KVANTOVÁ PROVÁZANOST SPOJITÝCH PROMĚNNÝCH

Ladislav Mišta
Katedra optiky, Univerzita Palackého, Česká Republika

Fakulta informatiky MUNI, Brno, 26. 10. 2011

Název projektu: Mezinárodní centrum pro informaci a neurčitost
Registrační číslo: CZ.1.07/2.3.00/20.0060

Spojité proměnné

Systémy s $\dim\mathcal{H} = \infty$.

Např.: lineární harmonický oscilátor, $\hat{H} = \left(\hat{x}^2 + \hat{p}^2\right)/2$,

$\hat{x}, \hat{p}$, $[\hat{x}, \hat{p}] = i$ kanonické proměnné (spojité spektrum).

Fyz. realizace: mód elektromagnetického pole.

Mód elmag. pole – $\hat{x}, \hat{p}$ kvadraturní operátory.

Wignerova funkce

N módů, fázový prostor $x_A, p_A, \ldots, x_N, p_N$;

$$\widehat{\rho} \quad \rightarrow \quad W(\mathbf{r}) = \frac{1}{(2\pi)^N} \int e^{i\mathbf{x}'^T \cdot \mathbf{p}} \left\langle \mathbf{x} - \frac{\mathbf{x}'}{2} \right| \widehat{\rho} \left| \mathbf{x} + \frac{\mathbf{x}'}{2} \right\rangle d^N \mathbf{x}',$$

$\mathbf{r} = (x_A, p_A, \ldots, x_N, p_N)^T$.

Gaussovské stavy:

$$W(\mathbf{r}) = \frac{e^{-(\mathbf{r}-\mathbf{d})^T \gamma^{-1} (\mathbf{r}-\mathbf{d})}}{\pi^N \sqrt{\det \gamma}},$$

$\mathbf{d} = \langle \widehat{\mathbf{r}} \rangle$-posunutí, γ – kovarianční matice (KM),

$$\gamma_{ij} = \langle \Delta\hat{r}_i \Delta\hat{r}_j + \Delta\hat{r}_j \Delta\hat{r}_i \rangle, \quad \Delta\hat{r}_i = \hat{r}_i - \langle \hat{r}_i \rangle,$$

$\hat{\mathbf{r}} = (\hat{x}_A, \hat{p}_A, \ldots, \hat{x}_N, \hat{p}_N)^T$.

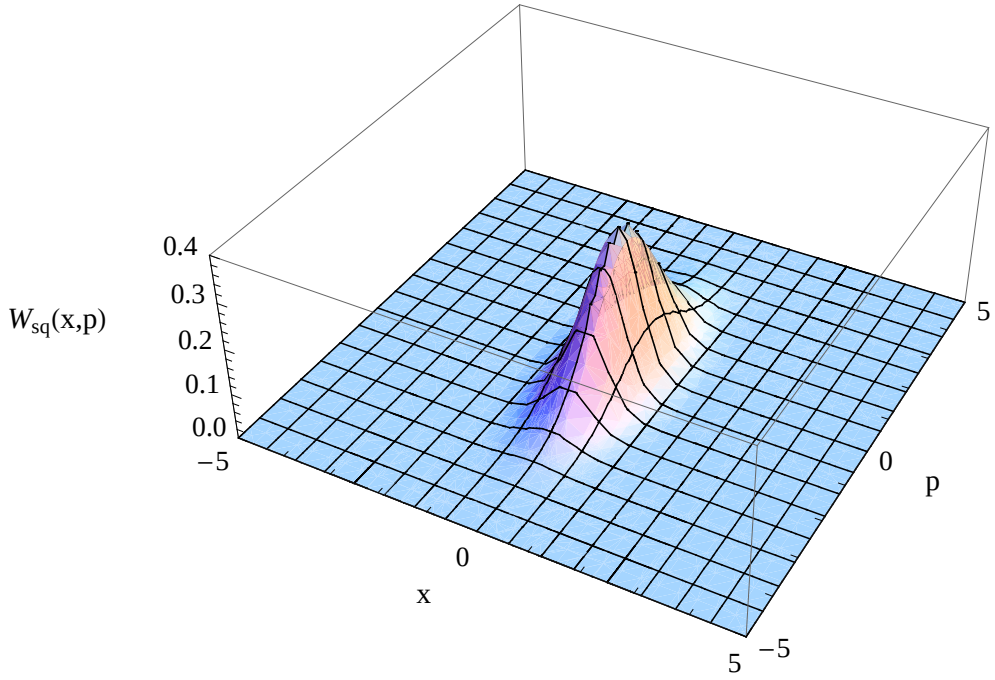
γ – $2N \times 2N$, reálná, symetrická, $\gamma > 0$.

