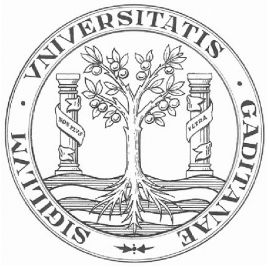

UNIVERSIDAD DE CÁDIZ

FACULTAD DE CIENCIAS

GRADO EN MATEMÁTICAS

CRIPTOGRAFÍA POSCUÁNTICA

Trabajo de fin de grado presentado por

Juan Antonio Guitarte Fernández

Tutor: Dr. Nombre apellidos del tutor

Firma del alumno Firma del tutor

Puerto Real, Cádiz, Julio de 2.020

Abstract

Five years ago, a first volume of open problems in Mathematical Systems and Control Theory appeared.

Some of the 53 problems that were published in this volume attracted considerable attention in the research community. The book in front of you contains a new collection of 63 open problems. The contents of both volumes show the evolution of the field in the half decade since the publication of the first volume. One noticeable feature is the shift toward a wider class of questions and more emphasis on issues driven by physical modeling.

Early versions of some of the problems in this book have been presented at the Open Problem sessions of the Oberwolfach Tagung on Regelungstheorie, on February 27, 2002, and of the Conference on Mathematical Theory of Networks and Systems (MTNS) in Notre Dame, Indiana, on August 12, 2002. The editors thank the organizers of these meetings for their willingness to provide the problems this welcome exposure. Since the appearance of the first volume, open problems have continued to meet with large interest in the mathematical community. Undoubtedly, the most spectacular event in this arena was the announcement by the Clay Mathematics Institute of the Millennium Prize Problems whose solution will be rewarded by one million U.S. dollars each. Modesty and modesty of means have prevented the editors of the present volume from offering similar rewards toward the solution of the problems in this book. However, we trust that, notwithstanding this absence of a financial incentive, the intellectual challenge will stimulate many readers to attack the problems. The editors thank in the first place the researchers who have submitted the problems. We are also very thankful to the Princeton University Press, and in particular Vickie Kearn, for their willingness to publish this vol- ume. The full text of the problems, together with comments, additions,

and solutions, will be posted on the book website at Princeton Univer- sity Press (link available from `http://pup.princeton.edu/math/`) and on `http://www.inma.ucl.ac.be/?blondel/op/`.

Readers are encouraged to submit contributions by following the instructions given on these websites.

The editors, Louvain-la-Neuve, March 15, 2003.

A mis padres.

Resumen

Se ha creado e investigado un modelo de interacción entre un fabricante y el estado donde el fabricante produce un solo producto y el estado controla el nivel de contaminación. Se considera una economía local con un problema de contaminación almacenada, que debe escoger entre inversiones en producción y medio ambiente (funciones de control). El modelo es descrito por un sistema de dos ecuaciones diferenciales con dos controles acotados. La mejor estrategia de control se encuentra analíticamente usando el Principio del Máximo de Pontryagin y el Teorema de Green.

En este trabajo analizamos algunos aspectos de la Teoría de Control que incluyen consideraciones sobre sus orígenes, sus motivaciones y su evolución. Describimos algunos elementos matemáticos fundamentales y diversos avances que se caracterizan a la vez por su interés científico y su transcendencia desde un punto de vista social, tecnológico e industrial. También, mencionamos algunos de los retos que se plantean en esta disciplina para un futuro inmediato.

Hay dos divisiones principales de la teoría de control, es decir, clásicos y modernos, que tienen implicaciones directas sobre las aplicaciones de ingeniería de control. La teoría desarrollada para el control de procesos, desde el punto clásico y moderno tiene su base esencial en el conocimiento de la dinámica del proceso que se desea controlar.Desde la teoría clásica de control, considerando el caso más sencillo de un sistema lineal de una entrada y una salida (SISO) del diseño del sistema. Estadinámica normalmente se expresa asiendo uso de ecuaciones diferenciales ordinarias, y en el caso de sistemas lineales, usando de igual manera la transformada de Laplace para obtener así de una representación matemática que relaciona la señal que se quiere controlar y la señal de

entrada al sistemas.Un controlador diseñado por la teoría clásica por lo general requiere en ellugar de sintonía debido a las aproximaciones de diseño. Los controladores diseñado con la teoría de control clásica comunes son los CONTROLADORESPID.En contraste, la teoría de control moderna se lleva acabo estrictamente enel complejo-s o el dominio de la frecuencia y puede lidiar con múltiples entradas y múltiples salidas (MIMO) de sistemas. Esto para diseño sofisticado, como el control de aviones de combate etc.,. En el diseño moderno, un sistema representa como un conjunto de primer orden ecuaciones diferenciales. El área de control moderno tiene muchas áreas que explorar. Lo cual se detallara en este trabajo.

Agradecimientos

Por mi excelencia y formación profesional, gracias a su cariño, guía y apoyo. Este presente simboliza mi gratitud por toda la responsabilidad e inestimable ayuda que siempre me han proporcionado. Porque gracias a su apoyo y consejos, he llegado a realizar una de mis grandes metas lo cual constituye la herencia más valiosa que piduera recibir.

Con un testimonio de eterno agradecimiento por el apoyo moral que desde siempre me brindaron y con el cual he logrado terminar mi carrera profesional, que es para mi la mejor de las herencias. Gracias por ayudarme cada día a cruzar con firmeza el camino de la superación, por que con su apoyo y aliento hoy he logrado uno de mis más grandes anhelos.

Por el cariño y apoyo moral que siempre he recibido de ustedes y con el cual he logrado culminar mi esfuerzo, terminando así mi carrera profesional, que es para mi la mejor de las herencias.

Al término de esta etapa de mi vida, quiero expresar un profundo agradecimiento a quienes con su ayuda, apoyo y compresión me alentaron a lograr esta hermosa realidad. Como un testimonio de eterno agradecimiento por el gran amor y la confianza que siempre me brindaron, gracias por darme la fuerza para irme superando. Sabiendo que jamás encontraré la forma de agradecer su constante apoyo y confianza, sólo espero que comprendan que mis ideales, esfuerzos y logros han sido también suyos e inspirados en ustedes. Por que gracias a su cariño, apoyo y confianza he llegado a realizar dos de mis más grandes metas en la vida. La culminación de mi carrera profesional y el hacerlos sentirse orgullosos de esta persona que tanto los ama.

A quien jamás encontraré la forma de agradecer el que me haya brindado su mano en las derrotas y logros de mi vida, haciendo de este triunfo más suyo que mío por la forma en la que guió mi vida con amor y energía.

Agradezco de todo corazón a dios y a mis padres por que a través de ellos me concedió la vida en este mundo, así como a mis abuelos, tíos, hermanos, suegros, esposa e hijos y a todas las personas que directa o indirectamente han tenido a bien ayudarme en forma moral y económica para mi formación como ser humano y profesional, en respuesta a esto, cuenten con un gran amigo.

