Title: The Smooth Entropy Formalism on Operator Algebras and Applications to the Security Analysis of CV Crypto Schemes

Date: May 30, 2012 04:00 PM

URL: http://pirsa.org/12050047

Abstract: We discuss the extension of the smooth entropy formalism to arbitrary physical systems with no bound on the number of degrees of freedom, comparing them with already existing notions of entropy for infinite-dimensional systems. Our analysis is both conceptual as well as based on operational primitives, for example we ask for the ability to perform privacy amplification against any kind of quantum side information. As an application, we show how to employ a version of the entropic uncertainty relation to provide a security analysis for continuous variable quantum key distribution protocols.   based on arXiv:1107.5460, 1112.2179. This is joint work with Mario Berta, Fabian Furrer as well as with Torsten Franz, Marco Tomamichel, Reinhard Werner

Entropic Quantities on von Neumann algebras

with applications to quantum cryptography

Volkher B. Scholz, ETH Zurich
joint work with Fabian Furrer & Mario Berta,
based on arXiv:1107.5406

Overview

- Algebraic description of infinite dimensional quantum systems
- Quantum information theoretic concepts on von Neumann algebras
- Entropic quantities and their operational interpretation
- Entropic uncertainty inequalities and applications

Overview

- Algebraic description of infinite dimensional quantum systems
- Quantum information theoretic concepts on von Neumann algebras
- Entropic quantities and their operational interpretation
- Entropic uncertainty inequalities and applications

∞-dim quantum systems

...but first a short remainder

quantum system with finitely many degrees of freedom = finite-dimensional Hilbert space

$$\mathcal{H} \simeq \mathbb{C}^d,\ d < \infty$$

∞-dim quantum systems

...but first a short remainder

observables (POVM's) are positive elements, summing up to the identity

$$\{E_i\},\ E_i \in M_d(\mathbb{C}),$$
$$E_i \geq 0,\ \sum_i E_i = \mathbb{1}$$

States can be seen as positive, normalized functionals

$$\rho \in M_d,\ \rho \geq 0, \mathrm{Tr}\rho = 1$$
$$M_d \ni X \mapsto \mathrm{Tr}\rho\, X \in \mathbb{C}$$

tensor product is "unique"

$$M_{d_1} \otimes M_{d_2} \simeq M_{d_1 d_2}$$

every state can be purified

$$\rho \rightsquigarrow |\xi_\rho\rangle = \mathbb{1} \otimes \rho^{\frac{1}{2}} |\phi\rangle,$$
$$|\phi\rangle = \sum_i |ii\rangle\,, \quad \mathrm{Tr}\rho X = \langle \xi_\rho | X \otimes \mathbb{1} \xi_\rho \rangle$$

∞-dim quantum systems

...but first a short remainder

quantum system with finitely many degrees of freedom = finite-dimensional Hilbert space

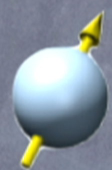
$$\mathcal{H} \simeq \mathbb{C}^d,\ d < \infty$$

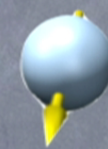
Examples:

spin systems, finite dimensions are due to physical symmetry group(s)
[Peter-Weyl theorem: compact Lie groups have only finite dimensional irreducible representations]

∞-dim quantum systems

best example of non-compact symmetry group: request Poincare invariance

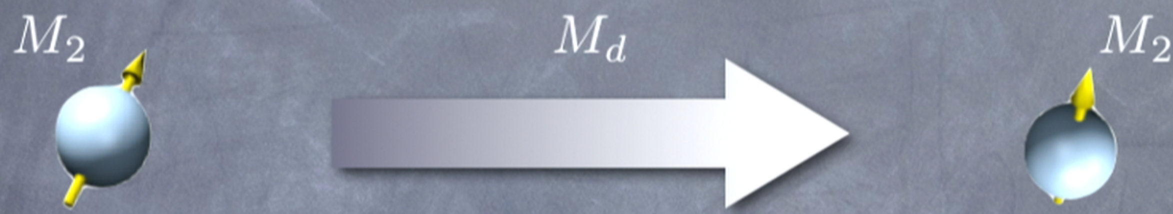




two distant atoms, one excited, the other one in the ground state, interact via electromagnetic radiation

