Factorización Prima en Computación Cuántica: Algoritmo de Shor y Método de Factorización Adiabática.

Título provisional

Alberto García Planes

Tutores:
Prof. María Antonia Cárdenas Viedma
Prof. Leandro Marín Muñoz

2018

Cosas por hacer

1. Por qué solo existe una fracción que cumple toda la movida esa.
2. Comprobar que el razonamiento lógico de las probabilidades es correcto
3. En la prueba del 5.2.2, el caso que falta.
4. Revisar aserciones del código.
5. Unificar notación gorros hamiltonianos
6. Crear el simulador para la QFT (en C++ preferiblemente)
7. Hacer el simulador de Schrodinger y dibujar gráficas de autoenergías
8. Comprobar formato de la bibliografía
9. ¿«Bibliografía» o «Referencias»?
10. Revisar y revisar

Declaración de Originalidad

Alberto García Planes, autor del trabajo de fin de grado titulado *Factorización Prima en Computación Cuántica: Algoritmo de Shor y Método de Factorización Adiabática* bajo la tutela de la profesora **María Antonia Cárdenas Viedma** y el profesor **Leandro Marín Muñoz**,

DECLARA

que el trabajo que presenta es original, en el sentido de que ha puesto el mayor empeño en citar debidamente todas las fuentes utilizadas.

En Murcia, a 20 de octubre de 2018

Fdo.: Alberto García Planes

Una copia de este documento ha sido depositada en la secretaría de la Facultad de Informática de la Universidad de Murcia.

Resumen

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Extended Abstract

Ut facilisis sem est, sed malesuada tortor porttitor sit amet. Mauris vitae dolor at sem porta feugiat sed vel nisi. Mauris non enim faucibus, tempor lorem id, laoreet dolor. Phasellus et est blandit, malesuada enim et, dictum mi. Phasellus quis quam facilisis, facilisis justo sed, fermentum ligula. Pellentesque luctus maximus ipsum sit amet ornare. Nam enim lorem, commodo quis scelerisque accumsan, tempus nec orci. Integer tristique scelerisque mauris, nec placerat libero. Donec consectetur eros dui, eu suscipit ligula viverra non. Nam urna eros, cursus quis rhoncus ut, placerat non nisl. Aenean id dolor in ipsum sodales imperdiet.

Vivamus vitae diam a diam imperdiet volutpat eget a ligula. Quisque tristique sollicitudin nulla, eu accumsan augue ultrices non. Vestibulum fermentum arcu massa, vel efficitur dolor tincidunt eget. Etiam in commodo velit. Quisque eu lacus ac ipsum aliquam aliquet id in metus. Nam feugiat a lectus et dignissim. Suspendisse nec ipsum sodales, vulputate ligula eu, fringilla erat. In sit amet bibendum magna, quis convallis tellus. Vivamus molestie lectus odio, in tempor ipsum cursus eget. Cras sed vestibulum massa. Nulla facilisi.

Donec vel purus luctus, suscipit nibh quis, pellentesque erat. Pellentesque id diam sollicitudin, scelerisque nisi sit amet, porttitor erat. Integer sed accumsan ligula. Sed blandit, lacus non porta scelerisque, sapien nibh dignissim felis, quis dignissim neque dolor id nulla. Aenean a nisl faucibus, accumsan orci nec, mollis lectus. Praesent at suscipit velit. Nunc quis tortor vitae ex sagittis fermentum. Maecenas non erat urna.

Maecenas a tincidunt metus, sed pretium nisi. Suspendisse sed ultrices neque, vitae tristique ipsum. Phasellus faucibus porttitor accumsan. Sed eu lacus quis metus efficitur fringilla. Praesent sit amet urna auctor turpis malesuada semper ut nec ante. Nunc enim neque, pellentesque ac nisl id, semper interdum massa. Curabitur vel neque id tortor tristique faucibus in vitae lacus. Sed leo erat, tincidunt at nunc at, suscipit mollis risus. Mauris tempus vitae nulla eu tempor. Donec malesuada, elit non interdum vestibulum, sem nulla sagittis dui, ac iaculis libero lacus nec eros. Duis et sodales urna. Duis massa lectus, aliquam sed velit sit amet, pharetra luctus tellus. Fusce volutpat lacus sed bibendum porttitor. Etiam tempus et velit et gravida. Maecenas ac aliquam sem, ut blandit nisi. Nulla placerat odio et blandit pharetra.

Things on a very small scale behave like nothing you have any direct experience about... or like anything that you have ever seen.

Richard Feynman

Índice general

CAPÍTULO 1

El Sorprendente Mundo Cuántico.

Es probable que muchos de los físicos del siglo XX consideren el descubrimiento de la teoría cuántica como uno de los mayores hitos de la historia de la ciencia, más incluso que la teoría del espaciotiempo curvo de la relatividad general de Einstein. Sin embargo, el comportamiento de la realidad a escalas microscópicas que describe esta teoría es absolutamente contrario a nuestra percepción del mundo. Tanto es así, que determinados físicos evitan conscientemente el término «realidad» para referirse a tales comportamientos y simplemente confían en el formalismo matemático que aquí presentamos como una descripción funcional de la idiosincrasia de la escala cuántica.

En la sección que introducimos trataremos de explicar, mediante un experimento conceptual, la génesis de estas ideas en un contexto histórico, tras lo cual veremos las bases sobre las que la teoría cuántica se apoya que servirán como motivación teórica para la definición de multitud de conceptos del área de la computación cuántica.

1.1. El Experimento de Davisson–Germer

A principios del S. XIX la comunidad científica empezaba a comprender la naturaleza del mundo que nos rodea, sin embargo, una pregunta se resistía a ser resuelta satisfactoriamente: ¿cuál es la naturaleza de la luz?. Fue entonces, en 1801, cuando un matemático-físico londinense llamado Thomas Young quiso demostrar el hecho de que la luz poseía una naturaleza ondulatoria (es decir, que se comportaba e interactuaba como una onda en algún tipo de medio). Para ello ideó un experimento, que más tarde fue denominado el **experimento de la doble rendija**, que consistía, conceptualmente, en una placa con dos pequeñas aberturas sobre la que se hacía incidir un haz de luz. Tras esta placa se colocaba un panel de algún material fotosensible que reaccionaba a la luz que conseguía atravesar las rendijas de la placa colocada anteriormente. Podemos ver un diagrama en la figura 1.1.1.

La idea de Young era simple: si la naturaleza de la luz fuese corpuscular (es decir, si la luz estuviese formada por «paquetes» que no interfieren con ellos mismos) el patrón que veríamos en la pantalla fotosensible sería algo similar al patrón de la figura 1.1.2a, puesto que sería más probable encontrar impactos de estos «paquetes» en la zona donde las rectas que pasan por una de las aberturas y el emisor del haz de luz intersecan la pantalla fotosensible. Además, esta probabilidad decaería conforme nos alejemos de estos puntos, pues allí solamente incidirían paquetes que de alguna forma hubiesen rebotado con los bordes de las rendijas y se hubiesen desviado de la trayectoria.

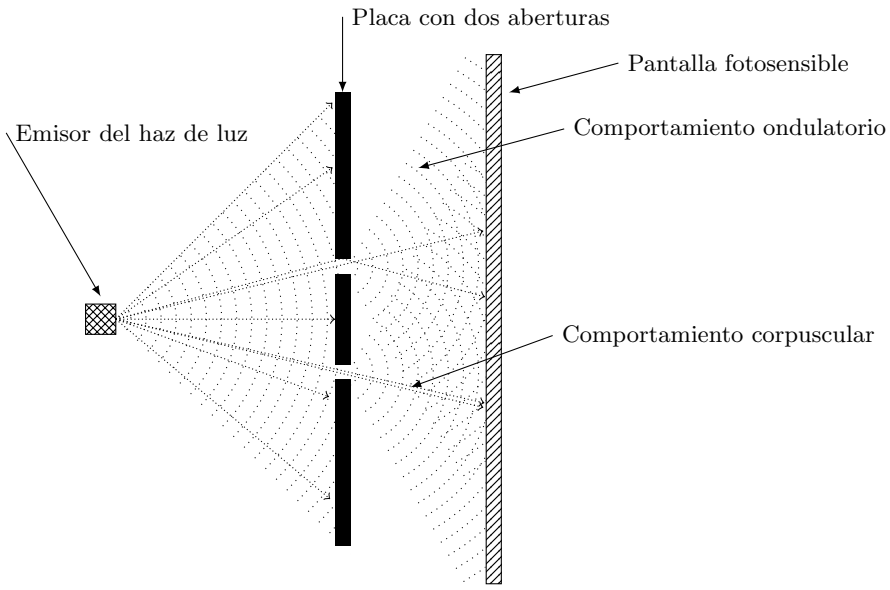
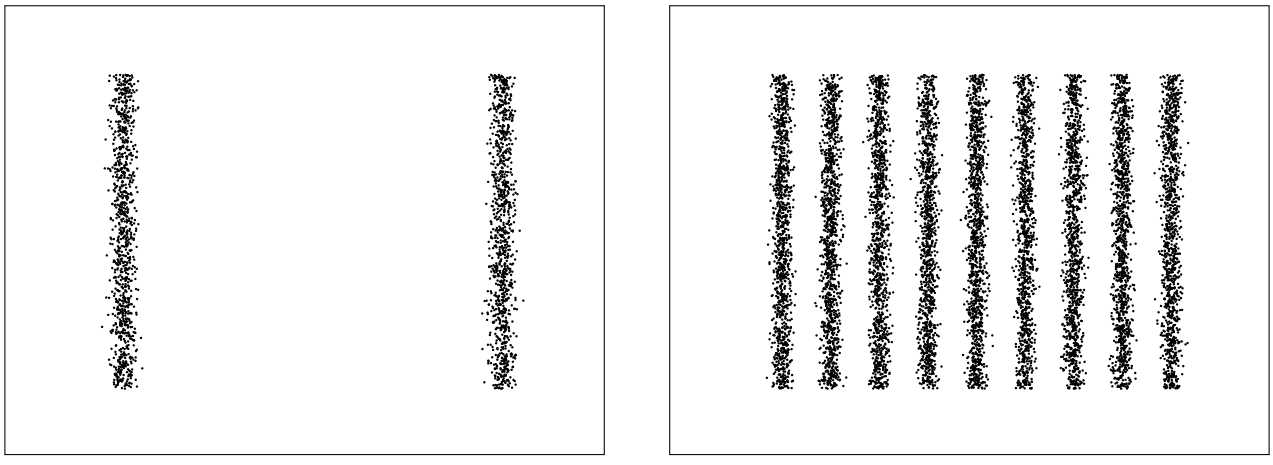


Figura 1.1.1: Vista cenital del modelo conceptual del experimento de Young.

No fue este patrón descrito el que Young encontró tras realizar el experimento, sino algo más parecido al patrón de la figura 1.1.2b, en la que se puede apreciar lo que se denota habitualmente como un *patrón de interferencia*. Young explicó estos resultados considerando que la luz era una onda que, al chocar contra la placa con las aberturas se dividía, mediante el principio de Huygens-Fresnel, en dos ondas, cada una de ellas centrada en una abertura, que interferían entre sí. La interferencia entre estas ondas implicaba que hubiese ciertas zonas donde las ondas se superponían con fases contrarias, resultando así en un punto donde la onda era muy poco (o nada) energética, los cuales correspondían a los puntos de la pantalla fotosensible donde no se conseguían detectar apenas «impactos». Por otro lado, en los puntos en los que ambas ondas interferían acopladas en fase se podía ver un alto número de detecciones en la pantalla receptora.



(a) (b)

Figura 1.1.2: En la gráfica *a*), el patrón de incidencia en la pantalla fotosensible para un comportamiento corpuscular. En *b*), el esperado para el comportamiento ondulatorio.

Las consecuencias del experimento de Young no conseguían explicar el porqué de este comportamiento, lo cual más tarde fue resuelto y enmarcado en un contexto más general en la teoría del electromagnetismo de Maxwell, pero sí dieron una evidencia científica de que ciertos comportamientos de la luz son fundamentalmente ondulatorios.

Años después, en 1924, el físico francés Louis de Broglie hipotetizó en su tesis doctoral [DB24], sobre una posible naturaleza ondulatoria similar a la que hemos visto para la luz aplicada a partículas materiales (tales como electrones). Este trabajo era fundamentalmente especulativo, pues no había hasta entonces ningún hecho experimental que avalase tal hipótesis. Fue por tanto mayúscula la sorpresa cuando, en 1925, los físicos Clinton Davisson y Lester Germer, al repetir el experimento de la doble rendija de Young sustituyendo el haz de luz por un haz de electrones [DG27] y la pantalla fotosensible por un cristal de níquel que era capaz de detectar impactos de electrones, detectaron un patrón de interferencia para los impactos de los electrones. Este hecho fue absolutamente deconcertante para una época en la que se creía que la materia era absolutamente corpuscular (de hecho ya existía un gran número de modelos atómicos como el de Rutherford o el de Bohr que suponían en todo momento las partículas como materiales).

Surgió así una nueva rama de la Física que intentaba explicar el hecho de que la materia exhibiese comportamientos ondulatorios y corpusculares simultáneamente. Esta corriente se llamó **Física Cuántica** y constituyó posiblemente el mayor hallazgo científico de la física del siglo XX.

1.2. Axiomática

La teoría matemática que surgió como respuesta a estos fenómenos y que constituyó la base de la teoría cuántica son un conjunto de postulados que, incluso a día de hoy, siguen impresionando tanto por su poder predictivo[1] como por su dificultad de interpretación.

Tanto es así que existen múltiples interpretaciones sobre el significado de la teoría, todas ellas en principio válidas, y discernir entre ellas sería una cuestión casi filosófica. Por ello, en nuestra presentación nos ceñiremos a la interpretación clásica de Copenhague, surgida en 1927 y desarrollada por físicos tan reputados como Bohr o Heisenberg, sobre otras más punteras y fantasiosas como por ejemplo la Interpretación de Multiversos de Hugh Everett [DG15], la cual han seguido teóricos reputados de la Computación Cuántica como David Deutsch [Deu98]. La interpretación de Copenhague, además, es la que más adeptos parece tener en la actualidad, y la mayoría de los textos sobre el tema han adoptado tal visión.

Para que la posterior formulación de la teoría de la computación cuántica no parezca arbitraria sino motivada por unas ideas concretas explicaremos conceptualmente en este momento una selección de axiomas de la Mecánica Cuántica, cuya formulación se da de una forma precisa en el apéndice A, que perfilará la axiomática de la teoría de la computación sobre la que este trabajo trata.

El primer postulado se refiere a la caracterización de la situación de los sistemas[2] físicos como estados. De hecho, el postulado afirma que cualquier sistema físico (desde sistemas constituidos por una sola partícula hasta sistemas muy complejos como gases) viene definido en la teoría cuántica por un elemento perteneciente a tipo de espacio matemático concreto. Este tipo de espacio, que formalmente se conoce como espacio de Hilbert[3] contendrá todos los posibles estados del sistema. Por tanto, tal y como veremos

[1] Ya nadie duda de la efectividad de la teoría, incluso aún cuando puede necesitar algún ajuste en ciertos entornos extremos, como aquellos en los que la gravedad es extremadamente fuerte, donde las teorías efectivas como la teoría cuántica de campos o la teoría de la gravedad cuántica se apoyan tanto en la teoría cuántica como en la relatividad de Einstein.

[2] Definiremos un «sistema» de forma general como una porción del Universo considerada para su estudio. De esta forma un sistema podría ser tanto un fotón o un bosón como un computador o un fluido.

[3] Un espacio $\mathcal{H}$ sobre un cuerpo $\mathbb{R}$ o $\mathbb{C}$ se dice de Hilbert si tiene definido un producto interior $\langle \cdot, \cdot \rangle$ y $\mathcal{H}$ es completo (toda

en breve, nuestra unidad básica de información en computación cuántica será un estado de un espacio de Hilbert, lo que indicará una posible vía para las implementaciones físicas de los computadores de este tipo.

El segundo, que será un componente clave del capítulo 4 cuando presentemos la Computación Adiabática, se refiere a la evolución temporal del estado de un sistema. Establece que la evolución de un sistema es determinista y además viene dada por un operador que llamaremos el hamiltoniano[4] mediante lo que se conoce como la ecuación de Schrödinger.

El tercero de los postulados (que tendrá una importancia crucial en la sección 2.2) establece cómo se construyen los espacios de estados de sistemas formados por una combinación de sistemas más pequeños. Para ello se introduce una operación algebraica, que permite combinar espacios de Hilbert cualesquiera de una forma totalmente general, conocido como el producto tensorial. Así pues el estado de un sistema complejo pertenecerá al producto tensorial de los espacios de estados de cada uno de los sistemas que lo componen.

Por último, los postulados restantes se pueden resumir como sigue: una característica medible[5] A de un sistema (por ejemplo, la posición de la partícula en un sistema formado por una partícula libre, o su velocidad) viene dada por un operador $\hat{A}$ que actúa sobre el sistema cuántico en cuestión. Al medir tal característica obtendremos un valor para ella de entre un conjunto de valores posibles[6] (que viene dado por el operador $\hat{A}$). Este valor no estará definido unívocamente sino que obtendremos cada valor de forma probabilista, cuyas probabilidades vienen dadas por el estado del sistema como veremos posteriormente. Ésta es una de las características más contraintuitivas de la Teoría Cuántica. De hecho, si seguimos con la analogía de un sistema formado por una partícula libre y quisiésemos medir su posición, la posición no estaría definida *a priori* sino que, al medirla, obtendríamos un valor de entre los diferentes valores posibles para esta posición de forma probabilista. Tras la medición de la característica, el estado se dice que *colapsa* y a partir de ese momento obtendremos el mismo valor para la característica en todas las sucesivas mediciones.

Veamos como todos estos aspectos de naturaleza tan incierta se aplican a nuestra área de estudio: la Computación.

sucesión de Cauchy converge) bajo la norma inducida por $\|\cdot\| = \sqrt{\langle \cdot, \cdot \rangle}$

[4]Veremos más adelante la definición precisa de operador, pero asumamos por el momento que es una caja negra que es capaz de extraer información del estado del sistema que hemos presentado con el postulado anterior

[5]En entornos científicos, una característica medible recibe el nombre de «observable».

[6]A este conjunto de valores se le denota comúnmente como el *espectro* de $\hat{A}$, denotado como $\sigma(\hat{A})$.

CAPÍTULO 2

Computación Cuántica: una Introducción.

Pincelada histórica aquí.

2.1. Bits Cuánticos

En el modelo de computación que aquí presentamos la unidad básica de información será el bit cuántico, o **qubit**[1] en clara analogía con el bit clásico de la computación clásica binaria. Podemos remarcar que el concepto de «bit» con el que tan familiarizados estamos es simplemente una entidad matemática (un elemento con un estado que corresponde a un elemento de $\mathbb{Z}_2 = \{0, 1\}$) desprovista de cualquier interpretación física con la que se pudiese implementar posteriormente en la construcción de computadores. De la misma forma, definiremos el qubit de forma conceptual como la base de la teoría de computación, evitando así preocuparnos por intrincados mecanismos de realización física.

Presentemos en primer lugar el concepto de forma intuitiva, tras lo que daremos una definición más precisa basadas en espacios matemáticos. Tal y como un bit clásico podía tomar dos valores (0 y 1), un qubit podrá tomar de igual manera un conjunto de estados diferentes. A dos de tales estados los llamaremos, por una clara analogía, $|0\rangle$ y $|1\rangle$, donde usamos la notación conocida como *notación de Dirac* o *notación ket*, que es ampliamente usada en entornos de la física cuántica.

Pero estos no son los únicos estados que el qubit puede tomar, pues si así fuese no habría una mejora con respecto a los bits que ya conocemos, sino que este puede estar en lo que llamaremos un estado de *superposición*. Un estado de superposición consiste en una combinación lineal de dos estados, que llamaremos *estados base*. Estos estados base tendrán que cumplir ciertas características de ortonormalidad que veremos en breve, pero por el momento asumamos que los estados ya presentados $\{|0\rangle, |1\rangle\}$ forman una base. De tal forma, un qubit en su estado más general $|\phi\rangle$ podrá escribirse como una combinación lineal de la forma

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{2.1.1}$$

¿Qué tipo de números son los coeficientes α y β de la ecuación anterior? Podríamos pensar en el modelo más simple, en el que resulten ser números reales, sin embargo, resulta que la física cuántica es fundamentalmente compleja por lo que definirlos como reales supondría una pérdida de generalidad que

[1] Elegimos el término «qubit» sobre el castellanizado «cúbit», pues parece haber un consenso internacional sobre mantener tal notación a pesar de que en ciertos textos se pueda encontrar el análogo castellano.

limitaría el potencial de futuras implementaciones de qubits en el mundo físico. Por ello los coeficientes los definiremos en el cuerpo complejo $\mathbb{C}$.

En los modelos clásicos de computación siempre hemos considerado que podemos observar un bit y determinar si está en el estado 0 o en el estado 1, así pues estaríamos tentados a suponer que podremos observar un qubit y obtener así su estado, es decir, obtener los coeficientes α y β. Nada más lejos de lo que ocurre en realidad. En la computación cuántica **el hecho de observar un qubit devuelve invariablemente un estado de la base** ($|0\rangle$ o $|1\rangle$) y **los coeficientes de la superposición solamente determinan las probabilidades con las que obtendremos cada uno de ellos**. La medición del qubit en el estado general de superposición como el de la ecuación 2.1.1 devolverá el valor de la base $|0\rangle$ con una probabilidad $|\alpha|^2$ y, respectivamente, el valor $|1\rangle$ con una probabilidad $|\beta|^2$.

Esto nos lleva a la interpretación probabilista de los coeficientes de la superposición. Al realizar la medición de un qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ obtendremos el estado $|0\rangle$ con una probabilidad $|\alpha|^2$ y el estado $|1\rangle$ con una probabilidad $|\beta|^2$. Esta interpretación nos obliga a imponer la restricción $|\alpha|^2 + |\beta|^2 = 1$, pues las probabilidades complementarias sabemos que deben sumar 1.

Otra particularidad, de nuevo restrictiva, sobre el comportamiento de los qubits es que **el hecho de medir su estado no deja el estado del qubit inmutado**, sino que lo hace colapsar al valor medido, perdiendo así cualquier información codificada en su superposición. La razón de ello es todavía desconocida, sin embargo es uno de los postulados[2] sobre los que se construye toda la teoría cuántica que tan buenos resultados ha dado, por lo que no parece probable que en un futuro pueda medirse el estado de un qubit sin hacerlo colapsar y por tanto no consideraremos tal posibilidad en nuestro marco teórico.[3]

Ejemplo 2.1.1. *Si tenemos un qubit preparado, digamos, al valor*

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{2.1.2}$$

y al medirlo obtenemos el valor $|1\rangle$ *(algo perfectamente posible pues las probabilidades de obtener este valor eran* $\left|\frac{1}{\sqrt{2}}\right|^2 = 50\,\%$*), el estado del qubit tras la medición será* $|\phi_1\rangle = |1\rangle = 0|0\rangle + 1|1\rangle$ *y por tanto todas las sucesivas mediciones no podrán dar un estado distinto a* $|1\rangle$*.*

Cabe preguntarse si nuestra base $\{|0\rangle, |1\rangle\}$ tiene algo de particular. Ciertamente no. Bajo las condiciones que hemos presentado, podemos ser matemáticamente algo más precisos y definir un qubit como un punto en un espacio vectorial complejo 2-dimensional. La ya mencionada base corresponde simplemente a una de las posibles bases que existen en este espacio y las identificaremos con los elementos de $\mathbb{C}^2$ $\begin{pmatrix}1\\0\end{pmatrix}$ y $\begin{pmatrix}0\\1\end{pmatrix}$ respectivamente. De tal forma el estado $|\phi\rangle$ que hemos presentado podría verse en notación vectorial como

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \equiv \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha\\\beta\end{pmatrix} \tag{2.1.3}$$

Con este tipo de notación vectorial en $\mathbb{C}^2$ podemos considerar fácilmente los conceptos de ortogonalidad y normalidad en función de sus componentes. Un vector $\begin{pmatrix}\alpha\\\beta\end{pmatrix}$ se dirá **normal** si $|\alpha|^2 + |\beta|^2 = 1$ y dos

[2] Postulado VI del apéndice A

[3] Aunque hemos presentado este comportamiento de forma arbitraria, el lector puede notar que es una consecuencia directa de los tres últimos postulados del apéndice A. En efecto, en la implementación de los qubits podemos asociar cada estado de la base con el valor un observable (a menudo la orientación del *spin* de una partícula; *up* $= |0\rangle$, *down* $= |1\rangle$) y el hecho de realizar esta medición, junto con dichos postulados, justifica todo el formalismo aquí presentado.

vectores $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ y $\begin{pmatrix}\hat{\alpha}\\ \hat{\beta}\end{pmatrix}$ se dirán **ortogonales** si $\alpha^*\hat{\alpha} + \beta^*\hat{\beta} = 0$.

Así pues la condición sobre los coeficientes $|\alpha|^2 + |\beta|^2 = 1$ que impusimos se puede ver como la condición de normalidad. Y por tanto solo consideraremos estados cuánticos normalizados.

La base $\{|0\rangle, |1\rangle\}$ no es la única que podemos considerar puesto que la única restricción que queremos para una base es que sea ortonormal. Así, por ejemplo, la siguiente base sería totalmente válida bajo nuestros axiomas

$$\left\{ \begin{pmatrix}1/\sqrt{2}\\ 1/\sqrt{2}\end{pmatrix}, \begin{pmatrix}1/\sqrt{2}\\ -1/\sqrt{2}\end{pmatrix} \right\} \tag{2.1.4}$$

De hecho esta base es comúnmente utilizada, tanto es así que tiene su notación *ket* particular. Muchos textos la escriben como $\{|+\rangle, |-\rangle\}$. Se puede comprobar que la relación con la base $\{|0\rangle, |1\rangle\}$ es

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \qquad |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \tag{2.1.5}$$

Pero en cualquier caso, dado un espacio con tal base, siempre podríamos reetiquetar los vectores de la base como $|0\rangle$ y $|1\rangle$, pues el espacio es igual bajo rotaciones (véase posteriormente la observación 2.1.4), por lo que podremos trabajar sin pérdida de generalidad con una base $\{|0\rangle, |1\rangle\}$.

Por otro lado, en un espacio vectorial complejo se puede considerar el conjugado de un vector $|\phi\rangle \equiv \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$ como el vector $\begin{pmatrix}\alpha^*\\ \beta^*\end{pmatrix}$. A este vector lo denotaremos mediante la notación *bra* $\langle\phi|$. Dados dos vectores se puede definir fácilmente su producto escalar interno $\langle\cdot,\cdot\rangle$ como

$$\langle \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \begin{pmatrix}\hat{\alpha}\\ \hat{\beta}\end{pmatrix} \rangle = \alpha^*\hat{\alpha} + \beta^*\hat{\beta} \tag{2.1.6}$$

que, usando la noción de vector conjugado, toma en su notación *bra-ket* la simpática forma

$$\langle\phi|\psi\rangle \tag{2.1.7}$$

Es bien sabido que un producto escalar $\langle\cdot,\cdot\rangle$ da lugar a una norma $\|\cdot\|$ mediante $\|\cdot\| = \sqrt{\langle\cdot,\cdot\rangle}$. La norma de un vector $|\phi\rangle$ en notación *ket* se podrá escribir como

$$\||\phi\rangle\| = \sqrt{\langle\phi|\phi\rangle} \tag{2.1.8}$$

Si reconsideramos en este punto la ortogonalidad de dos estados $|\phi\rangle$ y $|\psi\rangle$, podemos escribir la condición de ortogonalidad para estados como

$$\langle\phi|\psi\rangle = 0 \tag{2.1.9}$$

y la condición de normalidad como

$$\||\phi\rangle\| = 1 \tag{2.1.10}$$

a pesar de que en la mayoría de los casos prescindamos de la notación $\|\cdot\|$ y escribamos la norma como la raíz cuadrada del producto escalar en forma *bra-ket*.

