



COMPUTACIÓN CUÁNTICA: ESTUDIO TEÓRICO Y APLICACIÓN A LA FACTORIZACIÓN PRIMA.

Alberto García Planes

Tutora: Prof. María Antonia Cárdenas Viedma

Declaración de Originalidad

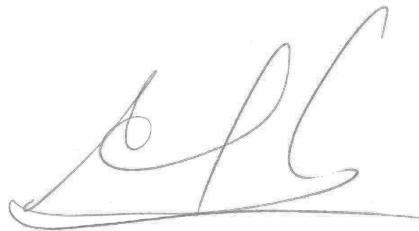
Alberto García Planes, autor del TFG titulado “Computación Cuántica: Estudio Teórico y Aplicación a la Factorización prima” bajo la tutela de la profesora **María Antonia Cárdenas Viedma**,

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 ** de 2018

Fdo.: Alberto García Planes

A handwritten signature in black ink, consisting of stylized, flowing letters that appear to be 'AGP'.

Resumen

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetur 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.

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.

Fusce consequat dignissim odio, eget congue dolor consequat in. Sed condimentum luctus imperdiet. Etiam vitae nulla convallis, vehicula libero eu, rhoncus sem. Donec nec elit at lorem interdum porta. Curabitur id augue euismod, euismod neque in, viverra turpis. Morbi pellentesque ullamcorper metus, ac luctus velit gravida non. Phasellus vel metus ac nunc feugiat suscipit. Nunc venenatis dolor quis augue viverra accumsan. Praesent sem eros, consequat rutrum nibh nec, placerat ultricies augue. Morbi suscipit molestie dictum.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Nam vehicula sed tellus sed egestas. Curabitur malesuada lorem at nibh mollis ultrices. Quisque eu cursus ligula. Curabitur feugiat justo leo, in tincidunt eros imperdiet ut. Phasellus facilisis, leo non ornare finibus, elit lectus vehicula turpis, ac volutpat felis lacus id nulla. Nullam ac tortor ac leo condimentum finibus sit amet eget nunc. Nulla commodo sit amet est a ornare. Vestibulum mi neque, tempor quis ornare in, viverra eu massa. Maecenas aliquet

ullamcorper rhoncus. Maecenas venenatis est vitae elit eleifend, quis malesuada sem consectetur.

Vestibulum feugiat hendrerit tellus, ut mattis tortor rutrum vel. Vivamus risus neque, ornare vel orci ac, blandit tristique massa. Nulla non velit varius, pretium erat non, suscipit tortor. Nunc eu laoreet purus. Vivamus ligula nibh, efficitur non rutrum vel, facilisis quis felis. Cras est lectus, vulputate eget augue non, commodo convallis arcu. Nam aliquet augue sapien, eget porttitor neque rhoncus eget. Donec mattis nibh ac tortor pharetra dictum. Integer et nibh et felis pellentesque sollicitudin ut sed orci. Aenean molestie pharetra felis, pulvinar dictum magna malesuada eu. Phasellus diam velit, aliquet sed euismod ac, mattis vel mi. Nunc interdum scelerisque eros quis ullamcorper. Proin justo erat, facilisis ac erat at, aliquet lacinia dui. Quisque imperdiet dolor id ligula aliquet, et sollicitudin augue fermentum.

In pulvinar, lorem nec imperdiet efficitur, augue dolor finibus ante, in varius erat erat at urna. Donec posuere tincidunt pretium. Proin non feugiat orci. Nunc quis tellus sagittis, laoreet lacus quis, hendrerit ligula. Cras facilisis sapien eget dolor tempor sodales. Sed ut odio sed enim elementum feugiat. Aliquam luctus orci non nisl hendrerit maximus. Praesent elementum turpis sed nulla condimentum, id sollicitudin nibh feugiat. Aliquam dictum sollicitudin metus, a hendrerit libero placerat eget. Proin eleifend interdum sapien, id dapibus enim suscipit eu. Vestibulum lacinia vitae ipsum vel hendrerit. Nunc non leo ac quam fermentum fermentum. Sed vitae gravida sem, a scelerisque urna. Cras ultricies ultricies magna et sollicitudin. Etiam eget nulla nec nunc placerat malesuada ac a lacus. Nunc in mauris lacus.

Maecenas iaculis augue at blandit consectetur. Donec a lectus condimentum, tristique lorem et, ullamcorper mi. Ut vitae sem id est ullamcorper condimentum. Donec ullamcorper risus ligula, ullamcorper pellentesque dolor imperdiet vitae. Praesent vel purus eleifend, cursus augue sit amet, fermentum orci. Suspendisse elementum pretium risus eget porttitor. Nunc quis convallis lectus.

Nam non sapien non massa semper gravida ac eu ex. Proin leo ligula, tempus eget suscipit sit amet, faucibus id ipsum. Duis pellentesque erat euismod lacus hendrerit tempor. Suspendisse justo massa, fringilla ac porttitor vel, efficitur nec erat. Integer in arcu sit amet nibh tempor luctus eu a odio. Integer sed metus nisl. Suspendisse quis pretium tortor, eget tempor velit. Sed id velit ac enim ultrices efficitur ut quis turpis. Sed eget suscipit mauris. Vestibulum id diam in velit iaculis malesuada. Donec auctor nulla id efficitur fermentum. Vivamus rhoncus turpis nisi. Integer ultricies, diam at tempus semper, metus purus pellentesque elit, et euismod urna erat vitae nibh. Vestibulum consectetur, felis in tempor pulvinar, leo odio mattis est, sed euismod ligula massa nec purus.

Suspendisse id mi leo. Aliquam a lectus non justo efficitur dapibus. Quisque congue magna nec risus viverra, dignissim laoreet dui consequat. Donec elit tellus, vestibulum ut dictum eget, tristique ut odio. Vivamus mauris justo, lacinia a lectus viverra, semper condimentum ligula. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Nullam sapien purus, vehicula molestie mi sed, convallis ultricies nisl. Aliquam posuere nulla felis, vel hendrerit ligula dapibus at. Ut rutrum nunc purus, ac consectetur justo volutpat quis.

Praesent suscipit urna id efficitur scelerisque. Sed sit amet lacus vel dui laoreet mattis vel sit amet metus. Pellentesque ante lectus, ullamcorper in pulvinar ac, posuere nec nulla. Aenean a ex sed mauris elementum posuere. Cras sed massa a tellus tristique consequat in nec enim. Integer ut nunc neque. Sed mattis sapien vel ultricies lobortis. Sed vitae gravida nibh. Proin risus nisi, tristique vitae libero sed, sagittis mollis libero. Phasellus sodales risus nec pretium ultrices. Vivamus consequat sem non nibh tincidunt pellentesque. Pellentesque sollicitudin magna dictum accumsan auctor. Curabitur pellentesque dolor erat, id pulvinar nisi fermentum vehicula. Nam laoreet, dolor at hendrerit accumsan, magna augue tincidunt quam, nec posuere orci justo vitae arcu. Phasellus fringilla leo tellus, vel hendrerit ipsum vulputate ac.

Aliquam sit amet diam lorem. Phasellus hendrerit auctor ligula, at molestie eros. Phasellus at nibh sollicitudin, elementum lacus eu, blandit ante. Aenean nec congue dui. Suspendisse pulvinar lorem vel maximus aliquam. Fusce scelerisque blandit laoreet. Aenean aliquet lorem a augue tincidunt viverra. Donec vitae nunc ipsum. Proin consequat leo sed finibus ullamcorper. Vestibulum mollis at metus eu gravida.

Donec ullamcorper, lacus nec accumsan finibus, dolor tortor faucibus arcu, eu dignissim dolor mauris a turpis. Sed bibendum, elit in pretium finibus, leo nibh maximus ante, ac porta turpis nisl eget sem. Praesent auctor

ipsum ut est feugiat vehicula. Vestibulum faucibus aliquet purus in suscipit. Suspendisse ac turpis ut lorem lacinia sodales vel vel velit. Aenean id magna laoreet, feugiat dui vitae, accumsan ligula. Mauris sit amet feugiat erat.

Nunc ligula tellus, accumsan nec sapien ut, ultrices posuere orci. Curabitur ullamcorper, eros nec posuere rutrum, tortor sapien porttitor diam, in rhoncus est tellus ut diam. Aliquam erat volutpat. Cras venenatis dapibus efficitur. Nulla facilisi. Pellentesque congue, nunc vel volutpat finibus, diam nisl semper leo, consectetur laoreet sem urna in ex. Aliquam ac ullamcorper ante. Donec ac finibus nibh. Duis ut neque interdum, rhoncus arcu in, rutrum ipsum. Praesent vitae pretium velit. Ut leo ligula, imperdiet eget velit nec, faucibus vestibulum dui. Suspendisse ornare mauris faucibus tortor semper rhoncus. Praesent vel purus in nisl viverra placerat. In hac habitasse platea dictumst.

Praesent odio urna, fringilla a sem non, congue volutpat diam. Vivamus sed mauris sem. Aenean iaculis erat ornare finibus cursus. In hac habitasse platea dictumst. In at massa nec augue gravida lacinia. Praesent porta lacus vel nunc rhoncus consequat. Mauris a malesuada enim, in posuere velit. Morbi maximus lectus varius, placerat lacus ac, hendrerit dolor. In sed libero vehicula, molestie mi non, bibendum sapien. Ut a enim dictum, eleifend orci eu, tempor justo. Mauris pellentesque, ex ut commodo facilisis, libero lacus porttitor neque, vel ullamcorper tortor metus eu magna.

Quisque luctus ut mauris non ultrices. Nullam aliquet elit sit amet velit aliquam viverra. In quam ipsum, ornare a mattis ac, malesuada eget risus. Vestibulum viverra velit risus, sit amet imperdiet libero euismod nec. Integer id dui tempor, sagittis sem placerat, sodales diam. Pellentesque libero lacus, hendrerit at odio quis, mollis cursus metus. Aenean interdum, quam sed elementum rutrum, dolor magna ultricies sem, nec iaculis arcu dui vitae justo. Nullam a imperdiet nunc, ut mollis purus. Aenean et urna ornare, rhoncus eros et, pharetra enim. Sed a faucibus turpis. Integer mi nibh, tincidunt vel volutpat vitae, maximus vitae nisi.

Praesent malesuada posuere neque, ac volutpat diam ullamcorper sit amet. Suspendisse viverra eleifend congue. Phasellus euismod est quis condimentum dictum. Praesent tempus maximus nibh, quis feugiat libero. Nam pretium vestibulum aliquam. Donec eu pretium nibh. Sed vel mi vestibulum metus gravida malesuada. Aenean et lorem in arcu luctus mattis sed cursus ipsum. Curabitur porta est ac mollis condimentum. Vestibulum euismod tempor luctus. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Suspendisse sollicitudin sagittis tempor. Sed ex velit, feugiat quis ornare at, cursus quis elit. Etiam commodo leo in odio auctor, ullamcorper iaculis sapien ultricies. Cras condimentum est tellus, nec pretium diam luctus ut. Pellentesque dolor dui, blandit eget odio vel, elementum cursus arcu.

