Universidad de Valladolid

Facultad de Ciencias

Trabajo Fin de Grado

Grado en Física

Circuitos cuánticos equivalentes para la generación de estados fotónicos entrelazados

Autor: Pablo Hervás García

Tutor/es: Mariano Santander Navarro, Juan Carlos García Escartín, Manuel Gadella Urquiza

Índice general

Introducción

La teoría cuántica tiene la reputación de ser una de las ramas más extrañas de la Física, hasta el punto de hacer materia de debate el estado de salud de un gato encerrado en una caja. No es de extrañar pues que muchos físicos cuestionaran inicialmente esta teoría, entre ellos el mismísimo Albert Einstein.
Pese a la controversia inicial, hoy en día la Mecánica Cuántica está bien aceptada y forma uno de los pilares fundamentales de la Física Moderna. En particular, a finales del siglo XX, surge la propuesta de aprovechar para computación los antaño paradójicos efectos cuánticos. Nace así el campo de la Computación Cuántica. Su interés radica en que permitirá realizar cálculos que no son posibles con ningún ordenador clásico.
En el fondo, el poder de los ordenadores cuánticos procede del fenómeno de entrelazamiento. Este es un recurso fundamental no tan solo en Computación Cuántica, sino también para otras áreas relacionadas como la Comunicación Cuántica y la Criptografía Cuántica. En particular, la única forma razonable de transmitir información cuántica es a base de fotones, pero resulta que entrelazar fotones es un problema notablemente difícil para el que se no existe ninguna solución plenamente satisfactoria.

Este Trabajo de Fin de Grado comienza con el estudio la teoría de Información Cuántica en el **Capítulo 1**. Ahí se explica la paradoja EPR junto a varios teoremas de imposibilidad en Mecánica Cuántica. Por el camino se señala la importancia del entrelazamiento y se introduce el concepto de qubit. En el **Capítulo 2** se proporciona una visión global de la Computación Cuántica en la actualidad. Su cubren tantos aspectos teóricos (como la descripción de varios algoritmos cuánticos), como aspectos prácticos de implementación (como los ordenadores cuánticos superconductores). Se hace especial énfasis en el modelo de circuito cuántico. Este énfasis continua en el **Capítulo 3**, que es una recopilación de equivalencias de circuitos cuánticos. Recogemos muchas reglas de la litaratura y añadimos alguna de nuestra cosecha. Para terminar, aplicamos todas las técnicas e ideas expuestas en los capítulos previos para proponer en el **Capítulo 4** una solución al problema del triple entrelazamiento remoto de fotones. Más específicamente, se producen los estados triplemente entrelazados $|GHZ\rangle$ y $|W\rangle$ mediante técnicas de teleportación, postselección y corrección aplicadas a pares de Bell obtenidos por conversión paramétrica.

Capítulo 1

Información cuántica

> If I were forced to sum up in one sentence what the Copenhagen interpretation says to me, it would be "Shut up and calculate!"
>
> *David Mermin*

El comienzo del siglo XX vino acompañado por una doble revolución en la Física: la Relatividad y la Mecánica Cuántica. Ambas ramas trajeron consigo una variedad de predicciones paradójicas, aunque se podría argumentar que este carácter paradójico es un reflejo de nuestra limitada intuición, acostumbrada al mundo clásico.
Durante ese mismo siglo surgió la Teoría de la Información. Por primera vez, se formalizó la noción tan familiar pero abstracta de "información". Esto trajo resultados importantes a campos tan diversos como los Códigos Correctores o la Mecánica Estadística.
Interesa pues extender esta herramienta tan potente al mundo cuántico: surge así el campo de la Información Cuántica. Este Capítulo no pretende en ningún caso ser una "Introducción a la Información Cuántica". En particular, se omiten muchas temas fundamentales, como la entropía de von Neumann, la cantidad de entrelazamiento, los sistemas abiertos, los canales cuánticos, la coherencia o las medidas generalizadas. Aún así, merece la pena exponer algunas de las ideas básicas de este campo, que sirven para ilustrar la extrañeza del mundo cuántico. Dichas ideas servirán como motivación durante el resto de este Trabajo.

1.1. Entrelazamiento

En Mecánica Cuántica, los estados de un sistema cuántico se representan en un espacio de Hilbert $\mathcal{H}$. Cuando se requiere describir conjuntamente dos sistemas A y B, resulta que no es suficiente considerar la suma directa de los espacios correspondientes, $\mathcal{H}_A \oplus \mathcal{H}_B$, sino que es necesario considerar el producto tensorial $\mathcal{H}_A \otimes \mathcal{H}_B$. Este es, matemáticamente hablando, el origen del entrelazamiento.
Se dice que un estado $|\Psi\rangle \in \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ está desacoplado o es separable si se puede escribir como producto tensorial $|\Psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle = |\psi_A\rangle\,|\psi_B\rangle$, donde $|\psi_A\rangle \in \mathcal{H}_A$ y $|\psi_B\rangle \in \mathcal{H}_B$. Como bien es sabido, una medida que proyecte el subsistema A con cierto proyector Π afecta al sistema conjunto como $\Pi \otimes \mathrm{Id}$, mientras que la evolución del subsistema A bajo cierto operador unitario U resultará en la aplicación de $U \otimes \mathrm{Id}$ en el sistema conjunto. En todo caso, lo que ocurra en el subsistema A no afecta al subsistema B y viceversa: el sistema conjunto se comporta como si los dos subsistemas fueran independientes.
Si, por el contrario, no es posible escribir $|\Psi\rangle$ como producto tensorial de un estado de $\mathcal{H}_A$ y otro de $\mathcal{H}_B$, se dice que el estado $|\Psi\rangle$ no es separable, está acoplado, o está entrelazado. En ocasiones

abusaremos de la notación y aplicaremos estos términos también a los subsistemas físicos A y B, en vez de a sus estados. Cuando estemos considerando más de dos sistemas físicos, será posible que el acomplamiento entre ellos exista, pero sea incompleto (por ejemplo, un sistema A está acoplado a otro B, pero ambos están desacoplados de un tercero C). Para distinguir esta situación, hablaremos de "acoplamiento parcial", frente al desacoplamiento o acoplamiento "completo" que definimos antes.

Se han propuesto diversas fórmulas para medir el grado de entrelazamiento entre varios sistemas cuánticos, y no todas son compatibles entre sí. Este tema alcanza mucho más allá de nuestros objetivos. Nosotros solo indicaremos que, para un sistema bipartito, su entrelazamiento es máximo si y solo si los operadores de densidad reducidos de cada subsistema son iguales a la identidad (normalizada). Este será el caso de los estados de Bell, que introduciremos más adelante.

Una vez definido matemáticamente, cabe preguntar cuál es el significado del entrelazamiento. Desde el punto de vista de la Física, los sistemas entrelazados son aquellos que no es posible describir por separado. Ilustremos esta afirmación con un experimento mental.

Imaginemos que tratamos con un sistema conjunto $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, y queremos medir un observable T_A en el subsistema A, y otro observable T_B en el subsistema B. Supongamos que la función de onda del estado conjunto es

$$|\Psi\rangle = \frac{1}{\sqrt{2}}[|\chi_1\rangle\,|\phi_1\rangle + |\chi_2\rangle\,|\phi_2\rangle],$$

donde $|\chi_1\rangle\,, |\chi_2\rangle \in \mathcal{H}_A$ son autovectores de T_A con autovalores λ_1 y λ_2 distintos, y $|\phi_1\rangle\,, |\phi_2\rangle \in \mathcal{H}_B$ son autovectores de T_B con autovalores μ_1 y μ_2 distintos. Si medimos T_B podemos obtener μ_1 o μ_2, ambos con probabilidad $1/2$.

Supongamos por el contrario que decidimos medir primero T_A. Ahora podemos obtener λ_1 o λ_2, también ambos con probabilidad $1/2$. Si obtenemos λ_1 el estado final queda como

$$\frac{1}{\sqrt{2}}[|\chi_1\rangle\,|\phi_1\rangle + |\chi_2\rangle\,|\phi_2\rangle] \mapsto |\chi_1\rangle\,|\phi_1\rangle\,,$$

mientras que si obtenemos λ_2, el estado final queda como

$$\frac{1}{\sqrt{2}}[|\chi_1\rangle\,|\phi_1\rangle + |\chi_2\rangle\,|\phi_2\rangle] \mapsto |\chi_2\rangle\,|\phi_2\rangle\,.$$

Tras medir T_A, ahora medimos T_B en el estado resultante. Si antes obtuvimos λ_1, ahora obtendremos μ_1 con probabilidad 1. Si antes obtuvimos λ_2, ahora obtendremos μ_2 con probabilidad 1. Recopilando:

- Si no medimos T_A: $P(\mu_1) = 1/2$, $P(\mu_2) = 1/2$.
- Si medimos T_A y obtenemos λ_1: $P(\mu_1) = 1$, $P(\mu_2) = 0$.
- Si medimos T_A y obtenemos λ_2: $P(\mu_1) = 0$, $P(\mu_2) = 1$.

Es decir, condicionado a lo que suceda en el subsistema A (medir o no, y que resultado obtenemos si medimos) cambian las estadísticas que observamos al medir en el subsistema B.

Esto es sorprendente, ya que no tiene por qué haber ningún tipo de contacto entre A y B. Incluso si, en un caso extremo, nos aseguramos de que los eventos "medir T_A" y "medir T_B" se encuentren cada uno fuera del cono de luz del otro (de esta forma, no puede haber relación causal entre ambos), se seguirá observando la correlación. Los resultados serán siempre (λ_1, μ_1) o (λ_2, μ_2).

Este fenómeno es a priori muy extraño, y, sin embargo, es una consecuencia inevitable de las leyes

de la Mecánica Cuántica. Con buen motivo, sembró las dudas en los físicos de la época sobre la veracidad de dichas leyes. El mismísmo Albert Einstein no estaba convencido, y bautizó este efecto como "spooky action at a distance". Sin embargo, no debemos temer al entrelazamiento. Como veremos, es una de las consecuencias más interesantes de la teoría cuántica.

1.2. Paradoja EPR

Como mencionamos en la sección anterior, el entrelazamiento fue sin duda la consecuencia menos intuitiva de la Mecánica Cuántica, por lo que atrajo gran controversia entre los físicos de la época. Albert Einstein, junto con los físicos Boris Podolsky y Nathan Rosen, objetaron en el famoso artículo [1] que la descripción proporcionada por la Mecánica Cuántica debía ser incompleta, utilizando el concepto de entrelazamiento para llegar a una aparente contradicción. En ese artículo se plantea un experimento mental: se considera un sistema de dos partículas separadas físicamente, pero cuyos estados están entrelazados. En particular, si bien al medir cada partícula podemos encontrar un rango de estados o de momentos, el centro de masas del conjunto es siempre x_0 y el momento total es siempre 0. Esto significa que si se mide la posición de la partícula 1 y se obtiene x_1, automáticamente sabemos que la posición de la partícula 2 es $x_2 = x_0 - x_1$ (en particular, la partícula 2 se encuentra en un estado que es autovector del operador X). Así mismo, si se mide el momento de la partícula 1 y se obtiene p, de forma inmediata deducimos que la partícula 2 tiene momento $-p$ (en particular, la partícula 2 se encuentra en un estado que es autovector del operador P).
Cabe en este momento contrastar con experimento mental que propusimos en la sección anterior. Para nuestro estado $|\Psi\rangle$, alguien podría pensar que en realidad siempre fue $|\Psi\rangle = |\chi_1\rangle\,|\phi_1\rangle$ o $|\Psi\rangle = |\chi_2\rangle\,|\phi_2\rangle$. Que las probabilidades de 1/2 que obteníamos, era la probabilidad de encontrar $|\Psi\rangle$ en cada uno de estos estados iniciales. Que, al medir, lo único que se logró fue averiguar en que estado inicial de los dos se encontraba del sistema.
Ahora ya no es posible esta interpretación errónea. El detalle crucial es que los operadores X y P no conmutan, $[X, P] = i\hbar$. En consecuencia, el estado de la partícula 2 no puede ser simultáneamente un autovector de X y un autovector de P. De qué operador sea autovector debe depender pues de cómo se decidió medir la partícula 1. Pero las partículas se encontraban bien separadas, y no parecía haber ninguna interacción entre ellas en el momento de la medida. La partícula 2 no podía saber lo que le ocurrió a la 1, para así cambiar su estado a un autovector de X o un autovector de P.
Ante tal (aparente) absurdo, los autores concluyeron que la descripción que da la Mecánica Cuántica del sistema no podía ser completa, que faltaba algo. En particular, Einstein argumentó que debe existir algún parámetro desconocido, una *variable oculta* asociada a cada partícula, que la Mecánica Cuántica no tenía en cuenta, y cuya inclusión explicaría los a priori paradójicos resultados.
Esta paradoja EPR (iniciales de los apellidos de los autores) se considera el argumento más contundente de Einstein en su rivalidad con Niels Bohr sobre la corrección de la Mecánica Cuántica y, naturalmente, recibió un extenso excrutinio durante las décadas posteriores. En particular, mencionamos que David Bohm propuso una variante de la paradoja que involucraba solo partículas de espín 1/2, lo cuál se relacionará posteriormente con la computación cuántica y los qubits.
La controversia fue analizada formalmente por John Stewart Bell en 1964 [2]. Bell planteó un estado concreto con dos partículas de spín 1/2 entrelazadas y calculó las correlaciones que uno esperaría obtener al medir sus espines según tres direcciones distintas. Notablemente, Bell proporcionó una desigualdad estricta entre las predicciones de la Mecánica Cuántica y las predicciones de cualquier teoría local de variables ocultas. Esta desigualdad fue generalizada en 1969 por John Clauser, Michael Horne, Abner Shimony y Richard Holt, en lo que se conoce como

la desigualdad CHSH [3]. Ambos resultados fueron cruciales para la resolución de la disputa, pues por primera vez era posible la diferenciación experimentalmente entre ambas teorías.
En las décadas posteriores se realizaron numerosos experimentos, en los que se comprobó que partículas entrelazadas adecuadamente podían violar la desigualdad CHSH [4]. Ante toda la evidencia experimental, el debate se ha cerrado en favor de Bohr.
En la formulación moderna, se llama *realismo local* a la idea de que los elementos de la realidad pertenecen a un punto concreto del espacio-tiempo y solo se ven influidos por lo que sucede en su cono de luz pasado. Es una idea muy razonable, y, sin embargo, como hemos visto:

La Mecánica Cuántica es incompatible con el realismo local.

1.3. Qubits

Se denomina qubit a cualquier sistema cuántico con solo dos estados ortogonales. Por supuesto, esta es una condición idealizada: incluso para un átomo de hidrógeno, que es un sistema relativamente simple, podemos encontrar muchos más estados ortogonales dependiendo de la energía, momento angular total, momentos angular orbital, etc. del electrón. En la realidad, nosotros simplemente supondremos que en el espacio de Hilbert total $\mathcal{H}$ se ha conseguido aislar un subespacio $\mathcal{H}_{qubit}$ de dimensión 2. Damos nombre a los vectores de una base del subespacio:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \qquad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Esta notación procede de la analogía con el bit clásico, que puede tomar valores 0 o 1. Esta analogía es también el origen del nombre de "qubit", *quantum bit*. En cierto sentido, si el bit es la unidad elemental de información clásica, el qubit es la unidad elemental de información cuántica.
Recordemos que cualquier otro estado $|\phi\rangle$ del qubit se puede representar como combinación lineal de $|0\rangle$ y $|1\rangle$:

$$|\phi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,\ \alpha, \beta \in \mathbb{C},$$
$$|\alpha|^2 + |\beta|^2 = 1 \text{ (condición de normalización).}$$

Adicionalmente establecemos que $|\phi\rangle$ y $e^{i\theta}\,|\phi\rangle$ representan el mismo estado, para cualquier fase $\theta \in [0, 2\pi)$. Esto refleja que la fase globar de un sistema cuántico "no tiene significado físico". De este modo, el conjunto de estados posibles de un qubit corresponde a la recta proyectiva compleja $\mathbb{PC}^1$. Geométricamente hablando, el estado de un qubit se representa sobre la esfera de Bloch:

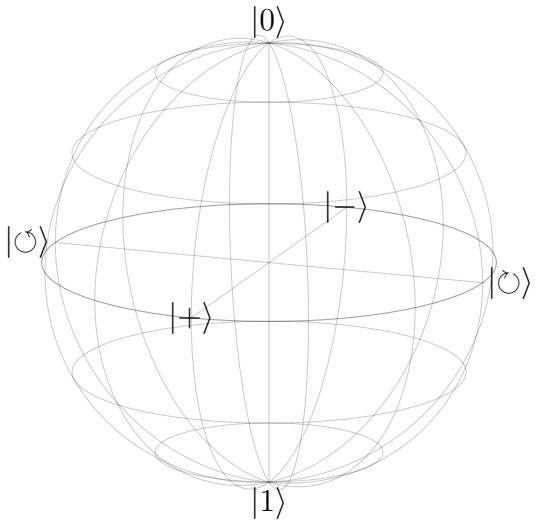


Figura 1.1:
Representación en 3 dimensiones reales de la esfera de Bloch, junto con algunos estados importantes (que definiremos más adelante). Es importante recordar que dos estados son ortogonoles si y solo son antipodales en la esfera.

La evolución de todo sistema cuántico viene regida por operadores unitarios. Para un solo qubit, cuando despreciamos la fase global, se puede comprobar que todo operator unitario se escribe como

$$U = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -e^{i\lambda}\sin\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) & e^{i(\phi+\lambda)}\cos\left(\frac{\theta}{2}\right) \end{bmatrix} \begin{cases} \theta \in [0,\pi], \\ \phi \in [0,2\pi), \\ \lambda \in [0,2\pi). \end{cases}$$

Las tres fases θ, ϕ, λ se denominan ángulos de Euler (en realidad se pueden considerar extendidos a todo $\mathbb{R}$, pero basta considerarlos en los rangos indicados). Como insinúa esta notación, cualquier operación unitaria sobre 1 qubit constituye una rotación de la esfera de Bloch.
Para terminar, conviene pararse a reflexionar entre la diferencia de los bits con los qubits. Un bit toma solo uno de dos valores, los del conjunto discreto $\{0,1\}$. Por otro lado, un qubit toma valores en $\mathbb{PC}^1$, un conjunto no numerable, pero si medimos en la base $\{|0\rangle, |1\rangle\}$ (o en cualquier otra base) nos seguimos quedando con solo uno de dos valores. Esto sigue ocurriendo cuando consideramos n bits o qubits: en ambos casos, solo hay 2^n resultados posibles al medir, y el no determinismo de la medida cuántica también podría ser un no determinismo en la preparación de los bits clásicos.
La ventaja de los qubits frente a los bits (es decir, del mundo cuántico frente al mundo clásico) se manifiesta pues durante la evolución, cuando se forman *estados entrelazados*.

1.4. Estados entrelazados

Para sistemas sencillos, como los formados por dos o tres qubits, es interesante clasificar los distintos tipos de estados entrelazados que pueden surgir. Para el propósito de esta clasificación, consideraremos que "se puede pasar de un estado a otro" cuando, mediante operaciones locales sobre los qubits y comunicación clásica, exista una estrategia que permita obtener el segundo estado a partir del primero. Si es posible pasar de un estado a otro en ambos sentidos, diremos que los estados "son equivalentes". Esta situación recibe el nombre de LOCC (Local Operations and Classical Communication). Si las estrategias anteriores solo funcionan con cierta probabilidad

menor que 1, diremos que estamos en la situación SLOCC (Stochastic LOCC) [5]. Esta sección se plantea para SLOCC.

1.4.1. Estados de Bell (dos qubits)

Para un sistema de dos qubits, existen dos clases de equivalencia: los estados separables, y los estados entrelazados. Los estados separables siempre se pueden obtener de forma determinista a partir de cualquier otro estado: basta preparar cada qubit en el estado que le corresponde. Sin embargo, un estado entrelazado solo puede obtenerse a partir de otro estado entrelazado, ya que no es posible producir entrelazamiento sin hacer interactuar los qubits. En ese sentido, los estados máximamente entrelazados cobran especial importancia, ya que a partir de ellos se puede obtener cualquier otro estado entrelazado de dos qubits de forma determinista [6].
Los llamados "estados de Bell" forman una base de estados máximamente entrelazados. Estos estados también se llaman "pares EPR", en honor a la paradoja que discutimos previamente. La notación más tradicional para estos estados es

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \qquad |\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}},$$
$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \qquad |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}.$$

Otro modo de escribir los estados de Bell es con la notación

$$|\beta_{ab}\rangle = \frac{|0b\rangle + (-1)^a\,|1\bar{b}\rangle}{\sqrt{2}}.$$

donde $\bar{b}$ representa la operación lógica NOT sobre el número binario b ($0 \mapsto 1$, $1 \mapsto 0$). Escritos de esta forma, se hace evidente que cualquier estado EPR se puede transformar en cualquier otro mediante operaciones locales *sobre solo uno de los qubits*. Este hecho será clave para la codificación superdensa en el **Capítulo 2**.
Los estados de Bell son los ejemplos más sencillos de entrelazamiento y, en consecuencia, presentan gran interés teórico y experimental. No será sorpresa pues que estos estados jueguen un papel fundamental en este Trabajo de Fin de Grado.

1.4.2. Estados GHZ y W (tres qubits)

Para tres qubits, se puede demostrar que existen dos familias no equivalentes de estados a partir de las cuales se pueden obtener el resto (pero esta vez, ya no de forma determinista)[6]. Proporcionamos un representante para cada familia:

- El estado GHZ (Greenberger-Horne-Zeilinger), dado por

$$|GHZ\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}.$$

- El estado W, dado por

$$|W\rangle = \frac{|100\rangle + |010\rangle + |001\rangle}{\sqrt{3}}.$$

Cada una a su manera, ambas clases de estados generalizan los estados de Bell. Los estados GHZ están "máximamente entrelazados". Los estados W poseen entrelazamiento "máximamente robusto". Para más detalles, consultar [6].
Por supuesto, ambos estados se pueden generalizar para un número arbitrario de qubits:

- Estado GHZ para n qubits

$$|GHZ_n\rangle = \frac{|000\ldots000\rangle + |111\ldots111\rangle}{\sqrt{2}}.$$

- Estado W para n qubits

$$|W_n\rangle = \frac{|100\ldots000\rangle + |010\ldots000\rangle + \ldots + |000\ldots010\rangle + |000\ldots001\rangle}{\sqrt{n}}.$$

Nosotros nos limitaremos a los estados GHZ y los estados W de tres qubits. Cobrarán un papel protagonista en el **Capítulo 4**.

1.5. Teoremas de imposibilidad

Pese a sus consecuencia contraintuitivas, la Mecánica Cuántica no es "magia" que permita cualquier posibilidad. Por el contrario, a lo largo de los años se ha recopilado una lista de resultados que recogen las varias limitaciones que impone esta teoría. Estos resultados reciben el nombre de teoremas de"no-go" y tienen una gran importancia teórica. En particular, nos ayudarán a poner en contexto algunos protocolos de comunicación que hacen uso del poder de la Mecánica Cuántica, como el protocolo de teleportación y la codificación superdensa.

1.5.1. No comunicación

Ya comprobamos cómo, si tenemos un estado entrelazado $|\Psi\rangle \in \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ y realizamos una medida sobre un subsistema A, todo el estado colapsa, también la parte correspondiente a B. Uno se podría imaginar que el cambio de la distribución de probabilidad que la medida de T_A provoca en la medida de T_B es, de algún modo, detectable. Si lo fuera, entonces podríamos comunicar "instantáneamente" información entre A y B, decidiendo medir o no un subsistema del sistema conjunto entrelazado. Pero las comunicaciones instantáneas violan la causalidad, lo cuál suele traer problemas (en películas de viajes temporales, sobre todo). Este es un motivo de peso para pensar que el esquema propuesto no puede realizarse.
Efectivamente, se puede demostrar que, haga lo que haga el observador que maneja el sistema A, en B se observarán siempre las mismas estadísticas (dicho de otro modo, no podrá recibir información alguna de A). De forma intuitiva: si bien el resultado que B medirá está ya determinado una vez que A realizó su medida, la clave consiste en que A no tiene forma de controlar que resultado obtendrá. Si bien cada observador conoce los resultados de que midió o medirá el otro nada más miden su propio subsistema, no se ha comunicado ninguna información.
En [7] se puede consultar una demostración de este Teorema con toda generalidad, que es sobre todo un ejercicio de no liarse con los índices al considerar matrices de densidad y trazas parciales. Nosotros nos limitaremos a presentar una analogía intuitiva. Imaginemos un par de monedas mágicas que se pueden lanzar solo una vez, y que están predestinadas a caer del mismo lado. Cuando B lanza su moneda, no sabe si A ya había lanzado la suya o no. Si bien la magia de las monedas le permite deducir al instante qué resultado corresponde a la moneda de A, esto no es ningún tipo de información. Desde su punto de vista, B simplemente ha lanzado una moneda y, ya sea por azar o por destino mágico, ha obtenido un resultado.

1.5.2. No teleportación

Imaginemos que tenemos en nuestro laboratorio un objeto con estado $|\Psi\rangle \in \mathcal{H}$ desconocido. Nos planteamos el problema de describir completamente el estado de nuestro objeto. Si T es un observable para el objeto, por definición de observable, el conjunto de autovectores $\{|\chi_i\rangle\}$ de T genera $\mathcal{H}$. Entonces el estado se puede escribir como

$$|\Psi\rangle = c_1 |\chi_1\rangle + \ldots + c_n |\chi_n\rangle ,$$

para ciertos coeficientes c_i desconocidos. Al medir T obtendremos pues uno de los λ_i. Incluso si concedemos que este autovalor no es degenerado, el resultado de la medida anterior solo nos dirá que $|\Psi\rangle$ se encuentra en una superposición de $|\chi_i\rangle$ con quizás otros estados. Si se pudiera repetir la medición de T sobre el estado original, entonces podríamos construir estadísticas para la probabilidad de los distintos autovalores. Considerando distintos observables y suficientes medidas, acabaríamos obteniendo una descripción arbitrariamente precisa del estado $|\Psi\rangle$.
Desafortunadamente, solo podemos medir una vez. Cuando se realiza la primera medida, el estado colapsa a cierto $|\chi_i\rangle$: el resto de la información cuántica se pierde. Esta es la esencia del Teorema de No Teleportación, que nos dice que no existe ningún procedimiento de medida que permite convertir íntegramente la información cuántica en clásica [8, pg. 41]. Por otro lado, sí se puede convertir íntegramente la información clásica en cuántica, basta codificarla en estados ortogonales. Por ejemplo, en el caso de los qubits, basta asociar los estados $|0\rangle$, $|1\rangle$ a sus respectivos bits 0, 1.
El Teorema de No Teleportación también se puede ver como una consecuencia del Teorema de No Clonación (el siguiente que enunciaremos): si fuera posible obtener la descripción completa de un estado arbitrario, podríamos preparar otro idéntico. Veremos en la siguiente subsección que no es posible copiar un estado arbitrario desconocido.