Todo el formalismo presentado nos permite definir en este punto un qubit de forma totalmente precisa como sigue:

Definición 2.1.2 (Qubit)**.** *Un* qubit[4] *es la unidad básica de información en la computación cuántica que toma un valor, llamado* estado*, en un espacio de Hilbert $\mathcal{H}$ complejo bidimensional.*

Si quisiésemos parametrizar un qubit con números reales necesitaríamos cuatro de tales números pues para cada coeficiente complejo necesitaríamos dos reales para identificarlo (su parte real y su parte imaginaria, si lo consideramos en coordenadas cartesianas, o su módulo y su argumento en coordenadas esféricas), sin embargo, como vemos en la siguiente proposición, podremos hacer uso de la condición de normalidad y representarlo con tan solo tres números reales.

Proposición 2.1.3. *El estado general de un qubit puede escribirse sin pérdida de generalidad como*

$$|\phi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\right) \tag{2.1.11}$$

donde θ, φ y γ son valores en $\mathbb{R}$.

Demostración. Efectivamente, dado que el estado del qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ debe estar normalizado, se debe cumplir para algún $\hat{\theta} \in \mathbb{R}$ que

$$|\alpha| = \cos\hat{\theta}, \quad |\beta| = \sin\hat{\theta} \tag{2.1.12}$$

Pero un número complejo α de módulo $\cos\hat{\theta}$ se puede escribir de forma no ambigua como

$$\alpha = e^{i\hat{\gamma}}\cos\hat{\theta} \tag{2.1.13}$$

con $\gamma \in \mathbb{R}$, y de la misma forma

$$\beta = e^{i\hat{\varphi}}\sin\hat{\theta} \tag{2.1.14}$$

Por lo que, usando ambas ecuaciones vemos que

$$|\phi\rangle = e^{i\hat{\gamma}}\cos\hat{\theta}|0\rangle + e^{i\hat{\varphi}}\sin\hat{\theta}|1\rangle = e^{i\hat{\gamma}}(\cos\hat{\theta}|0\rangle + e^{i(\hat{\varphi}-\hat{\gamma})}\sin\hat{\theta}|1\rangle) \tag{2.1.15}$$

y, de una redefinición de variables, se sigue lo que queríamos demostrar.

□

Observación 2.1.4. *El factor $e^{i\gamma}$ en la ecuación 2.1.11 no tiene efectos observables mediante medición. Por ello consideraremos que los estados de dos qubits son iguales si simplemente se diferencian en un desplazamiento de fase $e^{i\gamma}$.*

Observación 2.1.5. *Si prescindimos del factor $e^{i\gamma}$ (y por tanto de la variable γ), podremos representar el estado del qubit sin ambigüedad con dos parámetros (θ, ϕ) que además, por su dominio de definición, pueden ser considerados como ángulos. Aprovechando esta particularidad, podremos representar el qubit como un punto en una esfera de radio unidad, que comúnmente se conoce como esfera de Bloch, y constituye una poderosa herramienta de representación gráfica de los qubits.*

[4] Vemos que la definición es perfectamente compatible con el concepto de sistema cuántico del apéndice A, dada la analogía del postulado I. De hecho, este postulado es el que motivó esta definición para el qubit.

2.2. Registros de n Qubits.

Vemos en este punto que el concepto de estado del qubit como un elemento de un espacio de Hilbert se puede extender de forma natural a sistemas formados por un número arbitrario de qubits, que llamaremos *registros*.

Por el postulado III parece que la forma natural de proceder es considerar el *producto tensorial* de todos los espacios $\mathcal{H}$ de estados de un qubit y suponer que el estado del registro de los qubits es simplemente un elemento del espacio producto, que denotaremos $\mathcal{H}^{\otimes n} = \mathcal{H} \otimes \cdots \otimes \mathcal{H}$.

Definamos pues el producto tensorial de dos espacios de Hilbert $\mathcal{H}$ y $\tilde{\mathcal{H}}$, denotado $\mathcal{H} \otimes \tilde{\mathcal{H}}$, como sigue.

Si $\{|i\rangle\}_i$ y $\{|j\rangle\}_j$ son bases para $\mathcal{H}$ y $\tilde{\mathcal{H}}$ respectivamente entonces consideramos que el conjunto $\{|i\rangle \otimes |j\rangle\}_{i,j}$ es una base del espacio de Hilbert $\mathcal{H} \otimes \tilde{\mathcal{H}}$. Por tanto si n y m son las dimensiones de $\mathcal{H}$ y $\tilde{\mathcal{H}}$ respectivamente entonces la dimensión de $\mathcal{H} \otimes \tilde{\mathcal{H}}$ es mn y la dimensión de $\mathcal{H}^{\otimes k}$ es n^k.

Así pues, con esta definición de la base para $\mathcal{H} \otimes \tilde{\mathcal{H}}$ podemos concluir que los elementos de $\mathcal{H}$ y $\tilde{\mathcal{H}}$ serán combinaciones lineales de elementos $|\phi\rangle \otimes |\psi\rangle$ con $|\phi\rangle \in \mathcal{H}$ y $|\psi\rangle \in \tilde{\mathcal{H}}$.

Es fácilmente comprobable ([Fol95]: teorema 7.12) que este espacio es, a su vez, un espacio de Hilbert, lo que nos asegura que los sistemas de n qubits son consistentes con la definición de *sistema* del postulado I. Además, el producto tensorial es una operación que satisface las siguientes propiedades, que serán útiles para realizar cálculos posteriores.

1. Si z es un escalar, $|\phi\rangle \in \mathcal{H}$ y $|\psi\rangle \in \tilde{\mathcal{H}}$ entonces

$$z(|\phi\rangle \otimes |\psi\rangle) = (z\,|\phi\rangle) \otimes |\psi\rangle = |\phi\rangle \otimes (z\,|\psi\rangle) \tag{2.2.1}$$

2. Si $|\phi\rangle\,, |\gamma\rangle \in \mathcal{H}$ y $|\psi\rangle \in \tilde{\mathcal{H}}$ entonces

$$(|\phi\rangle + |\gamma\rangle) \otimes |\psi\rangle = |\phi\rangle \otimes |\psi\rangle + |\gamma\rangle \otimes |\psi\rangle \tag{2.2.2}$$

3. Si $|\phi\rangle \in \mathcal{H}$ y $|\psi\rangle\,, |\gamma\rangle \in \tilde{\mathcal{H}}$ entonces

$$|\phi\rangle \otimes (|\psi\rangle + |\gamma\rangle) = |\phi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\gamma\rangle \tag{2.2.3}$$

Para abreviar y dado que el producto tensorial será el único tipo de producto, a excepción del producto escalar para el cual ya conocemos la notación, definido entre dos elementos de un espacio de Hilbert, a veces obviaremos el símbolo $\otimes$ y escribiremos el elemento $|\phi\rangle \otimes |\psi\rangle$ como $|\phi\rangle\,|\psi\rangle$ o incluso $|\phi\psi\rangle$.

Por otro lado, dado que ya conocemos la dimensionalidad de los espacios para qubits, que resulta ser 2, sabemos que el espacio correspondiente a un registro de n qubits tiene 2^n dimensiones y la base

$$\{\underbrace{|00\cdots0\rangle}_{n}, \cdots, \underbrace{|11\cdots1\rangle}_{n}\} \tag{2.2.4}$$

constituye una base del espacio $\mathcal{H}^{\otimes n}$. Como cada uno de los enteros binarios que usamos para la notación de la base corresponde unívocamente a un entero de $\{0, \cdots, 2^n - 1\}$ comúnmente denotaremos a tal base como $\{|0\rangle\,, \cdots, |2^n - 1\rangle\}$.

Veamos ahora una serie particular de estados de $\mathcal{H}$ que, como veremos en la sección B.3, jugarán un papel crucial en la teoría de la información cuántica.

Definición 2.2.1 (Estados de Bell)**.** *Los estados de Bell (a veces llamados pares EPR, por Einstein, Podolsky y Rosen que los introdujeron en su famoso artículo de 1935 [EPR35]) son los siguientes*

- $|\mathbf{\Phi}^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$;
- $|\mathbf{\Phi}^-\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$;
- $|\mathbf{\Psi}^+\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$;
- $|\mathbf{\Psi}^-\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$;

Observación 2.2.2 ($|\mathbf{\Phi}^+\rangle$ es un estado entrelazado)**.** *El par EPR $|\mathbf{\Phi}^+\rangle$ tiene una característica muy peculiar que será la base para ciertos comportamientos cuánticos que veremos más adelante. Esta característica es:*

No existen estados cuánticos para un solo qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ y $|\psi\rangle = \gamma|0\rangle + \delta|1\rangle$ tal que $|\mathbf{\Phi}^+\rangle = |\phi\rangle \otimes |\psi\rangle$, en efecto esto se puede comprobar fácilmente comprobando que el sistema

$$\begin{cases} \alpha\gamma = \beta\delta = \frac{1}{\sqrt{2}} \\ \alpha\delta = \beta\gamma \ = \ 0 \end{cases} \tag{2.2.5}$$

no tiene soluciones en el plano complejo.

Los estados con la propiedad mencionada serán referidos como ***estados entrelazados*** *y serán de vital importancia cuando estudiemos la transmisión de información.*

2.3. Puertas y Circuitos Cuánticos.

Tal y como en computación clásica ya nos son familiares ciertas puertas lógicas como, por ejemplo, las puertas OR, NOT, AND y múltiples combinaciones de ellas, podremos definir ciertos operadores que, conceptualmente, serán entidades análogas a las puertas booleanas ya mencionadas. Estas puertas, en el marco cuántico, las denominaremos indistinguidamente **puertas cuánticas** u **operadores cuánticos**.

Una de las propiedades de las puertas cuánticas es que cada uno de estos operadores debe actuar linealmente[5] sobre el estado del qubit (o qubits) sobre el que se aplica. Ésta es una de las claves del potencial de los circuitos cuánticos en relación a su eficiencia ya que, al aplicar un operador sobre una superposición, obtendremos un estado de superposición resultado de aplicar el operador a cada uno de los vectores de la base.

La linealidad se puede escribir como sigue: para cada registro, ya sea de un solo qubit o de múltiples, $|\phi\rangle = \sum_i \alpha_i |i\rangle$, si denotamos como $U|\phi\rangle$ al valor del registro tras aplicar la puerta cuántica U, entonces por linealidad debe cumplirse que

$$U|\phi\rangle = \sum_i \alpha_i U|i\rangle \tag{2.3.1}$$

Así pues, usando la linealidad, una puerta cuántica queda totalmente definida por los valores que toma sobre una base cualquiera del espacio de estados del registro. Además, aprovechando la linealidad podremos escribir cualquier puerta cuántica U en forma matricial usando la forma en la que ésta actúa sobre

[5] La razón para esto viene dada por el famoso *Teorema de Wigner* [SMCS08] que establece que, para que sea posible mantener ciertas simetrías en los espacios de Hilbert, los operadores que actúan sobre él deben ser lineales.

los vectores de la base en la representación en $\mathbb{C}^2$.

Ejemplo 2.3.1 (El análogo cuántico al NOT)**.** *Como ya hemos esbozado, encontrar un operador análogo al NOT clásico en un circuito cuántico es equivalente a encontrar una matriz compleja (una puerta cuántica) que actúe sobre los estados de la base* $\{|0\rangle, |1\rangle\}$ *tal y como actuaría una puerta NOT clásica. Es decir, debemos hallar una matriz* X *tal que*

$$\begin{aligned} X|0\rangle &= |1\rangle \\ X|1\rangle &= |0\rangle \end{aligned} \tag{2.3.2}$$

Pero usando la representación de $|0\rangle$ *y* $|1\rangle$ *como vectores vemos que la matriz*

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{2.3.3}$$

actúa tal y como deseamos, pues

$$X|0\rangle \equiv X\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv |1\rangle \tag{2.3.4}$$

Y análogamente podemos comprobar que $X|1\rangle = |0\rangle$*.*

A esta matriz que aquí definimos la denotaremos la[6] ***puerta NOT cuántica****.*

Observación 2.3.2 (Puertas en notación *ket-bra*)**.** *Con la notación que hemos definido, tal y como se remarca en [FLS65], dados dos estados* $|\phi\rangle$ *y* $|\psi\rangle$*, la notación ket-bra* $|\phi\rangle\langle\psi|$ *representa un operador, puesto que actúa sobre un estado arbitrario* $|\delta\rangle$ *tal que*

$$(|\phi\rangle\langle\psi|)|\delta\rangle = |\phi\rangle\langle\psi|\delta\rangle = \underbrace{\langle\psi|\delta\rangle}_{\omega\in\mathbb{C}}|\phi\rangle = \omega|\phi\rangle \tag{2.3.7}$$

que de hecho puede comprobarse que es unitario. Usando esta notación, si tenemos un subespacio $\mathcal{W}$ *del espacio de estados con base* $\{|\tilde{0}\rangle, |\tilde{1}\rangle, \cdots, |\tilde{k}\rangle\}$ *podemos proyectar cualquier estado en este subespacio mediante el operador*

$$\mathcal{P}_{\mathcal{W}} = \sum_{i=0}^{k} |\tilde{i}\rangle\langle\tilde{i}| \tag{2.3.8}$$

que llamaremos el proyector sobre $\mathcal{W}$*.*

[6] A pesar de que trabajaremos con operadores casi exclusivamente en forma de matrices, es conveniente remarcar que también es posible escribir operadores sin tener que recurrir a la notación matricial. Como ejemplo, la puerta NOT cuántica es posible escribirla en notación de Dirac como

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{2.3.5}$$

pues podemos ver que, por ejemplo,

$$X|0\rangle = (|0\rangle\langle 1| + |1\rangle\langle 0|)|0\rangle = |0\rangle\langle 1|0\rangle + |1\rangle\langle 0|0\rangle = 0|0\rangle + 1|1\rangle = |1\rangle \tag{2.3.6}$$

Pero la linealidad no es la única restricción que debemos imponer a nuestras puertas cuánticas. Como ya vimos en la sección 2.1, un estado cuántico corresponde a un estado *normalizado*, por lo que, para obtener un registro en un estado válido (normalizado) la puerta cuántica no debería alterar la norma del estado, es decir, debería cumplirse que $\|U|\phi\rangle\| = \||\phi\rangle\| = 1$. Los operadores (matrices) que satisfacen este requisito son las denominadas matrices unitarias, es decir, aquellas tales que

$$U^\dagger U = I \tag{2.3.9}$$

Donde el símbolo $U^\dagger$ indica la **matriz adjunta**, tambien denotada como la **matriz adjunta hermítica**, es decir, aquella que está definida implícitamente como

$$\langle U|x\rangle, |y\rangle\rangle = \langle |x\rangle, U^\dagger|y\rangle\rangle \qquad \text{para estados cualesquiera } |x\rangle, |y\rangle \tag{2.3.10}$$

Posiblemente el mayor exponente de las puertas cuánticas aplicables a un solo qubit sea la conocida como **puerta H de Hadamard**. Esta puerta se define unívocamente como la puerta que actúa sobre la base $\{|0\rangle, |1\rangle\}$ como $H|0\rangle = |+\rangle$ y $H|1\rangle = |-\rangle$. Con tal definición y como hemos hecho para la puerta NOT, podemos obtener de forma simple la representación matricial de la puerta de Hadamard como

$$H := \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{2.3.11}$$

Es un ejercicio elemental comprobar que en efecto el operador de Hadamard es unitario[7].

Ejemplo 2.3.3. *La puerta de Hadamard se puede usar para generar números realmente aleatorios.*

De hecho, basta preparar un qubit al estado $|0\rangle$ y aplicarle la puerta de Hadamard, obteniendo así el qubit en el estado $|+\rangle$. Al medir el registro obtendremos los estados $|0\rangle$ y $|1\rangle$ con un 50 % de probabilidad cada uno. Así pues, para generar un entero de n bits completamente aleatorio bastará preparar un registro de n qubits, cada uno al estado $|0\rangle$, aplicarle la operación de Hadamard a cada uno de ellos y medir el valor del registro, obteniendo así un valor $k \in \{0, \cdots, 2^n - 1\}$.

Por último presentaremos una puerta cuántica (que en realidad serán una familia uni-paramétrica de puertas con la misma estructura), llamada puerta de desplazamiento de fase (denotada R_s), que será de relevancia en secciones posteriores de trabajo. Este operador es diferente a los vistos hasta ahora en el sentido de que no cambia la probabilidad de las diferentes mediciones del qubit, sino tan solo la fase del coeficiente cuántico del estado. De tal forma definimos implícitamente la puerta R_s como el operador cuántico que transforma la base tal que $R_s|0\rangle = |0\rangle$ y $R_s|1\rangle = \exp(is)|1\rangle$.

$$R_s := \begin{pmatrix} 1 & 0 \\ 0 & \exp(is) \end{pmatrix} \tag{2.3.13}$$

El caso $s = \pi$ es particularmente importante, puesto que invierte la fase del estado del qubit. Por lo que es utilizada en multitud de contextos. Denotaremos a R_π mediante el símbolo Z y la llamaremos la función Z de Pauli.

Para una registro de n qubits podremos seguir el mismo mecanismo y escribir operadores como matrices de dimensión 2^n. Podemos construir operadores a partir de otros más pequeños mediante el *producto*

[7] La puerta de Hadamard se puede escribir en notación de Dirac simplemente como

$$H = \frac{1}{\sqrt{2}}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\Big) = \frac{1}{\sqrt{2}}\Big((|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|\Big) = |+\rangle\langle 0| + |-\rangle\langle 1| \tag{2.3.12}$$

por lo que el lector puede notar de forma clara la relación entre los coeficientes del operador en representación matricial y los términos de la suma del operador en notación de Dirac.

de Kronecker definido tal que, si la representación matricial de dos operadores A y B en $\mathcal{H}$ y $\tilde{\mathcal{H}}$ respectivamente es

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \qquad B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1q} \\ b_{21} & b_{22} & \cdots & b_{2q} \\ \vdots & \vdots & \vdots & \vdots \\ b_{p1} & b_{p2} & \cdots & b_{pq} \end{pmatrix} \tag{2.3.14}$$

entonces su producto tensorial de Kronecker $A \otimes B$ actúa sobre $\mathcal{H} \otimes \tilde{\mathcal{H}}$ y su representación matricial[8] es la matriz de dimensiones $mp \times nq$

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix} \tag{2.3.15}$$

Al igual que con el producto tensorial de espacios de Hilbert, podemos escribir la acción sucesiva del producto tensorial de un operador A consigo mismo n veces como $A^{\otimes n}$. Es fácil comprobar (y esto motiva la definición) que

$$(A \otimes B)(|\psi\rangle \otimes |\phi\rangle) = (A\,|\psi\rangle) \otimes (B\,|\phi\rangle) \tag{2.3.17}$$

Pero trabajar con la representación matricial tan solo es útil para realizar cálculos algebraicos, sin embargo, cuando queremos representar conceptualmente ciertas puertas cuánticas actuando sobre qubits usamos los *diagramas de circuitos cuánticos* que procedemos a describir.

Un diagrama de circuito cuántico se puede ver como la evolución temporal de un registro. Cada línea horizontal del diagrama corresponderá a un qubit y la evolución del sistema se supondrá de izquierda a derecha. De esta forma, el extremo izquierdo de cada una de las líneas se puede ver como la entrada del circuito, y el extremo derecho como la salida (o resultado) del circuito.

Cada una de las puertas se representarán en el circuito simplemente escribiendo un recuadro sobre la línea correspondiente al qubit sobre el que actúan con el nombre de la puerta que actúa. Podemos ver ejemplos de esto en la figura 2.3.1.

Para puertas que actúan en más de un qubit podríamos seguir la misma idea simplemente dibujando recuadros más grandes, y ciertamente eso haremos para puertas arbitrarias, sin embargo algunas más famosas y comunes tienen su propia notación como podemos ver en la figura 2.3.2.

Veamos ahora puertas que actúan en más de un solo qubit. Teóricamente podemos considerar puertas que actúen en registros con un número arbitrario de qubits, y de hecho eso haremos en el estudio teórico. Sin embargo, en ciertos textos que estudian la complejidad de los circuitos cuánticos como en [AB09] se restringe el dominio de actuación de las puertas cuánticas a, como máximo, 3 qubits. Esta restricción se impone por varias razones: en primer lugar, la implementación física de puertas arbitrariamente grandes

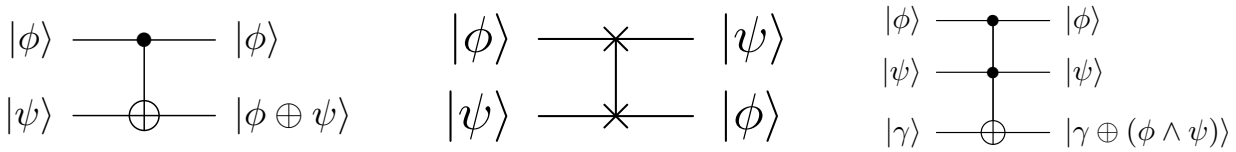
[8] Al igual que antes, cabe mencionar que la notación de Dirac se erige por sí sola como una notación suficiente para los cálculos. En efecto, con la notación de Dirac para H expuesta, se tiene que (basándonos en las ideas de [RT18] sección 3.1)

$$H^{\otimes n} = \Big(\frac{1}{\sqrt{2}}\Big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\Big)\Big)^{\otimes n} = \frac{1}{2^{n/2}} \sum_{i,j=0}^{2^n-1} (-1)^{i\cdot j} |i\rangle\langle j| \tag{2.3.16}$$

donde $i \cdot j$ es el producto escalar entre las representaciones binarias de n bits de i y j.

(a) Puerta de Hadamard (b) Puerta Z (c) Puerta NOT (d) Puerta de desplazamiento de fase

Figura 2.3.1: Representación de algunas de las puertas lógicas mencionadas para un solo qubit.



(a) Puerta controlled-NOT (b) Puerta de intercambio (c) Puerta Toffoli

Figura 2.3.2: Representación de algunas de las puertas lógicas para múltiples qubit.

no es posible a día de hoy excepto descomponiéndolas en puertas más pequeñas. El estudio teórico de ellas tampoco es simple a no ser que se encuentren formas de escribirlas implícitamente dado que la dimensionalidad crece increíblemente rápido (exponencialmente) con el número de qubits sobre los que actúan. Y por último, cualquier puerta cuántica arbitrariamente grande se puede descomponer, como veremos en la sección B.1, como la acción sucesiva de ciertas puertas cuánticas actuando en un máximo de tres qubits.

Veamos ahora ciertos ejemplos de puertas cuánticas que tienen nombre propio y que usaremos posteriormente en los circuitos cuánticos. Una de ellas se conoce como la puerta de intercambio (puerta $SWAP$) cuya función es, dados dos qubits, intercambiar sus estados tal y como se ve en 2.3.2b, se puede comprobar fácilmente que es unitaria y que su representación matricial viene dada por:

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.3.18}$$

Otro famoso ejemplo que de hecho tendrá un papel importante más adelante es la puerta de *Toffoli*, también conocida como *controlled-controlled-NOT* o, abreviadamente, como $CCNOT$ que actúa sobre la base de forma que si los dos primeros qubits están en el estado $|1\rangle$ entonces se invierte el tercer qubit, y se deja inmutado si alguno de los dos primeros qubit está en el estado $|0\rangle$. La representación circuital se puede ver en 2.3.2c y su representación matricial es:

$$CCNOT = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \tag{2.3.19}$$

Veamos cómo la puerta Toffoli puede exhibir un comportamiento que nos resultará familiar

Observación 2.3.4 (Toffoli para calcular la operación AND)**.** *Si preparamos el tercer qubit que introducimos a la puerta Toffoli al estado* $|0\rangle$ *entonces esta puerta actúa como un AND reversible, es decir, como*

un AND cuántico, sobre los estados de los dos primeros qubits. En efecto podemos ver que actúa sobre los vectores de la base de forma que, para cualesquiera $a, b \in \{0, 1\}$

$$CCNOT\Big(|a\rangle |b\rangle |0\rangle \Big) = |a\rangle |b\rangle |a \wedge b\rangle \tag{2.3.20}$$

Esto nos permite, utilizando las leyes de Morgan, definir la puerta cuántica OR *como*

$$OR\Big(|\phi\rangle |\varphi\rangle |\psi\rangle \Big) = X^{\otimes 3} \cdot CCNOT\Big((X |\phi\rangle)(X |\varphi\rangle) |\psi\rangle \Big) \tag{2.3.21}$$

o usando extensión podemos escribirla como

$$|\phi\rangle |\varphi\rangle |\psi\rangle \xrightarrow{\text{OR}} |\phi\rangle |\varphi\rangle |\neg(\psi \oplus (\neg\phi \wedge \neg\varphi))\rangle = |\phi\rangle |\varphi\rangle |\neg(\psi \oplus (\neg(\phi \vee \varphi)))\rangle \tag{2.3.22}$$

Lo cual nos servirá en un futuro para simular circuitos booleanos con circuitos cuánticos.

2.4. El operador de medición

Hemos presentado en la sección 2.1 la característica axiomática del colapso por medición de los qubits. Veamos cómo este particular comportamiento es extrapolable de forma natural a registros de más de un qubit. Tal y como hemos visto, para un qubit en un estado $|\phi\rangle \in \mathcal{H}$ la probabilidad de obtener un estado $|i\rangle$ con $i \in \{0, 1\}$ es $|\langle i|\phi\rangle|^2$. De la misma forma y sin cambio apenas de notación, para un registro en el estado $|\psi\rangle \in \mathcal{H}^{\otimes n}$ la probabilidad de obtener un estado $|j\rangle$ de la base será $|\langle j|\psi\rangle|^2$. Esta caracterización de la probabilidad de medición será usada más adelante en el trabajo.

Para indicar en un circuito cuántico que se efectúa una medición de un qubit usaremos una representación que se muestra en la figura 2.4.1, en la que la doble línea que codifica la salida representa que el operador devuelve un valor clásico binario indicando si se ha medido el vector de la base $|0\rangle$ o $|1\rangle$.

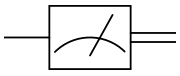


Figura 2.4.1: Diagrama para el operador de medición en un circuito cuántico.

Podremos en cualquier momento usar el mismo diagrama para el operador de medición a registros de n qubits simplemente representando n líneas para la puerta y sabiendo que el valor de salida será un entero en $\mathbb{Z}_{2^n}$.

CAPÍTULO 3

El Algoritmo de Shor

Desde los orígenes de la computación una de las ramas más estudiadas en Teoría Algorítimica ha sido la Teoría de Números, siendo uno de sus problemas cumbre la factorización prima. Sabemos por el teorema fundamental de la aritmética que cualquier entero n puede descomponerse como producto de potencias de números primos $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ y el hecho de encontrar estos números primos ha sido un problema recurrente a lo largo de los años dadas las múltilples ventajas de poseer una descomposición prima de un número para problemas de muy distinta índole.

Durante todos estos años, la búsqueda de un algoritmo eficiente en los computadores clásicos para hallar esta factorización ha sido infructuosa, sin claras perspectivas de cambio en los próximos años. El mejor algoritmo general que hasta la fecha conocemos para factorización en computación clásica conocido como *GNFS* tiene un orden[1] de ejecución sub-exponencial[2] (ver [LV18])

$$L_N\Big[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\Big] \tag{3.0.1}$$

donde N es el entero a factorizar.

Sin embargo, fue en 1994 cuando Peter Shor mostró ([Sho95]) que, en el paradigma de la computación cuántica, esta descomposición sí podría realizarse en tiempo aceptable. Presentamos en esta sección tal algoritmo, conocido como el *Algoritmo de Shor*.

Teorema 3.0.1 (Algoritmo de Shor)**.** *Existe un algoritmo cuántico que, dado un entero N, devuelve la factorización prima de N en orden temporal*[3] *$polylog(N)$.*

[1] Usamos para las complejidades la notación L definida tal que $L_N[\alpha, c] = \exp\Big((c + o(1))(\log N)^{\alpha}(\log\log N)^{1-\alpha}\Big)$

[2] Decimos que un problema pertenece a la clase **SUBEXP** de los problemas subexponenciales si para cada $\varepsilon > 0$ existe un algoritmo con orden temporal $O\Big(2^{n^{\varepsilon}}\Big)$ que lo resuelve.

[3] Definiremos *polylog*(N) como el conjunto de los órdendes $O(P(\log N))$ donde P es un polinomio cualquiera. El orden se define de forma análoga a como se define en la complejidad clásica, basándonos en máquinas de Turing (en este caso cuánticas). Sin embargo aquí el lector notará que usaremos para la caracterización de complejidad el número de puertas cuánticas necesarias para implementar el algoritmo. Esto se justifica en los apéndices D y **??**, donde se da una equivalencia polinomial entre la complejidad basada en máquinas de Turing cuánticas y la basada en circuitos cuánticos.

