On the general property of correlation

Gen Kimura[†,1] and Shuichi Tasaki

[†] *College of Systems Engineering and Science, Shibaura Institute of Technology, 307 Fukasaku, Minuma-ku, Saitama-shi, Saitama, 337-8570, Japan*

1 Introduction

Professor Shuichi Tasaki was one of the greatest visionaries in science who understands not only physics but also mathematics and — most importantly — the philosophy of science. With the talented and fruitful ideas and views, he possessed a generous and great personality as well and has attracted so many people. There would be many difficult questions in life. One of the most difficult ones to accept is that the precious opportunity to talk with him and hear his beautiful ideas was deprived from us. As one of his pupils, I would sincerely like to dedicate this memorial article to him as a joint work with him.

More than eleven years has passed since I first met him. It was the year when I started my master course in Waseda University. As many students go thorough, I was struggled with the foundational issues on quantum mechanics. Fortunately, there were many people at Waseda university who could share and discuss the same problem, and I gradually understand that there are several different kinds of questions — about theory and experiment, about physics, mathematics and philosophy, about interpretation and its actual use, etc. Around that time, Professor Tasaki had moved to Waseda University, and it didn't take much time to know that he is a quite rare researcher who can grasp and integrate all these problems together. Since then, I was blessed with a wonderful time to hear and learn so many things from Professor Tasaki. This forms into my basis not only on science but also my life nowadays.

Among many problems I could discuss with him, in this article let me focus on one theme — on the general property on correlations — since we even had a plan to write the paper about this. Unfortunately we later noticed that the similar result had already pointed out by Takesaki [1] in the theory of C^* algebra, and we deferred this plan for a while. Now I feel a great regret that we didn't continue this, since we immediately noticed that the property of correlations universally holds in any physical theories. Moreover, the property has an important application

[1]E-mail: gen[atmark]sic.shibaura-it.ac.jp

in the context of quantum key distribution. Therefore, I believe the fact should be widely known and I would like to use this opportunity to put this into shape in the most general setting as much as possible and give its rigorous proof.

The property of correlations we will discuss is the following:

[A] *If the state of a physical system (in which you are interested) is pure, then the system has no correlations with any other systems (environments).*

This fact is indeed generally true and has many interesting implications. First, experimentalists can assure that their systems has no correlations with any other environment once they check that their system is in a pure state. Notice that whether your system is in a pure state or not can be locally checked (e.g., with a state tomography) even if you don't have any knowledge about the environment. Indeed, in quantum theory, this fact is used as one of the principal reasons for the unconditionally security of some of the protocols of quantum key distribution [2]: Once Alice and Bob assure to share a pure state, then it is guaranteed that their composite system is safely isolated from other system which is possibly prepared by an eavesdropper. Notice that, in quantum theory (but not in classical theory), a pure composite system can have correlations, i.e., *entanglement.* Therefore, Alice and Bob can use their correlations (entanglement) to share the secret keys, which is safely uncorrelated from an eavesdropper. Second, the contraposition of the statement [A] tells that if there are correlations between a system and its environment, the reduced state is a mixed state. In particular, since a pure composite system can have correlations in quantum theory (but again not in classical theory), the reduced state can be a mixed state *even if the total state is in a pure state*, which is one of the peculiar features of quantum systems. This origin of mixtures is sometimes called *improper mixture* [3].

The importance of statement [A] has been pointed out by d'Espagnat and a simple proof is given in quantum systems with finite levels [5][2], although the mathematical part of this had been proved by Takesaki in a C^* algebraic setting (See Lemma 4.11 in [1]). However, in a next section, we show that the statement is indeed a universal fact which is true in any and all operationally valid physical theories. This was also pointed out by other group [6] independently in a slightly restricted setting.

