Quantum Information and Quantum Computing, Solutions 8

Assistants : sara.alvesdossantos@epfl.ch, clemens.giuliani@epfl.ch

Problem 1 : The quantum counting algorithm

In this problem we want to estimate the number M of solutions of a search problem in a database of size $N = 2^n$. We assume to have a circuit to perform the $\hat{G}$ operator and the controlled-$\hat{G}$.

1. The subspace spanned by $|\alpha\rangle = (N-M)^{-1/2} \sum_x'' |x\rangle$ and $|\beta\rangle = M^{-1/2} \sum_x' |x\rangle$ has dimension 2, hence the operator $\hat{G}$ is represented by a $2x2$ matrix. To find the elements of this matrix, we apply the operator on $|\alpha\rangle$ and $|\beta\rangle$. Recall that the input state $|\psi\rangle$ of the algorithm is written as a superposition of $|\alpha\rangle$ and $|\beta\rangle$, which represent the projections of $|\psi\rangle$ parallel and orthogonal to the solution respectively. More precisely

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle \tag{1}$$

which can be expressed in terms of an angle θ as

$$|\psi\rangle = \cos\frac{\theta}{2}|\alpha\rangle + \sin\frac{\theta}{2}|\beta\rangle \tag{2}$$

with

$$\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}} \quad , \quad \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}} \quad . \tag{3}$$

Now we transform the vector $|\psi\rangle$ twice: first, we apply a reflection with respect to its $|\beta\rangle$ component. This is accomplished by the oracle operator. Then we we apply a second reflection with respect to the initial vector $|\psi\rangle$.

As can be seen in Figure 1, the net result of these transformations is a rotation that takes the initial state to

$$|\psi\rangle = \cos\frac{3\theta}{2}|\alpha\rangle + \sin\frac{3\theta}{2}|\beta\rangle\,. \tag{4}$$

We conclude that the overall effect of $\hat{G}$ is a counter-clockwise rotation by an angle θ! Its expression in matrix form is

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \tag{5}$$

We know from elementary algebra that this matrix does not have real eigenvalues; in fact its two eigenvalues are $e^{i\theta}$ and $e^{i(2\pi-\theta)}$. From (3) we know that

$$\theta = 2\arcsin\sqrt{\frac{M}{N}}\,. \tag{6}$$

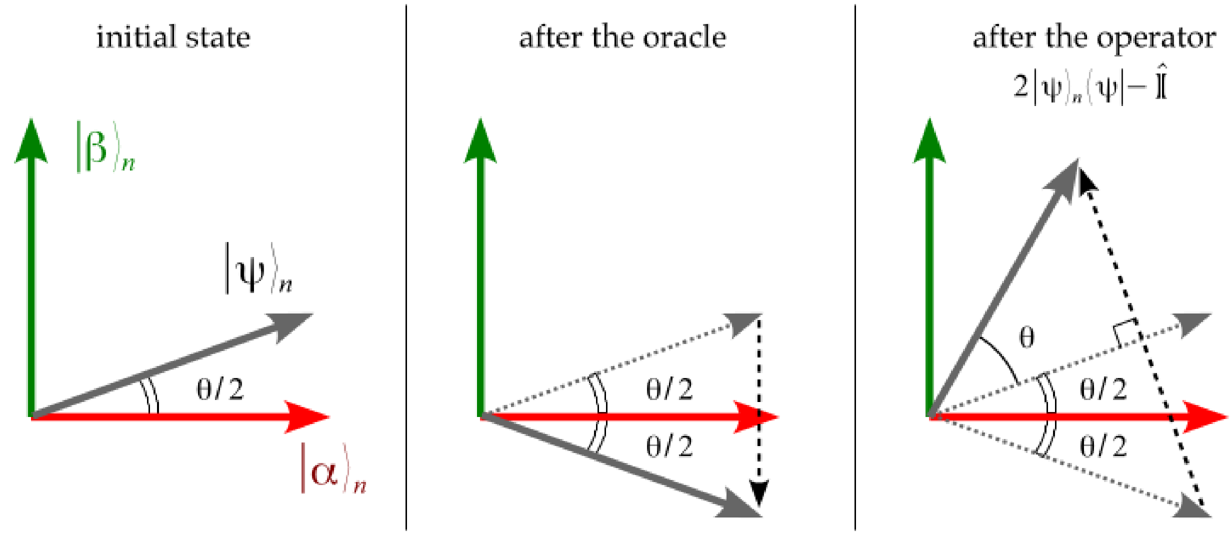

Figure 1: Graphic representation of Grover transformations

Therefore, if we can measure θ using a phase estimation algorithm, then by knowing the size of the database we can retrieve the number M of solutions. This is the principle underlying the quantum counting algorithm.