1.5.3. No clonación, no borrado y no ocultación

En el Teorema de No Teleportación, el colapso era una barrera aparentemente insalvable. Un esquema alternativo podría consistir en copiar el estado a otros objetos idénticos, y medir (y colapsar) cada uno de esos estados, hasta que obtuviéramos toda la información que buscamos. De nuevo, desafortunadamente, existe un teorema no-go que nos dice que esto no es posible. De manera precisa: el Teorema de No Clonación afirma que, dado un espacio de Hilbert no trivial $\mathcal{H}$ y $|0\rangle \in \mathcal{H}$ un estado auxiliar, no existe ningún operador unitario U que, dado un estado arbitrario $|\psi\rangle \in \mathcal{H}$, realice la operación de clonación

$$|\psi\rangle |0\rangle \mapsto |\psi\rangle |\psi\rangle .$$

La prueba es inmediata por linealidad: Supongamos que existe tal operador U. Es inmediato llegar a una contradicción por linealidad. Sean $|\psi_1\rangle$, $|\psi_2\rangle \in \mathcal{H}$ dos estados ortogonales. Si aplicamos U a cada uno de ellos tenemos

$$U[|\psi_i\rangle |0\rangle] = |\psi_i\rangle |\psi_i\rangle ,$$

pero por linealidad

$$U\left[\left(\frac{|\psi_1\rangle + |\psi_2\rangle}{\sqrt{2}}\right)|0\rangle\right] = \frac{1}{\sqrt{2}} |\psi_1\rangle |\psi_1\rangle + \frac{1}{\sqrt{2}} |\psi_2\rangle |\psi_2\rangle \neq \left(\frac{|\psi_1\rangle + |\psi_2\rangle}{\sqrt{2}}\right)\left(\frac{|\psi_1\rangle + |\psi_2\rangle}{\sqrt{2}}\right),$$

lo que nos dice que U no puede clonar el estado $\left(\frac{|\psi_1\rangle+|\psi_2\rangle}{\sqrt{2}}\right)$, absurdo.
El Teorema de No Clonación se puede generalizar al Teorema de No Difusión. Este nos dice que,

incluso si relajamos las condiciones sobre el estado final, exigiendo solamente que las medidas en cada subsistema proporcionen las mismas estadísticas que si el estado final fuera $|\Psi\rangle\,|\Psi\rangle$, tampoco es posible realizar la "difusión" [9].
Otra forma de relajar las condiciones de clonación consiste en pedir solo un parecido aproximado entre los estados clonados y los originales. En este sentido, sí existen máquinas de "clonación imperfecta", que pueden alcanzar una fidelidad (medida de la superposición entre el estado original y la copia imperfecta) de hasta 5/6 para el caso de qubits [10].
Cabe citar también el Teorema de No Borrado, que es el dual del Teorema de No Clonación: dado un espacio de Hilbert no trivial $\mathcal{H}$ y $|0\rangle \in \mathcal{H}$ un estado auxiliar, no existe ningún operador unitario U que, dadas dos copias de un mismo estado $|\psi\rangle \in \mathcal{H}$, realice la operación de borrado

$$|\psi\rangle\,|\psi\rangle \mapsto |\psi\rangle\,|0\rangle\,.$$

Esta operación de borrado es simplemente el inverso temporal de la operación de clonación, y en consecuencia, el razonamiento anterior también demuestra que no es posible tener una máquina universal de borrado.
Por último, mencionaremos el Teorema de No Ocultación, que afirma cuando un sistema sufre decoherencia como consecuencia de la interacción con su entorno, la información cuántica (es decir, el estado inicial del sistema) no queda "oculta" en las correlaciones entre el sistema y el entorno, sino que pasa directamente a formar parte de la función de onda del estado conjunto [11].
Todos estos teoremas se pueden resumir en una máxima: "la información cuántica no se crea ni se destruye, solo se transforma".

1.5.4. Teorema de Holevo

Si bien nuestro esquema para transmitir una cantidad virtualmente ilimitada de información clásica a partir de objetos cuánticos ha sido frustrado, aún así podríamos tener la esperanza de lograr cierta mejora frente a la comunicación clásica. El Teorema de Holevo nos da una cota sobre la máxima cantidad de información clásica que podemos transmitir con un sistema cuántico [12]. Como caso particular notable, solo es posible comunicar n bits de información transmitiendo n qubits. Este resultado quizás es sorprendente, pues describir el estado conjunto de los n qubits requiere $2^n - 1$ coeficientes complejos, pero quizás no tanto, pues, en el fondo, son n qubits, y medir individualmente cada uno solo proporciona un bit.
En todo caso, esto termina nuestra discusión sobre Información Cuántica. Sin duda, es un tema muy interesante y en el que todavía queda mucho por decir.

Capítulo 2

Computación Cuántica

> Quantum computation is ... nothing less than a distinctly new way of harnessing nature
>
> *David Deutsch*

Un ordenador cuántico es, como su nombre indica, un ordenador que aprovecha fenómenos cuánticos para realizar computaciones. Por supuesto, la descripción del universo que nos rodea, y en particular de los ordenadores convencionales, también viene en última instancia proporcionada por la Mecánica Cuántica. La distinción estriba en que el entrelazamiento, que es el fenómeno fundamental y central de la computación cuántica, *no tiene explicación clásica*.
Los ordenadores cuánticos prometen un incremento de velocidad sustancial, a veces incluso exponencial, para diversos problemas computacionales. Debido a ello, este nuevo campo es increíblemente atractivo desde el punto de vista comercial. Por supuesto, los ordenadores cuánticos también presentan notable interés académico: se manipulan estados cuánticos con pocos grados de libertad y aislados de cualquier otra influencia. Estas condiciones evocan al test de Bohm para la paradoja EPR, por lo que no es de extrañar que algunos físicos afirmen que la Computación Cuántica constituye el test más riguroso y complejo de los principios de la Mecánica Cuántica que se ha realizado hasta ahora.
En este Capítulo haremos un breve tour por la Computación Cuántica. Es imposible cubrir todo, o incluso lo más relevante, de este área tan amplia, por lo que abundarán las sobresimplificaciones y omisiones. Aún así, esperamos que constituya un contexto, un punto de partida sólido, y, sobre todo, una invitación al mundo de la Computación Cuántica.

2.1. Breve perspectiva histórica

Si bien ya empezaban a surgir artículos apuntando en esa dirección ya en los años 70, se podría decir que el campo de la computación cuántica nace en 1980 con la *First Conference on the Physics of Computation*. En esa conferencia cabe citar la charla que dió el famoso físico americano Richard Feymann, en la que estableció la impractibilidad de realizar simulaciones de sistemas cuánticos "grandes" en ordenadores clásicos [13]. Feynmann argumentaba que, para combatir el creciemiento exponencial del número de variables involucradas, que era necesario construir ordenadores que de algún modo sean "cuánticos" para afrontar la simulación de sistemas cuánticos a gran escala. Unos años después, en 1985 el físico británico David Deutsch propone un modelo de ordenador cuántico [14]. Este modelo es análogo a la operación de un ordenador clásico digital (visto como una máquina de Turing) con bits, pero ahora se emplean operaciones unitarias sobre qubits.
No mucho más tarde, en 1989, se empieza a considerar la posibilidad de controlar la evolución

de un sistema cuántico ordenado mediante el ajuste externo de los parámetros de interacción de sus partículas (por ejemplo, aplicando un campo magnético a un cristal de espines) [15]. La actuación del efecto túnel permite que, aunque lentamente, el sistema siga evolucionando hacia estados de energía cada vez más baja. Tras esperar suficiente tiempo, el sistema alcanzará su mínimo global. Esta es la base del "quantum annealing", una importante forma de computación cuántica analógica que aprovecha la tendencia de los sistemas cuánticos para resolver problemas de optimización. Nosotros preferiremos centrarnos en los ordenadores cuánticos "digitales", el lector interesado en las aplicaciones y métodos del quantum annealing puede encontrar una buena revisión en [16]

En los años 90 se descubren varios problemas teóricos que pueden ser resueltos por un ordenador cuántico más rápido que por uno clásico. Quizás el más importante es el problema de factorización: en 1994, el matemático americano Peter Shor propuso en 1994 un algoritmo que permitiría a un ordenador cuántico factorizar un número en tiempo polinómico [1] [17]. También se propone una realización experimental de la puerta CNOT en 1995 [18]. Esta puerta lógica cuántica, que es la primera que involucra más de un qubit (y que crea entrelazamiento), se implementó en el laboratorio ese mismo año [19].
Justo a comienzo de milenio, se consigue fabricar los primeros ordenadores cuánticos, y con ello, se produce una explosión de nuevos resultados y tecnologías. En la carrera cuántica no solo participan institutos de investigación con fondos gubernamentales, este campo también ha atraído una gran inversión privada por distintos gigantes de la tecnología como Google, Intel e IBM, y también por nuevas empresas emprendedoras como Rigetti, IonQ y D-Wave. Poco a poco, se comienzan a fabricar unidades integradas de computación cuántica. De momento, el mayor procesador cuántico es el procesador Bristlecone de Google con 72 qubits (ver [20]): este número de qubits ya no es una mera "prueba de concepto".

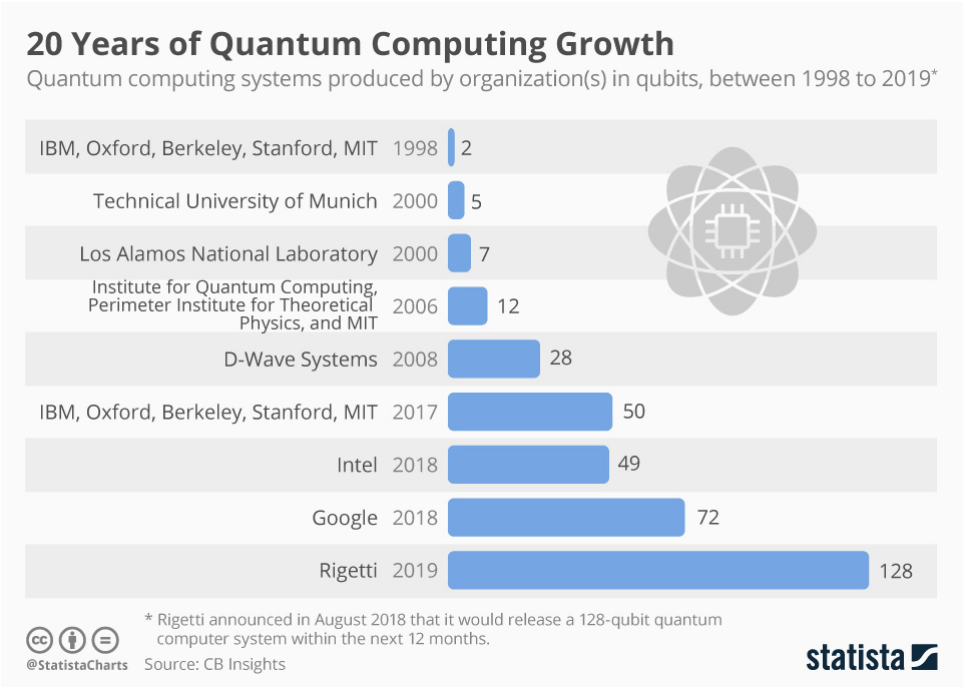


Figura 2.1: Gráfica de Statista ilustrando el progreso en computación cuántica durante las últimas dos décadas [21]. Si bien es pronto para hablar de un análogo cuántico a la ley de Moore, se aprecia una aceleración considerable en los últimos años. Cabe mencionar que algunos de estos ordenadores no eran realmente digitales, como el procesador de D-Wave, y que Rigetti todavía no ha producido el prometido procesador de 128 qubits.

A finales de 2019, Google anunció que su ordenador cuántico había alcanzado la "supremacía cuántica", es decir, había realizado una cálculo que sería completamente inviable en un ordenador clásico [22]. Su procesador Sycamore, de 53 qubits, fue capaz de analizar la estructura de cierta

[1] Aquí "en tiempo polinómico" significa que el tiempo necesario para la resolución del problema crece como un polinomio del número de bits de la entrada. De momento no se ha descubierto ningún procedimiento para factorizar un número en tiempo polinómico con un ordenador clásico.

transformación pseudoaleatoria en unos minutos, tarea que en el artículo estimaron que llevaría más de 10000 años al superordenador más potente de la época (el superordenador Summit). Esta afirmación fue inmediatamente disputada por IBM [23], empresa que también disponía de un ordenador cuántico de 53 qubits, y para más inri, era la que había construido el superordenador Summit en 2018. Si bien parece que Google se quedó corto en su intento de demostrar la supremacía cuántica, alcanzarla es cuestión de tiempo, y, sin duda, la computación cuántica está cada año más cerca de alcanzar la viabilidad científica y comercial.

2.2. Circuitos y puertas cuánticas

Los ordenadores cuánticos digitales operan aplicando secuencialmente operaciones unitarias sobre un conjunto de qubits. Al final del algoritmo cuántico, se extrae información del sistema midiendo los n qubits, lo que nos da uno de 2^n resultados posibles. La ciencia y el arte del diseño de algoritmos cuánticos radica en formar un estado final, que, al medirlo, nos proporcione con alta probabilidad los resultados que buscamos.
Para describir el estado conjunto de n qubits con comodidad, introducimos la base computacional, que es la base de estados completamente desacoplados que se obtiene haciendo el producto tensorial de las n bases $\{|0\rangle, |1\rangle\}$. Adoptaremos la notación $|x_0x_1x_2\cdots x_{n-2}x_{n-1}\rangle$ para referirnos a estos estados, cada x_i será 0 o 1 dependiendo de si el qubit i-ésimo (de arriba a abajo en los circuitos) se encuentra en el estado $|0\rangle$ o $|1\rangle$. Los numeramos como si fueran binario (escritos de derecha a izquierda), de forma totalmente análoga a los bits clásicos: $|[x]\rangle := |x_0x_1x_2\cdots x_{n-2}x_{n-1}\rangle$ donde $x = 2^{n-1}x_0 + 2^{n-2}x_1 + \ldots + 4x_{n-3} + 2x_{n-2} + x_{n-1}$.
Para pares $[x]$, $[y]$, consideramos las operaciones componente a componente:

$$[x] \oplus [y] = [(x_0 \oplus y_0)(x_1 \oplus y_1)\ldots(x_{n-1} \oplus y_{n-1})],$$
$$[x] \cdot [y] = [(x_0 \cdot y_0)(x_1 \cdot y_1)\ldots(x_{n-1} \cdot y_{n-1})].$$

Comenzaremos introduciendo los circuitos cuánticos, que son uno de los pilares básicos de este Trabajo de Fin de Grado.

2.2.1. Modelo de circuito cuántico

El modelo de circuito cuántico proporciona una abstracción de la operación de un ordenador cuántico. Los programas se representan con diagramas análogos a los de circuitos electrónicos, pero ahora los "cables" o "registros" horizontales son qubits y las "puertas lógicas" son operaciones unitarias sobre uno o varios de estos. Los qubits evolucionan en el tiempo de izquierda a derecha, según se les aplica distintos operadores unitarios que se representan con cajas u otros símbolos. Sin embargo, aquí los qubits no tienen porque estar en movimiento en el dispositivo físico. De hecho, en la mayor parte de los casos son entidades físicas fijas. Así mismo, las puertas cuánticas que se aplican, aunque aparezcan distintas en el diagrama, no tienen por qué corresponder a diferentes componentes. En ocasiones querremos introducir o extraer información clásica, de control o medida, en el circuito. Para representar los bits clásicos se emplea una línea doble.
En este modelo, se supone que todos los qubits comienzan sin entrelazar, cada uno en el estado $|0\rangle$. Así mismo, las medidas se realizan en la base $\{|0\rangle, |1\rangle\}$. Si se desea representar o formar estados iniciales distintos, o medir en bases diferentes, se deben aplicar los operadores unitarios de cambio de base correspondientes. Recordemos que los circuitos cuánticos son un modelo, es posible que el sistema físico subyacente opere de modo diferente, realizando operaciones distintas en otro orden. Lo importante es que el estado inicial y el estado final de los dos sistemas coincidan.

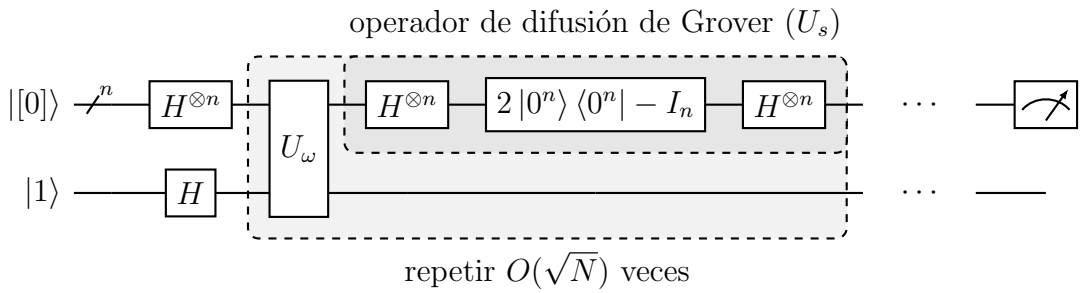


Figura 2.2:
Circuito que representa el algoritmo de Grover [24, pg. 89].
Todos los circuitos en este Trabajo de Fin de Grado se han dibujado con el paquete `quantikz` de LaTeX [25].

2.2.2. Principales puertas cuánticas

Al igual que un ordenador clásico, un ordenador cuántico manipula qubits a través de las llamadas puertas cuánticas (por analogía con las puertas lógicas de la electrónica). Estas puertas se implementan modificando durante un tiempo adecuado el hamiltoniano bajo el cuál evoluciona la función de onda. Estos operadores de evolución son siempre unitarios, en particular, la acción de un ordenador cuántico siempre es reversible hasta que no realicemos las medidas.
Como operadores que son, proporcionaremos la forma matricial de las puertas cuánticas que describamos. Dichas matrices están escritas en la base computacional, recordemos que el orden sería $|[0]\rangle = |0\cdots 00\rangle$, $|[1]\rangle = |0\cdots 01\rangle$, $|[2]\rangle = |0\cdots 10\rangle$, $|[3]\rangle = |0\cdots 11\rangle$, etc.
Las puertas cuánticas se clasifican según el número de qubits que se ven afectados por ellos. Por lo general, cuantos menos qubits se vean afectados por una puerta cuántica, será radicalmente más sencilla de implementar en hardware: las puertas de 1 qubit se dan por supuesto, las de 2 qubits constituyen el principal desafío en el construcción de ordenadores cuánticos, y raramente se construyen puertas de 3 o más qubits: cuando se necesitan esta clase de operaciones, se contruyen mediante la combinación de puertas de 1 y 2 qubits. Esto se tratará más en detalle en una subsección posterior.
Tipográficamente, distinguiremos entre puertas U y operadores unitarios U, según escribamos en letra redonda o en cursiva.

Puertas de 1 qubit

Dos de las puertas de 1 qubit más comunes corresponden a operadores de Pauli con el mismo nombre: X (también llamada NOT) y Z. Menos importante es la puerta Y, que raramente aparece en circuitos, pues ya se puede formar concatenando una puerta X y una puerta Z. Recordemos cómo eran las matrices correspondientes y la forma de sus autovectores:

Matriz	Autovectores
$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\|+\rangle = \frac{1}{\sqrt{2}}[\|0\rangle + \|1\rangle]$ $\|-\rangle = \frac{1}{\sqrt{2}}[\|0\rangle - \|1\rangle]$
$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	$\|\circlearrowleft\rangle = \frac{1}{\sqrt{2}}[\|0\rangle + i\,\|1\rangle]$ $\|\circlearrowright\rangle = \frac{1}{\sqrt{2}}[\|0\rangle - i\,\|1\rangle]$
$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\|0\rangle = \|0\rangle$ $\|1\rangle = \|1\rangle$

Puesto que manejamos con frecuencia las bases $\{|0\rangle, |1\rangle\}$ (computacional) y $\{|+\rangle, |-\rangle\}$ (de estados máximamente superpuestos), es útil la operación unitaria de cambio de base entre ellas. Esta puerta recibe el nombre de H o Hadamard, ya que es un caso particular para $m = 2$ de la transformada de Walsh-Hadamard [26]. La matriz de la puerta de Hadamard es:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Cuando se combinan varias operadores U_i actuando cada sobre el qubit i correspondiente (con $U_i = \text{Id}$ si no se actúa sobre dicho qubit), sabemos que el operador conjunto es $U_1 \otimes \ldots \otimes U_n$. En este sentido, se define la puerta de Hadamard para n qubits como $\text{H}^{\otimes \text{n}}$: es la operación resultante al aplicar una puerta de Hadamard sobre cada qubit. Por inducción, se puede probar que el operador $H^{\otimes n}$ actúa en los estados de la base computacional como:

$$H^{\otimes n} |[x]\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |[y]\rangle .$$

Es decir, $H^{\otimes n}$ transforma cada estado de la base computacional en una superposición uniforme de estados de la misma.
Otra puerta muy común es la de desfase R_ϕ, con $\phi \in [0, 2\pi)$. Como su nombre indica, introduce un desfase ϕ entre el estado $|0\rangle$ y el estado $|1\rangle$:

$$R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}.$$

Por último, introduciremos otro conjunto paramétrico de puertas G_p, con $\text{p} \in [0, 1]$. Este conjunto de puertas no es estándar, hemos tomado la notación de [27]:

$$G_p = \begin{bmatrix} \sqrt{p} & \sqrt{1-p} \\ \sqrt{1-p} & -\sqrt{p} \end{bmatrix}.$$

Estas puertas G_p son, en el fondo, rotaciones arbitraria por el ángulo de Euler $\theta = 2 \arctan\left(\sqrt{\frac{p}{1-p}}\right)$.
Aunque sea evidente, cabe destacar que ninguna de estas puertas genera entrelazamiento (ni tampoco la combinación de ellas), pues cada una actúa sobre un solo qubit. En consecuencia, se representan como cajas sobre dicho qubit:

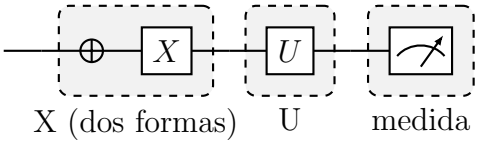


Figura 2.3:
Notación para una puerta X (ambas formas son aceptables), para una puerta de 1 qubit genérica U, y para una medida.

Puertas de 2 qubits

La clase más abundante de puertas de 2 qubits son las controladas. Dada una puerta U, se representa la puerta controlada *cuánticamente* por CU. En esta puerta, se distingue el qubit de control y el qubit objetivo. Si el qubit de control es $|0\rangle$, el qubit objetivo permanece invariante.

Si por otro lado, el qubit de control vale $|1\rangle$, se aplica la puerta U al qubit objetivo. Para $U = \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix}$, la matriz de CU será

$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_1 & u_3 \\ 0 & 0 & u_2 & u_4 \end{bmatrix}.$$

Evidentemente, las puertas controladas cuánticamente son capaces de producir entrelazamiento. Muy relacionadas, pero sin esa propiedad entrelazante, están las puertas de 1 qubit controladas *clásicamente*, que se representa por cU. Su funcionamiento es idéntico, pero ahora el control es clásico: el control es un bit, solo puede valer 0 o 1.
Otra puerta de 2 qubit importante es la puerta SWAP. Esto en realidad no es más que un intercambio del estado de los qubits (que no siempre corresponde a un intercambio de los propios qubits, como entidades físicas). En consecuencia, no produce entrelazamiento. Se representa simplemente cruzando la líneas horizontales que representan los qubits.
Su matriz es

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

Por supuesto, existen otras muchas puertas de 2 qubits. Pero, como se comprueba de forma explícita en [28], basta conbinar puertas CNOT con puertas de 1 qubit para obtener todas las operaciones unitarias de 2 qubits. Veamos cómo se representan todas las puertas anteriores:

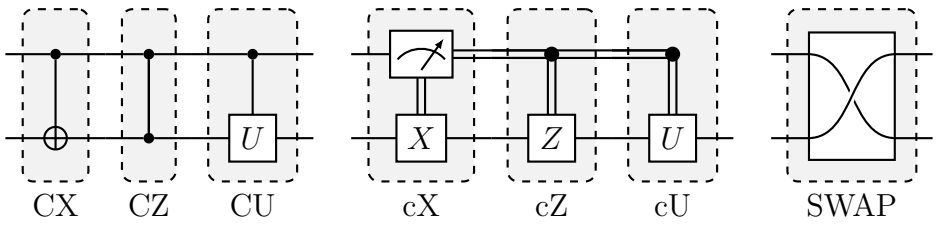


Figura 2.4:
Puertas de 2 qubits, en orden de aparición. La puerta CZ recibe notación especial, para simbolizar la simetría entre control y objetivo en este caso. Cuando el control es clásico, se revierte a la notación "normal".

Terminamos con una reflexión de cierto peso. La función esencial de las puertas controladas (y en general, de todas las puertas de 2 qubits que no se describan como producto tensorial de puertas de 1 qubit junto con un posible SWAP) es generar entrelazamiento. El control de las puertas controladas es en la base de autovectores de Z. En consecuencia, para que una puerta controlada CU produzca entrelazamiento entre dos qubits desacoplados, el qubit de control debe no ser un autovector de Z y el qubit objetivo debe no ser un autovector de U (estas condiciones también son suficientes).

Puertas de 3 o más qubits

Cuanto se combinan dos puertas de 2 qubits que comparten solo un extremo, se obtiene una puerta de 3 qubits. Pocas puertas de 3 qubits reciben un símbolo y nombre estándar, la mayoría se escriben como combinación de varias de dos qubits. La única que mencionaremos de este tipo es la puerta TOFFOLI. Esta puerta fue introducida por el ingeniero informático italiano

Tommaso Toffoli en su artículo pionero *Reversible Computing* [29] (este artículo también formó parte del proceso intelectual que condujo a la idea de computación cuántica a principios de los 80).
La puerta TOFFOLI es un ejemplo de puerta doblemente controlada:

- Si ambos qubits de control valen $|1\rangle$, se aplica el operador X al qubit objetivo.
- De lo contrario, se deja invariante el qubit objetivo.