Donec tellus quam, congue rhoncus mi nec, eleifend venenatis dolor. Ut in odio mattis, dignissim nunc eget, interdum libero. Maecenas vehicula augue odio. Phasellus tincidunt turpis eget aliquet cursus. Nulla tellus lacus, laoreet eu sem non, molestie pulvinar tortor. Duis neque ligula, tincidunt ac accumsan et, elementum vitae leo. Duis malesuada justo in enim pellentesque, in sodales leo luctus. Sed efficitur, sem ut bibendum fermentum, urna elit iaculis turpis, nec aliquet felis elit sed massa.

Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Vestibulum cursus nisl ac pharetra dictum. Nam dapibus nisi ac commodo fringilla. Nam viverra tincidunt enim et posuere. Morbi quis tortor suscipit, consectetur elit in, consequat arcu. Morbi a felis placerat lectus luctus placerat. Vivamus a semper eros, sed fermentum velit. Sed eu congue nibh. Phasellus vestibulum diam egestas aliquam elementum. Vivamus mattis sodales leo, sed cursus metus tincidunt sit amet. Proin eu enim a mauris eleifend mattis et tempus risus. Fusce felis libero, lacinia eget imperdiet vitae, ultrices sit amet ipsum.

Integer malesuada tellus a elit accumsan, eu convallis felis placerat. Praesent euismod augue turpis. Fusce vulputate eros vitae nisl accumsan, in vestibulum mauris dignissim. Nunc ut sapien ornare magna ultricies vehicula. Cras ut dui sollicitudin, efficitur felis eget, laoreet metus. Maecenas in felis vel nisi fermentum scelerisque id non elit. Etiam libero nisi, tincidunt a luctus sit amet, volutpat sit amet eros. Aenean tellus mi, aliquam vel libero a, dapibus vehicula sem. Suspendisse cursus ipsum eget justo hendrerit, at bibendum felis pellentesque. Proin fringilla ipsum non aliquet mollis.

Integer non ornare augue. Nam vitae enim ultricies, mattis mauris sit amet, viverra dui. Phasellus diam

urna, vestibulum id vehicula id, dapibus sed massa. Pellentesque at enim quis magna malesuada placerat sed sit amet felis. Duis convallis massa vel turpis ultrices, vel varius nulla eleifend. Donec ac mollis felis. Ut tristique viverra iaculis. Vestibulum suscipit vestibulum metus, eu ullamcorper lectus. Nam condimentum lectus et diam accumsan dapibus. Suspendisse non diam faucibus, auctor tortor eu, rutrum ipsum. Nam tempor bibendum dapibus. Nulla est mi, aliquam vulputate cursus nec, interdum eu quam. Nullam blandit erat ipsum, eu.

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

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.

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 ??.

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 ??, 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 alejamos 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.

No fue este patrón descrito el que Young encontró tras realizar el experimento, sino algo más parecido al patrón de la figura ??, 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.

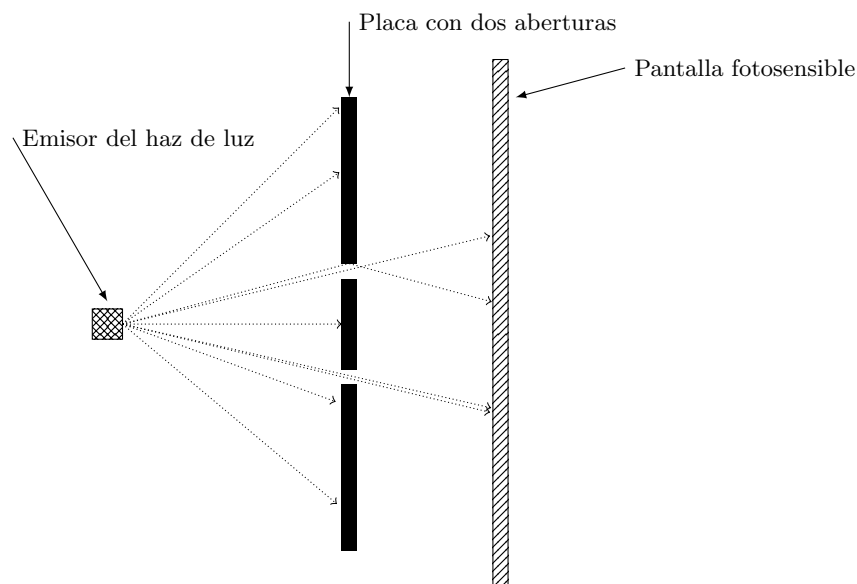


Figura 1.1.1: Vista cenital del modelo conceptual del experimento de Young.

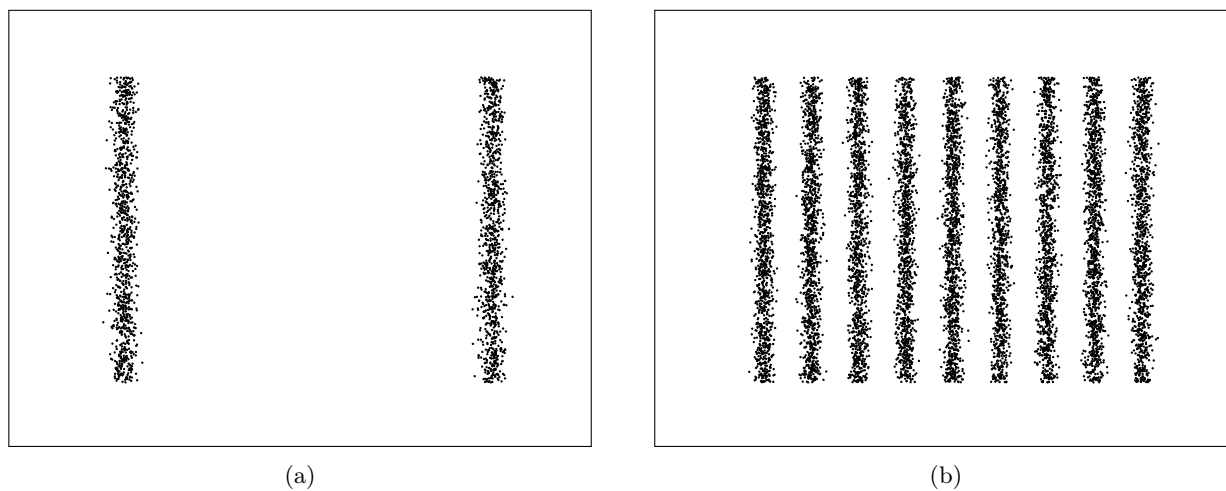


Figura 1.1.2: En la gráfica *a*), el patrón de incidencia en la pantalla fotosensible para un comportamiento corpuscular. En *b*), el esperado para el comportamiento ondulatorio.

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 (ver [?]), 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 (ver [?]) 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 existían 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 predictivo¹ como por su dificultad de interpretación.

Tanto es así que existen múltiples interpretaciones 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. Esta interpretación, 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 cuatro axiomas de la física cuántica, cuya formulación se da de una forma precisa en el apéndice ??, 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 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 Hilbert² contendrá todos los posibles estados del sistema. Por tanto, tal y como veremos 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, aunque menos relevante para los temas que tratamos en este trabajo a excepción de la sección ??, 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 (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) mediante lo que se conoce como la ecuación de Schrödinger.

El tercero de los postulados establece que...

Y por último, el cuarto postulado (que tendrá una importancia crucial en la sección ??) establece cómo se construyen los espacios de estados de sistemas formados por una combinación de sistemas más pequeños. Para ello usaremos un truco algebraico, que permite combinar estados sin una idiosincracia concreta 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.

¹Ya 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.

²Un 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 sucesión de Cauchy converge) bajo la norma inducida por $\|\cdot\| = \sqrt{\langle \cdot, \cdot \rangle}$

Computación Cuántica: una Introducción.

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

$$|\phi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (2.1.1)$$

¿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 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 este punto el lector puede preguntarse cuánta cantidad de información se está almacenando en un qubit. Dado que los coeficientes pueden tomar en principio (lo restringiremos más adelante) cualquier valor, podríamos

¹Elegimos 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.

decir que, debido a que podríamos codificar información como la expansión decimal de un número real, podríamos almacenar información arbitrariamente grande. Sin embargo la información almacenada no es obtenible en su totalidad y esto ocurre por el hecho de que **no es observable**. Si, una vez más, realizamos la analogía con el bit clásico, una medición del bit nos devolvería su estado y no modificaría de ninguna forma la información que este contiene. No es así en el qubit. Al medir un qubit **solamente podemos obtener un estado de la base** y los coeficientes α y β solamente nos indican cuál obtendremos, o mejor dicho, con qué probabilidad obtendremos cada uno de ellos.

Esto nos lleva a la interpretación probabilista de los coeficientes de la combinación lineal. 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 deben sumar 1.

Otra particularidad, de nuevo restrictiva, sobre el comportamiento de los qubits es que el hecho de medir la información que contienen 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 sobre los que se construye toda la teoría de la física 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.

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

$$|\phi_0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad (2.1.2)$$

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

$$|\phi_1\rangle = 0|0\rangle + 1|1\rangle \quad (2.1.3)$$

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. Bajos 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

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle \equiv \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \quad (2.1.4)$$

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 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

$$\left\{ \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix}, \begin{pmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{pmatrix} \right\} \quad (2.1.5)$$

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

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \quad (2.1.6)$$

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

$$\langle\begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \begin{pmatrix} \hat{\alpha} \\ \hat{\beta} \end{pmatrix}\rangle = \alpha^* \hat{\alpha} + \beta^* \hat{\beta} \quad (2.1.7)$$

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

$$\langle\phi|\psi\rangle \quad (2.1.8)$$

Y 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

$$\| |\phi\rangle \| = \sqrt{\langle\phi|\phi\rangle} \quad (2.1.9)$$

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

$$\langle\phi|\psi\rangle = 0 \quad (2.1.10)$$

y la condición de normalidad como

$$\| |\phi\rangle \| = 1 \quad (2.1.11)$$

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 qubit² 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, 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*

$$|\phi\rangle = e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right) \quad (2.1.12)$$

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

²Veamos que la definición es perfectamente compatible con el concepto de sistema cuántico, dada la analogía del postulado ?? de la mecánica cuántica. De hecho, este postulado es el que motivó esta definición para el qubit.

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

$$|\alpha| = \cos \hat{\theta}, \quad |\beta| = \sin \hat{\theta} \quad (2.1.13)$$

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

$$\alpha = e^{i\hat{\gamma}} \cos \hat{\theta} \quad (2.1.14)$$

y de la misma forma

$$\beta = e^{i\hat{\varphi}} \sin \hat{\theta} \quad (2.1.15)$$

Por lo que, usando ambas ecuaciones vemos que

$$|\phi\rangle = e^{i\hat{\gamma}} \cos \hat{\theta} |0\rangle + e^{i\hat{\varphi}} \sin \hat{\theta} |1\rangle = e^{i\hat{\gamma}} (\cos \hat{\theta} |0\rangle + e^{i(\hat{\varphi}-\hat{\gamma})} \sin \hat{\theta} |1\rangle) \quad (2.1.16)$$

Y, de una redefinición de índices, se sigue lo que queríamos demostrar. \square

Observación 2.1.4. El factor $e^{i\gamma}$ en la ecuación ?? no tiene efectos observables mediante medición.