2. To compute M, we apply the quantum phase estimation (QPE) algorithm to obtain an estimate of the Grover operator, relying on the assumption that we know how to perform the controlled-$\hat{G}$. To set up the algorithm, we need two registers: a first register to perform the $QFT^\dagger$ and a second register for the $\hat{G}$ operator. Clearly, the second register will have n qubits, where $N = 2^n$ is the dimension of the search space, while the number of qubits in the first register is set by the required accuracy in the phase estimation. In particular, we set

$$t = m + \lceil \log \left(2 + \frac{1}{2\epsilon} \right) \rceil \tag{7}$$

to estimate the phase to m bits accuracy with a probability of success of $1-\epsilon$. As required by the algorithm, the first register has to be prepared in a superposition of all the possible states by applying Hadamard gates to all the qubits. The second register should be prepared in a state which has a large overlap with the eigenstates of $\hat{G}$ which we are targeting. However, estimating $e^{i\theta}$ is the same as estimating $e^{i(2\pi-\theta)}$. Hence, the choice of the initial state for this register is irrelevant.

3. Let us compute the accuracy ΔM of the estimate of M. Again, from (3) we know that

$$\frac{M}{N} = \sin^2 \left(\frac{\theta}{2} \right) \tag{8}$$

and ΔM is the difference between the actual value of M and the value measured with an error $\Delta\theta$ on the angle

$$
\begin{aligned}
\frac{|\Delta M|}{N} &= \left| \sin^2\left(\frac{\theta+\Delta\theta}{2}\right) - \sin^2\left(\frac{\theta}{2}\right) \right| \\
&= \left[\sin\left(\frac{\theta+\Delta\theta}{2}\right) + \sin\left(\frac{\theta}{2}\right)\right] \left| \sin\left(\frac{\theta+\Delta\theta}{2}\right) - \sin\left(\frac{\theta}{2}\right) \right| \qquad (9)
\end{aligned}
$$

since $|\Delta\theta| < 2^{-m}$, we can expand the term in modulus and obtain

$$
\left| \sin\left(\frac{\theta+\Delta\theta}{2}\right) - \sin\left(\frac{\theta}{2}\right) \right| \leq \frac{|\Delta\theta|}{2} \tag{10}
$$

while for the first term we have

$$
\begin{aligned}
\left| \sin\left(\frac{\theta+\Delta\theta}{2}\right) \right| &= \left| \sin\left(\frac{\theta}{2}\right)\cos\left(\frac{\Delta\theta}{2}\right) + \sin\left(\frac{\Delta\theta}{2}\right)\cos\left(\frac{\theta}{2}\right) \right| && (11)\\
&\sim \left| \sin\left(\frac{\theta}{2}\right) + \frac{\Delta\theta}{2}\cos\left(\frac{\theta}{2}\right) \right| && (12)\\
&< \sin\left(\frac{\theta}{2}\right) + \frac{|\Delta\theta|}{2} && (13)
\end{aligned}
$$

and we obtain

$$
\begin{aligned}
|\Delta M| &< N\left[2\sin\left(\frac{\theta}{2}\right) + \frac{|\Delta\theta|}{2}\right]\frac{|\Delta\theta|}{2} && (14)\\
&< N\left[2\sqrt{\frac{M}{N}} + \frac{2^{-m}}{2}\right]\frac{2^{-m}}{2}\,. && (15)
\end{aligned}
$$

Assuming $m \sim n$ (for simplicity $m = \frac{n}{2}$) and knowing that $N = 2^n$ we obtain

$$
|\Delta M| < \left[\sqrt{MN} + \frac{N}{2^{m+2}}\right]2^{-m} = \sqrt{M} + \frac{1}{4} \tag{16}
$$

so the error is of $O(\sqrt{M})$.

Problem 2 : Code Grover's search algorithm

This is a coding hands-on exercise that requires Python and the Qiskit library.
For the solution, see the related notebook.