10 Cwiczenia

22 maja 2014
23:56

1. Ile max. ilości informacji klasycznej 1 qubit

$p_i, |\psi_i\rangle$

$$\chi = S\left(\sum_i p_i |\psi_i\rangle\langle\psi_i|\right) - \sum_i p_i S(|\psi_i\rangle\langle\psi_i|)$$

$$\leq 1.$$

2. Sprawdzić, że wielkość χ odkodujemy po przekształceniu kodowania:

$$\chi = S\left(\underbrace{\sum_i p_i \rho_i}_{\rho}\right) - \sum_i p_i S(\rho_i)$$

kodujemy $\rho_{i_1} \cdots \rho_{i_N} \rho_{i_1} \otimes \cdots \otimes \rho_{i_N}$

$$\chi^{(N)} = S(\rho^{\otimes N}) - \sum_i p_{i_1} \cdots p_{i_N} S(\rho_{i_1} \otimes \cdots \otimes \rho_{i_N}) =$$

$$= N\chi$$

zwracamy uwagę, że tu dopuszczamy pomiary kolektywne

3. Pewien układ kanału kwantowego w którym kodujemy informację używając dwóch nieortogonalnych stanów kwantowych:

$$|\theta\rangle = \cos\theta |0\rangle + \sin\theta |1\rangle \qquad p_1 = \tfrac{1}{2}$$

$$|-\theta\rangle = \cos\theta |0\rangle - \sin\theta |1\rangle \qquad p_2 = \tfrac{1}{2}$$

$\langle \theta | -\theta \rangle = \cos 2\theta$.

a) ile informacji można jeszcze uzyskać mierząc optymalnie

$$C = \frac{1}{2}\left(1 - \sqrt{1 - \cos^2 2\theta}\right) = \frac{1}{2}(1 - \sin 2\theta)$$

$$I(A:B) = 1 - h(C) = 1 - h\left(\frac{1}{2}(1 - \sin 2\theta)\right)$$

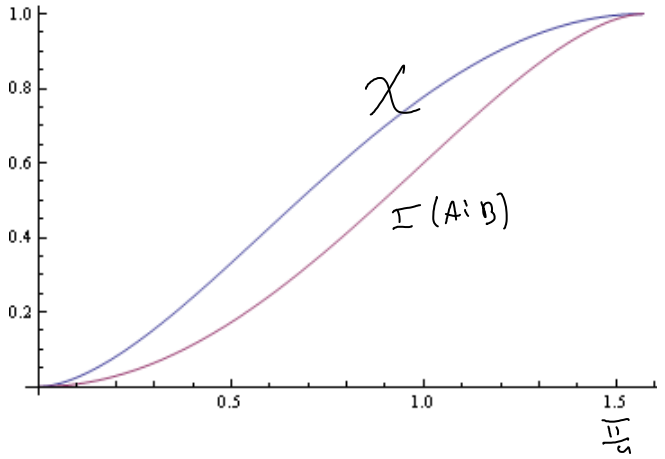
b) ile wynosi wektor Holevo?

$$\chi = S(\rho)$$

$$\rho = \frac{1}{2}\left(|\theta\rangle\langle\theta| + |-\theta\rangle\langle -\theta|\right) =$$

$$= \begin{bmatrix} \cos^2\theta & 0 \\ 0 & \sin^2\theta \end{bmatrix}$$

$$S(\rho) = h(\cos^2\theta)$$



Ale nie można wysyłać dopiero dla wielu kopii kubitów i pomiarów kolektywnych.

4. Optymalny atak na BB84

A wysyła do B 4 stany $|0\rangle, |1\rangle, |+\rangle, |-\rangle$

Rozważmy atak E polegający na wprowadzeniu oddziaływania:

$$|0\rangle_A |0\rangle_E \to |0\rangle_A |\theta\rangle_E$$

$$|1\rangle_A |0\rangle_E \to |1\rangle_A |-\theta\rangle_E$$

E pozyskuje pewną informację o bitach A ale nie pełną ponieważ $|\psi_1\rangle$ i $|\psi_2\rangle$ nieortogonalne

Ale jeśli spojrzymy w bazie $|+\rangle, |-\rangle$

$$|+\rangle_A |0\rangle_E \to \frac{1}{\sqrt{2}}\left(|0\rangle_A |\theta\rangle + |1\rangle |-\theta\rangle \right) =$$

$$= \left(|+\rangle |0\rangle \cos\theta + |-\rangle |1\rangle \sin\theta \right)$$

$$|-\rangle_A |0\rangle_E \to \frac{1}{\sqrt{2}}\left(|0\rangle_A |\theta\rangle - |1\rangle |-\theta\rangle \right) =$$

$$\left(\cos\theta \, |-\rangle |0\rangle + \sin\theta \, |+\rangle |1\rangle \right)$$

