Complementary Information Principle and Universal Uncertainty Regions

(arXiv:1908.07694)

Yunlong Xiao[1], Kun Fang[2] and Gilad Gour[1]

1. University of Calgary

2. DAMTP, University of Cambridge

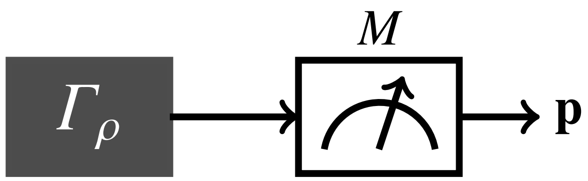
Presented at AQIS 2019, KIAS Seoul

UNIVERSITY OF CALGARY

UNIVERSITY OF CAMBRIDGE

A Bit of History

Physical scenario of preparational UR



A short history [see e.g. Coles-Berta-Tomamichel-Wehner'17, RMP]

- **1927, Heisenberg: (heuristic idea)** impossible to prepare a state such that its outcome probability distributions from the position and moment observables are both sharp.
- **1927, Kennard/ 1928, Weyl:** $\Delta(Q)\Delta(P) \geq \hbar/2$

- **1983, Deutsch:** $H(M) + H(N) \geq \text{const.}$
- **1988, Maassen-Uffink:** $H_\alpha(M) + H_\beta(N) \geq -\log c, \quad 1/\alpha + 1/\beta = 2$
- **2010, Berta-Christandl-Colbeck-Renes-Renner:** $H(M|B) + H(N|B) \geq -\log c + H(A|B)$

- **2011, Partovi/ 2013, Friedland-Gheorghiu-Gour:** $\mathbf{p} \otimes \mathbf{q} \prec \omega$

A Plethora of Applications

Uncertainty Relation

Determine → **Nonlocality**

e.g. Oppenheim, J. and Wehner, S., 2010. The uncertainty principle determines the nonlocality of quantum mechanics. *Science*, *330*(6007), pp.1072-1074.

Witness → **Entanglement**

e.g. Hofmann, H.F. and Takeuchi, S., 2003. Violation of local uncertainty relations as a signature of entanglement. *Physical Review A*, *68*(3), p.032103.

Detect → **Non-Markovianity**

e.g. Maity, A.G., Bhattacharya, S. and Maujmdar, A.S., 2019. Detecting non-Markovianity via uncertainty relations. *arXiv preprint arXiv:1901.02372*.

Secure → **Quantum Cryptography/QKD**

e.g. Ng, N.H.Y., Berta, M. and Wehner, S., 2012. Min-entropy uncertainty relation for finite-size cryptography. *Physical Review A*, *86*(4), p.042315.

Certify → **Quantum Randomness**

e.g. Miller, C.A. and Shi, Y., 2016. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *Journal of the ACM (JACM)*, *63*(4), p.33.

Majorization as Uncertainty Measure

How to quantify "uncertainty"?

1. Standard deviation, drawback: change under relabeling;
2. Entropy, no fundamental reason which entropy to use.

Axiomatic approach (Two intuitive assumptions):

1. Uncertainty should not be changed by relabeling (permutation);

$$(0.3, 0.6, 0.1) \text{ v.s. } (0.1, 0.3, 0.6)$$

2. Uncertainty should not be decreased by forgetting information (discarding).

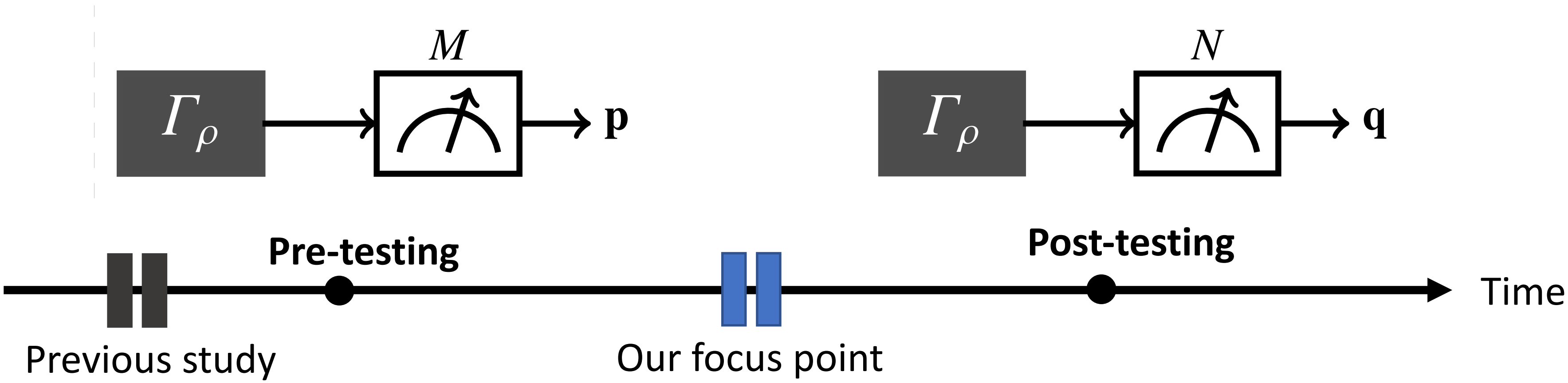
$$r\mathbf{p} + (1-r)\pi\mathbf{p} \text{ should be more uncertain than } \mathbf{p} (\text{ or } \pi\mathbf{p})$$

[Friedland-Gheorghiu-Gour'13]

majorization is the most nature choice of uncertainty order;
any measure of uncertainty has to preserve the partial order induced by majorization,
i.e. any Schur-concave function is a valid uncertainty measure .

$$\mathbf{x} \prec \mathbf{y} \Longleftrightarrow \sum_{j=1}^{k} x_j^{\downarrow} \leq \sum_{j=1}^{k} y_j^{\downarrow}, \quad \forall k$$

Main Result



Question: Given the ***information gain*** from the pre-testing, what is the ***uncertainty*** of the post-testing before it is actually performed?

Complementary Information Principle

Let $M = \{|u_j\rangle\}_{j=1}^n$ and $N = \{|v_\ell\rangle\}_{\ell=1}^n$ be the measurements of pre- and post-testing respectively. If the pre-testing outcome probability is given by $\mathbf{p} = (c_j)_{j=1}^n$, then the post-testing outcome probability $\mathbf{q}$ is bounded as $\mathbf{r} \prec \mathbf{q} \prec \mathbf{t}$.

1. **r** and **t** can be explicitly computed via semidefinite programs (SDPs).

   r : n independent SDPs of size n by n; **t** : 2^n independent SDPs of size n by n.

