Aplicaciones de algoritmos cuánticos en la resolución de problemas algebraicos

Proyecto Teórico/Computacional 2021-20

Autor:

Daniel Felipe Afanador Rodríguez

Estudiante de Física

Profesor Asesor:

Gabriel Téllez Acosta Ph.D.
Bogotá, D.C. - Colombia

28 de noviembre de 2021

Resumen

La computación cuántica ha desarrollado, en las últimas decadas, varias herramientas útiles para la resolución de problemas algebraicos basadas en los postulados de la mecánica cuántica, así como a partir de conceptos fundamentales de la física estadística. La posibilidad de crear computadores cuyo funcionamiento está basado en las leyes de la física cuántica, por oposición a la física clásica, ha despertado un gran interés y se ha convertido en un importante tema de investigación científica. Como ejemplos meritorios, los algoritmos de Deustch-Josza, Grover y Shor llegan a soluciones específicas de situaciones planteables dentro de la teoría de la mecánica estadística y la experimentación, de manera que un análisis detallado de las propiedades más relevantes de cada uno de estos permitiría extraer nueva información correspondiente al manejo y desarrollo de los algoritmos cuánticos. En este sentido, este proyecto teórico/computacional pretende investigar las técnicas usadas en los algoritmos cuánticos para solucionar problemas numéricos, polinomiales y probabilísticos, con respecto a implementaciones básicas de circuitos cuánticos en unidades de procesamiento clásico y cuántico. Más aún, con objeto de evaluar el poder computacional de cada algoritmo desarrolado, la cuantificación de la precisión y de los tiempos de procesamientos resulta esencial para la comprensión de un análisis concreto. Los resultados de este proyecto mostraron que los métodos de amplificación de amplitud, la técnica de búsqueda no estructurada, el método de estimación de fase y la transformada cuántica de Fourier determinan las operaciones algebraicas y cuánticas más importantes de los algoritmos de Deustch-Josza, Grover y Shor. Desde ejemplos que van desde el experimento de doble rendija hasta las transformaciones de estados cuánticos por medio de sus fases, se verifica cómo la superposición de estados y el concpeto de paralelismo cuántico resulta fundamental en el análisis y el cómputo de las amplitudes de probabilidad de cada cubit. En particular, el algoritmo de Shor permitió la factorización de los números $N = 15$, $N = 35$ y $N = 65$ para ambas unidades de procesamiento, a pesar de remarcadas diferencias en la probabilidad de éxito y los timepos de ejecución de cada sistema. La aplicabilidad de los algoritmos cuánticos en computadores clásicos, a pesar de errores computacionales, es coherente y permite llegar a resultados con precisión cercana a 0,5. No obstante, la simulación del circuito cuántico implementado determina tiempos de ejecución polinomiales, como se esperaba. En conclusión, los algoritmos cuánticos construidos para la resolución de problemas algebraicos son extrapolables a una gran variedad de sistema físicos, ya sean clásicos o cuánticos, y pueden reproducir, con buena precisión, resultados en tiempos de ejecución realizables.

Abstract

Quantum computing has developed, in recent the decades, several useful tools for solving algebraic problems based on the postulates of quantum mechanics, as well as from fundamental concepts of statistical physics. The possibility of creating computers whose operation is based on the laws of quantum physics, as opposed to classical physics, has aroused great interest and has become an important topic of scientific research. As meritorious examples, the Deustch-Josza, Grover and Shor algorithms arrive at specific solutions of situations posed within the theory of statistical mechanics and experimentation, so that a detailed analysis of the most relevant properties of each of these would allow the extraction of new information corresponding to the handling and development of quantum algorithms. In this sense, this theoretical / computational project aims to investigate the techniques used in quantum algorithms to solve numerical, polynomial and probabilistic problems, with respect to basic implementations of quantum circuits in classical and quantum processing units. Furthermore, in order to evaluate the computational power of each developed algorithm, quantifying the precision and processing times is essential for the analytical understanding of the system. The results of this project showed that the amplitude amplification methods, the unstructured search technique, the phase estimation method and the quantum Fourier transform determine the most important algebraic operations of the Deustch-Josza, Grover and Shor algorithms. From examples that go from the double-slit experiment to the transformations of quantum states through their phases, it is verified how the superposition of states and the concept of quantum parallelism is fundamental in the analysis and computation of the probability amplitudes of each cubit. In particular, the Shor algorithm allowed the factorization of the numbers $N = 15$, $N = 35$ and $N = 65$ for both processing units, despite notable differences in the probability of success and the times of success. execution of each system. The applicability of quantum algorithms in classical computers, despite computational errors, is consistent and allows the user to reach results with precision close to 0,5. However, the simulation of the implemented quantum circuit determines polynomial execution times, as expected. In conclusion, quantum algorithms built for solving algebraic problems can be extrapolated to a great variety of physical systems, whether classical or quantum, and can reproduce, with good precision, results at achievable execution times.

Índice

Índice de figuras

Índice de cuadros

1. Introducción

Un algoritmo cuántico es un conjunto ordenado de operaciones sistemáticas que se ejecutan en una computadora cuántica con el objetivo de lograr una mayor eficiencia con respecto a cualquier algoritmo clásico posible [1]. Esta eficiencia, así como una gran variedad de características intrínsecas de los algoritmos cuánticos, se encuentra estrechamente relacionada a su construcción, en tanto que uno de los propósitos primordiales de la computación cuántica es solucionar cualquier tarea computacional en una sucesión de pasos, o en un tiempo de ejecución, que sea escalable de manera polinomial al tamaño de la entrada del algoritmo [2]. Lo anterior implica que un algoritmo cuántico debe poder manejar y analizar información coherentemente para reproducir resultados que muestren la validez de los efectos físicos cuánticos con respecto a un tiempo de ejecución realizable.

A partir de la fundamentación de varios principios de la mecánica cuántica aplicados a la computación, se ha abierto la posibilidad de crear nuevos métodos relacionados a la resolución de problemas algebráicos. Como ejemplo meritorio, el algoritmo de Shor [3] expone la eficiencia de la factorización de números enteros por medio del principio de superposición y a través de transformaciones cuánticas de Fourier [4]. No obstante, el uso de procedimientos más sencillos, pero menos eficientes, también permiten determinar un punto de partida para el aprendizaje y la comprensión de las técnicas básicas para el desarrollo de algoritmos cuánticos.

En primer lugar, resulta importante contextualizar los uso de la computación cuántica a partir de su herramienta básica: los cubits. El cubit es un sistema cuántico que se define a partir de una combinación lineal de dos estados propios, $|0\rangle$ y $|1\rangle$. En virtud del álgebra lineal, cada cubit se puede considerar como un vector de norma unitaria sobre un espacio vectorial complejo, de manera que su base esté determinada por el conjunto $\{0, 1\}$ y que su representación sea de la forma $\alpha|0\rangle + \beta|1\rangle$, donde α, β son números complejos. Otras herramientas esenciales para el desarrollo de algoritmos cuánticos están relacionadas a la implementación de puertas lógicas cuánticas, las cuales permiten que se minimice la sucesión de pasos lógicos a utilizar, así como los tiempos de ejecución. Las puertas cuánticas son operadores unitarios que permiten, principalmente, preparar la superposición de estados, modificar las fases relacionadas a cada qubit y medir la información para representarla en un bit clásico.

La información codificada en un algoritmo cuántico se expresa, por lo general, en unidades de procesamiento cuántico. A partir de computadores que utilizan circuitos superconductores basados en procesadores cuánticos, las unidades de procesamiento cuántico generan pulsos de microondas a distintas frecuencias y duraciones para controlar y medir la información contenida en cada cubit. No obstante, para que esta información no sea destruida por medio de energía térmica en forma de calor, es necesario contener los procesadores cuánticos aislados en refrigeradores a temperaturas cercanas a los 15 mK [5]. Otras aproximaciones para la configuración de un computador cuántico están basadas en trampas de iones, puntos cuánticos, atomos neutros, etc.

Con respecto a la teoría de las unidades de procesamiento cuántico, en virtud de los criterios de DiVincenzo [6], los computadores cuánticos deben estar caracterizados por:

- (i) Un sistema físico escalable con cubits bien definidos.
- (ii) La habilidad para inicializar el estado de los cubits a un estado de referencia $|0 \cdots 0\rangle$.
- (iii) Tiempos largos de decoherencia cuántica, mucho mayores a los tiempos de operación de las sucesiones lógicas del circuito.

•(iv) Un conjunto completo de compuertas (cuánticas) lógicas.
•(v) La capacidad de medir cada cubit del sistema.

