Jeremy Bejanin
20518945

QIP Assignment 3

24/10/2013

1. a) $S = \{(kr, k) \mid kr, k \in \mathbb{Z}_m\}$

Define $S_a = \{S + (a, 0) \mid a \in \mathbb{Z}_m\}$

i. take an element in S_a and S_b, $S_a \cap S_b \neq \phi$ iff $(k_a r + a, k_a) = (k_b r + b, k_b)$ for at least one element

ie: $k_a r + a = k_b r + b$ & $k_a = k_b$ $\rightarrow$ mod m

thus $k_b r + a = k_b r + b \Rightarrow a = b$

but we want $a \neq b$, thus $\boxed{S_a \cap S_b = \phi}$

ii. Take $S_0 = \{(kr, k) \mid kr, k \in \mathbb{Z}_m\}$.

This set contains elements for which kr & k both cover $\mathbb{Z}_m$. However, because the two numbers are related (by k), the set cannot cover $\mathbb{Z}_m \times \mathbb{Z}_m$.

Adding "a" to kr removes this limitation.

Take (i, j), any element of $\mathbb{Z}_m \times \mathbb{Z}_m$.
this element is always equal to one element in $S_0 \cup S_1 \cup \dots \cup S_{m-1}$:

$(i, j) = (kr + a, k)$ all algebra is mod m

$\Rightarrow k = j$ & $a = i - kr = i - jr$

By i, there is no overlap between S_a and S_b when $a \neq b$ thus

$S_0 \cup S_1 \cup \dots \cup S_{m-1} = \mathbb{Z}_m \times \mathbb{Z}_m$

b) If $f(x_1,x_2) = f(y_1,y_2)$

$(x_1,x_2)-(y_1,y_2) \in S$ so

$$x_1 - y_1 = kr \quad , \quad x_2 - y_2 = k$$

Now, assume that $(x_1,x_2) \in S_a$ and that $(y_1,y_2) \in S_b$

$$(x_1,x_2) = (k_a r + a, k_a) \quad , \quad (k_b r + b, k_b) = (y_1, y_2)$$

$$x_1 - y_1 = (k_a - k_b) r + a - b \quad , \quad x_2 - y_2 = k_a - k_b$$

Thus, $k_a - k_b = k$ and $x_1 - y_1 = kr + a - b$

Equating the equations for $x_1 - y_1$:

$$kr + a - b = kr \Rightarrow \boxed{a = b} \ \blacksquare$$

c) We have the state

$$\frac{1}{m}\sum_a \sum_k |k_a r + a\rangle |k_a\rangle |f(a,k)\rangle$$

But because we are in S_a, f does not depend on k_a, only on a. This is because, as shown in b), for $f(x_1,x_2) = f(y_1,y_2)$ k can be anything, as long as $a = b$. Thus:

$$|\psi\rangle = \frac{1}{m}\sum_a \sum_k |k_a r + a\rangle |k_a\rangle |f(a)\rangle$$

After the QFT

$$|\psi'\rangle = \frac{1}{m^2}\sum_a \sum_k \sum_{s_1} \sum_{s_2} e^{-2\pi i (k_a r + a) s_1/m} e^{-2\pi i k_a s_2/m} |s_1\rangle |s_2\rangle |f\rangle$$

$$|\psi\rangle = \frac{1}{m^2}\sum_a \sum_{s_1} \sum_{s_2} \underbrace{\sum_k e^{-2\pi i k_a (r s_1 + s_2)/m}}_{m \text{ iff } (s_1,s_2)\cdot(r,1) = 0 \ , \ s_2 = -s_1 r} e^{-2\pi i a s_1/m} |s_1\rangle |s_2\rangle |f\rangle$$

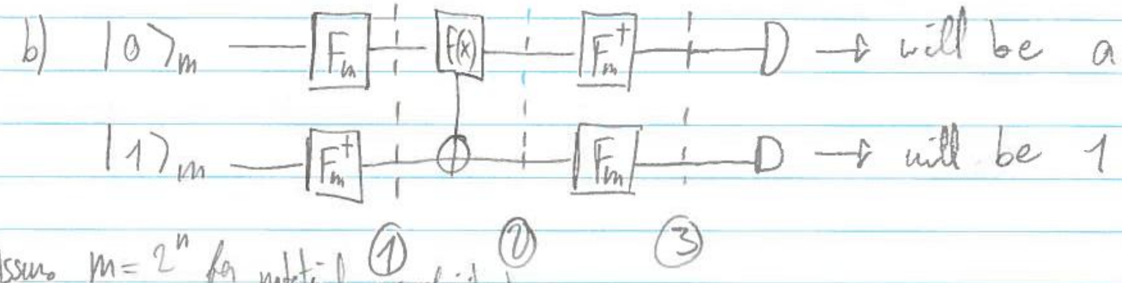
$$|\psi'\rangle = \frac{1}{m} \sum_a \sum_{s_1} e^{-2\pi i a s_1/m} |s_1\rangle |-s_1 r\rangle |f(a)\rangle$$

Now, when we measure registers 1 & 2, there are m^2 possible states, and so we have a probability $1/m^2$ to measure s_1 & $-s_1 r$.

