No. 173 Octubre - Diciembre DOI: 10.29236/sistemas ISSN 0120-5919

SISTEMAS

Tecnologías cuánticas

Nuevos desafíos, nuevos escenarios

ACIS
ASOCIACIÓN COLOMBIANA DE INGENIEROS DE SISTEMAS
Calle 93 No. 13 - 32 of. 102
Bogotá, D.C.
www.acis.org.co

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

ARQUITECTURA DE SOFTWARE

Curso virtual

Fechas
Febrero 2025

3, 4, 5, 6 y
10, 11, 12, 13

Hora:
4:00 a 7:00 pm

Dalia Trujillo Penagos

Guillermo Posse

mas información en :
www.acis.org.co
suscripciones@acis.org.co
3015530540

En esta edición

Publicación de la Asociación Colombiana de Ingenieros de Sistemas (ACIS)
Resolución No. 003983 del Ministerio de Gobierno
Tarifa Postal Reducida Servicios Postales Nacional S.A. No. 2015-186 4-72
ISSN 0120-5919
Apartado Aéreo No. 94334
Bogotá D.C., Colombia

Octubre - Diciembre 2024
Calle 93 No.13 - 32 Of. 102
Teléfonos 616 1407 - 616 1409
A.A. 94334
Bogotá D.C.
www.acis.org.co

ACIS

ASOCIACIÓN COLOMBIANA DE INFORMÁTICA, SISTEMAS Y TECNOLOGÍAS AFINES

JORNADA INTERNACIONAL DE SEGURIDAD INFORMÁTICA

"Retando las certezas para anticipar y adaptar el futuro"

Julio 30 y 31 de 2025

Computación Cuántica: Mitos y realidades

DOI: 10.29236/sistemas.n173a1

Juan G. Lalinde Pulido

Daniel Sierra Sosa

La computación cuántica ha trascendido los límites del laboratorio para convertirse en un tema central en la tecnología, la economía y la sociedad. En palabras de Isaac Chuang, profesor del MIT que trabajó con IBM en el desarrollo de los primeros computadores cuánticos, “Lo que está impulsando el entusiasmo es la verificación de que la computación cuántica es real. Ya no es el sueño de los físicos, sino la pesadilla de los ingenieros” [1].

El desarrollo de la computación cuántica ha sido un camino largo que comienza hace 100 años con la formulación de la mecánica cuánti-

ca. En 1965 Richard Feynman recibe el Premio Nobel de Física por su trabajo en electrodinámica cuántica y su relación con el espacio-tiempo [2]. En 1980, en la introducción de su libro *Computable and Uncomputable*, Manin propuso la idea de un autómata cuántico que utilizara superposición y entrelazamiento [3]. En 1981, en la conferencia *Physics of Computation* organizada por el MIT e IBM, Feynman afirmó: *'Nature is quantum, goddamn it! So if we want to simulate it, we need a quantum computer.*[1]*'* [1] [3], apoyando la idea de Manin.

A partir de estas propuestas surgen varias líneas de investigación. En 1984 se propone BB84 [4], un esquema cuántico para la distribución segura de claves criptográficas haciendo uso de propiedades cuánticas para garantizar la seguridad criptográfica, tema que luego sería desarrollado por Ekert [5]. En 1985, Deutsch demuestra que la computación cuántica es universal y equivalente a la máquina de Turing [6]. Su principal ventaja es el paralelismo masivo. Adicionalmente, en 1991, Landauer[7] muestra la relación estrecha y profunda entre la información y la física, lo que conduce a que sea natural tratar de utilizar cualquier teoría física, y especialmente la mecánica cuántica, para procesar información.

Finalmente, en los 90s se publican los dos algoritmos que mostraron la aplicabilidad de la computación cuántica y motivaron el desarrollo de los computadores cuánticos. En 1994 Peter Shor propone un algoritmo cuántico que factoriza un número en tiempo polinomial [7], que puede ser considerado el factor crítico que disparó el desarrollo de la computación cuántica por sus implicaciones para los sistemas criptográficos basados en la dificultad de la factorización y del cálculo del logaritmo discreto. En 1996, Grover publica su algoritmo que implica una aceleración cuadrática en la búsqueda de información en una colección de datos no organizados [8].

El desarrollo acelerado que tiene la computación cuántica nos ha llevado en tan solo 26 años de una primera implementación de un qubit controlable, lograda en [9], hasta los computadores cuánticos universales basados en compuertas de IBM con 1.121 qubits [10] o los computadores cuánticos especializados en *quantum annealing* de D-Wave con 5.000 qubits [11].

Ahora bien, ¿cuál es la importancia real de la computación cuántica en el mundo actual? El BID, en su informe [12], dice que *"Si bien es imposible saber con certeza cuál será su impacto social y tecnológico, se espera que haya un antes y un después de la adopción de esta nueva generación de tecnologías, tal y como ocurrió con las tecnolo-*

[1] La naturaleza es cuántica, ¡maldita sea! Así que si queremos simularla, necesitamos un ordenador cuántico.

gías digitales". Por su parte, McKinsey & Company presenta en 2021 un informe sobre el ecosistema de computación cuántica [13] en el cual dice que los lideres de la industria deben comenzar a formular estrategias para la adopción de manera que puedan aprovechar las capacidades de la computación cuántica comercial. El Foro Económico Mundial, en su reporte [14], reconoce que las economías más importantes del mundo consideran la computación cuántica como una tecnología estratégica porque su potencial económico y su impacto en la economía digital las hacen estratégicas desde el punto de vista geopolítico.

Dados los avances tecnológicos de los últimos años y la importancia estratégica de la computación cuántica, es necesario que el país se prepare para poder incorporar esta tecnología a su economía. En este contexto, esta edición de la revista SISTEMAS de ACIS dedicada a la computación cuántica es una invitación a asumir el reto de la computación cuántica rigurosamente, pero sin temores. No se debe olvidar que la definición más simple de algoritmo, colección finita de pasos no ambiguos que en un tiempo finito producen un resultado, no depende de ninguna tecnología particular.

La computación cuántica es una tecnología que va a cambiar el mundo tal como lo conocemos. Este número busca ayudar a los interesados en participar activamente en este viaje hacia el futuro a comprender esta tecnología.

Referencias

1 W. Knight, «MIT Technology Review,» 21 Febrero 2018. [En línea]. Available: https://www.technologyreview.com/2018/02/21/145300/serious-quantum-computers-are-finally-here-what-are-we-going-to-do-with-them/. [Último acceso: 3 Diciembre 2024].

2 R. P. Feynman, «Richard P. Feynman Nobel Lecture: The Development of the Space-Time View of Quantum Electrodynamics,» 11 Diciembre 1965. [En línea]. Available: https://www.nobelprize.org/prizes/physics/1965/feynman/lecture/. [Último acceso: 3 Diciembre 2024].

3 «40 years of quantum computing,» *Nature Reviews Physics,* vol. 4, p. 1–1, 2022.

4 G. &. B. C. H. Brassard, «Quantum cryptography: Public key distribution and coin tossing,» de *International conference on computers, systems and signal processing*, Bangalore, 1984.

5 A. K. Ekert, «Quantum cryptography based on Bell's theorem,» *Physical review letters*, vol. 67, nº 6, p. 661, 1991.

6 D. Deutsch, «Quantum theory, the Church–Turing principle and the universal quantum computer,» *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 400, nº 1818, pp. 97-117, 1985.

7 P. W. Shor, «Algorithms for quantum computation: discrete logarithms and factoring,» de *Proceedings 35th annual symposium on foundations of computer science*, Santa Fe, 1994.

8 L. K. Grover, «A fast quantum mechanical algorithm for database search.,» de *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, Philadelphia, 1996.

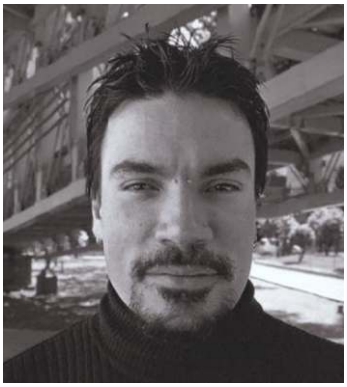
9 I. L. Chuang, N. Gershendfeld y M. Kubinec, «Experimental Implementation of Fast Quantum Searching,» *Physical Review Letters*, vol. 80, nº 15, pp. 3408-3411, 1998.

10 J. Gambetta, «IBM Quantum System Two: The era of quantum utility is here,» 4 12 2023. [En línea]. Available: https://www.ibm.com/quantum/blog/quantum-roadmap-2033. [Último acceso: 3 12 2024].

11 D-Wave Quantum Inc., «The advantage quantum computer,» 2023. [En línea]. Available: https://www.dwavesys.com/solutions-and-products/systems/. [Último acceso: 3 12 2024].

De vuelta a la moda cuántica

DOI: 10.29236/sistemas.n173a2



Las modas vienen y van y muchas veces se repiten. Estamos ahora en la segunda o tercera ola de la "cuántica" tomándose el "main stream" pero esta vez viene con descubrimientos concretos y la posibilidad de afectar nuestro día a día.

Jaime Enrique Gómez Hernández

Un día cualquiera después de una cita odontológica, la doctora, una gran amiga mía, me pidió que le explicara brevemente mecánica cuántica. Vaya mi sorpresa. Para nada dudé de la inteligencia de mi amiga, ni de su capacidad para entender, ni que yo no pudiera explicar los principios cuánticos de forma sencilla, pero con lo que no pude fue con la curiosidad de saber de dónde se había originado la pregunta tan particular.

Sucede que al igual que muchos términos científicos, la denominación de "cuántica" está siendo usada por una corriente de "nueva era" para tratar de validar, darle visos de seriedad o de fundamento formal de sus creencias. Entonces se encuentra uno con términos tan diversos como homeopatía cuántica, coaching cuántico, mente cuántica, sanación cuántica por entrelazamiento de mentes (análogo del entrelazamiento cuántico), en fin, toda una selva de términos. Y sorpresivamente no es una cuestión nueva. Esta manipulación perversa de términos es tan vieja como el habla y es parte de la evolución de las len-

guas humanas, tenga fundamento o no, nos guste o no.

Por ejemplo, hoy en día vivimos el boom de la inteligencia artificial, así esta exista en el mundo de la ciencia ficción hace varias décadas (o quizá más de un siglo): Vicky (I Robot), SkyNet (Terminator), HAL (Odisea 2001), nombres que vienen a mi cabeza. Este tema me parece divertidísimo, sobre todo siendo un lector apasionado por Asimov y ahora que veo todas las sociedades, entidades políticas, gobiernos, EU, ONU, USA, en pánico tratando de regular el uso de las IA y, pero nadie menciona a Asimov, quizá por ser considerado una sobre-simplificación de la ética para IAs, pero sus 3 leyes fundamentales de la robótica serían un muy buen comienzo para una discusión. A propósito, y como nota al margen, el pasado 29 de agosto de 2024 SkyNet tomó conciencia en el universo de Terminator. Lastimosamente, como la gran mayoría de nuestra tecnología es ideada por militares buscando una forma más rápida y eficiente de matarnos entre nosotros, no vamos a hacer nada hasta que lo logremos (Recuerden las bombas H que aun parece que no aprendemos).

Volvamos a los términos populares que nos rondan todo el tiempo, algunos con más resistencia que otros y nuestras disciplinas suelen ser muy propensas a esto por ser consideradas "modernas". Existen muchos en todos los campos del conocimiento humano como "Cloud", "híbrido", "bipolar", "pandemia", "fintech" y yendo más atrás "compacto", "relatividad", "atracción", "coaching", "coworking". etc. Y al volverse términos de moda, estos comienzan a ser utilizados de manera indiscriminada solo por el hecho de sonar elegantes y estar en la vanguardia del conocimiento. Nada más recordar los escalofríos que siento cada vez que escucho a algún servidor público al que le van a "aperturar" una investigación.

Hoy estamos empezando a vivir quizá la segunda o tercera ola del término "cuántico", por varios eventos particulares que están ocurriendo en nuestra época y a pesar de la desconfianza que nos generan los términos de moda, que son usados de manera indiscriminada, esta vez anuncia un cambio de nuestro día a día. El primer evento son los experimentos exitosos del acoplamiento cuántico, cada vez a mayor distancia.

Este fenómeno dicta que dos partículas que pertenecen a un mismo sistema, mantendrán esa relación no importa la distancia entre ellas. En otras palabras, si una cantidad constante que se conserva como el momentum angular o la energía (en mecánica clásica) o los estados en mecánica cuántica, cuando parte del sistema es afectada una de las partículas, la otra reacciona para balancear y conservar los valores /estados. Aun cuando este fenómeno no tiene equivalente en mecánica clásica podemos usar un

ejemplo que todos hemos visto (los experimentos mentales de Einstein): Tomemos el patinador girando que recoge sus brazos y aumenta su velocidad por la conservación de momentum angular del sistema. Ahora separen al patinador y dejen sus patines en el camerino, y observen cómo los patines giran más rápido cuando el patinador cierra sus brazos en el hielo. Así de bizarro es el entrelazamiento cuántico, que no solo es instantáneo, sino que no importa la distancia.

Lo más interesante ocurre cuando empiezo a ver las implicaciones: Yo separo estas partículas relacionadas kilómetros y generó una reacción a distancia implica que estoy, teóricamente, llevando información a velocidades mayores a la velocidad de la luz (1). Sí, tal como se oye y esto es fascinante porque rompe, teóricamente, una camisa de fuerza que nos incomoda a todos: la famosa C que Einstein nos dió en e=mC^2. El mismo Einstein consideraba este fenómeno "espeluznante". Inclusive muchos han llegado a especular que este fenómeno tan particular nos abre la puerta a la teletransportación de la materia, quizá aún demasiada ciencia ficción y en este momento estamos lejos de hacer realidad alguna de estas posibilidades, pero Verne y Wells nos llamarían la atención por incrédulos (3).

El siguiente fenómeno y muy relacionado con el anterior es la expectativa de las redes cuánticas: Como al entrelazar dos partículas y al hacerlas cambiar de estado, estoy transmitiendo información, es natural pensar en mensajes más complejos utilizando la misma tecnología. En 2020 un grupo de investigación china publica en Nature (2) que transmitió un mensaje cifrado a 1200 Km de distancia usando fenómenos cuánticos de entrelazamiento (en 2023 ya se replicó con 3400Km). Además de abrir el camino a las redes cuánticas también es no interceptable. Tratemos de imaginar como intercepta una comunicación de este tipo, no hay cable para cortar ni señal que escuchar. Desconocemos el "medio". Claro está, como todo el conocimiento científico es temporal y pueden ser revaluado, re-escrito, disputado y posiblemente reemplazado; quizá llegue el día que entendamos el entramado del universo del entrelazamiento cuántico y descubramos las partículas que lo transmiten, y solo hasta entonces podamos interceptarlas.

Las redes cuánticas me llevan a soñar con el Ansible de los Fórmicos (originalmente considerada telepatía) en la Saga de Ender de Orson Scott Card que inicia con el "Juego de Ender". En esta serie se habla de unas comunicaciones que llevan mensajes más allá de la velocidad de la luz, a pesar que los viajes espaciales aún siguen siendo relativistas (exactamente la situación que tendríamos algún día) y entonces plantea la proliferación de conocimiento, libros, leyendas y re-

ligiones, más allá de las personas. Como cualquier red social galáctica.

No quiero dejar de mencionar la "detección" cuántica, que no es más que la implementación del scanner de Star Trek donde podían detectar lo que desearan a casi cualquier distancia. La Marina de UK ha probado una tecnología que suena similar a la creación de Rodenberry, pero aún no tenemos mucha información detallada ya que es una publicación militar (7).

Y por último estos fenómenos nos traen a la computación cuántica con todas sus promesas y realidades, algunas sorprendentes y otras decepcionantes. Esta tecnología es considerada el siguiente gran hito en la escala de procesamiento de datos: la escala de crecimiento de la capacidad deja de ser aritmética para ser exponencial. Por lo tanto, el flujo de dinero $$ es inmensa en muchos países concentrando en USA y China, pero sin dejar atrás a Australia, Alemania, Francia, India, Reino Unido, Rusia, Canadá, Japón y Corea del Sur que invierten en su desarrollo

Las realidades hasta el momento son:

- Ya superamos el umbral de la supremacía cuántica: Ya puedo hacer cosas más rápidas con computadoras cuánticas que con tradicionales. En 2019 Google e IBM declararon haberlo conseguido resolviendo un problema en 3:20 minutos que en un supercomputador clásico de 200 petaflops pudiera haberle tomado 10.000 años (4).

- Se están usando para resolver problemas prácticos como la simulación de la hemocianina (5) en una investigación de vacunas contra el cáncer

- Nos despediremos de nuestro querido ciframiento: Un equipo de investigadores de la Universidad de Shanghái (China) anunció que había vulnerado con éxito el cifrado militar. Fue rápidamente desmentido pero la alarma ha sonado: hay equipos trabajando en esto tanto en la vulneración como en la construcción del universo de cifrado cuántico (8).

Lo que no es tan chévere

- Temperatura: Desde el punto de vista de la mecánica estadística, la temperatura no es más que el promedio de velocidad de las partículas. Entonces la temperatura es el peor enemigo ya que introduce variabilidad en los resultados y aumenta la producción de errores. Los computadores cuánticos suelen operar a temperaturas cercanas al cero absoluto lo que introduce costos bastante altos en energía e infraestructura para poder conseguir la temperatura de operación. Es exactamente el mismo problema

de llevar la superconductividad al mundo real: la conocemos hace décadas, pero aún no tengo un tren maglev de superconductores.

- La decoherencia cuántica. Los sistemas cuánticos son extremadamente temperamentales, y mantienen sus estados por períodos cortos de tiempo dependiendo de una infinidad de factores. Esto nos lleva a que "repentinamente" un par de partículas entrelazadas pueden "desconectarse" y olvidar a su compañera, lo que produce el fenómeno de decoherencia cuántica y, por lo tanto, errores en mis cálculos.

- Hijo del anterior, viene la Corrección de Errores: Técnicamente aislar un sistema a nivel cuántico es cercano a imposible y si a esto le agregamos un poco de temperatura, la cuestión se vuelve un sancocho. En computación cuántica esto implica tener un sistema de corrección de errores. Pero no nos engañemos, no lo podemos heredar de ningún protocolo de comunicación, esto es cuántico, lo que implica nuevas tecnologías que aún están en pruebas y desarrollo.

- Tengo que hacer todo de cero: Los cubits no son bits, lo que implica que nada es re-utilizable, ni el álgebra booleana, ni las compuertas, ni los transistores, ni las memorias, ni los algoritmos, ni NADA parecido. Muy parecido a lo que ocurrió en los principios de la mecánica cuántica que fue necesario inventar una notación de bra-kets o formalidad de Dirac. O sea, toca volver a aprender.

Estos problemas eventualmente serán resueltos o al menos mitigados y nos dejarán un mundo completamente nuevo. Esta situación me hace recordar al emérito profesor José Rafael Toro de Uniandes cuando la Universidad decidió adquirir un mini supercomputador Cray J-90 en los años 90s, Y muy preocupado nos decía ... "*¿En que nos metimos? ... Ahora no es el momento de hacer lo mismo más rápido, llegó el momento de cambiar de problemas*…". Lo mismo ocurre con la computación cuántica, una vez esto se normalice iniciaremos a confrontar problemas más complejos de los que hemos venido enfrentando hasta ahora partiendo de nuevos algoritmos hasta nuevas matemáticas. Por ejemplo, la referencia (1) es uno de los casos de sistemas supremamente complejos que harían muy buen uso de la nueva capacidad: usar computadores cuánticos para resolver sistemas cuánticos. Divertido y natural.

Por otro lado, este nuevo mundo trae amenazas que antes consideramos inexistentes. Considerar que el cifrado moderno es vul-nerable, afecta fundamentalmente

uno de los pilares de nuestro universo digital, poniendo en peligro todo lo que consideramos "seguro": las comunicaciones, las transacciones financieras, mis compras, mi privacidad, etc., etc. Y si el cifrado clásico es superfluo, quizá enfrentemos un mundo sin ciframi-ento como ocurre en países en donde está prohibido cifrar (como lo estuvo en Francia durante muchos años) y busquemos asegurar de otra forma o muy seguramente vendrá la siguiente generación de algoritmos basados y ejecutados en computación cuántica lo que obligará a que todos tengamos acceso a ella (la NIST ya está liberando estándares nuevos (8)). ¿O quizá no?, y el gran hermano tome el control.

Referencias

1. Se ha simulado el tiempo que toma el entrelazamiento cuántico y no es instantáneo, pero define attosegundos, o sea, solo 10 a la -18 (10-18) segundos. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.133.163201

2. Redes cuánticas y transmisión instantánea e invulnerable en revista Nature. https://www.nature.com/articles/s41586-020-2401-y

3. Teletransporte cuántico. https://www.xataka.com/investigacion/teleportacion-cuantica-funciona-promete-revolucionar-manera-que-transferimos-informacion

4. Google claims to have reached quantum supremacy. https://www.ft.com/content/b9bb4e54-dbc1-11e9-8f9b-77216ebe1f17

5. Quantum Embedding of Non-local Quantum Many-body Interactions in Prototypal Anti-tumor Vaccine Metalloprotein on Near Term Quantum Computing Hardware. https://arxiv.org/abs/2410.12733

6. Algoritmo de ataque criptográfico de clave pública basado en procesado cuántico con la ventaja de D-Wave. http://cjc.ict.ac.cn/online/onlinepaper/wc-202458160402.pdf

7. Royal Navy Successfully Tests Quantum-Sensing Technology. https://www.royalnavy.mod.uk/news/2024/october/31/20241101-royal-navy-successfully-tests-quantum-sensing-technology

8. NIST libera 3 estándares de ciframi-ento Post-Cuántico. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Jaime Enrique Gómez Hernández (Pato). *Físico, Ing. Mecánico MSc. Universidad de Los Andes; PhD. Mecánica Computacional Universidad de Gales UK; Becario de Colfuturo, BID, Colciencias y FCO-British Council (Chevening), Profesor Asistente Uniandes en Física e Ing. Mecánica del 1998 a 2002; Coordinador portales de software libre como LinuxCOL y OrfeoLibre; fundador de empresas de tecnología como Azuan, Skina, Simulmax y SkinaTech; Creador y patrocinador de proyectos de software como Orfeo NG, Check, Entregalo, Legacy, Efica y Kuine Linux. Y al final, cocinero, artista marcial, skater, lector. incansable de ciencia ficción y cacharrero permanente de software y hardware.*

Catalina Albornoz

En conversación con los editores técnicos de esta edición de la revista Sistemas.

DOI: 10.29236/sistemas.n173a3

Juan G. Lalinde Pulido

Daniel Sierra Sosa

Tu formación académica diversa, háblanos un poco acerca de tu formación y cómo decidiste orientar tu educación.

Lo primero es que me encantan las matemáticas y la física. Cuando estaba en el colegio hice una prueba de aptitud, y me salió que podía estudiar lo que quisiera, y yo pensé: gracias, pero no me sirve ¿qué debería estudiar? Creo que la primera carrera que me salió fue medicina, pero me daba miedo ser cirujana la verdad tener a la vida a alguien en las manos me daba miedo entonces dije no. La segunda opción era ingeniería entonces le pregunté a la persona que me hizo la prueba ¿qué es lo que más tiene física y matemáticas? Y curiosamente en vez de decirme estudia física y matemáticas me sugirieron ingeniería mecánica. Creí que estudiar ingeniería mecánica era ser inventora, después, hablando con un amigo en la universidad, descubrí que ingeniería electrónica, estaba súper chévere, y tenía más matemáticas y más física. Así que, en realidad

me terminó gustando más electrónica, y en el fondo me siento un poquito más como ingeniera electrónica. Me encantó, me enfoqué en sistemas de control, hice maestría en eso, estaba muy orientada hacia la academia. Estudiando en la Universidad de los Andes en Colombia, y desde allá hice un énfasis en educación, mis intereses siempre han sido muy variados y me he dejado llevar por lo que me gusta, no importa que no combinen. Así que estudie ingeniería mecánica, ingeniería electrónica y opción de educación.

