6 Splatanie

3 listopada 2015
15:07

Rozkład Schmidta, PPT, Monogamia splątania
miary splątania, No-cloning (impossibility of superluminal communication)
Ent. based QKD.

Splątanie stanów czystych — rozkład Schmidta

$$|\psi\rangle = \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} c_{ij} \, |i\rangle_A \otimes |j\rangle_B$$

Potraktujmy c_{ij} jako macierz $C^i_j = c_{ij}$
Dla każdej macierzy — rozkład singularny

$$C = U D V^\dagger \qquad D = \begin{array}{c} \\ d_A \end{array}\underbrace{\begin{bmatrix} \lambda_1 & & & 0 \\ & \ddots & & 0 \\ & & \lambda_d & 0 \end{bmatrix}}_{d_B} \qquad \lambda_i \geq 0$$

U, V — macierze unitarne
$d_A \times d_A$, $d_B \times d_B$

$$|\psi\rangle = \sum_i \sum_j U_{ik} D_{kk} V^\dagger_{kj} \, |i\rangle \otimes |j\rangle =$$

$$= \sum_k \lambda_k \underbrace{\Big(\sum_i U_{ik} |i\rangle\Big)}_{|k_A\rangle} \otimes \underbrace{\Big(\sum_j V_{kj} |j\rangle\Big)}_{|k_B\rangle}$$

Istnieją bazy w A i B, że i

$$|\psi\rangle = \sum_{k=1}^{\min(d_A, d_B)} \lambda_k \, |k_A\rangle \otimes |k_B\rangle$$

Rząd Schmidta — liczba niezerowych λ_k

Stany produktowe — rząd Schmidta 1
stany max splątane: $\lambda_1 = \ldots = \lambda_d = \frac{1}{d}$

$$\rho_A = \sum_k \lambda_k |k_A\rangle\langle k_A| \quad \Big| \quad \rho_B = \sum_k \lambda_k |k_B\rangle\langle k_B|$$

Mając SVD C^i_j mamy wszystko, stwierdzenie splątania stanu czystego proste.

Splątanie stanów mieszanych

Splątanie stanów mieszanych

Dla czystych splątanie ⟺ korelacje

Przykład 1 telefon

A ~~~~~~~~ B

z $p=\frac{1}{2}$ przygotowuje $|0\rangle_A|0\rangle_B$ z $p=\frac{1}{2}$ $|1\rangle_A|1\rangle_B$

$$\rho_{AB} = \frac{1}{2}\left(|0\rangle_A\langle 0| \otimes |0\rangle_B\langle 0| + |1\rangle_A\langle 1| \otimes |1\rangle_B\langle 1|\right)$$

$\rho_{AB} \neq \rho_A \otimes \rho_B$ co oznacza korelacje, ale nie pozwalamy było ich kw. odpowiadanie, korelacje czysto klasyczne (nie łamie nierówności Bella)

Definicja

stan separowalny: jeśli da się zapisać jako

$$\rho_{AB} = \sum_i p_i \rho_A^i \otimes \rho_B^i \qquad p_i \geq 0$$

stan splątany jest nie da się zapisać.

Kryterium PPT

Przykład

Weźmy stan dwóch qubitów

$$\rho = p|\psi^-\rangle\langle\psi^-| + \underbrace{(1-p)\cdot\frac{\mathbb{1}}{4}}_{\text{szum}}$$

(np. jedna cząstka puszczana przez zaszumiony kanał
np. Pauli chanel ⇗)

Jasne jest że dla $p=1$ stan jest splątany a dla $p=0$ jest separowalny.
Ale gdzie jest granica splątania?

Definicja Częściowa transpozycja

Definicja Częściowa transpozycja

$$\rho = \sum \rho^{i_A i_B}_{j_A j_B} |i_A\rangle\langle j_A| \otimes |i_B\rangle\langle j_B|$$

ogólny stan dwóch podukładów.

