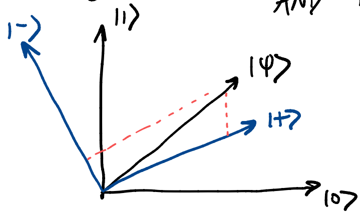
[TU DELFT - QUANTUM CRYPTOGRAPHY]

- measuring a qubit → GET INNER PRODUCT BETWEEN QUBIT STATE AND BASIS



$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Basis: $|+\rangle, |-\rangle$

outcome "$|+\rangle$"

$P_+ = |\langle\psi|+\rangle|^2$

outcome "$|-\rangle$"

$P_- = |\langle\psi|-\rangle|^2$

GENERAL RULE

Basis → $\{|b\rangle\}$ $\quad |b\rangle \in \mathbb{C}^d \quad d = 2^n$

probability of measurement outcomes

$P_b = |\langle\psi|b\rangle|^2$

outcome b → post measurement state

Ex:

State: $|\psi\rangle = \sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle \qquad \{|0\rangle, |1\rangle\}$

$P_0 = |\langle\psi|0\rangle|^2 = \left|\left(\sqrt{\frac{1}{3}}\langle 0| + \sqrt{\frac{2}{3}}\langle 1|\right)|0\rangle\right|^2$

$= \left|\sqrt{\frac{1}{3}}\underbrace{\langle 0|0\rangle}_{1} + \sqrt{\frac{2}{3}}\underbrace{\langle 1|0\rangle}_{0}\right|^2$ orthogonal

$= \left|\sqrt{\frac{1}{3}}\right|^2 = \frac{1}{3} \leftarrow P_0$

Ex: complex amplitude

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$$

BASIS $\{|+\rangle, |-\rangle\}$

$$P_+ = |\langle\psi|+\rangle|^2$$
$$= \left|\left(\tfrac{1}{2}\langle 0| - \tfrac{1}{2}i\langle 1|\right)|+\rangle\right|^2$$
$$= \frac{1}{4}\left|\langle 0|0\rangle - i\langle 1|0\rangle - i\langle 1|1\rangle + \langle 0|1\rangle\right|^2$$
$$= \frac{1}{4}\left|1 - 0 + i + 0\right|^2 = \frac{1}{4}|1-i|^2$$
$$= \frac{1}{4}\left[1 - i^2\right] = \frac{1}{4}\cdot 2 = \frac{1}{2} \leftarrow P_+$$

Ex: Measuring 2 Qubits

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

$$P_{00} = |\langle\psi|00\rangle|^2$$
$$= \left|\left(\frac{1}{\sqrt{2}}\langle 00| + \langle 11|\right)|00\rangle\right|^2 = \left|\frac{1}{\sqrt{2}}\langle 00|00\rangle + \frac{1}{\sqrt{2}}\langle 11|00\rangle\right|^2$$
$$= \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}$$

Note $P_{01} = P_{10} = \emptyset$! b/c entangled Bell State

What operations can we perform on a qubit

$|\psi_{new}\rangle = U|\psi\rangle$ For $U \rightarrow$ needs to preserve normalization

$\langle\psi_{new}| = \langle\psi|U^\dagger$ such that $\langle\psi_{new}|\psi_{new}\rangle = 1 = \langle\psi|U^\dagger U|\psi\rangle$

Allowed Unitary Transformation

Unitary matrices

U is unitary $\rightarrow U^\dagger U = UU^\dagger = \mathbb{I}$

$(U)^T = (U^*)^T$

[Density Matrix]

$$\underset{\text{VECTOR}}{|\psi\rangle} \longrightarrow \underset{\text{MATRIX}}{\rho} = |\psi\rangle\langle\psi| \text{ outer product}$$

Ex:

$$|0\rangle \rightarrow \rho = |0\rangle\langle 0| = \begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \text{ pure state}$$

Solving mixtures

state $|\psi_j\rangle \longrightarrow \rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$

$P_0 = \mathrm{Tr}\left[|0\rangle\langle 0|\rho\right]$ where ρ

Measuring a density matrix in a basis

$\{|b\rangle\}_b \rightarrow P_b = \langle b|\rho|b\rangle$

Pure & Mixed

$|\psi\rangle \longrightarrow \rho = |\psi\rangle\langle\psi|$ rank $= 1$

if $\mathrm{rank}(\rho) > 1$ = mixed state