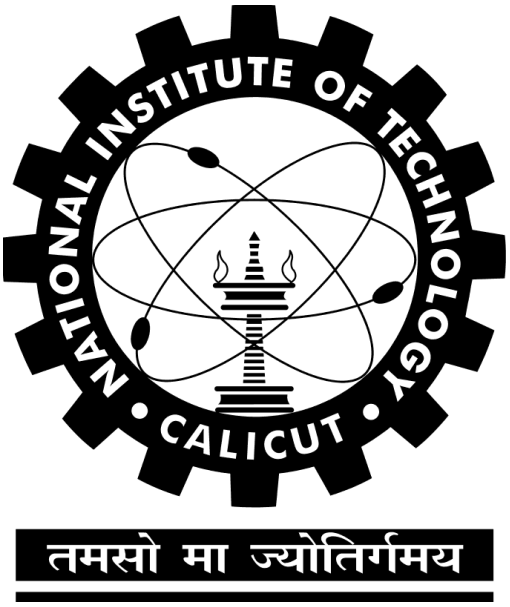
Report on

QUANTUM SEARCH AND ITS BREADTH OF APPLICATIONS

Submitted by

Gagan Lal B190480CS
Geethika S B190449CS
Moturu Manogna B190695CS
Nihal Muhammad Asharaf B190721CS



Department of Computer Science and Engineering
National Institute of Technology Calicut
Calicut, Kerala, India - 673 601

DECEMBER 05, 2022

QUANTUM SEARCH AND ITS BREADTH OF APPLICATIONS

Gagan Lal *Geethika S* *Moturu Manogna* *Nihal Muhammad Asharaf*

Abstract- **Informally, the search problem can be described as finding an item with a specific property in a given set of N items. A search algorithm retrieves the desired information or path from a specific search space, where instances can be categorical or continuous. Recent studies in the domain of quantum computing have paved way for the development of quantum algorithms. Quantum computing search algorithms have greatly outperformed classical algorithms. The property of superposition of states exhibited by qubits allows them to exist in multiple states at a time using which the quantum algorithm is able to perform multiple operations at the same time and this has reduced the search time complexity when compared to classical algorithms. Here we review some of the search algorithms and applications of quantum search algorithms.**

I. INTRODUCTION

Informally, the search problem can be described as finding an item with a specific property in a given set of N items. A search algorithm retrieves the desired information or path from a specific search space, where instances can be categorical or continuous. The efficiency of an algorithm is decided by its time complexity and space complexity. Unlike classical computers which can only perform operations by manipulating binary bits with the values 0 and 1, quantum bits can represent data in multiple states. The property of inheriting multiple states at the same time provides quantum computers with enormous power over classical computers. With this power, algorithms designed on quantum computers to solve search queries can produce results much faster than classical algorithms.

A quantum bit, or qubit, is the fundamental unit of quantum computing, similar to its classical computing counterparts. At the same time, qubits can exist in a coherent superposition of several states between 0 and 1. The main difference between classical bits and qubits is that measuring the value of bits does not disturb the classical bit's state, whereas the Qubit loses coherence and its superposition state is irreversibly disturbed.

Quantum computing search algorithms have greatly outperformed classical algorithm speed using the property of superposition. The property of superposition of states exhibited by qubits allows them to exist in multiple states at a time using which the algorithm is able to perform multiple operations at the same time and this has reduced the search time complexity to O ($\sqrt{N}$) which is even lower than O (N) in the classical computing where N is the total number of instances present in the search space.

II. QUANTUM SEARCH ALGORITHMS

A. Grover's search algorithm

Grover quantum search algorithm was proposed by Indian scientist Lov Kumar Grover in 1996. It is one of the most important quantum search algorithm. The Grover's algorithm solves the problem of searching in an unstructured database with N entries in O ($\sqrt{N}$) time and using O (log N) storage space. This algorithm significantly improves the efficiency of search. It achieves quadratic speedup over classical search algorithms. Grover's algorithm is probabilistic in the sense that it gives correct answer with high probability. The probability of failure can be reduced by repeating the algorithm.