Después me fui a Francia dos años a hacer una maestría en doble programa con los Andes, entonces era un doble programa a nivel de maestría, dos años en Francia, una en Colombia y en este caso enfocada en sistemas de control. Allá en Francia tuve la oportunidad de aprender sobre vehículos autónomos, entonces me interesé por ese lado y cuando volví a Colombia seguí en el área, trabajando con drones y metida en eso ahí tuve la oportunidad de ser asistente graduada entonces eso era como ser profesora de laboratorio de algunas clases incluida optimización y control y estaba en esas cuando un amigo de mecánica curiosamente me dijo están buscando a alguien en la empresa donde estoy traba-

jando y lo que él hacía era eficiencia energética y cambio climático, eficiencia energética. Decidí ir a trabajar, salir a la industria, en vez de realizar un doctorado, que era lo que creí que quería hacer. Cambié rumbo y me fui a la industria a trabajar como Project Manager de Eficiencia Energética, fue una aterrizada la vida real. Saliendo de la academia a tener que tomar decisiones instantáneas sin poder modelar las cosas. Eso fue importante, útil y difícil. Y también me sacó un poquito de mí, como de mi zona de confort, de mi rumbo, salir de sistemas de control, de matemáticas y de todo. Yo desde la universidad había hecho cosas prácticas, por ejemplo, organicé un evento que me sirvió más adelante, que es un makeathon, que es como un hackathon, pero de hacer cosas. Entonces, en conjunto con varios colegas de ingeniería mecánica, organizamos el primer makeathon, creo que fue mi primera experiencia organizando un evento grande, era con bastantes universidades en Colombia.

Ya trabajando, estuve dos años trabajando en eficiencia energética y después decidí que no me gustaba tanto la termodinámica. Si hubiera querido seguir ahí, hubiera debido tener un amor que no le tenía a la termodinámica. Así que cambié de rumbo y descubrí la computación en la nube. Me pareció interesante, y me puse a aprender de eso, aplique a IBM y entré. Fue una dosis de buen timing y la verdad mucha determinación porque yo de eso no tenía ni idea. lo aprendí sola, y apliqué, me fue bien en la entrevista y entré y ya trabajé en el equipo del CTO en Colombia y tenía algo súper bueno y es que tenía mucho material de entrenamiento entonces me entrenaron muy bien en ventas, en cosas técnicas, en de todo y durante más o menos un año estuve entre aprender y hacer demos, que eran mini pruebas de concepto para algunos clientes usando los servicios de nube que tenían ellos entonces bueno

¿Cómo te decidiste a trabajar en Computación Cuántica?

Estando en IBM mi jefe dio una charla de cuántica y no entendí tanto, no entendí lo suficiente. Así que investigué un poquito, un poco más, un poco más y me fui metiendo en el cuento. Y cada vez que quería que entendía, me da cuenta que no he entendido nada. Y ya creo que eso fue, en ese momento era pandemia, 2020, y había un montón de eventos virtuales, incluso algunos que organicé yo sobre otros temas. Entonces, por ejemplo, con mis compañeros, los que entramos al tiempo, decidimos organizar unos eventos de nube, entonces parte de ese tema de organizar eventos, decidimos enseñarle a la gente en IBM sobre en la nube, que muchos no sabían nada. Y al mismo tiempo yo estaba tomando cursos online, yendo a eventos de networking, etc. En uno de esos eventos había una organización

que era Women in Quantum, que estaban organizando unos eventos virtuales. En uno de esos habló Maria Schultz, por ejemplo. Fue la primera vez que escuché de Sanadu, que es la empresa donde trabajo ahorita. Y en uno de esos eventos conocí a una persona que antes trabajaba en IBM y que me dijo, oye, tú eres ingeniera, estás interesada en cuántica o sabes de cuántica, ¿por qué no aplicas este tema a los embajadores de computación cuántica de IBM? Entonces, no es lo mismo que los advocates, los embajadores tienen que ser empleados de IBM. Y yo no tenía ni idea que esto existía. De hecho, me habían dicho que, por no haber estudiado física, no podía hacer cuántica; manifesté que como ingeniera yo sabía. Al final descubrí que no tenía ni idea; en Colombia nadie sabía que esto era un programa que existía, pero esa información no nos había llegado.

Así que yo por fuera, por haber estado en un evento de networking, nada que ver con me terminé enterando que existían los embajadores y me, digamos que conecté con la persona que era líder de este tema de los embajadores. Me entrevistaron, dijeron, sí, tu perfil aplica y entonces entré en un programa de entrenamiento muy bueno donde al final tienes que dar una presentación sobre cuántica y si la das bien, si no estás diciendo cualquier cosa, pasas. Entonces ya me convertí en embajadora y eso me abrió muchísimas puertas porque tuve acceso a entrenamientos frecuentes, más información, yo misma dar charlas. Entonces llegué a la cuántica por estar en el lugar correcto en el momento correcto porque mi jefe dio una charla que no entendí y porque decidí yo misma entrar a investigar al respecto porque me pareció chévere. Algo que conectó mucho conmigo fue las matemáticas del asunto. Cuando vi entrelazamiento, pero en matemáticas, fue el momento en el que hice clic. Entonces es industria, pero un poco académica, creo que es el punto correcto para mí. Fui embajadora por un tiempo, supe que quería dedicarme a esto.

Has participado en muchos eventos públicos de formación de comunidad. Por ejemplo, estuviste como participante del Quantum Open Source Foundation, en donde propusiste una solución híbrida para el problema ruteo de vehículos, ¿Por qué escoger un problema tan complejo? ¿Cuáles problemas se pueden resolver con computadores cuánticos?

Justamente porque era complejo y yo no tenía ni idea de lo que estaba haciendo. Me dije: cuántica parece que va a resolver todos los problemas y este es súper difícil y creo que lo puede resolver; además, yo sé optimización. Muchas veces al enfrentarnos a un problema es que nos damos cuenta de la realidad.

Porque la solución no es que funcione muy bien. Funcionaba a una escala súper pequeñita y ya. A una

escala un poquito más grande ya no funciona para nada, con cinco nodos ya no funcionaba. Así que eso es importante, porque muchas veces vamos a estar en esa situación cuando yo creí que me las sabía todas y escogí un problema súper difícil y fui a tratar de resolverlo y resulta que ahí es donde yo entiendo porque siempre la gente decía los computadores cuánticos en este momento no son muy buenos, ver en realidad qué es a lo que se refieren con eso. Así que para mí fue importante, primero, empezar a saber cómo resolver el problema. A veces no se sabe ni por dónde empezar, tuve que aprender a resolverlo sola, comparar la solución cuántica con la clásica y darme cuenta que la solución cuántica para cinco nodos funcionaba terrible.

A pesar de que no funcionó, para mí fue muy importante, y me conectó también con otra gente. Mi mentor, que fue súper importante para mí porque me guió en ese proceso, tenía otros estudiantes y nos reuníamos cada semana o dos semanas, no recuerdo muy bien, y presentamos nuestros avances, como en un grupo de investigación. Cada cierto tiempo, todos los miembros presentan sus avances al grupo. Así que, aunque mi proyecto no estaba funcionando tan bien, pude aprender de mi proyecto y del de los otros. Pude aprender qué era FeMoco; hasta ese momento, no tenía idea de qué era. No solamente se aprende haciendo, se aprende escuchando lo que otros están haciendo. Entonces, eso fue el Quantum Open Source Foundation.

Otros eventos de comunidad en los que he participado o que he organizado fue el primer simposio latinoamericano de computación cuántica. Yo sé lo importante que es la comunidad, y en Latinoamérica es enorme y tiene muchísimo talento, pero a veces no tenemos esos espacios en donde nos juntemos para hablar.

Parte del éxito fue tener un súper grupo de organización, porque obviamente no lo hice yo sola. En equipo logramos armar algo que fue valioso y al final tuvimos alrededor de 200 personas que llegaron y pudimos tener ponentes que nunca se nos hubieran ocurrido, como el caso de Zaira Nazario, hoy en día, una de las personas más relevantes en el área.

Empezaste a hacer computación cuántica en Colombia desde la industria sin tener una formación formal en computación cuántica, y ahora estás de tiempo completo en un trabajo de cuántica. Desde tu punto de vista y desde tu propia historia ¿Cuáles fueron los retos más grandes?

El primer reto fue cuando me dijeron tú no estudiaste física; estuve cerquita de 'tirar la toalla'. Y en medio de la frustración interna me pregunté y ¿qué hago? No puedo devolverme a la universidad a estudiar otra vez una carrera. Estuve

cerquita, pero dije, no como así, no me parece, ese es un momento donde muchísima gente piensa, pues si me dijeron que no se puede, pues debe ser que tienen razón. El siguiente punto es, a veces te salen buenas oportunidades en otras cosas, hay un costo-oportunidad de hacer esto. Yo me vine a un nuevo país, a una startup. Me fui de IBM, que es una empresa establecida en el mundo, a una startup que nadie en mi familia conocía. Hacer algo que podía morirse a los dos años, en ese momento, y de hecho todavía no sabemos si alguien va a sacar un paper y decir, esto no funciona. Tenemos suficiente evidencia para pensar que esto sí tiene un impacto a largo plazo, que esto va a ser importante, pero no hay garantías.

Así que tomar esa decisión de asumir el riesgo la tuve que afrontar; en otras palabras, poner en juego un trabajo en una empresa estable en Colombia, por algo inestable en todos los sentidos, pero que me encantaba. El segundo reto es dejarlo todo por perseguir algo que podría no salir, pero que, si saliera, sería espectacular.

Una ventaja que tuve es que hablaba bien inglés, para muchísima gente, ese es el reto y esa es la dificultad. No significa que tengas que hablar perfecto, tengo compañeros que no hablan perfecto, pero que son excelentes para su rol. Esa es una barrera que yo he notado. Siempre hay más barreras, por ejemplo, el hecho de no haber tenido una formación formal en física ha sido algo que he tenido que aprender sobre la marcha. Esa es una barrera que sigo superando todos los días, porque sale un concepto nuevo, un término nuevo, del que no tengo ni idea, y me toca preguntarlo, investigarlo, tener la valentía de preguntar, o estar dispuesta a no entender, estar dispuesta a sentirme qué me falta. No haber tenido formación en física lo dificulta, pero no es imposible.

Eres Quantum Community Manager de Xanadu, cuéntanos un poco qué tienes que hacer, cuál es tu rol, y cuáles responsabilidades tienes.

Muchas empresas no tienen un rol en tal sentido, pero muchas sí tienen una comunidad de personas que usan sus productos y servicios. Así que fue una decisión estratégica de las personas llegaron antes de mí a Xanadu, es decir, querían tener un equipo dedicado a lo que necesita esa comunidad de personas que usan los productos y servicios. Para cada comunidad o para cada empresa esto es diferente, en nuestro caso, la mayoría de las personas usan nuestro software principal Pennylane; de ahí que pase una muy buena parte de mi tiempo ayudando a resolver las preguntas de los miembros de nuestra comunidad. Tenemos un montón de canales por donde la gente puede preguntar sobre el uso de nuestros productos y servicios o sobre temas de cuántica. Ese es uno de los

aspectos preferidos de la gente sobre Pennylane y Xanadu.

En otra dirección y a nivel de estrategia, trabajo con el CTO de software, la persona encargada del área de software, para entender a un nivel un poco más elevado las necesidades de nuestros usuarios. Ya no son solamente las necesidades del día a día, sino entender más allá Pennylane como herramienta.

Cuando hablas de comunidad, esa comunidad estará compuesta por un grupo diverso de personas, profesionales, entusiastas, y académicos, ¿qué tan difícil ha sido hacer esto? ¿Cómo haces para balancear ese conocimiento técnico con hacerte entender?

Nosotros nos enfocamos donde podemos aportar mayor valor y lo hacemos con las personas que tienen un conocimiento básico de algebra lineal. Nada de lo que hacemos contempla un nivel de niños de colegio, para citar un ejemplo. Existe un grupo que ha hecho muy buen trabajo para llegar a tales personas. Se trata de llevar la investigación a un lenguaje entendible para un público con una base mínima. No significa que tengan que saber de cuántica, pero sí que cuenten con una base mínima de matemáticas. Y lo hacemos interna o externamente a través de aliados en el marco de un lenguaje entendible, hecho muy valorado por los diferentes miembros y niveles de la comunidad.

Contamos con miembros del equipo especializados en escribir contenido, contemplando dibujos o links y otros recursos para hacer que el mensaje llegue. En mi caso los aplico en mis charlas o entrenamientos.

¿Qué consejo le darías a alguien en Colombia o en Latinoamérica que quisiera empezar en la computación cuántica o que quisiera migrar su ejercicio profesional a la computación cuántica?

Hay muchísimo material online gratuito. El primero que recomendaría es el Pennylane Codebook, empezando desde qué es un Qubit; la única base necesaria es saber matemáticas básicas, algebra lineal, y

Python básico, porque también incluye ejercicios de código. Para una persona que está en la universidad, si pueden entrar a un grupo de investigación, puede ser en física o ingeniería, usualmente hay los grupos de investigación que trabajan estos temas, o ciencias de la computación. Muchísimas empresas tienen eventos que son online y donde pueden conocer a otros miembros de la comunidad que los motiven cuando sea difícil. En mi caso, el grupo de mentoría de QOSF fue de gran ayuda. Es muy importante estar dispuestos a manifestar lo que no les gusta, como me sucedió cuando sentí que la termodinámica no era para mí. Somos muy afortunados porque estamos en un momento en que hay mucha gente dispuesta a ayudar. Se trata de una comunidad construida a partir de ayudarnos unos a otros.

De manera que, para las personas interesadas en entrar al campo, vale la pena aprovechar estas iniciativas globales o locales, para encontrar personas que los ayude a arrancar. Si quieren empezar por el Codebook es buenísimo. Hoy contamos con un montón de plataformas para ayudarlos. Una vez estudian un poco por su cuenta, hacer un proyecto siempre es una buena forma de darse cuenta hacia dónde seguir o qué seguir aprendiendo.

Hay bastante debate acerca de la utilidad de la computación cuántica, sobre qué tanto va a durar en el tiempo, si va a sobrevivir la prueba del tiempo o no ¿tú dónde ves el futuro de la computación cuántica?

Hay que ser muy cuidadoso en entender la diferencia entre el potencial a futuro y la realidad actual, el potencial de la computación cuántica es grande en el sentido de que hay algoritmos o herramientas que nos pueden permitir resolver problemas que hoy en día no es posible hacerlo con un computador clásico. Ejemplo, el algoritmo de Shor es algo que está demostrado, eso no se puede resolver en un tiempo razonable con un computador clásico, pero si tuviéramos uno cuántico muy grande y poderoso, podríamos. Obviamente esto va a llegar en muchísimos años. Puede haber unos temas a más cercano plazo, que son problemas en química, donde hay problemas donde el computador clásico no te permite llegar a la precisión que necesitas para poder entender un sistema químico al nivel correcto. Si quisieras desarrollar un nuevo material, hoy en día muchas veces hay que hacer muchas pruebas físicas con materiales. Pero, si pudieras simularlo, podrías tener una ventaja y llegar a la solución, más rápido y con menos costo. Estos son un tipo de problemas que son interesantes a ese mediano plazo. En Xanadu lo llamamos ISC o Intermediate Scale Quantum. No necesitamos miles o millones de qubits, sino algo más de cercano plazo, asumiendo que esos qubits no son súper ruidosos, porque con ruido no podemos hacer nada realmente.

Asumamos que tenemos ese sistema intermedio, con algunos cientos de qubits lógicos, yo sé que esto igual es mucho, pero parte de lo que estamos haciendo en Xanadu y a lo que le vemos una buena promesa, es a resolver esos tipos de problemas en química, donde podamos llegar a entender sistemas en materiales; por ejemplo, poder simularlos a nivel de detalle que nos permitan encontrar una ventaja, descubrir algo nuevo. Con relación a los materiales, pueden ser de diferente nivel, por ejemplo, para baterías. Diferentes empresas están enfocadas en distintas áreas también. Xanadu no hace absolutamente todo, estamos muy enfocados en algo que sabemos hacer muy bien, que son simulaciones en química cuántica. También tenemos un equipo enfocado en machine learning cuántico, pero a más alto nivel, no tan aplicada. Así que, si yo dijera en los próximos 10 años, mi apuesta personal sería más en los temas de química, química cuántica, donde esto pueda llegar a ayudar el desarrollo de materiales. Y bueno, otras empresas tienen muchos, están haciendo muchos trabajos en otros campos que no conozco.

Juan Guillermo Lalinde Pulido. *Universidad EAFIT. Ingeniero de Sistemas, Matemático y PhD en Telecomunicaciones. Profesor del área de Ciencias Fundamentales y director del Centro de Computación Científica Apolo. Investigador activo en los campos de computación cuántica y computación de alto rendimiento.*

Daniel Sierra Sosa. *Catholic Univesity of America. Ingeniero Físico y PhD en Física. Profesor del Departamento de Ingeniería Eléctrica y Ciencias de la Computación. Es investigador activo en los campos de la computación cuántica, el aprendizaje automático, el procesamiento de datos para el sector salud, el procesamiento de imágenes y el análisis de datos. Es también Qiskit advocator e instructor certificado en computación cuántica, ciencia de datos e inteligencia artificial.*

Calendario de Eventos.

ACIS

- Curso virtual: Arquitectura de Software 4:00 p.m. a 7:00 p.m. — Febrero 3 al 13
- II programadores de america 2025 salvador bahia, brasil — Marzo 12 al 17
- Asamblea ACIS — Marzo 20
- ACISTIC 2025 — Abril 29,30
- Jornada de gestion de productos y proyectos TI — Mayo 14 al 16
- Encuentro REDIS Rionegro antioquia — Junio 11 al 14
- Jornada Internacional de seguridad informática Retando las certezas para anticipar y adaptar el futuro — Julio 30 y 31
- GEODATOS 2025 — Septiembre
- REDUC@TE — Octubre 14 al 18
- Maratón Nacional de programación 2025 — Octubre
- Maratón regional latinoamericana de programación 2025 — Noviembre

2025

Pronóstico de Mediciones Eléctricas utilizando aprendizaje de máquina cuántico

DOI: 10.29236/sistemas.n173a4

Jonathan J. Montes Campos, Daniel Sierra Sosa, Juan G. Lalinde Pulido

1. Conceptos Básicos sobre Telemedida en el sector eléctrico

La telemedida es un conjunto de actividades que hacen parte del subproceso de aseguramiento de ingresos en las empresas del sector eléctrico. Utiliza plataformas de software y hardware especializadas que permiten el acceso remoto a los datos capturados por los medidores habilitados para ello, con el propósito de hacer análisis y crítica de los consumos de los clientes y registros de energía generada por las centrales de generación de energía. En este trabajo se presenta un experimento desarrollado en conjunto con EPM - Empresas Públicas de Medellín E.S.P., en el cual se usa computación cuántica para predecir valores futuros de las mediciones eléctricas.

La Telemedida se hace utilizando redes de comunicación de datos que permiten obtener las medidas de consumos y generación acorde con las exigencias normativas: cada 15 minutos en generación y cada 60 minutos para consumos de clientes.

El marco regulatorio que dicta normas con respecto a la gestión de la medida y telemedida está dado por: Leyes de servicios públicos 142 y 143, Resolución CREG 038 de 2014 código de medida.

La medición, es decir la toma de las medidas de los medidores, se puede llevar a cabo mediante dos estrategias: la medición tradicional y la telemedida. En la medición tradicional es presencial y física en cambio, en la telemedida, la tecnología incluye el uso de redes de datos para acceder a la información del medidor, lo cual permite:

- Predecir la generación de energía.
- Gestionar la entrega de excedentes de energía generada al sistema interconectado.
- Predecir la demanda de energía.
- Detectar anomalías en las lecturas registradas en los medidores.
- Detectar variaciones en las frecuencias de lectura, cálculo de consumos y facturación.
- Optimizar la eficiencia energética.
- Mejorar el relacionamiento con los clientes mediante recomendaciones que optimicen su uso de energía.

2. Experimento

2.1 Descripción y Alcance del Experimento

Partiendo de la problemática para la gestión de la telemedida, descrita anteriormente, se plantea la realización de un experimento para verificar si las métricas de rendimiento, calidad y tiempos de procesamientos, que se obtienen utilizando la computación clásica se mantienen o mejoran al usar la computación cuántica.

Para realizar este experimento se requiere la implementación de modelos de gestión de información a partir de algoritmos de computación clásica y cuántica, y el uso de computadores clásicos y computadores cuánticos.

2.2 Diseño Experimental

En este diseño se definen los elementos o parámetros necesarios para el desarrollo del algoritmo para computación clásica y para el algoritmo de computación cuántica, lo cual permite evaluar y comparar los resultados de ambos esce-narios para poder sacar conclusiones.

El *dataset* utilizado contiene 2,765,004 lecturas pertenecientes a 1,925 medidores, y tiene la siguiente estructura (Tabla 1).

La infraestructura de cómputo utilizada fue la siguiente (Tabla 2).

3. Modelos de Pronóstico

Generalmente, el pronóstico de carga se centra en la carga eléctrica total por hora, pero puede extenderse a la predicción de cargas del sistema por hora, diaria, semanal y mensual, incluidas las cargas máximas. Los pronósticos se clasifican según el horizonte temporal en: pronóstico de carga a corto plazo (STLF) para hasta un día; a mediano plazo (MTLF) para entre un día y un año; y a largo plazo (LTLF) para entre uno y diez años. Para sistemas grandes como redes regionales o nacionales, estos modelos logran una precisión relativamente alta [1] [2].

Diferentes investigaciones han demostrado que las técnicas cuantitativas de pronóstico, como promedios móviles [3], series temporales [4] y métodos de aprendizaje profundo [5], son útiles cuando la situación es estable y se dispone de datos previos, como es el caso de este experimento. Por otra parte, otras investigaciones sugieren que las técnicas tradicionales de análisis de series temporales, como modelos de regresión, ARIMA, GARCH y modelos híbridos que combinan ARIMA y GARCH con transformadas wavelet, no son adecuadas para pronósticos a corto plazo en configuraciones de datos de alta dimensión o alta volatilidad [6], ya que estos métodos a menudo tienen dificultades con la escalabilidad y la adaptabilidad en tales contextos.

En contraste, las redes neuronales artificiales (ANNs) son más aptas para manejar la complejidad de los pronósticos a corto plazo ya que sus capas ocultas y capacidades de aprendizaje identifican y explotan patrones ocultos en datos de series temporales, lo que lleva a pronósticos más precisos. Estas son particularmente valoradas por varias características clave:

1. Robustez: Las ANNs pueden generalizar bien incluso con datos incompletos o ruidosos.
2. Naturaleza no paramétrica: No requieren suposiciones predefinidas sobre la distribución de los datos, lo que las hace flexibles en diversas aplicaciones. En general, en problemas de ciencia de datos, esta es una aproximación que a menudo se pasa por alto, y se asume una distribución normal en los datos, lo cual no es cierto en todos los casos.
3. Aproximación universal: Las ANNs pueden modelar cualquier función continua con el nivel de precisión deseado.

Los avances recientes en el pronóstico de carga a corto plazo han visto la integración de técnicas

Variable	Descripción	Valores
SERIE	Identificador único del cliente o medidor eléctrico.	Numérico (ej., 18741849).
FECHA	Fecha de la medición. Va desde el 2023-06-01 hasta el 2023-07-31	Formato YYYY-MM-DD.
HORA	Hora de la medición. Va de 0 a 23 horas del día.	Numérico (0, 1, 2, ..., 23).
SERVICIO_SUSCRITO	Servicio suscrito, identificado por un código numérico (ej., Residencial, Industrial)	Numérico (ej., 130820443 corresponde a la categoría Industrial con subcategoría 11-220 Voltios).
ACTIVA_IMP	Energía activa importada (kWh).	Numérico (ej., 0.33).
REACTIVA_IMP	Energía reactiva importada (kVARh).	Numérico (ej., 0.04).
ACTIVA_EXP	Energía activa exportada (kWh).	Numérico (ej., 0.03).
REACTIVA_EXP	Energía reactiva exportada (kVARh)	Numérico (ej., 0.05).
V1, V2, V3	Voltaje de las fases 1, 2 o 3 (V).	Numérico (ej., 230.5).
I1, I2, I3	Corriente de las fases 1, 2 o 3 (A).	Numérico (ej., 13.2).
ALARM.NAME	Nombre de la alarma activada durante la medición.	Alfanumérico (ej., Overload).
CATEGORÍA	Categoría de la medición	1: RESIDENCIAL. 2: COMERCIAL. 3: INDUSTRIAL. 4: OFICIAL. 5: ESPECIAL. 7: AUTOCONSUMO.
SUBCATEGORÍA	Subcategoría de la medición.	1: ESTRATO 1. 2: ESTRATO 2. 3: ESTRATO 3. 4: ESTRATO 4. 5: ESTRATO 5. 6: ESTRATO 6. 11-220 Voltios. 12: 132000 Voltios.
X, Y	Coordenadas de latitud y longitud, respectivamente.	Numérico (ej., -74.00597, 40.71278).

