De Hilbert a los algoritmos cuánticos: el rol del álgebra en el desarrollo de la computación

From Hilbert to quantum algorithms: the role of algebra in the development of computing

[1]Daniel Steven Moran Pizarro, [2]Sandra Johana Domínguez Bonilla, [3]Carolina Castaño Gutiérrez, [4]Ciro Efraín Martínez Baez

[1,2,3,4] *Universidad Nacional Abierta y a Distancia, Colombia*

Recibido:20/10/2023 Aprobado 20/11/2023

Resumen

En este artículo se examina el papel fundamental y transformador que ha desempeñado el álgebra en la evolución de la computación, desde la formulación de los problemas de Hilbert hasta el desarrollo de los algoritmos cuánticos modernos. Al iniciar con un análisis histórico, se destaca cómo la evolución del álgebra se entrelaza intrínsecamente con los avances en la resolución de los problemas planteados por Hilbert. A medida que se avanza en la línea del tiempo, es clara la influencia de los fundamentos algebraicos sólidos en la aparición de la teoría de la computación y los primeros algoritmos, abriendo el camino a una era de desarrollo tecnológico sin precedentes. En la era contemporánea, surge la computación cuántica como tecnología emergente de la industria 5.0, que se basa en conceptos algebraicos avanzados para su funcionamiento. Se termina con una discusión de la relevancia continua del álgebra en los desarrollos tecnológicos pasados y futuros y la importancia de una sólida base matemática para abordar los desafíos de la industria 5.0. A través de esta exploración, se resalta la importancia del álgebra como un pilar central en el desarrollo de la ciencia de la computación y, en última instancia, su impacto en la configuración de nuestro futuro tecnológico.

Palabras clave: álgebra, computación cuántica, historia de las matemáticas, industria 5.0, problemas de Hilbert, teorías de la computación.

Citación: Moran Pizarro, D. S. ., Dominguez Bonilla, S. J. ., Castaño Gutierrez, C. ., & Martinez Bez, C. E. . (2023). De Hilbert a los algoritmos cuánticos: el rol del álgebra en el desarrollo de la computación. Publicaciones E Investigación, 17(4). https://doi.org/10.22490/25394088.7503

[1]Cdaniel.moran@unad.edu.co / https://orcid.org/0000-0003-1791-2818
[2]sandra.dominguez@unad.edu.co / https://orcid.org/0000-0002-8993-5800
[3]carolina.castano@unad.edu.co / https://orcid.org/0000-0002-4521-979X
[4]ciro.martinez@unad.edu.co / https://orcid.org/0000-0001-9335-8885

https://doi.org/10.22490/25394088.7503

Abstract

This presentation examines the fundamental and transformative role algebra has played in the evolution of computing, from the formulation of Hilbert's problems to the development of modern quantum algorithms. By starting with a historical analysis, it highlights how the evolution of algebra is intrinsically intertwined with advances in solving the problems posed by Hilbert. As we move along the timeline, the influence of solid algebraic foundations on the emergence of computation theory and early algorithms is clear, paving the way for an unprecedented era of technological development. In the contemporary era, quantum computing emerges as an emerging Industry 5.0 technology, which relies on advanced algebraic concepts for its operation. It concludes with a discussion of the continuing relevance of algebra in past and future technological developments and the importance of a solid mathematical foundation to address the challenges of Industry 5.0. Through this exploration, the importance of algebra as a central pillar in the development of computer science is highlighted, and ultimately its impact in shaping our technological future.

Keywords: Algebra, quantum computing, history of mathematics, industry 5.0, Hilbert problems, theories of computation.

1. Introducción

La evaluación de la computación y la tecnología tienen una herramienta fundamental y básica, la cuál es el álgebra. Este artículo atraviesa por la formulación y comprensión de los problemas de Hilbert avanzando hacia el seguimiento de los algoritmos cuánticos modernos. Esta herramienta fundamental ha facilitado el camino para el desarrollo tecnológico sin precedentes que favorece el surgimiento de la computación cuántica como tecnología emergente de la industria 5.0.

2. Materiales y métodos

Éste estudio se basa en un enfoque de investigación cualitativa y documental (Colomer, 1990; Corona *et al.,* 2016; Morin, 1999). Para trazar la relación entre el álgebra y la evolución de la computación, se utilizan herramientas de múltiples disciplinas, incluyendo matemáticas, historia de las matemáticas, ciencias de la computación e ingeniería (Recalde, 2018).

