

1 Introduction

Quantum computing has meant a paradigm shift in computer science, introducing a new era of computational power and possibilities. By leveraging the principles of quantum mechanics, quantum computing offers capabilities far beyond those of classical computers. Although quantum hardware is still evolving, Noisy Intermediate-Scale Quantum (NISQ) [1] computers have already begun to unveil the potential of quantum computing, igniting widespread interest in implementing quantum algorithms that promise significant speedups over classical counterparts. In particular, the speedup of solving NP-complete problems is an area that quantum computing can tackle. In this paper, we have focused on the Hamiltonian Cycle Problem.

This problem is one of Karp’s 21 seminal NP-complete problems, it involves determining whether a given graph contains a Hamiltonian cycle—a cycle that visits every vertex exactly once. The problem is significant because of its similarities with the TSP, and its applications span various domains, including logistics and network optimization, where identifying optimal cycles is crucial AGREGAR CITAS. Traditional solution methods range from brute force approaches to sophisticated algorithms like dynamic programming and Monte Carlo simulations. In this paper, we propose utilizing Grover’s algorithm to tackle the HC problem, offering the potential for quadratic speedup.

The structure of this paper is as follows. An explanation of Grover’s algorithm is given in Section II. The proposed methodology is given in Section III. Section IV explores the existing solutions for the problem and compares the theoretical results.

2 Background

2.1 Grover’s Algorithm

The search algorithm developed by Lov K. Grover in 1997 [2] is a milestone in the development of quantum algorithms. It solves the problem of finding a tagged element (or M elements) in a disordered set of N elements using $k_{Gr} = \lfloor \frac{\pi}{4} \sqrt{\frac{N}{M}} \rfloor$ times a system, called oracle, which is able to identify this element. It presents a quadratic improvement in order relative to the classical brute-force search algorithm, which requires in the worst-case scenario N system calls. Grover’s algorithm does not converge with 100% probability to the desired state, it converges with an arbitrarily high probability that depends on the relationship between solutions and the size of the search space.

As Grover proposed later, the algorithm can be used to speed up the solution of NP-complete problems [3]. Since, its application has been explored with some problems such as Clique problem [4, 5], k-coloring [6, 7] and SAT [8, 9]. Nielsen and Chuang predicted the solution of the HC problem using Grover[10].

The original problem presented by Grover [2] is as follows. Let there be a set of $N = 2^n$ quantum states in a Hilbert space (\mathcal{H}_n), where n is the number of qubits, and an unknown canonical basis state marked between them (solution to the problem). Given a system, an operator, called an oracle that identifies the marked element, the objective is to find this marked element with high probability, using as few queries to the oracle as possible.

Let $|t\rangle$ be the marked element of the base, and $|s\rangle$ the uniform superposition of all basis states. An oracle operator $O = I_d - 2|t\rangle\langle t|$ is applied and changes the phase of the marked state. A diffusion operator $D = I_d - 2|s\rangle\langle s|$ is applied and amplifies the amplitude of the marked state. Applying the Grover operator ($G = DO$) k_{Gr} times maximizes the probability of measuring $|t\rangle$. A more detailed and extended explanation for when the set has more than one solution can be found in reference [10].

AGREGAR DIAGRAMA DE GROVER QUE ESTE LINDO.

2.2 Hamiltonian Cycle Problem

Explicamos qué es el Hamiltonian Cycle Problem. Explicamos cuáles son los principales usos de resolver el HCP. Consultamos las heurísticas actuales de resolución del HCP.

3 Proposed Algorithm for Hamiltonian Cycle Problem

In order to solve a NP-complete problem with Grover's algorithm, it is necessary to translate a decision problem into a search problem. First, every possible cycle is encoded into a binary code. Let $G = (V, E)$ be the input graph with N vertices and e edges. $V = (v_1, \dots, v_N)$ For every vertex, $n = \lceil \log_2 N \rceil$ are used to indicate the position it occupies in the cycle.

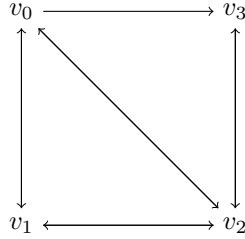


Figure 1: Example Graph

For example the bitstring 11,00,01,10 would be translated to $3 - 0 - 1 - 2$. This means v_0 is on the position 3, v_1 in on the position 0 and so on. The resulting cycle is (v_1, v_2, v_3, v_0) . The search space includes every possible permutation of the positions of the vertices in the hamiltonian cycle. Therefore, its size is $2^{N \log n} = N^N$. The solutions of the HC problem satisfy two conditions:

1. Each vertex should have a different position.
2. Vertices with consecutive positions have to be connected by an edge. (The last and first positions are considered adjacent)

An algorithm to solve the HCP of a directed graph with $N = 2^n$ vertices is presented. The main contribution of this paper is the oracle O that flips the phase of the states that satisfy both constraints. Later, possible adaptations of the algorithm for arbitrary graphs are proposed.

The comparator circuit is applied to the C_2^N combinations of position indexes, and each result is stored in a different qubit of $|\theta\rangle$. If any two vertices are assigned the same position, at least one qubit in $|\theta\rangle$ will be in state $|0\rangle$.