A quien jamás encontraré la forma de agradecer su apoyo, comprensión y confianza esperando que comprendas que mis logros son también tuyos e inspirados en tí, hago de este un triunfo y quiero compartirlo por siempre contigo.

A quienes jamás encontraré la forma de agradecer el cariño, comprensión y apoyo brindado en los momentos buenos y malos de mi vida, hago este triunfo compartido, sólo esperando que comprendan que mis ideales y esfuerzos son inspirados en cada uno de ustedes.

Sabiendo que no existirá forma alguna de agradecer una vida de sacrificios, esfuerzos y amor, quiero que sientan que el objetivo alcanzado también es de ustedes y que la fuerza que me ayudo a conseguirlos fue su gran apoyo.

A dios que me ha heredado el tesoro más valioso que puede dársele a un hijo ”sus padres”. A mis padres quienes sin escatimar esfuerzo alguno sacrificaron gran parte de su vida para educarme. A mis hermanos quienes la ilusión de su vida ha sido verme convertido en un hombre de provecho. Y a todas aquellas personas que comparten conmigo este triunfo.

Con la mayor gratitud por los esfuezos realizados para que yo lograra terminar mi carrera profesional siendo para mi la mejor herencia. A mi madre que es el ser más maravilloso de todo el mundo. Gracias por el apoyo moral, tu cariño y comprensión que desde niño me has brindado, por guiar mi camino y estar junto a mi en los momentos más difíciles. A mi padre porque desde pequeño ha sido para mi un gran hombre maravilloso al que siempre he admirado. Gracias por guiar mi vida con energía, esto ha hecho que sea lo que soy.

Con amor, admiración y respeto.

Pepito Pérez

abril 2020

Índice general

Hay a quien le gusta comenzar cada capítulo con una cita...

Mulachenski

CAPITULO

1

Introduction

CAPITULO

2

Planteamiento y motivación

2.1 El problema de los ordenadores cuánticos

Hoy día, la criptografía está más presente que nunca en nuestro día a día: hacer compras por Internet, navegar por casi cualquier página web, chatear a través del teléfono móvil... Gracias a la criptografía, podemos mantener nuestras comunicaciones privadas y asegurarnos de que cualquier pago que realicemos o documento que publiquemos sólo podemos hacerlo nosotros, es decir, que nadie pueda falsificarlo.

El continuo desarrollo de los ordenadores cuánticos, que romperán los principales algoritmos de firma digital y criptosistemas de clave pública usados hoy en día (por ejemplo, *RSA*, *DSA* y *ECDSA*), puede hacer pensar que cuando la computación cuántica sea una realidad, la criptografía quedará obsoleta, que será imposible modificar información para que sea incomprensible o infalsificable por atacantes y personas no autorizadas; y que por tanto, la única forma de proteger nuestras comunicaciones y nuestros datos será aislarlos físicamente de ellos, por ejemplo, con dispositivos USB cerrados bajo llave en un maletín. Pero, ¿hasta qué punto es esto cierto?

Un estudio más detallado de los algoritmos criptográficos existentes muestra, sin embargo, que existen muchos otros criptosistemas más allá del *RSA*, *DSA* y *ECDSA*:

- **Criptografía basada en funciones hash**. El ejemplo más destacado dentro de este grupo es el sistema de firma con clave pública basado en árboles hash de Merkle

(en inglés, *Merkle's hash-tree public-key signature system*) de 1979, basado en un sistema de firma digital de un solo uso de Lamport y Diffie.

- **Criptografía basada en códigos**. El ejemplo clásico es el sistema de encriptación de clave pública con códigos Goppa ocultos de McEliece (1978).

- **Criptografía basada en retículos**. El ejemplo que más interés ha conseguido atraer, aunque no es el primero propuesto históricamente, esl el sistema de encriptación de clave pública "NTRU" de Hoffstein-Pipher-Silverman (1998).

- **Criptografía de ecuaciones cuadráticas de varias variables**. Uno de los ejemplos más interesantes es el sistema de firma con clave pública "HFE^{v-}" de Patarin (1996), que generaliza una propuesta de Matsumoto e Imai.

- **Criptografía de clave secreta**. El ejemplo más conocido (y usado actualmente) es el cifrado "Rijndael" de Daemen-Rijmen (1998), renombrado como "AES", siglas que significan Estándar de Encriptación Avanzada (Advanced Encryption Standard).

Se cree que todos estos sistemas son resistentes a los ordenadores clásicos y cuánticos, es decir, que no existe un algoritmo eficiente que pueda ser implementado en un ordenador clásico o cuántico que rompa estos sistemas. El algoritmo de Shor (el cual analizaremos más adelante en este trabajo), que permite resolver de manera eficiente el problema de la factorización de números enteros en ordenadores cuánticos (y por tanto rompe los sistemas de criptografía clásica como el *RSA*), no ha podido ser aplicado a ninguno de estos sistemas. Aunque existen otros algoritmos cuánticos, como el algoritmo de Grover, que pueden ser aplicados a algunos de estos sistemas, no son tan eficientes como el algoritmo de Shor y los criptógrafos pueden compensarlo eligiendo claves un poco más grandes.

Hay que notar que esto no implica que estos sistemas sean totalmente seguros. Este es un problema muy común en criptografía: algunas veces se encuentran ataques a sistemas que son devastadores, demostrando que un sistema es inútil para la criptografía; otras veces, se encuentran ataques que no son tan devastadores pero que obligan a elegir claves más grandes para que sigan siendo seguros; y otras, se estudian criptosistemas durante años sin encontrar ningún ataque efectivo. En este punto, la comunidad puede ganar confianza en el sistema creyendo que el mejor ataque posible ya ha sido encontrado, o que existe muy poco margen de mejora.

2.2 Criptosistemas

El objetivo principal de la criptografía es permitir que dos personas, normalmente referidas como Alice y Bob, puedan comunicarse entre ellas a través de un canal inseguro de tal manera que una tercera persona, Oscar, no pueda entender qué están diciendo entre ellos, aun teniendo acceso a toda la conversación. La información que Alice quiere enviar a Bob la denominamos "texto plano", aunque no tiene que ser necesariamente texto; puede tener la estructura que deseemos: datos numéricos, cadenas de bits, sonido... Alice encripta el texto plano usando una "clave" que solo conocen Alice y Bob, obteniendo así un "texto encriptado". Oscar, al ver la información a través del canal inseguro, no puede determinar cuál era el texto plano original; pero Bob, que sí conoce la clave, puede desencriptar el texto cifrado y recuperar el texto plano.

Formalmente, un criptosistema se define de la siguiente manera:

Definición 2.1. Un *criptosistema* es una 5-tupla $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ que satisface las siguientes condiciones:

1. $\mathcal{P}$ es un conjunto finito de *textos planos* posibles,
2. $\mathcal{C}$ es un conjunto finito de *textos cifrados* posibles,
3. $\mathcal{K}$ es el conjunto finito de todas las claves posibles,
4. Para cada $K \in \mathcal{K}$, existen dos aplicaciones $e_K : \mathcal{P} \to \mathcal{C}$ y $d_K : \mathcal{C} \to \mathcal{P}$, denominadas *regla de encriptación* y *regla de desencriptación* respectivamente, que verifican que $d_K(e_K(x)) = x$ para todo $x \in \mathcal{P}$.

