^2\left(\frac{\varphi}{2}\right) = \cos^2\left(\arcsin\left(\sqrt{M/N}\right)\right) = 1 - \frac{M}{N}. \end{aligned}$$

Per tant, $q = 1 - p \le M/N$.

EXEMPLE 5.3. Il·lustrem les idees anteriors en el cas $n = 8$ i $M = 1$. Tenim $N = 256$, $\varphi = 7.166\,643°$, $m = 12$. L'argument del vector $\boldsymbol{u}_{12}$ és $89.583\,042°$ i la probabilitat d'un resultat correcte és $p = 0.999\,947$. Notem que p és molt més propera a 1 que la fita inferior $1 - M/N = 1 - 1/256 = 0.996\,094$. La probabilitat d'error és $q = 0.000\,053$, de nou molt més propera a 0 que la fita superior $M/N = 1/256 = 0.003\,906$.



q-algorisme de Grover. Donada una aplicació $f\colon \boldsymbol{B}^n \to \boldsymbol{B}$ de la qual sabem que $M = |f^{-1}(1)| > 0$, el q-algorisme en qüestió computa el q-procediment de Grover per a f. Treballem amb un q-computador d'ordre $n+1$ i posem $\widetilde{f}$ per a denotar la computació clàssica reversible definida per $(x,b) \mapsto (x, b+f(x))$, $x \in \boldsymbol{B}^n$, $b \in \boldsymbol{B}$. Posem $U_{\tilde{f}}$ per a denotar la q-computació associada i usem les notacions m i $\boldsymbol{u}_j$ ($j = 0,1,\dots,m$) de la discussió precedent.

És fàcil formular el q-algorisme que cerquem, GROVER$[f]$, en termes de q-algorismes GROVERG$[f]$ i GROVERK per a computar G_f i K:

GROVER$[f,m]$

	$\to \lvert \mathbf{0}_n \rangle$
HADAMARD	$\to \boldsymbol{u}_0 = \boldsymbol{h}^{(n)}$
for $j \in \{1,\dots,m\}$ do	
GROVERK GROVERG$[f]$ $\lvert \boldsymbol{u}_{j-1} \rangle$	$\to \lvert \boldsymbol{u}_j \rangle$
$M(\boldsymbol{u}_m)$	$\to M$ ∎

Per a descriure GROVERG$[f]$, també treballem amb un q-computador d'ordre $n+1$, on el darrer q-bit fa un paper auxiliar, amb valor inicial $|1\rangle$. Com que al final acaba tenint el mateix valor, el resultat útil de GROVERG$[f]$ és l'estat final dels altres q-bits.

GROVERG$[f]$

	$\to \lvert \boldsymbol{x} \rangle \lvert 1 \rangle$
	// Set $\boldsymbol{x} = \boldsymbol{x}^0 + \boldsymbol{x}^1$, $\boldsymbol{x}^i = \sum_{j \in J_i} x_j \lvert j \rangle$, $i = 0,1$.
$R_{n+1}(H)$	$\to \rho(\lvert \boldsymbol{x}^0 \rangle \lvert 0 \rangle + \lvert \boldsymbol{x}^1 \rangle \lvert 0 \rangle - \lvert \boldsymbol{x}^0 \rangle \lvert 1 \rangle - \lvert \boldsymbol{x}^1 \rangle \lvert 1 \rangle)$
$U_{\tilde{f}}$	$\to \rho(\lvert \boldsymbol{x}^0 \rangle \lvert 0 \rangle + \lvert \boldsymbol{x}^1 \rangle \lvert 1 \rangle - \lvert \boldsymbol{x}^0 \rangle \lvert 1 \rangle - \lvert \boldsymbol{x}^1 \rangle \lvert 0 \rangle)$
	$= (\lvert \boldsymbol{x}^0 \rangle - \lvert \boldsymbol{x}^1 \rangle)(H \lvert 1 \rangle)$
$R_{n+1}(H)$	$\to \lvert G_f \boldsymbol{x} \rangle \lvert 1 \rangle$ ∎

Per a descriure GROVERK, és suficient treballar amb els n primers q-bits partint de l'estat $\boldsymbol{y} = G_f(\boldsymbol{x})$ produït pel q-algorisme anterior:

GROVERK

	$\to \lvert \boldsymbol{y} \rangle$
HADAMARD	
for $l \in \{1,\dots,n\}$ do	
$R_l(X)$	
//Aquest bucle actua com $X^{\otimes n}$	
$C_{\{2,\dots,n\},1}(Z)$	
//Z al primer q-bit controlat per tots els altres.	
for $l \in \{1,\dots,n\}$ do	
$R_l(X)$	
//$X^{\otimes n}$	
HADAMARD	$\to \lvert K(\boldsymbol{y}) \rangle$ ∎

La justificació que aquest q-algorisme computa K es basa en les observacions següents:

1) $K = 2P_{\boldsymbol{h}^{(n)}} - I_N$, on $P_{\boldsymbol{a}}$ denota la projecció ortogonal sobre $\boldsymbol{a}$ (per a un vector unitari $\boldsymbol{a}$, $P_{\boldsymbol{a}}\boldsymbol{x} = \langle \boldsymbol{a}|\boldsymbol{x}\rangle \boldsymbol{a}$). En efecte, l'afirmació resulta directament de la definició de K i la relació

$$P_{\boldsymbol{h}^{(n)}}\boldsymbol{x} = \langle \boldsymbol{h}^{(n)}|\boldsymbol{x}\rangle \boldsymbol{h}^{(n)} = \rho^{2n}(\textstyle\sum x_j) \sum |j\rangle = \mu(\boldsymbol{x}) \sum |j\rangle.$$

2) $K = H^{\otimes n}(2P_{|\mathbf{0}_n\rangle} - I_N)H^{\otimes n}$. Això és una conseqüència de la fórmula $UP_{\boldsymbol{a}}U^{-1} = P_{U\boldsymbol{a}}$, on U és una q-computació arbitrària i $\boldsymbol{a}$ qualsevol q-vector, i de la fórmula anterior. Fixem-nos que, si apliquem $UP_{\boldsymbol{a}}U^{-1}$ a $U\boldsymbol{x}$, obtenim $U\boldsymbol{a}$ si $\boldsymbol{x} = \boldsymbol{a}$ i 0 si $\boldsymbol{x}$ és ortogonal a $\boldsymbol{a}$.

3) $I_N - 2P_{|\mathbf{0}_n\rangle} = X^{\otimes n} C_{\{2,\dots,n\},1}(Z) X^{\otimes n}$. Notem que $I_N - 2P_{|\mathbf{0}_n\rangle}$ canvia el signe de $|\mathbf{0}_n\rangle$ i és la identitat per als $|j\rangle$ amb $j \neq \mathbf{0}_n$. En relació amb l'expressió de la dreta de la fórmula, observem que $C_{\{2,\dots,n\},1}(Z)$, i, per tant, tota la composició no fa res sobre $|j\rangle$ llevat quan $j_2, \dots, j_n$ són tots 0. Si $j_2 = \cdots j_n = 0$, llavors $C_{\{2,\dots,n\},1}(Z)$ aplica Z a $|\tilde{j}_1\rangle$, i, per la definició de Z ($Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$), l'acció no fa res si $j_1 = 1$ i li canvia el signe si $j_1 = 0$.

4) L'anàlisi del q-algorisme de Grover s'ha de completar amb un q-algoritme per computar $C_{\{2,\dots,n\},1}(Z)$. Però aquest q-algorisme es pot obtenir tal com s'ha indicat a l'exemple 4.5.

6 Estimació de la fase d'un valor propi

Sigui U una q-computació d'ordre n, i sigui $\boldsymbol{u} \in \boldsymbol{H}^{(n)}$ un vector propi de U. El valor propi corresponent a $\boldsymbol{u}$ té la forma $e^{2\pi i\varphi}$, amb $\varphi \in [0,1)$. Suposant que U i $\boldsymbol{u}$ són coneguts, llavors el *problema d'estimació de la fase* consisteix a obtenir r bits $\varphi_1, \dots, \varphi_r$, per a qualsevol $r > 0$ fixat, del desenvolupament binari $0.\varphi_1\varphi_2\cdots$ de φ.

L'objecte d'aquesta secció és formular i analitzar un q-algorisme interessant descobert per Kitaev [11] per a resoldre aquest problema. Com que hem de menester alguns q-bits auxiliars, diguem m, treballem a $\boldsymbol{H}^{(m)} \times \boldsymbol{H}^{(n)}$. L'algorisme pressuposa que podem inicialitzar $\boldsymbol{H}^{(n)}$ amb el q-vector $\boldsymbol{u}$ i també que podem efectuar les q-computacions «controlades» $C_{m-l+1}(U^{2^{l-1}})$ definides a $\boldsymbol{H}^{(m)} \times \boldsymbol{H}^{(n)}$ com segueix ($l = 1, \dots, n$):

