Masakazu Yoshida

A Solution of Quantum Estimation Problem Using Quantum Error-Correcting Codes and Its Applications

Acknowledgements

I would like to express my sincere gratitude to my supervisor, Prof.Hideki Imai for providing me this precious study opportunity as a Ph.D student. I especially would like to express my deepest appreciation to my advisers, Dr.Takayuki Miyadera, associate professor of Kyoto University, Dr.Manabu Hagiwara, research scientist of National Institute of Advanced Industrial Science and Technology, Dr.Gen Kimura, assistant professor of Shibaura Institute of Thechnology, and Dr.Takashi Kitagawa, associate professor of Center for Research and Development Initiative, Chuo University, for their elaborated guidance, considerable encouragement, and invaluable discussion that have made my greatest research and my study life unforgettable. I would like to express my gratitude to Prof.Hideki Imai, Prof.Shuji Tsukiyama, Prof.Chao Jinhui, in Chuo University, and Dr.Kentaro Imafuku, senior research scientist of National Institute of Advanced Industrial Science and Technology, for taking on examiners of the Ph.D thesis. Finally I would like to extend my indebtedness to my family for their endless love, understanding, support, encouragement, and sacrifice throughout my study.

Abstract

Quantum information theory plays a role of not only a resource of advanced technologies such as quantum cryptography, quantum computer, and so on, but also a bridge between information science and physics. It is necessary for remarkable development of scientific technology and engineering. We focus on Mean King's problem which is a kind of quantum estimation problems with delayed information. This problem is also interpreted as an uncertainty principle among noncommutative observables with delayed information. That is, if Mean King's problem is solved with several methods, it induces improvement of the precision of the measurements with the delayed information in the experimental setting corresponding to the problem. A purpose of research shown in this thesis is to give new information scientific insights to the problem and to obtain novel knowledge about the problem. Specifically, we show a solution to the problem using quantum error-correcting codes and reformulate the problem using Shannon entropy. We also consider the relationship between solutions to the problem and security of quantum key distribution with the problem.

Mean King's problem is told as a tale that mean King gives physicist Alice a retrodiction problem, and is constructed form the following steps: 1) Alice's preparation of an initial quantum state, 2) King's measurement, 3) Alice's measurement, 4) Revealing the measurement employed by King as a delayed information, 5) Estimating King's outcome with Alice's outcome and the delayed information. In this problem, we try to find a pair of an initial state and a measurement employed by Alice such that she can estimate King's outcome perfectly. This problem is solved in several settings, for instance, generalization of King's measurements, preparation of entanglement as an initial state, and so on. The problem is also applied to quantum key distribution protocol as which is a technique to share secret keys used for one-time pad cryptosystem. Security analysis of the protocol is studied against several attack models. In this way, both of the problem and the protocol are studied in the previous works. However, those works are results from viewpoints of physics and information science, respectively.

In the thesis, we show three main results. As the first result, we show a solution to general Mean King's problem using quantum error-correcting codes which are a technique to prevent disturbing of quantum states on quantum communications, and so on. We also prove existence of solutions of the problem in several cases. Furthermore, we extend classes of settings of the problem solved using the above solution method. As the second result, we reformulate Mean King's problem using Shannon entropy and introduce an alternative proof of nonexistence of solutions to the problem in a case of qubit system without quantum entanglement. In the last result, we modify measurement scheme in the quantum key distribution protocol using Mean King's problem, and consider security of the protocol against several attacks.

As a result, we show that solving Mean King's problem is necessary but not sufficient to construct secure quantum key distribution protocols. Making an outline of something, from the first and the second results, we give new informational scientific insights to Mean King's problem from viewpoints of quantum coding theory and information theory. From the last result, we give a new physical insight to security analysis of the quantum key distribution protocols from a viewpoint of the quantum estimation problems.

Contents

List of Figures

List of Tables

Notation

- $\mathbb{C}$ and $\mathbb{R}$ denote complex numbers and real numbers, respectively.
- $\mathbb{F}_2 = \{0, 1\}$ denotes the prime field with characteristic number 2.
- i denotes the imaginary unit.
- e denotes the Napier's constant.
- $a := b$ denotes "a is defined as b ".
- $\forall$ denotes "for any ".
- $\exists$ denotes "there exist(s) ". $\exists!$ denotes "there uniquely exist(s) ".
- For a complex number α, $\bar{\alpha}$ denotes the complex conjugate of α.
- For a matrix T and a vector x, $T^\top$ and $x^\top$ denote the transpose of T and x, respectively.
- For a matrix T and a vector x, $\bar{T}$ and $\bar{x}$ denote the complex conjugate of T and x, respectively.
- For a vector space V, $\mathrm{dim}V$ denotes the dimension of V.
- For a subset W of a vector space V over $\mathbb{C}$, $\mathrm{span}W$ denotes the subvector space spanned by W.
- For an ordered set A, $\max A$ denotes the maximum element of A.
- For an ordered set A, $\sup A$ denotes the supremum element of A.
- For an ordered set A, $\inf A$ denotes the infimum element of A.
- $\log_b(\cdot)$ denotes logarithm function with base b, especially $\log(\cdot)$ denotes logarithm function with base 2.
- $|\cdot|$ denotes absolute value.
- For vector spaces V and V', $V \simeq V'$ denotes "V is isomorphic to V'".

Chapter 1

Introduction

1.1 Back Ground

Engineering has made remarkable development in the twentieth century. In particular, software engineering and materials engineering play crucial roles. We focus on materials engineering. The field has been applied to hardware industry such as semiconductors, integrated circuits, and so on as it is developed. On the other hand, software engineering has been applied to software industry such as information systems, software applications, and so on as it is developed. As seen from the above, applications of those engineerings are indispensable to carrying out life in society. However, we should review the engineerings and give new insights to them if stagnation of progress of them is shown. Indeed, it is expected that there is a limit of the progress of hardware industry in the conventional thoughts and methodology, e.g., a limit of integration of electronic circuits, a limit of low power consumption, and so on. For further evolution, we suggest consideration of information science applied to software engineering from a viewpoint of physics applied to materials engineering to researchers of industry and engineering, and vice versa. Thus, we hope that novel theory, engineering, and technology are developed from the combined fields. To do so, we need paradigm shift in engineering and science. Quantum information theory could be a solution for the purpose. Quantum information theory serves to bridge a gap between physics and information science on the basis of probabilistic theory. Thus, the theory gives new physical insight to information science and also gives new information scientific insight to physics conversely.