La recopilación de fuentes primarias y secundarias proporcionan una visión detallada de la formulación y el intento de resolución de los problemas de Hilbert en su contexto histórico. Al revisar trabajos académicos y textos históricos se detalla el desarrollo del álgebra y su influencia en la solución a los problemas de Hilbert.

Para analizar la evolución de la relación entre el álgebra y la computación, se analizan fuentes académicas que trazan el desarrollo de la teoría de la computación y los algoritmos desde sus inicios hasta la actualidad. Tanto textos históricos como de literatura contemporánea sirven para entender cómo el álgebra ha influenciado en estos avances.

Finalmente, para explorar la aplicación actual y futura del álgebra en la computación cuántica, se recurre a estudios recientes en el campo de la computación cuántica. Se utilizan textos académicos y técnicos que detallan el funcionamiento de la computación cuántica y cómo se basa en principios algebraicos.

3.Desarrollo

David Hilbert, un matemático alemán de finales del siglo XIX y principios del XX, introdujo una lista de 23 problemas no resueltos en 1900 (Hilbert, 1900; Kinyon, 2002), que catalizaron mucha de la investigación matemática en el siglo XX. Dentro de los problemas planteados por Hilbert, llama la atención especialmente el segundo, el cual puede enunciarse de la siguiente manera:

"Probar que los axiomas de la aritmética son consistentes (esto es, que la aritmética es un sistema formal que no supone una contradicción)".

Su segundo problema pidió una prueba de que los axiomas que subyacen a la aritmética son consistentes. La consistencia, en este sentido, significaría que no hay contradicciones inherentes en las reglas de la aritmética.

Maxime esto, de ser una época muy delicada respecto a los fundamentos de las matemáticas. Por ejemplo, la paradoja de Russell generó gran preocupación por los cimientos de la lógica, la teoría de conjuntos y los propios cimientos de las matemáticas.

Russell define el conjunto R de la siguiente manera:

R={x/x no se pertenecen a sí mismos}.

Supongamos que el conjunto R se pertenece a sí mismo. Al ser un elemento de R, y dado que en R están los conjuntos que no se pertenecen a sí mismos, el conjunto R no se pertenece a sí mismo. De otro lado, si R no se pertenece a R, tendríamos que R es un elemento del mismo R. En conclusión, R∈R y R∉R.

Aunado a esto, tratando de fundamentar la aritmética y evitar todo el caos de la paradoja de Russell, en 1912 aparece Russell en coautoría de Whitehead, con el primer capítulo de los *Principia Mathematica*, cuyo propósito principal era demostrar que la lógica constituía el fundamento de las matemáticas, pero, aun así, el problema segundo de Hilbert seguía sin resolver.

En el esfuerzo por resolver este problema, se creó un cuerpo de trabajo conocido como los fundamentos de las matemáticas, que buscaba descubrir la base lógica de todos los cálculos matemáticos. Se esperaba que esta base lógica permitiese una prueba de consistencia, dando así una respuesta al segundo problema de Hilbert.

En 1931, Kurt Gödel, un matemático austriaco, demostró con sus teoremas de incompletitud que tal prueba de consistencia no puede existir. Estos teoremas establecen que en cualquier sistema formal suficientemente potente como para describir los números enteros, siempre existen proposiciones que no pueden ser probadas ni refutadas dentro del sistema. Esto significa que la consistencia de los axiomas de la aritmética no puede probarse utilizando solo la aritmética.

Este resultado fue un terremoto en el campo de los fundamentos de las matemáticas, dejando una crisis en su estela. Sin embargo, también abrió la puerta a nuevas formas de entender la lógica y la computación.

Uno de los que se sintieron inspirados por los resultados de Gödel fue Alan Turing, un matemático británico. Turing desarrolló el concepto de una "máquina universal" que podría realizar cualquier cálculo dado un conjunto de instrucciones y suficiente tiempo. Este concepto, conocido como la máquina de Turing, es el fundamento de todas las computadoras digitales modernas. Y, de cierta forma, podríamos apreciar que, en las ideas de Turing, está Gödel, dado que en los problemas de decidibilidad están en esencia los problemas de incompletitud.

Pero la máquina de Turing, aunque poderosa, tiene sus limitaciones. Existen problemas que no puede resolver, un ejemplo destacado de esto es el halting problem, el cual fue demostrado como indecidible por el mismo Turing en 1936 (Turing, 1936). Turing demostró que no existe un algoritmo general que pueda determinar si un programa arbitrario terminará o no. Si bien, existe el algoritmo para la solución del problema, no necesariamente va a resolverse en un "tiempo razonable". De este tipo de problemas se ocupa la complejidad computacional.

