Antes de comenzar, hay una cuestión técnica importante. Necesitas tener en LaTeX un paquete para representar circuitos cuánticos. Hasta donde yo sé, hay dos principales y me he decidido por `qcircuit` *que es el más simple (y, al parecer, menos poderoso) por la sencilla razón de que es el único que me funcionaba. Entonces en la cabecera de este documento verás:*

```
\usepackage[braket,qm]{qcircuit}
```

En realidad las opciones `[braket,qm]` *no son estrictamente necesarias, pero te las recomiendo porque permiten escribir, por ejemplo* $|\Psi\rangle$ *con* `\ket{\Psi}` *o* $\langle\Psi|\Phi\rangle$ *con* `\ip{\Psi}{\Phi}`*, que es más simple que lo que veníamos haciendo hasta ahora (al menos yo). Si quieres copiar código de la fuente de esta hoja, debes tener instalado* `qcircuit` *en tu distribución. En [2] hay documentación breve y clara. La filosofía subyacente es que, con este paquete, un circuito se escribe en LaTeX como una especie de matriz dada por sus componentes.*

Una vez que has adquirido los rudimentos teóricos necesarios en la hoja anterior y has practicado con el concepto de *qubit*, en esta hoja vamos a entrar por fin en la computación cuántica definiendo las operaciones que un ordenador cuántico puede llevar a cabo.

Recordemos que un registro de n qubits, es un elemento de $\mathbb{C}^{2^n} \cong \mathbb{C}^2 \otimes \overset{n \text{ veces}}{\cdots\cdots} \otimes \mathbb{C}^2$, el espacio de Hilbert subyacente, y se representa como

$$|\Psi\rangle = \sum_{b\in\mathcal{B}_n} a_b|b\rangle \qquad \text{con} \quad \sum_{b\in\mathcal{B}_n} |a_b|^2 = 1$$

donde $\mathcal{B}_n$ son las cadenas de ceros y unos de longitud n. Abusando de la notación, cuando está claro cuál es n, a veces se identifica cada cadena con el entero en $[0, 2^n)$ que expresa en binario. Por ejemplo, si $n = 3$, $|0\rangle = |000\rangle$, $|3\rangle = |011\rangle$ y $|4\rangle = |100\rangle$.

Según el postulado 2, la evolución de un sistema cuántico viene dada por un operador unitario y según el postulado 3, el resultado de una medición es una proyección ortogonal que colapsa el estado con cierta probabilidad. En nuestro contexto de dimensión finita, se traduce en que una *computación cuántica* es una serie de aplicaciones de matrices unitarias y proyecciones sobre elementos de $\mathcal{B}_n$. También se usa el término *circuito cuántico* en vez de computación cuántica, sobre todo para referirse a su representación mediante un esquema.

Recuerda de la asignatura de Álgebra Lineal que las aplicaciones que conservan la norma en $\mathbb{C}^N$ son necesariamente lineales y sus matrices son exactamente las matrices unitarias. En nuestro caso estas matrices tienen dimensión $\dim \mathbb{C}^{2^n} = 2^n$. Aunque no hay una definición precisa, cuando son sencillas, o bien porque n es pequeño o porque tienen una estructura especial, se llaman *puertas cuánticas* a las aplicaciones que corresponden a las matrices debido a que guardan cierta analogía con las puertas lógicas en la teoría de la arquitectura de los ordenadores convencionales. Nota que 2^n crece exponencialmente, por eso en computación cuántica no se escriben demasiadas matrices completas, más bien se indica cómo construirlas a partir de otras más sencillas.

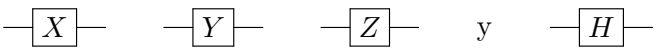
El caso más simple es $n = 1$, el de un solo qubit, con matrices de dimensión $2^1 = 2$. Por ejemplo, se llama *matriz de Hadamard* a la que tiene como matriz en la base $\{ |0\rangle, |1\rangle \}$

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

Este primer ejercicio es solo para que practiques con la definición. Tú verás si lo reflejas en tu trabajo.