2 General Probabilistic Theories

We start from reviewing the general framework to use probability [7, 8, 9, 10, 11], recently referred as general probabilistic theories [6, 12, 13]. This framework covers not only the classical theory of probability but also quantum theory and indeed mores; any operationally valid physical

[2]One can find the rigorous proof in infinite dimensional Hilbert space in my doctor thesis [4].

theory you can think of should be included here[3]. Our basis is operational and we use the notion of a physical system, a state (preparation), a measurement (of an observable), and a composition of systems. In particular, we assume that in each fixed physical system there is a physical law to determine a probability to get a measurement outcome in a given state: We denote by

$$\Pr\{x \in \Delta \,|X, s\} \tag{1}$$

the *probability to obtain an outcome x in an event Δ when performing a measurement X under a state s*. For instance, in the theory of classical probability, a physical system is represented by a measurable space $(\Omega, \mathcal{A})$[4]. A measurement is a random variable $X : \Omega \to \mathbb{R}$ and a state is a probability measure μ on Ω. The probability to obtain an outcome in an event $\Delta \in \mathcal{A}$ is then given by $\Pr\{x \in \Delta \,|X, \mu\} = \mu(X^{-1}(\Delta))$. Another typical example is the theory of quantum mechanics: A quantum system is represented by a Hilbert space $\mathcal{H}$. A measurement of an observable X is represented by a self-adjoint operator (though most generally by a positive operator valued measure) and a state is represented by a density operator ρ on $\mathcal{H}$. The probability (1) is given by the Born's rule: $\Pr\{x \in \Delta \,|X, \rho\} = \mathrm{tr}(\rho E^X(\Delta))$ where $E^X(\cdot)$ is the spectral measure of X. However, one can go further to formulate the most general framework of probability, which is explained in details in the following.

In order to have an operational meaning in the theory, we require the following natural assumptions [A1]-[A4]:

[A1] (Probability) As mentioned above, we require that in each physical system, there exists a physical law to predict a probability (1), which satisfies the Kolmogorov's axiom of probability. Precisely speaking, we assume that an each measurement X possesses an intrinsic measurable space $(\Omega_X, \mathcal{A}_X)$, which determines the sets of outcomes and events[5], and $\mu_{X,s}(\cdot) := \Pr\{x \in \cdot \,|X, s\}$ with state s gives a probability measure over Ω_X: (i) $0 \leq \mu_{X,s}(\Delta) \leq 1$ for any $\Delta \in \mathcal{A}_X$, (ii) $\mu_{X,s}(\Omega_X) = 1$, and (iii) (Countable Additivity) $\mu_{X,s}(\Delta_1 \cup \Delta_2 \cup \cdots) = \sum_i \mu_{X,s}(\Delta_i)$ for mutually exclusive events $\Delta_1, \Delta_2, \ldots \in \mathcal{A}_X$.

[A2] (Identification of States) We naturally identify states s_1 and s_2 iff the statistical properties for any measurement X under s_1 and s_2 are the same. Namely, $s_1 = s_2$ if and only if

$$\Pr\{x \in \Delta \,|X, s_1\} = \Pr\{x \in \Delta \,|X, s_2\} \quad \forall \Delta \in \mathcal{A}_X$$

[3]There are several motivations to consider this general framework: one of them is for the inquiry of physical principles of quantum theory [13, 14]

[4]Ω is a sample space and $\mathcal{A}$ is a σ-algebra over Ω, i.e., the set of all the events. In the following, readers who are not familiar with the measure theory can always replace Ω to the set of real numbers $\mathbb{R}$ and $\Delta \in \mathcal{A}$ to an interval $[a, b] \subset \mathbb{R}$.

[5]If one (supposed to be a physicist) feels that this is artificially too general, think that $\Omega_X = \mathbb{R}$ and $\mathcal{A}_X = \mathcal{B}(\mathbb{R})$ (the Borel set over $\mathbb{R}$) for any measurement X. However, in general, each measurement could have different and arbitrary set of measurement outcomes.

for any measurement X. (This usually gives an operational definition of states[6].)