Los postulados previos indican, en primer lugar, la selección de una base computacional construida a partir de dos estados cuánticos, $|0\rangle$ y $|1\rangle$, de manera que se defina cada cubit según la superposición de estos estados. Por ejemplo: $|101\rangle = |1\rangle \otimes |0\rangle \otimes |1\rangle = \frac{1}{\sqrt{2}}(|011\rangle + |111\rangle)$. Luego, la definición del estado $|0 \cdots 0\rangle$ debe ser única, de forma tal que las mediciones subsecuentes tengan un orden con respecto al cubit de referencia. Por otra parte, debido a la naturaleza delicada de la información contenida en un cubit, es importante tomar en cuenta los timepos de relajación y de desfase de cada cubit, ya que en la medida que la información del qubit sea degradada por efectos de ruido, calor, fluctuaciones electromagnéticas o vibraciones, las mediciones de las fases obtenidas tendrán una cantidad considerable de errores cuantitativos. Para evitar este problema, resulta relevante considerar cada cubit como un sistema aislado. Además, para poder manipular los cubits, es necesario construir un conjunto completo de operaciones, compuesto generalmente por compuertas lógicas de dos cubits y un operador unitario de un cubit. Evidentemente, las condiciones dadas en (iii) y (iv) pueden llegar a ser contrarias, ya que largos tiempos de decoherencia implican tiempos de operación grandes, por lo que encontrar un equilibrio entre ambos postulados es importante dentro de la práctica. Finalmente, cada unidad de procesamiento cuántico debe estar en la capacidad de evaluar, cuantitativamente, los errores computacionales suscitados dentro de cualquier algoritmo cuántico.

Para interpretar el mecanismo de un programa cuántico básico por medio de los anteriores criterios, es posible considerar uno de los primeros algoritmos cuánticos que manejó una mayor velocidad de cómputo que su contraparte clásica: el algoritmo de Deutsch-Jozsa. Este algoritmo permite exponer de manera sencilla las 3 principales componentes para la creación de un sistema algebraico cuántico: la superposición de estados cuánticos, una función de *Oracle* o de *caja negra*, y el paralelismo cuántico.

Considere una función f que tome como entrada un valor entero entre 0 y 1 y devuelve un valor entre 0 y 1:

$$f : \{0, 1\} \to \{0, 1\}. \tag{1}$$

Se define que f es una función **balanceada** si f asigna a la mitad de sus elementos de su conjunto de entrada al valor 0 y asigna la otra mitad al valor 1. Por otro lado, se define que f es una función **constante** si su valor de salida es el mismo a pesar del valor de entrada:

$$\text{Balanceada:} \quad f(0) = 0, f(1) = 1, \tag{2}$$

$$\text{Balanceada:} \quad f(0) = 1, f(1) = 0, \tag{3}$$

$$\text{Constante:} \quad f(0) = 0, f(1) = 0, \tag{4}$$

$$\text{Constante:} \quad f(0) = 1, f(1) = 1. \tag{5}$$

La tarea computacional a desarrollar involucra determinar si, debido a una función f dada, f es balanceada o es constante. A pesar de que el procedimiento a realizar resulta sencillo, los conceptos cuánticos que se aplican resultan importantes para la construcción de algoritmos cuánticos algebráicos. Por un lado, dentro de la computación clásica, la solución de este tipo de sistemas es dada a partir de un par de preguntas lógicas que determinan los valores de $f(0)$

y $f(1)$ y por medio de afirmaciones lógicas de la forma *if* y *then* que permitan llegar a una conclusión. Lo anterior conlleva una sucesión de 3 pasos lógicos. Sin embargo, si el conjunto de entrada tiene un número n de elementos, el tiempo de ejecución crece exponencialmente, **en tanto que es necesario realizar, clásicamente,** $2^{n-1}+1$ **pasos lógicos para verificar cada hipótesis.**

Por otra parte, resulta relevante notar que la codificación de cada uno de los pasos lógicos del algoritmo de Deustch-Jozsa puede extrapolarse, en el sentido de que su implementación puede llevarse a cabo en cualquier sistema computacional que considere un número par de elementos. En virtud de las ecuaciones (2), (3), (4) y (5), si se configuran los $n = 2$ elementos del conjunto de entrada por medio de 2 cubits (relacionados a los valores de entrada y de salida 0 y 1), entonces resulta posible usar puertas lógicas de Hadamard [7] para determinar una superposición α de estados cuánticos que represente todas las combinaciones de los 4 bits resultantes:

$$|\alpha\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle . \tag{6}$$

Para el algoritmo de Deutsch-Jozsa, la base de Hadamard permite escribir los dos cubits resultantes x y y por medio del producto tensorial mostrado en la ecuación (7),

$$(x \otimes y) := \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{7}$$

Luego, continuando con el subsecuente paso lógico, se determina una función *Oracle* o de *caja negra* U_f [8] por medio de una transformación lineal $U_f|xy\rangle = |xy \oplus f(x)\rangle$, la cual considera los siguientes casos:

• Si $f(x) = 0$, el segundo cubit toma el mismo valor de entrada, de manera que

$$U_f : (x, y) \to (x, y \oplus 0) = (x, y), \tag{8}$$

$$U_f : |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \mapsto |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right). \tag{9}$$

• Si $f(x) = 1$, el segundo cubit toma el valor opuesto al valor de entrada, de manera que

$$U_f : (x, y) \to (x, y \oplus 0) = (x, -y), \tag{10}$$

$$U_f : |x\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \mapsto |x\rangle \left(\frac{|1\rangle - |0\rangle}{\sqrt{2}} \right). \tag{11}$$

Examinando los valores de salida, se generaliza la ecuación resultante como

$$U_f : \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} \to (-1)^{f(x)}|x\rangle|y\rangle = \frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}}. \tag{12}$$

Así, se observa que debido a los 4 conjuntos de valores que pueden tomar $\{f(0), f(1)\}$, la superposición del primer cubit indica que si la primera entrada de $U_f(x, y)$ es $\pm\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, entonces f debe ser constante, mientras que si es $\pm\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, entonces f debe ser balanceada. No obstante, el signo $\pm$ no afecta la medida de los resultados de la superposición, en tanto que su valor matemático es equivalente al de un corrimiento de fase que es físicamente indistiguible. Esto nos indica que el algoritmo desarrollado va a medir los mismos resultados con respecto a la función f, ya sea constante o balanceada. Finalmente, para verificar que las medidas de las funciones constantes y balanceadas sean distintas, se aplica nuevamente una puerta lógica de Hadamard para determinar que la función constante será medida como $|0\rangle$ y la función balanceada será medida como $|1\rangle$:

$$H\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] = |0\rangle, \tag{13}$$

$$H\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] = |1\rangle. \tag{14}$$

El concepto de paralelismo cuántico permitirá, entonces, calcular los estados resultantes para el caso n-ésimo, y consecuentemente se podrán medir los correspondientes valores resultantes entre 0 y 1. Esta explicación simplificada de un algoritmo cuántico básico resulta replicable dentro de esquemas y circuitos más complejos, tales como el algoritmo de Grover [9], pero también encuentra restricciones relacionadas a la implementación de la unidad de cómputo cuántica a utilizar para ejecutar el algoritmo cuántico [10].

2. Objetivos

2.1. Objetivo General

• Desarrollar algoritmos algebraicos propios de la computación cuántica para ser aplicados en una unidad simulada de procesamiento cuántico.

2.2. Objetivos Específicos

• Aprender las técnicas usadas en los algoritmos cuánticos para solucionar problemas numéricos, polinomiales y probabilísticos.

• Investigar las implementaciones de los algoritmos algebraicos básicos, tales como el algoritmo de Deustch-Jozsa, el algoritmo de Grover y el algoritmo de Shor, en unidades de cómputo cuántica simuladas.

• Cuantificar la precisión y los tiempos de procesamiento de los algoritmos algebraicos en computadores cuánticos.

3. Problema de investigación y justificación

El progreso de la mecánica cuántica dentro de varios sistemas algebraicos y computacionales ha permitido la exploración de nuevas características propias de los algoritmos cuánticos en unidades de procesamiento cuántico, ya sean reales o simuladas. Más aún, el auge de la computación cuántica ha revolucionado la teoría computacional, y ha renovado los métodos para realizar cálculos complejos en tiempos razonables. En esta medida, la posibilidad de crear computadores y algoritmos cuyo funcionamiento está basado en las leyes de la física cuántica, por oposición a la física clásica, resulta atractivo no solo por su utilidad práctica y comercial, sino porque también propone una nueva forma de conocimiento, en la cual una próxima generación de científicos deberá retarse a pensar, intuir y trabajar de acuerdo a procesos y sistemas lógico-cuánticos.

Debido a esto, el presente trabajo buscará exponer las técnicas más comunes para el desarrollo de algoritmos cuánticos y sus respectivas limitaciones, las cuales se encuentran relacionadas a una diversa gama de factores, que van desde la intuición computacional de los desarrolladores hasta la constitución misma de las unidades de cómputo cuántica. De manera específica, este proyecto de investigación pretende dar respuesta a la siguiente pregunta: **¿Cómo se desarrollan los algoritmos cuánticos, enfocados a la resolución de problemas algebráicos, en unidades de procesamiento cuántico?**

4. Metodología

Inicialmente, se realizó una búsqueda literaria en Google Scholar, SpringerMaterials y arXiv sobre los conceptos básicos y las técnicas para el desarrollo de algoritmos cuánticos. De manera análoga, se revisaron libros y *papers* informativos que expongan los fundamentos teóricos de la computación cuántica. Posteriormente, se indagó a profundidad sobre los algoritmos de Deutsch-Jozsa, Grover y Shor para llegar a un consenso sobre las mejoras y las dificultades más relevantes de la computación cuántica en comparación a la computación clásica. Así mismo, se identificaron cualidades cuantitativas que permitieron estudiar y describir analíticamente la eficiencia de cada algoritmo a detalle, de manera que se reprodujeron y se graficaron los resultados obtenidos por medio del editor **IBM Quantum Composer**, así como a través de un código fuente de Python realizado desde un computador personal.