2.2. Registros de n Qubits.

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

Por el postulado ?? parece que la forma natural de proceder es considerar el *producto tensorial* de todos los espacios \mathcal{H} de estados de un qubit³ 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 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 ?. 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

$$z(|\phi\rangle \otimes |\psi\rangle) = (z|\phi\rangle) \otimes |\psi\rangle = |\phi\rangle \otimes (z|\psi\rangle) \quad (2.2.1)$$

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

$$(|\phi\rangle + |\gamma\rangle) \otimes |\psi\rangle = |\phi\rangle \otimes |\psi\rangle + |\gamma\rangle \otimes |\psi\rangle \quad (2.2.2)$$

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

$$|\phi\rangle \otimes (|\psi\rangle + |\gamma\rangle) = |\phi\rangle \otimes |\psi\rangle + |\phi\rangle \otimes |\gamma\rangle \quad (2.2.3)$$

³Supondremos que todos los espacios de los qubits son iguales, pues no tenemos constancia de que se haya hecho de forma diferente en ninguna otra ocasión.

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

$$\{\underbrace{|00\cdots 0\rangle}_n, \dots, \underbrace{|11\cdots 1\rangle}_n\} \quad (2.2.4)$$

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 $\{0, \dots, 2^n - 1\}$ comúnmente denotaremos a tal base como $\{|0\rangle, \dots, |2^n - 1\rangle\}$.

Veamos ahora una serie particular de estados de \mathcal{H} que, como veremos en la sección ??, 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 [?]) son los siguientes*

$$\begin{aligned} \blacksquare |\Phi^+\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}; & \blacksquare |\Phi^-\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}}; \\ \blacksquare |\Psi^+\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}; & \blacksquare |\Psi^-\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}}; \end{aligned}$$

Observación 2.2.2 ($|\Phi^+\rangle$ es un estado entrelazado). *El par EPR $|\Phi^+\rangle$ 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 $|\Phi^+\rangle = |\phi\rangle \otimes |\psi\rangle$, en efecto esto se puede comprobar fácilmente comprobando que el sistema

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

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 indistintamente **puertas cuánticas** u **operadores cuánticos**.

Una de las propiedades de las puertas cuánticas, que se define axiomáticamente debido a los postulados de la física cuántica, es que cada uno de estos operadores debe actuar linealmente sobre el estado del qubit (o qubits) sobre el que actúe.

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

$$U|\phi\rangle = \sum_i \alpha_i U|i\rangle \quad (2.3.1)$$

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 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*

$$\begin{aligned} X|0\rangle &= |1\rangle \\ X|1\rangle &= |0\rangle \end{aligned} \quad (2.3.2)$$

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

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (2.3.3)$$

Actúa tal y como deseamos, pues

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

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

A esta matriz que aquí definimos la denotaremos la puerta NOT cuántica.

Pero esta no es la única restricción que debemos imponer a nuestras puertas cuánticas. Como ya vimos en la sección ??, 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. Los operadores (matrices) que satisfacen este requisito son las denominadas matrices unitarias, es decir, aquellas tales que

$$U^\dagger U = I \quad (2.3.5)$$

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

$$\langle U|x\rangle, |y\rangle\rangle = \langle |x\rangle, U^\dagger |y\rangle\rangle \quad \text{para estados cualesquiera } |x\rangle, |y\rangle \quad (2.3.6)$$

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

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (2.3.7)$$

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

Ejemplo 2.3.2. *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 $k \in \{0, \dots, 2^n - 1\}$.

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 $R_s |1\rangle = \exp\left(\frac{-2\pi i}{2^s}\right) |1\rangle$.

$$R_s := \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(\frac{-2\pi i}{2^s}\right) \end{pmatrix} \quad (2.3.8)$$

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

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} \quad B = \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1q} \\ b_{21} & b_{22} & \cdots & b_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ b_{p1} & b_{p2} & \cdots & b_{pq} \end{pmatrix} \quad (2.3.9)$$

entonces su producto tensorial $A \otimes B$ está definido en $\mathcal{H} \otimes \tilde{\mathcal{H}}$ y su representación matricial es la matriz de dimensiones $mp \times nq$

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix} \quad (2.3.10)$$

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 $A^{\otimes n}$.

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 ??.

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 ??.

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 [?] 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 no es posible a día de hoy excepto descomponiéndolas en puertas más pequeñas. El estudio teórico de ellas tampoco es simple a no ser

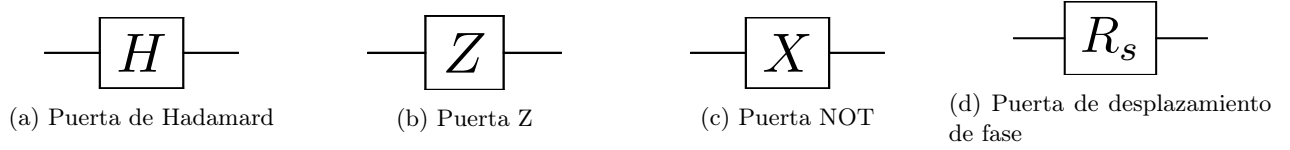


Figura 2.3.1: Representación de algunas de las puertas lógicas mencionadas para un solo qubit.

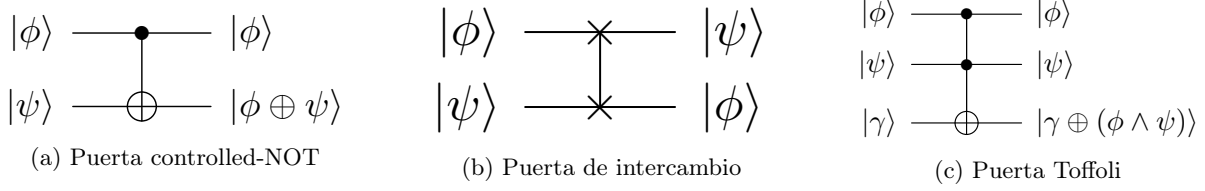


Figura 2.3.2: Representación de algunas de las puertas lógicas para múltiples qubit.

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 ??, como la acción sucesiva de ciertas puertas cuánticas actuando en un máximo de tres qubits.

Ejemplo 2.3.3 (Puertas cuánticas pequeñas o puertas cuánticas grandes). *Imaginemos que tenemos un registro de n qubits en el estado $|\varphi\rangle$ y queremos escribir el resultado de aplicar la función de Hadamard a cada uno de los qubits. Podríamos considerar, y consideraremos en el plano teórico, esta acción como un operador cuántico que es el producto tensorial de la puerta de Hadamard H consigo misma n veces que denotaremos como $H^{\otimes n} = \underbrace{H \otimes \cdots \otimes H}_n$ pues es más simple escribir $|\phi\rangle = H^{\otimes n} |\varphi\rangle$ que el hecho de indicar que la puerta de Hadamard se aplica sobre cada uno de los qubits, a pesar de que es así como se implementaría en un circuito físico.*

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 ??, se puede comprobar fácilmente que es unitaria y que su representación matricial viene dada por:

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (2.3.11)$$

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 ?? y su representación matricial es:

$$CCNOT = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad (2.3.12)$$

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 $a, b \in \{0, 1\}$*

$$CCNOT(|a\rangle|b\rangle|0\rangle) = |a\rangle|b\rangle|a \wedge b\rangle \quad (2.3.13)$$

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

$$OR(|\phi\rangle|\varphi\rangle|\psi\rangle) = X^{\otimes 3} \cdot CCNOT((X|\phi\rangle)(X|\varphi\rangle)|\psi\rangle) \quad (2.3.14)$$

o usando extensión podemos escribirla como

$$|\phi\rangle|\varphi\rangle|\psi\rangle \xrightarrow{\text{OR}} |\phi\rangle|\varphi\rangle|\neg(\psi \oplus (\neg\phi \wedge \neg\varphi))\rangle = |\phi\rangle|\varphi\rangle|\neg(\psi \oplus (\neg(\phi \vee \varphi)))\rangle \quad (2.3.15)$$

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

2.4. El operador de medición

3.1. 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, en el artículo [?], 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 [?], 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 3.1.1 (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 arbitrario¹.

Teorema 3.1.2 ($\{H, R_s, CCNOT\}$ 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, \dots, U_l de forma que si (i, j) son números menores o iguales que D se satisface

$$\left| U_{i,j} - (U_l \cdots U_1)_{i,j} \right| < \varepsilon \quad (3.1.1)$$

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 [?] y en [?], las puertas de Hadamard y Toffoli bastan. Esto es debido a la mencionada observación ?? por la cual podemos, grosso modo, despreciar los desplazamientos de

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

fase compleja común a los coeficientes de una superposición.

Definición 3.1.3. *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.*

3.2. 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 ??, 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 3.2.1 (Teorema de no clonación). *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*

$$U(|\phi\rangle |0\rangle) = e^{i\alpha(\phi,0)} |\phi\rangle |\phi\rangle \quad (3.2.1)$$

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

$$\begin{aligned} \langle\phi|\psi\rangle \langle 0|0\rangle &= \langle\phi| \langle 0|\psi\rangle |0\rangle = \langle\phi| \langle 0| U^\dagger U |\psi\rangle |0\rangle \\ &= e^{-i(\alpha(\phi,0)-\alpha(\psi,0))} \langle\phi| \langle\phi| \text{Id} |\psi\rangle |\psi\rangle \\ &= e^{-i(\alpha(\phi,0)-\alpha(\psi,0))} \langle\phi|\psi\rangle^2 \end{aligned} \quad (3.2.2)$$

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**. \square

Nota 3.2.2. *Una consecuencia interesante de la demostración anterior es que un computador cuántico **si** 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 $|i\rangle |0\rangle \rightarrow |i\rangle |i\rangle$. De hecho usaremos este tipo de operaciones más adelante en este trabajo.*

3.3. Teleportación Cuántica

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 astronautas 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 $|\Phi^+\rangle$, 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 ?? . 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 $|\phi\rangle$.²

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 $|\varphi_0\rangle = |\varphi\rangle |\Phi^+\rangle$ al registro inicial, usando la definición explícita que conocemos del par EPR obtenemos

$$|\varphi_0\rangle = \frac{1}{\sqrt{2}} \left(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle) \right) \quad (3.3.1)$$

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

$$|\varphi_1\rangle = \frac{1}{\sqrt{2}} \left(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle) \right) \quad (3.3.2)$$

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

$$|\varphi_2\rangle = \frac{1}{2} \left(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle) \right) \quad (3.3.3)$$

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

$$|\varphi_2\rangle = \frac{1}{2} \left(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle) \right) \quad (3.3.4)$$

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 ?? 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.³

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

$$|\varphi\rangle = \begin{cases} |\theta\rangle & \text{si } M_1 = 0, M_2 = 0 \\ X|\theta\rangle & \text{si } M_1 = 0, M_2 = 1 \\ Z|\theta\rangle & \text{si } M_1 = 1, M_2 = 0 \\ ZX|\theta\rangle & \text{si } M_1 = 1, M_2 = 1 \end{cases} \quad (3.3.5)$$

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

²Este 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.

