Shor's algorithm

Course at IUM Ch. Pittet

III

Recall that if V is a (finite dimensional) complex Hilbert space, a <u>orthogonal projector</u> $P : V \to V$ is a $\mathbb{C}$ linear map such that $P^2 = P$ and such that $P^* = P$ (that is $\forall v, w \in V$ $\langle Pv, w \rangle = \langle v, Pw \rangle$).

<u>Proposition</u> Let V be a finite dimensional complex Hilbert space.

i) Let $P : V \to V$ be a linear map. Then $[P^* = P$ and $P^2 = P]$ if and only if $V = \ker P \boxplus \operatorname{Im} P$. ($\boxplus$: orthogonal sum)

ii) Let $P_1, \dots, P_k : V \to V$ be orthogonal projectors. Then $[P_i \circ P_j = 0 \ \forall i \neq j$ and $id_V = \sum_{i=1}^{k} P_i]$ if and only $V = \boxplus_{i=1}^{k} \operatorname{Im} P_i$.

Proof: (exercise)

i) if $P^2 = P$ then $\ker P \cap \operatorname{Im} P = \{0\}$

if $P^* = P$ then $\ker P$ is orthogonal to $\operatorname{Im} P$

Hence $[P^2 = P$ and $P^* = P] \Rightarrow V = \ker P \boxplus \operatorname{Im} P$ ($\uparrow$ $\dim V < \infty$.)

If $V = \ker P \boxplus \operatorname{Im} P$ then

$x + y \xmapsto{P} y$ satisfies $P^2 = P$

and $\langle x+y, P(x'+y') \rangle = \langle x+y, y' \rangle = \langle y, y' \rangle$

$\langle P(x+y), x'+y' \rangle = \langle y, x'+y' \rangle = \langle y, y' \rangle$

ii) If $P_i \circ P_j = 0$ then $\mathrm{Im}\, P_i \cap \left(\sum_{j \neq i} \mathrm{Im}\, P_j \right)$

$= \{0\}$: $P_i(x) = y = \sum_{j \neq i} P_j(x_j)$

$\Rightarrow \quad y = P_i^2(x) = \sum_{j \neq i} P_i \cdot P_j(x_j) \quad = 0$.

If $id_V = \sum_{i=1}^{k} P_i$ then $V = \sum_{i=1}^{k} \mathrm{Im}\, P_i$.

If $V = \boxplus_{i=1}^{k} \mathrm{Im}\, P_i$ then $\mathrm{Ker}\, P_i = \mathrm{Im}\, P_i^{\perp}$

$= \boxplus_{j \neq i} \mathrm{Im}\, P_j \quad \Rightarrow \quad P_i P_j = 0 \quad$ if $i \neq j$.

Also $v = \sum_i P_i(x_i)$ hence $P_j(v) = \sum_i P_j P_i(x_i)$

$= P_j^2(x_j) = P_j(x_j)$. That is

$v = \sum_i P_i(v)$ ie $id_V = \sum_{i=1}^{k} P_i$. ∎

Measurement of a quantum system

Let V be a finite dimensional complex Hilbert space. A <u>measurement</u> on V is a finite collection of orthogonal projectors $P_1, \ldots, P_k : V \to V$ s.t. $id_V = \sum_{i=1}^{k} P_i$ and $P_i \circ P_j = 0$ if $i \neq j$.

(Also called a <u>projective measurement</u>)

If the quantum system V is in the state $v \in V$, ($\|v\| = 1$ by def. of a state) and the measurement $(P_1, \ldots, P_k)$ is applied, then we observe $1 \leq i \leq k$ with probability $\mathcal{P}(i) = \| P_i(v) \|^2$.

Notice that

$$\sum_{i=1}^{k} \mathcal{P}(i) = \sum_{i=1}^{k} \|P_i(v)\|^2 \overset{\text{Pyth.}}{=} \| \sum_{i=1}^{k} P_i(v) \|^2 = \|v\|^2 = 1.$$

If the measurement $(P_1, \dots, P_k)$ is applied to the state $v \in V$ and if $1 \le i \le k$ is observed, then the system after measurement is in state $\dfrac{P_i(v)}{\|P_i(v)\|}$.

(Notice that $P_i(v) \neq 0$ if i is observed when the measurement $(P_1 \dots P_k)$ is applied to v.)

<u>Examples of measurements</u>: 1) $V = \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$ that is the system is a single q-bit.

$P_0 : \mathbb{C}[\mathbb{Z}/2\mathbb{Z}] \to \mathbb{C}[\mathbb{Z}/2\mathbb{Z}]$ orthogonal proj. on the line $\mathbb{C} \cdot 0$ and

$P_1 =$ orthogonal projection on the line $\mathbb{C} \cdot 1$. The measurement is (P_0, P_1).

If $v = \alpha \cdot 0 + \beta \cdot 1$, $\alpha, \beta \in \mathbb{C}$: and (P_0, P_1) is $|\alpha|^2 + |\beta|^2 = 1$

applied to the state v then we get 0 with probability

$\mathcal{P}(0) = \|P_0(v)\|^2 = \|\alpha \cdot 0\|^2 = |\alpha|^2$

and if 0 is observed then the system is in state $\dfrac{\alpha}{\|\alpha\|} \cdot 0$.

We get 1 with probability

$\mathcal{P}(1) = \|P_1(v)\|^2 = \|\beta \cdot 1\|^2 = |\beta|^2$

and if 1 is observed then the system is in state $\dfrac{\beta}{\|\beta\|} \cdot 1$.

2) Suppose $(P_1, \dots, P_k)$ is a measurement on V and W is another finite dimensional complex Hilbert space. Then $(P_1 \otimes id_W, P_2 \otimes id_W, \dots, P_k \otimes id_W)$ is a measurement on $V \otimes W$.