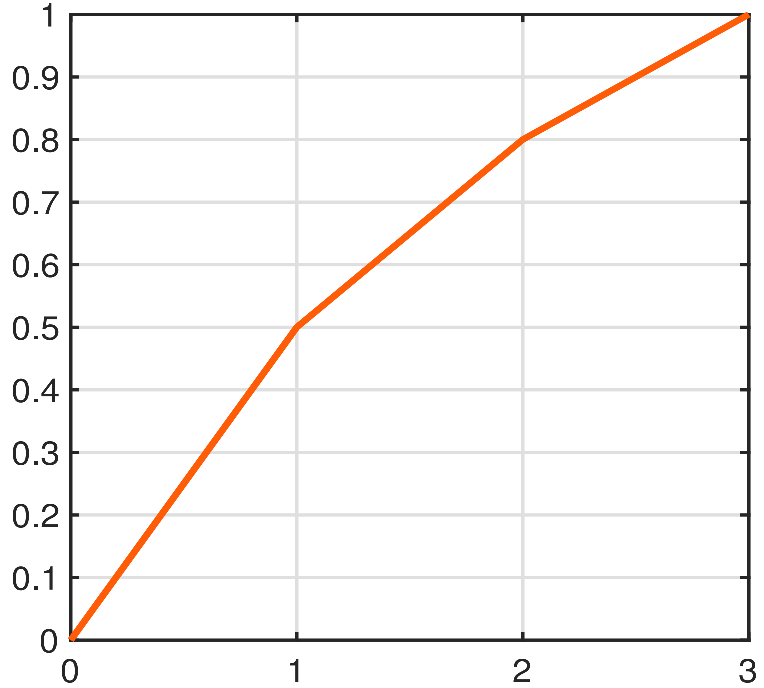
2. **r** and **t** are both **unique** and **tight** in majorization!

$$\mathbf{x} \prec \mathbf{q} \prec \mathbf{y} \quad \Longrightarrow \mathbf{x} \prec \mathbf{r} \prec \mathbf{q} \prec \mathbf{t} \prec \mathbf{y}$$

Lorenz Curve

$\boldsymbol{x} = (x_i)_{i=1}^n$ in non-increasing order **Lorenz curve** $\mathcal{L}(\boldsymbol{x}) = \left\{ \left(k, \sum_{i=1}^k x_i \right) \right\}_{k=0}^n$

$$\boldsymbol{x} = (0.5, 0.3, 0.2) \qquad \mathcal{L}(\boldsymbol{x}) = \{(0,0), (1, 0.5), (2, 0.8), (3, 1)\}$$



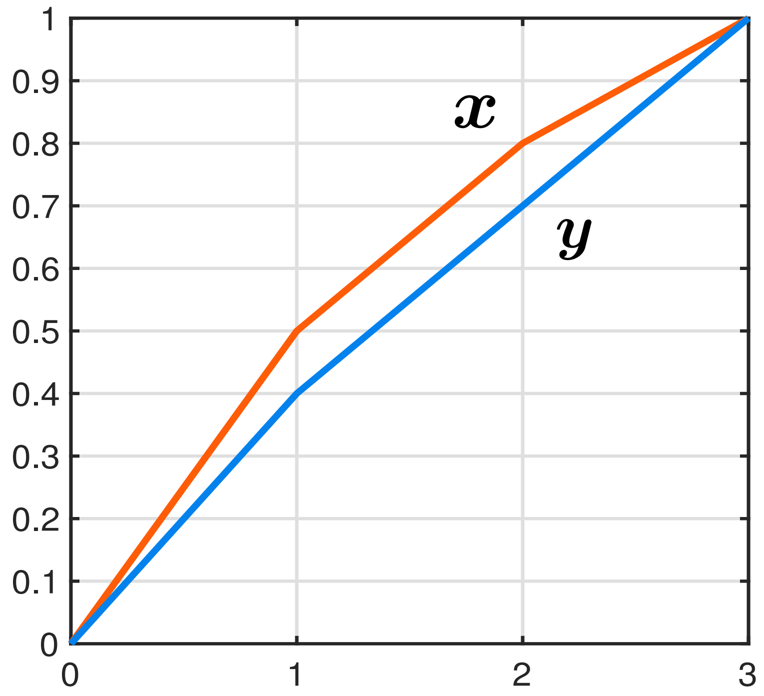
Lorenz Curve

$\boldsymbol{x} = (x_i)_{i=1}^n$ in non-increasing order **Lorenz curve** $\mathcal{L}(\boldsymbol{x}) = \left\{ \left(k, \sum_{i=1}^{k} x_i \right) \right\}_{k=0}^{n}$

$$\boldsymbol{x} = (0.5, 0.3, 0.2) \qquad \mathcal{L}(\boldsymbol{x}) = \{(0,0),(1,0.5),(2,0.8),(3,1)\}$$

$$\boldsymbol{y} = (0.4, 0.3, 0.3) \qquad \mathcal{L}(\boldsymbol{y}) = \{(0,0),(1,0.4),(2,0.7),(3,1)\}$$

Majorization relation $\boldsymbol{y} \prec \boldsymbol{x}$ if and only if $\mathcal{L}(\boldsymbol{y})$ is everywhere below $\mathcal{L}(\boldsymbol{x})$



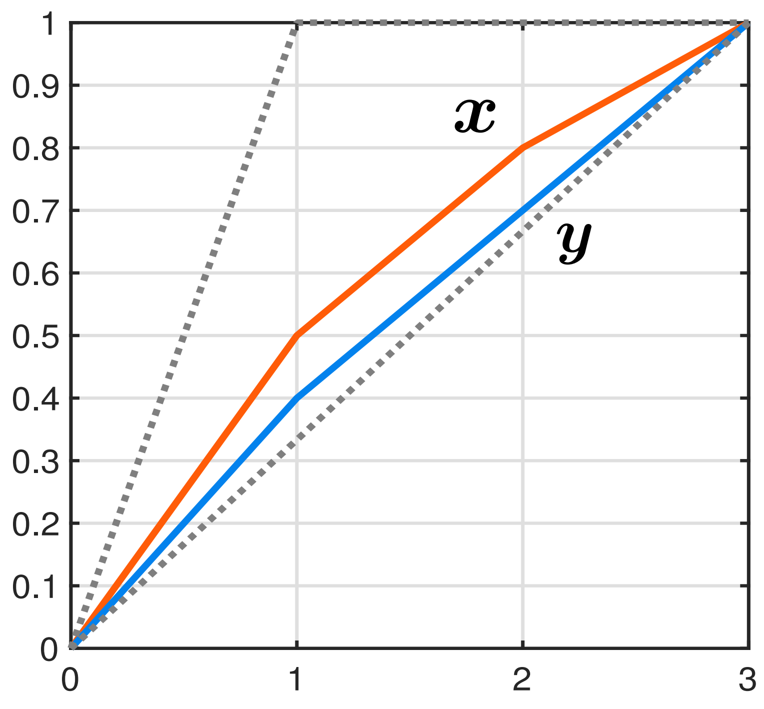
Lorenz Curve

$\boldsymbol{x} = (x_i)_{i=1}^n$ in non-increasing order **Lorenz curve** $\mathcal{L}(\boldsymbol{x}) = \left\{ \left(k, \sum_{i=1}^k x_i \right) \right\}_{k=0}^n$

$$\boldsymbol{x} = (0.5, 0.3, 0.2) \qquad \mathcal{L}(\boldsymbol{x}) = \{(0,0), (1,0.5), (2,0.8), (3,1)\}$$