Electronic devices are treated as black boxes when we design information systems, i.e., we focus on only inputs and outputs of the devices and disregard microscopic changes in the devices. However, the smaller the devices and its circuits become, the more important the changes become. Such changes interpreted as phenomena in quantum physics are called quantum effects. It is expected that performance of whole information system could be enhanced if we made active use of quantum effects for designing the system. Generally, quantum information theory is a field of study where quantum effects are used for wide variety of areas such as information processing, computation, and so on. However, it has no consensus of definition of the theory. Quantum information theory made progress as not a part of quantum physics but a role of a resource of future technologies. Indeed, experts of cryptography focused on the theory when quantum cryptography was introduced in 1984. Furthermore, many researchers of computation theory, information theory, mathematical science, physics, and so on have been studying quantum information theory since an amazing quantum algorithm was introduced and computational power of quantum computation was predicted in 1994.

Quantum cryptography was introduced by Bennett and Brassard in 1984 [1]. The proposed technique is a combination of quantum key distribution and one-time pad cryptosystem. Quantum key distribution is a kind of schemes of sharing secret keys used for symmetric cryptography by using quantum effects of qubit systems. No one generally distinguish quantum states of qubit systems in principle. Therefore, an eavesdropper cannot gain information from encoded qubit systems according to secret keys on a quantum channel. Thus , it is expected that quantum key distribution could be unconditional security against any eavesdropper. Most famous and impactful quantum algorithm was introduced by Shor in 1994 [2]. Non quantum useful techniques for factorization of large size integer are not known. However, we can factorize large size integer in realistic time by using the algorithm on quantum computer. In quantum physics, we can prepare one quantum system in two kinds of quantum states probabilistically and simultaneously. This principle is called quantum superposition. Quantum superposition enables us to realize massively parallel computing. Shor's algorithm using quantum superposition is implemented on quantum computer. Feasibility of quantum computer is not known. However, the impact of quantum computer and Shor's algorithm on society is great since several cryptosystems are easily deciphered by using the techniques.

Quantum information theory became popular and also had a positive impact on quantum physics as its applied technologies were suggested. Quantum teleportation which sounds too good to be true was introduced in 1993 [3]. This technique enables us to transmit any quantum state from one location to another. Basic quantum teleportation is realized with so called EPR state (later it is called Bell state) which is a kind of quantum entangled states. In quantum physics, EPR state plays a crucial role of so called EPR paradox. In 1935, Einstein, Podolsky, and Rosen introduced the paradox as a claim against quantum physics [4]. They claimed that quantum physics is not perfect even if quantum physics is correct. They also believed that there is a theory with which we can describe element of reality perfectly. However, it was shown that their claim is wrong with accepting entanglement. Thus, quantum entanglement is sensitive subject and requires careful handling over the years. However, the subject was reconsidered as the applied technologies such as quantum teleportation were introduced. Moreover, new fundamental subjects such as separability of entanglement, a boundary between quantum physics and Newtonian physics from a viewpoint of entanglement, and so on have been being considered. In this manner, both of applied subjects and fundamental subjects in quantum information theory are important and interesting. Furthermore, the theory is an example of bridges between science and engineering, and plays an essential role as a future resource for remarkable progress of both of science and engineering.

We focus on quantum estimation problems because the problems have aspects as a fundamental subject, an applied subject, furthermore, reading of information be condensed to the problems. Indeed, there is no method of reading information from objects except for identifying information by estimating the objects. In quantum physics, as we mentioned the above, we cannot distinguish quantum states of quantum systems in generally. Thus, we cannot estimate quantum states (information is possibly encoded to them) perfectly by distinguishing the quantum states. However, it is considered whether we can estimate or distinguish the states partially with allowing error probability. Those problems are considered as so called quantum hypothesis testing, discrimination of quantum states problem, and so on. Those subjects are closely to allied subjects or fundamental subjects such as quantum communications and quantum uncertainty principles, respectively.

In this thesis, we study Mean King's problem as a kind of quantum estimation (discrimination or distinguishing) problems with delayed information. In 1987, Vaidman, Aharonov, and Albert introduced Mean King's problem as a challenge to an uncertainty principle among noncommutative observables [5]. In the proposed setting, the problem is told as a tale that mean King and physicist Alice play their roles: King asks Alice to prepare qubit system (two-level quantum system) in an arbitrary quantum state. King measures the system with a measurement corresponding to one of three observables. Alice is permitted to measure the post measurement state once with 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. Mean King's problem has two aspects of a pre- and post-selected model and an uncertainty principle with delayed information. As the first aspect, we try to give value 1 to conditional probability that King obtains an outcome given a pair of a pre-selected state (an initial state) and a post-selected state (a sate after Alice measures the system). Recently, the pre- and post-selected models are studied as weak measurements, strong measurements, and so on. As the second aspect, we try to decrease uncertainty among noncommutative observables employed by King with delayed information. Note that we can estimate King's outcome perfectly if the observables are commutative with one another. Mean King's problem is interpreted as a problem that we try to eliminate uncertainty of measuring precision with the delayed information.

In the original setting, Mean King's problem was solved by using Bell state as an initial state. In this case, Alice prepares a bipartite system and sends one of the systems to King. She measures the bipartite system in the post measurement state. Many other studies were introduced (later, we introduce the details in Chapter 6) in several settings: generalized King's measurements, state preparations with entanglement, state preparations without entanglement. However, the problem in those related works was considered only as a kind of physical problems. In 2001, Bub introduced a quantum key distribution protocol using Mean King's problem [6]. In the protocol, Alice and King try to share secret key used for one-time pad cryptosystem. Alice obtains an outcome as a result of estimation of King's outcome in the problem. Alice and King can share same outcome if Alice can estimate King's outcome perfectly. Then, they share secret key transposed from the outcomes. In the related works, security of the protocol was analyzed against several attack models (later, we introduce the details in Chapter 6). Those works are interesting and important as security analyses of quantum key distribution protocols. However, it is not said that physical significance of the results is clarified.

1.2 Research Results

A purpose of the thesis is to give new information scientific insights to Mean King's problem, and new physical insights to quantum key distribution protocol using the problem. Thus, we show novel solutions to the general Mean King's problem and consider physical significance of the quantum key distribution using Mean King's problem. In this thesis, we introduce three main results for this purpose.

As the first result, we clarify the relationship between Mean King's problem and quantum error-correcting codes which are a technique used for guaranteeing performance of quantum communication, computation, and so on. We show a solution of general Mean King's problem by using quantum error-correcting codes. By interpreting King's measurements as an error on the initial state, we show that the state is a quantum error-correcting code against the error and a kind of error detection gives one of the solutions of Mean King's problem. Existence of our solution is shown for prime-power dimensional quantum systems. By constructing the problem solved by our solution method from any orthonormal bases, we expand the class of setting of the problem that the solution exists.