³Esta 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.

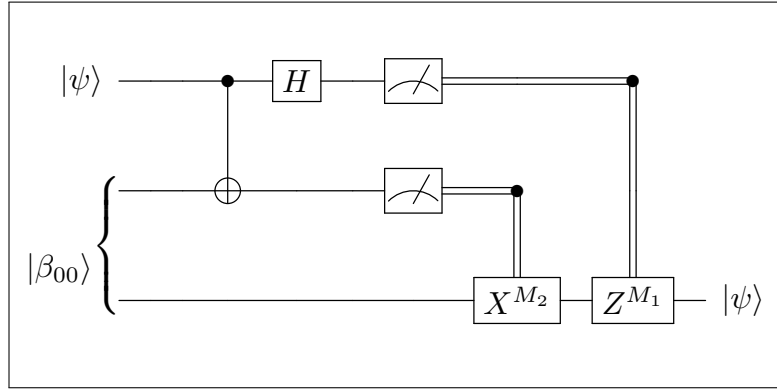


Figura 3.3.1: Circuito cuántico para la realización de la teleportación.

$$|\varphi\rangle = Z^{M_1} X^{M_2} |\theta\rangle \quad (3.3.6)$$

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*.

Factorización Prima.

Desde los orígenes de la computación una de las ramas más estudiadas en teoría algorítmica 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 múltiples 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 que hasta la fecha conocemos para factorización en computación clásica conocido como *GNFS* tiene un orden de ejecución sub-exponencial¹ (ver [?])

$$L_N \left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}} \right] \quad (4.0.1)$$

Sin embargo, fue en 1994 cuando Peter Shor mostró 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 4.0.1 (Algoritmo de Shor). *Existe un algoritmo cuántico que, dado un entero N , devuelve la factorización prima de N en un tiempo $\text{polylog}(N)$.*

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 algoritmo. Dado un número N , bastará demostrar que podremos encontrar un solo factor K en tiempo polilogarítmico², 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 [?] 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 ??, $A^{r/2} - 1$

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

² ¿Esta palabra existe?

compartirá un factor primo no trivial con N , que se podrá calcular con el simple algoritmo de Euclides (algoritmo ??) para el máximo común divisor, que es altamente eficiente.

Encontraremos por tanto un algoritmo en $\text{polylog}(N)$ 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 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 resultado de la QFT contenida en un estado cuántico no es medible en su completitud, sino 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.

Corolario 4.0.2. *El problema de la factorización prima pertenece a BQP.*

4.1. Preeliminaries: la Transformada de Fourier Cuántica en \mathbb{Z}_m .

Definición 4.1.1 (Transformada 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*

$$\hat{f}(j) = \frac{1}{\sqrt{M}} \sum_{k \in \mathbb{Z}_M} f(k) \exp\left(\frac{2\pi i}{M} jk\right) \quad (4.1.1)$$

Podemos dar en este punto una revisión del algoritmo clásico para calcular la transformada de Fourier, conocido como la *Fast Fourier Transform* (TTF) 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 algoritmo de la transformada cuántica seguirá una forma de proceder similar, veamos un resumen del algoritmo FFT.

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

$$\begin{aligned} \hat{f}(j) &= \frac{1}{\sqrt{M}} \sum_{k \in \mathbb{Z}_M} f(k) \zeta^{jk} \\ &= \frac{1}{\sqrt{M}} \sum_{k=0}^{N/2-1} \zeta^{-2kj} f_{\text{par}}(k) + \frac{1}{\sqrt{M}} \sum_{k=0}^{N/2-1} \zeta^{-j(2k+1)} f_{\text{impar}}(k) \\ &= \frac{1}{\sqrt{M}} \sum_{k=0}^{N/2-1} \zeta^{-2kj} f_{\text{par}}(k) + \frac{\zeta^{-j}}{\sqrt{M}} \sum_{k=0}^{N/2-1} \zeta^{-2jk} f_{\text{impar}}(k) \\ &= \frac{1}{\sqrt{2}} \left(\frac{1}{\sqrt{M/2}} \sum_{k=0}^{N/2-1} \zeta^{-2kj} f_{\text{par}}(k) + \frac{\zeta^{-j}}{\sqrt{M/2}} \sum_{k=0}^{N/2-1} \zeta^{-2jk} f_{\text{impar}}(k) \right) \\ &= \frac{1}{\sqrt{2}} \left(\hat{f}_{\text{par}}(j) + \zeta^{-j} \hat{f}_{\text{impar}}(j) \right) \end{aligned} \quad (4.1.2)$$

Así pues obtenemos, usando el hecho de que³ $\zeta^{M/2+j} = -\zeta^j$ y $\zeta^{M+j} = \zeta^j$

³Se sigue directamente de la identidad de Euler $e^{xi} = \cos x + i \sin x$ y de la periodicidad de las funciones trigonométricas.

$$\sqrt{2}\hat{f}(j) = \begin{cases} \hat{f}_{\text{par}} + \zeta^{-j}\hat{f}_{\text{impar}} & \text{si } 0 \leq j \leq M/2 - 1 \\ \hat{f}_{\text{par}} - \zeta^{-j}\hat{f}_{\text{impar}} & \text{si } M/2 \leq j \leq M - 1 \end{cases} \quad (4.1.3)$$

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 4.1.2 (Transformada de Fourier cuántica en \mathbb{Z}_M (QFT)). Sea $\{|0\rangle, \dots, |M-1\rangle\}$ una base ortonormal de un sistema cuántico y sea $|\varphi\rangle = \sum_{j=0}^{M-1} \alpha_j |j\rangle$ un estado cuántico. La **transformada de Fourier cuántica** F_M es una operación definida por

$$|\varphi\rangle = \sum_{j=0}^{M-1} \alpha_j |j\rangle \rightarrow \sum_{j=0}^{M-1} \frac{\alpha_j}{\sqrt{M}} \sum_{k=0}^{M-1} \zeta^{-jk} |k\rangle \quad (4.1.4)$$

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

$$|j\rangle \rightarrow \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \zeta^{-jk} |k\rangle \quad (4.1.5)$$

Lema 4.1.3. El estado transformado de $|j\rangle$ se puede escribir como producto de qubits de la forma que sigue.

$$|j\rangle \rightarrow \frac{1}{\sqrt{M}} \left(|0\rangle + e^{-2\pi i(0 \cdot j_m)} |1\rangle \right) \otimes \dots \otimes \left(|0\rangle + e^{-2\pi i(0 \cdot j_1 \dots j_{m-1} j_m)} |1\rangle \right) \quad (4.1.6)$$

Donde

$$(0 \cdot j_1 \dots j_{m-1} j_m) := \sum_{i=1}^m j_i 2^{-i}, \quad m = \lceil \log_2(M) \rceil \quad (4.1.7)$$

Demostración. Si tomamos la expansión binaria de k , $k = (k_1 k_2 \dots k_m)_2$ podemos escribir, para un estado de la base $|j\rangle$

$$\begin{aligned} |j\rangle &\rightarrow \frac{1}{\sqrt{M}} \sum_{k=0}^{M-1} \zeta^{-jk} |k\rangle = \frac{1}{\sqrt{M}} \sum_{k_1, k_2, \dots, k_m \in \{0,1\}} \zeta^{-j \sum_{r=1}^m 2^{m-r} k_r} |k_1\rangle \otimes \dots \otimes |k_m\rangle \\ &= \frac{1}{\sqrt{M}} \sum_{k_1, k_2, \dots, k_m \in \{0,1\}} \bigotimes_{r=1}^m \zeta^{-j 2^{m-r} k_r} |k_r\rangle \\ &= \frac{1}{\sqrt{M}} \bigotimes_{r=1}^m \left(\sum_{k_r \in \{0,1\}} \zeta^{-j 2^{m-r} k_r} |k_r\rangle \right) = \frac{1}{\sqrt{M}} \bigotimes_{r=1}^m \left(|0\rangle + \zeta^{-j 2^{m-r}} |1\rangle \right) \\ &= \frac{1}{\sqrt{M}} \bigotimes_{r=1}^m \left(|0\rangle + e^{-\frac{2\pi i}{2^m} j 2^{m-r}} |1\rangle \right) = \frac{1}{\sqrt{M}} \bigotimes_{r=1}^m \left(|0\rangle + e^{-2\pi i j 2^{-r}} |1\rangle \right) \end{aligned} \quad (4.1.8)$$

Expandiendo el exponente j del *factor de rotación* mediante su representación binaria $j = (j_1 j_2 \dots j_m)_2 = \sum_{l=1}^m 2^{m-l} j_l$ podemos escribir la exponencial del último término como

$$\begin{aligned} \exp\left(-2\pi i \sum_{l=1}^m 2^{m-l} j_l / 2^r\right) &= \exp\left(-2\pi i \sum_{l=1}^m 2^{m-r-l} j_l\right) \\ &= \exp(-2\pi i (0.j_{m-r+1} j_{m-r+2} \cdots j_m)) \end{aligned} \quad (4.1.9)$$

Permitiéndonos escribir finalmente

$$|j\rangle \rightarrow \frac{1}{\sqrt{M}} \bigotimes_{r=1}^m \left(|0\rangle + \exp(-2\pi i (0.j_{m-r+1} j_{m-r+2} \cdots j_m)) |1\rangle \right) \quad (4.1.10)$$

Lo que completa la prueba. \square

Teorema 4.1.4 (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. Supongamos que nuestro estado de entrada es un estado base $|j\rangle = \bigotimes_{r=1}^m |j_r\rangle$. Apliquemos la operación de Hadamard al primer qubit, obteniendo

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i (0.j_1)} |1\rangle) \otimes |j_2\rangle \otimes \cdots \otimes |j_m\rangle \quad (4.1.11)$$

Si aplicamos en este punto la puerta R_2 , obtenemos

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i (0.j_1 j_2)} |1\rangle) \otimes |j_2\rangle \otimes \cdots \otimes |j_m\rangle \quad (4.1.12)$$

Y aplicando iterativamente las operaciones de rotación llegamos a

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i (0.j_1 j_2 \cdots j_m)} |1\rangle) \otimes |j_2\rangle \otimes \cdots \otimes |j_m\rangle \quad (4.1.13)$$

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

$$\frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i (0.j_1 j_2 \cdots j_m)} |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + e^{-2\pi i (0.j_2 \cdots j_m)} |1\rangle) \otimes \cdots \otimes |j_m\rangle \quad (4.1.14)$$