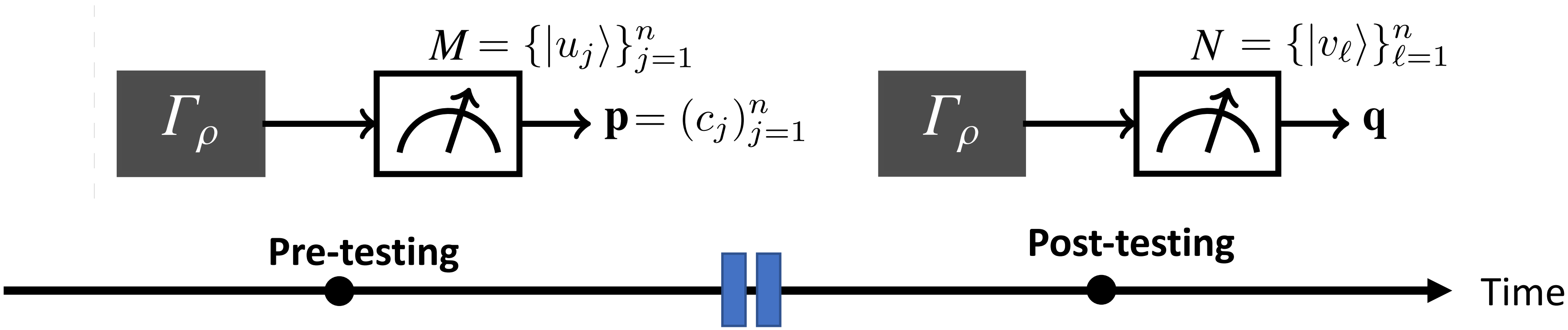
$$\boldsymbol{y} = (0.4, 0.3, 0.3) \qquad \mathcal{L}(\boldsymbol{y}) = \{(0,0), (1,0.4), (2,0.7), (3,1)\}$$

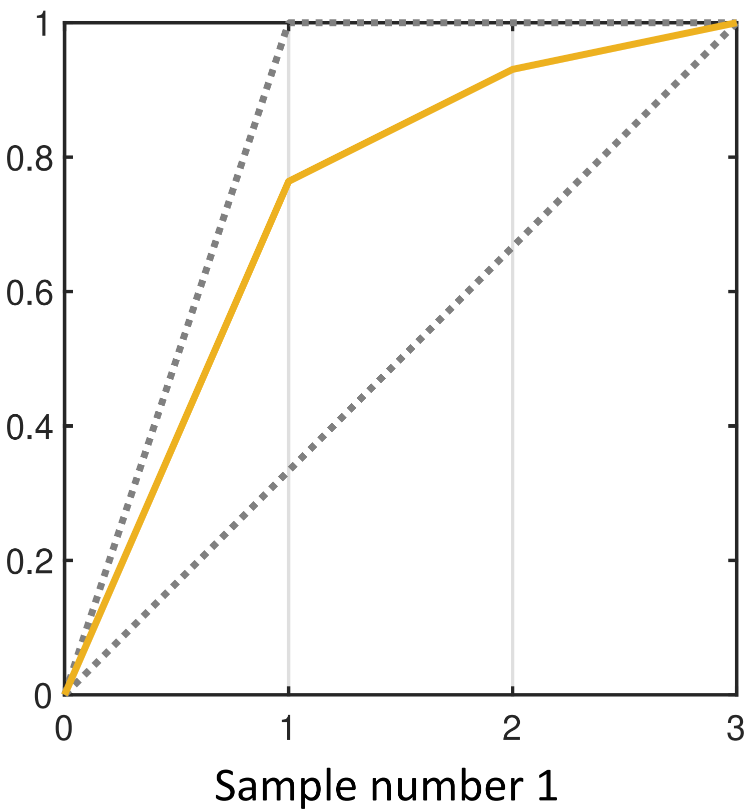
Majorization relation $\boldsymbol{y} \prec \boldsymbol{x}$ if and only if $\mathcal{L}(\boldsymbol{y})$ is everywhere below $\mathcal{L}(\boldsymbol{x})$



Remark:
a valid Lorenz curve is necessarily concave.

Proof Intuition

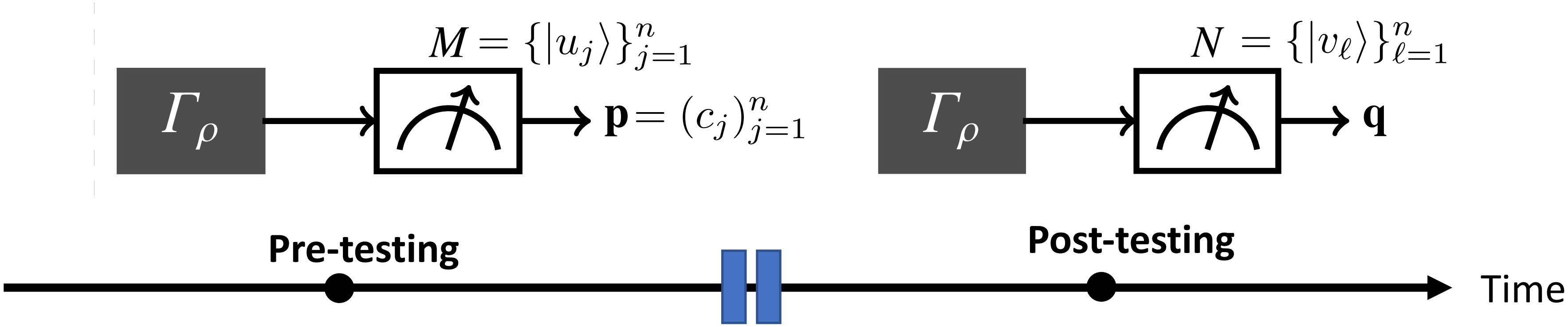


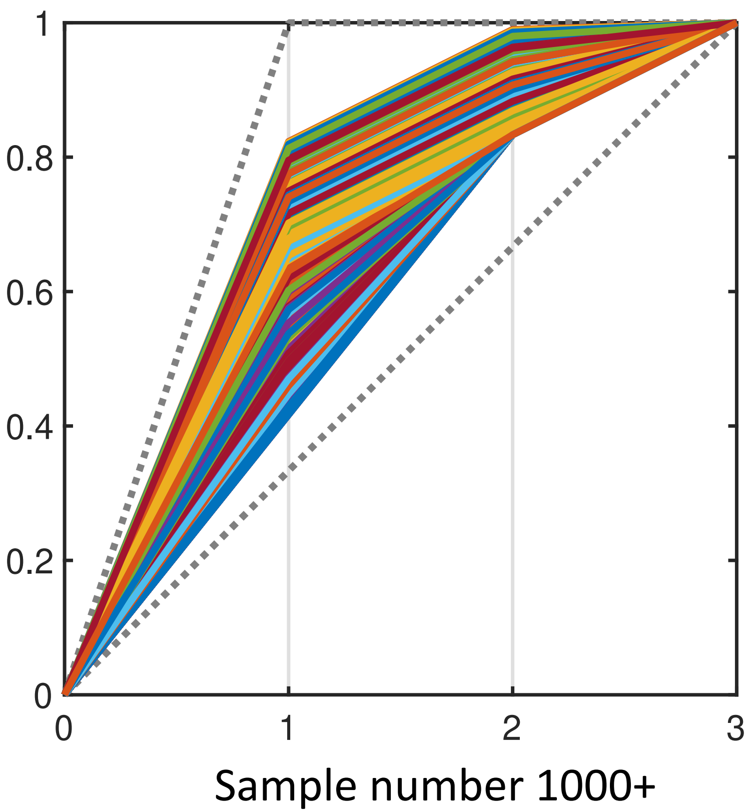


The set of states compatible with the pre-testing

$$S(M, \mathbf{p}) = \{\rho : \mathrm{Tr}\, |u_j\rangle\langle u_j| \rho = c_j, \forall j\}$$