Tras haber realizar un exhaustivo estudio de las características primordiales de los algoritmos cuánticos algebraicos, se desarrollaron dos sucesiones de pasos lógicos que lograron determinar soluciones a varias tareas computacionales análogas al algoritmo de Shor, las cuales fueron ejecutadas por medio del software Qiskit. Luego, se evaluó la eficiencia de los algoritmos desarrollados en Qiskit, con respecto a la computación clásica, por medio de su tiempo de ejecución, de manera que se identificaron las fallas y las virtudes del sistema en cuestión. Finalmente, se realizó, en la plataforma de edición de textos Overleaf, un informe descriptivo sobre los resultados computacionales de la aplicación de algoritmos cuánticos en la resolución de problemas algebraicos.

5. Consideraciones éticas

Los algoritmos cuánticos a desarrollar tienen un propósito puramente académico, de manera que sus usos estarán completamente relacionados a un estudio teórico/computacional universitario. Los resultados y los códigos usados de este proyecto estarán abiertos al público en un repositorio de Github.[1] Además, la literatura usada en este proyecto será debidamente referenciada.

6. Resultados y Análisis

Los algoritimos cuánticos algebraicos permiten caracterizar, primeramente, fenómenos de interferencia a partir de modelos matemáticos sencillos. En virtud del algorimto de Deustch-Jozsa, resulta posible considerar el siguiente ejemplo demostrativo: Una partícula, determinada por un comportamiento ondulatorio, viaja desde una fuente hasta un arreglo de detectores, identificados por puntos negros, a partir de dos o más caminos de manera simultánea, como se observa en la Figura 1. La probabilidad de que la partícula sea observada estará concentrada en los detectores que identifiquen ondas entrantes de igual fase.

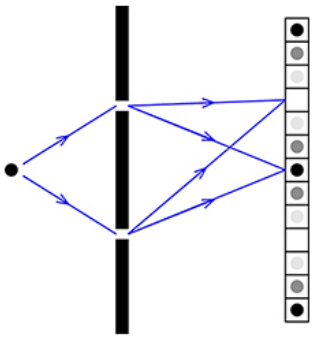

Figura 1: Diagrama de los posibles recorridos de dos caminos que parten desde una fuente hasta un arreglo de detectores, identificados por puntos negros, en virtud del uso de una doble rendija.

La construcción de este experimento de interferencia puede plantearse teóricamente, y de manera simplificada, a partir de 2^n detectores y 2^n posibles caminos desde la fuente a cada uno de los detectores: En primer lugar, se denominan, a partir de bits de entrada de tamaño n, los posibles caminos y los detectores como x y y, respectivamente. Luego, considere que la fase φ relacionada a un camino x, que llega hasta un detector y, se define como

$$\varphi(x, y) = C(-1)^{f(x)+x\cdot y}, \tag{15}$$

donde C es una constante de normalización, $f(x)$ es la función implementada en el algoritmo de Deustch-Jozsa, y $x \cdot y = \sum_{i=1}^{n} x_i y_i$ es el producto interno usual. De esta forma, la probabilidad $\mathcal{P}$ de observar la partícula en el detector y es calculada al tomar la norma al cuadrado de la suma de las amplitudes de todos los caminos posibles x que terminan en el detector y:

[1] https://github.com/SushiDeLosAndes

$$\mathcal{P}(y) = \left| \sum_x \varphi(x,y) \right|^2 = \left| C \sum_x (-1)^{f(x)+x\cdot y} \right|^2 . \tag{16}$$

Nótese que las amplitudes de este problema, caracterizadas desde la mecánica cuántica, pueden tomar valores negativos y positivos, a diferencia de las probabilidades clásicas que toman únicamente valores no negativos. La condición de normalización $\sum_y \mathcal{P}(y) = 1$ permite deducir que $C = 2^{-n}$.

Ahora, al calcular la probabilidad $\mathcal{P}(y = 0^n)$ de observar la partícula en el detector $y = 0^n$, codificado a partir de un bit donde cada una de sus n entradas es igual a 0, se obtiene que

$$\mathcal{P}(y = 0^n) = \left| 2^{-n} \sum_x (-1)^{f(x)} \right|^2 . \tag{17}$$

Este caso específico permite contextualizar la aplicación del algoritmo de Deutsch-Jozsa, en tanto que si $f(x) = c$ es una función constante, se determina que

$$\mathcal{P}(y = 0^n) = \left| 2^{-n} \sum_x (-1)^{c} \right|^2 = |(-1)^c|^2 = 1. \tag{18}$$

Por otro lado, si $f(x)$ es una función balanceada, tal que la mitad de sus elementos serán enviados al 0 y la otra mitad al 1, se obtendrá que $\mathcal{P}(y = 0^n) = 0$, debido a que los términos de la sumatoria con respecto a x se cancelarán entre sí. La interpretación de cada uno de estos pasos algebraicos desde la computación cuántica facilita el proceso de determinar, con buena precisión, si una función f es constante o balanceada tras aplicar una vez el algoritmo de Deutsch-Jozsa: Tras inicializar n cubits en el estado $|0\cdots0\rangle$, se aplica una puerta lógica de Hadamard a cada cubit y una función *Oracle* U_f al circuito lógico para finalmente interferir los cálculos cuánticos a partir de otras n puertas de Hadamard y medir la amplitud de cada cubit. Si la medición da como resultado, con precisión $\mathcal{P}(y = 0^n) = 1$, que el estado final es $|0\cdots0\rangle$, entonces f es constante, mientras que si la probabilidad de obtener $|0\cdots0\rangle$ en el estado final es nula, f será balanceada. Si los resultados muestran probabilidades distintas a 0 y 1, se concluiría, entonces, de que f no es constante ni balanceada.

El paralelismo entre la teoría computacional y la experimentación del ejemplo previo puede investigarse a mayor profundidad por medio del **método de amplificación de amplitud**, demostrado desde la computación cuántica por el operador de Grover. El estudio de las propiedades intrínsecas y únicas de un sistema se encuentra expuesto, principalmente, por el algoritmo de Grover, el cual a su vez está construido por medio del **algoritmo de búsquedas no estructuradas**: Considere un conjunto de N elementos definido de forma tal que solo uno de sus elementos, llamado ω, tenga una propiedad única y distinguible. Para encontrar este elemento único desde la computación clásica, resulta necesario verificar, en promedio, $N/2$ de los elementos del conjunto. No obstante, la computación cuántica ha demostrado que es posible reducir el tiempo de ejecución a órdenes cercanos a $\sqrt{N}$ pasos lógicos. [11] La aceleración cuadrática en el rendimiento computacional permite obtener resultados óptimos que no dependen de la estructura intrínseca del problema, haciendo que la construcción de los algoritmos cuánticos algebraicos tenga un componente estrucutural global y, en muchos casos,

genérico. El problema de la implementación ahora recae sobre la búsqueda de la función *Oracle* adecuada para cada algoritmo.

La función *Oracle* U_ω del algoritmo de Grover considera todos los posibles estados computacionales $|x\rangle$ como una base vectorial con respecto al sistema de cubits pertinentes al problema. Esto permite codificar la información del elemento ω en un estado independiente de los demás elementos del conjunto. Luego, se define U_ω a partir de la adición de una fase negativa al estado de solución. Esto es,

$$U_\omega|x\rangle = \begin{cases} |x\rangle, & \text{si } x \neq \omega, \\ -|x\rangle, & \text{si } x = \omega. \end{cases} \tag{19}$$

Las ventajas del algoritmo de Grover se observan en tanto que se facilita la resolución de los parámetros de cada posible configuración por medio de su operador U_ω. Si bien resulta complejo encontrar una solución a un problema computacional, el algoritmo de Grover permite verificar la validez de la solución de cada problema enmarcado en la computación cuántica: Considere una función de prueba f definida sobre un conjunto de soluciones propuestas x, de forma tal que, si x no es una solución al problema ($x \neq \omega$), entonces $f(x) = 0$. De lo contrario, si la solución es válida ($x = \omega$), $f(x) = 1$. A partir de la función de prueba f, se redefine la función *Oracle* U_ω como

$$U_\omega|x\rangle = (-1)^{f(x)}|x\rangle, \tag{20}$$

de manera tal que U_ω es una matriz diagonal de la forma

$$U_\omega = \begin{bmatrix} (-1)^{f(0)} & 0 & \cdots & 0 \\ 0 & (-1)^{f(1)} & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots \\ 0 & 0 & \cdots & (-1)^{f(2^n-1)} \end{bmatrix}. \tag{21}$$

Luego, la piedra angular del algoritmo de Grover se basa en la aplicación del **método de amplificación de amplitud** sobre una superposición uniforme $|s\rangle$ con respecto a cada uno de los N elementos del conjunto caracterizados en la base estándar $|x\rangle$:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = H^{\otimes n}|0\rangle^n. \tag{22}$$

La Figura 2 muestra el caso particular de la configuración de $n = 3$ cubits para cada uno de los $N = 2^n = 8$ estados posibles de solución. Posteriormente, la función *Oracle* de reflexión U_ω es aplicada al estado $|s\rangle$ de forma tal que la amplitud del estado correspondiente a ω, representado en la Figura 3 por $\omega = |011\rangle$, tome un valor negativo. Observe que el promedio de las amplitudes del sistema de N elementos se desfasa ligeramente hacia abajo tras aplicar U_ω. En la Figura 3 se indica la nueva posición del promedio de amplitudes por medio de una línea color carmesí.