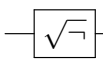
1) Verifica que H es una matriz unitaria y aplícala a $|\Psi\rangle = \frac{5+i}{6}|0\rangle + \frac{1-3i}{6}|1\rangle$ comprobando que realmente preserva su norma.

Las puertas cuánticas que actúan sobre un solo qubit se representan mediante un rectángulo que encierra el nombre de la matriz unitaria con una línea a la derecha y otra a la izquierda que representan los "cables" de entrada y de salida. A las matrices de Pauli en computación cuántica se les cambia el nombre a X, Y y Z. Así, las representaciones pictóricas de las puertas cuánticas asociadas a ellas y a H, esta última llamada *puerta de Hadamard*, serían:



La primera, la correspondiente a la primera matriz de Pauli σ_1, también se representa con el símbolo y a veces se dice que es la puerta NOT.

2) Estudia la acción de σ_1 sobre los elementos de la base y explica de dónde viene el nombre NOT y por qué a veces se representa con

 a la puerta cuántica con matriz $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$.

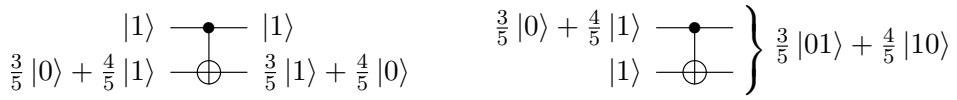
Comprueba que esta matriz es realmente unitaria.

La operación más básica con dos bit es la puerta CNOT (que abrevia *controlled* NOT). Su representación pictórica habitual es la siguiente:

Su efecto sobre los elementos de la base usual $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$ es que si el primer qubit es 0, entonces se comporta como la identidad y si es 1, entonces preserva el primer qubit y aplica NOT al segundo.

3) Halla razonadamente la matriz unitaria 4×4 que corresponde a la puerta CNOT en la base indicada. ¿Ves claro que es unitaria?

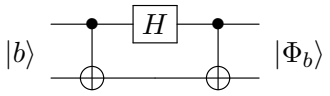
Por supuesto, cuando la puerta CNOT se aplica a elementos que no son de la base, se procede por linealidad. Por ejemplo, aplicaría $\frac{3}{5}|10\rangle + \frac{4}{5}|11\rangle$ en $\frac{3}{5}|11\rangle + \frac{4}{5}|10\rangle$ y $\frac{3}{5}|01\rangle + \frac{4}{5}|11\rangle$ en $\frac{3}{5}|01\rangle + \frac{4}{5}|10\rangle$, lo que podríamos representar como:



En el siguiente ejercicio te pido que muestres que la puerta CNOT es "nueva", no puede construirse a partir de operaciones sobre cada qubit[1].

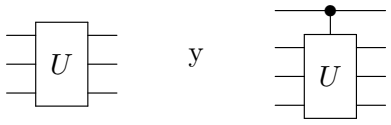
4) Demuestra CNOT $\neq U \otimes V$ con U y V operadores unitarios actuando sobre un qubit.

5) Muestra que para $b \in \mathcal{B}_2$ se cumple lo que se afirma en el siguiente circuito:



donde $|\Phi_b\rangle$ son los estados de Bell salvo por una constante multiplicativa global en Φ_2 y hacemos la identificación de b con su valor en binario.

Generalizando lo visto para $n = 1$ y para la puerta CNOT, cuando una matriz unitaria actúa en $\mathcal{B}_n$ (por tanto tiene dimensión 2^n), se representa mediante una caja con n cables de entrada y de salida. Además, un punto relleno en un cable unido a la caja de una matriz significa que si el qubit que pasa por ese cable es 0, el bloque actúa como la identidad y si es 1, conserva ese 1 y al registro correspondiente a los cables que pasan por la caja le aplica la matriz. Se dice que el primer qubit *controla* la puerta cuántica asociada a la matriz. Para U unitaria de dimensión $8 = 2^3$, la puerta correspondiente y dicha puerta controlada por un qubit situado en la primera posición, se representarían mediante:



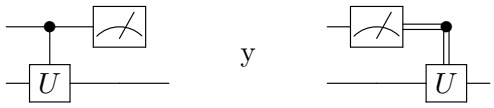
6) Explica por qué la puerta controlada corresponde al operador $P_{|0\rangle} \otimes I + P_{|1\rangle} \otimes U$ donde $P_{|j\rangle}$ es la proyección ortogonal sobre $|j\rangle$, $j = 0, 1$.

