USC UNIVERSIDADE DE SANTIAGO DE COMPOSTELA
FACULTADE DE MATEMÁTICAS

Traballo Fin de Grao

ELEMENTOS DE CRIPTOGRAFÍA CUÁNTICA

Raquel Alfonso Rodríguez

Setembro 2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

GRAO DE MATEMÁTICAS

Traballo Fin de Grao

ELEMENTOS DE CRIPTOGRAFÍA CUÁNTICA

Raquel Alfonso Rodríguez

Setembro 2024

UNIVERSIDADE DE SANTIAGO DE COMPOSTELA

Traballo proposto

Área de Coñecemento: Álxebra
Título: Elementos de criptografía cuántica
Breve descrición do contido
Trátase de facer unha revisión dos principais conceptos involucrados na criptografía cuántica. Unha posible lista de contidos podería ser: ▪ Introdución á computación cuántica. ▪ Superposición, interferencia e codificación superdensa. ▪ Intercambio seguro de chaves: comparación co caso clásico. ▪ Complexidade dos algoritmos cuánticos comparados cos clásicos. ▪ Exemplos en Qiskit.
Recomendacións
Outras observacións

Índice

Resumo

As comunicacións cuánticas xorden de maneira contemporánea á Teoría da Información clásica, cun maior potencial de computación pero tamén cunha maior desvantaxe de transmisión física. O presente traballo trata da comparación entre estas dúas formas de enviar información, do formalismo matemático detrás da mecánica cuántica, dos protocolos máis relevantes dunha nova criptografía adaptada a este fenómeno e dos primeiros códigos correctores de erros cuánticos.

Resumen

Las comunicaciones cuánticas surgen de manera contemporánea a la Teoría de la Información clásica, con un mayor potencial de computación pero también con una mayor desventaja de transmisión física. El presente trabajo trata de la comparación entre estas dos formas de enviar información, del formalismo matemático detrás de la mecánica cuántica, de los protocolos más relevantes de una nueva criptografía adaptada a este fenómeno y de los primeros códigos correctores de errores cuánticos.

Abstract

Quantum communication spawns contemporaneously to classical Information Theory, with a bigger potential for computations but a handicap when it comes to physical transmission. The present manuscript seeks to compare these two ways of sending information and to present the mathematical formalism behind quantum mechanics, as well as the most relevant protocols of this newly adapted cryptography and the first quantum error correcting codes.

Agradecementos

Debido ao meu peculiar paso por este grao, gustaríame adicarlle brevemente unhas palabras ás persoas que me acompañaron todos estes anos. Para comezar, como non podía ser doutra maneira, ao meu titor Felipe Gago por impartir a asignatura de Códigos Correctores e Criptografía que tanto me interesou e por acoller a idea da mecánica cuántica, bastante alonxada (aínda que non tanto) do departamento de Álxebra, que me permitiu interiorizar os coñecementos adquiridos no grao de Física e unificalos cos aprendidos nesta materia.

Por outro lado, quería agradecer aos meus pais polas súas incontables horas de traballo que me permitiron estar todos estes anos na capital. Aínda que nalgún momento llas puidera retribuír economicamente, nunca poderei compensar o esforzo que fixeron.

Finalmente, aos meus amigos do grao, que aínda que a vida nos levou por camiños moi distintos, seguen a manter o contacto comigo dende fóra de Galicia. A Andrea, Jose, Tamara, Carlos, Gonzalo, María, Manuel e Sandra, grazas por axudarme, tanto académica como moralmente, por confiar en min e por lograr que me divirta, a pesar de todo.

Introdución

En 1948, Shannon publica o seu famoso artigo *A Mathematical Theory of Communication* (Shannon, 1948), co que se considera que deu comezo a teoría da información clásica de hoxe en día. Neste artigo, describe detalladamente en que consiste transmitir información, consegue cuantificala e, máis importante se cabe, pon límites á comunicación clásica.

Case contemporaneamente, nace a última rama da Física: a mecánica cuántica. En 1915 postúlase a teoría xeral da relatividade, dando por fin resposta a moitos fenómenos que as demais ramas non lograran explicar. Custou uns cantos anos formalizar estes novos descubrimentos nanométricos, co incalculable esforzo dos físicos Schrödinger e Heisenberg, aos cales lle debemos o nome dos fenómenos máis coñecidos da cuántica. Non obstante, non foi ata a publicación do artigo de Gordon (1962) que se empezou a empregar esta nova ferramenta como un instrumento de comunicación. Cando aínda os primeiros ordenadores clásicos ocupaban unha parede enteira, xa había quen se atrevía a soñar cun dispositivo capaz de enviar e interpretar fotóns como unidade básica de información, empregando mecanismos de entrelazamento e superposición que aínda non eramos quen de dominar.

Este traballo proponse explicar estes mecanismos agora que temos máis afianzado en que consisten, hai experimentos que os demostran e contamos finalmente cuns aparellos prototípicos capaces de transmitilos.

Comezaremos cunha revisión da información clásica, co concepto do bit e procuraremos explicalo dun xeito que posteriormente resulte análogo á introdución do cúbit, o bit cuántico. Falaremos un pouco das portas lóxicas clásicas e a súa representación matricial para logo pasar aos operadores lóxicos cuánticos. Introduciremos a notación de Dirac, unha nova forma de representar vectores e matrices que propuxo Dirac (1939) para facilitar a comprensión e escritura daquel novo fenómeno cuántico que acababa de xurdir. Continuaremos cos circuítos cuánticos, que dun xeito similar ao caso clásico, pretenden representar os cúbits e as portas que se lles aplican para poder entendelos mellor visualmente. Remataremos a introdución cunhas pinceladas de teoría de información cuántica, pasando polos seus resultados máis importantes: o teorema de non clonación, a teleportación cuántica e a codificación superdensa.

O segundo capítulo trata os protocolos de maior relevancia histórica no ámbito da criptografía. Comeza cunha reseña do algoritmo de Shor, que teoricamente rompe ca seguridade clásica, permitindo unha mellora exponencial no algoritmo de factorización en números primos. Segue co protocolo BB84, o primeiro protocolo de distribución cuántica de chaves segura e sobre o que se basan algúns mecanismos de criptografía cuántica como o caderno de uso único. Para rematar esta sección, estudaremos o protocolo de Kak en tres etapas, o primeiro sistema criptográfico basado unicamente en comunicacións cuánticas, sen axuda de canles clásicas para a transmisión de información adicional.

O derradeiro capítulo fai un percorrido polos primeiros códigos correctores neste ámbito. Ao igual que no caso clásico, as canles de comunicación non están exentas de ruído (perturbacións, interferencias...), polo que fai falla desenvolver uns métodos de seguridade que permitan reter a maior cantidade de información posible. Aparece o primeiro código corrector sobre un cúbit, que corrixe un erro de inversión de bit. A continuación, temos o caso da inversión de fase, un novo tipo de erro que non ten análogo clásico por ser intrínseco á natureza cuántica. Finalmente, tratamos o código de Shor, que corrixe unha mestura destes dous tipos de erros e podemos comprobar como, simplemente corrixindo dous casos, quedamos protexidos contra calquera tipo de erro arbitrario sobre un só cúbit.

Capítulo 1

Introdución á teoría da información cuántica

1.1. Teoría da información clásica

Antes de comezar, faremos un pequeno repaso dos elementos de información clásica para posteriormente poder comparalos cos cuánticos.

1.1.1. O bit

O bit é a unidade básica de información clásica. Trátase dunha variable que pode tomar dous estados $\{0, 1\}$. Valéndonos do sistema binario, podemos codificar a información nun *string* de bits, de xeito que o primeiro bit é o máis significativo e o último, o menos. Por exemplo, o número 5 no sistema decimal escribiríase en binario como

$$110 = 1 \cdot 2^2 + 1 \cdot 2^1 + 2^0.$$

Esta representación seranos de utilidade máis adiante.

1.1.2. As portas lóxicas

Un conxunto completo ou universal de portas lóxicas, ou sexa, coas cales podemos construir calquera outra operación, serían: a identidade, a negación, a porta AND e a porta OR[1].

[1]Existen outros conxuntos máis breves que tamén son universais, por exemplo os operadores {AND, NOT}, dos cales obtemos OR, ou simplemente o operador {NAND} (Moret-Bonillo, 2018).

Identidade. A porta identidade, ou I, é unha función dunha soa variable que non modifica o estado entrante, é dicir

$$I(0) = 0$$
$$I(1) = 1.$$

Negación. A negación, que denotaremos por X, asigna a cada un dos valores o seu oposto

$$X(0) = 1$$
$$X(1) = 0.$$

Nótese que en ambos os anteriores casos as portas lóxicas son reversibles, no senso de que se nos atopamos cun valor de saída 1 e sabemos que se aplicou a porta X, podemos concluír con seguridade que a variable entrante foi un 0. Isto non ocorre coas seguintes portas lóxicas.

AND. A porta AND toma dúas variables de entrada e devolve unha soa de saída como segue

$$\mathrm{AND}(0,0) = 0 \qquad \mathrm{AND}(1,0) = 0$$
$$\mathrm{AND}(0,1) = 0 \qquad \mathrm{AND}(1,1) = 1.$$

OR. A función OR compórtase do seguinte xeito

$$\mathrm{OR}(0,0) = 0 \qquad \mathrm{OR}(1,0) = 1$$
$$\mathrm{OR}(0,1) = 1 \qquad \mathrm{OR}(1,1) = 1.$$

Como adiantabamos antes, nestes casos, ao atoparnos cun resultado de 0 tras aplicar unha porta AND, non temos maneira de adiviñar se o *input* foi $(0,0)$, $(0,1)$ ou $(1,0)$. Estamos ante unha perda de información, consecuencia da irreversibilidade dos operadores lóxicos AND e OR.

Con estas catro portas, podemos construír calquer operador lóxico na teoría da información clásica. Por exemplo, o coñecido operador XOR

$$\mathrm{XOR}(0,0) = 0 \qquad \mathrm{XOR}(1,0) = 1$$
$$\mathrm{XOR}(0,1) = 1 \qquad \mathrm{XOR}(1,1) = 0,$$

non é máis que a actuación combinada de X, AND e OR

$$\mathrm{XOR}(a,b) := \mathrm{OR}(\mathrm{AND}(a, X(b)), \mathrm{AND}(X(a), b)).$$

A continuación, faremos unha presentación dos conceptos e propiedades matemáticas do formalismo cuántico relacionadas coa criptografía cuántica, seguindo as didácticas presentacións de Abers (2004) e Scherer (2019).

1.2. Espazos de Hilbert

Un espazo de Hilbert $\mathcal{H}$ é unha xeralización dun espazo euclídeo a dimensións arbitrarias (incluíndo dimensión infinita). No ámbito do formalismo matemático da mecánica cuántica, empregaremos espazos de Hilbert de dimensión finita sobre o corpo dos números complexos $\mathbb{C}$. Marxinalmente, tamén se empregan espazos de Hilbert de dimensión infinita na física cuántica, mais non na computación cuántica, que é o obxecto do noso estudo, polo que obviaremos describilos.

1.2.1. Notación de Dirac

A notación de Dirac, introducida por Dirac (1939), emprégase a miúdo no ámbito da mecánica cuántica debido á súa fácil lectura á hora de traballar con conxugacións hermíticas en espazos de Hilbert.

Definición 1.1. Un *ket*, denotado por $|\varphi\rangle$, é un vector $\boldsymbol{v} \in \mathcal{H}$ de xeito que $\boldsymbol{v} = |\varphi\rangle$, onde φ é tan só unha etiqueta.

1.2.2. Espazo dual

Definimos o produto interior hermítico como a aplicación

$$\begin{aligned} \mathcal{H} \times \mathcal{H} &\longrightarrow \mathbb{C} \\ (|\chi\rangle, |\varphi\rangle) &\longrightarrow \langle\chi|\varphi\rangle, \end{aligned}$$

que cumpre as propiedades de bilinearidade[2],

$$\langle\chi|\alpha\varphi_1 + \beta\varphi_2\rangle = \alpha\langle\chi|\varphi_1\rangle + \beta\langle\chi|\varphi_2\rangle,$$

hermiticidade[3],

$$\langle\chi|\varphi\rangle = \overline{\langle\varphi|\chi\rangle},$$

e semidefinido positivo,

$$\langle\varphi|\varphi\rangle \geq 0,$$

[2]Abuso de notación: será habitual referirse a $\alpha|\varphi_1\rangle + \beta|\varphi_2\rangle$ como $|\alpha\varphi_1 + \beta\varphi_2\rangle$.

[3]$\overline{\alpha}$ denota o conxugado de $\alpha \in \mathbb{C}$.

con

$$\langle\varphi|\varphi\rangle = 0 \Longleftrightarrow |\varphi\rangle = 0.$$

Grazas a estas propiedades, cúmprese a antilinearidade, de gran relevancia no desenvolvemento do formalismo cuántico,

$$\langle\alpha\chi_1 + \beta\chi_2|\varphi\rangle = \overline{\alpha}\,\langle\chi_1|\varphi\rangle + \overline{\beta}\,\langle\chi_2|\varphi\rangle\,.$$

Para cada vector $|\varphi\rangle \in \mathcal{H}$ existe unha aplicación $f = \langle\chi|$ tal que $\langle\chi|\varphi\rangle \in \mathbb{C}$.

Definición 1.2. Chamaremos *bra* aos elementos do espazo dual f e denotarémolos por $\langle\chi|$.

Vexamos agora a relación entre o espazo dos *bras* e o dos *kets*.