A medida que las demandas de cálculos más rápidos y eficientes crecieron en el siglo XXI, las limitaciones de las máquinas de Turing se hicieron más evidentes. Aquí es donde entra en juego la computación cuántica.

Es en 1980 que el físico Paul Benioff sugiere que la mecánica cuántica podría utilizarse para la computación. La computación cuántica aprovecha los fenómenos cuánticos de superposición y entrelazamiento para realizar cálculos. A diferencia de la computación clásica, que se basa en bits que pueden estar en uno de dos estados (0 o 1), la computación cuántica utiliza qubits que pueden existir en múltiples estados a la vez. Esta capacidad permite a las computadoras cuánticas procesar una gran cantidad de información simultáneamente, ofreciendo la posibilidad de realizar cálculos mucho más rápidos que las computadoras clásicas para ciertas clases de problemas.

De cierta manera, la computación cuántica es a las máquinas de Turing, lo que la mecánica cuántica fue a la mecánica clásica de Newton, un total cambio de paradigma desde su epistemología intrínseca hasta el uso de sus métodos. En la siguiente tabla, se muestran algunas de las matemáticas modernas que confluyen en el desarrollo de la computación cuántica Hayashi, 2016; Microsoft, 2023; Ramírez, 2020; Turing, 1936).

4. Discusión

A medida que las demandas de cálculos más rápidos y eficientes crecieron en el siglo XXI, las limitaciones de las máquinas de Turing se hicieron más evidentes. Aquí es donde entra en juego la computación cuántica.

Es en 1980 que el físico Paul Benioff sugiere que la mecánica cuántica podría utilizarse para la computación. La computación cuántica aprovecha los fenómenos cuánticos de superposición y entrelazamiento para realizar cálculos. A diferencia de la computación clásica, que se basa en bits que pueden estar en uno de dos estados (0 o 1), la computación cuántica utiliza qubits que pueden existir en múltiples estados a la vez. Esta capacidad permite a las computadoras cuánticas procesar una gran cantidad de información simultáneamente, ofreciendo la posibilidad de realizar cálculos mucho más rápidos que las computadoras clásicas para ciertas clases de problemas.

De cierta manera, la computación cuántica es a las máquinas de Turing, lo que la mecánica cuántica fue a la mecánica clásica de Newton, un total cambio de paradigma desde su epistemología intrínseca hasta el uso de sus métodos. En la siguiente tabla, se muestran algunas de las matemáticas modernas que confluyen en el desarrollo de la computación cuántica (Hayashi, 2016; Microsoft, 2023; Ramírez, 2020; Turing, 1936).

Tabla 1. Ramas de las matemáticas que alimentan la computación cuántica

Objeto matemático	Descripción	Aplicación en computación cuántica
Notación de Dirac	La notación bra-ket es utilizada en la mecánica cuántica para describir los estados cuánticos.	Facilita la descripción de los estados cuánticos (qubits) y las amplitudes de probabilidad asociadas.
Operadores lineales	En álgebra lineal, los operadores lineales actúan sobre vectores para producir nuevos vectores.	Se utilizan para describir las transformaciones cuánticas (puertas cuánticas), incluyendo la evolución de los sistemas cuánticos con el tiempo.
Producto tensorial	Es una operación entre dos espacios vectoriales que genera un nuevo espacio.	Esencial para describir sistemas de múltiples qubits y el entrelazamiento cuántico, un recurso crucial para el cómputo cuántico y la teleportación cuántica.
Álgebra de Clifford	Es un tipo de álgebra asociativa que generaliza el álgebra de los números reales, complejos y cuaternios.	Provee una descripción eficiente de las puertas cuánticas, permitiendo la manipulación algebraica de las operaciones cuánticas.
Álgebra de Pauli	Es un conjunto de matrices 2x2 que forman una base para las operaciones de un solo qubit.	Provee una descripción de las operaciones básicas sobre un solo qubit. Estas operaciones son fundamentales para los algoritmos cuánticos, incluyendo la rotación de qubits y el cambio de fase.
Grupos y campos finitos	Son estructuras algebraicas utilizadas para describir operaciones y relaciones entre elementos.	Fundamentales para los códigos de corrección de errores cuánticos, que son esenciales para contrarrestar los efectos de la decoherencia y el ruido, permitiendo así el funcionamiento confiable de una computadora cuántica.

Dada esta amplia gama de las matemáticas, dentro de la exploración se muestra la siguiente tabla de dualidad de objetos matemáticos. Este tipo de análisis aporta a la propia epistemología de los conceptos matemáticos, y a la ontología de estos. Este paralelo, relaciona los conceptos de la computación clásica, con los objetos de la computación cuántica.