However, we will measure these values for any value of a, of which there are m. The probability to obtain s_1 & $-s_1 r$ for <u>any</u> a is thus $m \cdot \frac{1}{m^2} = \frac{1}{m}$.

2. a) This function, $f(x) = ax + b$, is a first order polynomial. Both its coefficients can be found given $f(x_1)$, $f(x_2)$ where $x_1 \neq x_2$. Then $\dfrac{f(x_2) - f(x_1)}{x_2 - x_1} = a$.

b)



(Assume $m = 2^n$ for notational simplicity)

① Start by applying a QFT to state $|0\rangle$. Like a $H^{\otimes n}$, this will give us a superposition of all states.

We set the second register to $F_m^\dagger |1\rangle$. This is also a superposition over all states, each with a different phase.

We have, at ①:

$$|\psi_①\rangle = \frac{1}{\sqrt{m}} \sum_{x=0}^{m-1} |x\rangle \otimes \frac{1}{\sqrt{m}} \sum_{y=0}^{m-1} e^{-2\pi i y/m} |y\rangle$$

② After applying the function, we have, at ②

$$|\psi_②\rangle = \frac{1}{m} \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} e^{-2\pi i y/m} |x\rangle |y + f(x)\rangle$$

③ We now apply F_m and $F_m^\dagger$ to registers 2 and 1.

$$|\psi_③\rangle = \frac{1}{m^2} \sum_{x=0}^{m-1} \sum_{y=0}^{m-1} \sum_{x'=0}^{m-1} \sum_{y'=0}^{m-1} e^{-2\pi i y/m} e^{-2\pi i x x'/m} e^{2\pi i (y + f(x)) y'/m} |x'\rangle |y'\rangle$$

$$= \frac{1}{m^2} \sum_{x,y,x',y'} e^{-2\pi i y/m} e^{-2\pi i x x'/m} e^{2\pi i \frac{(y + ax + b) y'}{m}} |x'\rangle |y'\rangle$$

$$= \frac{1}{m^2} \sum_{x,y,x',y'} e^{-2\pi i y(1 - y')/m} e^{-2\pi i x (x' - a y')/m} e^{\frac{2\pi i b y'}{m}} |x'\rangle |y'\rangle$$

If we now do the sum over x and y, we notice that the only terms that stay are those for which

$$1 - y' = 0 \quad \text{and} \quad x' - ay' = 0$$

Thus we are left with the $y' = 1$, $x' = a$ term only!

$$|\psi_3\rangle = \frac{1}{m^2}\sum_{x'}\sum_{y'} \underbrace{\left(\sum_{y} e^{2\pi i(1-y')y/m}\right)}_{m \text{ iff } y'=1,\ 0 \text{ otherwise}} \left(\sum_{x} e^{-2\pi i(x'-ay')x/m}\right) e^{\frac{2\pi i}{m}by'} |x'\rangle|y'\rangle$$

$$= \frac{1}{m}\sum_{x'} \underbrace{\left(\sum_{x} e^{-2\pi i(x'-a)m}\right)}_{m \text{ iff } x'=a,\ 0 \text{ otherwise}} e^{\frac{2\pi i}{m}b} |x'\rangle|1\rangle$$

$$\boxed{|\psi_3\rangle = e^{\frac{2\pi i}{m}b} |a\rangle|1\rangle}$$

3. a) $F_{pq}|\varphi_1\rangle = F_{pq}\frac{1}{\sqrt{q}}\sum_{x=0}^{q-1}|xp\rangle$

$$= \frac{1}{\sqrt{q}}\frac{1}{\sqrt{pq}}\sum_{x=0}^{q-1}\sum_{y=0}^{pq-1} e^{2\pi i x\cancel{p}y/\cancel{p}q}|y\rangle$$

$$= \frac{1}{q\sqrt{p}}\sum_{y=0}^{pq-1}\underbrace{\left(\sum_{x}^{q-1} e^{2\pi i xy/q}\right)}_{\substack{q \text{ iff } y = nq,\ n = 0,1,2,\dots,p-1 \\ 0 \text{ otherwise}}}|y\rangle$$