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

$$\frac{1}{\sqrt{2^m}}(|0\rangle + e^{-2\pi i (0.j_1 j_2 \cdots j_m)} |1\rangle) \otimes (|0\rangle + e^{-2\pi i (0.j_2 \cdots j_m)} |1\rangle) \otimes \cdots \otimes (|0\rangle + e^{-2\pi i (0.j_m)} |1\rangle) \quad (4.1.15)$$

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

$$m + \sum_{r=1}^m (r - 1) + \lfloor m/2 \rfloor \sim \frac{3m + (m - 1)m}{2} = O(m^2) \quad (4.1.16)$$

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. \square

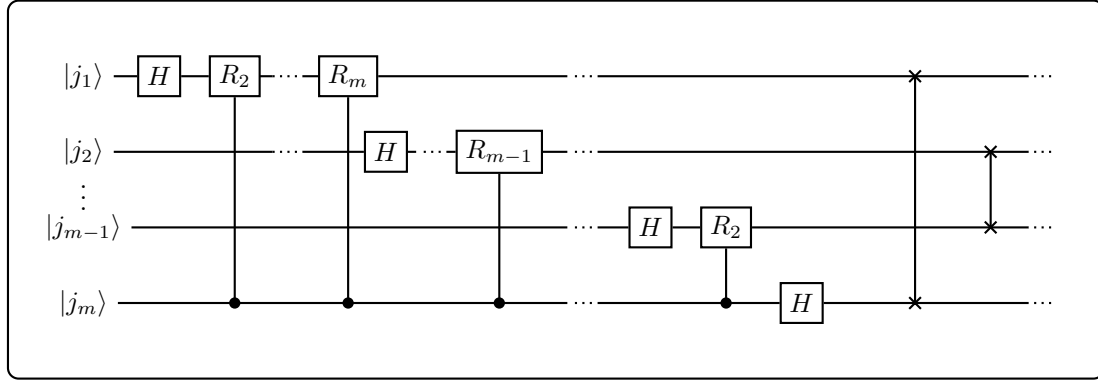


Figura 4.1.1: Circuito cuántico para el algoritmo QFT.

Observación 4.1.5. 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 sucesiva de operadores Hadamard.

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

$$|0\rangle \rightarrow \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} \zeta^{-0x} |x\rangle = \frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle \quad (4.1.17)$$

□

4.2. Algoritmo de Shor

4.2.1. Búsqueda del Orden.

Teorema 4.2.1. Existe un algoritmo cuántico que se ejecuta en tiempo polilogarítmico⁴ que, dada una entrada binaria (A, N) encuentra el menor r tal que $A^r \equiv 1 \pmod{N}$.

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 4.2.2. La función $x \rightarrow A^x \pmod{N}$ puede computarse en tiempo $\text{polylog}(N)$ en un circuito cuántico.

Demostración. De hecho esta computación se puede realizar únicamente con un circuito clásico. Si demostramos esta afirmación habremos demostrado (las equivalencias entre circuitos booleanos y cuánticos se verán en el teorema del anexo ??, por ahora pedimos al lector que admita tal correspondencia de forma provisional) que existe un circuito booleano de tamaño polilogarítmico que la computará y, utilizando la inclusión de circuitos booleanos en cuánticos, que existirá por extensión un circuito booleano que realizará el algoritmo también de tamaño polilogarítmico. Elegiremos el algoritmo expuesto en [?] para exponenciación modular que presentamos a continuación y comprobaremos que, en efecto, se ejecuta en tiempo polinómico sobre $\log N$.

Podemos ver que el algoritmo presentado realiza $k = \log_2 x$ 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 [?]) se sigue que el algoritmo, como queríamos, se realiza en un tiempo $\text{polylog}(N)$. □

⁴Polinómico/polilogarítmico. Explicar toda eso.

Algoritmo 1 Algoritmo para exponenciación modular

```

1: procedure EXPONENCIACIÓNMODULAR( $A$ : entero,  $x = (x_{k-1}, \dots, x_0)_2$ : entero positivo,  $N$ : entero positivo)
2:    $u \leftarrow 1$ 
3:    $potencia \leftarrow A \bmod N$ 
4:   for  $i \leftarrow 1$  to  $k - 1$  do
5:     if  $x_i = 1$  then  $u \leftarrow (u \cdot potencia) \bmod N$ 
        $potencia \leftarrow (potencia \cdot potencia) \bmod N$ 
   return  $u$  ( $u = A^x \bmod N$ )

```

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

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 $n^2 \leq 2^m < 2n^2$. 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 el ejemplo ??, podemos cambiar el estado del primer m -registro a una superposición uniforme de la forma

$$\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle \otimes |0\rangle \quad (4.2.1)$$

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

$$\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} |x\rangle \otimes |A^x \pmod n\rangle \quad (4.2.2)$$

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

$$\frac{1}{\sqrt{2^m}} \sum_{x=0}^{2^m-1} (F_{2^m} |x\rangle) \otimes |A^x \pmod n\rangle = \frac{1}{2^m} \sum_{x,y=0}^{2^m-1} \zeta^{-xy} |y\rangle \otimes |A^x \pmod n\rangle \quad (4.2.3)$$

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

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 $|z\rangle |A^k \pmod n\rangle$ la probabilidad será

$$\left| \frac{1}{N} \langle z | \langle A^k \pmod n | \sum_{x,y=0}^{2^m-1} \zeta^{-xy} |y\rangle |A^x \pmod n\rangle \right|^2 = \left| \frac{1}{N} \sum_{A^x \equiv A^k \pmod n} \zeta^{-xz} \right|^2 \quad (4.2.4)$$

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 siempre⁵ será un múltiplo del orden r de A . Así pues, escribiendo $x = br + k$ tenemos

$$\left| \frac{1}{N} \sum_{b=0}^{\lfloor (2^m-k-1)/r \rfloor} \zeta^{-(br+k)z} \right|^2 = \left| \frac{1}{N} \sum_{b=0}^{\lfloor (2^m-k-1)/r \rfloor} \zeta^{-brz} \right|^2 \quad (4.2.5)$$

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

⁵Esto es sencillo de probar usando el resultado ?? del apéndice.

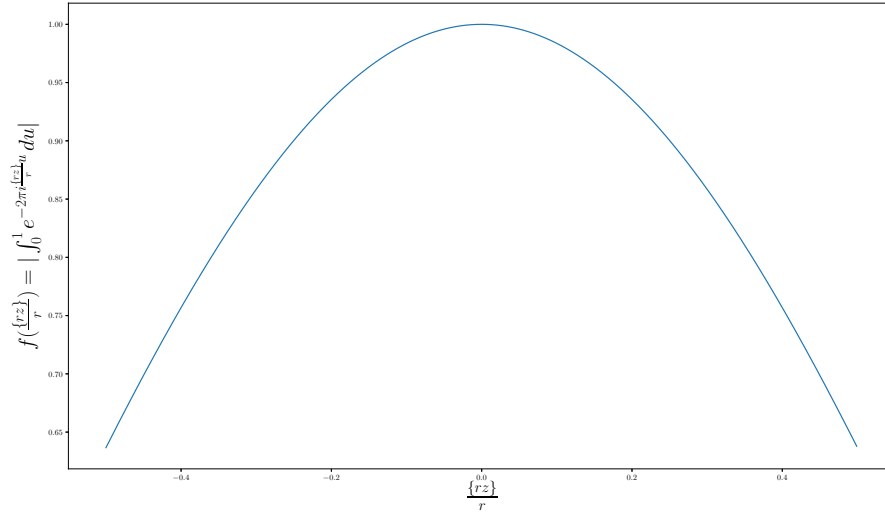


Figura 4.2.1: Módulo de la integral de la ecuación ?? para valores de $\frac{\{rz\}}{r}$ entre $-1/2$ y $1/2$.

$\zeta^i = \zeta^{2^m+i}$, así pues $\zeta^{-brz+2^m} = \zeta^{-brz}$. Esto nos motiva a definir $\{rz\}$ como el valor congruente con rz módulo 2^m tal que $-2^{m-1} \leq \{rz\} < 2^{m-1}$.

Aproximando⁶ el valor del sumatorio con una integral podemos escribir

$$\frac{1}{2^m} \sum_{b=0}^{\lfloor (2^m-k-1)/r \rfloor} \zeta^{-b\{rz\}} = \frac{1}{2^m} \int_{b=0}^{\lfloor (2^m-k-1)/r \rfloor} \zeta^{-b\{rz\}} db + \mathcal{O}(2^{-m}) \quad (4.2.6)$$

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

$$\frac{1}{r} \int_{u=0}^{\frac{r}{2^m} \lfloor (2^m-k-1)/r \rfloor} e^{-2\pi i u \{rz\}/r} du + \mathcal{O}(2^{-m}) \quad (4.2.7)$$

Como además $k < r$, podemos aproximar la cota superior de la integral por el valor 1 cometiendo⁷ tan solo un error $\mathcal{O}(2^{-m})$, obteniendo así el sumatorio como

$$\frac{1}{r} \int_{u=0}^1 e^{-2\pi i u \{rz\}/r} du + \mathcal{O}(2^{-m}) \quad (4.2.8)$$

Supongamos en este punto que $-\frac{1}{2} \leq \frac{\{rz\}}{r} < \frac{1}{2}$ (lo cual parece ciertamente más restrictivo que el rango de valores que podía tomar $\{rz\}$ por su definición) entonces podemos ver en la figura ?? que el valor de la integral para tales valores es mínimo para $\frac{\{rz\}}{r} = \pm \frac{1}{2}$, es decir, en los extremos. En cuyo caso la integral toma el valor $\pm \frac{2}{\pi r} + \mathcal{O}(2^{-m})$, cuyo signo no debe preocuparnos pues recordemos que estamos elevando este valor 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.

⁶Probar 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.

⁷El 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 $2^m \geq n^2 \geq n \geq r \geq k$.

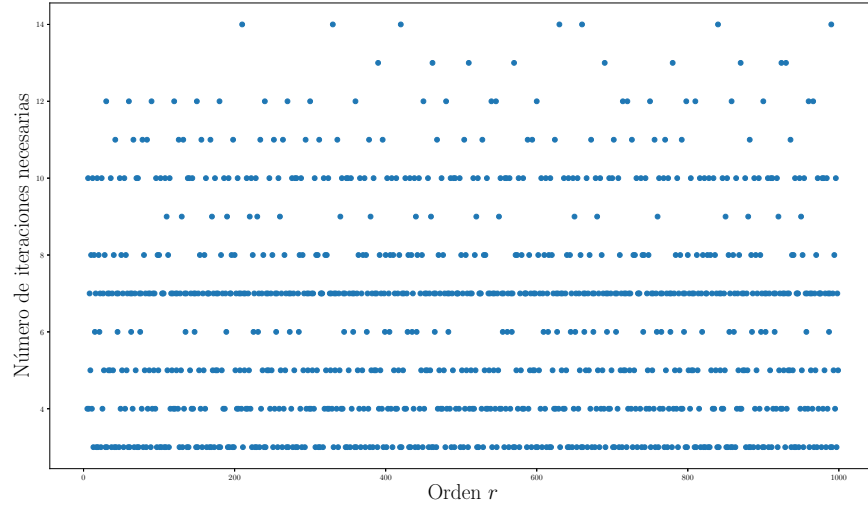


Figura 4.2.2: Iteraciones necesarias del algoritmo de la búsqueda del orden para que la probabilidad de encontrar el valor correcto de r sea mayor que $2/3$.