Se puede considerar este control como un análogo cuántico al control "no lineal" de las puertas AND u OR en circuitos clásicos. De esta forma, cualquier circuito clásico puede ser trasladado a uno cuántico. Esto es especialmente útil para implementar operaciones aritméticas, lo que permite contruir un análogo cuántico de las ALUs clásicas [30].
Dado un estado $|c_1, c_2, 0\rangle$, la puerta Toffoli lo traslada al estado $|c_1, c_2, c_1c_2\rangle$. Observemos que no podría existir ningún mecanismo cuántico que realizara directamente el producto $|c_1, c_2\rangle \mapsto |c_1c_2\rangle$, puesto que esta operación no es lineal. Es justo la presencia del tercer qubit lo que evita la no linealidad. Esta estrategia de añadir qubits se traslada al caso general. Dada una operación clásica $f\colon \{0,1\}^n \to \{0,1\}^m$, podemos transformarla en una puerta cuántica $\mathrm{U_f}$ que se aplica a un registro [2] de $n+m$ qubits: en el subregistro de n qubits, $|[x]\rangle$ es el argumento y se deja invariante; en el subregistro de m qubits, al estado $|[y]\rangle$ se le suma (en el sentido $\oplus$) la imagen $|[f(x)]\rangle$.
Veamos cómo denotar todo esto:

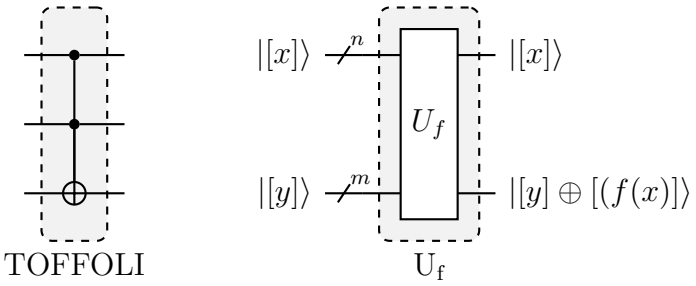


Figura 2.5:
Varias puertas de más de 2 qubits.

2.2.3. Una nota sobre conjuntos universales de puertas

Los ordenadores cuánticos reales solo pueden implementar de manera práctica un conjunto limitado de puertas. La cuestión es, ¿se puede, a partir de estas puertas, realizar cualquier operación unitaria? Si la respuesta es afirmativa, se dice que ese conjunto de puertas es "exactamente universal". Si la respuesta es negativa, pero sí es posible aproximar arbitrariamente cualquier operación unitaria con un número finito de puertas, se dice que ese conjunto de puertas es "universal". Denotamos por S_n al conjunto de operadores unitarios sobre n qubits. En orden de menor a mayor fuerza, se tiene que:

1. Un conjunto de puertas que implemente S_3 es universal.
2. Un conjunto de puertas que implemente S_2 es universal.
3. Un conjunto de puertas que implemente S_1, junto con una puerta G que produzca entrelazamiento, es exactamente universal [3].

[2] "registro" es otro nombre que se da a un conjunto de qubits.
[3] Esta puerta G no tiene nada que ver con el conjunto paramétrico $\mathrm{G_p}$ que definimos antes.

También podemos lograr un conjunto universal si tomamos la puerta CNOT junto con otra puerta g de 1 qubit, a cuyo operador g exigimos que g^2 no deje invariante la base computacional. Todos estos resultados se pueden encontrar en el excelente artículo review [31]. Sería interesante estudiar, en el caso anterior, bajo que condiciones se puede sustituir la puerta CNOT por la puerta G de más arriba. Esta tarea se desvía mucho del propósito de este Trabajo de Fin de Grado, así que dejamos la cuestión abierta.
En los sistemas físicos reales, el estándar y lo más razonable es suponer que se puede realizar cualquier puerta de 1 qubit y la puerta CNOT o CZ. Cualquier otra puerta controlada CU se puede obtener con facilidad a partir de estas [32], por lo que también es razonable considerarlas como puertas elementales en estos casos.

2.3. Estados entrelazados en computación cuántica

Como comprobaremos más adelante, el entrelazamiento juega un papel fundamental en Computación Cuántica y en Comunicación Cuántica. En esta sección volvemos a tratar los estados entrelazados de dos y tres qubits que se introdujeron previamente en el **Capítulo 1**, ahora desde el punto de vista de los circuitos cuánticos.

2.3.1. Estados de Bell

En cierto modo, cuando trabajamos con estados de Bell, estamos aprovechando el entrelazamiento entre dos qubits todo lo que es matemáticamente/físicamente posible. Esto explica que los estados de Bell sean extremadamente valiosos, hecho que ya se señaló en el **Capítulo 1**. Por tanto, es importante conocer los circuitos estándar para manejar estos estados.
Para generar estados de Bell a partir de la base computacional, basta realizar una rotación sobre uno de los qubits aplicando una puerta H, y entrelazarlos después aplicando una puerta CNOT. Esto induce un cambio de base:

$$|00\rangle \mapsto \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle] = |\Phi^+\rangle = |\beta_{00}\rangle$$
$$|01\rangle \mapsto \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle] = |\Psi^+\rangle = |\beta_{01}\rangle$$
$$|10\rangle \mapsto \frac{1}{\sqrt{2}}[|00\rangle - |11\rangle] = |\Phi^-\rangle = |\beta_{10}\rangle$$
$$|11\rangle \mapsto \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle] = |\Psi^-\rangle = |\beta_{11}\rangle$$

Por supuesto, podemos invertir el orden del circuito y así realizar el cambio de base inverso. Esto es muy útil cuando queremos medir dos qubits en la base de estados de Bell en vez de en la base computacional.

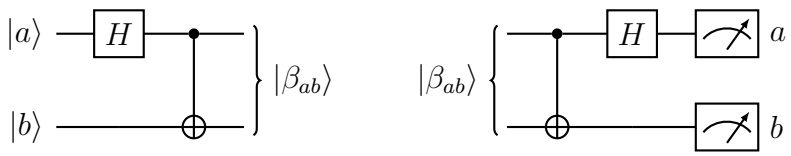


Figura 2.6:
Generador de estados de Bell y medida de Bell. Este tipo de circuitos son clave en los esquemas de teleportación y de codificación superdensa.

A nosotros nos interesará especialmente emplear estados $|\Phi^+\rangle$. Abreviamos estos estados de la siguiente forma:

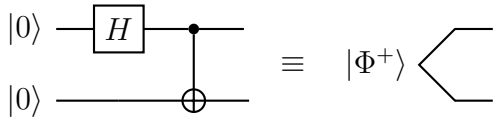


Figura 2.7:
Notación para los estados $|\Phi^+\rangle$. En algunas ocasiones se omitirá el "$|\Phi^+\rangle$" para evitar la acumulación visual de símbolos.

Cabe notar que, por supuesto, nuestros estados $|\Phi^+\rangle$ no tienen por qué provenir de aplicar una puerta H seguida de una CNOT. Simplemente los representamos de esa forma en el modelo de circuitos.

2.3.2. Estados GHZ y estados W

En muchas ocasiones es interesante generar estados entrelazados de más de dos qubits. En [27] se proporcionan circuitos sencillos y escalables para crear estados $|GHZ_n\rangle$ y $|W_n\rangle$. Nosotros nos reduciremos simplemente al caso $n = 3$:

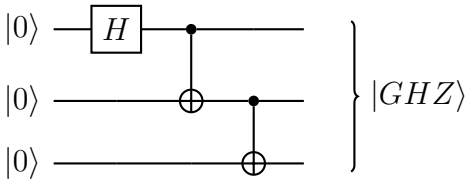


Figura 2.8:
Generador de estados GHZ para el caso $n = 3$. Como vemos, este circuito es una generalización directa del anterior para estados de Bell.

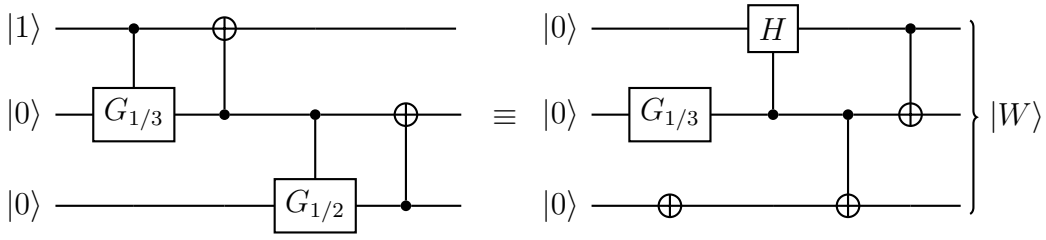


Figura 2.9:
Generador de estados W para el caso $n = 3$ (izquierda), y su versión simplificada (derecha). Para obtener la versión simplificada, se quita el control superfluo de $G_{1/3}$ (pues este control vale $|1\rangle$ siempre) y se sustituye $G_{1/2}$ por H (pues ambas actúan igual sobre $|0\rangle$). Para terminar, se escribe $|1\rangle$ como $|0\rangle$ seguido de X, se cambia el orden de los controles de las puertas CNOT y se invierte verticalmente todo el circuito (lo que no altera el resultado, ya que el estado $|W\rangle$ es simétrico frente a permutaciones). El razonamiento anterior quizás sea más fácil de seguir tras la lectura del **Capítulo 3**.

En el **Capítulo 4** buscaremos esquemas para generar estos estados a partir de pares EPR. Esta no es tarea sin recompensa: los estados triplemente entrelazados también tienen multitud de aplicaciones. Por citar cuatro casos concretos:

- El estado $|GHZ\rangle$ proporciona una violación determinista del realismo local [33][34], lo cuál podría resultar más convincente que la violación probabilista que describían las desigualdades de Bell.

- El estado $|GHZ\rangle$ también permite crear con medidas y control clásico el estado entrelazado $|\chi\rangle = \frac{|0000\rangle+|1100\rangle+|0111\rangle+|1011\rangle}{2}$ para circuitos de teleportación de puertas cuánticas [35].
- El estado $|W\rangle$ permite crear entrelazamiento remoto simétrico [36].
- Los estados $|W_n\rangle$ y $|GHZ_n\rangle$ permiten respectivamente elegir un líder y formar un consenso en protocolos de decisión cuántica [37].

2.4. Ventaja computacional, algortimos cuánticos y otros protocolos

Una de las principales razones detrás del masivo interés en la computación cuántica es la conocida muletilla "los ordenadores cuánticos pueden resolver "de forma eficiente" problemas que resultan "difíciles" para un ordenador clásico". Para precisar la afirmación anterior, conviene repasar rápidamente algunas clases de complejidad computacional clásicas y cuánticas:

1. P: Problemas que se pueden resolver de forma determinista en tiempo polinómico con un ordenador clásico.
2. BPP: Problemas que se pueden resolver correctamente con probabilidad $> 2/3$ (convenio) en tiempo polinómico con un ordenador clásico junto con una fuente de aleatoriedad.
3. NP: Problemas cuya solución se puede comprobar que es correcta de forma de determinista en tiempo polinómico con un ordenador clásico.
4. EQP: Problemas que se pueden resolver de forma determinista en tiempo polinómico con un ordenador cuántico universal dotado de un conjunto de puertas finito (puede depender del conjunto de puertas).
5. BQP: Problemas que se pueden resolver correctamente con probabilidad $> 2/3$ en tiempo polinómico con un ordenador cuántico universal dotado de un conjunto de puertas finito (no hay dependencia del conjunto de puertas por el Teorema de Solovay-Kitaev [31]).

Las definiciones anteriores no se pretende que sean absolutamente rigurosos (de hecho, hay algunos aspectos bastante delicados), pero sí dan una idea general. Se pueden encontrar definiciones más precisas, junto con diversas referencias, en [38].
Respecto a la relación entre clases, se sabe que $P \subseteq BPP$, $P \subseteq NP$ y $P \subseteq EQP \subseteq BQP$. Intuitivamente, BPP es la clase de problemas que es viable resolver en un ordenador clásico. Se sospecha que $P = BPP \neq NP$. Por otra parte BQP es la clase de problemas que es viable resolver en un ordenador cuántico. Si ocurriera que $BPP \neq BQP$, lo cual también parece probable, la construicción de ordenadores cuánticos aumentará estrictamente la clase de problemas computacionalmente viables. De nuevo, en [38] se pueden encontrar todos estos resultados, junto con citas a los artículos correspondientes.
Por supuesto, no basta con la descripción de las clases de complejidad, es necesario diseñar algoritmos que hagan realidad esa "ventaja computacional". Existe una gran cantidad de algoritmos cuánticos de este tipo, muchos de los cuáles quedan recogidos en [39]. Aún así, debemos ser cautelosamente optimistas. Es improbable que los ordenadores cuánticos reemplacen completamente a los clásicos: para la mayoría de las tareas comunes para un usuario doméstico (jugar a videojuegos, ver vídeos, etc.), no parece existor ventaja computacional. Además, los ordenadores cuánticos son *mucho* menos escalables, baratos y fáciles de construir y mantener que los ordenadores clásicos. Estos dos factores hacen difícil que algún día reemplacen al omnipresente PC. Donde sín duda sí encontrarán lugar los ordenadores cuánticos será en centros de datos y

de supercomputación. Ahí constituirán una herramienta valiosa para resolver muchos problemas de simulación, búsqueda, factorización, optimización, aprendizaje automático, etc., que están fuera del alcance de los sistemas clásicos.
Para ilustrar la "ventaja cuántica", en esta sección expondremos brevemente los algoritmos cuánticos de Deutsch–Jozsa y de Bernstein-Vazirani, junto con una pequeña reseña sobre otros algoritmos [4]. Por otro lado, recogeremos dos protocolos clave relativos a la Comunicación Cuántica: el de teleportación y el de codificación superdensa. Si bien no son algoritmos cuánticos en estricto rigor, estos protocolos presentan gran interés práctico, e ilustran el papel clave que juegan los estados entrelazados en computación cuántica.

2.4.1. Algoritmo de Deutsch–Jozsa

Imaginemos que tenemos una función $f\colon \{0,1\}^n \to \{0,1\}$ que sabemos que verifica una de estas dos propiedades:

- Todos los valores de f son 0 o todos los valores de f son 1 (es decir, f es constante).
- La mitad de sus valores de f son 0 y la otra mitad son 1 (es decir, f está equilibrada).

El algoritmo de Deutsch–Jozsa permite, con probabilidad 1 y con una sola evaluación de la función, comprobar cuál de estas alternativas es la correcta [24, pg. 41]. Por el contrario, el mejor algoritmo clásico consistiría en ir probando secuencialmente todos los posibles valores de f, hasta que encontremos dos distintos, o veamos que $2^{n-1}+1$ son iguales. Por tanto, el algoritmo de Deutsch–Jozsa demuestra que, *respecto a una caja negra que implemente la función* (lo que se suele llamar un oráculo), $P \neq EQP$. Por otro lado, si se admite la posibilidad de cometer un error, basta evaluar la función 3 veces para poder acertar con probabilidad al menos $3/4 > 1/3$. Esto nos dice que el algoritmo de Deutsch-Jozsa no prueba que $BPP \neq EQP$ respecto al oráculo.
Veamos como funciona este algoritmo. Imaginemos que tenemos una caja negra que implementa la función, es decir, la puerta cuántica $\mathrm{U_f}$. Evaluar la caja negra en la base computacional es una pérdida de tiempo, estaríamos haciendo lo mismo que un ordenador clásico. Pero si aplicamos una transformada de Hadamard, la situación cambia:

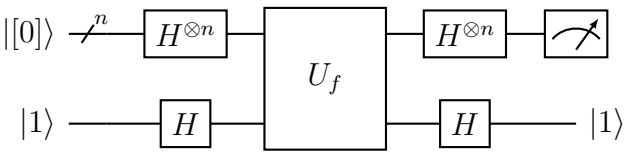


Figura 2.10:
Circuito cuántico implementando el algoritmo de Deutsch–Jozsa. Este circuito también servirá para el siguiente ejemplo, el algoritmo de Bernstein-Vazirani.

Comprobemos el funcionamiento de este algoritmo. Primero, las puertas de Hadamard transforman el estado inicial $|[0]\rangle\,|1\rangle$:

$$|[0]\rangle\,|1\rangle \mapsto \frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|[x]\rangle\,[|0\rangle - |1\rangle],$$

[4]Por supuesto, se podría decir mucho más. En particular, los algoritmos de Grover y de Shor son mucho más importantes. La razón por la que no los escogemos es que también son más complicados. Entretenerse demasiado en los algoritmos cuánticos no es el propósito de este Trabajo de Fin de Grado.

después aplicamos la función f:

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|[x]\rangle\left[|0\rangle-|1\rangle\right]\mapsto\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}|[x]\rangle\left[|f(x)\rangle-|1\oplus f(x)\rangle\right]=$$
$$\frac{1}{\sqrt{2^{n+1}}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|[x]\rangle\left[|0\rangle-|1\rangle\right]=\left[\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|[x]\rangle\right]|-\rangle$$

El estado del registro inferior queda desacoplado del registro superior, y lo podemos ignorar. Ahora, si realizamos de nuevo una transformada de Hadamard de n qubits en el registro superior obtenemos (reciclamos la variable y):

$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|[x]\rangle\mapsto\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}\left[\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|[y]\rangle\right]=\sum_{y=0}^{2^n-1}\left[\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot y}\right]|[y]\rangle$$

En este estado, el módulo de la amplitud que acompaña a $|[0]\rangle$ será 1 si f es constante (interferencia constructiva) y será 0 si f está equilibrada (interferencia destructiva). Así que bastará medir el estado final para averiguar a qué categoría pertenece la función.

2.4.2. Algoritmo de Bernstein-Vazirani

Si cambiamos la exigencia sobre la función que admitimos, obtenemos el algoritmo de Bernstein-Vazirani. Ahora f debe poder escribirse como

$$f(x)=x_0s_0\oplus x_1s_1\oplus\ldots\oplus x_{n-1}s_{n-1}$$

para cierto vector s desconocido. Se pide buscar dicho vector. El mejor algoritmo clásico consistiría en evaluar la función para $x=2^0=1$, $x=2^1=2$, $x=2^2=4$, etc., n veces en total (cada evaluación tiene un solo bit igual a 1). Incluso si admitimos la posibilidad de error, este sigue siendo el mejor curso de acción. Sin embargo, con un algoritmo cuántico, basta de nuevo una única evaluación de la función [24, pg. 50]. El circuito es el mismo, y la justificación similar. Por lo que vimos en el apartado anterior, el estado final toma la forma

$$\sum_{y=0}^{2^n-1}\left[\sum_{x=0}^{2^n-1}(-1)^{x\cdot s}(-1)^{x\cdot y}\right]|[y]\rangle=\sum_{y=0}^{2^n-1}\left[\sum_{x=0}^{2^n-1}(-1)^{x\cdot(s+y)}\right]|[y]\rangle$$

La suma interna se anula si $s\neq y$, ya que para la mitad los términos tendremos $(-1)^{x\cdot(s+y)}=0$, y para la otra mitad tendremos $(-1)^{x\cdot(s+y)}=1$. Concluimos que el estado final es ahora simplemente $|[s]\rangle$, y basta con medirlo.

2.4.3. Otros algoritmos

Los algoritmos citados previamente tienen sobre todo interés teórico. Para completar la lista, citaremos los dos algoritmos cuánticos con aplicaciones prácticas más icónicos:

- Algoritmo de Grover: algoritmo que dada una función arbitraria $f\colon X\to Y$ y dado un elemento de la imagen $y\in Y$, encuentra con alta probabilidad una preimagen $x\in f^{-1}(y)$ evaluando f $O(\sqrt{N})$ veces [24, pg. 89]. Su funcionamiento es un ejemplo de aumento de amplitudes: el algoritmo empieza en una superposición uniforme de todas las preimagenes posibles, pero con cada iteración (que tiene una bonita interpretación geométrica como un par de reflexiones), disminuye la amplitud de las respuestas incorrectas, en favor de la

correcta.
Si bien el algoritmo de Grover solo ofrecen una mejora de velocidad polinómica frente al algoritmo clásico con $O(n)$ evaluaciones (y por tanto, no establece una separación entre P y BPQ), su ventaja es que es completamente genérico, aplicable a cualquier problema de búsqueda.

- Algoritmo de Shor: algoritmo que aplica la transformada de Fourier cuántica (un concepto interesante, pero que queda fuera de este Trabajo de Fin de Grado) para encontrar el periodo de ciertas funciones y, con ello, resolver problemas como el de factorización y el del logaritmo discreto en tiempo polinómico y con alta probabilidad [24, pg. 63].
  Se sospecha que los anteriores problemas no están en P, en cuyo caso el algoritmo de Shor constituiría una mejora casi exponencial frente a cualquier algoritmo clásico (establece una separación entre P y BQP). En particular, rompería los principales criptosistemas de asimétricos (RSA y Diffie-Hellman, respectivamente). Esto no es una amenaza pequeña: todos los principales protocolos de clave pública actuales son vulnerables al algoritmo de Shor. Esto ha provocado el surgimiento de un nuevo campo, la Cripografía Postcuántica, que busca diseñar criptosistemas asimétricos inmunes a la computación cuántica.

Con esto terminamos la breve muestra de algoritmos cuánticos. Por supuesto, este es un campo relativamente nuevo, y en el que seguramente quede mucho progreso por realizar, pero los algoritmos cuánticos existentes ya muestran el gran potencial de la computación cuántica.

2.4.4. Codificación superdensa

La codificación superdensa es un protocolo de comunicación cuántica que permite transmitir dos bits de información mediante el envío de un solo qubit. Esto aparenta violar la cota de Holevo. El truco aquí es que, al contrario que en la situación en la que se planteaba esta cota, ahora se dispone de entrelazamiento inicial.

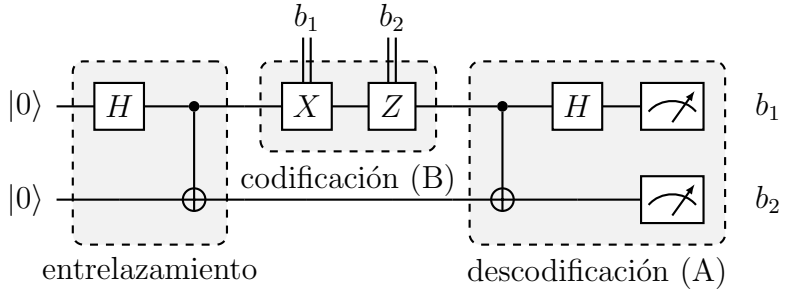


Figura 2.11:
Protocolo de codificación superdensa. A recibe su qubit después de la generación del estado de Bell. Tras actuar sobre él, le devuelve el qubit a B, que realiza una medida de Bell en el conjunto de ambos.

Supongamos que un emisor A pretende transmitir dos bits a un receptor B mediante el envío de un solo qubit. El funcionamiento del protocolo es como sigue: primero se comparte un par EPR $|\Phi^+\rangle$ entre A y B. Mediante operaciones locales sobre su qubit (respectivamente, Id, X, $Y \equiv XZ$ y Z), el emisor A puede transformar el estado conjunto de los dos qubits $|\Phi^+\rangle$ a uno de los cuatro estados de Bell $|\Phi^+\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$, $|\Phi^-\rangle$. Este proceso codifica dos bits de información. Tras completarlo, A envía su qubit a B. Ahora en posesión de ambos qubits, B puede realizar una medida de Bell en el estado conjunto, lo que le permite deducir qué operación de las cuatro realizó A sobre su qubit.
Si preferimos entender este circuito en términos de equivalencias (que será el método que emplearemos siempre, a partir del **Capítulo 3**), el protocolo de codificación superdensa se puede derivar de un circuito elemental de copia [40].

2.4.5. Teleportación cuántica

La teleportación cuántica permite transmitir un qubit enviando solo dos bits de información. De nuevo, el truco está en compartir un entrelazamiento inicial, pero aquí el resultado podría parecer más sorprendente, ya que podemos enviar el estado cuántico sin un canal cuántico.
Pese a las apariencias, este protocolo tampoco no viola ninguno de los teoremas "no-go". En particular, el Teorema de No Teleportación no es aplicable, ya que la información sobre el estado del qubit nunca queda codificada en los bits transmitidos, estos solo indican al receptor qué correcciones debe aplicar al estado transferido por entrelazamiento.
Este protocolo recibe el nombre de "teleportación" porque el estado inicial $|\psi\rangle$ del emisor A se destruye, y aparece en posesión del receptor B. En ningún caso se debe esperar que sea posible teletransportar objetos macroscópicos, este protocolo sirve principalmente para comunicar información cuántica a partir de un canal (el entrelazamiento) establecido en un tiempo previo.
El circuito de teleportación es

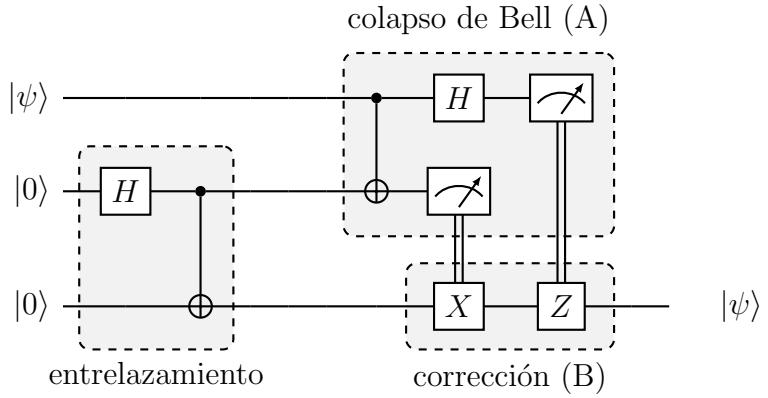


Figura 2.12:
Protocolo de teleportación. A y B comparten un par EPR $|\Phi^+\rangle$. A mide su qubit del par junto con el qubit que quiere transmitir (en estado arbitrario $|\psi\rangle$), ambos en la base de Bell. Según los resultados de esta medida conjunta, A envía datos (dos bits) a B sobre qué correcciones debe realizar en el otro qubit del par para que quede en estado $|\psi\rangle$.

Supongamos que un emisor A pretende transmitir un qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ a un receptor B mediante el envío de dos bits. Realmente solo haría falta comprobar el protocolo para estados computacionales (porque en realidad la medida se puede postergar y no afecta a la linealidad), pero es ilustrativo probarlo para un estado general. El protocolo de teleportación es como sigue: inicialmente, A y B deben compartir un par EPR $|\Phi^+\rangle$. Después A entrelaza el estado $|\psi\rangle$ que quiere transmitir a su qubit del par entrelazado, y con ello, también queda el qubit de B entrelazado con $|\psi\rangle$. Los dos qubits inferiores están en el estado de Bell $|\Phi^+\rangle$, desacoplados del primero. Pero también se puede ver el estado de los dos primeros qubits como una superposición de estados de Bell. Con esta idea, el estado se puede escribir como:

$$[\alpha\,|0\rangle + \beta\,|1\rangle]\,|\Phi^+\rangle = \cdots = \frac{1}{2}\Big[\,|\Phi^+\rangle\,[\alpha\,|0\rangle + \beta\,|1\rangle] + |\Phi^-\rangle\,[\alpha\,|0\rangle - \beta\,|1\rangle] + |\Psi^+\rangle\,[\beta\,|0\rangle + \alpha\,|1\rangle] + |\Psi^-\rangle\,[-\beta\,|0\rangle + \alpha\,|1\rangle]\Big].$$

Entonces, cuando A mide en la base de Bell el qubit $|\psi\rangle$ junto con su qubit del par, tiene una probabilidad de 1/4 de obtener cada uno de los estados de Bell $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$ y $|\Psi^-\rangle$. Por otro lado, el qubit del par que corresponde a B queda en un estado muy similar (o idéntico) a $|\psi\rangle$. Para corregirlo solo es necesario aplicar, respectivamente, los operadores Id, Z, X e $Y \equiv XZ$. A partir de la información clásica (dos bits) que A envíe a B sobre los resultados de la medida de Bell, B será capaz de realizar la corrección adecuada.