Stany E: $\rho_E^+ = \rho_E^-$ (czyli E nie dowiaduje się niczego o stanach tej bazy a co więcej wprowadza zaburzenie:

$$\rho_A^+ = \cos^2\theta \, |+\rangle\langle+| + \sin^2\theta \, |-\rangle\langle-|$$

trzeba uwzględnić typ

[illegible] $|\theta\rangle, |-\theta\rangle$

silnej im bardziej zmieszane są $|\theta\rangle, |1-\theta\rangle$

Uogólnij moją transformację:

$$|+\rangle_A |0\rangle_E |0\rangle_{E'} \to \left(\cos\theta |+\rangle |0\rangle |\theta\rangle + \sin\theta |-\rangle |1\rangle |1-\theta\rangle \right)$$

$$|-\rangle_A |0\rangle_E |0\rangle_{E'} \to \left(\cos\theta |-\rangle |0\rangle |1-\theta\rangle + \sin\theta |+\rangle |1\rangle |\theta\rangle \right)$$

informacja w bicie $|+\rangle, |-\rangle$

Zamiana unitarna ta w bicie $|0\rangle, |1\rangle$ wygląda tak:

$$|0\rangle |0\rangle |0\rangle \to \frac{1}{\sqrt{2}} \left(\cos\theta |+0\theta\rangle + \sin\theta |-1\theta\rangle + \cos\theta |-0\theta\rangle + \sin\theta |+1\theta\rangle \right)$$

$$= \frac{1}{2} \left(\left[\cos\theta |0\rangle (|0\rangle + |1\rangle) |0\rangle + \sin\theta (|0\rangle - |1\rangle) |1\rangle \right] |\theta\rangle \right.$$
$$\left. + \left[\cos\theta |0\rangle (|0\rangle - |1\rangle) |0\rangle + \sin\theta (|0\rangle + |1\rangle) |1\rangle \right] |1-\theta\rangle \right)$$

$$= \frac{1}{2} \left(\left[|0\rangle |\theta\rangle + |1\rangle |1-\theta\rangle \right] \cos\theta |0\rangle \right.$$
$$\left. + \left[|0\rangle |\theta\rangle - |1\rangle |1-\theta\rangle \right] \sin\theta |1\rangle \right) =$$

$$= \cos\theta |0\rangle |\theta\rangle |0\rangle + \sin\theta |1\rangle |1-\theta\rangle |1\rangle$$

analogicznie

$$|1\rangle |0\rangle |0\rangle \to \cos\theta |1\rangle |\theta\rangle |0\rangle + \sin\theta |0\rangle |1-\theta\rangle |1\rangle$$

Jeśli E dwa pierwsze bity w bicie $|+\rangle, |-\rangle$ mają qubit E' jest stan $|\theta\rangle |1-\theta\rangle$

Jeśli w bicie $|0\rangle, |1\rangle$ mają qubit E i pierwsze $|\theta\rangle, |1-\theta\rangle$ to dodatkowy qubit E' to bit informacji bity.

E' ... bo to odwrócone bity.

Jeśli błąd wprowadza to do kanałów A, B

$QBER = c_0^2\theta$

$$I(A:B) = 1 - h(c_0^2\theta)$$

Jeśli E wybiera min-error discriminator między bazą B: to

$$I(A:E) = 1 - h\left(\frac{1}{2}(1-\sin 2\theta)\right)$$

$$I(A:B) > I(A:E) \iff$$

$$c_0^2\theta > \frac{1}{2}(1-\sin 2\theta)$$

$$\sin 2\theta > 1 - 2c_0^2\theta$$

$$\sin 2\theta > \cos 2\theta$$

$$\operatorname{tg} 2\theta > 1 \qquad 2\theta > \frac{\pi}{4} \qquad \theta > \frac{\pi}{8}$$

$$QBER < c_0^2\frac{\pi}{8} = \frac{1-\frac{\sqrt{2}}{2}}{2} = \frac{2-\sqrt{2}}{4} \approx 14{,}6\%$$

Bezpieczne z punktu widzenia ataków indywidualnych.

Można też wymyślić taki silniejszy ograniczający założenie że E może wybierać pomiędzy dowolnymi

$$I(A:E) < \chi = h(c_0^2\theta)$$

$I(A:B) > I(A:E)$ jeśli

$$1 - 2h(\cos^2\theta) > 0$$

$$h(QBER) < \frac{1}{2}$$

$$QBER < 11\%$$

Okazuje się, że ten warunek obowiązuje również dla ogólniejszych ataków gdy E nie może odczytywać koherentnego z wielu qubitów...