QC #11 Sanjay Kumar Keshava

Collaborators : Peter Lande, Gus Santaella

(1) @ assume $p \cdot x \equiv p \cdot y \mod(q)$

then $p \cdot x \equiv p \cdot y \equiv r \mod(q)$

where $0 \leq r < q$

then we can claim $p \cdot x = N_1 q + r$

and $p \cdot y = N_2 q + r$

(by definition)

$\Rightarrow p(x-y) = q(N_1 - N_2)$

$\therefore p(x-y) \equiv 0 \mod(q)$

since p and q are coprime, this above relation can be true only if $x-y = cq$ where c is some integer. But we notice that $0 \leq x < q-1$ and $0 \leq y < q-1$

$\therefore c = 0 \Rightarrow x = y$

$\therefore x \equiv y \mod(q)$

∴ we have showed

if $p \cdot x \equiv p \cdot y \pmod{qr}$

then $x \equiv y \pmod{qr}$

now, assume $x \equiv y \pmod{qr}$

then $x = y$ because $0 \leq x < qr-1$ and $0 \leq y \leq qr-1$

∴ $p \cdot x = p \cdot y$

and ∴ $p \cdot x \equiv p \cdot y \pmod{qr}$

∴ we have showed

if $x \equiv y \pmod{qr}$

then $p \cdot x \equiv p \cdot y \pmod{qr}$

so

$p \cdot x \equiv p \cdot y \pmod{qr}$

iff $x \equiv y \pmod{qr}$

the map $x \to p \cdot x$ is injective

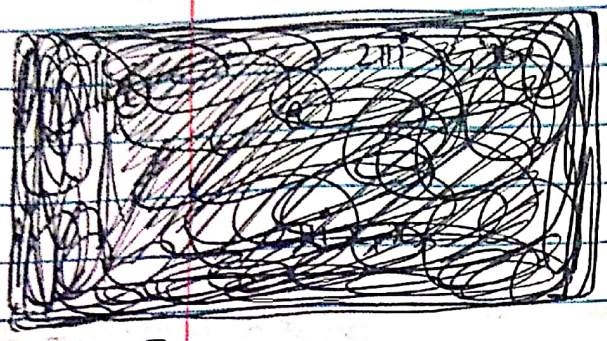
to complete our proof we notice sets A and B both have [redacted] qr elements, they are the same size

so the sets A and B are equal using these two properties given above

(b) (i) pq

(ii) q

(iii) p



(c) $\left(\frac{2\pi i\, x_1 y_2}{q} + \frac{2\pi i\, x_2 y_1}{p} + \frac{2\pi i\, x_2 y_2}{pq} \right)$

$= \frac{2\pi i}{pq}\left(px_1 y_2 + qx_2 y_1 + x_2 y_2 \right)$

$= \frac{2\pi i}{pq}\left((x_1 p + x_2) y_2 + qx_2 y_1 \right)$

$= \frac{2\pi i}{pq}\left(x y_2 + qx_2 y_1 \right)$

$= \frac{2\pi i}{pq}\left(xy_2 + y_1 q\,(x - x_1 p) \right)$

$= \frac{2\pi i}{pq}\left(x(y_1 q + y_2) - x_1 y_1 pq \right)$

$= \frac{2\pi i}{pq}(xy) - 2\pi i\,(x_1 y_1)$

$$\therefore e^{\frac{2\pi i x_1 y_2}{q}} e^{\frac{2\pi i x_2 y_1}{p}} e^{\frac{2\pi i x_2 y_2}{pq}} = e^{\frac{2\pi i xy}{pq}} e^{-2\pi i x_1 y_1}$$

↑ is just 1

$$\therefore \boxed{e^{\frac{2\pi i xy}{pq}} = e^{\frac{2\pi i x_1 y_2}{q}} e^{\frac{2\pi i x_2 y_1}{p}} e^{\frac{2\pi i x_2 y_2}{pq}}}$$

(d) U_a is the [redacted] q dimensional QFT matrix and its entries are given by

$$\left(U_a\right)_{ij} = \left(\frac{1}{\sqrt{q}} \left(e^{\frac{2\pi i}{q}}\right)^{ij}\right)$$

(e) U_b is the p dimensional QFT matrix and its entries are given by

$$\left(U_b\right)_{ij} = \left(\frac{1}{\sqrt{p}} \left(e^{\frac{2\pi i}{p}}\right)^{ij}\right)$$

