Quantum Computing CO484

Tutorial*

Sheet 4 – Solutions

Exercise 1 *Consider Grover's algorithm (as in the lecture notes).*

(i) Show that

$$(2\left|\psi\right\rangle\left\langle\psi\right| - \mathbf{I})(\sum_x \alpha_x \left|x\right\rangle) = \sum_x (-\alpha_x + 2\left\langle\alpha\right\rangle)\left|x\right\rangle$$

where $\left\langle\alpha\right\rangle = \frac{1}{N}\sum_x \alpha_x$.

(ii) Explain why the operation $2\left|\psi\right\rangle\left\langle\psi\right| - \mathbf{I}$ *in Grover's algorithm is called* inversion about mean.

Solution

(i) We have: $\left|\psi\right\rangle = \frac{1}{\sqrt{N}}\sum_y \left|y\right\rangle$ and hence $\left\langle\psi\right| = \frac{1}{\sqrt{N}}\sum_y \left\langle y\right|$.

Therefore:

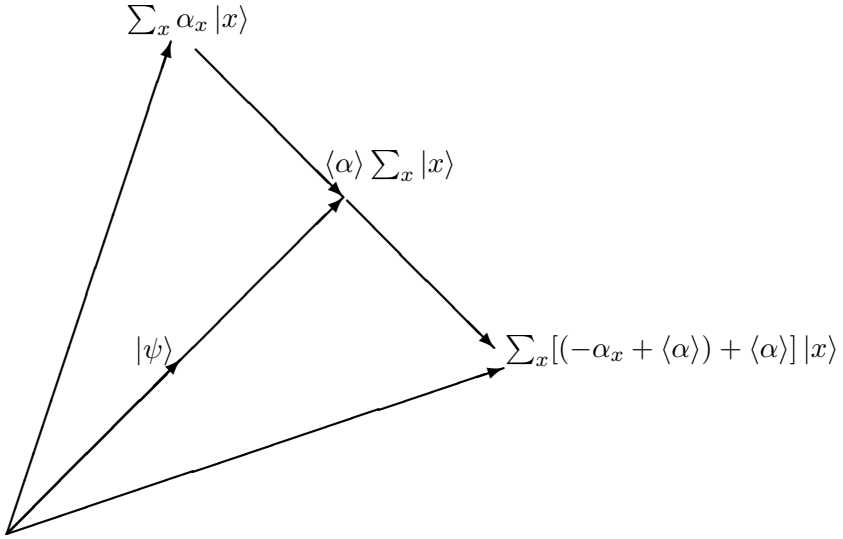
$$\begin{aligned}(2\left|\psi\right\rangle\left\langle\psi\right| - \mathbf{I})(\sum_x \alpha_x|x\rangle) &= (\frac{2}{N}(\sum_y \left|y\right\rangle \sum_y \left\langle y\right|) - \mathbf{I})(\sum_x \alpha_x \left|x\right\rangle) = \\ &= \frac{2}{N}(\sum_y \left|y\right\rangle)\sum_x \alpha_x - \sum_x \alpha_x \left|x\right\rangle = \\ &= \sum_x (-\alpha_x + 2\left\langle\alpha\right\rangle)\left|x\right\rangle\end{aligned}$$

(ii) From part (i), we have:

$$\begin{aligned}(2\left|\psi\right\rangle\left\langle\psi\right| - \mathbf{I})(\sum_x \alpha_x \left|x\right\rangle) &= \sum_x (-\alpha_x + 2\left\langle\alpha\right\rangle)\left|x\right\rangle = \\ &= \sum_x [(-\alpha_x + \left\langle\alpha\right\rangle + \left\langle\alpha\right\rangle]\left|x\right\rangle\end{aligned}$$

*Partly based on the tutorials by Abbas Edalat and Herbert Wiklicky.

The two terms in the first bracket is the difference between the mean and the state $\sum_x \alpha_x |x\rangle$; hence after adding this to the mean we have inverted the state $\sum_x \alpha_x |x\rangle$ about the mean. It is also easy by direct calculation to show that the two vectors $\sum_x(-\alpha_x + \langle\alpha\rangle)|x\rangle$ and $\langle\alpha\rangle \sum_x |x\rangle$ are orthogonal; hence the output is actually reflection about the direction $\sum_x |x\rangle$ (which is the same as the direction of $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_y |y\rangle$). A geometrical representation in the general case is sketched as:



Exercise 2 *Show that, in Grover's algorithm, the action of* $2|\psi\rangle\langle\psi| - \mathbf{I}$ *is a reflection about* $|\psi\rangle$*.*

Solution This follows from the solution to problem above.