[A3] (Probabilistic Mixture of States) We assume that for any states s_1 and s_2 and for any probability $p \in [0,1]$ there exists a state s which satisfies

$$\Pr\{x \in \Delta \mid X, s\} = p\Pr\{x \in \Delta \mid X, s_1\} + (1-p)\Pr\{x \in \Delta \mid X, s_2\} \quad \forall \Delta \in \mathcal{A}_X, \tag{2}$$

for any measurement X. A typical preparation (realization) of such state is given by a probabilistic mixture of states [15]: one can operationally prepare s by preparing state s_1 with probability p and state s_2 with probability $1-p$. Note that (2) then follows from the definition of conditional probability and the countable additivity of probability. Notice that from [A2] such state is uniquely determined by the fixed states s_1, s_2 and $p \in [0,1]$; in the following we denote it by $s = \langle p; s_1, s_2 \rangle$ [9]. In the classical and quantum theories, this is given by a convex combination of states[7]. For instance, $\langle p; \rho_1, \rho_2 \rangle = p\rho_1 + (1-p)\rho_2$ with density operators ρ_1, ρ_2 and $p \in [0,1]$.

Now we have an operational definition of a pure state. A state is called a *pure* state iff there exist no preparations with *nontrivial* probabilistic mixture[8]. In other words, s is a pure state iff $s = \langle p; s_1, s_2 \rangle$ for states s_1, s_2 and $p \in (0,1)$ implies $s = s_1 = s_2$. For instance, in quantum systems, a density operator on $\mathcal{H}$ represents a pure state iff it is a one dimensional projection on $\mathcal{H}$. A state is called a *mixed* state if it is not a pure state.

[A4] (Composition of Systems and Relativistic Causality) In order to consider the composition of physical systems A and B, we also assume that there exists a physical law for a joint probability:

$$\Pr\{x \in \Delta, y \in \Gamma \mid X, Y, s\} \quad (\Delta \in \mathcal{A}_X, \Gamma \in \mathcal{A}_Y) \tag{3}$$

for any local measurements X of A and Y of B, which gives the *joint probability to obtain outcomes* $x \in \Delta$ *and* $y \in \Gamma$ *when we perform a joint measurement of* X *and* Y *under a composite state* s. Additionally, we assume the relativistic causality [16] (sometimes referred as the *no-signaling condition*):

$$\Pr\{x \in \Delta, y \in \Omega_Y \mid X, Y, s\} = \Pr\{x \in \Delta, y' \in \Omega_{Y'} \mid X, Y', s\} \quad (\forall \Delta \in \mathcal{A}_X) \tag{4}$$

for any measurement X of A and for any *possibly different* measurements Y and Y' of B. (The same assumption for the change of A and B, of course, should be assumed.) Notice that $\Pr\{x \in \Delta, y \in \Omega_Y \mid X, Y, s\}$ gives the marginal probability distribution of X subject to no-communications between A and B. Therefore, condition (4) assures the impossibility of an

[6] One can also consider an identification of measurements with the same philosophy, but logically this is unnecessary for the following discussion.

[7] Indeed, there always exists a vector representation of states so that $s = \langle p; s_1, s_2 \rangle$ is given by a convex combination of states [9]. However, in the following discussion, we don't resort to any mathematical representation.

[8] We say that state s has a preparation with nontrivial probabilistic mixtures if there exists states s_1, s_2 which are different from s and $p \in (0,1)$ such that $s = \langle p; s_1, s_2 \rangle$.

instantaneously sending of an information (by means of changing Y and Y') from B to system A, which could be located far away each other. Of course, in both classical and quantum systems, this is satisfied[9], assuring the peaceful coexistence of (especially) quantum mechanics and relativity theory.

Now the reduced state s_A of A from a composite state s can be well-defined as a state which satisfies

$$\Pr\{x \in \Delta \,|X, s_A\} := \Pr\{x \in \Delta, y \in \Omega_Y \,|X, Y, s\} \ (\forall \Delta \in \mathcal{A}_X) \tag{5}$$

for any measurement X of A with an arbitrary fixed measurement Y of B[10]. In quantum systems, the reduced state of A is described by the reduced density operator $\rho_A := \mathrm{tr}_B \rho$ as one observes $\Pr\{x \in \Delta, y \in \Omega_Y \,|X, Y, \rho\} = \mathrm{tr}_{AB}(\rho E^X(\Delta) \otimes E^Y(\Omega_Y)) = \mathrm{tr}_{AB}(\rho E^X(\Delta) \otimes \mathbb{I}_B) = \mathrm{tr}_A((\mathrm{tr}_B \rho) E^X(\Delta))$.

