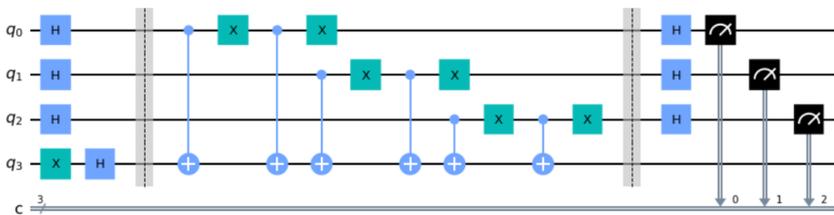


Sonia Rubio Herranz
Rebeca Carpio López
Antonio Díaz-Cano Ocaña
Antonio López Montes

COMPUTACIÓN CUÁNTICA. EMPEZAMOS.

Estados Cuánticos Entrelazados, Puertas
Cuánticas, Criptografía Postcuántica y Oráculos



PRIMERA EDICIÓN.

Dentro del universo hay cosas que son conocidas
y hay cosas que son desconocidas.

En medio de esas cosas hay puertas.

William Blake (1757 - 1827)

Prologo.

Suelo decir a mis colaboradores que un porcentaje de la actividad investigadora tiene que estar dirigido a áreas y cuestiones distintas al área en el que uno está centrado. No sólo para conectar su investigación con problemáticas, metodologías y soluciones aparentemente lejanas, sino para potenciar la necesaria creatividad que exige una auténtica mentalidad investigadora.

Y consistentemente, también les suelo decir a mis colaboradores que otro porcentaje de su tiempo debe dedicarse a lo que podríamos llamar “divulgación”, entendiendo esta “divulgación” como anzuelos que lanzamos casi al azar para provocar en otros profesionales esas conexiones, y atraer a otros investigadores (y sobre todo estudiantes), para que quieran colaborar con nosotros.

Los científicos tenemos que hacer un esfuerzo constante para encontrar las visiones de otros investigadores que puedan sernos útiles, y en justa reciprocidad, tenemos que facilitar que esos investigadores (y sobre todo estudiantes) puedan identificar nuestras propias visiones.

Los estudiantes (y los que no son especialistas) siempre agradecen textos que les ayuden a comprender mejor las bases y componentes de cada modelo, a través de documentos de carácter más docente, intermedios entre la conferencia y los textos puramente científicos, que serán en todo caso la referencia última a estudiar.

Los documentos intermedios son más necesarios en áreas como la computación cuántica, campo en el que por su relativa novedad pueden existir pocos textos de este tipo.

Como me dijo hace ya muchos años un tutor que me escuchó en una de mis primeras conferencias en el extranjero, el objetivo último del

profesor tiene que ser enganchar al otro, para que le lean y le estudien.

El planteamiento de este manuscrito que acabo de leer (su estructura, el lenguaje utilizado, las motivadoras explicaciones y los ilustrativos ejemplos) cumplen con la misión de motivar al lector, sembrando en su cabeza la necesidad de aprender más sobre el tema.

Los autores han conseguido plenamente el objetivo de acercar su ciencia y conocimiento a los no especialistas.

De entrada, han conseguido que yo mismo, que no sabía nada de computación cuántica, me ponga a estudiar cómo implementar la computación cuántica en mi propia investigación.

Prof. Francisco Javier Montero de Juan.

Catedrático del Departamento de Estadística e Investigación
Operativa.

Universidad Complutense de Madrid.

Nota sobre los autores.

Sonia Rubio Herranz es Licenciada en Matemáticas por la Universidad Complutense de Madrid. Actualmente es Profesora en la Universidad Nacional de Educación a Distancia y del Departamento de Estadística e Investigación Operativa de la Universidad Complutense de Madrid.

Rebeca Carpio López es graduada en Ingeniería Matemática por la Universidad Complutense de Madrid. Actualmente desarrolla proyectos de Data Science e Inteligencia Artificial

Antonio Díaz-Cano Ocaña es Licenciado en Físicas y Matemáticas y Doctor en Matemáticas. Actualmente es Profesor Titular del Departamento de Álgebra, Geometría y Topología de la Universidad Complutense de Madrid.

Antonio López Montes es Licenciado en Físicas y Doctor en Matemáticas. Actualmente es Profesor Contratado Doctor en el Departamento de Análisis Matemático y Matemática Aplicada de la Universidad Complutense de Madrid.

Índice

Introducción: ¿por qué este libro y por qué ahora?

PRIMERA PARTE. CONCEPTOS TEÓRICOS Y FUNDAMENTO MATEMÁTICO

1. Introducción a la Computación Cuántica.
 - 1.1 Bits y Bytes.
 - 1.2 Física y Mecánica Cuántica, Bases Cuánticas de la Computación Cuántica y Supremacía Cuántica
 - 1.3 Algebra y Mecánica Cuántica.
 - 1.4 Origen y evolución de la Computación Cuántica.

2. Conceptos básicos en Computación Cuántica. Puertas Cuánticas y Circuitos Cuánticos.
 - 2.1 Bits y Cúbits. Esfera de Bloch.
 - 2.2 Operaciones con Bits y Cúbits.
Compuertas Clásicas vs Puertas Cuánticas.
 - 2.3 Sistemas con múltiples Cúbits.
Puertas Cuánticas para n Cúbits.
 - 2.4 Un Circuito Cuántico con equivalente clásico. La Suma Cuántica.
 - 2.5 Un Circuito Cuántico sin equivalente clásico.
 - 2.6 Transformada Cuántica de Fourier.

3. Criptografía, Criptografía Cuántica, Criptografía Postcuántica.
 - 3.1 Clave Privada y Clave Pública.
 - 3.2 Sistema Criptográfico RSA y Números Primos.
 - 3.3 Criptografía Cuántica y Postcuántica. Intercambio Cuántico de Claves.

SEGUNDA PARTE. PROGRAMACIÓN Y ALGORITMOS CUÁNTICOS.

4. Algoritmos Cuánticos y Programación en Qiskit.
 - 4.1 Primeros Pasos.
 - 4.2 Algoritmo de Suma de tres Cúbits.
 - 4.3 Los Oráculos en Computación Cuántica. Algoritmo de Deutsh-Jozsa.
 - 4.4 Los Números Primos y la Computación Cuántica. Algoritmo de Shor.
 - 4.5 Un ejemplo de aplicación de la Computación Cuántica a la resolución de un problema de regresión.

5. Referencias