Grover's algorithm with mistakes

Artūrs Bačkurs

Main quantum algorithm classes:

- Based upon Shor's quantum Fourier transform
- Based upon Grover's algorithm

Grover's algorithm (Lov Grover, 1996)

Input:

- An unsorted database with n entries;
- A unique element in the database that satisfies a certain property.

Output:

The index of this element.

Input:

A function $f : \{0, 1, ..., n-1\} \mapsto \{0, 1\}$ satisfying:

- $f(i) = 1$
- $f(j) = 0$ where $j \neq i$.

i corresponds to an element from the database that is a solution to our search problem.

Output:

i

Grover's algorithm

Oracle transformation:

$O : |i\rangle \mapsto -|i\rangle$
$O : |j\rangle \mapsto |j\rangle$ if $j \neq i$

Grover's algorithm

$$D = \begin{bmatrix} \frac{2-n}{n} & \frac{2}{n} & \frac{2}{n} & \cdots \\ \frac{2}{n} & \frac{2-n}{n} & \frac{2}{n} & \cdots \\ \frac{2}{n} & \frac{2}{n} & \frac{2-n}{n} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

Grover's algorithm

Procedure:

- Prepare the initial state - a uniform superposition of all basis states,
  $|\psi\rangle = \frac{1}{\sqrt{n}}|0\rangle + \frac{1}{\sqrt{n}}|1\rangle + ... + \frac{1}{\sqrt{n}}|n-1\rangle$,
- Apply the DO transformation $O(\sqrt{n})$ times,
- Measure the final state in the computational basis.

Grover's algorithm

Input:

A function $f : \{0, 1, ..., n-1\} \mapsto \{0, 1\}$ satisfying:

- $f(i) = 1$ for k elements
- $f(j) = 0$ for $n - k$ elements

Output:

i, such that $f(i) = 1$.

Procedure:

- Prepare the initial state - a uniform superposition of all basis states,
- Apply the *DO* transformation $O(\sqrt{\frac{n}{k}})$ times,
- Measure the final state in the computational basis.

Note: In the classical case the time complexity for a search algorithm - $O(\frac{n}{k})$

Grover's algorithm with mistakes

Oracle transformation:

$O' : |i\rangle \mapsto |i\rangle$ if $f(i) = 0$

$O' : |i\rangle \mapsto |i\rangle$ with probability p if $f(i) = 1$

$O' : |i\rangle \mapsto -|i\rangle$ with probability $1 - p$ if $f(i) = 1$

Grover's algorithm with mistakes

Procedure:

- Prepare the initial state - a uniform superposition of all basis states,
- Apply the DO' transformation $O(\frac{n}{\epsilon^2})$ times,
- Measure the final state in the computational basis.

Probability of success: t, such that $\left|\frac{k}{k+1} - t\right| < \epsilon$.

Modified Grover's algorithm with mistakes

Oracle transformation:

$O' : |i\rangle \mapsto |i\rangle$ if $f(i) = 0$

$O' : |i\rangle \mapsto |i\rangle$ with probability p if $f(i) = 1$

$O' : |i\rangle \mapsto -|i\rangle$ with probability $1 - p$ if $f(i) = 1$

$O'_{2r} = O'_{2r+1}$

Modified Grover's algorithm with mistakes

Procedure:

- Prepare the initial state - a uniform superposition of all basis states,
- Apply the DO' transformation $O(\sqrt{\frac{n}{k}})$ times,
- Measure the final state in the computational basis.

Probability of success: $1 - o(1)$.

Density matrix of a pure state $|\psi\rangle$

$$\rho = |\psi\rangle\langle\psi|$$

$$|\psi\rangle = \frac{1}{\sqrt{3}}|0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{3}} \\ \frac{\sqrt{2}}{\sqrt{3}} \end{pmatrix}$$

$$\langle\psi| = (|\psi\rangle)^\dagger = \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{\sqrt{2}}{\sqrt{3}} \end{pmatrix}$$

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \frac{1}{\sqrt{3}} \\ \frac{\sqrt{2}}{\sqrt{3}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{3}} & \frac{\sqrt{2}}{\sqrt{3}} \end{pmatrix} = \begin{pmatrix} \frac{1}{3} & \frac{\sqrt{2}}{3} \\ \frac{\sqrt{2}}{3} & \frac{2}{3} \end{pmatrix}$$

Density matrix of an ensemble of pure states

$\rho = \sum_{i=1}^{n} p_i \left|\psi_i\right\rangle \left\langle\psi_i\right|,$

where $\sum_{i=1}^{n} p_i = 1$

Methods (Density matrix)

$$p_1 = \frac{1}{4}$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

$$p_2 = \frac{3}{4}$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$$

$$\rho = p_1 |\psi_1\rangle \langle\psi_1| + p_2 |\psi_2\rangle \langle\psi_2| =$$

$$= \frac{1}{4}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} + \frac{3}{4}\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & -\frac{1}{4} \\ -\frac{1}{4} & \frac{1}{2} \end{pmatrix}$$

Methods (Density matrix)

Application of a unitary matrix

$\rho \mapsto U\rho U^{\dagger}$

A_r **transformation**:
$A_r |r\rangle = -|r\rangle$
$A_r |j\rangle = |j\rangle$ if $j \neq r$

Sign shifts for states $|r_1\rangle, |r_2\rangle, ..., |r_j\rangle$:
$\rho \mapsto A_{r_1} ... A_{r_j} \rho A_{r_j} ... A_{r_1}$

Methods (Frobenius norm)

$$||M||_F = \sqrt{\sum_{i,j} |m_{ij}|^2}$$

$||MU||_F = ||UM||_F = ||M||_F$ if U is a unitary matrix.

