Device-independent uncertainty relations for binary observables

Jed Kaniewski, Marco Tomamichel, Stephanie Wehner

Centre for Quantum Technologies, National University of Singapore, Singapore

Phys. Rev. A **90**, 012332
(arXiv:1402.5722)

QCrypt'14, Paris, France
3 September 2014

Centre for Quantum Technologies
National University of Singapore

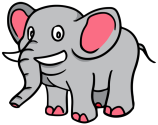
Outline

Outline

- (Mini-)**Framework** for uncertainty relations
- Binary observables and **anti-commutation**
- Partial anti-commutation, **ellipsoid condition** and **entropic uncertainty** (**technical**)
- Summary: simple procedure for **device-independent** uncertainty
- **Two** open questions

The Zoo of Uncertainty Relations

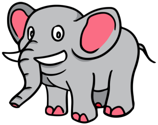
The Zoo of Uncertainty Relations



$$\sigma_X \sigma_P \geq \frac{\hbar}{2}$$

(Heisenberg, 1927)

The Zoo of Uncertainty Relations



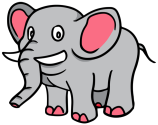
$$\sigma_X \sigma_P \geq \frac{\hbar}{2}$$

(Heisenberg, 1927)

$$\sigma_A \sigma_B \geq \frac{1}{2} \left| \langle [A, B] \rangle \right|$$

(Robertson, 1929)

The Zoo of Uncertainty Relations



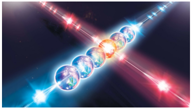
$$\sigma_X \sigma_P \geq \frac{\hbar}{2}$$
(Heisenberg, 1927)

$$\sigma_A \sigma_B \geq \frac{1}{2}\left|\langle [A, B] \rangle\right|$$
(Robertson, 1929)

$$H(X) + H(Z) \geq -\frac{1}{2} \log c$$
(Maassen-Uffink, 1988)

and many more. . .

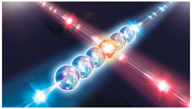
What is an uncertainty relation?



ρ

What is an uncertainty relation?

M_1

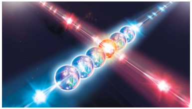


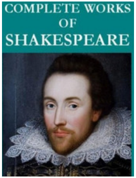
ρ

What is an uncertainty relation?

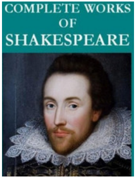
M_1

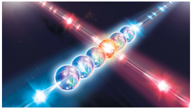
$\rho \longrightarrow \rho_{X_1}$





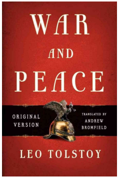
What is an uncertainty relation?



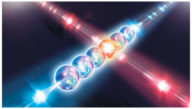


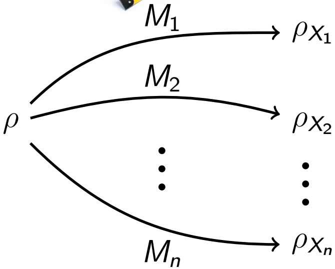
$$\rho \xrightarrow{M_1} \rho_{X_1}$$

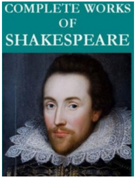
$$\rho \xrightarrow{M_2} \rho_{X_2}$$

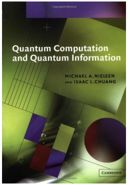


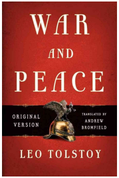
What is an uncertainty relation?