$[\hat{r}_i, \hat{r}_j] = i\Omega_{ij}$, $\quad \Omega = \oplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ (symplektická matice).

γ je KM stavu $\Leftrightarrow$ $\gamma + i\Omega \geq 0$ (princip neurčitosti).

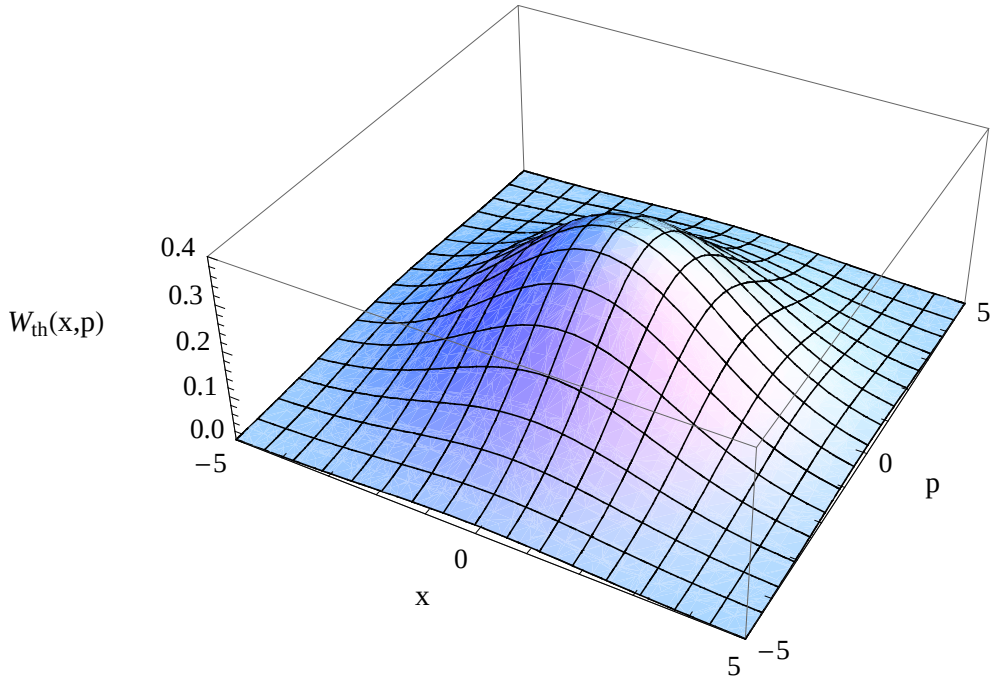
Příklady gaussovských stavů

- Stlačený stav: $|r\rangle = \widehat{S}(r)|0\rangle$,
  $\widehat{S}(r) = e^{\frac{r}{2}\left[\hat{a}^2 - \left(\hat{a}^\dagger\right)^2\right]}$ stlačovací operátor.



Fyzikální aproximace $|x\rangle$ ($|p\rangle$ pro $-r$).

- Termální stav: $\hat{\rho}_{\text{th}} = \frac{1}{1+\langle n\rangle} \sum_{n=0}^{\infty} \left(\frac{\langle n\rangle}{1+\langle n\rangle}\right)^n |n\rangle\langle n|$,
  $\langle n\rangle$ – střední počet termálních fotonů.



