KVANTOVÁ PROVÁZANOST TŘÍ MÓDŮ

Ladislav Mišta

Katedra optiky, Univerzita Palackého, Česká Republika

Přírodovědecká fakulta UP, Olomouc, 25. 10. 2011

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

evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Spojité proměnné

Systémy se stavovým prostorem $\mathcal{H}$, kde 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, kolektivní spin atomového mraku...

Mód elmag. pole – $\hat{x}, \hat{p}$ amplitudová a fázová kvadratura.

Gaussovské stavy

N–módů, $\hat{\mathbf{r}} = (\hat{x}_A, \hat{p}_A, \ldots, \hat{x}_N, \hat{p}_N)^T$, $\quad [\hat{r}_i, \hat{r}_j] = i\Omega_{ij}$,

$$\Omega = \oplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ (symplektická matice).}$$

Fázový prostor $x_A, p_A, \ldots, x_N, p_N$; $\hat{\rho}$ lze znázornit

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

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

Gaussovské stavy:

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

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

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

γ – $2N \times 2N$, reálná, symetrická.

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

Např. Dvoumódové stlačené vakuum

$$|TMSV\rangle_{AB} = e^{r\left(a^\dagger b^\dagger - ab\right)}|0,0\rangle_{AB} = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n,n\rangle_{AB},$$

$\lambda = \tanh(r)$, r–parametr stlačení.

$$\gamma_{AB}^{TMSV} = \begin{pmatrix} \cosh(2r)\cdot I & \sinh(2r)\cdot\sigma_z \\ \sinh(2r)\cdot\sigma_z & \cosh(2r)\cdot I \end{pmatrix}$$

$$\langle[\Delta\left(x_A - x_B\right)]^2\rangle = \langle[\Delta\left(p_A + p_B\right)]^2\rangle = e^{-2r}.$$

Fyzikální aproximace $|EPR\rangle \propto \int dx|x,x\rangle \propto \int dp|p,-p\rangle$.

Kvantová provázanost

Provázané stavy 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: $\hat{\rho}_{AB} \neq \sum_i p_i \hat{\rho}_A^{(i)} \otimes \hat{\rho}_B^{(i)}, \quad \hat{\rho}_A^{(i)} \in \mathcal{H}_A, \hat{\rho}_B^{(i)} \in \mathcal{H}_B.$
$p_i \geq 0, \sum_i p_i = 1.$

PH Kritérium: $\hat{\rho}_{AB}^{T_A} \ngeq 0 \Rightarrow$ stav je provázaný.

$\left(\hat{\rho}^{T_A}\right)_{m\mu,n\nu} = (\hat{\rho})_{n\mu,m\nu}$ (**částečná transpozice (PT)**).

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

Destilace provázanosti

Provázanost lze někdy destilovat pomocí LOCC.

Částečně provázané $\hat{\rho} \xrightarrow{\text{LOCC}}$ čistá maximální provázanost.

$\hat{\rho}^{T_A} \geq 0$ (PPT) $\quad \Rightarrow$ 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 čistou maximální provázanost.

NPT stačí pro destilovatelnost bipartitních gaussovských stavů.

(G. Giedke et al., Quant. Inf. Comp. 3, 79 (2001).)

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).)

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

$$\Leftrightarrow s_i \geq 1, \; s_i \text{ sympl. vl. čísla } \gamma^{(T_A)}, \text{ Eig}\left\{\Omega\gamma^{(T_A)}\right\} = \{\pm i s_i\}$$

$$\Leftrightarrow \textstyle\sum_{j=0}^{M+1} (-1)^{M+1+j} \Delta_j \geq 0, \quad \Delta_j \text{ hlavní minory } \Omega\gamma^{(T_A)} \text{ řádu } 2j.$$

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

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

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

$\Rightarrow \ \widehat{\rho} = \sum_k p_k \widehat{\rho}_k, \ \ \widehat{\rho}_k = \widehat{\rho}_k^{(A)} \otimes \widehat{\rho}_k^{(B)}, \ \ \gamma \leftrightarrow \widehat{\rho}, \quad \gamma^k \leftrightarrow \widehat{\rho}_k$ (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

Módy A, B, C.

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

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

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))

Třídy 3 a 4 nelze destilovat operacemi $\sum_i p_i \mathcal{E}_i^{(A)} \otimes \mathcal{E}_i^{(B)} \otimes \mathcal{E}_i^{(C)}$.

Tripartitní nedestilovatelná provázanost.

Lokální operace neumožňují přechod z třídy k do třídy $k' < k$.

$\exists$ stav třídy 5, který lze přepnout operací na (AC) na stav třídy 3, který lze přepnout operací na (BC) na stav kde A je provázáno s B (třída 2).

Aplikace: protokol pro distribuci provázanosti separabilními stavy.

Distribuce provázanosti

- **Přímým přenosem provázanosti**.

  Systém C provázaný s A je přenesen k systému B kde jsou vyměněny.

- **Zasláním separabilního systému**.