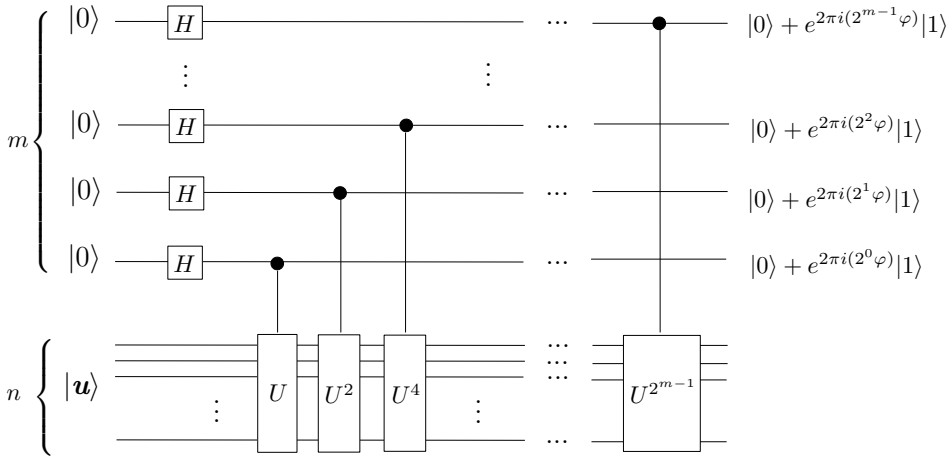
$$C_{m-l+1}(U^{2^{l-1}})(|\varphi_1\cdots\varphi_m\rangle|\boldsymbol{u}\rangle) = \begin{cases} |\varphi_1\cdots\varphi_m\rangle|\boldsymbol{u}\rangle & \text{si } \varphi_{m-l+1} = 0, \\ |\varphi_1\cdots\varphi_m\rangle \left(U^{2^{l-1}}|\boldsymbol{u}\rangle\right) & \text{si } \varphi_{m-l+1} = 1. \end{cases}$$

q-algorisme de Kitaev

KITAEV$[U, \boldsymbol{u}]$

0. $\to |\mathbf{0}_m\rangle|\boldsymbol{u}\rangle$
1. HADAMARD$[m]$ $\to |\boldsymbol{h}^{(m)}\rangle|\boldsymbol{u}\rangle$
2. for $l \in 1..m$ do
   $C_{m-l+1}(U^{2^{l-1}})$
3. QFT$^\dagger[m]$
4. $M_{\{1,\dots,m\}}$

L'anàlisi d'aquest algorisme, el farem en dues parts, A i B. En la primera, suposem que $\varphi = 0.\varphi_1 \cdots \varphi_m$ i, en la segona, considerem el cas general. El diagrama següent il·lustra els passos 0-2.



A. L'acció de $U^{2^{l-1}}$ sobre $|\boldsymbol{u}\rangle$ es redueix a multiplicar-lo per 1 o $e^{2\pi i 2^{l-1}\varphi}$ segons que el q-bit de control sigui $|0\rangle$ o $|1\rangle$. Aquest factor es pot moure just davant del q-bit de control, de manera que l'estat al final del bucle 2 es pot escriure en la forma

$$\rho^m \left(|0\rangle + e^{2\pi i 2^{m-1}\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{m-2}\varphi}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 2^0\varphi}|1\rangle\right). \qquad (1)$$

Això, emprant la notació dels desenvolupaments binaris, adopta la forma

$$\rho^m\left(|0\rangle + e^{2\pi i\, 0.\varphi_m}|1\rangle\right)\left(|0\rangle + e^{2\pi i\, 0.\varphi_{m-1}\varphi_m}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i\, 0.\varphi_1\cdots\varphi_m}|1\rangle\right), \quad (2)$$

ja que $e^{2\pi i k} = 1$ per a tot nombre enter k. Però per la remarca 4.8, aquesta expressió és igual a $F|\varphi\rangle$, que és el q-output del q-algorisme QFT (exemple 4.7). És clar, per tant, que podem recuperar l'estat $|\varphi\rangle|\boldsymbol{u}\rangle$ aplicant $F^\dagger \otimes I_{2^n}$, on $F^\dagger$ és la inversa de F, inversa que es pot calcular amb el q-algorisme QFT$^\dagger[m]$ consistent a efectuar QFT en ordre invers. Així, doncs, KITAEV subministra φ exactament en el cas en què φ es pot expressar amb m bits.

B. El raonament és una mica més tècnic quan φ no es pot expressar amb m bits. En aquest cas, $F^\dagger \otimes I_{2^n}$ no produeix el q-vector $|\varphi\rangle|\boldsymbol{u}\rangle$, sinó una superposició de la forma $\sum a_l|l\rangle|\boldsymbol{u}\rangle$. Com veurem tot seguit, aquesta dificultat es pot superar i obtenir els primers r bits de φ sempre que $r \leq m$.

Desenvolupant el producte (2), veiem que es pot escriure en la forma

$$\rho^m \sum_{k=0}^{2^m-1} e^{2\pi i\varphi k}|k\rangle|\boldsymbol{u}\rangle.$$

Llavors, el resultat del pas 3 és

$$\begin{aligned}\rho^m \sum_{k=0}^{2^m-1} e^{2\pi i\varphi k}(F^\dagger|k\rangle)|\boldsymbol{u}\rangle &= \rho^{2m} \sum_{k=0}^{2^m-1} e^{2\pi i\varphi k} \sum_{l=0}^{2^m-1} e^{-\frac{2\pi ikl}{2^m}}|l\rangle|\boldsymbol{u}\rangle \\ &= \rho^{2m} \sum_{l=0}^{2^m-1} \left(\sum_{k=0}^{2^m-1} e^{2\pi i(\varphi-l/2^m)k}\right)|l\rangle|\boldsymbol{u}\rangle \\ &= \rho^{2m} \sum_{l=0}^{2^m-1} \frac{1-e^{2\pi i(\varphi-l/2^m)2^m}}{1-e^{2\pi i(\varphi-l/2^m)}}|l\rangle|\boldsymbol{u}\rangle.\end{aligned}$$

Finalment, el resultat del pas 4, la q-mesura dels m primers q-bits, també és clar: serà un nombre enter l de m bits extret amb probabilitat[7]

$$p_l = \rho^{4m}\left|\frac{1-e^{2\pi i(\varphi-l/2^m)2^m}}{1-e^{2\pi i(\varphi-l/2^m)}}\right|^2 = \rho^{4m}\frac{\sin^2\pi(\varphi-l/2^m)2^m}{\sin^2\pi(\varphi-l/2^m)}. \qquad (*)$$

Amb aquesta llei de distribució podem estimar quines són les possibilitats que els primers r bits de l ($0 < r \leq m$) coincideixin amb $f = \varphi_1 \cdots \varphi_r$. En efecte, usant les probabilitats p_l es pot veure (▷ **6**) que

$$p\left(|2^m\varphi - l| > 2^{m-r}\right) \leq \frac{1}{2(2^{m-r}-2)}. \qquad (**)$$

Per tant, podem garantir que r bits són correctes amb probabilitat $1-\varepsilon$ si $\frac{1}{2(2^{m-r}-2)} \leq \varepsilon$, una relació que és equivalent a

$$m \geq r + \log_2\left(2 + \frac{1}{2\varepsilon}\right).$$

7 Ordre modular d'un nombre enter

El propòsit d'aquesta secció és presentar el q-algorisme de Shor per a trobar $r = \mathrm{ord}_N(a)$, on N i a són nombres enters positius amb $(a, N) = 1$. Per definició,

7 Usem la fórmula $\left|1-e^{i\alpha}\right|^2 = 4\sin^2(\alpha/2)$, que és una conseqüència de la relació $\left|1-e^{i\alpha}\right|^2 = (1-e^{i\alpha})(1-e^{-i\alpha}) = 2-(e^{i\alpha}+e^{-i\alpha}) = 2(1-\cos\alpha)$.

r és el menor nombre enter positiu tal que $a^r \equiv 1 \mod N$ o, en altres paraules, l'ordre de a vist com un element del grup $\mathbb{Z}_N^*$.

Des d'un punt de vista clàssic, el càlcul de r està relacionat amb la cerca dels divisors de $\phi(N)$,[8] un problema que té complexitat exponencial en $\log_2(N)$ (vegeu [1]). Per contrast, el q-algorisme de Shor subministra una solució probabilista en un temps que és polinòmic en $\log_2(N)$.

Fixem primer unes notacions. Posem $n = \lceil \log_2(N) \rceil$ i definim la q-computació $U_a = U_{a,N}$ d'ordre n per la relació

$$U_a|j\rangle = \begin{cases} |aj \bmod N\rangle & \text{si } j < N \\ |j\rangle & \text{si } N \le j < 2^n \end{cases}.$$

És efectivament una q-computació, ja que l'aplicació $\mathbb{Z}_N \to \mathbb{Z}_N$ tal que $j \mapsto aj \mod N$ és bijectiva. La q-computació inversa és $U_{a^{-1},N}$. Finalment, posem $\boldsymbol{u}_s$, per a cada $s \in \{0, \dots, r-1\}$, per a denotar el q-vector d'ordre n

$$\boldsymbol{u}_s = \sum_{j=0}^{r-1} e^{-2\pi i j \frac{s}{r}} |a^j \bmod N\rangle.$$

Aplicant l'operador U_a a $\boldsymbol{u}_s$, obtenim

$$U_a \boldsymbol{u}_s = \sum_{j=0}^{r-1} e^{-2\pi i j \frac{s}{r}} |a^{j+1} \bmod N\rangle = e^{2\pi i \frac{s}{r}} \boldsymbol{u}_s,$$

la qual cosa significa que $\boldsymbol{u}_s$ és un vector propi de $U_{a,N}$ amb valor propi $e^{2\pi i \frac{s}{r}}$.