La propiedad 4, que es la más importante, asegura que conociendo la clave $K \in \mathcal{K}$, se puede recuperar el texto sin cifrar original usando la función d_K. El proceso por el cual Alice y Bob utilizarían un criptosistema es el siguiente:

1. Alice y Bob seleccionan una misma clave $K \in \mathcal{K}$ de forma aleatoria.
2. Supongamos que Alice quiere enviar un mensaje $x = x_1 x_2 \cdots x_n$, con $x_i \in \mathcal{P}$ para todo $1 \leq i \leq n$. Alice calcula, para cada $1 \leq i \leq n$, $y_i = e_K(x_i)$, resultando en el mensaje cifrado
$$y = y_1 y_2 \cdots y_n$$

que Alice envía a través del canal inseguro a Bob.

3. Bob, al recibir y, calcula usando la clave K que conoce $d_K(y_i)$, que coincidirán con los x_i originales por la propiedad 4 de la Definición 2.1, obteniendo así el texto original x.

Hay que notar que para que este método funcione, Alice y Bob deben escoger la misma clave K para encriptar y desencriptar los mensajes. En algunos criptosistemas (como el AES mencionado anteriormente), sabiendo e_K o d_K, es sencillo obtener la otra función porque se conoce la clave secreta K. Un criptosistema de este tipo se denomina *criptosistema de clave simétrica*, ya que si un atacante obtuviese la función e_K o d_K, podría romper el sistema desencriptando los mensajes cifrados, bien usando d_K directamente en el segundo caso o bien calculando d_K a partir de e_K a través de la clave en el primero.

Por tanto, es fundamental que Alice y Bob, antes de iniciar cualquier comunicación a través del canal inseguro, se pongan de acuerdo a través de un canal seguro en la clave que van a utilizar. En la práctica, esto es muy difícil de conseguir (por ejemplo, en el caso de Internet). Para resolver este problema, existen los *criptosistemas de clave pública*.

La idea tras estos criptosistemas es que dada una función de encriptación e_K, sea computacionalmente infactible calcular d_K. En este caso, el receptor del mensaje, Bob, publicaría una *clave pública* que permitiría a cualquier persona determinar una función de encriptación e_K. Así, Alice encriptaría el mensaje que quiere enviar usando esta función. El mensaje cifrado llegaría entonces a Bob, que es el único que conoce su *clave privada* con la cual puede calcular la función de desencriptación d_K correspondiente a e_K, desencriptando así el mensaje.

Estos criptosistemas son los que se ven principalmente afectados por la aparición de los ordenadores cuánticos: mientras que en un ordenador clásico puede ser muy difícil calcular la clave privada a partir de la clave pública, pueden existir algoritmos cuánticos que resuelvan el problema en un tiempo razonable. Es por ello que se necesitan nuevos sistemas en los que no existan algoritmos conocidos, ni clásicos ni cuánticos, que permitan calcular eficientemente d_K a partir de e_K.

2.3 Sistemas de firma

El otro gran objetivo de la criptografía es permitir la firma de documentos. En este caso, Alice publicaría el mensaje o documento con una *firma* que permite a cualquier persona

verificar que el mensaje sólo ha podido ser escrito por Alice. De esta manera, un atacante Oscar que quisiese publicar un documento haciéndose pasar por Alice, debe generar una firma con él para que pueda ser validado por el resto de personas. El proceso de firmar, por tanto, debe ser computacionalmente sencillo para Alice, pero infactible para Oscar, como sucede en los criptosistemas de clave pública.

Formalmente, un sistema de firma se define de la siguiente manera:

Definición 2.2. Un *sistema de firma* es una 5-tupla $(\mathcal{P}, \mathcal{A}, \mathcal{K}, \mathcal{S}, \mathcal{V})$ que verifica:

1. $\mathcal{P}$ es un conjunto finito de posibles *mensajes*,
2. $\mathcal{A}$ es un conjunto finito de *firmas* posibles,
3. $\mathcal{K}$ es el conjunto de las claves posibles,
4. Para cada $K \in \mathcal{K}$, hay dos aplicaciones $sig_K \in S$ y $ver_K \in V$, denominadas algoritmos de *firma* y *verificación* respectivamente, siendo $sig_K : \mathcal{P} \to \mathcal{A}$ y $ver_K : \mathcal{P} \times \mathcal{A} \to \{0, 1\}$, que verifican para cada mensaje $x \in \mathcal{P}$ y cada firma $y \in \mathcal{A}$:
$$ver_K(x, y) = \begin{cases} 1 & \text{si } y = sig_K(x) \\ 0 & \text{si } y \neq sig_K(x) \end{cases}$$
A un par ordenado de la forma $(x, y) \in \mathcal{P} \times \mathcal{A}$ se le denomina *mensaje firmado*.

CAPITULO

3

Espacios de Hilbert

3.1 Definiciones básicas

Un concepto vital en el desarrollo de la teoría de ordenadores cuánticos es el concepto de espacio de Hilbert, que se apoya en los productos escalares. En este desarrollo, consideraremos en todo momento que el espacio vectorial subyacente X es de dimensión finita, es decir, $\dim X = n \in \mathbb{N}$; ya que no trabajaremos en los capítulos siguientes con espacios de Hilbert de dimensión infinita. Esto simplificará algunas demostraciones aquí presentadas; no obstante, con un poco más de esfuerzo, se pueden hacer para el caso general.

Definición 3.1. Sean E y F dos espacios vectoriales sobre un cuerpo $\mathbb{K}$ (consideraremos $\mathbb{R}$ ó $\mathbb{C}$). Una aplicación $u : E \to F$ es una *aplicación semilineal* si para cada $x, y \in E$ y para cada $\alpha \in \mathbb{K}$ verifica:

1. $u(x + y) = u(x) + u(y)$
2. $u(\alpha x) = \overline{\alpha} u(x)$

donde $\bar{\cdot}$ denota la conjugación compleja.

Esta noción generaliza el concepto de aplicación lineal en espacios vectoriales reales, puesto que si $\mathbb{K} = \mathbb{R}$, entonces el concepto de aplicación semilineal coincide con el de

lineal (ya que $\overline{\alpha} = \alpha$ para todo $\alpha \in \mathbb{R}$). El siguiente es una generalización del concepto de forma bilineal.

Definición 3.2. Sea E un espacio vectorial sobre un cuerpo $\mathbb{K}$. Una aplicación $B : E \times E \to \mathbb{K}$ se dice que es una *forma sesquilineal* si es lineal respecto de la primera componente y semilineal respecto de la segunda; es decir, si para cada $x, x', y, y' \in E$ y para cada $\alpha, \lambda \in \mathbb{K}$ se verifica:

1. $B(x + x', y) = B(x, y) + B(x', y)$
2. $B(\lambda x, y) = \lambda B(x, y)$
3. $B(x, y + y') = B(x, y) + B(x, y')$
4. $B(x, \alpha y) = \overline{\alpha} B(x, y)$

Si además B verifica que $B(x, y) = \overline{B(y, x)}$, entonces se dice que es *hermítica*.