  1. Úplně separabilní stav módů A, B and C.
  2. Interakce A s C vede na stav separabilní vzhledem $B-(AC)$ a $C-(AB)$ dělení (provázanost A s (BC)).
  3. Separabilní C je zasláno k B kde interagují a vytvoří provázanost A a B.

  (Pro kvantové bity – T. S. Cubitt et al., PRL 91, 037902 (2003).)

Gaussovský protokol

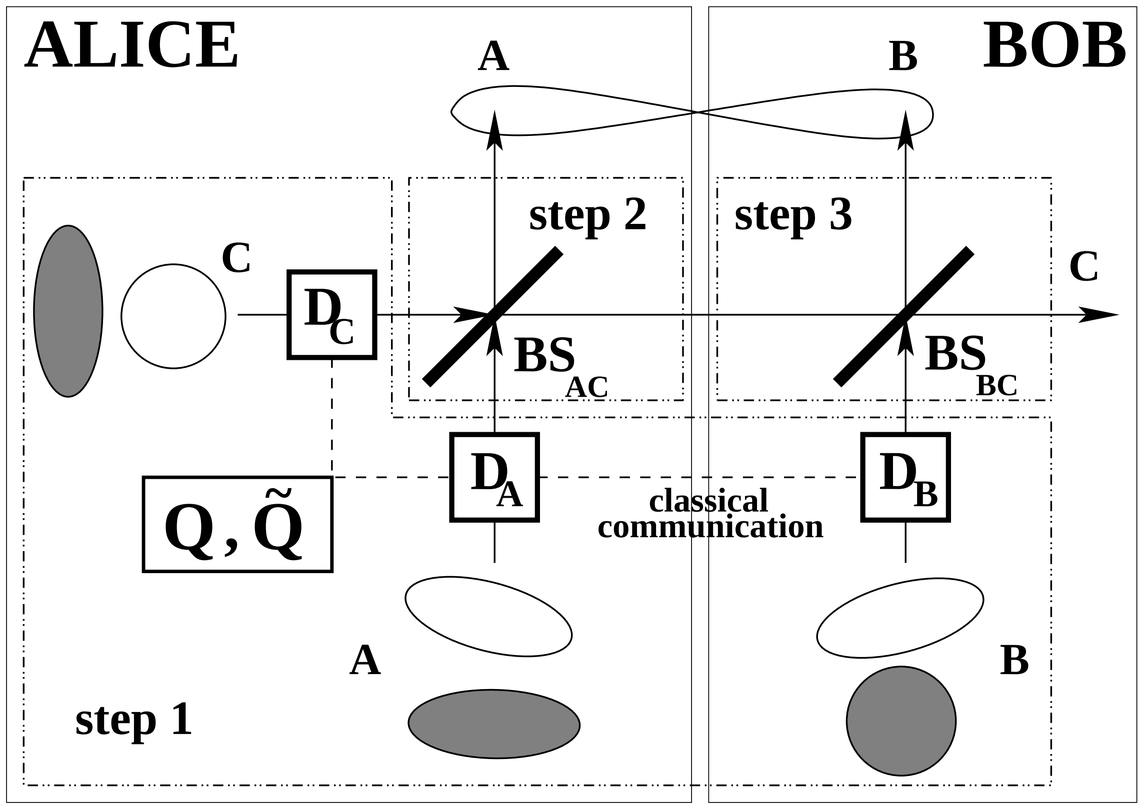
(Mišta and Korolkova, PRA 09')

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.



Krok 1: Úplně separabilní stav (třída 5).

$\gamma_{A,C} = \mathrm{diag}(e^{\pm 2r}, e^{\mp 2r}), \gamma_B = I$.

$\hat{p}_A \to \hat{p}_A - \frac{u}{\sqrt{2}}, \hat{x}_C \to \hat{x}_C + \frac{v}{\sqrt{2}}, \hat{x}_B \to \hat{x}_B + v, \hat{p}_B \to \hat{p}_B + u, \langle {}^{u^2}_{v^2} \rangle = 2x.$

Krok 2: $BS_{AC} \to B-(AC)$ a $C-(AB)$ separabilita (třída 3).

Krok 3: $BS_{BC} \to$ provázanost A a B (třída 2) ($E_{\mathcal{N}} = 1.3$ ebitů).

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),tj., $P(A, B)$ nelze distribuovat veřejnou komunikací nejvýše proměnné E.

Bezpečné korelace lze někdy destilovat pomocí LOPC na bezpečný klíč. (sdílený náhodný řetězec bitů, o kterém nemá Eva prakticky žádnou informaci).

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

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

(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. Nelze je distribuovat LOPC.
2. Nelze z nich vydestilovat bezpečný klíč.

Bipartitní případ není znám.

Existuje pro tripartitní diskrétní případ (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 bound informaci jestliže:

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

2. Rozdělení nelze vytvořit pomocí LOPC.

Konstrukce tripartitní BI (Acín et al, PRL 04'):

1. BE stav $\hat{\rho}_{ABC}$ tří kvantových bitů A, B and C:
   • separabilita $B-(AC)$, $C-(AB)$ $\Rightarrow$ provázanost nelze vydestilovat mezi libovolnými dvěma stranami pomocí LOCC.
   • provázanost $A-(BC)$ $\Rightarrow$ stav nelze připravit pomocí LOCC.