Para terminar con la representación esquemática básica de circuitos cuánticos, quedan las mediciones. Estas se indican con una especie de dial con una aguja, a veces con un cable de

[1] Esto tiene que ver con un tema llamado *universalidad*. En pocas palabras la pregunta es qué puertas cuánticas debemos diseñar para conseguir todas las matrices unitarias. Un análogo matemático sería, por ejemplo, que todas las matrices ortogonales se pueden obtener como productos de giros por los ejes y simetrías por el plano $z = 0$. Si tienes curiosidad, mira [4, §4.6], [5, §4.5.2] y [1].

entrada y sin el de salida: —  y, si no se especifica otra cosa, se supone que lo que se mide es si el qubit que pasa por el cables es $|0\rangle$ o $|1\rangle$. Es decir, en el postulado 3 se están usando las proyecciones $\left\{P_{|0\rangle}, P_{|1\rangle}\right\}$. Cuando se dibuja un cable de salida, muchas veces se pone duplicado, —  . Los cables duplicados se usan para indicar "bits clásicos". Una vez que el estado ha colapsado a $|0\rangle$ o a $|1\rangle$, ya está totalmente determinado y ulteriores mediciones del mismo tipo no están afectadas por probabilidades, darán el mismo resultado. Estos bits clásicos no dejan de ser estados especiales de qubits y por consiguiente se pueden seguir usando dentro de una computación cuántica, para controlar una puerta o para servir de entrada a ella.

7) Comprueba que



son equivalentes. Es decir, que actuando sobre un estado genérico $\sum_{b=0}^{3} a_b |b\rangle$, con $n = 2$, dan los mismos resultados con las mismas probabilidades en el cable de salida. Habitualmente se representa la segunda figura uniendo directamente con una línea vertical doble el medidor con la caja de la U.

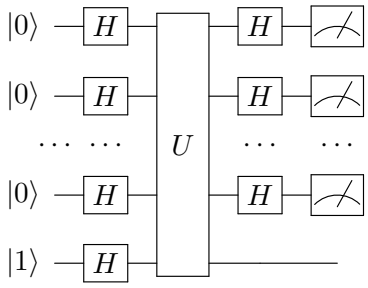
Por fin vamos a ver un algoritmo que implementado en un ordenador cuántico teóricamente resolvería un problema mucho más rápido de lo que sabemos hacer con un ordenador clásico, esto es lo que se llama *supremacía cuántica* [7] sobre todo cuando se lleva a la práctica (lo cual no está claro en este caso). Seguro que cuando lo leas pensarás que es un problema muy raro. Considéralo una primera constatación de que la computación cuántica puede tener sentido ofreciendo resultados deterministas. Es solo un ejemplo académico, sin aplicaciones. Por cierto, a día de hoy no está nada claro que en un futuro cercano puedan construirse ordenadores cuánticos de propósito general, esto es, que hagan las mismas cosas que nuestros portátiles y más rápido (mira el apartado "Engineering" de [6], especialmente "Skepticism", y [3]).

Supongamos que tenemos una función $f : \mathcal{B}_n \longrightarrow \{0, 1\}$. Es decir, a cada cadena de lo que podríamos considerar n bits clásicos, f les asigna un cero o un uno. Imaginemos que por alguna ignota razón sabemos que f cumple una de estas dos propiedades y queremos saber cuál de ellas es:

1. $\#f^{-1}(\{0\}) = \#f^{-1}(\{1\})$, se dice que f es *equilibrada* (*balanced*, en inglés).
2. $\#f(\mathcal{B}_n) = 1$, esto es, la función es constante.

Por ejemplo, para $n = 2$ la función $f(|00\rangle) = f(|11\rangle) = 1$, $f(|01\rangle) = f(|10\rangle) = 0$ es equilibrada y la función $f(|00\rangle) = 1$, $f(|01\rangle) = f(|10\rangle) = f(|11\rangle) = 0$ no entra en el problema porque estamos dando por supuesto que conocemos de antemano que la función es de uno de los dos tipos indicados.