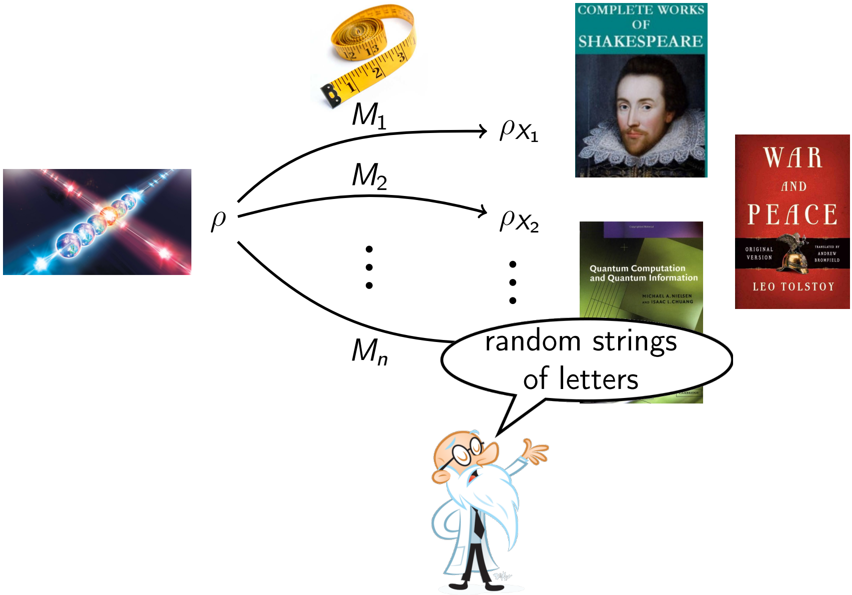




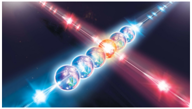


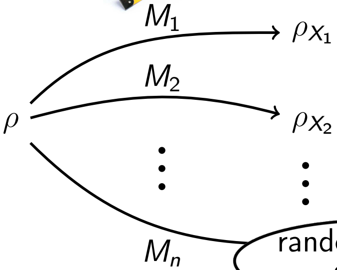


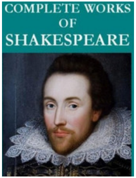
What is an uncertainty relation?

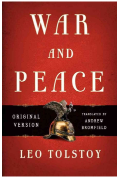


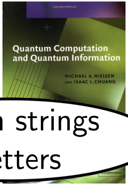
What is an uncertainty relation?

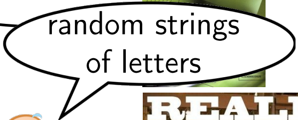




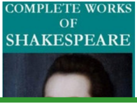


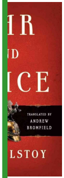






What is an uncertainty relation?



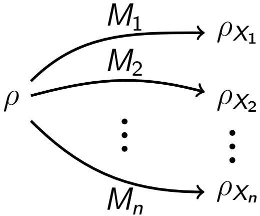


Any statement which relates the
properties of ρ and $M_1, M_2, \ldots$
with the
non-determinism of the outcomes $\rho_{X_1}, \rho_{X_2}, \ldots$
is an **uncertainty relation**.

M_n

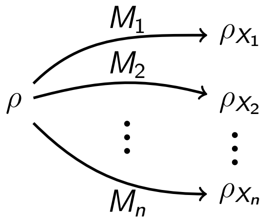
of letters

How to make it rigorous?



We need **3** components:

How to make it rigorous?

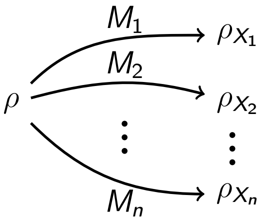


We need **3** components:

[1] A measure of incompatibility

$$\text{Inc} = f(\rho, M_1, M_2, \dots)$$

How to make it rigorous?

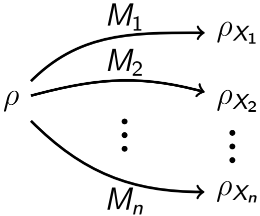


We need 3 components:

[1] A measure of incompatibility
$\text{Inc} = f(\rho, M_1, M_2, \ldots)$

[2] A measure of uncertainty
$\text{Unc} = g(\rho_{X_1}, \rho_{X_2}, \ldots)$

How to make it rigorous?



We need 3 components:

[1] A measure of incompatibility
$\mathrm{Inc} = f(\rho, M_1, M_2, \dots)$

[2] A measure of uncertainty
$\mathrm{Unc} = g(\rho_{X_1}, \rho_{X_2}, \dots)$

[3] A non-trivial relation between **[1]** and **[2]**
$\mathrm{Unc} \geq h(\mathrm{Inc})$

How to make it rigorous?

Warning! For every pair of measures there exists a well-defined trade-off, which can be found by solving the following minimisation problem for all admissible t:

$$\text{minimise} \quad \mathsf{Unc}$$
$$\text{over} \quad \rho, M_1, M_2, \ldots, M_n$$
$$\text{which satisfy} \quad \mathsf{Inc} = t$$

Are **all of them** interesting?

How to make it rigorous?

Warning! For every pair of measures there exists a well-defined trade-off, which can be found by solving the following minimisation problem for all admissible t:

$$\text{minimise} \quad \mathsf{Unc}$$
$$\text{over} \quad \rho, M_1, M_2, \ldots, M_n$$
$$\text{which satisfy} \quad \mathsf{Inc} = t$$

Are **all of them** interesting?

No!

What do we want? What makes us happy?

What do we want? What makes us happy?

Measure of incompatibility
Simple function of ρ and $M_1, M_2, \ldots$
easily verifiable, maybe
even **device-independently**?

What do we want? What makes us happy?