A.1 Statement of The Problem

Given a classical function f (x): $\{0, 1\}^n \rightarrow \{0, 1\}$ where n is the bit-size of the search space, find an input x0 for which f(x0) = 1. The complexity of the algorithm is measured by the number of uses of the function f(x). Classically, in the worst-case scenario f(x) has to be evaluated a total of N-1times, where $N = 2^n$, trying out all the possibilities. After N-1 elements it must be the last element. Grover's quantum algorithm can solve this problem much faster, providing a quadratic speed up. Quadratic here implies that only about $\sqrt{N}$ evaluations would be required, compared to N.
.

A.2 Algorithm

Assume there are $N = 2^n$ eligible items for the search task, and they are indexed by assigning each item an integer between 0 and N-1. Assume that there are M different valid inputs,

which means that there are M inputs for which f (x) = 1. The steps of algorithm are as follows:

1) Begin with an n-qubit register initialized in the state |0>
2) Apply *H* to each qubit of the register to make it into a uniform superposition.
3) Use the register N optimal times to perform the following operations:
    - For the solution items, the phase oracle of applies a conditional phase shift of -1.
    - Apply *H* to each qubit in the register.
    - A conditional phase shift of -1 to every computational basis state except |0>.
    - Apply *H* to each qubit in the register.
4) Measure the register to get the index of an item that has a very high probability of being a solution.
5) Check to see if it's a viable solution. If not, start over.

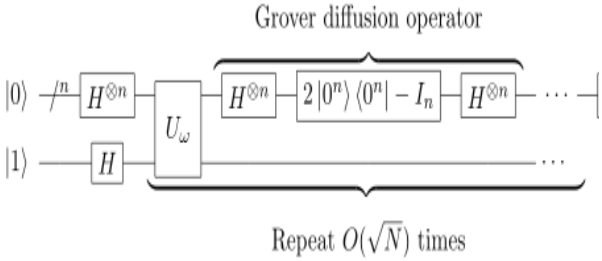


Fig 1: Quantum circuit of Grover's algorithm

A.3 Implementation of Grover's Search Algorithm

We implemented the Grover's search algorithm using qiskit.

PROBLEM:

Find |11> state from all 2 qubit states (|00>, |01>, |10>, |11>).

Creating an oracle: An oracle can be used to check whether a value is target value or not, but it cannot find the target value from a range of values. Since we are finding |11>, we use CZ gate. The sign of |11> will be reversed.

Amplitude amplification: It will increase the probability of target state. 2S><S-I is the reflection operator. The Grover's Diffusion is the reflection operator sandwiched between Hadamard gates. (H 2S><S-I H).

Geometrical Interpretation:

Let |w> denote the winning state and |s> denote super position state. |s'> denote state perpendicular to |w> in a way |w> component removed from |s>. In our implementation

|w> = [0, 0, 0, 1]

|s> = (1/2)*[1, 1, 1, 1]

|s'> = (1/√3)*[1, 1, 1, 0]

<w|s'> = 0, means |w> and |s'> are perpendicular.

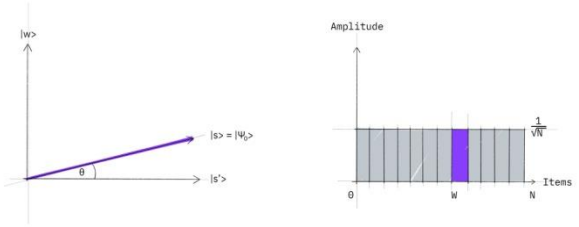


Fig 2: Initial state

The oracle will flip the amplitude of the winning state |w>.

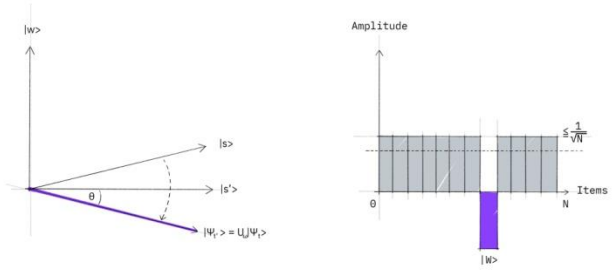


Fig 3: The amplitude in front of the |w⟩ state becomes negative.

