Short proofs of the Quantum Substate Theorem

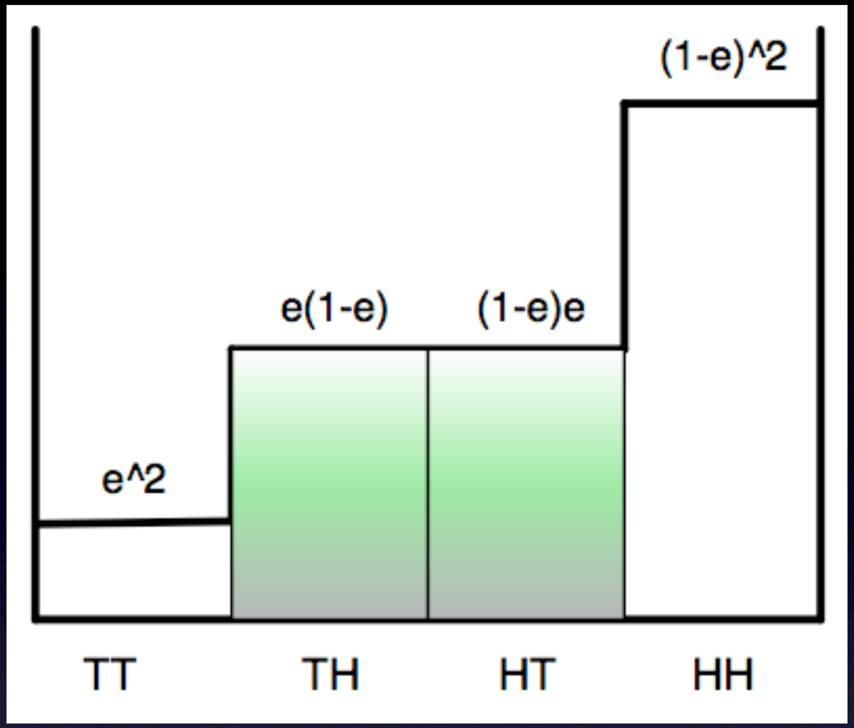
Rahul Jain
CQT and NUS, Singapore

Ashwin Nayak
University of Waterloo

Classic problem

- Given a biased coin c
  - $\Pr(c = H) = 1 - e$
  - $\Pr(c = T) = e$
- Can we generate a fair coin toss ?

