QUANTUM ALGORITHMS
HOMEWORK 11 SELECTED SOLUTIONS

PROF. MATTHEW MOORE

1. Let $t \in \mathbb{N}$.

(i) Prove that

$$x^t - 1 = (x-1)\sum_{k=0}^{t-1} x^k.$$

(ii) Prove that $x = e^{2\pi i(m/t)}$ is a solution to $x^t - 1$ for $m \in \mathbb{Z}$.

(iii) Let $m \in \mathbb{Z}$ with $0 \leq m < t$. Use the previous parts to prove that

$$\sum_{k=0}^{t-1} e^{2\pi i(km/t)} = \begin{cases} t & \text{if } m = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Solution:

(i): *Proof.* We have

$$\begin{aligned} x^t - 1 &= x^t + \left(x^{t-1} - x^{t-1}\right) + \left(x^{t-2} - x^{t-2}\right) + \cdots + \left(x - x\right) - 1 \\ &= \left(x^t - x^{t-1}\right) + \left(x^{t-1} - x^{t-2}\right) + \cdots + \left(x^2 - x\right) + \left(x - 1\right) \\ &= \left(x-1\right)x^{t-1} + \left(x-1\right)x^{t-2} + \cdots + \left(x-1\right)x + \left(x-1\right) \\ &= (x-1)\Big(x^{t-1} + x^{t-2} + \cdots + x + 1\Big) = (x-1)\sum_{k=0}^{t-1} x^k, \end{aligned}$$

as claimed. ☐

(ii): *Proof.* Recall that $e^{2\pi i} = 1$. We have

$$\begin{aligned} \left(e^{2\pi i(m/t)}\right)^t - 1 &= e^{2\pi i(mt/t)} - 1 = e^{2\pi i\, m} - 1 = \left(e^{2\pi i}\right)^m - 1 = (1)^m - 1 \\ &= 1 - 1 = 0. \end{aligned}$$

Therefore $e^{2\pi i(m/t)}$ is a root of $x^t - 1$. ☐

(iii): *Proof.* Let $z = e^{2\pi i(m/t)}$. We have

$$0 = z^t - 1 = (z-1)\sum_{k=0}^{t-1} z^k,$$

so $z = 1$ or $\sum z^k = 0$. If $m \neq 0$ then $z = e^{2\pi i(m/t)} \neq 1$, so it must be that $\sum z^k = 0$. If $m = 0$ then $z = e^{2\pi i(m/t)} = 1$, so $\sum z^k = t$. Hence

$$\sum_{k=0}^{t-1} e^{2\pi i(km/t)} = \sum_{k=0}^{t-1} z^k = \begin{cases} t & \text{if } m = 0, \\ 0 & \text{otherwise.} \end{cases}$$ ☐

Date: April 29, 2021.

2. **(i)** Explicitly calculate $\mathcal{QFT}_n\,|0^n\rangle$.

(ii) Explicitly calculate $\mathcal{QFT}_n\,|1^n\rangle$.

Solution: We have

$$\begin{aligned}
\mathcal{QFT}_n\,|0^n\rangle &= 2^{-n/2}\bigotimes_{k=1}^{n}|0\rangle + e^{2\pi i(0)/2^k}\,|1\rangle = 2^{-n/2}\bigotimes_{k=1}^{n}|0\rangle + |1\rangle = 2^{-n/2}\big(\,|0\rangle + |1\rangle\,\big)^{\otimes n}\\
&= 2^{-n/2}\sum_{x\in\{0,1\}^n}|x\rangle\,,\\
\mathcal{QFT}_n\,|1^n\rangle &= 2^{-n/2}\bigotimes_{k=1}^{n}|0\rangle + e^{2\pi i[1^n]/2^k}\,|1\rangle = 2^{-n/2}\bigotimes_{k=1}^{n}|0\rangle + e^{2\pi i(2^n-1)/2^k}\,|1\rangle\\
&= 2^{-n/2}\bigotimes_{k=1}^{n}|0\rangle + e^{-2\pi i/2^k}\,|1\rangle = 2^{-n/2}\sum_{x_1,\dots,x_n\in\{0,1\}}\left(\prod_{k=1}^{n}e^{-2\pi i x_k/2^k}\right)|x_1\cdots x_n\rangle\\
&= 2^{-n/2}\sum_{x_1,\dots,x_n\in\{0,1\}}e^{-2\pi i\sum x_k/2^k}\,|x_1\cdots x_n\rangle\\
&= 2^{-n/2}\sum_{x\in\{0,1\}^n}e^{-2\pi i[x]/2^n}\,|x\rangle\,.
\end{aligned}$$

3. Show that

$$\mathcal{QFT}_n\,|x\rangle = 2^{-n/2}\sum_{y\in\{0,1\}^n}e^{2\pi i[x][y]/2^n}\,|y\rangle\,,$$

where $[x]$ represents the number with binary representation $x\in\{0,1\}^n$ (and so $[x][y]$ is the product of x and y, regarded as binary numbers).