As the second result, we reformulate Mean King's problem from a viewpoint of Shannon 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 proof of nonexistence of solutions of Mean King's problem for qubit setting without using any entangled state.

As the last result, we propose and analyze modified quantum key distribution protocols using Mean King's problem. Note that the above original protocol proposed by Bub employs Alice's measurement that can solve Mean King's problem for three observables, while the protocol uses only a pair of observables. We propose three protocols using simplified observables that solve Mean King's problem for a pair of observables by using the solution method given in the first result. We analyze security of the protocols against three attack models. We show that two of the protocols are insecure against rather simple attacks. It means that not all the solutions of Mean King problem for the pair of observables are available for secure quantum key distribution. On the other hand, nontrivial information-disturbance theorems, which mean that no one can gain information from quantum systems without disturbing quantum state of the system, holds for the original protocol and one of proposed protocols. That is, the protocols could be secure against the attack models.

1.3 Thesis Overview

This thesis is organized as follows. In the next chapter, we remind mathematical materials to introduce quantum information theory. In Chapter 3, we introduce quantum information theory from a viewpoint of axiomatism of quantum physics. In Chapter 4 and 5, we review basics of quantum error-correcting codes and quantum cryptography, and also review modern coding theory and modern cryptography. In Chapter 6, we introduce conventional setting of Mean King's problem and a quantum key distribution protocol using the problem. We introduce main results after the Chapter 6. In Chapter 7, we derive a solution of general Mean King's problem using quantum error-correcting codes as the first main result. In Chapter 8, the problem is reformulated from a viewpoint of Shannon entropy as the second main result. In Chapter 9, we analyze security of the protocol and derive several information disturbance theorems as the third main result. Finally, in Chapter 10, we summarize this thesis.

Chapter 2

Mathematical Materials

2.1 Hilbert Space and Linear Operator

We review Hilbert spaces, linear operators, and its properties [1] . Let V be a complex vector space. A map $(\cdot, \cdot) : V \times V \to \mathbb{C}$ is called an inner product [2] if the followings hold:

1. $(x, \alpha y + \beta z) = \alpha(x, y) + \beta(x, z), \quad \forall \alpha, \beta \in \mathbb{C}, \ \forall x, y, z \in V,$
2. $(x, y) = \overline{(y, x)}, \quad \forall x, y \in V,$
3. $(x, x) \geq 0, \quad \forall x \in V,$
4. $(x, x) = 0$ if and only if $x = 0, \quad \forall x \in V.$

Remark that the above condition 1 is different from a condition in linear algebra [3] as a matter of principle of physics. We define a norm $\|\cdot\| := (\cdot, \cdot)^{1/2}$ using the inner product. Let $E = \{e_i\}_{i=1}^d$ be a base of d dimensional complex vector space. E is called an orthonormal base (ONB) if $(e_i, e_j) = \delta_{ij}$ holds, where $\delta_{ij} : (i, j) \mapsto k \in \{0, 1\}$ so called Kronecker delta is defined as $\delta_{ij} = 1$ for $i = j$ and $\delta_{ij} = 0$ for $i \neq j$.

Definition 1 *A complex vector space $\mathcal{H}$ is called a (complex) Hilbert space if an inner product is equipped on $\mathcal{H}$ and $\mathcal{H}$ is complete [4] for a norm defined by the inner product.*

Throughout this thesis, complex vector spaces and Hilbert spaces are **finite dimensional spaces**.

[1] For more details, see Ref.[7, 8, 9, 10, 11, 12].

[2] For sets A and B, direct sum of A and B is described as $A \times B := \{(a, b) \mid a \in A, b \in B\}$. For vector spaces, we use the notation in a similar way.

[3] In linear algebra, the condition 1 is $(\alpha x + \beta y, z) = \alpha(x, z) + \beta(y, z), \forall \alpha, \beta \in \mathbb{C}, \forall x, y, z \in V$.

[4] $\mathcal{H}$ is called complete if $\lim_{n,m\to\infty} \|a_n - a_m\| = 0$ holds for an arbitrary sequence of vectors $(a_l)_l$, then there exists $a \in \mathcal{H}$ such that $\lim_{n\to\infty} \|a_n - a\| = 0$.

In quantum physics, Dirac's bra-ket notation is used for describing a vector. Let $\mathcal{H}$ be a Hilbert space. $|x\rangle$ is called a ket vector for a vector $x \in \mathcal{H}$ and a bra vector $\langle x|$ denotes the dual vector [5] for x. We describe an inner product with bra-ket notation:

$$\langle x|y\rangle := \langle x|(|y\rangle) = (x, y),$$

for $x, y \in \mathcal{H}$.

$T : \mathcal{H} \to \mathcal{H}$ is called a linear operator on $\mathcal{H}$ if $T(\alpha|x\rangle + \beta|y\rangle) = \alpha T|x\rangle + \beta T|y\rangle$ holds for any $|x\rangle, |y\rangle \in \mathcal{H}$ and $\alpha, \beta \in \mathbb{C}$. Define a trace

$$\operatorname{tr} T := \sum_i \langle e_i|T|e_i\rangle,$$

where $\{e_i\}_i$ is an ONB of $\mathcal{H}$ and $\langle x|Ty\rangle = \langle x|T|y\rangle := (|x\rangle, T|y\rangle)$. Remark that $\sum_i \langle e_i|T|e_i\rangle = \sum_i \langle f_i|T|f_i\rangle$ for any ONBs $\{e_i\}_i$ and $\{f_i\}_i$. Trace has the following properties: (1) $\operatorname{tr} TR = \operatorname{tr} RT$, (2) $\operatorname{tr}(\alpha T + \beta R) = \alpha \operatorname{tr} T + \beta \operatorname{tr} R$, for any operators T, R and $\alpha, \beta \in \mathbb{C}$.