Measure of incompatibility
Simple function of ρ and $M_1, M_2, \ldots$
easily verifiable, maybe
even **device-independently**?

Measure of uncertainty
Invariant under physically irrelevant operations (e.g. permuting/relabelling the outcomes) and maybe even some **operational interpretation**?

What do we want? What makes us happy?

Measure of incompatibility

Simple function of ρ and $M_1, M_2, \ldots$ easily verifiable, maybe even **device-independently**?

Measure of uncertainty

Invariant under physically irrelevant operations (e.g. permuting/relabelling the outcomes) and maybe even some **operational interpretation**?

The relation

Neat mathematical formulation

The main object of study

A set of **multiple** **binary** measurements

The main object of study

(more than 2)

A set of **multiple** **binary** measurements

The main object of study

(more than 2) **(with two outcomes)**

A set of **multiple** **binary** measurements

The main object of study

(more than 2) **(with two outcomes)**

A set of **multiple** **binary** measurements

- The usual dimension reduction based on Jordan's lemma does not work for more than 2 measurements
- We want uncertainty based on measures that can be certified device-independently (e.g. no assumption on the dimension)
- This has been studied for a very special family of observables which are pairwise "maximally incompatible" [Wehner, Winter'08]. Can we provide a generalised statement that applies to an arbitrary set of binary observables?

Binary observables 101

A binary (projective) observable A:

$$A = A^\dagger \quad \text{and} \quad A^2 = \mathbb{1},$$

where $\mathbb{1}$ is the identity matrix.

Binary observables 101

A binary (projective) observable A:

$$A = A^\dagger \quad \text{and} \quad A^2 = \mathbb{1},$$

where $\mathbb{1}$ is the identity matrix.
Measuring A on ρ gives probability distribution $\{p(+1), p(-1)\}$
Two outcomes $\implies$ fully characterised by its **expectation value**

$$g = \mathrm{tr}(A\rho) = p(+1) - p(-1) \in [-1, 1].$$

Binary observables 101

A binary (projective) observable A:

$$A = A^\dagger \quad \text{and} \quad A^2 = \mathbb{1},$$

where $\mathbb{1}$ is the identity matrix.
Measuring A on ρ gives probability distribution $\{p(+1), p(-1)\}$
Two outcomes $\implies$ fully characterised by its **expectation value**

$$g = \mathrm{tr}(A\rho) = p(+1) - p(-1) \in [-1, 1].$$

Intuition: Anti-commutation (in the operator sense) is a signature of incompatibility, e.g. $\{\sigma_X, \sigma_Z\} = \sigma_X\sigma_Z + \sigma_Z\sigma_X = 0$.

Binary observables – intuition made rigorous

Theorem (Wehner, Winter'08)

Let $A_1, A_2, \ldots, A_n$ *be binary observables, which pairwise anti-commute* $\{A_j, A_k\} = 2\,\delta_{jk}\,\mathbb{1}$ *and let* $g \in [-1,1]^n$ *be a (column) vector of expectation values,* $g_j = \mathrm{tr}(A_j\rho)$*. For every* ρ *we have*

$$g^\mathsf{T} g = \sum_j g_j^2 \leq 1.$$

Binary observables – intuition made rigorous

Theorem (Wehner, Winter'08)

Let $A_1, A_2, \ldots, A_n$ be binary observables, which pairwise anti-commute $\{A_j, A_k\} = 2\,\delta_{jk}\,\mathbb{1}$ and let $g \in [-1,1]^n$ be a (column) vector of expectation values, $g_j = \operatorname{tr}(A_j \rho)$. For every ρ we have

$$g^{\mathsf{T}} g = \sum_j g_j^2 \leq 1.$$

Uncertainty relation in disguise!

anti-commutation of observables (measure of incompatibility)	$\Longrightarrow$	$\sum_j g_j^2 \leq 1$ (measure of uncertainty)

Binary observables – intuition made rigorous

Theorem (Wehner, Winter'08)

Let $A_1, A_2, \ldots, A_n$ be binary observables, which pairwise anti-commute $\{A_j, A_k\} = 2\,\delta_{jk}\,\mathbb{1}$ and let $g \in [-1,1]^n$ be a (column) vector of expectation values, $g_j = \mathrm{tr}(A_j \rho)$. For every ρ we have

$$g^\top g = \sum_j g_j^2 \leq 1.$$

Uncertainty relation in disguise!

anti-commutation of observables (measure of incompatibility) $\Longrightarrow$ $\sum_j g_j^2 \leq 1$ (measure of uncertainty)

Strong statement: if one is deterministic ($g_1 = \pm 1$), then everything else is uniform ($g_j = 0$ for $j \geq 2$)!