Here is a more geometric alternative proof. Let $|x\rangle$ be an arbitrary state. Consider $|y\rangle = |x\rangle - \langle\psi|x\rangle|\psi\rangle$. Then $\langle\psi|y\rangle = \langle\psi|x\rangle - \langle\psi|x\rangle\langle\psi|\psi\rangle = 0$. Hence $|y\rangle$ is orthogonal to $|\psi\rangle$. On the other hand, $\langle\psi|x\rangle|\psi\rangle$ is the projection of $|x\rangle$ in the state $|\psi\rangle$. We have:

$$(2|\psi\rangle\langle\psi| - \mathbf{I})|x\rangle = (2|\psi\rangle\langle\psi| - \mathbf{I})(\langle\psi|x\rangle|\psi\rangle + |y\rangle) = \langle\psi|x\rangle|\psi\rangle - |y\rangle\,.$$

Thus, the action of the operator is reflection about $|\psi\rangle$.

Exercise 3 *Show that if we change the computational basis so that* $|\sigma\rangle$ *and* $|\tau\rangle$ *are basis elements, then the matrix representation of the Grover's transform G will be;*

$$G_{\sigma,\tau} = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix},$$

where $\theta/2$ is the angle between $|\sigma\rangle$ and $|\psi\rangle$.

Solution The action of the oracle O is reflection about $|\sigma\rangle$. By the previous problem, the action of $2|\psi\rangle\langle\psi| - I$ in the $|\sigma\rangle$ and $|\tau\rangle$ plane is reflection about $|\psi\rangle$. The composition of two reflections is rotation by twice the angle between the axes of reflection. Hence, the action of $G = (2|\psi\rangle\langle\psi| - I)O$ is rotation by $2(\theta/2) = \theta$. But the matrix for rotation by θ is precisely

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}.$$

In fact any vector in the real plane of $|\sigma\rangle$ and $|\tau\rangle$ is of the form $\binom{\cos\gamma}{\sin\gamma}$, where γ is the angle made from σ. A simple calculation with elementary trigonometry shows:

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \cos\gamma \\ \sin\gamma \end{pmatrix} = \begin{pmatrix} \cos(\gamma+\theta) \\ \sin(\gamma+\theta) \end{pmatrix}$$

and hence the state vector has rotated by θ.

Exercise 4 ** We have shown in the lecture that a quantum computer can search N items, consulting the black box that can access the database and tells you if an item is marked only $O(\sqrt{N})$ times. We now prove that no quantum algorithm can perform this task using fewer than $\Omega(\sqrt{N})$ accesses to the black box. Suppose the algorithm starts in the state $|\phi\rangle$. To determine the marked x we are allowed to apply a black box Q_x, which gives a phase shift of -1 to the solution $|x\rangle$ and leaves all other states invariant, i.e.,*

$$Q_x = 1 - 2|x\rangle\langle x|.$$

We suppose the algorithm applies Q_x exactly k-times, with unitary operations $U_1, U_2, \ldots, U_k$ interleaved between the black box operations. Define

$$|\phi_k^x\rangle = U_k Q_x U_{k-1} Q_x \ldots U_1 Q_x |\phi\rangle, \quad |\phi_k\rangle = U_k U_{k-1} \ldots U_1 |\phi\rangle,$$

and let $|\phi_0\rangle = |\phi\rangle$. Our goal is then to bound the quantity

$$D_k = \sum_x \|\phi_k^x - \phi_k\|^2 .$$

(i) Show that $D_k \leq 4k^2$.
Hint*: Do a proof by induction and employ the Cauchy-Schwarz inequality.*

(ii) Show that if the algorithm yields a solution with probability at least one-half, i.e., $|\langle x|\phi_k^x\rangle|^2 \geq 1/2$ for all x, then $D_k = \Omega(N)$.
Hint: *Employ the Cauchy-Schwarz inequality.*

(iii) Argue why this shows that Grover's algorithm is optimal.