Cabe hacer una aclaración importante, de cara a desarrollos posteriores. El estado teleportado es *idéntico* al original. Si el estado original estaba entrelazado con otro estado oculto fuera del circuito, el estado teleportado también quedará entrelazado a ese estado oculto. Al igual que para la codificación superdensa, Mermin escribió un artículo para la teleportación cuántica, en el que explica cómo se puede obtener esta a partir de un circuito estándar de intercambio de estados con puertas CNOT [41]. La derivación en dicho artículo es quizás el argumento más directo para convencerse de que la anterior afirmación es cierta. En todo caso, trataremos este tema de nuevo en el siguiente Capítulo, cuando hablemos de postergar medidas.

2.5. Realización de ordenadores cuánticos (estado de la técnica)

La construcción de ordenadores cuánticos es un problema formidable de Física e Ingeniería, en el que numerosas grandes empresas y gobiernos están invirtiendo considerable esfuerzo. La evolución de este campo es extremadamente rápida, con una cantidad virtualmente ilimitada de propuestas. En consecuencia, es difícil saber a ciencia cierta que tecnología prevalecerá, y cuál pasará a ser una mera curiosidad. Nosotros presentaremos las dos iniciativas más desarrolladas en la actualidad: los ordenadores cuánticos superconductores, y los ordenadores cuánticos de trampas de iones. Tras esto, terminaremos con una mínima reseña sobre los llamados "códigos correctores cuánticos".
Cabe aclarar, que esta sección no pretende en ningún caso ser una descripción completa, precisa y estrictamente correcta del hardware de ordenadores cuánticos. Más bien, el objetivo es proporcionar una pequeña muestra de la cantidad nada trivial de Física que hay detrás de los ordenadores cuánticos.
Para situarnos, comenzaremos enumerando los llamados " criterios de DiVincenzo" [42]. Estos criterios constituyen una referencia sólida para evaluar la viabilidad de un esquema de computación cuántica. Según DiVicenzo, un esquema de computación cuántica viable:

1. Es escalable y posee qubits están bien caracterizados.
2. Tiene capacidad de establecerse en un estado puro inicial.
3. Es estable, en el sentido de que el tiempo de coherencia de los qubits es mucho mayor que el tiempo de operación de las puertas.
4. Implementa un conjunto de puertas universal.
5. Puede medir correctamente el conjunto de sus qubits.

Estos criterios son *de mínimos* y parecen muy básicos, pero pocos sistemas reales se acercan a cumplirlos. Con ánimos de ajustarnos al artículo original, comentaremos que de cara a las comunicaciones cuánticas es deseable si nuestro sistema además:

6. Transforma de forma efectiva entre qubits "estáticos" y fotones.
7. Transmite fielmente fotones.

Con esto, estamos listos para adentrarnos en el mundo del hardware de ordenadores cuánticos.

2.5.1. Ordenadores cuánticos superconductores

En su eterna persecución de la ley de Moore, la industria de los semiconductores fabrica transistores cada vez más pequeños. A esas escalas empiezan a aparecer fenómenos como el efecto túnel: la Física Clásica comienza a fallar. En última instancia, el poder de los ordenadores convencionales vendrá limitado por estos efectos cuánticos. Sin embargo, para ordenadores cuánticos, estos efectos son justamente lo que necesitamos. La idea de los ordenadores cuánticos superconductores es pues utilizar las técnicas litográficas ya existente para fabricar diminutos circuitos que funcionen como qubits.
Se considera un pequeño circuito resonante LC en la escala micrométrica. Mediante helio líquido, estos circuitos se enfrían con el objetivo de eliminar todo ruido térmico. En particular, el circuito entra en régimen superconductor: los electrones pasan a formar pares de Cooper, por lo que se comportan como bosones.
A esas temperaturas, el circuito es un oscilador armónico cuántico, con niveles de energía $E_n\hbar\omega = \left(n + \frac{1}{2}\right)$ bien definidos y claramente separados. Entonces, el estado $|0\rangle$ corresponde al nivel con energía E_0 y el estado $|1\rangle$ corresponde al nivel de energía E_1. Pero surge un problema: al estar todos los niveles energéticos equiespaciados, es imposible evitar que, durante la operación, pueda acabar el qubit en superposición con niveles superiores E_2, E_3, etc. En ese caso, el sistema dejaría de consistir en dos niveles y realmente ya no tendríamos un qubit, tendríamos otra cosa más difícil de controlar y operar.
Este problema se corrige reemplazando la inductancia por una unión de Josephson, lo que rompe la linealidad: el pozo de potencial se vuelve anarmónico, y ahora el salto de energía $\omega_1 - \omega_0$ es diferente al resto de saltos. Cabe aclarar que el diseño descrito es una simplificación: hay muchos tipos de qubits superconductores, dónde los estados corresponden a cuantización de distintas cantidades (flujo, carga, fase). En particular, los más utilizados son los llamados "qubit transmon", que son particularmente estables.
Para implementar las puertas cuánticas, se envían pulsos de microondas de frecuencia y duración adecuada a los qubit (en cierto modo, los qubits están diseñan para operar en esta frecuencia, para la que ya hay multitud de equipamiento existente). Las puertas de 2 qubits requieren que los qubits involucrados interactúen de algún modo, lo que se logra conectándolos temporalmente a una cavidad resonante común. Las medidas se realizan con métodos similares (por supuesto, todo depende del tipo de qubit superconductor que tratemos). El lector que desee más información sobre qubits superconductores puede consultar los artículos de revisión [43, 44].
Sin duda, esta tecnología es la más madura en la actualidad. Como reflejo de esto, los ordenadores cuánticos de IBM, Google, Intel, Rigetti, etc., al igual que el "quantum annealer" de D-Wave, están todos ellos basados en qubits superconductores. Sin embargo, existe otra tecnología competidora: los ordenadores cuánticos de trampas de iones.

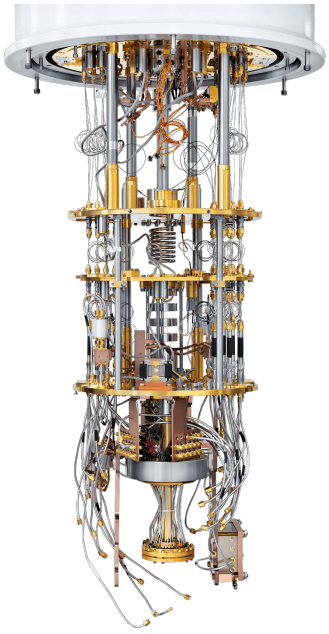


Figura 2.13: Foto del ordenador cuántico de Rigetti. En su página web, `https://www.rigetti.com/` hay una presentación visual de sus componentes.

2.5.2. Ordenadores cuánticos de trampas de iones

Otro enfoque natural consiste en utilizar los primeros entes físicos que se reconocieron como cuánticos: la nube electrónica de los átomos. Para aislar átomos individuales se deben tomar esencialmente dos pasos:

1. Extraer átomos de metales mediante vaporización, e ionizarlos mediante un láser con

frecuencia ajustada para solo pueda quitar los electrones más externos.

2. Meterlos en una trampa de iones. La trampa más común es la de Paul, donde se combina un campo eléctrico fijo con otro oscilante, para crear un potencial 2D en el plano XY, con un mínimo en el centro. Aplicando un tercer campo oscilante en el eje Z, se logra que los iones se organicen en una línea recta sobre el eje de la trampa.

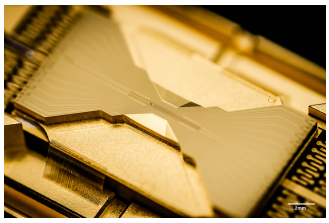


Figura 2.14:
Trampa de iones del ordenador de 32 qubits de IonQ. Fotografía de Kai Hudek. Página web: `https://ionq.com/`.

Una vez se ha logrado aislar un conjunto pequeño de iones en la trampa de Paul, es necesario enfriarlos hasta cerca de su estado vibracional base, para controlar la interacción entre los estados vibracionales y los estados electrónicos de los iones. Esto solo es posible mediante técnicas de enfriamiento láser (enfriamiento Doppler $\rightarrow$ enfriamiento de banda lateral).
En estas condiciones, para el par de niveles que constituye el qubit se pueden tomar una transición óptica, o una transición hiperfina (con el campo magnético externo correspondiente). En ambos casos, los qubits se inicializan y manipulan mediante láseres. Finalmente, la interacción entre qubits se logra mediante la transferencia de información cuántica entre estados electrónicos y estados vibracionales de la cadena. De esta forma, se logra una interconexión completa entre los qubits, frente a la interconexión solo de vecinos cercanos para qubits superconductores.
Además de esta interconexión completa, los ordenadores cuánticos de trampas de iones son menos sensibles a errores (para puertas de 2 qubits, fidelidad de $99,9$ frente a $99,4$ para los superconductores) y presentan mayor estabilidad (tiempo medio de decaimiento del orden de $1\ s$, frente a $100\ \mu s$ para los superconductores)[5]. Sin embargo, también tienen serios inconvenientes: son más difíciles de construir (en el sentido de que la tecnología no está tan desarrollada) y presentan problemas de escalado (las puertas de 2 qubits empiezan a ser difíciles de implementar para cadenas de más de 50 qubits, se requieren arquitecturas mucho más complejas para solucionar esto).
Hasta recientemente, no existía un ordenador cuántico de trampa de iones. La empresa emprendedora IonQ produjo en 2019 un ordenador cuántico de 11 qubits [45] y en Octubre de 2020 anunció por su página web un nuevo ordenador cuántico de 32 qubits, que declararon "el ordenador cuántico más potente del mundo" [46][6].

2.5.3. Corrección de errores y otras apreciaciones

La inherente fragilidad de los qubits es el principal obstáculo entre los primigenios ordenadores cuánticos actuales y las prometida revolución en computación. El problema es claro: mantener el sistema cuántico aislado de su entorno, salvo para la actuación de las puertas cuánticas, es extremadamente difícil.
En este sentido, se definen dos parámetros para medir los tipos de errores de un qubit:

- $T1$ es la constante de decaimiento exponencial para que los qubits en estado $|1\rangle$ pasen a ser una mezcla estadística perfecta.
- $T2$ es la constante de decaimiento exponencial para que los qubits en estado $\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$ pasen a ser una mezcla estadística perfecta.

[5]Los números citados son estrictamente orientativos, es extremadamente difícil conocer las capacidades concretas de los sistemas más modernos sin tener acceso directo a ellos.

[6]Pese a tener menos qubits que otros ordenadores cuánticos ya existentes, afirman que es mucho más estable y preciso, permitiendo la ejecución de algoritmos más largos en la práctica. Nosotros no entraremos más a valorar los méritos particulares de cada sistema: al fin y al cabo, todos ellos quedarán completamente obsoletos en cuestión de un par de años.

Respectivamente, miden la tendencia del sistema a relajarse, y a desfasarse, de cada qubit. A estos errores, debemos añadir los problemas de fidelidad (en el sentido [47, Chapter 2, pg.36]) de las puertas cuánticas: el estado final no corresponde, ni exactamente, ni consistentemente, al esperado para la operación implementada.
Los ordenadores cuánticos son ordenadores *analógicos*, en el sentido de que los estados están conectados por un continuo. En consecuencia, los errores que acabamos de plantear son *acumulativos*. Cuando los algoritmos cuánticos son suficientemente grandes (y esto, con la tecnología actual, significa prácticamente cualquier ejemplo que no sea de juguete), el estado final estará radicalmente alejado del previsto. Dicho de otro modo: el algoritmo falla.

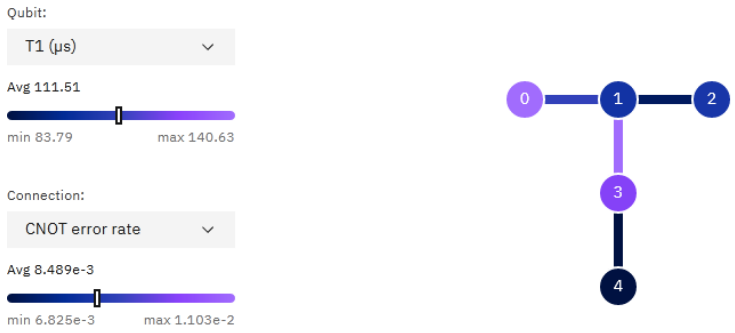


Figura 2.15:
Parámetro T_1 y ratio de error de las puertas CNOT del ordenador cuántico ibmq_vigo de IBM. Se aprecia claramente la individualidad de los qubits y de sus interconexiones.

Aquí cabe hacer un inciso. Si bien, especialemente en la figura 2.1, hemos estado marcando el número de qubits como indicación del progreso del hardware en Computación Cuántica, esta medida es entre incompleta y directamente engañosa. Con frecuencia, es más útil un ordenador cuántico con pocos qubits estables, que uno con muchos qubits ruidosos. Una métrica alternativa más fiable es el "volumen cuántico", término acuñado por el equipo de IBM en [48] que intuitivamente nos dice cómo de grandes son los algoritmos cuánticos que puede ejecutar un ordenador cuántico dado.
Para poder obtener ordenadores cuánticos efectivos, de momento se busca reducir los ratios de error todo lo posible. Pero esta estrategia que no es sostenible a largo plazo: una cierta cantidad de error es inevitable y el tiempo de coherencia es finito (y no tan largo). Se plantea pues la necesidad de utilizar *códigos correctores*.
Al igual que en los ordenadores clásicos existen los códigos correctores de errores, también existen esquemas similares para los ordenadores cuánticos. La gran diferencia es que, debido al Teorema de No Clonación, no es posible copiar la información de un estado cuántico repetidas veces. En vez de eso, la estrategia consiste en esparcir el estado de un solo qubit entre varios, con la esperanza de que los errores en múltiples qubits sean más raros que los errores de un solo qubit. De esta manera, con varios qubits "físicos" defectuosos, se logra un qubit "lógico" arbitrariamente perfecto.

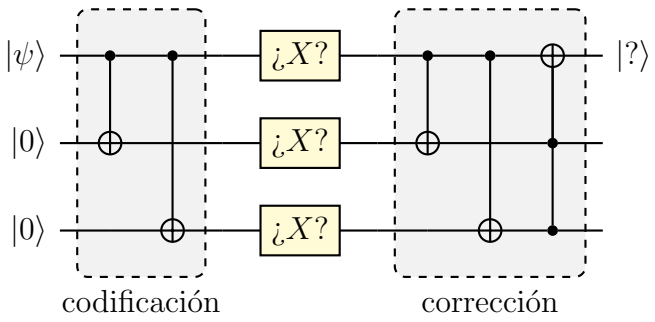


Figura 2.16:
Código corrector cuántico para errores de tipo inversión de qubit [49, pg.427]. Cada una de las puertas X amarillas representa un posible error sobre el qubit correspondiente. Todos estos errores son independientes, y cada uno ocurre con igual probabilidad p. Si no ocurre ningún error, o solo ocurre uno de ellos (lo cuál es el error más probable para p pequeña), es posible corregir el error de forma que el primer qubit queda en el estado original $|\psi\rangle$.

Cabe destacar que limitar los errores sigue siendo extremadamente importante. El ratio de qubits lógicos a qubits físicos, depende críticamente de ello. Para tecnologías actuales, se suele considerar un desesperanzador ratio de entre 1 : 1000 y 1 : 100, si bien recientemente se anunció un espectacular ratio de 1 : 13 [46].
En [50] se proporciona una perspectiva del progreso actual de la Computación Cuántica, en una fase caracterizada por tener decenas de qubits a los que no es posible aplicar corrección de errores. Si bien la tecnología de la Computación Cuántica se enfrenta a numerosos desafíos, eso no impide el continuo desarrollando los aspectos teóricos. Con esta apreciación finalizamos el Capítulo.

Capítulo 3

Equivalencia de circuitos cúanticos

> Back in the 1940s, researchers were just discovering how to use vacuum tubes as simple switches. ... These switches could then form logic gates, which could be linked together to form the first logic circuits. That's where we're at now with quantum processors. We have verified that all the components work. The next step is to engineer the smallest, yet most interesting circuit possible.
>
> *Jungsang Kim*

Los ordenadores cuánticos actuales tienen capacidades muy limitadas. Es por tanto natural que se programe "a bajo nivel", diseñando los circuitos cuánticos puerta por puerta. Tanto como para la compilación de algoritmos cuánticos como para la manipulación ágil de estos, es extremadamente útil conocer varias reglas de equivalencia, que permiten cambiar localmente estos circuito mientras se preserva su funcionamiento global.
El objetivo de este Capítulo es formar una base de reglas y técnicas básicas de equivalencia de circuitos. No se pretende ser exhaustivo, solo se introducen las equivalencias que necesitaremos más adelante. Para comenzar, haremos un par de apreciaciones:

- Todos los cálculos se han realizado en el modelo estándar de circuitos cuánticos. Existen otros métodos de cálculo basados en diagramas, como el cálculo ZX [51] o el cálculo ZH [52], pero en última instancia, se llega a los mismos resultados.
- Las equivalencias también se pueden obtener mediante el cálculo matricial, pero este es tedioso y no se recomienda.
- Si queremos comprobar que dos circuitos son equivalentes, por linealidad, basta comprobar que actúan de forma idéntica sobre los elementos de una base del espacio (normalmente, la base computacional).
- La fase de un estado cuántico no tiene significado físico cuando se considera ese estado cuántico aislado. Dicho de otro modo, la fase *global* no es relevante para las equivalencias.
- Por brevedad, se omite la mayor parte de las demostraciones, que en el fondo no son más que pura casuística. El lector que lo desee, podrá con pequeño esfuerzo comprobar por inspección que todas las equivalencias son ciertas.

- Muchas equivalencias son versiones simétricas de otras y se podría decir que son redundantes. Nosotros siempre optaremos a errar *por exceso* a errar *por defecto* en cuanto a la cantidad de equivalencias que enunciemos.

3.1. Equivalencias "del artículo"

Un buen artículo de referencia para equivalencias de circuitos cuánticos es [53]. Esta sección esta (tenuemente) basada en el artículo citado.

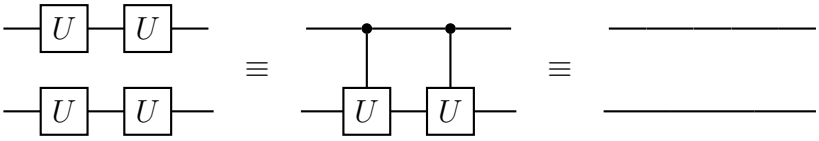
3.1.1. Reflexiones varias sobre equivalencias de puertas de 1 qubit, involuciones e inversiones de orden

Supongamos que tenemos dos operadores $U = U_1U_2 \dots U_n$ y $V = V_1V_2 \dots V_m$, correspondientes a dos circuitos equivalentes (es decir, $U = V$). Entonces $U^\dagger = V^\dagger$, lo cuál se expande a otra equivalencia:

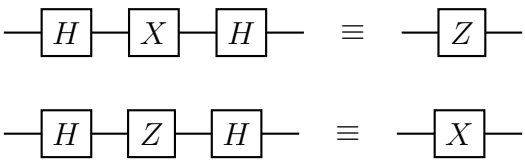
Frecuentemente, todas las puertas anteriores son involuciones, es decir, $U_i^\dagger = U_i$ para cada i, $V_j^\dagger = V_j$ para cada j. En ese caso, solo es necesario invertir el orden de aparición de las puertas para revertir la acción del circuito.
Para el caso más común de 1 qubit, un operador unitario es una involución si y solo si se verifica que $\phi + \lambda = \pi$, es decir, tiene matriz:

$$U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{ó} \quad U = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & e^{-i\phi}\sin\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) & -\cos\left(\frac{\theta}{2}\right) \end{bmatrix} \quad \begin{cases} \theta \in [0, \pi], \\ \phi \in [0, 2\pi). \end{cases}$$

En particular, los operadores de Pauli X, Y, Z son involuciones. Resulta que cualquier otra involución (no necesariamente unitaria) es combinación lineal de estos. El operador de Hadamard H también una involución.
A partir de estas involuciones de 1 qubit, pueden obtenerse involuciones de más qubits. Aunque sea trivial, notemos que si U es una involución, tanto $U^{\otimes n}$ como CU son involuciones:

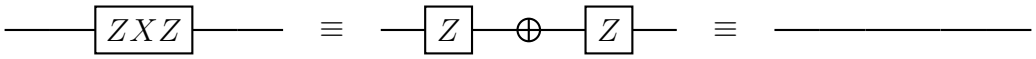


Para terminar, mencionamos la otra equivalencia importante de puertas de 1 qubit. Rotando la esfera de Bloch, es sencillo ver que $HXH = Z$. También se tiene que $HZH = X$, teniendo en cuenta que H es una involución:

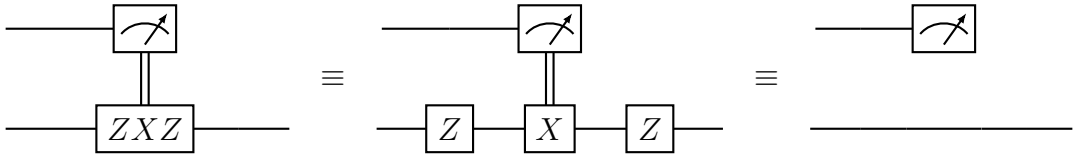


3.1.2. Una pequeña nota sobre equivalencias y control

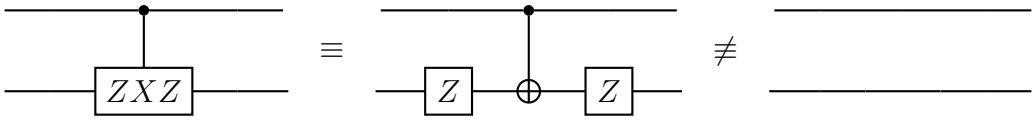
Si dos puertas A y B son equivalentes, no es necesariamente cierto que las puertas controladas CA y CB sean equivalentes. Se debe exigir además que la equivalencia entre A y B sea sin cambio de fase global.
Pongamos un ejemplo. Tenemos que $ZXZ = -\mathrm{Id}$, es decir, esta combinación de puertas induce un cambio de fase global. Esto se puede despreciar: realmente $ZXZ \equiv \mathrm{Id}$:



La situación es idéntica cuando estas puertas tienen control clásico:



Sin embargo, la cosa cambia cuando el control es cuántico e interviene otro qubit:

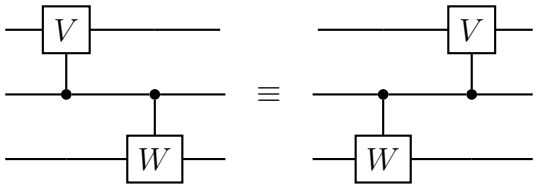


3.1.3. Movimiento de puertas controladas: generalidades

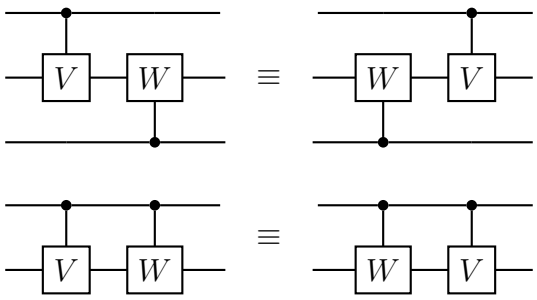
A riesgo de escribir una obviedad; para comprobar las equivalencias con puertas controladas CU, se deben distinguir dos casos:

- Si el qubit de control es $|0\rangle$, es como si la puerta U no estuviera presente.
- Si el qubit de control es $|1\rangle$, es como si la puerta U estuviera presente.

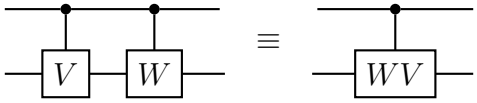
Cuando dos puertas (de cualquier tipo) no comparten qubits, es evidente que conmutan. Así que los casos que se deben analizar es cuando coinciden en algún qubit.
Sean CV, CW dos puertas controladas, correspondientes a los operadores unitarios V y W. Si estas puertas controladas comparten qubit de control, pero difieren en qubit objetivo, entonces siempre conmutan:



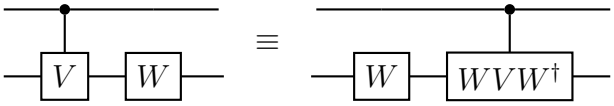
En este punto, cabe recordar que las puertas CZ son como un "doble control". Por ello, se pueden deslizar entre ellas y a través de otros controles (pero no de otros objetivos) con impunidad.
Además, si los operadores unitarios V y W conmutan, entonces las versiones controladas también conmutan cuando los objetivos están en el mismo qubit:



En particular, esto ocurre cuanto $V = W$.
Por otro lado, cuando aparecen dos puertas controladas seguidas con igual qubit de control e igual qubit objetivo, es evidente que se pueden combinar en una sola:



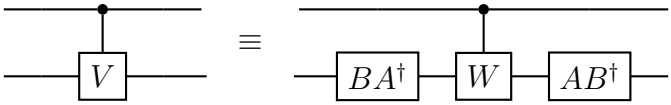
Una idea similar es la de hacer atravesar una puerta de 1 qubit a través del objetivo de una puerta controlada:



En esa línea, si V y W tienen los mismos autovalores, y como toda matriz unitaria es normal, por el Teorema Espectral se puede escribir

$$V = ADA^\dagger,$$
$$W = BDB^\dagger,$$

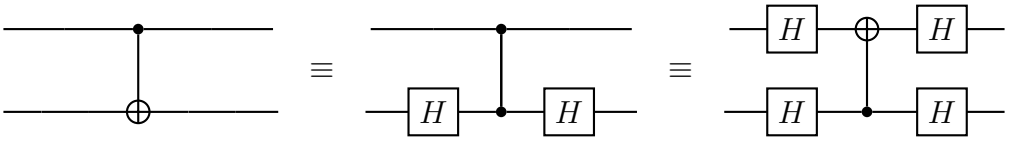
con A, B operadores unitarios y D una matriz diagonal. De este modo,

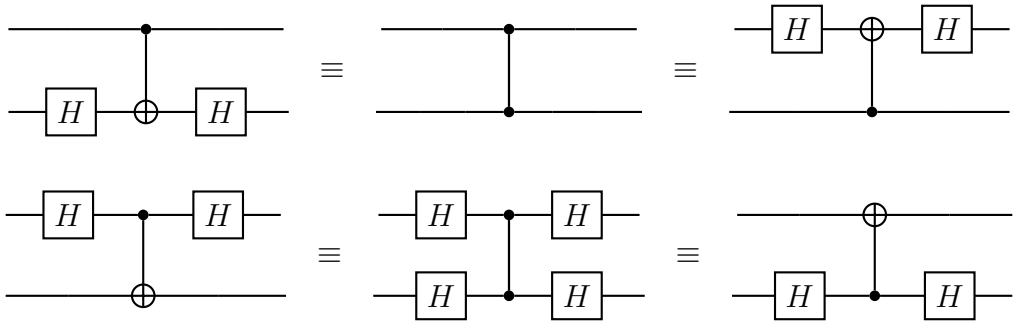


Para las tres equivalencias anteriores, es importante recordar que las puertas se leen de izquierda a derecha en el circuito, mientras que se leen de derecha a izquierda como fórmula. Es decir, si en el circuito aparece la puerta VW, primero se aplica el operador W y luego el operador V.