Tabla 1. Variables del dataset

Tipo de infraestructura	Descripción
Clásica:	laptop personal
Clásica para simulación cuántica con GPU:	Centro de Computación Científica Apolo: Cola Accel-2 con 3 GPU habilitadas para el experimento
Clásica para simulación cuántica con CPU:	Centro de Computación Científica Apolo: Cola longjobs, nodo con 32 núcleos.
Computador cuántico:	IBM, 127 qubits.

Tabla 2. Infraestructura computacional

avanzadas de aprendizaje automático. En China, un modelo híbrido que combina descomposición por modo de variación (VMD) con redes de memoria a corto y largo plazo (LSTM), con optimización bayesiana (BOA), presentó un rendimiento superior, logrando un MAPE de 0.4186 % y un coeficiente R^2 de 0.9945, comparado con otros modelos como SVR, regresión MLP, LR, RF y EMD-LSTM [7].

Las redes neuronales artificiales (ANNs) han sido utilizadas de manera efectiva para pronosticar la carga a corto plazo, especialmente con datos no lineales. En [8], por ejemplo, los autores desarrollaron un modelo basado en ANNs para procesar conjuntos grandes de datos históricos de carga, dinámicos y no lineales, contrastando los resultados en una instalación real de pruebas. Otras arquitecturas de redes neuronales, incluidas las RNNs, CNNs, LSTMs y redes profundas, también se han utilizado para mejorar la precisión de los pronósticos [9]. En particular, las redes LSTM han demostrado superar a los enfoques estadísticos y de aprendizaje automático tradicionales en la reducción de los errores de predicción [10], mostrando específicamente que los modelos LSTM son efectivos para el pronóstico de carga residencial a corto plazo y superando significativamente a modelos como ELM, BP-NN y regresión de k-vecinos más cercanos.

En este trabajo, se propone un método para el pronóstico preciso de la carga eléctrica a corto plazo, para las siguientes 24 horas y la siguiente semana, para hogares individual agrupados por clase social y para la industria. Inicialmente se aplicaron modelos LSTM clásicos para evaluar sus capacidades de pronóstico con diferentes grupos de usuarios y para evaluar las dependencias e independencias de los grupos en el pronóstico de se-

ries temporales. Este enfoque clásico fue la base para el desarrollo de modelos LSTM mejorados cuánticamente (QLSTM) y también se utilizó como línea base para la comparación.

Como en el aprendizaje automático (ML), los paradigmas QML pueden clasificarse en aprendizaje supervisado o basado en tareas, aprendizaje no supervisado o basado en datos, y aprendizaje reforzado o basado en recompensas. Debido a su resiliencia al ruido, buena generalización y su potencial para aprovechar la ventaja cuántica, el aprendizaje supervisado ha recibido especial atención en los últimos años [11]. Los algoritmos QML aceleran los sistemas cuánticos para mejorar las tareas de regresión o clasificación de ML, por ejemplo, mediante el Support Vector Machine Cuántico, PCA Cuántico, Clasificador Cuántico Variacional, Máquina Boltzmann Cuántica, Red Neuronal Cuántica (QNN), Red Neuronal Convolucional Cuántica y Red Neuronal Profunda Cuántica [12].

Las redes neuronales cuánticas (QNNs) se refieren a la utilización de circuitos cuánticos parametrizados, que son una secuencia de compuertas, algunas de las cuales tienen parámetros libres, que serán entrenados para resolver el problema. Este algoritmo merece especial atención ya que se utiliza en los tres paradigmas de QML: aprendizaje supervisado, aprendizaje no supervisado y aprendizaje reforzado. En algunos casos, se utilizan enfoques híbridos con modelos que combinan redes neuronales clásicas y cuánticas, los cuales buscan distribuir la capacidad de representación y la complejidad computacional entre la computación clásica y cuántica. En otros casos se han propuesto versiones cuánticas de métodos de núcleo (kernel) [11].

Los computadores cuánticos actuales, particularmente los dispositivos cuánticos de escala intermedia ruidosos (NISQ), enfrentan dificultades para ejecutar circuitos cuánticos con muchos qubits o con muy profundos debido a la falta de mecanismos efectivos de corrección de errores cuánticos [13]. Para abordar este problema, un trabajo reciente de investigadores chinos introduce un nuevo marco que utiliza Circuitos Cuánticos Variacionales (VQC) para implementar Redes Neuronales Recurrentes (RNNs), específicamente redes de Memoria a Largo Corto Plazo (LSTM). Su enfoque, denominado LSTM Cuántico (QLSTM), combina computación cuántica y clásica para aprovechar el poder expresivo del entrelazamiento cuántico mientras mantiene la viabilidad práctica para dispositivos NISQ. Este marco híbrido cuántico-clásico presenta resultados prometedores, incluyendo un aprendizaje más rápido y una convergencia más estable en comparación con las LSTM clásicas y ha sido utilizado en varias aplica-

ciones físicas [13] y en la predicción de irradiancia solar [14]. Además, los VQC se han utilizado para algoritmos cuánticos poco profundos, siendo exitosos en tareas de clasificación, agrupamiento e incluso aprendizaje por refuerzo profundo [14].

Basándose en estos avances, este en este trabajo se utiliza el QLSTM, logrando un desempeño mejor en términos de función de pérdida, aprendiendo más rápido, aproximadamente en la mitad de las épocas que el LSTM clásico, en el contexto de pronóstico de mediciones de carga eléctrica. A continuación, se presentan los modelos LSTM y QLSTM con el fin de clarificar la relación que hay entre ellos.

3.1 LSTM

Las redes de Memoria a Largo Plazo (LSTM) fueron introducidas por Sepp Hochreiter y Jürgen Schmidhuber para abordar los problemas de memoria inherentes a las Redes Neuronales Recurrentes (RNNs) [15], [16]. Las RNNs tienen la capacidad de mantener una forma de memoria a corto plazo, lo que les permite procesar secuencias de datos. Sin embargo, tienen dificultades para retener información a lo largo de secuencias largas debido al problema del gradiente que desaparece, lo que lleva a la pérdida de información importante a medida que pasa por múltiples pasos. Esto hace que sea un desafío para las RNNs aprender dependencias a largo plazo en las secuencias de datos [16].

Las LSTM se desarrollaron para aliviar estos problemas. Una célula LSTM es similar a una célula RNN estándar, pero introduce dos vectores separados: h(t), el estado a corto plazo, y c(t), el estado a largo plazo. Estos dos vectores trabajan junto para retener y descartar selectivamente información a lo largo de la secuencia, lo que permite a la red aprender dependencias a lo largo de períodos de tiempo más largos. La estructura de una célula LSTM incluye tres componentes principales llamados puertas: la Puerta de Olvido, la Puerta de Entrada y la Puerta de Salida, como se ve en la Figura 1.

La Puerta de Olvido determina qué información del estado a corto plazo anterior y la entrada actual debe ser descartada, la Puerta de Entrada procesa la información que recibe la neurona y obtiene ciertas características de la etapa actual de la secuencia, mientras que la Puerta de Salida se encarga de definir qué información se guardará para el término a corto plazo para el siguiente paso en la secuencia. Usando las Puertas de Olvido, de Entrada y de Salida, las LSTMs retienen selectivamente la información relevante mientras descartan detalles menos importantes, de manera similar a cómo el cerebro humano simplifica y retiene información esencial mientras descarta detalles menos relevantes [13].

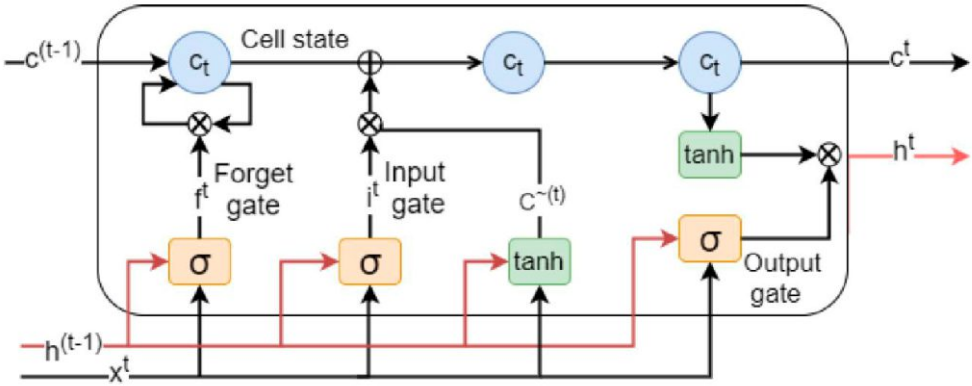


Figura 1. Componentes de una célula de una red LSTM

3.2 QLSTM

QLSTM es un algoritmo híbrido cuántico-clásico que utiliza VQC en lugar de las puertas en una LSTM clásica y también dos funciones de activación, como se ve en la figura 2.

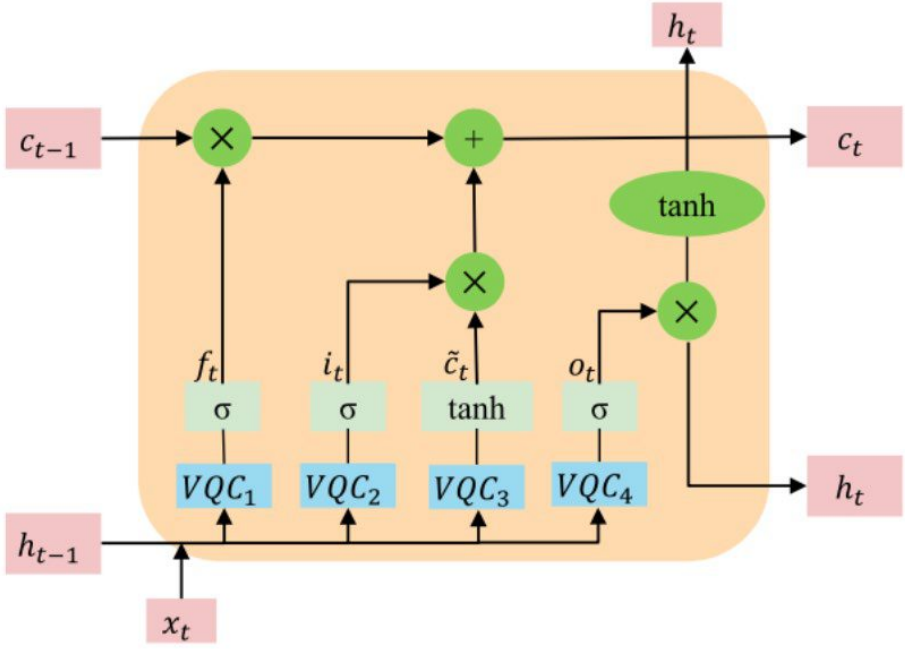


Figura 2. QLSTM

En QLSTM se reemplaza las compuertas de la red clásica por un circuito VQC, circuito variacional cuántico, que incluye los parámetros que serán optimizados mediante un algoritmo de QML que se aplica iterativamente. Para poder realizar el entrenamiento, se incluye una capa que codifica los datos en estados cuánticos, luego hay una capa variacional que se evalúa y se realiza la medición. A partir de estos resultados se ajustan los parámetros del VQC para lograr el aprendizaje.

4. Ingeniería de datos y características

Empresas Públicas de Medellín E.S.P., conocida por su acrónimo EPM, una empresa colombiana de servicios públicos proporcionó la base de datos utilizada. Tiene 2.765.004 registros divididos en 1.975 clientes totales en todo el departamento de Antioquia en 1.876 localidades. Estos clientes se dividieron en diferentes categorías como Residencial, Comercial, Industrial, Oficial, Especial y Auto Consumos EPM que pertenecen al mercado naciente de AGEP. La Tabla 1 resume las características del conjunto de datos. Los registros del medidor eléctrico, ACTIVA_IMP, van del 6 de junio de 2023 al 31 de julio de 2023. El 1,9% de los valores fueron NaN[1] o valores nulos. Esta variable se refiere a la energía eléctrica consumida por un sistema o instalación, medida en kilovatios-hora (kWh). Es la energía total recibida de la red (importada) durante un período de tiempo con frecuencia horaria. La energía activa es la energía que realmente realiza un trabajo útil, como hacer funcionar la maquinaria, la iluminación, la calefacción, etc. Es la variable elegida para la predicción debido a la importancia del negocio.

Existen dos enfoques de pronóstico para los modelos LSTM (Long short-term memory) y QLSTM (Quantum Long Short-Term Memory): el primero solo tiene en cuenta la variable de pronóstico ACTIVA_IMP (la variable de pronóstico y) en términos de las horas, y el segundo modelo toma la variable de pronóstico ACTIVA_IMP, las variables más correlacionadas y las variables que tiene influencia en la variable de pronóstico según el experto en el negocio eléctrico. Las variables más correlacionadas se encontraron mediante un mapa de correlación descrito en la figura 3 que encuentra la correlación lineal entre variables con base en la ecuación del coeficiente de correlación de Pearson:

$$r_{xy} = \frac{\sum(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum(x_i-\bar{x})^2\sum(y_i-\bar{y})^2}},$$

El rango de este coeficiente va de -1 a 1, donde r=1 indica una correlación positiva perfecta, r=-1 una correlación negativa perfecta y r=0 ninguna correlación lineal.

[1] NaN: Not a Number

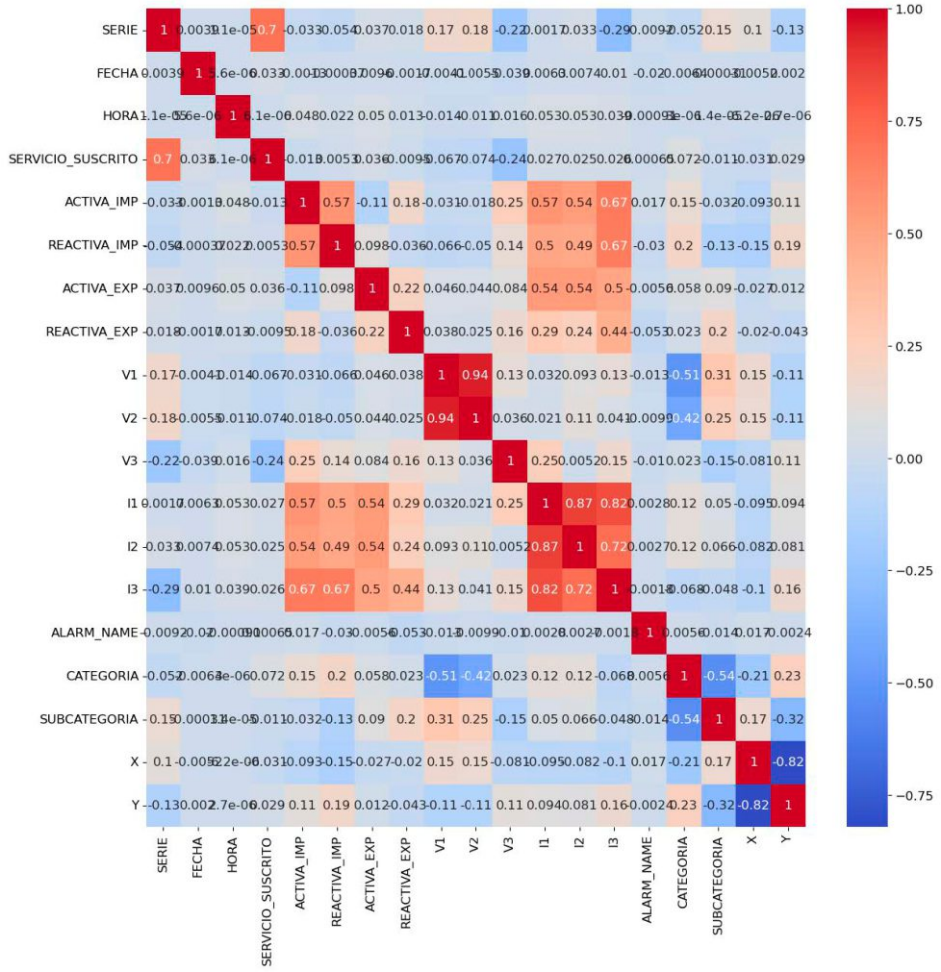


Figura 3. Correlación lineal entre las variables del dataset entregado por EPM

A partir del mapa de correlación se identificaron las variables más correlacionadas como: V1, V2, V3, I1, I2, I3, REACTIVA_EXP y HORA. De estas, HORA se considera una variable exógena porque es un factor externo que influye en el sistema eléctrico, pero no es influenciado por él. Las variables restantes se consideran endógenas, ya que forman parte del sistema eléctrico que genera ACTIVA_IMP. Estas variables se utilizaron para el enfoque descrito en las secciones 5.4 y 5.5. Los mejores hiper- parámetros para los modelos LSTM y QLSTM se seleccionaron utilizando una validación cruzada de series temporales con 3 pliegues, siguiendo múltiples divisiones de entrenamiento y prueba: 60% entrenamiento, 20% prueba, 70% entrenamiento, 20% prueba y 80% entrenamiento, 20% prueba. Después

de esto, se implementó un proceso de selección paso a paso, pero el mejor rendimiento del modelo se logró utilizando todas las variables mencionadas anteriormente.

Se tomaron los registros de los clientes de los últimos 16 días y se filtraron para eliminar los clientes con menos de 408 horas registradas, quedando 1,938 clientes.

Para cada experimento se normalizaron los datos utilizando standard scaler, tanto para el pronóstico con LSTM y como QLSTM. Las variables utilizadas para cada modelo se escalaron también con el método Min-Max y se convirtieron en el rango de [0,1].

5. Resultados y Discusiones

Esta sección contiene los resultados obtenidos en este trabajo y las explicaciones de los dos enfoques desarrollados para el LSTM y el QLSTM mostrando los, resultados y conclusiones de los modelos.

5.1 Herramientas y enfoques utilizados para LSTM y QLSTM

Para este trabajo, los modelos clásicos se construyeron utilizando Python 3.11.5, las bibliotecas Pytorch para LSTM y QLSTM. Se utilizó Pennylane para la construcción de los circuitos VQC (Variatonal Quantum Circuit) y la arquitectura QSLTM basada en el repositorio de GitHub de Pennylane [17] y el estudio realizado sobre la predicción del precio de las acciones utilizando BERT y GAN desarrollado en el repositorio de GitHub [18]. Hay dos enfoques utilizados para los modelos LSTM y QLSTM:

Enfoque 1: La variable ACTIVA_IMP es la única que se tiene en cuenta para los datos de entrenamiento $X_{training}$ y $Y_{training,}$ y los datos de prueba X_{test} y Y_{test} siguiendo el enfoque de [19]. Este enfoque se utilizó solo para mostrar la independencia entre categorías en la sección 5.3 y la demostración de la mejor función de costo en la sección 5.2.

Enfoque 2: La variable de pronóstico y es la variable de pronóstico ACTIVA_IMP que tiene una relación de dependencia con las variables V1, V2, V3, I1, I2, I3, REACTIVA_EXP y HORA. Este enfoque se basa en [20].

5.2 Mejor función de Costo o Funcional: MSE vs MAE

Para demostrar cuál es la mejor función de costo o función de error, se realizó la predicción y el desempeño del modelo usando el cliente 18741848. Con este objetivo, se eligieron los siguientes hiper parámetros para los modelos LSTM (Tabla 3).

En la Figura 4, el rendimiento del modelo de pronóstico LSTM se evalúa utilizando funciones de costo MSE y MAE, lo que demuestra que la pérdida de entrenamiento

Hiperparámetro	Valor
División Entrenamiento/Prueba	80% entrenamiento, 20% prueba
Longitud de Secuencia (Entrenamiento)	10
Longitud de Secuencia (Prueba)	5
Tamaño de Entrada	1
Número de Capas	3
Tamaño Oculto	64
Tamaño de Salida	1
Tamaño del Lote	8
Número de Épocas	50
Pasos de Predicción	5
Tasa de Aprendizaje	0.0001
Número de Unidades Ocultas	16

Tabla 3 Hiperparámetros

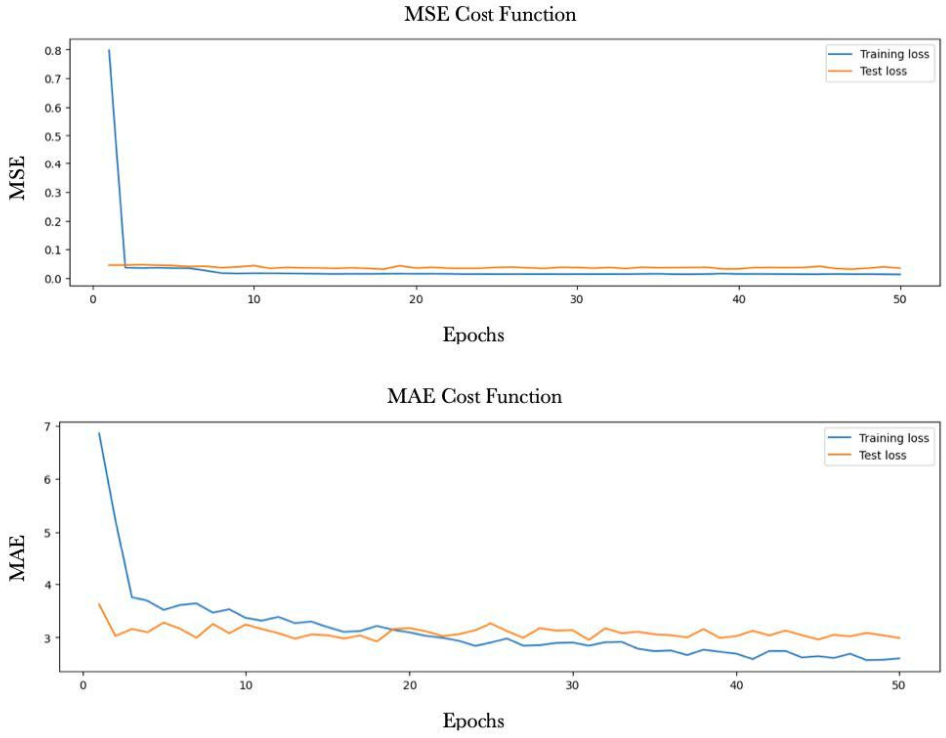


Figura 4. El rendimiento del modelo de pronóstico LSTM

disminuye con el tiempo, lo que indica optimización, y se mantiene consistentemente por debajo de la pérdida de prueba. MSE demuestra un rendimiento superior, con valores de pérdida de entrenamiento y prueba más bajos en comparación con MAE, que exhibe pérdidas significativamente más altas durante el entrenamiento. Muestra que la función de costo MSE tiene un mejor desempeño a medida que pasan las épocas de entrenamiento. A diferencia de la función de costo MAE (error absoluto medio), en la que podemos ver en la figura que, tanto la pérdida de entrenamiento como la pérdida de prueba, tienen valores mayores (valores enormes) en comparación con la función de costo MSE. Además, podemos ver que, para las primeras 20 épocas, la pérdida de prueba está por debajo de la pérdida de entrenamiento, lo que muestra un ajuste insuficiente, es decir, el modelo puede ser demasiado simple o no lo suficientemente complejo para capturar los patrones subyacentes en los datos de entrenamiento y puede que no esté aprendiendo de manera efectiva del conjunto de entrenamiento, lo que da como resultado una pérdida de prueba menor pero una pérdida de entrenamiento mayor.

En la Figura 5 se puede observar que para este cliente el mejor ajuste para los valores reales, KWh de las últimas 10 horas, es con la función de costo MSE que tiene un R^2=0.9312 y MAPE = 0.075 lo que significa un 7.5 % para este último, lo cual es un porcentaje de error bastante bueno. Para la función de costo MAE obtuvimos un R^2=0.68 y MAPE = 0.27.

