Quantum Computing - Solutions 8

Abbas Edalat

1. Suppose the states $|u\rangle$ for $u \in T$ are eigenstates of U with eigenvalue ϕ_u. The phase estimation algorithm (Section 9 in the lecture notes) maps the normalized state

$$|0\rangle(\sum_{u\in T} d_u|u\rangle)$$

to the state

$$\sum_{u\in T} d_u|\hat{\phi}_u\rangle|u\rangle,$$

where the state $|\hat{\phi}_u\rangle$ gives a good estimate of ϕ_u. Show that with t chosen as

$$t = s + \left\lceil \log(2 + \frac{1}{2\epsilon}) \right\rceil,$$

the probability of measuring ϕ_u accurate to s bits in the output of the phase estimation algorithm is at least $|d_u|^2(1-\epsilon)$.

Solution: If we measure the second quantum register before the first, then we with probability $|d_u|^2$, the state of the output collapses to $|\hat{\phi}_u\rangle|u\rangle$ for some $u \in T$. Therefore, the whole analysis in the lecture notes implies that with t chosen as above, the probability of measuring ϕ_u accurate to s bits in the output of the phase estimation algorithm is at least $|d_u|^2(1-\epsilon)$.

More formally, note that

$$\sum_{u\in T} d_u|\hat{\phi}_u\rangle|u\rangle$$

$$= \frac{1}{2^t}\sum_{u\in T}\sum_{k=0}^{2^t-1}\sum_{y=0}^{2^t-1} e^{\frac{2\pi i}{2^t}(a_u-k)y}e^{2\pi i\delta_u y}|k\rangle|u\rangle,$$

where $\phi_u = a_u + \delta_u$ and a_u is the best t-bit approximatioon less than or equal to ϕ_u. We let $\alpha_{u,k}$ be the amplitude of $|(a_u+k)(\text{mod } 2^t)\rangle$ in $\sum_{u\in T} d_u|\hat{\phi}_u\rangle|u\rangle$. Then, we have:

$$\alpha_{u,k} = \frac{d_u}{2^t}\sum_{y=0}^{2^t-1}(e^{2\pi i(\phi_u-(a_u+k)/2^t)})^y.$$

Hence, the analysis in the lecture notes goes through with an additional factor of d_u as required.

2.

(i) Show that, in the Grover's algorithm, the eigenvalues of

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

are $e^{i\theta}$ and $e^{-i\theta}$ corresponding to the eigenvectors $|a\rangle = i|\sigma\rangle + |\tau\rangle$ and $|b\rangle = |\sigma\rangle + i|\tau\rangle$.

(ii) Express

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

as linear combination of the eigenvectors of $G_{\sigma,\tau}$, i.e. find d_a and d_b such that

$$|\psi\rangle = d_a|a\rangle + d_b|b\rangle.$$

(iii) Check that, in the quantum counting algorithm, measurement of the first register with

$$t = s + \lceil \log(2 + 1/(2\epsilon)) \rceil$$

will provide with a probability of at least $1-\epsilon$, an approximation to θ or $-\theta$ correct to s bits.

Solution: (i)

$$\left| \begin{pmatrix} \cos\theta - \lambda & -\sin\theta \\ \sin\theta & \cos\theta - \lambda \end{pmatrix} \right| = \lambda^2 - 2\cos\theta + 1 = 0$$

has solutions $\lambda = \cos\theta \pm i\sin\theta = e^{\pm i\theta}$. For $\lambda = e^{i\theta}$, the eigenvector satisfies:

$$\begin{pmatrix} -i\sin\theta & -\sin\theta \\ \sin\theta & -i\sin\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 0,$$

which has solution $\binom{i}{1}$. Similarly, for $\lambda = e^{-i\theta}$, the eigenvector satisfies:

$$\begin{pmatrix} i\sin\theta & -\sin\theta \\ \sin\theta & i\sin\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 0,$$

which has solution $\binom{1}{i}$.

(ii) In $\psi\rangle = \sqrt{\frac{N-M}{N}}|\sigma\rangle + \sqrt{\frac{M}{N}}|\tau\rangle$ replace $|\sigma\rangle$ and $\tau\rangle$ in terms of $|a\rangle$ and $|b\rangle$.

(iii) This follows from the fact that $|d_a|^2 + |d_b|^2 = 1$.

3.

(i) Find the inverse of 8 mod 21.

(ii) Show that if a and b are both inverses of x modulo n then $a = b \pmod{n}$.

(iii) Show that the order r of x modulo n satisfies $r \leq n$.

Solution:

(i) $2\times 8 = 16 \pmod{21}$, $3\times 8 = 24 = 3 \pmod{21}$,$4\times 8 = 32 = 11 \pmod{21}$, $5\times 8 = 40 = 19 \pmod{21}$, $6\times 8 = 48 = 4 \pmod{21}$, $7\times 8 = 56 = 14 \pmod{21}$, $8 \times 8 = 64 = 1 \pmod{21}$. Hence, $8^{-1} = 8 \pmod{21}$.

(ii) $a = a \times 1 = a \times x \times b = 1 \times b = b \pmod{n}$.

(iii) Consider the set of $n-1$ integers $\text{mod}(n)$ given by the powers, x^s, of x for $1 \leq s \leq n-1$: $x, x^2, x^3, \cdots x^{n-1}$. Since $\gcd(x, n) = 1$, these are all non-zero $\text{mod}(n)$. If they are different from 1 $\text{mod}(n)$, then there exist r and s (with $1 \leq s < r \leq n-1$) such that $x^r = x^s \text{ mod}(n)$. Hence, $x^{r-s} = x^r x^{-s} = x^r (x^s)^{-1} = 1 \pmod{n}$, which is a contradiction, since $1 \leq r - s \leq n-1$.

4. Show that, if $0 < x < N$, $\gcd(x, N) = 1$ and $L = \lceil \log N \rceil$, then the operation $U : \mathbb{C}^{2^L} \to \mathbb{C}^{2^L}$ defined by:

$$U|y\rangle = |xy (\text{mod } N)\rangle,$$

for $0 \leq y \leq N-1$ and $U|y\rangle = |y\rangle$ for $N \leq y \leq 2^L - 1$, is unitary.

Solution: It is easy to see that U permutes the basis vectors. In fact, for $0 \leq y \leq z \leq N-1$, if $U|y\rangle = U|z\rangle$ then we get $xy(\text{mod } N) = xz(\text{mod } N)$ and since x has an inverse mod N we get $y = z$.