3.1.4. Inversión del control

Las puertas CNOT son, junto con las CZ, son las más comunes en las representaciones de circuitos cuánticos. Por eso, la mayoría de las equivalencias tratan sobre ellas. En particular, aquí tratamos la "inversión de control": bajo qué condiciones se puede intercambiar el qubit objetivo y el qubit de control de una puerta CNOT (recordemos que para la puerta CZ no existe distinción entre ambos).
A partir de $HXH = \mathrm{Id}$ y de $\mathrm{Id} = HH$ tenemos $CX = (\mathrm{Id} \otimes H)CZ(\mathrm{Id} \otimes H)$. Operando, obtenemos de manera inmediata las siguientes identidades:



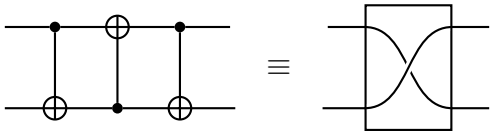


3.1.5. Diversas equivalencias con puertas CNOT

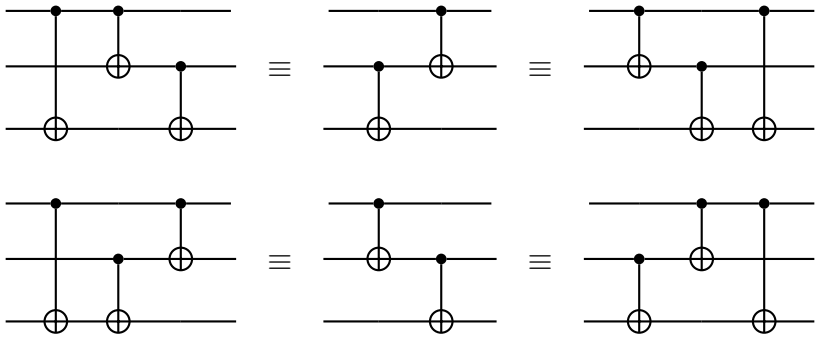
Como hemos remarcado, las principales puertas de 2 o más qubits que aparecen son las puertas CNOT. La primera equivalencia entre ellas que recogeremos es la de intercambio de qubits. La idea es idéntica al siguiente truco clásico con operaciones `XOR` bit a bit:

- Tenemos variables $[a]$ y $[b]$ que contiene dos números representados por cadenas de bits: $[a] = [\alpha]$ y $[b] = [\beta]$.
- Se asigna $[a] = [a] \oplus [b]$. Ahora queda $[a] = [\alpha] \oplus [\beta]$.
- Se asigna $[b] = [a] \oplus [b]$. Ahora queda $[b] = ([\alpha] \oplus [\beta]) \oplus [\beta] = [\alpha]$
- Se asigna $[a] = [a] \oplus [b]$. Ahora queda $[a] = ([\alpha] \oplus [\beta]) \oplus [\alpha] = [\beta]$. Ha terminado el intercambio.

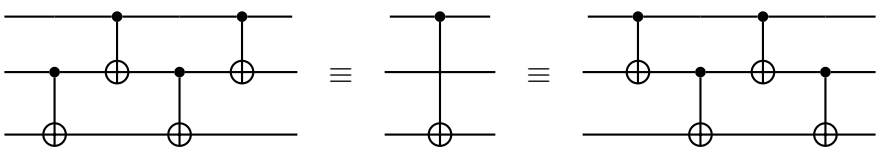
Si aplicamos esta idea a circuitos cuánticos, obtenemos la siguiente equivalencia:



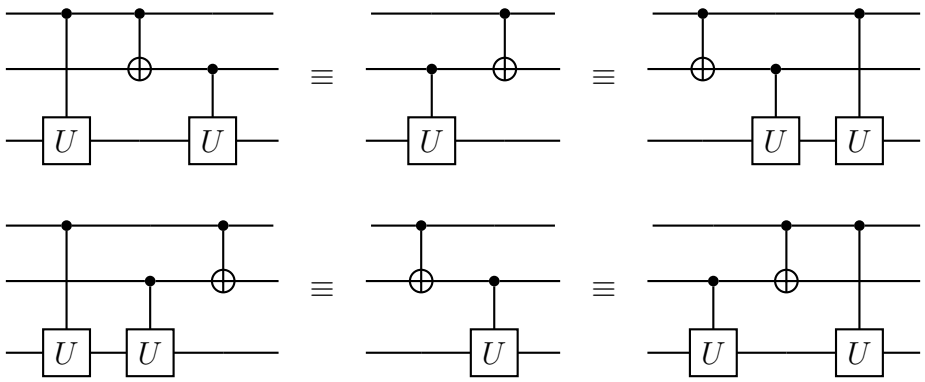
Además de este caso, el único otro caso no trivial ocurre cuando el control de una puerta CNOT está precedido por el objetivo de otra puerta CNOT. En ese caso, se tienen las equivalencias de "reflejo" siguientes:



Finalmente, a partir de cualquiera de las dos anteriores, obtenemos:



De cara a una aplicación posterior, enunciamos también una generalización de las equivalencias anteriores para cualquier puerta controlada CU que es una involución ($U^\dagger = U$):



3.1.6. Medidas

Existe controversia acerca de lo que constituye exactamente una medida en Mecánica Cuántica. Lo que está claro es que "la medida" es una herramienta conceptual que explica adecuadamente los resultados experimentales. Más allá de estos debates, aquí explicaremos bajo qué condiciones se pueden adelantar o atrasar las medidas en un circuito cuántico. Puesto que este es un punto algo delicado y muy crucial, proporcionaremos más detalles de los que seguramente sean necesarios.

Cuando termina la ejecución de un algoritmo cuántico, se obtienen estadísticas midiendo los qubits. No se tiene porqué medir todos: llamemos A al subconjunto de qubits medidos y B al subconjunto de qubits sin medir. La observación esencial es la siguiente: si no se realizan más operaciones de entrelazamiento conjunto entre A y B, todo lo que suceda en B (incluyendo mediciones) no puede tener efecto alguno en las estadísticas que obtengamos al medir A. Esto era el Teorema de No Comunicación. Al igual que no se incluyó una prueba de este Teorema en el **Capítulo 1**, tampoco se incluirá aquí. Pero sí que conviene reincidir en la idea, esta vez con un pequeño ejemplo. Imaginemos que tenemos un sistema de dos qubits, con estado:

$$|\psi\rangle = a_{00}\,|00\rangle + a_{01}\,|01\rangle + a_{10}\,|10\rangle + a_{11}\,|11\rangle\,,$$

Podríamos aplicar un operador unitario U al primer qubit:

$$U = \begin{bmatrix} u_1 & u_2 \\ u_3 & u_4 \end{bmatrix} \quad \begin{cases} |u_1|^2 + |u_3|^2 = |u_2|^2 + |u_4|^2 = 1, \\ u_1^\dagger u_2 + u_3^\dagger u_4 = 0. \end{cases}$$

Alternativamente, podríamos medir el primer qubit. Nos preguntamos cómo afecta cualquiera de estas acciones a las estadísticas del segundo qubit. Denotamos por m_i al resultado de la medida

del i-ésimo qubit. Resulta que:

$$\begin{aligned}
&P(m_2 = 0) \\
&= |\langle 00 \mid \psi \rangle|^2 + |\langle 10 \mid \psi \rangle|^2 \\
&= |a_{00}|^2 + |a_{10}|^2
\end{aligned}$$

$$\begin{aligned}
&P(m_2 = 0 \mid \text{ se mide antes el qubit 1}) \\
&= P(m_2 = 0 \mid m_1 = 0)P(m_1 = 0) + P(m_2 = 0 \mid m_1 = 1)P(m_1 = 1) \\
&= \left| \frac{a_{00}}{\sqrt{|a_{00}|^2 + |a_{01}|^2}} \right|^2 (|a_{00}|^2 + |a_{01}|^2) + \left| \frac{a_{10}}{\sqrt{|a_{10}|^2 + |a_{11}|^2}} \right|^2 (|a_{10}|^2 + |a_{11}|^2) \\
&= |a_{00}|^2 + |a_{10}|^2
\end{aligned}$$

$$\begin{aligned}
&P(m_2 = 0 \mid \text{ se aplica } U \text{ antes al qubit 1}) \\
&= |\langle 00| (U \otimes \mathrm{Id}) |\psi\rangle|^2 + |\langle 10| (U \otimes \mathrm{Id}) |\psi\rangle|^2 \\
&= |u_1 a_{00} + u_2 a_{10}|^2 + |u_3 a_{00} + u_4 a_{10}|^2 \\
&= (|u_1|^2 + |u_3|^2)|a_{00}|^2 + (|u_2|^2 + |u_4|^2)|a_{10}|^2 + (u_1^* u_2 + u_3^* u_4) a_{00}^* a_{10} + (u_1 u_2^* + u_3 u_4^*) a_{00} a_{10}^* \\
&= |a_{00}|^2 + |a_{10}|^2
\end{aligned}$$

Esto justifica que se tome el convenio de que todos los qubits se miden al final del algoritmo cuántico. También hemos visto que no importa en que base se realice esta medición.
Una vez que planteamos todas las medidas, surge en ocasiones la posibilidad de reemplazar puertas cuánticas por clásicas (lo cuál suele ser muy deseable). Cuando la base formada por los productos tensoriales los autovectores de cada medida permanezca invariante por los elementos cuánticos que les preceden, estos elementos se pueden sustituir por operaciones clásicas sin cambiar las estadísticas.
En el caso de las puertas controladas ocurre algo especial. Si tenemos el control de una puerta controlada cuántica CV justo antes de una medida, es posible cambiar el orden. De esta forma, primero se realizaría la medida y luego se ejecutaría o no la puerta controlada clásica cV dependiendo del resultado.
Hagamos las cuentas. Apliquemos primero el operador CV al estado $|\psi\rangle$:

$$CV |\psi\rangle = a_{00} |00\rangle + a_{01} |01\rangle + a_{10} |1\rangle V |0\rangle + a_{11} |1\rangle V |1\rangle .$$

Si medimos el primer qubit, obtenemos:

Con probabilidad $|a_{00}|^2 + |a_{01}|^2$,
la medida es $m_1 = 0$ y el estado resultante es (salvo normalización) $a_{00} |0\rangle + a_{01} |1\rangle$,
Con probabilidad $|a_{10}|^2 + |a_{11}|^2$,
la medida es $m_1 = 1$ y el estado resultante es (salvo normalización) $a_{10} V |0\rangle + a_{11} V |1\rangle$.

Imaginemos por el contrario que primero medimos el primer qubit:

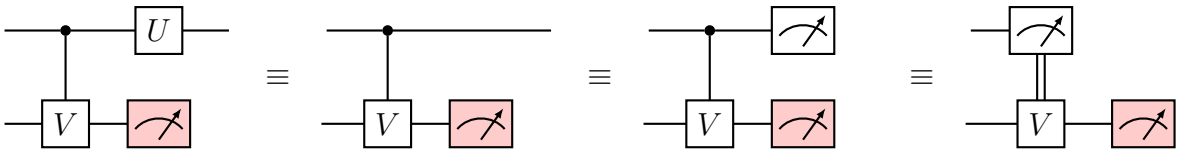
Con probabilidad $|a_{00}|^2 + |a_{01}|^2$,
la medida es $m_1 = 0$ y el estado resultante es (salvo normalización) $a_{00} |0\rangle + a_{01} |1\rangle$,
Con probabilidad $|a_{10}|^2 + |a_{11}|^2$,
la medida es $m_1 = 1$ y el estado resultante es (salvo normalización) $a_{10} |0\rangle + a_{11} |1\rangle$.

Las probabilidades, obviamente, son iguales. Solo en el segundo caso corresponde aplicar la puerta V, ahora con control clásico. De este modo obtenemos:

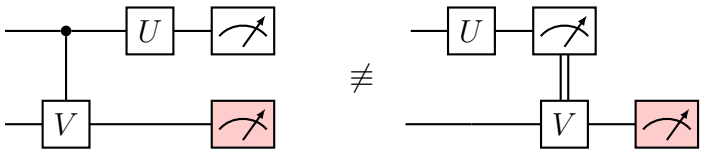
Con probabilidad $|a_{00}|^2 + |a_{01}|^2$,
la medida es $m_1 = 0$ y el estado resultante es (salvo normalización) $a_{00}|0\rangle + a_{01}|1\rangle$,
Con probabilidad $|a_{10}|^2 + |a_{11}|^2$,
la medida es $m_1 = 1$ y el estado resultante es (salvo normalización) $a_{10}V|0\rangle + a_{11}V|1\rangle$,

es decir, exactamente los mismos estados, con las mismas probabilidades.

Traduzcamos los dos resultados anteriores al lenguaje de circuitos. Pintamos de rojo la última operación que se realiza en el circuito, una medida. En los cuatro casos, se obtienen *las misma estadísticas* en la medida roja:



Por otro lado, cuando hay una puerta (que no tenga como autovectores la base computacional) precediendo a la medida, no se puede adelantar el control cuántico:



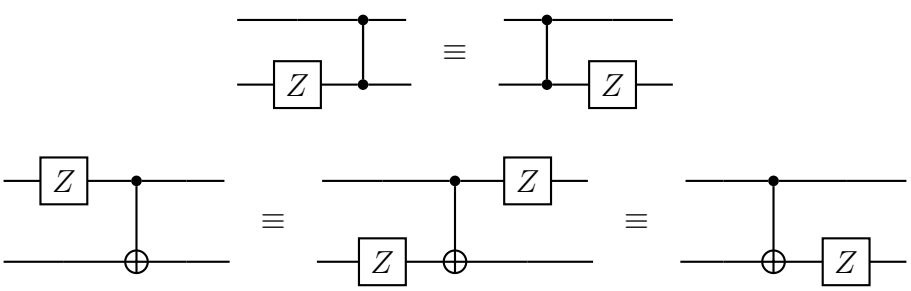
3.2. Equivalencias adicionales

En la elaboración de los circuitos de este Trabajo de Fin de Grado, el alumno se vio forzado a derivar nuevas equivalencias que no venían recogidas en [53]. Todas ellas son fáciles: sin duda, la mayoría vendrán recogidas en otros textos.

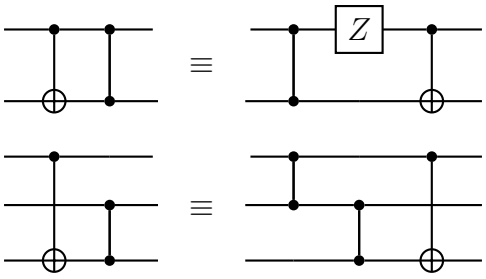
3.2.1. Conmutación de CNOT con Z y CZ

Primero consideramos la igualdad $XZ = -ZX$. Como el cambio de fase global no importa, se pueden conmutar ambas puertas cuánticas de 1 qubit.

Pero, de nuevo, la cosa cambia cuando intervienen controles cuánticos. Sin más dilación, proporcionamos las reglas de movimiento de Zs con CZs y CNOTs. Por evitar seguir añadiendo a la ya exagerada redundancia, omitiremos las versiones reflejadas de las equivalencias:



Ahora, damos las equivalencias que faltan para mover CZs y CNOTs entre sí.



3.2.2. Algunos trucos con el estado $|\Phi^+\rangle$

Cuando, en vez de para todas las entradas, consideramos equivalencias para un circuito con una entrada concreta, se pueden hacer muchos trucos que de otro modo no serían posibles (es decir, plantear equivalencias que no son ciertas en general). Nosotros nos centraremos en el estado $|\Phi^+\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$, que admite mucho juego debido a su alta simetría.
Para comenzar, analicemos lo que ocurre cuando aplicamos un operador U genérico, escrito en ángulos de Euler, al qubit inferior del estado $|\Phi^+\rangle$:

$$(\mathrm{Id} \otimes U)\left[\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right] =$$
$$\frac{1}{\sqrt{2}}\left[\cos(\theta/2)\,|00\rangle + e^{i\phi}\sin(\theta/2)\,|01\rangle - e^{i\lambda}\sin(\theta/2)\,|10\rangle + e^{i(\phi+\lambda)}\cos(\theta/2)\,|11\rangle\right].$$

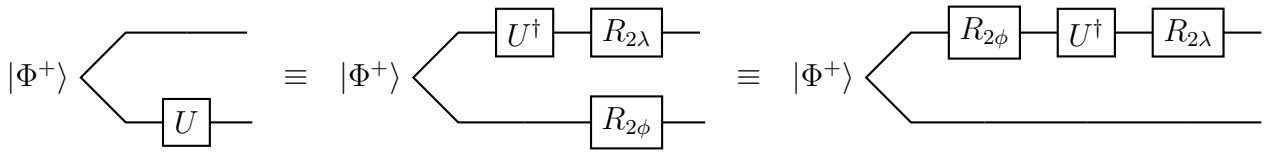
Por otra parte, si aplicamos $U^\dagger$ al qubit superior, obtenemos:

$$(U^\dagger \otimes \mathrm{Id})\left[\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right] =$$
$$\frac{1}{\sqrt{2}}\left[\cos(\theta/2)\,|00\rangle + e^{-i\phi}\sin(\theta/2)\,|01\rangle - e^{-i\lambda}\sin(\theta/2)\,|10\rangle + e^{i(-\phi-\lambda)}\cos(\theta/2)\,|11\rangle\right],$$

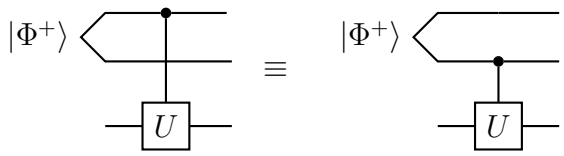
que es un estado bastante parecido al anterior. Las diferencias se arreglan mediante un par de correcciones de fase,

$$(\mathrm{Id} \otimes U)\,|\Phi^+\rangle = (R_{2\lambda} \otimes R_{2\phi})(U^\dagger \otimes \mathrm{Id})\,|\Phi^+\rangle = ((R_{2\lambda}U^\dagger R_{2\phi}) \otimes \mathrm{Id})\,|\Phi^+\rangle\,.$$

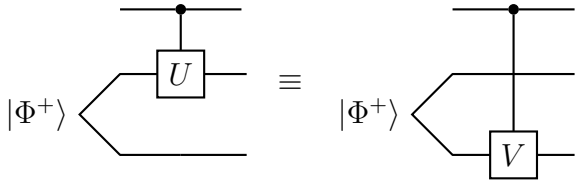
La segunda igualdad se obtiene o bien a mano, o bien por la primera igualdad, teniendo en cuenta que el operador $R_{2\phi}$ tiene ángulos de Euler $\phi = \lambda = 0$ (el "2ϕ" de $R_{2\phi}$ marca el valor del ángulo de Euler θ). Representemos la equivalencia de circuitos resultante:



Por supuesto, también se podría realizar el cambio contrario, poniendo la puerta U en el qubit superior. Lo escribimos así porque esta será en la forma en la que aplicaremos la equivalencia más adelante.
Ahora estudiamos el movimiento de puertas controladas entre qubits distintos. Como para el estado $|\Phi^+\rangle$, ambos qubits valen $|0\rangle$, o ambos valen $|1\rangle$, el control de una puerta que esté sobre este estado, puede cambiar de qubit sin afectar el circuito:



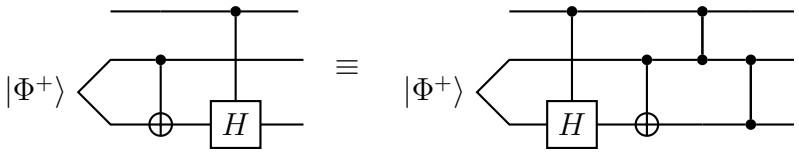
Por otro lado, imaginemos que tenemos una situación como la anterior: sobre un estado $|\Phi^+\rangle$, es equivalente aplicar la puerta U en el qubit inferior, que la puerta V (correspondiente al operador $V = R_{2\lambda}U^\dagger R_{2\phi}$) en el qubit superior. En ese caso, también se puede realizar el movimiento si U y V están controladas:



Esta técnica se puede generalizar considerablemente. Podríamos considerar cualesquiera dos circuitos controlados que sean equivalentes cuando actúan sobre un estado prefijado. Pero, en la práctica, nosotros solo la aplicaremos como aparece en los diagramas de circuitos anteriores.

3.2.3. Una equivalencia "sacada de la manga"

Para finalizar, planteamos una equivalencia[1]muy específica, que se aplicará a un paso muy específico de un desarrollo posterior. No hay mucho más que decir. Se comprueba distinguiendo dos casos: si el qubit superior vale $|0\rangle$, los dos qubits inferiores acaban en el estado $|+0\rangle$; si el qubit superior vale $|1\rangle$, los dos qubits inferiores acaban en el estado $|{+}{+}\rangle$:



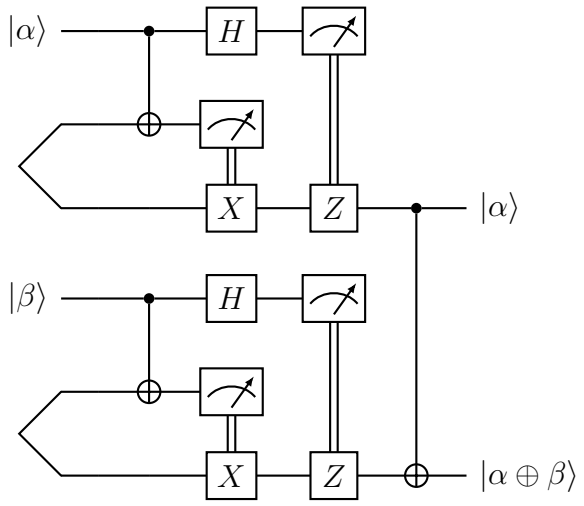
3.3. Entrelazamiento remoto a partir de teleportación

Terminamos este Capítulo con una explicación de la técnica que se usará para producir los circuitos que figuran en el **Capítulo 4** de este Trabajo de Fin de Grado.

3.3.1. Teleportación de puertas

Recordemos que el circuito cuántico de teleportación permitía transmitir un estado cuántico de forma íntegra, *incluyendo su entrelazamiento*.
Consideramos pues la siguiente situación. Teleportamos dos qubits y tras esto les aplicamos una puerta CNOT. Naturalmente, el estado final resultante será el mismo que si hubiéramos aplicado una puerta CNOT a los qubits iniciales y teleportáramos el resultado.

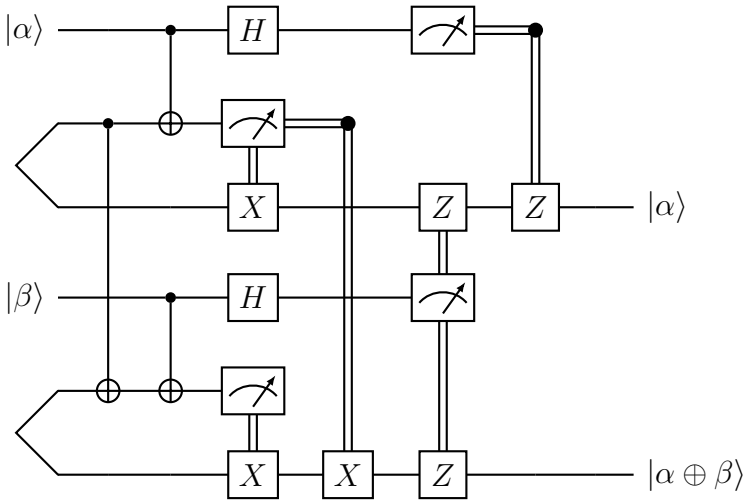
[1]Si realmente se puede llamar "equivalencia" a este apaño, fruto de trastear con el editor de circuitos de IBM a altas horas de la madrugada.



En su famoso artículo [35], Gottesman y Chuang propusieron la idea de realizar computación cuántica a través de estados entrelazados recurso, de medidas y de puertas cuánticas de un solo qubit. En [53], mediante la aplicación diligente de las equivalencias recogidas en este Capítulo, se da una interpretación del esquema de Gottesman-Chuang en términos de teleportación de puertas cuánticas. La técnica básica es como sigue:

1. **Se plantea el circuito inicial teleportado.**
2. **Se postergan las medidas, de manera que las puertas controladas clásicamente se conviertan en controladas cuánticamente.**
3. **Para cada puerta teleportada, se emplean equivalencias para moverla hacia la izquierda, hasta llegar al inicio de los estados de Bell $|\Phi^+\rangle$.**
4. **Con las propiedades de estos pares EPR, se mueve ahora la puerta hacia arriba. En el caso de puertas controladas cuánticas, esto significa cambiar tanto el qubit de control como el qubit objetivo.**
5. **Se repiten los dos pasos anteriores, para todas las puertas del circuito cuántico teleportado.**
6. **Se adelantan las medidas, con la esperanza de que todas las puertas nuevas que se hayan introducido durante las equivalencias queden con control clásico.**

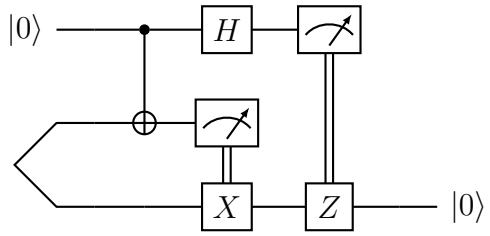
Este procedimiento permite llegar sin mucha dificultad al siguiente circuito equivalente:



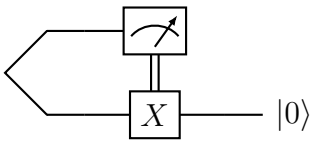
Notemos que ahora la puerta CNOT actúa sobre los qubits auxiliares (el $2^{\underline{o}}$ y el $5^{\underline{o}}$), en vez de actuar sobre los qubits de entrada (el $1^{\underline{o}}$ y el $4^{\underline{o}}$) o los qubits de salida (el $3^{\underline{o}}$ o el $6^{\underline{o}}$). Dicho de otro modo, una vez compartidos los dos pares EPR, *una medida conjunta adecuada sobre los qubits auxiliares entrelaza remotamente los dos qubits de salida.*
Cabe destacar que no siempre queda el circuito final tan sencillo. En particular, para operadores unitarios arbitrarios U y V, no siempre es posible intercambiar de orden las puertas CU y CV sin aumentar la complejidad del circuito. En esos casos es necesario introducir puertas Toffoli, que son más costosas computacionalmente y más difíciles de manejar. Nosotros tenemos la suerte de poder evitar la aparición de puertas Toffoli, aunque queda abierta esa posibilidad para futuras exploraciones de esta técnica.