Proposición 1.3. *Sexa V un K-espazo vectorial de dimensión n e sexa $B = \{v_1, v_2, \dots, v_n\}$ unha base de V. Existe unha única base $\widehat{B} = \{f_1, f_2, \dots, f_n\}$ tal que*

$$f_i(v_j) = \delta_{ij},$$

onde δ_{ij} denota a Delta de Kronecker, definida como

$$\delta_{ij} = \begin{cases} 1 & \text{se} \quad i = j \\ 0 & \text{se} \quad i \neq j. \end{cases}$$

Entón, $\widehat{B}$ chámase base dual de B.

Demostración 1.4. Sexa $\mathcal{B} = \{|1\rangle, |2\rangle, \dots, |n\rangle\}$ unha base ortonormal de $\mathcal{H}$. Pola condición de ortonormalidade temos que

$$\langle i|j\rangle = \delta_{ij}.$$

Sexa agora $\widehat{\mathcal{B}} = \{\widehat{|1\rangle}, \widehat{|2\rangle}, \dots, \widehat{|n\rangle}\} = \{\langle 1|, \langle 2|, \dots, \langle n|\}$. Vemos que, facendo actuar os *bras* da base $\widehat{\mathcal{B}}$ sobre os *kets* de $\mathcal{B}$, obtemos

$$\widehat{|i\rangle}\,(|j\rangle) = \langle i|j\rangle = \delta_{ij}.$$

Logo a base $\widehat{\mathcal{B}}$ é a do espazo dual xerado polos elementos da base $\mathcal{B}$. □

Deste xeito, podemos establecer unha relación entre un vector $|\varphi\rangle \in \mathcal{H}$ e o seu conxugado hermítico,

$$\langle\varphi| = \overline{|\varphi\rangle},$$

o cal fai que o espazo dos *bras* se converta no espazo dual dos *kets*.

1.2.3. Representación matricial

Como en todo espazo vectorial, podemos escribir os vectores $|\varphi\rangle \in \mathcal{H}$ en función dos elementos da base B,

$$|\varphi\rangle = \sum_{j=1}^{n} c_j \, |j\rangle \, .$$

Tamén os vectores da base dual $\langle\chi| \in \mathcal{H}$ terán esta expresión,

$$\langle\chi| = \sum_{i=1}^{n} d_i \, \langle i| \, .$$

Desta maneira, ambos admitirán unha representación matricial. Escribiremos os vectores *ket* como vectores columna e os *bra* como filas,

$$|\varphi\rangle = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}, \qquad \langle\chi| = \begin{pmatrix} d_1 & d_2 & \dots & d_n \end{pmatrix},$$

o que permite a fácil computación do produto hermítico como un produto de matrices,

$$\langle\chi|\varphi\rangle = \left(\sum_{i=1}^{n} d_i \, \langle i|\right)\left(\sum_{j=1}^{n} c_j \, |j\rangle\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} d_i c_j \, \langle i|j\rangle = \sum_{i=1}^{n} c_i d_i = \begin{pmatrix} c_1 & c_2 & \dots & c_n \end{pmatrix} \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix}$$

Máis adiante, veremos que os operadores tamén se poderán escribir como matrices e, de feito, será a súa expresión máis habitual á hora de actuar como portas lóxicas cuánticas.

1.3. O cúbit

Unha vez presentados os vectores no espazo de Hilbert, precisamos dunha unidade de información para a nosa teoría da información cuántica. Analogamente ao caso do bit, que podía estar en dous estados, presentamos unha base do espazo de Hilbert de dimensión dous, $\mathcal{B} = \{|0\rangle, |1\rangle\}$. Os vectores deste espazo expresaranse como combinación linear dos vectores base,

$$|q\rangle = \alpha \, |0\rangle + \beta \, |1\rangle \, .$$

Isto é ao que chamamos cúbit. Como podemos observar, o estado do cúbit non se restrinxe ao dun só vector base, senón que se atopa nun estado de superposición entre os dous, dependendo das denominadas amplitudes α e $\beta \in \mathbb{C}$.

Todos os vectores que trataremos de agora en diante estarán normalizados, é dicir,

$$||q|| = \sqrt{\langle q|q\rangle} = 1,$$

o que implica que ao facer a norma do vector $|q\rangle$ cúmprese

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

$|\alpha|^2$ e $|\beta|^2$ serán as probabilidades de atopar o cúbit no estado $|0\rangle$ ou $|1\rangle$, respectivamente. Máis adiante, relacionaremos este concepto co de medida ou colapso do vector de onda cando estudiemos os operadores e proxectores.

1.4. Operadores

Un operador A é unha aplicación linear entre vectores do espazo de Hilbert

$$\begin{aligned} A : \mathcal{H} &\longrightarrow \mathcal{H} \\ |\varphi\rangle &\longrightarrow |A\varphi\rangle . \end{aligned}$$

Como aplicación linear, cumpre as propiedades de linearidade habituais. Sexan $|\varphi_1\rangle , |\varphi_2\rangle \in \mathcal{H}$ e $\lambda_1, \lambda_2 \in \mathbb{C}$, logo

$$|A\left(\lambda_1\varphi_1 + \lambda_2\varphi_2\right)\rangle = \lambda_1 |A\varphi_1\rangle + \lambda_2 |A\varphi_2\rangle .$$

Vexamos que podemos escribir os operadores A en forma matricial. Sexa $|\varphi\rangle$ un vector no espazo de Hilbert $\mathcal{H}$ con base $\mathcal{B} = \{|1\rangle , |2\rangle , \dots , |n\rangle\}$. Logo $|\varphi\rangle$ pode expresarse en función dos vectores base como

$$|\varphi\rangle = \sum_{i=1}^{n} c_i |i\rangle .$$

Se agora facemos actuar A sobre este vector, aplicando a propiedade de linearidade anterior,

$$|A\varphi\rangle = \sum_{i=1}^{n} c_i |Ai\rangle .$$

Por outra banda, $|A\varphi\rangle$ é un vector de $\mathcal{H}$ que admite tamén a súa representación sobre a base $\mathcal{B}$,

$$|A\varphi\rangle = \sum_{j=1}^{n} d_j |j\rangle .$$

Recompilando estas dúas expresións,

$$|A\varphi\rangle = \sum_{i=1}^{n} c_i |Ai\rangle = \sum_{j=1}^{n} d_j |j\rangle .$$

Se agora multiplicamos escalarmente polo elemento dual $\langle k|$ da base $\mathcal{B}$,

$$\sum_{i=1}^{n} c_i \langle k|Ai\rangle = \sum_{j=1}^{n} d_j \langle k|j\rangle = \sum_{j=1}^{n} d_j \delta_{kj} = \sum_{j=1}^{n} d_j.$$

Obtemos, elemento a elemento,

$$d_j = \sum_{i=1}^{n} c_i a_{ji}, \ \forall j \in \{1, 2, \dots, n\}.$$

Esta relación pode escribirse matricialmente como

$$\begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}.$$

Por tanto, de agora en diante, relacionaremos os operadores A coa súa representación matricial e tratarémolos como matrices.

Veremos agora algunhas propiedades que teñen que ter os operadores no formalismo cuántico. Para comezar, os operadores representan observables nun sistema físico, isto é, cantidades que se poden medir. Parece razoable supoñer que un observable brinde un valor esperado real, posto que se trata dunha cantidade que debemos percibir fisicamente. Con esta premisa, xorden os operadores hermíticos.

Definición 1.5. Unha matriz A dise hermítica cando é igual á súa trasposta conxugada, que denotaremos $A^\dagger$; é dicir, $A = \overline{(A^t)} = A^\dagger$.

A hermiticidade do operador transfírese á notación de Dirac segundo[4]

$$\langle \chi|A^\dagger \varphi\rangle = \langle A\chi|\varphi\rangle = \overline{\langle \chi|A\varphi\rangle}.$$

Cando vaiamos calcular o valor esperado do operador A sobre o vector $|\varphi\rangle$,

$$\langle \varphi|A|\varphi\rangle = \langle \varphi|A^\dagger|\varphi\rangle = \overline{\langle \varphi|A|\varphi\rangle}.$$

obteremos un valor real, posto que se $\alpha = \overline{\alpha}$ con $\alpha \in \mathbb{C}$, entón $\alpha \in \mathbb{R}$. Esta é a motivación detrás da aparición dos operadores hermíticos no formalismo cuántico.

Vexamos outra cualidade dos operadores que será de moita utilidade no ámbito da computación cuántica.

Definición 1.6. Un operador U dise unitario se $UU^\dagger = U^\dagger U = I$.

[4] Abuso de notación: de agora en diante, seguindo os pasos de Dirac, empregaremos a notación $\langle \chi|A|\varphi\rangle = \langle \chi|A\varphi\rangle$ para referirnos ao operador A actuando sobre o vector $|\varphi\rangle$.

Os operadores unitarios son de vital importancia posto que conservan a norma dos vectores. Como xa dixemos antes, trataremos con vectores normalizados

$$\langle\varphi|\varphi\rangle = 1.$$

Por tanto, a norma dun novo vector $|U\varphi\rangle$ ao que se lle aplicou o operador U será

$$\langle U\varphi|U\varphi\rangle = \langle\varphi|U^\dagger U|\varphi\rangle = \langle\varphi|I|\varphi\rangle = \langle\varphi|\varphi\rangle = 1.$$

Observación 1.7. Habemos de ter en conta que todas as matrices unitarias son invertibles, dado que se U é unitaria, $UU^\dagger = I$, entón $U^{-1} = U^\dagger$, que sempre existe.

A computación cuántica constrúese na súa totalidade con operadores unitarios (excepto no momento da medición). Dado que son invertibles, podemos dicir que todos os procesos son reversibles, é dicir, sempre podemos aplicar o operador U^{-1} despois de U e obter o *input*, cousa que non ocorría coas portas lóxicas AND e OR na computación clásica. Por tanto, non hai perda de información.

A continuación, veremos algúns dos operadores ou portas lóxicas cuánticas máis relevantes no ámbito da criptografía cuántica e daremos conta das súas propiedades máis relevantes.

1.4.1. Matrices de Pauli

As matrices de Pauli constitúen a base da computación cuántica, igual que o eran I, X, AND e OR no análogo clásico. Trátase de matrices 2×2 que actúan sobre os dous posibles estados da base $\mathcal{B} = \{|0\rangle, |1\rangle\}$. Denomínanse X, Y e Z e xunto coa identidade, permiten escribir calquera outro operador U actuando sobre un único cúbit como combinación linear delas,

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Estas matrices non só son unitarias, como deben ser todas as portas lóxicas cuánticas, senón que tamén son hermíticas, o cal fai que $XX^\dagger = XX = X^2 = I$. É dicir, a multiplicación dunha matriz de Pauli por si mesma dá a identidade.

A matriz de Pauli Z é de especial relevancia pois sobre ela mídense os estados. Ao calcular os autovectores normalizados destas matrices,

$$|+x\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad |+y\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix}, \qquad |+z\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

$$|-x\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \qquad |-y\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}, \qquad |-z\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

vemos que os autovectores de Z coinciden cos vectores que escollemos como base do noso espazo de Hilbert,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |+z\rangle\,, \qquad\qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |-z\rangle\,.$$

Por tanto, cando midamos o cúbit, en realidade estaremos facendo unha proxección sobre os autovectores da matriz de Pauli Z.

Vexamos como actúan cada unha destas matrices sobre os estados $|0\rangle$ e $|1\rangle$, ao igual que o fixemos coas portas lóxicas clásicas. Primeiramente, representemos o estado do noso cúbit matricialmente,

$$|q\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix},$$

e agora, apliquemos as respectivas matrices de Pauli sobre este estado,

$$\begin{aligned}
X\,|q\rangle &= \alpha X\,|0\rangle + \beta X\,|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta\,|0\rangle + \alpha\,|1\rangle\,, \\
Y\,|q\rangle &= \alpha Y\,|0\rangle + \beta Y\,|1\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = i\begin{pmatrix} -\beta \\ \alpha \end{pmatrix} = -i\beta\,|0\rangle + i\alpha\,|1\rangle\,, \\
Z\,|q\rangle &= \alpha Z\,|0\rangle + \beta Z\,|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix} = \alpha\,|0\rangle - \beta\,|1\rangle\,.
\end{aligned}$$

Recompilando as actuacións individuais das matrices sobre os vectores base, podemos concluír que

$$\begin{aligned}
&X\,|0\rangle = |1\rangle\,, && Y\,|0\rangle = i\,|1\rangle\,, && Z\,|0\rangle = |0\rangle\,, \\
&X\,|1\rangle = |0\rangle\,, && Y\,|1\rangle = -i\,|0\rangle\,, && Z\,|1\rangle = -\,|1\rangle\,.
\end{aligned}$$

Cabe destacar que podemos obter cada unha das matrices de Pauli a partir das outras dúas, o cal será de utilidade á hora de construir rotacións. Por exemplo,

$$Y\,|q\rangle = \alpha Y\,|0\rangle + \beta Y\,|1\rangle = -i\beta\,|0\rangle + i\alpha\,|1\rangle = i\alpha X\,|0\rangle - i\beta X\,|1\rangle = i\alpha XZ\,|0\rangle + i\beta XZ\,|1\rangle\,.$$

Analogamente para as outras dúas combinacións, obteríamos as relacións de conmutación

$$X = -iYZ, \qquad\qquad Y = iXZ, \qquad\qquad Z = -iXY.$$

1.4.2. Matrices de rotación

Para explicar xeometricamente as matrices de rotación, primeiramente introduciremos a esfera de Bloch.

A esfera de Bloch

A esfera de Bloch é unha representación xeométrica de todos os posibles estados dun sistema cuántico de dous niveis na forma dunha esfera en $\mathbb{R}^3$. Os seus eixos ortonormais son os autovectores $|+x\rangle$, $|+y\rangle$ e $|+z\rangle$.

Empregamos o eixo Z para medir, polo que $|+z\rangle = |0\rangle$ e $|-z\rangle = |1\rangle$. Deste xeito, os vectores que caian máis preto dos polos terán máis probabilidade de colapsar sobre ese estado (Figura 1.1).