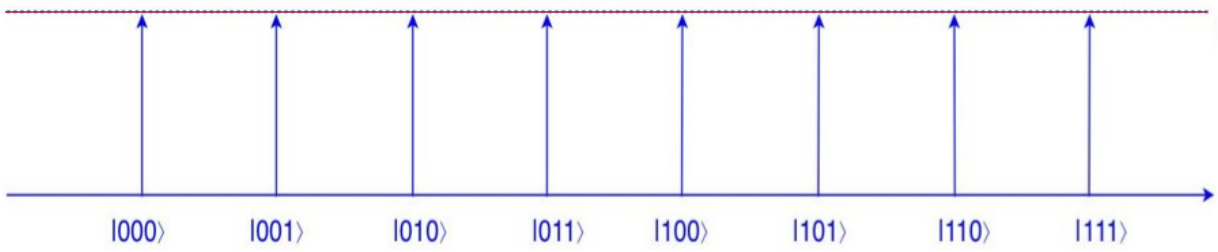

Figura 2: Diagrama de las amplitudes de cada uno de los 8 posibles estados de solución de la superposición $|s\rangle$.

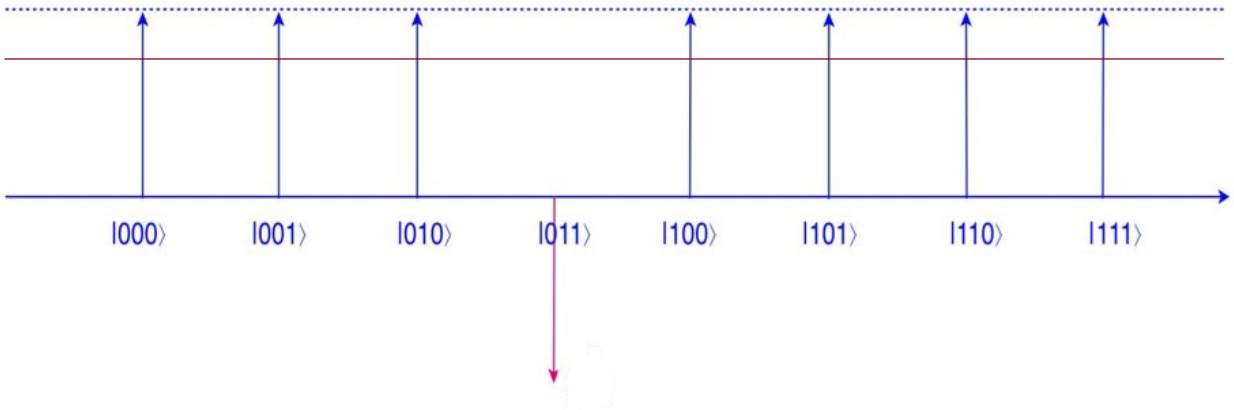

Figura 3: Diagrama de las amplitudes de cada uno de los 8 posibles estados de solución de la superposición $|s\rangle$ tras la aplicación del operador U_ω.

Para dar cuenta de la diferencia entre las amplitudes de cada estado en la medición final, es menester aplicar otro operador de reflexión U_s con respecto al estado $|s\rangle$ que determine la diferencia de amplitudes de cada estado con respecto al nuevo promedio. La transformación U_s se define como

$$U_s = 2|s\rangle\langle s| - I, \quad U_s U_\omega |s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} U_s U_\omega |x\rangle = \sum_{x=0}^{N-1} \left(2\langle s\rangle - \frac{1}{\sqrt{N}} \right) U_\omega |x\rangle, \qquad (23)$$

de forma tal que la transformación $U_s U_\omega |s\rangle$ mapea cada estado con solución incorrecta a una nueva amplitud correspondiente al nuevo promedio $\langle s\rangle$ menos un desfase debido la diferencia entre $\langle s\rangle$ y la amplitud inicial $\frac{1}{\sqrt{N}}$, mientras que la solución correcta, representada por el estado $|\omega\rangle$, toma una nueva amplitud dada por $2\langle s\rangle + \frac{1}{\sqrt{N}}$.

La Figura 4 muestra la aplicación del operador de Grover para el mismo ejemplo de $n = 3$ cubits. Aplicar varias veces el algoritmo de Grover permite acentuar más la diferencia entre amplitudes de las soluciones incorrectas y la solución correcta, haciendo que la medición de la solución correcta sea más precisa y exacta tras cada iteración.

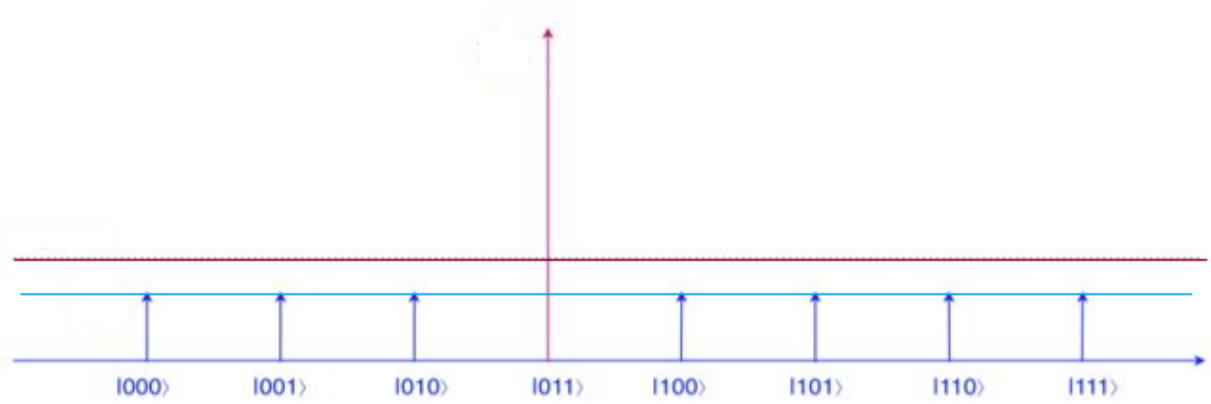

Figura 4: Diagrama de las amplitudes de cada uno de los 8 posibles estados de solución de la superposición $|s\rangle$ tras la aplicación del operador $U_s U_\omega$.

Por otro lado, el uso de la estimación de fase cuántica, basada en la transformada cuántica de Fourier, permite generar subrutinas eficientes en la computación cuántica en virtud de fenómeno de paralelismo cuántico. Las mediciones realizadas a partir de la estimación de fase cuántica son desarrollables en cualquier operador hermítico, de manera que varios observables puedan ser cuantificados dentro de un mismo algoritmo cuántico. Siguiendo los principios básicos de la transformada clásica de Fourier, en donde se transforma una señal arbitraria en el dominio temporal $f(t)$ al dominio de frecuencias $\mathcal{F}(\omega)$, o viceversa, es posible definir la transformada cuántica de Fourier (QFT) desde un dominio arbitrario j hasta un dominio arbitrario k como

$$QFT\left(\sum_j \alpha_j |j\rangle\right) = \sum_k \tilde{\alpha}_k |k\rangle\,, \quad \text{donde } \tilde{\alpha}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} \alpha_j. \tag{24}$$

De manera análoga a la transformada clásica de Fourier, QFT permite transformar una función delta a una función sinusoidal, en tanto que cada estado final estará descrito por medio de una superposición de los estados iniciales. Las aplicaciones de la transformada cuántica de Fourier resultan importantes para la construcción de algoritmos cuánticos, debido a que QFT permite redistribuir la información condensada en un qubit a una configuración que involucre todos y cada uno de los posibles estados propios. La Figura 5 visualiza un ejemplo específico en que el estado $|10\rangle$ se transforma en la superposición de estados $|00\rangle - |01\rangle + |10\rangle - |11\rangle$.

