Санкт-Петербургский
политехнический университет
Петра Великого

Институт
электроники
и телекоммуникаций

Grover’s algorithm (A quantum search algorithm)

Предмет:
Оптоинформатика и
квантовая криптография

Учитель:
Ушаков Николай
Александрович

Студент:
Парра Орельяна
Фредди Андрес

Дата:
17 апреля 2023 г.

Content

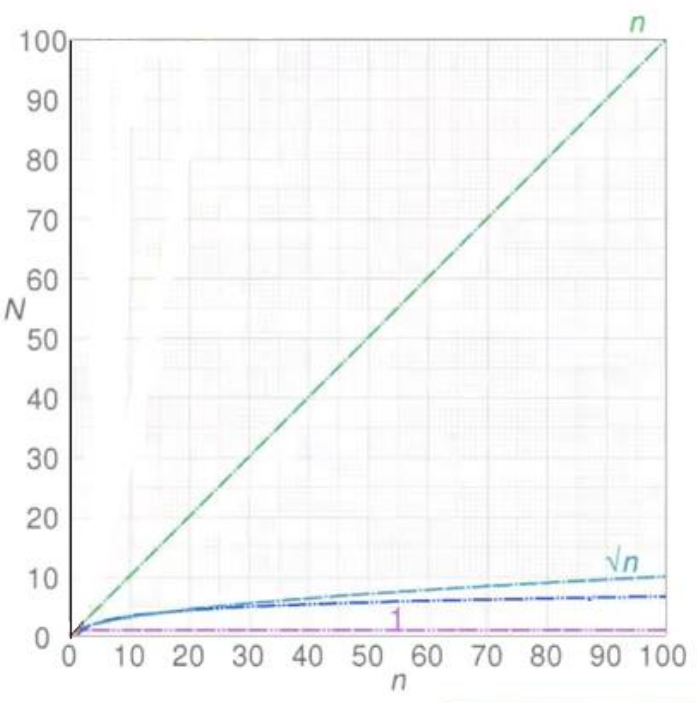
1. Precedent

Some important concepts: *Optimization, Identification and One-Way Functions.*

Grover's algorithm is most effective on problems with limited structure in potential solution space.

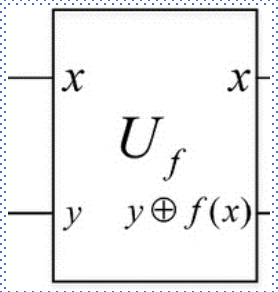
SUDOKU

Grover's algorithm takes advantage of qubit superposition and phase interference to improve unstructured database of N elements from $O(N)$ to $O(\sqrt{N})$.



2. Analysis of the quantum circuit for Grover's algorithm

Grover Oracle



$$(-1)^{f_w(x)}|x\rangle \otimes \frac{|x\rangle - |1\rangle}{\sqrt{2}}$$ If $f_w(x) = 1$ the sign of register flipped.

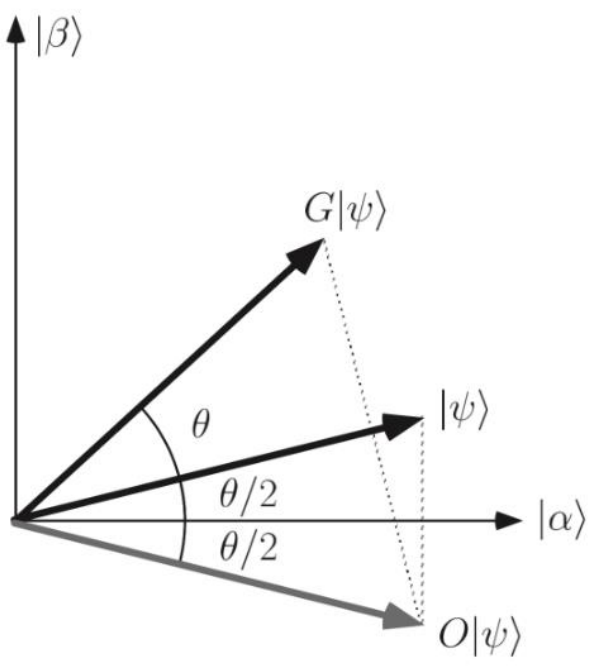
Unitary operator $U_w = \mathrm{I} - 2|w\rangle\langle w|$

Reflection operator $U_s = 2|s\rangle\langle s| - \mathrm{I}$

Grover operator $R_G = U_s U_w$

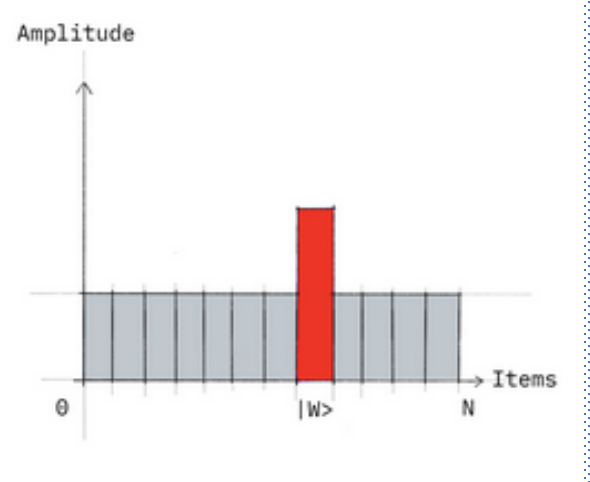
Grover rotation would make the standard state come closer and closer to the marked state.