Para resolver este problema mediante computación cuántica vamos a introducir el *algoritmo de Deutsch-Jozsa* que responde a un esquema de la forma:



En la entrada hay $n+1$ qubits. El efecto de la primera columna de puertas de Hadamard es

$$|\psi_1\rangle = (H \otimes \overset{n \text{ veces}}{\cdots\cdots} \otimes H) \left|0 \overset{n \text{ veces}}{\cdots\cdots} 0\right\rangle \otimes H\,|1\rangle$$

que, con la notación obvia, escribimos $H^{\otimes n}\,|0\rangle^{\otimes n} \otimes H\,|1\rangle$.

El operador $H^{\otimes n}$ aparece en varios algoritmos (incluso recibe un nombre, *transformada de Hadamard* o de *Walsh-Hadamard*), esta es la razón principal por la que la puerta de Hadamard es importante. Su acción sobre $|0\rangle^{\otimes n}$ es especialmente sencilla. Es posible que el siguiente ejercicio te parezca una obviedad. Incluso si es así, intenta explicarlo.

8) Prueba $H^{\otimes n}\,|0\rangle^{\otimes n} = 2^{-n/2}\sum_{b\in\mathcal{B}_n}|b\rangle$. Escribe con ello una fórmula para $|\psi_1\rangle$.

Ahora vamos con la definición de U. Si $b \in \mathcal{B}_n$ y $c \in \{0,1\}$, la acción de U sobre $|bc\rangle = |b\rangle \otimes |c\rangle$ viene dada por

$$U\,|bc\rangle = |b\rangle \otimes |c \oplus f(b)\rangle$$

donde $\oplus$ representa la suma módulo 2, por si te suena, es lo que en informática se llama la operación XOR. Esto es, $U\,|b0\rangle = |b\,f(b)\rangle$ y $U\,|b1\rangle = |b\,f^*(b)\rangle$ con $f^* = 1 - f$.

Una vez que el operador asociado a U está definido sobre los elementos de la base, por linealidad su definición se extiende a cualquier estado. Si lo piensas un poco, U permuta los elementos de la base y por tanto, esta extensión da lugar a un operador unitario.

9) Escribe para tu trabajo una explicación muy breve que extienda un poco más la justificación de que U es una matriz unitaria dada en el párrafo anterior.

La gracia de U es que asigna al estado de entrada coeficientes que determinan si f toma el valor 0 o 1 en los elementos de $\mathcal{B}_n$.

10) Sea $|\psi_2\rangle = U\,|\psi_1\rangle$. Muestra la fórmula $|\psi_2\rangle = 2^{-n/2}\sum_{b\in\mathcal{B}_n}(-1)^{f(b)}\,|b\rangle \otimes H\,|1\rangle$.

Toda la información sobre los valores de $f(b)$ para cualquier $b \in \mathcal{B}_n$ está contenida en $|\psi_2\rangle$. Esto puede parecer espectacular porque usando $n+1$ qubits, de hecho bastan los n primeros,

tenemos un estado que si lo conociéramos, nos daría los 2^n valores posibles de la función en los elementos de la base. En el contexto clásico, con una entrada de n bits fijados, solo determinamos un número entre 0 y $2^n - 1$ y por tanto solo podríamos codificar uno de los valores de la función. Sin embargo la ventaja cuántica es por ahora ilusoria porque no podemos recuperar valores específicos $f(b)$ ya que proyectar sobre $|b\rangle$, hacer una medición, nos llevaría a un resultado probabilista, según el tercer postulado. El truco está en aplicar una transformación que acumule toda la probabilidad de que sea constante o equilibrada en un solo coeficiente.

11) Sea $|\psi_3\rangle$ el estado justo antes de las mediciones en el circuito. Es decir, $|\psi_3\rangle = \left(H^{\otimes n} \otimes I\right)|\psi_2\rangle$. Demuestra la fórmula:

$$|\psi_3\rangle = 2^{-n} \sum_{b_1 \in \mathcal{B}_n} \sum_{b_2 \in \mathcal{B}_n} (-1)^{b_1 \cdot b_2 + f(b_1)} |b_2\rangle \otimes H|1\rangle$$

donde $b_1 \cdot b_2$ indica el producto escalar al identificar b_1 y b_2 con vectores de ceros y unos.