Más aún, la transformada cuántica de Fourier puede comprenderse como un operador unitario [12], de forma tal que es posible realizar un proceso iterativo para la ejecución de QFT con respecto a cada estado del dominio de entrada. Sin pérdida de generalidad, partiendo desde la expansión decimal de cada elemento j del dominio $[0, 1]$, de forma tal que se escribe $j = 0.j_1 j_2 \cdots j_n$, donde $j_i \in \{0, \cdots, 9\}$ para cada $1 \leq i \leq n$, se llega a que

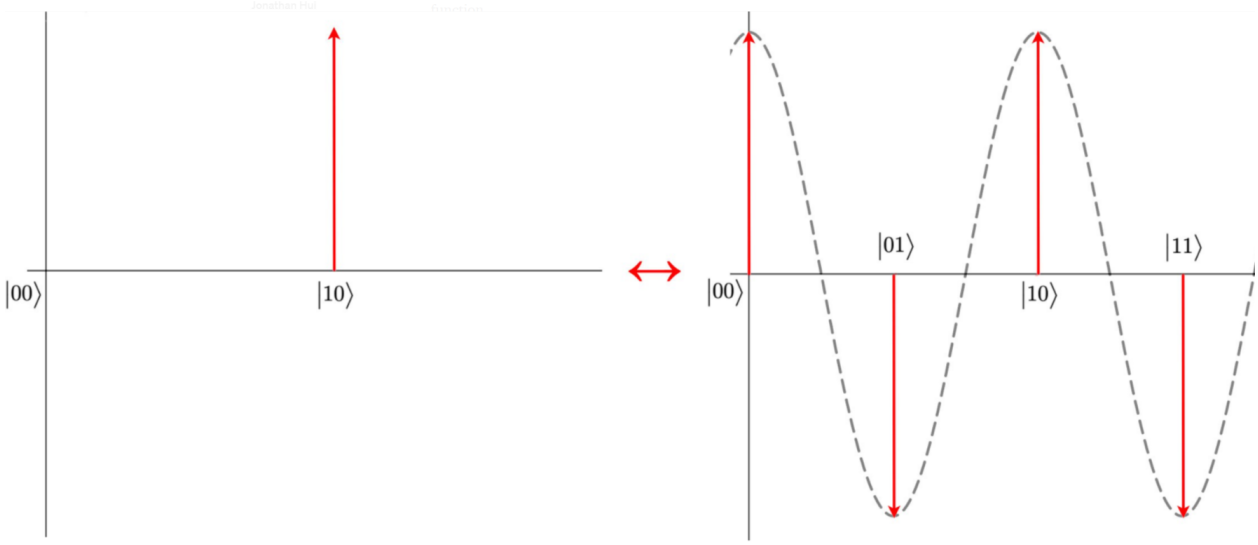

Figura 5: Diagrama expositivo de la transformación de un estado cuántico ($|10\rangle$) a una superposición de estados ($|00\rangle - |01\rangle + |10\rangle - |11\rangle$). Las transformaciones representadas permiten comprender el paso de una función delta a una función sinusoidal a partir de la transformada cuántica de Fourier.

$$QFT|j_1, \cdots, j_n\rangle = \frac{\left(|0\rangle + e^{2\pi i(0.j_n)}|1\rangle\right)\left(|0\rangle + e^{2\pi i(0.j_{n-1}j_n)}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i(0.j_1 j_2 \cdots j_n)}|1\rangle\right)}{2^{n/2}}. \tag{25}$$

Así, la información de cada elemento $j = 0.j_1 j_2 \cdots j_n$, expresada inicialmente en forma decimal, quedará codificada en forma binaria y podrá ser reconstruida según el método de estimación de fase, el cual permite determinar, hasta una precisión de t decimales, la fase $\phi = 0.\phi_1\phi_2\cdots\phi_t$ del dominio de entrada.

De esta forma, la ejecución de QFT en un algoritmo cuántico se realizará de la siguiente manera: Primeramente, tras tomar una fase de entrada ϕ, se implementa una sucesión de operadores $U^{2^{t'}}$, donde $t' \in \{0, 1, \cdots, t-1\}$, que retornen las entradas decimales de ϕ desde el t'-ésimo decimal, tal que

$$U^{2^{t'}}(\phi) = 0.\phi_{t'}\phi_{t'+1}\cdots\phi_t. \tag{26}$$

La implementación de cada operador $U^{2^{t'}}$ con respecto a un circuito cuántico de n cubits de registro se halla visualizada en la Figura 6. Luego, el método de estimación de fase preparará, en virtud de las compuertas lógicas de Hadamard, una superposición de estados del dominio j:

$$2^{-t/2}\left(|0\rangle + e^{2\pi i(0.\phi_t)}|1\rangle\right)\otimes\cdots\otimes\left(|0\rangle + e^{2\pi i(0.\phi_1\phi_2\cdots\phi_t)}|1\rangle\right) = \frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1} e^{2\pi i\phi j}|j\rangle. \tag{27}$$

Así, tras aplicar la transformada cuántica inversa de Fourier, QFT^{-1}, se obtiene la fase correspondiente a un estado propio $|u\rangle$, de forma que

$$QFT^{-1}\left(\frac{1}{\sqrt{2^t}}\sum_{j=0}^{2^t-1} e^{2\pi i\phi j}|j\rangle\right)|u\rangle = |\phi\rangle|u\rangle. \tag{28}$$

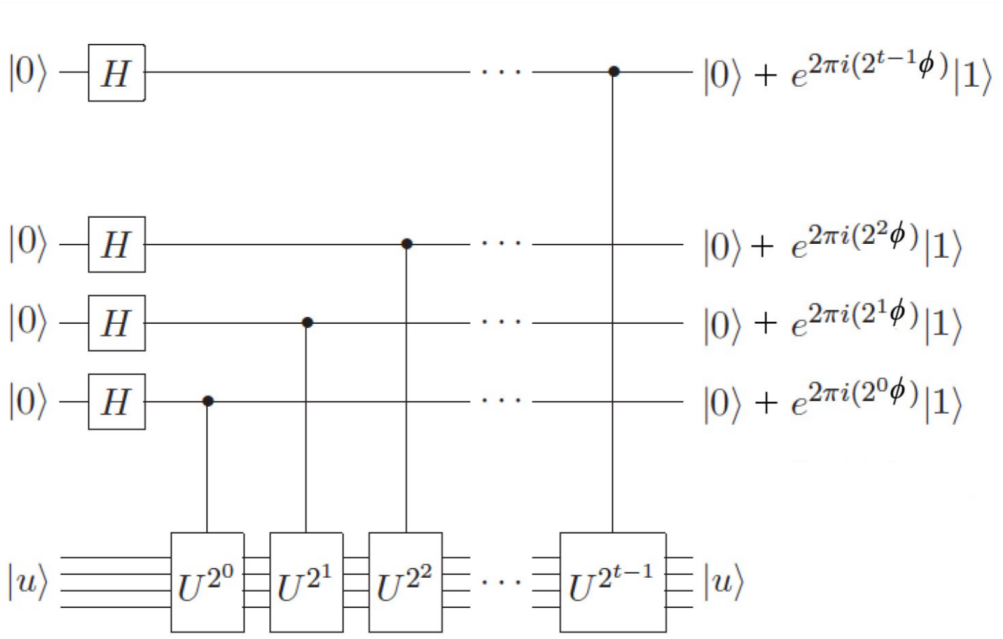

Figura 6: Representación del algoritmo cuántico del método de estimación de fase.

El desarrollo de la teoría computacional previa, a partir de la transformada cuántica de Fourier y del método de estimación de fase, establece las bases del algoritmo de Shor, el cual se fundamenta en la búsqueda del periodo r de una función modular $f(x) = a^x \bmod N$ que permita determinar los factores primos de un número natural N en virtud de un parámetro inicial a: En primer lugar, defina el operador U_a como

$$U_a|x\rangle = |ax \bmod N\rangle, \tag{29}$$

el cual tiene valores propios $e^{2\pi is/r}$, $s \in \{0, 1, \cdots, r-1\}$, y estados propios

$$|u_s\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1} e^{\frac{-2\pi isk}{r}}|a^k \bmod N\rangle. \tag{30}$$

Posteriormente, a través de los estados propios $|u_s\rangle$, se desarrolla una superposición de estados propios $|\psi_a\rangle$, tal que

$$|\psi_a\rangle = \frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = \frac{1}{r}\sum_{s=0}^{r-1}\sum_{k=0}^{r-1} e^{\frac{-2\pi iks}{r}}|a^k \bmod N\rangle = |1\rangle. \tag{31}$$

Luego, el concepto de paralelismo cuántico permitirá calcular, a través de la sucesión de compuertas lógicas $U_a^{2^{t'}}$, la superposición de todas las posibles entradas binarias $|x\rangle$ (con respecto a $|\psi_a\rangle$) como

$$|\psi\rangle = \frac{1}{\sqrt{2^t}} \sum_{x\in\{0,1\}^t} |x\rangle U_a^x |\psi_a\rangle = \frac{1}{\sqrt{2^t}} \sum_{x\in\{0,1\}^t} |x\rangle U_a^x |1\rangle = \frac{1}{\sqrt{2^t}} \sum_{x\in\{0,1\}^t} |x\rangle |f(x)\rangle. \tag{32}$$

Finalmente, tras aplicar QFT^{-1} al registro de t cubits, se obtiene la fase relacionada al valor propio de U, s/r, de forma tal que la superposición de salida del algoritmo cuántico de Shor es

$$|\tilde{\psi}\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |s/r\rangle |u_s\rangle. \tag{33}$$