Methods (Proof of convergence)

$$|\psi\rangle = \frac{1}{\sqrt{n}}|0\rangle + \frac{1}{\sqrt{n}}|1\rangle + \ldots + \frac{1}{\sqrt{n}}|n-1\rangle$$

$$\rho = |\psi\rangle\langle\psi| = \begin{pmatrix} \frac{1}{n} & \cdots & \frac{1}{n} \\ \vdots & \ddots & \vdots \\ \frac{1}{n} & \cdots & \frac{1}{n} \end{pmatrix}$$

Methods (Proof of convergence)

Application of the O' transformation:

$$O' : \rho \mapsto p^k \rho + \sum_r p^{k-1}(1-p)A_r \rho A_r +$$

$$+ \sum_{1 \le r < t \le k} p^{k-2}(1-p)^2 A_r A_t \rho A_t A_r + \ldots$$

Application of the DO' transformation:

$$DO' : \rho \mapsto D[p^k \rho + \sum_r p^{k-1}(1-p)A_r \rho A_r +$$

$$+ \sum_{1 \le r < t \le k} p^{k-2}(1-p)^2 A_r A_t \rho A_t A_r + \ldots]D$$

Methods (Proof of convergence)

Solution states - the first k basis states.

$$\rho = \begin{bmatrix} a & b & b & c & \dots & c \\ b & a & b & \vdots & \ddots & \vdots \\ b & b & a & c & \dots & c \\ c & \dots & c & d & \dots & d \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ c & \dots & c & d & \dots & d \end{bmatrix} \mapsto$$

$$\begin{bmatrix} \frac{1}{k+1} & 0 & 0 & 0 & \dots & 0 \\ 0 & \frac{1}{k+1} & 0 & \vdots & \ddots & \vdots \\ 0 & 0 & \frac{1}{k+1} & 0 & \dots & 0 \\ 0 & \dots & 0 & \frac{1}{(n-k)(k+1)} & \dots & \frac{1}{(n-k)(k+1)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \frac{1}{(n-k)(k+1)} & \dots & \frac{1}{(n-k)(k+1)} \end{bmatrix}$$

Methods (Proof of convergence)

Application of the O' transformation:

$$\rho \mapsto p^k \rho + \sum_r p^{k-1}(1-p) A_r \rho A_r +$$

$$+ \sum_{1 \le r < t \le k} p^{k-2}(1-p)^2 A_r A_t \rho A_t A_r + ..$$

$a \mapsto a$ (Transformation A_t does not change diagonal entries.)
$b \mapsto b(2p-1)^2$
$c \mapsto c(2p-1)$
$d \mapsto d$ (A_t acts only on the first k basis states.)

Methods (Proof of convergence)

$$b \mapsto b \sum_{s=0}^{k} \left[p^{k-s}(1-p)^s \left(\binom{k-2}{s} + \binom{k-2}{s-2} - 2\binom{k-2}{s-1} \right) \right]$$

$$\sum_{s=0}^{k} \left[p^{k-s}(1-p)^s \left(\binom{k-2}{s} + \binom{k-2}{s-2} - 2\binom{k-2}{s-1} \right) \right] = (2p-1)^2$$

Methods (Proof of convergence)

$$c \mapsto c \sum_{s=0}^{k} \left[p^{k-s}(1-p)^s \left(\binom{k-1}{s} - \binom{k-1}{s-1} \right) \right]$$

$$\sum_{s=0}^{k} \left[p^{k-s}(1-p)^s \left(\binom{k-1}{s} - \binom{k-1}{s-1} \right) \right] = 2p - 1$$

Methods (Proof of convergence)

The Frobenius norm before an application of the oracle transformation:
$||\rho||^2 = ka^2 + (n-k)^2 d^2 + 2k(n-k)c^2 + k(k-1)b^2$

The Frobenius norm after an application of the oracle transformation:
$||\rho||^2 = ka^2 + (n-k)^2 d^2 + 2k(n-k)c^2(2p-1)^2 + k(k-1)b^2(2p-1)^4$

Because $\lim ||\rho||$ exists, it follows that $b \to 0$, $c \to 0$.

Methods (Proof of convergence)

Because b and c converges to 0, ρ converges to

$$\begin{bmatrix} a & 0 & 0 & 0 & \dots & 0 \\ 0 & a & 0 & \vdots & \ddots & \vdots \\ 0 & 0 & a & 0 & \dots & 0 \\ 0 & \dots & 0 & d & \dots & d \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & d & \dots & d \end{bmatrix}$$

$a = ?$

$$ka + (n-k)d = 1$$
$$a = \frac{1-(n-k)d}{k}$$

$\rho \mapsto D\rho D$

The upper right value of $D\rho D$:

$\frac{2(n-2k)(d(k+1)(n-k)-1)}{kn^2}$

Because $\lim \rho = \lim D\rho D$, it follows that

$\frac{2(n-2k)(d(k+1)(n-k)-1)}{kn^2} = 0$

$d = \frac{1}{(k+1)(n-k)}$
$a = \frac{1}{k+1}$

Questions

Questions?