Lemonade from lemons



Von Neumann: rejection sampling

- Toss *c* twice
- Repeat if HH or TT, else output result

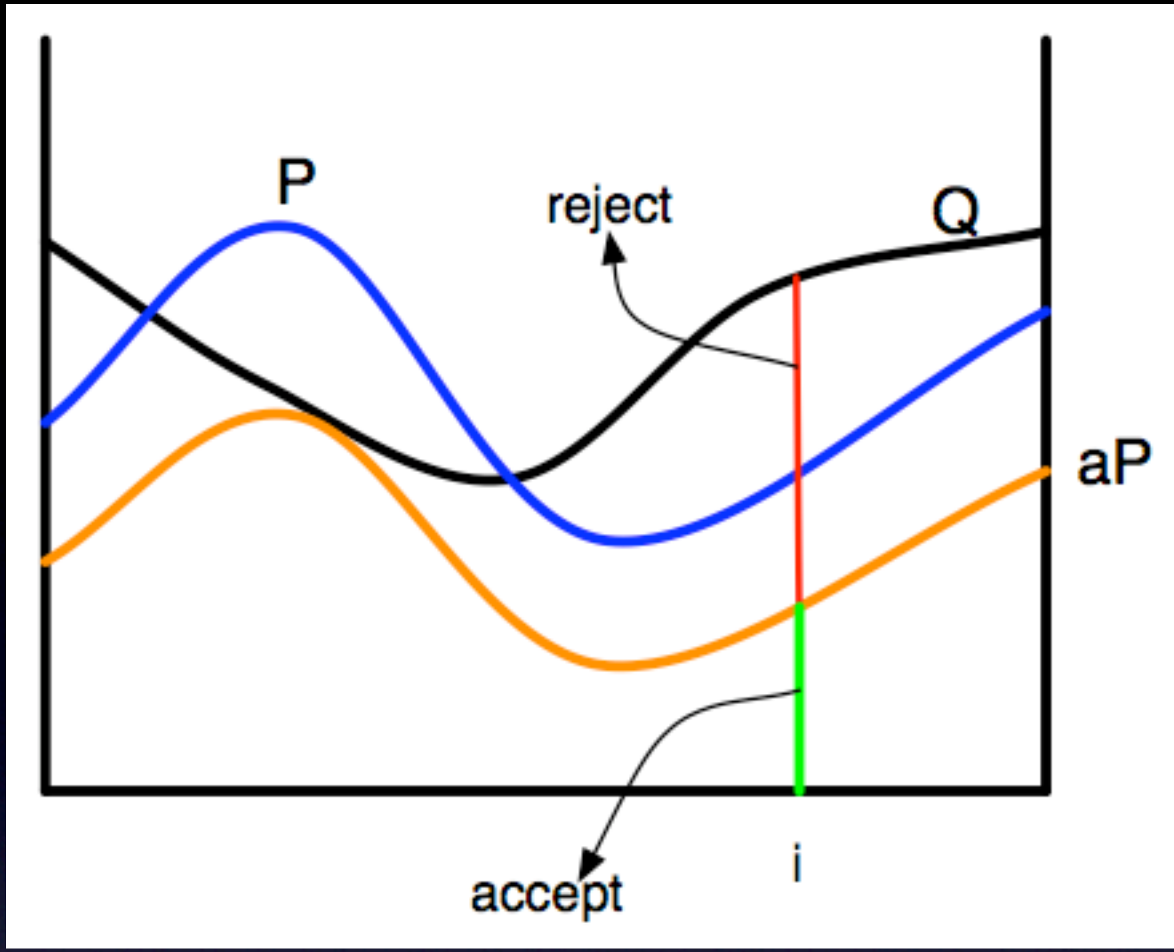
Pr(success in 1 trial) = p = $2e(1-e)$

E(# trials for success) = $1/p$

Quantum substate theorem

- Say we are given a quantum state Q, but we wish to prepare state P
- The theorem gives a bound on the number of trials a quantum analogue of rejection sampling takes (formal statement later)
- Original proof by Jain, Radhakrishnan, and Sen (2002)
- Applications in cryptography, communication and information theory
- This talk: short, conceptually simple proof of the theorem
- Stronger statement, optimal up to a constant factor

