

Introducción

December 8, 2023

Contents

En los últimos años, se encuentra en el centro de la discusión el avance que supone la computación cuántica. Al respecto se suele mencionar la revolución en el campo de la encriptación que supondría el algoritmo de Shor [3], que impediría utilizar algoritmos que se basen en que la factorización en primos de un entero es NP. No obstante, este no es el único caso en el que la computación cuántica podría significar una diferencia con respecto a la computación clásica, ya que en el campo de la optimización combinatoria de problemas también se proponen varios algoritmos alternativos que permitirían una mejora en la complejidad.

Esta superioridad, es todavía teórica, ya que en la era NISQ (Noisy Intermediate-Scale Quantum era [2]) no es posible el uso de procesadores cuánticos con muchos qubits y poco ruido en sus ejecuciones. Esto provoca la aparición de algoritmos híbridos, como QAOA [1] o VQE, que combinan la ejecución de circuitos cuánticos pequeños con el pre y postprocesamiento en un ordenador clásico.

Esto provoca la aparición de algoritmos híbridos, en los que un procesador cuántico genera un estado cuántico a través de un circuito parametrizado según un conjunto de variables obtenidas de un procesador clásico.

Dentro de los llamados algoritmos híbridos

Tanto el algoritmo QAOA como el algoritmo de quantum annealing tienen como utilidad resolver problemas tipo QUBO (Quadratic Unconstrained Binary Optimization), en los que se busca un extremo (máximo o mínimo global) de una función binaria. Aunque sirvan para el mismo propósito, las técnicas que se utilizan son completamente diferentes.

- El algoritmo QAOA está pensado para ser aplicado en computadores cuánticos de uso generalista basados en puertas, los cuales son el proyecto más ambicioso a día de hoy dentro del campo de la computación cuántica, que servirían para resolver cualquier tipo de problema al ser sistemas Turing completos.
- Los computadores en los que se aplica quantum annealing, como es el caso de los proporcionados por D-Wave, no son Turing-completos y tienen como única utilidad resolver problemas utilizando este algoritmo. Este es el motivo por el que parece haber una superioridad tan grande entre D-Wave, que comercializa sistemas con más de 5000 qubits, y los sistemas de uso generalista, que no alcanzan los 1000 qubits manteniendo un funcionamiento tolerante a fallos ¹.

References

- [1] E. Farhi, J. Goldstone, and S. Gutmann. A quantum approximate optimization algorithm, 2014.
- [2] J. Preskill. Quantum computing in the nisq era and beyond. *Quantum*, 2:79, Aug. 2018.

¹Es importante recalcar que el auténtico problema de estos computadores no es aumentar el número de qubits, sino aumentarlo sin incrementar el ruido del sistema.

- [3] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, Oct. 1997.