El algoritmo de Shor requiere ciertos fundamentos teóricos que deberemos abordar primero, lo que no nos impide en este punto dar una descripción conceptual del mismo. Dado un número N, bastará demostrar que podremos encontrar un solo factor K no trivial en tiempo polilogarítmico, dado que podremos ejecutar el algoritmo de nuevo con las entradas K y N/K y esto necesitaremos hacerlo un máximo de $\log N$ veces, pues un número N no puede tener más de $\log N$ divisores primos distintos de 1, y por tanto el algoritmo sería polilogarítmico de igual forma.

Una de las ideas clave del algoritmo fue propuesta por Miller en [Mil76] y consistirá en la reducción del problema de la factorización prima al problema conocido como *búsqueda del orden*, es decir, deberemos encontrar el orden r de un entero A en el grupo $\mathbb{Z}_N^*$. La razón de ello es que, con buena probabilidad (afinaremos esta afirmación más adelante), el orden r de A será par y además $A^{r/2}+1 \not\equiv 0 \pmod N$ por lo que, por el lema 3.2.1, $A^{r/2}-1$ compartirá un factor primo no trivial con N, que se podrá calcular con el simple algoritmo de Euclides (algoritmo 5) para el máximo común divisor, que es altamente eficiente en tiempo y memoria.

Encontraremos por tanto un algoritmo en $polylog(N)$ que será como sigue: dado un registro cuántico inicializado al estado cero $|0\cdots 0\rangle$ el algoritmo transformará tal estado a la superposición de todos los estados $|x\rangle$ tal que $x \leq N$ que cumplan $A^x \equiv y_0 \pmod N$. Usando resultados básicos de la Teoría de Números, el conjunto de valores x que cumplen tal condición será de la forma $\{x_0 + ri\}_{i\in\mathbb{N}}$ y además r será el orden de A.

¿Cómo computaremos el *periodo* r de la serie armónica? Usaremos la ya conocida transformada de Fourier, en su eficiente forma cuántica (QFT). De hecho probaremos que existe un circuito cuántico de tamaño polilogarítmico que la computa. En ciertos problemas esto podría no ser suficiente pues, como ya hemos mencionado, la información del resutlado de la QFT contenida en un estado cuántico no es medible en su completitud, sino tan solo un estado de colapso. Sin embargo veremos que podremos obtener información significativa para nuestro problema a partir de una sola medición del estado resultado del algoritmo.

Por el teorema anterior y sabiendo que el número de bits n necesario para codificar un entero N es $\lceil \log_2 N \rceil$ podemos decir que el problema de la factorización prima pertenece al análogo cuántico para la clase **P**, llamada **BQP**. Por si el lector desease conocer más a fondo la definición de **BQP** y su caracterización dentro de la Teoría de la Complejidad hemos incluido en el apéndice **??** un breve estudio sobre esta clase.

Corolario 3.0.2. *El problema de la factorización prima pertenece a* **BQP**.

3.1. Preliminares para la factorización cuántica

3.1.1. Transformada de Fourier Cuántica en $\mathbb{Z}_m$.

Definición 3.1.1 (Tansformada de Fourier Discreta en $\mathbb{Z}_M$(DFT))**.** *Para cada vector $f \in \mathbb{C}^M$, definimos la* ***transformada de Fourier en*** *$\mathbb{Z}_m$ de f como el vector $\hat{f}$ donde la coordenada j-ésima de $\hat{f}$ es*

$$\hat{f}(j) = \frac{1}{\sqrt{M}} \sum_{k\in\mathbb{Z}_M} f(k) \exp\left(\frac{2\pi i}{M} jk\right) \tag{3.1.1}$$

Podemos dar en este punto una revisión del algoritmo clásico para calcular la transformada de Fourier,

conocido como la *Fast Fourier Transform* (FFT) y que se tiene un lugar hegemónico entre los algoritmos de cálculo de la DFT, tanto es así que ciertos textos usan la notación DFT y FFT casi indistintamente. Dado que el algortimo de la transformada cuántica seguirá una forma de proceder similar, veamos un resumen del algoritmo FFT.

Denotamos de ahora en adelante $\exp\left(\frac{2\pi}{M}i\right) = \zeta$, al que llamaremos *factor de rotación*. Si dado un vector $v = (v_0, \cdots, v_{M-1})$ definimos $v_{\text{par}} = (v_0, v_2, v_4, \cdots, v_{M-2})$ y $v_{\text{impar}} = (v_1, v_3, \cdots, v_{M-1})$ podemos escribir la ecuación 3.1.1 como sigue

$$\begin{aligned}
\hat{f}(j) &= \frac{1}{\sqrt{M}} \sum_{k\in\mathbb{Z}_M} f(k)\zeta^{jk} \\
&= \frac{1}{\sqrt{M}} \sum_{k=0}^{N/2-1} \zeta^{-2kj} f_{\text{par}}(k) + \frac{1}{\sqrt{M}} \sum_{k=0}^{N/2-1} \zeta^{-j(2k+1)} f_{\text{impar}}(k) \\
&= \frac{1}{\sqrt{M}} \sum_{k=0}^{N/2-1} \zeta^{-2kj} f_{\text{par}}(k) + \frac{\zeta^{-1}}{\sqrt{M}} \sum_{k=0}^{N/2-1} \zeta^{-2jk} f_{\text{impar}}(k) \\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{M/2}} \sum_{k=0}^{N/2-1} \zeta^{-2kj} f_{\text{par}}(k) + \frac{\zeta^{-1}}{\sqrt{M/2}} \sum_{k=0}^{N/2-1} \zeta^{-2jk} f_{\text{impar}}(k)\right) \\
&= \frac{1}{\sqrt{2}}\left(\hat{f}_{\text{par}}(j) + \zeta^{-j}\hat{f}_{\text{impar}}(j)\right)
\end{aligned} \tag{3.1.2}$$

Así pues obtenemos, usando el hecho de que[4] $\zeta^{M/2+j} = -\zeta^j$ y $\zeta^{M+j} = \zeta^j$

$$\sqrt{2}\hat{f}(j) = \begin{cases} \hat{f}_{\text{par}} + \zeta^{-j}\hat{f}_{\text{impar}} & \text{si } 0 \le j \le M/2-1 \\ \hat{f}_{\text{par}} - \zeta^{-j}\hat{f}_{\text{impar}} & \text{si } M/2 \le j \le M-1 \end{cases} \tag{3.1.3}$$

Esta descomposición nos proporciona una forma de calcular la DFT de un vector de tamaño 2^m en función de dos vectores de tamaño 2^{m-1}. Se puede comprobar, simplemente resolviendo la ecuación de recurrencia para el orden de ejecución y suponiendo un caso base realizable en un tiempo constante, que el número de operaciones (clásicas) necesario para realizar la FFT de un entero de m bits es $O(m2^m) = O(M\log(M))$ que crece exponencialmente con el tamaño de la entrada.

Habiendo visto cómo funciona la FFT, usemos la teoría cuántica para optimizarla.

Definición 3.1.2 (Tansformada de Fourier Cuántica en $\mathbb{Z}_M$(QFT))**.** *Suponemos que $M = 2^m$ es una potencia exacta de 2, sea $\{|0\rangle, \cdots, |M-1\rangle\}$ una base ortonormal de un sistema cuántico y sea $|\varphi\rangle = \sum_{j=0}^{M-1} |j\rangle$ un estado cuántico. La* ***transformada de Fourier cuántica*** *F_M es una operación definida por*

$$|\varphi\rangle = \sum_{j=0}^{M-1} \alpha_j |j\rangle \to \sum_{j=0}^{M-1} \frac{\alpha_j}{\sqrt{M}} \sum_{k=0}^{M-1} \zeta^{-jk} |k\rangle \tag{3.1.4}$$

En particular, podemos ver que cada estado cuántico base $|j\rangle$ transforma como sigue[5]

$$|j\rangle \to \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \zeta^{-jk} |k\rangle \tag{3.1.5}$$

[4] Se sigue directamente de la identidad de Euler $e^{xi} = \cos x + i \sin x$ y de la periodicidad de las funciones trigonométricas.

Lema 3.1.3. *El estado transformado de $|j\rangle$ se puede escribir como producto de qubits de la forma que sigue.*

$$|j\rangle \to \frac{1}{\sqrt{M}}\Big(|0\rangle + e^{-2\pi i(0.j_m)}|1\rangle\Big)\otimes\cdots\otimes\Big(|0\rangle + e^{-2\pi i(0.j_1\cdots j_{m-1}j_m)}|1\rangle\Big) \tag{3.1.6}$$

Donde

$$(0.j_1\cdots j_{m-1}j_m) := \sum_{i=1}^{m} j_i\, 2^{-i} \tag{3.1.7}$$

Demostración. Si tomamos la expansión binaria de un entero de m bits k, $k = (k_1k_2\cdots k_m)_2$ podemos escribir, para un estado de la base $|j\rangle$

$$\begin{aligned}
|j\rangle \to \frac{1}{\sqrt{M}}\sum_{k=0}^{m-1}\zeta^{-jk}|k\rangle &= \frac{1}{\sqrt{M}}\sum_{k_1,k_2\cdots,k_m\in\{0,1\}}\zeta^{-j\sum_{r=1}^{m}2^{m-r}k_r}|k_1\rangle\otimes\cdots\otimes|k_m\rangle \\
&= \frac{1}{\sqrt{M}}\sum_{k_1,k_2,\cdots,k_m\in\{0,1\}}\bigotimes_{r=1}^{m}\zeta^{-j2^{m-r}k_r}|k_r\rangle \\
&= \frac{1}{\sqrt{M}}\bigotimes_{r=1}^{m}\Big(\sum_{k_r\in\{0,1\}}\zeta^{-j2^{m-r}k_r}|k_r\rangle\Big) = \frac{1}{\sqrt{M}}\bigotimes_{r=1}^{m}\Big(|0\rangle + \zeta^{-j2^{m-r}}|1\rangle\Big) \\
&= \frac{1}{\sqrt{M}}\bigotimes_{r=1}^{m}\Big(|0\rangle + e^{-\frac{2\pi i}{2^m}j2^{m-r}}|1\rangle\Big) = \frac{1}{\sqrt{M}}\bigotimes_{r=1}^{m}\Big(|0\rangle + e^{-2\pi ij2^{-r}}|1\rangle\Big)
\end{aligned} \tag{3.1.8}$$

Expandiendo el exponente j del *factor de rotación* mediante su representación binaria $j = (j_1j_2\cdots j_m)_2 = \sum_{l=1}^{m}2^{m-l}j_l$ podemos escribir la exponencial del último término como

$$\begin{aligned}
\exp\left(-2\pi i\sum_{l=1}^{m}2^{m-l}j_l/2^r\right) &= \exp\left(-2\pi i\sum_{l=1}^{m}2^{m-r-l}j_l\right) \\
&= \exp(-2\pi i(0.j_{m-r+1}j_{m-r+2}\cdots j_m))
\end{aligned} \tag{3.1.9}$$

Permitiéndonos escribir finalmente

$$|j\rangle \to \frac{1}{\sqrt{M}}\bigotimes_{r=1}^{m}\Big(|0\rangle + \exp(-2\pi i(0.j_{m-r+1}j_{m-r+2}\cdots j_m))|1\rangle\Big) \tag{3.1.10}$$

Lo que completa la prueba. □

[5] Sabiendo que cada estado cuántico de la base transforma como se ha mostrado es sencillo ver que F_M puede escribirse en representación como operador (observación 2.3.2) de la forma

$$F_M = \frac{1}{\sqrt{M}}\sum_{j,k=0}^{M-1}\zeta^{-jk}|k\rangle\langle j|$$

y no es difícil comprobar ([XL95]) que esta operación es unitaria. Además, si escribiésemos la representación matricial del operador veríamos que la matriz asociada $\mathbb{F}_M \in \mathcal{M}_{M\times M}(\mathbb{C})$ es una matriz que en su posición (j,k)-ésima toma el valor $\zeta^{-jk}/\sqrt{M}$, lo que concuerda con la presentación que se ha dado para la DFT clásica en $\mathbb{Z}_M$.

Podemos usar esta caracterización del estado transformado por la QFT para crear un circuito cuántico que la compute, como vemos a continuación.

Teorema 3.1.4 (Algoritmo para la transformada de Fourier cuántica)**.** *Para cada m, M con $M = 2^m$ existe un algoritmo cuántico que usa $O(m^2) = O(\log M)$ operaciones cuánticas elementales y calcula la QFT de un estado cualquiera.*

Demostración. Definimos en primer lugar una notación abreviada para un modelo de puerta cuántica que usaremos en este circuito cuántico que se utiliza [XL95]. Será una redefinición de la puerta de desplazamiento de fase y la denotaremos como *puerta de rotación*, que estará definida por

$$\tilde{R}_s = R_{-\frac{2\pi}{2^s}} = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{-2\pi i}{2^s}\right) \end{pmatrix} \tag{3.1.11}$$

Supongamos que nuestro estado de entrada es un estado producto de qubits $|j\rangle = \bigotimes_{r=1}^{m} |j_r\rangle$. Apliquemos la operación de Hadamard al primer qubit, obteniendo

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i(0.j_1)} |1\rangle) \otimes |j_2\rangle \otimes \cdots \otimes |j_m\rangle \tag{3.1.12}$$

Si aplicamos en este punto la puerta $\tilde{R}_2$, obtenemos

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i(0.j_1 j_2)} |1\rangle) \otimes |j_2\rangle \otimes \cdots \otimes |j_m\rangle \tag{3.1.13}$$

Y aplicando iterativamente las operaciónes de rotación llegamos a

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i(0.j_1 j_2 \cdots j_m)} |1\rangle) \otimes |j_2\rangle \otimes \cdots \otimes |j_m\rangle \tag{3.1.14}$$

Si repetimos el mismo procedimiento con el segundo qubit del producto, que será igual excepto con una puerta de rotación menos, llegamos a

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i(0.j_1 j_2 \cdots j_m)} |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i(0.j_2 \cdots j_m)} |1\rangle) \otimes \cdots \otimes |j_m\rangle \tag{3.1.15}$$

Y por tanto, aplicando iterativamente para cada qubit, cada vez con una rotación menos que en la iteración anterior, obtendremos un estado final

$$\frac{1}{\sqrt{2^m}}(|0\rangle + e^{-2\pi i(0.j_1 j_2 \cdots j_m)} |1\rangle) \otimes (|0\rangle + e^{-2\pi i(0.j_2 \cdots j_m)} |1\rangle) \otimes \cdots \otimes (|0\rangle + e^{-2\pi i(0.j_m)} |1\rangle) \tag{3.1.16}$$

Que es exactamente el estado que queríamos, excepto por el orden. Nada nos impide rotarlo usando $\lfloor m/2 \rfloor$ puertas de intercambio (fig 2.3.2b) al final del circuito.

¿Cuántas puertas cuánticas usa el circuito que aquí hemos expuesto? Para el qubit en la posición r en el producto usamos una puerta de Hadamard y $r-1$ puertas de rotación, además, al final del circuito le damos la vuelta con $\lfloor m/2 \rfloor$ puertas de intercambio, obteniendo así un número de puertas

$$m + \sum_{r=1}^{m}(r-1) + \lfloor m/2 \rfloor \sim \frac{3m + (m-1)m}{2} = O(m^2) \tag{3.1.17}$$

Hemos obtenido de esta forma una agilización exponencial del algoritmo clásico FFT dado que el algoritmo QFT se ejecuta usando tan solo $O(m^2)$ operaciones.

□

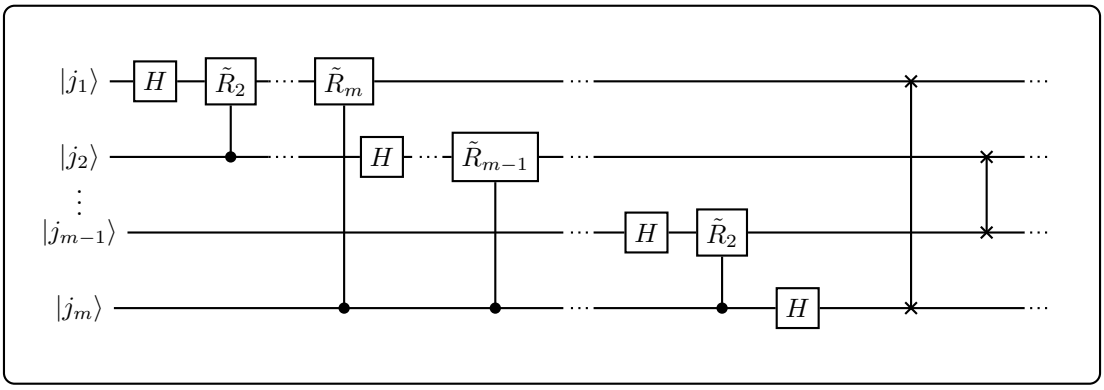


Figura 3.1.1: Circuito cuántico para el algoritmo QFT.

Observación 3.1.5. *La QFT transforma un registro preparado al valor $|0\rangle$ a una superposición uniforme de todos los estados del sistema, tal y como haría la aplicación del operador de Hadamard m-dimensional $H^{\otimes m}$.*

Demostración. En efecto, dado un registro con m qubits inicializados cada uno de ellos al valor $|0\rangle$, el efecto de aplicar la QFT es

$$|0\rangle \xrightarrow{F_M} \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} \zeta^{-0x} |x\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle = H^{\otimes m} |0\rangle \tag{3.1.18}$$

□

3.1.2. Búsqueda del Orden.

Teorema 3.1.6. *Existe un algoritmo cuántico que se ejecuta en tiempo polylog(N) que, dada una entrada binaria (A, N) con $mcd(A, N) = 1$ encuentra el menor r tal que $A^r \equiv 1 \,(mod\ N)$, es decir, encuentra el orden de A en el grupo $\mathbb{Z}_N^*$.*

La sección entera constituirá una demostración del teorema que acabamos de presentar, pero probemos en primer lugar un lema que nos permitirá agilizar ciertos pasos más adelante.

Lema 3.1.7. *La función $x \to A^x \,(mod\ N)$ puede computarse en tiempo polylog(N) en un circuito cuántico.*

Demostración. De hecho veamos que esta computación se puede realizar eficiéntemente con un circuito clásico. Si demostramos esta afirmación, dado que por cualquier cómputo que se pueda realizar en tiempo $T(N)$ sobre una máquina de Turing existe un circuito booleano de de tamaño $T(N) \log T(N)$ que la computará (para una prueba véase la demostración de [AB09], Teorema 6.6, en la que se usa un modelo de máquina de Turing conocida como *máquina de Turing inconsciente*, que es totalmente equivalente a los circuitos booleanos), sabremos que existe un circuito booleano de tamaño $O(\log N \log\log N)$ que lo realiza. Utilizando la inclusión de circuitos booleanos en cuánticos (Teorema D.6.1 del apéndice), habremos demostrado por extensión que existirá un circuito cuántico que realizará el algoritmo y tendrá también un tamaño en *polylog*(N). Elegiremos el algoritmo expuesto en [Ros03] para exponenciación modular que presentamos en la figura 1 y comprobaremos que, en efecto, se ejecuta en tiempo polinómico sobre $\log N$.

Algoritmo 1 Algoritmo para exponenciación modular

```
1: procedure EXPONENCIACIÓNMODULAR(A: entero, x = (x_{k-1}, ..., x_0)_2: entero positivo, N: entero positivo)
2:     u ← 1
3:     potencia ← A mod N
4:     for i ← 1 to k − 1 do
5:         if x_i = 1 then u ← (u · potencia) mod N
           potencia ← (potencia · potencia) mod N
       return u        (u = A^x mod N)
```

Podemos ver que el algoritmo presentado realiza $k-1 = \log_2 x - 1$ bucles en los cuales realiza un máximo de dos multiplicaciones y toma dos módulos. Como la multiplicación de *potencia* se puede realizar en $O(log(N^2))$ (pues *potencia* y u nunca serán mayores que N) y la operación módulo también tiene una complejidad de $O(log(N))$ (se puede consultar en [BZ10]) se sigue que el algoritmo, como queríamos, se realiza en un tiempo $polylog(N)$. □

Observación 3.1.8. *Este circuito cuántico, cuya existencia hemos demostrado, al ser lineal podrá actuar sobre un estado de superposición y por tanto convertirá un estado arbitrario como sigue*

$$\sum_i \alpha_i |i\rangle \to \sum_i \alpha_i \left|A^i \ (mod\ N)\right\rangle \tag{3.1.19}$$

por lo que podemos considerar conceptualmente que este circuito cuántico realizará la exponenciación modular en paralelo para distintos valores.

Aunque hemos elegido este algoritmo por su sencillez, existen otros algoritmos como el expuesto por Peter L. Montgomery en [Mon85] que son ligeramente más eficientes asintóticamente, aunque siguen teniendo una complejidad $polylog(N)$.

Recordemos que el objetivo es encontrar, para un elemento A concreto en $\mathbb{Z}_n^*$, su orden. Definamos ahora el algoritmo de la búsqueda del orden. Partiremos, como en casi todos los algoritmos cuánticos, de un registro preparado al valor $|0\rangle$. El registro estará formado por $2m$ qubits donde m es el entero tal que[6] $n^2 \leq 2^m < 2n^2$. Usaremos la notación $|0\rangle = |0\rangle \otimes |0\rangle$ para enfatizar que el registro (formado por $2m$ qubits) es el registro producto de dos registros de m qubits.

Usando la QFT tal y como vimos en la observación 3.1.5, podemos cambiar el estado del primer m-registro a una superposición uniforme de la forma

$$\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle \otimes |0\rangle \tag{3.1.20}$$

Ahora, dado este registro, lo queremos transformar a una superposición de estados $|x\rangle |A^x \pmod n\rangle$. Por el lema 3.1.7 esto se puede llevar a cabo en tiempo polilogarítmico, obteniendo así

$$\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle \otimes |A^x \pmod n\rangle \tag{3.1.21}$$

[6] P. Shor no da en su artículo original ninguna razón para esta elección, tampoco así ciertos artículos consultados que analizan el trabajo de Shor, sin embargo creemos firmemente que la elección para m viene motivada por lo siguiente: dado que A será un elemento menor que n, usando el Teorema de Lagrange ([Gal12] Teorema 9.1) sabemos que su orden dividirá al orden del grupo multiplicativo, es decir, a $|\mathbb{Z}_n^*| = \phi(n)$. Por lo que, en particular, su orden será menor que n. Tomando tal elección para el valor de m tendremos por seguro que al menos encontraremos n ciclos completos en la sucesión $\{A^x \pmod n \mid x \in \{0, \cdots, 2^m - 1\}\}$, lo que nos permitirá que la QFT halle el periodo r con gran precisión.

Y aplicando de nuevo la QFT al primer registro obtenemos el estado

$$\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} (F_{2^m} |x\rangle) \otimes |A^x \pmod n\rangle = \frac{1}{2^m} \sum_{x,y=0}^{2^m-1} \zeta^{-xy} |y\rangle \otimes |A^x \pmod n\rangle \tag{3.1.22}$$

Donde ζ es el factor de rotación $e^{\frac{2\pi i}{2^m}}$, análogamente a como se definió en la sección 3.1.1.

En este estado particular, cabe preguntarse qué valor es probable obtener cuando se lleve a cabo la medición sobre el registro. Para un valor arbitrario $|z\rangle \left|A^k \pmod n\right\rangle$ la probabilidad será[7]

$$\left| \frac{1}{N} \sum_{x,y=0}^{2^m-1} \zeta^{-xy} \underbrace{\left\langle A^k \pmod n \middle| A^x \pmod n \right\rangle}_{\delta^{A^k \pmod n}_{A^k \pmod n}} \underbrace{\langle z|y\rangle}_{\delta^y_z} \right|^2 = \left| \frac{1}{N} \sum_{A^x \equiv A^k \pmod n} \zeta^{-xz} \right|^2 \tag{3.1.23}$$

Donde δ^j_i hace referencia a la función delta de Kronecker y donde la última igualdad se justifica por la ortogonalidad de la base. Como en este último término solamente sumamos los términos en x tal que $A^x \equiv A^k \pmod n$, la diferencia entre x y k siempre[8] será un múltiplo del orden r de A. Así pues, escribiendo $x = br + k$ tenemos

$$\left| \frac{1}{N} \sum_{b=0}^{\lfloor (2^m-k-1)/r \rfloor} \zeta^{-(br+k)z} \right|^2 = \left| \frac{1}{N} \sum_{b=0}^{\lfloor (2^m-k-1)/r \rfloor} \zeta^{-brz} \right|^2 \tag{3.1.24}$$

Donde hemos sacado factor común ζ^{-kz} y al tomar módulos, por ser $|\zeta^{-kz}| = 1$, el término es despreciable. Es más, como vimos, por definición de ζ y usando la periodicidad de la exponencial compleja, se tiene que $\zeta^i = \zeta^{2^m+i}$, así pues $\zeta^{-brz+2^m} = \zeta^{-brz}$. Esto nos motiva a definir sin pérdida de generalidad $\{rz\}$ como el valor congruente con rz módulo 2^m tal que $-2^{m-1} \leq \{rz\} < 2^{m-1}$.

Aproximando[9] el valor del sumatorio con una integral podemos escribir

$$\frac{1}{2^m} \sum_{b=0}^{\lfloor (2^m-k-1)/r \rfloor} \zeta^{-b\{rz\}} = \frac{1}{2^m} \int_0^{\lfloor (2^m-k-1)/r \rfloor} \zeta^{-b\{rz\}} \, db + \mathcal{O}(2^{-m}) \tag{3.1.25}$$

Donde haciendo el cambio de variable $u = rb/2^m$, $du = db\, r/2^m$ obtenemos que el sumatorio se puede escribir como

$$\frac{1}{r} \int_0^{\frac{r}{2^m} \lfloor (2^m-k-1)/r \rfloor} e^{-2\pi i u\{rz\}/r} \, du + \mathcal{O}(2^{-m}) \tag{3.1.26}$$

Como además $k < r$, podemos aproximar la cota superior de la integral por el valor 1 cometiendo[10] tan solo un error $\mathcal{O}(2^{-m})$, obteniendo así el sumatorio como

[7] Tan solo es necesario aplicar la interpretación del producto escalar como probabilidad del postulado V y usar que la operación "tomar adjunto" invierte el orden de los productos tensoriales.

[8] Esto es sencillo de probar usando el resultado C.0.9 del apéndice.

[9] Probar que el error es efectivamente $\mathcal{O}(2^{-m})$ excede las pretensiones de este trabajo. Sin embargo, si el lector quiere ver una prueba rigurosa le recomendamos acudir a un texto de análisis matemático clásico en el que se introduzca la integral de Riemann. Para probar que la definición clásica de las sumas de Darboux tienden en efecto al valor de la integral se usa un argumento que serviría perfectamente para acotar el error que aquí cometemos.

[10] El error que cometemos es fácilmente verificable acotando el valor de la función suelo ($\lfloor \cdot \rfloor$) entre el valor de su argumento y el valor de su argumento menos uno y usando el hecho de que $2^m \geq n^2 \geq n \geq r \geq k$.