Let T be a linear operator on a Hilbert space $\mathcal{H}$. A linear operator $T^\dagger$ on $\mathcal{H}$ is called an adjoint operator of T if

$$(|x\rangle, T|y\rangle) = (T^\dagger|x\rangle, |y\rangle), \quad \forall |x\rangle, |y\rangle \in \mathcal{H},$$

holds. Using the above notation, the dual vector for $T|x\rangle$ is $\langle Tx| = \langle x|T^\dagger$. Remark that there uniquely exists the adjoint operator for a fixed linear operator. This is shown using the Riesz representation theorem. We can prove the following properties for any linear operators T and R easily:

1. $(T + R)^\dagger = T^\dagger + R^\dagger$,
2. $(\alpha T)^\dagger = \overline{\alpha} T^\dagger, \quad \forall \alpha \in \mathbb{C}$,
3. $(TR)^\dagger = R^\dagger T^\dagger$,
4. $(T^\dagger)^\dagger = T$.

Note that we define operations on the set of operators on $\mathcal{H}$: $(T \pm R)|x\rangle := T|x\rangle \pm R|x\rangle, \alpha T|x\rangle := \alpha \times T|x\rangle$ for any $|x\rangle \in \mathcal{H}$, and $TR := T \circ R$ (composite map of T and R).

Definition 2 *A linear operator T is called an Hermitian operator if $T = T^\dagger$ holds.*

Definition 3 *A linear operator P is called a projection (operator) if $P = P^\dagger = P^2$ holds, where $P^2 := PP$.*

[5] Define $x^* : y \in \mathcal{H} \mapsto (x, y) \in \mathbb{C}$ for $x \in \mathcal{H}$, then the map x^* is called the duel vector for x.

Definition 4 *A linear operator T is called a positive operator (we use the notation $T \geq 0$) if $\langle x|T|x\rangle \geq 0$ holds for any $|x\rangle \in \mathcal{H}$.*

Remark that T is a positive operator if the operator is a projection, and R is an Hermitian operator if the operator is a positive operator.

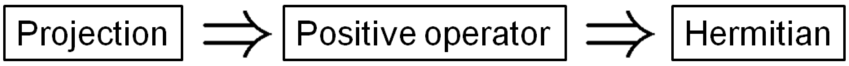

Figure 2.1: Relationship among classes of operators

Definition 5 *A linear operator U is called a unitary operator if $U^{\dagger}U = \mathbb{I}$ holds, where $\mathbb{I}$ is the identity operator*[6] *on $\mathcal{H}$*

Remark that $U^{\dagger}U = UU^{\dagger} = \mathbb{I}$ holds for any unitary operator U.

Lastly, a linear map $|x\rangle\langle y|$ for $|x\rangle, |y\rangle \in \mathcal{H}$ is defined by $|x\rangle\langle y||z\rangle := |x\rangle\langle y|z\rangle = \langle y|z\rangle|x\rangle$. This definition is interpreted as (1) the operator $|x\rangle\langle y|$ acts on the vector $|z\rangle$, (2) the vector $|x\rangle$ is multiplied by the complex number $\langle y|z\rangle$.

2.2 Tensor Product Hilbert Space

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be d_1 dimensional and d_2 dimensional Hilbert spaces, respectively. Define

$$|x\rangle \otimes |y\rangle : (|u\rangle, |v\rangle) \in \mathcal{H}_1 \times \mathcal{H}_2 \mapsto \langle x|u\rangle\langle y|v\rangle \in \mathbb{C},$$

for $|x\rangle \in \mathcal{H}_1$ and $|y\rangle \in \mathcal{H}_2$. We use often the abbreviated notation $|x\rangle \otimes |y\rangle = |x\rangle|y\rangle = |xy\rangle$. Define $\mathcal{H}_1 \otimes \mathcal{H}_2$ spanned by $\{|x\rangle \otimes |y\rangle \mid |x\rangle \in \mathcal{H}_1, |y\rangle \in \mathcal{H}_2\}$ with the following properties:

1. $\alpha(|x\rangle \otimes |y\rangle) = (\alpha|x\rangle) \otimes |y\rangle = |x\rangle \otimes (\alpha|y\rangle), \quad \forall \alpha \in \mathbb{C}$,
2. $(|x_1\rangle + |x_2\rangle) \otimes |y\rangle = |x_1\rangle \otimes |y\rangle + |x_2\rangle \otimes |y\rangle$,
3. $|x\rangle \otimes (|y_1\rangle + |y_2\rangle) = |x\rangle \otimes |y_1\rangle + |x\rangle \otimes |y_2\rangle$.

We define an inner product equipped on $\mathcal{H}_1 \otimes \mathcal{H}_2$:

$$(|x_1\rangle \otimes |y_1\rangle, |x_2\rangle \otimes |y_2\rangle) := \langle x_1|x_2\rangle\langle y_1|y_2\rangle.$$

We use the abbreviated notation $(|x_1\rangle \otimes |y_1\rangle, |x_2\rangle \otimes |y_2\rangle) = (\langle x_1| \otimes \langle y_1|)(|x_2\rangle \otimes |y_2\rangle) = \langle x_1 y_1|x_2 y_2\rangle$, where $\langle x_1| \otimes \langle y_1|$ denotes the dual vector of $|x_1\rangle \otimes |y_1\rangle$. Then, $\mathcal{H}_1 \otimes \mathcal{H}_2$ is a $d_1 d_2$ dimensional Hilbert space with the above inner

[6] $\mathbb{I}$ is called the identity operator on $\mathcal{H}$ if $\mathbb{I}\,|x\rangle = |x\rangle$ holds for any $|x\rangle \in \mathcal{H}$.

product, and we call $\mathcal{H}_1 \otimes \mathcal{H}_2$ a tensor product Hilbert space for $\mathcal{H}_1$ and $\mathcal{H}_2$. Let $\{|e_i\rangle\}_{i=1}^{d_1}$ and $\{|f_j\rangle\}_{j=1}^{d_2}$ be ONBs of $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Then, $\{|e_i\rangle \otimes |f_j\rangle\}_{i,j=1}^{d_1,d_2}$ is an ONB of $\mathcal{H}_1 \otimes \mathcal{H}_2$, thus $\mathcal{H}_1 \otimes \mathcal{H}_2$ is $d_1 d_2$ dimensional space.

Let T_1 and T_2 be linear operators on $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. Define a linear operator $T \otimes R$ on $\mathcal{H}_1 \otimes \mathcal{H}_2$:

$$T_1 \otimes T_2(|x\rangle \otimes |y\rangle) := T_1|x\rangle \otimes T_2|y\rangle.$$

Note that linear operators on $\mathcal{H}_1 \otimes \mathcal{H}_2$ have properties similar to linear operator on $\mathcal{H}_1$ ($\mathcal{H}_2$), Furthermore, $(T_1 \otimes T_2)(R_1 \otimes R_2) = T_1R_1 \otimes T_2R_2$, $(T_1 \otimes T_2)^\dagger = T_1{}^\dagger \otimes T_2{}^\dagger$, and $\operatorname{tr} T_1 \otimes T_2 = \operatorname{tr} T_1 \operatorname{tr} T_2$ hold especially.