∞-dim quantum systems

best example of non-compact symmetry group: request Poincare invariance



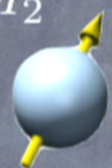
state at time t: $|\psi_t\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^d$

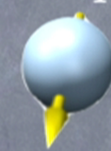
two distant atoms, one excited, the other one in the ground state, interact via electromagnetic radiation

∞-dim quantum systems

best example of non-compact symmetry group: request Poincare invariance

M_2 $\qquad$ M_d $\qquad$ M_2





state at time t: $|\psi_t\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^d$

for a finite time interval T, the probability to find the second atom in an excited state is zero

$$\forall t \in [0,T) \ : \langle \psi_t | P_{\text{atom 2 is excited}} | \psi_t \rangle = 0$$

∞-dim quantum systems

let's try to model the electromagnetic radiation by one (quantized) mode of light

$$\mathcal{H} \simeq \mathcal{L}^2(\mathbb{R})\,,\ dim\,\mathcal{H} = \infty$$

we can check that the algebra of matrices is replaced by all bounded operators on the Hilbert space

$$M_d \rightsquigarrow \mathcal{B}(\mathcal{H})$$

these types of algebras are called "type I factors", "simplest" infinite dimensional case due to the existence of enough projections onto finite dimensional subspaces

∞-dim quantum systems

Solution: restrict to a subalgebra of bounded operators, fulfilling the invariance condition.

von Neumann algebra: *-subalgebra of the bounded operators on some Hilbert space, closed with respect to the weak operator topology ("expectation value topology")

$\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ closed under addition and multiplication

$$X \in \mathcal{M} \Rightarrow X^* \, (= X^\dagger) \in \mathcal{M}$$

$$X_i \in \mathcal{M} \, : \, \forall |\psi\rangle \in \mathcal{H} \, : \lim_i \langle\psi|X_i|\psi\rangle \text{ exists}$$

$$\Rightarrow \exists X \in \mathcal{M} \, : \, \lim_i \langle\psi|X_i|\psi\rangle = \langle\psi|X|\psi\rangle$$

QIT on vN-algebras

observables (POVM's) are positive elements, summing up to the identity $\{E_i\},\, E_i \in \mathcal{M},\; E_i \geq 0,\, \sum_i E_i = \mathbb{I}$

States are continuous positive, normalized functionals $\mathcal{M} \ni X \mapsto \omega(X) \in \mathbb{C}$

$$\omega(\mathbb{I}) = 1,\; \omega(X^*X) \geq 0\,,\; \forall X \in \mathcal{M}$$

every state can be purified $\omega \rightsquigarrow (\pi_\omega, \mathcal{H}_\omega, |\xi_\omega\rangle)$

*-homomorphism $\pi_\omega : \mathcal{M} \to \mathcal{B}(\mathcal{H}_\omega)\,,\, |\xi_\omega\rangle \in \mathcal{H}_\omega$

$$\omega(X) = \langle \xi_\omega | \pi_\omega(X) \xi_\omega \rangle$$

QIT on vN-algebras

observables (POVM's) are positive elements, summing up to the identity

$$\{E_i\},\ E_i \in \mathcal{M},\quad E_i \geq 0,\ \sum_i E_i = \mathbb{I}$$

States are continuous positive, normalized functionals

$$\mathcal{M} \ni X \mapsto \omega(X) \in \mathbb{C}$$

$$\omega(\mathbb{I}) = 1,\ \omega(X^*X) \geq 0\,,\ \forall X \in \mathcal{M}$$

every state can be purified

$$\omega \rightsquigarrow (\pi_\omega, \mathcal{H}_\omega, |\xi_\omega\rangle)$$

*-homomorphism $\pi_\omega : \mathcal{M} \to \mathcal{B}(\mathcal{H}_\omega)\,,\ |\xi_\omega\rangle \in \mathcal{H}_\omega$

