7 Cwiczenia

15 listopada 2015
23:25

2. Optymalne klonowanie qubitu.

Wiemy że nie da się ale można się do niego w sposób przybliżony (z pewnym szumem). Chcemy, żeby szum był jak najmniejszy.

To ważne z punktu widzenia np. analizy bezpieczeństwa kryptografii kwantowej

Problem sformułowany ogólnie:

$$|\psi\rangle_1 \otimes |0\rangle_2 \otimes |A\rangle_A \xrightarrow{U} |\Phi_\psi\rangle_{12A}$$

$|\psi\rangle_1$ – stan klonowany; $|0\rangle_2$ – „pusta kartka"; $|A\rangle_A$ – „maszyna"

Jak ocenimy jakość klonowania? Spojrzymy na zredukowane macierze gęstości 1 i 2:

$$\rho_1(\psi) = Tr_{2,A}\left(|\Phi_\psi\rangle\langle\Phi_\psi|\right) \qquad \rho_2(\psi) = Tr_{1,A}\left(|\Phi_\psi\rangle\langle\Phi_\psi|\right)$$

Co będzie miarą wierności klonowania:

$F_1 = \langle\psi|\rho_1(\psi)|\psi\rangle$ – wierność klonu 1

$F_2 = \langle\psi|\rho_2(\psi)|\psi\rangle$ – wierność klonu 2

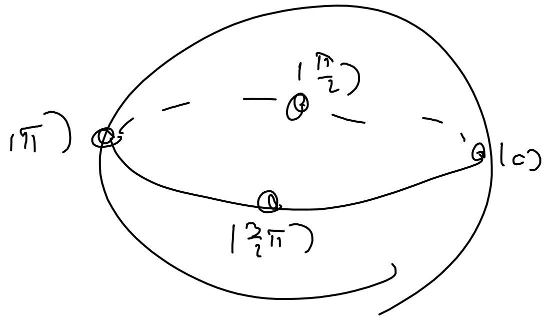
jeśli $\rho_i(\psi) = |\psi\rangle\langle\psi|$, $F_i = 1$ – idealne klonowanie

Chcemy, żeby oba klony były tej samej jakości

$$F_1 = F_2 =: F$$

Ponadto, trzeba określić jakich stanów $|\psi\rangle$ spodziewamy się na wejściu. F nie powinno zależeć od $|\psi\rangle$. Każdy z możliwych stanów klonowany z równą wiernością i szukamy U, maksymalizującego F

Jeśli myślimy o atomach na BB84, to interesują nas stany np. na równiku



Sfery Blocha

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\varphi}|1\rangle\right)$$

Rozważamy: (Optimal phase covariant cloning)

a) $|0\rangle_1|0\rangle_2 \to |0\rangle_1|0\rangle_2$

$|1\rangle_1|0\rangle_2 \to \frac{1}{\sqrt{2}}\left(|0\rangle|1\rangle + |1\rangle|0\rangle\right)$

$$|\varphi\rangle|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + e^{i\varphi}|1\rangle|0\rangle\right) \longrightarrow$$

$$\longrightarrow \frac{1}{\sqrt{2}}|0,0\rangle + \frac{1}{2}e^{i\varphi}\left(|0 1\rangle + |1 0\rangle\right) = \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{2}e^{i\varphi}|1\rangle\right)|0\rangle + \frac{1}{2}e^{i\varphi}|0\rangle|1\rangle$$

$$\rho_1 = \begin{bmatrix} \frac{3}{4} & \frac{1}{2\sqrt{2}}e^{-i\varphi} \\ \frac{1}{2\sqrt{2}}e^{i\varphi} & \frac{1}{4} \end{bmatrix} = \frac{1}{\sqrt{2}}|\varphi\rangle\langle\varphi| + \left(\frac{3}{4} - \frac{1}{2\sqrt{2}}\right)|0\rangle\langle 0| + \left(\frac{1}{4} - \frac{1}{2\sqrt{2}}\right)|1\rangle\langle 1|$$

$$F = \frac{1}{\sqrt{2}} + \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right) = \frac{1}{2} + \frac{1}{2\sqrt{2}} = \frac{\sqrt{2}+1}{2\sqrt{2}} = \frac{2+\sqrt{2}}{4} \simeq 0,85$$

$\rho_2 = \rho_1$

Trochę nie tędy bo stany nie są na równiku.

b) Spróbujmy zrobić wszystko na równiku

$|0\rangle_1|0\rangle_2|0\rangle_A \to \frac{1}{\sqrt{2}}|0 0 0\rangle + \frac{1}{2}\left(|01\rangle + |10\rangle\right)|1\rangle$

$|1\rangle|0\rangle|0\rangle \to \frac{1}{2}\left(|01\rangle + |10\rangle\right)|0\rangle + \frac{1}{\sqrt{2}}|1 1 1\rangle$

$$|\varphi\rangle|0\rangle|0\rangle = \frac{1}{\sqrt{2}}\left(|000\rangle + e^{i\varphi}|100\rangle\right) \longrightarrow$$

$$\longrightarrow \frac{1}{2}|000\rangle + \frac{1}{2\sqrt{2}}\left(|01\rangle + |10\rangle\right)|1\rangle +$$

$$+e^{i\varphi}\frac{1}{2\sqrt{2}}(|01\rangle+|10\rangle)|0\rangle + e^{i\varphi}\frac{1}{2}|111\rangle =$$