5.3 Independencia entre categorías utilizando LSTM

El objetivo de este trabajo es comparar el desempeño de los modelos LSTM y QLSTM. Para lograrlo es esencial desarrollar modelos basados en predicciones para clientes individuales (para intereses comerciales) así como para grupos de clientes. A continuación se verá que ciertas categorías exhiben baja correlación empleando una técnica analítica para el análisis de series de tiempo. Esta técnica utiliza datos de una categoría como conjunto de datos de entrenamiento y datos de otra categoría como conjunto de datos de prueba. Si ambos modelos para las categorías o subcategorías muestran un desempeño sólido en términos de la función de costo (que mide la optimización de errores) y las métricas utilizadas, como R^2 y MAPE, se puede concluir que existe una correlación entre estas categorías o subcategorías.

Para todas las pruebas realizadas para diferentes subcategorías se obtuvo un buen desempeño en términos de la función de pérdida de MSE. El primer caso fue para ambos clientes de la misma categoría 1-RESIDENCIAL y subcategoría 6-ESTRATO 6. Se pueden ver en

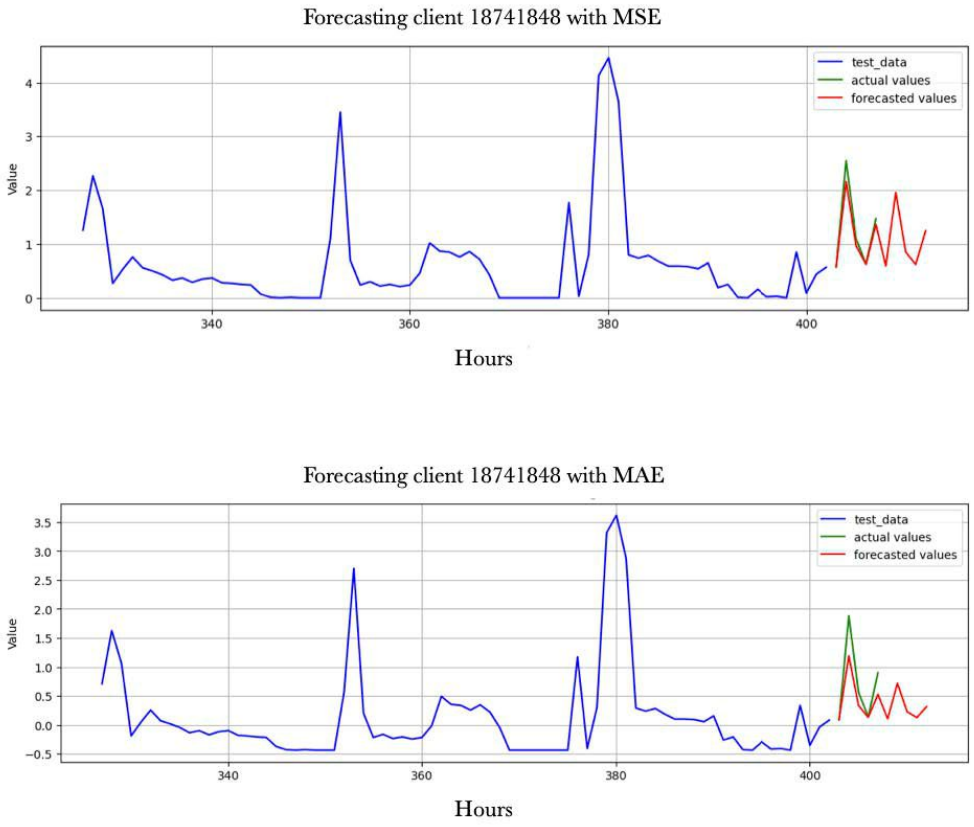


Figura 5. Pronóstico para el cliente 18741848 utilizando funciones de costo MSE y MAE.

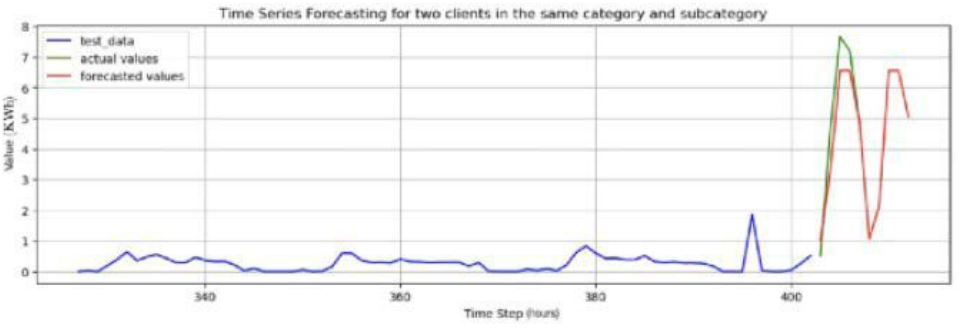


Figura 6. Pronóstico LSTM utilizando la función de costo MSE para dos clientes en la misma categoría y subcategoría

la Figura 6 los datos de entrenamiento y prueba y los valores de ACTIVA_IMP para las últimas 10 horas. Para este caso se tiene R^2=0.8865 y MAPE= 0.3028472, que son buenos resultados. Se puede inferir que los clientes de la misma subcategoría tienen un comportamiento de consumo de energía eléctrica similar.

Sin embargo, tomando dos clientes en diferentes subcategorías 6-ESTRATO 6 y 2- ESTRATO 2 los resultados son malos, como se ve en la Figura 7 con R^2= -108.014921 y MAPE=0.3261. Con un R^2 negativo podemos concluir una correlación inversa entre estos dos clientes.

La Figura 8 es la predicción del modelo LSTM con el conjunto de datos de entrenamiento para un cliente de la subcategoría 6-ESTRATO 6 y el conjunto de datos de prueba para un cliente de la categoría COMMERCIAL. Se observa una correlación incorrecta con R^2=-2.16484 y MAPE=0.2104.

La Figura 9 es la predicción del modelo LSTM con el conjunto de datos de entrenamiento para un clien-

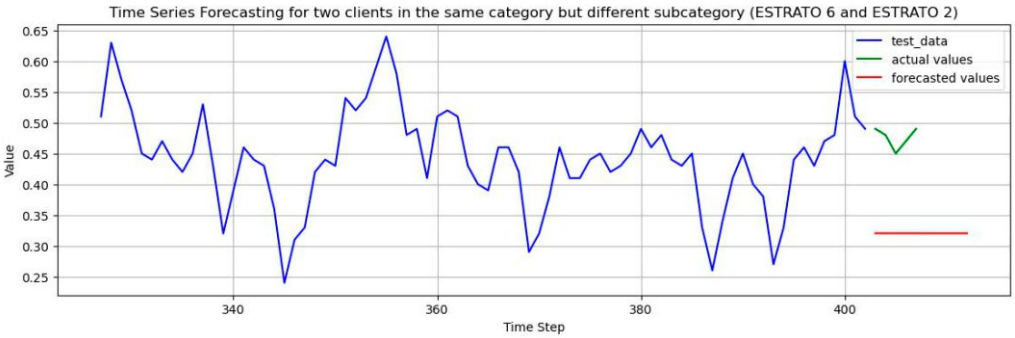


Figura 7. Pronóstico LSTM utilizando la función de costo MSE para dos clientes en la misma categoría pero en diferentes subcategorías

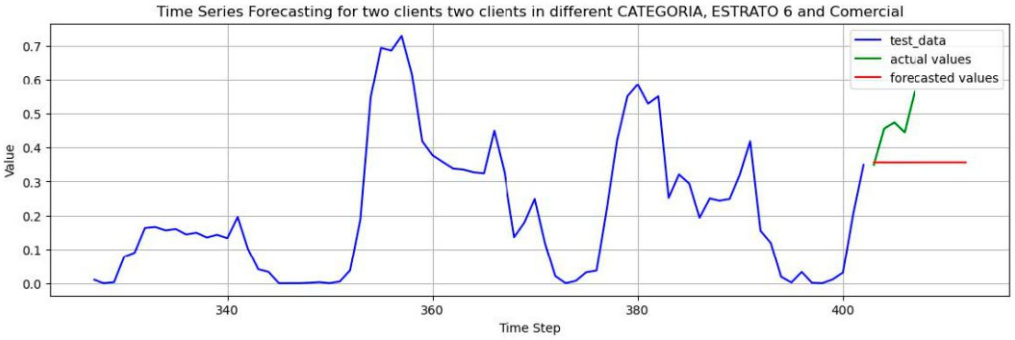


Figura 8. Pronóstico LSTM utilizando la función de costo MSE para dos clientes en diferentes categorías.

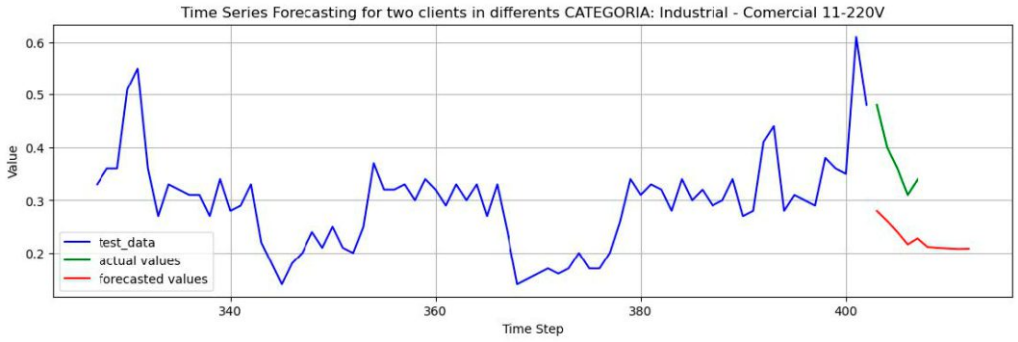


Figura 9. Pronóstico LSTM utilizando la función de costo MSE para dos clientes en la misma categoría, pero en diferentes subcategorías.

te de la subcategoría INDUSTRIAL y el conjunto de datos de prueba para un cliente de la categoría COMMERCIAL, 11-220V. Se observa una correlación deficiente con R^2=-4.4936 y MAPE= 0.3454.

5.4 Predicción con un solo cliente: LSTM vs QLSTM

El modelo evaluado para LSTM y QLSTM fue para un cliente. El cliente 18741848 fue elegido utilizando el enfoque 2 en el que se eligieron las variables más correlacionadas. Los dos modelos se tomaron con los mejores hiper parámetros descritos en la Tabla 4.

Además, los mejores hiper parámetros para la capa cuántica (hiper parámetros de los VQC) que fueron elegidos se exponen en la tabla 5.

Se trabajaron tres rotaciones de ángulos en la codificación para el embedding cuántico. La Figura 10

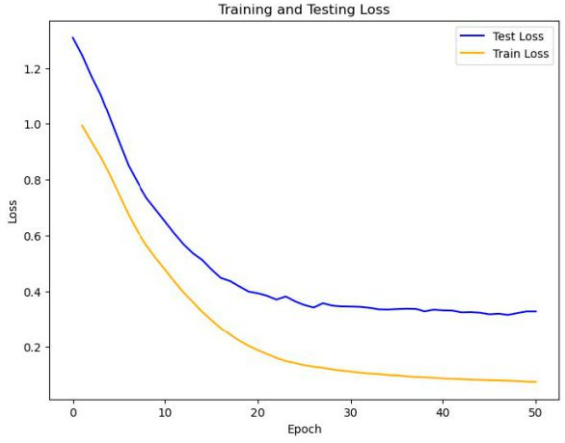


Figura 10. El rendimiento del modelo de pronóstico LSTM en términos de la función de costo MSE

Hiperparámetro	Valor
División Entrenamiento/Prueba	67% entrenamiento, 33% prueba
Longitud de Secuencia (Entrenamiento)	5
Longitud de Secuencia (Prueba)	5
Tamaño de Entrada	1
Número de Capas	4
Tamaño Oculto	52
Tamaño de Salida	1
Tamaño del Lote	1
Número de Épocas	50
Pasos de Predicción	5
Tasa de Aprendizaje	0.0001
Número de Unidades Ocultas	52

Tabla 4. Hiperparámetros

Hyperparámetro	Valor
Número de qubits	4
Rotaciones de ángulos	3
Capas cuánticas	4

Tabla 5. Hiperparámetros cuánticos

muestra el rendimiento del modelo LSTM en términos de la función de costo MSE. Las métricas de rendimiento para este modelo fueron R^2=0,8580 y "MAPE"=0,1796. El rendimiento del modelo de pronóstico LSTM en términos de la función de costo MSE muestra que la pérdida del tren a medida que las épocas avanzan en el tiempo obtiene valores más bajos, lo que muestra optimización (aprendizaje del algoritmo) y siempre está por debajo de la pérdida de prueba.

La Figura 11 muestra el desempeño del modelo QLSTM en términos de la función de costo MSE. Las métricas de desempeño para este modelo fueron R^2=0.8585 y MAPE =0.2217. En términos de la métrica de varianza, ambos modelos QLSTM y LSTM tienen los mismos resultados con los mejores hiper parámetros, pero el modelo clásico gana con un 3% en la métrica de sesgo.

El rendimiento del modelo de pronóstico QLSTMEl rendimiento del modelo de pronóstico QLSTM en términos de la función de costo "MSE" muestra que a medida que las épocas avanzan la pérdida de entrenamiento obtiene valores más bajos, lo que muestra optimización (aprendizaje del algoritmo) y siempre está por debajo de la pérdida de prueba.

En la Figura 12 y la Figura 13 muestran la comparación entre LSTM y QLSTM en términos de pérdida de entrenamiento y prueba respectivamente. De la figura 15 es posible observar cómo el modelo de pronóstico QLSTM aprende más rápido que su contraparte clásica, en la

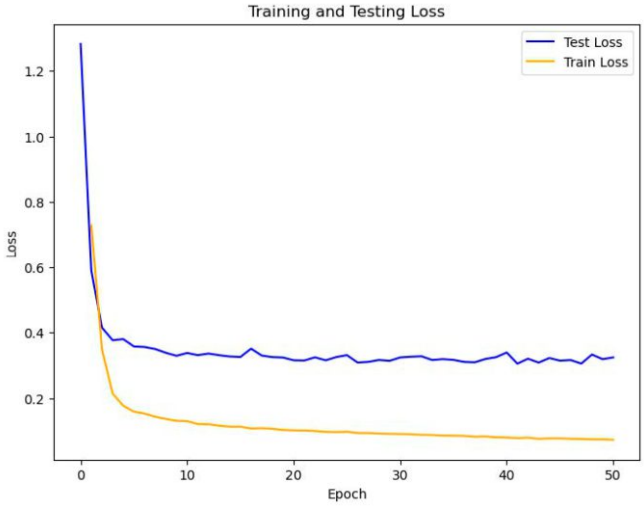


Figura 11. El rendimiento del modelo de pronóstico QLSTM

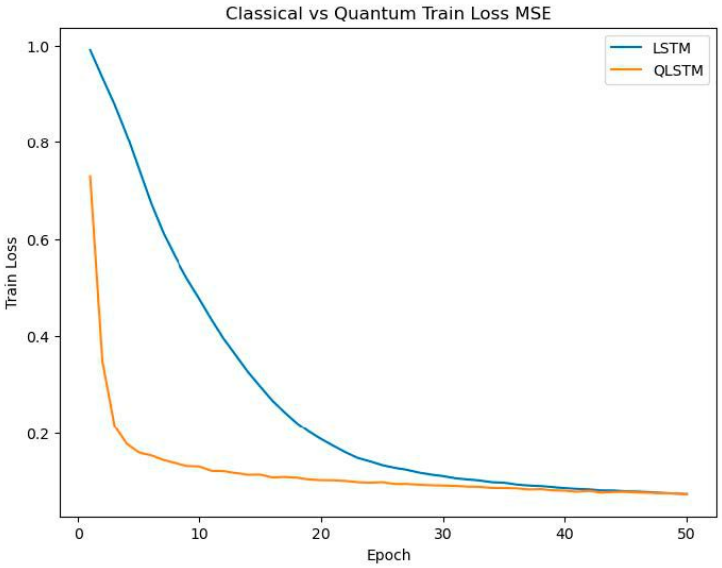


Figura 12. LSTM vs QLSTM en términos de pérdida de entrenamiento

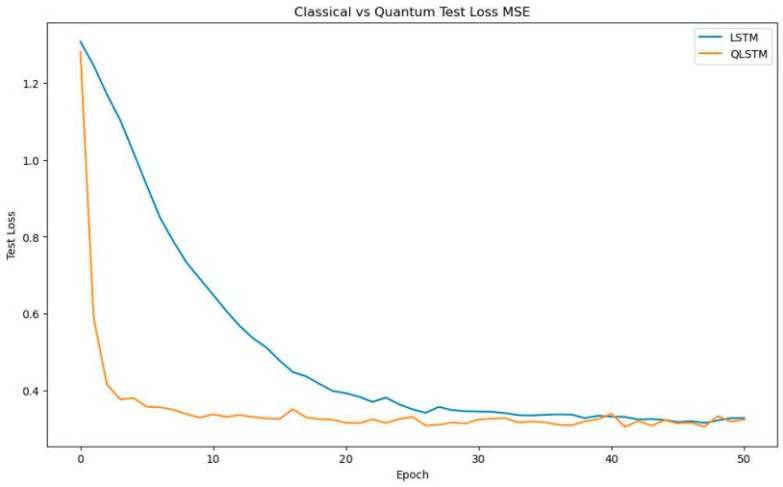


Figura 13. LSTM vs QLSTM en términos de la función de pérdida para los datos de prueba.

mitad de las épocas, aproximadamente en la época 25, la pérdida de entrenamiento tiene el mismo valor de la pérdida de entrenamiento del modelo LSTM en la época 50 demostrando cómo QLSTM, al utilizar el VQC muestra una mejor optimización en términos de la sintonización de ángulos (decidiendo qué parámetros olvidar y cuáles actualizar), que luego se utilizan en las funciones de activación de una infraestructura LSTM clásica.

En la Figura 12 se ve que el algoritmo híbrido QLSTM tiene el mismo valor de la función de pérdida de entrenamiento o función de costo MSE para los datos de entrenamiento en la mitad de las épocas.

Finalmente, la Figura 14 muestra el pronóstico para las 408 horas del consumo del medidor eléctrico (KHh) del cliente 18741848, mostrando cómo tanto el modelo LSTM clásico como el modelo híbrido cuántico tienen un buen ajuste con respecto a los datos reales.

Es importante mencionar que el número de parámetros fueron 1553 y los parámetros del QLSTM fueron 228, mostrando cómo el QLSTM es más eficiente en términos de los parámetros que debe aprender.

5.5 Resumen de los Resultados Obtenidos

Luego de implementar los algoritmos y procesarlos en máquinas clásicas y máquinas cuánticas, se obtuvieron los siguientes resultados (Tabla 6).

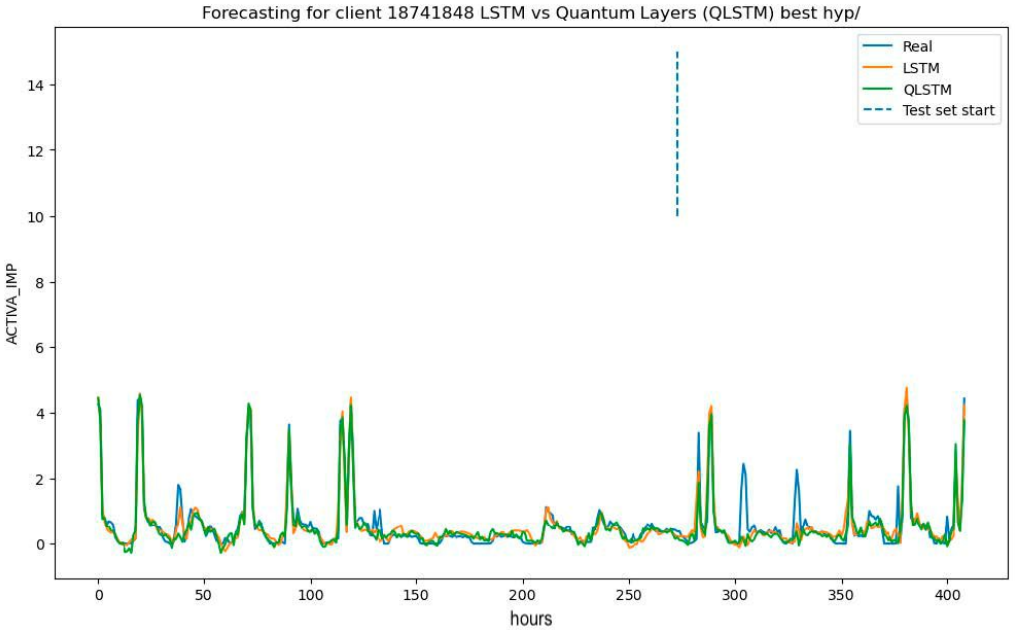


Figura 14. Predicción de ACTIVA_IMP para LSTM y QLSTM

Modelo y Tipo Computación	Características Físicas de las Máquinas Usadas	Datos Utilizados (cantidades y dimensionalidad)	Tiempo de Procesamiento promedio por época	Valores Métricas (R^2,MSE, MAPE)	Épocas	Época de convergencia
Predicción un cliente LSTM: Clásica	Máquina clásica.	Un cliente (cliente **18741848**) Dimensionalidad: 408 filas Variables/columnas: 6 ['HORA', 'I1', 'I3', 'REACTIVA_EXP', 'V1', 'V3']	0.477 segundos	R^2: 0.845 MAPE: 0.240 MSE (última época): Train loss: 0.0821 Test loss: 0.345	50	49
Predicción un cliente LSTM: Cuántica	Simulación en máquina clásica.	408 filas cliente Dimensionalidad: Variables/columnas: 6 ['HORA', 'I1', 'I3', 'REACTIVA_EXP', 'V1', 'V3']	100.05 segundos	R^2: 0.846 MAPE: 0.244 MSE (última época): Train loss: 0.066 Test loss: 0.375	50	25
Predicción un cliente LSTM: Cuántica	Máquina cuántica real: IBM sherbrooke	408 filas cliente Dimensionalidad: Variables/columnas: 6 ['HORA', 'I1', 'I3', 'REACTIVA_EXP', 'V1', 'V3']	6 segundos	Por calcular	50	Por calcular

Tabla 6 Resultados

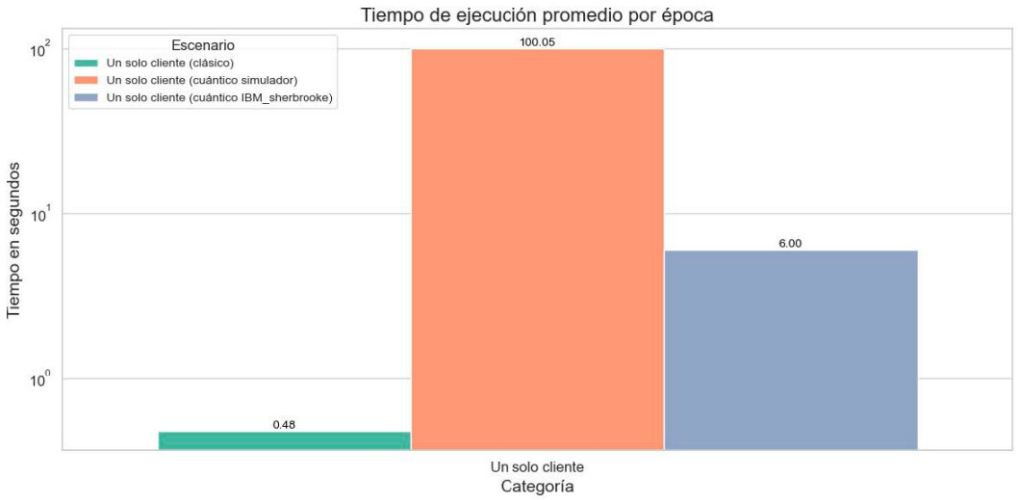


Figura 24 Tiempos de ejecución

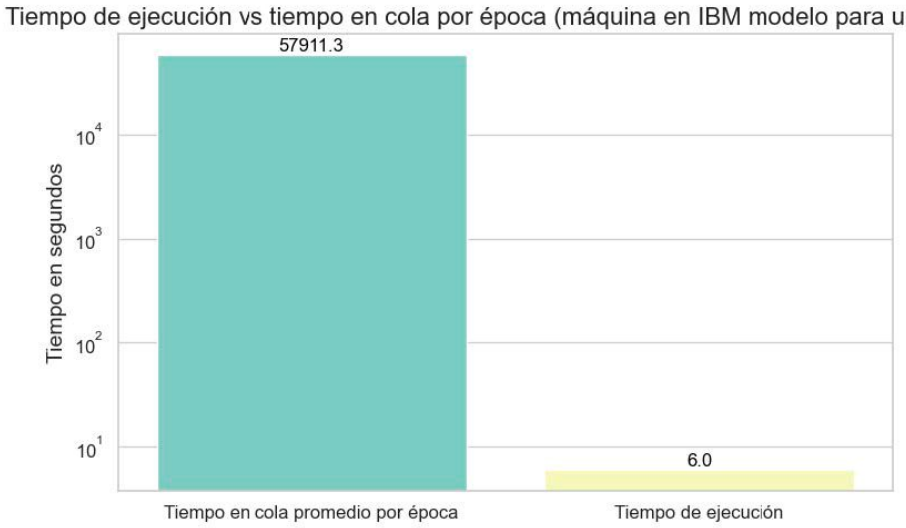


Figura 25 Tiempo de ejecución vs tiempo de espera en cola

6. Conclusiones

Durante la ejecución de esta fase del proyecto se generaron dos modelos, un modelo de aprendizaje de maquina clásico donde se implementó una red neuronal LSTM para el pronóstico de valores futuros en series de tiempo; un modelo hibrido donde se introdujeron capas de procesamiento cuántico de la información, este último se entrenó en simuladores de computación cuántica y en dispositivos cuánticos reales de IBM.

