GAUSSIAN INTRINSIC ENTANGLEMENT

Palacký University
Olomouc

Ladislav Mišta

QULIPS – School of Physical & Mathematical Sciences, NTU

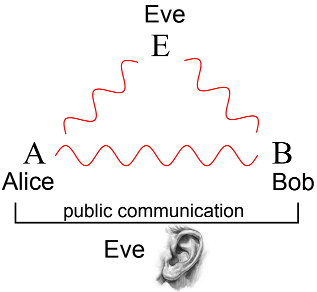
March 4-10, 2016

Collaboration:

Richard Tatham

U. Maurer, IEEE TIT 39, 733 (1993).

Secret key agreement protocol



- A, B, E obey $P(A,B,E)$.
- Alice and Bob want a secret key.
- They can use only local operations and public communication (LOPC).

SKA is possible only if P cannot be created by LOPC – secret correlations.

U. Maurer *et al.*, IEEE TIT 45, 499 (1999).
N. Gisin *et al.*, CRYPTO 2000, 482 (2000).

Intrinsic information

$$I\left(A:B\downarrow E\right):=\inf_{E\rightarrow\tilde{E}}[I(A:B|\tilde{E})],$$

$I\left(A;B|E\right)$ - conditional mutual information; minimization over channels $P(\tilde{E}|E)$.

- Quantifies how much Bob learns about Alice's data by looking at his own data after Eve announces her data (or a function of her data).
- Upper bound on secret key rate:

$$S\left(A;B\|E\right)\leq I\left(A:B\downarrow E\right).$$

- $P(A,B,E)$ contains secret correlations $\Longleftrightarrow I\left(A:B\downarrow E\right)>0$.

U. Maurer *et al.*, IEEE TIT 45, 499 (1999).
N. Gisin *et al.*, CRYPTO 2000, 482 (2000).

Classical measure of entanglement

Mapping entanglement onto intrinsic information by measurement:

$$\rho_{AB} \rightarrow |\Psi\rangle_{ABE} \rightarrow P(A,B,E) = \mathrm{Tr}(\Pi_A \otimes \Pi_B \otimes \Pi_E |\Psi\rangle_{ABE}\langle\Psi|).$$

Entanglement quantifier:

$$\mu\left(\rho_{AB}\right) := \inf_{\{\Pi_E, |\Psi\rangle_{ABE}\}} \sup_{\{\Pi_A, \Pi_B\}} \left[I\left(A;B\downarrow E\right)\right]$$

- Vanishes on separable states.
- Equal to von Neumann entropy on pure states.
- Computed for Werner state (hard otherwise).

L. Mišta, Jr. *et al.*, PRA 91, 062313 (2015).
I. M. Gelfand *et al.*, Usp. Mat. Nauk 12, 3 (1957).
L. Magnin *et al.*, Phys. Rev. A 81, 010302 (2010).
R. F. Werner *et al.*, Phys. Rev. Lett. 86, 3658 (2001).

Intrinsic entanglement

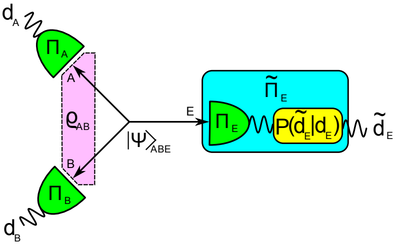
$$\boxed{E_{\downarrow}\left(\rho_{AB}\right) := \sup_{\{\Pi_A,\Pi_B\}} \inf_{\{\Pi_E,|\Psi\rangle_{ABE}\}} \left[I\left(A;B\downarrow E\right)\right]}$$

Gaussian scenario:

- ρ_{AB} – $(N+M)$-mode **Gaussian state** with covariance matrix (CM) γ_{AB},
- $|\Psi\rangle_{ABE}$ – **Gaussian purification** with CM $\gamma_\pi = \begin{pmatrix} \gamma_{AB} & \gamma_{ABE} \\ \gamma_{ABE}^T & \gamma_E \end{pmatrix}$,
- $\Pi_{A,B,E}$ – **Gaussian measurements**; outcomes d_A, d_B, d_E, CMs $\Gamma_{A,B,E}$,
- $E \to \tilde{E}$ – **Gaussian channel** characterized by Gaussian $P(\tilde{d}_E|d_E)$.