Los resultados computacionales de la implementación de un algoritmo cuántico análogo al algoritmo de Shor muestran que, para una valor específico de a, en la medida que el número objetivo N se hace arbitrariamente grande, los tiempos de ejecución crecen exponencialmente en un computador clásico. A partir del software de desarrollo **Qiskit**, es posible modelar, en una unidad de procesamiento clásico, circuitos fuertemente codificados en virtud de un número finito de $3m = 3\lceil \log_2 N \rceil$ entradas lógicas, donde se usarán $2m$ cubits para el primer registro y m pseudo-cubits correspondientes a salidas clásicas para las medicones correspondientes. Tras realizar una implementación análoga al circuito cuántico de la Figura 6 para $a = 8$ y $N = 15$, se obtienen mediciones relacionadas a las amplitudes de probabilidad con respecto a cada una de las fases s en formato binario, donde inicialmente se ha tomado $r = 256$ para luego mejorar el resultado por medio del algoritmo de las fracciones continuas. La Figura 7 muestra las amplitudes encontradas:

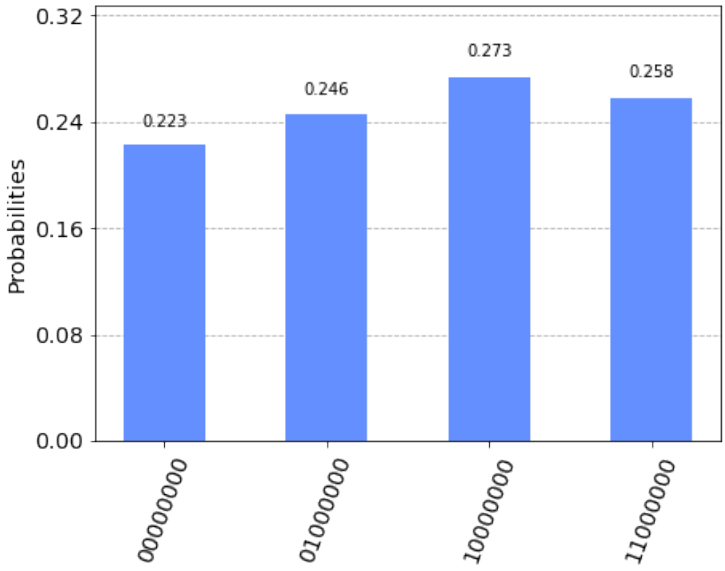

Figura 7: Amplitudes de probabilidad con respecto a los valores (en formato binario) más reiterativos en las fases del circuito cuántico con $a = 8$ y $N = 15$.

En formato decimal, se obtienen los valores de $s = 0, 64, 128$ y 192 con respecto a $r = 256$, de manera que, tras aplicar el algoritmo de las fracciones continuas, se obtiene $s/r \in \{0, 1/4, 1/2, 3/4\}$, dando como resultado el $50\,\%$ de las veces el período correcto de $r = 4$. En virtud de un computador clásico, se halla un tiempo de ejecución de 10 segundos, lo cual es aceptable considerando la facilidad para factorizar $N = 15$ en $a^{r/2} + 1 \,(\mathrm{mod}\, 15) = 65 \,(\mathrm{mod}\, 15) = 5$ y $a^{r/2} - 1 \,(\mathrm{mod}\, 15) = 63 \,(\mathrm{mod}\, 15) = 3$. No obstante, para $a = 3$ y $N = 35$, el tiempo de ejecución se incrementó considerablemente a 3 minutos, en la medida que las amplitudes de varias de las fases ya no serían nulas, sino que tendrían asociada una leve probabilidad, como se observa cualitativamente en la Figura 8:

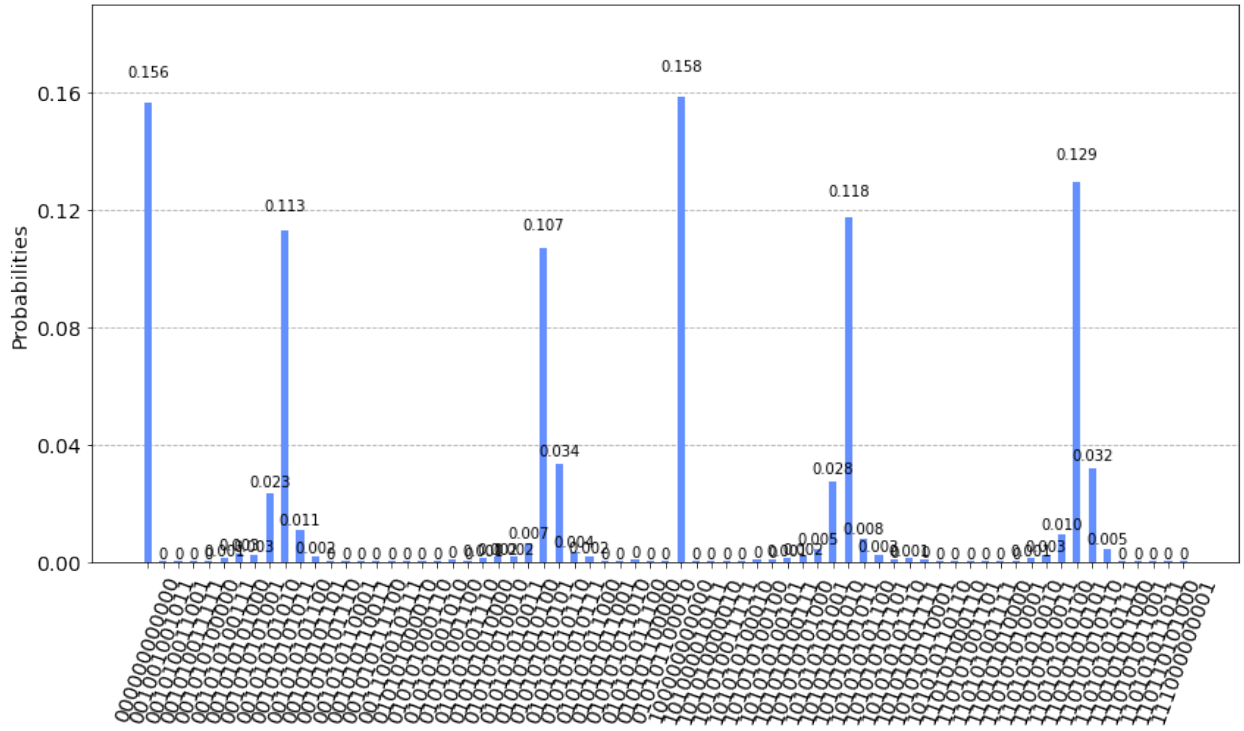

Figura 8: Amplitudes de probabilidad con respecto a los valores (en formato binario) de las fases del circuito cuántico con $a = 3$ y $N = 35$.

El algoritmo de las fracciones continuas permite deducir que, para los valores más reiterativos de las fases s/r, inicializadas por $r = 4096$, los periodos obtenidos son $r = 6$ en el $47\,\%$ de los casos y $r = 12$ en el $53\,\%$ de los casos, siendo este último el periodo correcto que permite factorizar $N = 65$ en $a^{r/2} + 1 \,(\mathrm{mod}\, 35) = 730 \,(\mathrm{mod}\, 35) = 5$ y $a^{r/2} - 1 \,(\mathrm{mod}\, 35) = 728 \,(\mathrm{mod}\, 15) = 7$. Por otro lado, se registran tiempos cercanos a 15 minutos para realizar la factorización de $N = 65$ con $a = 27$ con probabilidad de éxito del $45\,\%$, lo cual indica que el desarrollo de los algoritmos cuánticos por medio de computadores clásicos toman una sucesión de pasos lógicos que crecen exponencialmente, como se esperaba. Para determinar la validez del algoritmo cuántico desarrollado, es menester usar una unidad de procesamiento cuántico simulada que precise la diferencia de tiempos de ejecución de ambos sistemas.

Por medio de la herramienta de graficación cuántica **IBM Quantum Composer**, se realizó la construcción de algoritmo cuántico en un software predeterminado para estimar las fases

del circuito en virtud de las compuertas controladas **C-NOT** y no a partir de intercambios o *swaps* entre cubits para la distribución uniforme de la información, como se hizo en la unidad de procesamiento clásico. Sin embargo, este cambio no representa un cambio apreciable en la sucesión de pasos lógicos, sino corresponde a una alternativa en el diseño del circuito cuántico que es completamente análoga a la realizada previamente. La Figura 9 muestra el diseño gráfico del algoritmo cuántico para $a = 7$ y $N = 15$:

Figura 9: Diseño gráfico del circuito cuántico en **IBM Quantum Composer** para $a = 7$ y $N = 15$. Las compuertas controladas **C-NOT** se hallan representadas por los símbolos $\bigoplus$ y una conexión hasta el cubit de interés, mientras que la compuerta lógica **NOT** está dada por el símbolo $\oplus$ sin conexiones. Las últimas componentes hacen referencia a la medición de cada cubit.

