On divergence, relative entropy and the substate property

Rahul Jain
U.C. Berkeley
rahulj@cs.berkeley.edu *

Jaikumar Radhakrishnan
Tata Institute of Fundamental Research, Mumbai, India
jaikumar@tti-c.org

Pranab Sen
NEC Labs, Princeton
pranab@nec-labs.com

April 1, 2022

Abstract
In this article we study relationship between three measures of distinguishability of quantum states called as divergence [JRS02], relative entropy and the substate property [JRS02].

1 Introduction
We consider three measures of distinguishability between quantum states and show various relationships between them. The first measure that we consider is called divergence. It was first considered in [JRS02] and is defined as follows:

**Definition 1 (Divergence)** Let \( \rho, \sigma \) be two quantum states. Let \( M \) be a Positive operator-valued measurement (POVM). Then divergence between them denoted \( D(\rho|\sigma) \), is defined as,

\[
D(\rho|\sigma) \triangleq \max_{M:POVM} \text{Tr} M \rho \log \frac{\text{Tr} M \rho}{\text{Tr} M \sigma}
\]

The second is the well known measure called the relative entropy also known as Kullberg-Liebeck divergence (\[NC00\]). It is defined as follows:

**Definition 2 (Relative entropy)** Let \( \rho, \sigma \) be quantum states. Then relative entropy between them, denoted \( S(\rho|\sigma) \) is defined as,

\[
S(\rho|\sigma) \triangleq \text{Tr} (\rho \log \rho - \rho \log \sigma)
\]

The third measure that we consider we call the substate property. It was also first considered in [JRS02]. It is defined as follows:

*This work was supported by an Army Research Office (ARO), North California, grant number DAAD 19-03-1-00082.
Definition 3 (Substate property) Two states $\rho$ and $\sigma$ are said to have the $k$-substate property if, $\forall r > 1, \exists \rho_r$ such that

$$\|\rho - \rho_r\|_t \leq 2/\sqrt{r} \text{ and } \sigma - (1 - \frac{1}{r})\rho_r^{2/r} \geq 0$$

2 Results in this article

The following theorem is a compilation of all the results in this article.

Theorem 1 Let $\rho$ and $\sigma$ be two quantum states in $\mathbb{C}^n$. Then,

1. $D(\rho|\sigma) \leq S(\rho|\sigma) + 1$. This is not new and was shown in [JRS02]. We present a proof for completeness.

2. Given classical distributions $P$ and $Q$ on $[n]$, $S(P|Q) \leq D(P|Q)(n-1)$.

3. $S(\rho|\sigma) \leq D(\rho|\sigma)(n-1) + \log n$.

4. There exists classical distributions $P$ and $Q$ on $[n]$ such that,

$$S(P|Q) > (D(P|Q)/2 - 1)(n-2) - 1.$$  

5. (Substate theorem) $\rho$ and $\sigma$ have the $(8D(\rho|\sigma) + 14)$-substate property. This is not new and was shown in [JRS02]. Please refer to [JRS02] for a proof.

6. (Converse of substate theorem for classical distributions) If distributions $P$ and $Q$ have the $k$-substate property then $D(P|Q) \leq 2k + 2$.

7. If the following strong $k$-substate property holds, i.e. $\sigma - \frac{\rho}{2^k} \geq 0$, then $S(\rho|\sigma) \leq k$.

8. There exists a POVM such that, if $P$ and $Q$ are resulting classical distributions then,

$$S(P|Q) \geq \frac{S(\rho|\sigma) - \log n}{n-1} - 1.$$  

Proof:

1. Let $M$ be the POVM that achieves $D(\rho|\sigma)$. Let $\text{Tr} M \rho \overset{\Delta}{=} p$ and $\text{Tr} M \sigma \overset{\Delta}{=} q$.