After Grover's diffusion, the |s> formed after Oracle treatment is reflected along initial |s>, making it closer towards winning state. In order to find reflection, one way of thinking is adding a negative phase π to all except |11>

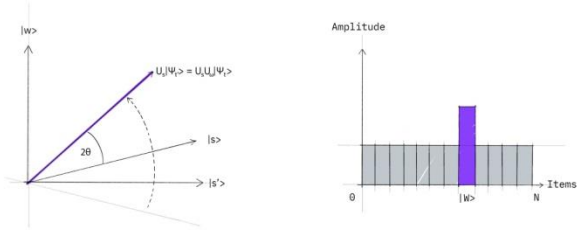


Fig 4: The negative amplitude of |w⟩ is boosted to roughly three times its original value, while it decreases the other amplitudes.

Grover's Iter: Both Oracle and Diffusion together constituent the Grover's iter. After √N iterations, the probability of a winning state (|w>) will be maximized.

```
grover_iter =
QuantumCircuit(2,name="Grover's Iter")
grover_iter.append(oracle,[0,1])
grover_iter.append(diffusion,[0,1])
grover_iter.draw()
```

Since we used a two-qubit system, only one iteration is sufficient.

RESULT OBTAINED:

a) Qasm_simulator

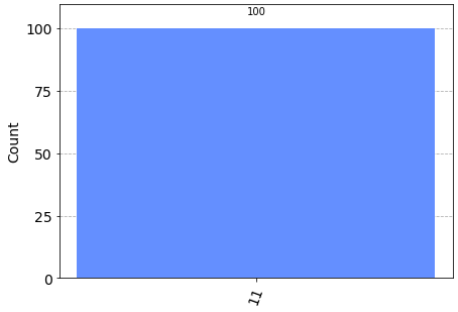


Fig 5: All measurement falls to winning state |11>.

b) Ibm_oslo

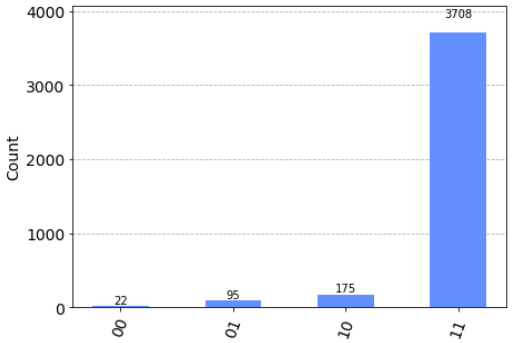


Fig 6: In the majority of the cases the state |11⟩ is measured. The other results are due to errors because of quantum noise.

B. Quantum Partial Search

Quantum partial search algorithm is a variant of Grover's algorithm. The algorithm does not find the exact location of the desired item. It divides the search space into chunks or blocks and returns the address of the block containing the desired item. The Grover's algorithm yields the answer in √ N steps whereas the partial algorithm returns the answer faster by a numerical factor dependent on the number of blocks K.

B.1 Algorithm

Assume that N items are divided into K blocks of b = N/K items each. We do a partial search for the appropriate block. The steps of algorithm are as follows:

1) Π/4 √ N - √ 3b/4 Grover iterations.
2) Π/6 √ b iterations of local searches in each block done in parallel. Note that this drives the amplitude negative in the target block.
3) One global inversion about average annihilates amplitudes of all items in non-target blocks and finds the target block.

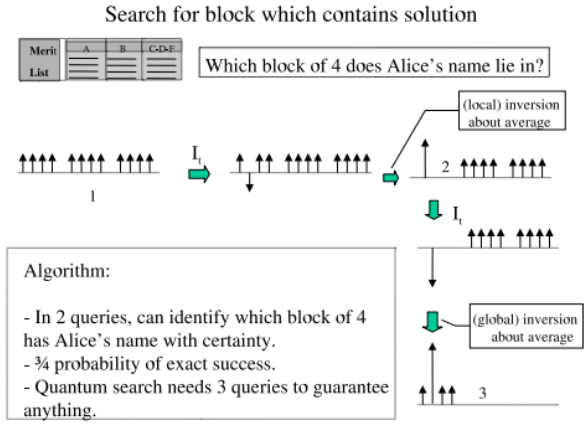


Fig 7: A partial quantum search is able to find partial information about the solution faster than the complete quantum search can.

So the total number of queries (Q) is

$$Q = \pi/4 \sqrt{N} - (\sqrt{3}/4 - \pi/6)\sqrt{b}.$$

The coefficient of √ b is $(\sqrt{3}/4 - \pi/6) \approx 0.34$ and so the improvement over quantum searching is $0.34\sqrt{b}$ iterations.