Las *aplicaciones sesquilineales* entre dos espacios vectoriales se definen de forma análoga con las propiedades 1-4 de la definición anterior, cambiando el producto en $\mathbb{K}$ por el producto exterior del espacio vectorial de llegada.

Definición 3.3. Sea E un espacio vectorial y sea B una forma sesquilineal y hermítica sobre E. Si para cada $x \in E$ se verifica $B(x, x) \geq 0$ entonces se dirá que B es *positiva*.

Si además se verifica que $x = 0$ cuando $B(x, x) = 0$ entonces se dice que B es *definida positiva*.

Ya estamos en condiciones de presentar lo que es un espacio de Hilbert.

Definición 3.4. Sea X un espacio vectorial sobre $\mathbb{K}$. Un *producto escalar* o *producto interior* en X es una forma sesquilineal hermítica definida positiva B sobre $X \times X$. Se suele denotar por $(x|y) = B(x, y)$ o bien por $\langle x, y \rangle = B(x, y)$.

Un espacio vectorial X que está dotado de un producto escalar diremos es un *espacio prehilbertiano*.

Un espacio prehilbertiano es un *espacio de Hilbert* si es completo.

Esta definición generaliza el concepto de producto escalar en espacios vectoriales reales.

Ejemplo 3.1. Sea $X = \mathbb{C}^2$. El producto escalar usual en este espacio se define como

$$\langle (z_1, z_2), (z_1', z_2') \rangle = z_1\overline{z_1'} + z_2\overline{z_2'}$$

En efecto, es un producto escalar, ya que:

1. $\langle (z_1, z_2)+(z_3, z_4), (z_1', z_2') \rangle = (z_1+z_3)\overline{z_1'}+(z_2+z_3)\overline{z_2'} = z_1\overline{z_1'}+z_2\overline{z_2'}+z_3\overline{z_1'}+z_4\overline{z_2'} = \langle (z_1, z_2), (z_1', z_2') \rangle + \langle (z_3, z_4), (z_1', z_2') \rangle$.
2. $\langle \lambda(z_1, z_2), (z_1', z_2') \rangle = \lambda z_1\overline{z_1'} + \lambda z_2\overline{z_2'} = \lambda\langle (z_1, z_2), (z_1', z_2') \rangle$
3. $\langle (z_1, z_2), (z_1', z_2') + (z_3', z_4') \rangle = z_1\overline{z_1' + z_3'} + z_2\overline{z_2' + z_4'} = z_1\overline{z_1'} + z_2\overline{z_2'} + z_1\overline{z_3'} + +z_2\overline{z_4'} = \langle (z_1, z_2), (z_1', z_2') \rangle + \langle (z_1, z_2), (z_3', z_4') \rangle$.
4. $\langle (z_1, z_2), \alpha(z_1', z_2') \rangle = \lambda z_1\overline{\alpha z_1'} + z_2\overline{\alpha z_2'} = \overline{\alpha}\langle (z_1, z_2), (z_1', z_2') \rangle$

Análogamente al caso real, dado $H \subseteq X$ un subespacio vectorial de un espacio de Hilbert X, podemos definir

$$H^{\perp} = \{x \in X : \langle x, h \rangle = 0 \text{ para todo } x \in X\}$$

Y es sencillo comprobar, por las propiedades del producto escalar, que es un subespacio vectorial y que $\dim H + \dim H^{\perp} = \dim X$.

También podemos definir el concepto de base ortonormal como una base $\{u_i\}_{i=1,\cdots,n}$ que verifica que $\langle u_i, u_j \rangle = \delta_{ij}$ (la delta de Kronecker). Análogamente al caso real, todo espacio de Hilbert tiene una base ortonormal; pues siempre podemos construir una usando el método de Gram-Schmidt (ver [1], pág. 167).

Notemos que en un espacio de Hilbert X es posible definir una norma de la siguiente manera: para cada $x \in X$,

$$\|x\| = \sqrt{\langle x, x \rangle}$$

Es fácil ver que esta norma está bien definida, por ser $\langle x, x \rangle \geq 0$ (es definida positiva), y que por las propiedades del producto escalar, es una norma. De esta manera, todo espacio de Hilbert es un espacio normado, y al ser completo, es un *espacio de Banach* (ver [1], pág. 27). Este hecho justifica el exigir la propiedad de completitud a un espacio de Hilbert, pues esta norma induce una métrica en X, y gracias a ello podemos hablar de sucesiones de Cauchy y sucesiones convergentes (un conjunto es completo si toda sucesión de Cauchy en él es convergente).

Ejemplo 3.2. Sea $X = \mathbb{C}^2$. La *norma usual* inducida por el producto escalar usual es

$$\|(z_1, z_2)\| = \sqrt{\langle (z_1, z_2), (z_1, z_2) \rangle} = \sqrt{z_1\overline{z_1} + z_2\overline{z_2}} = \sqrt{|z_1|^2 + |z_2|^2}$$

Una propiedad conocida es la desigualdad de Cauchy-Schwarz, que se verifica en espacios prehilbertianos.

Teorema 3.1 (Desigualdad de Cauchy-Schwarz). *Sea E un espacio vectorial y $B(x, y)$ una forma sesquilineal hermítica y positiva sobre E. Se verifica, para cada $x, y \in E$, que*

$$|B(x, y)| \leq B(x, x)^{1/2} B(y, y)^{1/2}$$

Una demostración clásica de este hecho puede consultarse en [1], pág. 154.

Como consecuencia inmediata de la definición de $\|\cdot\|$, tenemos el siguiente importante resultado.

Corolario 3.1. *Sea X un espacio prehilbertiano. Entonces, para cada $x, y \in X$, se verifica que:*

$$|\langle x, y \rangle| \leq \|x\| \|y\|$$

3.2 El operador adjunto y operadores unitarios

Ya que los espacios de Hilbert son espacios vectoriales, podemos hablar de aplicaciones lineales entre ellos y de formas lineales. De entre ellas, en el contexto de la computación cuántica nos interesarán aquellas que sean *unitarias*. Para poder definirlas correctamente, necesitamos un poco de teoría de espacios de Hilbert.

Lema 3.1. *Sean X, Y, Z tres espacios normados y $u : X \times Y \to Z$ una aplicación sesquilineal, entonces las siguientes afirmaciones son equivalentes:*

i) u es continua en $(0, 0)$.

ii) Existe $M > 0$ tal que $\|u(x, y)\| \leq M\|x\|\|y\|$ para cada $(x, y) \in X \times Y$

iii) u es continua en $X \times Y$.