Geometrical Interpretation



2. Analysis of the quantum circuit for Grover's algorithm

How the amplitude changes? $U_s|\psi\rangle = \sum_x (2\overline{a} - a_x)|x\rangle$



Selective Amplification of Amplitude [1]

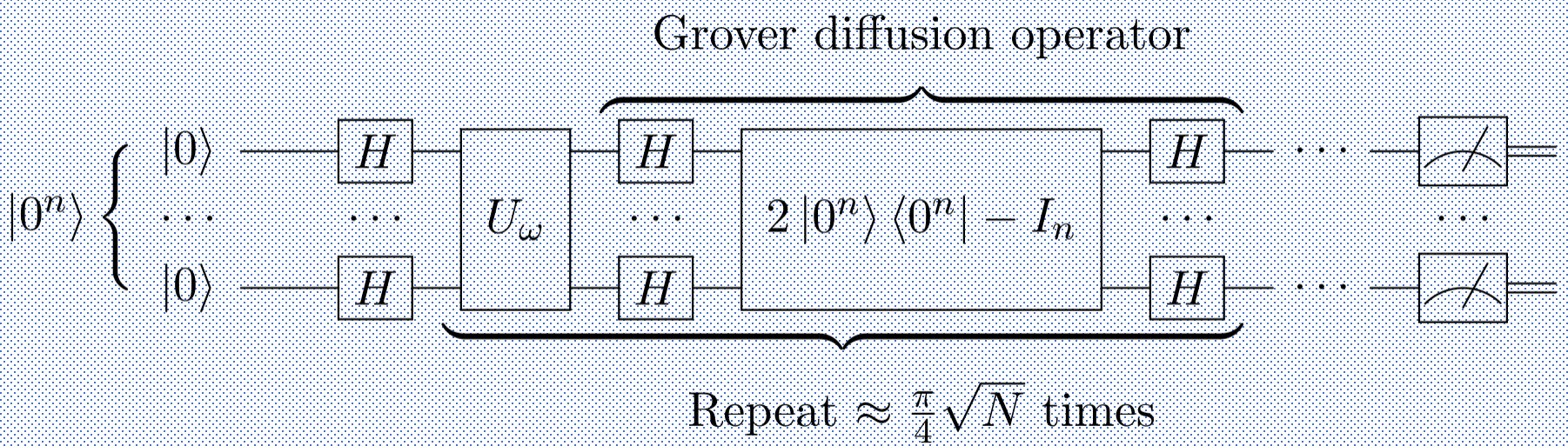
Its time to resolve an exercise.

What is the maximum number of iterations? $m \approx \frac{\pi\sqrt{N}}{4}$

What is the amplitude of $|w\rangle$ in $|s\rangle$ after m iterations? $\sin(2m+1)\theta = 1 - \frac{1}{2N}$

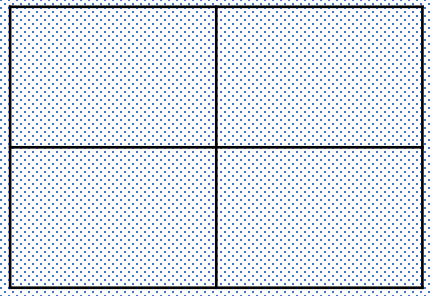
Diffusion operator $D|\psi\rangle = \sum_x (2\overline{a} - a_x)|x\rangle$

3. Quantum circuit for Grover's algorithm



4. Example

Solve the following 2x2 binary sudoku using Grover's algorithm.



4.1. Solution

The general rules for solving a binary sudoku are:

1. Each cell will either be black (0) or white (1).
2. Each column/ow must have an equal number of black and white cells.
3. No more than two cells of the same color may be orthogonally adjacent to one another.
4. Each row and columns must be unique.

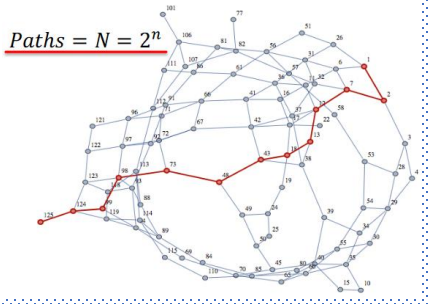
Answers (Sudoku binary 2x2): {1, 0, 0, 1}, {0, 1, 1, 0}

5. Conclusion

When performing the analysis of the quantum circuit of Grover's algorithm it was shown that this required $O(\sqrt{N})$ operations to find an element on an unstructured database.

A challenge would be to solve:

- Find shortest path between two cities.



- Find an element on an Ozon database.

$Entries = N = 2^n$

Person	Height	Age	Weight	IQ
John	173	25	200	95
Peter	175	26	185	75
Greg	195	32	191	65
James	165	28	160	150
Matthew	152	15	140	135
Peter	145	12	130	100

6. Bibliography

[1] Quantum Computing IBM (2023). Grover's algorithm. (Date of consultation: 18.04.2023). Link: https://quantum-computing.ibm.com/lab/docs/iqx/guide/grovers-algorithm.

[2] Zapata, C. & Yang, X. (2016). The Grover's Algorithm. ETH Zürich.