$$\omega(X) = \langle \xi_\omega | \pi_\omega(X) \xi_\omega \rangle$$

QIT on vN-algebras

observables (POVM's) are positive elements, summing up to the identity

$$\{E_i\},\ E_i \in \mathcal{M},$$
$$E_i \geq 0,\ \sum_i E_i = \mathbb{I}$$

States are continuous positive, normalized functionals

$$\mathcal{M} \ni X \mapsto \omega(X) \in \mathbb{C}$$
$$\omega(\mathbb{I}) = 1,\ \omega(X^* X) \geq 0\,,\ \forall X \in \mathcal{M}$$

every state can be purified

$$\omega \rightsquigarrow (\pi_\omega, \mathcal{H}_\omega, |\xi_\omega\rangle)$$

*-homomorphism $\pi_\omega : \mathcal{M} \to \mathcal{B}(\mathcal{H}_\omega)\,,\ |\xi_\omega\rangle \in \mathcal{H}_\omega$

$$\omega(X) = \langle \xi_\omega | \pi_\omega(X) \xi_\omega \rangle$$

QIT on vN-algebras

tensor products are not unique!

joint systems consists are generated by commuting subalgebras

$$\mathcal{M}_{AB} = \mathcal{M}_A \vee \mathcal{M}_B$$

$$= \text{weak-closure}\left[\sum_i X_i Y_i \,:\, X_i \in \mathcal{M}_A\,,\, Y_i \in \mathcal{M}_B\right]$$

whether this is leads to correlations unobservable in the "usual" tensor product setup is a wide open problem ("Tsirelson's problem")

QIT on vN-algebras

norm distance:

$$\|\sigma - \omega\| = \sup\{ \,|\sigma(X) - \omega(X)| \,:\, X \in \mathcal{M}, \|X\|_{\mathcal{B}(\mathcal{H})} \leq 1 \,\}$$

fidelity:

$$F(\sigma, \omega) = \sup\{ \,|\langle \xi_\sigma | \xi_\omega \rangle|^2 \,\}$$

supremum goes over all purifications in the same Hilbert space

"generalized" fidelity for non-normalized functionals:

$$\mathcal{F}(\omega, \sigma)^{\frac{1}{2}} = F(\omega, \sigma)^{\frac{1}{2}} + (1 - \omega(\mathbb{1}))^{\frac{1}{2}} (1 - \sigma(\mathbb{1}))^{\frac{1}{2}}$$

QIT on vN-algebras

two useful operators

purifications of any two states can be mapped onto each other in a self-adjoint way: the relative modular operator

$$\omega \rightsquigarrow (\pi_\omega, \mathcal{H}_\omega, |\xi_\omega\rangle)\,,\ \sigma \rightsquigarrow (\pi_\sigma, \mathcal{H}_\sigma, |\xi_\sigma\rangle)$$
$$\Delta(\sigma/\omega) : \mathcal{H}_\omega \to \mathcal{H}_\sigma\,,\ |\xi_\sigma\rangle = \Delta(\sigma/\omega)|\xi_\omega\rangle$$

if one pos. functional dominates another one:

$$\exists c > 0 \,:\, \forall X \in \mathcal{M} \,:\, \omega(X^*X) \leq c\,\sigma(X^*X)$$

then there exists a bounded operator in the commutant

$$D(\sigma/\omega) \in \mathcal{M}' = \{\, Y \in \mathcal{B}(\mathcal{H}) \,:\, [Y, X] = 0\ \forall X \in \mathcal{M}\,\}$$
$$\sigma(X) = \langle D(\sigma/\omega)\xi_\omega \,|X\, D(\sigma/\omega)\xi_\omega\,\rangle\ \ \&\ \|D\|^2 = c$$

