QINTRO - TD5

Ex. 6

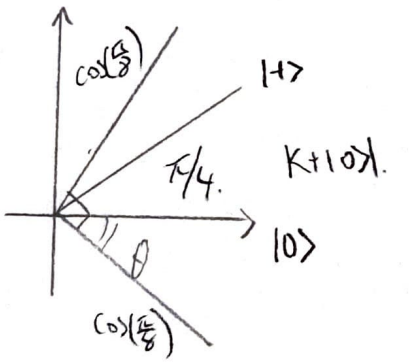
Commit phase: Alice sends $|0\rangle$ to commit to $b=0$

$|+\rangle$ to commit to $b=1$

Reveal: if Alice says she had commited to 0, Bob measure in $|0\rangle, |1\rangle$. If Alice said 1, Bob measures in $|+\rangle|-\rangle$.

1. $\Pr(\text{Bobs cheats}) = \Pr(\text{distinguish } |0\rangle \text{ and } |+\rangle)$

$$= \frac{1}{2}\left(\cos^2\left(\frac{\pi}{8}\right) + \cos^2\left(\frac{\pi}{8}\right)\right) = \cos^2\left(\frac{\pi}{8}\right)$$



$$|+\rangle = \frac{|1\rangle + |0\rangle}{\sqrt{2}}$$

$$\theta = \frac{\pi}{4} - \frac{\pi}{8} = \frac{\pi}{8}$$

$$2\theta + \text{angle}(|0\rangle, |+\rangle) = \frac{\pi}{2}$$

$$\rightarrow \theta = \pi/8$$

2. Alice sends $|\phi\rangle$

$$\Pr(\text{Alice wins}) = \frac{1}{2}\left(\Pr\left(\begin{array}{l}\text{Alice say that she}\\ \text{commit to 0, and}\\ \text{bob trust her}\end{array}\right) + \Pr\left(\begin{array}{l}\text{Alice says} \sim 1.\\ \text{and} \sim\end{array}\right)\right)$$

$$= \frac{1}{2}\left(|K\phi|0\rangle|^2 + |K\phi|+\rangle|^2\right)$$

$\exists \theta \in [0, 2\pi[$,

$|\phi\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$

$$Pr\left(\begin{matrix}\text{Alice wins}\\ \text{cheating}\end{matrix}\right) = \frac{1}{2}\left(\cos^2\theta + \frac{(\cos\theta + \sin\theta)^2}{2}\right) = f(\theta)$$

we want $\max Pr(\text{Alice win})$

$$f'(\theta) = 0 \iff \cos(2\theta) = \sin(2\theta)$$

$$\rightarrow \theta = \frac{\pi}{8}$$