La medición de las amplitudes de probabilidad para el simulador cuántico fueron realizadas en un tiempo cercano a 8 segundos, llegando a un resultado similar que su contraparte clásica. No obstante, la precisión de los resultados es del 100 %, en tanto que la Figura 10 muestra un único resultado posible para la fase s/r, tal que $s = 0100 = 4$ y se inicializó el algoritmo a partir de $r = 16$, lo cual permite llegar rápidamente a que el resultado del algoritmo de las fracciones continuas es, exactamente, $s/r = 1/4$, llegando así nuevamente al periodo deseado. De manera análoga, se realizaron los circuitos correspondientes a $N = 35$ y $N = 65$ para llegar a una comparación concreta entre las unidades de procesamiento clásico y cuántico. Los tiempos de ejecución y la probabilidad de éxito en ambos sistemas, con respecto al algoritmo de Shor, se presentan en el Cuadro 1.

Unidades de Procesamiento	Clásico			Cuántico		
(a, N)	$(8, 15)$	$(3, 35)$	$(27, 65)$	$(7, 15)$	$(3, 35)$	$(7, 65)$
Tiempos de ejecución (min)	0,16	3,02	15,48	0,13	1,23	2,94
Precisión de los resultados (%)	50	53	47	100	86	78

Cuadro 1: Tabla de tiempos de ejecución y probabilidad de éxito del algoritmo de Shor con respecto a un computador clásico y un simulador cuántico.

Los resultados previos permiten comprender, de manera discreta, cómo los tiempos de ejecución del simulador cuántico de IBM crecen, con respecto a las unidades de procesamiento

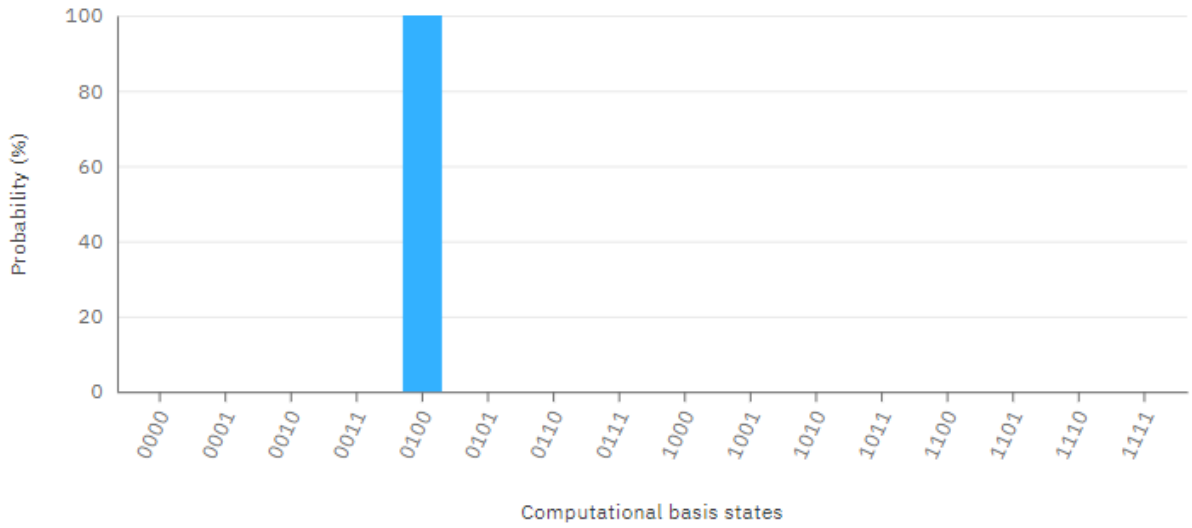

Figura 10: Amplitudes de probabilidad con respecto a los valores (en formato binario) de las fases del circuito cuántico en **IBM Quantum Composer** para $a = 7$ y $N = 15$.

clásico, a una menor razón en la medida que se aumenta N. Más aún, la precisión de los resultados es considerablemente distinta, en tanto que el paralelismo cuántico realizado en el simulador de IBM permite llegar a mediciones concretas sin la necesidad de iterar varios procesos dentro del mismo código, como sucede en el circuito clásico. El algoritmo de Shor clásico necesita realizar varios intentos para llegar a una precisión aceptable de las fases funcionales para el período r, mientras que el algoritmo de Shor cuántico permite disminuir considerablemente el número de ejecuciones, aumentando así su precisión intrínseca, sin importar el valor de N a considerar. Finalmente, para obtener un espectro continuo de valores para (a, N) que permitan determinar el crecimiento de los tiempos de ejecución en un computador clásico y cuántico, se realizó un último algoritmo basado en Shor que factoriza cualquier número N a pesar de un alto costo computacional. Estos resultados permiten inferir que la aplicación de un algoritmo cuántico en una unidad de procesamiento cuántico requiere una formidable cantidad de intentos para obtener factores precisos y sin errores, en tanto que los tiempos de procesamiento deben ser realizables. No obstante, los computadores cuánticos permiten realizar estos cálculos con mayor facilidad, de manera que el análisis de la gran cantidad de datos que conlleva un algoritmo cuántico no debe estar caracterizado solo por sus propiedades y usos, sino también por medio del sistema en el cual se ejecutan cada una de las operaciones.

7. Conclusiones

Los algoritmos cuánticos tienen una gran gama de aplicaciones físicas, que parten desde sencillos problemas téoricos hasta varios fundamentos experimentales propios de la mecánica cuántica. En particular, con respecto a la resolución de problemas algebraicos, el estudio de los algoritmos de Deustch-Josza, Grover y Shor permiten determinar que por medio de una superposición uniforme de estados cuánticos, la aplicación de compuertas lógicas y la ejecución de varios pasos lógicos en virtud del paralelismo cuántico, el esquema y el diseño general de cualquier circuito cuántico es realizable dentro de parámetros coherentes.

Se observa esencialmente que el método de amplificación de amplitud, el algoritmo de búsquedas no estructuradas, la transformada cuántica de Fourier y el método de estimación de fase son las aplicaciones más relevantes que permiten un reducción considerable a los tiempos de ejecución de un sistema cuántico. Como ejemplo meritorio, el algoritmo de Shor emplea cada una de las técnicas previas para solucionar un problema con aplicaciones numéricas, polinomiales y probailísitiscas, tal que su desarrollo permite un punto de compración entre los tiempos de ejecución y la precisión de los resultados. Se logra desarrollar por medio de la función *Oracle* $U_a|x\rangle = |ax \bmod x\rangle$ varios circuitos que permitan determinar el periodo relacionado a distintos valores de N con respecto a determinadas amplitudes de probabilidad. Para $N = 15$, $N = 35$ y $N = 65$, se observa un crecimiento razonable en la incertidumbre de las fases, tal que la existencia de cierto ruido en la aplicación del algoritmo dentro del computador clásico es evidente. Sin embargo, a partir de una razonable cantidad de intentos de ejecución, el algoritmo desarrollado llega a una precisión cercana a 0,5, lo cual indica que a pesar del aumento progresivo de errores computacionales dentro de las operaciones del algoritmo, para cada N analizado se tiene un desarrollo prácticamente constante y coherente con las dificultades de la programación de un circuito cuántico en un computador clásico.

Obtener una precisión significativa a partir de una unidad de procesamiento clásico implica, a pesar de largos de tiempos de ejecución, que el algoritmo cuántico podrá modificarse dentro de un simulador cuántico para visualizar un mejor funcionamiento de cada una de sus propiedades intrínsecas. La comparación entre ambos sistema de cómputo muestra no solo que los tiempos de ejecución crecen a una razón más baja para un computador cuántico, sino que su probabilidad de éxito se incrementa hasta obtener factores correctos de cada número N en la mayoría de intentos. Finalmente, en virtud de un último algoritmo desarrollado, se llega a que la solución de problemas algebraicos relacionados a la factorización de números enteros es aplicable en buena medida dentro de un computador clásico, pero que el poder de cómputo de los circuitos cuánticos, incluso en un simulador, permite evaluar claramente varios fenómenos de la mecánica cuántica desde algoritmos y operaciones sencillas.

Agradecimientos

En primer lugar, se realizan agradecimientos especiales al profesor Alejandro García de la Universidad de los Andes por la asesoría brindada en la realización de este proyecto teórico/computacional. Los temas enseñados por el profesor Alejandro componen gran parte del contenido presentado en este documento. De manera análoga, se reconoce el apoyo y la guía dada por el profesor asesor Gabriel Téllez, en tanto que los comentarios hechos en los seminarios de Física Estadísitica fueron valiosos con respecto a los resultados de los algoritmos cuánticos algebraicos desarrollados.

Referencias

[1] A. Montanaro. Quantum algorithms: an overview. *Quantum Information*, 2(1), Jan 2016.

[2] Y. Wu et al. Strong quantum computational advantage using a superconducting quantum processor. *Physical review letters*, 127(18):180501, 2021.

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

[4] R. Jozsa. Quantum factoring, discrete logarithms, and the hidden subgroup problem. *Computing in Science Engineering*, 3:34 – 43, 04 2001.

[5] H. Huang et al. Superconducting quantum computing: A review. *Science China Information Sciences*, 63(5):1–32, 2020.

[6] Ray LaPierre. *DiVincenzo Criteria*, pages 241–244. Springer International Publishing, Cham, 2021.

[7] A. Adedoyin et al. Quantum algorithm implementations for beginners. *arXiv*, 2020.