QIT on vN-algebras

two useful operators

purifications of any two states can be mapped onto each other in a self-adjoint way: the relative modular operator

$$\omega \rightsquigarrow (\pi_\omega, \mathcal{H}_\omega, |\xi_\omega\rangle)\,,\ \sigma \rightsquigarrow (\pi_\sigma, \mathcal{H}_\sigma, |\xi_\sigma\rangle)$$
$$\Delta(\sigma/\omega) : \mathcal{H}_\omega \to \mathcal{H}_\sigma\,,\ |\xi_\sigma\rangle = \Delta(\sigma/\omega)|\xi_\omega\rangle$$

if one pos. functional dominates another one:

$$\exists c > 0 \,:\, \forall X \in \mathcal{M} \,:\, \omega(X^*X) \leq c\,\sigma(X^*X)$$

then there exists a bounded operator in the commutant

$$D(\sigma/\omega) \in \mathcal{M}' = \{\, Y \in \mathcal{B}(\mathcal{H}) \,:\, [Y, X] = 0\ \forall X \in \mathcal{M}\,\}$$
$$\sigma(X) = \langle D(\sigma/\omega)\xi_\omega \,|X\, D(\sigma/\omega)\xi_\omega \rangle \ \ \&\ \|D\|^2 = c$$

Entropic quantities

The relative modular operator allows for the extension of Renyi relative entropies to states on von Neumann algebras

$$S_\alpha(\omega,\sigma) = -\langle \xi_\omega \,| f[\Delta(\sigma/\omega)]\, \xi_\omega \rangle$$

$$f[x] = \frac{1}{\alpha(1-\alpha)}(1 - x^\alpha)$$

with the usual properties of relative entropies

Entropic quantities

The relative modular operator allows for the extension of Renyi relative entropies to states on von Neumann algebras

$$S_\alpha(\omega,\sigma) = -\langle \xi_\omega \,| f[\Delta(\sigma/\omega)]\, \xi_\omega \rangle$$

$$f[x] = \frac{1}{\alpha(1-\alpha)}(1-x^\alpha)$$

with the usual properties of relative entropies

but up to very recently, Renyi entropies had less clear operational meaning -> smooth entropy formalism of Renner et.al. captures one-shot scenarios

Entropic quantities

max-relative entropy

$$\mathrm{D}_{\max}(\omega\,||\,\sigma) = \inf\{\mu \in \mathbb{R} : \omega \leq 2^{\mu} \cdot \sigma\}$$
$$= 2\log\|D(\omega/\sigma)\|$$

min-relative entropy

$$\mathrm{D}_{\min}(\omega\,||\,\sigma) = -\log F(\omega, \sigma)$$

Prop: These quantities fulfill the usual requirements of relative entropies. In addition, if the von Neumann algebra admits nice finite-dimensional approximations, then the min/max relative entropies can be written as limits of finite-dimensional quantities.

Entropic quantities

$$\mathcal{B}^{\epsilon}_{\mathcal{M}}(\omega) = \{\sigma \in \mathcal{S}_{\leq}(\mathcal{M}) : \sqrt{1 - \mathcal{F}_{\mathcal{M}}(\omega, \sigma)} \leq \epsilon\}$$

$\mathcal{S}_{\leq}(\mathcal{M})$: set of sub-normalized positive functionals

$$\mathrm{H}^{\epsilon}_{\min}(A|B)_{\omega} = \sup_{\bar{\omega}_{AB} \in \mathcal{B}^{\epsilon}_{\mathcal{M}_{AB}}(\omega_{AB})} \mathrm{H}_{\min}(A|B)_{\bar{\omega}}$$

$$\mathrm{H}^{\epsilon}_{\max}(A|B)_{\omega} = \inf_{\bar{\omega}_{AB} \in \mathcal{B}^{\epsilon}_{\mathcal{M}_{AB}}(\omega_{AB})} \mathrm{H}_{\max}(A|B)_{\bar{\omega}}$$