A partir de estos experimentos se llevó a las siguientes conclusiones:

- La computación cuántica abre nuevas posibilidades para pronosticar series de tiempo, al permitir obtener representaciones alternativas de procesamiento de la información.
- Los algoritmos implementados permitieron realizar pronósticos sobre las series de tiempo, produciendo resultados que se ajustan con los datos experimentales utilizados, en particular, se comprueba la pertinencia del uso de técnicas de aprendizaje de maquina cuántico para este problema de negocio.
- En los experimentos se evidencio que el algoritmo híbrido, que usa computación clásica y cuántica, converge más rápido que la alternativa clásica, necesitando menos iteraciones (épocas) para su entrenamiento, obteniendo indicadores de calidad que se comparan con los obtenidos por las técnicas clásicas.
- Es posible concluir entonces que el uso de la computación cuántica es viable técnicamente

y conduce, en algunos casos como el analizado en este experimento, a mejoras significativas en términos de eficiencia.

- Se evaluó la ejecución del algoritmo mediante simulación utilizando CPU, simulación utilizando GPU y máquinas cuánticas, analizando tiempos de ejecución, tiempos de acceso al recurso y costo de la ejecución, lo que permite concluir que la solución más viable desde el punto de vista del costo es utilizar simulación de dispositivos cuánticos empleando GPUs para realizar el entrenamiento y máquinas cuánticas para el pronóstico. De esta manera el sobretiempo para realizar el entrenamiento no impacta sobre los algoritmos de pronóstico desplegados para la inferencia de los datos, y beneficiándose de las tecnologías cuánticas.

Adicionalmente, en el desarrollo del experimento se identificaron algunos frentes de trabajo futuro en donde se evidencia las posibles ventajas de la utilización de la computación cuántica en este problema, si bien existen dificultades técnicas para su implementación, estas alternativas son viables y deberían explorarse, ya que podrían conducir a posibles ventajas competitivas:

- Implementar un modelo de entrenamiento robusto empleando modelos de ruido de las maquinas físicas, desplegando los modelos entrenados en ambientes con máquinas físicas para la inferencia y pronóstico de los datos.

- Evaluar el uso de diferentes proveedores de servicios cuánticos en la nube, reduciendo los sobretiempos de espera para el acceso a los dispositivos cuánticos.

- Evaluar estrategias alternativas en la configuración de las cargas de datos y la actualización de parámetros para facilitar el acceso oportuno a máquinas físicas.

- Evaluar otras aproximaciones, como por ejemplo redes totalmente conexas, que puedan mejorar la eficiencia o la calidad de las respuestas.

7. Referencias

1 H. K. Alfares y M. Nazeeruddin, «Electric Load Forecasting: Literature Survey and Classification of Methods,» *International Journal of Systems Science*, vol. 33, p. 3–34, 2002.

2 A. Khotanzad, E. Zhou y H. Elragal, «A Neuro-Fuzzy Approach to Short-Term Load Forecasting in a Price-Sensitive Environment,» *IEEE Transactions on Power Systems*, vol. 17, p. 1273–1282, 2006.

3 S. Arora y J. W. Taylor, «Rule-based autoregressive moving average models for forecasting load on special days: A case study for France,» *European Journal of Operational Research*, vol. 266, pp. 259-268, 2018.

4 S. Maldonado, A. González y S. Crone, «Automatic time series analysis for electric load forecasting via support vector regression,» *Applied Soft Computing*, vol. 83, p. 105616, 2019.

5 N. M. M. Bendaoud y N. Farah, «Using deep learning for short-term load forecasting,» *Neural Computing and Applications*, vol. 32, p. 15029–15041, 1 September 2020.

6 F. Javed, N. Arshad, F. Wallin, I. Vassileva y E. Dahlquist, «Forecasting for Demand Response in Smart Grids: An Analysis on Use of Anthropologic and Structural Data and Short Term Multiple Loads Forecasting,» *Applied Energy*, vol. 69, p. 15–160, 2012.

7 F. He, J. Zhou, Z.-k. Feng, G. Liu y Y. Yang, «A hybrid short-term load forecasting model based on variational mode decomposition and long short-term memory networks considering relevant factors with Bayesian optimization algorithm,» A*pplied Energy*, vol. 237, pp. 103-116, 2019.

8 M. A. R. Biswas, M. D. Robinson y N. Fumo, «Prediction of residential building energy consumption: A neural network approach,» *Energy*, vol. 117, pp. 84-92, 2016.

9 K. Amarasinghe, D. L. Marino y M. Manic, «Deep Neural Networks for Energy Load Forecasting,» de *Proceedings of the 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE)*, Edinburgh, 2017.

10 W. Kong, Z. Y. Dong, Y. Jia, D. J. Hill, Y. Xu y Y. Zhang, «Short-Term Residential Load Forecasting Based on LSTM Recurrent Neural Network,» *IEEE Transactions on Smart Grid*, vol. 10, pp. 841-851, 2019.

11 M. Cerezo, G. Verdon, H. Y. Huang, L. Cincio y P. J. Coles, «Challenges and opportunities in quantum machine learning,» *Nat Comput Sci*, vol. 2, p. 567–576, September 2022.

12 D. Maheshwari, B. Garcia-Zapirain y D. Sierra-Sosa, «Quantum Machine Learning Applications in the Biomedical Domain: A Systematic Review,» I*EEE Access*, vol. 10, p. 80463–80484, 2022.

13 S. Y.-C. Chen, S. Yoo y Y.-L. L. Fang, «Quantum Long Short-Term Memory,» de *ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2022.

14 Y. Yu, G. Hu, C. Liu, J. Xiong y Z. Wu, «Prediction of Solar Irradiance One Hour Ahead Based on Quantum Long Short-Term Memory Network,» *IEEE Transactions on Quantum Engineering*, vol. 4, pp. 1-15, 2023.

15 I. Goodfellow, Y. Bengio y A. Courville, Deep Learning, MIT Press, 2016.

16 C. C. Aggarwal, Neural Networks and Deep Learning: A Textbook, 1 ed., Springer Cham, 2018, pp. XXIII, 497.

17 R. Disipio, *QLSTM Implementation in PennyLane*, 2023.

18 D. Dulal, *Data Collection Notebook for SoftServe QLSTM*, 2023.

19 GeeksforGeeks, *Time Series Forecasting Using PyTorch*, 2023.

20 B. Kent, *How to use PyTorch LSTMs for time series regression*, 2021.

Computación cuántica

DOI: 10.29236/sistemas.n173a5

Daniel Sierra Sosa y Juan Guillermo Lalinde Pulido, editores técnicos, fueron los moderadores del encuentro.

Antes de abordar el temario a tratar, cada uno de los invitados hizo un breve resumen de su trayectoria profesional:

Alberto Maldonado, doctorado del Centro de Investigación en Computación del Instituto Politécnico Nacional (CIC IPN) de México; Qiskit Advocate @ IBM Quantum; | Mentor @ QOSF Mentorship Program and Womanium in quantum; | Ambassador @ Unitary Fund y| Admin @ Quantum Universal Education.

Diego Emilio Serrano, Director de Ingeniería en Panasonic, USA, Promotor y divulgador de la computación cuántica por diversos medios, incluido su propio canal en YouTube.

Y Gonzalo Mejía Jaramillo, EPM, Medellín, Colombia. Arquitecto de TI que lidera el proyecto de utilización de Computación Cuántica para detectar *outliers* en telemedidas.

Juan Guillermo Lalinde
¿Qué relación tiene con la computación cuántica en su trabajo? ¿En su desarrollo profesional?

Alberto Maldonado
En cualquiera de mis actividades diarias hago uso de la computación cuántica. Organizando eventos,

dictando charlas y en revisorías técnicas. Mi tesis es sobre Quantum Machine Learning, asuntos sobre los que giran mis proyectos. Se trata de abordar problemas de Quantum Machine Learning, Quantum Optimization, y Quantum Chemistry aplicadas a hardware. En la actualidad también soy asesor de alumnos de maestría.

Diego Serrano

En Panasonic, estamos explorando cómo aplicar la computación cuántica al desarrollo de materiales para baterías, adicionalmente estamos investigando algunos proyectos en el desarrollo de hardware cuántico. Estoy mirando cómo usar la computación cuántica en el desarrollo de materiales para baterías, además de invertir tiempo en unos proyectos de hardware.

La comunicación entre la interfaz que el usuario utiliza para programar y el chip con los qubits que procesan los algoritmos cuánticos es clave en estos proyectos. A nivel personal, también estoy evaluando ideas similares a las que mencionó Alberto. De hecho, Alberto lidera un programa interesante llamado Quantum Open Source Foundation, donde estudiantes y mentores colaboran en mini proyectos beneficiosos para ambas partes. Estoy considerando participar en uno de esos proyectos, aunque no he tenido mucho tiempo.

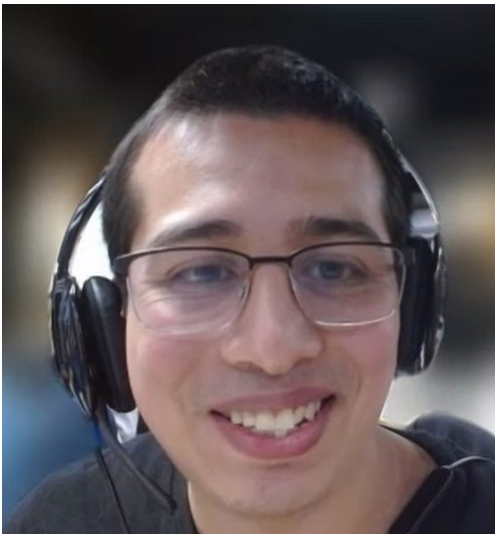
Gonzalo Mejía

En nuestra empresa mantenemos la práctica de monitoreo del entorno tecnológico, entonces hemos iniciado un experimento de computación cuántica para analizar medidas o consumos de medidores de energía eléctrica. Actualmente hay cierta cantidad de medidores que se acceden remotamente mediante telemedida, de ese universo de medidores tomamos unos 1.800 y consideramos alrededor de 2.700.000 de registros de consumo, la idea es hacer una comparación enfocada en encontrar las diferencias que hay al utilizar algoritmos clásicos versus algoritmos cuánticos. ¿Que es lo que nosotros queremos comprobar en el experimento? Saber si se logran mejoras en tiempos de procesamiento, o se logran mejoras en la calidad de las estimaciones. Con este experimento buscamos hacer la comparación con un tema real, basado en un asunto de negocio, no imaginando datos. Hicimos un equipo de trabajo, con ex-

pertos en ese tema en el tema de computación cuántica e inteligencia artificial, y con el apoyo de la Universidad EAFIT vimos que si era si era posible y aprovechando con un convenio que tenemos con varias universidades y bajo la sombrilla de ese convenio hicimos un acuerdo ya de trabajo específico para abordar el experimento. Ya tenemos algunas conclusiones y ha sido de mucha utilidad internamente para los directivos nuestros y para los lideres de los procesos.

¿Cómo llegó al mundo de la computación cuántica? ¿Por qué considera que la computación cuántica es importante?

Alberto Maldonado



En mi opinión es importante en muchos aspectos, para procesos complejos como la química y la optimización, y el aprendizaje de máquina.

Para mí, la importancia de la computación cuántica es que podemos ver una perspectiva diferente de la computación y resolver problemas complejos y eso se me hace muy interesante. Yo lo he vivido en la academia como estudiante, siempre está la pregunta de ¿cuál es el beneficio de estudiar geometría, trigonometría? y ahora además computación cuántica?

En términos de recursos el avance nos está dando una ventaja, toda vez que las capacidades de los procesadores lo facilitan. Existe mayor naturaleza en trabajar con circuitos o algoritmos cuánticos, en el momento de codificar algunos problemas. Es más cómodo hacerlo en un circuito cuántico que tratar de ejemplificarlo con una computadora con GPUs.

Diego Serrano

Hay dos aspectos importantes que destacar sobre la computación cuántica.

Primero, la computación cuántica puede ser una herramienta poderosa para enseñar conceptos complejos en física. Para ingenieros como yo, es más intuitivo programar un computador cuántico que intentar implementar experimentos físicos complejos en un laboratorio, como trabajar con partículas, fotones o láseres. En lugar de enfrentarse a las complicaciones técnicas de un laboratorio, uno puede simplemente escribir código en su computador, ejecutarlo en un com-

putador cuántico real, y analizar los resultados. Esto facilita la comprensión de fenómenos físicos de manera más accesible y práctica, lo que considero extremadamente valioso.

Segundo, está demostrado que ciertos algoritmos son significativamente más eficientes en un computador cuántico que en uno clásico. Esto abre un abanico de oportunidades en campos como la optimización, el desarrollo de materiales, y la creación de compuestos químicos. Por ejemplo, en empresas como Panasonic estamos explorando cómo aprovechar esta tecnología para acelerar estos procesos de manera exponencial.

Aunque aún no podemos implementar estas aplicaciones a gran escala, el potencial es enorme. Por esta razón, las universidades de todo el mundo deberían comenzar a enseñar estos temas, ya que representan una oportunidad transformadora para el futuro.

Gonzalo Mejía
La importancia de la computación cuántica yo la veo en temas más complejos de la humanidad, que para el mundo empresarial. Por ejemplo, en los viajes espaciales, en la astronomía, áreas en las que la computación clásica no puede resolver. Así mismo en asuntos de la medicina, sobre todo en lo relacionado con los medicamentos, vacunas, etc. Basta observar lo sucedido en la pandemia período en el que nos parecía una eternidad encontrar una vacuna. Así mismo, en lo relacionado con el medio ambiente, hay que ir más allá de quemar combustibles. Esto se resuelve con otras tecnologías, otras estrategias, otras prácticas y me parece que la computación cuántica es una buena herramienta para eso.

A nivel personal, yo me voy mucho al mundo de la ciencia ficción, y uno ve que todas esas cosas que uno veía en las películas de los años 80 y 90 son hoy una realidad, por ejemplo, el uso de un celular, o el hacer una conversación con imagen en tiempo real, cosas que uno en esos años lo veía como imposible. Cosas como por ejemplo la teletransportación de objetos o personas, este ir de un planeta al otro planeta como si estuviera yendo de una ciudad a otra, cosas de ese estilo creo que unos años la computación cuántica podría ayudar a que eso sea posible.

Juan Lalinde
¿Cuáles fueron (o son) las principales dificultades que ha encontrado en su proceso de acercarse a la computación cuántica?

Alberto Maldonado
En mi primer acercamiento a esta área no sabía lo que estaba haciendo. En este contexto, el hecho de que alguien te diga "vas bien" o "vas mal" puede ser un verdadero privilegio, especialmente en áreas nuevas como esta.

Cuando decidí estudiar computación cuántica, me surgieron muchas dudas. Como me dijo un amigo una vez: "¿Y qué pasa si lo que entendiste está mal? ¿Qué tal si no era de esa manera?" Esa pregunta me dejó pensando y sembró una inquietud en mí. Imaginé el escenario: estar en mi examen de grado y que me dijeran que había malinterpretado todo, que no era posible lo que planteaba. Esto me llevó a reflexionar y no limitarme a lo que hacía, sino a buscar todos los recursos posibles para validar mi trabajo. Quería que alguien con más experiencia me dijera si estaba en el camino correcto.

Fue en una escuela de verano donde finalmente encontré ese respaldo. Ahí comprendí la importancia de conocer a alguien que pueda orientarte, decirte si vas bien, si te gusta lo que haces, cómo corregir errores y cuáles son las referencias adecuadas. Durante este proceso, aprendí mucho utilizando el *Qiskit Textbook*, y de ahí encontré otros libros, como el de Nielsen & Chuang. Curiosamente, no pasé por el famoso proceso del "Hola Mundo" que muchos mencionan. Para mí, ese "Hola Mundo" fue experimentar directamente con *Qiskit Composer* y jugar con sus herramientas, preguntándome: "¿Por qué hace esto?" y "¿Por qué hace aquello?". Estudiar de forma empírica es un proceso muy tardado y complejo.

Además, encontrar personas que hablen español en esta área resulta complicado, especialmente viniendo de un país como México. Curiosamente, siento que conozco a más colombianos que mexicanos en este ámbito. De hecho, irónicamente, de todos los amigos que he conocido en línea, he llegado a conocer más colombianos en persona que mexicanos, y eso que estamos en el mismo país. No sé cómo funciona esto, pero incluso encontrar a alguien en este "mundo cuántico" es un evento raro. Es como si no estuviéramos tanto en el quantum, sino más bien en macrocosmos.

Diego Serrano

Estoy de acuerdo con Alberto en que hacen falta recursos en español sobre computación cuántica. Es difícil encontrar información accesible en este idioma, lo que complica el aprendizaje para quienes no dominan el inglés técnico.

Otro aspecto desafiante para mí fue entender los conceptos básicos necesarios para comenzar en este campo, ya que la computación cuántica requiere conocimientos en áreas que no siempre se aprenden en ciertas carreras. En mi caso, estudié Ingeniería Electrónica y tomé una clase de álgebra lineal durante la universidad, pero no llegué a profundizar en el tema. Al adentrarme en la computación cuántica, me di cuenta de que tenía muchas carencias, especialmente en álgebra lineal y números complejos. Aunque los números complejos se usan bastante en ingeniería elec-

trónica, en computación cuántica se aplican de una manera diferente, lo que requiere adaptarse a nuevos enfoques.

Creo que para quienes tienen experiencia en áreas como Machine Learning o Inteligencia Artificial, tal vez sea más fácil adquirir estos fundamentos. Sin embargo, para personas de otras disciplinas, comenzar en computación cuántica puede ser difícil debido a la falta de conocimientos básicos esenciales. Por ejemplo, conceptos como matemáticas modulares, fundamentales en algoritmos como el de Shor, o temas avanzados de álgebra lineal aplicados en algoritmos como el de Grover, no suelen enseñarse en profundidad en muchas universidades.

Por ello, cualquier universidad o institución que quiera enseñar computación cuántica debería enfocarse primero en desarrollar el aprendizaje de estos fundamentos matemáticos. Sin esta base, es fácil sentirse abrumado y retrasar el progreso en el campo. Personalmente, esta falta de preparación básica fue el principal obstáculo que enfrenté al adentrarme en la computación cuántica.

Gonzalo Mejía
En este tema los conceptos básicos definitivamente son esenciales y en nuestro caso que llevamos más de 30 años en el mundo de la informática clásica es todavía mucho más complejo porque aparte de que uno no tiene conceptos de mecánica cuántica, y toda esa fundamentación matemática debe salirse de lo que tradicionalmente hace.

Yo me acuerdo de las primeras conversaciones con Juan Guillermo, donde le preguntaba: "¿qué sistema operativo se? ¿Qué lenguaje? ¿Qué base de datos?" Poco a poco fui entendiendo que el estado actual de la computación cuántica no es comparable con la computación clásica. Nos han dicho que la computación cuántica está más o menos en el nivel donde estaba la computación clásica en los años 1950. Entonces, trato de imaginarme en esa época: una persona en una empresa, manejando una nómina o un sistema comercial, y que le hablen de un computador. Seguramente no entendía para qué servía eso. Es decir, entender qué necesidad puede resolver una máquina de computación cuántica hoy en día no es sencillo.

Eso es algo que nos ha costado a nosotros también. Por ejemplo, cuando nuestros directivos o superiores nos preguntan: "Bueno, ¿y qué problema resolvería en nuestra empresa un algoritmo cuántico? ¿Una máquina cuántica?" A veces cuesta responder a esa pregunta. Creo que es una de las grandes dificultades. Además de los conceptos básicos, está el reto de entender qué problemática empresarial se puede abordar hoy con esta tecnología, porque la computación

cuántica todavía está en un mundo muy experimental y de desarrollo.

Yo trato de dividir esto por niveles: una capa física, una capa de sistemas operativos o firmware, una capa de datos, una capa lógica o de software. En la computación clásica, ya estamos trabajando en esas capas superiores. Un ingeniero de sistemas no necesita entender los componentes físicos de una máquina; interactúa con ella a través de un sistema operativo o software.

En cambio, en la computación cuántica, estamos en el nivel físico, manejando puertas lógicas y conceptos que son muy complejos. Esto es algo que desconcierta porque, en la computación clásica, nunca tuvimos que hacerlo. Entonces, adaptarse a este enfoque y comprender por qué es necesario hacerlo en la computación cuántica es un desafío enorme.

¿Es posible trabajar con computación cuántica en Colombia y en América Latina?

Gonzalo Mejía
Yo trato de hacer una distinción. La pregunta fue: ¿es posible que nosotros podamos ayudar a desarrollar y hacer avanzar más la computación cuántica? Ahí es donde uno sí lo duda, especialmente en un país como Colombia o en América Latina.

Ahora bien, si me preguntan si podemos estar ahí como usuarios, como personas o entidades que adopten todo lo que se está descubriendo alrededor de la computación cuántica, ahí sí no tengo ninguna duda. ¡Claro que sí! Es algo que tenemos que hacer, y entre más rápido adoptemos esa tecnología, mejor nos va a ir y más provecho le vamos a sacar.

Sin embargo, hay que poner sobre la mesa otra situación: en América Latina, los presupuestos que los gobiernos asignan para temas de innovación y desarrollo son mínimos, y las estrategias en torno a la innovación no son claras ni están bien divulgadas. Esto dificulta muchísimo pensar que vamos a ser actores de primera línea en el desarrollo o avance de esta tecnología.

Pero lo que sí podemos hacer es mantenernos monitoreando, estudiando, aprendiendo, y observando cómo se aplica esta tecnología. De esa forma, estaremos listos para adoptar tempranamente todo lo que venga y aprovechar al máximo las oportunidades.

Alberto Maldonado
Ok, yo he tratado de organizar eventos en Latinoamérica, y al menos sé que en Uruguay existe la empresa *QuantumSouth*, que está trabajando en esta área. En Perú tienen el equipo *Quantum* haciendo cosas interesantes, y en Brasil también hay iniciativas. Pero, en general, las situaciones nos permiten avanzar gracias a la globalización y el internet, ya que muchas cosas

sobre computación cuántica se pueden hacer de forma remota.

El problema surge cuando hablamos de obtener un beneficio, especialmente monetario. ¿Alguien realmente nos va a pagar por aprender esto? Es algo complejo, porque llegar con una idea y convencer a alguien de que esto no es *Skynet* ni va a dominar el mundo es todo un reto. Además, explicar que la computación cuántica tiene beneficios reales y no solo implica riesgos futuros también puede ser contraproducente. Entonces, pensar en recibir beneficios tangibles por esto sigue siendo complicado.