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

$$\frac{-r}{2} \leq \{rz\} < \frac{r}{2} \quad (4.2.9)$$

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

$$\frac{-r}{2} \leq rz - d2^m < \frac{r}{2} \quad (4.2.10)$$

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

$$\left| \frac{z}{2^m} - \frac{d}{r} \right| \leq \frac{1}{2^{m+1}} \quad (4.2.11)$$

Como al inicio de la explicación del algoritmo hemos elegido el valor m tal que $2^m \geq n^2$ tenemos que al menos existe una fracción d/r con $r < n$ que cumple la ecuación ???. El cómo obtener esta fracción es simple: básicamente intentaremos aproximar la fracción $\frac{z}{2^m}$ mediante la fracción más cercana con un denominador menor que n (recordemos que $r < n$), lo cual podemos realizar mediante la potente técnica (que se verá en la sección ??) de la expansión en fracciones continuas y, de hecho, una vez más esto lo podemos lograr en tiempo polilogarítmico.

Por qué.

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 último preguntarse el número de estados $|z\rangle |A^k \pmod n\rangle$ que nos permitirán calcular r de la forma mencionada.

Como existen $\phi(r)$ (ver definición ?? 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 ??) 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 [?], se tiene que $\frac{\phi(r)}{r} \approx \frac{1}{e^\gamma \log \log r}$ donde γ es la constante de Euler $0,57721 \dots$, lo que da una probabilidad más que aceptable 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 ??.

4.2.2. Relacionando Factorización con Búsqueda del Orden.

Lema 4.2.3. Para cada par de enteros n e y , con $y \leq n$, si $y^2 \equiv 1 \pmod{n}$ y además se cumple que $y \pmod{n} \notin \{+1, -1\}$ entonces $\gcd(y-1, n) \notin \{1, n\}$.

Demostración. Como $y^2 \equiv 1 \pmod{n}$ entonces n debe dividir a $y^2 - 1 = (y+1)(y-1)$ pero como $\gcd(y-1, n) \notin \{1, n\}$ 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 $\gcd(y-1, n) > 1$). Además como $y-1 < n$ entonces $\gcd(y-1, n) \leq y-1 < n$, lo que demuestra el lema. \square

Lema 4.2.4. Sea n un entero impar y sea $n = p_1^{e_1} \cdots p_k^{e_k}$ su factorización prima. Entonces la probabilidad de que un x aleatorio de $\{1, \dots, n-1\}$ 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. Por el Teorema Chino de los Restos (corolario ??), elegir un $x \in \mathbb{Z}_n^*$ aleatoriamente es equivalente a elegir $x_i \in \mathbb{Z}_{(p_i^{e_i})}^*$ para cada p_i aleatoriamente. Denotemos por r al orden de x y por r_i al orden de cada p_i . Como el orden de x es r , se tiene que

$$x^{r/2} \not\equiv 1 \pmod{n} \quad (4.2.12)$$

ya que por definición del orden no puede existir ninguna potencia de x con un exponente menor que r congruente con 1. Queremos demostrar que la probabilidad de que $x^{r/2} \equiv -1 \pmod{n}$ o de que r sea par es como máximo $(1/2)^{k-1}$.

Veamos primero la probabilidad para la condición de paridad del orden. Supongamos que r es impar, como por la proposición ??, se tiene que $r = \text{mcm}(r_1, \dots, r_k)$ entonces los r_i deberán tener todos orden impar, lo cual ocurre individualmente e independientemente con probabilidad menor o igual que $1/2$ (pues por el lema ?? al menos la mitad de los elementos del grupo tienen orden par), por lo que la probabilidad de que todos los órdenes sean impares es menor o igual que $(1/2)^k$.

Supongamos ahora que r es par, debemos ver cuál es la probabilidad de que $x^{r/2} \not\equiv -1 \pmod{n}$. Una vez más, por el Teorema Chino de los Restos, debe ser que para todos los $p_i^{e_i}$ se cumpla que $x^{r/2}$ sea congruente con ± 1 módulo $p_i^{e_i}$, lo cual ocurre con probabilidad 2^{-k+1} .

Combinando las probabilidades, obtenemos una probabilidad de éxito de al menos

$$(1 - 2^{-k})(1 - 2^{-k+1}) = 1 - 3 \cdot 2^{-k} + 2^{-2k+1} \geq 1 - 3 \cdot 2^{-k} \quad (4.2.13)$$

\square

4.2.3. Aproximación Racional de Números Reales.

Como hemos visto en la ecuación ??, en cierto momento del algoritmo de Shor queremos, dado un real $\frac{z}{2^m}$, aproximarlos por una fracción $\frac{d}{r}$ con el denominador acotado 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.

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}} \quad (4.2.14)$$

Dado un número real $\alpha > 0$, en el marco teórico, se puede calcular su expansión infinita 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

$$\alpha = \lfloor \alpha \rfloor + \frac{1}{R} \quad (4.2.15)$$

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

$$\lfloor \alpha \rfloor + \frac{1}{\lfloor R \rfloor + \frac{1}{R}} \quad (4.2.16)$$

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

Lema 4.2.5 ([?]). *En las condiciones anteriores*

- $p_0 = a_0, q_0 = 1$ y además $\forall n > 1, p_n = a_n p_{n-1} + p_{n-2}, q_n = a_n q_{n-1} + q_{n-2}$.
- $\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n-1}}{q_n q_{n-1}}$.

Y además se cumple que

$$\left| \frac{p_n}{q_n} - \alpha \right| < \frac{1}{q_n q_{n+1}} \quad (4.2.17)$$

Este último lema implica que $\frac{p_n}{q_n}$ es la fracción más cercana a α cuyo denominador no es superior a q_n . También podemos deducir que si $\frac{a}{b}$ es muy cercano a α , digamos, $\left| \alpha - \frac{a}{b} \right| < \frac{1}{4b^4}$ con a y b coprimos entonces podemos hallar a y b iterando usando el algoritmo de las fracciones continuas, de hecho, esto puede realizarse en $\text{polylog}(b)$ pasos. Veámoslo. Sea q_n el primer denominador de la serie tal que $q_{n+1} \geq b$ entonces la ecuación ?? implica que $\left| \frac{p_n}{q_n} - \alpha \right| < \frac{1}{2b^2}$. Pero esto implica que $\frac{p_n}{q_n} = \frac{a}{b}$ porque hay como máximo un número racional de denominador menor o igual que b que está tan cerca de α . Por otro lado, si $q_{n+1} \leq 2b^2$ entonces como $\frac{p_{n+1}}{q_{n+1}}$ está más cerca de α que $\frac{a}{b}$ entonces de nuevo $\frac{p_{n+1}}{q_{n+1}} = \frac{a}{b}$. No es difícil ver que $q_n \geq 2^{n/2}$, por lo que p_n y q_n pueden obtenerse en tiempo $\text{polylog}(q_n)$.

4.2.4. Algoritmo Explícito

Presentamos ahora una propuesta para un algoritmo cuántico de descomposición prima basado en la técnica que ya hemos propuesto, se puede ver el pseudocódigo en la figura para el algoritmo ??.

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*⁸ ([?]), 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* ([?]) 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 2 Algoritmo para hallar la factorización prima basado en Shor

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

```

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 ?? para obtener  $\frac{1}{\sqrt{2^m}} \sum_x |x\rangle|a^x \pmod{n}\rangle$ 
5:   Aplicar QFT al primer registro obteniendo  $\frac{1}{2^m} \sum_x \sum_y e^{2\pi i xy/2^m} |y\rangle|a^x \pmod{n}\rangle$ 
6:   Medir el primer registro, obteniendo el valor  $y$ .
7:   Convertir  $y/2^m$  a fracción irreducible y extraer el denominador  $r'$ .
8:   if  $a^{x+r'} \pmod{n} = a^x \pmod{n}$  then return  $r'$ 
9:   else return BúsquedaOrden( $a, m$ )
10: procedure SHOR( $n$ : entero)
11:   if esPrimo( $n$ ) then return  $\{n\}$ 
12:    $a \leftarrow$  entero (pseudo9-)aleatorio en el rango  $\{2, \dots, n-1\}$ 
13:    $d \leftarrow \text{mcd}(a, n)$ 
14:   if ( $d \neq 1$ ) then return  $\text{Shor}(n/d) \cup \text{Shor}(d)$ 
15:   else  $r \leftarrow \text{búsquedaOrden}(a, n)$ 
16:   if ( $r$  es impar) then return  $\text{Shor}(n)$ 
17:   else
18:     if  $a^{r/2} \not\equiv -1 \pmod{n}$  then return  $\text{Shor}(n)$ 
19:      $d \leftarrow \text{mcd}(a^{r/2} + 1, n)$ 
20:   return  $\text{Shor}(n/d) \cup \text{Shor}(d)$ 

```

4.2.5. Ejemplo de Ejecución del Algoritmo

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 $a \in \{2, \dots, 21-1\}$. Elegimos aleatoriamente el número 10. Calculamos $d = \text{mcd}(10, 21) = 1$. 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 ?? y aplicamos la QFT al primer registro, obteniendo así una superposición de $262144 = 512^2$ estados cuánticos de los cuales solamente tienen coeficientes no nulos los mostrados en la figura ??.

Podemos ver en la figura ?? incluida en el anexo 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

⁸La 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 Instituto Clay. No obstante se vio en el artículo [?] que el tiempo de ejecución experimental parece ser incluso mejor que el propuesto teóricamente.

⁹La elección podrá ser realmente aleatoria si esta parte del algoritmo se ejecuta sobre un ordenador cuántico. Si por el contrario solo ejecutamos la QFT de forma cuántica y esta parte se realiza sobre un computador clásico nos deberemos conformar con un entero pseudo-aleatorio, que funcionará perfectamente para nuestros propósitos.