L. Mišta, Jr. *et al.*, PRA 91, 062313 (2015).
I. M. Gelfand *et al.*, Usp. Mat. Nauk 12, 3 (1957).
L. Magnin *et al.*, Phys. Rev. A 81, 010302 (2010).
R. F. Werner *et al.*, Phys. Rev. Lett. 86, 3658 (2001).

Simplification



1. $P(d_A, d_B, d_E)$ - Gaussian with CM

$$\gamma_\pi + \Gamma_A \oplus \Gamma_B \oplus \Gamma_E.$$

$$\begin{aligned} I(A:B|E) &= \langle I(A:B|E=e)\rangle \\ &= I(A:B|E=e) \end{aligned}$$

mutual information of $P(d_A, d_B|d_E)$ with CM

$$\sigma_{AB} = \Gamma_A \oplus \Gamma_B + \gamma_{AB} - \gamma_{ABE}\frac{1}{\gamma_E + \Gamma_E}\gamma_{ABE}^T$$

$$\Downarrow$$

$$\boxed{I(A:B|E) = \frac{1}{2}\ln\left(\frac{\det\sigma_A \det\sigma_B}{\det\sigma_{AB}}\right)}$$

2. $P(\tilde{d}_E|d_E) \propto e^{-(\tilde{d}_E - Xd_E)^T Y^{-1}(\tilde{d}_E - Xd_E)}$,

$$\tilde{\sigma}_{AB} = \ldots - \gamma_{ABE}X^T\frac{1}{X(\gamma_E+\Gamma_E)X^T+Y}X\gamma_{ABE}^T$$

$= [\text{SVD, blockwise inversion, some algebra}]$

$$= \ldots - \gamma_{ABE}\frac{1}{\gamma_E+\Gamma'_E}\gamma_{ABE}^T, \quad \Gamma'_E - \text{CM},$$

$$\Downarrow$$

$$\boxed{E \to \tilde{E} \text{ can be integrated into } \Gamma_E}$$

L. Mišta, Jr. *et al.*, PRA 91, 062313 (2015).
I. M. Gelfand *et al.*, Usp. Mat. Nauk 12, 3 (1957).
L. Magnin *et al.*, Phys. Rev. A 81, 010302 (2010).
R. F. Werner *et al.*, Phys. Rev. Lett. 86, 3658 (2001).

Simplification

Symplectic transformations: $S\Omega S^T = \Omega$, $\Omega = \oplus_{i=1}^{N+M} i\sigma_y$.

Symplectic diagonalization: $S\gamma_{AB}S^T = \oplus_{i=1}^{N+M}\nu_i I$, $\nu_i \geq 1$ - symplectic eigenvalues.

3. Purifications $|\bar{\Psi}\rangle$ (K modes E) and $|\Psi\rangle$ ($R \leq K$ modes E),

$$\bar{\gamma}_\pi = [I_{AB} \oplus S_E^{-1}][\gamma_\pi \oplus I_{2(K-R)}][I_{AB} \oplus (S_E^T)^{-1}],$$

$$\bar{\sigma}_{AB} = \ldots \bar{\gamma}_{ABE}(\bar{\gamma}_E + \bar{\Gamma}_E)^{-1}\bar{\gamma}_{ABE}^T = \ldots \gamma_{ABE}(\gamma_E + \Gamma_E)^{-1}\gamma_{ABE}^T = \sigma_{AB}$$

$$\Downarrow$$

For any $|\bar{\Psi}\rangle$ and $\bar{\Gamma}_E$ there is Γ_E on fixed $|\Psi\rangle$ giving $\bar{\sigma}_{AB} = \sigma_{AB}$

L. Mišta, Jr. *et al.*, PRA 91, 062313 (2015).
I. M. Gelfand *et al.*, Usp. Mat. Nauk 12, 3 (1957).
L. Magnin *et al.*, Phys. Rev. A 81, 010302 (2010).
R. F. Werner *et al.*, Phys. Rev. Lett. 86, 3658 (2001).