2. Purifikace $|\pi\rangle_{ABCE}$ ($\hat{\rho}_{ABC} = \mathrm{Tr}_E[|\pi\rangle_{ABCE}\langle\pi|]$).

3. $P(A, B, C, E) = |\langle \text{comp. basis}|\pi\rangle_{ABCE}|^2$ obsahuje BI.

Důkaz: $I_{AB\downarrow E} = \min_{E\to\tilde{E}}\left(I_{AB|\tilde{E}}\right)$ (intrinsic information).

(Maurer et al, IEEE Tr. Inf. Th. 99')

$I_{AB\downarrow E} = 0 \Rightarrow$ Žádný bezpečný klíč; $I_{AB\downarrow E} > 0 \Rightarrow$ Neexistuje LOPC příprava.

$$I_{C(AB)\downarrow E} = I_{B(AC)\downarrow E} = 0, \quad I_{A(BC)\downarrow E} > 0.$$

1. Purifikace stavu z kroku 2: γ lze připravit z $\gamma_{AC} \oplus I_B$

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

Purifikace $|\pi\rangle$:

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

Nemá $x-p$ korelace $\rightarrow \gamma_\pi = X \oplus X^{-1}$

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

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

2. **Klasické 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}:

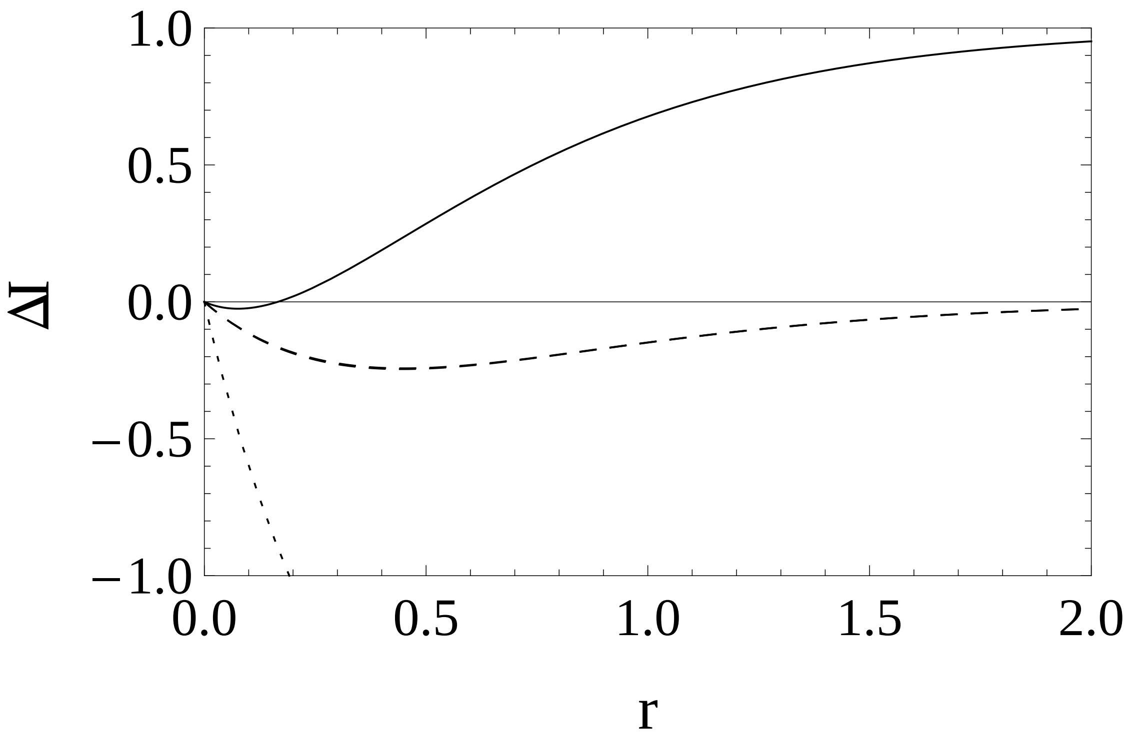
$$x_A \to x_A + \frac{x_{E_2}}{2y}, \quad x_B \to x_B - e^{2r}\frac{x_{E_2}}{y}, \quad x_C \to x_C + \left(1 - e^{-2r}\right) x_{E_2},$$

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

$\Rightarrow$ 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, QIC 03'; Assche et al, IEEE Tr. Inf. Th. 04').

$\Rightarrow$ P nelze vytvořit LOPC.

Gaussovské rozdělení P obsahuje tripartitní bound informaci!

Závěr

- Příklad tripartitní gaussovské bound informace.

- Její explicitní vyjádření pomocí LOPC vzhledem k jednotlivým dělením (vhled do její struktury).

- Aktivace bound informace, nové druhy bound informace?