Proof Intuition

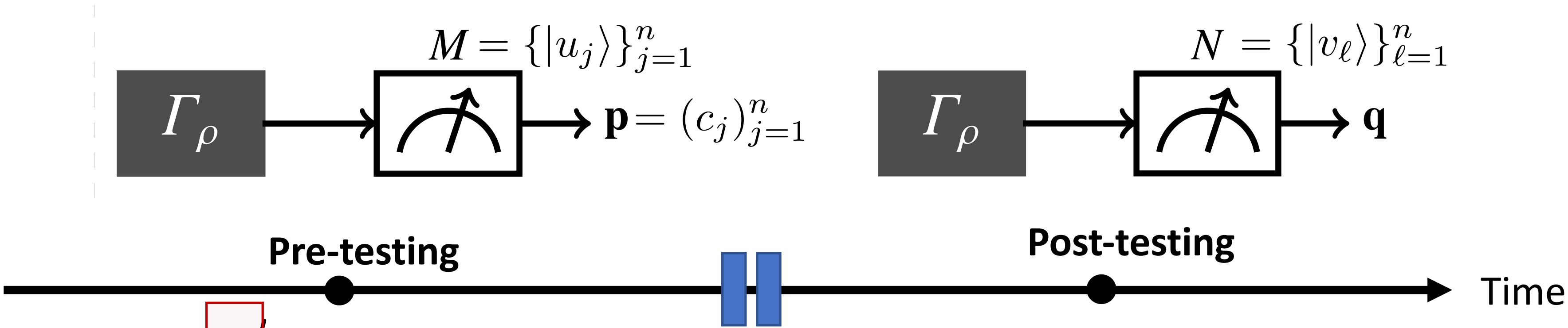


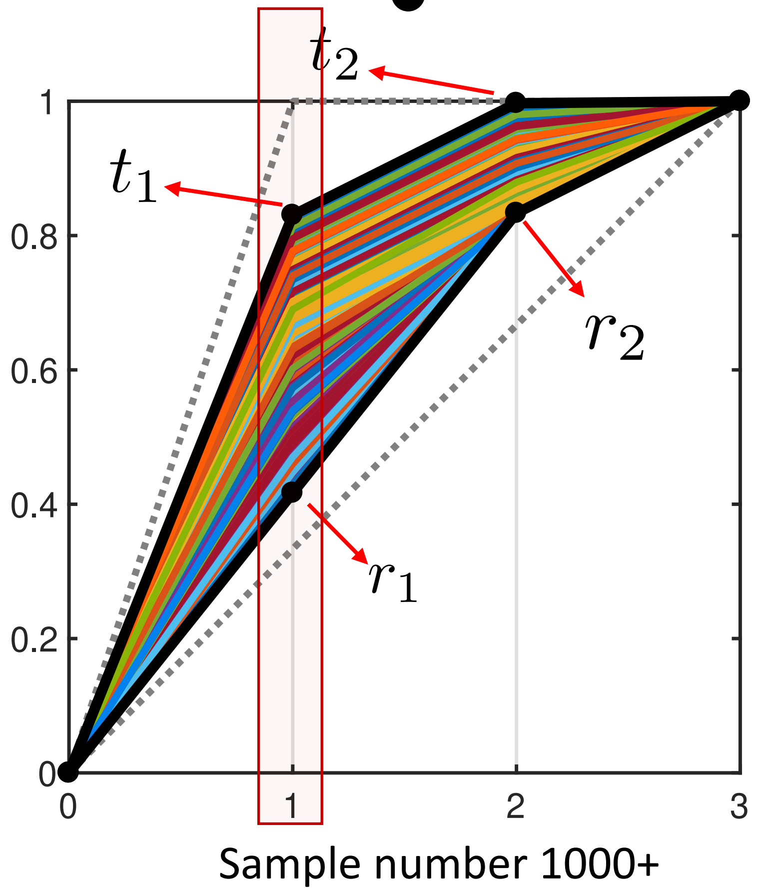


The set of states compatible with the pre-testing

$$S(M, \mathbf{p}) = \{\rho : \mathrm{Tr}\, |u_j\rangle\langle u_j| \rho = c_j, \forall j\}$$

Proof Intuition





The set of states compatible with the pre-testing

$$S(M, \mathbf{p}) = \{\rho : \mathrm{Tr}\, |u_j\rangle\langle u_j| \rho = c_j, \forall j\}$$

For given $\rho \in S(M, \mathbf{p})$, the largest partial sum of $\mathbf{q}$

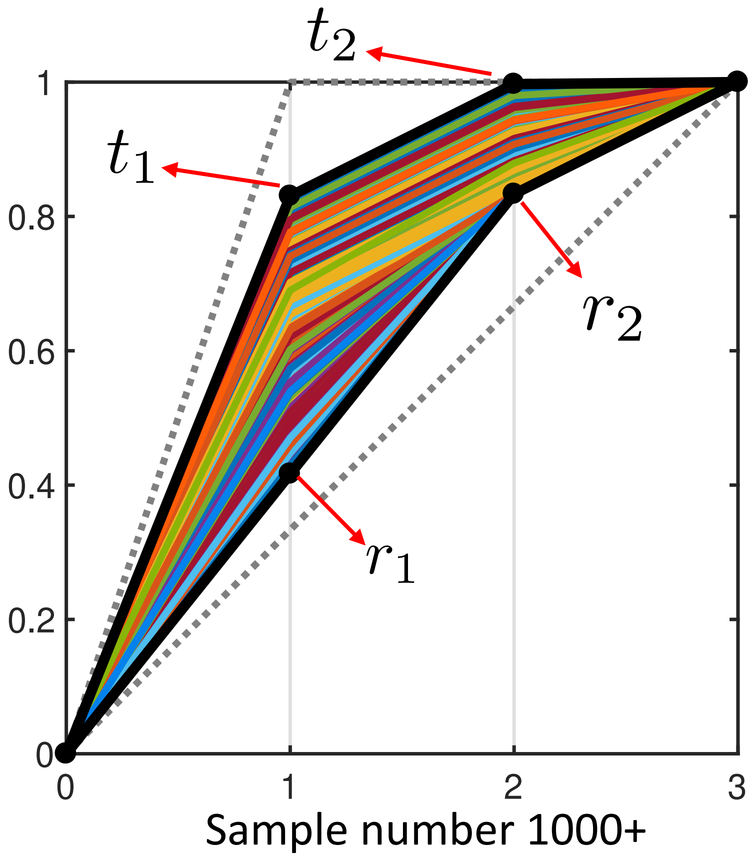
$$\max_{I_k \subset [n]} \mathrm{Tr}\, N_{I_k} \rho \qquad N_{I_k} = \sum_{\ell \in I_k} |v_\ell\rangle\langle v_\ell|$$

