RESEARCHING THE POSSIBILITIES OF CREATING MATHEMATICAL ORACLE FUNCTIONS FOR GROVER'S QUANTUM SEARCH ALGORITHM

Pronin Cesar Borisovich

Ostroukh Andrey Vladimirovich

MOSCOW AUTOMOBILE AND ROAD CONSTRUCTION STATE TECHNICAL UNIVERSITY (MADI)., 64, Leningradsky prospect, Moscow, Russia

Abstract: In this article the key operating principles of Grover's algorithm were researched, and the results were used to make a new oracle function, that illustrates the possibility of using Grover's algorithm for solving more common search problems. The efficiency of this algorithm was also analyzed.

Key words: Grover's algorithm, oracle function, quantum informatics, qubit, superposition, quantum gate.

Basic definitions from a quantum informatics point of view

Qubit (quantum bit) — smallest element used for data storage in a quantum computer, compared to a classical bit a qubit has two simultaneously analyzable states $|0>$ and $|1>$, each of them has a superposition.

Superposition – probability of a certain state in a qubit (or in a quantum register), to remain after passing through a measurement gate [1].

Quantum register – a system that consists of two or more qubits, which are in a state of quantum entanglement, that makes analyzing and editing parameters of all states generated by this system possible. The number of states in which a quantum register can be is 2^n, where "n" is the number of qubits, that are a part of that register.

Researching the key operating principles of Grover's algorithm

Grover's search algorithm (GSA) — a quantum algorithm that can serve as an alternative to classical linear search algorithms. GSA can find solutions to a problem (function) by analyzing all states of a quantum register [2].

The main phase of the algorithm is the oracle function $f(x) = y$, which serves as a search criteria. It gets all of the possible states of the register x on input and inverts the amplitude value of states which can serve as its solutions.

Grover's algorithm can be composed of 3 main steps:

1) Forming uniform superpositions for all possible states of a quantum register, using Hadamart transformation gates.
2) Developing and applying an oracle function that will invert the amplitude of states, that can serve as its solutions.
3) Applying an amplitude amplification function, which will amplify the amplitude and superposition of states that were chosen by the oracle, also the amplitude of those states will be inverted again.

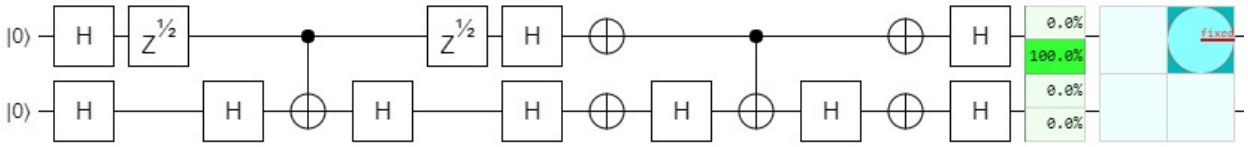
Steps 2-3 are called **Grover iterations** and are repeated $N_G \approx \frac{\pi}{4} * \sqrt{\frac{N}{l}}$ times (rounded down to the nearest whole number), to achieve the highest probability of receiving correct results, where N is the number of all possible states of the system $N = 2^n$, n – number of qubits in the register, l – number of expected solutions [3]. When the number of iterations exceeds N_G, amplitude and superposition values of states chosen by the oracle will start decreasing. In similar circumstances a classic linear search algorithm in worst cases will need N iterations, to find all possible solutions. To calculate the difference in required iterations between Grover's algorithm and classical linear search we can use this formula:

$$N_\Delta = \frac{N}{N_G} = \frac{N}{\frac{\pi}{4} * \sqrt{\frac{N}{l}}} = \frac{4 * \sqrt{N * l}}{\pi}$$

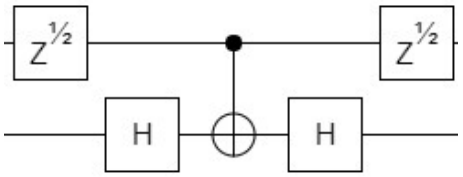
Quantum circuit simulator «Quirk» was used for algorithm implementation and debugging purposes. It offers many useful sensors, that make analyzing

transformations in quantum circuits a lot easier. Qubit numeration from high to low is performed from bottom to top, all qubits have $|0>$ value by default [4].