Classical version



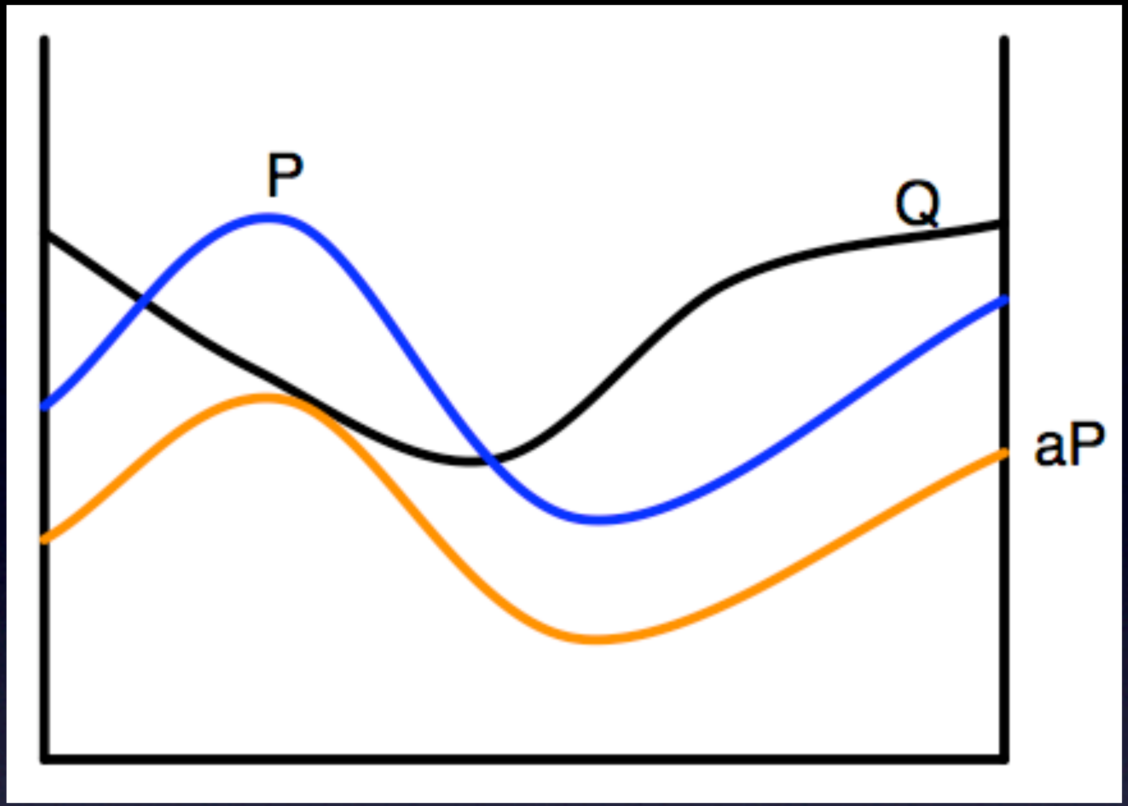
Rejection sampling

- Scale P so its graph is contained within Q: $aP \leq Q$
- We get a sample i from Q
- Throw a dart uniformly at random on the vertical line up to Q
- Repeat with new sample if dart above aP, else output i

