Wyklad4

1 maja 2011
17:09

Klonowanie stanów kwantowych

1. Klonowanie

Czy możliwe jest powielenie nieznanego stanu kwantowego?

$$|\psi\rangle \otimes |o\rangle \otimes |A\rangle \xrightarrow{?} |\psi\rangle|\psi\rangle|A_\psi\rangle$$

gdyby było możliwe...

- moglibyśmy rozróżnić nieortogonalne st. kwantowe

$$p_e^{(n)} = \frac{1}{2}\left(1-\sqrt{1-\langle\psi|\varphi\rangle^{n}}\right) \xrightarrow{n\to\infty} 0 \qquad \langle\psi|\varphi\rangle < 1$$

- komunikacja ponadświetlna.

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 (op. unitarna) dokonująca klonowania obu stanów. Matematycznie:

„czysta kartka" ↓ maszyna klonująca ↓

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

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

z unitarności:

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

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

sprzeczność

Ufff.... Klonować się nie da.

Pamiętamy że w teleportacji rzeczywiście oryginał

Pamiętamy że w teleportacji rzeczywiście argument był mieszany. Czyli wszystko OK.

Nie da się klonować idealnie, a jak da się najlepiej?

Wiemy że nie da się ale może się da w sposób przybliżony (z pełnym sensem). Chcemy, żeby sens był jak najmniejszy.

To ważne z punktu widzenia np. analizy bezpieczeństwa kryptografii kwantowej

Problem sformułowany ogólnie:

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

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

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

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

Co będzie miarą wierności klonowania:

$$F_1 = \langle\psi|\rho_1(\psi)|\psi\rangle \quad \text{– wierność klonu 1}$$

$$F_2 = \langle\psi|\rho_2(\psi)|\psi\rangle \quad \text{– wierność klonu 2}$$

$\Big\}$ 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, a F nie powinno zależeć od $|\psi\rangle$. Każdy z możliwych stanów klonowany z równą wiernością

I szukamy $\mathcal{U}$, maksymalizującego F

2. Uniwersalne klonowanie qubitu

Spróbujmy:

$$|0\rangle|0\rangle|0\rangle \longrightarrow |0\rangle|0\rangle|0\rangle$$

$$|1\rangle|0\rangle|0\rangle \longrightarrow |1\rangle|1\rangle|1\rangle$$

i zostaniemy się niczego źle ?

Rozważmy transformację:

$$|0\rangle_1|0\rangle_2|0\rangle_A \xrightarrow{U} \sqrt{\tfrac{2}{3}}|000\rangle + \frac{1}{\sqrt{6}}\left(|01\rangle+|10\rangle\right)|1\rangle$$

$$|1\rangle|0\rangle|0\rangle \longrightarrow \frac{1}{\sqrt{6}}\left(|01\rangle+|10\rangle\right)|0\rangle+\sqrt{\tfrac{2}{3}}|111\rangle$$

$$|\psi\rangle|0\rangle|0\rangle = \left(a|0\rangle+b|1\rangle\right)|00\rangle \xrightarrow{U}$$

$$\longrightarrow \frac{1}{\sqrt{6}}\Big(2a|000\rangle+a|011\rangle+a|101\rangle + b|010\rangle+b|100\rangle+2b|111\rangle\Big)$$

$$\rho_1 = \frac{1}{6}\cdot\Big(|a|^2|1\rangle\langle 1| + |b|^2|0\rangle\langle 0| + \left(2a|0\rangle+b|1\rangle\right)\left(2a^*\langle 0|+b^*\langle 1|\right) + \left(a|0\rangle+2b|1\rangle\right)\left(\text{---}\,\text{''}\,\text{---}\right)\Big)$$

$$= \frac{1}{6}\begin{bmatrix} 4|a|^2+1 & 3ab^* \\ 3a^*b & 4|b|^2+1 \end{bmatrix} = \frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{6}\mathbb{1}$$

$F = \frac{5}{6}$. Nie zależy od ψ !

Czy to najlepiej jak się da ?

3. Dowód optymalności klonowania $(1\to 2)$

$$\rho_{12}(\psi) = \mathrm{Tr}_A\left(|\varphi_\psi\rangle\langle\varphi_\psi|\right) =$$

$$= \mathrm{Tr}_A\left(U\,|\psi\rangle\langle\psi|\otimes|0\rangle\langle 0|\otimes|A\rangle\langle A|\,U^\dagger\right)$$

Bez utraty ogólności możemy zawsze wykonać symetryzację ρ_{12}

$$\rho_{12} \longrightarrow \frac{1}{2}\left(\rho_{12}+\rho_{21}\right) \quad \Big\}\ \text{to nie zmienia}$$

$$\rho_{12} \longrightarrow \tfrac{1}{2}(\rho_{12} + \rho_{21}) \Big\}$$ to nie zmienia F_1, F_2

Natomiast ρ_{12} jest perm. niezmiennicze.