Entropic quantities

Thm: Consider a purification $\omega_{AB} \rightsquigarrow (\pi_\omega, \mathcal{H}_\omega, |\xi_\omega\rangle)$.
Then we have

$$\mathrm{H}_{\max}(A|B)_\omega = -\mathrm{H}_{\min}(A|C)_\omega$$
$$\mathrm{H}^{\epsilon}_{\max}(A|B)_\omega = -\mathrm{H}^{\epsilon}_{\min}(A|C)_\omega$$

where the additional system corresponds to the commutant of the first two von Neumann algebras,

$$\mathcal{M}_C \simeq \pi_\omega(\mathcal{M}_{AB})' \,.$$

Entropic quantities

Thm: operational interpretation of the non-smooth min-entropy.

$$2^{-\mathrm{H}_{\min}(A|B)_\omega} = \sup_{\mathcal{E}_*} F((\mathrm{id}_A \otimes \mathcal{E}_*)(\omega_{AB}), |\phi\rangle)$$

where the supremum goes over all weakly continuous completely positive mappings from states on $\mathcal{M}_B$ to density matrices.

Entropic quantities

Thm: operational interpretation of the non-smooth min-entropy.

$$2^{-\mathrm{H}_{\min}(A|B)_\omega} = \sup_{\mathcal{E}_*} F((\mathrm{id}_A \otimes \mathcal{E}_*)(\omega_{AB}), |\phi\rangle)$$

where the supremum goes over all weakly continuous completely positive mappings from states on $\mathcal{M}_B$ to density matrices.

Entropic quantities

conditional min-entropy for continuous output alphabet:

$$H_{\min}(X|B)_\omega = -\log\sup\left\{\int \omega_B^x(E_B^x)\mathrm{d}\mu(\mathrm{x}) : \right.$$
$$\left. E \in \mathcal{L}^\infty(X, \mathcal{M}_{B,+}),\ \int E_B^x \mathrm{d}\mu = \mathbb{1}\right\}$$

conditional max-entropy for continuous output alphabet:

$$H_{\max}(X|B)_\omega = 2\log\sup\left\{\int \sqrt{F(\omega_B^x, \sigma_B)}\mathrm{d}\mu(\mathrm{x}) : \right.$$
$$\left. \sigma_B \in \mathcal{S}(\mathcal{M}_B)\right\}$$

Investigation under way!

(jointly with F.Furrer, M.Berta, T.Franz, M.Christandl, M.Tomamichel)

Entropic quantities

conditional min-entropy for continuous output alphabet:

$$H_{\min}(X|B)_\omega = -\log\sup\left\{\int \omega_B^x(E_B^x)\mathrm{d}\mu(\mathrm{x}) : \right.$$

$$\left. E \in \mathcal{L}^\infty(X, \mathcal{M}_{B,+})\,,\ \int E_B^x \mathrm{d}\mu = \mathbb{1}\right\}$$

conditional max-entropy for continuous output alphabet:

$$H_{\max}(X|B)_\omega = 2\log\sup\left\{\int \sqrt{F(\omega_B^x, \sigma_B)}\mathrm{d}\mu(\mathrm{x}) : \right.$$

$$\left. \sigma_B \in \mathcal{S}(\mathcal{M}_B)\right\}$$

Investigation under way!

(jointly with F.Furrer, M.Berta, T.Franz, M.Christandl, M.Tomamichel)

Entropic quantities

conditional min-entropy for continuous output alphabet:

$$H_{\min}(X|B)_\omega = -\log\sup\left\{\int \omega_B^x(E_B^x)\mathrm{d}\mu(\mathrm{x}) : \right.$$
$$\left. E \in \mathcal{L}^\infty(X, \mathcal{M}_{B,+}),\ \int E_B^x \mathrm{d}\mu = \mathbb{1}\right\}$$

conditional max-entropy for continuous output alphabet:

$$H_{\max}(X|B)_\omega = 2\log\sup\left\{\int \sqrt{F(\omega_B^x, \sigma_B)}\mathrm{d}\mu(\mathrm{x}) : \right.$$
$$\left. \sigma_B \in \mathcal{S}(\mathcal{M}_B)\right\}$$

Investigation under way!