Al menos en la academia se ha dado un pequeño paso, pero en la industria es mucho más complejo. Recuerdo que estuve en un bootcamp en Canadá sobre el estado de la computación cuántica, y todo el panorama es como un campo de batalla: ciberseguridad, software, hardware, todos quieren hardware, todos quieren competir. Están Google, IBM, y otros gigantes luchando por liderar, mientras uno apenas sobrevive día a día con su sueldo. Pensar en competir con estos titanes y que alguien invierta millones de dólares para crear una computadora cuántica que compita con IBM o Google parece un sueño distante.

Creo que el principal problema son las oportunidades. Incluso en Estados Unidos no es tan viable como parece. No todos están detrás de la computación cuántica, y lograr que alguien crea en tu idea y te apoye financieramente es complicado. Sin embargo, creo que algo más accesible es iniciar ayudando a otras personas en otros países, generando colaboración. Crear mi propia startup en países como México, Colombia o Venezuela es un desafío enorme. En Canadá todavía hay oportunidades, pero cuando hablamos del sur, ahí sí se vuelve mucho más complicado.

Diego Serrano

Creo que definitivamente es posible trabajar en computación cuántica en Colombia. Como menciona Alberto, gracias al internet tenemos acceso a computadores cuánticos, lo que abre muchas oportunidades. Además, estamos en un punto del desarrollo de esta tecnología en el que las aplicaciones prácticas aún no existen completamente. Aunque hay ideas sobre cómo usar la computación cuántica para resolver problemas más rápido, la realidad es que los computadores cuánticos actuales presentan muchos errores, lo que limita su aplicación inmediata.

La mayoría del trabajo en computación cuántica hoy en día se concentra en dos áreas principales: el desarrollo de hardware y el desarrollo teórico y académico. El desarrollo de hardware, por su naturaleza, es extremadamente complejo en países como Colombia debido a los recursos inmensos que requiere. Sin embargo, el desarrollo teó-

rico y académico, como la creación de nuevos algoritmos, es igual de importante y puede realizarse desde cualquier parte del mundo, incluyendo Colombia.

Desde un punto de vista académico, hay oportunidades claras que pueden aprovecharse con los recursos disponibles. En cuanto a la parte más aplicada, incluso en países desarrollados el avance es limitado por las condiciones actuales de la tecnología. Sin embargo, esto cambiará con el tiempo. Si países como Colombia comienzan a invertir en educación y en el desarrollo teórico, podrían competir a cierto nivel una vez los computadores cuánticos sean más prácticos y ampliamente utilizables.

Juan Lalinde

¿Qué le recomienda a las personas interesadas en la computación cuántica?

Gonzalo Mejía

Alguien interesado en aplicar la computación cuántica tiene que empezar entendiendo que esto no es un tema para involucrarse por moda. Es imposible que, por seguir una tendencia, uno logre entender, usar, y sacar provecho de la computación cuántica. Si alguien lo aborda sin un propósito claro, lo más seguro es que termine gastando tiempo y recursos en vano.

Yo creo que es fundamental tener muy claro para qué sirve la computación cuántica, qué problemáticas puede resolver. Por ejemplo, uno no puede pretender que, si en mi empresa tengo problemas porque la nómina es lenta para hacer los pagos, simplemente voy a comprar una máquina cuántica, pagarle a alguien para que me haga un algoritmo, y problema resuelto. Eso no es así.

Entonces, lo primero es entender para qué sirve y de dónde viene. Si esto proviene de la física cuántica y las teorías de grandes científicos del siglo XX, hay que empezar por comprender al menos un poco esos fundamentos.

Una vez entendido eso, hay que preguntarse: ¿qué tipo de problemas puede resolver la computación cuántica? Y, solo entonces, decidir si vale la pena involucrarse.

Es clave evaluar si se tienen la motivación, los conocimientos básicos, y la capacidad para avanzar en este campo. Si no se tienen esos

conocimientos, lo primero es empezar a adquirirlos. Pero lo que considero más importante es entender en qué escenarios, situaciones, o casos de uso la computación cuántica es realmente relevante. De lo contrario, creo que los esfuerzos pueden terminar siendo en vano.

Alberto Maldonado

Yo creo que el mayor limitante es la palabra "cuántica", que nos da miedo a todos. Creo que es importante quitarle ese peso o perspectiva intimidante. Como dijeron antes, se puede aprender desde cualquier lugar. Por ejemplo, yo ni siquiera sabía qué era una notación de sombra, apenas me acordaba de lo básico sobre vectores y matrices, y ahora estoy jugando con eso.

La situación, en mi opinión, es no esperar un tiempo fijo, como pensar que en un año ya voy a hacer algo grande o ser alguien importante en la comunidad. Lo más importante es aprender. Algo que me ha gustado mucho es que hay conceptos correlacionados. Por ejemplo, el *Machine Learning* y la computación cuántica tienen puntos en común, al menos en la parte de álgebra. En algunos aspectos, son muy similares.

Si quieres trabajar en optimización cuántica, necesitas ser experto en optimización clásica y luego aplicar ese conocimiento a la cuántica. Es como pasar al "volumen 2". Primero aprendes computación clásica, y luego aplicas una nueva versión con la cuántica. Es un proceso que puede ser divertido, pero no sucede de la noche a la mañana. No somos Iron Man o Tony Stark, que se vuelven expertos en una noche.

Aquí, las cosas toman tiempo: te desvelas, estudias, y quizás después de un año o dos logras entender qué funciona.

El punto es que la perspectiva es diferente. A veces incluso parece más fácil aprender computación cuántica sin saber nada de computación clásica o física cuántica, porque no te cuestionas tanto. No te rompes la cabeza preguntándote: "¿Cómo es esto posible?" o "¿Por qué aquí sí sirve y allá no?"

Creo que se trata de tener una perspectiva diferente y enfocarse en el aprendizaje. Y, al final, si no te gusta la computación cuántica, al menos te vuelves experto en otra área. Eso es lo que siempre les digo a mis alumnos: "¿Te gusta *Machine Learning*? Pues mira, aquí puedes trabajar con *reinforcement learning* y luego aplicar un enfoque cuántico. ¿No te gusta la cuántica? Al menos ya eres experto en *reinforcement learning*."

Creo que ese es el aspecto positivo: mientras aprendes computación cuántica, puedes convertirte en experto en una o dos áreas relacionadas. Y si además logras combinar ambas y crear algo nuevo, entonces ya la hiciste.

Diego Serrano
Yo estoy de acuerdo con esa perspectiva porque incluso cuando uno aprende los algoritmos cuánticos, para hacer la comparación uno tiene que aprender los clásicos entonces se vuelve uno también experto en el campo del desarrollo de algoritmos clásicos óptimos.

Juan Lalinde
¿Cuál creen que debería ser la estrategia para desarrollar las capacidades en computación cuántica?

Alberto Maldonado
Yo creo que la situación no es esperar a que venga una empresa a decirnos: "Este es el resultado" o "Esta es la computadora, sigue este proceso". Más bien, se trata de iniciar en cualquier momento, es decir, empezar ahora, especialmente con los jóvenes en la universidad. Por ejemplo, esta mañana tuve que dar una plática sobre computación cuántica a un grupo. Ellos ya están estudiando estos temas, pero como tópicos selectos, no porque lo hayan elegido, sino porque se lo asignaron.

Lo interesante es que, aunque sea de forma muy básica, van aprendiendo. No como uno esperaría, pero sí van entendiendo. Creo que a los jóvenes les resulta más fácil captar estos conceptos. El problema es que para los adultos, ya sea de mediana edad o mayores, es mucho más complicado. Por eso creo que vale la pena apostar por estos jóvenes, que pueden superar barreras que a nosotros nos parecen insalvables. Es algo positivo porque demuestra cómo la tecnología nos está rebasando constantemente.

Hoy en día, por ejemplo, ya uso más *ChatGPT* que el año pasado. La tecnología siempre nos reta, pero al mismo tiempo nos impulsa. Con la computación cuántica, creo que la ventaja está en enseñar que existe. No se trata de prometerles que habrá un trabajo seguro, pero al menos sembrar la semilla desde la licenciatura.

De hecho, ya existen iniciativas como *Qubit by Qubit*, que apoya a jóvenes desde la preparatoria, o *Womanium Quantum* y *QWord*, que también ofrecen beneficios. *Quantum Open Source Foundation* respalda a personas desde los 15 o 16 años hasta adultos de más de 50.

Recuerdo una plática de la *IEEE Quantum Education Initiative* donde mencionaban algo clave: "Nosotros ya estamos viejos, pero queremos que las nuevas generaciones se interesen en esto. Si no, esta tecnología se quedará sin impulso y podría morir". Este miedo no es exclusivo; también lo comparten en Estados Unidos.

Por eso, creo que la perspectiva debe ser enseñar computación cuántica a las nuevas generaciones, no para que se conviertan en expertos de inmediato, sino para despertar su curiosidad. Que vean

que, aunque no encuentren un trabajo directamente relacionado, al menos habrán aprendido algo valioso, como física o computación. Si logran entrar en la cuántica, excelente; si no, igual tendrán una base sólida en otras áreas.

Personalmente, cuando experimenté con el *Quantum Computing Composer*, me pareció muy sencillo. Estaba programando con bloquecitos, como si fuera un juego de LEGO. Ese enfoque me ayudó a entenderlo y me quitó el miedo. Creo que esa es la clave: desmitificar la complejidad de la computación cuántica. No es ciencia ficción; es una oportunidad accesible para todos.

Diego Serrano

Sí, estoy completamente de acuerdo con lo que mencionó Alberto: el desarrollo de la computación cuántica debe comenzar desde el sector académico, probablemente en las universidades. Por ejemplo, en mi caso particular, durante mi último año de universidad, tomé una clase electiva sobre circuitos integrados.

En ese momento, era algo completamente nuevo para mí. Hasta entonces, todos los circuitos que había trabajado eran a nivel de componentes, probándolos en el laboratorio.

Esa clase, dictada por un profesor que decidió introducir el tema, cambió completamente el rumbo de mi carrera. Con una sola materia, logré desarrollar toda mi trayectoria profesional a partir de ese punto. Esto demuestra que algo tan sencillo como una electiva en computación cuántica podría despertar la curiosidad de los estudiantes. Es un primer paso que permitiría identificar quiénes están interesados y, con el tiempo, expandir esta iniciativa dentro de las universidades.

Eventualmente, esta semilla sembrada en el ámbito académico podría extenderse al campo empresarial, abriendo nuevas oportunidades en el desarrollo y la aplicación de la computación cuántica.

Gonzalo Mejía

Yo, de pronto, me alejo un poco del campo educativo cuando me pongo a pensar en cuál debería ser la estrategia de un país. Me imagino en la posición de una empresa de utilities, como en nuestro caso, o de una empresa de manufactura, o cualquier otra en el mundo empresarial. Y digo que lo primero es preguntarse: ¿el Estado, el país, tiene una estrategia de innovación y tecnología? ¿Tiene realmente una estrategia bien definida en este ámbito?

Si no la tiene, es fundamental crearla y, sobre todo, divulgarla, porque muchas veces creo que estas estrategias existen, pero no se comunican adecuadamente. Ahora bien, si el Estado tiene una estrategia, lo siguiente es preguntarse: ¿hay presupuesto? Porque sin recursos esto no funciona. Y si hay

presupuesto, entonces: ¿hasta dónde alcanza para llegar a las empresas?

En el caso de Colombia, por ejemplo, está el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y también el Ministerio de Ciencia, Tecnología e Innovación. Sin embargo, creo que mucha gente ni siquiera sabe que este último existe. Ese ministerio, en particular, debería velar por que haya una estrategia nacional clara, que existan los recursos necesarios y un presupuesto asignado.

Aunque sabemos que ese presupuesto seguramente no será suficiente, es aquí donde se vuelve clave pensar en qué acciones se pueden tomar para llegar a las empresas y universidades. Es necesario fomentar la integración entre la empresa privada, las universidades y el gobierno. No necesariamente el gobierno tiene que aportar todos los recursos, pero sí debe convertirse en un promotor activo de la estrategia.

Si logramos tener una estrategia clara, un promotor que la divulgue y un presupuesto que puede ser público o privado, creo que se puede avanzar mucho en esta área.

Es crucial darle importancia a la divulgación: divulgar la estrategia, promover proyectos asociativos, e integrar diferentes actores, no solo privados ni exclusivamente gubernamentales, sino una combinación. Creo que esa debería ser la estrategia de país: una estrategia que una esfuerzos, promueva la colaboración, y garantice que tanto el sector público como el privado trabajen hacia un objetivo común.

Daniel Sierra-Sosa
Cada uno de ustedes tiene un rol diferente y está en un momento diferente de su carrera profesional.

Gonzalo: *¿Como debemos prepararnos para la adopción de estas tecnologías de cara al futuro? ¿como ves el futuro?*

Gonzalo Mejía
Bueno, sí, creo que primero debemos, como decimos por acá, "asincerar" nuestras expectativas. Pensar que una empresa privada en el contexto colombiano pueda ponerse en la tarea de competir con IBM, Microsoft, Google o Amazon en el desarrollo de la computación cuántica no es el camino. Yo insisto en que el camino está en la **adopción temprana**: en aprender, estudiar, y encontrar cómo aplicar y aprovechar los avances de esta tecnología.

Pienso que nuestro rol está más enfocado en ser usuarios y adoptadores de la tecnología cuántica, en lugar de fabricantes de máquinas o desarrolladores de infraestructura. Lo que hacen, por ejemplo, las universidades como la Universidad FIIRD, y todos ustedes que están en el mundo académico, es clave. Es el primer paso: que haya gente

que esté aprendiendo, que sepa para qué sirve esta tecnología y cómo utilizarla. Eso es fundamental, y la empresa privada debe entenderlo.

Por eso vuelvo a insistir en lo que mencioné antes: la idea es que la empresa privada trabaje de la mano con las universidades y el gobierno en proyectos conjuntos. Esa colaboración puede ser el motor para impulsar la adopción y aplicación de la computación cuántica.

En cuanto a posibles escenarios, creo que la clave está en identificar problemas que la computación clásica no puede resolver de manera eficiente o que son demasiado costosos. Muchas empresas tienden a pensar solo en tecnologías que soporten sus procesos empresariales actuales, como sistemas de facturación o gestión humana. Esos problemas ya están resueltos con la tecnología actual: almacenamiento es accesible y barato, procesamiento ni se diga.

La clave está en identificar esos **escenarios específicos** donde la computación cuántica pueda ofrecer una ventaja real. Por ejemplo, en el ámbito de la **gestión humana**, uno de los mayores desafíos es la selección de personal. ¿Podría la computación cuántica desarrollar un sistema que vaya mucho más allá de entrevistas y pruebas técnicas? Un sistema que prediga actitudes, capacidades y ajuste perfecto a los perfiles requeridos, considerando factores psicológicos, médicos y de actitud.

Otro ejemplo podría ser en el desarrollo de **nuevos mercados o productos**. Aunque hoy en día ya se hacen estudios de mercado, la exactitud sigue siendo un problema. Si las herramientas actuales fueran 100% precisas, cada nuevo producto lanzado al mercado tendría éxito asegurado, y sabemos que no es así. Lo mismo ocurre con las estrategias de mercadeo. Aquí es donde la computación cuántica podría marcar la diferencia, aumentando la probabilidad de éxito de un producto o una estrategia hasta acercarse al 100%.

En resumen, creo que la industria tiene mucho potencial para apalancar proyectos donde la computación cuántica ofrezca precisión, predicción y optimización en áreas donde la tecnología clásica tiene limitaciones. Esa es la oportunidad que debemos aprovechar.

Daniel Sierra-Sosa
Diego ¿Cómo ves el impacto de todos estos medios digitales para la computación cuántica en Colombia y en Latinoamérica?

Diego Serrano
Esa es una pregunta muy interesante. La verdad, nunca había reflexionado mucho sobre esto, pero creo que evaluar el impacto es algo relativo. Si comparamos con países como Estados Unidos, obviamente el impacto no es tan signifi-

cativo. Sin embargo, si lo comparamos con otros países de Latinoamérica, creo que en el caso de Colombia el impacto es considerablemente alto.

Como mencionó Alberto, él conoce a más personas de Colombia involucradas en la computación cuántica que incluso de México. Personalmente, he conocido a más colombianos a través de este campo que a personas de cualquier otro país de la región. Esto muestra que hay un interés generalizado en Colombia por la computación cuántica. Desafortunadamente, no tengo claro por qué esto es así. No sé por qué hay tantos colombianos interesados en este campo, pero el impacto de programas como Qiskit ha sido notable. Hay bastantes colombianos en el programa de *Qiskit Advocates* y en empresas de computación cuántica. Por ejemplo, en Xanadu hay al menos tres colombianos, en Zapata (aunque ya no esté tan enfocada en este campo) también hubo varios, e incluso en IBM hay unos cuantos.

Esto evidencia que hay un interés considerable. El desafío, sin embargo, es que todos los colombianos que he conocido en este ámbito están en otros países. Entonces, surge la pregunta: *¿cómo podemos aprovechar los recursos que están atrayendo a colombianos al campo de la computación cuántica y usarlos para motivar a quienes están en el país a seguir desarrollando este interés localmente?* Si logramos canalizar ese interés hacia proyectos constructivos en Colombia, podríamos maximizar el impacto.

En resumen, creo que el impacto de la computación cuántica en Colombia es grande, especialmente en comparación con otros países de Latinoamérica, y representa una oportunidad significativa para el futuro.

La amenaza cuántica. El día “Q” y sus implicaciones para la seguridad global

DOI: 10.29236/sistemas.n173a6

Resumen
El “Día Q” marca un punto de inflexión en la ciberseguridad global: el día en que las computadoras cuánticas tengan la capacidad de romper los algoritmos criptográficos clásicos, que protegen gran parte de la información sensible a nivel mundial. Aunque la llegada precisa de este día es incierta, las fuentes coinciden en que la amenaza es real y requiere una acción inmediata por parte de Estados y organizaciones. Esta breve reflexión hace una revisión los desafíos claves de esta amenaza cuántica revisando algunos de los algoritmos vigentes para la seguridad de las comunicaciones por internet, los retos de la migración a algoritmos poscuánticos y el plan de migración que se debe concretar para limitar las consecuencias por la materialización de esta amenaza. En este sentido, la planeación estratégica, la colaboración y una visión integral se convierten en el marco de trabajo básico para disminuir la amenaza, reducir la vulnerabilidad y mitigar los impactos para hacer más resiliente la infraestructura de seguridad y control global y empresarial.

Palabras clave
Computación cuántica, cúbits, seguridad global, Día Q, amenaza cuántica

Introducción

La computación cuántica aparece en el escenario como un nuevo paradigma en ciencias de la computación que aprovecha los principios de la mecánica cuántica para resolver problemas complejos que están más allá de las capacidades de los computadores tradicionales. En este contexto, a diferencia de estos computadores, que almacenan información en bits que representan 1 o 0, las computadoras cuánticas utilizan qubits (cúbits). Los qubits pueden representar 0 o 1 o una combinación de ambos estados al mismo tiempo, un fenómeno conocido como superposición, lo que habilita a estas máquinas a trabajar de forma masiva en paralelo, explorando múltiples posibilidades a la vez (Shafique et al., 2024).

Este novedoso avance de la ciencia abre fuentes inexploradas de oportunidades que pueden generar avances importantes en diferentes disciplinas como: (Kietzmann et al., 2021)

- Ciencias de la salud y la vida: desarrollo de nuevos medicamentos, terapias de medicina de precisión, estudios de asociación de genoma completo.

- Energía: prevención y resolución de interrupciones en el servicio de energía, optimización de la red eléctrica.

- Logística: optimización de rutas, reducción de emisiones de gases de efecto invernadero.

- Ciencias de los materiales: diseño de nuevos materiales.

- Finanzas: análisis de riesgos, fijación de precios de derivados, detección de fraudes, puntuación de crédito/activos.

- Ciberseguridad: desarrollo de algoritmos criptográficos resistentes a la computación cuántica.

Sin perjuicio de lo anterior, la computación cuántica funda amenazas importantes a la seguridad digital comoquiera que las comunicaciones y transacciones globales ahora basadas en algoritmos de criptografía clásica, podrán ser superados una vez se alcance el momento donde esta computación se encuentre completamente confiable y funcional. Con los avances que se presentan en la actualidad para concretar una computación cuántica funcional, las naciones y organizaciones requieren avanzar rápidamente en planes de migración a esquemas de protección poscuánticas (PQC – *Post Quantum Computing*) que anticipen los posibles riesgos anunciados (Bhat et al., 2022).

En este sentido, la experiencia previa del “Y2K”, puede ser útil para

avanzar con celeridad en este contexto, para lo cual es importante capitalizar lecciones aprendidas como: (Vermeer & Peet, 2020)

- *Riesgo del ataque "cosechar ahora y descifrar después":* si se almacena información sensible y cifrada en la actualidad y el día "Q" llegase a tiempo, se produciría un incalculable perjuicio de consecuencias difíciles de calcular (Amos, 2024).

- *Actuación de forma temprana*: Cuanto más tiempo espere una organización para comenzar la migración a PQC, mayor será el riesgo y la complejidad de la transición.

- *Colaboración entre sectores*: La coordinación entre gobiernos, industria y la comunidad de investigación es crucial para desarrollar, estandarizar e implementar soluciones PQC efectivas.

- *Planificación y la evaluación de riesgos*: Las organizaciones deben evaluar su exposición a la amenaza cuántica, identificar sistemas y datos críticos, y desarrollar planes de migración integrales.

Por tanto, este breve artículo presenta una revisión de la amenaza cuántica situada en el día "Q", esto es, el momento en el futuro cuando los computadores cuánticos sean lo suficientemente robustos como para romper los algoritmos criptográficos asimétricos y debilitar los simétricos clásicos que actualmente protegen la información sensible en línea (Chen et al., 2016) para lo cual es necesario entender los desafíos propios en la computación cuántica, los algoritmos cuánticos utilizados en la actualidad, el reto de la migración hacia algoritmos poscuánticos y el plan de migración que tanto naciones como organizaciones deben emprender para anticipar este momento que tarde o temprano cambiará la dinámica de la seguridad global.

Desafíos actuales de la computación cuántica

La computación cuántica enfrenta diversos retos que la comunidad científica internacional viene afrontando con el fin de aprovechar toda su potencialidad y concretar la promesa de cambio y transformación de la computación actual. Algunos de ellos se detallan a continuación: (Pupillo et al., 2023)

- *Fragilidad de los cúbits* - Los qubits son extremadamente sensibles a las perturbaciones ambientales, como los campos electromagnéticos, y requieren condiciones extremas para mantener su estabilidad, como temperaturas cercanas al cero absoluto (- 273.15 grados Celsius)

- *Escalabilidad y corrección de errores* - A medida que aumenta el número de cúbits, también lo

hace la complejidad de las interacciones entre ellos y la susceptibilidad a los errores.

- *Desarrollo de algoritmos cuánticos* - Si bien se han logrado avances significativos en el desarrollo de algoritmos para problemas específicos, como la factorización y la búsqueda, la exploración de nuevas aplicaciones y la optimización de los algoritmos existentes son áreas de investigación activa.

- *Retos para la ciberseguridad* – En este contexto los desafíos se centran en: romper los criptosistemas actuales, la transición a la criptografía poscuántica, y la evaluación de riesgos y la planeación de la migración lo que implica un trabajo coordinado en las organizaciones.

- *Acceso equitativo* – Asegurar un acceso equitativo a la computación cuántica es importante para fomentar la innovación y evitar la concentración del poder en manos de unos pocos.

Estos desafíos requieren importantes recursos financieros y experiencia especializada que implica no sólo formación de alto nivel sino instalaciones dedicadas con equipo específico que por lo general requiere apoyo de los proveedores y las alianzas necesarias con los gobiernos y universidades para lograr el desarrollo de las aplicaciones o proyectos de investigación. Así mismo, Iniciativas como el *Open Quantum Institute* promueven el acceso abierto a los recursos cuánticos con el fin de motivar una colaboración global (Pupillo et al., 2023)

Lo anterior implica un cambio fundamental en la forma que se generan los algoritmos de programación y particularmente para los temas criptográficos la comprensión de una dinámica de protección basada en el tratamiento de los cúbits que se ve reflejada particularmente en los algoritmos de Shor y Grover.