Demostración.

iii) $\implies$ i) Es trivial.

i) $\implies$ ii) Tomando $\epsilon = 1$, entonces por i) existe $\delta > 0$ tal que si $\|x\| \leq \delta$, $\|y\| \leq \delta$, entonces $\|u(x,y)\| \leq \epsilon = 1$. Si fuese $x = 0$ ó $y = 0$, el resultado es claro puesto que

$$\|u(0,y)\| = \|u(x,0)\| = \|0\| = 0 \leq M\|x\|\|0\| = M\|0\|\|y\| = 0$$

Si es $x \neq 0, y \neq 0$, entonces se verifica que $\left\| \frac{\delta x}{\|x\|} \right\| = \frac{\delta \|x\|}{\|x\|} = \delta$, $\left\| \frac{\delta y}{\|y\|} \right\| = \frac{\delta \|y\|}{\|y\|} = \delta$, y por tanto por el razonamiento anterior,

$$\left\| u\left(\frac{\delta x}{\|x\|}, \frac{\delta y}{\|y\|} \right) \right\| \leq 1$$

Aplicando finalmente sesquilinealidad, tenemos que

$$\frac{\delta^2}{\|x\|\|y\|}\|u(x,y)\| \leq 1$$

$$\|u(x,y)\| \leq \delta^2 \|x\|\|y\|$$

ii) $\implies$ iii) Sea $(a,b) \in X \times Y$. Se verifican, para cada $(x,y) \in X \times Y$, usando la desigualdad triangular y la sesquilinealidad:

$$\|u(x,y) - u(a,b)\| = \|u(x,y) - u(a,y) + u(a,y) - u(a,b)\| \leq \|u(x-a,y)\| + \|u(a,y-b)\|$$

Y además, por hipótesis, se verifica que

$$\|u(x,y) - u(a,b)\| \leq \|u(x-a,y)\| + \|u(a,y-b)\| \leq M\|x-a\|\|y\| + M\|a\|\|y-b\|$$

□

Teorema 3.2 (Fréchet-Riesz). *Sea X un espacio de Hilbert y sea $f : X \to \mathbb{K}$ una aplicación lineal y continua. Existe un único $a \in X$ tal que $f = f_a$, donde $f_a : X \to \mathbb{K}$ es la aplicación definida por $f_a(x) = \langle x, a \rangle$.*

Demostración. Sea $H = \ker f$. Observemos que se verifica, por ser f lineal:

$$\dim H + \dim \text{Im } f = \dim X$$

Como $\dim \mathbb{K} = 1$ como $\mathbb{K}$-espacio vectorial, entonces $\dim \text{Im } f \leq 1$. Si fuese 0, entonces es $f = 0$ (la aplicación nula), y bastaría tomar $a = 0$.

Supongamos pues, que $\dim \text{Im}\, f = 1$. Entonces, $\dim H = \dim X - 1$, y por ser $\dim H + \dim H^\perp = \dim X$, entonces $\dim H^\perp = 1$. Luego podemos tomar $b \in H^\perp$ con $b \neq 0$, y se cumple que $H^\perp = \mathcal{L}(b)$. De esta manera, como $X = H + H^\perp$, cada $x \in X$ se puede expresar de la forma $x = y + \alpha b$, $y \in H, \alpha \in \mathbb{K}$.

Tomamos $a = \frac{\overline{f(b)}}{\|b\|^2} b$. Veamos que a verifica las propiedades del enunciado: sea $x \in X$. Por un lado,

$$f(x) = f(y + \alpha b) = f(y) + \alpha f(b) = \alpha f(b)$$

por la linealidad de f y que $y \in \ker f$.

Por otro lado,

$$\langle x, a \rangle = \langle y + \alpha b, \frac{\overline{f(b)}}{\|b\|^2} b \rangle = \frac{f(b)}{\|b\|^2} \langle y, b \rangle + \alpha \frac{f(b)}{\|b\|^2} \langle b, b \rangle = \alpha f(b)$$

Ya que $\langle y, b \rangle = 0$ por ser $y \in H$, $b \in H^\perp$. Esto prueba que $f = f_a$.

Veamos la unicidad. Sea $a' \in X$ tal que $f = f_{a'}$. Entonces, para cada $x \in X$, se verifica que:

$$f(x) = \langle x, a \rangle = \langle x, a' \rangle$$

de donde deducimos que

$$0 = \langle x, a - a' \rangle$$

Lo que significa que $a - a' \in X^\perp = \{0\}$. De aquí, $a = a'$. □

El siguiente teorema finalmente nos termina de preparar el camino para definir los operadores unitarios.

Teorema 3.3. *Sea X un espacio de Hilbert y sea $B : X \times X \to \mathbb{K}$ una forma sesquilineal y continua. Entonces, existe una única aplicación lineal y continua $f : X \to X$ tal que $B(x, y) = \langle x, f(y) \rangle$ para cada $(x, y) \in X \times X$.*

Demostración. Fijado $y \in X$, podemos definir $g_y : X \to \mathbb{K}$ dada por $g_y(x) = B(x, y)$. Claramente g_y es lineal por serlo la primera componente de B, y además tenemos que, gracias al Lema 3.1, por ser B continua:

$$|g_y(x)| = |B(x, y)| \leq M\|x\|\|y\|$$

Esto implica que, para $(x, y) \in S_X$, $|g_y(x)| \leq M$, y por tanto, g_y es continua. Usando ahora el Teorema 3.2, existe un único $z_y \in X$ tal que, para cada $x \in X$, se verifica que $g_y(x) = \langle x, z_y \rangle$. Esto permite definir una aplicación $f : X \to X$ como $f(y) = z_y$.

Por construcción, f verifica la igualdad del enunciado, ya que

$$\langle x, f(y)\rangle = \langle x, z_y\rangle = g_y(x) = B(x,y)$$

Veamos que f es lineal: sean $y, z \in X$, $\alpha, \beta \in \mathbb{K}$. Entonces, aplicando la sesquilinealidad de B, se tiene que

$$\begin{aligned}\langle x, f(\alpha y + \beta z)\rangle &= B(x, \alpha y + \beta z) = \\ &= \overline{\alpha} B(x,y) + \overline{\beta} B(x,z) = \overline{\alpha}\langle x, f(y)\rangle + \overline{\beta}\langle x, f(z) = \langle x, \alpha f(y) + \beta f(z)\rangle\end{aligned}$$

Con lo que tenemos que, para cada $x \in X$,

$$0 = \langle x, f(\alpha y + \beta z) - (\alpha f(y) + \beta f(z))\rangle$$

Y por tanto $f(\alpha y + \beta z) - (\alpha f(y) + \beta f(z)) \in X^{\perp} = \{0\}$.