$$S(\rho|\sigma) \geq p \log \frac{p}{q} + (1-p) \log \frac{(1-p)}{(1-q)}$$

$$> p \log \frac{p}{q} + (1-p) \log \frac{1}{(1-q)} - 1$$

$$\geq p \log \frac{p}{q} - 1$$

$$= D(\rho|\sigma) - 1.$$  

The first inequality follows from the Lindblad-Uhlmann monotonicity of relative entropy [NC00] and the second inequality follows because $(1-p) \log(1-p) \geq (- \log e)/e > -1$, for $0 \leq p \leq 1$. ■
2. Define $x_i = \log(p_i/q_i)$. We can assume without loss of generality, by perturbing $Q$ slightly, that the values $x_i$ are distinct for distinct $i$. Let $S' = \{i : x_i > 0\}$. Let $D(P\|Q) = k$. Let 

$$\forall \text{positive real } l, S_l = \{i \in [n] : x_i \geq l\}.$$ 

Therefore, 

$$k \geq Pr_P[S_l] \frac{Pr_P[S_l]}{Pr_Q[S_l]} \geq Pr_P[S_l]l$$ 

$$\Rightarrow Pr_P[S_l] \leq k/l$$ 

Assume without loss of generality that $x_1 < x_2 < \cdots < x_n$. Then if $x_i > 0$, $Pr_P[S_{x_i}] \leq k/x_i$. Since $S(P\|Q) \leq \sum_{i \in S'} p_i x_i$, the upper bound on $S(P\|Q)$ is maximized when $S' = \{2, \ldots, n\}$, $p_n = k/x_n$, $p_i = k(1/x_i - 1/x_{i+1})$ for all $i \in \{2, \ldots, n - 1\}$, $p_n = k/x_n$, and $p_1 = 1 - \sum_{i=2}^n p_i$. Then, 

$$S(P\|Q) \leq \sum_{i=2}^n p_i x_i$$ 

$$= k \sum_{i=2}^{n-1} x_i (1/x_i - 1/x_{i+1}) + k$$ 

$$= k \sum_{i=2}^{n-1} \frac{x_{i+1} - x_i}{x_i x_{i+1}} + k$$ 

$$\leq k \sum_{i=2}^{n-1} 1 + k$$ 

$$= k(n - 1).$$ 

3. Let us measure $\rho$ and $\sigma$ in the eigenbasis of $\sigma$. We get two distributions: $P_\rho$ and $P_\sigma$. Let $D(P_\rho\|P_\sigma) = k$. From Part 2, it follows, 

$$k(n - 1) = D(P_\rho\|P_\sigma)(n - 1) \geq S(P_\rho\|P_\sigma)$$ 

$$= \text{Tr } P_\rho \log P_\rho - \text{Tr } P_\rho \log P_\sigma$$ 

$$\geq -\log n - \text{Tr } P_\rho \log P_\sigma$$ 

$$= -\log n - \text{Tr } \rho \log \sigma$$ 

$$= -\log n + S(\rho|\sigma) - \text{Tr } \rho \log \rho$$ 

$$\geq -\log n + S(\rho|\sigma)$$ 

The second equality above holds since the measurement was in the eigenbasis of $\sigma$. Thus 

$$S(\rho|\sigma) \leq D(P\|Q)(n - 1) + \log n$$
4. Fix \( a > 1, k > 0 \). Let \( p_1 = (a - 1)/a \),
\[
\forall i \in \{2, \ldots, n - 1\} \quad p_i = (a - 1)/a^i,
\]
and \( p_n = 1/a^{n-1} \). Let
\[
\forall i \in \{2, \ldots, n\} \quad q_i = p_i/2^ka^{i-1},
\]
and \( q_1 = 1 - \sum_{i=2}^{n} q_i \). For any \( r > 1 \), consider \( \tilde{P} = (p_1, \ldots, p_{\log_a r + 1}, 0, \ldots, 0) \) normalized to make it a probability vector. It is easy to see that \( \|P - \tilde{P}\|_1 \leq 2/r \) and \( \frac{(r-1)\tilde{P}}{2^{r^2}k} \leq Q \). This shows that \( P, Q \) satisfy the classical \( k \)-substate property, hence \( D(P|Q) \leq 2(k + 1) \).

