State Discrimination In General Probabilistic Theories

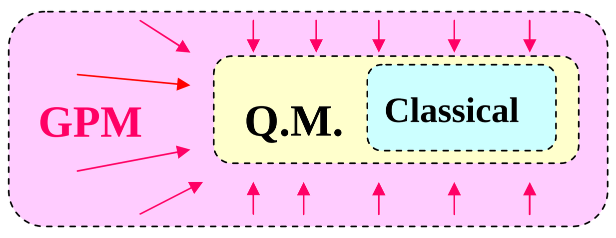
木村 元
(独)産業技術総合研究所
情報セキュリティ研究センター　物理解析研究チーム

What is Generic Probability Models ?

* Operationally Most General Theory to use probability,
  including Classical and Quantum theory, and more..

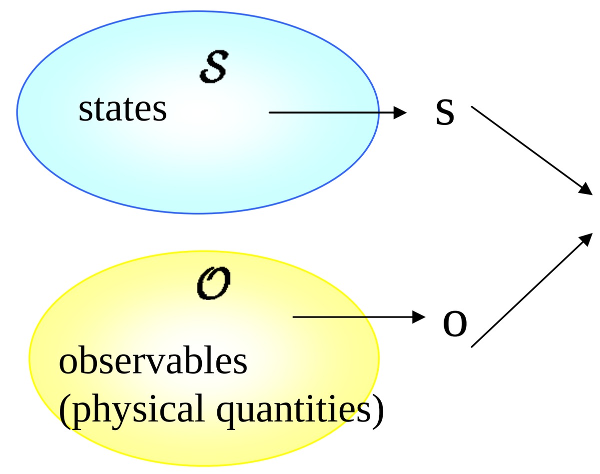
* To understand the mystery of Quantum Mechanics (QM) from outside !!
  --- why QM starts from Hilbert space. etc. ?
  --- why QM provides secure key distribution ?
  --- why QM provides a ultrahigh-speed computation, teleportation ?
  --- why QM prohibits local hidden variable (or KS theorem)
  => Information theoretic characterization of Quantum Mechanics??

* Information Theory for Generic Probability Models (GPM) !!
  --- Secure Key distribution with no-signaling condition
  --- No-cloning (or broadcasting) theorem in GPM
  --- Teleportation in GPM.



Mackey (1950s); Ludwig (1964-); Davies and Lewis (1970);
Gudder (1973); Recently, Fuchs,Barret;d'ariano;Hardy; et.al.

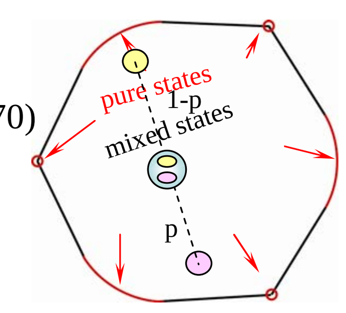
Operational Approach: Convex Structure



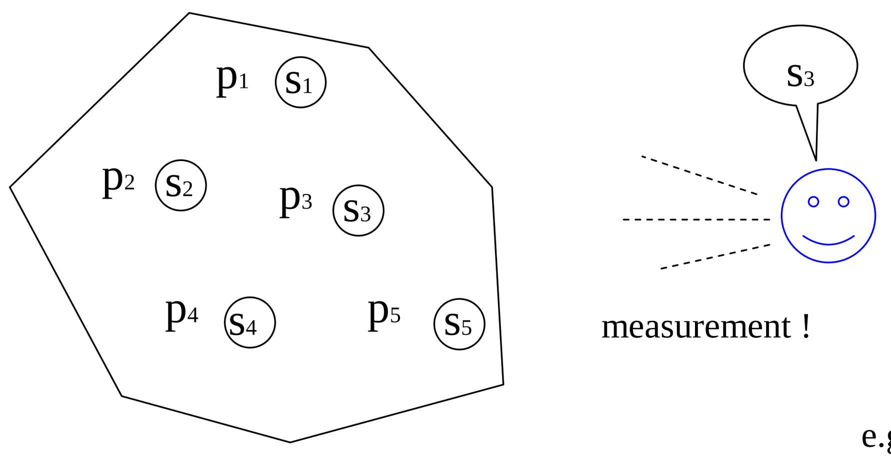
[A1] Convex Prestructure
=> Affine property
[A2] Separablity of Observables