Oznacza to, że $\rho_{12} = p_- \cdot \rho_- + p_+ \rho_+$

ρ_- ↑ stan na przestrzeni singletowej; ρ_+ ↑ stan na przestrzeni trypletowej

$\rho_- = |\psi_-\rangle\langle\psi_-|$ daje $\rho_1 = \rho_2 = \frac{1}{2}\mathbb{1}$ czyli bezużyteczne

Można zawsze dokonać operacji:

- zmierz P_-, P_+
- jeśli P_- przygotuj stan $|\psi_+\rangle\langle\psi_+|$

to do tej samej redukcji może gdzieś a można myśleć, że $\rho_{12} = \rho_+$ żyje tylko ~~nad~~ przestrzeni trypletowej (symetrycznej)

Fakt:

ρ_+ stan z podprzestrzeni symetrycznej to

$$\rho_+ = \int d\psi \, \alpha(\psi) \, |\psi\rangle\langle\psi|^{\otimes 2} \qquad \alpha(\psi) \in \mathbb{R}$$

Dowód

$\Leftarrow$ oczywiste $\quad P_+ \rho_+ P_+ = \rho_+$

$\Rightarrow$ $\rho_+ = \sum c_{ij} |\psi_i\rangle\langle\psi_j|$ $\quad |\psi_1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, $|\psi_2\rangle = |00\rangle$, $|\psi_3\rangle = |11\rangle$ $\Big\}$ baza przestrzeni trypletowej

$$\int d\psi \, \alpha(\psi) \left(\langle\psi_i| |\psi\rangle^{\otimes 2}\right) \cdot \left(\langle\psi|^{\otimes 2} |\psi_j\rangle\right) = c_{ij}$$

$$\langle\psi_1| |\psi\rangle^{\otimes 2} = \frac{1}{\sqrt{2}}(\langle 01| + \langle 10|)\left(\cos\tfrac{\theta}{2}|0\rangle + \sin\tfrac{\theta}{2} e^{i\varphi}|1\rangle\right)\left(\cos\tfrac{\theta}{2}|0\rangle + \sin\tfrac{\theta}{2} e^{i\varphi}|1\rangle\right)$$

$$= \frac{1}{\sqrt{2}} \cdot \left(2 \cdot \cos\tfrac{\theta}{2} \sin\tfrac{\theta}{2} e^{i\varphi}\right) = \frac{\sin\theta \, e^{i\varphi}}{\sqrt{2}} = f_1(\psi)$$

$$\langle\psi_2| |\psi\rangle^{\otimes 2} = \cos^2\tfrac{\theta}{2} = f_2(\psi)$$

$$\langle\psi_3| |\psi\rangle^{\otimes 2} = \sin^2\tfrac{\theta}{2} \, e^{2i\varphi} = f_3(\psi)$$

$\langle\psi_3|\psi\rangle^{\otimes 2} = \quad \sin^2\frac{\theta}{2}\, e^{2i\varphi} \quad = \ell_3(\psi)$

$\ell_{ij}(\psi) = \ell_i(\psi)\,\ell_j^*(\psi)$

$\int d\psi\, \alpha(\psi)\, \ell_{ij}(\psi) = c_{ij} \qquad i,j = 1\ldots 3$

gdzie $\ell_{ij}(\psi)$ – lin. niezależne funkcje ψ (w $\mathbb{R}$)

tzn. mogę wybrać ψ_{kl} t.że wektory $(k,l = 1\ldots 3)$

$\forall_{i,j}$ $\ell_{ij}(\psi_{kl})$ są lin niezależne $\Rightarrow$

czyli problem: $\sum_{kl} \alpha(\psi_{kl})\, \ell_{ij}(\psi_{kl}) = c_{ij}$

Mogę odwrócić i wyliczyć $\alpha(\psi_{kl}) = \ldots$

<u>Uwaga</u> Estymacja stanu można traktować jako operacja w której można uzyskać dowolną liczbę klonów:

$|\psi\rangle^{\otimes N} \xrightarrow{\{\Pi_x\}} x \longrightarrow |\psi_x\rangle \longrightarrow |\psi_x\rangle^{\otimes M}$