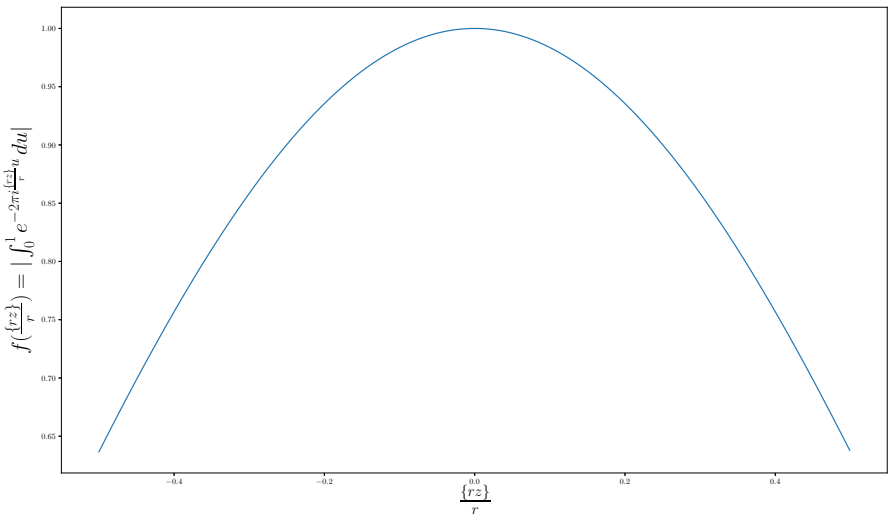


Figura 3.1.2: Módulo de la integral de la ecuación 3.1.27 para valores de $\frac{\{rz\}}{r}$ entre $-1/2$ y $1/2$.

$$\frac{1}{r}\int_0^1 e^{-2\pi i u\{rz\}/r}\, du + \mathcal{O}(2^{-m}) \tag{3.1.27}$$

Supongamos en este punto que $-\frac{1}{2} \leq \frac{\{rz\}}{r} < \frac{1}{2}$ (lo cual es ciertamente más restrictivo que el rango de valores que podía tomar $\{rz\}$ por su definición) entonces podemos ver en la figura 3.1.2 que el valor de la integral para tales valores es mínimo para $\frac{\{rz\}}{r} = \pm\frac{1}{2}$, es decir, en los extremos[11]. En cuyo caso la integral toma el valor $\frac{2}{\pi r} + \mathcal{O}(2^{-m})$, valor que elevaremos al cuadrado para obtener la probabilidad. Este cuadrado es $\frac{4}{\pi^2 r^2} + \mathcal{O}(2^{-m})^2$ que es mayor que $\frac{1}{3r^2}$ para un valor de 2^m suficientemente grande (para que el error en el término $\mathcal{O}(2^{-m})$ sea suficientemente pequeño), cota inferior que usaremos de ahora en adelante.

Si recapitulamos, hemos probado que la probabilidad de, al realizar la medición, encontrar el registro en un estado $|z\rangle\left|A^k \pmod n\right\rangle$ es mayor (de hecho, estrictamente mayor) que $\frac{1}{3r^2}$ si se cumple que

$$\frac{-r}{2} \leq \{rz\} < \frac{r}{2} \tag{3.1.28}$$

Pero por nuestra definición de la magnitud $\{rz\}$, esto es equivalente a que exista un d tal que

$$\frac{-r}{2} \leq rz - d2^m < \frac{r}{2} \tag{3.1.29}$$

Que, con un poco de aritmética elemental, podremos escribir como

$$\left|\frac{z}{2^m} - \frac{d}{r}\right| \leq \frac{1}{2^{m+1}} \tag{3.1.30}$$

Como al inicio de la explicación del algoritmo hemos elegido el valor m tal que $2^m \geq n^2$ tenemos que existe como máximo una fracción d/r con $r < n$ que cumple la ecuación 3.1.30. El cómo obtener esta fracción es simple: básicamente intentaremos aproximar la fracción $\frac{z}{2^m}$ mediante la fracción más cercana

[11] Esta afirmación es fácilmente demostrable analíticamente ya que la integral de una exponencial tiene solución explícita simple. A pesar de ello y para no introducir complejidad adicional, la calculamos numéricamente con *scipy* y un *wrapper* para cálculo complejo.

con un denominador menor que n (recordemos que $r < n$), lo cual podemos realizar mediante la potente técnica (que se verá en la sección 3.3) de la expansión en fracciones continuas y, de hecho, una vez más esto lo podemos lograr en tiempo polilogarítmico en N.

Recapitulemos lo que sabemos hasta el momento: hemos hallado la probabilidad de que el orden r, junto con los valores conocidos de m y z, cumpla la ecuación 3.1.30 para algún entero d, que ha resultado ser mayor que $1/3r^2$. Supongamos entonces que se ha dado este caso y por tanto queremos hallar r. Para ello, dado $z/2^m$ intentamos aproximar esta fracción lo máximo posible con otra fracción cuyo denominador no sea mayor que r. como solamente podrá haber una fracción que cumpla estas características y que además cumpla la cota de 3.1.30, sabremos que esta fracción es precisamente d/r, si suponemos que d y r son coprimos entonces bastará tomar el denominador, y habremos obtenido r. Si, en caso contrario, no eran coprimos el algoritmo habrá fallado (pues la fracción estará reducida y el denominador tan solo será un divisor de r) y deberemos ejecutarlo de nuevo.

Una vez obtengamos la fracción $\frac{d}{r}$ como hemos mencionado y si además el numerador es coprimo con el denominador habremos encontrado r, lo cual era el objetivo desde el principio, si no, el algoritmo habrá fallado. Cabe por tanto preguntarse el número de estados $|z\rangle \left|A^k \pmod n\right\rangle$ que nos permitirán calcular r de la forma mencionada.

Como existen $\phi(r)$ (ver definición C.0.5 si no se está familiarizado con la función ϕ de Euler) números coprimos con r y r valores diferentes para las potencias de A (proposición C.0.9) entonces existen $r\phi(r)$ estados que nos permiten obtener r de la forma mencionada. Cada uno de esos estados hemos visto que se medirá con una probabilidad mayor que $\frac{1}{3r^2}$, por lo que obtendremos r con una probabilidad mayor que $\frac{\phi(r)}{3r}$. Además, como se muestra en el clásico [HW+79], se tiene que $\frac{\phi(r)}{r} \approx \frac{1}{e^\gamma \log\log r}$ donde γ es la constante de Euler $0{,}57721\cdots$, lo que da una probabilidad más que aceptable[12] de que hallemos r en $O(\log\log r)$ iteraciones. De hecho podemos ver, usando cálculo numérico, que las iteraciones necesarias del algoritmo para asegurar que la probabilidad de obtener un valor de r correcto sea mayor que $2/3$ vienen dadas por la figura 3.1.3.

Algoritmo 2 Algoritmo para hallar el periodo r de un elemento a en $\mathbb{Z}_n^*$ usando la QFT.

1: **procedure** BÚSQUEDAORDEN(a entero, n: entero de longitud m.)
2: Inicializar (preparar) un estado de $2m$ qubits $|0\rangle\,|0\rangle$
3: Aplicar QFT al primer registro para obtener la superposición $\frac{1}{\sqrt{2^m}} \sum_x |x\rangle\,|0\rangle$
4: Aplicar el algoritmo 1 para obtener $\frac{1}{\sqrt{2^m}} \sum_x |x\rangle\,|a^x \pmod n\rangle$
5: Aplicar QFT al primer registro obteniendo $\frac{1}{2^m} \sum_x \sum_y e^{2\pi i x y/2^m} |y\rangle\,|a^x \pmod n\rangle$
6: Medir el primer registro, obteniendo el valor y.
7: $r' \leftarrow$ CalcularR(y, m)
8: **if** $a^{x+r'} \pmod n = a^x \pmod n$ **then return** r'
9: **else return** BúsquedaOrden(a, m)

[12] Dado que el suceso «obtener un r válido» se puede modelar con una distribución discreta de Bernoulli de probabilidad, digamos, p (en nuestro caso será mayor que $O\left(\frac{1}{3e^\gamma \log\log r}\right)$); la cantidad de intentos necesarios para hallar un r válido se puede modelar con una distribución geométrica X de probabilidades $P(X = k) = (1-p)^{k-1}p$ y, calculando la esperanza de esta variable aleatoria, que resulta ser $1/p$ obtenemos que el número de intentos necesarios para obtener un r válido es, de media, $1/p$ con varianza $\frac{1-p}{p^2}$.

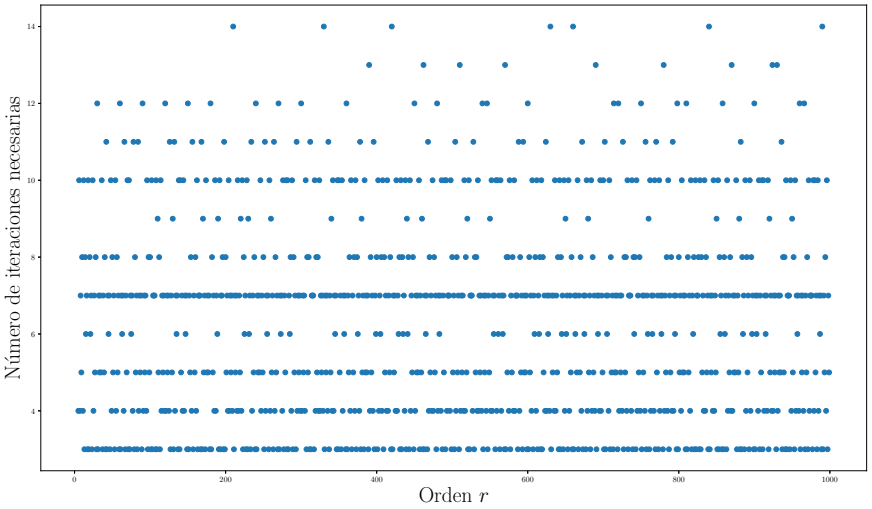


Figura 3.1.3: Iteraciones necesarias del algoritmo de la búsqueda del orden para que la probabilidad de encontrar el valor correcto de r sea mayor que 2/3.

3.2. Relacionando Factorización con Búsqueda del Orden.

Lema 3.2.1. *Para cada par de enteros n e y, con $y \leq n$, si $y^2 = 1 \pmod n$ y además se cumple que $y \pmod n \notin \{+1, -1\}$ entonces* $\text{mcd}(y-1, n) \notin \{1, n\}$.

Demostración. Como $y^2 = 1 \pmod n$ entonces n debe dividir a $y^2 - 1 = (y+1)(y-1)$ pero como $\text{mcd}(y-1, n) \notin \{1, n\}$ entonces n no puede dividir a $(y+1)$ ni a $(y-1)$. Supongamos que $y-1$ y n son coprimos. Como n divide a $(y+1)(y-1)$, bajo este supuesto, n también dividiría a $y+1$, lo que no es posible por hipótesis. Lo que implica que $y-1$ y n no pueden ser coprimos (y por tanto $mcd(Y-1, N) > 1$). Además como $y - 1 < n$ entonces $mcd(y-1, n) \leq y - 1 < n$, lo que demuestra el lema.

□

Lema 3.2.2. *Sea n un entero impar*[13] *y sea $n = p_1^{e_1} \cdots p_k^{e_k}$ su factorización prima. Entonces la probabilidad de que un x aleatorio de $\{1, \cdots, n-1\}$ tenga orden par y además $x^{r/2} \not\equiv -1 \pmod n$ es, al menos, $1 - \left(\frac{1}{2}\right)^{k-1}$*

Demostración. Definamos para la prueba la notación r_i para referirnos al orden del x aleatorio en el grupo multipicativo $\mathbb{Z}^*_{p_i^{e_i}}$. Como los r_i son coprimos, por el lema C.0.6 tenemos que el orden r de x es $\text{mcm}\{r_i\}$. Consideremos la descomposición de cada r_i como un producto de una potencia de dos por un número impar, esto es $r_i = 2^{k_i}\tilde{r}_i$. Podemos comprobar que la conclusión no se cumple solo cuando los 2^{k_i} coinciden.

En efecto, supongamos que los k_i son todos iguales a 0, es decir, los órdenes son impares. El mínimo común múltiplo r será por tanto impar. Supongamos ahora que los k_i son iguales a un entero k no nulo.

[13]Esto no supone una pérdida de generalidad para el caso al que aplicamos el algoritmo pues en el caso en el que n no sea un número par podremos dividirlo entre 2 iterativamente, obteniendo así factores no triviales, hasta obtener un número impar..

De esta forma r será

$$r = 2^k \prod_{i=1}^{k} \tilde{r}_i = r_i \prod_{j \neq i} \tilde{r}_j \ \forall i \tag{3.2.1}$$

Para calcular $x^{r/2} \pmod n$, lo cual podemos hacer pues r por la ecuación anterior es par, basta, por el teorema chino de los restos (corolario C.0.11), calcular $x^{r/2} \pmod{p_i^{e_i}}$ y realizar el producto. Pero sabemos que

$$x^{r/2} \pmod{p_i^{e_i}} \equiv x^{r_i/2 \prod_{j \neq i} \tilde{r}_j} \pmod{p_i^{e_i}} \equiv \left(x^{r_i/2}\right)^{\prod_{j \neq i} \tilde{r}_j} \pmod{p_i^{e_i}} \tag{3.2.2}$$

Como por [Meu16], la ecuación de $x^2 \equiv 1 \pmod{p_i^{e_i}}$ con p_i primo y $e_i \geq 1$ tiene solo ± 1 como posibles soluciones y no puede ser que $x^{r_i/2}$ sea 1 pues esto contradiría el hecho de que r_i es el orden de x, tenemos que $x^{r_i/2} \equiv -1 (\mod p_i^{e_i})$ y por tanto

$$\left(x^{r_i/2}\right)^{\prod_{j \neq i} \tilde{r}_j} \pmod{p_i^{e_i}} \equiv (-1)^{\prod_{j \neq i} \tilde{r}_j} \pmod{p_i^{e_i}} \equiv -1 \pmod{p_i^{e_i}} \tag{3.2.3}$$

donde la última congruencia se tiene del hecho de que por construcción $\prod_{j \neq i} \tilde{r}_j$ es un número impar.

Veamos la probabilidad de que se dé esta situación particular de que todas las potencias de dos sean iguales. Sabemos de nuevo por el teorema chino de los restos que elegir un x aleatorio en $\mathbb{Z}_n$ es equivalente a elegir un elemento aleatorio en cada $\mathbb{Z}_{p_i^{e_i}}$. Por [Knu68b] sabemos que para cada primo p el grupo $\mathbb{Z}_{p^\alpha}^*$ es cíclico y por tanto la probabilidad de que elijamos un elemento cuyo orden sea múltiplo de una potencia de dos particular por un número impar será, como mucho, $1/2$. Así pues los múltiplos potencias de dos de los órdenes coincidirán con una probabilidad de $\left(\frac{1}{2}\right)^{k-1}$ lo que completa la prueba. □

Observación 3.2.3. *No debe preocuparnos el hecho de que, en el caso de que n sea primo, la probabilidad reduzca a* 0*. Tiene sentido por el hecho de que si supusiésemos que existe un x bajo las condiciones anteriores, por el lema 3.2.1 existiría un divisor no trivial de n, lo cual no es posible. Además, nunca ejecutaremos la búsqueda del orden, como veremos más adelante, con un n primo*

3.3. Método de las Fracciones Continuas

Como hemos visto en la ecuación 3.1.30, en cierto momento del algoritmo de Shor queremos, dado un real $\frac{z}{2^m}$, aproximarlo por una fracción $\frac{d}{r}$ con el denominador acotado estrictamente superiormente por n. Para ello usaremos el método de las fracciones continuas. Una *fracción continua* es un número representado de la forma que sigue, con a_0 un entero no negativo y los demás a_i enteros estrictamente positivos.

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \tag{3.3.1}$$

Dado un número real $\alpha > 0$, en el marco teórico, se puede calcular su expansión (finita o infinita, según si α pertenecía a $\mathbb{Q}$ o a $\mathbb{R} \setminus \mathbb{Q}$) como fracción continua como sigue: en primer lugar extraemos de α su parte entera $\lfloor \alpha \rfloor$ y su parte decimal $\alpha - \lfloor \alpha \rfloor$. Si denotamos $R = 1/(\alpha - \lfloor \alpha \rfloor)$ entonces $R \geq 1$ y podemos escribir

$$\alpha = \lfloor \alpha \rfloor + \frac{1}{R} \tag{3.3.2}$$

Si obtenemos la representación para R tal y como hemos hecho con α entonces obtenemos una fracción de la forma

$$\lfloor \alpha \rfloor + \frac{1}{\lfloor R \rfloor + \frac{1}{\tilde{R}}} \tag{3.3.3}$$

Si repetimos iterativamente este proceso obtenemos para cada iteración un número racional (que denotaremos $[a_0, a_1, \cdots, a_n]$), que puede representarse mediante una fracción $\frac{p_n}{q_n}$ con $mcd(p_n, q_n) = 1$ y, además, se tiene lo siguiente

Lema 3.3.1 ([AB09]). *En las condiciones anteriores*

- $p_0 = a_0,\ q_0 = 1,\ p_1 = a_0a_1 + 1,\ q_0 = a_1$ *y además* $\forall n > 1,\ p_n = a_np_{n-1} + p_{n-2},\ q_n = a_nq_{n-1} + q_{n-2}$.
- $\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_nq_{n-1}}$.

Y además se cumple que

$$\left| \frac{p_n}{q_n} - \alpha \right| < \frac{1}{q_nq_{n+1}} \tag{3.3.4}$$

Lo que implica que p_n/q_n es el número racional más cercano a α cuyo denominador no excede q_n.

Demos ahora un algoritmo basado en este método que usaremos para la implementación del algoritmo de Shor.

Algoritmo 3 Algoritmo para hallar el periodo r basado en el método de las fracciones continuas y el lema 3.3.1.

```
1: procedure CalcularR(z entero, m: entero, n: entero.)
2:     [a_0, ..., a_k] ← representación en fracciones continuas de z/2^m.
3:     p_0, q_0, p_1, q_1 ← a_0, 1, 1 + a_0a_1, a_1
4:     n ← 1
5:     while q_n < n and n ≤ k do
6:         n ← n + 1
7:         p_n ← a_n p_{n-1} + p_{n-2}
8:         q_n ← a_n q_{n-1} + q_{n-2}
       return q_n
```

3.4. Algoritmo Explícito

Presentamos ahora una propuesta para un algoritmo cuántico de descomposición prima basado en la técnica que ya hemos propuesto. Se puede consultar el pseudocódigo en la figura para el algoritmo 4.

Nuestro algoritmo se basará principalmente en la recursividad para el manejo de los posibles errores que puedan darse durante la ejecución producto del hecho de que nuestro algoritmo es fundamentalmente probabilista. Para ello y dado que las situaciones desfavorables pueden detectarse usando un número de operaciones despreciable, en el momento que nuestro algoritmo detecte uno de estos casos, simplemente volverá a ejecutarse recursivamente, eligiendo otro número aleatorio para realizar la búsqueda del orden. Veremos en el apartado sobre implementación cuántas llamadas de recursividad realiza el algoritmo, pero confiamos en que, al ser la probabilidad de acierto como hemos visto suficientemente buena, serán pocas y por tanto no nos tendremos que preocupar en principio por los desbordamientos de pila.

Por otro lado cabe preguntarse en qué momento el algoritmo detectará que hemos alcanzado un factor primo y, por tanto, no debe seguir avanzando en recursividad. Resulta que, de hecho, hay muy buenos

algoritmos en tiempo polilogarítmico que realizan esta tarea. En nuestra implementación usaremos el *algoritmo de Miller-Rabin*[14] ([Mil76]), de naturaleza probabilista, que sabemos que devuelve la respuesta correcta sobre la primalidad de un número n en k iteraciones sucesivas con probabilidad de acierto $1 - \frac{1}{4^k}$. Sin embargo, sabemos que existe un algoritmo no probabilista, conocido como *Algoritmo AKS* ([AKS04]) que devuelve la primalidad de n de forma determinista en el mismo orden de complejidad, aunque su implementación es ligeramente más compleja y su eficiencia algo menor. Además, al ser el algoritmo de Shor probabilista y al tener el algoritmo de Miller-Rabin tan buena tasa de acierto, no notaremos una diferencia de fiabilidad significativa.

Algoritmo 4 Algoritmo para hallar la factorización prima basado en Shor

Entrada: Un entero n positivo a factorizar.
Salida: Con probabilidad cercana a 1, el conjunto de divisores primos de n.

```
1: procedure SHOR(n: entero)
2:     if esPrimo(n) then return {n}
3:     a ← entero (pseudo[15]-)aleatorio en el rango {2, ··· , n − 1}
4:     d ← mcd(a, n)
5:     if (d ≠ 1) then return Shor(n/d) ⋃ Shor(d)
6:     else r ←búsquedaOrden(a, n)
7:     if (r es impar) then return Shor(n)
8:     else
9:         if a^{r/2} ≢ −1 (mod n) then return Shor(n)
10:    d ← mcd(a^{r/2} + 1, n)
11:    return Shor(n/d) ⋃ Shor(d)
```

3.5. ¿El Fin de RSA? La Criptografía Postcuántica

Una pregunta que surge de manera muy natural al comprobar que en el marco de la computación cuántica la factorización prima se torna tan sencilla es: ¿Qué ocurre con los sistemas de criptografía basados en factorización?

Aunque en este trabajo solamente hemos probado que el algoritmo de descomposición prima puede ejecutarse en tiempo polilogarítmico necesitaríamos una cota más certera para establecer tiempos de ejecucuión concretos para debatir si podríamos romper claves RSA en tiempo aceptable. Tal cota se da en la publicación [BCDP96], donde se establece una aproximación de $72 \log^3 N$ operaciones necesarias para factorizar un entero N. Sin embargo, uno de los mayores problemas a día de hoy para realizar una factorización no es tanto el tiempo de ejecución sino el espacio necesario, que dada la reversibilidad de las operaciones cuánticas debe ser el mayor número de qubits en uso en cualquier momento del algoritmo. Se ha demostrado (ver [Bea02]) que el algoritmo de Shor se puede implementar eficientemente en memoria, haciendo uso de tan solo $2 \log N + 3$ qubits.

[14] La afirmación que hemos hecho sobre la eficiencia en tiempo del algoritmo no está demostrada teóricamente sino tan solo comprobada experimentalmente. La razón reside en que sería necesario un resultado increíblemente difícil de probar, conocido como la *hipótesis generalizada de Riemann*, que constituye de hecho uno de los problemas del Milenio del Instituo Clay. No obstante se vio en el artículo [DLP93] que el tiempo de ejecución experimental parece ser incluso mejor que el propuesto teóricamente.

[15] La elección podrá ser realmente aleatoria si esta parte del algoritmo se ejecuta sobre un ordenador cuántico (ejemplo 2.3.3). Si por el contrario solo ejecutamos la QFT de forma cuántica y esta parte se realiza sobre un computador clásico no probabilista nos deberemos conformar con un entero pseudo-aleatorio, que funcionará perfectamente para nuestros propósitos.

Así pues, una clave RSA de 4096 bits[16] necesitaría aproximadamente $72 \cdot 4096^3 \sim 4 \cdot 10^{12}$ operaciones cuánticas. Número que es ligeramente alto, pero aun así tremendamente bajo comparado con las aproximadamente 10^{41} operaciones necesarias para factorizarlo en un computador clásico usando el mejor algoritmo clásico conocido hasta la fecha (conocido como *GNFS*) con orden de ejecución temporal $L_N\left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right]$, lo que supone un factor de mejora de 10^{29}.

Por otro lado como hemos visto necesitaremos un máximo de $2 \cdot 4096 + 3 = 8195$ qubits. Este número queda lejos del máximo que hemos conseguido construir hasta la fecha y lejos incluso de la perspectiva para los próximos años. En la fecha en la que se escribe esta frase, el mayor computador que se ha conseguido construir consta de 51 qubits. Sin embargo, si tenemos esperanza en que se cumpla un equivalente a la Ley de Moore para computadores cuánticos, podemos esperar conseguir tal capacidad en aproximadamente diez años.

Aunque aquí solo hemos mencionado la aplicación a RSA, existen otros mecanismos de criptografía que también quedan amenazados. Esto es debido a que la búsqueda exhaustiva en un computador cuántico puede realizarse de forma más eficiente usando un algoritmo conocido como el *algoritmo de Grover* (ver [Gro96]) que reduce una búsqueda exhaustiva desde $O(N)$ a $O(\sqrt{N})$, lo cual es una mejora significativa aunque no tan drástica como la mejora exponencial del algoritmo de Shor. Un grupo de investigadores estudió las implicaciones de este algoritmo en el cifrado por bloque AES en [GLRS15]. En concreto en el artículo se demuestra que para la versión de 256 bloques AES-256 el número de qubits necesarios para la búsqueda a fuerza bruta de la solución es tan solo 6681 qubits.

Podría parecer por tanto que la seguridad está gravemente comprometida en su totalidad por este nuevo paradigma de computación. Nada más lejos. De hecho, Daniel J. Bernstein en su artículo [Ber11] realiza un análisis de qué tecnologías son vulnerables e indica que muchas de las que hoy en día utilizamos son perfectamente seguras. Al conjunto de técnicas seguras se le denomina criptografía post-cuántica. Por ejemplo, la autenticación ampliamente usada Kerberos es resistente a cualquier tipo de ataque por factorización. Incluso ha surgido un análogo a Diffie-Hellman resistente a los algoritmos cuánticos llamado *DIDH* cuyas siglas significan *supersingular isogeny Diffie-Hellman* el cual se expone en el artículo [JDF11].

3.6. Implementación del Algoritmo de Shor

...SECCIÓN EN PROGRESO...

Todo el software, realizado con el lenguaje de programación Julia, que aquí se comenta no se incluye en la memoria por ser excesivamente largo y no considerarse los detalles de vital importancia. A pesar de ello se puede consultar perfectamente, e incluso clonar el repositorio, desde el enlace `https://github.com/albgp/TFGQuant.git`.

[16] Elegimos tal tamaño pues las más utilizadas varían entre 1024 y 4096 bits en promedio. Realizaremos por tanto en análisis del caso más difícil.

CAPÍTULO 4

Factorización en Computación Cuántica Adiabática

...SECCIÓN EN PROGRESO...

4.1. Computación Adiabática en Resumen

(Hay más cosas en el apéndice)

En las secciones anteriores hemos presentado un modelo de computación cuántica en el que hemos construido los algoritmos mediante la aplicación sucesiva de operadores cuánticos hasta obtener el estado solución del problema que queríamos resolver. Presentamos en esta sección una perspectiva radicalmente diferente de computación cuántica aplicada al mismo problema: la factorización prima. Veamos en primer lugar ciertos requisitos técnicos que nos permitirán abordarla en profundidad.

La idea reside en el postulado II que hemos presentado en el apéndice A. En él se establece que un sistema cuántico en un estado $|\phi(t)\rangle$ en el instante t debe evolucionar siguiendo una ecuación que se conoce como la ecuación de Schrödinger, que se puede escribir en su forma diferencial como sigue

$$i\hbar\frac{d}{dt}|\phi(t)\rangle = \hat{H}(t)\,|\phi(t)\rangle \tag{4.1.1}$$

Donde $H(t)$ es, para cada t, un operador unitario que se conoce como el Hamiltoniano del sistema, que define la evolución. En el caso en el que el hamiltoniano es constante en el tiempo tenemos una ecuación diferencial lineal de primer orden cuya solución es

$$|\phi(t)\rangle = e^{-i\hbar t\hat{H}}\,|\phi(0)\rangle := U(t)\,|\phi(0)\rangle \tag{4.1.2}$$

donde definimos la exponencial de un operador A como

$$e^{A} = \sum_{k=0}^{\infty}\frac{1}{k!}A^{k} \tag{4.1.3}$$

siempre que esta suma tenga sentido.

Sin embargo, la solución explícita cuando el hamiltoniano no es constante no es obtenible en general, por lo que tendremos que hallarla por con métodos numéricos siempre que no sea muy ¿cómo se traduce

stiff?

El hamiltoniano para un instante t que hemos presentado puede presentar ciertos estados que consideraremos especiales, estos son los llamados *autoestados* $|\varepsilon_0(t)\rangle, |\varepsilon_1(t)\rangle, \cdots$ que cumplen que

$$\hat{H}(t)\,|\varepsilon_i(t)\rangle = \varepsilon_i(t)\,|\varepsilon_i(t)\rangle \tag{4.1.4}$$

es decir, cuando se aplica el hamiltoniano a cada uno de ellos se obtiene el mismo estado, salvo constante multiplicativa $\varepsilon_i(t)$. A este valor $\varepsilon_i(t)$ se le denomina la *autoenergía* asociada al autoestado $|\varepsilon_i(t)\rangle$. Supondremos sin pérdida de generalidad que las autoenergías están ordenadas $\varepsilon_0(t) < \varepsilon_1(t) < \cdots$. Bajo estos supuestos, al autoestado de mínima energía de un instante t cualquiera $|\varepsilon_0(t)\rangle$ lo denotaremos *estado base*. El conjunto de autoenergías $\varepsilon_0(t), \varepsilon_1(t), \cdots$ lo llamaremos el *espectro* del hamiltoniano $\hat{H}(t)$, a veces denotado como $\sigma(\hat{H}(t))$.