Binary observables – intuition made rigorous

Theorem (Wehner, Winter'08)

Let $A_1, A_2, \ldots, A_n$ be binary observables, which pairwise anti-commute $\{A_j, A_k\} = 2\,\delta_{jk}\,\mathbb{1}$ and let $g \in [-1,1]^n$ be a (column) vector of expectation values, $g_j = \mathrm{tr}(A_j \rho)$. For every ρ we have

$$g^{\mathsf{T}} g = \sum_j g_j^2 \leq 1.$$

Uncertainty relation in disguise!

anti-commutation of observables (measure of incompatibility) $\implies$ $\sum_j g_j^2 \leq 1$ (measure of uncertainty)

Strong statement: if one is deterministic ($g_1 = \pm 1$), then everything else is uniform ($g_j = 0$ for $j \geq 2$)!

What if the observables only **approximately** anti-commute?
How do we even quantify **partial** anti-commutation?

Partial anti-commutation

Effective anti-commutator of A_j and A_k:

$$\varepsilon_{jk} := \frac{1}{2}\,\mathrm{tr}(\{A_j, A_k\}\rho)$$

Note $\varepsilon_{jk} \in [-1, 1]$ and if $\{A_j, A_k\} = 0$ (operator sense) then $\varepsilon_{jk} = 0$ **for all** states.

Partial anti-commutation

Effective anti-commutator of A_j and A_k:

$$\varepsilon_{jk} := \frac{1}{2} \operatorname{tr}(\{A_j, A_k\}\rho)$$

Note $\varepsilon_{jk} \in [-1, 1]$ and if $\{A_j, A_k\} = 0$ (operator sense) then $\varepsilon_{jk} = 0$ **for all** states.

Anti-commutation matrix:

$$T := \begin{pmatrix} 1 & \varepsilon_{12} & \cdot & \varepsilon_{1n} \\ \varepsilon_{12} & 1 & \cdot & \varepsilon_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \varepsilon_{1n} & \varepsilon_{2n} & \cdot & 1 \end{pmatrix}$$

Partial anti-commutation

Effective anti-commutator of A_j and A_k:

$$\varepsilon_{jk} := \frac{1}{2}\,\mathrm{tr}(\{A_j, A_k\}\rho)$$

Note $\varepsilon_{jk} \in [-1, 1]$ and if $\{A_j, A_k\} = 0$ (operator sense) then $\varepsilon_{jk} = 0$ **for all** states.

Anti-commutation matrix:

$$T := \begin{pmatrix} 1 & \varepsilon_{12} & \cdot & \varepsilon_{1n} \\ \varepsilon_{12} & 1 & \cdot & \varepsilon_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ \varepsilon_{1n} & \varepsilon_{2n} & \cdot & 1 \end{pmatrix}$$

If $\{A_j, A_k\} = 0$ for all $j \neq k$ then $T = \mathbb{1}$

exactly the case considered in [WW'08].

Partial anti-commutation

Theorem

A vector of expectation values g and an anti-commutation matrix T are compatible iff

$$gg^{\mathsf{T}} \leq T.$$

Proof: Suppose $\rho = |\psi\rangle\langle\psi|$ and consider $x_0 = |\psi\rangle$, $x_j = A_j|\psi\rangle$ for $j = 1, 2, \ldots, n$. The Gram matrix of $\{x_0, x_1, \ldots, x_n\}$ is

$$G = \begin{pmatrix} 1 & g^{\mathsf{T}} \\ g & T \end{pmatrix} \geq 0 \quad \text{(by definition)}$$

Partial anti-commutation

Theorem

A vector of expectation values g and an anti-commutation matrix T are compatible iff

$$gg^{\intercal} \leq T.$$

Proof: Suppose $\rho = |\psi\rangle\langle\psi|$ and consider $x_0 = |\psi\rangle$, $x_j = A_j|\psi\rangle$ for $j = 1, 2, \ldots, n$. The Gram matrix of $\{x_0, x_1, \ldots, x_n\}$ is

$$G = \begin{pmatrix} 1 & g^{\intercal} \\ g & T \end{pmatrix} \geq 0 \quad \text{(by definition)}$$

Schur complement condition: if $A > 0$ and $X = \begin{pmatrix} A & B^{\intercal} \\ B & C \end{pmatrix}$ then $X \geq 0 \iff C - BA^{-1}B^{\intercal} \geq 0$.