Możemy więc myśleć że:

$$\rho_M = \int dx\, \langle\psi|^{\otimes N}\, \Pi_x\, |\psi\rangle^{\otimes N} \left(|\psi_x\rangle\langle\psi_x|\right)^{\otimes M}$$

Patrząc na jeden egzemplarz

$$\rho_1 = \int dx\, \langle\psi|^{\otimes N}\, \Pi_x\, |\psi\rangle^{\otimes N}\, |\psi_x\rangle\langle\psi_x|$$

Pamiętamy że $F = \frac{N+1}{N+2}$, co oznacza:

$$\rho_1 = \frac{N+1}{N+2}\, |\psi\rangle\langle\psi| + \left(\frac{1}{N+2}\right)\left(\mathbb{1} - |\psi\rangle\langle\psi|\right) \quad \Big\}\ \text{dla każdego } |\psi\rangle\ !$$

$$\rho_1 = \int dx\, \mathrm{Tr}\left(\Pi_x\, |\psi\rangle\langle\psi|^{\otimes N}\right) |\psi_x\rangle\langle\psi_x|$$

– zauważmy że $\rho_1 = \mathcal{E}_{est}\left(|\psi\rangle\langle\psi|^{\otimes N}\right)$ jest op liniowa

$$\Big\{\ \mathcal{E}_{est}\left(\sum_i \alpha_i |\psi_i\rangle\langle\psi_i|^{\otimes N}\right) = \sum_i \alpha_i\, \mathcal{E}_{est}\left(|\psi_i\rangle\langle\psi_i|^{\otimes N}\right)$$

Zauważmy uwaga że moglibyśmy tego użyć do klonowania

$F^{klon}_{N\to M} \geq F^{est}_N = \frac{N+1}{N+2}$ czyli $F_{klon\,1\to 2} \geq \frac{2}{3}$

Czy można tą obserwację wykorzystać <u>lepiej</u>?

Czy można tą obserwację wykorzystać lepiej?

Idea: możemy ograniczyć wierność klonowania $1 \to 2$ korzystając z faktu, że mamy opt. estymację na 1 i 2 kopiach qubitu. Nie może być tak, że klonowanie $1 \to 2$ + estymacja na 2 da coś lepszego niż optymalna estymacja na 1 ($F = \frac{2}{3}$)

$$\underbrace{F_{\text{klon } 1\to 2 \text{ + estymacja na } 2} \leq F_{\text{estymacja na } 1} = \frac{2}{3}}$$

$$\varrho_{12}(\psi) = \int d\psi' \, \alpha_\psi(\psi') \, |\psi'\rangle\langle\psi'|^{\otimes 2}$$

Zauważmy, że $\varrho_1(\psi) = \varrho_2(\psi) = \int d\psi' \alpha_\psi(\psi') |\psi'\rangle\langle\psi'|$

$$F^{\text{klon}}_{1\to 2} = \int d\psi' \, \alpha_\psi(\psi') \left(|\langle\psi|\psi'\rangle|\right)^2$$

Korzystając z $\varrho_{12}(\psi)$ wykonujemy opt. estymację na dwóch kopiach. Subtelność: $\alpha_\psi(\psi')$ mogą być ujemne, czyli nie możemy myśleć, że to są stany $|\psi'\rangle\langle\psi'|$ przygotowane z różnymi prawdop.-ństwami. Ale to nic, bo $\mathcal{E}_{est}$ jest operacją liniową:

$$\mathcal{E}_{est}\left(\varrho_{12}(\psi)\right) = \int d\psi' \, \alpha_\psi(\psi') \Big(\overset{= F_2^{est}}{\tfrac{3}{4}} |\psi'\rangle\langle\psi'| + \tfrac{1}{4}(\mathbb{1} - |\psi'\rangle\langle\psi'|) \Big)$$

$$= \frac{1}{4}\mathbb{1} + \frac{1}{2}\int d\psi' \, \alpha_\psi(\psi') \, |\psi'\rangle\langle\psi'|$$

Wiemy, że $\langle\psi| \mathcal{E}_{est}(\varrho_{12}(\psi)) |\psi\rangle \leq \frac{2}{3} = F_1^{est}$:

$$\frac{1}{4} + \frac{1}{2}\int d\psi' \alpha_\psi(\psi') \, |\langle\psi|\psi'\rangle|^2 \leq \frac{2}{3}$$

$$F_{\text{klon } 1\to 2} \leq \frac{4}{3} - \frac{1}{2} = \frac{5}{6}$$

Przykład:

Klonowanie 1 modowych st. światła. (lub równoważnie stanów cząstki 1D)

Wyobraźmy sobie że dostajemy pewien stan światła (np. koherentny) i chcemy go rozesłać do dwóch odbiorców w niezmienionej postaci. Przy czym nie wiemy dokładnie co to za stan: $|\alpha\rangle$

$\alpha = ?$.