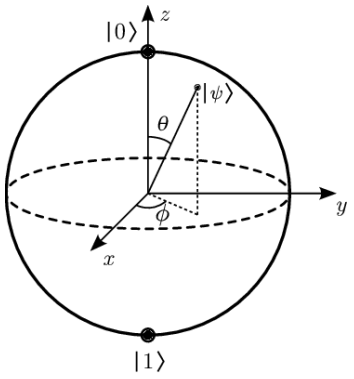


Figura 1.1: Esfera de Bloch. Extraída de Rasmussen et al. (2021)

Con esta ferramenta tan útil, podemos visualizar as matrices de rotación R_X, R_Y e R_Z como unha rotación arredor dos eixos X, Y e Z, respectivamente. Formalmente, empregamos un desenrolo exponencial da matriz de rotación do seguinte xeito

$$e^A = \sum_{k=0}^{\infty} \frac{A^k}{k!},$$

que se aplicamos ao caso particular da matriz X e do xiro θ sería

$$e^{i\frac{\theta}{2}X} = I + iX\frac{\theta}{2} + \frac{i^2X^2}{2!}\left(\frac{\theta}{2}\right)^2 + \frac{i^3X^3}{3!}\left(\frac{\theta}{2}\right)^3 + \frac{i^4X^4}{4!}\left(\frac{\theta}{2}\right)^4 + ...$$

Se agora separamos a parte real da imaxinaria

$$e^{i\frac{\theta}{2}X} = \left[I - \frac{X^2}{2!}\left(\frac{\theta}{2}\right)^2 + \frac{i^4X^4}{4!}\left(\frac{\theta}{2}\right)^4 + ...\right] + i\left[X\frac{\theta}{2} - \frac{X^3}{3!}\left(\frac{\theta}{2}\right)^3 + ...\right],$$

vemos que os termos da parte real conforman a expansión do coseno, mentres que os da parte imaxinaria son os do seno. Deste xeito, temos a expresión da expansión máis compacta

$$e^{i\frac{\theta}{2}X} = I\cos(\theta/2) + iX\,\mathrm{sen}(\theta/2),$$

que explicitamos a continuación, xunto coas análogas para Y e Z,

$$R_X(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\,\mathrm{sen}\,\frac{\theta}{2} \\ -i\,\mathrm{sen}\,\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \quad R_Y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\,\mathrm{sen}\,\frac{\theta}{2} \\ \mathrm{sen}\,\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \quad R_Z(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

Estas matrices son comunmente empregadas nos algoritmos de computación cuántica, especialmente nos de *machine learning* e, tanxencialmente, nalgúns de criptografía cuántica, por ter unha gran expresibilidade.

1.4.3. Outros operadores

Outros operadores moi comúns e de interese no ámbito da computación cuántica son as portas Hadamard e as portas condicionais CNOT.

Hadamard

A porta Hadamard, denotada H, vén dada pola seguinte expresión

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{1.1}$$

Trátase dun operador de especial relevancia pois cando actúa sobre os estados base $\{|0\rangle, |1\rangle\}$, pon o cúbit en superposición[5]

$$\begin{aligned} H|0\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |+x\rangle = |+\rangle, \\ H|1\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-x\rangle = |-\rangle. \end{aligned}$$

É importante notar que todas as portas son unitarias e reversibles, polo que se temos un estado de superposición $|+\rangle$ e aplicamos Hadamard, obteremos o estado base $|0\rangle$,

$$H|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = |0\rangle.$$

Por tanto, podemos dicir que a porta H sirve de transición entre as bases $\{|0\rangle, |1\rangle\}$ e $\{|+\rangle, |-\rangle\}$, o cal é de vital importancia para os primeiros algoritmos criptográficos que veremos no seguinte capítulo. Non é habitual empregar a base $\{|+y\rangle, |-y\rangle\}$ para medicións, polo que non listaremos ningunha porta de transición a esta base.

Se queremos visualizar a actuación de H sobre a esfera de Bloch, vemos que estamos levando o estado $|0\rangle$ a $|+\rangle$, o cal é equivalente a aplicar unha rotación de $\pi/2$ radiáns arredor do eixo Y

$$R_Y(\pi/2) = \begin{pmatrix} \cos\frac{\pi}{4} & -\operatorname{sen}\frac{\pi}{4} \\ \operatorname{sen}\frac{\pi}{4} & \cos\frac{\pi}{4} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

[5] É habitual denotar os estados $|+x\rangle = |+\rangle$ e $|-x\rangle = |-\rangle$ no ámbito da computación cuántica.

Se aplicamos esta porta sobre os estados base $|0\rangle$ e $|1\rangle$, teremos

$$R_Y(\pi/2)\,|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$
$$R_Y(\pi/2)\,|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\left(-|0\rangle + |1\rangle\right),$$

Vemos que o estado $R_Y(\pi/2)\,|1\rangle$ non é exactamente $|-\rangle$. Diferénciase nun factor -1, que a priori sería unha fase global módulo 1 e caería sobre o mesmo punto da esfera de Bloch. Mais habemos de ter en conta que se imos encadear varias portas lóxicas, estas discrepancias nas expresións das matrices poden levar a diferentes resultados. Por tanto, ímonos guiar pola álxebra e aplicar unha porta X despois da rotación para obter o mesmo resultado que coa porta de Hadamard

$$XR_Y(\pi/2) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = H.$$

Agora si teriamos os estados $|+\rangle$ e $|-\rangle$,

$$XR_Y(\pi/2)\,|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle,$$
$$XR_Y(\pi/2)\,|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle.$$

Logo, acabamos de ver que podemos obter a porta Hadamard en función doutras portas que xa viramos (Nielsen e Chuang, 2011),

$$H = XR_Y(\pi/2).$$

CNOT

A porta CNOT é unha das portas condicionais máis básicas e a única que precisaremos para os nosos algoritmos. Trátase da aplicación dunha negación X sobre o cúbit diana en función do valor do cúbit de control. Así, se o cúbit de control q_0 vale 0, non se modificará o valor do cúbit q_1, mais se o cúbit q_0 vale 1, aplicarase a porta X sobre q_1. Matematicamente, a expresión matricial desta porta será

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

Vemos que agora precisamos unha matriz 4×4 dado que estamos a traballar nun espazo de 2 cúbits e, por tanto, necesitamos 4 elementos para representar todos os posibles valores

destes dous cúbits

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

Facendo as multiplicacións matriciais, comprobamos o resultado que comentabamos antes

$$\begin{aligned} CNOT\,|00\rangle &= |00\rangle \\ CNOT\,|01\rangle &= |01\rangle \\ CNOT\,|10\rangle &= |11\rangle \\ CNOT\,|11\rangle &= |10\rangle\,. \end{aligned}$$

Nótese que de cambiar o cúbit de control, a expresión da matriz sería diferente. Supoñamos que q_1 é agora o cúbit de control e q_0 o cúbit diana. Logo, CNOT sería

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

Podemos imaxinar a matriz como unha función na que o *input* entra por columnas e o *output* sae por filas. Logo se queremos transformar $|01\rangle$ en $|11\rangle$ teremos que poñer un 1 no elemento m_{42}

$$\begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \end{array}$$

1.4.4. Proxectores

Os proxectores son os únicos operadores non reversibles que empregaremos na computación cuántica. Funcionan de maneira análoga aos proxectores sobre un espazo no ámbito da álxebra. A súa expresión vectorial é

$$\mathcal{P}_k = |k\rangle\langle k|\,,\ \forall k \in \{0,1\}.$$

Unha vez medido o cúbit e obtido o valor k, o colapso da función de onda escribirase, segundo Scherer (2019), como

$$|q\rangle \to \frac{\mathcal{P}_k\,|q\rangle}{\langle q|\,\mathcal{P}_k\,|q\rangle^{\frac{1}{2}}}.$$

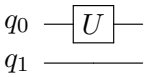
Poñamos un exemplo: supoñamos que temos $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ e medimos o valor $|0\rangle$, logo

$$\frac{\mathcal{P}_0|q\rangle}{\langle q|\mathcal{P}_0|q\rangle^{\frac{1}{2}}} = \frac{|0\rangle\langle 0|(\alpha|0\rangle + \beta|1\rangle)}{\left[(\overline{\alpha}\langle 0| + \overline{\beta}\langle 1|)|0\rangle\langle 0|(\alpha|0\rangle + \beta|1\rangle)\right]^{\frac{1}{2}}} = \frac{\alpha|0\rangle}{\sqrt{|\alpha|^2}} = |0\rangle,$$

como queríamos demostrar.

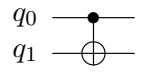
1.5. Circuítos cuánticos

Representaremos os circuítos cuánticos con diagramas como o seguinte



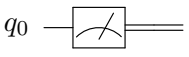
onde U representa calquera porta unitaria que lle queiramos aplicar ao cúbit q_0, habitualmente iniciado no estado $|0\rangle$.

No caso de portas condicionadas, no que precisamos especificar o cúbit control e o cúbit diana, empregaremos unha representación análoga á da porta CNOT[6]



na que o cúbit control é q_0 e, en función do seu valor, aplicaráselle un NOT ao cúbit q_1.

Atoparémonos tamén con algúns símbolos especiais, como a medición para cando colapsamos a función de onda



e a posterior doble liña, que indica unha canle clásica.

En sistemas de varios cúbits, cando queiramos expresar o estado conxunto

$$|q_0\rangle \otimes |q_1\rangle \otimes |q_2\rangle \otimes ...$$

habitualmente omitiremos o produto tensorial e referirémonos a el como $|q_0 q_1 q_2 ...\rangle$.

1.6. Comunicacións cuánticas

Existen unha serie de fenómenos e teorías da física cuántica que dictaminan os límites das comunicacións cuánticas. A continuación, explicaremos os máis relevantes.

[6] O símbolo de $\bigoplus$ sobre o segundo cúbit denota unha suma binaria.

1.6.1. Teorema de non clonación

A diferencia da computación clásica, a información cuántica non pode ser copiada. Supoñamos que temos un cúbit $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, con α e β descoñecidos, e pretendemos copiar esta información nun cúbit baleiro $|\chi\rangle$ de xeito que obteñamos $|\chi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. É dicir, buscamos un operador unitario U que realice a transformación

$$U\left(|\varphi\rangle \otimes |\chi\rangle\right) = |\varphi\rangle \otimes |\varphi\rangle\,.$$

Vexamos por que isto non é posible (Scherer, 2019). Asumindo que existe dito operador U, este tería que ser quen de facer as seguintes copias

$$U\left(|0\rangle \otimes |\chi\rangle\right) = |0\rangle \otimes |0\rangle\,, \tag{1.2}$$

$$U\left(|1\rangle \otimes |\chi\rangle\right) = |1\rangle \otimes |1\rangle\,, \tag{1.3}$$

$$U\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\chi\rangle\right) = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}. \tag{1.4}$$

Mais, se explicitamos a última expresión (1.4),

$$U\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |\chi\rangle\right) = U\left(\frac{1}{\sqrt{2}}\left(|0\rangle \otimes |\chi\rangle\right) + \frac{1}{\sqrt{2}}\left(|1\rangle \otimes |\chi\rangle\right)\right),$$

e aplicamos a linearidade do operador U no espazo de Hilbert,

$$U\left(\frac{1}{\sqrt{2}}\left(|0\rangle \otimes |\chi\rangle\right) + \frac{1}{\sqrt{2}}\left(|1\rangle \otimes |\chi\rangle\right)\right) = \frac{1}{\sqrt{2}}\left[U\left(|0\rangle \otimes |\chi\rangle\right) + U\left(|1\rangle \otimes |\chi\rangle\right)\right],$$

podemos agora empregar as dúas primeiras Ecuacións (1.2) e (1.3). Así, obteremos

$$\frac{1}{\sqrt{2}}\left[U\left(|0\rangle \otimes |\chi\rangle\right) + U\left(|1\rangle \otimes |\chi\rangle\right)\right] = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right),$$

que non é o mesmo que o resultado esperado de copiar o cúbit inicial. Máis explicitamente, podemos ver que faltan os termos cruzados

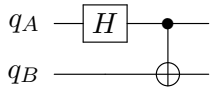
$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right) \neq \frac{1}{\sqrt{2}}\left(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\right).$$

1.6.2. Teleportación cuántica

A teleportación cuántica foi un dos primeiros fenómenos que se estudou dentro das comunicacións cuánticas por sospeita de que podería romper o principio de transmisión de información a velocidades superiores ás da luz.

