Grover's algorithm with probabilistic solutions

EUROPEAN UNION

Nikolajs Nahimovs
nikolajs.nahimovs@lais.lv
University of Latvia

Alexander Rivosh
aleksandrs.rivoss@lais.lv
Faculty of Computing

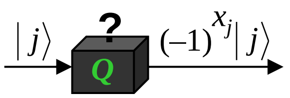
Supported by European Social Fund Project 2009/0216/1DP/1.1.1.2.0/09/APIA/VIAA/044

Supported by ESF EUROPEAN SOCIAL FUND

Original Grover's algorithm

Grover's algorithm is a quantum algorithm for exhaustive search in unsorted solution space with n entries in $O(n^{1/2})$ time. At each step two unitary transformations are applied: $\boldsymbol{Q}$ and $\boldsymbol{D}$.

Query transformation (**Q**)



Performing conditional phase flip.

Diffusion transformation (**D**)

$$D = \begin{pmatrix} -1+\frac{2}{n} & \cdots & \frac{2}{n} \\ & \ddots & \\ \frac{2}{n} & \cdots & -1+\frac{2}{n} \end{pmatrix}$$

These transformation must be applied repeatedly $O(n^{1/2})$ times in order to find the solution.

$$\underbrace{QD\ QD\ \ldots\ QD\ QD}_{}$$

repeat $N = O(\sqrt{n})$ times

Our model

Omitting $\boldsymbol{Q}$ with probability p:

$$|j\rangle \rightarrow \begin{cases} |j\rangle, & \text{if } x_j=0 \\ -|j\rangle, & \text{if } x_j=1 \text{ with probability } 1-p \\ |j\rangle, & \text{if } x_j=1 \text{ with probability } p \end{cases}$$

Motivation

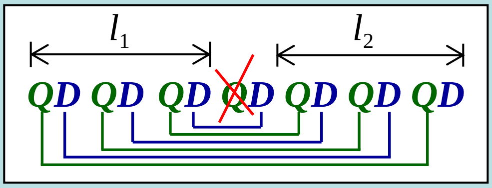
- Model a "software" error
- Mathematically equivalent to another more realistic model:

$$|j\rangle \rightarrow \begin{cases} |j\rangle, & \text{if } x_j=0 \\ (-1)^{(\pi\pm\varepsilon)i}|j\rangle, & \text{if } x_j=1 \end{cases}$$

Analysis

Let $K = \lfloor (1-p)\cdot N \rfloor$ be number of omitted queries

$K = 1$



$\boldsymbol{Q}\cdot\boldsymbol{Q} = \boldsymbol{I}$

$\boldsymbol{D}\cdot\boldsymbol{D} = \boldsymbol{I}$

The illustration shows the worst case, when omitted query is in the middle of sequence of transformations. Thus, number of successful queries is 0:

For arbitrary location of omitted query:

$$(QD)^{l_1} D\ (QD)^{l_2} \Rightarrow (QD)^{l_1} (DQ)^{l_2} D$$

$$\begin{cases} l_1 \geq l_2: & (QD)^{l_1-l_2} D \\ l_1 < l_2: & (DQ)^{l_2-l_1} D \end{cases} \Rightarrow O(|l_1 - l_2|)$$

$K > 1$ Omitting multiple queries

$$(QD)^{l_1} D\ (QD)^{l_2} D \ldots (QD)^{l_{K+1}}$$

The following commutativity property $(QD)^i (DQ)^j = (DQ)^j (QD)^i$ lead us to:

$$\begin{cases} l_1 + l_3 + \ldots \geq l_2 + l_4 + \ldots: & (QD)^{l_1 - l_2 + l_3 - \ldots} \\ l_1 + l_3 + \ldots < l_2 + l_4 + \ldots: & (DQ)^{-l_1 + l_2 - l_3 + \ldots} \end{cases} \Rightarrow$$

$$\Rightarrow O(|l_1 - l_2 + l_3 - \ldots|)$$

Results

$L = l_1 + l_2 - l_3 + \ldots$ Is a random variable

K is odd	K is even
• $E[L] = 0$	• $E[L] = \frac{L}{K}$
• $D[L] = O\left(\frac{L^2}{K}\right)$	• $D[L] = O\left(\frac{L^2}{K}\right)$

Therefore with a very high probability the length of the resulting transformation sequence $O\left(\frac{L}{\sqrt{K}}\right)$ times.

In other words $\boldsymbol{K}$ failed query transformations decrease the length of the resulting transformation sequence $O(\sqrt{K})$ times.

Open problems

What happens if $\boldsymbol{Q}$ has a small error even for $x_j = 0$?

$$|j\rangle \xrightarrow{Q} (-1)^{(\pi\cdot x_j \pm\varepsilon)i}|j\rangle$$