Czy da się to zrobić?

Nie bo stany koherentne nie są ortogonalne:

$$|\langle\alpha|\beta\rangle|^2 = \left|e^{-\frac{|\alpha|^2}{2}}\sum_n \frac{\alpha^{*n}}{\sqrt{n!}}\langle n|\, e^{-\frac{|\beta|^2}{2}}\sum_m \frac{\beta^m}{\sqrt{m!}}|m\rangle\right|^2 =$$

$$= e^{-|\alpha|^2-|\beta|^2}\left|\sum_n \frac{(\alpha^*\beta)^n}{n!}\right|^2 = e^{-|\alpha|^2-|\beta|^2+\alpha^*\beta+\alpha\beta^*} = e^{-|\alpha-\beta|^2}$$

Ale z drugiej strony istnieją wzmacniacze optyczne oparte o zjawisko emisji wymuszonej

Co nam zabrania zrobić - $|\alpha\rangle$

$$|\alpha\rangle - \boxed{\text{wzmacniacz}} - |2\alpha\rangle - /\!\!/ - |\alpha\rangle \quad ?$$

Coś musi zabraniać

Co robi wzmacniacz? Chcemy żeby:

$$a^\dagger \longrightarrow \underset{\text{wzmocnienie}}{\sqrt{\gamma}}\, a^\dagger = a^{\dagger\prime}$$

dzięki temu $|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}}\sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle \longrightarrow e^{-\frac{|\alpha|^2}{2}}\sum_n \frac{\alpha^n\sqrt{\gamma}^n}{\sqrt{n!}}|n\rangle$

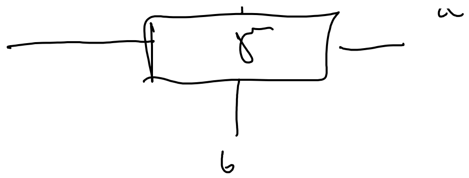
$\propto |\gamma\alpha\rangle$

problem z normalizacją

Tak nie może być bo $[a', a^{\dagger\prime}] \neq 1$!

Musimy coś dodać

$a \qquad b'$



$$\begin{cases} a'^{+} = \sqrt{\gamma}\, a^{+} + \sqrt{\gamma-1}\, b \\ b'^{+} = \sqrt{\gamma}\, b^{+} + \sqrt{\gamma-1}\, a \end{cases}$$

różnica z beam splitterem $\gamma > 1$ i b zamiast b^{+}

$$a' = \sqrt{\gamma}\, a + \sqrt{\gamma-1}\, b^{+}$$

$[a', a'^{+}] = \gamma - (\gamma - 1) = 1$ ok

$[a'^{+}, b'^{+}] = 0$ ok

$[a', b'^{+}] = 0$ ok

tu się mieszają op. kreacji i anihilacji trzeba uważać, np. jeśli na obu wejściach jest próżnia to na wyjściu już nie koniecznie?

{nie mamy wartości bezkarnie $U |0\rangle\langle 0| U^{+} = |0\rangle\langle 0|$

Będziemy używać obrazu Heisenberga:

$f(a, a^{+}, b, b^{+}, \dots)$ - pewna obserwabla mierzona na wyjściu

ρ_{in} - stan wejściowy

$\rho_{out} = U \rho_{in} U^{+}$

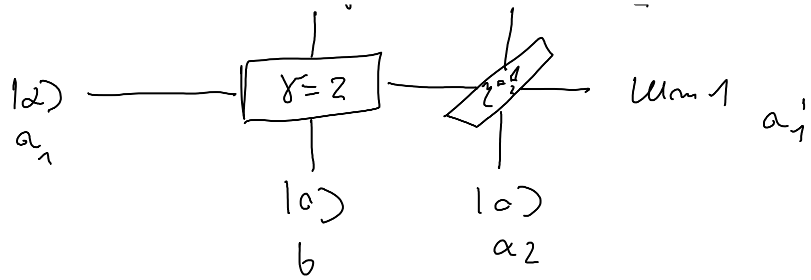
$$\langle f \rangle = Tr(\rho_{out}\, f(a, a^{+}, \dots)) = Tr(\rho_{in} U^{+} f(a, a^{+}, \dots) U) =$$

