Information Theory In General Probabilistic Theories

Gen Kimura
Research Center for Information Security
National Institute of Advanced Industrial Science and Technology

"Operational" Probability Theory

State + Measurement ⇒ Probability

<Classical Prob. Theory.>

Probability Distribution p_ω + Random Variable $X \Rightarrow \Pr[X = x|p] = \sum_{\omega \in \Omega, x = X(\omega)} p_\omega$

<Quantum Prob. Theory.>

Density Operator ρ + POVM $E = (E_i) \Rightarrow \Pr[E = e_i|\rho] = \mathrm{Tr}(E_i\rho)$

with some natural postulates

* **Mixing Postulates for States**: Existence of probabilistic mixture of states
* **Separating Postulates for States and Measurements**:
Identify states if they have the same physical properties
Identify measurements if they have the same physical properties

Facts: There are many probability theories
other than neither classical nor quantum,

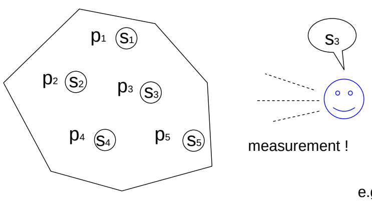
General Probabilistic Theories (GPT)

Study: We consider "Information Theory" on GPT

Motivations:
Following (and developing) Shannon's philosophy, we believe that
Information Theory should be constructed independently on the specific physical theories, but only on abstract theory of probability
so that
(I) the mutual relation among several information processings are clarified
(II) we understand the structure of quantum mechanics (from outside)
(III) we investigate classical and quantum info. theory. with measurement restrictions,
(IV) we prepare (possible) post quantum attack in future
, etc

Math: Convex set S in Locally Compact Hausdoff Topological Vector Space and Affine Functions on S

State Discrimination Problem in GPM [1,2]



* $P_S(\mathbf{E}) = \sum_{i=1}^N p_i e_i(s_i)$

-- Success Probability by measuring E

* $P_S = \max_{\mathbf{E} \in \mathcal{O}_N} P_S(\mathbf{E})$

-- Optimal Success Probability

e.g., QM with N = 2

$$P_S = \frac{1}{2}(1 + \|p_0\rho_0 - p_1\rho_1\|_1) : HelstromBound$$

Purpose: Investigation of the optimal state discrimination in GPT

Result → We proposed a (geometrical) method to search the Optimal State Discrimination by introducing Helstrom Family of Ensembles (See [1],[2])

"Derivation" of Qubit from Physical Postulates [4]

Fact: Quantum Mechanics is just a particular theory in GPTs
Motivation: Derive QM (e.g., Qubit) based on physical principles

Principles
* Equality for pure states (symmetricity)
* Decomposability with distinguishable pure states

[Thm.] 2 dimensional Symmetric GPT are either polygon or quantum.

[Thm.] 2 dimensional Symmetric DDPS GPT are either classical or quantum.

[Thm] For strong symmetric and DDPS GPT with dim $S = 3$,
S is either simplex (classical system) or satisfy following:
Every boundary states are pure
so pure-states set are topologicaly equivalent to the unit sphere (Bloch sphere).

Introductions of Distinguishability Measures [3]

$$\boxed{D(s,t) := \max_{M \in \mathcal{M}} D_c(p_s(M), p_t(M))}$$ where $D_c(p_\omega, q_\omega) = \frac{1}{2}\sum_\omega |p_\omega - q_\omega|$: Kolmogorov distance

$$\boxed{F(s,t) := \inf_{M \in \mathcal{M}} F_c(p_s(M), p_t(M))}$$ where $F_c(p_\omega, q_\omega) = \sum_\omega \sqrt{p_\omega q_\omega}$: Bhattacharyya coefficient

[Thm] For all $s, t \in S$,
- $0 \le D(s,t) \le 1$
- $D(s,t)$ is a metric on S
- $D(F(s), F(t)) \le D(s,t)$ for all $F \in A(S)$: Monotonicity
- D satisfies strong convexity, joint convexity, and convexity.
- $D(s,t) = 2P_s(s,t) - 1$; where $P_s(s,t)$: Optimal Success prob. to discriminate s and t.
- $D(s,t)$ coincides with the Gudder's intrinsic metric
- $0 \le F(s,t) \le 1$, $F(s,t) = 1$ iff $s = t$
- $F(F(s), F(t)) \ge F(s,t)$ for all $F \in A(S)$: Monotonicity
- F satisfies strong concavity, joint concavity, and concavity
- $1 - F(s,t) \le D(s,t) \le \sqrt{1 - F^2(s,t)}$: Equivalence with D
- (I) $F(s_A, t_A) \ge F(s,t)$ for any $s, t \in S_A \otimes S_B$ where s_A and t_A are the reduced states to the system A.
(II) $F(s_1, s_2)F(t_1, t_2) \ge F(s_1 \otimes t_1, s_2 \otimes t_2)$ for any $s_1, s_2 \in S_A, t_1, t_2 \in S_B$.
(III) $F(s_1, s_2) = F(s_1 \otimes t, s_2 \otimes t)$ for any $s_1, s_2 \in S_A, t \in S_B$.

Applications

No-Cloning in GPT

[Thm. 1] Distinct states s_1 and s_2 are clonable iff they are perfectly distinguishable.

[Thm. 2] If there exists at least two distinct states, there are no universal cloning machine.

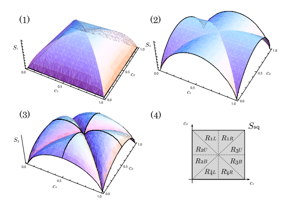
[Thm. 3] GPT is classical iff there exists universal cloning machine for pure states.

Information-Disturbance in GPT

[Thm. 4] Any attempt to distinguish two indistinguishable pure states causes non-zero disturbance, i.e., it is impossible to gain information without causing disturbance.

Introductions of Entropies [3]

$$S_1(s) := \inf_{M=(m_j)_j \in \mathcal{M}_{\mathrm{fml}}} H(m_j(s)).$$
$$S_2(s) := \sup_{\{p_\omega, s_\omega\} \in \mathcal{D}(s)} I(\{p_\omega, s_\omega\})$$
$$S_3(s) := \inf_{\{p_\omega, s_\omega\} \in \mathcal{P}(s)} H(p_\omega).$$



[Thm] All S_1, S_2, S_3 are Shannon (resp. von Neuman) entropy in classical (resp quantum) system.
[Thm] S_1 satisfies concavity while S_2, S_3 not generally.
[Thm] S_3 satisfy "weak" concavity.
[Thm] S_2 satisfy the same upper bound as von Neumann entropy
[Thm] $S_{2(3)}(s) = 0$ iff s is pure while not S_1 generally.
[Thm] $S_1(s) = 0 \Rightarrow s$ is on a boundary of S.
Moreover, if GPT is symmetric, $S_1(s) = 0$ if s is pure.

References:
[1] G. K., T. Miyadera, H. Imai, Phys. Rev. A79, 062306 (2009).
[2] K. Nuida, G. K., T. Miyadera, arXiv:0906.5419.
[3] G. K., K. Nuida, H. Imai, arXiv:0910.0994 (to appear in ROMP).
[4] G. K., K. Nuida, (in prep); K. Nuida, G. K., H.Imai, (in prep).
[5] G. K., K. Imafuku, et al (in prep). etc