- Dvoumódový stlačený vakuový stav (TMSV):
  $$|TMSV\rangle_{AB} = \sqrt{1-\tanh^2(r)} \sum_{n=0}^{\infty} \tanh^n(r)|n,n\rangle_{AB},$$
  r–parametr stlačení; fyzikální aproximace EPR stavu.

Gaussovské unitární transformace

Kvadratický hamiltonián: $\hat{H} = \sum_{i,j} \kappa_{ij} \hat{r}_i \hat{r}_j \rightarrow \hat{\mathbf{r}}(t) = S(t)\hat{\mathbf{r}}(0)$

S– reálná, $2N \times 2N$, $S\Omega S^T = \Omega$ (symplektická transformace).

Pasivní transformace: $SS^T = I$.

$$S_{\text{fáz. posuv}} = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}, \; S_{\text{dělič}} = \begin{pmatrix} T \cdot I & R \cdot I \\ R \cdot I & -T \cdot I \end{pmatrix},$$

$T^2 + R^2 = 1$.

Aktivní transformace: squeezer $S_{\text{sq}} = \text{diag}(e^{-r}, e^{r})$.

$+$

Posunutí: $\hat{D}^\dagger(\bar{\alpha})\, \hat{a} \hat{D}(\bar{\alpha}) = \hat{a} + \bar{\alpha}, \quad \hat{D}(\alpha) = e^{\bar{\alpha}\hat{a}^\dagger - \bar{\alpha}^* \hat{a}},$

$\hat{x} \rightarrow \hat{x} + \bar{x}, \quad \hat{p} \rightarrow \hat{p} + \bar{p}.$

Symplektická diagonalizace

Williamsonův teorém: $\forall \gamma \geq 0 \quad \exists S, \quad S\Omega S^T = \Omega,$

$S\gamma S^T = \oplus_{i=1}^{N} \gamma_{\text{th}}(\langle n_j \rangle) = \text{diag}\,(s_1, s_1, \ldots, s_N, s_N)\,.$

$s_j = 1 + 2\langle \hat{n}_j \rangle, \quad j = 1, 2, \ldots, N$–symplektické spektrum.

$P\,(\lambda) \equiv \det\,(\Omega\gamma - \lambda I) = 0, \quad \lambda = \pm i s_j.$

γ popisuje stav $\Leftrightarrow s_j \geq 1, \quad \forall j = 1, 2, \ldots, N.$

2 módy: $P\,(\lambda) = \lambda^4 + \Delta_1^2 \lambda^2 + \Delta_2^2$

$\Delta_1^2 = \det A + \det B + 2\det C, \quad \Delta_2^2 = \det\gamma$ (sympl. invarianty).

$\gamma = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}$ vzhledem k dělení $A|B$.

$$s_{1,2} = \sqrt{\frac{\Delta_1^2 \pm \sqrt{\left(\Delta_1^2\right)^2 - 4\Delta_2^2}}{2}}.$$

$s_2 \geq 1 \quad \Rightarrow \quad \Delta_2^2 - \Delta_1^2 + 1 \geq 0$ (symplektická relace neurčitosti).

N – módové zobecnění:

$P(\lambda) = \sum_{j=0}^{N} \Delta_j^N \lambda^{2(N-j)}$, $\Delta_0^N \equiv 1$, Δ_j^N hl. minory $\Omega\gamma$ řádu $2j$.

SRN: $\sum_{j=0}^{N} (-1)^{N+j} \Delta_j^N \geq 0$.

Kvantová provázanost

Nelze vytvořit lokálními operacemi a klasickou komunikací (LOCC).

Čisté p. stavy: $|\psi\rangle_{AB} \neq |\phi\rangle_A|\chi\rangle_B, \quad |\phi\rangle_A \in \mathcal{H}_A, |\chi\rangle_B \in \mathcal{H}_B.$

Např. $|TMSV\rangle_{AB} = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n,n\rangle_{AB}.$

Smíšené p. stavy: $\widehat{\rho}_{AB} \neq \sum_i p_i \widehat{\rho}_A^{(i)} \otimes \widehat{\rho}_B^{(i)}, \quad \widehat{\rho}_A^{(i)} \in \mathcal{H}_A, \widehat{\rho}_B^{(i)} \in \mathcal{H}_B.$

PPT kritérium: $\widehat{\rho}_{AB}^{T_A} \not\geq 0 \Rightarrow$ stav je provázaný (entanglovaný).

$$\left(\widehat{\rho}^{T_A}\right)_{m\mu,n\nu} = (\widehat{\rho})_{n\mu,m\nu}$$

(A. Peres, PRL 77, 1413 (1996), M. Horodecki et al., PLA 223, 1 (1996).)