En aquest punt podria semblar natural aplicar el q-algorisme de Kitaev per a estimar la fase s/r de $e^{2\pi i \frac{s}{r}}$, amb la idea que la informació obtinguda d'aquesta manera podria ser una bona pista per a trobar r. El problema és que el coneixement del vector propi $\boldsymbol{u}_s$ pressuposa el coneixement de r. Sortosament, aquest problema es pot eludir observant que

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |\boldsymbol{u}_s\rangle = |\mathbf{1}_n\rangle.$$

En efecte, si en el q-algorisme de Kitaev posem $m = 2n+1+\left\lceil 2 + \frac{1}{2\varepsilon} \right\rceil$, i partim de l'estat inicial $|\mathbf{0}_m\rangle|\mathbf{1}_n\rangle$, aleshores, amb probabilitat $1-\varepsilon$, obtenim una estimació $\tilde{\varphi} \approx s/r$ amb $2n+1$ bits correctes. Amb això,

$$\left| \frac{s}{r} - \tilde{\varphi} \right| \le \frac{1}{2^{2n+1}} \le \frac{1}{2r^2}$$

i posant $s/r = s'/r'$ amb $(s', r') = 1$, la desigualtat

$$\left| \frac{s'}{r'} - \tilde{\varphi} \right| \le \frac{1}{2r'^2}$$

8 ϕ denota l'indicador d'Euler, és a dir, el nombre d'enters positius $k \in \{1, \dots, N-1\}$ tals que $(k, N) = 1$.

també es compleix. Ara, per un resultat ben conegut de fraccions contínues (vegeu [9]), s'/r' és una convergent de $\widetilde{\varphi}$. Atès que $\widetilde{\varphi}$ és un nombre racional, el seu conjunt de convergents és finit i es pot calcular amb l'algorisme de les fraccions contínues. En resum, l'elecció de m en el procediment d'estimació de fase assegura que, amb probabilitat $1-\varepsilon$, existeix una convergent $\widetilde{\varphi}$ tal que el seu denominador és r si $(s,r)=1$ o un divisor de r si $(s,r)\neq 1$.

Si $(s,r)=1$, llavors r és l'ordre de a. Aquest fet es pot comprovar directament calculant $a^{r_n} \mod N$, on s_n/r_n és una convergent de $\widetilde{\varphi}$. Si $(s,r)\neq 1$, llavors $a^r \bmod N$ és diferent d'1, i cal repetir l'estimació de fase fins a obtenir un r tal que $(s,r)=1$. Amb el teorema dels nombres primers (vegeu [1]), hom pot mostrar que la repetició $O(n)$ vegades dóna una estimació $\widetilde{\varphi}$ que, amb una alta probabilitat, és una convergent s/r que compleix $(s,r)=1$ (▷ **7**).

El nombre de passos del q-algorisme complet és $O\left(n^4\right)$. La part més complexa és la relacionada amb l'algorisme de les fraccions contínues, que té complexitat $O\left(n^3\right)$, i que s'ha de repetir $O(n)$ vegades per a obtenir, amb una alta probabilitat, una convergent s/r tal que $(s,r)=1$.

Amb millores addicionals d'aquestes idees (vegeu [16]), la complexitat es pot reduir fins a $O\left(n^3\right)$.

Determinació de l'ordre amb el q-algorisme de Shor. Sigui a un nombre enter tal que $1<a<N$ i $(a,N)=1$, i $\varepsilon>0$ un nombre real (petit). L'algorisme que es descriu a continuació troba $r=\mathrm{ord}_N(a)$ amb probabilitat $1-\varepsilon$ en un nombre mitjà d'iteracions que és $O(n)$. La complexitat total és $O(n^4)$. L'algorisme ContFrac subministra, donat un nombre racional, la llista dels denominadors de les seves convergents (▷ **8**).

SHOR-ORDER$[a,N,\varepsilon]$

$n=\lceil \log_2(N)\rceil$, $m=2n+1+\log_2\left(2+\frac{1}{2\varepsilon}\right)$

//q-espai de treball: $\boldsymbol{H}^{(m)}\otimes\boldsymbol{H}^{(n)}$

0.	$\to \lvert\mathbf{0}_m\rangle\lvert\mathbf{0}_n\rangle$
1. HADAMARD$[m]$	$\to \rho^m\sum_{j=0}^{2^m-1}\lvert j\rangle\lvert\mathbf{0}_n\rangle$
2. $U_{a,N}$	$\to \frac{\rho^m}{\sqrt{r}}\sum_{s=0}^{r-1}\sum_{j=0}^{2^m-1} e^{2\pi i j\frac{s}{r}}\lvert j\rangle\lvert\boldsymbol{u}_s\rangle$
3. QFT$^\dagger[m]$	$\to \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}\left\lvert\widetilde{s/r}\right\rangle\lvert\boldsymbol{u}_s\rangle$
4. $M=M_{\{1,\ldots,n\}}$	$\to \widetilde{s/r}$
5. ContFrac	$\to D$

6. for $r'\in D$ do
   if $a^{r'} \mod N=1$, return r'
7. return Test fallit

//$r'\mid r$, i $r'=r$ en $O(n)$ iteracions ■

Atès que la condició $r'=r$ es compleix en $O(n)$ iteracions, obtenim l'ordre correcte r amb un temps mitjà que és $O(n^4)$. Aquest és l'algorisme que usem a la propera secció i que denotem per SHOR-ORDER(a,N).

8 q-algorisme de factorització de Shor

Un problema fonamental de la teoria computacional de nombres és la determinació d'un divisor propi d'un nombre enter positiu gran N (problema de factorització). La dificultat d'aquest problema, segons els algorismes clàssics, és la base d'algorismes criptogràfics eficients i emprats profusament [19]. Sorprenentment, existeix un q-algorisme que troba un divisor propi de N en un temps que és polinòmic en $n = \log_2(N)$. La idea clau és reduir el problema de factorització, emprant un procediment conegut, al problema de determinar l'ordre d'un enter positiu mòdul un altre, i aplicar aleshores el q-algorisme SHOR-ORDER estudiat a la secció anterior.

Així, doncs, primer recordem com es redueix el problema de la factorització a un problema de determinar l'ordre d'un nombre enter positiu mòdul un altre.

Factorització basada en el càlcul de l'ordre. Sigui N un nombre enter positiu. Atès que hi ha algorismes clàssics eficients per a decidir si N és la potència d'un nombre primer,[9] podem suposar que N té almenys dos divisors primers distints. També podem suposar que N és senar. Per a factoritzar N, basta saber trobar un divisor propi d de N, ja que aleshores $N = d \cdot (N/d)$ i podem iterar el procediment amb els factors d i N/d.

Ara l'observació principal és que podem obtenir un factor propi de N si podem trobar un nombre enter $x \in \{2, \ldots, N-1\}$ tal que

1. $(x, N) = 1$;
2. $r = \mathrm{ord}_N(x)$ és parell;
3. $x^{r/2} + 1$ no és divisible per N.

En efecte, r és el menor enter positiu tal que $x^r = 1 \bmod N$ (la condició 1 implica que aquest nombre existeix) i, per tant, usant la condició 2, $x^r - 1 = (x^{r/2} - 1)(x^{r/2} + 1)$ és divisible per N. Com que $x^{r/2} - 1$ no és divisible per N, per la definició de r, i $x^{r/2} + 1$ no és divisible per N, per la condició 3, és clar que tot divisor primer de N divideix un dels factors $x^{r/2} - 1$ o $x^{r/2} + 1$. En resulta que o bé $\mathrm{mcd}\,(x^{r/2} - 1, N)$ o bé $\mathrm{mcd}\,(x^{r/2} + 1, N)$ és un divisor propi del nombre N.

Així, doncs, la qüestió s'ha reconduït a trobar un x que satisfaci les condicions 1, 2 i 3. Sorprenentment, això es pot aconseguir escollint x aleatòriament a $\{2, \ldots, N-1\}$. De fet, si resulta que $(x, N) > 1$, llavors $d = (x, N)$ és un divisor propi de N. Altrament, $(x, N) = 1$ i, per tant, $r = \mathrm{ord}_N(x)$ existeix. Però, quines possibilitats tenim que r sigui parell i $x^{r/2} + 1$ no sigui divisible per N? La proposició que segueix ens dóna la resposta que necessitem.

9 Si $N = m^r$, $m > 1$, llavors $r \le \log_2(N)$. Per a cada $r > 1$ que satisfà aquesta condició, posem $m = \left\lfloor N^{1/r} \right\rfloor$ i comprovem si $m^r = N$. Si la igualtat es compleix, N és una potència de m i la factorització de N es redueix a la factorització de m. Altrament, N no és potència d'un nombre enter i, per tant, tampoc és potència d'un nombre primer.

PROPOSICIÓ 8.1. *Si N és un nombre enter positiu amb $m \geq 2$ factors primers diferents, llavors la densitat a $\mathbb{Z}_N^*$ del conjunt*

$$\{x \in \mathbb{Z}_N^* \mid r = \mathrm{ord}_N(x) \text{ és parell i } x^{r/2} + 1 \text{ no és divisible per } N\}$$

és més gran o igual que $1 - 1/2^{m-1}$.

PROVA. ▷ **9**. □

EXEMPLE 8.2. Considerem el nombre $N = 904\,279$, que és senar i no és potència d'un nombre primer. Escollim aleatòriament $x \in \{1, \ldots, N-1\}$ (podem pensar que és el valor d'una crida random(N)). Posem $x = 743\,579$. Comprovem que $(x, N) = 1$ (gcd(x,N)→1), de manera que $r = \mathrm{ord}_N(x)$ existeix. Ara order(x,N) ens dóna $r = 150\,396$. És un nombre parell i $(x^{r/2} - 1, N)$ ens proporciona el divisor 907, que és primer, i $(x^{r/2} + 1, N)$, el divisor 997, que també és primer. Finalment, comprovem que $N = 907 \cdot 997$.

El q-algorisme de Shor per a factoritzar nombres enters. Tal com hem explicat a la secció precedent, suposem que $N > 1$ és un nombre enter senar que no és potència d'un nombre primer.