Next, a correlation in a composite state is operationally defined. We say that a composite state s has *no correlations* iff there are no statistical correlations for any pair of local measurements X and Y, i.e.,

$$\Pr\{x \in \Delta, y \in \Gamma \,|X, Y, s\} = \Pr\{x \in \Delta \,|X, s_A\} \Pr\{y \in \Gamma \,|Y, s_B\} \quad (\forall \Delta \in \mathcal{A}_X, \Gamma \in \mathcal{A}_Y) \tag{6}$$

for any measurements X of A and Y of B. Otherwise, we say a composite state s has *non-zero correlations*. For instance, in a quantum mechanics, a state with no correlations is represented by a product of the reduced density operators: $\rho = \rho_A \otimes \rho_B$.

Now we are in position to prove the general property of correlations. First, we notice that a preparation of local states by a conditioning is possible: Let s be a composite state and let fix a measurement Y of B and an event $\Gamma \in \mathcal{A}_Y$. Then, unless $\Pr\{y \in \Gamma \,|Y, s_B\} \neq 0$, there exists a local state $s_A^{(Y,\Gamma)}$ of A which satisfies

$$\Pr\{x \in \Delta \,|X, s_A^{(Y,\Gamma)}\} = \frac{\Pr\{x \in \Delta, y \in \Gamma \,|X, Y, s\}}{\Pr\{y \in \Gamma \,|Y, s_B\}} \quad (\forall \Delta \in \mathcal{A}_X) \tag{7}$$

for any measurement X of A. Indeed, since the right hand side of (7) is the conditional probability with a given Γ, the preparation of $s_A^{(Y,\Gamma)}$ is realized by a preparation of state s with a conditioning of a measurement Y to be in an event Γ.

---

[9] In quantum case, the composite system is described by the tensor Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ and the joint probability of a measurement of self-adjoint operators X on $\mathcal{H}_A$ and Y on $\mathcal{H}_B$ under a density operator ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ is given by $\mathrm{tr}_{AB}(\rho E^X(\Delta) \otimes E^Y(\Gamma))$ with spectral projections $E^X(\cdot)$ of X and $E^Y(\cdot)$ of Y. Since $E^Y(\Omega_Y) = \mathbb{I}_B$ for any Y, condition (4) follows.

[10] Alternatively, one can define the reduced state as follows: Operationally, one can define a measurement of X of A in a composite state s of $A + B$ while no measurements on B are performed and let $\Pr\{x \in \Delta \,|X, \emptyset, s\}$ denotes the probability to obtain an output x in $\Delta \in \mathcal{A}_X$ in this situation. Relativistic causality then should also holds as $\Pr\{x \in \Delta, y \in \Omega_Y \,|X, Y, s\} = \Pr\{x \in \Delta \,|X, \emptyset, s\}$ for any Y. Then, the reduced state s_A is defined as the state which satisfies $\Pr\{x \in \Delta \,|X, s_A\} = \Pr\{x \in \Delta \,|X, \emptyset, s\}$, which is the same as (5).

The rigorous statement of [A] is now given by the following theorem:

Theorem 1 *In any general probabilistic theories with [A1] - [A4], if the reduced state s_A from a composite state s of $A+B$ is a pure state, then s has no correlations.*

Proof Assume that s_A is a pure state. Fix arbitrary measurements X of A and Y of B and $\Delta \in \mathcal{A}_X, \Gamma \in \mathcal{A}_Y$. We prove (6) for each case (I)-(III) below:

(Case I) If $\Pr\{y \in \Gamma \,|Y, s_B\} = 0$, then we have $\Pr\{x \in \Delta, y \in \Gamma \,|X, Y, s\} \leq \Pr\{x \in \Omega_X, y \in \Gamma \,|X, Y, s\} = \Pr\{y \in \Gamma \,|Y, s_B\} = 0$ and thus (6) holds.

