Journal of Quantum Information Science, **2013, 3, 6-9**
http://dx.doi.org/10.4236/jqis.2013.31002 Published Online March 2013 (http://www.scirp.org/journal/jqis)
Scientific Research

Re-Formulation of Mean King's Problem Using Shannon's Entropy

Masakazu Yoshida, Hideki Imai
Graduate School of Science and Engineering, Chuo University, Tokyo, Japan
Email: masakazu-yoshida@imailab.jp

Received November 23, 2012; revised December 30, 2012; accepted January 8, 2013

ABSTRACT

Mean King's problem is formulated as a retrodiction problem among noncommutative observables. In this paper, we reformulate Mean King's problem using Shannon's entropy as the first step of introducing quantum uncertainty relation with delayed classical information. As a result, we give informational and statistical meanings to the estimation on Mean King problem. As its application, we give an alternative proof of nonexistence of solutions of Mean King's problem for qubit system without using entanglement.

Keywords: Mean King's Problem; Quantum Retrodiction Problem; Quantum Estimation Problem; Shannon's Entropy

1. Introduction

In 1987, Vaidman, Aharonov, and Albert [1] introduced Mean King's problem as a challenge to an uncertainty principle among noncommutative observables. The problem can be interpreted as a kind of quantum estimation (or states discrimination) problem with a delayed classical information. In the proposed setting, two players King and Alice play their roles: King asks Alice to prepare qubit system in an arbitrary state. King measures the system with a projective measurement relevant to one of observables σ_x, σ_y, and σ_z. Alice is permitted to measure the post measurement state once in an arbitrary measurement. After Alice's measurement, King reveals the kind of observable employed by him to Alice. Then, Alice should retrodict King's outcome by using her outcome and the kind of observable. It is a problem to construct a pair of an initial quantum state and a measurement employed by Alice such that she estimates King's outcome with Probability 1, in which case we say that there exists a solution to the problem.

In the original work [1], it is shown that there is such a pair provided that Alice uses an entanglement: That is, Alice prepares not only one qubit system but also an ancillary qubit system secretly in the Bell state. Then, Alice gives one of the systems to King and the other system is kept by herself. She measures the bipartite system in the post measurement state and then can retrodict the King's output after King's reveal of his measurement kinds.

Mean King's problem has been generalized concerning the prepared quantum system and King's measurements [2-7]. In particular, it has been proved [2-5] that Alice can estimate King's outcome by using a maximally entangled state in a setting that King measures one of the systems with one of projective measurements constructed from Mutually Unbiased Basis [8,9]. On the other hand, Alice cannot retrodict the outcome with certainty without using entangled states in the setting [6,7]. In the reference, an upper bound of the success probability is also introduced.

In this paper, we reformulate Mean King's problem from a viewpoint of Shannon's entropy. We can naturally characterize the solution by means of the zero conditional entropy of King's outcome given Alice's outcome and kind of King's measurement. As its application, we give an alternative proof of nonexistence of solutions of Mean King's problem for qubit setting without using any entangled state.

This paper is organized as follows. In the next section, we introduce a general setting of Mean King's problem. In Section 3, we reformulate the problem using Shannon's conditional entropy. In Section 4, we give an alternative proof of nonexistence of solutions. Finally, in Section 5, we summarize this paper.

2. Setting of General Mean King's Problem

We introduce a general setting of Mean King's problem. The problem is constructed from the following steps:

1) By the King's order, Alice prepares a quantum system S_K, described by a d-dimensional Hilbert space $_K$, in an arbitrary initial state.

2) King performs one of measurements

$M^k = \left(M_j^k\right)_{j=0}^m, \left(k = 0,1, \quad ,m'\right)$ constructed from measurement operators on the system and obtains an outcome j.

[Remind that $\left(M_j^k\right)_{j=0}^m$ satisfies $\sum_{j=0}^m M_j^{k\dagger} M_j^k = I$, probability of obtaining an outcome j from a measurement of a state ρ is given by $trM_j^{k\dagger} M_j^k \rho$, then the post measurement state is given by $M_j^k \rho M_j^{k\dagger} \big/ trM_j^{k\dagger} M_j^k \rho$ [10,11]].

3) Alice performs a POVM (Positive Operator Valued Measure) measurement $R = \left(R_i\right)_{i=0}^n$ on the system in the post measurement state and obtains an outcome i.

[Remind that $\left(R_i\right)_{i=0}^n$ is called a POVM if $\sum_{i=0}^n R_i = I$ and $R_i \geq 0$ hold for any i [10,11]].