[8] J. Van Gael. The role of interference and entanglement in quantum computing. *Semantic Scholar*, 2005.

[9] L.K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA, 1996. Association for Computing Machinery.

[10] P.W. Shor. Why haven't more quantum algorithms been found? *J. ACM*, 50(1):87–90, January 2003.

[11] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, Oct 1997.

[12] Todd A. Brun. Hiding quantum information in the perfect code. *arXiv*, 2011.

Bibliografía Anotada

• P. W. Shor, Algorithms for quantum computation: discrete logarithms and factoring.

Se muestran las mejoras de la computación cuántica con respecto a dispositivos computacionales físicos, en tanto que los tiempos clásicos de computación resultan ser más largos, debido a un factor polinomial. La exposición de la superposición de los estados cuánticos dentro de un computador cuántico es sencilla de comprender y da a entender una relación importante de las máquinas de Turing cuánticas y la construcción de clases de complejidad uniforme.

Compara otros algoritmos desarrollados, como el algoritmo de Schönhage–Strassen, y las ventajas y desventajas que encuentra con respecto al algoritmo desarrollado por Shor. Esto me permite entender a mayor profundidad las características primordiales para minimizar el tiempo de computación del algoritmo. El apartado de las transformadas cuánticas de Fourier resulta interesante y expone mayores aplicaciones que solo la factorización de números enteros.

• Eric R. Johnston, Nic Harrigan, Mercedes Gimeno-Segovia, Programming Quantum Computers, OReilly media Inc.

El texto es largo, pero tiene apartados interesantes que permiten que el lector se guie cómodamente. Muestra algoritmos computacionales esenciales, y las facilidades y dificultades que el programador puede encontrar para su desarrollo. A pesar de que el texto se enfoca primordialmente en la construcción de computadores cuánticos, el texto desarrolla intuitivamente algoritmos relacionados a la amplificación de la amplitud de un sistema y la correspondiente estimación de fase.

Este texto desarrolla los temas demostrados en el artículo de P.W. Shor sobre computación cuántica para la factorización y le enseña al lector las posibles aplicaciones del algoritmo de Shor, en concordancia con las limitaciones en la simulación y en el hardware. Expone, además, usos del machine learning como apoyo para el análisis cuántico de sistemas de ecuaciones lineales y expresiones algebraicas más complejas.

• A. Montanaro. Quantum algorithms: an overview. Quantum Information.

El artículo desarrolla de manera resumida definiciones de conceptos necesarios para interpretar y desarrollar la información de los algoritmos cuánticos. Expone ejemplos propios del área de álgebra abstracta y del álgebra lineal, por lo que se hacen explicaciones constructivas sobre las aplicaciones algebraicas que tienen los algoritmos cuánticos diseñados en la última década.

Los conceptos de búsqueda y optimización son sencillos de entender dentro del contexto del algoritmo de Grover y del método de amplificación de amplitud. Presenta simulaciones cuánticas a partir de grafos, lo cual se aleja del alcance de este proyecto pero resulta interesante para fomentar ideas de aplicaciones que tengan una mayor complejidad algebraica. El apartado de caminatas cuánticas se compacta con varios conceptos de física estadística, lo que permite la exploración de otra idea futura en el desarrollo de este proyecto. La crítica que usa sobre la construcción de algoritmos cuánticos por medio de aproximaciones primitivas resulta valiosa para reflexionar sobre el impacto de la computación cuántica.

• R. Jozsa. Quantum factoring, discrete logarithms, and the hidden subgroup problem. Computing in Science Engineering.

La introducción del concepto de periodicidad permite comprender las motivaciones detrás del uso recursivo de algoritmos cuánticos y las similitudes que tienen cada uno de estos. Los cálculos de mediciones aleatoriamente uniformes que presenta son sencillos y útiles para este proyecto de investigación. La factorización cuántica y la evaluación de logaritmos discretos a partir de funciones modulares establecen gran parte de la base matemática que sustenta la parte computacional del proyecto. No obstante, en algunos apartados se destaca varias veces el problema del subgrupo abeliano oculto, el cual no resulta pertinente para el desarrollo teórico de este informe.

• A. Adedoyin et al. Quantum algorithm implementations for beginners, 2020.

El texto es largo pero presenta capítulos útiles para establecer de manera concisa aplicaciones sencillas de los algoritmos cuánticos. El lenguaje usado no es muy técnico, por lo que la lectura es rápida y concreta para cada uno de los temas presentados. No obstante, al no profundizar en varios aspectos teóricos, la información presentada es algunas veces inconclusa o sin un propósito evidente. El objetivo de este texto es el de presentar un aperitivo téorico de aspectos propios de la mecánica cuántica que son en realidad mucho más complejos.

• J. Van Gael. The role of interference and entanglement in quantum computing. 2005.

La perspectiva histórica de este documento contextualiza de buena manera los propósitos científicos que yacen detrás de la computación cuántica, a la vez que se argumentan las diferencias en la creación de modelos computacionales clásicos y cuánticos. Se proponen 3 conceptos esenciales que organizan el proceso lógico detrás de cada algoritmo cuántico: La interferencia, el entrelazamiento y la superposición de estados cuánticos paralelos. Estos conceptos permiten desarollar uno de los objetivos específicos de este proyecto, por lo que su información es de carácter esencial.

La estructura del texto es refinada, por lo que resulta como una guía válida para la composición de este informe. El texto, en general, tiene todos los conceptos teóricos pertinentes para este proyecto pero carece de implementación computacional.

• L.K. Grover. A fast quantum mechanical algorithm for database search. 1996.

El artículo es corto y concreto, de manera que los resultados y las explicaciones concisas conforman gran parte del texto. Muestra pasos lógicos y demostraciones necesarias para los fundamentos teóricos del estado del arte, pero también tiene apartados en los cuales se realiza una abstracción de los problemas algebraicos, lo que permite que su aplicabilidad sea más sencilla de comprender. Las observaciones finales realizadas permiten entender el componente global y genérico que tiene el algoritmo de Grover.

• P.W. Shor. Why haven't more quantum algorithms been found? J. ACM, 50(1):87–90, January 2003.

El texto no es precisamente académico, sino más bien reflexivo, en el cual se cuestiona sobre las dificultades de generar algoritmos cuánticos novedosos a pesar de su aplicabilidad. Las respuestas que se dan se relacionan fuertemente con las técnicas de desarrollo y la intuición de los científicos contemporáneos con respecto a los procesos de computación, lo cual indica que es necesario desligarse de la computación clásica en buena medida para comprender la computación cuántica como un ente aparte. El texto provee un contexto importante sobre los propósitos de los algoritmos cuánticos.

• Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. Oct 1997.

El concepto de complejidad computacional se desarrolla a lo largo del texto y construye el eje central de las virtudes de los algoritmos cuánticos. Se compara la relevancia entre varias funciones *Oracle* y se enfatiza en las diferencias sustanciales de cada algoritmo con respecto a la base computacional usada.

Se explican también las dificultades no deterministas de la computación cuántica y proponen el método de errores acotados como una nueva subrutina de los algoritmos cuánticos. El texto es innovador, ya que muchas de las ideas explicadas amplían el espectro de posibilidades y oportunidades de los computadores cuánticos.

• Todd A. Brun. Hiding quantum information in the perfect code, 2011.

Se presentan protocolos cuánticos detrás de la creación de un código ideal que permite ocultar información entre dos sistemas arbitrarios, además de demostraciones relacionadas a operadores unitarios. El escrito abarca temas muy avanzados, pero se encuentran contextualizados dentro de los objetivos computacionales de este proyecto.

• Y. Wu et al. Strong quantum computational advantage using a superconducting quantum processor, 2021.

El texto muestra aplicaciones experimentales de la computación cuántica a partir de materiales superconductores y procesadores. A pesar de que su propósito no esté relacionado con el de este proyecto, se muestran aspectos computacionales que demuestran las diferencias, en la velocidad de cómputo, entre las unidades de procesamiento clásicas y cuánticas.

La estimación del costo computacional que realizan en uno de sus apartados resulta interesante para establecer medidas experimentales de los tiempos de ejecución de los algoritmos cuánticos.

• H. Huang et al. Superconducting quantum computing: A review, 2020.

El texto en cuestión explora la computación cuántica desde un ámbito experimental y muestra la construcción de distintos tipos de cubits aplicables a sistema físicos computacionales. Los apartados sobre amplificadores para la lectura y retroalimentación de cubits resulta interesante para comprender la scorreciones cuánticas que se deben realizar sobre el código y el circuito cuántico.

• Ray LaPierre. DiVincenzo Criteria, 2021.

El apartado del texto *Introduction to Quantum Computing* de Ray LaPierre determina no solo los postulados de la computación cuántica a paritr de los criterios de DiVincenzo, sino que también explora las aplicaciones de estos criterios en experimentos computacionales, relacionados a la medición de cubits, de manera sencilla y didactica. La lectura del capítulo en cuestión permite comprender rápidamente los fundamentos introductorios de la mecánica cuántica por medio de algoritmos computacionales realizables en tiempos de procesamiento relativamente cortos, por lo que su información resulta valiosa para la construcción de circuitos cuánticos.