*1 State space can be represented by
a (compact) convex set S in a real vector space (Gudder 1970)

= p (s) + (1-p) (t)



State Discrimination Problems and Helstrom Family of Ensembles



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

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

Purpose: Investigation of the optimal state discrimination
in Generic Probability Model

Result → We provide a (geometrical) method to search the Optimal State Discrimination by introducing Helstrom Family of Ensembles

(weak) Helstrom family of ensembles

* $\{s_i\in\mathcal{S}\}_{i=1}^N$: N distinct states
* $p_i = 1/N$: uniform prior probability distribution

[Def] Weak Helstrom family of ensembles

$\{q, s_i; 1-q, t_i\}_{i=1}^N$ s.t.

$s := qs_i + (1-q)t_i \ (\forall i = 1,\dots,N)$

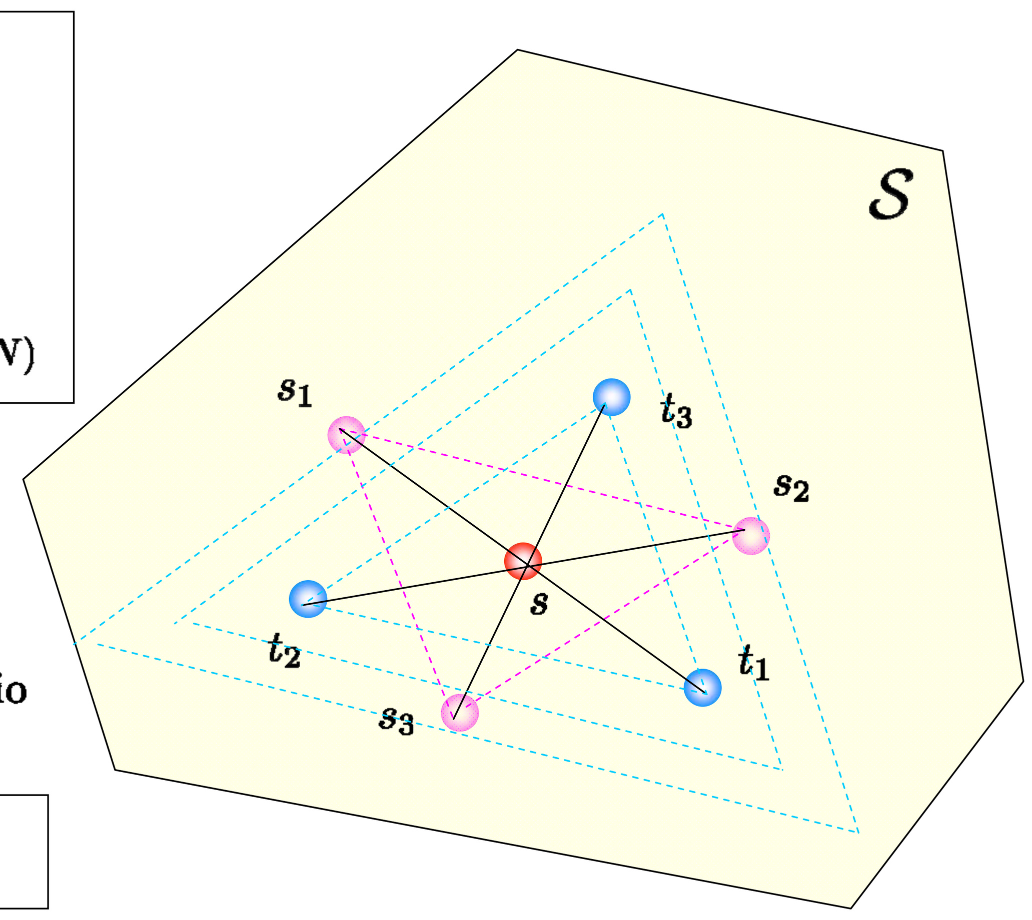
Point Symmetry

t_i : conjugate state to s_i

s : reference state

$p := 1/(Nq)$: Helstrom Ratio

Prop $P_S \leq \frac{1}{Nq}$



[Def] Helstrom family of ensembles: ⇔
a weak Helstrom family of ensembles with which $P_S = p$