SHOR-FACTOR[N]
x, r, d
1. random(N) → x
2. if $d = (x, N) > 1$, return d
3. SHOR-ORDER(x, N) → r
4. if $r \equiv 1 \bmod 2$, goto 1.
5. if $d = \left(x^{\frac{r}{2}} - 1, N\right) > 1$ return d
6. if $x^{\frac{r}{2}} + 1 \bmod N = 0$, goto 1.
7. return $d = \left(x^{\frac{r}{2}} + 1, N\right)$ ∎

La complexitat de SHOR-FACTOR depèn de la del pas 3, de manera que el cost mitjà total és $O(n^4)$, $n = \log_2(N)$.

Una anàlisi més detallada (▷ **10**) mostra que el nombre mitjà de goto en els passos 4 i 6 és $O(1)$.

9 Interpretació física

En aquesta secció expliquem quin és el contrapunt físic de les q-computacions. Per a aprofundir en la comprensió d'aquests aspectes físics, vegeu, per exemple, [21, 12, 24].

1. Estats quàntics. Un sistema quàntic Σ té associat un *espai vectorial complex E* dotat d'un producte escalar hermític $\langle \boldsymbol{x} | \boldsymbol{y} \rangle$ (és a dir, lineal en $\boldsymbol{y}$ i lineal-conjugat

en $\boldsymbol{x}$). Per als propòsits de la computació quàntica, podem suposar que E té dimensió finita.

Els vectors no nuls $\boldsymbol{x} \in E$ representen *estats* (purs) de Σ, i dos vectors no nuls $\boldsymbol{x}, \boldsymbol{y} \in E$ representen el mateix estat si i només si existeix $\xi \in \mathbb{C}$ tal que $\boldsymbol{y} = \xi \boldsymbol{x}$. En particular, qualsevol estat es pot representar per un vector unitari $\boldsymbol{u}$ determinat tret d'un factor $e^{i\alpha}$ (*factor de fase* o *fasor*). Podem, doncs, dir que l'espai d'estats (purs) de Σ és l'*espai projectiu* associat a E i que usualment es denota per $\mathbf{P}E$.

Seguint les notacions de Dirac, escrivim $|\boldsymbol{u}\rangle$ per a designar l'estat corresponent a $\boldsymbol{u}$ (en geometria projectiva se sol denotar per $[\boldsymbol{u}]$). Si $\boldsymbol{v} \in E$ és arbitrari, però no nul, tenim $|\boldsymbol{v}\rangle = |\hat{\boldsymbol{v}}\rangle$, on $\hat{\boldsymbol{v}}$ és el vector unitari $\boldsymbol{v}/|\boldsymbol{v}|$.

Superposició quàntica. Donats dos estats $|\boldsymbol{u}\rangle$ i $|\boldsymbol{u}'\rangle$, i nombres complexos a i a', podem formar l'estat $|a\boldsymbol{u} + a'\boldsymbol{u}'\rangle$, del qual es diu que és una *superposició quàntica* dels estats $|\boldsymbol{u}\rangle$ i $|\boldsymbol{u}'\rangle$ i que sovint denotem, amb un abús ben clar de notació, per $a|\boldsymbol{u}\rangle + a'|\boldsymbol{u}'\rangle$. Aquest abús resulta innocu, ja que, en tots els casos en què el cometem, els vectors $\boldsymbol{u}$ i $\boldsymbol{u'}$ són explícits. En termes geomètrics, les superposicions de $|\boldsymbol{u}\rangle$ i $|\boldsymbol{u}'\rangle$ són els punts de la recta determinada per $|\boldsymbol{u}\rangle$ i $|\boldsymbol{u}'\rangle$.

2. Observables. Un *observable* de Σ és una aplicació lineal $A\colon E \to E$ autoadjunta ($A^\dagger = A$), la qual cosa vol dir que compleix

$$\langle A\boldsymbol{x}|\boldsymbol{y}\rangle = \langle \boldsymbol{x}|A\boldsymbol{y}\rangle,$$

qualssevol que siguin $\boldsymbol{x}, \boldsymbol{y} \in E$, ja que $A^\dagger$ és l'aplicació lineal definida per la relació

$$\langle A^\dagger\boldsymbol{x}|\boldsymbol{y}\rangle = \langle \boldsymbol{x}|A\boldsymbol{y}\rangle.$$

Si (a_{ij}) denota la matriu de A respecte d'una base ortonormal, és immediat comprovar que A és autoadjunta si i només si $a_{ji} = \bar{a}_{ij}$, és a dir, si i només si la matriu és autoadjunta.

Si $a_1, \ldots, a_r$ són els valors propis diferents de A, aleshores $a_1, \ldots, a_r \in \mathbb{R}$ i

$$A = \sum_j a_j P_j, \tag{3}$$

on $P_j\colon E \to E_j$ és la projecció ortogonal de E sobre l'espai de vectors propis de A amb valor propi a_j, això és

$$E_j = \{\boldsymbol{x} \in E \mid A\boldsymbol{x} = a_j\boldsymbol{x}\}.$$

El resultat d'una *observació* o *mesura* de A, quan l'estat de Σ és $|\boldsymbol{u}\rangle$, és un valor propi a_j, amb probabilitat

$$p_j = \left|P_j\boldsymbol{u}\right|^2 = \langle \boldsymbol{u}|P_j\boldsymbol{u}\rangle,$$

i, ensems, és la mutació de l'estat de Σ a l'estat $P_j\boldsymbol{u}$ (o, més precisament, a $|P_j\boldsymbol{u}\rangle$). Adonem-nos que $\boldsymbol{u} = \sum_j P_j\boldsymbol{u}$ i, per tant,

$$1 = |\boldsymbol{u}|^2 = \sum_j \left|P_j\boldsymbol{u}\right|^2 = \sum_j p_j,$$

ja que els E_j són dos-a-dos ortogonals. Fixem-nos també que

$$\langle \boldsymbol{u}|P_j\boldsymbol{u}\rangle - \left|P_j\boldsymbol{u}\right|^2 = \langle \boldsymbol{u}|P_j\boldsymbol{u}\rangle - \langle P_j\boldsymbol{u}|P_j\boldsymbol{u}\rangle = \langle \boldsymbol{u} - P_j\boldsymbol{u}|P_j\boldsymbol{u}\rangle = 0,$$

atès que $\boldsymbol{u} - P_j\boldsymbol{u}$ és ortogonal a E_j per definició de P_j. En particular, si $\boldsymbol{u} \in E_j$, llavors l'observació subministra a_j amb certesa i Σ roman en l'estat $|\boldsymbol{u}\rangle$.

EXEMPLE 9.1. Si F és subespai de E, la projecció ortogonal $P_F\colon E \to F$ és un observable amb valors propis 1 i 0: $E_1 = F$ i $E_0 = F^\dagger$. Els observables d'aquesta mena s'anomenen *proposicions* o *eventualitats*. La probabilitat d'observar 1, si el sistema es troba en l'estat $\boldsymbol{u} \in E$, és $|P_F(\boldsymbol{u})|^2$.

REMARCA 9.2. La fórmula (3) mostra que tot observable és una combinació lineal, amb coeficients reals (els valors a_j) d'eventualitats (la projecció P_{a_j} és l'eventualitat corresponent a l'espai $E_j = E_{a_j}$). Vist així, un observable es pot identificar amb la llista de parells $\{(a_1, E_1), \ldots, (a_r, E_r)\}$, on $a_1, \ldots, a_r \in \mathbb{R}$ (els valors possibles de l'observable) i on $E_1, \ldots, E_r \subseteq E$ són subespais vectorials de E tals que $E = E_1 \oplus \cdots \oplus E_r$ i $E_j \perp E_k$ per a $j \neq k$. Els vectors no nuls de E_j representen estats per als quals el valor mesurat és a_j amb certesa, mentre que els vectors no nuls de l'espai ortogonal $E_j^\perp = \oplus_{k\neq j} E_k$ representen estats per als quals el valor mesurat és $\neq a_j$ amb certesa. Notem que la probabilitat d'obtenir a_j coincideix amb la probabilitat d'observar 1 per a l'eventualitat definida per E_j.

3. Dinàmica unitària. Si Σ està en un ambient no reactiu (és a dir, que l'ambient no és afectat per Σ) en l'interval $[0, t]$, existeix un operador unitari

$$U\colon E \to E$$

tal que

$$\boldsymbol{b} = U\boldsymbol{a}$$

representa l'estat de Σ en el temps t, si $\boldsymbol{a} \in E$ representa l'estat de Σ en el temps 0.

EXEMPLE 9.3. Si H és un observable, l'operador

$$U = e^{iHt}$$

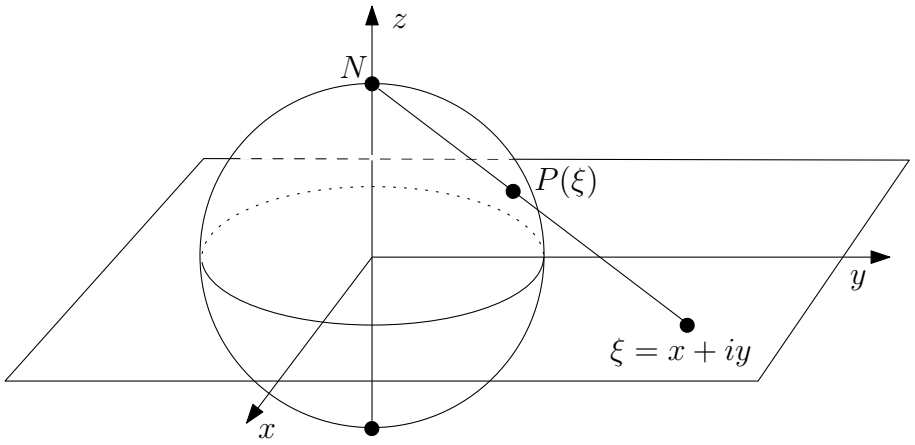
és unitari, ja que $U^\dagger = e^{-iH^\dagger t} = e^{-iHt} = U^{-1}$. És costum dir que $U = e^{iHt}$ és l'evolució temporal definida pel *hamiltonià* H.