Pr(success in 1 trial) = a = $\min_i \; q_i / p_i$

E(# trials for success) = $1/a$ = $\max_i \; p_i / q_i$

Relative min-entropy

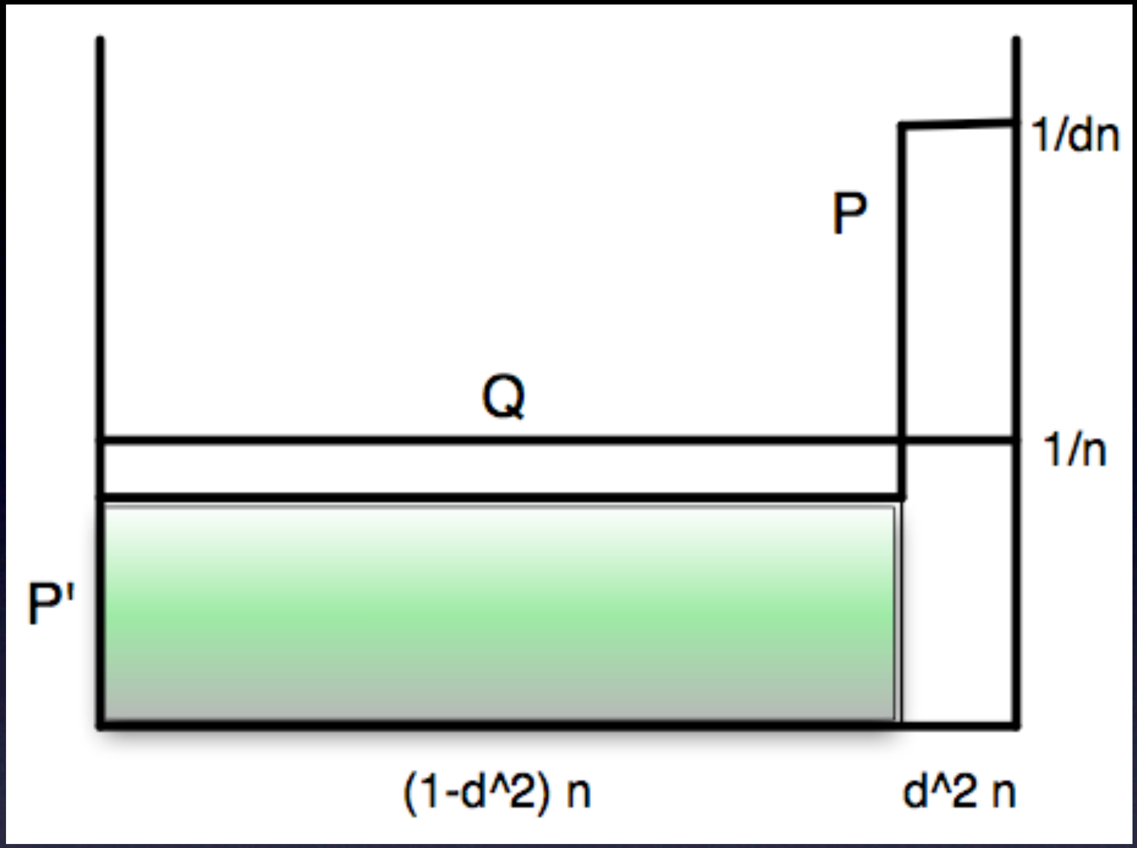


- We say aP is a *subdistribution* of Q
- E(# trials for success) = $1/a$ = $\max_i \; p_i / q_i$
- Important measure of distance between distributions P, Q
- $S_\infty(P|Q) = \log_2 (1/a) = \max_i \; \log_2 (p_i / q_i)$
- Relative entropy: $S(P|Q) = \sum_i \; p_i \log_2 (p_i / q_i) \leq S_\infty(P|Q)$

Approximate sampling

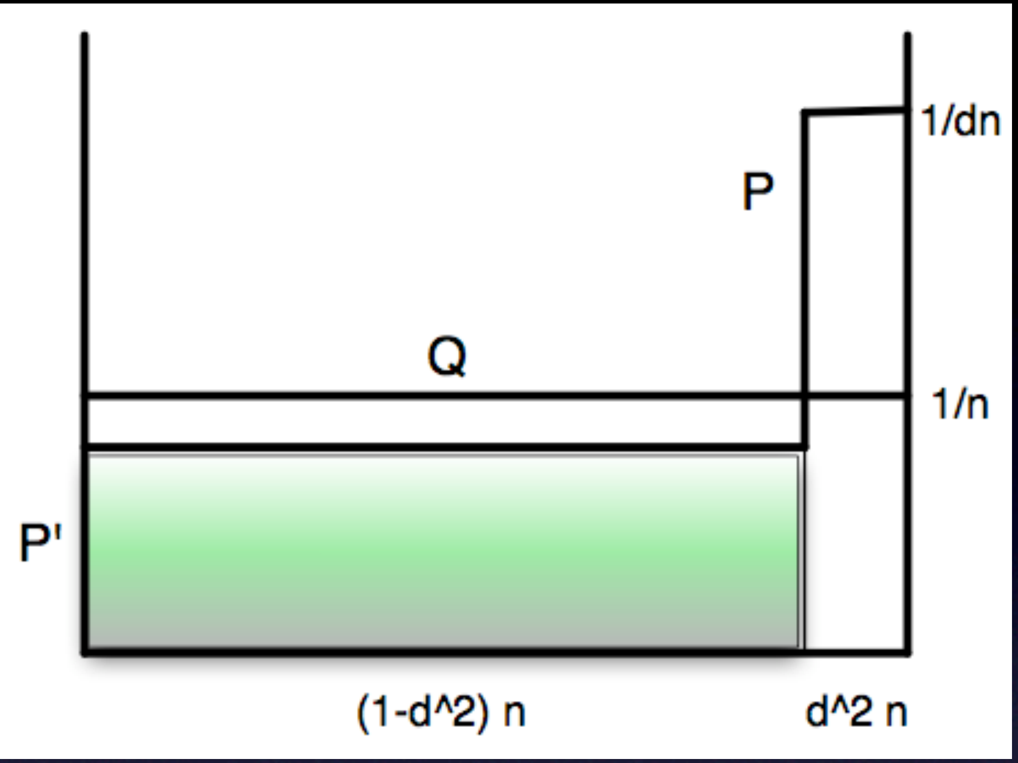
- Given Q often suffices to generate P' close to P
- Say, $|P' - P| \leq e$

