# Quantum Algorithms
# Homework 12

Patrick Canny

Due: 2019-04-30

## 1 Book Problems

1. Exercise 13.2

**Solution:** The goal is to generate some controlled $U_b$. This new operator acts on some set of input qubits, say $U_b[0, 1 \dots n]$.

Note that $U_b \left|b, x\right\rangle \mapsto \left|b, bx \mod q\right\rangle$, $0 \leq x < q$. So, if we let $b = 1$ in any case, we just get back $x$. This is how we will define some new operator that performs the following transformation:

$$V : \left|0, 0\right\rangle \mapsto \left|0, 1\right\rangle \left|1, 0\right\rangle \mapsto \left|1, b\right\rangle$$

So the first bit of our vectors act as a control bit. If the bit is not set, the input to $U_b$ will just be the same as its output, meaning that the operator will have no effect (as we would expect). The final value for the computation is carried through in the non-ancillary bits, while the ancillary bits will be set to 0.

If the bit is set, $b$ itself will actually be carried through and will be modified after the applicatioon of $U_b$: $U_b[1, b] \mapsto \left|1, bx \mod q\right\rangle$. The ancillary bits will then be set back to 0 as a result of applying the conjugate transpose of the operator $V$. The final realization is then:

$$(VU_bV^\dagger)[c, 1 \dots n]$$

## 2 Additional Problems

Fix $q \in \mathbb{N}$ and let $n = \lceil \lg(q) \rceil$ so that $2^{n-1} < q \leq 2^n$. Recall the operator $U_a$ was defined (on p123) for $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ as

$$U_a \left|x\right\rangle = \begin{cases} \left|ax \bmod q\right\rangle & \text{if } 0 \leq x < q, \\ \left|x\right\rangle & \text{if } q \leq x < 2^n \end{cases}$$

NB: $\left|x\right\rangle$ is some binary encoding of $x \in \{0, \dots, q-1\}$ that is pre-determined, and similarly for $\left|ax \bmod q\right\rangle$. Let $t = \mathrm{per}_q(a)$.

1. Show that $\left|\xi_k\right\rangle = \dfrac{1}{\sqrt{t}} \displaystyle\sum_{m=0}^{t-1} e^{-2\pi i(km/t)} \left|a^m\right\rangle$ is an eigenvector of $U_a$ with eigenvalue $\lambda_k = e^{2\pi i(k/t)}$.

**Solution:** For something to be an eigenvector, the following must hold:

$$Ax = \lambda x \qquad \lambda \text{ an eigenvalue of A}$$

i.e.:

$$\begin{aligned}
U_a |\xi_k\rangle &= U_a\left(\frac{1}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i(km/t)} |a^m\rangle\right) \\
&= \frac{1}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i(km/t)} U_a |a^m\rangle \\
&= \frac{1}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i(km/t)} \left|a^{m+1}\right\rangle \qquad \text{because } U_a |a^m\rangle = |a^m * a \mod q\rangle = \left|a^{m+1}\right\rangle \\
&= \frac{e^{2\pi i(k/t)}}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i(k(m+1)/t)} \left|a^{m+1}\right\rangle \\
&= \frac{e^{2\pi i(k/t)}}{\sqrt{t}} \sum_{m=0}^{t-1} e^{-2\pi i(km/t)} |a^m\rangle \\
&= e^{2\pi i(k/t)} |\xi_k\rangle
\end{aligned}$$

The second to last step is possible because when the summation is expanded, it reveals that this is a cyclic group since $|a^t\rangle = 1$.

2. (i) Prove that $x^t - 1 = (x-1)\sum_{k=0}^{t-1} x^k$ for $t \in \mathbb{N}$.

**Solution:**

*Proof.*

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

From here it can be seen that all terms in this series cancel each other out, leaving only $-x^0 + x^t = x^t - 1$ □

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

**Solution:**

*Proof.* Using induction:

Base Case:

$m = 0 \implies e^{\pi i(0/t)} = 1 \implies 1^t - 1 = 0$

Inductive Hypothesis: This holds up to $m = k$

Inductive Step: Want to Show that this holds for $m = k + 1$

$e^{2\pi i(k+1/t)} = e^{2\pi i(m/t)+(1/t)} = e^{2\pi i(m/t)} e^{2\pi i(1/t)} = x * e^{2\pi i(1/t)} = x * 1 = x$

The last step is due to the fact that $e^{2\pi i} * k = 1$ □

3. Use the previous question to show that

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

where "1" is the binary encoding of $1 \in (\mathbb{Z}/q\mathbb{Z})^\times$ and $|\xi_k\rangle$ is defined in the first question.

**Solution:**

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

This last part is due to the fact that the summation of the roots of unity will be equal to 0. Since this summation appears on each term, the factor on each vector will be 0.