El estado base tiene una estrecha relación con el procedimiento de la computación adiabática dado que ella se basa en el siguiente teorema formulado por M. Born y V. Fock en 1928.

Teorema 4.1.1 (Teorema de la Evolución Adiabática [BF28])**.** *Un sistema físico permanece en su autoestado instantáneo si la perturbación que actúa sobre él es lo bastante lenta y hay un salto energético entre su valor propio y el resto del espectro del hamiltoniano.*

Lo reformularemos de acuerdo a la notación que hemos dado y restringiendo su dominio de actuación a solamente estados base como sigue

Teorema 4.1.2 (Reformulación del Teorema de la Evolución Adiabática)**.** *Un sistema físico cuyo estado en el instante t es $|\phi(t)\rangle$ que se encuentra en el instante $t = 0$ en un estado base $|\varepsilon_0(0)\rangle$ y tal que $\varepsilon_0(t) < \varepsilon_1(t)$ para todo $t \in [0, T]$ entonces, si T es un número real suficientemente grande, la evolución mediante la ecuación de Schrödinger, con un hamiltoniano tanto constante como dependiente del tiempo, deja al sistema en un estado base*[1] *en $t = T$.*

La computación adiabática puede ser usada para optimizar (minimizar) una función $P : \mathbb{Z} \to \mathbb{R}$ como sigue:

1. Inicializamos un sistema al estado base $|\varepsilon_0(0)\rangle$ de un hamiltoniano inicial $\hat{H}_0$ tal que $\varepsilon_0(0) < \varepsilon_1(0)$.
2. Diseñamos un hamiltoniano $\hat{H}_f$ cuyas autoenergías sean exactamente los valores de $P(x)$.
3. Definimos el hamiltoniano dependiente del tiempo $H(t) = \left(1 - \frac{t}{T}\right)\hat{H}_0 + \frac{t}{T}\hat{H}_f$ como la interpolación lineal de los dos hamiltonianos (inicial y final) con un T suficientemente grande para asegurar que se dan las condiciones del teorema 4.1.2.
4. Por el teorema 4.1.2, el estado final $|\phi(T)\rangle$ será un estado base del hamiltoniano $\hat{H}_f$, por lo que será el autoestado que minimiza la autoenergía del sistema. Dado que las autoenergías eran los valores de la función $P(x)$, el autoestado final tiene «encapsulado» en su energía el valor mínimo de la función.

Veamos en las secciones que siguen cómo usar este método para hallar factores no triviales de un entero N.

[1] En realidad, como vemos en el apéndice con más rigor, el estado en el que se encuentra el sistema no es un estado base sino un estado arbitrariamente cercano al estado base (ε-cercano en la norma ℓ_2), por lo que para no añadir complejidad supondremos que es un estado base, lo que valdrá plenamente para nuestros razonamientos.

4.2. Reducción de la Factorización a un Problema de Optimización

En agosto de 2018, Tien D. Kieu reformuló en [Kie18] el problema de la factorización prima como un problema de optimización de un polinomio diofántico. Su idea consistía en que, si consideramos el polinomio multivariable definido sobre $\mathbb{N} \times \mathbb{N}$

$$Q_N(x, y) \equiv N^2(N - xy)^2 + x(x - y)^2 \tag{4.2.1}$$

el mínimo se alcanzará precisamente cuando x, y sean divisores de N, por lo que optimizar el polinomio se puede ver como encontrar dos divisores (no necesariamente primos) de N. Probemos tal afirmación.

Lema 4.2.1. *La función $Q_N(x, y) : \mathbb{N}^2 \to \mathbb{Z}$ definida en 4.2.1 alcanza su mínimo global estricto cuando $xy = N$ y además x es el divisor más cercano inferiormente a $\sqrt{N}$.*

Demostración. Sea $xy = N$ entonces el primer término de 4.2.1 se anula y el segundo término es obviamente menor cuando $1 \leq x \leq \sqrt{N} \leq y$, puesto que el término está multiplicado por x. Bajo estas suposiciones (que sabemos que serán ciertas) podemos considerar el segundo término de la ecuación como un término en una sola variable usando la relación $y = N/x$ obteniendo así $x(x - N/x)^2$. Además podemos comprobar que tal término es decreciente[2] con x. Por ello podemos escribir

$$\begin{aligned} Q_N(x, y)|_{N=xy} = Q_N(x, N/x) &\leq \max_{1 \leq x \leq \sqrt{N}} x(x - N/x)^2 \\ &\leq x(x - N/x)^2|_{x=1} \\ &\leq (N - 1)^2 \end{aligned} \tag{4.2.2}$$

Supongamos en este punto que $xy \neq N$, entonces $(N - xy)^2 \geq 1$ y por tanto el primer término de 4.2.1 es mayor o igual que N^2. Ello implica que

$$Q_N(x, y)|_{xy \neq N} \geq N^2 + x(x - y)^2 \geq N^2 \tag{4.2.3}$$

Combinando las dos desigualdades obtenidas tenemos trivialmente que

$$Q_N(x, y)|_{N \neq xy} > Q_N(x, y)|_{N=xy} \tag{4.2.4}$$

Lo que completa la prueba. □

Observación 4.2.2. *Cualquier múltiplo ΩQ de la función Q del teorema anterior con Ω una constante estrictamente positiva alcanza el mínimo en el mismo punto (x, y) en el que lo alcanza Q.*

4.3. Elección de los hamiltonianos inicial y final

Tomamos n mínimo tal que $2^n \geq N + 1$, es decir, $n = \lceil \log_2 N + 1 \rceil$, para poder codificar todos los divisores de N en la superposición; por lo que el estado base será $|\varepsilon_0(0)\rangle = \left|\tilde{0}\right\rangle = \sum_{k=0}^{2^{2n}-1} |k\rangle$

Introducimos un hamiltoniano inicial H_0, definido en [vMV02] en el contexto de la resolución adiabática del problema de la 3-SAT que veremos que servirá perfectamente para nuestros propósitos.

[2] Se puede ver claramente comprobando que su derivada $3x^2 - \left(\frac{N}{x}\right)^2 - 2N$ es negativa para todo $x \in (0, \sqrt{N}]$

$$\hat{H}_0 = \sum_{k=0}^{2^{2n}-1} h(z) \left|\tilde{z}\right\rangle \left\langle\tilde{z}\right| \tag{4.3.1}$$

donde $h(0) = 0$, $h(x) \geq 1 \ \forall x \in \{1, 2, \cdots, 2^{2n} - 1\}$ y $\left|\tilde{z}\right\rangle = \mathbb{H}^{\otimes 2n} \left|z\right\rangle$.

Donde además usamos la notación $\mathbb{H}$ para la puerta de Hadamard, a pesar de la notación H que se viene usando durante el texto, pues sería contraproducente usar la mismta tipografía para el hamiltoniano y la puerta de Hadamard.

Es sencillo comprobar, por la definición de la función h, que el estado base de H_0 es $\left|\tilde{0}\right\rangle = \mathbb{H}^{\otimes 2n} \left|0\right\rangle$.

Definimos el hamiltoniano del problema, siguendo la estrategia que hemos expuesto en la sección 4.1 y la reformulación como optimización de Kieu [Kie18] como el siguiente opeardor

$$\hat{H}_f = \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} Q_N(i,j) \left|i,j\right\rangle \left\langle i,j\right| \tag{4.3.2}$$

donde definimos $\left|i,j\right\rangle = \left|i2^n + j\right\rangle$, por razones que quedarán claras en breve. Es sencillo ver que, aplicando la ortonormalidad, que cualquier estado base es un autoestado del hamiltoniano con su autoenergía dada por la función Q

$$\hat{H}_f \left|x,y\right\rangle = \sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} Q_N(i,j) \left|i,j\right\rangle \left\langle i,j|x,y\right\rangle = Q_N(x,y) \left|x,y\right\rangle \tag{4.3.3}$$

E interpolando los dos hamiltonianos en el intervalo de tiempo $[0, T]$ obtenemos

$$\hat{H}(t) = \left(1 - \frac{t}{T}\right)\hat{H}_0 + \frac{t}{T}\hat{H}_f \tag{4.3.4}$$

que será el hamiltoniano dependiente del tiempo que usaremos para nuestra evolución.

4.4. Resultados experimentales

Describamos más en detalle el proceso y realicemos una simulación del mismo: dado un entero N a factorizar deberemos elegir un espacio de estados suficientemente grande como para poder codificar una superposición de pares (i, j) que representen divisores de N, entre los que se puede incluir el propio N, por lo que elegiremos la dimensión para cada uno de los valores del par como $n = \lceil \log_2 N + 1 \rceil$ y por tanto el espacio total tendrá una dimensión de 2^{2n}. A partir de este momento trabajaremos exclusivamente con la representación compleja (en $\mathbb{C}^{2n}$) del espacio de qubits, por lo que escribiremos de ahora en adelante v_t para el estado del sistema en el instante t.

Reescribiendo la ecuación 4.1.1 con la notación propuesta y suponiendo que $\hbar = 1$ (a lo que se le suele llamar una elección de coordenadas *naturales*), llegamos a que

$$\frac{dv_t}{dt} = -iH(t)v_t \tag{4.4.1}$$

¿Cómo calculamos el término $\hat{H}(t) \left|\phi(t)\right\rangle$? Por la ecuación 4.3.4 de interpolación bastará calcular la acción de $\hat{H}_0$ y $\hat{H}_f$ sobre v_t que será como sigue[3].

Para el primero de ellos, $\hat{H}_0 v_t$, procedemos de la siguiente manera

Con la fórmula para $\hat{H}_0$ basta ver que

$$\hat{H}_0 \left|\phi\right\rangle = \sum_{k=0}^{2^{2n}-1} h(z) \left|\tilde{z}\right\rangle \left\langle\tilde{z}|\phi\right\rangle = \sum_{k=0}^{2^{2n}-1} h(z) \left\langle z\right| \mathbb{H}^{2n} \left|\phi\right\rangle \mathbb{H}^{2n} \left|z\right\rangle \tag{4.4.2}$$

con lo que se justifica el siguiente cálculo.

1. Definimos un vector complejo r de dimensión $2n$ con todas sus componentes inicializadas al valor $0 + 0i$.
2. Para cada entero i en el rango $\{0, 1, \cdots, 2^{2n} - 1\}$
   a) Definimos e_i como el vector en $\mathbb{C}^{2n}$ nulo en todas sus coordenadas excepto en la coordenada i-ésima en la que toma el valor $1 + 0i$.
   b) Definimos $w_i = \mathbb{H}^{\otimes 2n} e_i$
   c) Hacemos $r = r + h(i)\Big(w_i \cdot v_t\Big) w_i$.
3. Devolvemos $r = \hat{H}_0 v_t$.

Veamos ahora el cálculo de $\hat{H}_f v_t$. Para ello realizaremos la descomposición de una base de nuestro espacio $\mathcal{H}^{\otimes 2n}$ como producto tensorial explícito de $\mathcal{H}^{\otimes n} \otimes \mathcal{H}^{\otimes n}$. De esta forma, hacemos corresponder un elemento de la base $|z\rangle$ con un elemento $|i\rangle\,|j\rangle$ donde i y j serán los elementos en el rango $\{0, \cdots, 2^n - 1\}$ que representarán los divisores propuestos. Elegimos la relación (que resulta ser arbitraria) $z \leftrightarrow i2^n + j$.

1. Creamos r como una copia de v_t.
2. Para cada i en $\{0, 1, \cdots, 2^n - 1\}$,
   a) Para cada j en $\{0, 1, \cdots, 2^n - 1\}$,
      1) Definimos index como $i2^n + j$.
      2) Multiplicamos $r[index]$ por $Q(i, j)$.
3. Devolvemos $r = \hat{H}_f v_t$.

Una vez ya hemos establecido cómo calcular $\hat{H}_0 v_t$ y $\hat{H}_f v_t$, usando la interpolación de 4.3.4 tendremos que

$$\hat{H}(t) v_t = \Big(1 - \frac{t}{T}\Big) \hat{H}_0 v_t + \frac{t}{T} \hat{H}_f v_t \tag{4.4.3}$$

Aunque realizaremos un único cambio más: tal y como hemos visto en la ecuación 4.1.2, la evolución del sistema toma valores exponenciales cuando el hamiltoniano es constante, por lo que podemos esperar un resultado similar si el hamiltoniano es variable y creciente, como es el caso; por lo que si no somos cuidadosos podríamos tener errores de rango numérico, pues usaremos números complejos de 128 bits. Para evitarlo introducimos lo que llamaremos un *factor de regularización*, para que el vector $H_f v_t$ no tome

[3] El cálculo que se va a presentar en esta sección no está optimizado en su totalidad dado que hemos preferido, por simplicidad, definir un cálculo que pudiese seguirse de una forma directa a partir de la definición de los hamiltonianos. Sería interesante, por tanto, estudiar en profundidad cómo sería posible realizar los cálculos de forma más eficiente, aunque esto quizá solo sería importante en un factor constante, dado que es inevitable que la dimensionalidad del espacio de estados crezca exponencialmente.

valores excesivamente grandes, lo que ocurriría dado que los valores de la función Q son relativamente grandes cuando los exponenciamos. Dado que los dos hamiltonianos no se diferencian más que en una constante multiplicativa es de esperar que esto no introduzca ningún cambio en la solución, pues las autoenergías cambiarán simplemente en un factor de escala, por lo que el estado base se mantendrá inalterado.

Obtenemos así la ecuación

$$\hat{H}(t)v_t = \Big(1 - \frac{t}{T}\Big)\hat{H}_0 v_t + \frac{t}{T}\Big(\frac{\hat{H}_f v_t}{\Omega}\Big) \tag{4.4.4}$$

Por tanto deberemos resolver numéricamente la ecuación siguiente, para un valor de T suficientemente grande, que corresponde a un sistema lineal de ecuaciones diferenciales de primer orden.

$$\frac{dv_t}{dt} = -i\left(\Big(1 - \frac{t}{T}\Big)\hat{H}_0 v_t + \frac{t}{T}\Big(\frac{\hat{H}_f v_t}{\Omega}\Big)\right) \tag{4.4.5}$$

Para resolver este sistema de ecuaciones diferenciales usaremos cálculo numérico en Python, concretamente usaremos la librería *scipy* y *numpy* junto con un *wrapper* [Wec14] creado por Warren Weckesser para adaptar la función de integración diferencial *odeint* de la librería *scipy* que funciona con sistemas de ecuaciones diferenciales reales a una función compleja, separando las partes real e imaginaria e integrando simultáneamente.

Dado el estado final del sistema, v_T, sabemos que este estado será ε-cercano al estado base, que como hemos visto encapsula la solución al problema de la factorización, por lo que el estado será una superposición donde el coeficiente del estado solución será grande (en norma) en comparación con el resto. Así pues, para no lidiar con estos pequeños errores en la evolución tomaremos como resultado el valor

$$k = \underset{i \in \{0,1,\cdots,2^{2n}\}}{\arg\max} \{v_T[i]\} \tag{4.4.6}$$

Por lo que N será

$$N = (\underbrace{k \ \mathbf{div}\ 2^n}_{i}) \cdot (\underbrace{k \ \mathbf{mod}\ 2^n}_{j}) \tag{4.4.7}$$

y, de hecho, sabremos que $N \neq 1$ es primo si y solo si $i = 1$ y $j = N$.

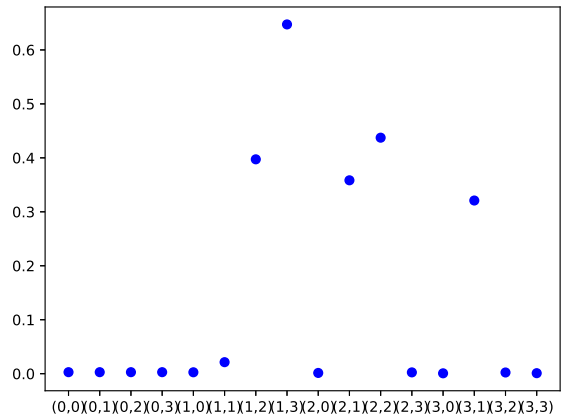
El código, de nuevo, se puede encontrar en el repositorio para el proyecto `https://github.com/albgp/TFGQuant.git`. Realizaremos a continuación un análisis de los resultados obtenidos, que se pueden visualizar en la figura 4.4.1.

(...)

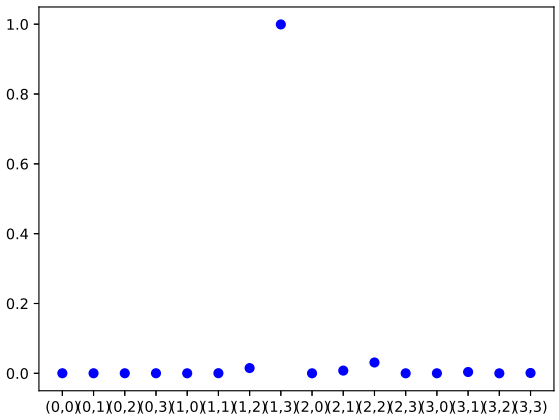
4.5. Simulando la Evolución Adiabática con Circuitos

$$U'_j(T) = e^{-i(T/r)\hat{H}'_r} \cdots e^{-i(T/r)\hat{H}'_1} \tag{4.5.1}$$

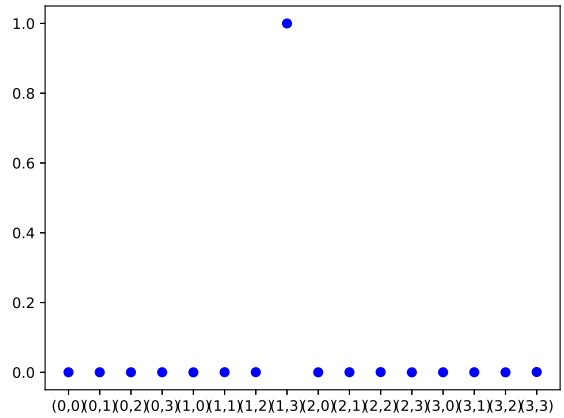
$$U'_j := e^{-iT/r(1-j/r)\hat{H}_0 - iT/r\, j/r \hat{H}_f} \tag{4.5.2}$$



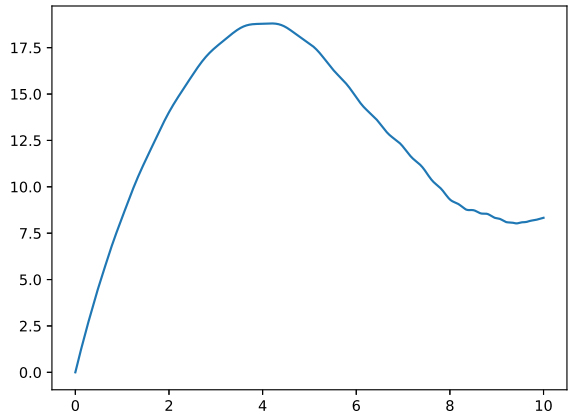
(a) $T = 10$



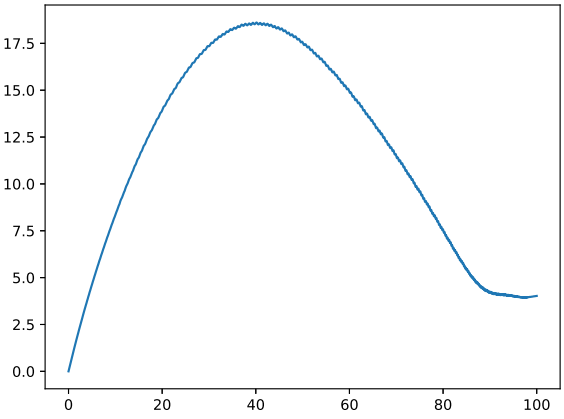
(b) $T = 100$



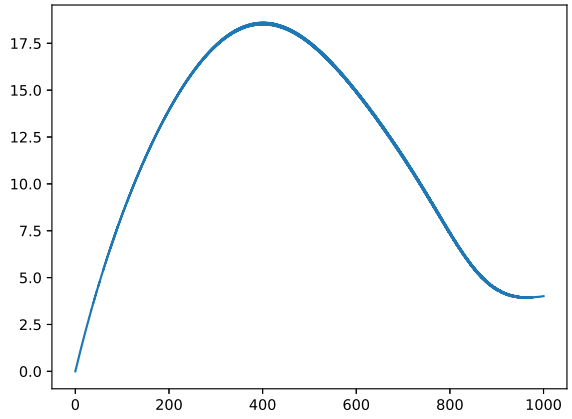
(c) $T = 1000$



(d) Evolución de la energía para $T = 10$



(e) Evolución de la energía para $T = 100$



(f) Evolución de la energía para $T = 1\,000$

Figura 4.4.1: Estado de superposición para cada qubit solución con cada índice k numerado tal que $k \sim (k \textbf{ div } 2^n, k \textbf{ mod } 2^n)$ y valor de la energía para distintos rangos de integración en el caso $N = 3$, $\Omega = 10^{-3}$.

Teorema 4.5.1 (Teorema de Campbell-Baker-Hausdorff. [Bha13]). *Sean A y B matrices unitarias, entonces*[4]

$$\left\|e^{A+B} - e^A e^B\right\|_2 \in O(\|AB\|_2) \tag{4.5.3}$$

$$U_j'' = e^{-iT/r(1-j/r)\hat{H}_0} e^{-iT/r\, j/r\hat{H}_f} \tag{4.5.5}$$

$$H_j'' = \mathbb{H}^{\otimes 2n} F_{0,j} \mathbb{H}^{\otimes 2n} F_{f,j} \tag{4.5.6}$$

donde

$$\begin{aligned} F_{0,j}\,|z\rangle &= e^{-iT/r(1-j/r)h(z)}\,|z\rangle \\ F_{f,j}\,|z\rangle &= e^{-iT/r(j/r)f(z)}\,|z\rangle \end{aligned} \tag{4.5.7}$$

Teorema 4.5.2. *Sean $\hat{H}_0$ y $\hat{H}_f$ los hamiltonianos iniciales y finales para el cómputo adiabático y $f \in O(n^d)$, entonces la transformación unitaria $U(T)$ inducida por el hamiltoniano $\hat{H}(s) = \left(1 - \frac{t}{T}\right)\hat{H}_0 + \frac{t}{T}\hat{H}_f$ dependiente del tiempo puede aproximarse mediante r puertas cuánticas consecutivas $U_1'', \cdots, U_r''$ con $r \in O(T^2 n^{d+1})$. Además cada U_j'' tiene la forma $\mathbb{H}^{\otimes 2n} F_{0,j} \mathbb{H}^{\otimes 2n} F_{f,j}$ y puede implementarse eficientemente en tiempo poly(nT).*

4.6. Relacionando Ambos Métodos

4.6.1. Caracterización de la Complejidad

[4] Se sigue de la fórmula de Campbell-Baker-Hausdorff en la que, usando el conmutador $[A, B] = AB - BA$, se tiene

$$e^A e^B = e^{A+B+[A,B]/2+[X,[X,Y]]/12+\cdots} \tag{4.5.4}$$

CAPÍTULO 5

Conclusiones y Vías Futuras.

Apéndices

APÉNDICE A

Postulados de la Mecánica Cuántica[1]

Presentamos en esta sección una colección de postulados básicos de la mecánica cuántica. Dependiendo de la fuente que se consulte, estos postulados pueden variar desde cuatro hasta siete o más postulados. La formulación axiomática de la teoría fue formalizada de forma temprana por el matemático John Von Neuman [VN18], aunque sus postulados incluían ciertas referencias a la dinámica de los sistemas que no será relevante en este trabajo, por lo que nos limitaremos a tres de los cuatro postulados más fundamentales para la teoría de la computación expuestos en [NC02] junto a una selección de tres más extraídos de [Jaf96].

Postulado I (**Principio de superposición**). *Cualquier sistema físico se puede considerar como un vector en un espacio de Hilbert $\mathcal{H}$, el cual denotamos como* espacio de estados*. El sistema queda descrito en su totalidad por este vector, que es unitario en el espacio de estados.*

Algunos textos no incluyen en su definición de estado la condición de que sea unitario, a cambio de establecer una relación de equivalencia $\sim$ bajo la cual dos estados son equivalentes si uno es múltiplo del otro por un escalar, y trabajan sobre el espacio cociente $\mathcal{H}/_{\sim}$.

Postulado II (**Evolución temportal determinista**). *La evolución de un sistema cuántico cerrado viene determinada por un operador lineal unitario. Usando el término «hamiltoniano» y la notación $\hat{H}$ para tal operador y la notación $|\phi(t)\rangle$ para el estado del sistema en el instante t, entonces la evolución temporal viene dada por la ecuación diferencial de Schrödinger*

$$i\hbar\frac{\partial}{\partial t}|\phi(t)\rangle = \hat{H}|\phi(t)\rangle \tag{A.0.1}$$

donde $\hbar$ es la conocida como constante de Planck normalizada $\hbar = \frac{h}{2\pi}$, cuyo valor es aproximadamente $1{,}054571 \cdot 10^{-34}$ *julios por segundo. Si el hamiltoniano no es constante en el tiempo y queremos enfatizarlo podremos escribir*

$$i\hbar\frac{\partial}{\partial t}|\phi(t)\rangle = \hat{H}(t)|\phi(t)\rangle \tag{A.0.2}$$

Observación A.0.1. *El lector puede haberse dado cuenta de que usamos la notación $\partial/\partial t$ para la derivada parcial en vez de la clásica d/dt para funciones de una sola variable. Esto simplemente lo hacemos por una consistencia notacional e histórica con la teoría más general, pues en la teoría cuántica más allá de la rama computacional un estado $|\phi(t)\rangle$ hace referencia a una entidad más general: una onda. Por esto podríamos ver el estado $|\phi(t)\rangle$ como una función $\phi(t, \vec{r})$ que asocia a cada punto $\vec{r}$ del espacio y cada instante t, un valor complejo, lo que justifica que usemos la notación multivariable y la derivada parcial. Sin embargo, como esta interpretación ondulatoria de los estados cuánticos no es necesaria para nuestro trabajo, usaremos en lo que respecta a las secciones en las que usemos la evolución de Schrödinger la notación d/dt.*

[1] Recomendamos leer esta sección una vez se esté familiarizado con la introducción del capítulo 2, pues en el caso contrario, la cantidad de información que aquí se presenta puede confundir al lector dado que usamos notación y conceptos que se introducen en dicho capítulo.

Ejemplo A.0.2. *El hamiltoniano para una partícula cuántica libre de masa m no sujeta a fuerzas externas moviéndose en una dimensión viene definido por*

$$\hat{H} = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} \tag{A.0.3}$$

y si suponemos que la partícula está sujeta al campo potencial de una fuerza conservativa $V(x)$ el hamiltoniano será

$$\hat{H} = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} + V(x) \tag{A.0.4}$$

que es la forma más común en la que podemos encontrarlo en la literatura.

Postulado III (**Sistemas compuestos**)**.** *El espacio de estados de un sistema compuesto es el producto tensorial de los espacios correspondientes a cada uno de los estados componentes del sistema.*

Postulado IV (**Caracterización de las mediciones**)**.** *Los únicos resultados posibles de una magnitud A (que llamaremos «observable») de un sistema cuántico son los autovalores del operador asociado $\hat{A}$.*

Podemos ver un ejemplo de este postulado como sigue: para una partícula libre podemos considerar su energía cinética K. Sea $\hat{K}$ el operador que dado un estado cuántico para la partícula encapsula su energía cinética, tal operador viene dado por

$$\hat{K} = -\frac{\hbar^2}{2m}\frac{\partial^2}{\partial x^2} \tag{A.0.5}$$

que, como es sencillo comprobar, es lineal y unitario.

Postulado V (**Caracterización probabilista de la medición**)**.** *Cuando se realiza una medida de un observable A sobre un estado $|\phi\rangle$, la probabilidad de obtener un autovalor a_n viene dada por la magnitud $|\langle a_n|\phi\rangle|^2$.*

Siguiendo el ejemplo anterior, si el operador $\hat{K}$ tiene autoestados $\{|k_i\rangle\}_{i\in I}$ con autovalores $\{k_i\}_{i\in I}$, la partícula en el estado $|\phi\rangle$ solo podrá tomar valores de energía cinética $\{k_i\}_{i\in I}$. Cada uno de ellos con probabilidad $|\langle k_i|\phi\rangle|^2$.