  (1/2 L_1 distance)



- $S_\infty(P|Q) = \log_2 (1/d)$
- Let P' be uniform on the first $(1 - d^2)\, n$ points
- Then $|P' - P| \leq d$
- $S_\infty(P'|Q) = \log_2 (1 / (1 - d^2)) \approx$ const d^2

Smooth relative min-entropy



- Interested in *P'* e-close to *P*, such that *aP'* is a subdistribution of *Q* and *a* is maximized
- E(# trials for success) = 1/*a*
- $S^e_\infty(P|Q)$ = $\log_2$ min { $1/a$: $aP' \leq Q$, $|P' - P| \leq e$ }

  = $\log_2$ min { k : $P' \leq kQ$, $|P' - P| \leq e$ }
- How do we estimate this quantity ?

Substate theorem [JRS'02]

Theorem

Suppose P, Q are probability distributions

with supp(P) $\subseteq$ supp(Q) .

For every $e \in (0,1)$ there is a distribution P' such that

$|P' - P| \leq e$, and

$P' \leq [\, 2^{(s+1)/e} / (1-e) \,]\; Q$,

where $s = S(P|Q)$.

I.e., $S^e_\infty(P|Q) \leq (S(P|Q) + 1) / e + \log_2 1/(1 - e)$

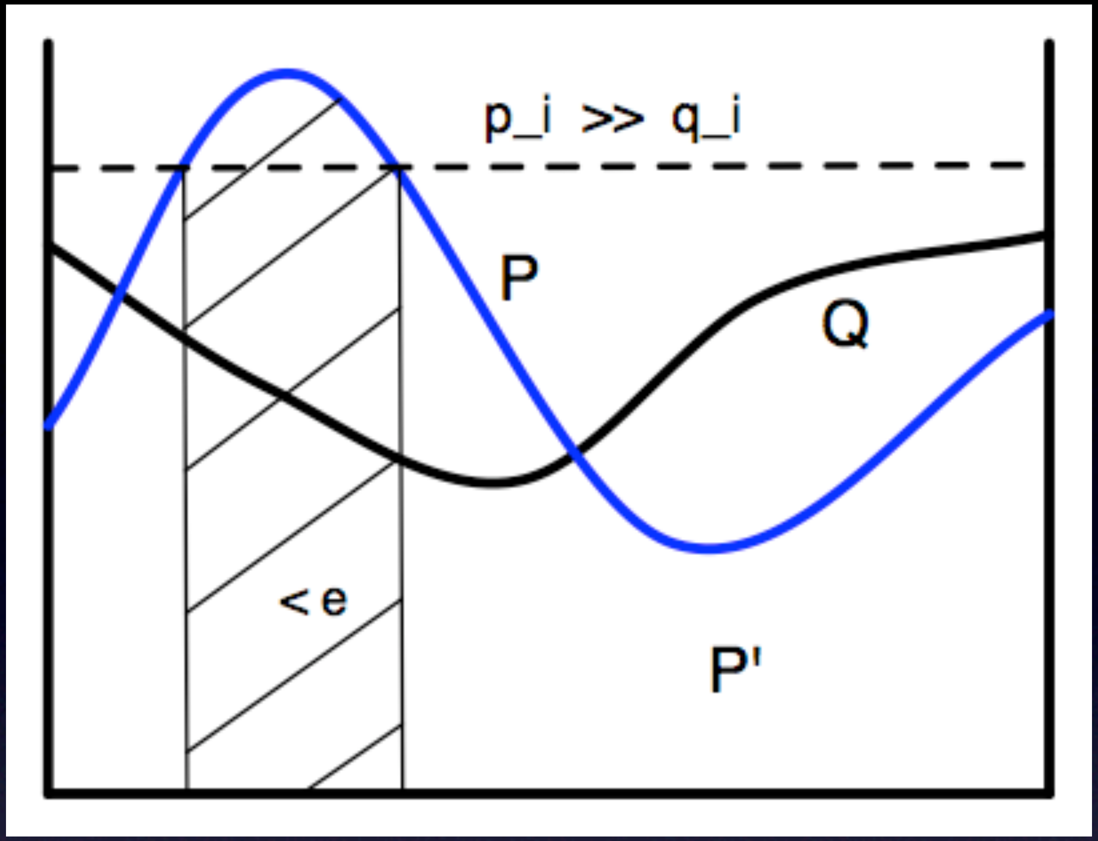
Recall: relative entropy $S(P|Q) = \sum_i p_i \log_2 (p_i / q_i)$.