Now,
\[
S(P|Q) = \sum_{i=1}^{n} p_i \log \frac{p_i}{q_i}
\]
\[
\geq p_1 \log p_1 + \sum_{i=2}^{n} p_i \log \frac{p_i}{q_i}
\]
\[
> -1 + (n - 2) \frac{k(a - 1)}{a} + k
\]
\[
= k(n - 1) - \frac{k(n - 2)}{a} - 1.
\]
By choosing \( a \) large enough, we can achieve \( S(P|Q) > k(n - 2) - 1 \). This shows that \( S(P|Q) > (D(P|Q)/2 - 1)(n - 2) - 1 \).

5. Proof skipped. Please see [JRS02] for a detailed proof.

6. Let \( M \) be a POVM such that
\[
k_1 \triangleq D(P|Q) = \text{Tr} MP \log \frac{\text{Tr} MP}{\text{Tr} MQ}
\]
Let \( p \triangleq \text{Tr} MP \) and \( q \triangleq \text{Tr} MQ \). Therefore,
\[
k_1 = p \log \frac{p}{q} \Rightarrow q = \frac{p}{2^{k_1/p}}
\]
Let \( r = 2/p \). Since \( P \) and \( Q \) have the \( k \)-substate property, let \( P_r \) be the distribution such that,
\[
\|P - P_r\|_r \leq \frac{2}{r} = p \quad \text{(holds for classical distributions [JRS02])}
\]
and
\[
Q - (1 - \frac{1}{r}) \frac{P_r}{2^{rk}} \geq 0
\]
Let \( p_r \triangleq \text{Tr} MP_r \). From (1) it follows,
\[
p_r \geq \frac{p}{2}
\]
Also
\[
\frac{p}{2^{k_1/p}} = q = \text{Tr} \ MQ \\
\geq (1 - \frac{1}{r}) \text{Tr} \ MP \frac{r}{2^{r_k}} \quad \text{(from } 3) \]
\[
= (1 - \frac{p}{2}) \frac{p_r}{2^{r_k}} \quad \text{(from definition)} \\
\geq (\frac{1}{2}) \frac{p_r}{2^{r_k}} \quad \text{(since } p \leq 1) \\
\geq (\frac{1}{2}) \frac{p}{2^{r_k+1}} \quad \text{(from } 3) \\
\Rightarrow 2^{rk+2} \geq 2^{k_1/p} \\
\Rightarrow rk + 2 \geq k_1/p \\
\Rightarrow p(rk + 2) \geq k_1 \\
\Rightarrow prk + 2 \geq k_1 \quad \text{(since } p \leq 1) \\
\Rightarrow 2k + 2 \geq k_1
\]

Remark : This proof does not work for the quantum case because of \(\sqrt(r)\) in the substate property.

7.

\[
S(\rho) = \text{Tr} \ \rho \log \rho - \text{Tr} \ \rho \log \sigma \\
\leq \text{Tr} \ \rho \log \rho - \text{Tr} \ \rho \log \frac{\rho}{2^k} \\
= k \text{Tr} \ \rho = k
\]

The first inequality above follows from monotonicity of the operator log function.

8. We know that there exists a POVM element \(M\) such that,

\[
D(\rho|\sigma) = \text{Tr} \ M \rho \log \frac{\text{Tr} \ M \rho}{\text{Tr} \ M \sigma}
\]

Let \(p = \text{Tr} \ M \rho\) and \(q = \text{Tr} \ M \sigma\). Let \(P = (p, 1 - p)\) and \(Q = (q, 1 - q)\). Note that

\[
S(P|Q) = p \log p/q + (1-p) \log (1-p)/(1-q) \\
\geq p \log p/q - 1 \\
= D(\rho|\sigma) - 1
\]

From Part 2 it follows that

\[
S(\rho|\sigma) \leq D(\rho|\sigma)(n-1) + \log n \\
\leq (S(P|Q) + 1)(n-1) + \log n \\
\Rightarrow S(P|Q) \geq \frac{S(\rho|\sigma) - \log n}{n-1} - 1
\]
References

[JRS02] R. Jain, J. Radhakrishnan, and P. Sen. Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states. In Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, pages 429–438, 2002.

[NC00] M. Nielsen and I. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2000.