Destilace provázanosti

Provázanost lze někdy destilovat pomocí LOCC.

N částečně provázaných $\widehat{\rho} \xrightarrow{\text{LOCC}} M < N$ perfektních singletů.

$\widehat{\rho}^{T_A} \geq 0$ (PPT) $\Rightarrow$ nedestilovatelnost.

$\exists$ PPT provázané stavy–nedestilovatelná (bound) provázanost.

(P Horodecki PLA 97', Horodeckis PRL 98')

NP nelze vytvořit pomocí LOCC.

Z NP stavů nelze vydestilovat čisté singlety.

Bipartitní provázanost gaussovských stavů

$N \times M - N$ módů má Alice a M Bob.

PT vzhledem k módu j: $\hat{p}_j \to -\hat{p}_j$

$$\gamma \to \gamma^{(T_j)} = \Lambda_j \gamma \Lambda_j, \quad \Lambda_j = \mathrm{diag}(\underbrace{1,1}_{1}, \ldots \underbrace{1,-1}_{j}, \ldots, \underbrace{1,1}_{N}).$$

$1 \times M$ gaussovský stav je separabilní $\Leftrightarrow$ stav je PPT

(R. F. Werner and M. M. Wolf, PRL 86, 3658 (2001).)

$$\Leftrightarrow \gamma^{(T_A)} + i\Omega \geq 0$$

$$\Leftrightarrow s_i \geq 1, \ s_i \text{ sympl. vl. čísla } \gamma^{(T_A)}$$

$$\Leftrightarrow \sum_{j=0}^{M+1} (-1)^{M+j+1} \tilde{\Delta}_j \geq 0, \quad \tilde{\Delta}_j \text{ hl. minory } \Omega\gamma^{(T_A)} \text{ řádu } 2j.$$

Neplatí pro 2×2 kde $\exists$ gaussovský PPT provázaný stav.

$N \times M$ gaussovský stav je separabilní $\Leftrightarrow \exists$ KM $\gamma_{A,B}$

$$\gamma - \gamma_A \oplus \gamma_B \geq 0.$$

$\Rightarrow \hat{\rho} = \sum_k p_k \hat{\rho}_k, \;\; \hat{\rho}_k = \hat{\rho}_k^{(A)} \otimes \hat{\rho}_k^{(B)}, \;\; \gamma \leftrightarrow \hat{\rho}, \quad \gamma^k \leftrightarrow \hat{\rho}_k$ (blok. diag.)

$$\gamma - \sum_k p_k \gamma^k \geq 0, \quad \sum_k p_k \gamma^k = \gamma_A \oplus \gamma_B.$$

$\Leftarrow Q \equiv \gamma - \gamma_A \oplus \gamma_B \geq 0,$

$$W_\gamma(\mathbf{r_A}, \mathbf{r_B}) = \int W_Q(\mathbf{r'_A}, \mathbf{r'_B}) W_{\gamma_A}(\mathbf{r_A} - \mathbf{r'_A}) W_{\gamma_B}(\mathbf{r_B} - \mathbf{r'_B}) d\mathbf{r'_A} d\mathbf{r'_B}.$$

Struktura rozdělení W_Q:

$$W_Q(\mathbf{r}) \propto \exp\left(-\mathbf{r}^T Q^{-1} \mathbf{r}\right) \Pi_j \delta\left[(U\mathbf{r})_j\right],$$

Q^{-1} je pseudoinverze, U diagonalizuje Q, j probíhá nulová vl. čísla Q.

$$\Downarrow$$

Návod jak vyrobit sep. KM γ z KM $\gamma_A \oplus \gamma_B$.

