Quantum Computing - Exercises 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

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

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

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

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

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

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, for $1 \leq x < n$, the order r of x modulo n satisfies $r < n$.

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.