4. Entrellaçament. Si Σ' és un segon sistema quàntic i el seu espai associat és E', aleshores l'espai associat al sistema conjunt $\Sigma + \Sigma'$ és $E \otimes E'$, amb el producte escalar hermític definit per la relació

$$\langle \boldsymbol{x} \otimes \boldsymbol{x}' | \boldsymbol{y} \otimes \boldsymbol{y}' \rangle = \langle \boldsymbol{x} | \boldsymbol{y} \rangle \cdot \langle \boldsymbol{x}' | \boldsymbol{y}' \rangle.$$

Si $\boldsymbol{u} \in E$ i $\boldsymbol{u}' \in E'$ són vectors unitaris, l'estat $|\boldsymbol{u} \otimes \boldsymbol{u}'\rangle$ també es denota per $|\boldsymbol{u}\rangle|\boldsymbol{u}'\rangle$, o simplement $|\boldsymbol{u}\boldsymbol{u}'\rangle$, i el mirem com l'estat del sistema conjunt corresponent a l'estat $|\boldsymbol{u}\rangle$ de Σ i $|\boldsymbol{u}'\rangle$ de Σ'. D'aquests estats, en diem *estats compostos*. És important observar que els estats del sistema conjunt no són en general estats compostos. Un exemple simple és $|\boldsymbol{u}_1 \otimes \boldsymbol{u}_1'\rangle + |\boldsymbol{u}_2 \otimes \boldsymbol{u}_2'\rangle$ si $\boldsymbol{u}_1, \boldsymbol{u}_2 \in E$ (respectivament $\boldsymbol{u}_1', \boldsymbol{u}_2' \in E'$) són vectors ortogonals unitaris (▷ **11**). Tanmateix tot estat del sistema conjunt és superposició d'estats compostos (tot vector de $E \otimes E'$ és una suma de vectors composots), i és per això que dels estats no compostos en diem *estats entrellaçats*.

EXEMPLE 9.4 (q-bits). Els estats d'una partícula d'espín $\frac{1}{2}$ (sistema $\Sigma^{(1)}$) es poden pensar com a punts de l'esfera S^2 de radi 1 (en unitats apropiades) i resulta que l'espai complex associat a aquest sistema, d'acord amb l'axioma 1 (estats quàntics), és $\mathbb{C}^2$ (*espai d'espinors*). Aquesta afirmació es pot justificar amb els arguments que segueixen.



- Identifiquem $\xi = x + iy \in \mathbb{C}$ amb el punt $(x, y, 0) \in \mathbb{R}^3$ i considerem el punt $P = P(\xi)$ de l'esfera

$$S^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$$

obtingut per la projecció estereogràfica amb centre $N = (0, 0, 1)$:

$$P = \left(\frac{2x}{x^2 + y^2 + 1}, \frac{2y}{x^2 + y^2 + 1}, \frac{x^2 + y^2 - 1}{x^2 + y^2 + 1} \right).$$

Posant $P(\infty) = N$, obtenim una bijecció entre $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ i S^2. L'aplicació inversa és

$$(x, y, z) \mapsto \frac{x}{1-z} + i\frac{y}{1-z}, \text{ per } z < 1,$$

i, per a $z = 1$, $N = [0, 0, 1] \mapsto \infty$.

- Per altra banda també tenim

$$\hat{\mathbb{C}} \simeq \mathbf{P}\mathbb{C}^2 = \mathbf{P}^1_{\mathbb{C}},$$

ja que qualsevol element $[\xi_0, \xi_1] \in \mathbb{C}^2$ és proporcional a un únic vector de la forma $[1, \xi]$ si $\xi_0 \neq 0$, i a $[0, 1]$ si $\xi_0 = 0$. Tenim, doncs, una aplicació bijectiva

$$\hat{\mathbb{C}} \to \mathbf{P}^1_{\mathbb{C}}, \quad \xi \mapsto [1, \xi], \quad \infty \mapsto [0, 1].$$

L'aplicació inversa és

$$[\xi_0, \xi_1] \mapsto \begin{cases} \xi = \xi_1/\xi_0 & \text{si } \xi_0 \neq 0 \\ \infty & \text{si } \xi_0 = 0 \end{cases}.$$

Aquestes consideracions indiquen que podem prendre $\mathbb{C}^2$ com l'espai associat a $\Sigma^{(1)}$.

REMARCA 9.5. L'esfera S^2, amb l'estructura de $\mathbf{P}^1_{\mathbb{C}}$, es coneix com a *esfera de Riemann*. És la més simple de les superfícies de Riemann compactes (és l'única que és simplement connexa), però en referències de computació quàntica és costum dir-ne *esfera de Bloch* o fins i tot *esfera de Poincaré–Bloch*.

REMARCA 9.6. Sigui $P = (x, y, z)$ un punt de S^2 i definim φ com l'argument de $x + iy$ i θ com l'angle entre OP i ON, on O és el centre de l'esfera. La relació entre les coordenades esfèriques (φ, θ) i les coordenades cartesianes (x, y, z) està donada per les fórmules

$$x = \sin\theta\cos\varphi, \quad y = \sin\theta\sin\varphi, \quad z = \cos\theta. \tag{4}$$

El punt de $\hat{\mathbb{C}}$ corresponent a $P(x, y, z)$ és

$$\xi = \frac{x}{1-z} + i\frac{y}{1-z} = \frac{\sin\theta\cos\varphi}{1-\cos\theta} + i\frac{\sin\theta\sin\varphi}{1-\cos\theta} = \frac{\sin\theta}{1-\cos\theta}e^{i\varphi} = e^{i\varphi}\cot\tfrac{\theta}{2}.$$

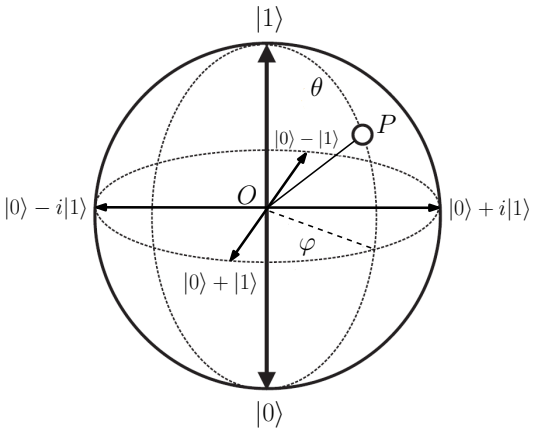
Com que aquest punt correspon a

$$[1, e^{i\varphi}\cot\tfrac{\theta}{2}] \sim [e^{-i\varphi/2}\sin\tfrac{\theta}{2}, e^{i\varphi/2}\cos\tfrac{\theta}{2}] \in \mathbf{P}^1_{\mathbb{C}},$$

la conclusió és que

$$\boldsymbol{p} = e^{-i\varphi/2}\sin\tfrac{\theta}{2}|0\rangle + e^{i\varphi/2}\cos\tfrac{\theta}{2}|1\rangle \in \mathbf{P}^1_{\mathbb{C}} \tag{5}$$

és el punt corresponent a P segons la identificació $S^2 \simeq \mathbf{P}^1_{\mathbb{C}}$. El gràfic que segueix il·lustra aquesta relació i mostra alguns casos especials (llevat d'un factor de normalització).



REMARCA 9.7. La fórmula (5) mostra que $R_z(\alpha)(\boldsymbol{p})$ correspon a $\rho_z(\alpha)(P)$, on $\rho_z(\alpha)$ denota la rotació d'eix Oz i amplitud α. Això és un cas especial d'una relació ben coneguda entre matrius $U \in S\boldsymbol{U}^{(1)}$ i rotacions de S^2. Aquesta relació es pot explicar com segueix.

Una matriu $U = \left[\begin{smallmatrix} u_0 & u_1 \\ -\bar{u}_1 & \bar{u}_0 \end{smallmatrix}\right] \in S\boldsymbol{U}^{(1)}$ es pot veure com una aplicació lineal $\mathbb{C}^2 \to \mathbb{C}^2$: $\left[\begin{smallmatrix} \xi_0 \\ \xi_1 \end{smallmatrix}\right] \mapsto U \left[\begin{smallmatrix} \xi_0 \\ \xi_1 \end{smallmatrix}\right]$. Aquesta aplicació indueix una aplicació projectiva de $\mathbf{P}^1_{\mathbb{C}}$ en sí mateix

$$[\xi_0, \xi_1] \mapsto [u_0\xi_0 + u_1\xi_1, -\bar{u}_1\xi_0 + \bar{u}_0\xi_1]$$

i, per tant, una aplicació $\hat{U}\colon \hat{\mathbb{C}} \to \hat{\mathbb{C}}$,

$$\xi \mapsto \frac{\bar{u}_0\xi - \bar{u}_1}{u_1\xi + u_0}, \quad \infty \mapsto \bar{u}_0/u_1.$$

Al seu torn, aquesta aplicació indueix l'aplicació $\widetilde{U}\colon S^2 \to S^2$ tal que $\widetilde{U}\,(P(\xi)) = P\left(\hat{U}\xi\right)$.