Además, f es continua. Ya que para cada $x, y \in X$ es $|\langle x, f(y)\rangle| = |B(x,y)| \leq M\|x\|\|y\|$ (por el Lema 3.1). En particular, para $x = f(y)$, tenemos que

$$\|f(y)\|^2 \leq M\|f(y)\|\|y\|$$

De aquí podemos deducir que

$$\|f(y)\| \leq M\|y\|$$

(desigualdad que también se verifica trivialmente si $f(y) = 0$). Si fijamos $y \in S_x$, $\|y\| = 1$, lo que significa que $\|f(y)\| \leq M$ y por tanto f es continua. □

Este teorema nos permite dar una definición importante. Sea X un espacio de Hilbert y sea $A : X \to X$ una aplicación lineal y continua. La aplicación que envía $(x, y) \to \langle A(x), y\rangle$ es sesquilineal y continua[1]. Por tanto, usando el teorema anterior, debe existir una aplicación lineal y continua $A' : X \to X$ de manera que

$$\langle A(x), y\rangle = \langle x, A'(y)\rangle$$

Definición 3.5. Sea X un espacio de Hilbert y sea $A : X \to X$ una aplicación lineal y continua. El *adjunto de* A, denotado A', es la única aplicación lineal y continua $A' : X \to X$ que satisface para cada $x, y \in X$ que

$$\langle A(x), y\rangle = \langle x, A'(y)\rangle$$

[1]En efecto, $\langle A(x+x'), y\rangle = \langle A(x) + A(x'), y\rangle = \langle A(x), y\rangle + \langle A(x'), y\rangle$ y $\langle A(\alpha x), y\rangle = \langle \alpha A(x), y\rangle = \alpha\langle A(x), y\rangle$ y en la segunda componente es trivial por la sesquilinealidad del producto escalar. La continuidad se debe a que se trata de la composición de dos funciones continuas, A y el producto escalar.

Supongamos ahora que $\{u_i\}_{i=1,\cdots,n}$ es una base ortonormal de X. Sea ahora $(k_{ij})_{i,j=1,\cdots,n}$ la matriz asociada de A y $(k'_{ij})_{i,j=1,\cdots,n}$ la de A' . Se verifica que, por ser la base ortonormal:

$$\langle A(u_j), u_i\rangle = \left\langle \sum_{l=1}^{n} k_{lj}u_l, u_i \right\rangle = \sum_{l=1}^{n} k_{lj}\langle u_l, u_i\rangle = k_{ij}$$

Entonces, usando que el producto escalar es hermítico:

$$k_{ij} = \langle A(u_j), u_i\rangle = \langle u_j, A'(u_i)\rangle = \overline{\langle A'(u_i), u_j\rangle} = \overline{k'_{ji}}$$

Es decir, tomando conjugados e intercambiando los papeles de i y de j:

$$k'_{ij} = \overline{k_{ji}}$$

para cada $i, j = 1, \cdots, n$. Hemos probado:

Proposición 3.1. *Sea X un espacio de Hilbert y sea $A : X \to X$ una aplicación lineal y continua. Sea $\mathcal{A}, \mathcal{B}$ las matrices asociadas a A y A' respectivamente fijando una base ortonormal en X. Entonces, se verifica que:*

$$\mathcal{B} = \mathcal{A}^\dagger$$

Donde $\mathcal{A}^\dagger$ denota la matriz traspuesta conjugada de A.

Ejemplo 3.3. Tomemos $X = \mathbb{C}^2$ con la base ortonormal canónica $\{(1,0),(0,1)\}$ y el producto escalar usual dado por $\langle (z_1, z_2), (z'_1, z'_2)\rangle = z_1\overline{z'_1} + z_2\overline{z'_2}$. Consideramos la aplicación $f : \mathbb{C}^2 \to \mathbb{C}^2$ dada por

$$f(z_1, z_2) = \frac{1}{\sqrt{3}}\left(z_1 + (-1+i)z_2, (1+i)z_1 + z_2\right)$$

Es fácil ver que f es lineal, y que su matriz asociada es

$$A = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & -1+i \\ 1+i & 1 \end{pmatrix}$$

Entonces, la matriz asociada del adjunto de f viene dada por

$$A' = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1-i \\ -1-i & 1 \end{pmatrix}$$

Es decir, el adjunto de f viene dado por

$$f'(z_1, z_2) = \frac{1}{\sqrt{3}}\left(z_1 + (1-i)z_2, (-1-i)z_1 + z_2\right)$$

Definición 3.6. Sea X un espacio de Hilbert y sea $A : X \to X$ una aplicación lineal y continua. Se dice que A es *unitaria* si $A' \circ A = A \circ A' = Id$, donde $Id : X \to X$ es la aplicación identidad en X.

Según lo visto antes, esta condición puede traducirse matricialmente a que $AA^\dagger = A^\dagger A = I$.

Ejemplo 3.4. El operador definido en el Ejemplo 3.3 es unitario, ya que

$$A'A = \frac{1}{3}\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = I$$

CAPITULO

4

El algoritmo de Shor

4.1 Introducción

El objetivo de este capítulo es describir el (principal) algoritmo que pone en peligro toda la criptografía clásica que se usa actualmente en gran medida: el algoritmo de Shor, que permite factorizar cualquier número natural en $O((\log N)^3)$ pasos ([2], pág. 233), donde N es el número a factorizar. El algoritmo contiene dos partes, una parte clásica que se ejecutaría en un ordenador clásico, y una parte cuántica que se ejecutaría en un ordenador cuántico. La idea clave del algoritmo subyace en el siguiente resultado.

Proposición 4.1. *Sea N un número compuesto de L bits, y sea $x \in \mathbb{Z}_N$ con $1 < x < N-1$ una solución de la ecuación*

$$x^2 = 1 \mod N \tag{4.1}$$

Entonces, o bien $\mathrm{mcd}(x-1, N)$ o bien $\mathrm{mcd}(x+1, N)$ es un factor no trivial de N y se puede calcular en $O(L^3)$ operaciones.

Demostración. Ya que $x^2 - 1 = 0 \mod N$, entonces $N|_{(x^2+1)=(x+1)(x-1)}$. De aquí, N debe tener un factor común con $(x+1)$ ó con $(x-1)$, es decir, $\mathrm{mcd}(x+1, N) > 1$ ó $\mathrm{mcd}(x-1, N) > 1$. Además, ya que $1 < x < N-1$, entonces $2 < x+1 < N$ y $0 < x-1 < N-2$, en cualquier caso, $x-1 < N$ y $x+1 < N$ y por tanto $\mathrm{mcd}(x-1, N) < N$

y $\mathrm{mcd}(x+1, N) < N$. Esto prueba que ninguno puede ser un factor trivial de N. Mediante el algoritmo de Euclides, estos factores pueden calcularse en $O(L^3)$ operaciones (ver [2], pág. 629). □

En general, encontrar una solución de (4.1) es difícil. Sin embargo, existe una estrategia para abordar este problema. Si $1 < y < N-1$ es cualquier número coprimo con N y resulta que el orden r del elemento y dentro del grupo multiplicativo $(\mathbb{Z}/N\mathbb{Z})^*$ (es decir, el menor natural tal que $y^r = 1 \mod N$) es par, entonces $y^{r/2}$ sería una solución de (4.1); y además cumpliría las hipótesis de la Proposición 4.1 si $y^{r/2} \neq -1 \mod N$ (observemos que no puede ser 1, ya que ello contradiría la definición de r). Resulta que si escogemos este número y aleatoriamente entre 2 y $N-2$ (si no es coprimo con N, entonces habríamos encontrado un factor calculando $\mathrm{mcd}(y, N)$), entonces es muy probable que verifique las condiciones expuestas, lo cual nos permitiría calcular los factores como enuncia la Proposición 4.1. Este hecho se recoge en el siguiente teorema.