En la línea de lo mencionado cuando introdujimos el símbolo, cada una de las mediciones corresponde a las proyecciones $\left\{P_{|0\rangle}, P_{|1\rangle}\right\}$. De este modo, el resultado de las n mediciones dará cierto $b_0 \in \mathcal{B}_n$ con una probabilidad asociada. Si esa probabilidad es 1 tendremos certeza absoluta pues $\mathcal{B}_n$ es finito.

12) Con la notación anterior, muestra que si f es constante $|b_0\rangle = |0\rangle^{\otimes n}$ con probabilidad 1 y si f es equilibrada, $|b_0\rangle = |0\rangle^{\otimes n}$ con probabilidad 0.

Así pues, como por hipótesis f es constante o equilibrada, no hay otros casos, el resultado de la medición será $|0\rangle^{\otimes n}$ si y solo si f es constante.

Los valores ordenados de la función f se pueden considerar como una lista de 2^n ceros y unos. Para estar totalmente seguros de que f es constante hay que extraer $2^{n-1} + 1$ valores iguales. Sin embargo, en la práctica cuando no sea constante terminaremos mucho antes. Todavía más, si escogemos al azar 11 valores de la f y decretamos que es constante si y solo si son iguales, nos equivocaremos con probabilidad menor que 0,001.

De todas formas, ¿cómo es posible que necesitemos hasta $2^{n-1} + 1$ "operaciones" en un ordenador convencional y solo 4 pasos por puertas cuánticas y mediciones? La respuesta es que U está tratando simultáneamente con los 2^n valores de f, como indica la fórmula para $|\psi_2\rangle$, y, de hecho, depende de ellos. Es lo que se llama *paralelismo cuántico* y sugiere un choque con la realidad: quizá ni sea fácil construir U en la práctica ni tenga mucho sentido porque alberga toda la información sobre f y si uno conoce ya bien f no se plantea el problema original. En la literatura de computación cuántica se dice que U es un *oráculo*, una caja negra de implementación desconocida que cumple cierta tarea. Para que te hagas una idea hasta el año 2015 no se había superado $n = 4$ en la construcción real de U y me sorprendería que hubiera habido avances espectaculares en ese sentido.

Tarea a entregar. Debes escribir un documento que combine las soluciones de los ejercicios anteriores. De nuevo, trata de ajustarte a 7 páginas. Mi sensación es que he puesto algunos ejercicios que son demasiado simples o que constituyen pasos muy pequeños. Tienes permiso para abreviar drásticamente (incluso suprimir) lo que te parezca insustancial. El documento debe dar lugar a un tercer capítulo de tu TFG llamado *Circuitos y algoritmos cuánticos* o alguna variante que te parezca adecuada.

Ya ves que he escrito muchas explicaciones generales con palabras y también alguna cosa de repaso (a la postre he escrito más sobre los enunciados de lo que espero sobre las soluciones). Decide lo que prefieras acerca de incluir o no comentarios en este sentido.

Referencias

[1] A. Barenco. A universal two-bit gate for quantum computation. *Proc. Roy. Soc. London Ser. A*, 449(1937):679–683, 1995.

[2] B. Eastin and S. T. Flammia. qcircuit 2.6.0 Tutorial. `https://tug.org/docs/latex/qcircuit/qcircuit.pdf`, 2018.

[3] T. Hoefler, T. Häner, and M. Troyer. Disentangling hype from practicality: On realistically achieving quantum advantage. *Commun. ACM*, 66(5):82–87, apr 2023.

[4] M. Nakahara and T. Ohmi. *Quantum computing*. CRC Press, Boca Raton, FL, 2008. From linear algebra to physical realizations.

[5] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, Cambridge, 2000.

[6] Wikipedia contributors. Quantum computing — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Quantum_computing&oldid=1190931617`, 2023. [Online; accessed 21-December-2023].

[7] Wikipedia contributors. Quantum supremacy — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/w/index.php?title=Quantum_supremacy&oldid=1183187134`, 2023. [Online; accessed 21-December-2023].