Gaussian intrinsic entanglement

$$\boxed{E_{\downarrow}^{G}\left(\rho_{AB}\right)=\sup_{\Gamma_A,\Gamma_B}\inf_{\Gamma_E}\left[\frac{1}{2}\ln\left(\frac{\det\sigma_A\det\sigma_B}{\det\sigma_{AB}}\right)\right]}$$

$$\sigma_{AB}=\Gamma_A\oplus\Gamma_B+\gamma_{AB}-\gamma_{ABE}\frac{1}{\gamma_E+\Gamma_E}\gamma_{ABE}^{T},$$

$\begin{pmatrix}\gamma_{AB} & \gamma_{ABE}\\ \gamma_{ABE}^{T} & \gamma_E\end{pmatrix}$ – CM of an arbitrary fixed purification.

Minimal purification:

$$\gamma_E=\bigoplus_{i=1}^{R}\nu_i I,\quad \gamma_{ABE}=S^{-1}\begin{pmatrix}\bigoplus_{i=1}^{R}\sqrt{\nu_i^2-1}\sigma_z\\ \mathbb{O}\end{pmatrix},$$

R – number of symplectic eigenvalues >1 of γ_{AB}.

L. Mišta, Jr. *et al.*, PRA 91, 062313 (2015).
I. M. Gelfand *et al.*, Usp. Mat. Nauk 12, 3 (1957).
L. Magnin *et al.*, Phys. Rev. A 81, 010302 (2010).
R. F. Werner *et al.*, Phys. Rev. Lett. 86, 3658 (2001).

Faithfulness

Gaussian separable state:

$$\rho_{AB}^{\mathrm{sep}} = \int P_{\mathrm{Gauss}}(\mathbf{r}) D(\mathcal{V}\mathbf{r}) |\chi_A\rangle_A\langle\chi_A| \otimes |\chi_B\rangle_B\langle\chi_B| D^{\dagger}(\mathcal{V}\mathbf{r}) d\mathbf{r},$$

Purification:

$$|\tilde{\Psi}\rangle_{ABE} = \int \sqrt{P_{\mathrm{Gauss}}(\mathbf{r})} D(\mathcal{V}\mathbf{r}) |\chi_A\rangle_A |\chi_B\rangle_B |\mathbf{r}\rangle_E d\mathbf{r},$$

$|\mathbf{r}\rangle_E$ – product of position eigenvectors.

Measurement of $|\mathbf{r}'\rangle_E$:

$$D(\mathcal{V}\mathbf{r}')|\chi_A\rangle_A|\chi_B\rangle_B \Rightarrow \sigma_{AB} = \sigma_A \oplus \sigma_B \Rightarrow E_{\downarrow}^{G}\left(\rho_{AB}^{\mathrm{sep}}\right) = 0.$$

One can also show that $E_{\downarrow}^{G}\left(\rho_{AB}\right) = 0 \Rightarrow \rho_{AB}$ is separable.

$$\boxed{\text{GIE vanishes} \Leftrightarrow \rho_{AB} \text{ is separable}}$$

L. Mišta, Jr. *et al.*, PRA 91, 062313 (2015).
I. M. Gelfand *et al.*, Usp. Mat. Nauk 12, 3 (1957).
L. Magnin *et al.*, Phys. Rev. A 81, 010302 (2010).
R. F. Werner *et al.*, Phys. Rev. Lett. 86, 3658 (2001).

