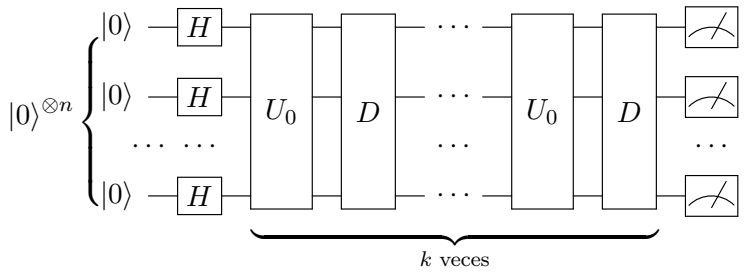
La primera parte de esta hoja está dedicada a un algoritmo cuántico de búsqueda. A diferencia de lo que ocurría con el algoritmo de Deutsch-Jozsa, el problema de partida es significativo desde el punto de vista práctico. Sin embargo, de nuevo depende de un oráculo, que representa la base de datos, cuya implementación no se especifica. De hecho, como veremos, equivale a la matriz U del algoritmo de Deutsch-Jozsa. Por lo que leo en [2] y [7], parece que el algoritmo cuántico de búsqueda solo se ha llegado a implementar con 4 qubits, lo que corresponde a una base de datos con solo 16 ítems.

Suponemos una lista de datos distintos que tiene cardinal dado por una potencia de 2 (esto no es una restricción significativa porque siempre se podría completar con datos artificiales). Queremos encontrar un dato en la lista determinando la posición que ocupa. Considerando la función $f : \{0, 1, 2, \ldots, 2^n - 1\} \longrightarrow \{0, 1\}$ que se anula excepto en el valor que indica la posición del dato buscado (comenzando por cero), el problema consiste en determinar $f^{-1}(\{1\})$. En computación cuántica el *algoritmo de Grover* ofrece una solución probabilista. Por razones obvias, los siguientes ejercicios los orientaré hacia una presentación de este algoritmo más cercana a temas de álgebra lineal que lo habitual en las referencias (cf. [3, §7], [4, §6.1], [5, §5]).

Identificamos, como hemos hecho otras veces, $\{0, 1, 2, \ldots, 2^n - 1\}$ con $\mathcal{B}_n$. Tenemos entonces $f : \mathcal{B}_n \longrightarrow \{0, 1\}$ y sabemos que $\#f^{-1}(\{1\}) = 1$. Nuestro objetivo es hallar el $b_0 \in \mathcal{B}_n$ que realice esta imagen inversa, es decir, que cumpla $f(b_0) = 1$. Llamaremos $|\phi_0\rangle$ a $|b_0\rangle$.

1) Escribe unas líneas para tu trabajo reflejando el modelo matemático con la f para el problema de búsqueda añadiendo las explicaciones que consideres necesarias si alguno de los puntos anteriores te resulta oscuro.

El circuito que corresponde al algoritmo de Grover es:



La salida es $|\phi_0\rangle$ con cierta probabilidad p cercana a 1. El hecho de que sea un algoritmo probabilista no es tan importante en términos prácticos porque si hacemos funcionar el algoritmo m veces, la probabilidad de que ninguna de ellas obtengamos la solución b_0 es $(1-p)^m$ que decae exponencialmente.

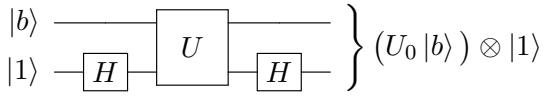
Ya sabemos por la hoja anterior que el efecto sobre $|0\rangle^{\otimes n}$ de la columna de puertas de Hadamard es $|\phi_1\rangle = 2^{-n/2} \sum_{b \in \mathcal{B}_n} |b\rangle$. Por tanto, el algoritmo de Grover consiste en medir los n qubits de $(DU_0)^k |\phi_1\rangle$. Aquí y en lo sucesivo considero U_0 y D, definidos a continuación, como operadores en vez de como matrices.

Para entender las definiciones de U_0 y D te conviene recordar unas matrices de la asignatura de Cálculo Numérico I. Dado un vector unitario $\vec{v} \in \mathbb{R}^N$ la *matriz de Householder* asociada a él es $H_{\vec{v}} = I - 2\,\vec{v}\,\vec{v}^{\,t}$ donde se identifica $\vec{v}$ con la matriz $N \times 1$ dada por sus coordenadas. Es una matriz ortogonal que representa una simetría. La definición se extiende al caso complejo.