Postulado VI (**Reducción de un estado cuántico**)**.** *Si la medición de un observable A ha devuelto un autovalor a_n, el estado del sistema tras la medición será $|a_n\rangle$.*

Y si al medir la energía cinética de la partícula hemos obtenido un autovalor para la energía cinética k_i entonces el estado de la partícula será $|k_i\rangle$.

APÉNDICE B

Aspectos de la Computación Cuántica

B.1. Circuitos Universales

Tal y como en computación clásica las puertas NAND proporcionan una puerta universal que basta para construir cualquier circuito booleano (se puede demostrar que cualquier otra puerta lógica booleana se puede construir con un número finito de puertas NAND), en computación cuántica ocurre algo similar. Ya en la década de los años 90 se comenzó a estudiar [BBC$^+$95] qué conjuntos de puertas eran suficientes para construir cualquier circuito cuántico. De hecho se puede demostrar que hay un gran número de bases universales, algunas de ellas se muestran en [BB02], nosotros aquí daremos un conjunto que consideramos el más importante pues está formado por tres (veremos posteriormente que tan solo dos) puertas cuánticas extremadamente comunes.

Definición B.1.1 (Conjunto universal)**.** *Un conjunto finito de puertas cuánticas se dice universal si cualquier operador unitario puede aproximarse con precisión arbitraria por un circuito cuántico finito que solamente contiene puertas del conjunto.*

La razón de que se defina la aproximación con un error arbitrario es que la cantidad de posibles puertas cuánticas unitarias es no numerable y la cantidad de circuitos finitos usando una puertas de un conjunto finito es numerable, así pues en general no podremos aproximar excepto por un error arbitrario[1].

Para cuantificar el error aquí contemplado solamente se requiere una norma definida en el espacio de las matrices complejas que denotaremos $\mathcal{M}_{N\times N}(\mathbb{C})$, sin embargo la norma que definamos es irrelevante dado que en un espacio de dimensión finita todas las normas son equivalentes ([Kre78]), y por tanto no difieren en más de una constante multiplicativa estrictamente positiva. Usando la norma infinito $\|\cdot\|_\infty$ componente a componente, o como es más conocida, la norma *entrywise*, que consiste en identificar $\mathcal{M}_{N\times N}(\mathbb{C})$ con $\mathbb{C}^{N^2}$ podemos escribir el siguiente teorema, publicado por primera vez en [Deu89].

[1]Por esta misma razón ciertos textos como [Tus04] distinguen entre *conjuntos universale*s, los cuales podrían aproximar exactamente cualquier puerta cuántica pero que, necesariamente, serían infinitos y los *conjuntos aproximadamente universales* que corresponderían a la definición que aquí se ha realizado.

Teorema B.1.2 ($\{H, R_s, CCNOT\}$ es universal.)**.** *Para cada $D \geq 3$ y $\varepsilon > 0$ existe un $l \geq (D \log \frac{1}{\varepsilon})^3$ tal que se cumple lo siguiente:*

Cada matriz unitaria $U \in \mathcal{M}_{D\times D}(\mathbb{C})$ puede ser aproximada por un producto de matrices unitarias $U_1, \cdots, U_l$ de forma que si (i, j) son números menores o iguales que D se satisface

$$\left| U_{i,j} - (U_l \cdots U_1)_{i,j} \right| < \varepsilon \tag{B.1.1}$$

y cada U_r corresponde a aplicar la puerta Hadamard H, la puerta Toffoli o la puerta de desplazamiento de fase en, como máximo, tres qubits.

De hecho, tal y como se demostró en el artículo [Shi02] y en [Aha03], las puertas de Hadamard y Toffoli bastan. Esto es debido a la mencionada observación 2.1.4 por la cual podemos despreciar los desplazamientos de fase compleja común a los coeficientes de una superposición.

Definición B.1.3. *Se dice que un circuito C tiene tamaño n con respecto a un conjunto $\mathcal{U}$ de puertas universales si n puertas cuánticas de $\mathcal{U}$ son necesarias para implementar el circuito.*

B.2. Principio de No Clonación

Vemos en este punto una de las particularidades más llamativas e importantes de la computación cuántica: **la información no se puede duplicar**. El teorema que mostramos a continuación, universalmente cierto, implica la imposibilidad de clonar un estado cualquiera en un registro arbitrario. Este hecho es importante pues dado que se pudiese clonar un estado un número arbitrario de veces podríamos, con medios técnicos ilimitados, obtener una precisión arbitraria de un estado cuántico (excepto, por la observación 2.1.4, desplazamientos de fase comunes) simplemente clonando el estado y realizando mediciones. De esta forma, podríamos establecer un muestreo probabilístico de los valores obtenidos en las mediciones y obtener de forma arbitrariamente precisa el estado original.

Teorema B.2.1 (Teorema de no clonación [Wha05])**.** *No existe ningún operador unitario U en un espacio producto $H \times H$ de un espacio de Hilbert H tal que para un estado normalizado cualquiera $|\phi\rangle$ en H se cumpla que*

$$U(|\phi\rangle |0\rangle) = e^{i\alpha(\phi,0)} |\phi\rangle |\phi\rangle \tag{B.2.1}$$

Demostración. Procedemos por reducción al absurdo. Consideremos que existe una puerta U como la mencionada, entonces se tiene que

$$\begin{aligned} \langle\phi|\psi\rangle \langle 0|0\rangle &= \langle\phi| \langle 0|\psi\rangle |0\rangle = \langle\phi| \langle 0| U^\dagger U |\psi\rangle |0\rangle \\ &= e^{-i(\alpha(\phi,0)-\alpha(\psi,0))} \langle\phi| \langle\phi| \operatorname{Id} |\psi\rangle |\psi\rangle \\ &= e^{-i(\alpha(\phi,0)-\alpha(\psi,0))} \langle\phi|\psi\rangle^2 \end{aligned} \tag{B.2.2}$$

Como $|0\rangle$ es un estado normalizado, $\langle 0|0\rangle = 1$ y por tanto $|\langle\phi|\psi\rangle| = |\langle\phi|\psi\rangle|^2$ (pues $|e^{-i(\alpha(\phi,0)-\alpha(\psi,0))}| = 1$). Esto implica que $|\langle\phi|\psi\rangle| = 0$ o bien $|\langle\phi|\psi\rangle| = 1$. Así, la desigualdad de Cauchy–Bunyakovsky–Schwarz implica que $\phi = e^{i\beta}\psi$ o bien que ϕ y ψ son ortogonales. Lo que, obviamente, no se da para cualquier $|\phi\rangle$ y $|\psi\rangle$ arbitrario, por lo que **un operador unitario U no puede clonar de forma general un estado cuántico**. □

Nota B.2.2. *Una consecuencia interesante de la demostración anterior es que un computador cuántico **sí** puede clonar de forma general un registro clásico. Es decir si tenemos un estado $|i\rangle$ con $i \in 0, 1$, se puede realizar sin ningún tipo de problema la operación cuántica $|i\rangle |0\rangle \to |i\rangle |i\rangle$. De hecho usaremos este tipo de operaciones más adelante en este trabajo.*

Podemos mencionar que existe un análogo inverso al Teorema de la No Clonación llamado el Teorema de No Borrado[2] que se puede enunciar como sigue

[2] No deleting theorem.

Nota B.2.3 (Teorema de No Borrado, [KB00])**.** *No existe ningún operador cuántico unitario U tal que, en general, se tenga que*

$$U(|\phi\rangle\,|\phi\rangle\,|A\rangle) = |\phi\rangle\,|0\rangle\,|A'\rangle \tag{B.2.3}$$

B.3. Teleportación Cuántica

Hay una inconsistencia narrativa en esta sección? Importa?

Veamos en este punto, y usando como medio una situación hipotética, cómo podremos, en condiciones especiales, transmitir un qubit cuántico usando solamente una pequeña cantidad de información clásica.

Supongamos que dos astrounautas llamadas, sin mucha originalidad, Alicia y Belén se encuentran en puntos distintos del sistema solar. Una de ellas, digamos que Alicia, quiere enviar la información del estado de un qubit que ella tiene en posesión a Belén, pero con la restricción de que su agencia espacial solo permite el envío de información clásica, pues los sistemas de comunicación cuántica no están todavía suficientemente desarrollados. Lo primero que Alicia podría pensar es en intentar mandar la información del estado completamente de forma clásica pero en este punto se encuentra dos problemas fundamentales:

- Alicia no puede saber en qué estado se encuentra el qubit dado que, como hemos visto, solo puede efectuar una única medición y no puede acceder al contenido de la superposición del qubit.
- Si pudiese, la situación no sería ciertamente mejor. Pues tendría que enviar a Belén una cantidad *infinita* de información para poder transmitir un estado en un rango continuo con total precisión.

En este punto Alicia recuerda que en sus años de formación en La Tierra, ellas crearon un par EPR $|\mathbf{\Phi}^+\rangle$, quedándose cada una con uno de los qubits del par. Esperando que Belén aún tenga el suyo consigo, Alicia idea una forma de transmitirle información.

Imaginemos que el qubit que Alicia quiere transmitir es $|\phi\rangle$. La idea será la siguiente: Alicia interactuará con su qubit del par EPR común mediante un circuito cuántico que se puede visualizar en la figura B.3.1. La medición tras la aplicación del circuito devolverá a Alicia un valor en $\{00, 01, 10, 11\}$. La principal sorpresa será que Belén, usando simplemente este valor medido (2 bits) puede recuperar completamente el estado $|\phi\rangle$.[3]

Supongamos que queremos enviar (teleportar) el qubit en el estado arbitrario $|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. Si suponemos que los tres qubits forman un registro (Alicia obviamente no podrá interactuar con el qubit del par EPR de Belén, pero conceptualmente nada nos impide considerar el qubit de Belén como parte del sistema, siempre que no realicemos ninguna operación sobre él) y si llamamos $|\varphi_0\rangle = |\varphi\rangle\,|\mathbf{\Phi}^+\rangle$ al registro inicial, usando la definición explícita que conocemos del par EPR obtenemos

$$|\varphi_0\rangle = \frac{1}{\sqrt{2}}\Big(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)\Big) \tag{B.3.1}$$

Cuando Alicia aplica la puerta CNOT sobre sus dos qubits como se aprecia en la figura B.3.1 el estado cambia a

$$|\varphi_1\rangle = \frac{1}{\sqrt{2}}\Big(\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)\Big) \tag{B.3.2}$$

Si aplicamos en este punto la puerta de Hadamard únicamente al primer qubit podemos obtener el estado

$$|\varphi_2\rangle = \frac{1}{2}\Big(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\Big) \tag{B.3.3}$$

Además, reagrupando términos, podemos ver el estado anterior fácilmente como

[3] Este hecho no contradice el principio de no clonación que hemos mostrado, puesto que en ningún momento se clona información. Debido a que el qubit original se destruye al medirlo, y esto ocurre antes de que el nuevo qubit se genere en la estación espacial de Belén, en ningún momento existen dos copias idénticas del estado $|\varphi\rangle$ simultáneas.

$$|\varphi_2\rangle = \frac{1}{2}\Big(|00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |00\rangle (\alpha |1\rangle - \beta |0\rangle)\Big) \tag{B.3.4}$$

Escribiendo el estado de tal forma podemos ver que si Alicia mide sus dos qubits y obtiene un valor de $\{00, 01, 10, 11\}$ concreto entonces el estado del qubit de Belén queda unívocamente definido. Por ejemplo, si Alicia obtiene el valor 01 al medir el qubit entonces por la ecuación B.3.4 el valor del qubit de Belén debe ser $\alpha |1\rangle + \beta |0\rangle$. Así pues, Belén podría obtener el qubit original $|\varphi\rangle$ simplemente aplicando un operador a su registro. Por tanto toda la información que necesitamos transferir es 2 bits para transmitir un valor teóricamente infinito de información.[4]

Supongamos que $|\theta\rangle$ es el estado del qubit de Belén tras la ejecución del circuito de Alicia y M_1 y M_2 los valores medidos y enviados a Belén, entonces el qubit original $|\varphi\rangle$ viene dado por

$$|\varphi\rangle = \begin{cases} |\theta\rangle & \text{si } M_1 = 0,\ M_2 = 0 \\ X|\theta\rangle & \text{si } M_1 = 0,\ M_2 = 1 \\ Z|\theta\rangle & \text{si } M_1 = 1,\ M_2 = 0 \\ ZX|\theta\rangle & \text{si } M_1 = 1,\ M_2 = 1 \end{cases} \tag{B.3.5}$$

Lo que podemos escribir más compactamente usando que la potencia nula de una matriz es la identidad como

$$|\varphi\rangle = Z^{M_1} X^{M_2} |\theta\rangle \tag{B.3.6}$$

Este mecanismo de codificación del estado completo de un qubit completo en tan solo dos bits clásicos se conoce comúnmente como *codificación superdensa* o, en inglés, *superdense coding*. Aunque esta particularidad cuántica se conocía desde 1935, la comunidad científica era escéptica al hecho de que realmente fuese posible que un cambio en un sistema cuántico pudiese tener efectos instantáneos en otro independientemente de la distancia que los separase pues esto parecía violar las leyes de causalidad de la Relatividad General de Einstein transmitiendo información más rápido que la propia luz, lo cual el propio Einstein denominó como la «acción fantasmal a distancia»[5] en un sentido claramente peyorativo, y dicha situación pasó a conocerse como la Paradoja Einstein-Podolsky-Rosen[6]. Análisis rigurosos posteriores propusieron que en realidad no había una violación del postulado de localidad de la Relatividad dado que se necesitaba el envío de los dos bits de forma clásica, de hecho, esto pasó a conocerse como el Teorema de la No Comunicación[7] ([PT04], sección 2.E.). Fue entonces, en 1993 cuando en [BBC$^+$93] se propuso la idea que hemos mencionado para la codificación superdensa abriendo una puerta a las comprobaciones experimentales de esta acción a distancia.

En 1998, investigadores del Caltech junto a institutos europeos consiguieron teleportar el primer estado de un fotón constituyendo así la teleportación como una realidad física. Durante todos los años siguientes se realizaron mayores experimentos, por ejemplo, se consiguió realizar una teleportación instantánea a 97km de distancia ([YRL$^+$12]) incluso teleportación mediante fibra óptica a 25km de distancia ([BCT$^+$14]). El récord a día de hoy lo ostenta un grupo de científicos chinos de diferentes universidades que consiguió teleportar en [RXY$^+$17] el estado de un fotón a 1400km de distancia, desde el Tibet hasta un satélite en órbita.

[4] Esta afirmación requeriría un estudio mucho más detallado sobre el significado del término «información». Si asumimos la definición clásica de la información como disminución de la incertidumbre, habría que preguntarse entonces cuánta incertidumbre es capaz de producir un qubit asumiendo que tenemos restricciones de extracción de la información por el colapso por medición. Dejamos tal tema de estudio a los teóricos de la información cuántica.

[5] Spooky action at a distance.

[6] Abreviadamente «Paradoja EPR»

[7] No-communication Theorem.

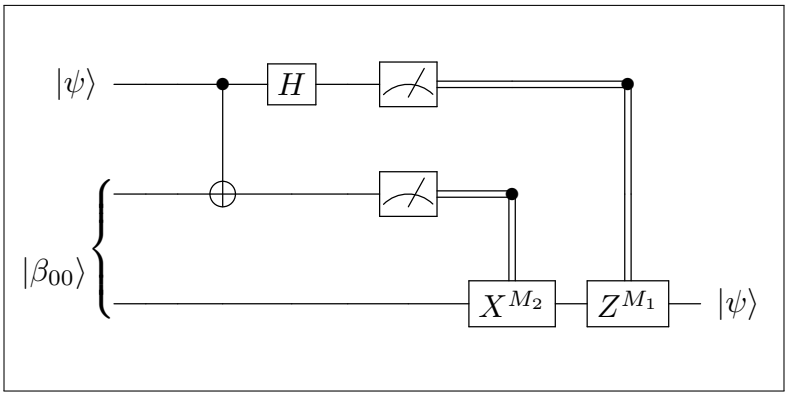


Figura B.3.1: Circuito cuántico para la realización de la teleportación.

APÉNDICE C

Resultados de Aritmética Elemental

Definición C.0.1 (Grupo)**.** *Un* ***grupo*** $(G, \cdot)$ *es un conjunto* G *junto a una operación interna* $(\cdot) : G \times G \to G$ *asociativa, con neutro y con simétrico para cada elemento.*

Definición C.0.2 (Subgrupo)**.** *Un grupo* $(H, \cdot_H)$ *se dice un* ***subgrupo*** *de un grupo* $(G, \cdot)$ *si* $H \subseteq G$ *y* $\cdot_H = \cdot|_H$*, es decir,* $\cdot_H$ *es la operación heredada de* G *aplicada sobre el subconjunto* H*.*

Definición C.0.3. *Denotaremos como* $\mathbb{Z}_m$ *al conjunto de números enteros* $1 \leq i \leq m$*. Este conjunto será un grupo* $(\mathbb{Z}_m, +)$ *junto la operación* $+$ *suma módulo* m*.*

Definición C.0.4. *Denotaremos como* $\mathbb{Z}_m^*$ *al conjunto de números enteros* $1 \leq i \leq m$ *tal que* m *es coprimo con* i*, es decir* $mcd(i, m) = 1$*. Este conjunto será un grupo* $(\mathbb{Z}_m^*, \cdot)$ *junto la operación* $\cdot$ *producto módulo* m*.*

Definiremos, para cada $r \in \mathbb{Z}_m$ *el conjunto* $r\mathbb{Z}_m^* \subseteq \mathbb{Z}_m$ *como el conjunto de los elementos* rx *con* $x \in \mathbb{Z}_m^*$*. Es sencillo comprobar que*

$$r\mathbb{Z}_m^* = \mathbb{Z}_m^* \quad \Leftrightarrow \quad r \in \mathbb{Z}_m^* \quad \Leftrightarrow \quad mcd(m, r) = 1 \tag{C.0.1}$$

Definición C.0.5 (Función ϕ de Euler)**.** *Definimos la función* ϕ *de Euler de un número* r *como el número de elementos menores que el propio* r *coprimos con él mismo. Es decir,* $\phi(r) = |\mathbb{Z}_r^*|$*.*

De hecho la función de Euler tiene una forma explícita relativamente sencilla basada en la descomposición prima del propio r*, aunque no la daremos por no ser relevante en el presente trabajo.*

Proposición C.0.6. *Si* G *es un grupo conmutativo y* $g = g_1 \cdots g_n \in G$ *entonces* $o(g) = mcm(o(g_1), \cdots, o(g_n))$*.*

Definición C.0.7 (Isomorfismo)**.** *Una función* $f : (G, \cdot_G) \to (G' \cdot_{G'})$ *se dice un* ***isomorfismo de grupos*** *si*

- f *es biyectiva. (*f *es suprayectiva e inyectiva).*
- $f(a \cdot_G b) = f(a) \cdot_{G'} f(b) \ \forall \ a, b \in G$

Definición C.0.8 (Orden)**.** *Definimos el* ***orden de un elemento*** $g \in G$ *como el mínimo* $n > 0$ *tal que* $g^n = 1$*, donde* 1 *es el elemento unidad de* G*. Análogamente definimos el* ***orden de un grupo*** G *como su cardinalidad, es decir, el número de elementos distintos que contiene. A este número lo denotaremos* $o(g)$*.*

Proposición C.0.9. *Sea* G *un grupo y* $g \in G$*. Si* $o(g) = r$ *entonces la secuencia* $\{1, g, g^2, \cdots, g^{r-1}\}$ *no contiene ninguna repetición.*

Teorema C.0.10 (Teorema Chino de los Restos)**.** *Sean* $I_1, \cdots, I_n$ *ideales de un anillo* R *tales que para todo* $i \neq j$*,* $I_i + I_j = R$ *entonces existe un isomorfismo*

$$f : R/(I_1 \cap \cdots \cap I_n) \to R/I_1 \times \cdots \times R/I_n \tag{C.0.2}$$

Corolario C.0.11 (Teorema Chino de los Restos, versión entera)**.** *Sean $n_1, \cdots, n_k$ enteros coprimos dos a dos, entonces dados k enteros $a_1, \cdots, a_k$ existe un entero x que resuelve el sistema de congruencias*

$$\begin{cases} x \equiv a_1 \ (mod\ n_1) \\ x \equiv a_2 \ (mod\ n_2) \\ \quad \vdots \\ x \equiv a_k \ (mod\ n_k) \end{cases} \tag{C.0.3}$$

Lema C.0.12. *Sea n impar, al menos la mitad de los elementos de $(\mathbb{Z}/n\mathbb{Z})^* = \mathbb{Z}_n^*$ tienen orden par.*

Demostración. Supongamos que tenemos un x con orden impar r. Entonces

$$(-x)^r = (-1)^r x^r = -1 \tag{C.0.4}$$

Lo que implica que el orden de $-x$ es $2r$ que es par. Por lo tanto al menos la mitad de elementos en $\mathbb{Z}_n^*$ tienen orden par. □

Teorema C.0.13 (Algoritmo de Euclides, [Sho09])**.** *Sean a, b pertenecientes a un dominio euclideo (en particular, a $\mathbb{Z}$) podemos obtener un máximo común divisor de a y b mediante el algoritmo*[1] *siguiente*

Algoritmo 5 Algoritmo de Euclides

```
1: procedure MCD(a, b: enteros)
2:     r_0 ← a
3:     r_1 ← b
4:     i ← 1
5:     while r_i ≠ 0 do
6:         r_{i+1} ← r_{i-1} mod r_i
7:         i ← i + 1
       return r_{i-1}
```

[1] De hecho, se puede ver de nuevo que este algoritmo se ejecuta en tiempo polilogarítmico.

APÉNDICE D

Complejidad cuántica.

D.1. Los modelos de computación de Turing

Definición D.1.1 (Máquina de Turing)**.** *Una* ***Máquina de Turing clásica determinista*** *(abreviado TM) es una hepta-tupla ordenada* $(\Sigma, \lambda, Q, q_i, A, F, \delta)$ *donde,*

- Σ *es un conjunto finito, llamado el* ***alfabeto*** *de símbolos.*
- Q *es un conjunto finito, llamado el conjunto de* ***estados****.*
- $\lambda \in \Sigma$ *es un símbolo llamado* ***símbolo blanco****.*
- $q_i \in Q$ *es el* ***estado inicial****.*
- $A \subseteq Q$ *es el conjunto de* ***estados de aceptación****.*
- $F \subseteq Q$ *es el conjunto de* ***estados finales****.*
- $\delta : \Sigma \times Q \to \Sigma \times Q \times \{L, R\}$ *es la* ***función de transición****.*

Definición D.1.2 (Máquina de Turing probabilista)**.** *Una máquina de Turing probabilista, que denotaremos como PTM, es una versión ligeramente modificada de la TM clásica donde cambiamos los espacios de actuación de la función de transición, provocando así que la función no devuelva un comportamiento unívoco que la máquina deberá realizar sino una distribución de probabilidad sobre los posibles comportamientos. Será la PTM la encargada de elegir aleatoriamente, aunque siguiendo la distribución de probabilidad que defina la función de transición, qué comportamiento realizar en cada paso. Así pues, una PTM corresponderá a una hepta-tupla* $(\Sigma, \lambda, Q, q_i, A, F, \delta)$ *donde todos los componentes corresponden en nombre y significado con los definidos para la TM excepto la función* δ *que se define en el dominio de* $Q \times \Sigma \times Q \times \Sigma \times \{L, R\}$ *y con imagen en* $[0, 1] \subseteq \mathbb{R}^+$*. Por tanto la probabilidad de, si nos encontramos en un estado* q_i *habiendo leído el símbolo* σ_1*, pasar al estado* q_2 *moviéndonos en la dirección* $D \in \{L, R\}$ *y escribiendo el símbolo* σ_2 *en la cinta es*

$$\delta(q_1, \sigma_1, q_2, \delta_2, D) \tag{D.1.1}$$

Si la probabilidad de que la PTM pare en un estado de $F \cap A$ *es* p*, entonces diremos que la PTM* acepta *con probabilidad* p*.*

D.2. La hipótesis de Church-Turing

Durante la segunda mitad del siglo XX se ha escrito numerosa literatura acerca de las máquinas de computación. Una máquina de computación es, en su forma más fundamental, un dispositivo físico cuya evolución dinámica transforma un conjunto de estados de entrada a un conjunto de estados de salida, estados que supondremos etiquetados en algún conjunto contable, por ejemplo $\mathbb{N}$. Si consideramos una máquina de cómputo clásica determinista como,

por ejemplo, una máquina de Turing clásica, podemos ver su funcionamiento como una función f que transforma el estado de entrada al estado de salida de forma determinista y unívoca.

Podemos entonces definir la "equivalencia computacional" de dos máquinas de computación clásicas y deterministas mediante la igualdad de las funciones que implementan bajo un mismo conjunto de etiquetado. El principal problema surge al intentar definir la equivalencia computacional para máquinas de computación que no son deterministas.

Conocemos bien un ejemplo de estas máquinas: Los circuitos cuánticos. Una vez ejecutado el circuito con una entrada determinada, la salida (es decir, el resultado tras la medición) no es, en general, siempre el mismo[1], dado que está sometido a una aleatoriedad. Por tanto la noción de equivalencia necesitará una generalización para este tipo de máquinas.

En las máquinas de computación no deterministas, la salida puede verse como una distribución de probabilidad de un estado definido por un observable (en los circuitos cuánticos, este observable será simplemente la medición que proyecta el estado sobre un estado de la base), así que etiquetaremos la salida de la máquina no determinista como un conjunto ordenado de pares (O, r) donde r es el resultado de la máquina al ser observada con el observable O. Tal dispositivo, dada una entrada, definirá una distribución de probabilidad sobre el conjunto de valores de salida. Consideraremos pues que dos máquinas de computación no deterministas serán computacionalmente equivalentes si existe una equivalencia entre los valores de salida de ambas máquinas de forma que una misma entrada define iguales distribuciones de probabilidad sobre los valores de salida relacionados.

Tal y como hemos visto, cada máquina de computación $\mathcal{M}$ computa una sola función f, aun así, no habría ningún problema en modificar el sistema de cómputo de $\mathcal{M}$ para obtener otra máquina $\mathcal{M}'$ que compute una función diferente. Para formalizar este cambio podemos considerar estas máquinas que computan una sola función como casos particulares de una máquina general $\mathcal{M}(\mathcal{P})$ que actúa sobre la entrada siguiendo las instrucciones codificadas en $\mathcal{P}$, a las que a veces nos referiremos como «programa». Podemos definir entonces el conjunto $C(\mathcal{M})$ como el conjunto de funciones que $\mathcal{M}$ puede computar si se le suministra el programa $\mathcal{P}$ adecuado. Es fácil comprobar que es posible construir, dadas dos máquinas generales $\mathcal{M}$ y $\mathcal{M}'$ una máquina compuesta que compute $C(\mathcal{M}) \cup C(\mathcal{M}')$.

Así pues, ¿por qué no proceder *ad infinitum* y construir una máquina universal $\tilde{\mathcal{M}}$ que sea capaz de computar cualquier función posible? La realidad es que, físicamente, parece haber un momento en el que añadir más hardware, es decir, crear máquinas de computación más complejas, no permite computar nuevas funciones. De hecho, se puede demostrar que el cualquier para funciones etiquetadas en los números enteros $\mathbb{Z}$, $C(\mathcal{M})$ siempre está contenido en $C(\mathcal{T})$, donde $\mathcal{T}$ es la conocida como máquina de computación universal de Turing [Tur37], es decir, que cualquier $f : \mathbb{Z} \to \mathbb{Z}$ que sea computable por una máquina de computación universal $\mathcal{M}$ es computable por la máquina universal de Turing $\mathcal{T}$.

Este hecho llevó a Alonzo Church [Chu36] y Alan Turing [Tur37] independientemente a conjeturar la llamada hipótesis de Church-Turing, que, en palabras del propio Turing puede formularse como

Hipótesis D.2.1 (Hipótesis de Church-Turing)**.** *Cada función que puede ser vista de forma natural como "computable" puede computarse por una máquina de computación universal de Turing.*

Esta afirmación, aunque comprensible, no está expresada de un modo formal matemáticamente aceptable. De hecho hay multitud de interpretaciones diferentes, como la expresada en el fantástico libro [Hof80] en el que se establece un interesante paralelismo entre las "funciones que pueden ser vistas de forma natural como computables" y los cálculos que puede realizar la mente humana.