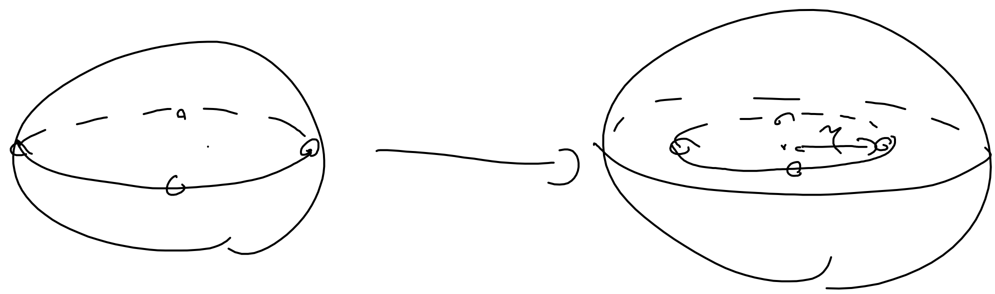
$$= \left(\frac{1}{2}|0\rangle + \frac{1}{2\sqrt{2}}e^{i\varphi}|1\rangle\right)|00\rangle + \frac{1}{2\sqrt{2}}|1\rangle|01\rangle$$

$$+ e^{i\varphi}\frac{1}{2\sqrt{2}}|0\rangle|10\rangle + \left(\frac{1}{2\sqrt{2}}|0\rangle + \frac{1}{2}e^{i\varphi}|1\rangle\right)|11\rangle$$

$$\rho_1 = \frac{1}{4}\begin{bmatrix} 1 & \frac{1}{\sqrt{2}}e^{-i\varphi} \\ \frac{1}{\sqrt{2}}e^{i\varphi} & \frac{1}{2}\end{bmatrix} + \frac{1}{4}\begin{bmatrix} \frac{1}{2} & \\ & \frac{1}{2}\end{bmatrix} + \frac{1}{4}\begin{bmatrix} \frac{1}{2} & \frac{1}{\sqrt{2}}e^{-i\varphi} \\ \frac{1}{\sqrt{2}}e^{i\varphi} & 1\end{bmatrix} =$$

$$= \frac{1}{2}\begin{bmatrix} 1 & \frac{1}{\sqrt{2}}e^{-i\varphi} \\ \frac{1}{\sqrt{2}}e^{i\varphi} & 1\end{bmatrix} = \frac{1}{\sqrt{2}}|\varphi\rangle\langle\varphi| + \left(\frac{1}{2} - \frac{1}{2\sqrt{2}}\right)\mathbb{1}$$

$$F = \frac{1}{\sqrt{2}} + \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\right) = \frac{1}{2} + \frac{1}{2\sqrt{2}} = \frac{\sqrt{2}+1}{2\sqrt{2}} = \frac{2+\sqrt{2}}{4} \quad \text{ok.}$$



stany stają się bardziej zmieszane.

Zauważmy że np. klonowanie $|0\rangle$ już gorsze: $\rho_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|$ $F = \frac{3}{4}$

⌂ Zmodyfikować tak żeby było uniwersalne klonowanie

3. Atak na protokół BB84

E może użyć optymalnego klonowania jako ataku. Tzn. wtedy ma taką samą jakość qubitu co B czyli,

samo pełni qubita co B czyli,
A i B nie mogą wydestylować klucza

Jednak QBER odpowiada tej sytuacji

$$\rho_1 = F|\psi\rangle\langle\psi| + \underbrace{(1-F)}_{\text{błąd}}|\psi+\pi\rangle\langle\psi+\pi|$$

czyli $QBER = 1-F = \frac{2-\sqrt{2}}{4} = 14{,}6\%$

To jest rzeczywiście najmniejszy atak na pojedynczy qubit !

4. Probabilistic Cloning

Dwa stany nieortogonalne

$|\psi_1\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle$

$|\psi_2\rangle = \cos\frac{\theta}{2}|0\rangle - \sin\frac{\theta}{2}|1\rangle$

$$|\psi_1\rangle|00\rangle \rightarrow \sqrt{\eta}\,|\psi_1\rangle|\psi_1\rangle|0\rangle + \sqrt{1-\eta}\,|\Phi_1\rangle\otimes|1\rangle$$

$$|\psi_2\rangle|00\rangle \rightarrow \sqrt{\eta}\,|\psi_2\rangle|\psi_2\rangle|0\rangle + \sqrt{1-\eta}\,|\Phi_2\rangle\otimes|1\rangle$$

$$\cos\theta = \eta\cos^2\theta + (1-\eta)\langle\Phi_1|\Phi_2\rangle$$

Chcemy największe η czyli najlepiej użyć
$\langle\Phi_1|\Phi_2\rangle = 1$ najlepiej wtedy i wtedy mamy

$$\eta(1-\cos^2\theta) = 1-\cos\theta$$

$$\eta = \frac{1}{1+\cos\theta} \quad \text{– prawdop. klonowania}$$

[illegible] nierozróżnialności stanu:

Przypomnijmy sobie warunek prawdopodobieństwa stycznej:

(wzór $\rho = 1 - \cos\theta$ wtedy i $\rho \leq \eta$

(czyli [illegible] [illegible] [illegible] - [illegible] się [illegible])