$$= Tr(\rho_{in}\, f(U^{+} a U, U^{+} a^{+} U, \dots))$$

Czyli musimy znaleźć transformację operatorów kreacji i anihilacji

Użyjmy tego rozumowania dla klonowania

...ł klon 2 a_2



Chcemy zbadać jakie są średnie i wariancje kwadratur (położeń, pędów) modów w stosunku do tego jakie były na wejściowym stanie $|\alpha\rangle$

$$\begin{cases} |\psi\rangle_{out} = \mathcal{U}\, |\alpha\rangle |0\rangle |0\rangle \\ \langle q_1\rangle_{out} = \langle\alpha|\langle 0|\langle 0|\, \mathcal{U}^\dagger \hat{q}_1\, \mathcal{U}\, |\alpha\rangle|0\rangle|0\rangle \\ \langle q_1^2\rangle_{out} \;\; \ldots\ldots \end{cases} \qquad \hat{q}_1 = \frac{a + a^\dagger}{\sqrt{2}} \;\; \vdots$$

Wyraźmy a_1', a_2' przez a_1, a_2, b :

$$\boxed{\gamma} \qquad\qquad\qquad \gamma = \tfrac{1}{2}$$

$$a_1^\dagger \longrightarrow \sqrt{2}\, a_1^\dagger + \quad b \longrightarrow a_1^\dagger + a_2^\dagger + b = a_1'^\dagger$$

$$a_2^\dagger \longrightarrow \frac{1}{\sqrt{2}}\left(a_2^\dagger - a_1^\dagger\right) \qquad = a_2'^\dagger$$

$$b^\dagger \longrightarrow \sqrt{2}\, b^\dagger + a_1 \longrightarrow \sqrt{2}\, b^\dagger + \frac{1}{\sqrt{2}}(a_1 + a_2) = b'^\dagger$$

Powinniśmy teraz odwrócić tę transformację. Ściśle mówiąc biorąc też a dopiero po dopisaniu transformacji a_1, a_2, b — macierz 6×6. Ale zauważmy że tylko 3 z tych równań się sprzęga

$$\begin{cases} a_1^\dagger \longrightarrow a_1^\dagger + a_2^\dagger + b = a_1'^\dagger \\ a_2^\dagger \longrightarrow \frac{1}{\sqrt{2}}\left(a_2^\dagger - a_1^\dagger\right) = a_2'^\dagger \\ b \longrightarrow \sqrt{2}\, b + \frac{1}{\sqrt{2}}\left(a_1^\dagger + a_2^\dagger\right) = b' \end{cases}$$

Szukamy transformacji odwrotnej :

$$(1) \quad \sqrt{2}\, b' - a_1'^\dagger = b \qquad \vdots$$

$$\begin{cases} (2) \quad a_1'^{+} - \frac{1}{\sqrt{2}}\left(a_2'^{+} + b'\right) = a_1^{+} & \quad q_1' - \frac{1}{\sqrt{2}}\left(q_2' + q_b'\right) = q_1 \\ (3) \quad a_1'^{+} + \frac{1}{\sqrt{2}}\left(a_2'^{+} - b'\right) = a_2^{+} & \quad \vdots \end{cases}$$

Liczymy średnie q_1, p_1, q_2, p_2 w klonach

$$\langle q_1 \rangle_{out} = \langle \alpha | \langle 0 | \langle 0 | \, q_1 - \frac{1}{\sqrt{2}}\left(q_2 + q_b\right) |\alpha\rangle |0\rangle |0\rangle =$$

$$= \langle \alpha | q_1 | \alpha \rangle = \langle q_1 \rangle_{in}$$

podobnie pozostałe. Czyli klony mają te same średnie. Co z wariancjami?

$$\langle q_1^2 \rangle_{out} = \left\langle q_1^2 + \frac{1}{2}\left(q_2^2 + 2 q_2 q_b + q_b^2\right) - \frac{2}{\sqrt{2}} q_1 \left(q_2' + q_b'\right) \right\rangle_{in} =$$

$$= \langle q_1^2 \rangle_{in} + \underbrace{\frac{1}{2}}$$ dodatkowy szum w porównaniu z tym co ma stan wejściowy

Klonowanie nie jest dokładne.

Podobnie pozostałe wariancje.

Widzimy, że nawet jak wyrzucimy przyczynę to na wyjściu widać szumy. (~ emisja spontaniczna)

Napiszę BS potem wrzucę.