2) Dado $\vec{v} \in \mathbb{C}^N$ con $\|\vec{v}\| = 1$, muestra que $H_{\vec{v}} = I - 2\,\vec{v}\,\vec{v}^{\,*}$ es una matriz unitaria, donde $*$ indica la traspuesta conjugada. Comprueba además que representa una simetría por el plano perpendicular a $\vec{v}$ en el sentido de que $H_{\vec{v}}\,\vec{v} = -\vec{v}$ y $H_{\vec{v}}\,\vec{w} = \vec{w}$ si $\vec{v} \perp \vec{w}$. Nota que, en general, para $\vec{u} \in \mathbb{C}^N$ se cumple $H_{\vec{v}}\,\vec{u} = \vec{u} - 2\langle \vec{v}, \vec{u} \rangle \vec{v}$.

Se define U_0 como el operador que en la base canónica $\{|b\rangle\}_{b \in \mathcal{B}_n}$ tiene como matriz $H_{|\phi_0\rangle}$ y D, llamado *operador de difusión de Grover*, se define análogamente con matriz $-H_{|\phi_1\rangle}$. En particular, $U_0\,|\phi_0\rangle = -\,|\phi_0\rangle$ y $U_0\,|b\rangle = |b\rangle$ para todo $b \in \mathcal{B}_n - \{b_0\}$.

La puerta cuántica asociada a U_0 depende de b_0 y por tanto de la propia f. Es un oráculo para consultar la base de datos sin que se especifique su implementación, al igual que la U en el algoritmo de Deutsch-Jozsa. De hecho, cambiando la función en la definición de U por nuestra f, es posible obtener U_0 a partir de U gracias al circuito



3) [Opcional] Si quieres, puedes incluir este circuito en tu trabajo y también explicarlo si el espacio lo permite.

4) Obviamente $\mathfrak{B}_2 = \{\, |\phi_0\rangle, |\phi_1\rangle \,\}$ es base de un subespacio de dimensión 2. Extendámosla con vectores ortogonales a ellos a una base $\mathfrak{B} = \{\, |\phi_0\rangle, |\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_{2^n-1}\rangle \,\}$ de todo el espacio. Muestra que la matriz del operador DU_0 en $\mathfrak{B}$ es

$$\left(\begin{array}{c|c} G & O_{2,\,2^n-2} \\ \hline O_{2^n-2,\,2} & -I_{2^n-2,\,2^n-2} \end{array}\right) \qquad \text{con} \qquad G = \begin{pmatrix} 1 & 2^{1-n/2} \\ -2^{1-n/2} & 1 - 2^{2-n} \end{pmatrix}$$

donde I y O denotan la matriz identidad y la matriz nula de las dimensiones señaladas. Indicación: Lo fundamental es hallar $DU_0\,|\phi_0\rangle$ y $DU_0\,|\phi_1\rangle$.

Ortonormalizamos $\mathfrak{B}$ con el proceso de Gram-Schmidt a $\mathfrak{B}' = \{\, |\psi_0\rangle, \ldots, |\psi_{2^n-1}\rangle \,\}$. Nota que por la estructura del proceso, $\mathfrak{B}_2$ y $\mathfrak{B}'_2 = \{\, |\psi_0\rangle, |\psi_1\rangle \,\}$ son bases del mismo subespacio.

5) Comprueba que $|\psi_0\rangle = |\phi_0\rangle$ y $|\psi_1\rangle = \big(2^{n/2}\,|\phi_1\rangle - |\phi_0\rangle\big)/\sqrt{2^n - 1}$ y explica por qué la matriz de DU_0 en la base $\mathfrak{B}'$ es igual que la anterior salvo cambiar G de la base $\mathfrak{B}_2$ a la base $\mathfrak{B}'_2$. Halla la matriz G en la base $\mathfrak{B}'_2$ y prueba que es un giro de ángulo $\alpha = -2 \operatorname{arc\,sen}\big(2^{-n/2}\big)$.