Exercise: prove it. $P_i^2 = P_i$ by hypoth.

$$(P_i \otimes id)^2 = P_i^2 \otimes id = (P_i \otimes id)$$

$$\langle (P_i \otimes id)(v \otimes w), v' \otimes w' \rangle = \langle P_i v \otimes w, v \otimes w' \rangle$$
$$= \langle P_i v, v' \rangle \langle w, w' \rangle$$

$$\langle v \otimes w, (P_i \otimes id)(v' \otimes w') \rangle = \langle v \otimes w, P_i v' \otimes w' \rangle$$
$$= \langle v, P_i v' \rangle \langle w, w' \rangle \quad \text{and} \quad P_i = P_i^*$$
by hypothesis -

$$(P_i \otimes id)(P_j \otimes id) = P_i P_j \otimes id = 0 \quad \text{if} \quad i \neq j$$

$$\sum_{i=1}^{k} (P_i \otimes id)(v \otimes w) = \sum_{i=1}^{k} P_i(v) \otimes w$$
$$= v \otimes w$$

3) Suppose $\{P_i\}_{i=1,\dots k}$ is a measurement on V, $\{Q_j\}_{j=1\dots,\ell}$ ——— on W then $\{P_i \otimes Q_j\}_{i,j}$ is a measurement on $V \otimes W$ which equals the composition of the measurements $\{(P_i \otimes id) \circ (id \otimes Q_j)\}_{i,j}$ as well as $\{(id \otimes Q_j) \circ (P_i \otimes id)\}_{j,i}$.

Exercise: prove it.

The composition $(P_i \otimes id) \circ (id \otimes Q_j)$
$= P_i \otimes Q_j$, as well as $(id \otimes Q_j) \circ (P_i \otimes id)$
hence it is enough to check that
$(P_i \otimes Q_j)_{ij}$ is a measurement.

$P_i \otimes Q_j \cdot P_i \otimes Q_j = P_i^2 \otimes Q_j^2 = P_i \otimes Q_j$

We checked that $(P_i \otimes id)^* = P_i^* \otimes id$
hence $(P_i \otimes Q_j)^* = [(P_i \otimes id)(id \otimes Q_j)]^*$
$= (id \otimes Q_j)^* (P_i \otimes id)^* = (id \otimes Q_j^*)(P_i^* \otimes id)$
$= P_i \otimes Q_j$.

$(P_i \otimes Q_j)(P_{i'} \otimes Q_{j'}) = P_i P_{i'} \otimes Q_j Q_{j'}$
$= 0$ if $(i,j) \neq (i',j')$.

$$\sum_{ij} (P_i \otimes Q_j)(v \otimes w) = \sum_{ij} P_i v \otimes Q_j w$$
$$= \sum_i P_i v \otimes \left(\sum_j Q_j w\right) = \sum_i P_i v \otimes w = v \otimes w \quad \square$$

Fourier transform on $\mathbb{Z}/n\mathbb{Z}$

All the homomorphisms $\chi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$
are given by the list:

$$\chi^c : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$$
$$x \longmapsto e^{\frac{2i\pi}{n} c \cdot x}$$

where $c = 0, \ldots, n-1$.

Indeed, χ is determined by $\chi(1)$
which is an n-root of 1 in $\mathbb{C}^*$
hence $\chi(1) = e^{\frac{2i\pi}{n} c}$ for some $c = 0, \ldots, n-1$.

The space of $\mathbb{C}$ valued functions on $\mathbb{Z}/n\mathbb{Z}$ is a Hilbert space $L^2(\mathbb{Z}/n\mathbb{Z})$ for the product

$$\langle \varphi, \psi \rangle = \sum_{x \in \mathbb{Z}/n\mathbb{Z}} \varphi(x)\,\overline{\psi(x)} .$$

The characteristic functions of points

$$\{\delta_x\}_{x \in \mathbb{Z}/n\mathbb{Z}} \qquad \delta_x(y) = \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases}$$

form an orthonormal basis of $L^2(\mathbb{Z}/n\mathbb{Z})$.

Proposition (Orthogonality relations of characters)

The functions

$$\frac{\chi^c}{\sqrt{n}}, \quad c = 0, \dots, n-1$$

form an orthonormal basis of $L^2(\mathbb{Z}/n\mathbb{Z})$

Proof: $\langle \chi^c, \chi^d \rangle = \sum_{x=0}^{n-1} e^{\frac{2i\pi}{n}cx} e^{-\frac{2i\pi}{n}dx}$

$$= \sum_{x=0}^{n-1} e^{\frac{2i\pi}{n}(c-d)x} .$$

If $c = d$, we get n. If $c - d \neq 0$ we get 0:

$$\sum_{k=0}^{n-1} w^k = \frac{1 - w^n}{1 - w}$$

is 0 if w is a nth root of unity $w \neq 1$. ∎

The **Fourier transform** $\mathcal{F} : L^2(\mathbb{Z}/n\mathbb{Z}) \to L^2(\mathbb{Z}/n\mathbb{Z})$ is the linear map defined by

$$\mathcal{F}\left(\frac{\chi^c}{\sqrt{n}}\right) \mapsto \delta_c , \quad c = 0, 1, \dots, n-1$$

As it sends an orthonormal basis to an orthonormal basis, it is a unitary transformation of $L^2(\mathbb{Z}/n\mathbb{Z})$.

Explicitly,

$$\sum_x \langle f, \delta_x \rangle \delta_x \xmapsto{\mathcal{F}} \sum_c \langle f, \frac{\chi^c}{\sqrt{n}} \rangle \delta_c \,.$$