Monotonicity

Gaussian local trace-preserving operations and classical communication (GLTPOCC):

$$\mathcal{M}\colon\ \rho_{AB} \rightarrow \rho_{AB}^{\mathcal{M}},$$

$$E_{\downarrow}^{G}\left(\rho_{AB}\right) \geq E_{\downarrow}^{G}\left(\rho_{AB}^{\mathcal{M}}\right).$$

$\mathcal{M}$ can be represented by a quantum state $M_{A_{\rm in}B_{\rm in}A_{\rm out}B_{\rm out}}$.

$\mathcal{M}$ can be implemented by teleportation via $M_{A_{\rm in}B_{\rm in}A_{\rm out}B_{\rm out}}$.

$\rho_{AB}^{\mathcal{M}} \rightarrow |\Psi^{\mathcal{M}}\rangle \propto {}_{AA_{\rm in}}\langle\{0\}|_{BB_{\rm in}}\langle\{0\}|\Psi\rangle_{ABE_{\rho}}|M\rangle_{A_{\rm in}B_{\rm in}A_{\rm out}B_{\rm out}E_{M}}$.

($|M\rangle$ purifies M, $|\Psi\rangle$ purifies ρ_{AB}.)

$\mathcal{M}$ is TPLOCC: $M_{A_{\rm in}B_{\rm in}A_{\rm out}B_{\rm out}} = \sum_i p_i M^{(i)}_{A_{\rm in}A_{\rm out}} \otimes M^{(i)}_{B_{\rm in}B_{\rm out}}$, $M^{(i)}_{j_{\rm in}j_{\rm out}}$ – TP.

Monotonicity

$\exists$ measurement with CM $\tilde{\Gamma}_{E_M}^{\mathcal{M}}$ projecting $|M\rangle$ to $M_{A_{\rm in}A_{\rm out}}^{(i)}\otimes M_{B_{\rm in}B_{\rm out}}^{(i)}$.

$$E_{\downarrow}^{G}\left(\rho_{AB}^{\mathcal{M}}\right)=f\left(\gamma_{\pi}^{\mathcal{M}},\Gamma_{A}^{\mathcal{M}},\Gamma_{B}^{\mathcal{M}},\Gamma_{E}^{\mathcal{M}}\right),\ E_{\downarrow}^{G}\left(\rho_{AB}\right)=f\left(\gamma_{\pi},\Gamma_{A}^{(0)},\Gamma_{B}^{(0)},\Gamma_{E_{\rho}}^{(0)}\right).$$

$$E_{\downarrow}^{G}\left(\rho_{AB}^{\mathcal{M}}\right)\leq f\left(\gamma_{\pi}^{\mathcal{M}},\Gamma_{A}^{\mathcal{M}},\Gamma_{B}^{\mathcal{M}},\Gamma_{E_{\rho}}^{(0)}\oplus\tilde{\Gamma}_{E_M}^{\mathcal{M}}\right)$$

$=$ MI of outcomes of measurements with CMs $\Gamma_{A,B}^{\mathcal{M}}$ on $(\mathcal{M}_A\otimes\mathcal{M}_B)(\rho_{AB|E_{\rho}})$.

$\mathcal{M}_{A,B}$ – TP $\Rightarrow$ realizable by unitaries on larger system + dropping of some output modes + addition of noise. The noise can be integrated into measurements with $\Gamma_{A,B}^{\mathcal{M}}$ and the new measurements never give a higher MI than their extension to dropped modes (CMs $\Gamma'_{A,B}$),

$$f\left(\gamma_{\pi}^{\mathcal{M}},\Gamma_{A}^{\mathcal{M}},\Gamma_{B}^{\mathcal{M}},\Gamma_{E_{\rho}}^{(0)}\oplus\tilde{\Gamma}_{E_M}^{\mathcal{M}}\right)\leq f\left(\gamma_{\pi},\Gamma'_{A},\Gamma'_{B},\Gamma_{E_{\rho}}^{(0)}\right)\leq E_{\downarrow}^{G}\left(\rho_{AB}\right).$$