6) Deduce $(DU_0)^k\,|\psi_0\rangle = \cos(k\alpha)\,|\psi_0\rangle + \operatorname{sen}(k\alpha)\,|\psi_1\rangle$ y $(DU_0)^k\,|\psi_1\rangle = -\operatorname{sen}(k\alpha)\,|\psi_0\rangle + \cos(k\alpha)\,|\psi_1\rangle$.

7) Demuestra que la probabilidad p de que al medir $(DU_0)^k\,|\phi_1\rangle$ obtengamos $|\phi_0\rangle$ viene dada por $p = \text{sen}^2\big((k+\frac{1}{2})\alpha\big)$. Indicación: ¿Ves claro que $p = |\,\langle\phi_0|(DU_0)^k|\phi_1\rangle\,|^2$ por la teoría general? Comprueba que $|\phi_1\rangle = \cos\frac{\alpha}{2}\,|\psi_1\rangle - \text{sen}\,\frac{\alpha}{2}\,|\psi_0\rangle$ y aplica el ejercicio anterior.

8) Escogiendo $k = \big\lfloor -\frac{\pi}{2\alpha}\big\rfloor$, con $\lfloor x\rfloor$ la función parte entera, obtén $p \geq 1 - 2^{-n}$. Indicación: Sea $\delta = -k - \frac{\pi}{2\alpha}$. Justifica $p = \cos^2\big((\delta - 1/2)\alpha\big) \geq \cos^2(\alpha/2)$.

Piensa que sin computación cuántica, hallar el b_0 que cumple $f(b_0) = 1$ requiere examinar los valores $f(0), f(1), f(2), \ldots$ hasta encontrar $f(b_0) = 1$ y en media haremos $\frac{1}{2}\cdot 2^n = 2^{n-1}$ llamadas a la función (a la base de datos). Mediante el algoritmo de Grover hay k llamadas al oráculo y como k es comparable a $2^{n/2}$, se gana una raíz cuadrada. De nuevo el truco está en el paralelismo cuántico, la posibilidad de trabajar con la superposición de muchos estados.

La parte final de esta hoja está dedicada a un par de aspectos que pertenecen a la teoría de la llamada *información cuántica* [6].

En nuestros ordenadores estamos acostumbrados a copiar información, borrarla y enviarla a otros usuarios. En computación cuántica siempre está el problema subyacente de que al medir un qubit colapsa y no está claro que estas manipulaciones de la información en las cuales se basa en gran medida la computación clásica tengan análogos cuánticos. De hecho, hay varios resultados con nombres ilustrativos como *no-cloning theorem*, *no-deleting theorem*, *no-broadcasting theorem* y otros (mira el segundo apartado de [6]), que imponen limitaciones muy severas en este sentido. Se dice que son *no-go theorems*, imposibilidades teóricas. Aquí nos ocuparemos del primero de ellos y después estudiaremos un resultado positivo más complicado del que seguro que has oído hablar.

El *teorema de no clonación* (*no-cloning theorem*, en inglés) dice que no podemos introducir un estado genérico y acabar con él por duplicado. Como las puertas cuánticas tienen el mismo tamaño de entrada y de salida, en la entrada debemos completar el estado a copiar con un "espacio" del mismo número de qubits (por ejemplo $|0\rangle^{\otimes n}$). En términos matemáticos precisos, el teorema de no-clonación afirma que fijado un estado (normalizado) $|\phi_0\rangle \in \big(\mathbb{C}^2\big)^{\otimes n}$ no existe un operador unitario U tal que $U\big(\,|\phi\rangle\otimes|\phi_0\rangle\,\big) = |\phi\rangle\otimes|\phi\rangle$ se verifique para todo $|\phi\rangle \in \big(\mathbb{C}^2\big)^{\otimes n}$.

9) Demuestra el teorema de no clonación. Indicación: Los operador unitarios conservan el producto escalar. Halla el producto escalar de $U\big(\,|\phi\rangle\otimes|\phi_0\rangle\,\big)$ y $U\big(\,|\psi\rangle\otimes|\phi_0\rangle\,\big)$ de dos formas distintas para $|\phi\rangle$ y $|\psi\rangle$ estados (normalizados) distintos no ortogonales.