Los algoritmos cuánticos utilizados en la actualidad

Si bien existen múltiples algoritmos utilizados para concretar diferentes proyectos de investigación y avances relevantes en diferentes temáticas, a continuación se presenta un resumen de aquellos que resultan de interés en la actualidad dada sus referencias en estudios científicos recientes (Shafique et al., 2024).

Particularmente para los efectos de este documento se hará énfasis en los algoritmos de Shor y de Grover dado que son los que en la actualidad se concentra la amenaza cuántica que busca romper los criptosistemas clásicos generalmente basado en RSA (*Rivest Shamir Adleman*) y curvas elípticas (ECC-*Elliptic Curve Cryptography*).

El algoritmo de Shor, fue desarrollado por el Dr. Peter Shor, profesor

Tabla 1.
Algunos algoritmos cuánticos. Características y aplicaciones

Algoritmo Cuántico	Características Claves	Aplicaciones
Algoritmo de Shor	· Factoriza números grandes y resuelve los problemas de búsqueda de orden multiplicativo y logaritmo discreto en tiempo polinomial. · Representa una amenaza significativa para los criptosistemas actuales basados en RSA (*Rivest Shamir Adleman*) y ECC (*Elliptic Curve Cryptography*).	· Criptoanálisis (romper el cifrado RSA y ECC). · Resolución de problemas matemáticos basados en factorización y otros vinculados.
Algoritmo de Grover	· Busca en una base de datos no ordenada en tiempo O(√N). · Ofrece una aceleración cuadrática sobre los algoritmos clásicos de búsqueda. · Para la criptografía simétrica y funciones “hash” (digesto), se impone el aumento del tamaño de las claves y parámetros vinculados.	· Búsqueda de datos en grandes bases de datos. · Aceleración de algoritmos de aprendizaje automático. · Resolución de problemas de optimización.
Algoritmo de Deutsch-Jozsa	· Determina si una función booleana es constante o balanceada con una sola consulta. · Supera a los algoritmos clásicos que requieren múltiples consultas para resolver el mismo problema.	· Demostración de la ventaja cuántica en la resolución de problemas específicos. · Aplicaciones en teoría de la computación.
QAOA (Quantum Approximate Optimization Algorithm)	· Un algoritmo híbrido cuántico-clásico para resolver problemas de optimización combinatoria. * Potencial para encontrar soluciones aproximadas a problemas difíciles.	· Optimización de carteras financieras. · Diseño de materiales. · Logística y planificación.
QSVM (Quantum Support Vector Machines)	· Una versión cuántica del algoritmo de aprendizaje automático de máquinas de vectores de soporte (SVM). · Potencial para mejorar la precisión y la eficiencia del aprendizaje automático.	· Clasificación de datos. · Reconocimiento de patrones. · Análisis de imágenes.

Nota: Basado en: Shafique et al., 2024

de matemáticas del MIT en 1994. Es un algoritmo cuántico relevante por su capacidad para factorizar números grandes y otros problemas numéricos vinculados en tiempo polinomial (tiempo de ejecución de un algoritmo (mediante el cual se obtiene una solución al problema) es menor o igual que un cierto valor calculado a partir del número de variables implicadas (generalmente variables de entrada) usando una fórmula polinómica o polinomio. Esta capacidad tiene implicaciones significativas para la ciberseguridad, ya que puede romper los esquemas de cifrado de clave pública ampliamente utilizados, como RSA, que se basan en la dificultad de factorizar números grandes (Clark et al., 2021).

El algoritmo de Shor se basa en conceptos clave de la mecánica cuántica: (Shafique et al., 2024)

- Superposición: Los cúbits pueden existir en una superposición de estados, es decir, pueden estar en el estado 0, en el estado 1 o en una combinación de ambos al mismo tiempo.

- Entrelazamiento: Dos o más cúbits pueden estar entrelazados, lo que significa que sus estados están supercorrelacionados (con entropía negativa), incluso si están infinitamente separados en tiempo y espacio.

- Transformada rápida de Fourier (FFT): el mérito principal de Shor fue el descubrimiento de un circuito cuántico que resuelve en tiempo polinomial el problema de la búsqueda de orden multiplicativo de enteros en grupos numéricos, el cual con métodos clásicos es de tiempo exponencial, o sea prácticamente incomputable (Nielsen & Chuang, 2010).

En la medida que se construyan computadores cuánticos más confiables y potentes el algoritmo de Shor tendrá mejores condiciones para concretar su amenaza sobre los criptosistemas mencionados previamente.

Mosca (2018) plantea la pregunta retadora: "¿Cuántos cúbit físicos necesitaremos para romper el RSA-2048? (...) Las estimaciones actuales oscilan entre decenas de millones y mil millones de cúbit físicos". Investigaciones posteriores indican que "en los cuatro años transcurridos desde 2015, el extremo superior de la estimación de cuántos cúbits serán necesarios para factorizar los enteros RSA de 2048 bits ha caído casi dos órdenes de magnitud; de mil millones a veinte millones" (Gidney & Ekerå, 2021).

A la fecha existe un reciente avance muy prometedor, el desarrollo de cúbits libre de errores, lo que haría caer esta última estimación otros dos o tres órdenes de magnitud que es lo que actualmente persiguen grandes actores como Google

(Shankland, 2020). De concretarse, el día "Q" estaría muy cercano.

De otra parte, el algoritmo de Grover, propuesto por Lov Grover en 1996, es un algoritmo cuántico que destaca por su capacidad para buscar un elemento específico en una base de datos no ordenada de tamaño N con una complejidad temporal de $O(\sqrt{N})$. Esto contrasta con los algoritmos clásicos de búsqueda, que requieren un tiempo de O(N) en el peor de los casos (Grover,1996).

El algoritmo de Grover se basa en los siguientes elementos: (Grover, 1996)

- Superposición: Al igual que el algoritmo de Shor, el algoritmo de Grover aprovecha la superposición cuántica. Inicialmente, se crea una superposición que representa todos los posibles elementos de la base de datos.

- Amplificación de Amplitud: El algoritmo aplica una serie de operaciones para amplificar la amplitud de probabilidad del estado que corresponde al elemento buscado.

- Operador de Oráculo: Un componente crucial del algoritmo es el operador de oráculo, que identifica el elemento objetivo. El oráculo invierte la fase del estado que representa el elemento buscado, sin revelar su ubicación.

- Operador de Difusión: El operador de difusión aumenta la amplitud del estado objetivo al invertir los estados alrededor del promedio de las amplitudes.

Si bien el algoritmo de Grover no proporciona una solución en tiempo polinomial para los problemas NP-completos (una clase de problemas computacionales para los cuales no se ha encontrado una solución eficiente, pero si se encontrara una solución, podría verificarse de manera eficiente), ya que la aceleración es cuadrática y no exponencial, sí ofrece una ventaja significativa sobre los algoritmos clásicos para ciertos problemas de búsqueda y optimización, por ejemplo un ataque de fuerza bruta a los algoritmos simétricos (AES) (Shafique et al., 2024).

El día "Q". La migración hacia algoritmos poscuánticos

La urgencia de la migración hacia los algoritmos poscuánticos se ha concretado en un marco de trabajo planteado por Mosca (2018) denominado la desigualdad de Mosca que se basa en tres variables: (Mosca, 2018)

- Tiempo de migración (M): El tiempo que tarda una organización en implementar completamente un criptosistema poscuántico. Este proceso incluye la selección de algoritmos apropiados, la actualización de sistemas y software, la capacitación del personal y las pruebas exhaustivas.

- Vida útil de la seguridad (S): El tiempo que la información en cuestión debe permanecer confidencial. Esto varía según el tipo de información: datos financieros o de salud pueden requerir protección durante décadas, mientras que otros datos pueden tener una vida útil más corta.

- Tiempo de colapso (C): El tiempo estimado hasta que se construya una computadora cuántica criptográficamente relevante (CRQC) capaz de romper los algoritmos criptográficos actuales.

La desigualdad de Mosca establece que si M + S > C, es decir, si el tiempo de migración más la vida útil de la seguridad es mayor que el tiempo de colapso, entonces una organización corre el riesgo de que sus datos sean descifrados en el futuro por una CRQC. En otras palabras, si no se migra a la criptografía poscuántica a tiempo, la información sensible podría volverse vulnerable a ataques una vez que las CRQC estén disponibles.

Lo anterior sugiere que el tiempo de migración previsto para toda una nación será significativamente mayor que el tiempo establecido para una organización. Esto implica que se deben articular esfuerzos entre los distintos sectores de la sociedad con el fin de aumentar la conciencia situacional sobre esta amenaza de mediano plazo para establecer un plan de migración coordinado que permita mejorar la postura de ciberseguridad empresarial de las organizaciones. Es claro que habrá sectores más expuestos que otros y por tanto, aquellos que soportan servicios críticos esenciales estarán en los primeros lugares (Mulholland et al., 2017).

Si bien la amenaza cuántica no sólo está centrada en el descifrado de los datos, igualmente podrá utilizarse para violar mecanismos de autenticación, superar firmas digitales y protocolos de confidencialidad disponibles a la fecha. La desigualdad de Mosca se debe usar como una guía en la toma de decisiones sobre los algoritmos criptográficos actuales, ya que existen muchos inciertos en las estimaciones alrededor de las tres variables que la componen.

Es importante anotar que el día “Q” (que según cálculos actuales llegará a finales de esta década o antes) tendrá graves implicaciones para diferentes sectores de la sociedad. Entre ellos están: (Vermeer & Peet, 2020)

- Seguridad nacional: la información clasificada y las comunicaciones militares podrían verse comprometidas.

- Servicios financieros: las transacciones bancarias y los datos financieros personales podrían ser robados o manipulados.

- Infraestructura crítica: los sistemas de control de la red eléctri-

ca, las telecomunicaciones y otros servicios esenciales podrían ser vulnerables a ataques.

- Privacidad personal: las historias médicas, los registros financieros y otros datos personales confidenciales podrían quedar expuestos.

Plan de migración a algoritmos poscuánticos. Retos para las organizaciones

La migración a algoritmos poscuánticos debe ser un proceso continuo que requiere adaptación y flexibilidad a medida que la tecnología cuántica avanza. En este sentido, las organizaciones y los países deben adelantar una planificación cuidadosa y una ejecución estratégica que permita de manera ordena establecer un plan de acción que termine fortaleciendo la postura de ciberseguridad de la empresa (Mckinsey, 2021).

Siguiendo las reflexiones de Hasan et al. (2024) y Pupillo et al. (2023) se detalla a continuación una propuesta de un plan de migración práctico para considerar frente a la amenaza cuántica:

1. Conciencia y Educación:

a. Comprender la amenaza cuántica: Es fundamental que las organizaciones comprendan la amenaza que representan los computadores cuánticos para los algoritmos criptográficos actuales. Este conocimiento debe extenderse a todos los niveles de la organización, desde la alta dirección hasta el personal de TI.

b. Conocer los algoritmos PQC: Familiarizarse con los diferentes tipos de algoritmos PQC, sus fortalezas, debilidades y casos de uso.

2. Inventario Criptográfico:

a. Identificar activos criptográficos: Crear un inventario completo de todos los activos criptográficos utilizados en la organización, incluyendo algoritmos, claves, certificados, protocolos y sistemas de gestión de claves. Este inventario debe incluir software, hardware, comunicaciones y servicios de terceros.

b. Analizar dependencias: Evaluar las dependencias entre los activos criptográficos y los datos que protegen. Este análisis debe considerar el flujo de datos dentro de la organización y las interacciones con sistemas externos.

3. Evaluación de Riesgos:

a. Determinar la sensibilidad de los datos: Clasificar los datos según su sensibilidad y el tiempo que deben permanecer protegidos.

b. Evaluar el impacto de la computación cuántica: Analizar el impacto potencial de las computadoras cuánticas en los activos criptográficos y los datos, utili-

zando herramientas como la desigualdad de Mosca.

c. Identificar prioridades de migración: Priorizar los sistemas y datos que requieren migración inmediata, basándose en la evaluación de riesgos. Los sistemas con una vida útil prolongada, como la infraestructura y los dispositivos IoT, deben ser priorizados.

4. Selección de Algoritmos PQC:

a. Investigar algoritmos PQC: Investigar y evaluar los algoritmos PQC candidatos que cumplan con los requisitos de seguridad y rendimiento de la organización.

b. Considerar la estandarización: Priorizar los algoritmos PQC que están siendo considerados para la estandarización por organismos como NIST.

c. Adoptar un enfoque híbrido: Considerar el uso de esquemas híbridos que combinen algoritmos clásicos con algoritmos PQC para asegurar una transición fluida y minimizar los riesgos. Estas soluciones parecen ser muy prometedoras para la protección casi inmediata de redes corporativas.

5. Implementación y Prueba:

a. Planificar la implementación: Desarrollar un plan de implementación detallado que incluya pruebas, capacitación y gestión de cambios.

b. Implementar algoritmos PQC: Implementar los algoritmos PQC seleccionados en los sistemas prioritarios, asegurando la interoperabilidad con los sistemas existentes.

c. Probar y validar: Probar y validar exhaustivamente la seguridad y el rendimiento de los sistemas migrados.

6. Monitoreo y Actualización:

a. Monitorear el panorama de amenazas: Monitorear continuamente el panorama de amenazas cuánticas y las actualizaciones de los estándares PQC.

b. Mantener la agilidad criptográfica: Diseñar sistemas con agilidad criptográfica para facilitar futuras actualizaciones y transiciones a nuevos algoritmos.

Conclusiones

La computación cuántica, aunque aún se encuentra en desarrollo, presenta una amenaza potencial significativa para la seguridad global a largo plazo. Los algoritmos cuánticos, como el algoritmo de Shor, tienen la capacidad de romper los criptosistemas ampliamente utilizados hoy en día, como RSA y ECC, que protegen la información confidencial en varios sectores, incluyendo finanzas, sector sanitario y gobierno y debilitar los criptosis-

temas simétricos y las funciones de digesto. (Brooks, 2023; Keary, 2023).

Por tanto, la amenaza cuántica establece una serie de retos para los países y las organizaciones en el mediano plazo, que no sólo van a afectar el cifrado de los archivos, sino crear efectos de orden nacional donde información sensible podrá estar expuesta en el futuro.

En esta línea, esta amenaza se puede dividir en dos momentos: (Tan et al., 2023)

- Recolección de datos actual ("cosecha ahora, descifra después"), como ya fuese mencionado: Los adversarios pueden estar recolectando datos cifrados hoy con la expectativa de que las computadoras cuánticas futuras puedan descifrarlos. Esta táctica subraya la urgencia de la acción, ya que los datos sensibles recopilados hoy podrían estar en riesgo en el futuro. Esta estrategia se puede estar usando hoy por diferentes países desarrollados para contar con información estratégica y determinante en sus esquemas de defensa o propiedad intelectual.

- Descifrado de datos: Una vez que las computadoras cuánticas alcancen la madurez, podrían usarse para descifrar datos cifrados previamente con algoritmos vulnerables a la computación cuántica.

De otra parte, las organizaciones deberán hacer su ejercicio para anticipar esta amenaza para lo cual el plan de migración a algoritmos poscuánticos será parte de la estrategia a seguir, sin perjuicio de la evaluación e impactos jurídicos que se puedan dar frente a eventuales ataque exitosos (acceso a información con deber de protección legal) sobre información cifrada con algoritmos clásicos que posiblemente no terminaron de migrarse o quedaron por fuera de los inventarios realizados. En este contexto pensar en ampliar las pólizas cibernéticas actuales en este sentido, podría ser una oportunidad para ajustar estos ejercicios de riesgos emergentes para las empresas.

Así las cosas, la materialización de la amenaza cuántica en las compañías deberá ser parte de los análisis de riesgos empresariales teniendo en cuenta situaciones como: (Vermeer & Peet, 2020)

- Pérdida de datos confidenciales: Esto podría incluir información financiera, propiedad intelectual, datos de clientes e información estratégica.

- Daño a la reputación: Una violación de datos exitosa debido a la computación cuántica podría dañar la reputación de su organización y erosionar la confianza de los clientes.

- Incumplimiento normativo: La incapacidad para proteger los da-

tos contra las amenazas cuánticas podría resultar en multas y sanciones por incumplimiento de las regulaciones de protección de datos.

- Interrupción operativa: Los sistemas críticos que dependen de la criptografía podrían verse afectados, lo que provocaría interrupciones operativas.

La amenaza cuántica es real y el día "Q" se acerca. En consecuencia, las organizaciones deben tomar las medidas proactivas necesarias y suficientes para prepararse frente a los nuevos escenarios de la computación cuántica y proteger sus datos de las amenazas futuras. La amenaza cuántica es semejante al dilema del volcán, es imperativo estar preparado para cuando se haga realidad, para lo cual habrá que estar atento a los avances y noticias del entorno (favorables frente a la resistencia de los algoritmos poscuánticos, así como de los adversarios en el aprovechamiento y uso adverso de estos algoritmos), mientras se avanza en la migración interna para disminuir las vulnerabilidades e impactos que se puedan tener en el futuro.

La inacción frente a esta realidad podrá tener consecuencias desfavorables significativas y por tanto, acompañarse de expertos en ciberseguridad y computación cuántica para obtener orientación y asistencia se convierte en un elemento estratégico y funcional para articular los esfuerzos de aseguramiento y control frente a un entorno cada vez más hostil y competitivo.

Agradecimientos

El autor agradece al doctor Juan Pedro Hecht, Profesor titular y *Research Fellow* en criptografía de la Universidad de Buenos Aires, Argentina, por sus valiosos y acertados comentarios, los cuales permitieron afinar las reflexiones de este artículo.

Referencias

Amos, Z. (2024). *"Harvest now, decrypt later": Why hackers are waiting for quantum computing*. VentureBeat. https://venturebeat.com/security/harvest-now-decrypt-later-why-hackers-are-waiting-for-quantum-computing/

Bhat, H. A., Khanday, F. A., Kaushik, B. K., Bashir, F., & Shah, K. A. (2022). Quantum computing: Fundamentals, implementations and applications. *IEEE open journal of nanotechnology*, *3*, 61–77. https://doi.org/10.1109/ojnano.2022.3178545

Brooks, C. (2023). *Quantum Tech Needed To Secure Critical Data From Quantum Decryption*. Forbes. https://www.forbes.com/sites/chuckbrooks/2023/01/19/quantum-tech-needed-to-secure-critical-data-from-quantum-decryption/

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography*. National Institute of Standards and Technology. http://dx.doi.org/10.6028/NIST.IR.8105

Clark, R., Bartlett, S., Bremner, M., Lam, P. K., & Ralph, T. (2021). *The impact of quantum technologies on secure communications*. Australian Strategic Policy Institute - ASPI. https://www.aspi.org.au/report/impact-quantum-technologies-secure-communications

Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, *5*(433), 433. https://doi.org/10.22331/q-2021-04-15-433

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing* - STOC '96. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/237814.237866

Hasan, K. F., Simpson, L., Baee, M. A. R., Islam, C., Rahman, Z., Armstrong, W., Gauravaram, P., & McKague, M. (2024). A framework for migrating to post-quantum cryptography: Security dependency analysis and case studies. *IEEE access: practical innovations, open solutions*, *12*, 23427–23450. https://doi.org/10.1109/access.2024.3360412

Keary, T. (2023). *IBM: Quantum computing poses an 'existential threat' to data encryption*. VentureBeat. https://venturebeat.com/security/ibm-quantum-computing/

Kietzmann, J., Demetis, D. S., Eriksson, T., & Dabirian, A. (2021). Hello quantum! How quantum computing will change the world. *IT Professional*, *23*(4), 106-111. https://doi.org/10.1109/MITP.2021.3086917

Mckinsey. (2021). Quantum computing: An emerging ecosystem and industry use cases. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/quantum%20computing%20use%20cases%20are%20getting%20real%20what%20you%20need%20to%20know/quantum-computing-an-emerging-ecosystem.pdf

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE security & privacy*, *16*(5), 38–41. https://doi.org/10.1109/msp.2018.3761723

Mulholland, J., Mosca, M., & Braun, J. (2017). The day the cryptography dies. *IEEE security & privacy*, *15*(4), 14–21. https://doi.org/10.1109/msp.2017.3151325

Nielsen, M. A. & Chuang, I. L. (2010). *Quantum Computation and Quantum Information*. 10th Anniversary Edition. Cambridge: Cambridge University Press.

Pupillo, L., Ferreira, A., Lipiainien, V. & Polito, C. (2023), *Quantum Technologies and Cybersecurity: Technology, governance and policy challenges*, Task Force Report, Centre for European Policy Studies - CEPS, Brussels. https://cdn.ceps.eu/wp-content/uploads/2023/12/CEPS-TFR-Quantum-Technologies-and-Cybersecurity.pdf

Shafique, M. A., Munir, A., & Latif, I. (2024). Quantum Computing: Circuits, Algorithms, and Applications. *IEEE access: practical innovations, open solutions*, *12*, 22296–22314. https://doi.org/10.1109/access.2024.3362955

Shankland, S. (2020).*Quantum computer makers like their odds for big progress*. CNET. https://www.cnet.com/tech/computing/quantum-computer-makers-like-their-odds-for-big-progress-soon/

Tan, T. G., Zhou, J., Sharma, V., & Mohanty, S. P. (2023). Post-quantum adversarial modeling: A user's perspective. *IEEE Computer*, *56*(8), 58–67. https://doi.org/10.1109/mc.2022.3218046

Vermeer, M., & Peet, E. (2020). *Securing communications in the quantum computing age: Managing the risks to encryption*. RAND Corporation. https://doi.org/10.7249/rr3102

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*

Métodos de Codificación para QML

DOI: 10.29236/sistemas.n173a7

Samuel Lopera Torres, Daniel Sierra Sosa, Juan G. Lalinde Pulido

1. Introducción

La fusión de la computación cuántica con el aprendizaje automático está allanando el camino para el Aprendizaje Automático Cuántico (QML, por sus siglas en inglés), un campo con el potencial de redefinir las capacidades computacionales en sectores como la criptografía, el descubrimiento de fármacos y las finanzas. En el núcleo de QML se encuentra la codificación de datos clásicos en estados cuánticos, una tarea tanto fundamental como compleja. El proceso de codificación permite representar la información clásica aprovechando las propiedades únicas de los sistemas cuánticos, como la superposición y el entrelazamiento, lo que facilita la ejecución de tareas intensivas en computación con una rapidez y eficiencia potencialmente sin precedentes.

No obstante, los desafíos de la codificación de datos en QML son numerosos. La codificación clásica representa los datos en el sistema binario, lo que la hace simple en el sentido de que solo cambia los

símbolos utilizados para representar los números enteros, pero no cambia sus propiedades. Los otros tipos de datos, como números de punto flotante, texto, imágenes y sonidos se codifican a partir de los enteros mediante algoritmos definidos para interpretar y transformar esas secuencias binarias. La codificación cuántica representa los datos mediante un estado cuántico, por lo que debe considerar las características específicas del entorno cuántico, tales como la superposición, el entrelazamiento y, especialmente, el hecho de que un estado cuántico es un vector unitario en un espacio de Hilbert.

Adicionalmente, las limitaciones en el número de qubits, los tiempos de coherencia y la fidelidad de las compuertas en el hardware cuántico actual afectan la viabilidad práctica de las estrategias de codificación. Estos desafíos hacen que sea esencial desarrollar métodos de codificación que no solo sean teóricamente sólidos, sino también resistentes al ruido, eficientes en términos de hardware y escalables.

Este estudio es motivado tanto por el potencial teórico del QML como de sus aplicaciones prácticas. Algoritmos cuánticos, como el de Shor y de Grover, muestran el potencial la computación cuántica. Sin embargo, materializarlo exige una comprensión profunda de cómo los datos clásicos pueden codificarse eficientemente dentro de sistemas cuánticos. Por ello, este trabajo se centra los métodos de codificación de datos.