Seguiremos a explicacion de Moret-Bonillo (2018) para ilustrar o problema. Supoñamos que Alice e Bob comparten un par de cúbits enlazados

$$|q_A q_B\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{1.5}$$



Agora Alice quere transmitir o seu cúbit $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ a Bob, sen saber a información que contén e sen poder facer unha copia del polo teorema de non clonación. Así, o que fai é entrelazalo co estado de Bell anterior (1.5) mediante unha porta CNOT

$$\begin{aligned} |\varphi\rangle \otimes |q_A q_B\rangle &= \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right), \\ CNOT_{1,2}\,|\varphi q_A q_B\rangle &= \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\right), \end{aligned} \tag{1.6}$$

e posteriormente aplicar unha porta H a (1.6). Para iso, beneficiaranos separar o estado da seguinte maneira

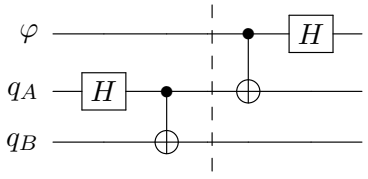
$$\frac{1}{\sqrt{2}}\left[\alpha|0\rangle \otimes (|00\rangle + |11\rangle) + \beta|1\rangle \otimes (|10\rangle + |01\rangle)\right],$$

e aplicar H a $a|0\rangle$ e $b|1\rangle$

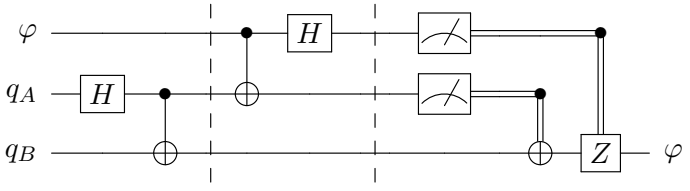
$$\frac{1}{\sqrt{2}}\left[\frac{1}{\sqrt{2}}\alpha\left(|0\rangle + |1\rangle\right) \otimes (|00\rangle + |11\rangle) + \frac{1}{\sqrt{2}}\beta\left(|0\rangle - |1\rangle\right) \otimes (|10\rangle + |01\rangle)\right].$$

Desenrolando e reordeando termos obtemos

$$\frac{1}{2}\left[|00\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) + |01\rangle\left(\alpha|1\rangle + \beta|0\rangle\right) + |10\rangle\left(\alpha|0\rangle - \beta|1\rangle\right) + |11\rangle\left(\alpha|1\rangle - \beta|0\rangle\right)\right].$$



Vemos como todos os termos entre parénteses da anterior ecuación son variacións do cúbit $|\varphi\rangle$ orixinal. O que resta agora é medir os dous cúbits de Alice (o cúbit $|\varphi\rangle$ que queremos teleportar e a súa parte do par entrelazado $|q_A\rangle$) e aplicar certas portas en función do resultado, como se amosa na Táboa 1.1. Con isto, recuperaremos sempre o cúbit que queriamos transportar $|\varphi\rangle$ en $|q_B\rangle$.



Cómpre aclarar que en ningún momento se violaron os dous principios fundamentais da información cuántica. Por un lado, non se está a transmitir información máis rápido ca

Medición $\|\varphi, q_A\rangle$	$\|q_B\rangle$ asociado	Portas a aplicar	Resultado
$\|00\rangle$	$\alpha\|0\rangle + \beta\|1\rangle$	I	$\alpha\|0\rangle + \beta\|1\rangle$
$\|01\rangle$	$\alpha\|1\rangle + \beta\|0\rangle$	X	$\alpha\|0\rangle + \beta\|1\rangle$
$\|10\rangle$	$\alpha\|0\rangle - \beta\|1\rangle$	Z	$\alpha\|0\rangle + \beta\|1\rangle$
$\|11\rangle$	$\alpha\|1\rangle - \beta\|0\rangle$	ZX	$\alpha\|0\rangle + \beta\|1\rangle$

Táboa 1.1: Resumo das portas a aplicar trala medición dos cúbits de Alice.

velocidade da luz dado que precisamos enviar dous bits clásicos (o resultado das medicións dos cúbits de Alice) e, por tanto, a transmisión desta información vese limitada polas velocidades das canles clásicas. Por outro lado, cúmprese o teorema de non clonación xa que en ningún momento chegamos a ter unha copia do cúbit $|\varphi\rangle$. No momento no que obtemos $|q_B\rangle = |\varphi\rangle$ no cúbit de Bob, xa o tiñamos medido e, por tanto, destruído, no cúbit de Alice.

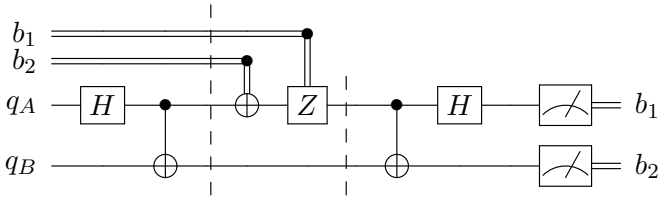
1.6.3. Codificación superdensa

Para rematar con este capítulo, veremos algunhas nocións de codificación superdensa. Dalgún xeito, búscase responder á pregunta inversa da teleportación cuántica, na que fumos capaces de enviar un cúbit coa axuda de dous bits. Agora, cantos bits somos capaces de codificar nun só cúbit?

Para iso, seguindo os pasos de Nielsen e Chuang (2011), estableceremos a comunicación entre Alice e Bob mediante un par enlazado

$$|\varphi\rangle = \frac{1}{\sqrt{2}}|00\rangle + |11\rangle\,.$$

Supoñamos que Alice quere enviar un par de bits b_1b_2. Se $b_2 = 1$, aplícalle unha porta X ao seu cúbit. Se $b_1 = 1$, entón aplícalle a porta Z, como podemos ver no circuíto.



Logo, envíalle o seu cúbit a Bob. Esta é a única transmisión de información neste protocolo, xa que o reparto inicial do par enlazado puido ser feito por unha terceira parte. Tras recibilo, Bob aplica as portas CNOT e H e mide ambos cúbits. O resultado será o par b_1b_2 que lle enviou Alice necesariamente.

Vexámolo cun exemplo. Supoñamos que Alice quixo enviar o par 11. Entón, aplicou primeiro a porta X sobre o par enlazado

$$\frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right),$$

e a continuación, a porta Z,

$$\frac{1}{\sqrt{2}}\left(-|10\rangle + |01\rangle\right).$$

Agora, cando o recibe Bob, aplica unha CNOT

$$\frac{1}{\sqrt{2}}\left(-|11\rangle + |01\rangle\right) = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)|1\rangle,$$

e unha porta Hadamard[7]

$$H\left[\frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)\right]|1\rangle = |11\rangle.$$

O único posible resultado da medición é $b_1 b_2 = 11$, que era o *string* que Alice quería enviar.

[7]Isto é equivalente a medir na base $\{|+\rangle, |-\rangle\}$.

Capítulo 2

Criptografía cuántica

Neste capítulo, revisaremos os principais protocolos de criptografía cuántica. Comezaremos vendo a orixe histórica dos primeiros algoritmos e por que se fixo necesaria a súa concepción. Continuaremos cun sistema de distribución de chaves cuántico e veremos a súa aplicación en casos clásicos. Tamén estudaremos os análogos cuánticos dalgúns algoritmos clásicos ben coñecidos e comentaremos outros concebidos puramente no ámbito da mecánica cuántica.

2.1. Motivación: o algoritmo de Shor

O algoritmo de Shor foi un dos primeiros en desafiar a criptografía clásica como se coñecía. Este método para descompoñer números enteiros nos seus factores primos podería potencialmente quebrantar os sistemas de chave pública como o RSA, que quedaría obsoleto (Moret-Bonillo, 2018).

En Scherer (2019) relátase en detalle o protocolo RSA. Este consiste en que Alice escolle dous número primos p e q, con $p \neq q$ e atopa un $a \in \mathbb{N}$ tal que se cumpla

$$\operatorname{mcd}(a, (p-1)(q-1)) = 1.$$

Logo, multiplica os primos $N = pq$ e publica a chave

$$k_{pub} = (a, N).$$

Agora, calquera persoa pode encriptar unha mensaxe $m < N$ ca chave pública, facendo

$$e(k_{pub}, m) = m^a \mod N,$$

sendo $c = e(k_{pub}, m)$ o criptotexto que se presenta en canles públicas. Se Bob, o receptor do criptotexto que coñece tanto p como q, quere descifrar esta criptomensaxe, deberá atopar

un $b \in \mathbb{N}$ tal que

$$ab \mod (p-1)(q-1) = 1,$$

co cal atopará a chave privada $k_{priv} = (b, N)$. Para descifrar o texto, tan só terá que facer

$$m = d(k_{priv}, c) = c^{ab} \mod N.$$

O lema e o teorema no que se basan estes últimos dous pasos pódense atopar ca súa demostración no propio Scherer (2019).

O algoritmo máis rápido para factorizar N que coñecemos é o *General Number Field Sieve* que, segundo Crandall e Pomerance (2006), estímase da orde de

$$S_{NFS}(N) \in O\left(\exp\left[\left(\frac{64}{9} + o(1)\right)^{\frac{1}{3}} (\log N)^{\frac{1}{3}} (\log\log N)^{\frac{2}{3}}\right]\right), \tag{2.1}$$

para un N de lonxitude $\log N$ bits. Este algoritmo heurístico é de tempo exponencial. Por exemplo, romper un N duns 250 decimais cun só ordenador podería levar da orde de miles de anos. É por iso que se considera un protocolo seguro hoxe en día.

Non obstante, coa introdución da teoría cuántica, Peter Shor presenta en Shor (1997) un algoritmo para factorizar números baseado nas transformadas de Fourier cuánticas e no algoritmo de búsqueda de orde, que non trataremos en detalle neste documento.

Para poder factorizar N nun ordenador cuántico, buscamos atopar unha solución non trivial da ecuación $x^2 \mod N = 1$. Os seguintes teoremas apórtannos os resultados necesarios para levalo a cabo (Nielsen e Chuang, 2011).

Teorema 2.1. *Supoñamos que N é un número composto e x é unha solución non trivial da ecuación $x^2 \mod N = 1$ no rango $1 \leq x \leq N$, é dicir, $x \neq \pm 1 \mod N$. Entón, polo menos,* $\mathrm{mcd}(x-1, N)$ *ou* $\mathrm{mcd}(x+1, N)$ *é un factor non trivial de N.*

Teorema 2.2. *Supoñamos $N = p_1^{\alpha_1} \ldots p_m^{\alpha_m}$ a factorización en primos dun enteiro positivo composto impar. Sexa x o enteiro escollido de maneira uniformemente aleatoria, suxeito ós requerimentos $1 \leq x \leq N-1$ e x coprimo con N. Sexa r a orde de x en módulo N. Entón, a probabilidade P de que r sexa par e $x^{r/2} \neq -1 \mod N$ sería*

$$P(r \text{ par e } x^{r/2} \neq -1 \mod N) \geq 1 - \frac{1}{2^m}.$$

No caso no que pretendemos aplicar o Teorema 2.2, N é un número composto que se pode factorizar en dous primos, p e q. Polo que $m = 2$ e atoparíamos un r satisfactorio con probabilidade maior a $1/2$.

Como se describe en Nielsen e Chuang (2011), o algoritmo comeza comprobando que N sexa impar e composto, buscando que 2 non sexa un divisor e $N \neq a^b$, para algúns $a \geq 1$ e

$b \geq 2$ enteiros. Unha vez feito isto, escóllese aleatoriamente un x entre 1 e $N-1$. Se se dá que $\text{mcd}(x, N) > 1$, entón atopamos o factor $\text{mcd}(x, N)$. Se non se cumple isto, estamos nas condicións do Teorema 2.2. Procedemos a empregar unha subrutina que busque a orde r de x módulo N, é dicir, un r tal que $x^r = 1 \mod N$. Se r é par e ademais $x^{r/2} \neq -1 \mod N$ (lembremos que a probabilidade de que isto suceda é maior que $1/2$), entón compútase o $\text{mcd}(x^{r/2} - 1, N)$ e o $\text{mcd}(x^{r/2} + 1, N)$ e, polo Teorema 2.1, un destes deberá ser factor de N. En caso de que non se cumpran as condicións para levar a cabo este último paso, o algoritmo falla.

Shor razonou, na súa primeira análise deste problema en 1994 (Shor, 1994), que podíamos atopar un r axeitado repetindo o experimento un número polinomial de veces. En Shor (1997) precisa con máis detalle a orde do algoritmo, que sería

$$O\left((\log N)^2(\log\log N)(\log\log\log N)\right),$$

ademais de $O(\log N)$ operacións de post-procesado nun ordenador clásico. En calqueira caso, se o comparamos co algoritmo heurístico do *NFS* (2.1), supón unha melloría exponencial no tempo de execución.

Isto supuxo toda unha revolución no mundo da criptografía, dado que, de ter ordenadores cuánticos perfectos (sen ruído), o sistema de cifrado de chaves máis importante quedaría obsoleto e podería supoñer o derrubamento da criptografía clásica como a coñecíamos. É por isto que se fixo necesario atopar unha nova criptografía que fose compatible co poder de execución dos ordenadores cuánticos.

2.2. Distribución cuántica de chaves

A distribución cuántica de chaves (QKD[1]) non é en si mesma criptografía cuántica no senso de que non se está a transmitir ningunha mensaxe, senon que é un protocolo de distribución de chaves de seguridade demostrable[2] sobre unha canle pública.

Este protocolo baséase no feito de que un posible atacante (Eve) non pode copiar ningún dos cúbits, polo teorema de non clonación e, ademais, calquer intento de acceso aos cúbits de Alice e Bob xeraría unha perturbación detectable no sistema. Vexamos a seguinte proposición e a súa demostración, extraídas de Nielsen e Chuang (2011).

Proposición 2.3. ***(A obtención de información implica perturbación)*** *Ante calquera intento de distinguir dous estados cuánticos non ortogonais, a obtención de información só é posible se se introduce unha perturbación no sinal.*

[1] Polas súas siglas en inglés *Quantum Key Distribution.*

[2] Seguridade demostrable refírese á ciberseguidade que pode ser probada matematicamente.

Demostración 2.4. Sexan $|\varphi\rangle$ e $|\chi\rangle$ dous estados cuánticos non ortogonais. Se Eve quere obter información, debe interactuar unitariamente cos dous estados. Sexa $|u\rangle$ o cúbit auxiliar que emprega Eve para esta tarefa. Asumindo que este proceso non perturba os estados orixinais (para que Alice e Bob non se enteren do ataque), entón

$$|\varphi\rangle\,|u\rangle \longrightarrow |\varphi\rangle\,|v\rangle$$
$$|\chi\rangle\,|u\rangle \longrightarrow |\chi\rangle\,|v'\rangle\,.$$

Para que Eve poida distinguir os estados, necesariamente $|v\rangle \neq |v'\rangle$. Non obstante, pola conservación do produto interior ante transformacións unitarias

$$\langle v|v'\rangle\,\langle\varphi|\chi\rangle = \langle u|u\rangle\,\langle\varphi|\chi\rangle\,,$$

e obtemos

$$\langle v|v'\rangle = \langle u|u\rangle = 1.$$

Co cal, só poder ser $|v\rangle = |v'\rangle$. Por tanto, Eve non poderá obter información sen perturbar algún dos estados. □

A continuación, comentaremos unha das implementacións máis directas desta proposición sobre a que se basea unha gran parte da criptografía cuántica, pois fan uso desta distribución de chaves segura.