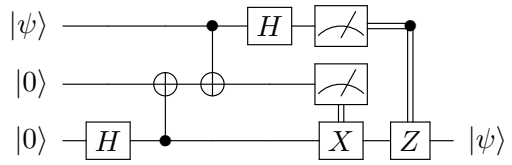
La siguiente extensión es relevante porque $|\phi\rangle\otimes|\phi\rangle$ y $u\,|\phi\rangle\otimes|\phi\rangle$ son físicamente indistinguibles si no interactúan con otros estados:

10) Adapta la demostración para obtener que $U\big(\,|\phi\rangle\otimes|\phi_0\rangle\,\big) = u\,|\phi\rangle\otimes|\phi\rangle$ es también imposible con $u \in \mathbb{C}$ de módulo 1, incluso permitiendo que u dependa de $|\phi\rangle$ y $|\phi_0\rangle$.

El fenómeno de la *teleportación cuántica* (o *teletransporte cuántico*, ninguno de los dos sustantivos aparece en el diccionario) es una especie de complemento o vía de escape del teorema de no clonación. Sobre todo en la literatura de divulgación se suele explicar bastante mal. No podemos duplicar estados y tampoco podemos medir estados sin alterarlos, sin que colapsen. La teleportación cuántica consiste en que, sorprendentemente, partiendo de un estado puedo destruirlo de una manera especial haciendo mediciones y con los resultados darle a una segunda persona suficientes pistas para que cree un estado como el inicial. Esas pistas se las enviaré por un canal convencional (llamando por teléfono, escribiendo una carta,...) y por tanto tardarán en llegar si el receptor está lejos. De todas formas, sorprende que alguien lejano sea capaz de reconstruir exactamente algo que estaba aquí y sobre lo que yo solo pude extraer información probabilista (y lo mismo le ocurrirá al destinatario). Es, en definitiva, una copia remota destruyendo el original. Ha habido bastantes experimentos, algunos con distancias gigantescas, ratificando que esto es posible.

11) Da un vistazo a [1, §2.6] sin meterte en los detalles si te resultan farragosos. Simplemente es una recomendación de lectura introductoria para que entiendas mejor algunos aspectos del fenómeno. Dejo a tu albedrío reflejar o no en tu trabajo algo de lo que leas ahí.

12) Lee [4, §1.3.7] y escribe con tus propias palabras su contenido para tu trabajo complementándolo con las explicaciones que consideres adecuadas. Tiende a algo sintético. Lo más importante es reflejar en qué consiste el fenómeno lo cual, como he dicho, suele explicarse mal. Incluye el circuito correspondiente (cópialo de la fuente de este documento):



Nota que en la figura 1.12 se definen los estados de Bell de una forma ligeramente distinta la nuestra en la hoja 2.

Tarea a entregar. Escribe un documento que combine las soluciones de los ejercicios anteriores. Trata de ajustarte a 8 páginas. Te recomiendo evitar detalles de los cálculos (por ejemplo del cambio de base de G o de la acción de los operadores en el último ejercicio). Mi idea original era incluir la teleportación en la segunda hoja. No lo hice porque habría quedado muy larga y ahora la parte de información cuántica pega poco con el algoritmo de Grover. Dos opciones son que dividas el material en dos capítulos breves llamados algo así como *Información cuántica* y *El algoritmo de búsqueda de Grover* o que los juntes en uno solo yuxtaponiendo ambos títulos.

Referencias

[1] F. Chamizo. Un poco de física cuántica para chicos listos de primero (del grado de física o matemáticas). http://matematicas.uam.es/~fernando.chamizo/physics/files/qf.pdf, 2015.

[2] Y. El Kaderi, A. Honecker, and I. Andriyanova. Performance of uncoded implementation of Grover's algorithm on today's quantum processors. In *2023 IEEE Information Theory Workshop (ITW)*, pages 209–214, 2023.

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

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

[5] J. Rué and S. Xambó. Mathematical introduction to quantum computing. *Butl. Soc. Catalana Mat.*, 28(2):183–231, 234, 2013. https://web.mat.upc.edu/sebastia.xambo/QC/qc.pdf.

[6] Wikipedia contributors. Quantum information – Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Quantum_information&oldid=1189111171, 2023. [Online; accessed 6-January-2024].

[7] K. Zhang, P. Rao, K. Yu, H. Lim, and V. Korepin. Implementation of efficient quantum search algorithms on NISQ computers. *Quantum Inf. Process.*, 20(7):Paper No. 233, 27, 2021.