(iv) Discuss why this result is both exciting and disappointing.

Solution

(i) We give an inductive proof. For $k = 0$ we have $D_k = 0$. Note that

$$D_{k+1} = \sum_x \|Q_x\phi_k^x - \phi_k\|^2 = \sum_x \|Q_x(\phi_k^x - \phi_k) + (Q_x - \mathbf{I})\phi_k\|^2 \ .$$

Applying $\|b + c\|^2 \leq \|b\|^2 + 2\|b\|\|c\| + \|c\|^2$ with $b = Q_x(\phi_k^x - \phi_k)$ and $c = (Q_x - \mathbf{I})\phi_k = -2\langle x|\phi_k\rangle\,|x\rangle$, gives

$$D_{k+1} \leq \sum_x (\|\phi_k^x - \phi_k\|^2 + 4\|\phi_k^x - \phi_k\||\langle x|\phi_k\rangle| + 4|\langle\phi_k|x\rangle|^2) \ .$$

Applying the Cauchy-Schwarz inequality to the second term on the right hand side, and noting that $\sum_x |\langle x|\phi_k\rangle|^2 = 1$ gives

$$\begin{aligned} D_{k+1} &\leq D_k + 4(\sum_x \|\phi_k^x - \phi_k\|^2)^{\frac{1}{2}}(\sum_{x'} |\langle\phi_k|x'\rangle|^2)^{\frac{1}{2}} + 4 \\ &\leq D_k + 4\sqrt{D_k} + 4 \end{aligned}$$

By the inductive hypothesis $D_k \leq 4k^2$ we obtain $D_{k+1} \leq 4k^2 + 8k + 4 = 4(k+1)^2$, which completes the induction.

(ii) Replacing $|x\rangle$ by $\exp(i\theta)\,|x\rangle$ for $\theta \in \mathbb{R}$ does not change the probability of success, so wlog we may assume that $\langle x|\phi_k^x\rangle = |\langle x|\phi_k^x\rangle|$, and therefore

$$\|\phi_k^x - x\|^2 = 2 - 2|\langle x|\phi_k^x\rangle| \leq 2 - \sqrt{2} \ .$$

Defining $E_k = \sum_x \|\phi_k^x - x\|^2$ we see that $E_k \leq (2 - \sqrt{2})N$. Defining $F_k = \sum_x \|x - \phi_k\|^2$ we have

$$\begin{aligned} D_k &= \sum_x \|(\phi_k^x - x) + (x - \phi_k)\|^2 \\ &\geq \sum_x \|\phi_k^x - x\|^2 - 2\sum_x \|\phi_k^x - x\|\|x - \phi_k\| + \sum_x \|x - \phi_k\|^2 \\ &= E_k + F_k - 2\sum_x \|\phi_k^x - x\|\|x - \phi_k\| \ . \end{aligned}$$

Applying the Cauchy-Schwarz inequality gives $\sum_x \|\phi_k^x - x\|\|x - \phi_k\| \leq \sqrt{E_k F_k}$, so we have

$$D_k \geq E_k + F_k - 2\sqrt{E_k F_k} = (\sqrt{F_k} - \sqrt{E_k})^2 \ .$$

Combining this with $F_k \geq 2N - 2\sqrt{N}$ and $E_k \leq (2 - \sqrt{2})N$ gives $D_k \geq cN$ for sufficiently large N, where c is any constant less then $(\sqrt{2} - \sqrt{2 - \sqrt{2}})^2$. Hence, we get $D_k = \Omega(N)$.

(iii) Combining (i) with (ii) implies that $k \geq \sqrt{cN/4}$ and thus we find $k = \Omega(\sqrt{N})$.

(iv) This result is exciting because it tells us that no further improvement is possible. In fact one can even show that Grover's algorithm is exactly optimal in the sense that the number of queries cannot be improved even by one. It is disappointing because we might have hoped to do much better than the square root speed-up. In particular, we might have hoped that it would be possible to search an N item space using $O(\log N)$ black box calls. Note that if such an algorithm would have existed, then it would have allowed us to solve **NP**-complete problems efficiently on a quantum computer.