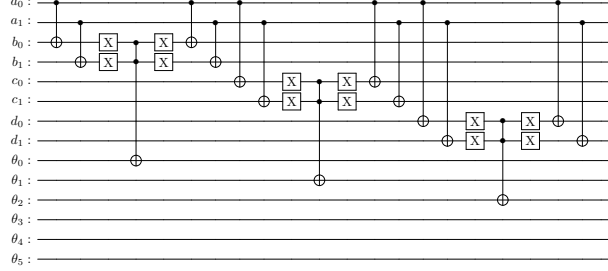


Figure 3: First three comparisons in the Positional Exclusivity block

3.3.2 Missing Edge Detector Block

Another subcircuit is introduced in this part, called the Plus One circuit. This circuit takes state $|i\rangle$ to state $|(i + 1) \bmod 2^p\rangle$. Given a register q with p qubits, a MCT is applied with the $p - 1$ least significant qubits as control, and the most significant qubit as the target. This process is repeated taking with the $p - 1$ least significant bits, so that every step the MCT has one less control. The inverse circuit, named Minus One circuit, takes state $|i\rangle$ to state $|(i - 1) \bmod 2^p\rangle$.

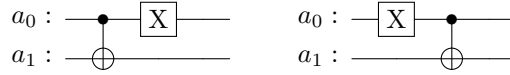


Figure 4: 2 qubits Plus One circuit and Minus One Circuit

The missing edges set is defined as the set of edges of the complementary graph. In the example, the set of missing edges is $\{(1, 3), (3, 1), (3, 0)\}$. To satisfy the second constraint, the vertices on adjacent positions should not have a missing edge between them.

The Plus One circuit is used to take the vertex to the next position, and then the Comparator circuit is used on the vertexes of the missing edge. If the next position of the vertex is occupied by a vertex that has a missing edge between them, the Comparator will flip an ancilla qubit.

3.3.3 Complete Oracle Structure

The complete oracle consists of the Positional Exclusivity Block, a Missing Edge Block, and a multi-controlled phase shift, acting in all the ancilla qubits. Then, the Positional Exclusivity Block and the Missing Edge Block are repeated to return the ancillas to their original state.

INSERTAR IMAGEN DE TODO EL ORACULO

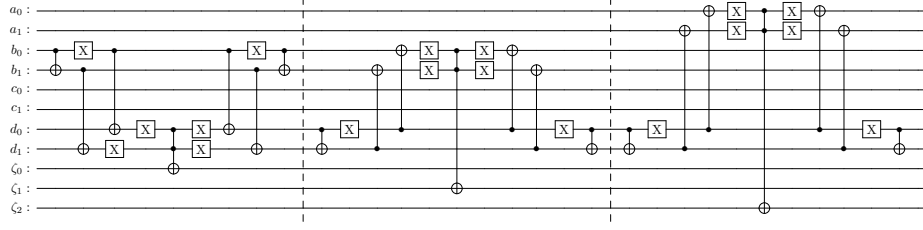


Figure 5: Missing Edge block of the example above

4 Generalization for an arbitrary graph

5 Informacion relevante para el futuro

References

- [1] J. Preskill, “Quantum computing in the nisq era and beyond,” *Quantum*, vol. 2, p. 79, Aug. 2018.
- [2] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC ’96, (New York, NY, USA), p. 212–219, Association for Computing Machinery, 1996.
- [3] N. J. Cerf, L. K. Grover, and C. P. Williams, “Nested quantum search and structured problems,” *Phys. Rev. A*, vol. 61, p. 032303, Feb 2000.
- [4] A. Bhaduri, A. Saha, B. Saha, and A. Chakrabarti, “Circuit design for clique problem and its implementation on quantum computer,” *IET Quantum Communication*, vol. 3, p. 30–49, Dec. 2021.
- [5] A. Bhaduri, A. Saha, B. Saha, and A. Chakrabarti, “Robust quantum circuit for clique problem with intermediate qudits,” *Nano Communication Networks*, vol. 37, p. 100466, Sept. 2023.
- [6] A. Saha, D. Saha, and A. Chakrabarti, “Circuit design for k-coloring problem and its implementation on near-term quantum devices,” in *2020 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNisS)*, pp. 17–22, 2020.
- [7] S. Mukherjee, “A grover search-based algorithm for the list coloring problem,” *IEEE Transactions on Quantum Engineering*, vol. 3, pp. 1–8, 2022.
- [8] W.-L. Yang, H. Wei, F. Zhou, W.-L. Chang, and M. Feng, “Solution to the satisfiability problem using a complete grover search with trapped ions,” *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 42, p. 145503, jun 2009.
- [9] S.-W. Lin, T.-F. Wang, Y.-R. Chen, Z. Hou, D. Sanán, and Y. S. Teo, “A parallel and distributed quantum sat solver based on entanglement and quantum teleportation,” 2023.

- [10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.
- [11] L. K. Grover, “Quantum mechanics helps in searching for a needle in a haystack,” *Physical Review Letters*, vol. 79, p. 325–328, July 1997.