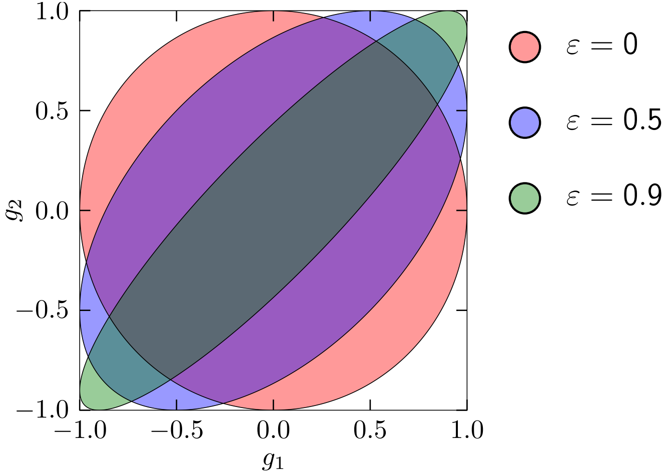
What the $gg^\intercal \preceq T$?

Geometric: T defines an **ellipsoid**, g must lie **inside**

What the $gg^\intercal \leq T$?

Geometric: T defines an **ellipsoid**, g must lie **inside**

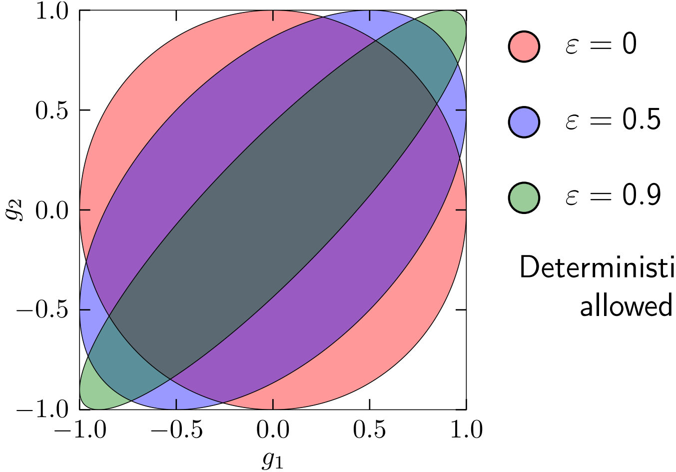
Example for 2 measurements
Allowed pairs (g_1, g_2) for fixed ε



What the $gg^\intercal \leq T$?

Geometric: T defines an **ellipsoid**, g must lie **inside**

Example for 2 measurements
Allowed pairs (g_1, g_2) for fixed ε

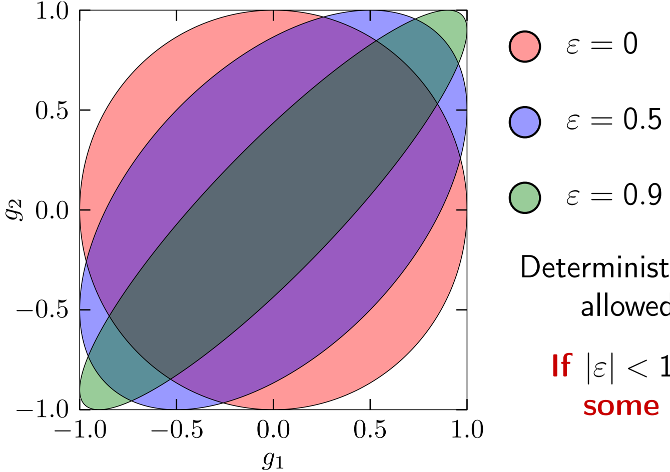


Deterministic $(g_1, g_2 = \pm 1)$
allowed **iff** $|\varepsilon| = 1$

What the $gg^\intercal \le T$?

Geometric: T defines an **ellipsoid**, g must lie **inside**

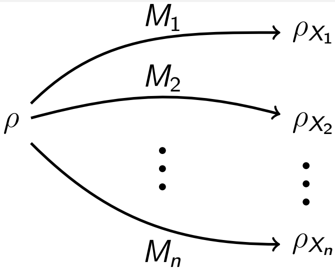
Example for 2 measurements
Allowed pairs (g_1, g_2) for fixed ε



Deterministic $(g_1, g_2 = \pm 1)$
allowed **iff** $|\varepsilon| = 1$

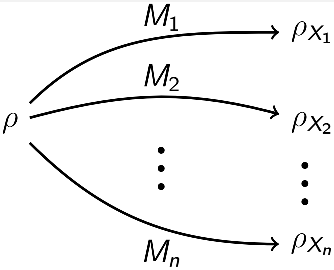
If $|\varepsilon| < 1$ then there is **some** uncertainty

But what about entropies?



But what about entropies?