Find the boundary points:

$$r_k = \min_{\rho \in S(M,\mathbf{p})} \max_{I_k} \mathrm{Tr}\, N_{I_k} \rho$$

$$t_k = \max_{\rho \in S(M,\mathbf{p})} \max_{I_k} \mathrm{Tr}\, N_{I_k} \rho$$

Proof Intuition



The set of states compatible with the pre-testing

$$S(M,\mathbf{p}) = \{\rho : \mathrm{Tr}\,|u_j\rangle\langle u_j|\rho = c_j, \forall j\}$$

For given $\rho \in S(M,\mathbf{p})$, the largest partial sum of $\mathbf{q}$

$$\max_{I_k} \mathrm{Tr}\, N_{I_k}\rho \qquad N_{I_k} = \sum\nolimits_{\ell \in I_k} |v_\ell\rangle\langle v_\ell|$$

Find the boundary points:

$$r_k = \min_{\rho\in S(M,\mathbf{p})} \max_{I_k} \mathrm{Tr}\, N_{I_k}\rho$$

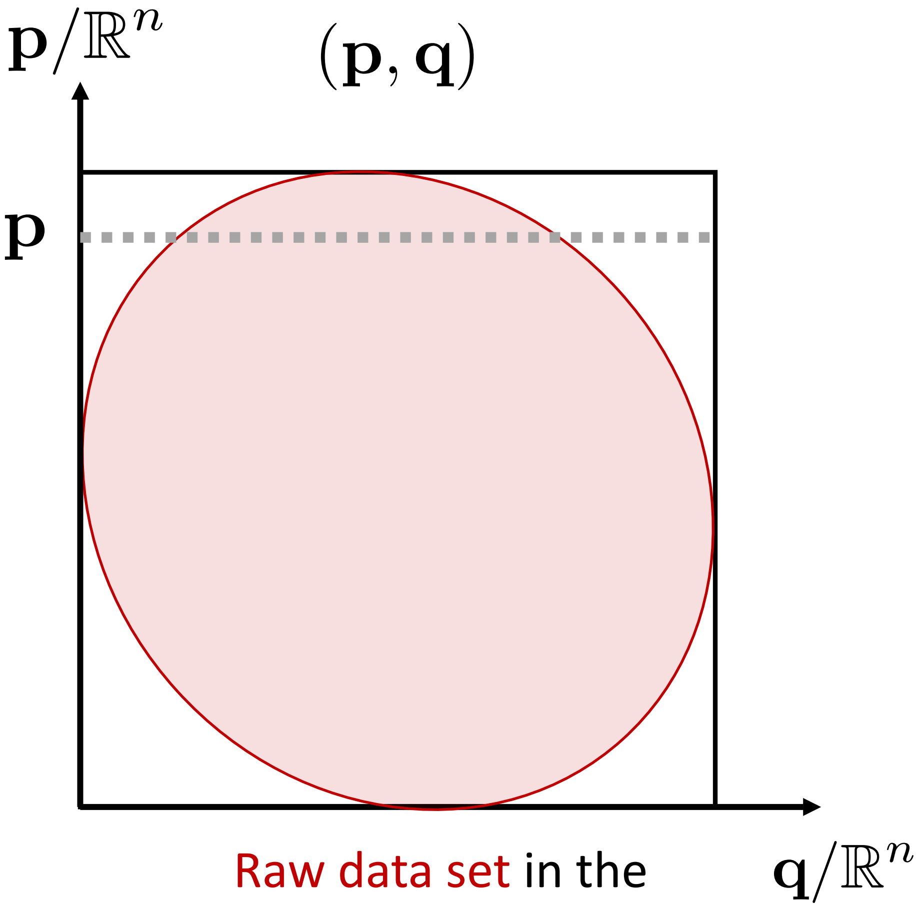
$$t_k = \max_{\rho\in S(M,\mathbf{p})} \max_{I_k} \mathrm{Tr}\, N_{I_k}\rho$$

Remarks:

1. $r_k = \min_{\rho\in S(M,\mathbf{p})} \max_{I_k} \mathrm{Tr}\, N_{I_k}\rho = \min_{\rho\in S(M,\mathbf{p})} \min\{x : x \geq \mathrm{Tr}\, N_{I_k}\rho, \forall I_k\}$

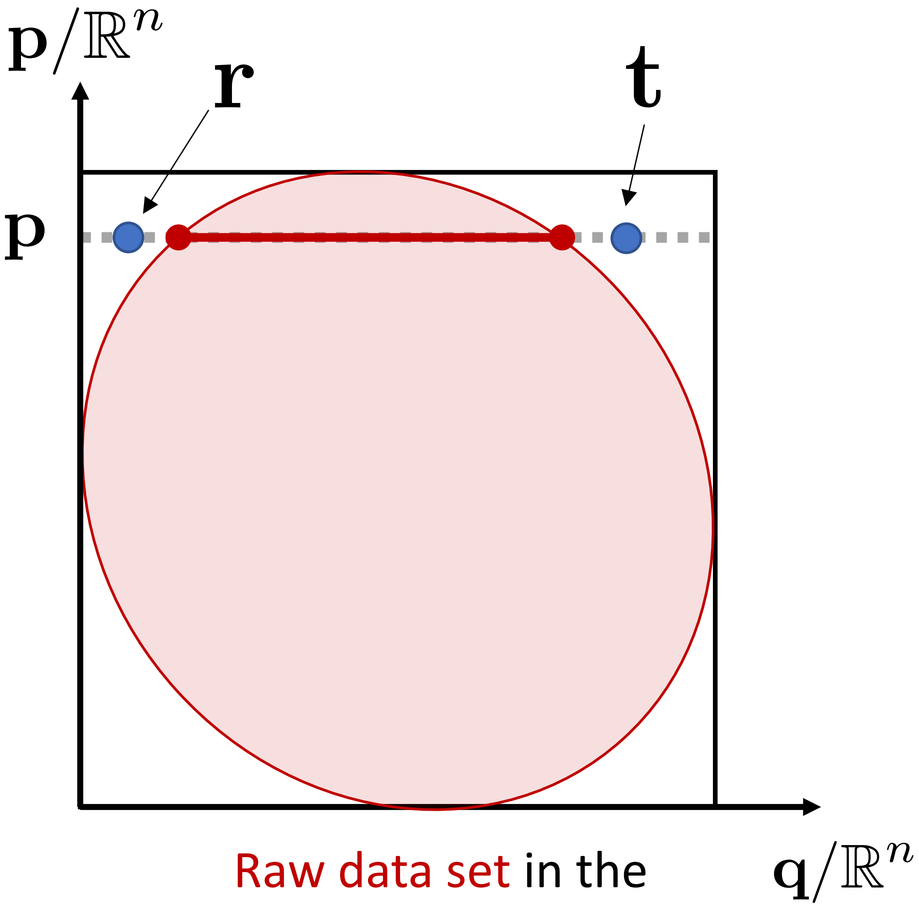
2. Upper boundary t_k is not necessarily concave, thus may not be a valid Lorenz curve. But we can construct a tightest concave curve above t_k by a standard process (*flatness process [see Cicalese- Vaccaro'02]*)

