QUANTUM ALGORITHMS
HOMEWORK 12 SELECTED SOLUTIONS

PROF. MATTHEW MOORE

AP 1. Let U be a unitary operator and suppose that $|\alpha\rangle$ and $|\beta\rangle$ are eigenvectors with respective eigenvalues $\lambda, \mu \in \mathbb{C}$. Prove that if $\lambda \neq \mu$ then $\langle \alpha \mid \beta \rangle = 0$ (i.e. $|\alpha\rangle$ and $|\beta\rangle$ are orthogonal).

Solution:

Proof. Without loss of generality, let us assume that $|\alpha\rangle$ and $|\beta\rangle$ have norm 1. We have

$$1 = \langle \alpha \mid \alpha \rangle = \langle \alpha | \, U^\dagger U \, | \alpha \rangle = \Big(\langle \alpha | \, \overline{\lambda} \Big) \Big(\lambda \, | \alpha \rangle \Big) = \overline{\lambda} \lambda \, \langle \alpha \mid \alpha \rangle \, ,$$

which implies that $\overline{\lambda}\lambda = 1$.

Replacing one instance of $|\alpha\rangle$ with $|\beta\rangle$ and performing a similar calculation yields

$$\langle \alpha \mid \beta \rangle = \langle \alpha | \, U^\dagger U \, | \beta \rangle = \Big(\langle \alpha | \, \overline{\lambda} \Big) \Big(\mu \, | \beta \rangle \Big) = \overline{\lambda} \mu \, \langle \alpha \mid \beta \rangle \, .$$

Let us assume that $\langle \alpha \mid \beta \rangle \neq 0$. The above series of equalities then implies that $\overline{\lambda}\mu = 1$. Multiplying both sides of this by λ and using the result from the previous paragraph that $\overline{\lambda}\lambda = 1$ results in $\mu = \lambda$, contradicting our initial hypothesis. □

Date: April 27, 2020.

AP 2. 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
$$\begin{aligned} x^t - 1 &= x^t + \big(x^{t-1} - x^{t-1}\big) + \big(x^{t-2} - x^{t-2}\big) + \cdots + \big(x - x\big) - 1 \\ &= \big(x^t - x^{t-1}\big) + \big(x^{t-1} - x^{t-2}\big) + \cdots + \big(x^2 - x\big) + \big(x - 1\big) \\ &= \big(x-1\big)x^{t-1} + \big(x-1\big)x^{t-2} + \cdots + \big(x-1\big)x + \big(x-1\big) \\ &= (x-1)\Big(x^{t-1} + x^{t-2} + \cdots + x + 1\Big) = (x-1)\sum_{k=0}^{t-1} x^k, \end{aligned}$$
as claimed. □

(ii): *Proof.* Recall that $e^{2\pi i} = 1$. We have
$$\begin{aligned} \big(e^{2\pi i(m/t)}\big)^t - 1 &= e^{2\pi i(mt/t)} - 1 = e^{2\pi i\, m} - 1 = \big(e^{2\pi i}\big)^m - 1 = (1)^m - 1 \\ &= 1 - 1 = 0. \end{aligned}$$
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
$$\sum_{k=0}^{t-1} e^{2\pi i(km/t)} = \sum_{k=0}^{t-1} z^k = \begin{cases} t & \text{if } m = 0, \\ 0 & \text{otherwise.} \end{cases}$$
□

AP 3. Fix $q \in \mathbb{N}$ and let $t = \mathrm{per}(a, q)$. Use the previous question to show that

$$|1\rangle = \frac{1}{\sqrt{t}} \sum_{k=0}^{t-1} |\alpha_k\rangle \,,$$

where

$$|\alpha_k\rangle = \frac{1}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i(km/t)} \, |a^m\rangle$$

and "1" and "a^m" are the binary encodings of $1, a^m \in (\mathbb{Z}/q\mathbb{Z})^\times$, respectively.

Solution:

Proof. We have

$$\begin{aligned}
\frac{1}{\sqrt{t}} \sum_{k=0}^{t-1} |\alpha_k\rangle &= \frac{1}{\sqrt{t}} \sum_{k=0}^{t-1} \left(\frac{1}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i(km/t)} \, |a^m\rangle \right) \\
&= \frac{1}{t} \sum_{k=0}^{t-1} \sum_{m=0}^{t-1} e^{-2\pi i(km/t)} \, |a^m\rangle = \frac{1}{t} \sum_{m=0}^{t-1} \sum_{k=0}^{t-1} e^{-2\pi i(km/t)} \, |a^m\rangle \\
&= \frac{1}{t} \sum_{m=0}^{t-1} \left(\sum_{k=0}^{t-1} e^{-2\pi i(km/t)} \right) |a^m\rangle \,.
\end{aligned}$$

Let us consider the coefficient $\sum_k e^{-2\pi i(km/t)}$. From the previous problem, $\sum_k e^{-2\pi i(km/t)} = 0$ except when $m = 0$, in which case $\sum_k e^{-2\pi i(km/t)} = t$. Returning to the main summation, we have

$$\frac{1}{t} \sum_{m=0}^{t-1} \left(\sum_{k=0}^{t-1} e^{-2\pi i(km/t)} \right) |a^m\rangle = \frac{1}{t} \Big(t \left|a^0\right\rangle + 0 \left|a^1\right\rangle + \cdots + 0 \left|a^{t-1}\right\rangle \Big) = |1\rangle \,,$$

finishing the proof. $\square$