2.2.1. Protocolo BB84

O protocolo BB84, que leva o nome dos seus creadores Charles Bennett e Gilles Brassard, toma como referencia a Proposición 2.3 para transmitir unha chave de maneira segura a través dunha canle pública. O método funciona como describen os seus autores en Bennett e Brassard (1984).

Traballamos cos seguintes estados non ortogonais[3]

$$|0\rangle\,, \qquad |1\rangle\,, \qquad |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \qquad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

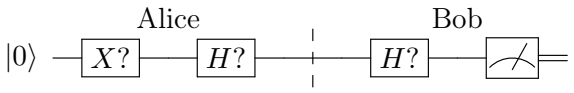
Para cambiar da base $\{|0\rangle\,, |1\rangle\}$ á base $\{|+\rangle\,, |-\rangle\}$ só cómpre aplicar unha porta de Hadamard. En efecto, vemos que entre os estados $|0\rangle$ e $|+\rangle$ non hai relación de ortogonalidade

$$\langle +|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \neq 0.$$

Alice comeza escollendo un estado do cúbit ao azar, $|0\rangle$ ou $|1\rangle$, e decidindo, tamén aleatoriamente, se aplica a porta H ou non. Deste xeito, a súa elección entre os estados non ortogonais debería ser uniformemente aleatoria. Posteriormente, envíalle o cúbit a Bob.

[3]Bennett e Brassard (1984) representan estes estados como polarizacións dun fotón a 0°, 90°, 45° e 135°, respectivamente.

Unha vez Bob o recibe, aplica tamén de xeito aleatorio a porta H e mide o resultado. O circuíto desta trasmisión sería



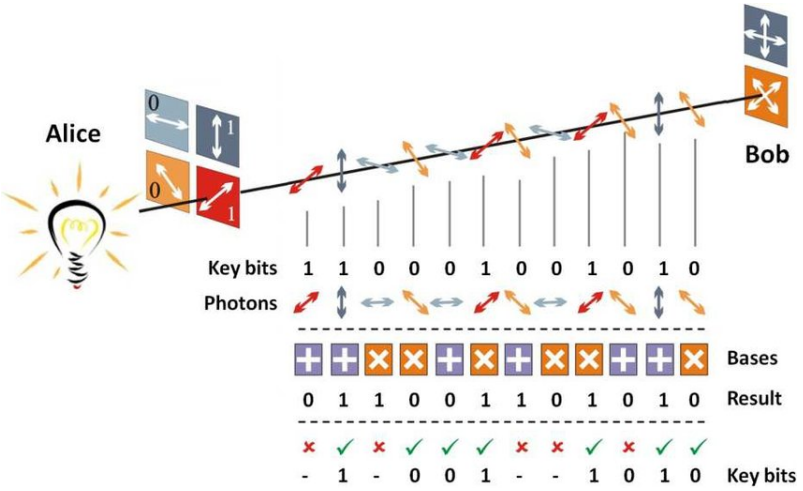


Figura 2.1: Esquema do protocolo BB84. Extraído de Carrasco-Casado et al. (2016).

Este proceso repítese cun número grande de cúbits. Unha vez finalizada a transmisión, Alice e Bob comunícanse a través dunha canle clásica, autenticada[4] pero non necesariamente segura. Alice procede a dicirlle as portas H que aplicou ós cúbits e Bob anota se coinciden coas que aplicou el. En caso afirmativo, Bob mantén o bit que mediu nesa transmisión e, en caso contrario, descártao (Figura 2.1).

O protocolo funciona porque, no caso trivial de non aplicar ningunha porta, a medición é necesariamente o estado inicial cun 100 % de probabilidade e, no caso de ambos aplicaren a porta H dúas veces consecutivas, recupérase o estado inicial do cúbit por hermiticidade ($HH = I$). Os cúbits que non cumplen estas condicións descártanse por brindar resultados aleatorios.

Plantexemos agora que ocorrería se Eve intentase interceptar a mensaxe. A súa única opción sería medir os cúbits ela mesma, dado que non ten maneira de clonalos e non pode interactuar con eles sen perturbar a comunicación, como vimos na Proposición 2.3. Logo disto, enviaría os cúbits xa colapsados a Bob ca pretensión de que non se percatara. Porén, como razonan Carrasco-Casado et al. (2016), a probabilidade de que Eve atine a aplicar a mesma porta que Alice é dun 50 %. Dos restantes cúbits, pola natureza cuántica da medición, aleatoriamente obterá os resultados correctos a metade das veces, é dicir, un 25 % sobre o total. O restante 25 % acadará resultados incorrectos. Bob recibirá estes

[4]Unha canle autenticada é aquela na que se verificou a identidade dos interlocutores.

cúbits colapsados e, ao comparar un anaco da chave con Alice, darase de conta de que hai un 25 % de erro na transmisión dos cúbits, fronte ao 0 % esperado no protocolo orixinal. Así, ambos saberán que houbo un ataque á comunicación e descartarán a chave.

2.3. Caderno de uso único

2.3.1. Caderno de uso único clásico

Unha aplicación moi útil que ten a distribución cuántica de chaves (QKD) é o caderno de uso único, tamén coñecido como *one-time pad* ou cifrado de Vernam, que é un sistema criptográfico que se desfai da chave cada vez que se envía unha mensaxe. Revisemos como funcionaba o caso clásico e vexamos en que axuda a QKD.

O cifrado de Vernam consiste en transcribir a mensaxe a código binario e sumala módulo 2 coa chave, é dicir,

$$c_i = m_i \oplus k_i \qquad \forall i \in \{1, \dots, M\},$$

sendo M a lonxitude da mensaxe m, c o criptotexto e k a chave. Para descifralo, basta con revertir o proceso, ou sexa, volver a sumar módulo 2

$$m_i = c_i \oplus k_i \qquad \forall i \in \{1, \dots, M\}.$$

Exemplo 2.5. Supoñamos que queremos enviar a mensaxe $m = 10011$ coa chave $k = 01010$. Logo o texto encriptado sería

$$c = 10011 \oplus 01010 = 11001,$$

e o texto desencriptado

$$11001 \oplus 01010 = 10011 = m,$$

recuperando a mensaxe orixinal.

O ideal neste cifrado é non empregar a mesma chave dúas veces, pois podería revelar información sobre as mensaxes encriptadas, como razona Assche (2006). Se m_k e m'_k son dous bits da mensaxe encriptados ca mesma chave k, entón a suma destes e a dos seus respectivos bits encriptados é a mesma,

$$m_k \oplus m'_k = c_k \oplus c'_k. \tag{2.2}$$

Logo Eve consegue obter información, dado que reduce as catro posibles combinacións iniciais a tan só dúas: $(m_k, m'_k) \in \{(0, c_k \oplus c'_k), (1, c_k \oplus c'_k \oplus 1)\}$.

De feito, empregar unha chave máis curta ca mensaxe sería equivalente a empregar a mesma chave dúas veces. É trivial ver que, partindo a mensaxe orixinal en m e m',

estamos nas condicións da Ecuación (2.2). Ademais, podería ser susceptible a ataques con algoritmos frecuentistas que atopasen o período de repetición.

Por tanto, se no caderno de uso único empregamos unha chave de lonxitude igual ou maior ca da mensaxe e a descartamos despois de utilizala unha soa vez, acaderemos seguridade perfecta; é dicir, Eve non ten maneira de obter información adicional sobre o texto sen cifrar, mesmo se este está sesgado estatisticamente (Assche, 2006).

O maior problema deste sistema é a necesidade dunha canle segreda a través da cal poder enviar unha nova chave cada vez que se queira enviar unha mensaxe. Este proceso é moi custoso e susceptible de ataques, dado que a seguridade recae na dificultade de resolver certos problemas, como vimos no caso do RSA. Non obstante, co método da QKD poderíamos mandar a chave a través dunha canle pública con seguridade demostrable. Xorde así unha simbiose entre un método de encriptado clásico e un sistema de distribución de chaves cuántico.

2.3.2. Caderno de uso único cuántico

Que ocorre se, en lugar de encriptar un bit, quixeramos encriptar un cúbit? Estamos ante o primeiro problema de criptografía cuántica desta sección: o análogo cuántico do caderno de uso único ou cifrado de Vernam.

No caso clásico, simplemente faciamos a suma módulo 2 da mensaxe coa chave. Facer a suma módulo 2 é equivalente a aplicar a negación X se o bit da chave é 1 e non facer nada se é 0. Por tanto, poderíamos pensar que nun análogo cuántico se aplicaría a porta X en función do valor k_i da chave

$$|c_i\rangle = X^{k_i} |m_i\rangle \qquad \forall i \in \{1, \dots, M\},$$

onde $X^0 = I$ e $X^1 = X$.

Porén, atopámonos cun problema. Pretendemos enviar toda a información dun estado cuántico, non só os valores $|0\rangle$ e $|1\rangle$, pois nisto consiste a criptografía cuántica. Se agora intentamos aplicar a porta X ao estado $|+\rangle$, ocorre o seguinte, como razonan Vidick e Wehner (2023),

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

Quedamos co mesmo estado inicial, sen importar cantas veces tentemos aplicar a porta X. Precisamos unha porta que nos axude a encriptar o estado $|+\rangle$, por exemplo, transformándoo no estado $|-\rangle$ sobre a base $\{|+\rangle , |-\rangle\}$. Este é o caso da porta Z,

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

Analogamente, $Z|-\rangle = |+\rangle$. Obsérvese que a porta Z por si soa tampouco podería encriptar todos os estados cuánticos, dado que

$$Z|0\rangle = |0\rangle\,,$$
$$Z|1\rangle = -|1\rangle\,.$$

Por tanto, precisamos unha combinación das portas X e Z,

$$|c_i\rangle = X^{k_{1i}} Z^{k_{2i}} |m_i\rangle\,, \qquad \forall i \in \{1, \ldots, M\}. \tag{2.3}$$

Observamos que para levar a cabo este protocolo cómpre empregar dous bits por cada cúbit que se queira encriptar, por tanto a chave k deberá ser o dobre de longa. Se nos lembramos da sección 1.6.3 sobre codificación superdensa, na que conseguiramos condensar dous bits de información nun só cúbit, poderíamos pensar que o seu inverso é o caderno de uso único cuántico.

Empregando tan só as portas X e Z pódense encriptar todos os estados posibles dun cúbit xenérico $|\varphi\rangle$. A demostración deste feito, detallada en Boykin e Roychowdhury (2003), emprega as matrices densidade ρ, moi útiles na teoría da información cuántica pero que non trataremos neste manuscrito. Non obstante, seguindo os pasos de Vidick e Wehner (2023), imos dar unhas pinceladas xeométricas de por que con estas dúas portas xa temos toda a información encriptada.

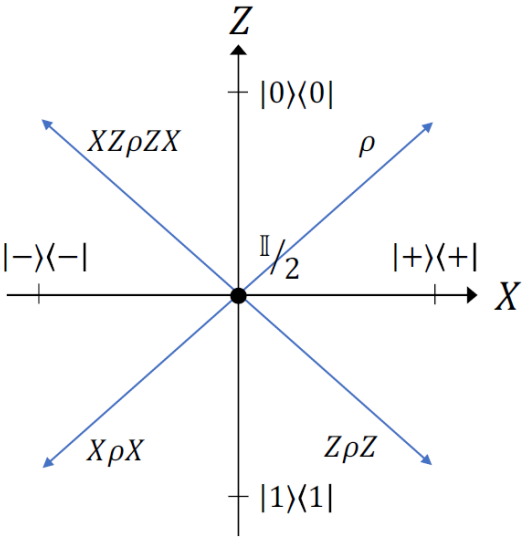


Figura 2.2: Representación bidimensional da bóla de Bloch colapsada sobre os eixos X e Z. Extraído de Vidick e Wehner (2023).

A matriz densidade podería considerarse xeometricamente como o vector que apunta a un estado na bóla de Bloch (a esfera de Bloch rechea). Canto máis se achegue á superficie da bóla, máis detallada é a información do estado cuántico. Habitualmente, en criptografía

cuántica só traballamos con puntos sobre a superficie da bóla de Bloch, é dicir, con estados puros. Observemos agora a Figura 2.2. As frechas representan as inversións sobre os eixos X e Z, equivalentes a empregar cada unha destas portas sobre un estado xenérico $|\varphi\rangle$. A probabilidade de obter cada un dos catro estados representados é uniformemente $1/4$, dado que cada unha das portas se aplica con probabilidade $1/2$. Por tanto, a matriz densidade ρ, calculada como a media destes catro estados, quedaría como un punto no centro da bóla, o estado de menor información posible. Deste xeito, encriptamos de forma óptima o estado $|\varphi\rangle$.

En resume, o protocolo do caderno de uso único consiste en que Alice encripta o seu cúbit $|\varphi\rangle$ aplicando as portas X e Z en función dos bits da súa chave, segundo a Ecuación (2.3). Para desencriptar, basta con que Bob aplique as mesmas portas cando recibe o cúbit,

$$|c_i\rangle\, Z^{k_{2i}} X^{k_{1i}} = X^{k_{1i}} Z^{k_{2i}}\, |m_i\rangle\, Z^{k_{2i}} X^{k_{1i}} = |m_i\rangle \qquad \forall i \in \{1, \dots, M\}.$$

Este é un protocolo que precisa dunha canle segreda a través da cal enviar a chave k. Tamén podería empregarse a QKD para xerar esta chave a través dunha canle pública.

