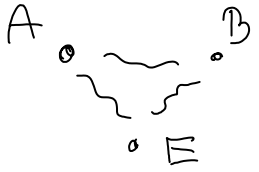
Cwiczenia9

13 kwietnia 2011
10:21

1. Mnożenie splątania



– trzy cząstki w stanie $|\Phi\rangle_{ABE}$

Jeśli $\rho_{AB} = \mathrm{Tr}_E(|\Phi\rangle\langle\Phi|_{ABE}) = |\psi\rangle\langle\psi|_{AB}$ – jest stanem czystym

↑ zredukowany macierz gęstości układu A i B

To $|\Phi\rangle_{ABE} = |\psi\rangle_{AB} \otimes |\varphi\rangle_E$ – nie ma korelacji między AB i E

{ jeśli mamy, że A i B są w stanie czystym np. $|\psi\rangle$ mamy że nie mogą być splątane z niczym innym

Dowód:

Niech $|i\rangle_E$ będzie bazą w przestrzeni E

Dowolny stan $|\Psi_{ABE}\rangle = \sum_i \alpha_i |\psi_i\rangle_{AB} \otimes |i\rangle_E$

$\rho_{ABE} = |\Phi\rangle\langle\Phi|_{ABE} = \sum_{i,i'} \alpha_i \alpha_{i'}^* |\psi_i\rangle\langle\psi_{i'}|_{AB} \otimes |i\rangle\langle i'|$

$\rho_{AB} = \mathrm{Tr}_E \rho_{ABE} = \sum_i |\alpha_i|^2 |\psi_i\rangle\langle\psi_i|_{AB}$

Żeby stan ρ_{AB} był czysty musi być rzutem na wektor (macierz rzutowa rzędu 1)

Tzn, że na wszystkie ortogonalne wektory musi być: $\langle\psi^\perp|\rho_{AB}|\psi^\perp\rangle = 0$. To można tylko jeśli wszystkie $\forall_i |\psi_i\rangle = |\psi\rangle$. Czyli

$|\Phi\rangle_{ABE} = |\psi\rangle_{AB} \otimes \underbrace{\sum_i \alpha_i |i\rangle}_{|\varphi\rangle_E}$

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 wiemy z punktu widzenia np. analizy bezpieczeństwa kryptografii kwantowej

Problem sformułowany ogólnie:

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

↑ stan klonowany, ↑ „pusta kartka", ↑ „maszyna"

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

$$S_1(\psi) = Tr_{2,A}\left(|\Phi_\psi\rangle\langle\Phi_\psi|\right) \qquad S_2(\psi) = Tr_{1,A}\left(|\Phi_\psi\rangle\langle\Phi_\psi|\right)$$

Co będzie miarą wierności klonowania:

$F_1 = \langle\psi| S_1(\psi) |\psi\rangle$ – wierność klonu 1

$F_2 = \langle\psi| S_2(\psi) |\psi\rangle$ – wierność klonu 2

jeśli $S_i(\psi) = |\psi\rangle\langle\psi|$, $F_i = 1$ – 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 $|\psi\rangle$

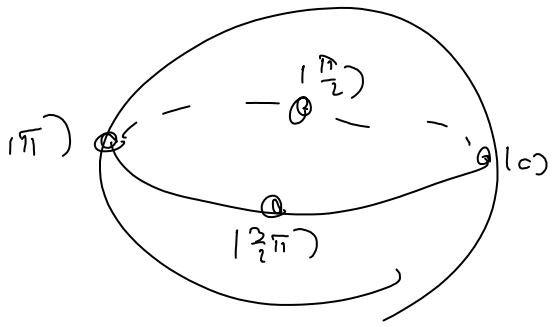
Każdy z możliwych stanów klonowany z różną wiernością

I szukamy U, maksymalizującego F

Jeśli myślimy o atomach np. BB84,

to interesują nas stany np. na różnych

to interesujące stany np. na równiku sfery Blocha



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

Rozważmy: (Optimal phase covariant cloning)

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

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

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

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

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

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

$\rho_2 = \rho_1$

Zwróćmy uwagę, że stany nie są na równiku.

b) Spróbujmy zrobić klonowanie na równiku

$|0\rangle_1|0\rangle_2|0\rangle_A \longrightarrow \frac{1}{\sqrt{2}}|000\rangle + \frac{1}{2}(|01\rangle + |10\rangle)|1\rangle$

$|1\rangle|0\rangle|0\rangle \longrightarrow \frac{1}{2}(|01\rangle + |10\rangle)|0\rangle + \frac{1}{\sqrt{2}}|111\rangle$

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

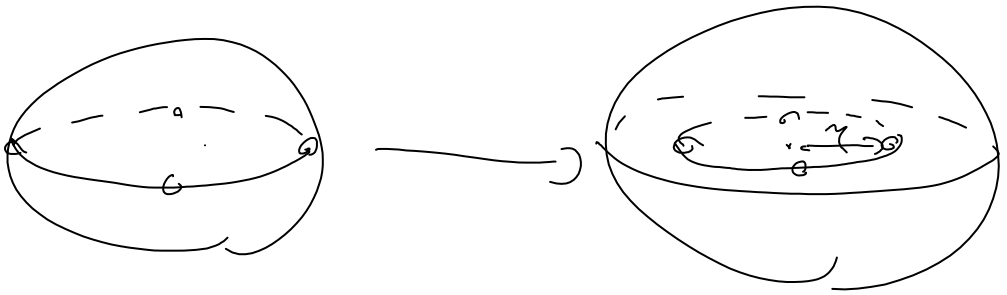
$$\longrightarrow \frac{1}{2}|00\rangle + \frac{1}{2\sqrt{2}}(|01\rangle+|10\rangle)|1\rangle +$$
$$+ e^{i\varphi}\frac{1}{2\sqrt{2}}(|01\rangle+|10\rangle)|0\rangle + e^{i\varphi}\frac{1}{2}|111\rangle =$$

$$= \left(\frac{1}{2}|0\rangle + \frac{1}{2\sqrt{2}}e^{i\varphi}|1\rangle\right)|00\rangle + \frac{1}{2\sqrt{2}}|1\rangle|01\rangle$$
$$+ e^{i\varphi}\frac{1}{2\sqrt{2}}|0\rangle|10\rangle + \left(\frac{1}{2\sqrt{2}}|0\rangle + \frac{1}{2}e^{i\varphi}|1\rangle\right)|11\rangle$$

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

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

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



stany stają się bardziej zmieszane.

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

⌂ Zmodyfikować tak żeby był uniwersalne klonowanie

3. Atak na protokół BB84

E ma inny optymalny klonowanie

Tylko stanu. Tzn. który ma taką samą jakość qubitu co B czyli, A i B nie mogą wydestylować klucza

Jednocześnie QBER odpowiada tej sytuacji

$$\rho_1 = F|\varphi\rangle\langle\varphi| + (1-F)|\varphi+\pi\rangle\langle\varphi+\pi|$$

↑ błąd

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

To jest rzeczywiście najmniejszy atak na pojedynczy qubit !