(jointly with F.Furrer, M.Berta, T.Franz, M.Christandl, M.Tomamichel)

Entropic quantities

conditional min-entropy for continuous output alphabet:

$$H_{\min}(X|B)_\omega = -\log \sup \left\{ \int \omega_B^x(E_B^x)\mathrm{d}\mu(\mathrm{x}) : \right.$$

$$\left. E \in \mathcal{L}^\infty(X, \mathcal{M}_{B,+}) \,, \; \int E_B^x \mathrm{d}\mu = \mathbb{1} \right\}$$

conditional max-entropy for continuous output alphabet:

$$H_{\max}(X|B)_\omega = 2\log \sup \left\{ \int \sqrt{F(\omega_B^x, \sigma_B)}\mathrm{d}\mu(\mathrm{x}) : \right.$$

$$\left. \sigma_B \in \mathcal{S}(\mathcal{M}_B) \right\}$$

Investigation under way!

(jointly with F.Furrer, M.Berta, T.Franz, M.Christandl, M.Tomamichel)

Entropic quantities

Cor: for classical A system the expression yields

$$\mathrm{H}_{\min}(X|B)_\omega = -\log p_{\mathrm{guess}}(X|B)_\omega$$

$$p_{\mathrm{guess}}(X|B)_\omega = \sup\{\sum_{x\in X} \omega_B^x(E_x) \ :$$

$$E_x \in \mathcal{M}_B,\ E_x \geq 0,\ \sum_x E_x = \mathbb{1}\}$$

Applications

operational meaning of smooth min-entropy
for classical A system: privacy amplification.

idea: Given a classical probability distribution (possibly correlated with some quantum system) with a promise on its (conditional) min-entropy. Map the alphabet to a smaller alphabet such that the distribution has maximal entropy (and is uncorrelated).

Applications

Thm: There exists a family of mappings $\mathcal{F} = \{ T_f : X \to K \}$, acting only on the classical system and reducing the alphabet size such that

$$\mathbb{E}_{\mathcal{F}} \| T_f \otimes \mathrm{id}(\omega_{XE}) - \tau_K \otimes \omega_E \| \leq \sqrt{|K| \cdot 2^{-\mathrm{H}_{\min}^{\epsilon}(X|E)_\omega}} + 4\epsilon$$

where τ_K is the state of maximal entropy. No restriction on the system E has to be made, in particular, no bound on the dimension.

Applications

$$\mathbb{E}_{\mathcal{F}} \| T_f \otimes \mathrm{id}(\omega_{XE}) - \tau_K \otimes \omega_E \| \leq \sqrt{|K| \cdot 2^{-\mathrm{H}^{\epsilon}_{\min}(X|E)_{\omega}}} + 4\epsilon$$

Remarks:

-> the conditional max-entropy corresponds to data compression with quantum side information.

-> extension to quantum case: replace classical system with quantum system and mappings by completely positive maps: under investigation, jointly with M.Berta, O.Szehr.

Applications

$$\mathbb{E}_{\mathcal{F}}\|T_f \otimes \mathrm{id}(\omega_{XE}) - \tau_K \otimes \omega_E\| \leq \sqrt{|K| \cdot 2^{-\mathrm{H}^{\epsilon}_{\min}(X|E)_{\omega}}} + 4\epsilon$$

Remarks:

-> the conditional max-entropy corresponds to data compression with quantum side information.

-> extension to quantum case: replace classical system with quantum system and mappings by completely positive maps: under investigation, jointly with M.Berta, O.Szehr.

Applications

Entropic uncertainty relations: measuring our uncertainty about measurements performed on quantum systems in terms of entropic quantities.

Applications

Entropic uncertainty relations: measuring our uncertainty about measurements performed on quantum systems in terms of entropic quantities.

Setup: tripartite quantum system ABC, subsystems modeled as commuting von Neumann algebras. Two measurements (POVM's) $\{E_A^x\}$, $\{F_A^y\}$ on subsystem A, with output alphabets X,Y. We start with some state ω on ABC and consider the two corresponding post-measurement states

Applications

Entropic uncertainty relations: measuring our uncertainty about measurements performed on quantum systems in terms of entropic quantities.