2.4. Kak's three stage protocol

Outro protocolo criptográfico de enorme interese é o protocolo en tres etapas, desenvolvido por Subhash Kak en 2006. Este sistema destaca por prescindir dunha chave k e das típicas bases $\{|0\rangle, |1\rangle\}$, $\{|+\rangle, |-\rangle\}$; no seu lugar, encríptase directamente o estado arbitrario do cúbit que se pretende enviar.

O protocolo, descrito por Kak (2006), funciona do seguinte xeito. Alice toma o seu cúbit $|\varphi\rangle$, aplícalle unha porta unitaria U_A e, a continuación, envíallo a Bob. Este engade ao cúbit a súa propia porta U_B, tal que a relación entre ambas portas sexa conmutativa $U_A U_B = U_B U_A$. Bob devólvelle o cúbit a Alice, e esta "desfai" a súa parte do encriptado aplicando a transformación conxugada inversa $U_A^\dagger$,

$$U_A^\dagger U_B U_A\, |\varphi\rangle = U_A^\dagger U_A U_B\, |\varphi\rangle = U_B\, |\varphi\rangle\,.$$

Por último, Bob recibe o cúbit e fai actuar $U_B^\dagger U_B\, |\varphi\rangle$, obtendo o cúbit de partida.

Como vemos no esquema da Figura 2.3, en ningún momento o cúbit viaxa sen encriptar. Un potencial ataque de Eve sería inutil, posto que, de querer colapsar o estado do cúbit, obtería un resultado totalmente aleatorio.

Unha das portas máis doadas de implementar que cumpren estes requisitos son as portas de rotación

$$R(\theta) = \begin{pmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta, \end{pmatrix},$$

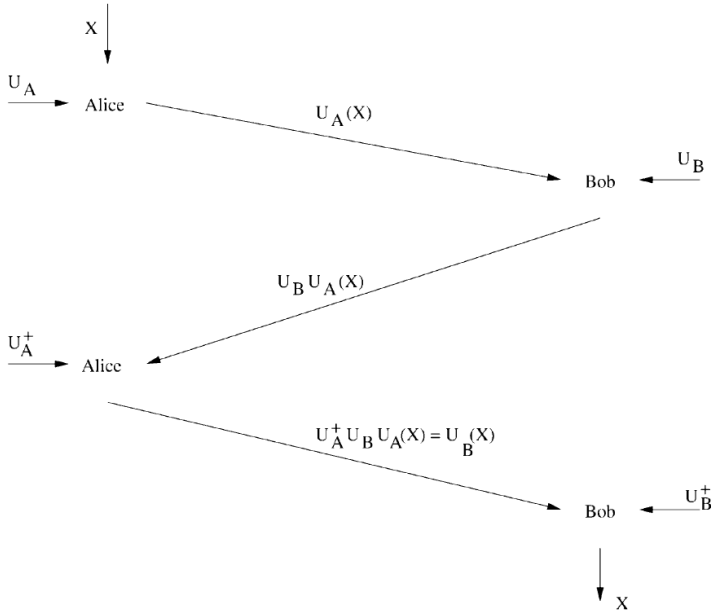


Figura 2.3: Esquema do protocolo criptográfico en tres etapas. Extraído de Kak (2006).

pois aplicar a súa trasposta conxugada consiste en reverter o ángulo $R(\theta)^\dagger = R(-\theta)$. Deste xeito, Alice e Bob poderían escoller cada un os seus propios ángulos θ, $\phi \in [0, 2\pi]$, sen depender do outro.

Como adiantábamos na introducción deste apartado, o protocolo logra prescindir dunha chave e dos requisitos asociados a ela (canle segura, segreda ou autenticada). Non obstante, engade a pega de que hai que triplicar a cantidade de comunicacións que se levan a cabo. Nos anteriores casos, bastaba con que Alice enviase a súa parte da encriptación unha soa vez, mentres que aquí Bob ten que devolver a información e Alice ten que volvela enviar. Isto pode supoñer un grave problema á hora de implementar este protocolo, dado que os estados cuánticos son coñecidos pola súa curta duración de coherencia.

Capítulo 3

Corrección de erros cuántica

A pesar de que a teoría cuántica e os protocolos criptográficos que vimos ata o de agora consideran unha canle ideal na que toda a información que se transmite chega ao destinatario sen interferencias, os ordenadores cuánticos e as canles cuánticas non son, en absoluto, perfectas. De feito, un dos maiores ralentizadores do avance cuántico é a presenza de ruído, que trata de colapsar a función de onda á hora de transmitir cúbits. Este capítulo trata sobre os principais códigos que intentan paliar este fenómeno.

3.1. Dificultades

A corrección de erros cuántica non pode pretender seguir os pasos da clásica, dado que a natureza da comunicación é intrinsecamente distinta. En Nielsen e Chuang (2011), preséntanse tres dificultades primordiais á hora de plantexar un código corrector:

1. **O teorema de non clonación.** Como vimos no apartado 1.6.1, non é posible facer sucesivas copias dun estado $|\varphi\rangle$ tal que $|\varphi\rangle \otimes |\varphi\rangle \otimes ...$, polo que non podemos aplicar directamente os métodos básicos de redundancia de información.

2. **Espectro continuo.** A diferencia dos bits que só toman valores entre 0 e 1, os cúbits cubren un espectro continuo entre ambos $\alpha |0\rangle + \beta |1\rangle$, polo que en moitos casos non basta con invertir unha medida.

3. **Medición.** No caso clásico, obtemos o *output* dunha canle e aplicamos os códigos correctores correspondentes. Non obstante, no caso cuántico, observar significa destruir a información, polo que precisamos de ferramentas que nos permitan identificar se se cometeu un erro sen medir o cúbit.

Tendo isto en mente, presentamos os primeiros códigos correctores de erros que se

desenvolveron no ámbito das comunicacións cuánticas.

3.2. Inversión de bit

Chamamos inversión de bit ao erro cometido cando obtemos o bit contrario ao que tiñamos enviado. Sexa P a probabilidade de que se dé a inversión dun bit a través da canle, supoñendo sempre que $P \leq 1/2$, unha hipótese razoable se pretendemos transmitir algunha información.

O código clásico máis sinxelo é a repetición do bit

$$0 \longrightarrow 000$$
$$1 \longrightarrow 111,$$

onde engadimos redundancia de información e, se se produce a inversión de bit, escollemos o bit maioritario no paquete recibido. Por exemplo: se recibimos 101, aceptamos que a información enviada orixinalmente foi 1 e se cometeu unha inversión accidental no segundo bit do paquete. A probabilidade de cometer un erro, é dicir, a probabilidade de que se tivesen volteado dous ou máis bits, é de

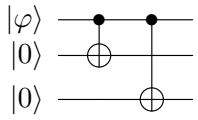
$$3P^2(1-P) + P^3 = 3P^2 - 2P^3 < P,$$

que se reduce en comparación á probabilidade P inicial.

Nas comunicacións cuánticas, suporemos que a inversión de bit é equivalente á aplicación accidental dunha porta X no cúbit. Como adiantabamos no apartado anterior, non podemos clonar un cúbit para emular o código clásico, pero si que podemos enlazalo con outros cúbits para xerar redundancia. Isto foi o que propuxo Peres (1985): entrelazar o estado $|\varphi\rangle$ con dous cúbits de redundancia inicializados a $|0\rangle$ para producir

$$\alpha\,|000\rangle + \beta\,|111\rangle\,.$$

Un posible circuíto que faga isto sería



Demostración 3.1. Sexa $|\varphi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ o cúbit que se pretende enviar e $|0\rangle \otimes |0\rangle$ dous cúbits de redundancia. Aplicando a primeira porta CNOT temos

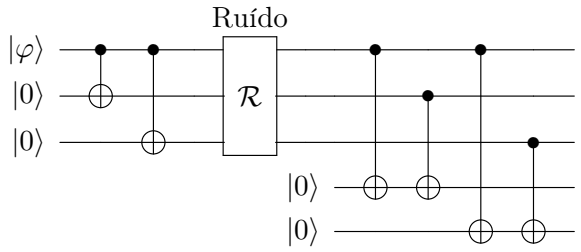
$$CNOT_{1,2}\,(\alpha\,|000\rangle + \beta\,|100\rangle) = \alpha\,|000\rangle + \beta\,|110\rangle\,,$$

e aplicando a segunda,

$$CNOT_{1,3}\,(\alpha\,|000\rangle + \beta\,|110\rangle) = \alpha\,|000\rangle + \beta\,|111\rangle\,.$$

□

Para detectar o síndrome[1], Peres (1985) propuxo enlazar outros dous cúbits que actuarán como identificadores do erro. Devitt et al. (2013) empregan o seguinte circuíto para tal tarefa.



Ao sair da canle con ruído, o estado pode terse transformado en calquera dos seguintes[2]

$$\alpha|000\rangle + \beta|111\rangle,$$
$$\alpha|001\rangle + \beta|110\rangle,$$
$$\alpha|010\rangle + \beta|101\rangle,$$
$$\alpha|100\rangle + \beta|011\rangle.$$

sendo o primeiro o orixinal e todos os demais, as posibles combinacións de producirse unha inversión dun bit. Supoñamos que se atopa en calquera dos catro con probabilidades $\gamma_i, \forall i \in \{1,2,3,4\}$,

$$\gamma_1(\alpha|000\rangle + \beta|111\rangle) + \gamma_2(\alpha|001\rangle + \beta|110\rangle) + \gamma_3(\alpha|010\rangle + \beta|101\rangle) + \gamma_4(\alpha|100\rangle + \beta|011\rangle).$$

Imos traballar agora só coa parte dos α e a parte dos β será completamente análoga,

$$\alpha(\gamma_1|000\rangle + \gamma_2|001\rangle\,\gamma_3|010\rangle + \gamma_4|100\rangle).$$

Engadimos os cúbits auxiliares $|0\rangle_4 \otimes |0\rangle_5$[3]

$$|q^{(1)}\rangle = \alpha(\gamma_1|00000\rangle + \gamma_2|00100\rangle\,\gamma_3|01000\rangle + \gamma_4|10000\rangle),$$

e aplicamos as portas CNOT que aparecen representadas no circuíto

$$CNOT_{1,4}|q^{(1)}\rangle = \alpha(\gamma_1|00000\rangle + \gamma_2|00100\rangle\,\gamma_3|01000\rangle + \gamma_4|10010\rangle) = |q^{(2)}\rangle$$
$$CNOT_{2,4}|q^{(2)}\rangle = \alpha(\gamma_1|00000\rangle + \gamma_2|00100\rangle\,\gamma_3|01010\rangle + \gamma_4|10010\rangle) = |q^{(3)}\rangle$$
$$CNOT_{1,5}|q^{(3)}\rangle = \alpha(\gamma_1|00000\rangle + \gamma_2|00100\rangle\,\gamma_3|01010\rangle + \gamma_4|10011\rangle) = |q^{(4)}\rangle$$
$$CNOT_{3,5}|q^{(4)}\rangle = \alpha(\gamma_1|00000\rangle + \gamma_2|00101\rangle\,\gamma_3|01010\rangle + \gamma_4|10011\rangle).$$

[1] O síndrome refírese ao tipo de erro que se cometeu.

[2] Asumiremos que só se invertiu un bit, dado que o código non corrixe máis dun erro.

[3] Empregaremos a nomenclatura auxiliar $|q^{(i)}\rangle, i \in \mathbb{N}$ para os seguintes pasos da demostración, por simplicidade.

Facemos o mesmo con β,

$$\beta\left(\gamma_1\left|11100\right\rangle + \gamma_2\left|11001\right\rangle + \gamma_3\left|10110\right\rangle + \gamma_4\left|01111\right\rangle\right),$$

e sumando ambas ecuacións e reescribíndoas, obtemos

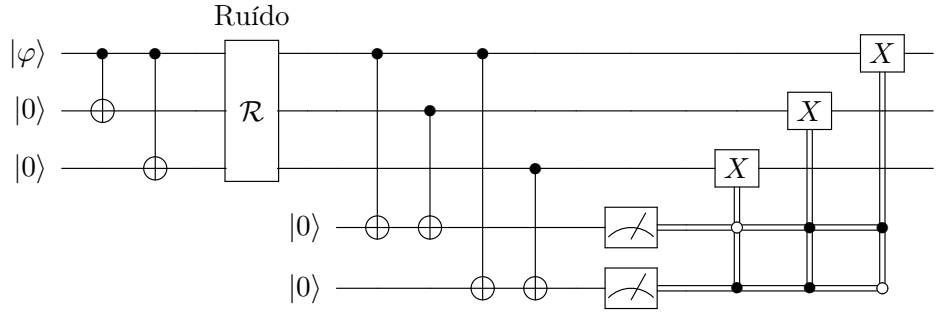
$$\begin{aligned}\gamma_1\left(\alpha\left|000\right\rangle + \beta\left|111\right\rangle\right)\otimes\left|00\right\rangle + \gamma_2\left(\alpha\left|001\right\rangle + \beta\left|110\right\rangle\right)\otimes\left|01\right\rangle + \\ + \gamma_3\left(\alpha\left|010\right\rangle + \beta\left|101\right\rangle\right)\otimes\left|11\right\rangle + \gamma_4\left(\alpha\left|100\right\rangle + \beta\left|011\right\rangle\right)\otimes\left|10\right\rangle. \quad (3.1)\end{aligned}$$

Os resultados desta Ecuación (3.1) quedan recollidos na Táboa 3.1 para maior claridade. Como podemos observar, os últimos dous bits auxiliares que engadimos dannos información sobre onde se cometeu o erro. Podemos establecer unha bixección entre o valor do síndrome en binario e a posición do cúbit na que ocorreu a inversión, sendo $\left|01\right\rangle$ o síndrome do cúbit menos significativo (terceira posición), e así sucesivamente.