4) After Alice's measurement, King reveals the kind of measurement M^k to Alice.

5) Alice tries to estimate King's outcome j perfectly with her measurement outcome i and King's measurement k.

With given d and measurements $M^k = \left(M_j^k\right)_{j=0}^m$, we say that a solution to the Mean King's problem exists if and only if a pair of an initial state and a measurement employed by Alice exist such that she estimates King's outcome with Probability 1.

Notice that Alice can utilize an entanglement: In step 1), she secretly prepares an ancilla system S_A and chooses an appropriate entangled state on the bipartite system $S_K + S_A$. In Step 3), she performs a general measurement (POVM measurement) on the bipartite system.

In the next section, we reformulate the problem using Shannon's conditional entropy.

3. Re-Formulation of the Problem

Let K, J, I be random variables expressing the kind of the measurements employed by King, the outcomes obtained by King, and the outcomes obtained by Alice's measurement *R*, respectively. Then, we can reformulate the Mean King's problem using the conditional entropy as follows:

Find an initial state ρ and a measurement R such that

$$H\left(J \middle| I, K\right) = 0, \tag{1}$$

where $H\left(\cdot\middle|\cdot\right)$ denotes Shannon's conditional entropy.

Note that $H\left(J \middle| I\right)$ is generally strictly positive, otherwise Alice can guess King's outcome without a delayed information K. By the chain rule of the conditional entropy, Equation (1) is equivalent to the following relation:

$$H\left(K, J \middle| I\right) = H\left(K \middle| I\right) \cdot \tag{2}$$

Let $P_{K,J,I}\left(k, j, i\right)$ be a joint probability of K, J, I, and let $P_{K,I}\left(k, i\right) = \sum_j P_{K,J,I}\left(k, j, i\right)$ be the marginal joint probability of K and I. We find that Equation (2) is equivalent to

$$P_{K,J,I}\left(k, j, i\right) = 0 \text{ or } P_{K,J,I}\left(k, j, i\right) = P_{K,I}\left(k, i\right), \tag{3}$$

for each K, J, I. Indeed, by the definition of conditional entropy, we can rewrite Equation (2) as follow:

$$\begin{aligned} &-\sum_{k,j,i} P_{K,J,I}\left(k, j, i\right) \log P_{K,J,I}\left(k, j \middle| i\right) \\ &= -\sum_{k,i} P_{K,I}\left(k, i\right) \log P_{K,I}\left(k \middle| i\right), \end{aligned} \tag{2'}$$

where $P\left(\cdot\middle|\cdot\right)$ denotes a conditional probability corresponding to the random variables. If $P_I\left(i\right)\left(= \sum_{k,j} P_{K,J,I}\left(k, j, i\right)\right) \neq 0$ holds, using the monotonically increasing property $\log P_{K,J,I}\left(k, j, i\right) \leq \log P_{K,I}\left(k, i\right)$, Equation (2') is equivalent to

$$\begin{aligned} &P_{K,J,I}\left(k, j, i\right) \log P_{K,J,I}\left(k, j, i\right) \\ &= P_{K,J,I}\left(k, j, i\right) \log P_{K,I}\left(k, i\right), \end{aligned} \tag{2''}$$

for any k, j, i. Noting that $P_I\left(i\right) = 0$ holds if and only if $P_{K,J,I}\left(k, j, i\right) = 0$ for any k, i, Equation (2') is equivalent to (2") also in this case. Therefore, we have obtained the equivalence between Equations (2) and (3). In our setting, a solution to the Mean King's problem is to find an initial state ρ and a measurement R such that Conditions (1), (2), or (3) holds.

4. Nonexistence of Solutions in Qubit Setting

In this section, we give an alternate proof of nonexistence of solutions to Mean King's problem without using entanglement in qubit system. In the setting, Alice prepares not bipartite system but one qubit in a state ρ. Recall that qubit is described by 2-dimensional complex vector space ^{2}. King employs one of three projective measurements,

$$M^k = \left(M_j^k := \left|\psi_j^k\right\rangle\left\langle\psi_j^k\right|\right)_{j=0,1}, \left(k = 0,1,2\right),$$