Proposition 2 *In generic cases, a necessary and sufficient condition for a weak Helstrom family of ensembles $\{q_i, s_i; 1-q_i, t_i\}$ to be Helstrom family is that there exists an observable $\mathbf{E} = \{e_i\}_{i=1}^N$ satisfying $e_i(t_i) = 0$ for all $i = 1,\dots,N$.*

[Def] Generic cases: $P_s > \max_i p_i$

Theorem 1 *A weak Helstrom family $\{q, s_i; 1-q, t_i\}$ $(i = 1,2)$ with distinguishable conjugate states t_1 and t_2 is a Helstrom famility. An optimal measurement to distinguish s_0 and s_1 is given by an observable to distinguish t_0 and t_1.*

$t_1, t_2 \in \mathcal{S}$ distinguishable
⇔ ∃ Observable $E = \{e_1, e_2\}$ such that $e_1(t_2) = 1, e_1(t_2) = 0$

Most Generally, we have

Theorem 2 In any generic probability models, Helstrom family exists for any generic binary state discrimination.

$$d_G(s_1,s_2) := \inf[\ \lambda\in(0,1/2] \mid \exists t_1,t_2\in\mathcal{S}\ s.t.\ (1-\lambda)s_1+\lambda t_1 = (1-\lambda)s_2+\lambda t_2]$$

⇒ Metric [Gudder 1973]

$$= 1 - \sup[\ q\in(1/2,1] \mid \exists t_1,t_2\in\mathcal{S}\ s.t.\ qs_1+(1-q)t_1 = qs_2+(1-q)t_2]$$

$$= 1 - 1/(2P_S) \quad \text{(From our Theorem 2)}$$

Operational Meaning of Gudder's Metric w.r.t. optimal success probability !

* We have provided a geometrical method, by introducing the Helstrom family of ensembles, to find the optimal success probability in any generic probability models
* We have shown the existence of the family, in any generic probability models

* Some applications:
  ** Reproduction of Helstrom Bound in QM
  ** N symmetrical state discrimination in QM
  ** operational meaning of Gudder's metric
  ** Generalization of Hwang-Bae's result

* G. Kimura, T. Miyadera, H. Imai, to appear in Phys. Rev. A; E-print: arXiv:0808.3844
* K. Nuida, G. Kimura, T. Miyadera, H. Imai (in preparation)

National Institute of Advanced Industrial Science and Technology AIST

State discrimination in General Probabilistic Theories

Research Center for Information Security

物理解析チーム 木村元

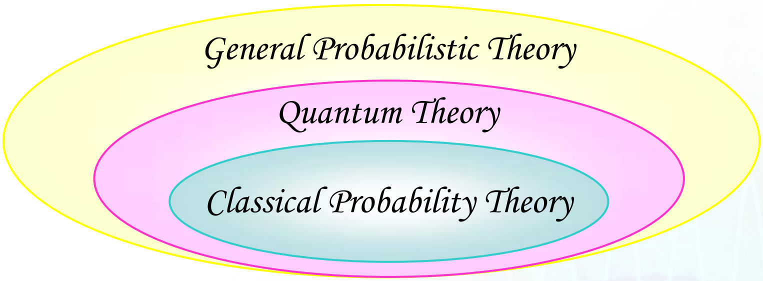
* General Probability Theories (GPT)

--- Operationally the most general Probability Theory including Quantum Mechanics (QM)

--- Two main Goals:

*** Cryptography in GPT

*** Characterization of QM from operational point of view



* State Discrimination Problems in GPT

--- First step to construct secure Key Distribution in GPT

--- Introduction of geometrical method to state discrimination problems in GPT

--- Several Applications