3.3.2. Teleportación de estados

Si fijamos el estado inicial en la teleportación de puertas, obtenemos la teleportación de estados. En particular, fijemos que los estados iniciales ($|\alpha\rangle$, $|\beta\rangle$ en los circuitos anteriores) sean ahora todos $|0\rangle$. La "unidad inicial de teleportación" queda como:



En estas condiciones, no se activará nunca la primera CNOT, y que la puerta Z controlada clásicamente no afecta al qubit de abajo, que se encontrará en el estado $|0\rangle$. Dichos de otro modo: el primer qubit y todas las puertas asociadas son superfluos. Si los eliminamos, ahora queda una "unidad inicial" más sencilla:



Si se desarrolla el estado $|\Phi^+\rangle$ con la puerta H y la puerta CNOT, vemos que este circuito es prácticamente trivial. Sin embargo, esconde ciertas ideas. La medida del qubit superior tiene igual probabilidad de dar 0 que 1. Esta propiedad, que se conservará durante todas las equivalencias, se puede interpretar como que "estamos aprovechando el máximo poder corrector que proporciona la medida". Por otro lado, el qubit inferior acaba en el estado $|0\rangle$, que es por excelencia el estado inicial de todo circuito cuántico.
Entonces, nuestra idea es emplear las equivalencias desarrolladas en este Capítulo, para mover puertas colocadas en estas "unidades iniciales". Esto se traduce en un entrelazamiento remoto, que buscaremos que sea tripartito. Más particularmente, queremos crear remotamente los estados $|GHZ\rangle$ y $|W\rangle$, aplicando la técnica que acabamos de exponer para los circuitos 2.8 y 2.9.

Capítulo 4

Creación de estados entrelazados mediante Fotónica

> At the first of the 1960's Rochester Coherence Conferences, I suggested that a license be required for use of the word photon, and offered to give such license to properly qualified people.
>
> *Willis Eugene Lamb*

Desde que en 1905 Einstein explicó el efecto fotoeléctrico mediante "cuantos de luz"[54], los fotones se han convertido en uno de los entes cuánticos mejor estudiados. No solo aparecen en el cálculo de diversas interacciones en las que se debe cuantizar el campo electromagnético, sino que también se pueden manejar con precisión en el laboratorio. En particular, las predicciones "paradójicas" de la Mecánica Cuántica han sido comprobadas numerosas veces mediante experimentos con fotones (ver [4, 55], por ejemplo).
En este Capítulo aplicaremos el método de teleportación de estados introducido en el **Capítulo 3** para tratar el problema de generación de los estados $|GHZ\rangle$ y $|W\rangle$ de tres fotones triplemente entrelazados. Por el camino, con el objetivo de añadir contexto y mostrar varias áreas fascinantes de la Física, exploramos brevemente el papel que juega la luz en la Computación Cuántica.

4.1. Computación cuántica a base de fotones

Un fotón posee diversos parámetros donde se puede codificar un qubit: cajas temporales, frecuencia, momento angular orbital... Por fijar ideas, supongamos de momento que los qubits están codificados en la polarización del fotón. El estado de polarización horizontal se denota por $|H\rangle$ y el de polarización vertical por $|V\rangle$. Tomamos el convenio de que

$$|H\rangle = |0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \qquad |V\rangle = |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}.$$

De este modo, un estado de polarización general se representa como[1] :

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$$
$$|\alpha|^2 + |\beta^2| = 1.$$

[1]Esto es idéntico al cálculo de Jones para luz clásica. La única diferencia es que $|\alpha|^2 + |\beta|^2$, que antes sería proporcional a la amplitud de la onda electromagnética, ahora se toma normalizado a 1. No tiene sentido hablar de la amplitud de un fotón. En todo caso, si la onda electromagnética fuera más o menos intensa, hablaríamos del número de fotones.

Los fotones son notablemente estables comparados con otras alternativas de qubits: las pérdidas son pequeñas cuando viajan a través del aire, el vidrio u otros medios transparentes. Los fotones se pueden crear e "inicializar" con facilidad mediante láseres y polarizadores, y también se puede medir su polarización mediante divisores de haces y detectores de fotones. Adicionalmente, los fotones son el único tipo de qubit que se puede transmitir íntegramente a través de largas distancias, como se ha podido comprobar en experimentos de teleportación cuántica por fibra óptica [55]. Añadamos a lo anterior que toda operación unitaria de 1 qubit se puede implementar con facilidad con Óptica Lineal [56, II-B]. ¿Cuál es el fallo?
Los fotones raramente interactúan entre ellos. Siendo más precisos y correctos, es difícil que un fotón produzca un cambio de polarización en otro. En esa situación, ¿cómo producir entrelazamiento?
Este es el mayor obstáculo al que se enfrenta la Computación Cuántica mediante fotones. En [57] se hace un análisis de las avenidas principales para crear ordenadores cuánticos en el ámbito de la Óptica Lineal. La idea principal, el llamado esquema KLM [58], consiste en utilizar fotones auxiliares para crear interferencias en divisores de haces y así generar entrelazamiento espacial. Nosotros no vamos a explicar este curioso esquema, si bien algunas de sus ideas intervendrán en los elementos que utilizaremos más adelante para construir el circuito óptico.
También cabe mencionar que existen otras propuestas tentativas para crear puertas controladas mediante efectos no lineales. Ya sea mediante efecto Zenon cuántico con absorción de dos fotones [59] o mediante efecto Kerr cruzado [60], estas otras vías son muy interesantes desde el punto de vista teórico y práctico.
Finalmente mencionamos una alternativa que, si bien no alcanzan el grado de "ordenador cuántico universal", sí permite realizar computaciones con fotones que no son viables con un ordenador convencional [61]. En ese sentido, recientemente (a finales de 2020) se ha logrado un nuevo hito de supremacía cuántica: se obtuvo la solución de cierto problema matemático[2] fuera del alcance de los ordenadores clásicos mediante la medida de las interferencias producidas por 100 fotones en un complejo interferómetro [62].
Tras esta presentación general nos metemos de lleno en las matemáticas del asunto.

4.1.1. Óptica Lineal y Mecánica Cuántica

Para operar de forma precisa debemos emplear estados de Fock (es decir, situarnos en el ámbito de la segunda cuantización). Nuestros fotones se pueden encontrar en un conjunto de modos ortogonales[3], y cada modo puede ser ocupado por cualquier cantidad de fotones. Nosotros consideraremos tan solo los modos definidos por la polarización y por la trayectoria espacial de los fotones.
Si tenemos un estado $|\psi\rangle$ que consiste en n_1 fotones en el modo 1, n_2 fotones en el modo 2, ..., n_m fotones en el modo m, la notación es

$$|n_1, n_2, \ldots, n_m\rangle_{1,2,\ldots,m} .$$

Todos los elementos ópticos actúan unitariamente, suponiendo que no hay pérdidas de energía. Describiremos dos elementos importantes: la lámina desfasadora y el divisor de haz.
Una lámina desfasadora permiten modificar la fase del modo horizontal con respecto a la fase del modo vertical. Si suponemos que su eje óptico alineado con la horizontal, la lámina de onda actúa sobre un fotón como

$$\alpha\,|10\rangle_{HV} + \beta\,|01\rangle_{HV} \to \alpha'\,|10\rangle_{HV} + \beta'\,|01\rangle_{HV} ,$$

[2] Más concretamente, la función de distribución del permanente de una matriz cuyas entradas son gaussianas.
[3] Intuitivamente, corresponden a los distintos modos de propagación de la onda electromagnética/luz por el circuito.

donde α' y β' vienen dados por

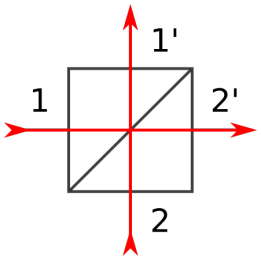
$$\begin{bmatrix}\alpha'\\ \beta'\end{bmatrix} = \begin{bmatrix}1 & 0\\ 0 & e^{i\phi}\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}.$$

Aquí ϕ es el ángulo de desfase ($\phi = \pi/2$ para láminas $\lambda/4$, $\phi = \pi$ para láminas $\lambda/2$). Cuando rotamos la lámina un ángulo θ, en sentido horario mirando a favor de la dirección de propagación de la luz, la matriz resultante es

$$\begin{bmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & e^{i\phi}\end{bmatrix}\begin{bmatrix}\cos(\theta) & \sin(\theta)\\ -\sin(\theta) & \cos(\theta)\end{bmatrix}.$$

Lo único que hemos hecho es multiplicar por una matriz de rotación a un lado y desahacer el cambio al otro. Esta misma idea funciona para cualquier otro elemento óptico (en la polarización). Mediante tan solo tres láminas de onda convenientemente rotadas es posible implementar cualquier operación unitaria sobre un fotón (en la polarización) [56, II-B].
Por otro lado, tenemos los divisores de haz. Estos elementos permiten que los fotones entren y salgan por distintos caminos.
Un divisor de haz actúa sobre un fotón como

$$\alpha\,|10\rangle_{12} + \beta\,|01\rangle_{12} \to \alpha'\,|1'2'\rangle_{HV} + \beta'\,|01\rangle_{1'2'},$$



donde α' y β' vienen dados por

$$\begin{bmatrix}\alpha'\\ \beta'\end{bmatrix} = \begin{bmatrix}\sqrt{R} & \sqrt{T}\\ \sqrt{T} & -\sqrt{R}\end{bmatrix}\begin{bmatrix}\alpha\\ \beta\end{bmatrix}.$$

Aquí T es el factor de transmisión y $R = 1 - T$ es el factor de reflexión[4]. Existen divisores de haz que actúan de forma distinta según la polarización. En ese caso, debemos especificar un T_H para la acción sobre la polarización horizontal y un T_V para la acción sobre la polarización vertical[5].
La cuestión se complica cuando interviene más de un fotón. Mediante el uso de los operadores de creación y aniquilación se puede llegar a una fórmula general (ver fórmula 28 en [63]). Intuitivamente, "hay que sumar sobre todos los caminos conjuntos que pueden seguir los fotones". Esto se ve mejor con un ejemplo:

Tomamos un divisor de haz con $T = 1/2$. Actúa sobre un solo fotón como:

$$|10\rangle_{12} \to \frac{1}{\sqrt{2}}\,|10\rangle_{1'2'} + \frac{1}{\sqrt{2}}\,|01\rangle_{1'2'}$$
$$|01\rangle_{12} \to \frac{1}{\sqrt{2}}\,|10\rangle_{1'2'} - \frac{1}{\sqrt{2}}\,|01\rangle_{1'2'}$$

Denotamos a sus coeficientes según la trayectoria que sigue el fotón correspondiente:

$$|10\rangle_{12} \to a_{1\to 1'}\,|10\rangle_{1'2'} + a_{1\to 2'}\,|01\rangle_{1'2'}$$
$$|01\rangle_{12} \to a_{2\to 1'}\,|10\rangle_{1'2'} + a_{2\to 2'}\,|01\rangle_{1'2'}$$

[4]Cabe notar que es posible escribir la matriz en otras formas, según convengamos los "puertos de entrada" y "puertos de salida" del elemento, es decir, desde dónde se empieza a medir la fase de cada entrada y cada salida. La forma que hemos escogido es quizás menos simétrica en su actuación que la otra forma habitual, que es $\begin{bmatrix}\sqrt{R} & i\sqrt{T}\\ i\sqrt{T} & \sqrt{R}\end{bmatrix}$, pero tiene la ventaja de evitar ir arrastrando los factores i.

[5]Ahora los "puertos de entrada" y "puertos de salida" se comparten para ambas polarizaciones, así que pueden aparecer desfases que no están recogidos en la forma de la matriz. Nosotros supondremos que no los hay. Si los hubiera, se podría arreglar situando láminas retardadoras en los "puertos" de los primas.

Si ahora consideramos dos fotones, uno por cada entrada, debemos hacer la suma sobre todos los caminos conjuntos[6]:

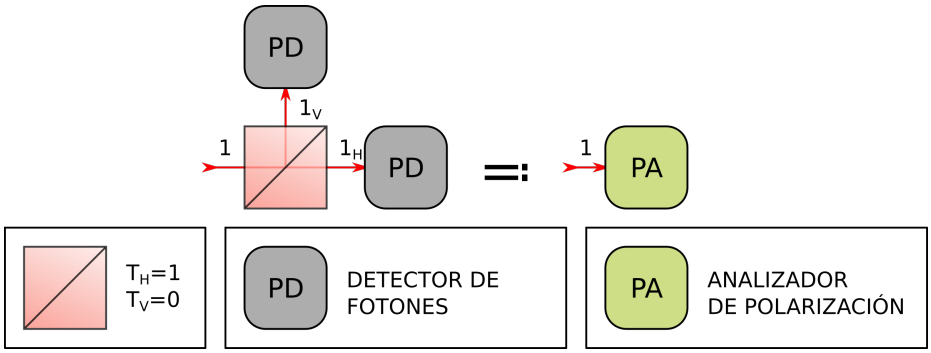
$$
\begin{aligned}
|11\rangle_{12} \to & \sqrt{2}[a_{1\to 1'}a_{2\to 1'}]\,|20\rangle_{1'2'} + && \text{(dos fotones salen por arriba)}\\
& [a_{1\to 1'}a_{2\to 2'} + a_{1\to 2'}a_{2\to 1'}]\,|11\rangle_{1'2'} + && \text{(un fotón sale por cada lado)}\\
& \sqrt{2}[a_{1\to 2'}a_{2\to 2'}]\,|02\rangle_{1'2'} + && \text{(dos fotones salen por abajo)}\\
& = \sqrt{2}\left[\tfrac{1}{\sqrt{2}}\tfrac{1}{\sqrt{2}}\right]|20\rangle_{1'2'} + \left[\tfrac{1}{\sqrt{2}}\tfrac{-1}{\sqrt{2}}+\tfrac{1}{\sqrt{2}}\tfrac{1}{\sqrt{2}}\right]|11\rangle_{1'2'} + \sqrt{2}\left[\tfrac{1}{\sqrt{2}}\tfrac{-1}{\sqrt{2}}\right]|02\rangle_{1'2'}\\
& = \frac{1}{\sqrt{2}}\,|20\rangle_{1'2'} - \frac{1}{\sqrt{2}}\,|02\rangle_{1'2'}
\end{aligned}
$$

En conclusión, ¡los dos fotones siempre salen juntos!

Este es el efecto Hong-Ou-Mandel [64]. El funcionamiento de varios de los elementos posteriores se explican con el mismo tipo de cálculos.

4.1.2. Analizador de polarización

El analizador de polarización (PA, de sus siglas en inglés) mide los fotones en la base $\{|H\rangle, |V\rangle\}$. No supondremos que tenga la capacidad de contar fotones, solo la capacidad de detectarlos. A cada detección (activación de un detector de fotones) se le llama también "click". El número de clicks no depende tan solo del número de fotones incidentes, sino también de su polarización. Por ejemplo, para el estado $|2,0\rangle_{HV}$ solo obtendremos un click en el detector superior, mientras que para el estado $|1,1\rangle_{HV}$ obtendremos dos clicks, uno en cada detector.



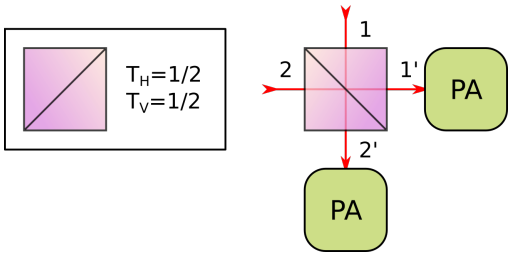
[6]Los factores $\sqrt{2}$ multiplicando a los términos con 2 fotones en un mismo modo aparecen por motivos de normalización (o, desde otro punto de vista, por motivos combinatorios). En general, cuando aparece un estado $|n_1, n_2, \ldots, n_m\rangle_{1,2,\ldots,m}$, debe ir acompañado por un factor $\sqrt{n_1!n_2!\ldots n_m!}$, ya sea a la entrada o a la salida del elemento óptico. Ver [63, III] para una justificación completa del método.

4.1.3. Medida parcial de Bell

Mediante la suma de todos los caminos conjuntos, se puede comprobar que este elemento actúa sobre los estados de Bell como:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}[|1,0,1,0\rangle_{1H,1V,2H,2V} + |0,1,0,1\rangle_{1H,1V,2H,2V}]$$
$$\rightarrow \frac{1}{2}[|2,0,0,0\rangle_{1'H,1'V,2'H,2'V} + |0,2,0,0\rangle_{1'H,1'V,2'H,2'V} - |0,0,2,0\rangle_{1'H,1'V,2'H,2'V} - |0,0,0,2\rangle_{1'H,1'V,2'H,2'V}],$$
$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}[|1,0,1,0\rangle_{1H,1V,2H,2V} - |0,1,0,1\rangle_{1H,1V,2H,2V}]$$
$$\rightarrow \frac{1}{2}[|2,0,0,0\rangle_{1'H,1'V,2'H,2'V} - |0,2,0,0\rangle_{1'H,1'V,2'H,2'V} - |0,0,2,0\rangle_{1'H,1'V,2'H,2'V} + |0,0,0,2\rangle_{1'H,1'V,2'H,2'V}],$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}[|1,0,0,1\rangle_{1H,1V,2H,2V} + |0,1,1,0\rangle_{1H,1V,2H,2V}]$$
$$\rightarrow \frac{1}{\sqrt{2}}[|1,1,0,0\rangle_{1'H,1'V,2'H,2'V} - |0,0,1,1\rangle_{1'H,1'V,2'H,2'V}],$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}[|1,0,0,1\rangle_{1H,1V,2H,2V} - |0,1,1,0\rangle_{1H,1V,2H,2V}]$$
$$\rightarrow \frac{1}{\sqrt{2}}[|0,1,1,0\rangle_{1'H,1'V,2'H,2'V} - |1,0,0,1\rangle_{1'H,1'V,2'H,2'V}].$$

En conclusión, este elemento permite medir los estados Ψ^+ (dos clicks en un PA) y Ψ^- (un click en cada PA), mientras que no distingue entre los estados Φ^+ y Φ^- (ambos producen un click en solo un PA).



4.1.4. CZ por postselección

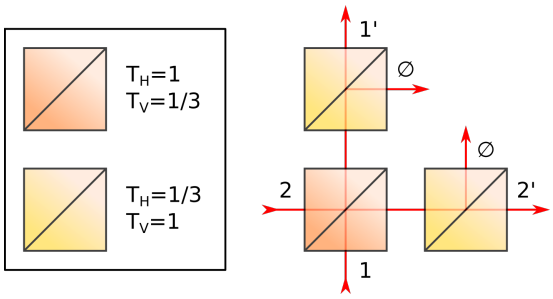
Esta elemento le tomamos directamente de [65][7]. Mediante la suma de todos los caminos conjuntos, se puede comprobar que actúa sobre la base computacional como:

$$|00\rangle = |1,0,1,0\rangle_{1H,1V,2H,2V} \rightarrow \frac{1}{3}|1,0,1,0\rangle_{1'H,1'V,2'H,2'V} + (\text{estados no válidos}),$$
$$|01\rangle = |1,0,0,1\rangle_{1H,1V,2H,2V} \rightarrow \frac{1}{3}|1,0,0,1\rangle_{1'H,1'V,2'H,2'V} + (\text{estados no válidos}),$$
$$|10\rangle = |0,1,1,0\rangle_{1H,1V,2H,2V} \rightarrow \frac{1}{3}|0,1,1,0\rangle_{1'H,1'V,2'H,2'V} + (\text{estados no válidos}),$$
$$|11\rangle = |0,1,0,1\rangle_{1H,1V,2H,2V} \rightarrow -\frac{1}{3}|0,1,0,1\rangle_{1'H,1'V,2'H,2'V} + (\text{estados no válidos}),$$

donde los estados no válidos son aquellos en los que no acaba saliendo un fotón por $1'$ y otro por $2'$ (en particular, también pueden escapar por los laterales). Si en algún momento, en el

[7] Curiosamente, el primer montaje de este mismo artículo inspiró prácticamente los dos últimos Capítulos de este Trabajo de Fin de Grado, si bien la idea ha evolucionado tanto desde entonces que no merece la pena tratar de establecer relaciones.

desarrollo posterior del circuito tras aplicar esta puerta, vemos que nos falta un fotón en $1'$ o en $2'$, entonces deducimos que esta puerta ha fallado. En ese caso, descartamos el resultado del circuito óptico, a esta técnica se le llama "postselección". Por los cálculos anteriores, obtenemos que la puerta funciona con probabilidad 1/9 para cualquier estado de entrada.



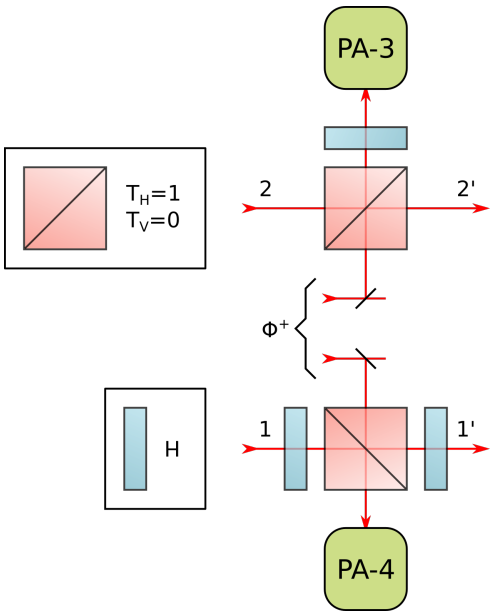
Cabe mencionar que el prisma amarillo se logra simplemente mediante una rotación de 90^{o} del prisma naranja respecto al plano de polarización horizontal.

4.1.5. CNOT con estado de Bell como recurso

Esta elemento con un estado de Bell como recurso le tomamos directamente de [66]. Por brevedad, relegaremos su explicación al artículo referenciado.
Mediante la suma de todos los caminos conjuntos, se puede comprobar que, si realizamos además ciertas correcciones a la salida controladas clásicamente por los clicks de PA-3 y PA-4 , este elemento actúa sobre la base computacional como:

$$|00\rangle = |1,0,1,0\rangle_{1H,1V,2H,2V} \rightarrow \frac{1}{2}|1,0,1,0\rangle_{1'H,1'V,2'H,2'V} + (\text{estados no válidos})$$
$$|01\rangle = |1,0,0,1\rangle_{1H,1V,2H,2V} \rightarrow \frac{1}{2}|1,0,0,1\rangle_{1'H,1'V,2'H,2'V} + (\text{estados no válidos})$$
$$|10\rangle = |0,1,1,0\rangle_{1H,1V,2H,2V} \rightarrow \frac{1}{2}|0,1,0,1\rangle_{1'H,1'V,2'H,2'V} + (\text{estados no válidos})$$
$$|11\rangle = |0,1,0,1\rangle_{1H,1V,2H,2V} \rightarrow \frac{1}{2}|0,1,1,0\rangle_{1'H,1'V,2'H,2'V} + (\text{estados no válidos})$$

donde los estados no válidos son aquellos en los que no acaba saliendo un fotón por $1'$ y otro por $2'$. Relegamos la explicación completa de esta puerta CNOT al artículo citado. Una cosa a remarcar es que, en el caso de salir más de un fotón por $1'$ o por $2'$, no habrá click en el correspondiente PA y podremos detectar el fallo en ese mismo momento. Por los cálculos anteriores, obtenemos que la puerta funciona con probabilidad 1/4 para cualquier estado de entrada.



Es importante fijarse de que, en la imagen, el qubit de control es el inferior y el qubit objetivo el superior. En la figura no se ha representado las correcciones controladas clásicamente por los clicks de PA-3 y PA-4, pero estas correcciones sí se representarán en los circuitos ópticos que plantearemos después.
Cabe mencionar que la puerta H se logra mediante una lámina $\lambda/2$ con eje a $22{,}5^{\text{o}}$ respecto a la horizontal. En realidad, las puertas H se podrían reemplazar por una rotación de 45^{o} de los elementos involucrados respecto a la horizontal, pero hay situaciones en las que ese ángulo no es práctico en el montaje.

4.1.6. Conversión paramétrica descendente espontánea para la generación de pares de Bell

En Óptica Lineal se calcula la respuesta de un medio dieléctrico ante el paso de la luz considerando solo los términos de primer orden. De ahí proceden notablemente las leyes de reflexión y refracción. Sin embargo, cuando la energía del campo electromagnético incidente es suficientemente alta, empieza a ser necesario considerar términos de orden superior para explicar los fenómenos que ocurren.
Uno de estos fenómenos es el de conversión paramétrica descendente espontánea (SPDC, de sus siglas en inglés). Consiste en la conversión de un fotón con frecuencia ω_1 en otros dos de frecuencia más baja $\omega_2 < \omega_1$. Más concretamente, debe ser $\omega_2 = \omega_1/2$ por conservación de la energía. Además, por conservacion del momento, los dos fotones resultantes deben salir formando cierto ángulo fijo entre ellos y simétricos respecto a la dirección del fotón incidente.
La SPDC ocurre principalmente en medios birrefringentes, por la necesidad de cumplir una relación del tipo $n(\omega_2) < n(\omega_1)$ que surge al analizar las ecuaciones. En particular tomaremos un cristal de β-borato de bario (BBO). Con la orientación adecuada, se puede lograr que uno de los fotones salga polarizado en el eje ordinario, y el otro en el eje extraordinario (y sabemos que ambas polarizaciones son ortogonales).

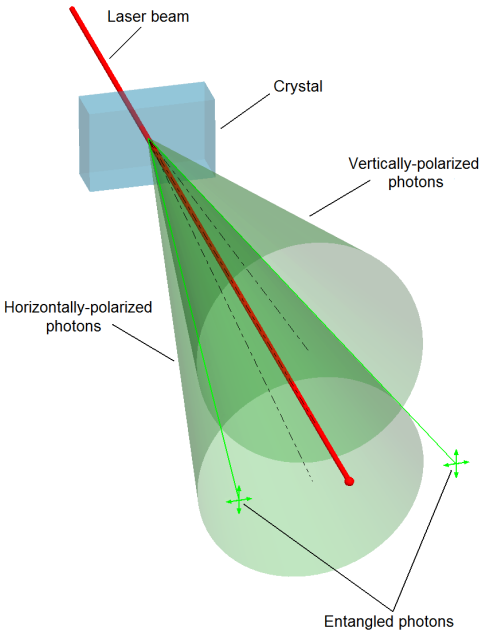
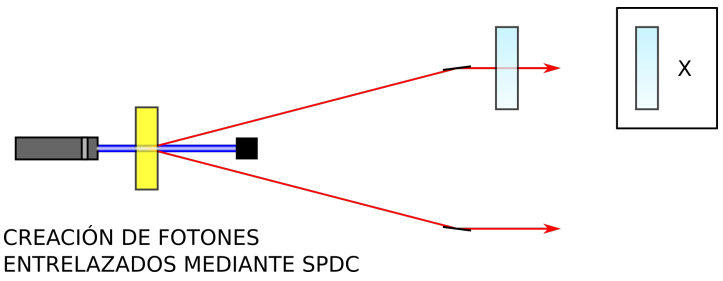


Figura 4.1:
Diagrama mostrando la obtención de fotones entrelazados mediante SPDC.
Esta imagen fue creado por el usuario *J-Wiki* de English Wikipedia y está cubierta por la versión 1.2 de la licencia de documentación libre GNU (`https://commons.wikimedia.org/wiki/Commons:GNU_Free_Documentation_License,_version_1.2`).