(f) $U = \tilde{U}_b \phi_{pq} \tilde{U}_a$

$U|x\rangle = \tilde{U}_b \phi_{pq} \tilde{U}_a |\tilde{x}_1\rangle|x_2\rangle = (I_q \otimes U_b)(\phi_{pq})(U_a \otimes I_p)|\tilde{x}_1\rangle|x_2\rangle$

$$\therefore U|x\rangle = (I_q \otimes U_b)(\phi_{pq})\left(\frac{1}{\sqrt{q}} \sum_{y_2=0}^{q-1} e^{2\pi i \tilde{x}_1 y_2/q} |y_2\rangle\right)|x_2\rangle$$

$$= (I_q \otimes U_b) \frac{1}{\sqrt{q}} \sum_{y_2=0}^{q-1} e^{\frac{2\pi i x_2 y_2}{pq}} e^{\frac{2\pi i \tilde{x}_1 y_2}{q}} |y_2\rangle|x_2\rangle$$

$$= \frac{1}{\sqrt{pq}} \sum_{y_1=0}^{p-1} \sum_{y_2=0}^{q-1} e^{\frac{2\pi i x_2 y_1}{p}} e^{\frac{2\pi i x_2 y_2}{pq}} e^{\frac{2\pi i \tilde{x}_1 y_2}{q}} |y_2\rangle|y_1\rangle$$

from part (a) since $\tilde{x}_1 = x_1 p \bmod (q)$ and the set of $\tilde{x}_1$ is equal to the set of x_1 values we can replace this in our sum

$$U|x\rangle = \frac{1}{\sqrt{pq}} \sum_{y_1=0}^{p-1} \sum_{y_2=0}^{q-1} e^{\frac{2\pi i x_2 y_1}{p}} e^{\frac{2\pi i x_2 y_2}{pq}} e^{\frac{2\pi i x_1 y_2}{q}} |y_2\rangle|y_1\rangle$$

now we have $|y\rangle = |y_2\rangle|y_1\rangle$ now re-indexing we get, and using the result from part (c) finally

$$U|x\rangle = \frac{1}{\sqrt{pq}} \sum_{y=0}^{pq-1} e^{\frac{2\pi i xy}{pq}} |y\rangle$$

$$\therefore \boxed{U = \tilde{U}_b \phi_{pq} \tilde{U}_a}$$

(2) @ $|\psi_2\rangle = \frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i\theta(2^{n-1})}|1\rangle\right) \otimes \cdots\cdots \left(|0\rangle + e^{2\pi i\theta 2^0}|1\rangle\right) \otimes |\psi\rangle$

Now, multiplying out the tensor products gives us

$$|\psi\rangle_2 = \frac{1}{2^{n/2}} \Big((|00\cdots000\rangle \otimes |\psi\rangle)\, e^{2\pi i\theta(0)} + (|00\cdots001\rangle \otimes |\psi\rangle)\, e^{2\pi i\theta(2^0)} + (|00\cdots010\rangle \otimes |\psi\rangle)\, e^{2\pi i\theta(2^1)} + (|00\cdots011\rangle \otimes |\psi\rangle)\, e^{2\pi i\theta(2^1+2^0)} \cdots + (|11\cdots111\rangle \otimes |\psi\rangle)\, e^{2\pi i\theta(2^{n-1}+2^{n-2}\cdots+2^1+2^0)} \Big)$$

$$= \frac{1}{2^{n/2}} \Big((|0\rangle \otimes |\psi\rangle)\, e^{2\pi i\theta(0)} + (|1\rangle \otimes |\psi\rangle)\, e^{2\pi i\theta(1)} + (|2\rangle \otimes |\psi\rangle)\, e^{2\pi i\theta(2)} + (|3\rangle \otimes |\psi\rangle)\, e^{2\pi i\theta(3)} \cdots + (|2^n-1\rangle \otimes |\psi\rangle)\, e^{2\pi i\theta(2^n-1)} \Big)$$

because we know that $2^{n-1} + 2^{n-2} \cdots 2^1 + 2^0 = 2^n - 1$

$$\therefore \quad |\psi_2\rangle = \frac{1}{2^{n/2}} \sum_{k=0}^{2^n-1} e^{2\pi i\theta k} |k\rangle \otimes |\psi\rangle$$

which shows the required relation

(b) $$|\psi_3\rangle = \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i k}{2^n}(x-2^n\theta)} |x\rangle \otimes |\psi\rangle$$

$$\therefore |\psi_3\rangle = \sum_{x=0}^{2^n-1} C_x \left(|x\rangle \otimes |\psi\rangle\right)$$

where $$C_x = \frac{1}{2^n} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i k}{2^n}(x-2^n\theta)}$$

note n is a fixed number here

So if we measure x

so if we measure x, we are most likely to measure the value of x which corresponds to the largest $|C_x|^2$

#1 if $x \approx 2^n\theta$

then $$C_x = \frac{1}{2^n} \sum_{k=0}^{2^n-1} 1 = 1$$

$$\therefore |C_x|^2 \approx 1$$

#1 $\therefore$ if $x \not\approx 2^n\theta$

$$|C_x|^2 \approx 0 \quad \left(\text{because } \sum_{x=0}^{2^n-1} |C_x|^2 = 1\right)$$

∴ if we measure x, it is highly likely that $x = 2^n\theta$ and therefore

$$\theta = \frac{x}{2^n}$$ can be found with ease