Remark that the above discussion is generalized n times tensor product Hilbert space naturally such as $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$, $|x_1\rangle \otimes |x_2\rangle \otimes \cdots \otimes |x_n\rangle$, and $T_1 \otimes T_2 \otimes \cdots \otimes T_n$.

2.3 An Example: A Simple Construction

We introduce a basic complex vector space as follow:

$$\mathbb{C}^d := \left\{ \begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_d \end{pmatrix} \;\middle|\; u_i \in \mathbb{C} \right\}.$$

Define an inner product on $\mathbb{C}^d$ by $\langle x|y\rangle := \sum_{i=1}^d \bar{x_i} y_i$, where $|x\rangle = (x_1, x_2, \dots, x_d)^\top, |y\rangle = (y_1, y_2, \dots, y_d)^\top \in \mathbb{C}^d$. Then, the dual vector of $|x\rangle$ has the following form: $\langle x| = (\bar{x_1}, \bar{x_2}, \dots, \bar{x_d})$. Define a norm $\||x\rangle\| := \langle x|x\rangle^{1/2}$ by using the above inner product, then, $\mathbb{C}^d$ is a d dimensional Hilbert space with the inner product. Remark that $\mathbb{C}^d$ is isomorphic [7] to a d dimensional abstract Hilbert space $\mathcal{H}$ for a fixed base.

As is easily shown, any d-by-d matrix on $\mathbb{C}$ is linear operator on $\mathbb{C}^d$. Let T be a d-by-d matrix. The conjugate transpose matrix of T is the adjoint matrix (operator) of it, i.e., $T^\dagger = (\bar{T})^\top$. Especially, the adjoint matrix of $|x\rangle\langle y| = (x_i \bar{y_j})_{ij}$ has the following form: $|y\rangle\langle x| = (y_i \bar{x_j})_{ij}$. Furthermore, several operations of the matrices, e.g., addition, multiplication, and trace [8], are corresponded to operations of linear operators on $\mathbb{C}^d$.

In a d dimensional Hilbert space $\mathbb{C}^d$, the following product so called Kronecker product is a tensor product:

$$|x\rangle \otimes |y\rangle := (x_1y_1, \dots, x_1y_d, x_2y_1, \dots, x_2y_d, \dots, x_dy_1, \cdots, x_dy_d)^\top,$$

[7] There exists a linear one-to-one map (bijection) from $\mathbb{C}^d$ to $\mathcal{H}$.

[8] $\operatorname{tr} T = \sum_i t_{ii}$ holds for a matrix $T = (t_{ij})_{ij}$.

for $|x\rangle = (x_1, x_2, \dots, x_d)^\top$ and $|y\rangle = (y_1, y_2, \dots, y_d)^\top \in \mathbb{C}^d$, and

$$T \otimes S := \begin{pmatrix} t_{11}S & t_{12}S & \dots & t_{1d}S \\ t_{21}S & t_{22}S & \dots & t_{2d}S \\ \vdots & \vdots & \vdots & \vdots \\ t_{d1}S & t_{d2}S & \dots & t_{dd}S \end{pmatrix},$$

for d-by-d matrices $T = (t_{ij})_{ij}$ and $S = (s_{ij})_{ij}$. Then, $|x\rangle \otimes |y\rangle$ is a vector of d^2 dimensional Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d$ and $T \otimes S$ is a d^2-by-d^2 matrix.

2.4 Shannon Entropy and Mutual Information

We consider security criteria of conventional and quantum cryptography described by entropy and mutual information. Cryptography guaranteeing such like security criteria is called cryptography guaranteeing unconditionally security or informational security. Information theory [9] was formulated by Shannon in 1948 [16] [10]. "Information" is quantified by using probability corresponding to the event in information theory. It is a basic idea that information of an event not tending to take place is greater than them of typically events.

Definition 6 *Let X be a (discrete) random variable and P_X the probability mass function relevant to X. Define*

$$H(X) := -\sum_{x \in X} P_X(x) \log_b P_X(x),$$

where we define $0 \log_b 0 = 0$. We call $H(\cdot)$ an entropy function and call value of $H(X)$ entropy or information for X

Particularly, $H(\cdot)$ is used for measuring bit if base of the logarithm is equal to 2. Remark that $H(X)$ is maximized for uniform distribution $P_X(x)$, i.e., $P_X(x) = P_X(x')$ for any x and x'. Therefore, entropy denotes uncertainty of events by using a random variable corresponding to them. Let X and Y be (discrete) random variables, $P_{X,Y}(x, y)$ and $P_{X,Y}(x \mid y)$ joint probability and conditional probability relevant to X and Y, respectively. Define a conditional entropy

$$H(X \mid Y) := -\sum_{x \in X} \sum_{y \in Y} P_{X,Y}(x, y) \log_b P_{X,Y}(x \mid y),$$

and a joint entropy

$$H(X, Y) := -\sum_{x \in X} \sum_{y \in Y} P_{X,Y}(x, y) \log_b P_{X,Y}(x, y),$$

[9] For more details, see Ref.[13, 14, 15]

[10] Recently, the paper is summarized in Ref.[17]

for X and Y. Remark that $H(X,Y) = H(X) + H(Y \mid X)$ holds. This equality is called the chain rule.

Definition 7 *Let X and Y be (discrete) random variables and $P_{X,Y}$ the joint probability relevant to X and Y. Define*

$$I(X;Y) := \sum_{x \in X} \sum_{y \in Y} P_{X,Y}(x,y) \log_b \frac{P_{X,Y}(x,y)}{P_X(x) P_Y(y)},$$

where $P_X(x) := \sum_{y \in Y} P_{X,Y}(x,y)$ and $P_Y(y) := \sum_{x \in X} P_{X,Y}(x,y)$. We call $I(\cdot;\cdot)$ an mutual information.

We introduce several properties:

$$\begin{aligned} I(X;Y) &= H(X) - H(X \mid Y) \qquad (2.1) \\ &= H(Y) - H(Y \mid X) \\ &= H(X) + H(Y) - H(X,Y) \\ &= H(X,Y) - H(X \mid Y) - H(Y \mid X) \end{aligned}$$

From eq.(2.1), mutual information $I(X;Y)$ denotes difference between uncertainty of X and uncertainty of it on condition that information of Y is given. In other words, $I(X;Y)$ denotes remaining uncertainty of X by obtaining information of Y. Note that $I(X;Y) = 0$ holds if and only if X and Y are independent.