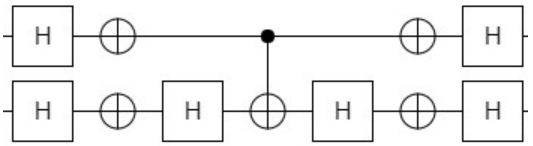
Let's look at IBM's implementation of Grover's algorithm [5], which was re-implemented in Quirk for easier analyzing:



Pic. 1. IBM's implementation of Grover's algorithm



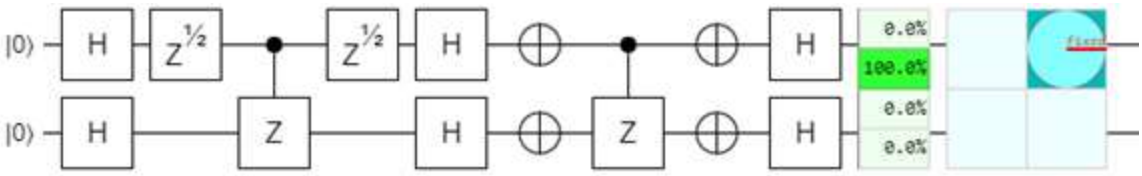
Pic. 2. Oracle of this algorithm



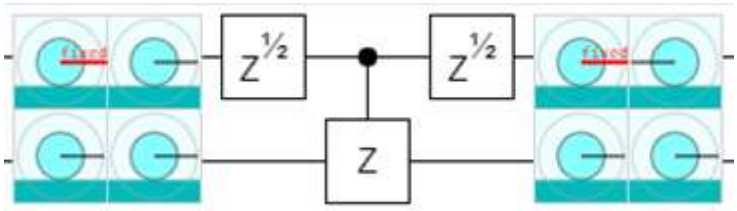
Pic. 3. Amplitude amplification

This circuit uses a 2-qubit register, so the number of required Grover iterations equals: $N_G \approx \frac{\pi}{4} * \sqrt{\frac{2^2}{1}} \approx 1{,}57 \approx 1$

The H-CNOT-H combination, is a more universal implementation of the controlled-Z gate (CZ), which isn't available on some systems, but in Quirk this replacement is possible:



Pic. 4. Circuit after replacing H-CNOT-H with CZ



Pic. 5. Oracle after replacing H-CNOT-H with CZ

It's visible that this oracle inverted the amplitude of state $|01>$

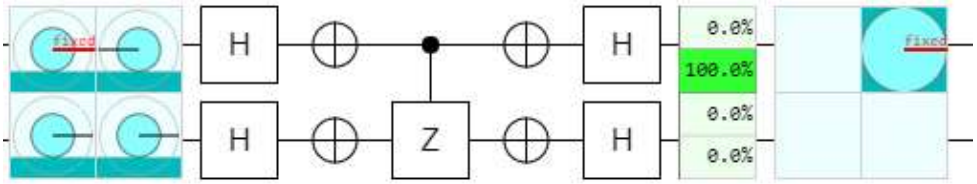
```
Amplitude of |01)
val:+0.50000+0.00000i
mag²:25.0000%, phase:+0.00°
```

Pic. 6. Amplitude of |01> before applying the oracle function

```
Amplitude of |01)
val:-0.50000+0.00000i
mag²:25.0000%, phase:+180.00°
```

Pic. 7. Amplitude of |01> after applying the oracle function

After the amplitude amplification step, the amplitude of $|01>$, becomes higher ang gets inverted again.



Pic. 8. Amplitude amplification function and results

```
Chance of |01) if measured
raw: 100.0000%
log: 0.0 dB
```

Pic. 9. Final superposition of state |01>

```
Amplitude of |01)
val:+1.00000+0.00000i
mag²:100.0000%, phase:+0.00°
```

Pic. 10. Final amplitude of state |01>

Since the state $|01>$ has the highest amplitude and superposition values, compared to other states, it is the solution for this oracle function.