Metoda hledání $\gamma_A \oplus \gamma_B$ pro 1×1 a 1×2.

(G. Giedke et al., PRA 64, 052303 (2001).)

Provázanost tří módů

Pro tři módy A, B a C $\exists$ pět tříd provázanosti:

1. Úplně neseparabilní: provázanost $A-(BC), B-(AC)$, $C-(AB)$.

2. 1-módově biseparabilní: provázanost $A-(BC)$ a $B-(AC)$.

3. 2-módově biseparabilní: provázanost $A-(BC)$.

4. 3-módově biseparabilní: separabilní pro všechna dělení, ale

$$\widehat{\rho}_{ABC} \neq \sum_i p_i \widehat{\rho}_A^{(i)} \otimes \widehat{\rho}_B^{(i)} \otimes \widehat{\rho}_C^{(i)}. \ (*)$$

5. Úplně separabilní: lze je napsat jako $(*)$.

Třídy 1-3 lze rozlišit PPT kritériem; 4 a 5 lze rozlišit kritériem:

$\hat{\rho}_{ABC}$ je úplně separabilní $\Leftrightarrow \exists\ \gamma_{A,B,C},\ \gamma - \gamma_A \oplus \gamma_B \oplus \gamma_C \geq 0.$

(G. Giedke et al., PRA 64, 052303 (2001))

Pro třídy 3 a 4 nelze vydestilovat provázanost LOCC mezi žádnými dvěma stranami i když mohou spolupracovat se třetí stranou.

Tripartitní nedestilovatelná provázanost.

Aplikace třídy 3: distribuce provázanosti separabilními stavy.

(kvantové bity – T. S. Cubitt et al., PRL 03'.)

(gaussovské stavy – L. Mišta and N. Korolkova, PRA 09'.)

Gaussovská tripartitní bound provázanost

Konstrukce stavu třídy 3:

$$\gamma = \gamma_{AC}^{(TMSV)} \oplus I_B + x\left(q_1 q_1^T + q_2 q_2^T\right),$$

$$x = \frac{e^{2r}-1}{2};\ q_1 = (0,-1,0,2,0,-1)^T,\ q_2 = (1,0,2,0,-1,0)^T.$$

PPT kritérium: separabilita $B-(AC)$ a $C-(AB)$; provázanost $A-(BC)$ $\rightarrow$ třímódová gaussovská nedestilovatelná provázanost.

Bezpečné klasické korelace

Alice, Bob a narušitel Eva sdílejí rozdělení $P(A, B, E)$.

P obsahuje bezpečné korelace pokud jej nelze vytvořit lokálními operacemi a veřejnou komunikací (LOPC).

Bezpečné korelace lze někdy destilovat pomocí LOPC na bezpečný klíč.

Bezpečný klíč lze destilovat jestliže (Csiszár et al, IEEE Tr. Inf. Th. 78'):

$$\max(I_{AB} - I_{AE}, I_{AB} - I_{BE}) > 0.$$

(I_{ij} – Shannonova vzájemná informace $P(i, j)$.)

Destilace bezpečného klíče se podobá destilaci provázanosti.

Analogie:

Kvantová provázanost	Bezpečné korelace
Klasická komunikace	Veřejná komunikace

...

(Collins et al, PRA 02')

Existují nedestilovatelné bezpečné korelace (bound informace)
což by byla klasická analogie nedestilovatelné provázanosti?

(N. Gisin and S. Wolf, in Proceedings of CRYPTO (2000).)

1. BI nelze distribuovat LOPC.
2. BI nelze destilovat na bezpečný klíč.

Bipartitní případ není znám.

Existuje tripartitní diskrétní BI (Acín et al, PRL 04').

Tripartitní bound informace

Spolupracující Alice, Bob, Clare, a nepřátelská Eva sdílejí $P(A, B, C, E)$.

Alice, Bob a Clare jsou spojeni veřejným kanálem.