Chapter 3

Preliminary of Quantum Information Theory

3.1 Axioms of Quantum Information Theory

Axiomatism is embraced in quantum information theory (quantum physics) [1]. Quantum systems, quantum states, several measurements, time evolution, and so on, are described by using Hilbert spaces and linear operators on the spaces. Throughout this paper, we deal with only finite level quantum systems. This request is sufficient to discuss applied technologies such as quantum cryptography, quantum error-correcting codes, quantum computation, and so on.

Axiom 1 *Associated to any d-level quantum system is described by a d dimensional Hilbert space and any d dimensional Hilbert space corresponds to a d-level quantum system. Any quantum state of a quantum system described by a unit vector of the Hilbert space associated with the quantum system.*

That is, we identify quantum systems (resp. quantum states of the systems) with Hilbert spaces (resp. unit vectors of the spaces) [2] in quantum information theory.

An action to obtain an outcome relevant to an observable from a quantum system is called a measurement relevant to the observable.

[1] There are many textbooks and papers about quantum physics, quantum information theory, and its applied technologies. We introduced typical and recommended books and paper. Quantum physics: Ref.[18, 19, 20, 21]. Especially, probabilistic and statistical aspects of quantum physics is shown in Ref.[22, 23, 24, 25, 26]. Quantum information theory: Ref.[27, 28, 29, 30]. Quantum computer, communication, and cryptography: Ref.[31, 32, 33, 34, 35, 36].

[2] In quantum physics, it is not postulated that there exists a quantum system associated with any Hilbert space.

Axiom 2 *An observable is described by an Hermitian operator*[3] *. We prepare a quantum system $\mathcal{H}$ in a quantum state $|x\rangle$ and measure it with measurement corresponding to an observable described by an Hermitian operator A on $\mathcal{H}$. Then, we obtain an outcome λ_i with probability given by*

$$\langle x|P_i|x\rangle,$$

where λ_i is an eigenvalue of A and P_i is the projection to the eigenspace of λ_i, i.e., spectral decomposition of A has the following form: $A = \sum_i \lambda_i P_i$.

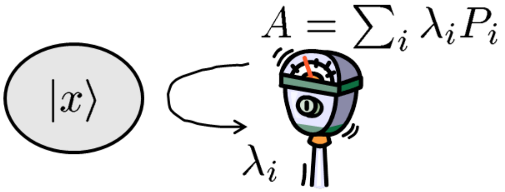

Figure 3.1: A measurement corresponding to an observable A on a quantum system in a quantum state $|x\rangle$

Disturbance of quantum states introduced by measurements is generally unavoidable in principle of quantum physics. Variation of quantum states such like the disturbance is called measurement process. We introduce a typical measurement process. Suppose that we measure a quantum system $\mathcal{H}$ in a quantum state $|x\rangle$ with an observable $A = \sum_i \lambda_i P_i$ and obtain an outcome i. If the post measurement quantum state of $\mathcal{H}$ is described by

$$\frac{P_i|x\rangle}{\|P_i|x\rangle\|},$$

this measurement is called a projective measurement[4] .

Time revolution of a quantum state is described by a unitary operator.

Axiom 3 *Let $|x_1\rangle$ be a quantum state of a quantum system $\mathcal{H}$. Time evolution of the state is described by a relevant unitary operator U on $\mathcal{H}$:*

$$|x_2\rangle = U|x_1\rangle,$$

where $|x_2\rangle$ denotes the quantum state after the time evolution.

We also postulate that time evolution described by any unitary operator is feasible.

In the above discussion, we deal with only one quantum system. We use tensor product Hilbert spaces for describing composite quantum systems.

[3] Furthermore, we identify an Hermitian operator with an observable.

[4] A projective measurement for a non degenerate observable is called a von Neumann's projective measurement. On the other hand, a projective measurement for a degenerate observable is called a Lüders's projective measurement. The measurement processes of the projective measurements are called projective postulate.

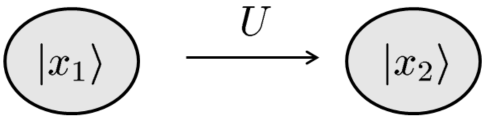

Figure 3.2: A time evolution corresponding to a unitary operator U

Axiom 4 *Let S_1 and S_2 be quantum systems described by Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$, respectively. A bipartite composite quantum system of S_1 and S_2 is described by a tensor product space $\mathcal{H}_1 \otimes \mathcal{H}_2$.*

$\mathcal{H}_1$
$|x\rangle$
$\otimes$
$\mathcal{H}_2$
$|y\rangle$

Figure 3.3: A bipartite quantum system consists of quantum systems $\mathcal{H}_1$ and $\mathcal{H}_2$

For example, $|x\rangle \otimes |y\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$ denotes that $\mathcal{H}_1$ and $\mathcal{H}_2$ are prepared in the state $|x\rangle$ and $|y\rangle$ respectively, a measurement relevant to an observable $A_1 \otimes A_2$ on $\mathcal{H}_1 \otimes \mathcal{H}_2$ denotes that $\mathcal{H}_1$ and $\mathcal{H}_2$ are measured with A_1 and A_2 separately, a measurement relevant to an observable $A_1 \otimes \mathbb{I}$ on $\mathcal{H}_1 \otimes \mathcal{H}_2$ denotes that only $\mathcal{H}_1$ is measured with A_1. Remark that we can generalize the axiom to multipartite composite quantum systems such as $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$.

3.2 Generalizations

Let us consider that we prepare a state $|x_j\rangle \in \mathcal{H}$ with probability p_j. In the situation, we measure the quantum system with an observable $A = \sum_i \lambda_i P_i$, then, probability of obtaining λ_i is given by

$$\sum_j p_j \langle x_i | P_i | x_i \rangle = \operatorname{tr} P_i \sum_j p_j |x_j\rangle\langle x_j|.$$

For a linear operator ρ, the following conditions are equivalent: (1) ρ has the following form $\sum_j p_j |x_j\rangle\langle x_j|$ for some probability $(p_j)_j$ and states $(|x_j\rangle)_j$, (2) $\rho \geq 0$ and $\operatorname{tr} \rho = 1$ hold.