GIE does not increase under GLTPOCC

Two-mode symmetric states

Monotonicity $\Rightarrow$ Invariance of GIE under Gaussian local unitaries $\Rightarrow$

$$\gamma_{AB} = \begin{pmatrix} a & 0 & k_x & 0 \\ 0 & a & 0 & -k_p \\ k_x & 0 & a & 0 \\ 0 & -k_p & 0 & a \end{pmatrix}, \quad k_x \geq k_p > 0.$$

Symplectic eigenvalues: $\nu_{1,2} = \sqrt{(a \pm k_x)(a \mp k_p)}$.

Symplectic matrix: $S = [\mathrm{diag}(z_A^{-1}, z_A) \oplus \mathrm{diag}(z_B, z_B^{-1})]U_{BS}^{50:50}; \quad z_{A,B} > 1.$

Calculation using an upper bound:

$$U(\rho_{AB}) := \inf_{\Gamma_E} \sup_{\Gamma_A, \Gamma_B} \left[\frac{1}{2} \ln \left(\frac{\det\sigma_A \det\sigma_B}{\det\sigma_{AB}}\right)\right].$$

If $(\tilde{a} + \tilde{b} + 1)^2 \geq \tilde{a}\tilde{b}(\tilde{a}\tilde{b} - \tilde{c}_x^2)$ homodyning of x_A and x_B is optimal and

$$\boxed{\sup_{\Gamma_A, \Gamma_B} \frac{1}{2} \ln \left(\frac{\det\sigma_A \det\sigma_B}{\det\sigma_{AB}}\right) = \frac{1}{2} \ln \frac{\tilde{a}\tilde{b}}{\tilde{a}\tilde{b} - \tilde{c}_x^2}}$$

$\tilde{a}, \tilde{b}, \tilde{c}_x$ - parameters of $\rho_{AB|E}$.

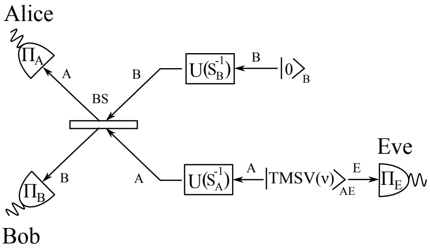
Symmetric states with a three-mode purification

States $\left(\equiv \rho_{AB}^{(1)}\right)$ satisfying:

$\nu_2 = 1 \quad \Rightarrow \quad k_x = a - \frac{1}{a+k_p}$,

$\nu_1 = \nu = \sqrt{\det\gamma_{AB}^{(1)}}$,

S_A^{-1} (S_B^{-1}) – squeezing in p_A (x_B).

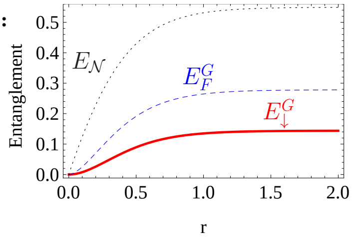


GIE for any $\rho_{AB}^{(1)}$:

$$\boxed{E_{\downarrow}^{G}\left(\rho_{AB}^{(1)}\right) = \ln\left(\frac{a}{\sqrt{a^2 - k_p^2}}\right)}$$

Reached by homodyning of x_A, x_B and x_E.

CV GHZ:



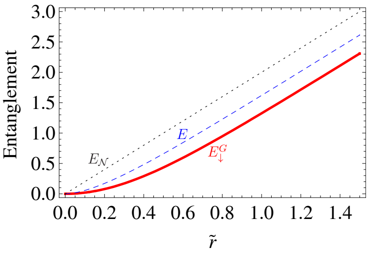
Pure states

For $k_x = k_p$ we get $a^2 - k_p^2 = 1$ and states $\rho_{AB}^{(1)}$ reduce to pure states ρ_{AB}^{p}.