Proof of Substate Theorem

Let $s = S(P|Q) = E_i \log_2 (p_i / q_i)$

If p_i/q_i were at least 1, we could use the Markov inequality:

$$\Pr(\log_2 (p_i/q_i) \geq s/e) \leq e$$



The sum of negative terms $p_i \log_2 (p_i / q_i)$ is at least -1 .

$$\Rightarrow \Pr(\log_2 (p_i/q_i) \geq (s+1)/e) \leq e$$

Let $P' = P$ conditioned on the complementary event.

We have $|P' - P| \leq e$, and $(1\text{-}e) P' \leq 2^{(s+1)/e} Q$ ▮

Quantum substate theorem [JRS'02]

Theorem

Suppose P, Q are ~~probability distributions~~ quantum states

with supp(P) $\subseteq$ supp(Q) .

For every e $\in$ (0,1) there is a ~~distribution~~ quantum state P' such that

$|P' - P| \leq$ ~~e~~ $\sqrt{e}$ and

$P' \leq [\, 2^{(s+1)/e} / (1\text{-}e) \,] \; Q$,

where $s = S(P|Q)$.

I.e., $S^d_\infty(P|Q) \leq (S(P|Q) + 1) / e + \log_2 1/(1 - e)$

where $d = \sqrt{e}$

Decoding this theorem

- What is a quantum state ?
- What is rejection sampling for quantum states ?
- What is the relative entropy of quantum states ?
- When are two quantum states close to each other ?

Quantum state

- A quantum state P is a positive semidefinite operator on C^n with unit trace
- Simplest case: rank 1 operator
  - $P = v v^*$, v is called a *superposition*
- Rank > 1: $P = \sum_i p_i v_i v_i^*$ (spectral decomposition)
  - may be viewed as a probability distribution (p_i) over the eigenvectors v_i
- Probability distribution over $\{1, ..., n\}$ is a diagonal such operator: $v_i = e_i$, standard basis vectors

Rejection sampling

- Given quantum state Q, would instead like to prepare state P
- We say aP is a *substate* of Q if $aP \leq Q$, i.e.,

$$Q = aP + (1-a)Q', \quad \text{where} \quad Q' \geq 0$$

- Several quantum variants of rejection sampling, all have success probability a
- Again, E (# trials for success) $= 1/a$

Relative min-entropy

- Important measure of distance between quantum states P, Q:
  - what is the maximum a such that $aP \leq Q$?
  - least E (# trials for success) = $1/a$
- $S_\infty(P|Q) = \log_2 \min \{ 1/a : aP \leq Q \}$

  $= \log_2 \min \{ k : P \leq kQ \}$

  No simple expression for this in terms of P, Q
- Relative entropy: $S(P|Q) = \mathrm{Tr}\; P (\log_2 P - \log_2 Q)$
- $\log_2$ is an operator monotone function
  - $\log_2 P \leq (\log_2 k)\, I + \log_2 Q$
- So $S(P|Q) \leq S_\infty(P|Q)$