Definition 8 *A linear operator ρ is called a density operator if $\rho \geq 0$ and* $\operatorname{tr} \rho = 1$ *hold.*

We can identify a density operator with a probabilistic mixture quantum state. Therefore, rewriting the axiom, probability of obtaining an outcome λ_i when a quantum system in a state ρ is measured with $A = \sum_i \lambda_i P_i$ is given by [5]

$$\operatorname{tr} \rho P_i.$$

We can also rewrite the axiom of time evolution for a density operator ρ_t:

$$\rho_{t+1} = U \rho_t U^\dagger,$$

where ρ_{t+1} denotes the density operator after the time evolution.

Let ρ_1 and ρ_2 be density operators. A convex combination $\rho_{12} = t\rho_1 + (1-t)\rho_2$ for $0 \leq t \leq 1$ is a density operator, i.e., $\rho_{12} \geq 0$ and $\operatorname{tr} \rho_{12} = 1$ hold. Let $\mathcal{S}(\mathcal{H})$ be the set of density operators on $\mathcal{H}$, i.e.,

$$\mathcal{S}(\mathcal{H}) := \{\rho \mid \rho \geq 0, \operatorname{tr} \rho = 1\}.$$

Note that $\mathcal{S}(\mathcal{H})$ is a convex set for the reasons stated above. $\rho \in \mathcal{S}(\mathcal{H})$ is called a pure state if there do not exist $\rho_1, \rho_2 (\neq \rho) \in \mathcal{S}(\mathcal{H})$ and $0 < t < 1$ such that $\rho = t\rho_1 + (1-t)\rho_2$, i.e., ρ is an extreme point of $\mathcal{S}(\mathcal{H})$. $\rho \in \mathcal{S}(\mathcal{H})$ is called a mixture state if ρ is not a pure state. Remark that the following conditions are equivalent: (1) $\rho \in \mathcal{S}(\mathcal{H})$ is a pure state, (2) there exits a unit vector $|x\rangle \in \mathcal{H}$ such that $\rho = |x\rangle\langle x|$.

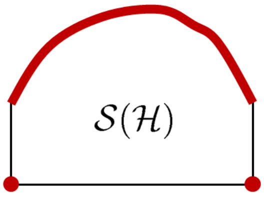

Figure 3.4: The set of all quantum states in a quantum system $\mathcal{H}$ as a convex set

Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces expressing quantum systems, respectively and ρ_{AB} a density operator on $\mathcal{H}_A \otimes \mathcal{H}_B$ expressing a quantum state on the bipartite system. Then, we use partial trace for describing a quantum state on $\mathcal{H}_A$ (resp. $\mathcal{H}_B$).

Theorem 9 *Let $\mathcal{H}_A \otimes \mathcal{H}_B$ be a bipartite system and $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ a quantum state. There exists a quantum state $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ such that*

$$\operatorname{tr}(\rho_{AB}(M \otimes \mathbb{I}_B)) = \operatorname{tr}(\rho_A M), \tag{3.1}$$

holds for any $M \in \mathcal{L}(\mathcal{H})$.

[5] Remind that $\operatorname{tr} \rho P_i = \operatorname{tr} P_i \rho$ holds.

Indeed,

$$\rho_A := \sum_{i_1,i_2,j} |e_{i_1}\rangle\langle e_{i_1} f_j|\rho_{AB}|e_{i_2} f_j\rangle\langle e_{i_2}|,$$

satisfies eq.(3.1) and it is a density operator on $\mathcal{H}_A$, where $\{|e_i\rangle\}_i$ and $\{|f_j\rangle\}_j$ are ONBs of $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. In a similar way, there exists $\rho_B \in \mathcal{S}(\mathcal{H}_B)$ for $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$. We call ρ_A (resp. ρ_B) partial trace [6] and we use a notation $\operatorname{tr}_B \rho_{AB} := \rho_A$ (resp. $\operatorname{tr}_A \rho_{AB} := \rho_B$).

We can generalize measurement and time evolution by using unitary operators and Hermitian operators on composite quantum systems [7] . Firstly, we discus generalized feasible measurements as follow.

Definition 10 *An n-tuple of linear operators $(M_i)_{i=1}^n$ is called a (discrete) positive-operator-valued measure (POVM) if $\sum_{i=1}^n M_i = \mathbb{I}$ and $M_i \geq 0$ hold for any i .*

Definition 11 *An n-tuple of linear operators $(N_i)_{i=1}^n$ is called a (discrete) projection-valued measure (PVM) if $\sum_{i=1}^n N_i = \mathbb{I}$ holds and N_i is a projection for any i .*

Remark that the set of PVMs is a subset of the set of POVMs since any projection is a positive operator. A measurement with a POVM (resp. PVM) $(M_i)_{i=1}^n$ in a state ρ is called a POVM (resp. PVM) measurement, then a probability of obtaining an ith index as an outcome is given by

$$\operatorname{tr} \rho M_i.$$

We also discus generalized feasible time evolution.

Definition 12 *Let $\mathcal{L}(\mathcal{H})$ be the set of all linear operators on a Hilbert space $\mathcal{H}$. A linear map $\Lambda : \mathcal{L}(\mathcal{H}_1) \to \mathcal{L}(\mathcal{H}_2)$ is called a trace-preserving completely-positive (TPCP) map if the following conditions hold:*

1. $\operatorname{tr} T = \operatorname{tr} \Lambda(T), \quad \forall T \in \mathcal{L}(\mathcal{H}_1)$,
2. $\Lambda \otimes \iota_n : \mathcal{L}(\mathcal{H}_1) \otimes \mathcal{L}(\mathbb{C}^n) \to \mathcal{L}(\mathcal{H}_2) \otimes \mathcal{L}(\mathbb{C}^n)$ *is a linear positive map* [8] *for any $n \in \mathbb{N}$.*

Remark that $\mathcal{L}(\mathcal{H})$ is a $(\dim \mathcal{H})^2$ dimensional Hilbert space with respect to some inner product [9] for linear operators on $\mathcal{H}$. Any generalized time evolution is described by some TPCP map. Inversely, we postulate that any TPCP map denotes some time evolution. In particular, we call an operation, e.g., time evolution, described by a TPCP map a quantum operation. We introduce useful representation of TPCP maps.

[6] Partial trace is sometimes called a reduced density operator.

[7] We omit proofs of the facts. For more details, see Ref.[27, 28, 29].

[8] $\Lambda \otimes \iota_n(A) \geq 0$ holds for any positive operator A.

[9] For instance, define an inner product called the Hilbert-Schmidt inner product $\langle T|S\rangle_{HS} := \operatorname{tr} T^{\dagger} S$ for $T, S \in \mathcal{L}(\mathcal{H})$. Then, $\mathcal{L}(\mathcal{H})$ is a Hilbert space with it.