$$= \frac{1}{\sqrt{p}}\sum_{n=0}^{p-1}|nq\rangle = |\varphi_2\rangle \ \checkmark$$

b) $F_{pq}|\varphi_3\rangle$

$$= \frac{1}{\sqrt{q}}\frac{1}{\sqrt{pq}}\sum_{x=0}^{q-1}\sum_{y=0}^{pq-1} e^{2\pi i (s+xp)y/pq}|y\rangle$$

$$= \frac{1}{\sqrt{q}}\cdot\frac{1}{\sqrt{pq}}\sum_{y=0}^{pq-1}\underbrace{\sum_{x} e^{2\pi i xy/q}}_{y=nq} e^{2\pi i sy/pq}|y\rangle$$

$$= \frac{1}{\sqrt{p}}\sum_{n=0}^{p-1} e^{2\pi i snp/pq}|nq\rangle$$

$$= \frac{1}{\sqrt{p}}\sum_{n=0}^{p-1} e^{2\pi i sn/p}|nq\rangle$$

4. a) $|\psi\rangle = U\left(\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle\right)$ by linearity

$= \alpha_1 U|\psi_1\rangle + \alpha_2 U|\psi_2\rangle$ by definition of $U|\psi_j\rangle = |a_j\rangle$

$= \alpha_1|a_1\rangle + \alpha_2|a_2\rangle$

Thus we will measure a_1 with probability $|\alpha_1|^2$ and a_2 with probability $|\alpha_2|^2$. $|a_1\rangle$ & $|a_2\rangle$ are still orthogonal since U is unitary. ∎

b) $|\psi\rangle = \alpha_1 U|\psi_1\rangle + \alpha_2 U|\psi_2\rangle$

$= \alpha_1\left(\sqrt{p_1}|a_1\rangle + \sqrt{q_1}|b_1\rangle\right) + \alpha_2\left(\sqrt{p_2}|a_2\rangle + \sqrt{q_2}|b_2\rangle\right)$

Now however, $|a_1\rangle$, $|b_1\rangle$, $|a_2\rangle$ & $|b_2\rangle$ are not nessessarily orthogonal to each other.

Eg, say $U|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$, $U|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$ then,

probabilities are not $p_1|\alpha_1|^2$ etc

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left[\overbrace{(\alpha_1+\alpha_2)}|0\rangle + \overbrace{(\alpha_1-\alpha_2)}|1\rangle\right]$$

Thus, even though $|\psi_1\rangle$ and $|\psi_2\rangle$ are orthogonal, "$|a_1\rangle, |b_1\rangle, |a_2\rangle$ & $|b_2\rangle$" are not.

5. $V\otimes I\, W|\phi\rangle|\psi_j\rangle$

since ψ_j is eigenvector of U

$= V|\phi\rangle \otimes U^\phi|\psi_j\rangle = V|\phi\rangle\, u_j^\phi|\psi_j\rangle$

$= \left(u_j^{a_j}\sqrt{p_j}|a_j\rangle + u_j^{b_j}\sqrt{q_j}|b_j\rangle\right) \otimes |\psi_j\rangle$

eigenvalues of unitary matrices are ± 1, there is thus only a phase in front of $|a_j\rangle$ or $|b_j\rangle$

This tells us that $U^\phi|\psi_j\rangle$ does not affect the probabilities

We now prove the statement of #5:

$$|\psi\rangle = (V \otimes I) W |\phi\rangle \left(\alpha_1 |\psi_1\rangle + \alpha_2 |\psi_2\rangle \right)$$

$$= (V \otimes I) |\phi\rangle \left(\alpha_1 U^{\phi} |\psi_1\rangle + \alpha_2 U^{\phi} |\psi_2\rangle \right)$$

$$= (V \otimes I) |\phi\rangle \left(\alpha_1 U_1^{\phi} |\psi_1\rangle + \alpha_2 U_2^{\phi} |\psi_2\rangle \right)$$

$$= U_1^{a_1} \sqrt{p_1}\, \alpha_1 |a_1 \psi_1\rangle + U_1^{b_1} \sqrt{q_1}\, \alpha_1 |b_1 \psi_1\rangle$$

$$+ U_2^{a_2} \sqrt{p_2}\, \alpha_2 |a_2 \psi_2\rangle + U_2^{b_2} \sqrt{q_2}\, \alpha_2 |b_2 \psi_2\rangle$$

Now, because ψ_1 & ψ_2 are orthogonal to each other, we can easily see that the probabilities are what was expected.