2. Principios Matemáticos y Físicos

Para entender los principios de representación de datos clásicos como estados cuánticos, hay que comprender algunos de los conceptos básicos de la mecánica cuántica [1]. En primer lugar, es importante entender la *Notación de Dirac*, también conocida como *braket*. Esta se utiliza para representar vectores en el espacio de Hilbert. Un estado cuántico es un vector columna y se representa mediante el *ket* $|\varphi\rangle = (a_1, a_2, \dots, a_n)^T$ .El *bra* es un vector fila que es el transpuesto conjugado del *ket*, $\langle\varphi| = |\varphi\rangle^\dagger = (a_1^*, a_2^*, \dots, a_n^*)$. Adicionalmente, el producto interno entre $|\varphi\rangle$ y $|\psi\rangle$,en la notación de Dirac[1], es $\langle\varphi|\psi\rangle$,el producto externo es $|\varphi\rangle\langle\psi|$ y la norma de un vector es $\langle\varphi|\varphi\rangle$.

El equivalente cuántico al bit clásico, entendido como la unidad fundamental para representar la información, es el *qubit*. Matemáticamente hablando, un qubit es un vector unitario en el espacio de Hilbert $\mathbb{C}^2$. Esto significa que se puede representar cualquier qubit genérico $|\varphi\rangle$ como un vector en $\mathbb{C}^2$, de la siguiente manera:

$$|\varphi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

1 La notación utilizada para el producto interno es un braket. La parte izquierda es el bra y la derecha el ket.

Todo espacio vectorial tiene infinitas bases. En la computación cuántica, cuando se tiene un qubit, se utiliza la base constituida por los estados $|0\rangle$ y $|1\rangle$ .y se denomina la base computacional[2], donde:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \text{ y } |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

Como cualquier vector en $\mathbb{C}^2$, $|\varphi\rangle$ se puede expresar como una combinación lineal de los elementos de la base de dicho espacio de Hilbert. Dado que cualquier qubit $|\varphi\rangle$ puede expresarse como una combinación lineal de los elementos de la base:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Esto es lo que se conoce como el principio de superposición. Adicionalmente, se debe cumplir que $|\alpha|^2 + |\beta|^2 = 1$,ya que, como se verá a continuación, todo estado cuántico es un verctor con norma 1. Finalmente, cuando se mide un qubit, su estado se altera y los únicos resultados posibles son $|0\rangle$ o $|1\rangle$. El resultado de la medición es aleatorio donde la probabilidad de que el resultado sea $|0\rangle$ ó $|1\rangle$ es $|\alpha|^2$ y $|\beta|^2$ respectivamente.

Cuando se tiene un sistema con múltiples qubits $|\varphi_s\rangle$, el sistema compuesto es el resultado del producto tensorial de cada uno de los estados.

$$|\varphi\rangle = |\varphi_0\rangle \otimes |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \dots \otimes |\varphi_{n-2}\rangle \otimes |\varphi_{n-1}\rangle$$

y la base del nuevo espacio es el producto tensorial de las bases de cada qubit y, por lo tanto, es una base ortonormal donde los elementos de la base se numeran[3] de $|0\rangle$ a $|2^n - 1\rangle$ Esto implica que si son n qubits, el espacio es $\mathbb{C}^{2^n}$. En general, el estado cuántico de un sistema de n qubits es vector unitario en $\mathbb{C}^{2^n}$ y se representa como

$$|\varphi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$$

donde los $\alpha_i \in \mathbb{C}$ y deben cumplir que

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

Aplicar una operación a un sistema cuántico es equivalente a multiplicar una matriz unitaria[4]; estas matrices unitarias se llaman compuertas. En sistema de n qubits la matriz unitaria es una matriz cuadrada de $2^n \times 2^n$. Si se aplican operaciones

2 La base computacional tiene un sentido físico muy claro: Es estado |0⟩ corresponde al estado de reposo. Esto es importante porque uno de los aspectos misteriosos de la mecánica cuántica es que es imposible conocer un estado cuántico porque al medirlo se produce el llamado colapso de la función de onda y cambia de estado. Adicionalmente, cuando un qubit está en el estado |0⟩ o en el estado |1⟩ se comporta como un bit clásico. Una muy buena introducción a la teoría de la información cuántica se puede encontrar en [10]

3 Dado que el espacio de Hilbert se construye mediante productos tensoriales, la representación binaria del número asociado con la base describe cuáles es el componente de cada qubit que aporta a ese estado.

4 La matriz debe ser unitaria porque el resultado debe ser un estado cuántico válido y por lo tanto la matriz no puede alterar la norma del vector. Esto tiene dos implicaciones importantes: toda operación cuántica es invertible y, por lo tanto, no disipa calor.

que afectan a algunos qubits, de todas maneras la operación afecta a todo el sistema y la compuerta se puede modelar matemáticamente como el producto tensorial de aplicar la operación al subespacio generado por los qubits afectados y aplicar la identidad al subespacio generado por los otros qubits. Uno de los resultados más importantes es que existe un conjunto de compuertas básicas tales que cualquier compuerta cuántica puede ser representada como aplicación sucesiva, es decir multiplicación, de las compuertas básicas. Por eso se puede hablar de computación cuántica universal.

Cuando se trabaja con sistemas compuestos, representar puertas cuánticas como multiplicaciones de matrices puede resultar complicado. Para resolver ese problema, generalmente se usan circuitos cuánticos para representar estas operaciones. En esta representación, el tiempo transcurre en el algoritmo de izquierda a derecha. El estado inicial de cada qubit es casi siempre $|0\rangle$,que es el estado de reposo. Las compuertas se representan por rectángulos donde el texto del rectángulo identifica la compuerta. Las líneas horizontales simples corresponden a qubits y las dobles a bits clásicos. Avanzar de izquierda a derecha implica multiplicar la matriz que representa el operador por el vector que representa el estado del sistema. En principio, toda operación debe afectar a todos los qubits. Si hay varias compuertas en la misma línea vertical, la compuerta a aplicar es el producto tensorial de estas. Si hay algún qubit al que no se le esté aplicando ninguna compuerta, se utiliza la matriz identidad para representar este hecho y se incluye en el producto tensorial.

La Figura 1 presenta un ejemplo de un circuito cuántico con dos qubits. El estado inicial es $|0\rangle \otimes |0\rangle$ Como la compuerta H se aplica únicamente al primer qubit, entonces la operación que realmente se aplica es $H \otimes I_{2\times 2}$, donde $I_{2\times 2}$ es la matriz identidad con dos filas y dos columnas.

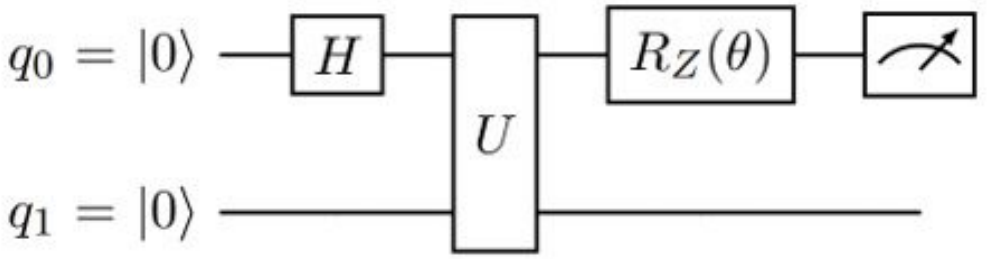


Figura 1 Ejemplo de un circuito cuántico

El estado después de haber aplicado $H \otimes I_{2\times 2}$ es $(H \otimes I_{2\times 2})(|0\rangle \otimes |0\rangle)$.

La Tabla 1 presenta las compuertas cuánticas más comunes y su representación en forma de matriz.

3. Algoritmos de Codificación

En el aprendizaje cuántico de máquinas (QML), la forma en que codificamos datos clásicos en estados cuánticos está relacionada con métodos de Kernel [2]. Formalmente, la codificación puede considerarse como un mapeo de características desde el espacio de entrada original X a un espacio de Hilbert $\mathbb{C}^{2^n}$. A diferencia de lo que pasa en la representación clásica en binario, este mapeo implica una transformación no trivial de los datos [3], [4]. La

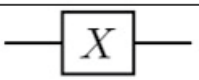
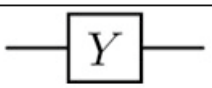
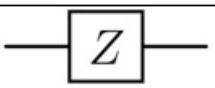
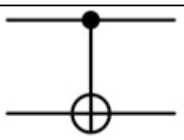
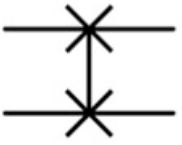
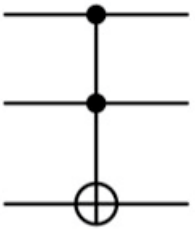
Compuerta	Representación en circuito	Representación en matriz
Hadamard		$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$
Pauli X		$\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$
Pauli Y		$\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}$
Pauli Z		$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}$
Negación controlada		$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$
Swap		$\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$
Toffoli		$\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\end{bmatrix}$

Tabla 1 Compuertas cuánticas más comunes

forma como se codifiquen va a influir no solo en qué modelos se pueden utilizar sino en también en su capacidad expresiva [5]. La codificación se lleva a cabo mediante un circuito cuántico parametrizado por los datos de entrada y, posiblemente, por otros parámetros. aplicados a un estado inicial que generalmente es $|0\rangle^{\otimes n}$. Formalmente, el mapa de características cuántico se define como una transformación:

$$\psi: X \rightarrow \mathbb{C}^{2^n}$$

donde n es el número de qubits necesarios para representar los datos y depende no solo del número de datos sino también de su naturaleza y su rango. La codificación, también conocida como preparación del estado, se realiza mediante una transformación unitaria parametrizada. En otras palabras, para codificar $x \in X$ como $|\psi(x)\rangle \in \mathbb{C}^{2^n}$, se utiliza una transformación paramétrica $U_\psi(x)$ tal que

$$|\psi(x)\rangle = U_\psi(x)|0\rangle^{\otimes n}$$

Todos los algoritmos en esta sección construyen un circuito cuántico desde cero, y como tal, no tienen la necesidad de instrucciones de retorno; ya que, en resumen, son una serie de operaciones que utilizan el vector de características $x \in X$ como parámetro. Se presentarán tres tipos de codificación básicos: en base, en amplitud y en fase. Estas son las formas de codificación naturales que surgen a partir de la estructura de un estado cuántico.

Antes de entrar en cada una de ellas, es importante presentar de dónde se derivan. El estado cuántico de un sistema de n qubits es vector unitario en y $\mathbb{C}^{2^n}$ se representa como

$$|\varphi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$$

donde los y deben cumplir que

$$\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

En esta representación, los $|i\rangle$ son 2^n las bases del espacio y se pueden utilizar para representar datos en binario. Los $\alpha_i \in \mathbb{C}$, como son números complejos, tienen una magnitud y una fase. Hay que recordar que si $z = a + ib$ es un número complejo, puede ser escrito como $z = re^{i\theta}$ donde $r = \sqrt{a^2 + b^2}$ y $\theta = \tan^{-1}(b/a)$. Así α_i, puede ser utilizado para representar los datos mediante su magnitud r o su fase θ.

3.1 Codificación en Base

La codificación de base, como su nombre lo indica, tiene como objetivo codificar los datos realizando una superposición uniforme de todos los estados base involucrados en el conjunto de datos.

Por ejemplo, dado un conjunto de datos $D = [2,5,9]$ o, en binario: $D = [0010, 0101, 1001]$, se necesita la siguiente superposición:

$$|\psi\rangle = \frac{|0010\rangle + |0101\rangle + |1001\rangle}{\sqrt{3}}$$

En general, se busca construir el estado:

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{2^n-1} I_D(i)\,|i\rangle$$

donde $I_D(i)$ es una función que devuelve 1 ó 0 dependiendo de la presencia del estado i en el conjunto de datos D. El número de qubits necesarios, n, está determinado por el rango del conjunto de datos, dado que un sistema cuántico de n qubits tiene 2^n estados base distintos. Se puede observar también que, dado que este esquema de codificación ignora la multiplicidad de los datos pues todos los datos iguales se representan con el mismo estado.

La manera más sencilla de implementar este tipo codificación es utilizando el algoritmo de Grover utilizando $I_D(i)$ como función oráculo. Para el algoritmo de grover se construye una compuerta unitaria que cumpla que

$$U_{I_D}|x -\rangle = (-1)^{I_D(x)}|x -\rangle$$

y luego de $\sqrt{N}$ iteraciones se obtiene una muy buena aproximación del estado deseado. Este tipo de codificación es fácil de entender pues, si bien utiliza la superposición cuántica, representa los datos clásicos mediante el sistema binario [6]

3.2 Codificación en Amplitud

La codificación en amplitud busca codificar los datos en el vector de estado haciendo cada dato sea codificado en la amplitud un estado diferente. En este caso, se Schuld [1] propone un algoritmo para codificar datos en tiempo lineal $O(n)$, que consiste en usar varias rotaciones controladas de los qubits en el sistema compuesto. En otras palabras, si $x = \{x_0, x_1, \dots, x_{N-1}\} \in X$ y se va a representar mediante el estado cuántico

$$|\varphi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$$

entonces el objetivo es que $\alpha_i = x_i$. Como $|\varphi\rangle$ es un estado cuántico, debe cumplir la condición de normalidad $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$ así que x debe ser normalizando antes de poder representarlo. La forma de construir los α_i es mediante rotaciones aplicadas a cada qubit.

Sin embargo, antes de entender el algoritmo detrás de la codificación de amplitud, es necesario comprender cómo rotar un qubit para lograr un resultado deseado. Una forma es utilizar una compuerta que rota el qubit sobre un eje

específico. Una compuerta[5] utilizada para es fin es la compuerta $R_y(\theta)$, que se define como

$$R_y(\theta) = \begin{bmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{bmatrix}$$

Como el espacio $\mathbb{C}^{2^n}$ es el resultado del producto tensorial de los espacios asociados a cada qubit, entonces en cada uno de los vectores de la base computacional de $\mathbb{C}^{2^n}$ están representados todos los qubits simultáneamente. Por ejemplo, si $n = 4$ se tiene el espacio $\mathbb{C}^{2^4}=\mathbb{C}^{16}$. La base computacional de este espacio tiene 16 vectores. Como se representa cada elemento de la base en binario, el noveno (9°) vector de la base sería $|1001\rangle$, lo que quiere decir que este vector corresponde al estado en el cuál es primer y el último qubit tienen estado 1 y los dos del medio tiene estado 0.

Con el fin de simplificar la explicación del algoritmo, se asumirá que el número de datos a codificar $N = 2^n$. Si esta situación no se da, se completa la colección de datos con ceros (0) hasta que el número esa una potencia de dos (2). El algoritmo procede de la siguiente manera:

1. Se determina cuál es la rotación que debe aplicarse al primer qubit. Si se tienen $N = 2^n$ datos, entonces el espacio es $\mathbb{C}^{2^n}$, y la primera mitad de los estados tienen el primer qubit en cero (0) mientras que la otra mitad lo tiene en uno (1). Como se cumple la condición de normalidad, se suma el cuadrado de las amplitudes de los primeros estados y con base en este valor se determina cuál es la rotación que se debe aplicar al primer qubit para que

$$P(0) = \sum_{i=0}^{(2^n-1)/2} |x_i|^2$$

donde $P(0)$ es la probabilidad de que al medir el primer qubit dé $|0\rangle$. El qubit se rota aplicando la compuerta $R_y(\theta)$.

2. Se determina cuál es la rotación que debe aplicarse al segundo qubit. Se divide el análisis en dos casos. Los estados para los cuales el primer qubit es cero (0) y los estados para los cuales el primer qubit es uno (1). Para cada caso se consideran solamente los estados que cumplen con la condición, o sea que para cada caso se analiza la mitad de los estados.

a. Para los casos en que el primer qubit es cero (0), se calcula $P(00)$, la probabilidad de que los dos primeros qubits sean cero (0) teniendo presente que ya se conoce la probabilidad P(0) de que el primer qubit sea cero (0).

5 La compuerta Pauli Y es un caso particular de la compuerta Ry (θ) donde θ= π.

En este caso

$$P(00) = \frac{\sum_{i=0}^{(2^n-1)/4} |x_{2i}|^2}{P(0)}$$

Con base en P(00) se calcula la rotación que hay que aplicar al segundo qubit cuando el primero es cero (0), y se implementa con una compuerta $R_y(\theta)$ controlada[6] por el primer qubit.

b. Para los casos en que el primer qubit es cero (1), se calcula $P(10)$, la probabilidad de que el primer qubit sea uno (1) y el segundo qubit sea cero (0) teniendo presente que ya se conoce la probabilidad $P(0)$ de que el primer qubit sea cero (0). En este caso

$$P(10) = \frac{\sum_{i=0}^{(2^n-1)/4} |x_{2i+1}|^2}{P(1)}$$

Con base en $P(10)$ se calcula la rotación θ que hay que aplicar al segundo qubit cuando el primero es uno (1), y se implementa con una compuerta $R_y(\theta)$ controlada[7] por el primer qubit.

3. En general, se debe determinar para cada qubit cuál es la rotación que se debe aplicar. Para calcular la rotación que debe aplicarse al *q*-ésimo qubit, se 2^{q-1} casos. sigue el mismo proceso de los pasos anteriores. Cada caso representa un estado con *q*-1 qubits. Sea $0 \leq t < 2^{q-1}$, caso asociado con t calcula cuál es la probabilidad de que el estado de *q* bits $2t$ tenga el *q*-ésimo qubit en cero (0). En general

$$P(2t) = \frac{\sum_{i=0}^{(2^n-1)/2^q} |x_{2^{q-1}i+t}|^2}{P(t)}$$

Con base en $\mathrm{P}(2\mathrm{t})$ se calcula la rotación θ que hay que aplicar al *q*-esimo qubit cuando los *q*-1 primeros qubit son t, y se implementa con una compuerta $R_y(\theta)$ controlada por los primeros *q*-1 qubits.

Ahora bien, el método presentado no es el único, pero si presenta claramente cómo se puede codificar en amplitud. Existen más propuestas de métodos de codificación en amplitud, como por ejemplo [2] que plantea una estrategia "dividir y conquistar". Otras propuestas incluyen la aplicación de la cascada, realizándola en el orden inverso, como se propone en [7], o utilizar una cascada de compuertas R_z previas a la cascada R_y.

Esta codificación es bastante útil para representar problemas físicos. [8] y en codificación de datos para aprendizaje de máquina cuántico, lo que lleva a que la investigación en este campo sea muy activa.

6 Una compuerta controlada realiza la operación específica solo si el qubit controlador está en un estado específico.

7 Una compuerta controlada realiza la operación específica solo si el qubit controlador está en un estado específico.

3.3 Codificación en Fase (Angulo)

Finalmente, la codificación en fase codifica los valores de la entrada en cada uno de los ángulos de cada qubit, resultando en un estado no entrelazado (separable). El algo ritmo propuesto por Weigold [34], recibe un vector de entrada $X = (x_0, x_1, \ldots, x_n)^T$ y produce un estado cuántico donde cada x_i de la entrada está representado en el ángulo del *i*-ésimo qubit.

Es importante tener en cuenta que $R(X_i)$ es una rotación arbitraria, lo que significa que se puede utilizar, por simplicidad, cualquiera de las puertas R_X, R_Y ó R_Z. Lo importante es que todas las rotaciones sean del mismo tipo. En su mayoría, la literatura y artículos utilizan la puerta R_y, ya que generalmente, el eje *X* se suele utilizar para negaciones, y el eje *Z* para la medición. No obstante, en caso de utilizar este método de codificación, la rotación más apropiada depende única y exclusivamente del problema a trabajar.

La construcción del estado cuántico correspondiente a esta forma de codificar es

$$|\varphi\rangle = \mathrm{R_Y}(x_0)|0\rangle \otimes \mathrm{R_Y}(x_1)|0\rangle \otimes \ldots \otimes \mathrm{R_Y}(x_n)|0\rangle$$

Este no suele ser utilizado generalmente para aspectos de ciencia de datos, es más orientado (debido a su alta complejidad en memoria), sino para algoritmos de optimización y búsqueda, como el algoritmo de Shor. [9]

4. Conclusión

La exploración y el desarrollo de métodos de codificación cuántica son fundamentales para el procesamiento de información y la comunicación cuánticas. Esta revisión ha examinado tres estrategias de codificación cuántica presentando sus fundamentos teóricos, implementaciones prácticas y los desafíos que enfrentan.

Los métodos que se presentaron tienen una sólida fundamentación teórica, pero su implementación en entornos reales enfrenta obstáculos adicionales como la decoherencia de qubits, el ruido cuántico y la necesidad de operaciones cuánticas de alta fidelidad. La investigación futura debería centrarse en superar estos desafíos mediante el desarrollo de algoritmos de corrección de errores cuánticos más robustos y escalables, mejorando la fidelidad de las operaciones cuánticas y optimizando la integración de sistemas cuánticos con tecnologías clásicas. Asimismo, explorar materiales y arquitecturas cuánticas novedosas, como qubits topológicos y sistemas cuánticos fotónicos, podría proporcionar nuevas vías para una codificación cuántica eficiente y resiliente.

En resumen, los métodos de codificación cuántica están a la vanguar-

dia del desarrollo de tecnologías cuánticas, pero continuar su desarrollo es un requisito para explotar el potencial transformador de la computación cuántica. La investigación interdisciplinaria y la colaboración continua serán esenciales para desbloquear el potencial completo de la codificación cuántica, lo que finalmente llevará a la realización de sistemas prácticos y poderosos de información cuántica.

Referencias

1 M. Schuld y F. Petruccione, Supervised Learning with Quantum Computers, 1st ed., Springer, 2018, p. 287.

2 M. Schuld, «Supervised quantum machine learning models are kernel methods,» *arXiv preprint arXiv*: 2101.11020, 2021.

3 M. Schuld y N. Killoran, «Quantum machine learning in feature hilbert spaces,» *Physical review letters*, vol. 122, p. 040504, 2019.

4 S. Lloyd, M. Schuld, A. Ijaz, J. Izaac y N. Killoran, «Quantum embeddings for machine learning,» *arXiv preprint arXiv*:2001.03622, 2020.

5 M. Schuld, R. Sweke y J. J. Meyer, «Effect of data encoding on the expressive power of variational quantum-machine-learning models,» *Physical Review A*, vol. 103, p. 032430, 2021.

6 C. Wetterich, «Entanglement in quantum mechanics,» *Physical Review A*, vol. 99, p. 022112, 2019.

7 M. Mangin-Brinet, J. Zhang, D. Lacroix y E. A. Ruiz Guzman, «Efficient solution of the non-unitary time-dependent Schrodinger equation on a quantum computer with complex absorbing potential,» *Quantum*, vol. 8, p. 1311, April 2024.

8 W. J. Munro y others, «Weak measurements with superconducting qubits,» *Physical Review Letters*, vol. 86, p. 4992–4995, 2001.

9 D. B. Szombati y others, «Josephson φ 0-junction in nanowire quantum dots,» *Nature Physics*, vol. 16, p. 568–573, 2020.

10 M. A. Nielsen y I. L. Chuang, Quantum Computation and Quantum Information, 10th anniv ed., Cambridge University Press, 2010, p. 676.

ACIS

ASOCIACION COLOMBIANA DE INFORMATICA, SISTEMAS Y TECNOLOGIAS AFINES

¡ Pongase al día en sus cuotas !

Recuerda que te da derecho a participar en un evento virtual

Comuniquese con nuestro equipo de atención al cliente.
suscripciones@acis.org.co
o al télefono 3015530540

Para más información
www.acis.org.co/

¡ Afiliate ya !

y disfruta de estos beneficios

Valor: $300.000 COP anuales + IVA

Candidatura a Codirector de Grupo de Interés.

Candidatura a Miembro del Consejo Editorial de la Revista SISTEMAS.

Candidatura a Miembro de la Junta Directiva de ACIS.

100% de descuento en un (1) evento ACIS.

25% de descuento a partir del segundo evento.

Recepción trimestral de la revista SISTEMAS en formato digital.

Acceso diferido a la base de Webinars de ACIS.

Consulta permanente de servicios al afiliado

Acceso exclusivo a oportunidades laborales a través de nuestro portal de empleo.

Participación como conferencista o participante en las charlas semanales.

Correo personal con @acis.org.co

Asista a las funciones del Teatro Nacional con un 20% de descuento. Consulte la Programación y solicite el descuento a cursos@acis.org.co.

30% de descuento en los libros de la Casa Editorial ALFAOMEGA, consulte el Catálogo

mas información en :
www.acis.org.co
suscripciones@acis.org.co
301553054