Teorema 4.1. *Sea $N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ una factorización en números primos de un número impar. Sea x un elemento escogido aleatoriamente de $(\mathbb{Z}/N\mathbb{Z})^*$, y sea r el orden de x módulo N. Entonces,*

$$P[r \text{ es par y que } x^{r/2} \neq -1 \mod N] \geq 1 - \frac{1}{2^m}$$

Para demostrarlo, necesitamos primero un lema previo.

Lema 4.1. *Sea p un número primo diferente de 2 y sea $\alpha \in \mathbb{N}$. Sea 2^d la mayor potencia de 2 que divide a $\varphi(p^\alpha)$. Entonces, con probabilidad de un medio 2^d divide al orden de cualquier elemento de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$.*

Demostración. Por ser $p \neq 2$, entonces es impar, y por tanto $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ es par. Esto implica que $d \geq 1$. Ya que el grupo $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ es cíclico, cualquier elemento se escribirá de la forma g^k, con g el generador del grupo y $1 \leq k \leq \varphi(p^\alpha)$. Sea r el orden de dicho elemento.

- Si es k impar, ya que $\left(g^k\right)^r = g^{kr} = 1 \mod p^\alpha$ entonces por el Teorema de Lagrange debe ser $\phi(p^\alpha) | kr$. De aquí, 2^d divide a kr, y por ser k impar, necesariamente 2^d divide a r, el orden del elemento.

- Si es k par, entonces

$$g^{\frac{k}{2}\varphi(p^\alpha)} = \left(g^{\varphi(p^\alpha)}\right)^{k/2} = 1^{k/2} = 1 \mod p^\alpha$$

  Como r es el orden del elemento g^k, entonces necesariamente $r|\varphi(p^\alpha)/2$. Ya que 2^{d-1} es la mayor potencia de 2 que divide a $\varphi(p^\alpha)/2$, de aquí deducimos que 2^d no puede dividir a r.

Como exactamente la mitad de elementos de $(\mathbb{Z}/p^\alpha\mathbb{Z})^*$ se expresan con k par y la mitad con k impar, esto concluye la demostración. □

Ahora podemos demostrar el Teorema 4.1.

Demostración. Probaremos que

$$P[r \text{ es impar ó } x^{r/2} = -1 \mod N] \leq \frac{1}{2^m}$$

Por el Teorema Chino de los Restos, elegir un elemento x aleatoriamente de $(\mathbb{Z}/N\mathbb{Z})^*$ es equivalente a elegir x_j aleatoriamente de $(\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z})^*$, para $j = 1, \ldots, m$ tales que $x = x_j \mod p_j^{\alpha_j}$. Sea r_j el orden de x_j en $(\mathbb{Z}/p_j^{\alpha_j}\mathbb{Z})^*$, r el orden de x en $(\mathbb{Z}/N\mathbb{Z})^*$, 2^d la mayor potencia de 2 que divide a r y 2^{d_j} la mayor potencia de 2 que divide a r_j.

- Si es r impar, entonces ya que $r_j|r$ para cada j (porque $x_j^r = x^r \mod p_j^{\alpha_j}$. Como $x^r = 1 \mod N$, entonces $x^r = 1 \mod p_j^{\alpha_j}$. Entonces, $x_j^r = 1 \mod p_j^{\alpha_j}$ y de aquí el orden $r_j|r$); si r es impar entonces r_j es impar, y de aquí, $d_j = 0$ para todo j.

- Si r es par y es $x^{r/2} = -1 \mod N$, entonces $x^{r/2} = -1 \mod p_j^{\alpha_j}$, esto es, $x_j^{r/2} = -1 \mod p_j^{\alpha_j}$. De aquí, $r_j \not| (r/2)$. Ya que $r_j|r$, necesariamente $d = d_j$ para cada j (porque la mayor potencia de 2 que divide a r_j será exactamente 2^d, no puede ser menor porque $r_j \not| (r/2)$).

En definitiva, hemos probado que si r es impar ó $x^{r/2} = -1 \mod N$, entonces d_j toma el mismo valor para cada j. Esto implica que cada d_j debe dividir (o no dividir) a cada r_j simultáneamente. Por el Lema 4.1, la probabilidad de que esto ocurra es

$$\frac{1}{2} \cdot \frac{1}{2} \cdots \frac{1}{2} = \frac{1}{2^m}$$

Por contención de sucesos, finalmente

$$P[r \text{ es impar ó } x^{r/2} = -1 \mod N] \leq P[d_j = k \text{ para cada } j] \leq P[d_j|r_j \text{ ó } d_j \not| r_j \text{ para cada } j] = \frac{1}{2^m}$$

□

Una consecuencia inmediata del Teorema 4.1 es que si el número que queremos factorizar N tiene 2 factores primos (como suele usarse en criptografía, como es el caso del algoritmo RSA), entonces tenemos la garantía de que usando el procedimiento descrito anteriormente, daremos al menos un 75 % de las veces con un elemento y que nos permita hallar los factores de N usando la Proposición 4.1. Un resumen de un algoritmo para factorizar sería el siguiente:

1. Si N es par, devolver el factor 2.
2. Elegir aleatoriamente y entre 2 y $N-2$. Si $\mathrm{mcd}(y, N) > 1$, devolver el factor $\mathrm{mcd}(y, N)$.
3. Encontrar el orden r del elemento y módulo N.
4. Si r es par y $x^{r/2} \neq -1 \mod N$, entonces calcular $\mathrm{mcd}(x^{r/2}-1, N)$ y $\mathrm{mcd}(x^{r/2}+1, N)$, comprobar cuál de ellos es un factor no trivial y devolver dicho factor. En caso contrario, volver al paso 2.

Gracias al algoritmo de Euclides y la exponenciación modular, todos los pasos de este algoritmo se pueden ejecutar en tiempo polinomial excepto el paso 3. Este problema se conoce como el problema de encontrar el orden, y no existe ningún método eficiente para resolverlo en un ordenador clásico. Sin embargo, usando la computación cuántica, sí es posible resolver este problema eficientemente. En realidad, el algoritmo descrito es un esquema del algoritmo de Shor, con la salvedad de que el paso 3 se resuelve con un circuito cuántico, se obtienen los resultados y se prosigue en un ordenador clásico para culminar con la obtención del factor. Veremos cómo se construye este circuito en un ordenador cuántico y por qué funciona.