El físico David Deutsch dio una reformulación física no ambigua en el artículo [Deu85], definiendo así el principio de Church-Turing como:

Principio D.2.2 (Principio de Church-Turing)**.** *Cada sistema físico finitamente realizable puede ser simulado perfectamente por una máquina de computación de forma finita.*

[1] A pesar de que el estado del sistema antes de la medición sí sea determinista.

Donde se define la "simulación perfecta" de un proceso físico de un sistema físico $\mathcal{S}$ por una máquina de computación $\mathcal{M}$ si existe un programa $\mathcal{P}(\mathcal{S})$ tal que $\mathcal{M}$ es computacionalmente equivalente a $\mathcal{S}$ bajo una elección apropiada para el etiquetado de sus entradas y salidas. El hecho de que la simulación sea "de forma finita" se puede formalizar como sigue. Si consideramos una máquina de computación como una secuencia de pasos cuya duración es estrictamente positiva acotada inferiormente por un valor ε, entonces diremos que la simulación es de forma finita si (i) solo un subsistema finito está en movimiento durante un paso, (ii) el movimiento solamente depende del estado de un subsistema finito, y (iii) la regla que especifica el movimiento puede especificarse formalmente con un número finito de instrucciones. La máquina universal de Turing $\mathcal{T}$ cumple trivialmente estas tres condiciones, así como el computador cuántico universal[2] $\mathcal{Q}$ que veremos en la sección siguiente.

Así pues, la formulación como principio de la hipótesis de Church-Turing debería incluir cualquier sistema físico que fuese realizable experimentalmente y la máquina de computación debería ser finitamente especificable.

El problema que surge al pensar más profundamente en el principio D.2.2 es que un sistema físico general no es simulable por una máquina de Turing universal, dado que sus estados forman un continuo[3] y la máquina universal de Turing tan solo puede trabajar con valores en un conjunto numerable. Sin embargo no debemos darnos por vencidos, pues se puede demostrar que el computador cuántico universal $\mathcal{Q}$ puede simular cualquier proceso real (es decir, disipativo). Así pues, la teoría cuántica es perfectamente compatible con el principio de Church-Turing en su versión física, no así la computación clásica.

D.3. El computador cuántico universal.

Una máquina de Turing cuántica (o, abreviadamente, QTM) es similar a una máquina de Turing probabilista a excepción de las siguientes diferencias:

1. Los coeficientes no son probabilidades sino números complejos que llamaremos «amplitudes».
2. En cada paso, los cuadrados de los módulos de las amplitudes suman 1.
3. Para cualquier entrada, la matriz de transición debe ser unitaria.

Establecemos la condición de parada de una QTM como que cada una de sus bifurcaciones alcance un estado final. En tal caso la salida estará escrita en la cinta desde la posición inicial hasta el primer símbolo blanco. La probabilidad de que la salida sea una determinada configuración viene dada por el módulo al cuadrado de la amplitud correspondiente.

Definición D.3.1 (Máquina de Turing cuántica)**.** *Una* ***Máquina de Turing cuántica*** *es una hexa-tupla ordenada* $(\Sigma, \lambda, Q, q_i, q_f, \delta)$ *donde,*

- Σ *es un conjunto finito, llamado el* ***alfabeto*** *de símbolos. Asumimos que* $\Sigma = \{0, 1, \lambda\}$
- Q *es un conjunto finito, llamado el conjunto de* ***estados****.*
- $\lambda \in \Sigma$ *es un símbolo llamado* ***símbolo blanco****.*
- $q_i \in Q$ *es el* ***estado inicial****.*
- $A \subseteq Q$ *es el conjunto de* ***estados de aceptación****.*
- q_f *es el* ***estado final****.*
- *La* ***función de transición*** *es* $\delta : \Sigma \times Q \to H$ *donde* H *es el espacio de Hilbert complejo generado por los vectores correspondientes a las ternas de* $\Sigma \times Q \times \{L, R\}$*.*

y además, la matriz de transición es unitaria para cualquier entrada.

[2] También conocido como máquina de Turing cuántica.

[3] Imaginemos como ejemplo un sistema físico simple, un péndulo. No es difícil comprobar que el péndulo puede tomar un número continuo (y por tanto infinito) de valores para la posición

Definición D.3.2 (Simulación)**.** *Decimos que una QTM Q simula un circuito cuántico C para una entrada I si Q, proporcionada la entrada I, resulta una distribución de probabilidad idéntica a la que proporciona C.*

D.4. Máquinas de Turing cuánticas y circuitos cuánticos.

Lema D.4.1. *Cada matriz de tamaño $2^k \times 2^k$ puede descomponerse en, como máximo, $2^{O(k)}$ puertas cuánticas de un solo qubit y puertas CNOT.*

Demostración. Ver [BBC+95] □

Lema D.4.2. *Para cada matriz unitaria U de tamaño $2^k \times 2^k$ existe una QTM que simula el circuito consistente en tan solo la puerta U.*

Demostración. Como una matriz unitaria U se puede ver como una función $f_U : H^{\otimes k} \to H^{\otimes k}$ definida en el espacio de Hilbert de estados de un registro de k qubits, tal función puede implementarse con una QTM. □

Proposición D.4.3. *Para cada circuito cuántico de tamaño n existe una máquina de Turing cuántica con complejidad $T(n)$ que simula tal circuito tal que $T(n) = O(n)$.*

Demostración. Cada puerta cuántica de tamaño 2^k puede simularse en una QTM usando, como máximo, $2^{O(k)}$ pasos, así pues, si acotamos el tamaño máximo de las puertas cuánticas que usamos (es decir, de las puertas del conjunto universal que consideremos) como hicimos en **??**, a 2^m, la simulación necesitará como máximo $2^{O(m)}n = O(n)$ pasos.

□

Proposición D.4.4. *Para cada entero positivo n y para cada QTM M con complejidad T existe un circuito con $poly(n, T)$ puertas cuánticas elementales que simula M para cualquier entrada de tamaño n.*

Demostración. Para cada uno de los T pasos que realiza M construiremos un circuito diferente. Como la QTM no puede recorrer más de T celdas desde la posición inicial supondremos que la cinta es finita con tan solo $2T + 1$ celdas. Así pues, para cada una de estas celdas añadimos $l = 1 + \lceil \log(|Q| + 1) \rceil) + \lceil \log |\Sigma| \rceil$ conexiones al circuito, donde cada una de ellas se usa para lo siguiente:

- Usamos las $\lceil \log(|Q| + 1) \rceil)$ conexiones para codificar el estado actual, donde suponemos que puede existir un nuevo estado (por ello se suma la constante 1) que codificará que la máquina nunca ha alcanzado esa celda.
- Usamos los $\lceil \log |\Sigma| \rceil$ bits para codificar el símbolo escrito en esa celda.
- Por último utilizamos una conexión más para indicar si la cabeza lectora-escritora de la QTM está en esa celda concreta.

Así pues, para cada paso de la ejecución de la QTM, centrémonos en la celda sobre la que la cabeza está situada. Queremos definir una matriz unitaria que transforme los estados de las $3l$ conexiones según como lo haría la función de transición δ. Lo escribimos formalmente como

$$\begin{aligned} U\Big(|n, a_l, 0\rangle\, |q_1, a_1, 1\rangle\, |n, a_r, 0\rangle \Big) = \sum_{a', q'} \delta(q, a, q', a', L)\, |q', a_l, 1\rangle\, |n, a', 0\rangle\, |n, a_r, 0\rangle \\ + \delta(q, a, q', a', R)\, |n, a_l, 0\rangle\, |n, a', 0\rangle\, |q', a_r, 1\rangle \end{aligned} \tag{D.4.1}$$

Pero podemos demostrar que los vectores $U\Big(|n, a_l, 0\rangle\, |q_1, a_1, 1\rangle\, |n, a_r, 0\rangle \Big)$ son mutuamente ortogonales entre sí:

$$
\begin{aligned}
\langle s, a_{l1}, 0|\, \langle q_1, a_1, 1|\, \langle s, a_{r1}, 0|\, U^\dagger U\, |s, a_{l2}, 0\rangle\, |q_2, a_2, 1\rangle\, |s, a_{r2}, 0\rangle = \\
\Big(\sum_{a_1', q_1'} \Big\{ \delta(q_1, a_1, q_1', a_1', L)\, \langle q_1' a_{l1}, 1|\, \langle s, a_1', 0|\, \langle s, a_{r1}, 0| + \\
\delta(q_1, a_1, q_1', a_1', R)\, \langle s, a_{l1}, 0|\, \langle s, a_1', 0|\, \langle q_1', a_{r1}, 1| \Big\} \Big) \\
\Big(\sum_{a_2', q_2'} \Big\{ \delta(q_2, a_2, q_2', a_2', L)\, \langle q_2' a_{l2}, 1|\, \langle s, a_2', 0|\, \langle s, a_{r2}, 0| + \\
\delta(q_2, a_2, q_2', a_2', R)\, \langle s, a_{l2}, 0|\, \langle s, a_2', 0|\, \langle q_2', a_{r2}, 1| \Big\} \Big) = \\
\sum_{a_q', q_1', a_2', q_2'} \delta(q_1, a_1, q_1', a_1', L) \delta(q_2, a_2, q_2', a_2', L) \Big(\\
\langle q_1' a_{l1}, 1|\, \langle s, a_1', 0|\, \langle s, a_{r1}, 0 | s, a_{r2}, 0\rangle\, |s, a_2', 0\rangle\, |q_2' a_{l2}, 1\rangle \Big) + \\
\delta(q_1, a_1, q_1', a_1', R) \delta(q_2, a_2, q_2', a_2', R) \Big(\\
\langle s, a_{l1}, 0|\, \langle s, a_1', 0|\, \langle q_1', a_{r1}, 1 | q_2', a_{r2}, 1\rangle\, |s, a_2', 0\rangle\, |s, a_{l2}, 0\rangle \Big) = \\
\delta_{a_{l2}}^{a_{l1}} \delta_{a_{r2}}^{a_{r1}} \Big(\sum_{a_1', q_1'} \delta(q_1, a_1, q_1', a_1', L) \delta(q_2, a_2, q_2', a_2', L) + \delta(q_1, a_1, q_1', a_1', R) \delta(q_2, a_2, q_2', a_2', R) \Big) \\
= 0
\end{aligned}
\tag{D.4.2}
$$

Donde δ_m^n es la función delta de Kronecker y donde la última igualdad surge de la condición de las QTM de tener transiciones unitarias, ya que todas las filas distintas de la matriz de transición serán ortogonales. El resto de los vectores de la base pueden establecerse entonces de forma que U sea una matriz ortogonal. Si añadimos al circuito una de estas puertas a cada terna de celdas adyacentes (no importa el orden porqueee...) este circuito simulará un paso de M. Para simular los T pasos necesitaremos T de estos circuitos.

Hemos usado $O(T \cdot (2T+1))$ matrices de tamaño $2^{3l} \times 2^{3l}$ y $2O(l(2T+1))$ conexiones. Por el teorema B.1.2 sabemos que tales matrices pueden realizarse con $2^{O(l)}$ puertas cuánticas elementales, por tanto hemos usado $T^2 2^{O(l)}$ puertas cuánticas elementales.

□

D.5. Definiciones de la clase BQP.

Definición D.5.1 (**BQP** mediante QTM.)**.** *Un lenguaje $\mathcal{L}$ está contenido en* **BQP** *si existe un polinomio $p(n)$ tal que $\mathcal{L}$ es aceptado por una máquina de Turing cuántica con complejidad temporal $p(n)$.*

Gracias a la proposición D.4.4 podemos definir la clase **BQP** usando circuitos cuánticos como sigue

Definición D.5.2 (**BQP** mediante circuitos.)**.** *Un lenguaje $\mathcal{L}$ está contenido en* **BQP** *si existe una función $f(n)$ y polinomios $p(n)$, $q(n)$ tal que para cada n la salida de $f(n)$ es un circuito C de anchura n y tamaño $p(n)$ tal que C acepta el lenguaje $\mathcal{L}_n \equiv \{x \in \mathcal{L} \mid |x| = n\}$ y el tiempo de ejecución de $f(n)$ es, como máximo, $q(n)$.*

D.6. Caracterización de BQP

Un resultado importante que nos permitirá relacionar la complejidad cuántica con la clásica es el hecho de que cada circuito clásico (booleano) puede implementarse eficientemente dentro de un circuito cuántico. De hecho,

demostraremos que el número de puertas necesarias en un circuito cuántico tiene exactamente el mismo orden que el número de puertas booleanas del circuito que implementa.

Teorema D.6.1. *Si $f : \{0,1\}^n \to \{0,1\}^m$ es computable por un circuito booleano de tamaño S, entonces existe una secuencia de $2S + m + n$ puertas cuánticas que computan la operación* [4]

$$|x\rangle \left|0^{2m+S}\right\rangle \to |x\rangle \left|f(x)\right\rangle \left|0^{S+m}\right\rangle \tag{D.6.1}$$

Demostración. El registro que utilizaremos para el circuito cuántico será un registro compuesto por $n+2m+S$ qubits, en la sección correspondiente a los n primeros qubits almacenaremos el valor de entrada sobre el que queremos computar f. Los $2m$ qubits a continuación los usaremos para almacenar el valor de la función ya computada y una copia[5] de ella. Por último los S qubits restantes son los conocidos como *scratchpad*, es decir, unos qubits necesarios para mantener la reversibilidad del circuito.

La primera parte del circuito corresponderá al circuito booleano en el que reemplazamos cada puerta lógica clásica (AND, OR, NOT) por su análogo cuántico visto en la sección **??**, y en el que la entrada no son tan solos los n qubits que corresponderían a la entrada de la función sino los $n+2m+S$ qubits que necesitaremos para el circuito.

Si la entrada al circuito es $|x\rangle \left|0^{2m+S}\right\rangle$ el resultado del cómputo será $|x\rangle \left|f(x)0^m\right\rangle |z\rangle$, que podremos realizar usando tan solo S puertas cuánticas. Tras este cómputo copiamos el valor $f(x)$ a los m registros siguientes, aún con el valor 0, usando m operaciones de la forma $|bc\rangle \to |b(b \oplus c)\rangle$. Si aplicamos en este punto una a una las inversas de las S puertas cuánticas en sentido contrario, esta operación eliminará el registro $f(x)$ original así como los valores $|z\rangle$ del scratchpad, dejándolos en el valor $|0\rangle$ de nuevo, alcanzando así el estado del enunciado. □

Para los teoremas que siguen recomendamos revisar las definiciones de las clases de complejidad clásica de un texto como [Pap03] o [Sip06].

Corolario D.6.2. P ⊆ BQP

Demostración. Sabemos que cada TM clásica M con orden de complejidad $T(n)$ tiene un circuito booleano equivalente con $O(T(n)\log T(n))$ puertas lógicas. Por el teorema anterior existirá por tanto un circuito cuántico con $O(T(n)\log T(n) + n)$ puertas cuánticas que computará la misma función que M lo que, usando la caracterización de **BQP** mediante circuitos cuánticos, prueba la afirmación. □

Corolario D.6.3. BPP ⊆ BQP

Demostración. Ver [AB09] □

Podemos comprobar que al menos, la computación cuántica no es infinitamente más potente que la clásica mediante los siguientes dos resultados:

Teorema D.6.4. BQP ⊆ PSPACE

Demostración. Ver [AB09] □

Corolario D.6.5. BQP ⊆ EXPTIME

Demostración. A pesar de que se sigue directamente de que **PSPACE** ⊆ **EXPTIME**, se puede consultar [Aar13] para una demostración explícita. □

Sin embargo, la veracidad de las siguientes afirmaciones sigue todavía siendo un problema abierto en teoría de la computación

1. **P** $\stackrel{?}{=}$ **BQP**
2. **BPP** $\stackrel{?}{=}$ **BQP**

[4] De dónde sale el n!!
[5] Blah blah B.2.

3. $\mathbf{NP} \stackrel{?}{=} \mathbf{BQP}$
4. $\mathbf{PH} \stackrel{?}{=} \mathbf{BQP}$

A pesar de que no exista una demostración todavía para las afirmaciones mencionadas, los teóricos de la computación creen tener una intuición sobre aquellas que serían falsas. La segunda de ellas, $\mathbf{BPP} \stackrel{?}{=} \mathbf{BQP}$, se cree falsa ([Aar13]) por la razón de que no se ha encontrado ningún algoritmo probabilista capaz de factorizar en tiempo polinomial sobre el tamaño de la entrada. La primera sería, usando la conocida relación de inclusión $\mathbf{P} \subseteq \mathbf{BPP}$, también falsa. Por otro lado no se cree que $\mathbf{NP} = \mathbf{BQP}$ dado que tal afirmación significaría que la computación cuántica es capaz de resolver cualquier problema **NP** en orden temporal lineal. Sin embargo, aún es posible que, contra la intuición de muchos científicos, alguna de estas afirmaciones resulte cierta provocando así profundos cambios sobre nuestra concepción de la potencia de los modelos de computación tanto clásica como cuántica.

Por otro lado, a pesar de que tales problemas estén a día de hoy aún sin resolver, se han encontrado oráculos O y $\tilde{O}$ relativos a los cuales $\mathbf{P}^O = \mathbf{BQP}^O$ ([FR99]) y $\mathbf{PH}^{\tilde{O}} = \mathbf{BQP}^{\tilde{O}}$ ([RT18]) tales que no colapsan la jerarquía, es decir, $\mathbf{P}^O \neq \mathbf{NP}^O$ y $\mathbf{P}^{\tilde{O}} \neq \mathbf{NP}^{\tilde{O}}$.

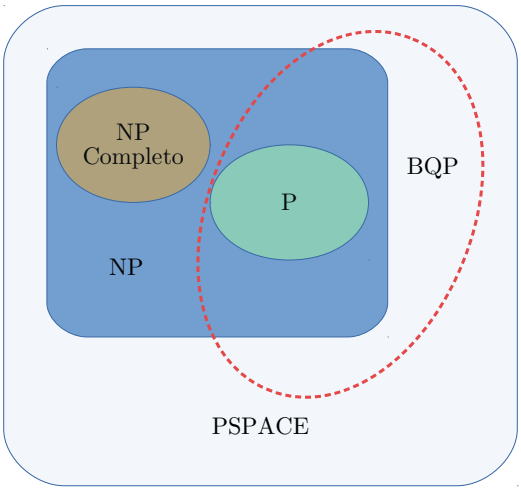


Figura D.6.1: Posible relación entre **P**, **BQP**, **NP** y **PSPACE**

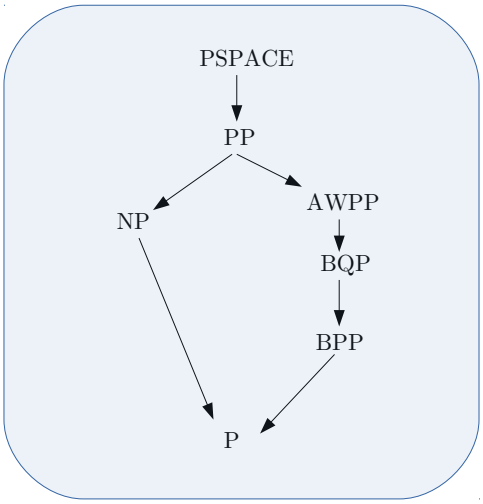


Figura D.6.2: Jerarquía de inclusión conocida para la clase **BQP**

APÉNDICE E

Computación Cuántica Adiabática

...SECCIÓN EN PROGRESO...

Sacado de [Kat50]

Definición E.0.1. *Diabatic process: Rapidly changing conditions prevent the system from adapting its configuration during the process, hence the spatial probability density remains unchanged. Typically there is no eigenstate of the final Hamiltonian with the same functional form as the initial state. The system ends in a linear combination of states that sum to reproduce the initial probability density.*

Definición E.0.2. *Adiabatic process: Gradually changing conditions allow the system to adapt its configuration, hence the probability density is modified by the process. If the system starts in an eigenstate of the initial Hamiltonian, it will end in the corresponding eigenstate of the final Hamiltonian.*

3-SAT

E.1. Evolución temporal de un sistema cuántico

E.2. Autovalores y autoestados

$[H_0, H_P]$ 0

E.3. El modelo de la AQC

La *computación cuántica adiabática* (AQC) es un modelo de computación cuántica radicalmente diferente al propuesto para la explicación del algoritmo de Shor basado en circuitos cuánticos. La diferencia consiste en que, mientras en el modelo basado en circuitos un cómputo puede evolucionar desde un estado a cualquier otro usando las puertas cuánticas adecuadas, en el modelo de la AQC un sistema cuántico se inicializa un sistema un estado base fácil de preparar correspondiente a un hamiltoniano adecuado H_0 y este evoluciona hasta el estado base de un hamiltoniano H_P que codifica la solución del problema.

El *teorema de la computación adiabática* garantiza que, si la evolución del sistema se realiza suficientemente lenta, entonces el estado en el que se encuentra el sistema tras la evolución es un estado base.

Este enfoque surgió en 1988 con el primer nombre de *optimización cuántica estocástica* ([ACdF89]) y poco después pasó a denominarse *temple cuántico* por sus similitudes con el proceso del temple simulado. Para nuestro

estudio usaremos la definición de la AQC dada en [AvK$^+$04]. Veamos ciertos términos que harán abordable la definición que presentaremos a continuación.

Diremos que un hamiltoniano H es k-local si es una matriz H hermítica que puede escribirse como $H = \sum_{i=1}^{r} H_i$ donde H_i actúa no trivialmente en, como máximo, k partículas del sistema o, en nuestro contexto, en k qubits del registro.

Definición E.3.1. *Un **cómputo cuántico adiabático** k-local queda definido por dos hamiltonianos k-locales H_0 y H_P actuando en n partículas. El estado base de H_0 se puede escribir como estado producto. La salida del cómputo es un estado ε-cercano en la norma ℓ_2 al estado base de H_P. Con $s(t) : [0, t_f] \to [0, 1]$ la* planificación *y con t_f el primer instante tal que el estado final de la evolución con $H(s) = (1 - s)H_0 + sH_P$ para t_f es ε-cercano en la norma ℓ_2 al estado base de H_P.*

En [AL18] los siguientes comentarios se realizan para la definición que acabamos de dar:

1. En [ACdF89] se impone una restricción de unicidad para el autoestado base del hamiltoniano final H_P pero esta restricción no es necesaria puesto que, en principio, si asumimos el cómputo adiabático como un problema de optimización como hacemos en este trabajo, cualquier solución que minimice la función será válida, a pesar de que existan más de una.
2. En ciertos contextos es conveniente considerar un cómputo adiabático en un estado excitado y no tan solo en un estado base.
3. La evolución lineal del hamiltoniano de la definición E.3.1 no es estrictamente necesaria, de hecho veremos que podemos considerar evoluciones más generales introduciendo un hamiltoniano intermedio que se anule en $s = 0, 1$.

E.3.1. Teoremas de la AQC

En 1928, M. Born y V. Fock dieron en su artículo *Beweis des adiabatensatzes* una caracterización del teorema cuántico en lenguaje natural como sigue

Teorema E.3.2 ([BF28])**.** *Un sistema físico permanece en su estado propio instantáneo si la perturbación que actúa sobre él es lo bastante lenta y hay un salto energético entre su valor propio y el resto del espectro del hamiltoniano.*

Versiones aproximadas

Sea $|\varepsilon_j(t)\rangle$ ($j \in \{0, 1, 2, \cdots\}$ el autoestado de $H(t)$ con energía instantánea $\varepsilon_j(t)$ de forma que $\varepsilon_j \leq \varepsilon_{j+1}\ \forall j, t$, es decir, $H(t)\,|\varepsilon_j(t)\rangle = \varepsilon_j\,|\varepsilon_j(t)\rangle$ y $|\varepsilon_0(t)\rangle$ es el autoestado base de $H(t)$. Asumiemos que el estado inicial está preparado en uno de los autoestados $|\varepsilon_j(0)\rangle$.

La versión más simple del teorema cuántico adiabático aproximado fue dado en 1962 por Messiah ([Mes64]) en el que se establecía que, dado un sistema en el autoestado inicial $|\varepsilon_j(0)\rangle$ se mantendrá en tal autoestado hasta el instante t_f siempre que

$$\max_{t\in[0,t_f]} \frac{|\,\langle\varepsilon_i|\partial_t\varepsilon_j\rangle\,|}{|\varepsilon_i - \varepsilon_j|} = \max_{t\in[0,t_f]} \frac{|\,\langle\varepsilon_i|\,\partial_t H\,|\varepsilon_j\rangle\,|}{|\varepsilon_i - \varepsilon_j|^2} \ll 1\ \forall i \neq j \tag{E.3.1}$$

Este teorema, aunque útil en la mayoría de ocasiones, ha sido ampliamente criticado dado que, en el caso en el que la evolución del hamiltoniano presente autovalores oscilantes. Por esta razón se dio en [Ami09] una condición diferente usando el parámetro adimensional s

$$\max_{s\in[0,1]} \frac{|\,\langle\varepsilon_i(s)|\,\partial_s H(s)\,|\varepsilon_j(s)\rangle\,|}{|\varepsilon_i(s) - \varepsilon_j(s)|^2} \ll t_f\ \forall i \neq j \tag{E.3.2}$$

que podemos abreviar usando la notación

$$\Delta_{ij}(s) = \varepsilon_i(s) - \varepsilon_j(s) \tag{E.3.3}$$

y si estamos trabajando, como normalmente haremos, con el estado base usaremos la notación $\Delta(s) = \Delta_{10}(s)$.

Esta última condición no da una acotación exacta sino aproximada, pero normalmente da un rango aproximado de valores para los cuales el algoritmo debería funcionar. Sin embargo existen otros teoremas más complicados que dan cotas exactas para t_f.

Versiones exactas

El primer teorema cuántico adiabático exacto fue dado por Kato en 1950 en [Kat50] y sentó una forma de proceder que ha sido usado ampliamente en muchas versiones del teorema que surgieron posteriormente, muchas de ellas basadas en diferentes supuestos y en diferentes contextos, muchas de ellas basadas en la suposición de que el hamiltoniano pertenezca una clase especial de funciones derivables definida en [Gev18] conocida como la clase de Gevrey. Sin embargo, presentaremos en esta sección una versión del teorema dada en [JRS07] donde la única condición sobre el hamiltoniano que se impone es la derivabilidad de $H(s)$.

Supondremos que el sistema está inicializado al estado base. Asumiremos también que el hamiltoniano $H(s)$ tiene un proyector $P(s)$ con autoenergía $\varepsilon_0(s)$ y con $\Delta > 0$. Sea $P_{t_f}(s) = \left|\phi_{t_f}(s)\right\rangle \left\langle\phi_{t_f}(s)\right|$ el proyector sobre el estado del sistema en s. Los teoremas cuánticos adiabáticos comúnmente dan cotas para $\left\|P_{t_f}(s) - P(s)\right\|$.

Teorema E.3.3 ([JRS07])**.** *Supongamos que el espectro de autovalores de $H(s)$ restringido a la proyección $P(s)$ consiste en $m(s)$ autovalores separados por un* incremento[1] *$\Delta(s)$ y que $H(s)$ es dos veces continuamente derivable. Suponiendo que $H(s)$, $\partial_t H(s)$ y $\partial_t^2 H(s)$ son operadores acotados, entonces, para cada $s \in [0,1]$ se cumple*

$$\left\|P_{t_f}(s) - P(s)\right\| \leq \frac{m(0)\|\partial_t H(0)\|}{t_f \Delta^2(0)} + \frac{m(s)\|\partial_t H(s)\|}{t_f \Delta^2(s)} + \frac{1}{t_f}\int_0^2 \left(\frac{m\left\|\partial_t^2 H\right\|}{\Delta^2} + \frac{7m\sqrt{m}\|\partial_t H\|^2}{\Delta^3}\right) dx \tag{E.3.4}$$

De hecho, ignorando por simplicidad la dependencia de m, este resultado muestra que es suficiente que

$$t_f \gg \text{máx}\left\{ \max_{s\in[0,1]} \frac{\left\|\partial_t^2 H(s)\right\|}{\Delta^2(s)}, \max_{s\in[0,1]} \frac{\|\partial_t H(s)\|^2}{\Delta^3(s)}, \max_{s\in[0,1]} \frac{\|\partial_t H(s)\|}{\Delta^2(s)} \right\} \tag{E.3.5}$$

E.3.2. Caracterización de la complejidad

[1] Gap.