Smooth relative min-entropy

- Suppose we can tolerate some error e in generating the quantum state *P* from *Q*:
  - would like *P'* e-close to *P*, such that *aP'* is a substate of *Q* and *a* is maximized
- Distance measure: induced by trace norm (Schatten 1-norm)
  - $|M| = (1/2)\ \mathrm{Tr}\ (M^*M)^{1/2} = (1/2)$ sum of singular values
  - tells us how well two quantum states may be distinguished
- $S^e_\infty(P|Q) = \log_2 \min \{\ 1/a : aP' \leq Q,\ |P' - P| \leq e\ \}$

  $= \log_2 \min \{\ k : P' \leq kQ,\ |P' - P| \leq e\ \}$
- How do we estimate this quantity ?

Quantum substate theorem [JRS'02]

Theorem

Suppose P, Q are quantum states, $\mathrm{supp}(P) \subseteq \mathrm{supp}(Q)$.

For every $e \in (0,1)$ there is a quantum state P' such that

$|P' - P| \leq \sqrt{e}$, and

$P' \leq [\, 2^{(s+1)/e} / (1-e) \,] \; Q$,

where $s = S(P|Q)$.

I.e., $S^{d}_{\infty}(P|Q) \leq (S(P|Q) + 1) / e + \log_2 1/(1 - e)$

where $d = \sqrt{e}$

New proof [Jain, N.'11]

- Key observation: smooth relative min-entropy is the logarithm of the following convex program (SDP) over variables P', k

$$\min \quad k$$

such that

$$P' \leq kQ$$

$$|P' - P| \leq e$$

$$\mathrm{Tr}(P') = 1$$

$$P' \geq 0$$

- Using strong duality, it suffices to bound the dual optimum
- Bound on dual is analogous to the substate theorem for distributions

First use of duality

$$A \leq B \quad \Leftrightarrow \quad v^*Av \leq v^*Bv \quad \text{for all} \quad v \in \mathbb{C}^n$$

$$\Leftrightarrow \quad \mathrm{Tr}(vv^*A) \leq \mathrm{Tr}(vv^*B) \quad \text{for all} \quad v \in \mathbb{C}^n$$

$$\Leftrightarrow \quad \mathrm{Tr}(MA) \leq \mathrm{Tr}(MB) \quad \text{for all} \quad M \geq 0$$

First use of duality

Lemma:

Suppose P', Q are quantum states with $\mathrm{supp}(P') \subseteq \mathrm{supp}(Q)$. Then

$$\min \{ k : P' \leq kQ \}$$

$$= \max \{ \mathrm{Tr}(MP') : \mathrm{Tr}(MQ) = 1, \; M \geq 0 \}.$$

Proof:

$P' \leq kQ \quad \Leftrightarrow \quad \mathrm{Tr}(MP') \leq k\,\mathrm{Tr}(MQ) \quad$ for all $M \geq 0$

$\Leftrightarrow \quad \mathrm{Tr}(MP') \leq k\,\mathrm{Tr}(MQ) \quad$ for all $M \geq 0, \; \mathrm{Tr}(MQ) \neq 0$

$\Leftrightarrow \quad \mathrm{Tr}(MP') \leq k \quad$ for all $M \geq 0, \; \mathrm{Tr}(MQ) = 1$

(scale M by $\mathrm{Tr}(MQ)$) ∎

A min-max formulation

The convex program over variables P', k

$$\min_{P', k \,:\, P' \leq kQ,\ |P' - P| \leq e,\ \mathrm{Tr}(P') = 1,\ P' \geq 0} k$$

may be rewritten as

$$\min_{P' \,:\, |P' - P| \leq e,\ \mathrm{Tr}(P') = 1,\ P' \geq 0} \ \min_{k \,:\, P' \leq kQ} k$$