4.2 Computación cuántica

Ahora que hemos visto la motivación por la que necesitamos un ordenador cuántico, trataremos de describir cómo funciona. En el corazón de la computación clásica se encuentra el concepto de *bit*, la unidad mínima de información que describe un sistema clásico 2-dimensional. Matemáticamente, podemos modelar un bit como un elemento de $\mathbb{Z}_2 = \{0, 1\}$. De este concepto surgen las *puertas lógicas*, mecanismos que convierten un conjunto de bits en otro. Matemáticamente, estas puertas lógicas se modelan como funciones $f : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$.

Ejemplo 4.1. La puerta lógica AND implementa la operación lógica de conjunción (&) y se define de esta manera:

$$f : \mathbb{Z}_2^2 \to \mathbb{Z}_2$$
$$(0,0) \longmapsto 0$$
$$(0,1) \longmapsto 0$$
$$(1,0) \longmapsto 0$$
$$(1,1) \longmapsto 1$$

La computación cuántica surge como una generalización de estos conceptos. De igual manera que en la computación clásica, en la computación cuántica se encuentra el concepto de *qubit*.

Definición 4.1. Un *qubit* es la unidad mínima de información describiendo un sistema cuántico 2-dimensional.

Un qubit se modela como un elemento del espacio de Hilbert $\mathbb{C}^2$. Como ya vimos, este es un espacio vectorial y posee una base, por ejemplo, la canónica: $\{(0,1),(1,0)\}$. Así, todo qubit puede expresarse como una combinación $\mathbb{C}$-lineal de estos dos elementos. En el contexto de la computación cuántica, a los elementos de la base canónica es usual denotarlos usando la notación de Dirac de esta manera:

$$|0\rangle = (1,0)$$

$$|1\rangle = (0,1)$$

y se denominan los *estados básicos*. Con lo que cualquier qubit puede expresarse de la forma $c_1|0\rangle + c_2|1\rangle$, $c_1, c_2 \in \mathbb{C}$. Una restricción importante que se impone sobre los qubits es que $|c_1|^2 + |c_2|^2 = 1$. Así, cuando $|c_1| = 1$ y $|c_2| = 0$ se dice que el qubit está en el estado básico 0 y al contrario, en el estado básico 1. En cualquier otra situación, el qubit se dice que está en estado de *superposición*.

Los qubits pueden ser, en cualquier momento, "observados". Esto saca al qubit de su estado de superposición, y hace que se comporte como un bit clásico, tomando el valor 0 o el valor 1. La probabilidad con la que toma cada valor viene dado por las coordenadas del qubit: así, un qubit $c_1|0\rangle + c_2|1\rangle$ tiene una probabilidad $|c_1|$ de valer 0 al ser observado, y $|c_2|$ de valer 1 (de aquí la imposición anterior de que $|c_1|^2 + |c_2|^2 = 1$).

CAPITULO

5

Segunda cosa

5.1 Lo siguiente

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut ultrices egestas nunc, venenatis rhoncus elit fermentum non. Pellentesque gravida nulla vitae ipsum lobortis ullamcorper. Ut adipiscing, tellus in egestas mattis, enim metus pretium erat, ac tempor dolor neque placerat nulla. Nullam nec ligula eu ipsum pharetra semper a in magna. Integer ut tortor quis nisi fringilla euismod eu ac ipsum. Pellentesque sodales consectetur erat eget rutrum. Proin ornare dolor ut arcu aliquet vestibulum. Pellentesque laoreet tincidunt sem eget semper.

Integer interdum mattis magna ullamcorper tristique. Nullam commodo nulla eget ipsum vulputate tincidunt auctor leo aliquet. Fusce euismod sagittis ante, eu vulputate eros dictum at. Cras non euismod nunc. Nullam velit diam, consectetur sed eleifend vitae, blandit at arcu. Maecenas ut urna nec turpis lobortis commodo. Aliquam aliquet turpis id massa viverra id sollicitudin est cursus. Sed a tortor non mauris cursus imperdiet.

Integer fermentum rutrum urna at vestibulum. Vivamus ullamcorper erat in sapien dignissim pellentesque. Integer convallis fringilla dictum. In bibendum lectus eu nulla pretium volutpat. Morbi hendrerit fringilla tortor, sed gravida neque lacinia a. In risus magna, hendrerit vitae cursus ac, vehicula at eros. Aenean quis ipsum sit amet leo vestibulum cursus.

5.2 Otra cosa más

Cras placerat mattis dui quis vehicula. Nulla sit amet metus nibh, at auctor enim. Quisque congue ultricies sapien in suscipit. Fusce vitae placerat ante. Praesent aliquet urna ac elit consequat nec mattis augue faucibus. Nunc et sapien vel felis mollis sodales. Aenean molestie nulla vestibulum nisi fringilla vel euismod dolor tristique. Aenean fermentum, dolor eget tincidunt faucibus, risus lorem feugiat elit, sagittis malesuada eros ligula in odio. Pellentesque ac libero lobortis justo bibendum laoreet. Cras egestas lorem eget ligula dignissim sollicitudin. Vestibulum sit amet augue ultrices erat faucibus vestibulum. Aenean tincidunt faucibus leo, nec auctor diam bibendum a. Sed varius, mauris in pellentesque scelerisque, nisl ligula viverra erat, in eleifend tellus enim ac magna. Pellentesque quis est risus. Cras mollis feugiat auctor. Proin ac eros vitae nulla gravida varius.

5.2.1 Una subcosa

Morbi at augue sapien. Duis tempus quam vitae velit interdum ultricies. Vivamus laoreet lacinia elit sit amet vehicula. Ut congue diam ac magna hendrerit sed fermentum justo lacinia. Curabitur vel odio neque, quis consequat mi. Proin lobortis justo quis enim fermentum accumsan sagittis ipsum imperdiet. Proin sem felis, laoreet placerat egestas id, fringilla id mauris. Pellentesque a nisi sit amet leo consectetur gravida nec et dui. Curabitur quis hendrerit augue. Etiam sed dui nec tortor convallis fringilla. Proin tempor mattis diam nec egestas. Quisque condimentum elementum lacus ac porta. Vivamus congue, odio eu ullamcorper elementum, leo turpis tempus sem, at condimentum dolor quam eu nunc. Pellentesque eget risus ac velit aliquam sollicitudin sed et ipsum.

Bibliografía

[1] A. Aizpuru Tomás. *Apuntes incompletos de Análisis Funcional*. Universidad de Cádiz, 2004. 11, 12

[2] Michael A. Nielsen and Isaac L.Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000. 19, 20

[3] Daniel J. Bernstein and Johannes Buchmann And Erik Dahmen, editors. *Post-Quantum Cryptography*. Springer, 2009.

[4] Douglas R. Stinson. *Cryptography, Theory and Practice*. Discrete Mathematics And Its Applications. Chapman & Hall/CRC, 3 edition, 2006.

[5] Noson S. Yanofsky and Mirco A. Mannucci. *Quantum computing for computer scientists*. Cambridge University Press, 2008.