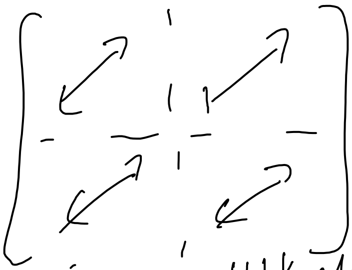
$$\rho^{T_B} = \sum \rho^{i_A j_B}_{j_A i_B} |i_1\rangle\langle j_1| \otimes |i_2\rangle\langle j_2|$$

częściowa transpozycja względem drugiego podukładu

Przykład

Dwa qubity (w bazie $|0,0\rangle, |0,1\rangle, |1,0\rangle, |1,1\rangle$)

$$\rho = \begin{bmatrix} \rho^{00}_{00} & \rho^{00}_{01} & \rho^{00}_{10} & \rho^{00}_{11} \\ \rho^{01}_{00} & \rho^{01}_{01} & \rho^{01}_{10} & \rho^{01}_{11} \\ \rho^{10}_{00} & \rho^{10}_{01} & \rho^{10}_{10} & \rho^{10}_{11} \\ \rho^{11}_{00} & \rho^{11}_{01} & \rho^{11}_{10} & \rho^{11}_{11} \end{bmatrix}$$

$\rho^{T_2} =$ 

Transpozycja w podblokach

Twierdzenie Jeśli stan ρ jest separowalny to $\rho^{T_B} \geq 0$ } równoważnie $\rho^{T_A} \geq 0$

Dowód:

Zauważmy że dla dowolnego operatora $\sigma \geq 0$ mamy $\sigma^T \geq 0$. Dlaczego:

$$\sigma = \sum_i \lambda_i |\varphi_i\rangle\langle\varphi_i| , \quad \lambda_i \geq 0$$

wekt. własne

$$|\varphi\rangle = \sum_k c_k |k\rangle \qquad |\varphi\rangle\langle\varphi| = \sum_{k,k'} c_k c_{k'}^* |k\rangle\langle k'|$$

$$|\varphi\rangle\langle\varphi|^T = \sum_{k,k'} c_{k'} c_k^* |k\rangle\langle k'| = |\varphi^*\rangle\langle\varphi^*|$$

gdzie $\varphi^* = \sum c_k^* |k\rangle$. Czyli wartości własne się nie zmieniają a jedynie mogą zmienić się wekt. własne

{ uwaga: transpozycja jest operacją, która jest zależna od bazy w której ją robimy.

Jeśli ρ separowalny:

$$\rho_{AB} = \sum_i p_i \, \rho_i^A \otimes \rho_i^B \qquad \rho_{AB}^{T_B} = \sum_i p_i \rho_i^A \otimes (\rho_i^B)^T$$

$(\rho_i^B)^T \geq 0$ czyli $\rho_{AB}^{T_B} \geq 0$ ∎

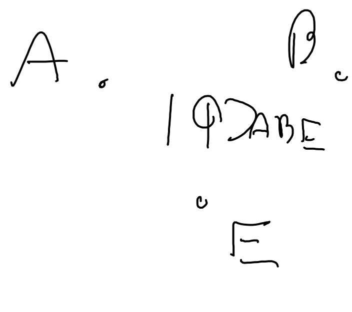
Wniosek:

Jeśli policzymy że $\rho_{AB}^{T_B} \ngeq 0$ wiemy na pewno że stan jest splątany!

(warunek dostateczny splątania, warunek konieczny separowalności

Uwaga: Dla niskowymiarowych przypadków 2×2, 2×3, jest to warunek konieczny i dostateczny. (Horodecki, korzystając z Woronowicza, charakteryzacja odwzorowań dodatnich – powiemy trochę później)

Monogamia splątania:



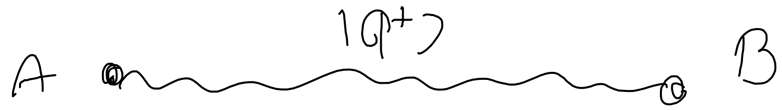
Jeśli $\rho_{AB} = Tr_E(|\varphi\rangle_{ABE}\langle\varphi|) = |\psi\rangle_{AB}\langle\psi_{AB}|$ czysty.

$$\Rightarrow |\varphi\rangle_{ABE} = |\psi\rangle_{AB} \otimes |\varphi\rangle_E$$