$P(A, B, C, E)$ obsahuje BI jestliže:

1. Bezpečný klíč nelze vydestilovat LOPC mezi žádnými dvěma spolupracujícími stranami i když mohou spolupracovat se třetí stranou.

2. Rozdělení nelze vytvořit pomocí LOPC.

Konstrukce gaussovské BI

1. Konstrukce purifikace: γ lze připravit z $\gamma_{AC}^{(TMSV)} \oplus I_B$

$$\begin{aligned}
\widehat{x}_A &\rightarrow \widehat{x}_A + \frac{v}{2}, \quad \widehat{x}_B \rightarrow \widehat{x}_B + v, \quad \widehat{x}_C \rightarrow \widehat{x}_C - \frac{v}{2}, \quad 2\langle v^2 \rangle = 4x. \\
\widehat{p}_A &\rightarrow \widehat{p}_A - \frac{u}{2}, \quad \widehat{p}_B \rightarrow \widehat{p}_B + u, \quad \widehat{p}_C \rightarrow \widehat{p}_C - \frac{u}{2}, \quad 2\langle u^2 \rangle = 4x.
\end{aligned}$$

Purifikace $|\pi\rangle$:

$$|\pi\rangle = \int \sqrt{\mathcal{P}(u,v)} \left| \frac{v-iu}{2\sqrt{2}}, -\frac{v+iu}{2\sqrt{2}}; r \right\rangle_{AC}^{(TMSV)} \left| \frac{v+iu}{\sqrt{2}} \right\rangle_{B}^{(vac)} |v\rangle_{E_1}^{(x)} |u\rangle_{E_2}^{(p)} \, du dv.$$

$$X = \begin{pmatrix}
a & 2x & b & 2x & \frac{e^{2r}}{2} - x \\
2x & 1+4x & -2x & 4x & -1-2x \\
b & -2x & a & -2x & \frac{e^{2r}}{2} + x \\
2x & 4x & -2x & 4x & -2x \\
\frac{e^{2r}}{2} - x & -1-2x & \frac{e^{2r}}{2} + x & -2x & y
\end{pmatrix},$$

$$a = \cosh(2r) + x, \quad b = \sinh(2r) - x, \quad y = \tfrac{e^{2r}(2e^{2r}-1)}{2(e^{2r}-1)}.$$

2. Konstrukce kl. rozdělení: homodynní detekce x

$$\downarrow$$

$$P(x_A, x_B, x_C, x_{E_1}, x_{E_2}) = |\langle x_A, x_B, x_C, x_{E_1}, x_{E_2}|\pi\rangle|^2,$$

Gaussovské rozdělení s korelační maticí X.

$P_{\text{red}}(x_A, x_B, x_C)$ lze vytvořit LO na B a (AC) + PC x_{E_1}:

$$x_A \to x_A + \frac{x_{E_1}}{2}, \quad x_B \to x_B + x_{E_1}, \quad x_C \to x_C - \frac{x_{E_1}}{2},$$

$$X_{AC} = \begin{pmatrix} \cosh(2r) & \sinh(2r) \\ \sinh(2r) & \cosh(2r) \end{pmatrix}, \quad 2\langle x_B^2\rangle = 1, \quad 2\langle x_{E_1}^2\rangle = 4x.$$

$\Rightarrow$ P nemá bezpečné korelace vzhledem k dělení $B - (AC)$.

$P_{\text{red}}(x_A, x_B, x_C)$ lze vytvořit LO na C a (AB) + PC x_{E_2}:

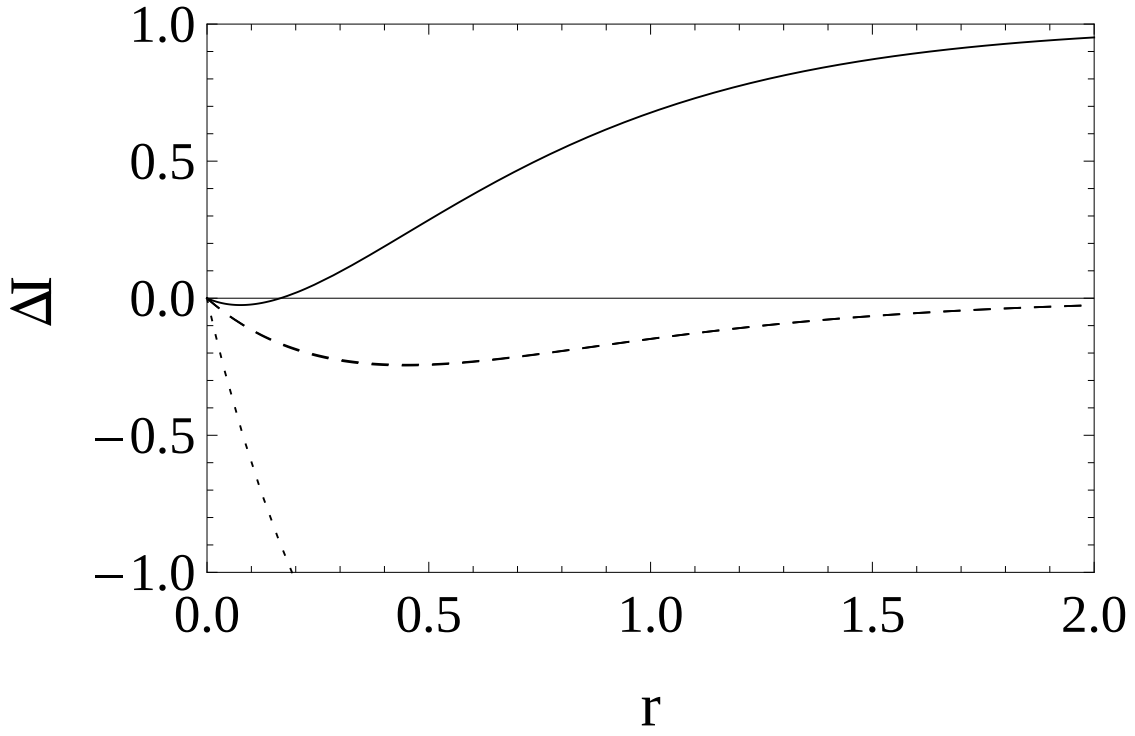
$$x_A \to x_A + \frac{x_{E_2}}{2y}, \quad x_B \to x_B - e^{2r}\frac{x_{E_2}}{y}, \quad x_C \to x_C + \left(1 - e^{-2r}\right) x_{E_2},$$

$$X_{AB} = \frac{1}{y}\begin{pmatrix} \sqrt{y^2 + e^{8r}} & e^{4r} \\ e^{4r} & \sqrt{y^2 + e^{8r}} \end{pmatrix}, \quad 2\langle x_C^2 \rangle = 1, \quad 2\langle x_{E_2}^2 \rangle = y.$$

$\Rightarrow$ P nemá bezpečné korelace vzhledem k dělení $C - (AB)$.

P má bezpečné korelace vzhledem k dělení $A - (BC)$.
"Aktivace" globální operací na (BC): $(x_B \pm x_C)/\sqrt{2}$. Pro získané rozdělení $\tilde{P}_{\text{red}}(x_A, x_B, x_{E_1}, x_{E_2})$ platí:

$\downarrow$



$I_{AB} - I_{AE}$ (čárkovaná č.), $I_{AB} - I_{BE}$ (souvislá č.) pro $\tilde{P}$.

$I_{AB} - I_{BE} > 0$ ($r > 0.166$) $\Rightarrow$ Alice a Bob mohou vydestilovat bezpečný klíč použitím protokolu pro reverzní rekonciliaci.

(Grosshans et al, OIC 03'; Assche et al, IEEE Tr. Inf. Th. 04').

$\Rightarrow$ P nelze vytvořit LOPC.

Gaussovské rozdělení P obsahuje tripartitní bound informaci!

(L. Mišta and N. Korolkova quant-ph/1108.0578).

Závěr

- Příklad tripartitní gaussovské bound informace.
- Její explicitní vyjádření pomocí LOPC.
- Aktivace bound informace, nové druhy bound informace?