where $\left\{\left|\psi_j^k\right\rangle\right\}_{j=0,1}$ are three kinds of orthonormal basis on ^{2}, e.g., three pairs of eigenvectors corresponding to Paulli matrices σ_x, σ_y, and σ_z. The post measurement state is $\left|\psi_j^k\right\rangle$ if King chooses $K = k$ and obtained an outcome j from the projection postulate. After that, Alice measures qubit in the post measurement state with a POVM measurement $R = \left(R_i\right)_{i=0,1}$. Then, we obtain the following joint probability,

$$P_{K,I,J}(k,j,i) = P_K(k)\langle\psi_j^k|\rho|\psi_j^k\rangle\langle\psi_j^k|R_i|\psi_j^k\rangle, \quad (4)$$

where $P_K(k)$ denotes the probability that King chooses the projective measurement M^k. For a fixed k, we observe that there are three types A, B, C of the joint probabilities satisfying Equation (3) characterized as follows:

Type A: There uniquely exists a pair of outcomes (j,i) such that $P_{K,J,I}(k,j,i) \neq 0$ holds. $P_{K,J,I}(k,j',i') = 0$ holds for any $(j',i') \neq (j,i)$.

Type B: There uniquely exists an outcome j such that $P_{K,J,I}(k,j,i) \neq 0$ holds for any i. $P_{K,J,I}(k,j',i) = 0$ holds for $j' \neq j$ and any i.

Type C: $P_{K,J,I}(k,j,i) \neq 0$, $P_{K,J,I}(k,j,i') = 0$, $P_{K,J,I}(k,j',i') \neq 0$, and $P_{K,J,I}(k,j',i) = 0$ hold for $i \neq i'$ and $j \neq j'$.

In **Figure 1**, we show a complete classification of probabilities for each type, where the number of kinds of the probabilities satisfying Type A, Type B, and Type C is 8. Now, we try to find ρ and R such that each three joint probabilities for $k = 0,1,2$ satisfies any of the above 8 kinds of the probabilities.

By using Equation (4), we obtain the equivalent relations for each types and the joint probability $P_{K,J,I}(k,j,i)$ as follows:

- The joint probability satisfies <u>Type A</u> if and only if $(\rho = M_0^k, R_0 = M_0^k, R_1 = M_1^k)$ or $(\rho = M_0^k, R_0 = M_1^k, R_1 = M_0^k)$ or $(\rho = M_1^k, R_0 = M_0^k, R_1 = M_1^k)$ or $(\rho = M_1^k, R_0 = M_1^k, R_1 = M_0^k)$ hold.
- The joint probability satisfies <u>Type B</u> if and only if $(\rho = M_0^k, R_0 \neq M_0^k, M_1^k, R_1 \neq M_0^k, M_1^k)$ or $(\rho = M_1^k, R_0 \neq M_0^k, M_1^k, R_1 \neq M_0^k, M_1^k)$ hold.
- The joint probability satisfies <u>Type C</u> if and only if $(\rho \neq M_0^k, M_1^k, R_0 = M_0^k, R_1 = M_1^k)$ or $(\rho \neq M_0^k, M_1^k, R_0 = M_1^k, R_1 = M_0^k)$ hold.

Let us focus on two probabilities $P_{K,J,I}(k,j,i)$ and $P_{K,J,I}(k',j,i)$ with $k \neq k'$. If both are Type A, $\rho = M_0^k$ or M_1^k holds for k and $\rho = M_0^{k'}$ or $M_1^{k'}$ holds for k'. Therefore, we cannot construct the probability satisfying a pair of (Type A, Type A). This fact is also derived from construction of R_0 and R_1. In a similar way, we cannot construct the probability satisfy- ing any of pairs of types (Type B, Type B), (Type C, Type C), (Type A, Type B), (Type B, Type A), (Type C, Type A), and (Type A, Type C). On the other hand, there are ρ and R such that the probabilities satisfy any of pairs of (Type B, Type C) and (Type C, Type B). For instance, $(\rho = M_0^k, R_0 = M_0^{k'}, R_1 = M_1^{k'})$ satisfies (Type B, Type C).