III. APPLICATIONS OF QUANTUM SEARCH

A. NP Complete Problem

A problem is referred to as NP (nondeterministic polynomial) if its solution can be guessed and verified in polynomial time; nondeterministic means that no specific rule is followed to make the guess. The problem is NP-complete if it is NP and all other NP problems are

polynomial-time reducible to it. Thus, discovering an efficient algorithm for any NP-complete problem implies discovering an efficient algorithm for all such problems, because any problem in this class can be recast into any other member of the class. Classically, the only way to solve an NP-complete problem was to use exhaustive search problems. But quantum search provides a square-root speedup.

B. Quantum Computing

The counting problem is to determine how many items in a set satisfy the given query. Its quantum solution is based on the fact that the iterative evolution in Grover search is periodic with angular frequency $2 \sin^{-1} (\sqrt{M/N})$.

C. Element Distinctness

The element distinctness problem is the problem of determining whether the elements of a list are distinct. We are given f: {1, 2. . . N} → {1, 2. . . N} specified by a black box that, given i, answers the value of f(i). The task is to determine if there are two inputs i, j, i != j for which f(i) = f(j). The solution in a classical computer requires N queries because it uses sorting to check whether there are equal elements. In quantum case, there are two algorithms. The first one uses Grover search in a clever two-level construction and solves the problem O ($N^{3/4}$) queries. The second one uses a technique combining search with quantum walks and solves the problem with O ($N^{2/3}$) queries. This is optimal, because of an Ω ($N^{2/3}$) lower bound.

D. Spatial Search

Spatial search is a search problem in which the items in a database are distributed across distinct physical locations and there is a restriction that one can only move from one location to its neighbors while searching for the target item.

E. Distributed Search

A straightforward distributed implementation of the quantum search algorithm solves the set intersection problem or the appointment problem. When A and B have respective data strings x, y ∈ $\{0, N\}^N$, and they want to find an index i such that xi = yi = 1, only O(√ N log N) qubits of communication is necessary.

F. 3-Satisfiability

The 3- satisfiability problem, also known as the Boolean satisfiability problem, asks what is the fastest algorithm to tell whether a given formula in Boolean algebra (with an unknown number of variables) is satisfiable, that is, whether there is some combination of the (binary) values of the variables that will give 1. Grover's algorithm can solve 3-satisfiability in O (1.41... ^{n} poly(n)) steps.

IV. CONCLUSION

We reviewed some the quantum search algorithms and their applications. Various research papers were analyzed. Grover's search algorithm was thoroughly studied. We successfully implemented the algorithm using Qiskit and obtained results. Research into quantum algorithms is picking up momentum. Researchers are trying to develop new algorithms as well as apply the known algorithms to new problem areas.

V. REFERENCES

[1] Leider, A., Siddiqui, S., Sabol, D.A. and Tappert, C.C., 2019, October. Quantum computer search algorithms: Can we outperform the classical search algorithms?. In Proceedings of the Future Technologies Conference (pp. 447-459). Springer, Cham.

[2] Korepin, V.E. and Grover, L.K., 2006. Simple algorithm for partial quantum search. *Quantum Information Processing*, *5*(1), pp.5-10.

[3] Zhang, K. and Korepin, V., 2018. Quantum partial search for uneven distribution of multiple target items. *Quantum Information Processing*, *17*(6), pp.1-20.

[4] Ambainis, A., 2005. Quantum search algorithms. *arXiv preprint quant-ph/0504012*.

[5] Jozsa, R., 1999. Searching in Grover's algorithm. *arXiv preprint quant-ph/9901021*.

[6] Viamontes, G.F., Markov, I.L. and Hayes, J.P., 2005. Is quantum search practical?. *Computing in science & engineering*, *7*(3), pp.62-70.

[7] Grover, L.K., 1998, February. Quantum search on structured problems. In *NASA International Conference on Quantum Computing and Quantum Communications* (pp. 126-139). Springer, Berlin, Heidelberg.]

[8] Patel, A.D. and Grover, L.K., 2016. Quantum Search.

[9] A. Ambainis. Quantum walk algorithm for element distinctness. quant-ph/03110001.

[10] P. Høyer, J. Neerbek, Y. Shi. Quantum complexities of ordered searching, sorting, and element distinctness. Algorithmica, 34(4): 429-448, 2002