Georgia Tech

Math, Physics & Computing
Math 4782, Phys 4782, CS4803

Quantum Information & Quantum Computing

Problems Set 2

Due March 2nd, 2006

1. Read carefully Nielsen-Chang, Section 5 .
2. Read carefully Box 5.2 .
3. Turn in exercises (*to be graded*) # 5.4, 5.5, 5.8, 5.10, 5.11, 5.12, 5.13 .

Exercises :

– **5.4-** *Give a decomposition of the controlled-R_k gate into single qubit and* CNOT *gates..*

Use the circuit shown in Nielsen-Chang, Section 4, Figure 4.6 . It is enough to use three single qubit gates, namely $C = R_{k+1}^{-1}$, $B = R_{k+1}$, $A = I$, $\alpha = 2\pi/2^{k+1}$.

– **5.5-** *Give a quantum circuit to compute the inverse Fourier transform.*

It is enough to take the circuit for the direct Fourier transform and just change the input into the output and vice-versa.

– **5.8-** *Suppose the phase estimation algorithm takes state $|0\rangle|u\rangle$ to the state $|\tilde{\varphi_u}\rangle|u\rangle$, so that given the input $|0\rangle \sum_u c_u|u\rangle$, the algorithm gives the outputs $\sum_u c_u|\tilde{\varphi_u}\rangle|u\rangle$. Show that if t is chosen according to (5.35), then the probability for measuring $\tilde{\varphi}_u$ accurate to n bits at the conclusion of the phase estimation algorithm is at least $|c_u|^2(1-\epsilon)$.*

From the reasoning found in Section 5.2.1, if the input is $|0\rangle|u\rangle$ the probability to obtain successfully φ accurate to n bits is at least $(1-\epsilon)$ if t is chosen according to (5.35), namely if $t \geq n+\ln(2+1/2\epsilon)$. On the other hand, if the input is now $|0\rangle \sum_u c_u|u\rangle$ instead, then the probability that it is given by $|0\rangle|u\rangle$ is exactly $|c_u|^2$ (this is one of the axiom of Quantum Mechanics). This later event is independent from the former, so that the probability for measuring $\tilde{\varphi_u}$ accurate to n bits at the conclusion of the phase estimation algorithm is the product of the two, namely it is at least $|c_u|^2(1-\epsilon)$.

– **5.10-** *Show that the order of $x = 5$ modulo $N = 21$ is* 6.

The order of x is the smallest positive integer r such that $x^r = 1$ (mod$N$). It is enough then to compute the successive powers of x (mod$N$) until 1 is obtained. If $N = 21$ and $x = 5$ this gives for instance $x^2 = 5 \times 5 = 25 = 25 - 21$ (mod 21) $= 4$, therefore $x^3 = 5 \times 4 = 20 = 20 - 21 = -1$ modulo 21. Proceeding in this way this gives

$$x = 5 \qquad x^2 = 4 \qquad x^3 = -1 \qquad x^4 = -5 \qquad x^5 = -4 \qquad x^6 = 1\,.$$

Consequently $r = 6$.

– **5.11-** *Show that the order of x satisfies $r \leq N$. (Here x has no common divisor with N.)*
The sequence $\{1, x, x^2, \cdots, x^n, \cdots, x^N\}$ computed modulo N contains $N+1$ elements. But there are at most N integers modulo N, so that at least two of these elements are equal modulo N. Namely there are $0 \leq m < n \leq N$ such that $x^m = x^n \mod N$. Since x has no common divisors with N, it follows that x is invertible modulo N, so that, dividing by x^m (modulo N) gives $1 = x^{n-m}$. It follows that $r \leq n - m \leq N$ (since $n - m > 0$).