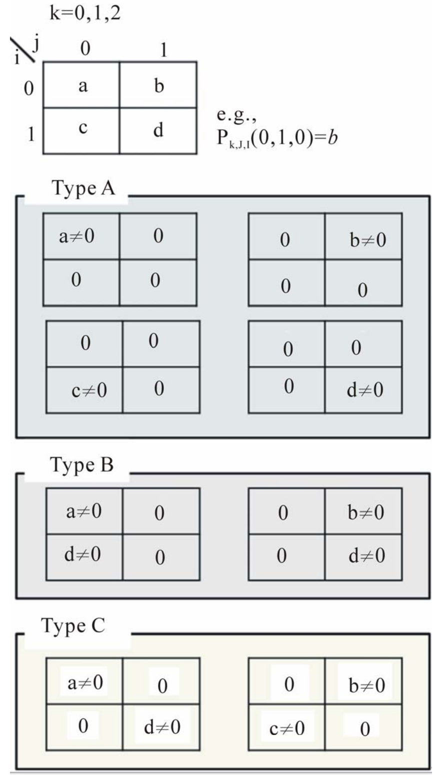

Figure 1. Three types of the probabilities.

According to the above fact, we obtain $H(J|I,K) = 0$ for two kinds of the projective measurements M^k and $M^{k'}$. However, it turns out that Alice cannot find a solution for three kinds of projective measurement as follows: First, from the above discussion, candidates of possibly pairs are (Type B, Type C, Type B) and (Type C, Type B, Type C) corresponding to $k = 0,1,2$. However, the first one, $\rho = M_0^0$ or M_1^0 holds for Type B of 1st term and $\rho = M_0^2$ or M_1^2 holds for Type B of 3rd term. Therefore, the first one is ruled out of the candidate. In a similar way, the second one is also ruled out of the candidate from a viewpoint of the measurement R. Thus, we can conclude that $H(J|I,K) = 0$ dose not hold for three kinds of the measurements.

5. Conclusion

We reformulated Mean King's problem and gave new insight to the problem from a view point of Shannon's entropy. As its application, we gave an alternative proof of nonexistence of solutions for qubit setting without using entanglement. We expect that new insights from viewpoints of quantum probabilistic theory, quantum communication, and so on will be given to Mean King's problem by using the reformulation given in this paper.

REFERENCES

[1] L. Vaidman, Y. Aharonov and D. Z. Albert, "How to Ascertain the Values of σx, σy, and σz of a Spin-1/2 Particle," *Physical Review Letters*, Vol. 58, No. 14, 1987, pp. 1385-1387. doi:10.1103/PhysRevLett.58.1385

[2] B.-G. Englert and Y. Aharonov, "The Mean King's Problem: Prime Degrees of Freedom," *Physics Letters A*, Vol. 284, No. 1, 2001, pp. 1-5. doi:10.1016/S0375-9601(01)00271-7

[3] A. Hayashi, M. Horibe and T. Hashimoto, "Mean King's Problem with Mutually Unbiased Bases and Orthogonal Latin Squares," *Physical Review A*, Vol. 71, No 5, 2005, Article ID: 052331. doi:10.1103/PhysRevA.71.052331

[4] G. Kimura, H. Tanaka and M. Ozawa, "Solution to the Mean King's Problem with Mutually Unbiased Bases for Arbitrary Levels," *Physical Review A*, Vol. 73, No. 5, 2006, Article ID: 050301(R). doi:10.1103/PhysRevA.73.050301

[5] M. Reimpell and R. F. Werner, "A Meaner King Uses Biased Bases," *Physical Review A*, Vol. 75, No. 6, 2007, Article ID: 062334. doi:10.1103/PhysRevA.75.062334

[6] G. Kimura, H. Tanaka and M. Ozawa, "Comments on "Best Conventional Solutions to the King's Problem," *Zeitschrift für Naturforschung*, Vol. 62a, 2007, pp. 152-156. http://www.znaturforsch.com/aa/v62a/s62a0152.pdf

[7] P. K. Aravind, "Best Conventional Solutions to the King's Problem," *Zeitschrift für Naturforschung*, Vol. 58a, 2003, pp. 682-690. http://www.znaturforsch.com/aa/v58a/s58a0085.pdf

[8] I. D. Ivanovic, "Geometrical Description of Quantum State Determination," *Journal of Physics A*: *Mathematical and General*, Vol. 14, No. 12, 1981, pp. 3241-3245. doi:10.1088/0305-4470/14/12/019

[9] W. K. Wootters and B. D. Fields, "Optimal State-Determination by Mutually Unbiased Measurements," *Annals of Physics*, Vol. 191, No. 2, 1988, pp. 363-381. doi:10.1016/0003-4916(89)90322-9

[10] M. A. Nielsen and I. L. Chuang, "Quantum Computation and Quantum Information," Cambridge University Press, Cambridge, 2000.

[11] M. Hayashi, "Quantum Information an Introduction," Springer-Verlag, Berlin and Heidelberg, 2006.