Application 1: Universal Uncertainty Region



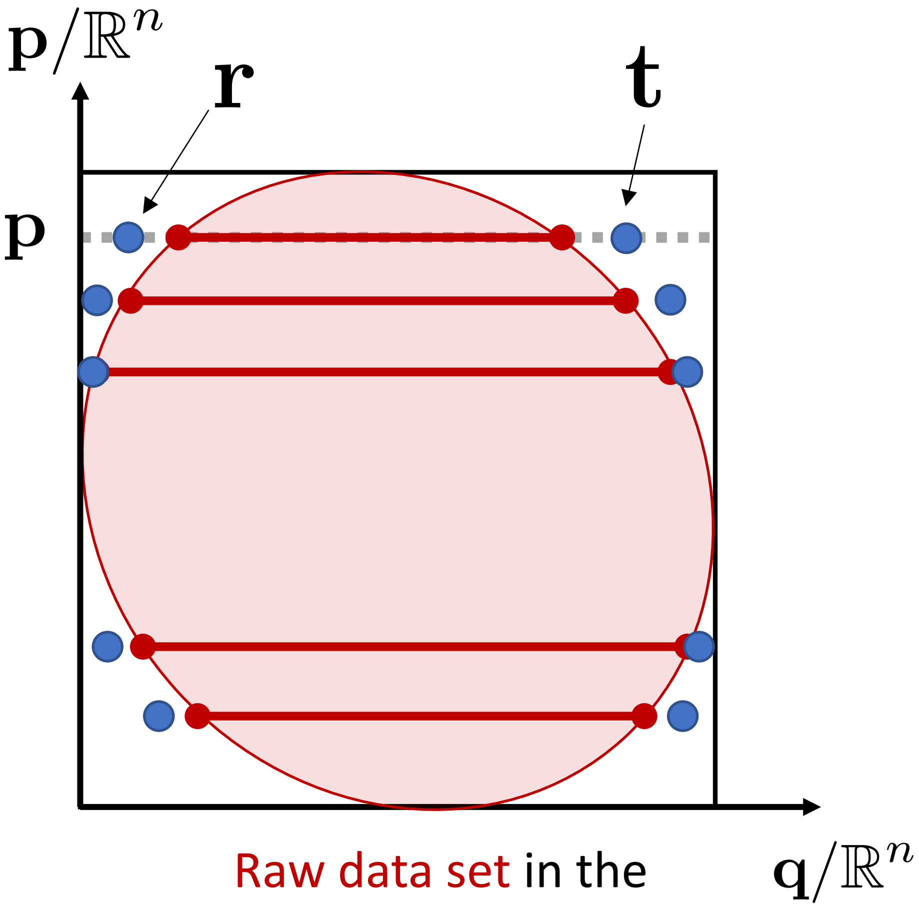
Raw data set in the
high dimensional space

Application 1: Universal Uncertainty Region



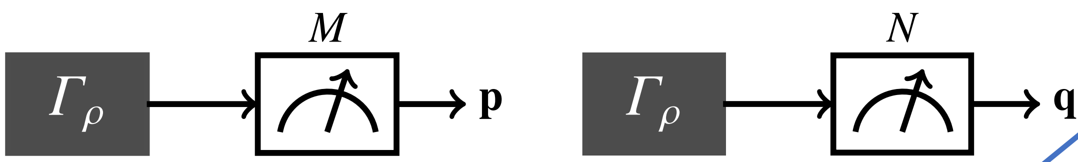
Raw data set in the
high dimensional space

Application 1: Universal Uncertainty Region



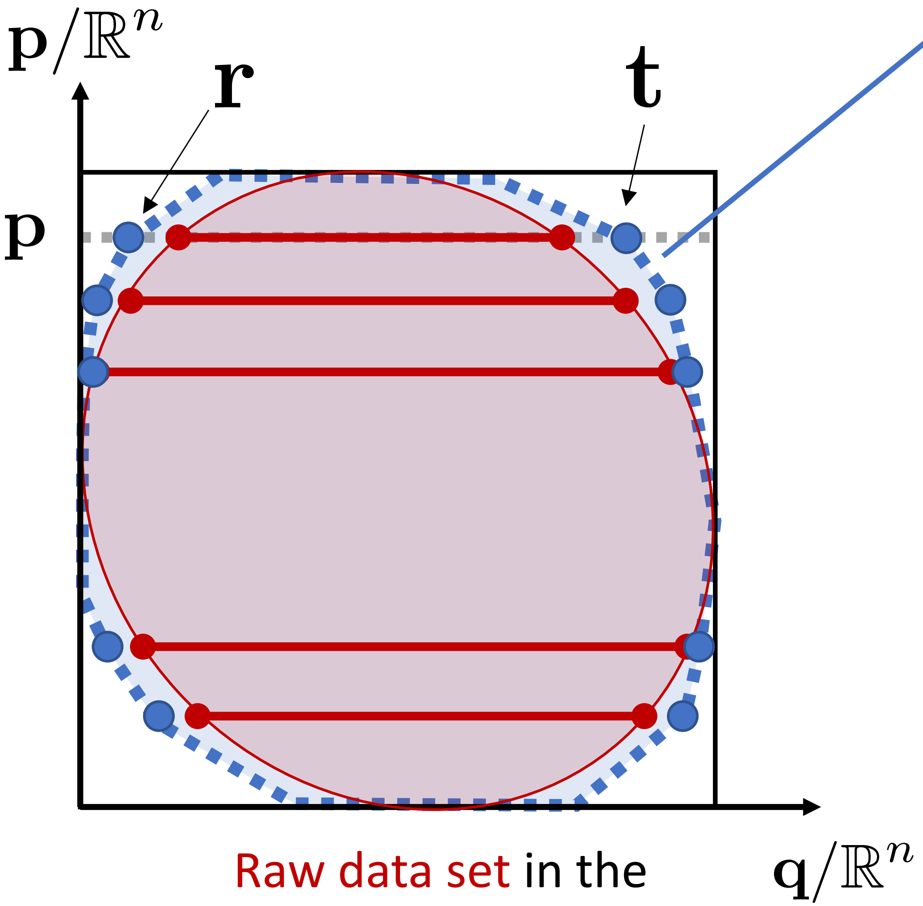
Raw data set in the high dimensional space