En la intersección del cono ordinario con el cono extraordinario podemos encontrar fotones polarizados en ambas direcciones. Ahí la trayectoria espacial no determina la polarización, y lo único que sabemos es que la polarización de un fotón es opuesta a la polarización del otro. Obtenemos pues un estado

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}.$$

Finalmente, aplicando una puerta X en cualquier da los dos fotones, se obtiene el estado $|\Phi^+\rangle$. En [67] se puede encontrar un artículo de revisión sobre este fenómenos de SPDC y sus aplicaciones.

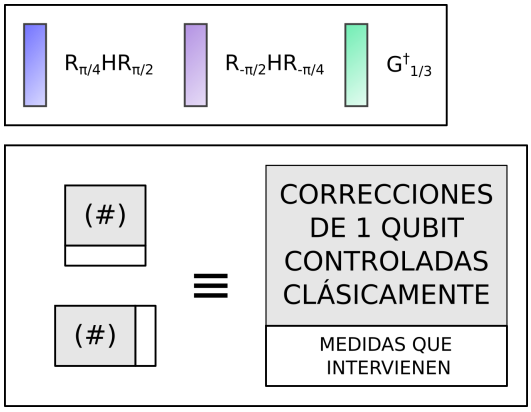


Cabe mencionar que la puerta X se logra mediante una lámina $\lambda/2$ con eje a 45^0 respecto al plano de polarización horizontal.

4.1.7. Otros elementos

Esta es una colección de tres puertas unitarias de 1 qubit que usaremos después, junto con una abreviación del control clásico. Como ya mencionamos que toda puerta unitaria se puede obtener combinando láminas desfasadoras, estos elementos no tienen ningún misterio. En contraposición, nosotros no consideraremos el problema de lograr un control clásico suficientemente rápido

para activarse antes de que pase el fotón. Seguramente sea necesario combinar un deflector electro-óptico rápido [68] con algún tipo de memoria cuántica óptica que retrase la llegada del fotón [69]. Otra alternativa más pedestre es simplemente no preocuparse del asunto: aplicar siempre una corrección concreta, y ya después comprobar si fue la correcta. Esto reduciría mucho la eficiencia del dispositivo, pero por otro lado es mucho más sencillo de implementar.



4.2. Esquemas para entrelazamiento triple de fotones

Ahora por fin estamos listos para presentar los resultados principales de este Trabajo de Fin de Grado.

4.2.1. Generación de estados GHZ de tres fotones

Aplicamos el esquema de teleportación del **Capítulo 3** al circuito para la generación de un estado $|GHZ\rangle$ que se planteó en el **Capítulo 2**. Las cuentas para llegar a este circuito final están realizadas en el **Apéndice A**.

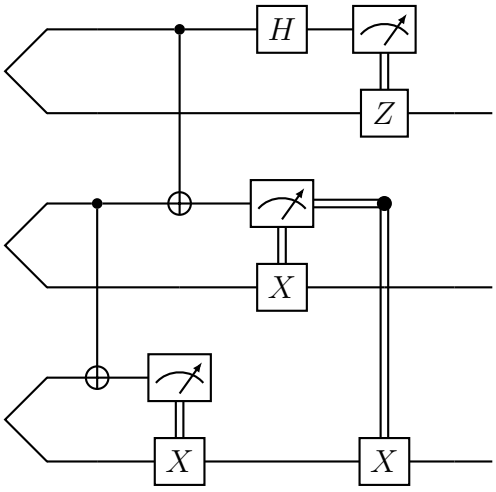


Figura 4.2:
Circuito teleportado para la generación del estado $|GHZ\rangle$.

Ahora transformamos una de las CNOTs en una CZ. Observemos que la otra forma, junto con la puerta H, una medida de Bell. Como el estado resultante anterior a las dos medidas individuales es $|{+}{+}\rangle$, el estado previo debe ser una superposición uniforme de los 4 estados de Bell. Eso hace que la medida parcial de Bell funcione con probabilidad 1/2.

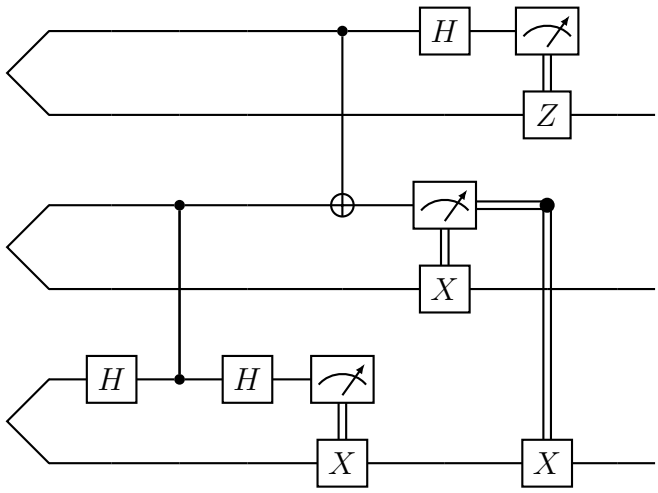
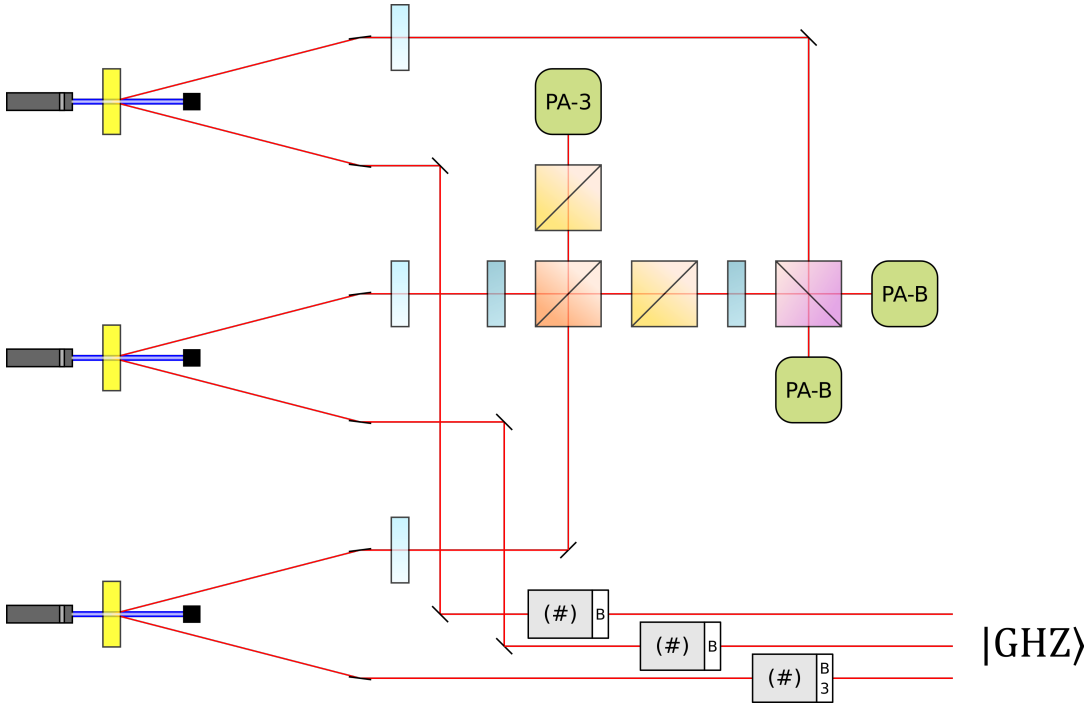


Figura 4.3:
Circuito teleportado para la generación del estado $|GHZ\rangle$, preparado para ser realizado conlos elementos ópticos anteriores.

Por último, presentamos el circuito óptico:



Para cada triple coincidencia de pares de Bell (es decir, que ocurra SPDC aproximadamente a la vez, de modo que todos los fotones coincidan en el tiempo en los divisores de haz, y por tanto estos puedan realizar su función), el circuito tiene éxito si y solo si ocurren dos clicks entre los dos PA-B y ocurre un click en PA-3.

4.2.2. Generación de estados W de tres fotones

Aplicamos el esquema de teleportación del **Capítulo 3** al circuito para la generación de un estado $|W\rangle$ que se planteó en el **Capítulo 2**. Las cuentas para llegar a este circuito final están realizadas en el **Apéndice A**.

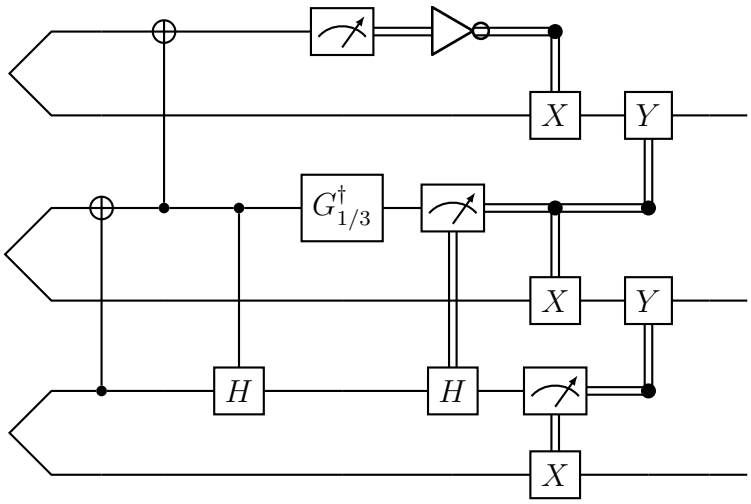


Figura 4.4:
Circuito teleportado para la generación del estado $|W\rangle$.

Ahora transformamos dos de las CNOTs en CZs. Como el operador X y el operador H tienen los mismos autovalores ($\{-1, 1\}$), se puede transformar la puerta CH en una CNOT. Sin embargo, ahora no nos interesa transformar esta nueva puerta CNOT en una CZ. Con nuestro sistema óptico, colocar dos CZs con igual control y objetivo haría imposible saber si la primera falló: podrían juntarse en una misma rama los dos fotones tras atravesar la primera terna de prismas, y luego volver a separarse en la segunda terna. Si ocurriera eso, el estado final sería incorrecto, pero no habría ninguna forma de detectarlo a través de los clicks de los PA.

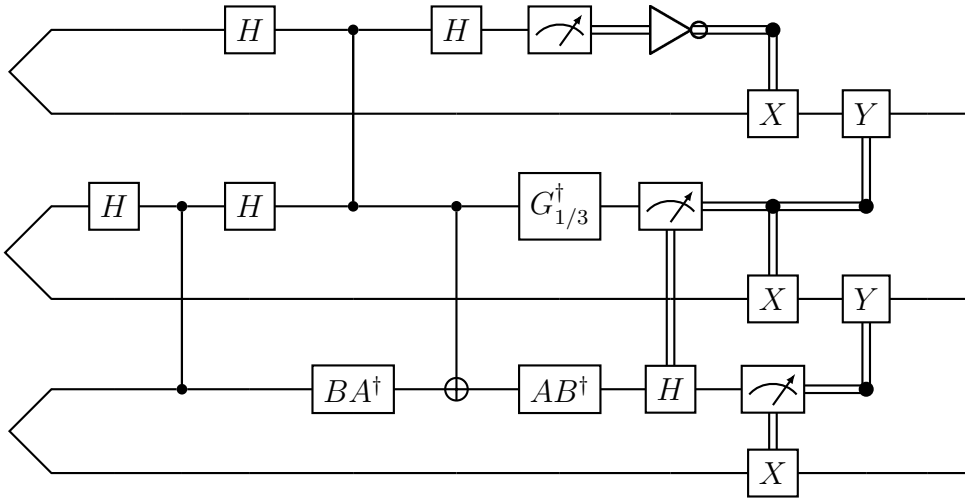
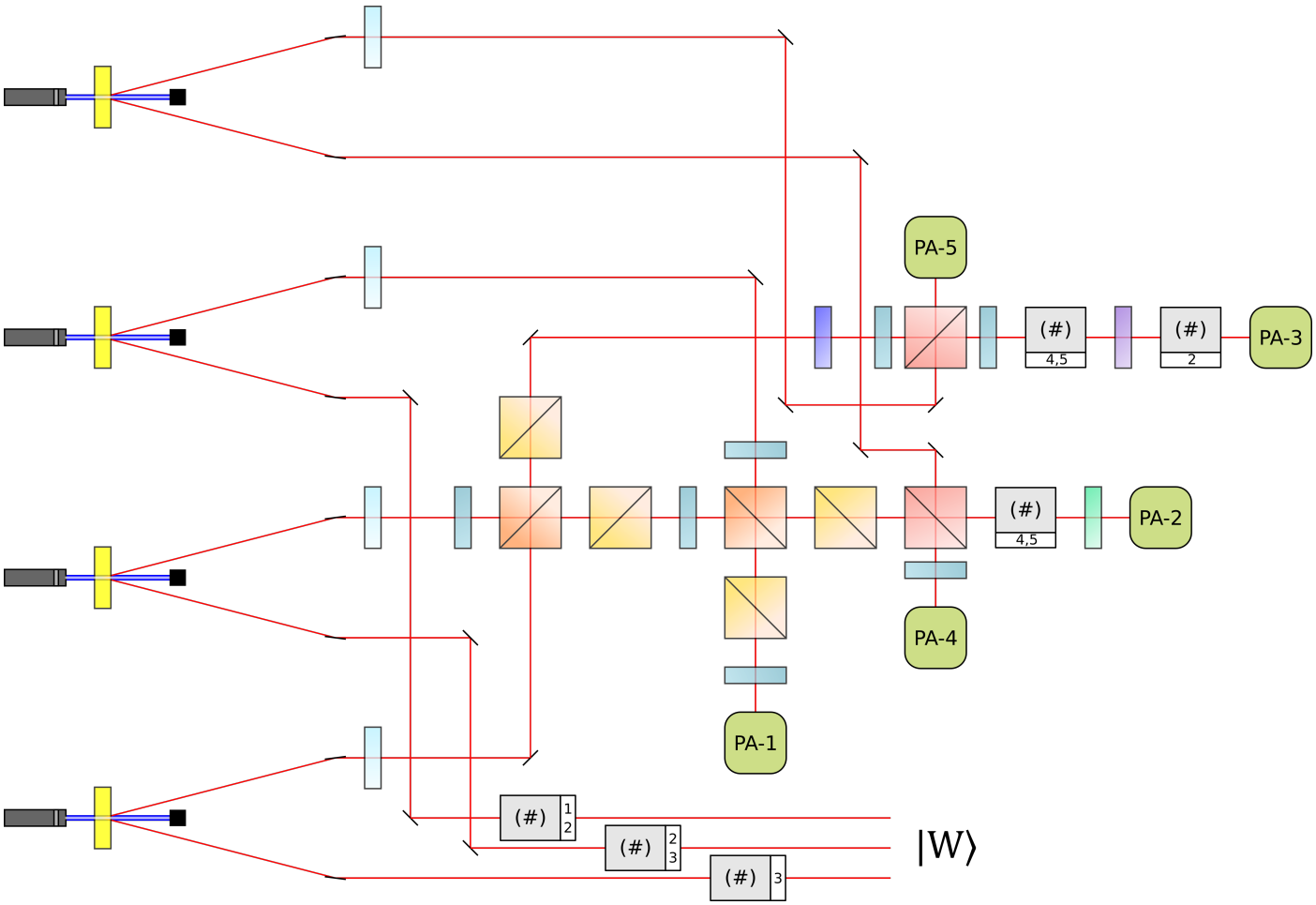


Figura 4.5:
Circuito teleportado para la generación del estado $|GHZ\rangle$, preparado para ser realizado conlos elementos ópticos anteriores.
Aquí $BA^{\dagger} = R_{\pi/2} H R_{\pi/4}$.

Por último, presentamos el circuito óptico:



Para cada cuádruple coincidencia de pares de Bell, el circuito tiene éxito si y solo si ocurre un click en cada PA-i, con i $= 1, \ldots, 5$.

4.2.3. Viabilidad, aplicaciones y otros comentarios

Hasta donde llega el conocimiento del autor de este Trabajo de Fin de Grado, el esquema presentado es original y no aparece en la literatura. Cabe citar otros esquemas que son similares en distintos aspectos (por ejemplo [70, 71]), pero ninguno de ellos actúa en polarización y produce entrelazamiento remoto triple (o lo primero, o lo segundo, en los artículos citados).
La principal limitación de nuestro sistema son los ratios extremadamente bajos de generación de tripletes entrelazados. Tomamos como referencia muy aproximada los datos del artículo [65]. De ahí se infiere que la frecuencia de triple coincidencia de pares de Bell es $f(\text{3-coincidencia}) = 126/\text{min}$ y suponemos que se puede aproximar la frecuencia de cuádruple coincidencia de pares de Bell como $f(\text{4-coincidencia}) = [f(\text{3-coincidencia})]^{3/4} \approx 37,61/\text{min}$.
Visto esto, recordemos los requerimientos de nuestros circuitos ópticos:

- El circuito óptico para GHZ requiere una triple coincidencia de pares de Bell, además de contener una puerta CZ con probabilidad de éxito 1/9 y una medida de Bell con probabilidad de éxito 1/2.
- El circuito óptico para W requiere una cuádruple coincidencia de pares de Bell, además de contener dos puerta CZ con probabilidad de éxito 1/9 y una puerta CNOT con probabilidad de éxito 1/4.

Con las consideraciones anteriores, podemos esperar un ratio

- 7/min en el circuito óptico para GHZ.
- $0,12$/min en el circuito óptico para W.

Existen muchas vías para potencialmente mejorar los números anteriores. Por ejemplo:

- Quizás se puedan sustituir las puertas probabilista de 2 qubits por otras deterministas.
- Probablemente surgirán técnicas más eficientes que SPDC para generar los pares de Bell iniciales.
- Es posible aumentar el ratio de coincidencia de fotones mediante filtros de frencuencia (aunque esto ya se hace en [65]).

Nuestra esperanza es que, con cualquiera de estas mejoras especulativas, los ratios aumenten hasta que este esquema sea viable en alguna de las avenidas que se mencionó en el **Capítulo 2**. Incluso si no fuera el caso, estos dos circuitos ópticos retienen su valor como prueba de concepto del método de equivalencias y teleportación de estados.
Con esto termina el último Capítulo de este Trabajo de Fin de Grado. A continuación se encuentra la **Conclusión**, donde disponemos una visión global del conjunto.

Conclusión

Este Trabajo de Fin de Grado tiene dos partes bien distinguidas, si bien complementarias. Durante los dos primeros Capítulos se realizó una incursión en el campo de la Computación Cuántica, procurando abarcar todos los temas clave desde un punto de vista moderno. Tras esto, los otros dos Capítulos se enfocaron en temas más concretos: las equivalencias de circuitos cuánticos, y la computación cuántica mediante fotones, respectivamente. De este modo se ha logrado un equilibrio entre extensión y profundidad.
El tema de este Trabajo de Fin de Grado ha evolucionado considerablemente desde el comienzo de su elaboración. El enfoque en las equivalencias del **Capítulo 3** surgió de un proyecto inicial que fue abandonado (optimización de operaciones aritméticas en ordenadores cuánticos). A su vez, el **Capítulo 4** está inspirado por nuestro fortuito encuentro con el artículo "Teleportation-based realization of an optical quantum two-qubit entangling gate" [65], cuyas ideas permitieron cumplir nuestro deseo de aplicar las equivalencias obtenidas en el **Capítulo 3**.
En cierto modo hay una aparente falta de dirección, pero esto es reflejo de la realidad del proceso de investigación. La exploración caótica ha dado sus frutos: se ha planteado una curiosa técnica de teleportación de estados, que desembocó en dos propuestas concretas de esquemas de generación remota de estados triplemente entrelazados. Por el camino han quedado sin responder varias cuestiones en esas dos líneas, entre ellas:

- ¿Es posible aplicar la estrategia de teleportación de estados en situaciones más complicadas? ¿Existe un modo algorítmico de hacerlo?
- ¿Qué ocurre si consideramos otros estados entrelazados iniciales con más qubits en vez de los Φ^+?
- ¿Se puede analizar el problema de teleportación de estados desde un punto de vista más matemático? ¿Cuáles son los límites?
- ¿Podemos plantear los diversos elementos ópticos considerados en un marco más general?
- ¿En el circuito óptico para W es estrictamente necesario añadir un 4^{o} par de Bell?
- ¿Cómo mejorar la eficiencia de los circuitos ópticos que hemos obtenido?

Estas puertas permanecen abiertas para futuros desarrollos. Sin duda, todavía queda mucho por explorar en el fascinante campo de la Computación Cuántica.

Apéndice A

Cuentas para los circuitos de teleportación de los estados $|GHZ\rangle$ y $|W\rangle$

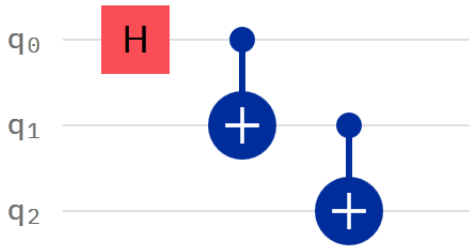
Para evitar interrumpir varias páginas el desarrollo del texto central, las cuentas realizadas se presentan en este Apéndice.
Dibujar todos estos circuitos en LaTeXes una tarea demasiado laboriosa para mis ya deterioradas manos (de tanto escribir). Así que hemos decidido presentar estos circuitos según se ven en el editor online de circuitos cuánticos de IBM, `https://quantum-computing.ibm.com/composer/`. Las cuentas más difíciles (para el circuito $|W\rangle$), se realizaron de hecho en esta plataforma.
Para comprender este nuevo formato de circuito cuántico, damos un par de indicaciones importantes:

- Recordemos en todo momento que los qubits que se acaban midiendo son siempre el $1^{\underline{o}}$, el $3^{\underline{o}}$, y el $5^{\underline{o}}$ (q0, q2 y q4). Los qubits $2^{\underline{o}}$, $4^{\underline{o}}$ y $6^{\underline{o}}$ (q1, q3 y q5), son la salida del circuito cuántico.

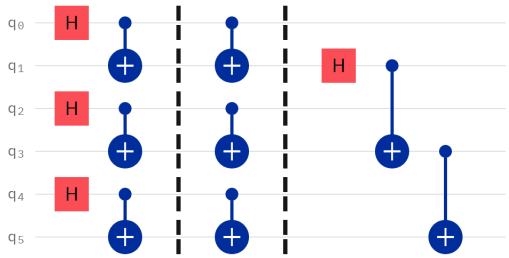
- En la plataforma de IBM no es posible escribir el par entrelazado $|\Phi^+\rangle$. Para dibujarlo, lo formamos con la puerta H y la puerta CNOT. Estas puertas no tienen porque tener entidad física, son tan solo una representación. Ponemos pues una barrera para separar esta parte del circuito y el resto. También, solo en el Paso 0, separamos las puertas CNOT de las unidades iniciales de teleportación del resto del circuito mediante otra barrera. En ese Paso 0, justo tras la segunda barrera, el estado de los $1^{\underline{o}}$, $3^{\underline{o}}$ y $5^{\underline{o}}$ qubit es $|+\rangle$ cada uno, mientras que el estado de los $2^{\underline{o}}$, $4^{\underline{o}}$ y $6^{\underline{o}}$ qubits es $|0\rangle$ cada uno.

- En la plataforma de IBM no es posible dibujar las puertas controladas clásicas de la manera que conocemos. En el "Paso Final", y de ahí en adelante, se separarán las puertas controladas clásicamente del resto del circuito mediante otra barrera.

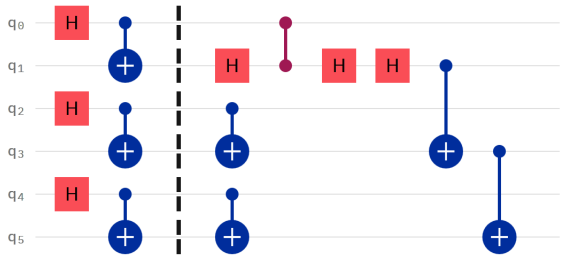
A.1. Circuito $|GHZ\rangle$



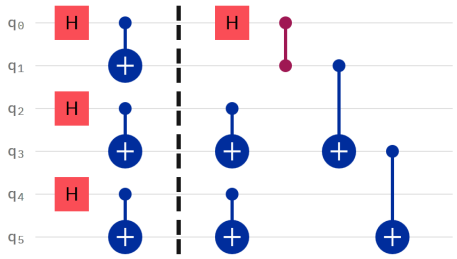
Circuito inicial para la generación de un estado GHZ



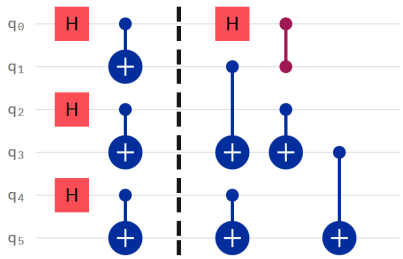
Paso 0
Se traslada el circuito original a las "unidades iniciales". Aquí ya se han postergado las medidas. El primer paso consistirá en mover la puerta H hacia la izquierda.



Paso 1
Se convierte el CNOT superior en un CZ y dos puertas de H.

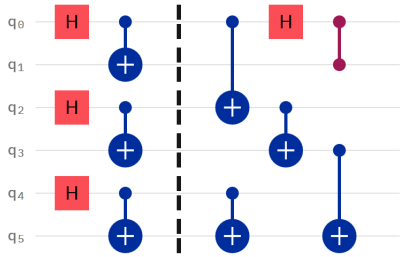


Paso 2
Se cancelan las dos puertas H de la derecha. Se eleva la puerta H. El siguiente paso consistirá en mover la primera puerta CNOT hacia la izquierda.



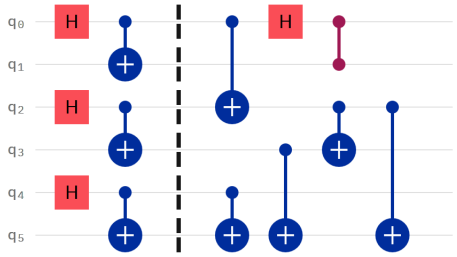
Paso 3

Se desplaza la primera puerta CNOT hacia la izquierda sin inconveniente.