Si ara prenem com U una de les matrius

$$R_z(\varphi) = \begin{bmatrix} e^{-i\varphi/2} & 0 \\ 0 & e^{i\varphi/2} \end{bmatrix},\ R_y(\theta) = \begin{bmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ -\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix},\ R_x(\psi) = \begin{bmatrix} \cos\frac{\psi}{2} & -i\sin\frac{\psi}{2} \\ -i\sin\frac{\psi}{2} & \cos\frac{\psi}{2} \end{bmatrix}$$

(vegeu la secció 2, p. 191), resulta que

$$\rho_z(\varphi) = \widetilde{R_z(\varphi)}, \quad \rho_y(\theta) = \widetilde{R_y(\theta)} \quad \text{i} \quad \rho_x(\psi) = \widetilde{R_x(\psi)}$$

són les rotacions d'amplitud φ, θ i ψ i eixos z, y i x, respectivament. Això, junt amb les relacions

$$\boldsymbol{p} = e^{-\varphi/2}\sin\tfrac{\theta}{2}|0\rangle + e^{\varphi/2}\cos\tfrac{\theta}{2}|1\rangle = R_z(\varphi)R_y(\theta)|1\rangle,$$

mostra que, en termes de S^2, és

$$P = \rho_z(\varphi)\rho_y(\theta)N,$$

una relació consistent amb el contingut geomètric de les definicions de φ i θ. Inversament, aquesta relació, junt amb la interpretació de R_z i R_y, forneix una prova de l'expressió de $\boldsymbol{p}$ donada.

EXEMPLE 9.8 (q-registres). Per l'axioma 4 (entrellaçament) i la fórmula $\boldsymbol{H}^{(n)} \simeq \boldsymbol{H}^{(1)} \otimes \cdots \otimes \boldsymbol{H}^{(1)}$, l'espai $\boldsymbol{H}^{(n)}$ és l'espai associat a $\Sigma^{(n)} = \Sigma^{(1)} + \cdots + \Sigma^{(1)}$ (n sumands), el sistema compost de n q-bits. Per analogia amb els registres de bits clàssics, en diem un *q-registre* d'ordre n.

Ara l'axioma 3 (dinàmica unitària) ens diu que l'evolució temporal de $\Sigma^{(n)}$ està donada per una matriu unitària d'ordre 2^n. En altres paraules, l'evolució temporal de $\Sigma^{(n)}$ és una q-computació.

Finalment, l'axioma 2 (observables) indica que l'operació [opcional] $\mathrm{M}(\boldsymbol{b})$ al final dels q-programes correspon a l'operació de mesurar l'observable (diagonal) L tal que

$$L|k\rangle = k|k\rangle \text{ per a tot } k$$

quan l'estat de $\Sigma^{(n)}$ és $|\boldsymbol{b}\rangle$. Notem que $\left(\boldsymbol{H}^{(n)}\right)_j = \mathbb{C}|j\rangle$, d'on $P_j\boldsymbol{b} = b_j|j\rangle$ i $p_j = \left|b_j\right|^2$.

Computadors quàntics

De les observacions precedents es desprèn que, per a efectuar q-programes d'ordre n en un suport físic, és suficient disposar d'un registre quàntic i «implementacions» de les operacions

$M(\boldsymbol{b})$
$R_j(U)$ [amb $U \in \{H, U_{\pi/2}, U_{\pi/4}\}$ en el cas restringit]
$C_{j,k}$.

Un *computador quàntic* (d'ordre n) és un registre quàntic $\Sigma^{(n)}$ dotat d'aquestes implementacions. La seva significació principal rau en el fet que permet efectuar [o aproximar] qualsevol q-computació.

Una característica interessant d'un computador quàntic és que incorpora l'anomenat *paral·lelisme quàntic*. Es tracta de la possibilitat d'inicialitzar-lo en estats com ara el q-vector d'Hadamard

$$\boldsymbol{h}^{(n)} = \frac{1}{\sqrt{2^n}}\left(|0\rangle + |1\rangle + \cdots |2^n - 1\rangle\right),$$

del qual podem dir que:

- Conté (de fet, és una suma normalitzada de) tots els nombres de n bits, per tant,
- Qualsevol operació del computador quàntic actua sobre tots els nombres simultàniament. Això «explica» per què el computador quàntic pot ser molt més ràpid que un computador clàssic.
- En general, la utilitat dels algorismes (com ara el de Shor per a trobar l'ordre d'un nombre enter mòdul un altre) es basa en el fet que, després de la seva execució, les amplituds dels nombres «útils» són altes i la resta són petites.

També és oportú esmentar el «problema de la decoherència», que sorgeix pel fet que les interaccions amb l'entorn poden «pertorbar» ràpidament els estats de $\Sigma^{(n)}$ (entrellaçament incontrolat entre els estats de l'entorn i els estats de $\Sigma^{(n)}$). Aquests problemes en el camí envers la construcció de computadors quàntics són de natura física i tecnològica. Les recerques en molts laboratoris d'arreu del món estan dirigides a superar aquestes dificultats i el progrés en moltes direccions és continu (▷ **12**).

Més referències

A més de les referències esmentades fins ara, consignem aquí alguns llibres addicionals, per ordre de l'any de publicació, que poden interessar tothom que desitgi aprofundir en l'estudi de la computació quàntica o, més generalment, en el processament de la informació quàntica: [18], [13, 14], [20], [3, 4], [15], [10], [2].

Un tema relacionat, en certa manera a mig camí entre la computació clàssica i la quàntica, és el de la simulació quàntica. Algunes referències actuals són [6], [23], [22] (amb una magnífica introducció de J. Ignacio Cirac i Peter Zoller titulada «Goals and opportunities in quantum simulations») i [25].

10 Remarques i demostracions

► **1** (p. 185, p. 195)**.** És un fet ben conegut que tota computació clàssica es pot realitzar amb una successió finita de *portes lògiques* que són o bé NOT actuant sobre un bit arbitrari o bé NAND actuant sobre dos bits qualssevol.[10] És, doncs, suficient inserir NAND en una computació reversible f. Això es pot aconseguir amb $f\colon \boldsymbol{B}^3 \to \boldsymbol{B}^3$ definida com l'aplicació que intercanvia 110 i 111 i altrament és la identitat. En efecte, mirant els quatre vectors binaris x que acaben amb 1 a la taula de f que segueix,

10 L'observació clau, i fàcil de comprovar, és que qualsevol aplicació $f\colon \boldsymbol{B}^n \to \boldsymbol{B}$ coincideix amb la donada per l'expressió booleana $\sum_{f(x)=1} T_1^{x_1} \cdots T_n^{x_n}$, on les T_j són variables booleanes i on $T_j^{x_j}$ denota T_j si $x_j = 1$ i $\overline{T}_j$ (negació de T_j) si $x_j = 0$. D'això, en resulta que f es pot obtenir combinant NOT, AND i OR. Atès que $\mathrm{OR}(p,q) \equiv \mathrm{NOT}\,(\mathrm{AND}\,(\overline{p},\overline{q}))$, NOT i AND són suficients. Un argument similar mostra que NOT i OR, o NOT i NAND, són també suficients. L'elecció de NAND és una simple qüestió de conveniència per a la nostra presentació.

x	000	**00**1	010	**01**1	100	**10**1	110	**11**1
$f(x)$	000	00**1**	010	01**1**	100	10**1**	111	11**0**

veiem que inclou NAND (bits en negreta). Explícitament, $ij1 \mapsto ij\text{NAND}(i,j) = ij(1+i\cdot j)$.

► **2** (p. 192)**.** Per a la demostració, seguim les indicacions donades a [17, secció 2.2.4]. Usarem les relacions

$$XR_y(\theta)X = R_y(-\theta), \quad XR_z(\varphi)X = R_z(-\varphi).$$

Notem que XM (respectivament MX) intercanvia les files (columnes) de M. L'afirmació es desprèn d'això i de les definicions de $R_y(\theta)$ i $R_z(\varphi)$. Per tant, podem escriure (la φ de la tercera igualtat és un angle auxiliar arbitrari):

$$\begin{aligned} R_z(\beta)R_y(\theta)R_z(\gamma) &= R_z(\beta)R_y(\theta/2)R_y(\theta/2)R_z(\gamma) \\ &= R_z(\beta)R_y(\theta/2)XR_y(-\theta/2)XR_z(\gamma) \\ &= R_z(\beta)R_y(\theta/2)XR_y(-\theta/2)R_z(\varphi)R_z(-\varphi)XR_z(\gamma) \\ &= R_z(\beta)R_y(\theta/2)XR_y(-\theta/2)R_z(\varphi)XR_z(\varphi+\gamma) \\ &= AXBXC \end{aligned}$$

amb

$$A = R_z(\beta)R_y(\theta/2), \quad B = R_y(-\theta/2)R_z(\varphi), \quad C = R_z(\varphi+\gamma).$$

Finalment, atès que $ABC = R_z(2\varphi+\beta+\gamma)$, basta escollir $\varphi = -(\beta+\gamma)/2$, la qual cosa significa que

$$A = R_z(\beta)R_y\left(\tfrac{\theta}{2}\right), \quad B = R_y(-\tfrac{\varphi}{2})R_z\left(-\tfrac{\beta+\gamma}{2}\right), \quad C = R_z\left(\tfrac{\gamma-\beta}{2}\right).$$

► **3** (p. 204)**.** Aquest resultat no s'usa en aquest article, però la seva demostració és un exercici interessant d'àlgebra lineal que esbossem tot seguit.

Sigui $U = [u_{jk}] \in \boldsymbol{U}^{(n)}$ i posem $N = 2^n$. Llavors $U = e^{i\alpha}U_1U_2\cdots U_{N-1}$, amb $\alpha \in \mathbb{R}$ i on $U_l = U_{l,l+1}\cdots U_{l,N}$, amb $U_{l,j}$ un element de $S\boldsymbol{U}^{(1)}$ actuant en el pla $[|l\rangle, |j\rangle]$ de la manera estàndard (és a dir, usant la referència $|l\rangle$ i $|j\rangle$) i deixant fixos tots els $|k\rangle$ per a $k \neq l, j$.