Application 1: Universal Uncertainty Region



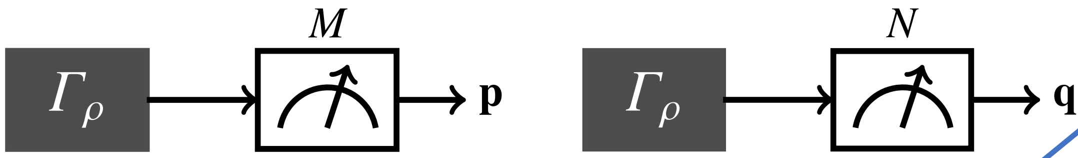
Universal Uncertainty Region (unique & tight in majorization)

Outer-approximation of the raw data set, coincide if n = 2



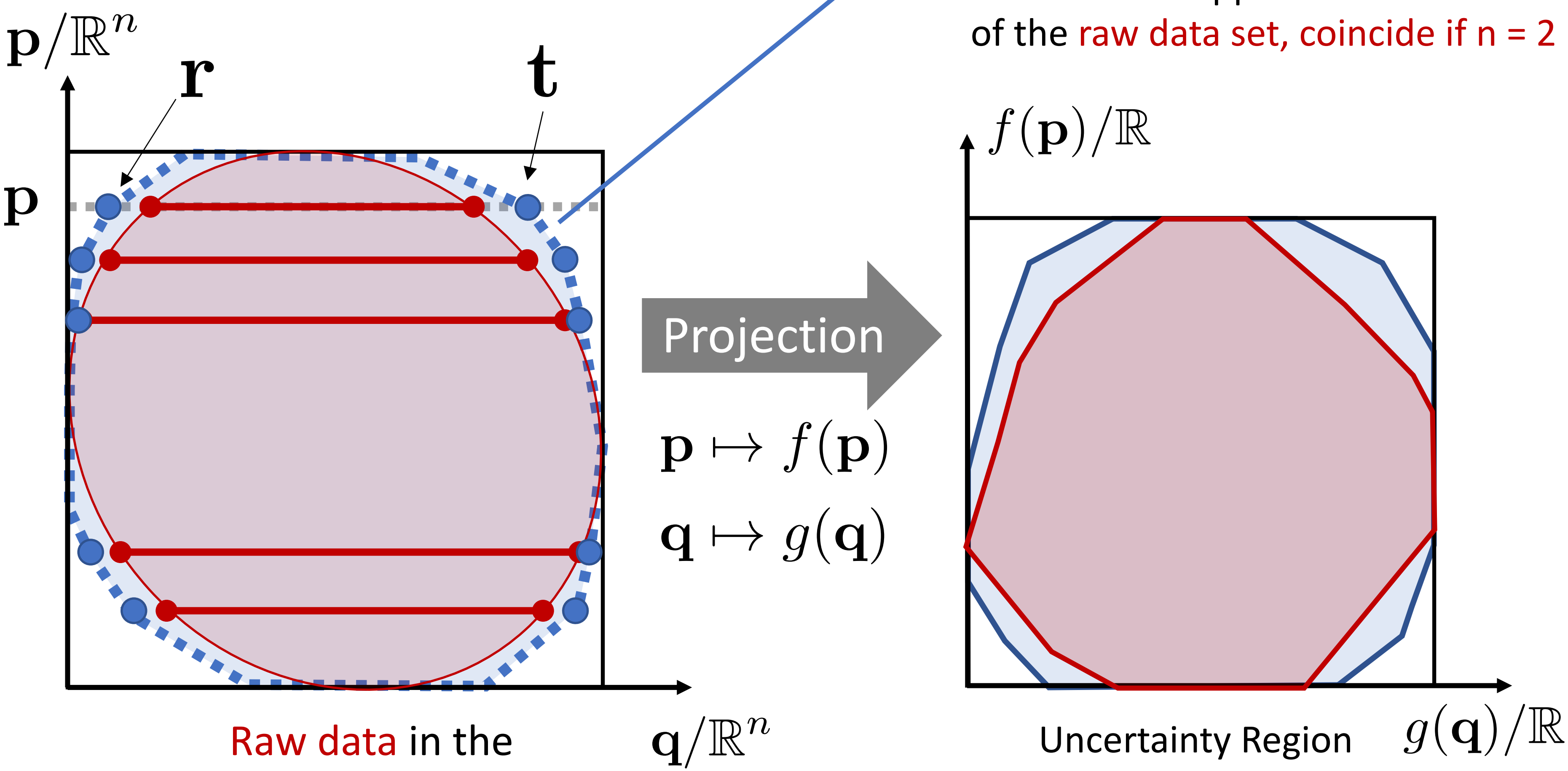
Raw data set in the high dimensional space

Application 1: Universal Uncertainty Region



Universal Uncertainty Region (unique & tight in majorization)

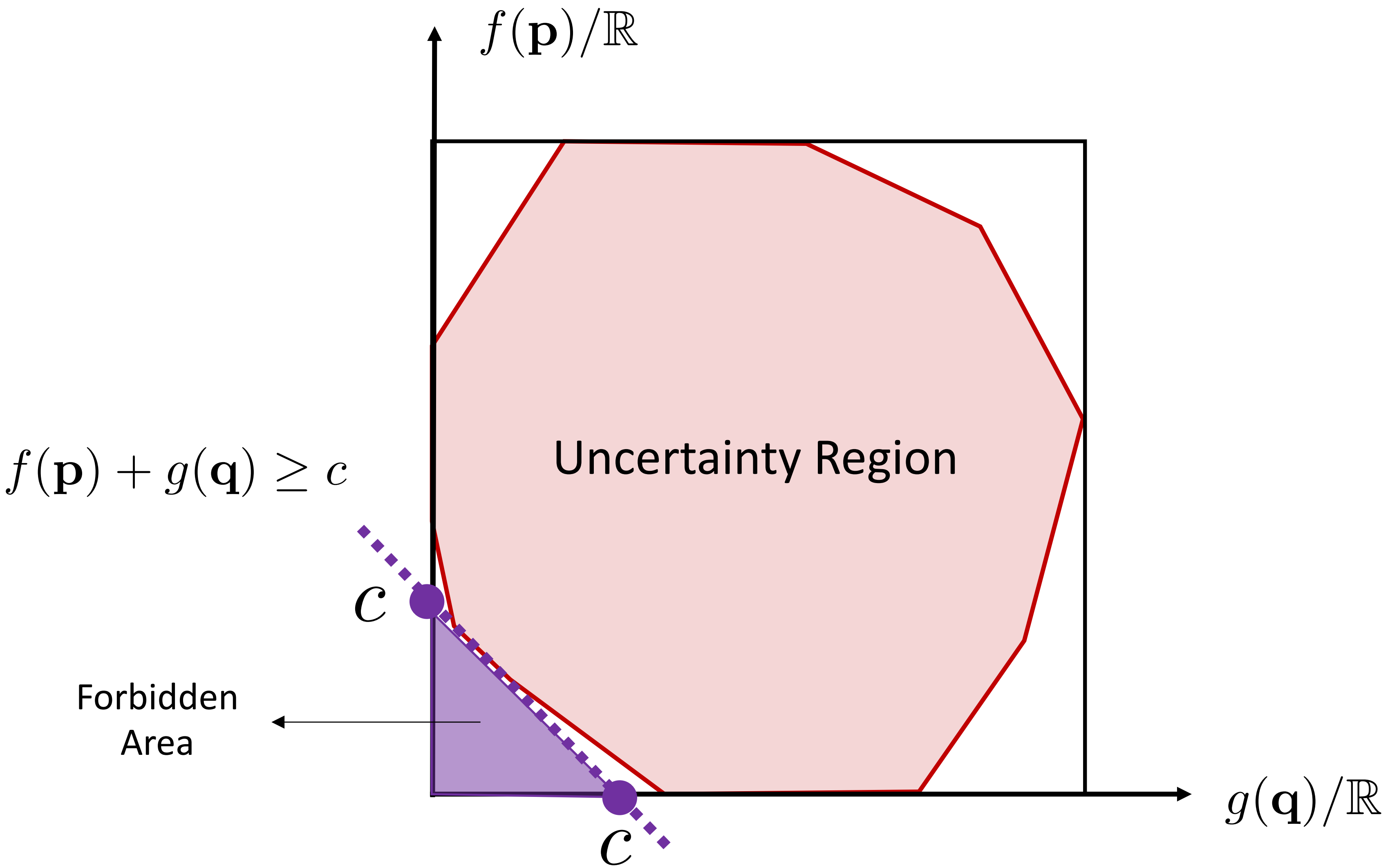
Outer-approximation of the raw data set, coincide if n = 2