By the previous lemma this is equal to

$$\min_{P' \,:\, |P' - P| \leq e,\ \mathrm{Tr}(P') = 1,\ P' \geq 0} \ \max_{M \,:\, \mathrm{Tr}(MQ) = 1,\ M \geq 0} \mathrm{Tr}(MP')$$

Min-max duality

A powerful min-max theorem from game theory implies

$$\min_{P' \,:\, |P' - P| \,\leq\, e,\;\; \mathrm{Tr}(P') \,=\, 1,\;\; P' \,\geq\, 0} \;\; \max_{M \,:\, \mathrm{Tr}(MQ) \,=\, 1,\;\; M \,\geq\, 0} \;\; \mathrm{Tr}(MP')$$

is equal to

$$\max_{M \,:\, \mathrm{Tr}(MQ) \,=\, 1,\;\; M \,\geq\, 0} \;\; \min_{P' \,:\, |P' - P| \,\leq\, e,\;\; \mathrm{Tr}(P') \,=\, 1,\;\; P' \,\geq\, 0} \;\; \mathrm{Tr}(MP')$$

To bound the optimum, it suffices to produce a suitable P' for each given M with bounded $\mathrm{Tr}(MP')$

The bound we seek: $\mathrm{Tr}(MP') \leq 2^{(s+1)/e} / (1-e)$, where $s = S(P|Q)$

Lemma: For any $M \geq 0$ such that $\mathrm{Tr}(MQ) = 1$, there is a quantum state P' e-close to P such that

$$\mathrm{Tr}(MP') \leq 2^{(s+1)/e} / (1-e) ,$$

where $s = S(P|Q)$.

Proof: Let $M = \sum_i m_i v_i v_i^*$ (spectral decomposition)

$\mathrm{Tr}(MQ) = \sum_i m_i \; v_i^* Q v_i$ (q_i) $\qquad Q_1 = (q_i)$

$\mathrm{Tr}(MP) = \sum_i m_i \; v_i^* P v_i$ (p_i) $\qquad P_1 = (p_i)$

Monotonicity of relative entropy implies

$$s_1 = S(P_1|Q_1) \leq S(P|Q)$$

We apply the result for distributions to P_1, Q_1 :

Let $B = \{ i : \log_2 (p_i/q_i) \geq (s_1+1)/e \}$

so that $\sum_{i \in B} p_i \leq e$

Let Π be the orthogonal projection onto Span $\{ v_i : i \notin B \}$

So $\Pi = \sum_{i \notin B} v_i v_i^*$

and $\mathrm{Tr}(\Pi P) = \sum_{i \notin B} v_i^* P v_i = \sum_{i \notin B} p_i \geq 1 - e$

Define $P' = \Pi P \Pi / \mathrm{Tr}(\Pi P)$

(we restrict P to the subspace with bounded p_i)

Lemma: $|P' - P| \leq \sqrt{e}$

(similar to the "gentle measurement lemma due to Winter)

Recall $B = \{ i : \log_2 (p_i/q_i) \geq (s_1+1)/e \}$

We have

$$\mathrm{Tr}(MP') = \sum_{i \notin B} m_i \; v_i^* P v_i \; / \; \mathrm{Tr}(\Pi P)$$

$$\leq (1/(1-e)) \sum_{i \notin B} m_i \, p_i$$

$$\leq (1/(1-e)) \sum_{i \notin B} m_i \; 2^{(s+1)/e} \; q_i$$

$$\leq [\, 2^{(s+1)/e} /(1-e) \,] \sum_{i \notin B} m_i \; q_i$$

$\leq \mathrm{Tr}(MQ)$

$$\leq 2^{(s+1)/e} /(1-e) \qquad \blacksquare$$

Remarks

- We get a stronger statement
  - use *fidelity* as a measure of distance
  - tighter bound in terms of *observational divergence*
- Optimal relationship between observational divergence and relative min-entropy (up to a constant factor)
- An alternative proof, albeit more abstract, using semidefinite programming duality
- Generalizes to smooth conditional entropy, which plays an important role in quantum cryptography and Shannon theory