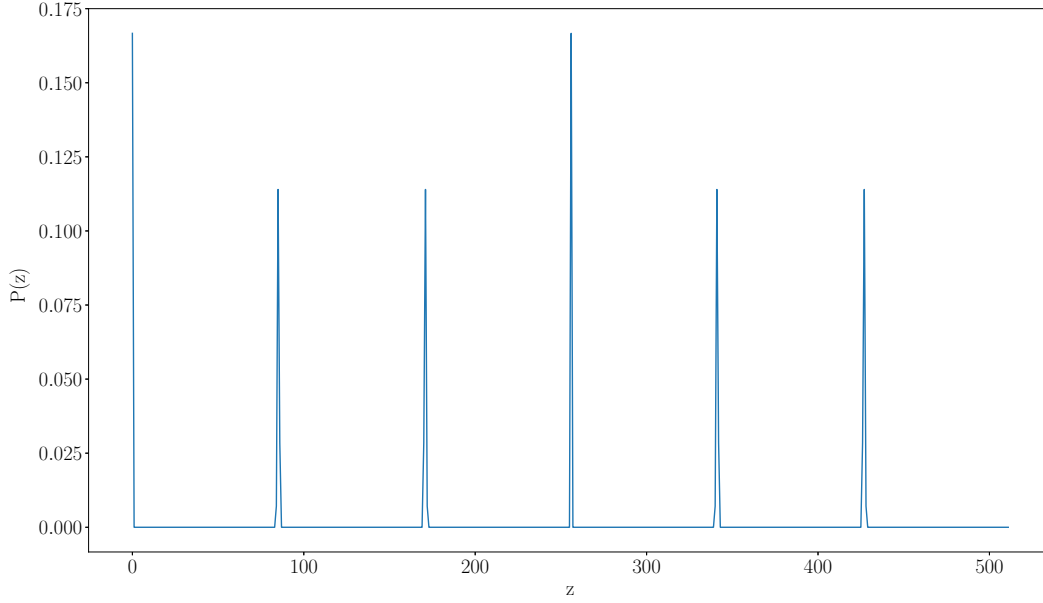


Figura 4.2.3: Probabilidades de obtener un valor z al medir el primer registro tras la QFT para $n = 21$ y $a = 10$.

también en la figura ?? 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

$$\left| \frac{427}{512} - \frac{d}{r} \right| \leq \frac{1}{1024} \quad (4.2.18)$$

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

$$0 + \frac{1}{5 + \frac{1}{42 + \frac{1}{2}}} \quad (4.2.19)$$

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

$$p_0 = a_0 = 0, \quad p_1 = 1, \quad p_2 = 5, \quad p_3 = 427, \quad \dots \quad (4.2.20)$$

$$q_0 = 1, \quad q_1 = 1, \quad q_2 = 6, \quad q_3 = 512, \quad \dots \quad (4.2.21)$$

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

Es fácil comprobar que $10^{6/2} \equiv 13 \pmod{21} \not\equiv -1 \pmod{21}$ por lo que podemos aplicar el lema ?? 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 $\gcd(12, 21) = 3$. 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 $\{3, 7\}$.

4.3. Factorización en Computación Cuántica Adiabática

...SECCIÓN EN PROGRESO...

4.3.1. Reducción de la Factorización a un Problema de Optimización

En agosto de 2018, Tien D. Kieu reformuló en [?] 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 $\mathbb{N} \times \mathbb{N}$

$$Q_N(x, y) \equiv N^2(N - xy)^2 + x(x - y)^2 \quad (4.3.1)$$

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 4.3.1. *La función $Q_N(x, y) : \mathbb{N}^2 \rightarrow \mathbb{Z}$ definida en ?? 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 ?? 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 decreciente¹⁰ con x . Por ello podemos escribir

$$\begin{aligned} Q_N(x, y)|_{N=xy} &= Q_N(x, N/x) \leq \max_{1 \leq x \leq \sqrt{N}} x(x - N/x)^2 \\ &\leq x(x - N/x)^2|_{x=1} \\ &\leq (N - 1)^2 \end{aligned} \quad (4.3.2)$$

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

$$Q_N(x, y)|_{xy \neq N} \geq N^2 + x(x - y)^2 \geq N^2 \quad (4.3.3)$$

Combinando las dos desigualdades obtenidas tenemos trivialmente que

$$Q_N(x, y)|_{N \neq xy} > Q_N(x, y)|_{N=xy} \quad (4.3.4)$$

Lo que completa la prueba. □

4.3.2. Elección de los hamiltonianos inicial y final

Usamos el H_0 de [?].

4.3.3. Resultados experimentales

4.4. ¿El Fin de RSA?

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 ejecución concretos para debatir si podríamos romper claves RSA en tiempo aceptable. Tal cota se da en la publicación [?], donde se da 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

¹⁰Se puede ver claramente comprobando que su derivada $3x^2 - \left(\frac{N}{x}\right)^2 - 2N$ es negativa para todo $x \in (0, \sqrt{N})$

cualquier momento del algoritmo. Se ha demostrado (ver [?]) que el algoritmo de Shor se puede implementar eficientemente en memoria, haciendo uso de tan solo $2 \log N + 3$ qubits.

Así pues, una clave RSA de 4096 bits¹¹ 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 $L_N \left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}} \right]$.

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 [?]) 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 [?]. 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 [?] 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 [?].

4.5. 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/albgo/TFGQuant.git>.

¹¹Elegimos tal tamaño pues las más utilizadas varían entre 1024 y 4096 bits en promedio. Realizaremos por tanto en análisis del caso más difícil.

CAPÍTULO 5

Conclusiones y Vías Futuras.

Apéndice

Postulados de la Mecánica Cuántica

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 [?], 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 los cuatro postulados más fundamentales para la teoría de la computación expuestos en [?].

Postulado A.0.1. *Cualquier sistema físico es 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 que luego establecen 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 A.0.2. *La evolución de un sistema cuántico cerrado viene determinada por un operador unitario dependiente del tiempo. Es decir, usando el término «hamiltoniano»¹ y la notación \hat{H} para tal matriz unitaria 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*

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

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

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

Postulado A.0.3. *Las mediciones cuánticas corresponden a una colección $\{M_m\}_m$ de operadores de medición. Estos operadores corresponden a operadores unitarios con dominio en el espacio de estados del sistema.*

Postulado A.0.4. *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.*

¹Este operador encapsula las energías cinética y potencial, por lo que encapsula, de forma que no veremos por contener la extensión del trabajo, la energía del estado.

APÉNDICE B

Teoría de Grupos

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

Definición B.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 B.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 B.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 $\text{mcd}(i, m) = 1$. 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

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

Definición B.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 B.0.6. Si G es un grupo conmutativo y $g = g_1 \cdots g_n \in G$ entonces $o(g) = \text{mcm}(o(g_1), \dots, o(g_n))$.

Definición B.0.7 (Isomorfismo). Una función $f : (G, \cdot_G) \rightarrow (G', \cdot_{G'})$ 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 B.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 B.0.9. Sea G un grupo y $g \in G$. Si $o(g) = r$ entonces la secuencia $\{1, g, g^2, \dots, g^{r-1}\}$ no contiene ninguna repetición.

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

$$f : R/(I_1 \cap \cdots \cap I_n) \rightarrow R/I_1 \times \cdots \times R/I_n \quad (\text{B.0.2})$$

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

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases} \quad (\text{B.0.3})$$

Lema B.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

$$(-x)^r = (-1)^r x^r = -1 \quad (\text{B.0.4})$$

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. \square

Teorema B.0.13 (Algoritmo de Euclides, [?]). Sean a, b pertenecientes a un dominio euclideo (en particular, a \mathbb{Z} o a \mathbb{Z}_n^*) podemos obtener un máximo común divisor de a y b mediante el algoritmo¹ siguiente

Algoritmo 3 Algoritmo de Euclides

```

1: procedure MCD( $a, b$ : enteros)
2:    $r_0 \leftarrow a$ 
3:    $r_1 \leftarrow b$ 
4:    $i \leftarrow 1$ 
5:   while  $r_i \neq 0$  do
6:      $r_{i+1} \leftarrow r_{i-1} \bmod r_i$ 
7:      $i \leftarrow i + 1$ 
   return  $r_{i-1}$ 

```

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

C.1. Los modelos de computación de Turing

Definición C.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**.
- $\delta : \Sigma \times Q \rightarrow \Sigma \times Q \times \{L, R\}$ es la **función de transición**.

Definición C.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*

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

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 .

C.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 mismo¹, 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 [?], es decir, que cualquier $f : \mathbb{Z} \rightarrow \mathbb{Z}$ 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 [?] y Alan Turing [?] independientemente a conjeturar la llamada hipótesis de Church-Turing, que, en palabras del propio Turing puede formularse como

Hipótesis C.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 [?] 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 [?], definiendo así el principio de Church-Turing como:

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

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 universal² \mathcal{Q} que veremos en la sección siguiente.

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

²También conocido como máquina de Turing cuántica.

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 ?? es que un sistema físico general no es simulable por una máquina de Turing universal, dado que sus estados forman un continuo³ 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.

C.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 C.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 $\delta : \Sigma \times Q \rightarrow H$ 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.

Definición C.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 .

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

Lema C.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 [?] □

Lema C.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 $f_U : H^{\otimes k} \rightarrow H^{\otimes k}$ definida en el espacio de Hilbert de estados de un registro de k qubits, tal función puede implementarse con una QTM . □

³Imaginemos 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

Proposición C.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. \square

Proposición C.4.4. Para cada entero positivo n y para cada QTM M con complejidad T existe un circuito con $\text{poly}(n, T)$ 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

$$U \left(|n, a_l, 0\rangle |q_1, a_1, 1\rangle |n, a_r, 0\rangle \right) = \sum_{a', q'} \delta(q, a, q', a', L) |q', a_l, 1\rangle |n, a', 0\rangle |n, a_r, 0\rangle + \delta(q, a, q', a', R) |n, a_l, 0\rangle |n, a', 0\rangle |q', a_r, 1\rangle \quad (\text{C.4.1})$$

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

$$\begin{aligned} & \langle s, a_{l1}, 0 | \langle q_1, a_1, 1 | \langle s, a_{r1}, 0 | U^\dagger U | s, a_{l2}, 0 \rangle | q_2, a_2, 1 \rangle | s, a_{r2}, 0 \rangle = \\ & \left(\sum_{a'_1, q'_1} \left\{ \delta(q_1, a_1, q'_1, a'_1, L) \langle q'_1 a_{l1}, 1 | \langle s, a'_{l1}, 0 | \langle s, a_{r1}, 0 | + \right. \right. \\ & \quad \left. \delta(q_1, a_1, q'_1, a'_1, R) \langle s, a_{l1}, 0 | \langle s, a'_{l1}, 0 | \langle q'_1, a_{r1}, 1 | \right\} \Big) \\ & \left(\sum_{a'_2, q'_2} \left\{ \delta(q_2, a_2, q'_2, a'_2, L) \langle q'_2 a_{l2}, 1 | \langle s, a'_{l2}, 0 | \langle s, a_{r2}, 0 | + \right. \right. \\ & \quad \left. \delta(q_2, a_2, q'_2, a'_2, R) \langle s, a_{l2}, 0 | \langle s, a'_{l2}, 0 | \langle q'_2, a_{r2}, 1 | \right\} \Big) = \\ & \sum_{a'_q, q'_1, a'_2, q'_2} \delta(q_1, a_1, q'_1, a'_1, L) \delta(q_2, a_2, q'_2, a'_2, L) \left(\right. \\ & \quad \left. \langle q'_1 a_{l1}, 1 | \langle s, a'_{l1}, 0 | \langle s, a_{r1}, 0 | \langle s, a_{r2}, 0 | \langle s, a'_{l2}, 0 | \langle q'_2 a_{l2}, 1 | \right) + \\ & \quad \delta(q_1, a_1, q'_1, a'_1, R) \delta(q_2, a_2, q'_2, a'_2, R) \left(\right. \\ & \quad \left. \langle s, a_{l1}, 0 | \langle s, a'_{l1}, 0 | \langle q'_1, a_{r1}, 1 | \langle q'_2, a_{r2}, 1 | \langle s, a'_{l2}, 0 | \langle s, a_{l2}, 0 | \right) \Big) = \\ & \delta_{a_{l2}}^{a_{l1}} \delta_{a_{r2}}^{a_{r1}} \left(\sum_{a'_1, q'_1} \delta(q_1, a_1, q'_1, a'_1, L) \delta(q_2, a_2, q'_2, a'_2, L) + \delta(q_1, a_1, q'_1, a'_1, R) \delta(q_2, a_2, q'_2, a'_2, R) \right) \\ & = 0 \end{aligned} \quad (\text{C.4.2})$$

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 ?? 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.1. Definiciones de la clase BQP.