Remark : the same proof actually shows that, whenever $x \neq 1$ then $1 < r < N$. For indeed in the list above, 0 never appears because x is invertible modulo N. Therefore the list contains at most $N-1$ distinct elements. Restricting the list to $\{1, x, x^2, \cdots, x^n, \cdots, x^{N-1}\}$ gives N elements with at most $N-1$ of them distincts. Thus, using the previous argument, $r \leq N - 1$. On the other hand $r \neq 1$ unless $x = 1$ which has been excluded. $\square$

– **5.12-** *Show that the operator U defined below is unitary (*Hint : *x is co-prime to N, and therefore has an inverse modulo N).*

$$U|y\rangle \;=\; |xy(\mathrm{mod}N)\rangle \qquad \textit{if} \qquad 0 \leq y \leq N-1\,, \qquad U|y\rangle \;=\; |y\rangle \qquad \textit{otherwise.} \tag{1}$$

where $0 \leq y < 2^L$ if L is the smallest positive integer such that $N \leq 2^L$.
First, it should be remarked that all numbers in the list $\{xy\ (\mathrm{mod}N)\,;\, 0 \leq y < N\}$ are contained between 0 and $N-1$, by definition. On the other hand, the adjoint $U^\dagger$ of U is defined such that $\langle y|U^\dagger|y'\rangle = (U|y\rangle, |y'\rangle)$. Thus if $0 \leq y < N$ the *r.h.s.* is given by $\langle xy\ (\mathrm{mod}N)|y'\rangle$, whereas if $N \leq y < 2^L$, it is given by $\langle y|y'\rangle$.
In the former case, this inner product vanishes unless $y' = xy\ (\mathrm{mod}N)$, namely unless $0 \leq y' < N$ and $y = x^{-1}y'\ (\mathrm{mod}N)$, in which case, it is equal to 1. Therefore $0 \leq y' < N \;\Rightarrow\; U^\dagger|y'\rangle = |x^{-1}y'\ (\mathrm{mod}N)\rangle$.
In the latter case the inner product vanishes unless $y = y'$, implying that $y' \geq N$. Thus $N \leq y' < 2^L \;\Rightarrow\; U^\dagger|y'\rangle = |y'\ (\mathrm{mod}N)\rangle$.
The previous result shows that $UU^\dagger|y'\rangle = U|x^{-1}y'\ (\mathrm{mod}N)\rangle = |xx^{-1}y'\ (\mathrm{mod}N)\rangle = |y'\rangle$ for $y' < N$, while $UU^\dagger|y'\rangle = U|y'\rangle = |y'\rangle$ if $N \leq y' < 2^L$. Since the family $\{|y'\rangle\,;\, 0 \leq y' < 2^L\}$ is an orthonormal basis in the Hilbert space of computer states, it follows that $UU^\dagger = I$. Therefore $U^\dagger$ is the inverse of U, namely U is unitary.

– **5.13-** *Prove the equation (5.44). (*Hint : *$\sum_{s=0}^{r-1} \exp(-2\imath\pi sk/r) = r\delta_{k0}$.) In fact prove that*

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\imath\pi sk/r}\, |u_s\rangle \;=\; |x^k \mod N\rangle\,. \tag{2}$$

Reminder : The operator U defined in eq. (1) above satisfies $U^r = I$. For indeed, for $y < N$ then $U^r|y\rangle = U^{r-1}|xy\ (\mathrm{mod}N)\rangle = \cdots = |x^r y\ (\mathrm{mod}N)\rangle = |y\rangle$ since, by definition of the order, $x^r = 1\ (\mathrm{mod}N)$. Hence if λ is an eigenvalue of U, then $\lambda^r = 1$. Therefore, there is $s \in [0, r)$ such that $\lambda = \lambda_s = e^{2\imath\pi s/r}$.
Moreover, by definition of the order, the sequence $\{1, x, \cdots, x^n, \cdots, x^{r-1}\}$ of integers modulo N contains exactly r distinct elements. Hence the vectors $|1\rangle, |x\rangle, \cdots, |x^n\ (\mathrm{mod}N)\rangle, \cdots, |x^{r-1}\ (\mathrm{mod}N)\rangle$ are orthonormal and make up an orthonormal basis of the subspace $\mathcal{H}_0$ they generated. In addition applying U to any of these vectors gives the next one $U|x^n\ (\mathrm{mod}N)\rangle = |x^{n+1}\ (\mathrm{mod}N)\rangle$. Thus $\mathcal{H}_0$ is invariant by U. Then $|u_s\rangle$ is defined as follows

$$|u_s\rangle \;=\; \frac{1}{\sqrt{r}}\sum_{n=0}^{r-1} e^{-2\imath\pi sn/r}|x^n\,(\mathrm{mod}\,N)\rangle\,. \qquad (3)$$