Probabilidade (P)	Estado	Síndrome	Corrección
γ_1	$\alpha\left\|000\right\rangle + \beta\left\|111\right\rangle$	$\left\|00\right\rangle$	I
γ_2	$\alpha\left\|001\right\rangle + \beta\left\|110\right\rangle$	$\left\|01\right\rangle$	X_3
γ_3	$\alpha\left\|010\right\rangle + \beta\left\|101\right\rangle$	$\left\|10\right\rangle$	X_2
γ_4	$\alpha\left\|100\right\rangle + \beta\left\|011\right\rangle$	$\left\|11\right\rangle$	X_1

Táboa 3.1: Táboa dos posibles estados despois da inversión dun bit cos seus síndromes correspondentes e as correccións a aplicar para volver obter o estado enviado.

Unha vez feito isto, teríamos que medir os cúbits auxiliares do síndrome e corrixir o erro no cúbit pertinente en función do resultado. Como podemos observar na Táboa 3.1, basta aplicar unha porta X no cúbit errado. Por exemplo, supoñamos que medimos $\left|11\right\rangle$ no síndrome. Entón sabemos que o estado inicial cambiou accidentalmente a $\alpha\left|100\right\rangle + \beta\left|011\right\rangle$ tras atravesar a canle con ruído. Por tanto, para corrixilo aplicamos unha porta X no primeiro cúbit, que foi o que sufriu a inversión. Deste xeito, recuperamos $\alpha\left|000\right\rangle + \beta\left|111\right\rangle$. O circuíto final, cas portas correctoras incluídas, sería[4]



[4]Neste circuíto, empregamos unha nova notación para as portas controladas no que o punto baleiro ou en blanco indica que o valor de contorl é o 0, fronte ao 1 habitual.

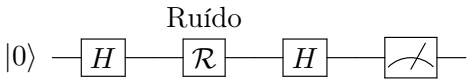
Segundo Nielsen e Chuang (2011), a probabilidade de que un erro quede sen corrixir con este circuíto cuántico é de

$$3P^2 - 2P^3,$$

ao igual que no caso clásico.

3.3. Inversión de fase

Outro tipo de erros que temos que considerar no caso cuántico son as inversións de fase, que non teñen análogo clásico; por exemplo, que o estado $\alpha|0\rangle + \beta|1\rangle$ se convirta en $\alpha|0\rangle - \beta|1\rangle$, ou sexa, a aplicación accidental dunha porta Z con probabilidade P. Podería parecer que este erro non é significativo, dado que as probabilidades de medir $|0\rangle$ ou $|1\rangle$ mantéñense igual ao non cambiar α nin β, mais habemos de ter en conta que os erros se poden producir en calquera punto do circuíto. Analicemos o seguinte caso.



Enviamos o cúbit $|0\rangle$ ao que lle aplicamos unha porta H e convertemos en $|+\rangle$. Esperamos poder recibir o cúbit sen problemas, para poder aplicar de novo a porta H e recuperar $|0\rangle$, dado que $HH = I$. Non obstante, produciuse unha interferencia entre as dúas portas, e o cúbit

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

sufriu unha inversión de fase,

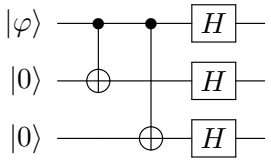
$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle\,.$$

Agora, ao aplicar a porta H,

$$H|-\rangle = |1\rangle\,,$$

obtivemos o cúbit $|1\rangle$, cando inicialmente tiñamos enviado $|0\rangle$. As inversións de fase poden ser, por tanto, igual de perigosas que as inversións de bit, así que debemos atopar un método para identificalas e corrixilas.

Segundo Nielsen e Chuang (2011), existe unha maneira de facer que a inversión de fase se convirta nunha inversión de bit e aplicar o método do apartado 3.2 anterior. Similar ao exemplo que acabamos de analizar, cambiamos de base $\{|0\rangle, |1\rangle\}$ a $\{|+\rangle, |-\rangle\}$ aplicando portas H a todos os cúbits.



Isto convertirá o noso estado $\alpha\,|000\rangle + \beta\,|111\rangle$ en $\alpha\,|+++\rangle + \beta\,|---\rangle$.

Demostración 3.2. Sexa $|\varphi\rangle = \alpha\,|000\rangle + \beta\,|111\rangle$ construído a partir das portas CNOT e dous cúbits de redundancia como no apartado 3.2. Agora, aplicamos sucesivamente as tres portas de Hadamard[5],

$$H_1\left(\alpha\,|0\rangle\otimes|00\rangle + \beta\,|1\rangle\otimes|11\rangle\right) = \alpha\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\otimes|00\rangle + \beta\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\otimes|11\rangle = \\ = \frac{\alpha}{\sqrt{2}}\left(|000\rangle+|100\rangle\right) + \frac{\beta}{\sqrt{2}}\left(|011\rangle-|100\rangle\right) = |q^{(1)}\rangle\,.$$

A segunda e a terceira son análogas á primeira, actuando nos seus respectivos cúbits

$$H_2\,|q^{(1)}\rangle = \frac{1}{2}\Big[\alpha\big(|000\rangle+|010\rangle+|100\rangle+|110\rangle\big)+\beta\big(|001\rangle-|011\rangle-|100\rangle+|110\rangle\big)\Big] = |q^{(2)}\rangle\,,$$

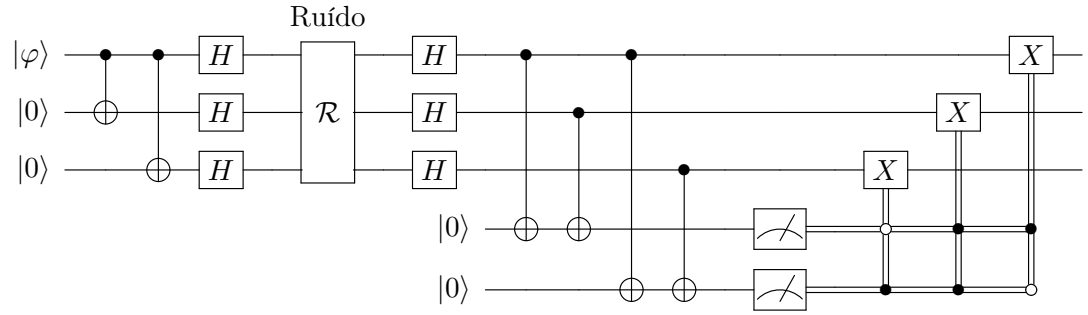
$$H_3\,|q^{(2)}\rangle = \frac{1}{2\sqrt{2}}\Big[\alpha\big(|000\rangle+|001\rangle+|010\rangle+|011\rangle+|100\rangle+|101\rangle+|110\rangle+|111\rangle\big)+ \\ +\beta\big(|000\rangle-|001\rangle-|010\rangle+|011\rangle-|100\rangle+|101\rangle+|110\rangle-|111\rangle\big)\Big] = |q^{(3)}\rangle\,.$$

Finalmente, $|q^{(3)}\rangle$ pódese reordenar para dar

$$|q^{(3)}\rangle = \frac{\alpha}{2\sqrt{2}}\big(|0\rangle+|1\rangle\big)\otimes\big(|0\rangle+|1\rangle\big)\otimes\big(|0\rangle+|1\rangle\big)+\frac{\beta}{2\sqrt{2}}\big(|0\rangle-|1\rangle\big)\otimes\big(|0\rangle-|1\rangle\big)\otimes\big(|0\rangle-|1\rangle\big) = \\ = \alpha\,|+++\rangle + \beta\,|---\rangle\,.$$

□

A partir deste punto, a potencial inversión de fase fará que os cúbits $|+\rangle$ se volvan $|-\rangle$, e viceversa. Por tanto, unha vez superada a fonte de ruído, basta con aplicar de novo as portas H para volver á base $\{|0\rangle\,,|1\rangle\}$ e a detección de síndrome e posterior corrección de erros sería exactamente igual que na inversión de bit.



[5]Será de axuda escribir explicitamente o estado $|000\rangle$ como o produto tensorial dos tres cúbits $|0\rangle\otimes|0\rangle\otimes|0\rangle$, para visualizar máis facilmente a aplicación das portas H.

3.4. O código de Shor

Existe a posibilidade de corrixir ambos erros, a inversión de bit e de fase, á vez? Esta foi a pregunta que se fixo Peter Shor e para a cal propuxo a seguinte solución (Shor, 1995).

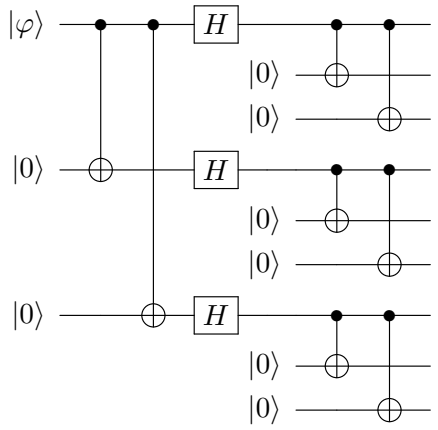
Tomemos desta vez 9 cúbits entrelazados

$$|0_S\rangle = \frac{1}{2\sqrt{2}} (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)$$
$$|1_S\rangle = \frac{1}{2\sqrt{2}} (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle),$$

de xeito que os cúbits terían o estado total

$$\alpha |0_S\rangle + \beta |1_S\rangle .$$

Nielsen e Chuang (2011) propoñen o circuíto a continuación para representar este estado.



Dispóñense os cúbits deste xeito para ver máis claramente que a construción é simplemente a concatenación dos dous casos anteriores. Na primeira parte, temos o circuíto correspondente á inversión de fase e, na segunda parte, temos en cada cúbit unha versión individual do cambio de bit.

Vexamos como se corrixen os erros neste formato. Lidar e Brun (2013) propoñen unha explicación baseada en subespazos. No que concirne aos erros de bit, observamos que todos os cúbits son combinacións de $|000\rangle$ e $|111\rangle$, e sabemos que o código os corrixe. Por outro lado, con respecto ás inversións de fase, estes paquetes de cúbits transfórmanse do mesmo xeito que os cúbits individuais

$$Z|0\rangle = |0\rangle \qquad Z_1|000\rangle = |000\rangle$$
$$Z|1\rangle = -|1\rangle \qquad Z_1|111\rangle = -|111\rangle .$$

Empregamos a porta Z_1 como exemplo, pero a regra é válida para unha porta Z actuando sobre calquera dos cúbits, sempre e cando só actué sobre un deles. Por tanto, podemos considerar que a nova base do noso estado é $\{|000\rangle, |111\rangle\}$ e o circuíto reduciríase ao da sección 3.3, corrixindo un erro de inversión de fase.

Non só iso, senón que o circuíto corrixe a acción combinada dunha porta X e unha porta Z sobre o mesmo cúbit. Como cada unha das portas actúa sobre un eixo distinto da esfera de Bloch, Nielsen e Chuang (2011) razonan que, de aplicarse accidentalmente o operador Z_1X_1, o sistema detectaría primeiro o cambio de bit e correxiríao e, despois, atoparía e solventaría a inversión de fase. O circuíto completo pódese atopar no Anexo A.

3.5. Erros arbitrarios nun único cúbit

O código de Shor é máis potente do que podería parecer inicialmente, dado que, como vimos na sección 1.4.1, as matrices de Pauli anticonmutan, polo que tamén corrixe aplicacións accidentais do operador Y,

$$ZX = iY, \tag{3.2}$$

onde i sería unha fase global que non afectaría ao sistema.

Ademais, Steane (1996), que desenvolveu o mesmo código que Shor paralelamente a el, afirma que calquera código que corrixa dous tipos de erros, tamén correxirá unha combinación linear deles.

Con estes datos, poderíamos plantexarnos que ocorre se se lle aplica ao sistema un operador arbitrario $\mathcal{R}$, por exemplo, unha porta de rotación $R(\theta)$ con ángulo $\theta \in [0, \pi]$. Como adiantabamos no apartado 1.4.1, calquera operador actuando sobre un único cúbit, pode poñerse como combinación linear das matrices de Pauli,

$$\mathcal{R} = r_1 I + r_2 X + r_3 Z + r_4 ZX, \tag{3.3}$$

onde xa substituímos a Ecuación (3.2) (Nielsen e Chuang, 2011). Así, como o código de Shor é capaz de corrixir erros X e Z, poderá corrixir a combinación linear da Ecuación (3.3) e, por tanto, calquera erro arbitrario que lle poida suceder a un cúbit do circuíto.

Este resultado é de importantísima relevancia no mundo da computación cuántica, pois mostra que se poden converter os erros continuos en erros discretos. Quere dicir que, sen importar o tipo de erro que se cometa na comunicación, un algoritmo que solvente un número finito e discreto de erros poderá corrixilo.

O código de Shor foi posteriormente mellorado por Steane (1996), que conseguiu o mesmo resultado empregando 7 cúbits cun código estabilizador e, finalmente, por Laflamme

et al. (1996) quenes atoparon un de 5 e demostraron que ese era o mínimo número necesario para corrixir erros arbitrarios sobre un só cúbit.