GIE for pure states:

$$\boxed{E_{\downarrow}^{G}\left(\rho_{AB}^{p}\right) = \ln\left(a\right)}$$

where $a = \cosh(\tilde{r})$.



GIE is not equal to local von Neumann entropy on pure states

Equality is established by non-Gaussian photon counting on A and B.

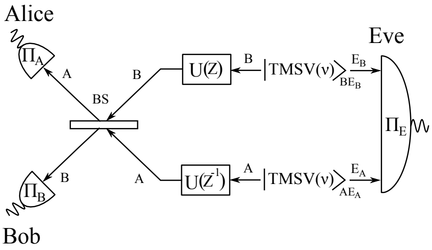
Symmetric squeezed thermal states

States $\left(\equiv \rho_{AB}^{(2)}\right)$ satisfying:

$k_x = k_p \equiv k,$

$\nu_1 = \nu_2 \equiv \nu = \sqrt{a^2 - k^2},$

Z (Z^{-1}) – squeezing in x_B (p_A).



GIE for any $\rho_{AB}^{(2)}$ with $a \leq 2.41$:

$$\boxed{E_{\downarrow}^{G}\left(\rho_{AB}^{(2)}\right) = \ln\left[\frac{(a-k)^2+1}{2(a-k)}\right]}$$

Reached by homodyning of x_A, x_B, x_{E_A} and p_{E_B}.

G. Adesso *et al.*, PRL 109, 190502 (2012).
G. Vidal and R. F. Werner, PRA 65, 032314 (2002).

Relation to Gaussian Rényi-2 entanglement

GIE for considered symmetric states:

$$E_{\downarrow}^{G}\left(\rho_{AB}\right)=\begin{cases}0, & \text{if } \tilde{\nu}_{-} \geq 1;\\ \ln\{[\tilde{\nu}_{-}+(\tilde{\nu}_{-})^{-1}]/2\}, & \text{if } \tilde{\nu}_{-} < 1,\end{cases}$$

where $\tilde{\nu}_{-}=\sqrt{(a-k_x)(a-k_p)}$ is a smaller symplectic eigenvalue of $\rho_{AB}^{T_A}$.

Gaussian Rényi-2 (GR2) entanglement:

$$E_2\left(\rho_{AB}\right)=\inf_{\substack{\theta_{AB}\leq\gamma_{AB}\\ \det\theta_{AB}=1}}\frac{1}{2}\ln\left(\det\theta_A\right).$$

$$\boxed{E_{\downarrow}^{G}\left(\rho_{AB}\right)=E_2\left(\rho_{AB}\right)}$$

Conjecture: GIE and GR2 entanglement are equal on all Gaussian states

G. Adesso *et al.*, PRL 109, 190502 (2012).
G. Vidal and R. F. Werner, PRA 65, 032314 (2002).

Relation to logarithmic negativity

Logarithmic negativity:

$$E_{\mathcal{N}}(\rho_{AB}) = \max[0, -\ln\tilde{\nu}_{-}].$$

For analyzed states:

- $E_{\downarrow}^{G}$ and $E_{\mathcal{N}}$ are monotonically decreasing functions of $\tilde{\nu}_{-}$.
- $E_{\mathcal{N}} \geq E_{\downarrow}^{G}$.

Not true in general:

- $E_{\downarrow}^{G}$ is not a function of $\tilde{\nu}_{-}$ for some asymmetric states.
- $E_{\mathcal{N}}(\rho_{AB}^{\mathrm{PPT}}) = 0$ but $E_{\downarrow}^{G}(\rho_{AB}^{\mathrm{PPT}}) > 0$ for PPT entangled states.

Conclusion

- New quantifier of Gaussian entanglement.
- Operationally associated to secret key agreement protocol.
- Computable for several classes of two-mode Gaussian states.
- GIE is equal to GR2 entanglement for the classes of states
  $\rightarrow$ conjecture that the equality holds for all Gaussian states.

Thank you!