APÉNDICE F

Ejemplo de Ejecución del Algoritmo de Shor

Factoricemos ahora el valor $n = 21$ con el algoritmo de Shor a mano, para ilustrar el funcionamiento.

En primer lugar debemos encontrar el orden de un número aleatorio $a \in \{2, \cdots, 21-1\}$. Elegimos aleatoriamente el número 10. Calculamos $d = mcd(10, 21) = 1$. Al ser 10 y 21 coprimos no hemos hallado ningún factor común, en otro caso devolveríamos el máximo común divisor d pues sería un factor no trivial de 21.

En este punto nuestra tarea es encontrar el orden de 10 en $\mathbb{Z}_{21}$, para lo cual usamos la transformada de Fourier cuántica.

Inicializamos los dos registros de 9 qubits (pues $21^2 \leq 2^9 < 2 \cdot 21^2$) al valor $|0\rangle$ y realizamos la superposición uniforme de los estados del primer registro, ya sea usando la QFT o con la aplicación de puertas H. Tras lo que realizamos el cálculo cuántico de la exponenciación modular visto en el algoritmo 1 y aplicamos la QFT al primer registro, obteniendo así una superposición de $262144 = 512^2$ estados cuánticos de los cuales solamente tienen, para los valores del primer registro, coeficientes no nulos los mostrados en la figura F.0.1.

Podemos ver en la figura F.0.2 la probabilidad de hallar cada valor concreto. Para el valor $z = 427$ la probabilidad de que sea medido es 0,114, que es uno de los valores más altos, como se puede visualizar también en la figura F.0.1. Supondremos que la medición sobre el primer registro cuántico nos devuelve el valor 427.

Ahora pues, sabemos que nuestro objetivo es buscar los enteros d, r con $r < n$ tal que

$$\left|\frac{427}{512} - \frac{d}{r}\right| \leq \frac{1}{1024} \tag{F.0.1}$$

La expansión de $\frac{427}{512}$ en fracción continua es

$$0 + \cfrac{1}{5 + \cfrac{1}{42 + \cfrac{1}{2}}} \tag{F.0.2}$$

Sabemos, por las ecuaciones del lema 3.3.1 que los valores de p_n y q_n serán

$$p_0 = a_0 = 0, \quad p_1 = 1, \quad p_2 = 5, \quad p_3 = 211, \quad p_4 = 427 \tag{F.0.3}$$

$$q_0 = 1, \quad q_1 = 1, \quad q_2 = 6, \quad q_3 = 253, \quad q_4 = 512 \tag{F.0.4}$$

Por lo que la fracción con numerador y denominador coprimos que mejor aproxima $\frac{427}{512}$ con un denominador menor que 21 es $\frac{5}{6}$. Así pues hemos obtenido el orden de 10 en $\mathbb{Z}_{21}$, $o(10) = 6$.

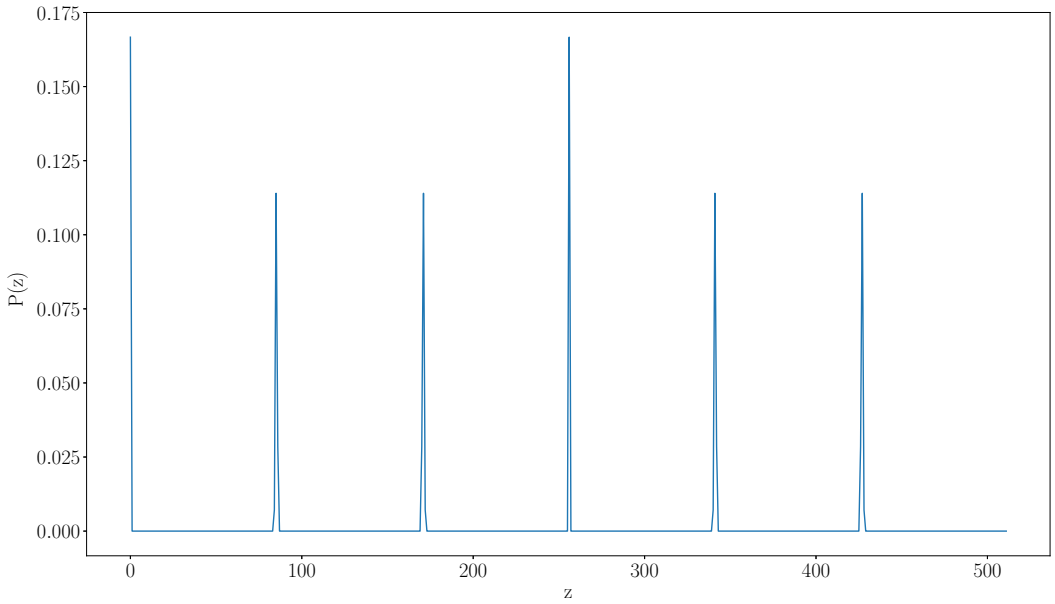


Figura F.0.1: Probabilidades de obtener un valor z al medir el primer registro tras la QFT para $n = 21$ y $a = 10$.

$P(|0\rangle|1\rangle) = 0{,}028$, $P(|0\rangle|10\rangle) = 0{,}028$, $P(|0\rangle|16\rangle) = 0{,}028$, $P(|0\rangle|13\rangle) = 0{,}028$, $P(|0\rangle|4\rangle) = 0{,}028$, $P(|0\rangle|19\rangle) = 0{,}028$,
$P(|84\rangle|1\rangle) = 0{,}001$, $P(|84\rangle|10\rangle) = 0{,}001$, $P(|84\rangle|16\rangle) = 0{,}001$, $P(|84\rangle|13\rangle) = 0{,}001$, $P(|84\rangle|4\rangle) = 0{,}001$, $P(|84\rangle|19\rangle) = 0{,}001$,
$P(|85\rangle|1\rangle) = 0{,}019$, $P(|85\rangle|10\rangle) = 0{,}019$, $P(|85\rangle|16\rangle) = 0{,}019$, $P(|85\rangle|13\rangle) = 0{,}019$, $P(|85\rangle|4\rangle) = 0{,}019$, $P(|85\rangle|19\rangle) = 0{,}019$,
$P(|86\rangle|1\rangle) = 0{,}005$, $P(|86\rangle|10\rangle) = 0{,}005$, $P(|86\rangle|16\rangle) = 0{,}005$, $P(|86\rangle|13\rangle) = 0{,}005$, $P(|86\rangle|4\rangle) = 0{,}005$, $P(|86\rangle|19\rangle) = 0{,}005$,
$P(|170\rangle|1\rangle) = 0{,}005$, $P(|170\rangle|10\rangle) = 0{,}005$, $P(|170\rangle|16\rangle) = 0{,}005$, $P(|170\rangle|13\rangle) = 0{,}005$, $P(|170\rangle|4\rangle) = 0{,}005$, $P(|170\rangle|19\rangle) = 0{,}005$,
$P(|171\rangle|1\rangle) = 0{,}019$, $P(|171\rangle|10\rangle) = 0{,}019$, $P(|171\rangle|16\rangle) = 0{,}019$, $P(|171\rangle|13\rangle) = 0{,}019$, $P(|171\rangle|4\rangle) = 0{,}019$, $P(|171\rangle|19\rangle) = 0{,}019$,
$P(|172\rangle|1\rangle) = 0{,}001$, $P(|172\rangle|10\rangle) = 0{,}001$, $P(|172\rangle|16\rangle) = 0{,}001$, $P(|172\rangle|13\rangle) = 0{,}001$, $P(|172\rangle|4\rangle) = 0{,}001$, $P(|172\rangle|19\rangle) = 0{,}001$,
$P(|256\rangle|1\rangle) = 0{,}028$, $P(|256\rangle|10\rangle) = 0{,}028$, $P(|256\rangle|16\rangle) = 0{,}028$, $P(|256\rangle|13\rangle) = 0{,}028$, $P(|256\rangle|4\rangle) = 0{,}028$, $P(|256\rangle|19\rangle) = 0{,}028$,
$P(|340\rangle|1\rangle) = 0{,}001$, $P(|340\rangle|10\rangle) = 0{,}001$, $P(|340\rangle|16\rangle) = 0{,}001$, $P(|340\rangle|13\rangle) = 0{,}001$, $P(|340\rangle|4\rangle) = 0{,}001$, $P(|340\rangle|19\rangle) = 0{,}001$,
$P(|341\rangle|1\rangle) = 0{,}019$, $P(|341\rangle|10\rangle) = 0{,}019$, $P(|341\rangle|16\rangle) = 0{,}019$, $P(|341\rangle|13\rangle) = 0{,}019$, $P(|341\rangle|4\rangle) = 0{,}019$, $P(|341\rangle|19\rangle) = 0{,}019$,
$P(|342\rangle|1\rangle) = 0{,}005$, $P(|342\rangle|10\rangle) = 0{,}005$, $P(|342\rangle|16\rangle) = 0{,}005$, $P(|342\rangle|13\rangle) = 0{,}005$, $P(|342\rangle|4\rangle) = 0{,}005$, $P(|342\rangle|19\rangle) = 0{,}005$,
$P(|426\rangle|1\rangle) = 0{,}005$, $P(|426\rangle|10\rangle) = 0{,}005$, $P(|426\rangle|16\rangle) = 0{,}005$, $P(|426\rangle|13\rangle) = 0{,}005$, $P(|426\rangle|4\rangle) = 0{,}005$, $P(|426\rangle|19\rangle) = 0{,}005$,
$P(|427\rangle|1\rangle) = 0{,}019$, $P(|427\rangle|10\rangle) = 0{,}019$, $P(|427\rangle|16\rangle) = 0{,}019$, $P(|427\rangle|13\rangle) = 0{,}019$, $P(|427\rangle|4\rangle) = 0{,}019$, $P(|427\rangle|19\rangle) = 0{,}019$,
$P(|428\rangle|1\rangle) = 0{,}001$, $P(|428\rangle|10\rangle) = 0{,}001$, $P(|428\rangle|16\rangle) = 0{,}001$, $P(|428\rangle|13\rangle) = 0{,}001$, $P(|428\rangle|4\rangle) = 0{,}001$, $P(|428\rangle|19\rangle) = 0{,}001$,

Figura F.0.2: Probabilidades mayores que 10^{-3} de los estados de la superposicón para la QFT con $n = 21$, $a = 10$.

Es fácil comprobar que $10^{6/2} \equiv 13 \pmod{21} \not\equiv -1 \pmod{21}$ por lo que podemos aplicar el lema 3.2.1 y asegurar que 12 y 21 tienen un factor común. De hecho se puede computar muy fácilmente calculando el máximo común divisor usando el algoritmo de Euclides y ver que $mcd(12, 21) = 3$. Por lo que el algoritmo ha encontrado el factor 3 de 21. Como $21/3 = 7$ que es primo el test de primalidad lo detectaría y el algoritmo pararía con la lista de divisores $\{3, 7\}$.

Bibliografía

[Aar03] Aaronson, S. The prime facts: From euclid to aks. *Lecture Notes*, 2003.

[Aar09] Aaronson, S. BQP and the Polynomial Hierarchy. *ArXiv e-prints*, October 2009.

[Aar13] Aaronson, S. *Quantum Computing since Democritus*. Cambridge University Press, 2013.

[AB09] Arora, S., y Barak, B. *Computational complexity: a modern approach*. Cambridge University Press, 2009.

[ACdF89] Apolloni, B., Carvalho, C., y de Falco, D. Quantum stochastic optimization. *Stochastic Processes and their Applications*, 33(2):233 – 244, 1989.

[ADH97] Adleman, L. M., DeMarrais, J., y Huang, M.-D. A. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997.

[Aha03] Aharonov, D. A Simple Proof that Toffoli and Hadamard are Quantum Universal. *eprint arXiv:quant-ph/0301040*, January 2003.

[AKG05] Aaronson, S., Kuperberg, G., y Granade, C. The complexity zoo, 2005.

[AKS04] Agrawal, M., Kayal, N., y Saxena, N. PRIMES is in P. *Ann. Math. (2)*, 160(2):781–793, 2004.

[AL18] Albash, T., y Lidar, D. A. Adiabatic quantum computation. *Reviews of Modern Physics*, 90(1):015002, January 2018.

[Ami09] Amin, M. H. S. Consistency of the adiabatic theorem. *Phys. Rev. Lett.*, 102:220401, Jun 2009.

[AvK+04] Aharonov, D., van Dam, W., Kempe, J., Landau, Z., Lloyd, S., y Regev, O. Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation. *eprint arXiv:quant-ph/0405098*, May 2004.

[AW09] Aaronson, S., y Watrous, J. Closed timelike curves make quantum and classical computing equivalent. *Proceedings of the Royal Society of London Series A*, 465:631–647, February 2009.

[BB02] Brylinski, J.-L., y Brylinski, R. Universal quantum gates. In *Mathematics of Quantum Computation*, pages 117–134. Chapman and Hall/CRC, 2002.

[BBC+93] Bennett, C. H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., y Wootters, W. K. Teleporting an unknown quantum state via dual classical and epr channels, 1993.

[BBC+95] Barenco, A., Bennett, C., Cleve, R., Divincenzo, D., Margolus, N., Shor, P., Sleator, T., Smolin, J., y Weinfurter, H. Elementary gates for quantum computation. 52:3457–3467, November 1995.

[BCDP96] Beckman, D., Chari, A. N., Devabhaktuni, S., y Preskill, J. Efficient networks for quantum factoring. *Phys. Rev. A*, 54:1034–1063, Aug 1996.

[BCT+14] Bussières, F., Clausen, C., Tiranov, A., Korzh, B., Verma, V. B., Nam, S. W., Marsili, F., Ferrier, A., Goldner, P., Herrmann, H., Silberhorn, C., Sohler, W., Afzelius, M., y Gisin, N. Quantum teleportation from a telecom-wavelength photon to a solid-state quantum memory. *Nature Photonics*, 8:775–778, October 2014.

[Bea02] Beauregard, S. Circuit for Shor's algorithm using 2n+3 qubits. *eprint arXiv:quant-ph/0205095*, May 2002.

[BEKS17] Bezanson, J., Edelman, A., Karpinski, S., y Shah, V. B. Julia: A fresh approach to numerical computing. *SIAM review*, 59(1):65–98, 2017.

[Ben80] Benioff, P. The computer as a physical system: A microscopic quantum mechanical hamiltonian model of computers as represented by turing machines. *Journal of Statistical Physics*, 22(5):563–591, May 1980.

[Ber11] Bernstein, D. J. Post-quantum cryptography. In *Encyclopedia of Cryptography and Security*, pages 949–950. Springer, 2011.

[BF28] Born, M., y Fock, V. Beweis des adiabatensatzes. *Zeitschrift für Physik*, 51(3):165–180, Mar 1928.

[Bha13] Bhatia, R. *Matrix analysis*, volume 169. Springer Science & Business Media, 2013.

[BS08] Benenti, G., y Strini, G. Quantum simulation of the single-particle Schrödinger equation. *American Journal of Physics*, 76:657–662, July 2008.

[BV97] Bernstein, E., y Vazirani, U. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[BZ10] Brent, R. P., y Zimmermann, P. *Modern computer arithmetic*, volume 18. Cambridge University Press, 2010.

[CD05] Chakrabarti, B. K., y Das, A. *Quantum Annealing and Other Optimization Methods*. Lecture Notes in Physics 679. Springer-Verlag Berlin Heidelberg, 1 edition, 2005.

[Chu36] Church, A. An unsolvable problem of elementary number theory. *American journal of mathematics*, 58(2):345–363, 1936.

[CJL+16] Costello, C., Jao, D., Longa, P., Naehrig, M., Renes, J., y Urbanik, D. Efficient compression of sidh public keys. Cryptology ePrint Archive, Report 2016/963, 2016. `https://eprint.iacr.org/2016/963`.

[CT65] Cooley, J. W., y Tukey, J. W. An algorithm for the machine calculation of complex fourier series. *Mathematics of Computation*, 19(90):297–301, 1965.

[DB24] De Broglie, L. *Recherches sur la théorie des quanta*. PhD thesis, Migration-université en cours d'affectation, 1924.

[Deu85] Deutsch, D. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London Series A*, 400:97–117, July 1985.

[Deu89] Deutsch, D. E. Quantum computational networks. *Proc. R. Soc. Lond. A*, 425(1868):73–90, 1989.

[Deu98] Deutsch, D. *The fabric of reality*. Penguin UK, 1998.

[DG27] Davisson, C., y Germer, L. H. Diffraction of electrons by a crystal of nickel. *Physical review*, 30(6):705, 1927.

[DG15] DeWitt, B. S., y Graham, N. *The many worlds interpretation of quantum mechanics*. Princeton University Press, 2015.

[DLP93] Damgård, I., Landrock, P., y Pomerance, C. Average case error estimates for the strong probable prime test. *Mathematics of Computation*, 61(203):177–194, 1993.

[dlP06] de la Peña, L. *Introducción a la mecánica cuántica*. 2006.

[DM04] De Raedt, H., y Michielsen, K. Computational Methods for Simulating Quantum Computers. *eprint arXiv:quant-ph/0406210*, June 2004.

[dT11] de Falco, D., y Tamascelli, D. An introduction to quantum annealing. *ArXiv e-prints*, July 2011.

[EF04] Eastin, B., y Flammia, S. T. Q-circuit tutorial. *arXiv preprint quant-ph/0406003*, 2004.

[EPR35] Einstein, A., Podolsky, B., y Rosen, N. Can quantum-mechanical description of physical reality be considered complete? *Physical review*, 47(10):777, 1935.

[Eps12] Epstein, C. Adiabatic quantum computing: An overview. *Quantum Complexity Theory*, 6(845):26, 2012.

[Fey82] Feynman, R. P. Simulating physics with computers. *International journal of theoretical physics*, 21(6-7):467–488, 1982.

[Fey86] Feynman, R. P. Quantum mechanical computers. *Foundations of Physics*, 16(6):507–531, Jun 1986.

[FGG+09] Farhi, E., Goldstone, J., Gosset, D., Gutmann, S., Meyer, H. B., y Shor, P. Quantum Adiabatic Algorithms, Small Gaps, and Different Paths. *ArXiv e-prints*, September 2009.

[FGGS00] Farhi, E., Goldstone, J., Gutmann, S., y Sipser, M. Quantum Computation by Adiabatic Evolution. *eprint arXiv:quant-ph/0001106*, January 2000.

[FGS+94] Finnila, A., Gomez, M., Sebenik, C., Stenson, C., y Doll, J. Quantum annealing: A new method for minimizing multidimensional functions. *Chemical Physics Letters*, 219(5):343 – 348, 1994.

[FLS65] Feynman, R. P., Leighton, R. B., y Sands, M. *Lectures on Physics, vol. III*. Addison-Wesley Reading, MA, 1965.

[Fol95] Folland, G. B. *A course in abstract harmonic analysis*. CRC Press BOCA. Raton, Florida, 1995.

[FR99] Fortnow, L., y Rogers, J. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240 – 252, 1999.

[Gal12] Gallian, J. *Contemporary abstract algebra*. Nelson Education, 2012.

[GEdG13] Giannozzi, P., Ercolessi, F., y de Gironcoli, S. Numerical methods in quantum mechanics. *University of Udine*, 2013.

[Ger05] Gerjuoy, E. Shor's factoring algorithm and modern cryptography. An illustration of the capabilities inherent in quantum computers. *American Journal of Physics*, 73:521–540, June 2005.

[Gev18] Gevrey, M. Sur la nature analytique des solutions des équations aux dérivées partielles. premier mémoire. 35:129–190, 1918.

[GGABGS12] García González, P., Alvarellos Bermejo, J. E., y García Sanz, J. J. *Física Cuántica I*. Editorial UNED, 2012.

[GLRS15] Grassl, M., Langenberg, B., Roetteler, M., y Steinwandt, R. Applying Grover's algorithm to AES: quantum resource estimates. *ArXiv e-prints*, December 2015.

[Gro96] Grover, L. K. A fast quantum mechanical algorithm for database search. *eprint arXiv:quant-ph/9605043*, May 1996.

[HD91] Heavens, O. S., y Ditchburn, R. W. *Insight into optics*. 1991.

[Hof80] Hofstadter, D. R. *Gödel, Escher, Bach*. Vintage Books New York, 1980.

[Hog96] Hogarth, M. *Predictability, computability, and spacetime*. PhD thesis, University of Cambridge, 1996.

[HW+79] Hardy, G. H., Wright, E. M., et al. *An introduction to the theory of numbers*. Oxford university press, 1979.

[Irv03] Irving, R. S. *Integers, polynomials, and rings: a course in algebra*. Springer Science & Business Media, 2003.

[Jaf96] Jaffe, R. L. Supplementary notes on dirac notation, quantum states, etc. 1996.

[JDF11] Jao, D., y De Feo, L. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

[JRS07] Jansen, S., Ruskai, M.-B., y Seiler, R. Bounds for the adiabatic approximation with applications to quantum computation. *Journal of Mathematical Physics*, 48(10):102111–102111, October 2007.

[Kat50] Kato, T. On the adiabatic theorem of quantum mechanics. *Journal of the Physical Society of Japan*, 5(6):435–439, 1950.

[KB00] Kumar Pati, A., y Braunstein, S. L. Impossibility of deleting an unknown quantum state. *Nature*, 404:164–165, March 2000.

[Kie18] Kieu, T. D. A Factorisation Algorithm in Adiabatic Quantum Computation. *ArXiv e-prints*, August 2018.

[Kit97] Kitaev, A. Y. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191, 1997.

[Knu68a] Knuth, D. The art of computer programming 1: Fundamental algorithms. *MA: Addison-Wesley*, 30, 1968.

[Knu68b] Knuth, D. The art of computer programming 2: Seminumerical algorithms. *MA: Addison-Wesley*, 1968.

[Kre78] Kreyszig, E. *Introductory functional analysis with applications*, volume 1. wiley New York, 1978.

[KWHZ82] K. Wootters, W., y H. Zurek, W. A single quantum cannot be cloned. 299:802, 10 1982.

[LV18] Lee, J. D., y Venkatesan, R. Rigorous analysis of a randomised number field sieve. *Journal of Number Theory*, 187:92 – 159, 2018.

[Mes64] Messiah, A. *Quantum Mechanics [Vol 1-2]*. 1964.

[Meu16] Meuser, D. Number theory lecture notes. square roots of one (mod m). 2016.

[Mil76] Miller, G. L. Riemann's hypothesis and tests for primality. *Journal of Computer and System Sciences*, 13(3):300 – 317, 1976.

[Mon85] Montgomery, P. L. Modular multiplication without trial division. *Mathematics of Computation*, 44(170):519–521, 1985.

[NC02] Nielsen, M. A., y Chuang, I. Quantum computation and quantum information, 2002.

[Pap03] Papadimitriou, C. H. *Computational complexity*. John Wiley and Sons Ltd., 2003.

[PCP05] Pomerance, R., Crandall, R., y Pomerance, C. *Prime Numbers: A Computational Perspective*. Lecture notes in statistics. Springer, 2005.

[PG12] Pavlidis, A., y Gizopoulos, D. Fast Quantum Modular Exponentiation Architecture for Shor's Factorization Algorithm. *ArXiv e-prints*, July 2012.

[Pre98] Preskill, J. *Lecture Notes: Quantum Information and Computation*. California Institute of Technology, 1998.

[PT04] Peres, A., y Terno, D. R. Quantum information and relativity theory. *Rev. Mod. Phys.*, 76:93–123, 2004.

[PZ03] Proos, J., y Zalka, C. Shor's discrete logarithm quantum algorithm for elliptic curves. *eprint arXiv:quant-ph/0301141*, January 2003.

[Rei96] Reif, F. *Física estadística*, volume 5. Reverté, 1996.

[RO15] Ryan O'Donnell, J. W. *Quantum Computation and Information. Lecture 23: Introduction to Quantum Complexity Theory.* Carnegie Mellon University, 2015.

[Ros03] Rosen, K. *Discrete Mathematics and Its Applications.* McGraw-Hill higher education. McGraw-Hill, 2003.

[RT18] Raz, R., y Tal, A. Oracle Separation of BQP and PH. 25:107, 2018.

[RXY+17] Ren, J.-G., Xu, P., Yong, H.-L., Zhang, L., Liao, S.-K., Yin, J., Liu, W.-Y., Cai, W.-Q., Yang, M., Li, L., Yang, K.-X., Han, X., Yao, Y.-Q., Li, J., Wu, H.-Y., Wan, S., Liu, L., Liu, D.-Q., Kuang, Y.-W., He, Z.-P., Shang, P., Guo, C., Zheng, R.-H., Tian, K., Zhu, Z.-C., Liu, N.-L., Lu, C.-Y., Shu, R., Chen, Y.-A., Peng, C.-Z., Wang, J.-Y., y Pan, J.-W. Ground-to-satellite quantum teleportation. *Nature*, 549:70–73, September 2017.

[Sch07] Schuster, A. *Intelligent Computing Everywhere.* 2007.

[Shi02] Shi, Y. Both Toffoli and Controlled-NOT need little help to do universal quantum computation. *eprint arXiv:quant-ph/0205115*, May 2002.

[Sho95] Shor, P. W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *eprint arXiv:quant-ph/9508027*, August 1995.

[Sho09] Shoup, V. *A computational introduction to number theory and algebra.* Cambridge university press, 2009.

[Sip06] Sipser, M. *Introduction to the Theory of Computation.* Thomson Course Technology Boston, 2006.

[SMCS08] Simon, R., Mukunda, N., Chaturvedi, S., y Srinivasan, V. Two elementary proofs of the Wigner theorem on symmetry in quantum mechanics. *Physics Letters A*, 372:6847–6852, November 2008.

[Tal17] Tal, A. Tight bounds on the fourier spectrum of ac0. In *LIPIcs-Leibniz International Proceedings in Informatics*, volume 79. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2017.

[Tes98] Teschl, G. Topics in real and functional analysis. *unpublished, available online at http://www. mat. univie. ac. at/˜ gerald*, 1998.

[Tur37] Turing, A. M. On computable numbers, with an application to the entscheidungsproblem. *Proceedings of the London mathematical society*, 2(1):230–265, 1937.

[Tus04] Tusarova, T. Quantum Complexity Classes. *eprint arXiv:cs/0409051*, September 2004.

[TW01] Tegmark, M., y Wheeler, J. A. 100 Years of the Quantum. *eprint arXiv:quant-ph/0101077*, January 2001.

[Vaz13] Vazirani, U. V. *BerkeleyX: CS191x Lecture Notes, Chapter 5.* University of California, Berkeley, 2013.

[Vig11] Vignat, C. A generalized Isserlis theorem for location mixtures of Gaussian random vectors. *ArXiv e-prints*, July 2011.

[vMV02] van Dam, W., Mosca, M., y Vazirani, U. How Powerful is Adiabatic Quantum Computation? *eprint arXiv:quant-ph/0206003*, May 2002.

[VN18] Von Neumann, J. *Mathematical Foundations of Quantum Mechanics: New Edition.* Princeton university press, 2018.

[Wai15] Wainwright, M. *Mathematical Statistics.* 2015.

[Wec14] Weckesser, W. Complex integration wrapper: odeintw. `https://github.com/WarrenWeckesser/odeintw`, 2014.

[Wha05] Whaley, B. *Phys191: Qubits, Quantum Mechanics, and Computers. No Cloning, Teleportation.* Berkeley Univesity, 2005.

[Wit14] Wittek, P. *Quantum Machine Learning : What Quantum Computing Means to Data Mining.* Elsevier Insights. Elsevier AP, Academic Press, 1 edition, 2014.

[XL95] Xi Lin, F. Shor's Algorithm and the Quantum Fourier Transform. 1995.

[YRL+12] Yin, J., Ren, J.-G., Lu, H., Cao, Y., Yong, H.-L., Wu, Y.-P., Liu, C., Liao, S.-K., Zhou, F., Jiang, Y., Cai, X.-D., Xu, P., Pan, G.-S., Jia, J.-J., Huang, Y.-M., Yin, H., Wang, J.-Y., Chen, Y.-A., Peng, C.-Z., y Pan, J.-W. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature*, 488:185–188, August 2012.

[Zwi96] Zwick, U. *Concrete Complexity: Lecture notes.*, volume 3. Tel Aviv University, 1996.

Índice alfabético

Índice de figuras

Índice de algoritmos