Tabla 2. Dualidad objetos de la computación clásica con los objetos de la computación cuántica

Concepto en computación clásica	Concepto en computación cuántica	Descripción
Bit	Qubit	Un bit es la unidad fundamental de información en la computación clásica, y puede estar en uno de dos estados: 0 o 1. Un qubit es la unidad fundamental de información en la computación cuántica, y puede estar en una superposición de estados 0 y 1.
Puertas lógicas	Operadores cuánticos	Las puertas lógicas son operaciones que actúan sobre uno o más bits, implementando funciones booleanas. Los operadores cuánticos son operaciones que actúan sobre uno o más qubits, implementando transformaciones lineales en el espacio de Hilbert.
Estados discretos (0 o 1)	Superposición de estados	En la computación clásica, un bit sólo puede estar en un estado a la vez (0 o 1). En la computación cuántica, un qubit puede estar en una superposición de estados, es decir, puede representar 0, 1, o cualquier combinación de ambos al mismo tiempo.
Almacenamiento de información	Entrelazamiento cuántico	En la computación clásica, los bits son entidades independientes. En la computación cuántica, los qubits pueden estar entrelazados, lo que significa que el estado de un qubit puede estar directamente correlacionado con el estado de otro, sin importar la distancia entre ellos.

5. Conclusiones

Desde Hilbert hasta la computación cuántica, hemos visto una increíble evolución en la forma en que entendemos y manipulamos la información, lo cual exalta la manera en la cual el progreso en matemáticas y física puede llevar a cambios revolucionarios en tecnología e industria. El papel de la historia en esto es de suma importancia, ya que entender cómo llegamos a la computación cuántica nos ayuda a entender mejor cómo podemos avanzar hacia el futuro.

La comprensión profunda del álgebra es fundamental para entender tanto la computación clásica como la cuántica. A nivel básico, el álgebra es esencial para entender las operaciones lógicas en la computación clásica. Pero a un nivel más profundo, los conceptos de álgebra lineal y espacios de Hilbert son esenciales para entender la naturaleza de los qubits y las operaciones cuánticas.

En la era de la industria 5.0, la computación cuántica tiene el potencial de cambiar completamente cómo resolvemos problemas y diseñamos tecnología. Por lo tanto, es vital que la educación y la formación en campos técnicos y científicos incluyan una sólida base en matemáticas y una comprensión de la historia de la computación. Esto permitirá a los futuros investigadores y profesionales comprender y aprovechar al máximo las posibilidades que ofrece la computación cuántica. Y al entender la historia y la evolución de la computación, estarán mejor equipados para prever y dar forma a futuros avances. Así, la historia de las matemáticas y el álgebra no son simplemente temas de interés académico, sino herramientas esenciales para preparar a la próxima generación para la era de la industria 5.0.

Referencias

Colomer, E. (1990). *Historia del Pensamiento Alemán de Kant a Heidegger.* Editorial Herder.

Corona, J., Kovac, M., Mijares, M., Grimaldos, R. (2016). The phenomenology of Edmund Husserl, Martin Heidegger and Alfred Schütz. *International Journal of Philosophy and Social-Psychological Sciences, 2*(4), 86-90.

Hayashi, M. (2016). *Quantum Information Theory: Mathematical Foundation*. Springer Verlag.

Hilbert, D. (1900). *Mathematische Probleme, Von David Hilbert (1900).* https://web.archive.org/web/20120205025851/http://www.mathematik.uni-bielefeld.de/~kersten/hilbert/rede.html

Kinyon, M. (Ed.). (2002). On Hilbert and his 24 Problems. En: *Proceedings of the Joint Meeting of the CSHPM 1 3*(2002)1-22.

Microsoft (2023). *Álgebra lineal para la computación cuántica. Azure Quantum.* https://learn.microsoft.com/es-es/azure/quantum/overview-algebra-for-quantum-computing

Morín, E. (1999). *Pensamiento Complejo.* Editorial L Harmattan.

Ramírez, P. (2020). *Introducción a la computación cuántica y sus aplicaciones*. (Trabajo de grado). Universidad de Cádiz.

Recalde, L. (2018). *Lecturas de historia de las matemáticas.* Editorial Universidad del Valle.

Turing, A. (1936). On Computable Numbers, with an Application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society, 2*(1), 230-265. doi:10.1112/plms/s2-42.1.230

Yanofsky, N. & Mannuci, M. (2008). *Quantum Computing for Computer Scientists.* Cambridge University Press.