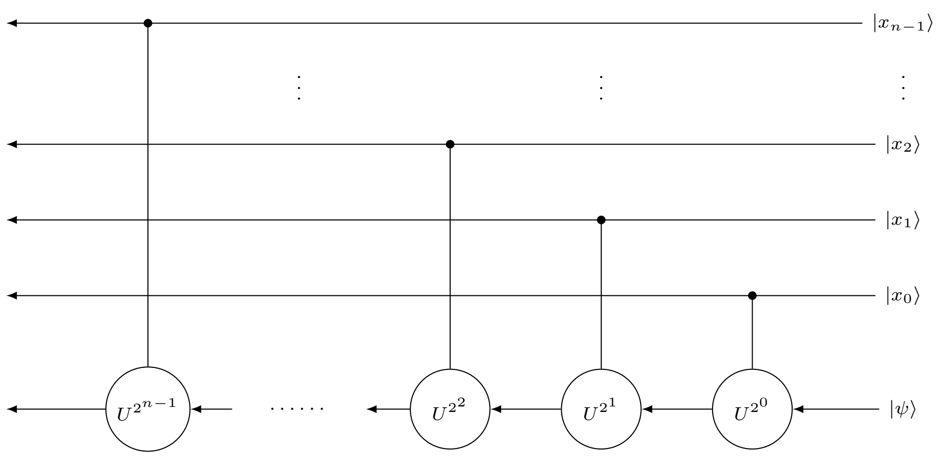
Quantum Algorithms
Homework 13 Solutions

Patrick Canny

Due: 2019-05-07

1. Consider the component of the phase-estimation circuit below.



This circuit is given formally as

$$\Upsilon(U) = \prod_{r=0}^{n-1} \Lambda\big(U^{2^r}\big)\,[r, P],$$

where P is the register containing the vector $|\psi\rangle$ and the other registers are enumerated as in the diagram.

For *arbitrary* quantum state $|\psi\rangle$, show that

$$\Upsilon(U)(|x\rangle \otimes |\psi\rangle) = |x\rangle \otimes U^{\underline{x}}\,|\psi\rangle\,,$$

where $\underline{x}$ is the base-2 number corresponding to the bit string $|x\rangle$.

Solution: Since the operation is controlled, when $r = 0$, the application of U acts like I. Otherwise, it acts like U^{2^r}. So, we can actually just represent this operation as $U^{x_r * 2^r}$. Then:

$$\begin{aligned}
\Upsilon(U)(|x\rangle \otimes |\psi\rangle) &= \prod_{r=0}^{n-1} (|x_r\rangle \otimes U^{x_r * 2^r} |\psi\rangle) \\
&= \prod_{r=0}^{n-1} |x_r\rangle \otimes \prod_{r=0}^{n-1} U^{x_r * 2^r} |\psi\rangle \\
&= |x\rangle \otimes U^{\sum_{n=0}^{n-1} x_r * 2^r} |\psi\rangle \\
&= |x\rangle \otimes U^{\underline{x}} |\psi\rangle
\end{aligned}$$

2. Let $\iota : \{0,1\} \to \{0,1\}$ be the identity function, defined by $\iota(x) = x$. The function $\iota_\oplus(x,y) = (x, x \oplus y)$ has the property that

$$\iota_\oplus(x,0) = (x,x),$$

meaning that it *clones* the bit x in the first register to the second register.

Let $|\psi\rangle \in \mathbb{B}$ be an arbitrary 1-qubit quantum state. Show that

$$\widehat{\iota}_\oplus(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

if and only if $|\psi\rangle = |0\rangle$ or $|\psi\rangle = |1\rangle$. That is, the quantum operator ($\widehat{\iota}_\oplus$) corresponding to the classical 1-bit cloning operator ($\iota_\oplus$) fails to clone $|\psi\rangle$ unless $|\psi\rangle$ is in a state corresponding to a classical bit.

Solution: Take generic vector $|\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$.

$$|\psi\rangle \otimes |0\rangle = \begin{pmatrix} a \\ 0 \\ b \\ 0 \end{pmatrix}$$

$$\widehat{\iota}_\oplus(|\psi\rangle) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} a \\ 0 \\ b \\ o \end{pmatrix} = \begin{pmatrix} a \\ 0 \\ 0 \\ b \end{pmatrix}$$

Similarly,

$$|\psi\rangle \otimes |\psi\rangle = \begin{pmatrix} a^2 \\ ab \\ ba \\ b^2 \end{pmatrix}$$

So, for

$$\widehat{\iota}_\oplus(|\psi\rangle \otimes |0\rangle) = |\psi\rangle \otimes |\psi\rangle$$

to hold:

$$a = a^2, ab = ba = 0, b^2 = b$$

So,

$$|\psi\rangle = (00), (10), (01)$$

But $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$ is not a valid quantum state, so $|\psi\rangle = |0\rangle, |1\rangle$.

3. Let U be a $2n$-qubit operator that *clones* two n-qubit quantum states, $|\varphi\rangle, |\psi\rangle\, \mathbb{B}^{\otimes n}$, meaning

$$U(|\varphi\rangle \otimes |0^n\rangle) = |\varphi\rangle \otimes |\varphi\rangle \qquad \text{and} \qquad U(|\psi\rangle \otimes |0^n\rangle) = |\psi\rangle \otimes |\psi\rangle .$$

Prove that U clones $|\varphi\rangle$ and $|\psi\rangle$ if and only if $|\varphi\rangle = |\psi\rangle$ or $\langle \varphi \mid \psi \rangle = 0$. [*Hint: take the inner product of the two equations.*]

Solution: Considering the hint, we will examine the inner product of the above equations.

$$\begin{aligned}\langle U(|\varphi\rangle \otimes |0^n\rangle) \mid U(|\psi\rangle \otimes |0^n\rangle)\rangle &= \langle \varphi 0^n | U^\dagger U |\psi 0^n\rangle \\ &= \langle \varphi\varphi \mid \psi\psi \rangle \\ &= \langle \varphi \mid \psi \rangle \langle 0^n \mid 0^n \rangle = \langle \varphi \mid \psi \rangle\end{aligned}$$

From here, we can establish the following:

$$\begin{aligned}\langle \varphi\varphi \mid \psi\psi \rangle = \langle \varphi \mid \psi \rangle &\Leftrightarrow \langle \varphi \mid \psi \rangle = 0 \text{ or } 1 \\ &\Leftrightarrow |\varphi\rangle = |\psi\rangle \text{ or } |\varphi\rangle \perp |\psi\rangle\end{aligned}$$

4. What does the previous question mean about the existence of a general cloning operators?

Solution: The previous question implies that some general cloning operator cannot exist. In fact, the previous solution specifies a specific cloning operator. This operator implies that in order to clone a state, that state must be $|0\rangle$ or itself. The general operator applied to two distinct states would not be capable of cloning them unless they were both $|0\rangle$ or literally the same state.