Conclusións

Comezamos presentando o cúbit e vendo como a analoxía co sistema binario funcionaba para representar varios cúbits en circuítos na notación de Dirac. Con isto puidemos introducir os operadores cuánticos, tamén chamados portas lóxicas, entre eles as matrices de Pauli (X, Y, Z), que conforman a base de todas as portas que se aplican sobre un só cúbit. Tamén vimos outras portas de grande utilidade á hora de estudar criptografía: a porta Hadamard, que xera unha superposición e nos permite cambiar á base $\{|+\rangle, |-\rangle\}$, e a porta CNOT, que entrelaza cúbits. Fixemos a representación gráfica dun estado cuántico sobre a esfera de Bloch, que sería de gran utilidade máis adiante para entender a cantidade de información que se está a enviar.

Sobre a teoría da información, vimos os teoremas e fenómenos máis representativos nas comunicacións cuánticas, que non teñen análogo clásico e fan desta unha teoría única. Son así o teorema de non clonación, que nos dificulta a tarefa de "repetir" cúbits nos códigos correctores, pero que finalmente se pode solventar; tamén a teleportación cuántica, na que se basan os códigos para saber o estado no que se atopa o cúbit sen colapsalo; e por último, a codificación superdensa, na que case podemos facer un intercambio de dous bits de información por un cúbit.

O capítulo segundo comeza presentando un dos problemas máis sonados a día de hoxe sobre a criptografía clásica: a dificultade de resolver o problema de factorización en números primos. Non obstante, grazas ao algoritmo de Shor, vemos que un ordenador cuántico sería potencialmente capaz de resolver este problema en exponencialmente menos tempo, podendo chegar a ser unha ameaza para os sistemas basados en RSA. É por iso que xorde a necesidade dunha criptografía cuántica, e aparecen os primeiros protocolos, como o BB84, o máis soado para a distribución cuántica de chaves. Grazas a el, podemos distribuir unha chave a través dunha canle pública e solventar os problemas das canles segredas ou privadas que teñen moitos protocolos da criptografía clásica. Vimos tamén como un protocolo sinxelo de criptografía clásica ten o seu análogo cuántico, o caderno de uso único. E para concluír este capítulo, presentamos o protocolo de Kak en tres etapas, unha maneira de facer criptografía cuántica sen necesidade dunha chave, coa desvantaxe de tripiclar o número de veces que se establece a comunicación entre as dúas partes.

No último capítulo, estudamos os códigos correctores de erros. Como adiantabamos, o teorema de non clonación podería supoñer un problema para xerar redundancia na información como se fai no caso clásico; non obstante, grazas ao entrelazamento cuántico somos quen de repetir o valor dos cúbits para cerciorarnos de que a canle con ruído non perturba o estado. Comezamos corrixindo un bit de información na base $\{|0\rangle, |1\rangle\}$ fronte a erros de aplicación da porta X. Seguimos coa corrección de erros de inversión de base, é dicir, a aplicación accidental de Z, que demostramos que son equivalentes aos de cambio de bit simplemente modificando a base a $\{|+\rangle, |-\rangle\}$. Despois disto, presentamos o código de Shor, un algoritmo que combina a corrección destes dous erros e que se proba máis potente do que inicialmente podería parecer, dado que grazas ao feito de que todas as portas sobre un cúbit se poden expresar como combinación linear das matrices de Pauli, o código de Shor acaba por corrixir todo tipo de erros arbitrarios sobre un cúbit.

Con isto remata o traballo, mais non o tema, pois quedan moitos protocolos e códigos sen comentar que escapan do alcance deste manuscrito por temática e extensión. Tales son o protocolo BBM92 (Bennett et al., 1992), que mellora o protocolo BB84 empregando só dous estados en lugar de catro; os códigos lineares cuánticos, análogos dos clásicos, dos que se pode falar tamén da distancia de Hamming e de matrices xeradoras; ou as matrices densidade ρ, das cales só demos un par de pinceladas, pero que permiten desenvolver unha teoría sólida da información cuántica, similar á de Shannon.

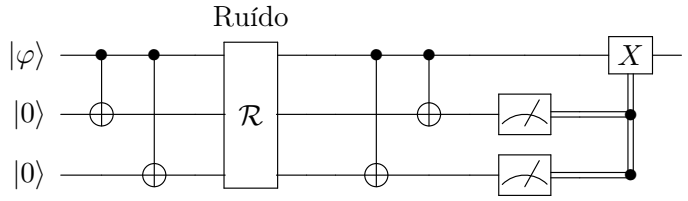
Con respecto ao futuro das comunicacións cuánticas, estamos comezando a ver os primeiros ordenadores de decenas ou incluso centos de cúbits. Lonxe están dos seus análogos clásicos, mais co rápido desenvolvemento das tecnoloxías, poderíamos ver estes protocolos postos a proba no próximo decenio. Para rematar, é preciso incidir en que as novas comunicacións cuánticas non buscan, ou non deberían buscar, substituír o traballo das clásicas, pois ningunha das dúas é capaz de cubrir por completo as funcións da outra. Como se viu nos protocolos de criptografía, hai lugar para combinar ambas tecnoloxías, e facéndoo, obtemos resultados óptimos.

> *A beautiful and complete theory has been developed of how entangled quantum states can assist classical communication over quantum channels.*
>
> (Michael A. Nielsen & Isaac L. Chuang)

Anexo A

O código de Shor

Antes de mostrar o circuíto completo para o código de Shor, imos empregar unha versión reducida do circuíto que corrixe unha inversión de bit, no cal se prescinde dos cúbits auxiliares para a detección do síndrome e se empregan directamente os cúbits de redundacia para tal función. Lidar e Brun (2013) propoñen o seguinte circuíto para esta tarefa.



Demostración A.1. Comprobemos que este circuíto corrixe unha inversión de cúbit. Sexa $|q^{(1)}\rangle$ o seguinte

$$\gamma_1 (\alpha |000\rangle + \beta |111\rangle) + \gamma_2 (\alpha |001\rangle + \beta |110\rangle) + \gamma_3 (\alpha |010\rangle + \beta |101\rangle) + \gamma_4 (\alpha |100\rangle + \beta |011\rangle),$$

o estado mestura despois de pasar pola canle con ruído. Entón, aplicando o par de portas CNOT, temos

$$CNOT_{1,3} |q^{(1)}\rangle = \gamma_1 (\alpha |000\rangle + \beta |110\rangle) + \gamma_2 (\alpha |001\rangle + \beta |111\rangle) + \\ + \gamma_3 (\alpha |010\rangle + \beta |100\rangle) + \gamma_4 (\alpha |101\rangle + \beta |011\rangle) = |q^{(2)}\rangle,$$

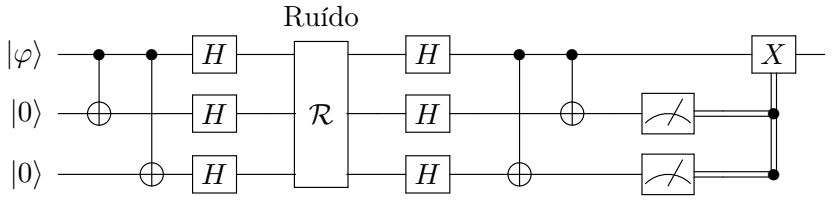
$$CNOT_{1,2} |q^{(2)}\rangle = \gamma_1 (\alpha |000\rangle + \beta |100\rangle) + \gamma_2 (\alpha |001\rangle + \beta |101\rangle) + \\ + \gamma_3 (\alpha |010\rangle + \beta |110\rangle) + \gamma_4 (\alpha |111\rangle + \beta |011\rangle) = |q^{(3)}\rangle.$$

O estado $|q^{(3)}\rangle$ pode reescribirse en función do cúbit inicial $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ e do síndrome como

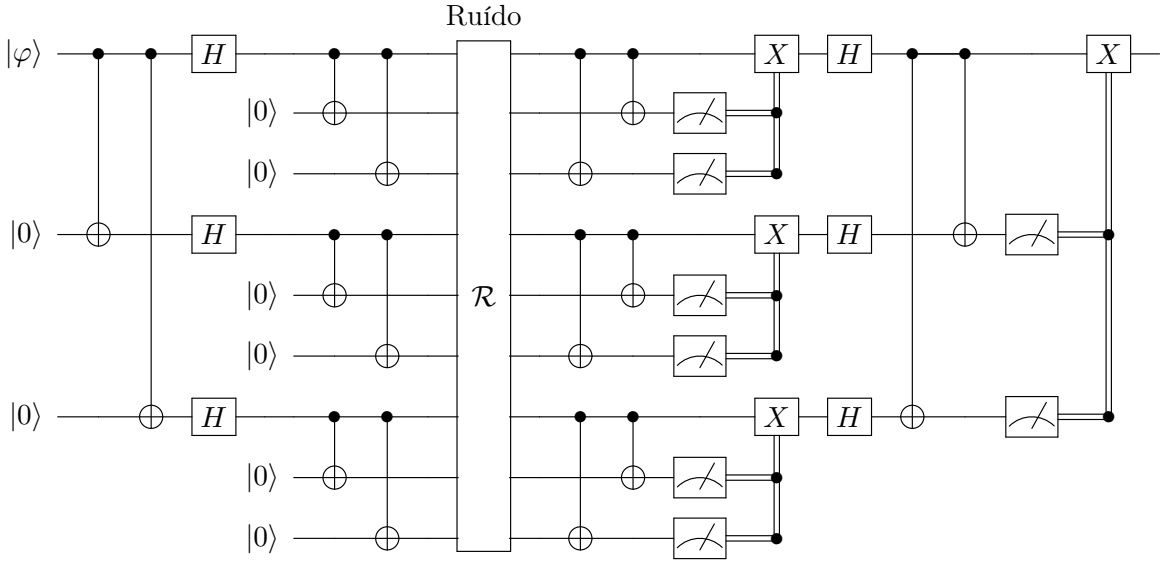
$$|q^{(3)}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma_1|00\rangle + \gamma_2|01\rangle + \gamma_3|10\rangle) + (\alpha|1\rangle + \beta|0\rangle) \otimes \gamma_4|11\rangle .$$

Logo, se medimos $|11\rangle$ nos cúbits de redundancia, deberemos aplicar unha porta X correctora. En calquera outro caso, o cúbit será xa $|\varphi\rangle$. □

Como vimos na sección 3.3., a inversión de fase é análoga á inversión de bit, cun cambio de base mediante portas H.



Por tanto, o circuíto completo do código de Shor será



Bibliografía

E. Abers. *Quantum Mechanics*. Pearson Education, 2004. ISBN 9780131461000.

G. V. Assche. *Quantum Cryptography and Secret-Key Distillation*. Cambridge University Press, USA, 2006. ISBN 0521864852.

C. H. Bennett e G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, Dec. 1984. ISSN 0304-3975. doi: 10.1016/j.tcs.2014.05.025.

C. H. Bennett, G. Brassard, e N. D. Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992. doi: 10.1103/PhysRevLett.68.557.

P. O. Boykin e V. Roychowdhury. Optimal encryption of quantum bits. *Physical Review A*, 67(4), Apr. 2003. ISSN 1094-1622. doi: 10.1103/physreva.67.042317.

A. Carrasco-Casado, V. Fernández, e N. Denisenko. *Free-Space Quantum Key Distribution*, page 589–607. Springer International Publishing, 2016. ISBN 9783319302010. doi: 10.1007/978-3-319-30201-0_27.

R. Crandall e C. Pomerance. *Prime Numbers: A Computational Perspective*. Lecture notes in statistics. Springer New York, 2006. ISBN 9780387289793.

S. J. Devitt, W. J. Munro, e K.Ñemoto. Quantum error correction for beginners. *Reports on Progress in Physics*, 76(7):076001, June 2013. ISSN 1361-6633. doi: 10.1088/0034-4885/76/7/076001.

P. A. M. Dirac. A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society*, 35(3):416–418, 1939. doi: 10.1017/S0305004100021162.

J. P. Gordon. Quantum effects in communications systems. *Proceedings of the IRE*, 50(9): 1898–1908, 1962. doi: 10.1109/JRPROC.1962.288169.

S. Kak. A three-stage quantum cryptography protocol. *Foundations of Physics Letters*, 19 (3):293–296, Apr. 2006. ISSN 1572-9524. doi: 10.1007/s10702-006-0520-9.

R. Laflamme, C. Miquel, J. P. Paz, e W. H. Zurek. Perfect quantum error correcting code. *Phys. Rev. Lett.*, 77:198–201, Jul 1996. doi: 10.1103/PhysRevLett.77.198.

D. Lidar e T. Brun. *Quantum Error Correction*. Cambridge University Press, 2013. ISBN 9780521897877.

V. Moret-Bonillo. *Adventures in Computer Science: From Classical Bits to Quantum Bits*. Springer International Publishing, 2018. ISBN 9783319878775.

M. A. Nielsen e I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, USA, 10th edition, 2011. ISBN 1107002176.

A. Peres. Reversible logic and quantum computers. *Phys. Rev. A*, 32:3266–3276, Dec 1985. doi: 10.1103/PhysRevA.32.3266.

S. Rasmussen, K. Christensen, S. Pedersen, L. Kristensen, T. Bækkegaard, N. Loft, e N. Zinner. Superconducting circuit companion—an introduction with worked examples. *PRX Quantum*, 2(4), Dec. 2021. ISSN 2691-3399. doi: 10.1103/prxquantum.2.040204.

W. Scherer. *Mathematics of Quantum Computing: An Introduction*. Springer Publishing Company, Incorporated, 1st edition, 2019. ISBN 303012357X.

C. E. Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423, 1948.

P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994. doi: 10.1109/SFCS.1994.365700.

P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52:R2493–R2496, Oct 1995. doi: 10.1103/PhysRevA.52.R2493.

P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, Oct. 1997. ISSN 1095-7111. doi: 10.1137/s0097539795293172.

A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77:793–797, Jul 1996. doi: 10.1103/PhysRevLett.77.793.

T. Vidick e S. Wehner. *Introduction to Quantum Cryptography*. Cambridge University Press, 2023. ISBN 9781316515655.