Aquesta expressió de U es pot construir com segueix. Definim $U_{1,2}$ com la identitat si $u_{21} = 0$ o, altrament, com

$$\begin{bmatrix} u_{11}/\lambda & -\bar{u}_{21}/\lambda \\ u_{21}/\lambda & \bar{u}_{11}/\lambda \end{bmatrix}, \quad \lambda = \sqrt{|u_{11}|^2 + |u_{12}|^2},$$

de manera que l'entrada 21 de la matriu $U_{1,2}^\dagger U$ és 0. Definint $U_{1,3}, \ldots, U_{1,N}$ d'una manera similar, aconseguim que les entrades $21, 31, \ldots, n1$ de la matriu

$$U' = U_{1,N}^\dagger \cdots U_{1,2}^\dagger U$$

siguin 0. Atès que U' és unitària, de manera que les seves columnes són ortogonals dues a dues, veiem que les entrades $12, 13, \ldots, 1n$ de la matriu U' també són 0. Essent l'entrada 11 de U' necessàriament un nombre complex unitari, veiem que existeix $\alpha_1 \in \mathbb{R}$ tal que $e^{-i\alpha_1} U_{1,N}^\dagger \cdots U_{1,2}^\dagger U$ té la forma

$$\begin{bmatrix} 1 & \mathbf{0}_n \\ \mathbf{0}_n^\dagger & V \end{bmatrix}, \quad V \in \boldsymbol{U}^{(N-1)}.$$

Ara, per inducció, $V = e^{i\beta} U_2 \cdots U_{N-1}$, amb $\beta \in \mathbb{R}$ i on $U_l = U_{l,l+1} \cdots U_{l,N}$ amb $U_{l,j}$ un element de $S\boldsymbol{U}^{(1)}$ que actua en el pla $[|l\rangle, |j\rangle]$ de la manera estàndard i deixa fixos tots els $|k\rangle$ per $k \neq l, j$. Finalment, l'afirmació queda provada definint $\alpha = \alpha_1 + \beta$ i $U_1 = U_{1,2} U_{1,3} \cdots U_{1,N}$. Notem que el nombre de les $U_{l,j}$ diferents de la identitat és com a molt $N(N-1)/2$.

Per a completar la demostració basta adonar-se que a l'exemple 4.6 hem establert que les $U_{l,j}$ es poden expressar com a producte de portes U i $N_{r,s}$.

► **4** (p. 204)**.** Us remetem a la secció 4.5.3 de [16], on podeu trobar un esbós de la prova. Tanmateix fins i tot en aquesta obra enciclopèdica es diu que fornir tots els detalls «is a little beyond our scope» (p. 198). Trobareu una demostració més completa, que inclou els detalls matemàtics més subtils, a [17, Lemma 3.1.8], com ara una demostració completa del fet clau següent: si $\cos\alpha = \cos^2(\pi/8)$, llavors α/π és irracional.

► **5** (p. 208)**.** Com que $\mu(\boldsymbol{a}) = \frac{1}{N}\frac{N-M}{\sqrt{N-M}} = \sqrt{N-M}/N$,

$$\begin{aligned} K(\boldsymbol{a}) &= \sum_{j\in J_0} (2\sqrt{N-M}/N - 1/\sqrt{N-M})|j\rangle + \sum_{j\in J_1} \frac{2\sqrt{N-M}}{N}|j\rangle \\ &= \sum_{j\in J_0} \frac{N-2M}{N\sqrt{N-M}}|j\rangle + \sum_{j\in J_1} \frac{2\sqrt{M}\sqrt{N-M}}{N\sqrt{M}}|j\rangle \\ &= \cos(\varphi)\boldsymbol{a} + \sin(\varphi)\boldsymbol{b}. \end{aligned}$$

Anàlogament, com que $\mu(\boldsymbol{v}) = M/N\sqrt{M} = \sqrt{M}/N$,

$$\begin{aligned} K(\boldsymbol{b}) &= \sum_{j\in J_0} \left(\frac{2\sqrt{M}}{N}\right)|j\rangle + \sum_{j\in J_1} \left(\frac{2\sqrt{M}}{N} - \frac{1}{\sqrt{M}}\right)|j\rangle \\ &= \sum_{j\in J_0} \left(\frac{2\sqrt{M}\sqrt{N-M}}{N}\frac{1}{\sqrt{N-M}}\right)|j\rangle + \sum_{j\in J_1} \left(\frac{2M-N}{N\sqrt{M}}\right)|j\rangle \\ &= \sin(\varphi)\boldsymbol{a} - \cos(\varphi)\boldsymbol{b}. \end{aligned}$$

Observem que les dues relacions precedents impliquen que K és, en el pla generat per $\boldsymbol{a}$ i $\boldsymbol{b}$, la reflexió respecte de $\boldsymbol{h}^{(n)} = \cos(\varphi/2)\boldsymbol{a} + \sin(\varphi/2)\boldsymbol{b}$.

En efecte, sigui $\boldsymbol{u}_\alpha = \cos(\alpha)\boldsymbol{a} + \sin(\alpha)\boldsymbol{b}$ (així $\boldsymbol{h}^{(n)} = \boldsymbol{u}_{\varphi/2}$) i posem R_φ per a denotar la rotació d'amplitud φ. Aleshores, $K = R_\varphi G$ (ja que $KG = R_\varphi$ i $G^2 = \mathrm{Id}$) i

$$K(\boldsymbol{h}^{(n)}) = R_\varphi(G(\boldsymbol{u}_{\varphi/2})) = R_\varphi(\boldsymbol{u}_{-\varphi/2}) = \boldsymbol{u}_{\varphi/2} = \boldsymbol{h}^{(n)},$$

mentre que si $\boldsymbol{k}^{(n)} = -\sin(\varphi/2)\boldsymbol{a} + \cos(\varphi/2)\boldsymbol{b} = \boldsymbol{u}_{\varphi/2+\pi/2}$, llavors

$$\begin{aligned} K(\boldsymbol{k}^{(n)}) &= R_\varphi G R_{\pi/2}\boldsymbol{u}_{\varphi/2} = R_\varphi R_{-\pi/2} G\boldsymbol{u}_{\varphi/2} \\ &= R_{\varphi-\pi/2}\boldsymbol{u}_{-\varphi/2} = \boldsymbol{u}_{\varphi/2-\pi/2} = -\boldsymbol{k}^{(n)}. \end{aligned}$$

► **6** (p. 213)**.** La probabilitat $p(|2^m\varphi - l| > 2^{m-r})$ és igual a

$$\sum_{l=-2^{m-1}+1}^{-(2^{m-r}+1)} p_l + \sum_{l=(2^{m-r}+1)}^{2^{m-1}} p_l.$$

Ara la fita de Kitaev (∗∗), p. 213, es pot deduir de l'expressió explícita (∗) de p_l (p. 213). Per a més detalls, vegeu [16].

► **7** (p. 215)**.** El teorema dels nombres primers afirma que la quantitat de nombres primers inferiors a un nombre real r és asimptòticament igual a $\frac{r}{\log(r)}$. D'aquí que la probabilitat p d'escollir (uniformement) un nombre primer s a l'atzar, $0 < s < r$ és asimptòticament igual a

$$p(0 < s < r, s \text{ és primer}) \sim \frac{1}{\log r} > \frac{1}{\log N}.$$

En resulta que el nombre esperat d'iteracions per tal de trobar un nombre primer $s < r$ és

$$\sum_{i=1}^{\infty} i(1-p)^{i-1}p = p\sum_{i=1}^{\infty} i(1-p)^{i-1} = \frac{p}{(1-(1-p))^2} = \frac{1}{p} \sim \log(r) < \log(N).$$

Per tant, esperem trobar un nombre primer s, $s < n$, amb $\log(N) = O(n)$ iteracions.

► **8** (p. 215)**.** La representació en fracció contínua d'un nombre racional x és un vector de nombres enters $[x_0, x_1, \ldots, x_n]$, amb $x_j > 0$ per a $j = 1, \ldots, n$. És costum representar la relació entre x i $[x_0, x_1, \ldots, x_n]$ en forma de «fracció contínua»:

$$x = x_0 + \cfrac{1}{x_1 + \cfrac{1}{\ddots \\ x_{n-1} + \cfrac{1}{x_n}}}.$$

Per abús de notació, també escrivim $x = [x_0, x_1, \ldots, x_n]$. D'aquesta manera, la fracció contínua es pot expressar recursivament per la fórmula

$$[x_0, x_1, \ldots, x_n] = x_0 + \frac{1}{[x_1, \ldots, x_n]}.$$

Dels nombres racionals $c_j = [x_0, x_1, \ldots, x_j]$, $j = 0, 1, \ldots, n$, en diem (fraccions) convergents del nombre x. La llista dels denominadors $\{d_0, d_1, \ldots, d_n\}$ d'aquestes convergents es pot calcular recursivament com segueix:

$$d_0 = 1, \quad d_1 = x_1, \quad d_j = x_j d_{j-1} + d_{j-2} \quad (j = 2, \ldots, n).$$

De fet, és fàcil provar per inducció que $c_j = m_j/d_j$, on

$$m_0 = x_0, \quad m_1 = x_1 x_0 + 1, \quad m_j = x_j m_{j-1} + m_{j-2} \quad (j = 2, \ldots, n).$$

En resulta que la llista $\{d_0, d_1, \ldots, d_n\}$ es pot calcular mitjançant l'algorisme següent:

ContFrac(x) :=
  a = terra(x), $j = 1$, $d = \{0, 1\}$
  mentre $x! = a$ fer
    $x = 1/(x - a)$
    a = terra(x)
    $d = d|\{a * d.(j-1) + d.(j-2)\}$
    $j = j + 1$
  retornar cua(d)

► **9** (p. 217)**.** Demostrem que

$$p\left(x \in \mathbb{Z}_N^* \mid r = \mathrm{ord}_N(x) \text{ és senar o } x^{\frac{r}{2}} + 1 \text{ és divisible per } N\right) \geq \frac{1}{2^m}.$$

Comencem escrivint $N = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$, on $p_1, \ldots, p_m$ són nombres primers diferents. Aleshores $\mathbb{Z}_N^* = \mathbb{Z}_{p_1^{\alpha_1}}^* \times \cdots \times \mathbb{Z}_{p_m^{\alpha_m}}^*$. Posem x_j per a denotar la reducció x mod $p_j^{\alpha_j}$, i r_j per a denotar l'ordre de x_j a $\mathbb{Z}_{p_j^{\alpha_j}}^*$. Sigui d_j el major exponent tal que 2^{d_j} divideix r_j i d el major exponent tal que 2^d divideix r. És fàcil veure que si r és senar o si r és parell i $x^{\frac{r}{2}} \equiv -1 \mod N$, llavors $d_j = d$ per a tot j.