Applying U to this vector gives

$$U|u_s\rangle \;=\; \frac{1}{\sqrt{r}}\sum_{n=0}^{r-1} e^{-2\imath\pi sn/r}|x^{n+1}\,(\mathrm{mod}\,N)\rangle\,.$$

The sequence $\{x,\cdots,x^{n+1},\cdots,x^r=1\}$ is the same as $\{1,x,\cdots,x^n,\cdots,x^{r-1}\}$ up to a circular permutation. So changing n into $n-1$ gives

$$U|u_s\rangle \;=\; \frac{1}{\sqrt{r}}\sum_{n=0}^{r-1} e^{-2\imath\pi s(n-1)/r}|x^n\,(\mathrm{mod}\,N)\rangle\,,$$

because $e^{-2\imath\pi s(-1)/r} = e^{-2\imath\pi s(r-1)/r}$. But then, it is possible to factorize $e^{-2\imath\pi s(-1)/r} = e^{2\imath\pi s/r} = \lambda_s$ to get

$$U|u_s\rangle \;=\; \lambda_s|u_s\rangle\,.$$

Thus $|u_s\rangle$ is an eigenvector of U for the eigenvalue λ_s, provided it is nonzero. Since the $|x^n\,(\mathrm{mod}N)\rangle$'s make up an orthonormal basis, the square of the norm of $|u_s\rangle$ is the sum of the square of its components namely

$$\langle u_s|u_s\rangle \;=\; \frac{1}{r}\sum_{n=0}^{r-1}|e^{-2\imath\pi s(n-1)/r}|^2 \;=\; \frac{1}{r}\sum_{n=0}^{r-1}1 \;=\; 1\,.$$

In much the same way, the inner product of two of such vectors vanishes. This can be seen in two ways :

(i) *First argument :* since $U|u_s\rangle = \lambda_s|u_s\rangle$ then $\lambda_t\langle u_s|u_t\rangle = \langle u_s|U|u_t\rangle = (U^\dagger|u_s\rangle,|u_t\rangle) = (\overline{\lambda_s}|u_s\rangle,|u_t\rangle) = \lambda_s\langle u_s|u_t\rangle$. But if $s\neq t$ then $\lambda_s\neq\lambda_t$ so that the only possibility is $\langle u_s|u_t\rangle = 0$.

(ii) *Second argument :* the inner product $\langle u_s|u_t\rangle$ can be computed directly using the *hint* above

$$\langle u_s|u_t\rangle \;=\; \frac{1}{r}\sum_{n=0}^{r-1} e^{-2\imath\pi(t-s)n/r} \;=\; \delta_{s,t} \;=\; 0 \quad \text{if} \quad s\neq t\,.$$

Hence, the family $\{|u_s\rangle\,;\,0\leq s\leq r-1\}$ is an orthonormal basis of $\mathcal{H}_0$ as well. □

Solution of 5.13 : The eq. (5,44) is

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}|u_s\rangle = |1\rangle\,.$$

Actually, it is a consequence of eq. (2) for $k=0$. Thus it is sufficient to prove eq. (2). Using the definition (3) of $|u_s\rangle$ gives

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1} e^{2\imath\pi sk/r}|u_s\rangle \;=\; \frac{1}{r}\sum_{s=0}^{r-1}\sum_{n=0}^{r-1} e^{2\imath\pi s(k-n)/r}|x^n \mod N\rangle\,.$$

Exchanging the order of the two sums, gives $\sum_{s=0}^{r-1} e^{2\imath\pi s(k-n)/r} = r\delta_{k,n}$ thanks to the *hint* above. Therefore, since $\delta_{k,n}=0$ for $n\neq k$ and 1 if $n=k$,

$$\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1} e^{2\imath\pi sk/r}|u_s\rangle \;=\; \sum_{n=0}^{r-1}\delta_{k,n}|x^n \mod N\rangle \;=\; |x^k \mod N\rangle\,.$$

□