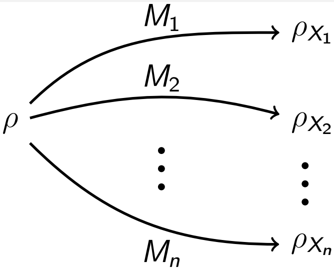
fair, n-sided coin
$\Pr[K = k] = \frac{1}{n}$



But what about entropies?

fair, n-sided coin

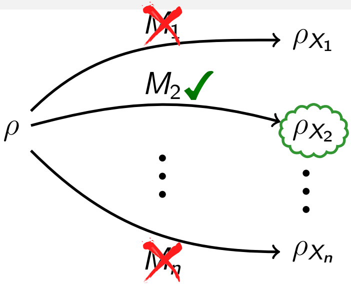
$\Pr[K = k] = \frac{1}{n}$



But what about entropies?

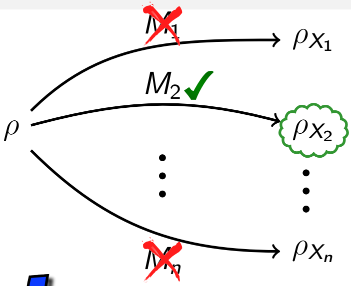
fair, n-sided coin

$\Pr[K = k] = \frac{1}{n}$



But what about entropies?

fair, n-sided coin
$\Pr[K = k] = \frac{1}{n}$

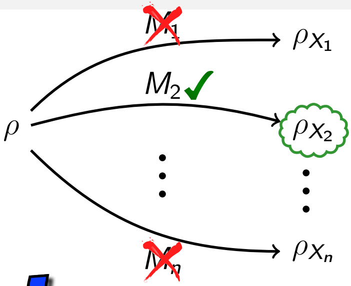


$$\rho_{XK} = \frac{1}{n} \sum_k \rho_{X_k} \otimes |k\rangle\langle k|$$

But what about entropies?

fair, n-sided coin

$\Pr[K = k] = \frac{1}{n}$



$$\rho_{XK} = \frac{1}{n} \sum_k \rho_{X_k} \otimes |k\rangle\langle k|$$

want to bound **α-Rényi entropy**

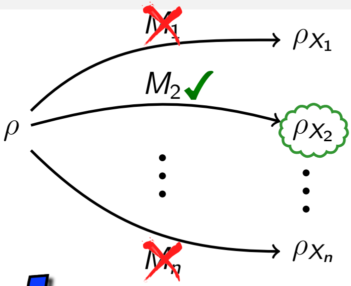
$$H_\alpha(X|K) = \frac{\alpha}{1-\alpha} \log \frac{\sum_k w_\alpha(g_k)}{n}$$

where $w_\alpha(g) = \left[\left(\frac{1+g}{2} \right)^\alpha + \left(\frac{1-g}{2} \right)^\alpha \right]^{1/\alpha}$

But what about entropies?

fair, n-sided coin

$\Pr[K = k] = \frac{1}{n}$



$$\rho_{XK} = \frac{1}{n} \sum_k \rho_{X_k} \otimes |k\rangle\langle k|$$

want to bound **α-Rényi entropy**

$$H_\alpha(X|K) = \frac{\alpha}{1-\alpha} \log \frac{\sum_k w_\alpha(g_k)}{n}$$

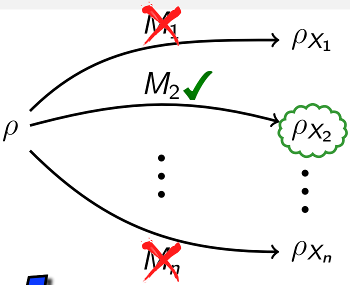
where $w_\alpha(g) = \left[\left(\frac{1+g}{2} \right)^\alpha + \left(\frac{1-g}{2} \right)^\alpha \right]^{1/\alpha}$

minimise $H_\alpha(X|K)$ over $gg^\intercal \leq T$

But what about entropies?

fair, n-sided coin

$\Pr[K = k] = \frac{1}{n}$



$$\rho_{XK} = \frac{1}{n} \sum_k \rho_{X_k} \otimes |k\rangle\langle k|$$

want to bound **α-Rényi entropy**

$$H_\alpha(X|K) = \frac{\alpha}{1-\alpha} \log \frac{\sum_k w_\alpha(g_k)}{n}$$

where $w_\alpha(g) = \left[\left(\frac{1+g}{2}\right)^\alpha + \left(\frac{1-g}{2}\right)^\alpha \right]^{1/\alpha}$

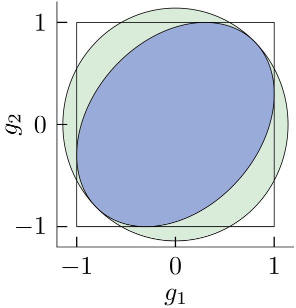
minimise $H_\alpha(X|K)$
over $gg^\intercal \leq T$

⋮

not **so** simple...