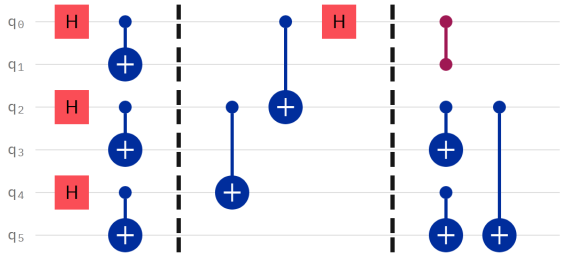
Paso 4

Se eleva tanto el control como el objetivo de la primera puerta CNOT. El siguiente paso consistirá en mover la segunda puerta CNOT hacia la izquierda.



Paso 5

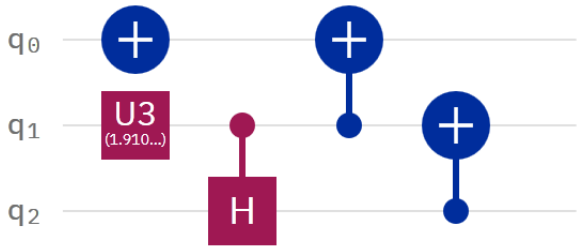
Se aplican las reglas de conmutatición para desplazar la segunda puerta CNOT hacia la izquierda. Aparece una nueva puerta CNOT.



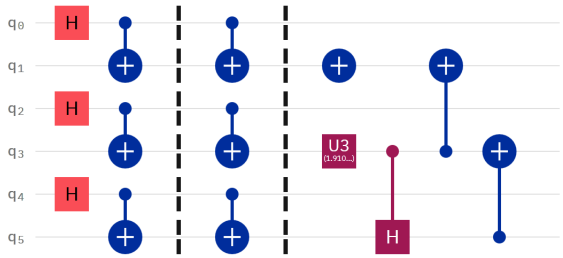
Paso Final

Se termina de desplazar la segunda puerta CNOT hacia la izquierda. Se eleva tanto el control como el objetivo de la segunda puerta CNOT

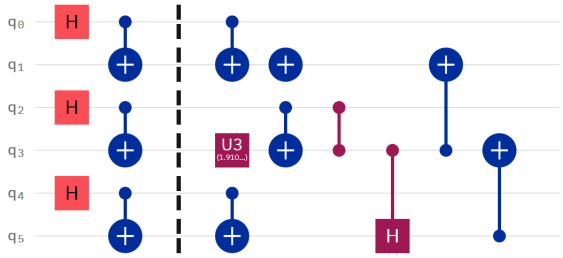
A.2. Circuito $|W\rangle$



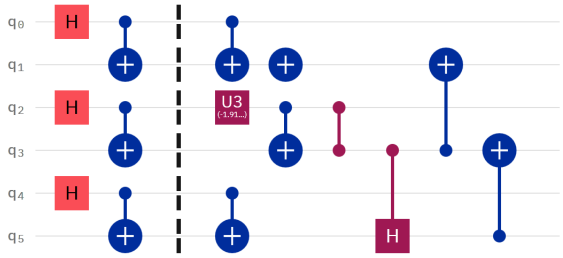
Circuito inicial para la generación de un estado W.
La puerta U3 es la puerta $G_{1/3}$. El número que aparece debajo es $\theta \approx 1{,}91063$, y quedan cortados los números $\phi = 0$, $\lambda = 0$.



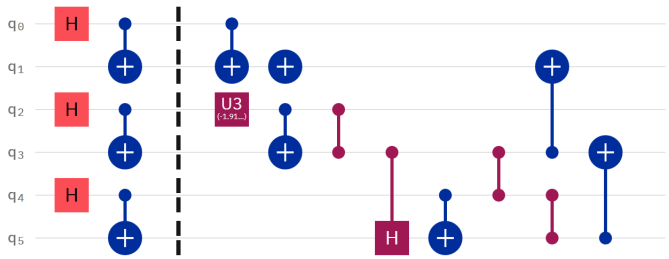
Paso 0
Se traslada el circuito original a las "unidades iniciales". Aquí ya se han postergado las medidas. El primer paso consistirá en mover la puerta U3 hacia la izquierda.



Paso 1
Se hace atravesar la puerta U3 por la puerta CNOT. Esta última se transforma en una puerta CU, con $U = ZX$. Se representa como una puerta CNOT seguida de una puerta CZ.

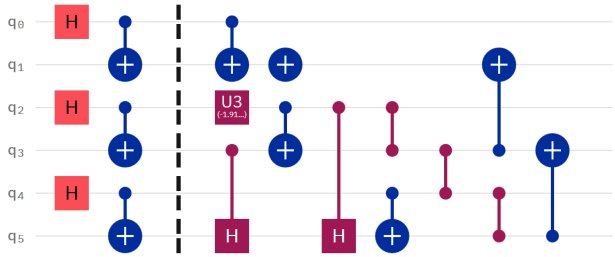


Paso 2
Se eleva la puerta U3. Como $\phi = \lambda = 0$ para esta puerta, basta considerar la conjugada. El siguiente paso consistirá en mover la puerta CH hacia la izquierda.



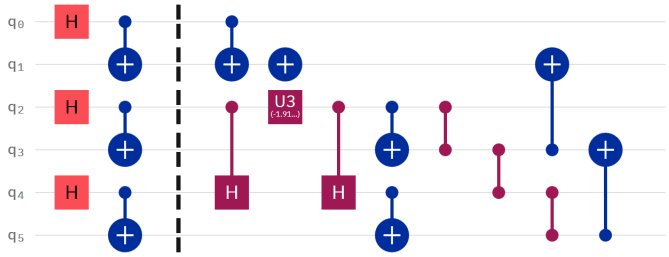
Paso 3

Se emplea la equivalencia "sacada de la manga" (sección 3.2.3) para desplazar la puerta CH hacia la izquierda de la puerta CNOT inferior. Aparecen dos nuevas puertas CZ.



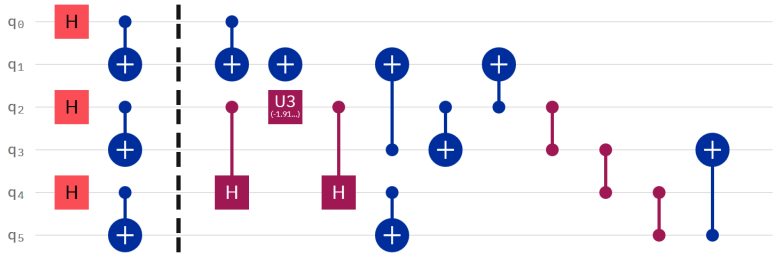
Paso 4

Se aplican las reglas de conmutación para terminar de desplazar la puerta CH hacia la izquierda. Aparece una nueva puerta CH.



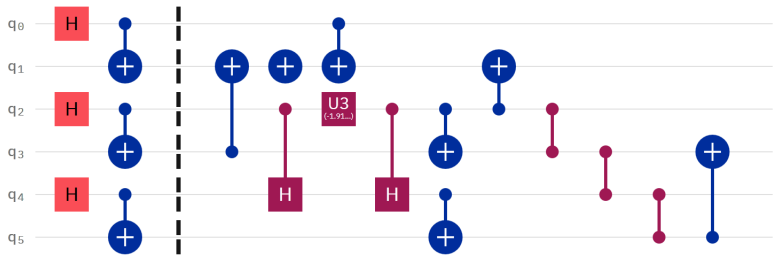
Paso 5

Se eleva tanto el control como el objetivo de la puerta CH de la izquierda. Se eleva el objetivo de la puerta CH de la derecha. Se intercambia de orden la puerta CH de la derecha con la puerta CNOT contigua. El siguiente paso consistirá en mover la primera puerta CNOT hacia la izquierda.



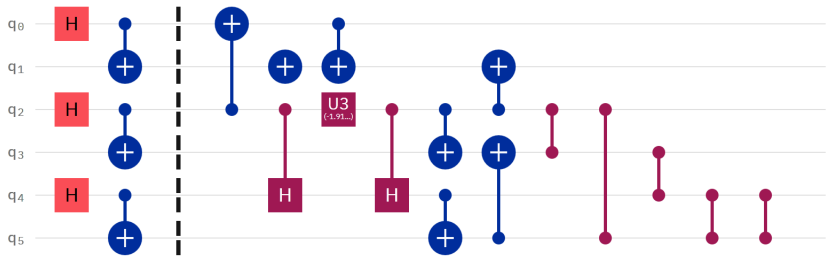
Paso 6

Se aplican las reglas de conmutación para desplazar la primera puerta CNOT hacia la izquierda. Aparece una nueva puerta CNOT.



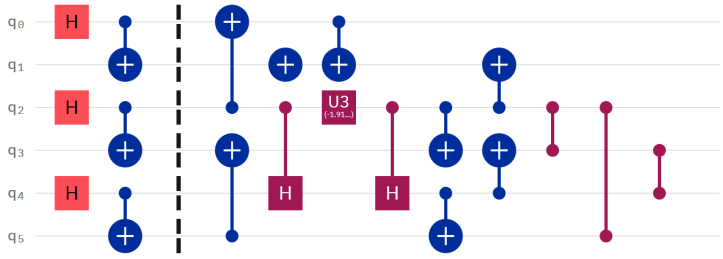
Paso 7

Se termina de desplazar la primera puerta CNOT hacia la izquierda. Se intercambia de orden la puerta X con la puerta CNOT contigua.



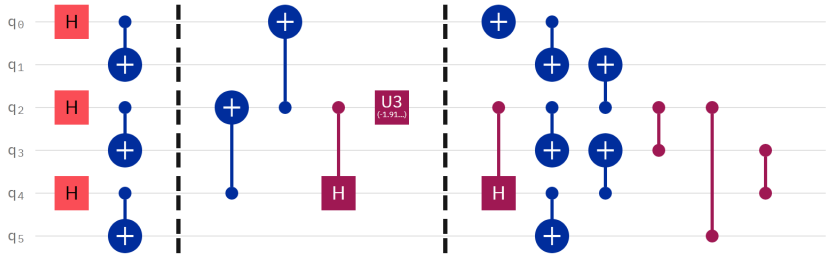
Paso 8

Se eleva tanto el control como el objetivo de la primera puerta CNOT. El siguiente paso consistirá en mover la segunda puerta CNOT hacia la izquierda. Se aplican las reglas de conmutación para desplazar la segunda puerta CNOT hacia la izquiera. Aparecen dos nuevas puertas CZ.



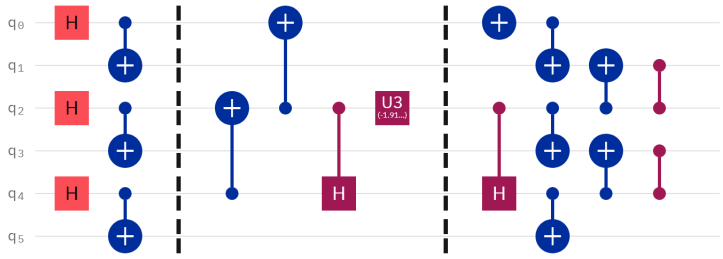
Paso 9

Se aplican las reglas de conmutación para terminar de desplazar la segunda puerta CNOT hacia la izquierda. Aparece una nueva puerta CNOT. Se cancelan las dos puertas CZ de la derecha. Se entiende que la puerta X tiene control clásico en el sentido de que invierte el bit de control ($0 \to 1$, $1 \to 0$).



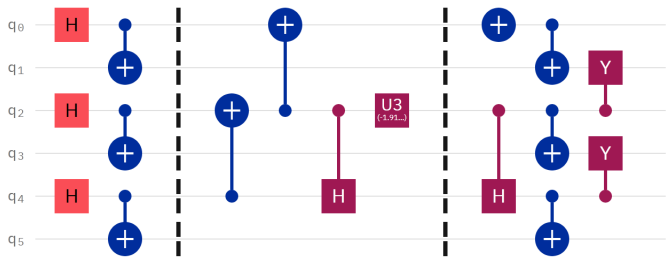
Paso Final

Se eleva tanto el control como el objetivo de la segunda puerta CNOT. Se eleva la puerta X. Se intercambia de orden la puerta X con la puerta CNOT contigua.



Paso Extra 1

¡Esta equivalencia solo funciona cuando ya se han medido los qubits 1º, 3º y 5º, y las puertas de la derecha tienen control clásico! Se convierten las dos puertas cZ controladas por la medida del qubit 3º y con objetivos los qubits 4º y 6º en otra puerta cZ controlada por la medida del qubit 3º pero ahora con objetivo el qubit 2º. Ver abajo para una explicación de este paso.



Paso Extra 2

¡Esta equivalencia solo funciona cuando ya se han medido los qubits 1º, 3º y 5º, y las puertas de la derecha tienen control clásico! Se combinan los dos pares de puertas contiguas cX y cZ en una puerta c(-iY). Como el control es clásico, se puede despreciar la fase global $-i$.

A.2.1. Explicación del Paso Extra 1

Imaginemos que el resultado de la medida del qubit $3^{\underline{o}}$ es 1 (es decir, se mide $|1\rangle$). Si, tras aplicar con control clásico las dos puertas Z en los qubits $4^{\underline{o}}$ y $6^{\underline{o}}$, el estado resultante es (en los qubits $2^{\underline{o}}$, $4^{\underline{o}}$ y $6^{\underline{o}}$):

$$|W\rangle = \frac{|100\rangle + |010\rangle + |001\rangle}{\sqrt{3}}.$$

Eso significa que antes de aplicarlas el estado era

$$\frac{|100\rangle - |010\rangle - |001\rangle}{\sqrt{3}}.$$

Alternativamente, aplicamos una puerta Z en el qubit $2^{\underline{o}}$. Entonces el estado final queda

$$\frac{-|100\rangle - |010\rangle - |001\rangle}{\sqrt{3}} = -|W\rangle.$$

Pero los qubits $1^{\underline{o}}$, $3^{\underline{o}}$ y $5^{\underline{o}}$ ya no existen (han sido medidos), así que ese signo $-$ es una fase global y lo podemos despreciar. De este modo se ahorra una puerta cZ y aumenta la simetría del circuito.

Bibliografía

[1] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Phys. Rev.*, vol. 47, pp. 777–780, May 1935.

[2] J. S. Bell, "On the Einstein–Podolsky–Rosen paradox," *Physics Physique Fizika*, vol. 1, pp. 195–200, Nov 1964.

[3] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, Oct. 1969.

[4] A. Aspect, "Bell's inequality test: more ideal than ever," *Nature*, vol. 398, pp. 189–190, Mar. 1999.

[5] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, and A. V. Thapliyal, "Exact and asymptotic measures of multipartite pure-state entanglement," *Phys. Rev. A*, vol. 63, p. 012307, Dec 2000.

[6] W. Dür, G. Vidal, and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways," *Physical Review A*, vol. 62, Nov 2000.

[7] A. Peres and D. R. Terno, "Quantum information and relativity theory," *Reviews of Modern Physics*, vol. 76, p. 93–123, Jan 2004.

[8] J. Gruska and H. Imai, "Power, puzzles and properties of entanglement," in *Machines, Computations, and Universality* (M. Margenstern and Y. Rogozhin, eds.), (Berlin, Heidelberg), pp. 25–68, Springer Berlin Heidelberg, 2001.

[9] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, "Noncommuting mixed states cannot be broadcast," *Physical Review Letters*, vol. 76, p. 2818–2821, Apr 1996.

[10] N. Gisin and S. Massar, "Optimal quantum cloning machines," *Physical Review Letters*, vol. 79, p. 2153–2156, Sep 1997.

[11] J. R. Samal, A. K. Pati, and A. Kumar, "Experimental test of the quantum no-hiding theorem," *Physical Review Letters*, vol. 106, Feb 2011.

[12] M. A. Nielsen and I. L. Chuang, "Number theory," in *Quantum Computation and Quantum Information*, pp. 531–533, Cambridge University Press.

[13] R. Feynmann, "Simulating physics with computers," *International Journal of Theoretical Physics*, vol. 21, pp. 467–488, jun 1982.

[14] D. Deutsch, "Quantum theory, the Church–Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, pp. 97–117, jul 1985.

[15] P. Ray, B. K. Chakrabarti, and A. Chakrabarti, "Quantum annealing," *Phys. Rev. B*, vol. 39, pp. 11828–11832, Jun 1989.

[16] A. Das and B. K. Chakrabarti, "Colloquium: Quantum annealing and analog quantum computation," *Reviews of Modern Physics*, vol. 80, no. 3, p. 1061, 2008.

[17] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pp. 124–134, 1994.

[18] J. I. Cirac and P. Zoller, "Quantum computations with cold trapped ions," *Phys. Rev. Lett.*, vol. 74, pp. 4091–4094, May 1995.

[19] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland, "Demonstration of a fundamental quantum logic gate," *Phys. Rev. Lett.*, vol. 75, pp. 4714–4717, Dec 1995.

[20] "List of quantum processors." `https://en.wikipedia.org/wiki/List_of_quantum_processors/`. Último acceso: 2020-09-07.

[21] S. Feldman, "20 years of quantum computing growth." `https://www.statista.com/chart/17896/quantum-computing-developments/`. Último acceso: 2021-01-26.

[22] F. Arute, K. Arya, R. Babbush, D. Bacon, J. Bardin, R. Barends, R. Biswas, S. Boixo, F. Brandao, D. Buell, B. Burkett, Y. Chen, Z. Chen, B. Chiaro, R. Collins, W. Courtney, A. Dunsworth, E. Farhi, B. Foxen, and J. Martinis, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, pp. 505–510, 10 2019.

[23] E. Pednault, J. Gunnels, D. Maslov, and G. Jay, "On "quantum supremacy"." `https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/`. Último acceso: 2020-09-07.

[24] N. D. Mermin, *Quantum Computer Science*. Cambridge University Press, 2007.

[25] A. Kay, "Tutorial on the quantikz package," *arXiv:1809.03842*, 2018.

[26] Kunz, "On the equivalence between one-dimensional discrete Walsh-Hadamard and multidimensional discrete Fourier transforms," *IEEE Transactions on Computers*, vol. C-28, no. 3, pp. 267–268, 1979.

[27] D. Cruz, R. Fournier, F. Gremion, A. Jeannerot, K. Komagata, T. Tosic, J. Thiesbrummel, C. L. Chan, N. Macris, M. Dupertuis, and et al., "Efficient quantum algorithms for GHZ and W states, and implementation on the IBM quantum computer," *Advanced Quantum Technologies*, vol. 2, p. 1900015, Apr 2019.

[28] F. Vatan and C. Williams, "Optimal quantum circuits for general two-qubit gates," *Physical Review A*, vol. 69, Mar 2004.

[29] T. Toffoli, "Reversible computing," in *Automata, Languages and Programming* (J. de Bakker and J. van Leeuwen, eds.), (Berlin, Heidelberg), pp. 632–644, Springer Berlin Heidelberg, 1980.

[30] V. Vedral, A. Barenco, and A. Ekert, "Quantum networks for elementary arithmetic operations," *Physical Review A*, vol. 54, p. 147–153, Jul 1996.

[31] A. Arkhipov, "Universal quantum gates." `https://quantumalgorithmzoo.org/`, 2009. Último acceso: 2021-01-29.

[32] "More circuit identities." https://qiskit.org/textbook/ch-gates/more-circuit-identities.html/. Último acceso: 2020-09-08.

[33] D. M. Greenberger, M. A. Horne, and A. Zeilinger, *Going Beyond Bell's Theorem*, pp. 69–72. Dordrecht: Springer Netherlands, 1989.

[34] N. D. Mermin, "Quantum mysteries revisited," *American Journal of Physics*, vol. 58, no. 8, pp. 731–734, 1990.

[35] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, p. 390–393, Nov 1999.

[36] B. A. Nguyen, "Optimal processing of quantum information via w-type entangled coherent states," *Physical Review A*, vol. 69, p. 022315, 02 2004.

[37] E. D'Hondt and P. Panangaden, "The computational power of the W and GHZ states," *Quantum Inf. Comput.*, vol. 6, pp. 173–183, 2006.

[38] "Complexity zoo." https://complexityzoo.uwaterloo.ca/Complexity_Zoo/. Último acceso: 2020-09-08.

[39] "Quantum zoo." https://quantumalgorithmzoo.org/. Último acceso: 2020-09-08.

[40] N. D. Mermin, "Deconstructing dense coding," *Physical Review A*, vol. 66, Sep 2002.

[41] N. D. Mermin, "From classical state swapping to quantum teleportation," *Physical Review A*, vol. 65, Dec 2001.

[42] D. P. DiVincenzo, "The physical implementation of quantum computation," *Fortschritte der Physik*, vol. 48, p. 771–783, Sep 2000.

[43] M. Kjaergaard, M. E. Schwartz, J. Braumüller, P. Krantz, J. I.-J. Wang, S. Gustavsson, and W. D. Oliver, "Superconducting qubits: Current state of play," *Annual Review of Condensed Matter Physics*, vol. 11, p. 369–395, Mar 2020.

[44] P. Krantz, M. Kjaergaard, F. Yan, T. P. Orlando, S. Gustavsson, and W. D. Oliver, "A quantum engineer's guide to superconducting qubits," *Applied Physics Reviews*, vol. 6, p. 021318, Jun 2019.

[45] K. Wright, K. M. Beck, S. Debnath, J. M. Amini, Y. Nam, N. Grzesiak, J.-S. Chen, N. C. Pisenti, M. Chmielewski, C. Collins, K. M. Hudek, J. Mizrahi, J. D. Wong-Campos, S. Allen, J. Apisdorf, P. Solomon, M. Williams, A. M. Ducore, A. Blinov, S. M. Kreikemeier, V. Chaplin, M. Keesan, C. Monroe, and J. Kim, "Benchmarking an 11-qubit quantum computer," *Nature Communications*, vol. 10, p. 5464, Nov 2019.

[46] "IonQ unveils world's most powerful quantum computer." https://ionq.com/news/october-01-2020-most-powerful-quantum-computer. Último acceso: 2021-01-08.

[47] J. Preskill, "Lecture notes for Physics 219." http://theory.caltech.edu/~preskill/ph219/index.html. Último acceso: 2021-01-08.

[48] A. W. Cross, L. S. Bishop, S. Sheldon, P. D. Nation, and J. M. Gambetta, "Validating quantum computers using randomized model circuits," *Physical Review A*, vol. 100, Sep 2019.

[49] M. A. Nielsen and I. L. Chuang, *Quantum information theory*. Cambridge University Press.

[50] J. Preskill, "Quantum computing in the NISQ era and beyond," *Quantum*, vol. 2, p. 79, Aug 2018.

[51] B. Coecke and R. Duncan, "Interacting quantum observables: categorical algebra and diagrammatics," *New Journal of Physics*, vol. 13, p. 043016, Apr 2011.

[52] M. Backens and A. Kissinger, "ZH: A complete graphical calculus for quantum computations involving classical non-linearity," *Electronic Proceedings in Theoretical Computer Science*, vol. 287, p. 23–42, Jan 2019.

[53] J. C. Garcia-Escartin and P. Chamorro-Posada, "Equivalent quantum circuits," *arXiv:1110.2998*, 2011.

[54] A. Einstein, "Über einen die erzeugung und verwandlung des lichtes betreffenden heuristischen gesichtspunkt," *Annalen der Physik*, vol. 322, no. 6, pp. 132–148, 1905.

[55] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. Braunstein, "Advances in quantum teleportation," *Nature Photonics*, vol. 9, 05 2015.

[56] B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, "Universal unitary gate for single-photon two-qubit states," *Physical Review A*, vol. 63, Feb 2001.

[57] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. J. Milburn, "Linear optical quantum computing with photonic qubits," *Reviews of Modern Physics*, vol. 79, p. 135–174, Jan 2007.

[58] E. Knill, R. Laflamme, and G. J. Milburn, "A scheme for efficient quantum computation with linear optics," *Nature*, vol. 409, pp. 46–52, Jan 2001.

[59] J. D. Franson, B. C. Jacobs, and T. B. Pittman, "Quantum computing using single photons and the zeno effect," *Phys. Rev. A*, vol. 70, p. 062302, Dec 2004.

[60] Q. Lin and J. Li, "Quantum control gates with weak cross-kerr nonlinearity," *Phys. Rev. A*, vol. 79, p. 022301, Feb 2009.

[61] S. Aaronson and A. Arkhipov, "The computational complexity of linear optics," in *Research in Optical Sciences*, p. QTh1A.2, Optical Society of America, 2014.

[62] H.-S. Zhong, H. Wang, Y.-H. Deng, M.-C. Chen, L.-C. Peng, Y.-H. Luo, J. Qin, D. Wu, X. Ding, Y. Hu, P. Hu, X.-Y. Yang, W.-J. Zhang, H. Li, Y. Li, X. Jiang, L. Gan, G. Yang, L. You, Z. Wang, L. Li, N.-L. Liu, C.-Y. Lu, and J.-W. Pan, "Quantum computational advantage using photons," *Science*, vol. 370, no. 6523, pp. 1460–1463, 2020.

[63] J. Skaar, J. C. Garcia Escartin, and H. Landro, "Quantum mechanical description of linear optics," *American Journal of Physics*, vol. 72, no. 11, pp. 1385–1391, 2004.

[64] Hong, Óù, and Mandel, "Measurement of subpicosecond time intervals between two photons by interference.," *Physical review letters*, vol. 59 18, pp. 2044–2046, 1987.

[65] W. Gao, A. Goebel, C.-Y. Lu, H.-N. Dai, C. Wagenknecht, Q. Zhang, B. Zhao, C.-Z. Peng, T. Chen, Y.-A. Chen, and J.-W. Pan, "Teleportation-based realization of an optical quantum two-qubit entangling gate," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 107, pp. 20869–74, 12 2010.

[66] T. B. Pittman, B. C. Jacobs, and J. D. Franson, "Probabilistic quantum logic operations using polarizing beam splitters," *Physical Review A*, vol. 64, Nov 2001.

[67] C. Couteau, "Spontaneous parametric down-conversion," *Contemporary Physics*, vol. 59, p. 291–304, Jul 2018.

[68] L. Sirleto, L. Petti, P. Mormile, G. Righini, and G. Abbate, "Fast integrated electro-optical switch and beam deflector based on nematic liquid crystal waveguides," *Fiber and Integrated Optics - FIBER INTEGRATED OPT*, vol. 21, pp. 435–449, 11 2002.

[69] A. I. Lvovsky, B. C. Sanders, and W. Tittel, "Optical quantum memory," *Nature Photonics*, vol. 3, pp. 706–714, Dec 2009.

[70] T. Tashima, T. Wakatsuki, i. m. c. K. Özdemir, T. Yamamoto, M. Koashi, and N. Imoto, "Local transformation of two einstein-podolsky-rosen photon pairs into a three-photon w state," *Phys. Rev. Lett.*, vol. 102, p. 130502, Apr 2009.

[71] P. Blasiak and M. Markiewicz, "Entangling three qubits without ever touching," *Scientific Reports*, vol. 9, p. 20131, Dec 2019.