Setup: tripartite quantum system ABC, subsystems modeled as commuting von Neumann algebras. Two measurements (POVM's) $\{E_A^x\}$, $\{F_A^y\}$ on subsystem A, with output alphabets X,Y. We start with some state ω on ABC and consider the two corresponding post-measurement states

Applications

Entropic uncertainty relations: measuring our uncertainty about measurements performed on quantum systems in terms of entropic quantities.

Setup: tripartite quantum system ABC, subsystems modeled as commuting von Neumann algebras. Two measurements (POVM's) $\{E_A^x\}$, $\{F_A^y\}$ on subsystem A, with output alphabets X,Y. We start with some state ω on ABC and consider the two corresponding post-measurement states

$$\mathrm{H}_{\min}^{\epsilon}(X|B)_{\omega} + \mathrm{H}_{\max}^{\epsilon}(Y|C)_{\omega} \geq -\log \max_{x,y} \left\| (E_A^x)^{\frac{1}{2}} \cdot (F_A^y)^{\frac{1}{2}} \right\|^2$$

Applications

Entropic uncertainty relations: measuring our uncertainty about measurements performed on quantum systems in terms of entropic quantities.

Setup: tripartite quantum system ABC, subsystems modeled as commuting von Neumann algebras. Two measurements (POVM's) $\{E_A^x\}$, $\{F_A^y\}$ on subsystem A, with output alphabets X,Y. We start with some state ω on ABC and consider the two corresponding post-measurement states

$$\mathrm{H}_{\min}^{\epsilon}(X|B)_{\omega} + \mathrm{H}_{\max}^{\epsilon}(Y|C)_{\omega} \geq -\log \max_{x,y} \left\| (E_A^x)^{\frac{1}{2}} \cdot (F_A^y)^{\frac{1}{2}} \right\|^2$$

Applications

$$\mathrm{H}^{\epsilon}_{\min}(X|B)_{\omega} + \mathrm{H}^{\epsilon}_{\max}(Y|C)_{\omega} \geq -\log \max_{x,y} \left\| (E^x_A)^{\frac{1}{2}} \cdot (F^y_A)^{\frac{1}{2}} \right\|^2$$

Remarks:

-> extension to continuous alphabets and general Renyi entropies is under investigation (jointly with F.Furrer, M.Berta, T.Franz, M.Christandl, M.Tomamichel).

-> corresponding version for von Neumann entropy was recently shown by Lieb & Frank for finite dimensional side information.

Applications

Quantum Key distillation: start with two-partite quantum state on two commuting von Neumann algebras, think of the commutant of the purification as Eve's system. Alice performs one out of two complementary observables.

Goal: estimate min-entropy to do privacy amplification.

Idea: use uncertainty relation to bound min-entropy of Alice conditioned on Eve via max-entropy between Alice and Bob.

$$\mathrm{H}^{\epsilon}_{\min}(X|E)_{\omega} \geq \mathrm{const} - \mathrm{H}^{\epsilon}_{\max}(Y|B)_{\omega}$$

Details in arXiv:1112.2179

Applications

Quantum Key distillation: start with two-partite quantum state on two commuting von Neumann algebras, think of the commutant of the purification as Eve's system. Alice performs one out of two complementary observables.

Goal: estimate min-entropy to do privacy amplification.

Idea: use uncertainty relation to bound min-entropy of Alice conditioned on Eve via max-entropy between Alice and Bob.

$$\mathrm{H}^{\epsilon}_{\min}(X|E)_{\omega} \geq \mathrm{const} - \mathrm{H}^{\epsilon}_{\max}(Y|B)_{\omega}$$

Details in arXiv:1112.2179

Outlook

-> conditional entropies for continuous output alphabets and corresponding uncertainty relations.

-> investigate the possibility of less or no restrictions on the A system

-> consider quantum statistical systems?

Outlook

-> conditional entropies for continuous output alphabets and corresponding uncertainty relations.

-> investigate the possibility of less or no restrictions on the A system

-> consider quantum statistical systems?