W szczególności jeśli A i B mają splątane

$|\psi\rangle = \frac{1}{\sqrt{d}}\sum_i |i\rangle|i\rangle$ to nie może być splątany z E

Entanglement based QKD



A wykonując pomiar w bazie $|0\rangle, |1\rangle$ lub $|+\rangle|-\rangle$ przygotowuje u B stan identyczny. Mamy ef. protokół BB84.
Aby mieć pewność że E nie ma wiedzy możemy sprawdzić łamanie nierówności Bella. (wykonujemy jeszcze pomiary w innych bazach)
Bardziej interesujące twierdzenie pokazuje monogamię CHSH

$$|\langle C\rangle_{AB}| + |\langle C\rangle_{AC}| \le 4$$

czyli gdy łamiemy w AB to mamy silniejsze korelacje między AB niż np. AC.

No-cloning i superluminal

. Klonowanie stanów kwantowych
Jeśli myślimy o stanach kwantowych jako

o [illegible] informacji. Pojawia się naturalne pytanie: Czy można informację zapisaną w stanach kwantowych kopiować?

Kluczowa kwestia bo jeśli się da ....

a) BB84 nie jest bezpieczne !

b) Możliwa jest rozróżnialność nieortogonalnych stanów kwantowych

$|\psi\rangle, |\varphi\rangle$ st. nieortogonalne. $0 < \langle\psi|\varphi\rangle < 1$

wiemy że $p_e = \frac{1}{2}\left(1 - \sqrt{1 - |\langle\psi|\varphi\rangle|^2}\right)$

Ale jeśli można je przepisać przez maszynę:

$$|\psi\rangle \longrightarrow |\psi\rangle^{\otimes N}$$

$$|\varphi\rangle \longrightarrow |\varphi\rangle^{\otimes N}$$

to $p_e^{(N)} = \frac{1}{2}\left(1 - \sqrt{1 - \underbrace{|{}^{\otimes N}\langle\psi|\varphi\rangle^{\otimes N}|^2}_{|\langle\psi|\varphi\rangle|^{2N}}}\right) \xrightarrow{N\to\infty} 0$!

c) Pozwoliłoby to w szczególności na komunikację ponadświetlną:

A $\quad |\psi^-\rangle \quad$ B

A decyduje czy mierzy w bazie: $\quad$ B ma

$\oplus$ (bit 0) $\quad |\leftrightarrow\rangle$ lub $|\updownarrow\rangle$

czy

$\otimes$ (bit 1) $\quad |\nearrow\rangle$ lub $|\searrow\rangle$

Ale B może teraz sklonować swój stan i dokładnie stwierdzić co dostał. Więc będzie wiedział dokładnie w jakiej bazie mierzył A !

Tw. Klonowanie nieortogonalnych stanów kwantowych jest niemożliwe

Dowód (Nie wprost)

Niech $|\psi\rangle, |\varphi\rangle$, $0 < |\langle\psi|\varphi\rangle| < 1$

Załóżmy że istnieje operacja zgodna z mech. kwantową (np. unitarna) dokonująca klonowania obu stanów. Matematycznie:

"czysta kartka" ↓ maszyna klonująca ↓

$$|\psi\rangle \otimes |0\rangle \otimes |A\rangle \xrightarrow{\mathcal{U}} |\psi\rangle \otimes |\psi\rangle \otimes |A_\psi\rangle$$

$$|\varphi\rangle \otimes |0\rangle \otimes |A\rangle \longrightarrow |\varphi\rangle \otimes |\varphi\rangle \otimes |A_\varphi\rangle$$

Z unitarności:

$$\langle\psi|\varphi\rangle \underbrace{\langle 0|0\rangle \langle A|A\rangle}_{1} = \langle\psi|\varphi\rangle \langle\psi|\varphi\rangle \langle A_\psi|A_\varphi\rangle$$

$$\underset{\neq 0}{\langle\psi|\varphi\rangle} \cdot \left(1 - \underbrace{\langle\psi|\varphi\rangle \langle A_\psi|A_\varphi\rangle}_{<1}\right) = 0$$

sprzeczność

Ufff.... Klonować się nie da.

Pamiętamy że w teleportacji rzeczywiście oryginał był niszczony. Czyli wszystko OK.