Raw data in the high dimensional space

Uncertainty Region

Uncertainty Region and Uncertainty relation



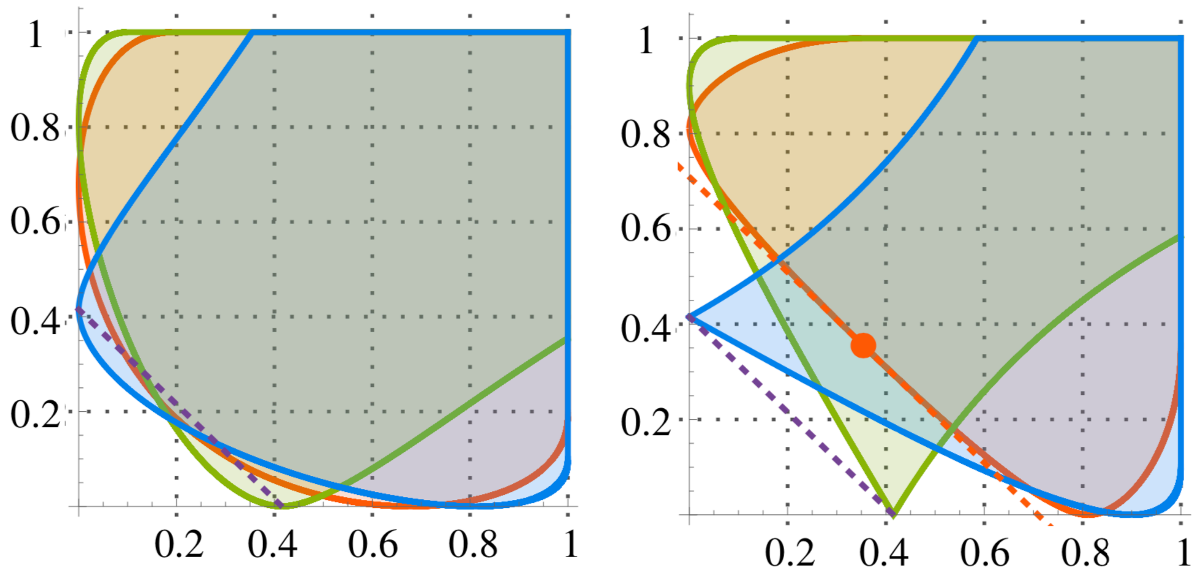
Uncertainty region is more informative than uncertainty relation in general.

Application 1: qubit case

$$M = \{|0\rangle, |1\rangle\}, N = \{(|0\rangle - \sqrt{3}|1\rangle)/2, (\sqrt{3}|0\rangle + |1\rangle)/2\}$$

MU bound $H_\alpha(M) + H_\beta(N) \geq \log(4/3)$, $1/\alpha + 1/\beta = 2$

$(\alpha, \beta) = \left(\frac{2}{c}, \frac{2}{c}\right)$ $(\alpha, \beta) = \left(\frac{1}{c}, \infty\right)$ $(\alpha, \beta) = \left(\infty, \frac{1}{c}\right)$



(a) $1/\alpha + 1/\beta = 1$ (b) $1/\alpha + 1/\beta = 2$

Application 2: Majorization based QRTs

Task: Given an unknown pure state $|\psi\rangle$ and measurement device M

$$|\psi\rangle \xrightarrow[\text{IO}]{?} |\varphi\rangle = \sum_{j=1}^{n} \sqrt{y_j}|j\rangle$$

$$|\psi\rangle = \sum_{j=1}^{n} \sqrt{x_j}|j\rangle \quad |\varphi\rangle = \sum_{j=1}^{n} \sqrt{y_j}|j\rangle \qquad |\psi\rangle \xrightarrow[\text{IO}]{\text{free}} |\varphi\rangle \Longleftrightarrow x \prec y$$

Strategy: 1. perform measurement M and obtain the pre-testing outcome $\mathbf{p}$

2. Let $N = \{|j\rangle\}_{j=1}^{n}$ be the post-testing and compute **r** and **t** by SDPs. We have $\mathbf{r} \prec \mathbf{x} \prec \mathbf{t}$.

3. $\mathbf{t} \prec \mathbf{y}$ ➡ $\mathbf{x} \prec \mathbf{t} \prec \mathbf{y}$ ➡ $|\psi\rangle \xrightarrow{\text{yes}} |\varphi\rangle$

$\mathbf{y} \prec \mathbf{r}$ ➡ $\mathbf{y} \prec \mathbf{r} \prec \mathbf{x}$ ➡ (w.p. 1) $|\psi\rangle \xrightarrow{\text{no}} |\varphi\rangle$

otherwise ➡ No enough information

Summary & Discussions

Summary

- **Complementary Information Principle:** given the information gain from the pre-testing outcome, we can fully characterize the uncertainty of the post-testing.
  - Majorization bounds are SDP computable;
  - Unique and tight in majorization.
  - works for POVMs and even multiple measurements.

- **Applications**
  - Universal uncertainty region
  - Determine quantum state transformation
  - Bounding joint uncertainty for any given measures

Open problems and future directions:

1. Is it possible to compute the majorization upper bound **t** in a single SDP, instead of exponential many independent SDPs ?

2. Is there any more concrete applications of our general framework?
   E.g. in quantum cryptography, ERP steering....

Thanks for your attention!

arXiv:1908.07694