Spherical relaxation

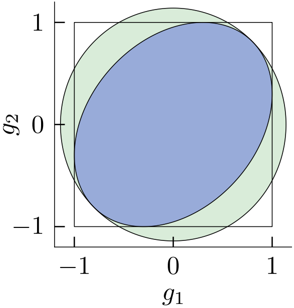
"bloat" the ellipsoid until it becomes a sphere...



radius $r = \|T\|_\infty$

Spherical relaxation

“bloat” the ellipsoid until it becomes a sphere. . .



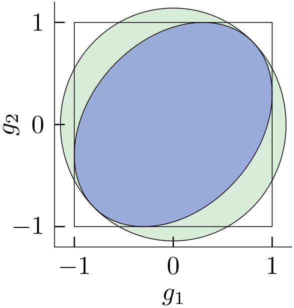
radius $r = \|T\|_\infty$

maximise $\sum_k w_\alpha(g_k)$
over $gg^\top \leq T$

maximise $\sum_k w_\alpha(g_k)$
over $g \in [-1, 1]^n, \sum_k g_k^2 \leq r$

Spherical relaxation

"bloat" the ellipsoid until it becomes a sphere...



radius $r = \| T \|_\infty$

maximise $\sum_k w_\alpha(g_k)$
over $gg^\intercal \leq T$

maximise $\sum_k w_\alpha(g_k)$
over $g \in [-1, 1]^n, \sum_k g_k^2 \leq r$

maximise $\sum_k w_\alpha(\sqrt{t_k})$
over $t \in [0, 1]^n, \ \sum_k t_k \leq r$

Spherical relaxation

$$\text{maximise } \sum_k w_\alpha(\sqrt{t_k})$$
$$\text{over } t \in [0,1]^n, \ \sum_k t_k \le r$$

Spherical relaxation

$$\text{maximise } \sum_k w_\alpha(\sqrt{t_k})$$
$$\text{over } t \in [0,1]^n, \ \sum_k t_k \le r$$

for $\alpha \in [1, \frac{3}{2}]$
$w_\alpha(\sqrt{t})$ is **convex**

Spherical relaxation

$$\text{maximise } \sum_k w_\alpha(\sqrt{t_k})$$
$$\text{over } t \in [0,1]^n,\ \sum_k t_k \le r$$

for $\alpha \in [1, \frac{3}{2}]$
$w_\alpha(\sqrt{t})$ is **convex**

optimal to choose

$$t_k = \begin{cases} 1 & \text{for } 1 \le k \le \lfloor r \rfloor, \\ r - \lfloor r \rfloor & \text{for } k = \lfloor r \rfloor + 1, \\ 0 & \text{otherwise.} \end{cases}$$

Spherical relaxation

maximise $\sum_k w_\alpha(\sqrt{t_k})$
over $t \in [0,1]^n,\ \sum_k t_k \leq r$

for $\alpha \in [1, \frac{3}{2}]$
$w_\alpha(\sqrt{t})$ is **convex**

optimal to choose

$$t_k = \begin{cases} 1 & \text{for} \quad 1 \leq k \leq \lfloor r \rfloor, \\ r - \lfloor r \rfloor & \text{for} \quad k = \lfloor r \rfloor + 1, \\ 0 & \text{otherwise.} \end{cases}$$

for $\alpha \in [2, \infty)$
$w_\alpha(\sqrt{t})$ is **concave**

optimal to choose

$$t_k = \frac{r}{n}$$

Spherical relaxation

$$\text{maximise } \sum_k w_\alpha(\sqrt{t_k})$$
$$\text{over } t \in [0,1]^n,\ \sum_k t_k \le r$$

for $\alpha \in [1, \frac{3}{2}]$

$w_\alpha(\sqrt{t})$ is **convex**

optimal to choose

$$t_k = \begin{cases} 1 & \text{for } \ 1 \le k \le \lfloor r \rfloor, \\ r - \lfloor r \rfloor & \text{for } \ k = \lfloor r \rfloor + 1, \\ 0 & \text{otherwise.} \end{cases}$$

for $\alpha \in [2, \infty)$

$w_\alpha(\sqrt{t})$ is **concave**

optimal to choose

$$t_k = \frac{r}{n}$$

Explicit lower bounds on $H_\alpha(X|K)$

for $\alpha \in [1, \frac{3}{2}] \cup [2, \infty)$ in terms of $r = \|T\|_\infty$ only

How good is this?