(Case II) If $\Pr\{y \in \Gamma \,|Y, s_B\} = 1$, then $\Pr\{y \in \Gamma^C \,|Y, s_B\} = 0$ where Γ^C denotes the complement of Γ. Note that, since $\Pr\{x \in \Delta, y \in \Gamma^C \,|X, Y, s\} \leq \Pr\{x \in \Omega_X, y \in \Gamma^C \,|X, Y, s\} = \Pr\{y \in \Gamma^C \,|Y, s_B\} = 0$, we have $\Pr\{x \in \Delta, y \in \Gamma \,|X, Y, s\} = \Pr\{x \in \Delta, y \in \Omega_Y \,|X, Y, s\} = \Pr\{x \in \Delta \,|X, s_A\}$ and thus (6) holds.

(Case III) If $0 < \Pr\{y \in \Gamma \,|Y, s_B\} < 1$, we have local states $s_A^{(Y,\Gamma)}$ and $s_A^{(Y,\Gamma^C)}$ (see (7)) which satisfy

$$\Pr\{x \in \Delta \,|X, s_A^{(Y,\Gamma)}\} = \frac{\Pr\{x \in \Delta, y \in \Gamma \,|X, Y, s\}}{p} \tag{8}$$

$$\begin{aligned}\Pr\{x \in \Delta \,|X, s_A^{(Y,\Gamma^C)}\} &= \frac{\Pr\{x \in \Delta, y \in \Gamma^C \,|X, Y, s\}}{\Pr\{y \in \Gamma^C \,|Y, s_B\}} \\ &= \frac{\Pr\{x \in \Delta | X, s_A\} - \Pr\{x \in \Delta, y \in \Gamma \,|X, Y, s\}}{1-p}\end{aligned} \tag{9}$$

where $p := \Pr\{y \in \Gamma \,|Y, s_B\}$. From (5), (8) and (9), the reduced state s_A satisfies

$$\Pr\{x \in \Delta \,|X, s_A\} = p\Pr\{x \in \Delta \,|X, s_A^{(Y,\Gamma)}\} + (1-p)\Pr\{x \in \Delta \,|X, s_A^{(Y,\Gamma^C)}\}$$

for arbitrary measurement X of A and $\Delta \in \mathcal{A}_X$. This means that the reduced state s_A can be prepared as a probabilistic mixture of state $s_A^{(Y,\Gamma)}$ and $s_A^{(Y,\Gamma^C)}$ with probability p and $1-p$. Since s_A is a pure state and $0 < p < 1$, we have

$$s_A = s_A^{(Y,\Gamma)} = s_A^{(Y,\Gamma^C)}.$$

In particular, from the first equality and (8), we have $\Pr\{x \in \Delta \,|X, s_A\} = \frac{\Pr\{x \in \Delta, y \in \Gamma \,|X, Y, s\}}{p}$ and thus (6) holds. This completes the proof. ■

Note that [A1-A4] are minimum required assumptions for any physical theory with notions of probability as well as pure state and correlations[11]. Therefore, a statement [A] has been proved to hold universally in any operationally valid physical theories.

We conclude this article with a short discussion on the application of Theorem 1 to a key distribution. In a usual argument of quantum key distribution, the unconditional security can be

[11] Note that a similar (and indeed almost parallel) argument is possible without no-signaling condition in [A4] by defining a reduced state of A *depending* on the choice of a measurement Y (or without measurement) of B. However, such argument would be too artificial to present here.

proved *provided that, of course, quantum theory is correct.* However, Theorem 1 can assure the security of key distribution not resort to the validity of quantum theory but to more general and natural assumptions [A1]-[A4]. (For instance, the security of quantum key distribution remains to be guaranteed even if there are some defeats in quantum theory — though nowadays this might be merely an armchair plan.) Precisely speaking, we notice that Theorem 1 is not enough for this application: First, as is also mentioned in Sec. 1, the legitimate users, Alice and Bob, should have non-zero correlations in order to share the secret keys. Therefore, there must exist a *pure* composite state (of Alice and Bob) with non-zero correlations. This holds in quantum systems (with an entanglement) but not in classical systems. Next, Alice and Bob, who are supposed to be located far away, should make sure that their composite system is a pure state. In order for Alice and Bob distantly can do this, another assumption is necessary:

[A5] (Local Tomography): A composite state is characterized by information of correlations, which assures that a composite state is locally determined by means of local measurements and communications.