Solution:

Proof. We have

$$\begin{aligned}
\mathcal{QFT}_n\,|x\rangle &= 2^{-n/2}\bigotimes_{k=1}^{n}|0\rangle + e^{2\pi i[x]/2^k}\,|1\rangle = 2^{-n/2}\bigotimes_{k=1}^{n}\sum_{y_k\in\{0,1\}}e^{2\pi i y_k[x]/2^k}\,|y_k\rangle\\
&= 2^{-n/2}\sum_{y_1,\dots,y_k\in\{0,1\}}e^{2\pi i[x]\sum y_k/2^k}\,|y_1\cdots y_n\rangle = 2^{-n/2}\sum_{y\in\{0,1\}^n}e^{2\pi i[x][y]/2^n}\,|y\rangle\,. \square
\end{aligned}$$

4. Use the previous problem to prove that

$$\mathcal{QFT}_n^{\dagger}\,|x\rangle = 2^{-n/2}\sum_{y\in\{0,1\}^n}e^{-2\pi i[x][y]/2^n}\,|y\rangle$$

for basis vector $|x\rangle\in\{0,1\}$ defines the inverse of $\mathcal{QFT}_n$.

Hint 1: Show that $\mathcal{QFT}_n\circ\mathcal{QFT}_n^{\dagger}\,|x\rangle = \mathcal{QFT}_n^{\dagger}\circ\mathcal{QFT}_n\,|x\rangle = |x\rangle$.

Hint 2: You may find this identity useful

$$\sum_{k=0}^{2^n-1}e^{2\pi i\;k\ell/2^n} = 0 \qquad\text{if}\qquad \ell\neq 0.$$

Solution:

Proof. We have

$$\begin{aligned}
\mathcal{QFT}_n \circ \mathcal{QFT}_n^\dagger |x\rangle &= \mathcal{QFT}_n \Big(2^{-n/2} \sum_{y \in \{0,1\}^n} e^{-2\pi i [x][y]/2^n} |y\rangle \Big) \\
&= 2^{-n/2} \sum_{y \in \{0,1\}^n} e^{-2\pi i [x][y]/2^n} \; \mathcal{QFT}_n |y\rangle \\
&= 2^{-n/2} \sum_{y \in \{0,1\}^n} e^{-2\pi i [x][y]/2^n} \Big(2^{-n/2} \sum_{z \in \{0,1\}^n} e^{2\pi i [y][z]/2^n} |z\rangle \Big) \\
&= 2^{-n} \sum_{z \in \{0,1\}^n} \Big(\sum_{y \in \{0,1\}^n} e^{2\pi i [y] \big([x]-[z]\big)/2^n} \Big) |z\rangle .
\end{aligned}$$

Using the identity in Hint 2, the inner sum simplifies,

$$\sum_{y \in \{0,1\}^n} e^{2\pi i [y] \big([x]-[z]\big)/2^n} = \left\{ \begin{array}{cc} 0 & \text{if } x \neq z \\ \displaystyle\sum_{y \in \{0,1\}^n} 1 & \text{if } x = z \end{array} \right\} = \begin{cases} 0 & \text{if } x \neq z, \\ 2^n & \text{if } x = z. \end{cases}$$

Therefore the summand is nonzero only when $z = x$, in which case it is $2^n |x\rangle$. Thus,

$$2^{-n} \sum_{z \in \{0,1\}^n} \Big(\sum_{y \in \{0,1\}^n} e^{2\pi i [y] \big([x]-[z]\big)/2^n} \Big) |z\rangle = 2^{-n} 2^n |x\rangle = |x\rangle ,$$

as desired. The calculation showing $\mathcal{QFT}_n^\dagger \circ \mathcal{QFT}_n |x\rangle = |x\rangle$ is quite similar. □