For the Shannon ($\alpha \to 1$) entropy for two measurements (**no assumptions on the dimension!**) we get:

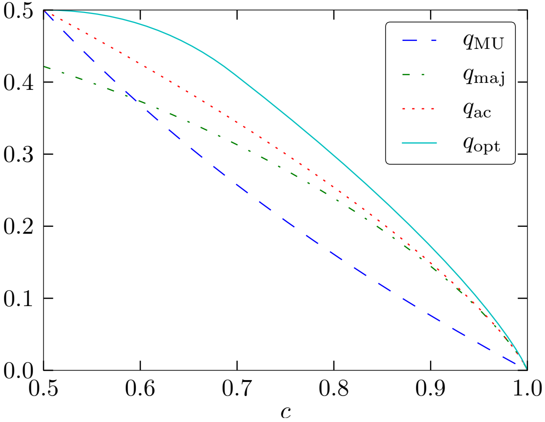
$$H(X|K) \geq \frac{1}{2} h_{\text{bin}}\left(\frac{1+\sqrt{|\varepsilon|}}{2}\right)$$

How good is this?

For the Shannon ($\alpha \to 1$) entropy for two measurements (**no assumptions on the dimension!**) we get:

$$H(X|K) \geq \frac{1}{2} h_{\text{bin}}\left(\frac{1+\sqrt{|\varepsilon|}}{2}\right)$$

qubit version known (Sánchez-Ruiz'05)



for two projective measurements on a qubit $c = \frac{1+|\varepsilon|}{2}$

Uncertainty can be certified device-independently!

A_j and A_k give CHSH violation of β_{jk} $\Rightarrow$ $|\varepsilon_{jk}| \leq \frac{\beta_{jk}}{4}\sqrt{8-\beta_{jk}^2}$

[Tomamichel, Hänggi'13]

Certification procedure

(based on a game proposed by Slofstra)

- For every pair (j,k) play a distinct CHSH game to estimate β_{jk} (need **i.i.d. assumption**) and calculate a bound on $|\varepsilon_{jk}|$
- Compute a bound on $\|T\|_\infty$
- Use $\|T\|_\infty$ to find explicit lower bounds on $H_\alpha(X|K)$
- Be uncertain about the outcome

Uncertainty can be certified device-independently!

A_j and A_k give CHSH violation of β_{jk} ➡ $|\varepsilon_{jk}| \leq \frac{\beta_{jk}}{4}\sqrt{8 - \beta_{jk}^2}$

[Tomamichel, Hänggi'13]

Certification procedure

(based on a game proposed by Slofstra)

- For every pair (j, k) play a distinct CHSH game to estimate β_{jk} (need **i.i.d. assumption**) and calculate a bound on $|\varepsilon_{jk}|$
- Compute a bound on $\|T\|_\infty$
- Use $\|T\|_\infty$ to find explicit lower bounds on $H_\alpha(X|K)$
- Be uncertain about the outcome 🙂

Procedure is **robust**:

any CHSH violation implies **strictly positive** uncertainty

Open questions

- Applications to **cryptography**
  For the application we had in mind we need to condition on additional **classical information**. Under our current assumptions this is not possible. Impose some extra assumptions? Find applications for which conditioning is not necessary?

Open questions

- Applications to **cryptography**
  For the application we had in mind we need to condition on additional **classical information**. Under our current assumptions this is not possible. Impose some extra assumptions? Find applications for which conditioning is not necessary?
- Extension to **ternary** observables
  Projective measurements with three outcomes can be represented as unitary matrices with eigenvalues $\{1, \omega, \omega^2\}$ where $\omega = \exp(\frac{2\pi i}{3})$. Incompatible (mutually unbiased) measurements are known to satisfy "twisted anti-commutation relation": $Z_3 X_3 = \omega X_3 Z_3$. Can we generalise our techniques to cover this case?

Thanks for you attention!

The annoying counterexample

Consider

$$A_1 = \begin{pmatrix} \sigma_z & \\ & \sigma_z \end{pmatrix}, A_2 = \begin{pmatrix} \sigma_z & \\ & -\sigma_z \end{pmatrix}, \rho = \frac{1}{2} \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & 1 & \\ & & & 0 \end{pmatrix}.$$

Easy to verify that

$$\{A_1, A_2\} = 2 \begin{pmatrix} \mathbb{1} & \\ & -\mathbb{1} \end{pmatrix} \quad \text{and} \quad \varepsilon_{12} = 0.$$

This implies that uncertainty: $g_1^2 + g_2^2 \leq 1$. This is actually true: $g_1 = 1$ and $g_2 = 0$.
Unfortunately, if we are told in which 2-dimensional subspace we are, no more uncertainty remains...