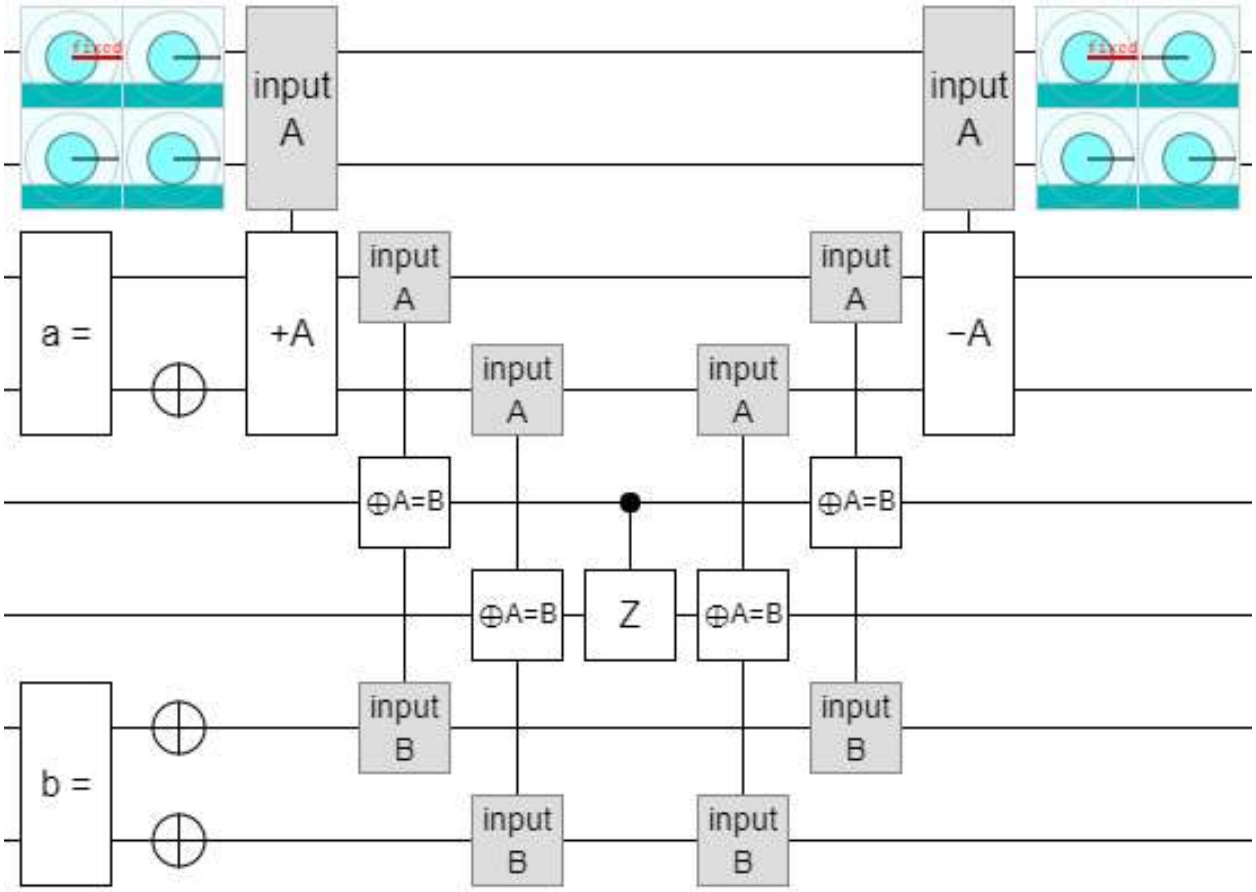
Developing mathematical oracles for Grover's algorithm

To develop a different oracle function, it's important that it will invert the amplitude value of the solution states, without causing decoherence. To avoid decoherence, it is better to use the reversibility property of quantum gates, which are a part of the oracle but aren't related to the amplitude inversion itself, for limiting their effect with the bounds of the oracle.

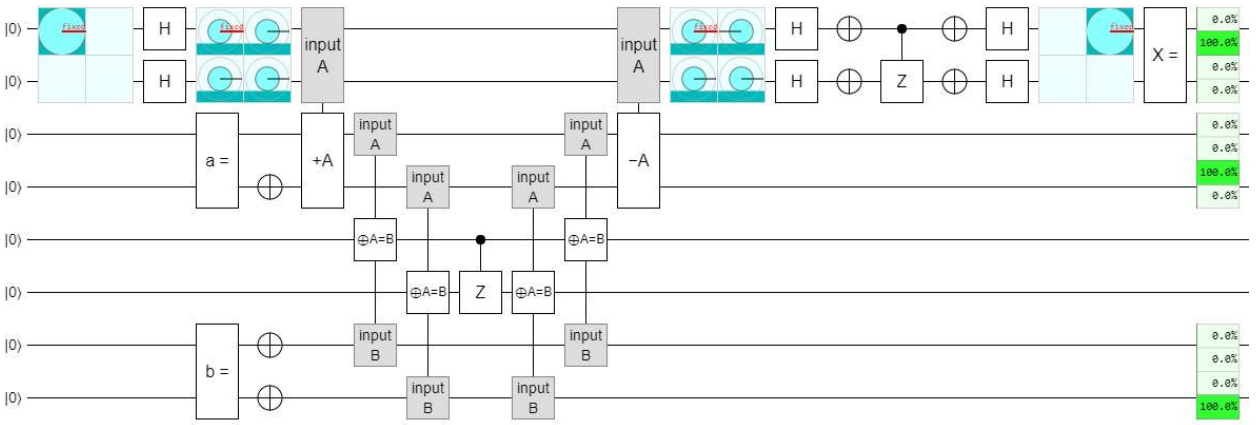
Using the concepts shown above, it's possible to make an algorithm with an oracle function for solving the problem of finding x in equation $x + a = b$, without transforming it. To solve this problem having two bits of data (n = 2), a classical linear search algorithm would require $N_c = 2^n = 2^2$ iterations, while Grover's algorithm would only need 1:

$$N_G \approx \frac{\pi}{4} * \sqrt{\frac{2^2}{1}} \approx 1{,}57 \approx 1$$

The oracle for this problem is made using the arithmetic and comparison operators available in Quirk, for demonstration purposes we assigned values to a = 10 and b = 11. Circuit elements «a =», «b =», «X =» are labels, that are made for clarification and don't have any effect on the circuit.

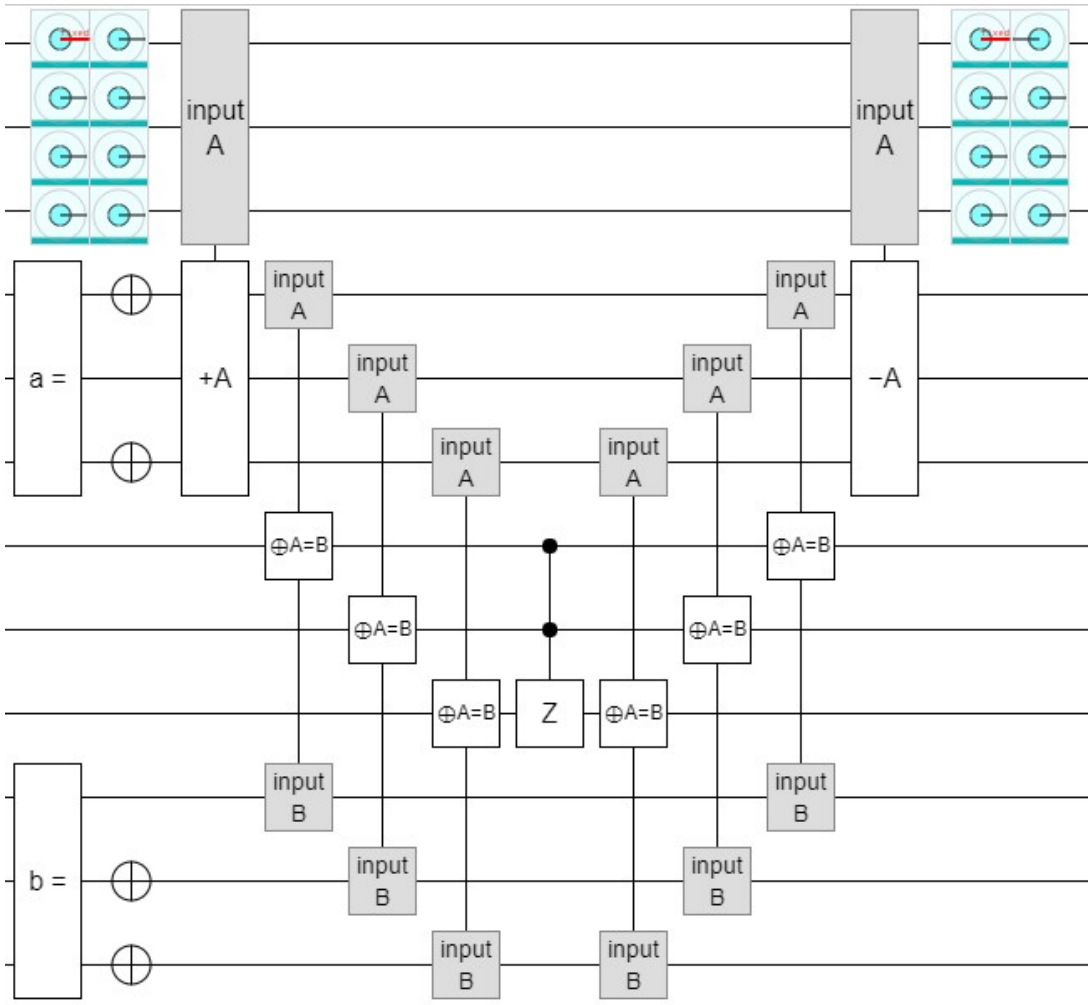


Pic. 11. Example oracle made using 2 qubit registers

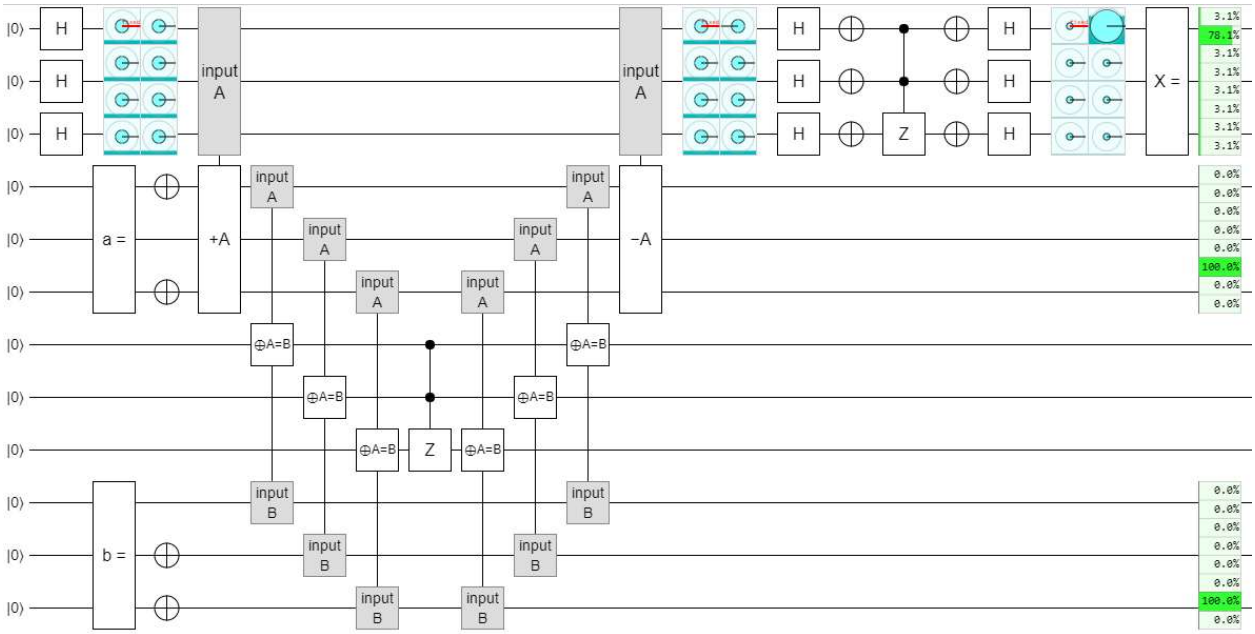


Pic. 12. Algorithm made using 2 qubit registers and it's result X = 01

This solution is scalable, a 3 qubit register version with a = 101 and b = 110 is shown below.



Pic. 13. Example oracle made using 3 qubit registers



Pic. 14. Algorithm made using 3 qubit registers and it's result X = 001

Conclusion

In this article the key operating principles of Grover's algorithm were researched, and the results were used to make a new oracle function, that illustrates the possibility of using Grover's algorithm for solving more common search problems. The efficiency of this algorithm was also analyzed, and a formula that calculates the ratio between required iterations of linear search and Grover's algorithm was proposed:

$$N_{\Delta} = \frac{N}{N_G} = \frac{N}{\frac{\pi}{4} * \sqrt{\frac{N}{l}}} = \frac{4 * \sqrt{N * l}}{\pi}$$

Grover's algorithm seems to be most efficient in problems that can't be effectively solved by common search algorithms due to there being too many possible states of a register, in the future it could even be applied to solve mathematical problems that may be harder to solve othervise.

List of used sources

1. Pronin C.B., Ostroukh A.V., Quantum logical elements, results and analysis of their effect on quantum circuits // Best Student's Article of 2017: Articles of the XI International Scientific and Practical competition. Volume 1. – Penza: ICSC «Science and Education», pages 73 -78, 2017.

2. Grover's algorithm [Web resource] // Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Grover%27s_algorithm (access date: 21.04.2018)

3. Grover L.K.: A fast quantum mechanical algorithm for database search [Web resource] // Cornell University Library. URL: https://arxiv.org/abs/quant-ph/9605043 (access date: 21.04.2018)

4. Quirk [Web resource] // Quirk – online quantum computer simulator. URL: http://algassert.com/quirk (access date: 21.04.2018)

5. IBM Quantum Experience [Web resource] // IBM Composer documentation. URL: https://quantumexperience.ng.bluemix.net/proxy/tutorial/full-user-guide (access date: 21.04.2018)