This is of course valid in both classical and quantum systems. What we have shown is that the property of correlations in Theorem 1 is correct only with [A1]-[A4], but to use this fact for the application of key distribution, we need a pure entanglement and [A5] as well. Fortunately, these can be operationally checked in experiments.

Acknowledgment

I would like to appreciate Dr. S. Ajisaka for giving me a chance to write this article and for his great contribution for projecting and organizing this memorial volume. I am grateful to Dr. K. Imafuku for his continuing discussion and comments. In particular, I learned an application of the correlation property in quantum key distribution from him. I thank Dr. T. Miyamoto for letting me to know Takesaki's result in the theory of C^* algebra and Prof. M. Koashi for his useful comments and advices on Theorem 1. I would also like to appreciate Mrs. Hiroko Tasaki, Prof. Tasaki's wife, for her kind acceptance to allow this letter to be a joint work with him. Finally, I would express my deep and sincere appreciation to Prof. Shuich Tasaki; he would be my perpetual teacher and remains to influence me in the future.

References

[1] M. Takesaki, *Theory of Operator Algebra I* (Springer, 1979).

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, *ibid.* **77**, 2818 (1996); **80**, 2022 (1998); M. Koashi and J.Preskill, *ibid.* **90**, 057902 (2003); M. Koashi, e-print arXiv:quant-ph/0505108.

[3] B. d ' Espagnat, S. C. Italo, Lett. Nuovo Cimento Soc. Ital. Fis. **2**, 823 (1971).

[4] G. Kimura, *State space and dynamics of open quantum systems with N levels* (in Japanese), Doctor Thesis (2004).

[5] B. d ' Espagnat, *Conceptual Foundations of Quantum Mechanics* (Benjamin, Reading, MA, 1976).

[6] H. Barnum, J. Barrett, M. Leifer, and A. Wilce, Phys. Rev. Lett. **99**, 240501 (2007); *ibid*, arXiv:0805.3553.

[7] G. Mackey, *Mathematical Foundations of Quantum Mechanics* (Dover, 1963).

[8] H. Araki, *Einfuhrung in die Axiomatische Quantenfeldtheorie, I, II* (Lecture note distributed by Swiss Federal Institute of Technology, 1962); *Mathematical Theory of Quantum Fields* (Oxford University Press, 1999).

[9] S. P. Gudder, *Stochastic Method in Quantum Mechanics* (Dover, 1979).

[10] M. Ozawa, Rep. Math. Phys. **18**, 11 (1980).

[11] A. S . Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam,1982).

[12] G. Kimura, K. Nuida, and H. Imai, Rep. Math. Phys. **66**, 175 (2010); K. Nuida, G. Kimura, and T. Miyadera, J. Math. Phys. **51**, 093505 (2010).

[13] G. Kimura, K. Nuida, and H. Imai, arXiv:1012.5361; G. Kimura, K. Nuida, arXiv:1012.5350.

[14] C. A. Fuchs, quant-ph/0205039; R. Clifton,J. Bub, and H. Halvorson , Found. Phys. 33, 1561 (2003); B. Dakić and C. Brukner, arXiv:0911.0695; L. Masanes, M. P. Mueller, New J. Phys. **13**, 063001 (2011); G. Chiribella, G. M. D'Ariano, and P. Perinotti, Phys. Rev. A **84**, 012311 (2011).

[15] J. von Neumann, O. Morgenstern, *Theory of Games and Economic Behavior* (Princeton, NJ. Princeton University Press, 1944, sec.ed. 1947, th.ed. 1953).

[16] S. Popescu and D. Rohrlich, Found. Phys. **24**, 379, (1994).