Per concloure, usem que si 2^{d_j} és la més gran potència de 2 que divideix $\varphi(p_j^{\alpha_j})$, aleshores

$$p\left(x \in \mathbb{Z}_N^* \mid 2^{d_j} \text{ divideix } \mathrm{ord}_{p_j^{\alpha_j}}(x)\right) = \frac{1}{2}.$$

► **10** (p. 217)**.** Denotem per p la probabilitat de l'esdeveniment

$$\{x \in \mathbb{Z}_N^* \mid r = \mathrm{ord}_N(x) \text{ és parell i } x^{\frac{r}{2}} + 1 \text{ no és divisible per } N\},$$

quan x s'escull (uniformement) a l'atzar a $\mathbb{Z}_N^*$. Llavors, el nombre esperat d'iteracions de l'algorisme és

$$\sum_{i=1}^{\infty} i(1-p)^{i-1}p = p\sum_{i=1}^{\infty} i(1-p)^{i-1} = \frac{1}{p} \leq \frac{2^{m-1}}{2^{m-1}-1} = 1 + \frac{1}{2^{m-1}-1}.$$

Com que $m > 1$, veiem que aquest nombre d'iteracions és $O(1)$.

► **11** (p. 220)**.** Si $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n$ és una base ortonormal de E, i $\boldsymbol{u}'_1, \ldots, \boldsymbol{u}'_{n'}$ una base ortonormal de E', llavors un vector general de l'espai $E \otimes E'$ té la forma $\sum_{j,j'} a_{j,j'} \boldsymbol{u}_j \otimes \boldsymbol{u}_{j'}$. D'altra banda, el vector compost $\boldsymbol{x} \otimes \boldsymbol{x}'$ té la forma

$$\sum_{j,j'} a_j a_{j'} \boldsymbol{u}_j \otimes \boldsymbol{u}_{j'} \text{ si } \boldsymbol{x} = \sum_j a_j \boldsymbol{u}_j \text{ i } \boldsymbol{x}' = \sum_{j'} a_{j'} \boldsymbol{u}_{j'}.$$

Però aquest vector no pot coincidir amb $\boldsymbol{u}_1 \otimes \boldsymbol{u}'_1 + \boldsymbol{u}_2 \otimes \boldsymbol{u}'_2$, ja que de la coincidència es desprendrien les relacions inconsistents

$$a_0 a'_0 = 1, \quad a_1 a'_1 = 1, \quad a_0 a'_1 = 0.$$

► **12** (p. 224)**.** Hi ha una explosió d'activitat en els darrers anys, i especialment des del l'any 2006, com es pot veure, per exemple, a

`http://en.wikipedia.org/wiki/Timeline_of_quantum_computing`
`http://en.wikipedia.org/wiki/Quantum_computer`

En la darrera es consignen, en particular, més d'una dotzena de línies d'investigació dirigides a la realització d'un computador quàntic.

Agraïments

El primer autor ha tingut el suport d'un ajut JAE-DOC de la Junta para la Ampliación de Estudios (CSIC), de l'ajut MTM2011-22851 i del projecte Severo Ochoa SEV-2011-0087 de l'ICMAT.

Referències

[1] APOSTOL, T. M. *Introduction to analytic number theory*. Nova York; Heidelberg: Springer-Verlag, 1976. (Undergraduate Texts in Mathematics)

[2] BENATTI, F.; FANNES, M.; FLOREANINI, R.; PETRITIS, D. (ed). *Quantum information, computation and cryptography. An introductory survey of theory, technology and experiments*. Berlín: Springer-Verlag, 2010. (Lecture Notes in Physics; 808)

[3] BENENTI, G.; CASATI, G.; STRINI, G. *Principles of quantum computation and information. Vol. I: Basic Concepts*. River Edge, NJ: World Scientific Publishing Co., Inc., 2004.

[4] BENENTI, G.; CASATI, G.; STRINI, G. *Principles of quantum computation and information. Vol. II: Basic tools and special topics*. Hackensack, NJ: World Scientific Publishing Co. Pte. Ltd., 2007.

[5] DEUTSCH, D.; JOZSA, R. «Rapid solution of problems by quantum computation». *Proc. Roy. Soc. London Ser. A*, 439 (1992), no 1907, 553–558.

[6] GROTENDORST, J.; MARX, D.; MURAMATSU, A. (ed). *Quantum Simulations of Complex Many-Body Systems: From Theory to Algorithms*. Zeuthen, Alemanya: John von Neumann Institute für Computing (NIC), 2002. (NIC Lecture Notes; 10)

[7] GROVER, L. K. «A fast quantum mechanical algorithm for database search». A: *Proceedings of the Twenty-eighth Annual ACM Symposium on the Theory of Computing* (Filadèlfia, 1996). Nova York: ACM, 1996, 212–219.

[8] GROVER, L. K. «From Schrödinger's equation to the quantum search algorithm». *Amer. J. Phys.*, 69 (7) (2001), 769–777.

[9] HARDY, G. H.; WRIGHT, E. M. *An introduction to the theory of numbers*. 6a ed. Revisada per D. R. Heath-Brown i J. H. Silverman. Oxford: Oxford University Press, 2008.

[10] JAEGER, G. *Quantum information. An overview*. Nova York: Springer, 2007.

[11] KITAEV, A. YU. «Quantum measurements and the Abelian stabilizer problem». *Electronic Colloquium on Computational Complexity (ECCC)*, 3 (1995). 22 p.

[12] KITAEV, A. YU.; SHEN, A. H.; VYALYI, M. N. *Classical and quantum computation*. Providence, RI: American Mathematical Society, 2002. (Graduate Studies in Mathematics; 47)

[13] LOMONACO, S. J., JR. (ed). *Quantum computation: a grand mathematical challenge for the twenty-first century and the millennium*. Lectures presentades a l'American Mathematical Society Short Course (Washington, 17–18 gener 2000). Providence, RI: American Mathematical Society 2002. (Proceedings of Symposia in Applied Mathematics; 58)

[14] LOMONACO, S. J., JR.; BRANDT, H. E. (ed). *Quantum computation and information*. Papers de l'American Mathematical Society Special Session (Washington, 19–21 gener 2000). Providence, RI: American Mathematical Society, 2002. (Contemporary Mathematics; 305)

[15] MERMIN, N. D. *Quantum computer science. An introduction*. Cambridge: Cambridge University Press, 2007.

[16] NIELSEN, M. A.; CHUANG, I. L. *Quantum computation and quantum information*. Cambridge: Cambridge University Press, 2000.

[17] PARTHASARATHY, K. R. *Quantum computation, quantum error correcting codes and information theory*. Nova Delhi: Narosa Publishing House, 2006. [Publicat per al Tata Institute of Fundamental Research, Bombai]

[18] Pittenger, A. O. *An introduction to quantum computing algorithms*. Boston, MA: Birkhäuser Boston, Inc., 2000. (Progress in Computer Science and Applied Logic; 19)

[19] Rivest, R. L.; Shamir, A.; Adleman, L. «A method for obtaining digital signatures and public-key cryptosystems». *Comm. ACM*, 21 (2) (1978), 120–126.

[20] Stolze, J.; Suter, D. *Quantum computing: a short course from theory to experiment*. 2a ed. Weinheim: Wiley-VCH, 2008.

[21] Sudbery, A. *Quantum mechanics and the particles of nature. An outline for mathematicians*. Cambridge: Cambridge University Press, 1988. [reimpressió, amb correccions, de l'edició de 1986]

[22] Trasebinger, A. (ed). *Quantum Simulation*. Nature Physics Insight. Macmillan Publishers Limited, 2012.

[23] Viamontes, G. F.; Markov, I. L.; Hayes, J. P. *Quantum circuit simulation*. Amb un prefaci d'Alfred V. Aho i Krysta M. Svore. Dordrecht: Springer, 2009.

[24] Weinberg, S. *Lectures on quantum mechanics*. Cambridge: Cambridge University Press, 2013.

[25] Will, S. *From Atom Optics to Quantum Simulation*. Springer Theses. Berlín; Heidelberg: Springer, 2013.

Juanjo Rué
Instituto de Ciencias Matemáticas-CSIC
Calle Nicolás Cabrera 13–15
Campus Cantoblanco UAM
28049 Madrid
juanjo.rue@icmat.es

Sebastià Xambó
Matemàtica Aplicada II
Universitat Politècnica de Catalunya
Edifici OMEGA
c/ Jordi Girona 1–3
08034 Barcelona
sebastia.xambo@upc.edu