Definición D.1.1 (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 ?? podemos definir la clase BQP usando circuitos cuánticos como sigue

Definición D.1.2 (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.2. 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.2.1. *Si $f : \{0,1\}^n \rightarrow \{0,1\}^m$ es computable por un circuito booleano de tamaño S , entonces existe una secuencia de $2S + m + n$ puertas cuánticas que computan la operación*¹

$$|x\rangle |0^{2m+S}\rangle \rightarrow |x\rangle |f(x)\rangle |0^{S+m}\rangle \quad (\text{D.2.1})$$

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 copia² 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

¹De dónde sale el n !!

²Blah blah ??.

corresponderían a la entrada de la función sino los $n + 2m + S$ qubits que necesitaremos para el circuito.

Si la entrada al circuito es $|x\rangle |0^{2m+S}\rangle$ el resultado del cómputo será $|x\rangle |f(x)0^m\rangle |z\rangle$, 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 $|bc\rangle \rightarrow |b(b \oplus c)\rangle$. 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. \square

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

Corolario D.2.2. $P \subseteq BQP$

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. \square

Corolario D.2.3. $BPP \subseteq BQP$

Demostración. Ver [?] \square

Podemos comprobar que al menos, la computación cuántica no es infinitamente más potente que la clásica:

Teorema D.2.4. $BQP \subseteq PSPACE$

Demostración. Ver [?] \square

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

1. $P \stackrel{?}{=} BQP$
2. $BPP \stackrel{?}{=} BQP$
3. $NP \stackrel{?}{=} BQP$
4. $PH \stackrel{?}{=} BQP$

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 $P^O = BQP^O$ ([?]) y $PH^{\tilde{O}} = BQP^{\tilde{O}}$ ([?]) tales que no colapsan la jerarquía, es decir, $P^O \neq NP^O$ y $P^{\tilde{O}} \neq NP^{\tilde{O}}$.

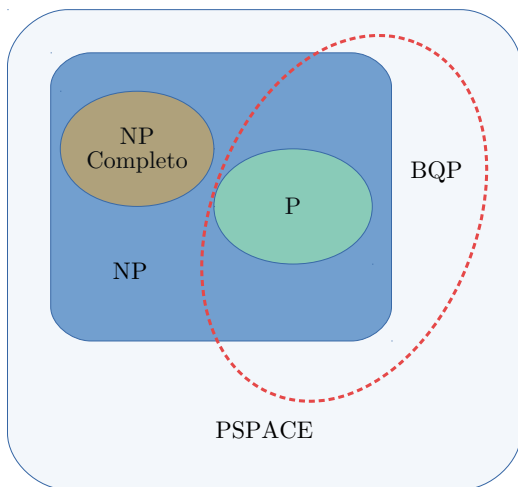


Figura D.2.1: Posible relación entre P , BQP , NP y $PSPACE$

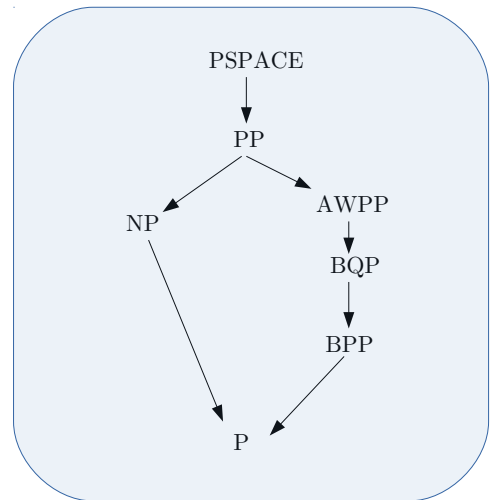


Figura D.2.2: Jerarquía de inclusión conocida para la clase BQP

E.1. Transformada de Fourier Cuántica

Teorema E.1.1. *La transformada de Fourier cuántica F_N es unitaria.*

Demostración.

$$\begin{aligned}
 F_N F_N^\dagger &= \frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \zeta^{-jk} |k\rangle \langle j| \sum_{r=0}^{N-1} \sum_{s=0}^{N-1} \zeta^{rs} |r\rangle \langle s| \\
 &= \frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \sum_{r=0}^{N-1} \sum_{s=0}^{N-1} \zeta^{rs-jk} |k\rangle \langle j| r\rangle \langle s| \\
 &\quad \text{(Aplicando la ortonormalidad de la base)} \\
 &= \frac{1}{N} \sum_{j=0}^{N-1} \sum_{k=0}^{N-1} \sum_{r=0}^{N-1} \sum_{s=0}^{N-1} \zeta^{rs-jk} \delta_j^r |k\rangle \langle s| \\
 &= \frac{1}{N} \sum_{k=0}^{N-1} \sum_{s=0}^{N-1} \left(\sum_{r=0}^{N-1} \zeta^{r(s-k)} \right) |k\rangle \langle s| \\
 &\quad \text{(Aplicando de nuevo la ortonormalidad)} \\
 &= \sum_{k=0}^{N-1} \sum_{s=0}^{N-1} \delta_k^s |k\rangle \langle s| \\
 &= \sum_{k=0}^{N-1} |k\rangle \langle k| \\
 &= I
 \end{aligned} \tag{E.1.1}$$

□

Computación Cuántica Adiabática

...SECCIÓN EN PROGRESO...

Sacado de [?]

Definición F.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 F.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

F.1. Evolución temporal de un sistema cuántico

F.2. Autovalores y autoestados

$[H_0, H_P] \neq$

F.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* ([?]) 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 [?]. 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 F.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 $s(t) : [0, t_f] \rightarrow [0, 1]$ 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 [?] los siguientes comentarios se realizan para la definición que acabamos de dar:

1. En [?] 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 ?? no es estrictamente necesaria, de hecho veremos que podemos considerar evoluciones más generales introduciendo un hamiltoniano intermedio que se anule en $s = 0, 1$.

F.3.1. Teoremas de la AQC

Versiones aproximadas

Sea $|\varepsilon_j(t)\rangle$ ($j \in \{0, 1, 2, \dots\}$) 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 $H(t)$. Asumimos 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 ([?]) 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

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

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 [?] una condición diferente usando el parámetro adimensional s

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

que podemos abreviar usando la notación

$$\Delta_{ij}(s) = \varepsilon_i(s) - \varepsilon_j(s) \quad (\text{F.3.3})$$

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 [?] 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 [?] conocida como la clase de Gevrey. Sin embargo, presentaremos en esta sección una versión del teorema dada en [?] 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 $P_{t_f}(s) = |\phi_{t_f}(s)\rangle \langle \phi_{t_f}(s)|$ el proyector sobre el estado del sistema en s . Los teoremas cuánticos adiabáticos comúnmente dan cotas para $\|P_{t_f}(s) - P(s)\|$.

Teorema F.3.2 ([?]). *Supongamos que el espectro de autovalores de $H(s)$ restringido a la proyección $P(s)$ consiste en $m(s)$ autovalores separados por un gap $\Delta(s)$ 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*

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

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

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

F.3.2. Caracterización de la complejidad

APÉNDICE G

Notas sobre la Realización Física de los Qubits

H.1. Resultado del Algoritmo QFT para $n = 21$, $a = 10$

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

Figura H.1.1: Probabilidades mayores que 10^{-3} de los estados de la superposición para la QFT con $n = 21$, $a = 10$.

- [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.
- [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⁺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.

- [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.
- [BR18] BUSQUÉ ROCA, C. *Grupos y Anillos. Notas de clase*. Universidad de Murcia, 2018.
- [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.
- [DG27] DAVISSON, C., Y GERMER, L. H. Diffraction of electrons by a crystal of nickel. *Physical review*, 30(6):705, 1927.
- [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.
- [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.
- [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.
- [FR99] FORTNOW, L., Y ROGERS, J. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240 – 252, 1999.
- [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.
- [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.
- [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.
- [Knu68] KNUTH, D. The art of computer programming 1: Fundamental algorithms. MA: Addison-Wesley, 30, 1968.
- [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.

- [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.
- [Pre98] PRESKILL, J. *Lecture Notes: Quantum Information and Computation*. California Institute of Technology, 1998.
- [PZ03] PROOS, J., Y ZALKA, C. Shor's discrete logarithm quantum algorithm for elliptic curves. *eprint arXiv:quant-ph/0301141*, January 2003.
- [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.
- [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.
- [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.
- [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.
- [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.
- [Zwi96] ZWICK, U. *Concrete Complexity: Lecture notes.*, volume 3. Tel Aviv University, 1996.

- Algoritmo de Euclides, 35
Algoritmo de Shor, 17
Búsqueda del orden, 21
Circuito universal, 13
Clase **BQP**, 41
Codificación superdensa, 14
El grupo \mathbb{Z}_m , 34
El grupo \mathbb{Z}_m^* , 34
Estado de Bell, 8
Exponenciación modular, 22
Fracción continua, 25
Función ϕ de Euler, 34
Grupo, 34
Hipótesis de Church-Turing, 37
Isomorfismo de grupos, 34
Máquina de Turing clásica determinista, 36
Máquina de Turing cuántica, 38
Máquina de Turing probabilista, 36
Matriz adjunta, 9
Operador cuántico, 8
Orden (grupo), 34
Par EPR, 8
Postulados de la Física Cuántica, 33
Principio de Church-Turing, 37
Producto de Kronecker, 10
Puerta H de Hadamard, 9
Puerta controlled-Not, 11
Puerta cuántica, 8
Puerta de desplazamiento de fase, 11
Puerta de Hadamard, 11
Puerta de intercambio, 11
Puerta NOT, 9, 11
Puerta NOT cuántica, 9
Puerta SWAP, 11
Puerta Toffoli, 11
Puerta Z, 11
Qubit, 6
Registro de qubits, 7
Simulación circuital, 38
Subgrupo, 34
Superposición, 4
Tamaño circuital, 14
Transformada de Fourier cuántica, 19
Transformada de Fourier discreta en \mathbb{Z}_M , 18
Teorema Chino de los Restos, 34
Teorema de no clonación, 14

Índice de figuras