Theorem 13 *(Kraus representation [37], Stinespring representation [38]). The following conditions are equivalent:*

1. $\Lambda : \mathcal{L}(\mathcal{H}_1) \to \mathcal{L}(\mathcal{H}_2)$ *is a TPCP map,*

2. *There exist linear maps* $V_i : \mathcal{H}_1 \to \mathcal{H}_2 (i = 1, 2, \ldots, l)$ *such that* $\sum_{i=1}^{l} {V_i}^\dagger V_i = \mathbb{I}$ *and*

$$\Lambda(T) = \sum_{i=1}^{l} V_i T {V_i}^\dagger, \tag{3.2}$$

hold for any $T \in \mathcal{L}(\mathcal{H}_1)$.

3. *Let* $\mathcal{H}_3 = \mathcal{H}_2$. *There exist a pure state* $\rho_0 \in \mathcal{S}(\mathcal{H}_2 \otimes \mathcal{H}_3)$ *and a unitary operator* U_Λ *on* $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \mathcal{H}_3$ *such that*

$$\Lambda(\rho) = \mathrm{tr}_{1,3}\, U_\Lambda(\rho \otimes \rho_0) U_\Lambda^\dagger, \tag{3.3}$$

holds for any $\rho \in \mathcal{S}(\mathcal{H}_1)$.

Then, eq.(3.2) is called Kraus representation of a TPCP map Λ and each V_i is called a Kraus operator. Eq.(3.3) is called Stinespring representation of the map. By observing eq.(3.3), it is possible to realize any TPCP map using relevant a pure state and a unitary operator.

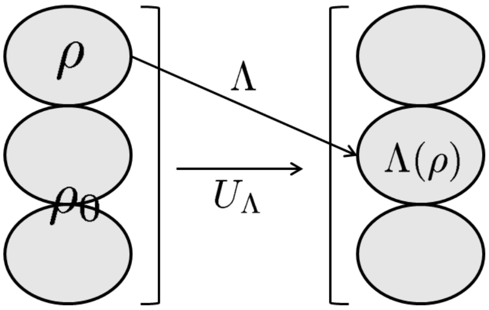

Figure 3.5: Realization of general time evolution

POVM measurements are most generalized measurements, but those measurements do not describe measurement processes. We introduce useful tool to describe probability and measurement process simultaneously.

Definition 14 *An n-tupple of linear operators* $V_i : \mathcal{H}_1 \to \mathcal{H}_2 (i = 1, 2, \ldots, n)$ *is called an n-tupple of measurement operators if* $\sum_i {V_i}^\dagger V_i = \mathbb{I}$ *holds.*

We can describe any measurement and its measurement process by using corresponding measurement operators. Suppose that we measure a quantum system in a quantum state ρ with a measurement described by measurement operators $(V_i)_{i=1}^n$. Then, probability of obtaining an index i as an outcome is given by

$$\operatorname{tr} {V_i}^\dagger V_i \rho,$$

and after measurement state is described by

$$\frac{V_i \rho {V_i}^\dagger}{\operatorname{tr} {V_i}^\dagger V_i \rho}.$$

For instance, $(\sqrt{M_i})_i$ [10] are measurement operators for any POVM $(M_i)_i$. The POVM measurement is described by the measurement operators, then corresponding probability is given by $\operatorname{tr} \sqrt{M_i}^\dagger \sqrt{M_i}\rho = \operatorname{tr} M_i \rho$, and typical measurement process [11] is described by $\sqrt{M_i}\rho\sqrt{M_i} / \operatorname{tr} M_i \rho$.

3.3 Entanglement

Quantum information theory enables us to overcome the limitations of the conventional computation and communication. To understand the reason why it is possible, it is helpful to investigate the different points between quantum physics and non quantum physics. The notion of entanglement shows one of the most drastic differences. Entanglement often plays crucial roles in quantum information theory.

Let A and B be two quantum systems described by Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. Their bipartite quantum system is described by a tensor product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. A quantum state described by a density operator $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$ is called a separable state if it can be decomposed into the following form:

$$\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B,$$

where $(p_i)_i$ is nonnegative values with $\sum_i p_i = 1$ and $(\rho_i^A)_i, (\rho_i^B)_i$ are quantum states of $\mathcal{H}_A, \mathcal{H}_B$, respectively.

A quantum state of the bipartite quantum system is called an entangled state (of the bipartite quantum system) if the quantum state is not a

[10] Remind that an operator T is an Hermitian if T is a positive operator. An Hermitian T takes spectral decomposition: $T = \sum_i \lambda_i P_i$, where λ_i is positive real number for any i, then, define $f(T) := \sum_i f(\lambda_i) P_i$ for a function f on $\mathbb{R}$, e.g., $\sqrt{T} = \sum_i \sqrt{\lambda_i} P_i$.

[11] Remark that after measurement state is not uniquely determined for a POVM, typically. For instance, $(\sqrt{M_i})_i$ and $(U\sqrt{M_i})_i$ are two measurement operators for any a POVM $(M_i)_i$, where $U (\neq \mathbb{I})$ is an arbitrary unitary operator. Then, $\operatorname{tr} \sqrt{M_i}^\dagger \sqrt{M_i}\rho = \operatorname{tr} (U\sqrt{M_i})^\dagger U \sqrt{M_i}\rho$ holds but $\sqrt{M_i}\rho\sqrt{M_i} / \operatorname{tr} M_i \rho \neq U\sqrt{M_i}\rho (U\sqrt{M_i})^\dagger / \operatorname{tr} (U\sqrt{M_i})^\dagger U \sqrt{M_i}\rho$.

separable state. Particularly, a pure state described by

$$\frac{1}{\sqrt{d}} \sum_{i=1}^{d} |e_i\rangle \otimes |f_i\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B,$$

is called a maximally entangled state, where $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$ and $\{|e_i\rangle\}_i, \{|f_i\rangle\}_i$ are ONBs of $\mathcal{H}_A, \mathcal{H}_B$, respectively.

Suppose that $\mathcal{H}_A$ and $\mathcal{H}_B$ are measured with same observable separately. There exist several observables to obtain correlated outcomes on measuring $\mathcal{H}_A$ and $\mathcal{H}_B$ separately if the quantum state of the bipartite quantum system is an entangled state, e.g., an outcome 1 is obtained on measuring $\mathcal{H}_A$ if and only if an outcome 1 is obtained on measuring $\mathcal{H}_B$, an outcome -1 is obtained on measuring $\mathcal{H}_A$ if and only if an outcome -1 is obtained on measuring $\mathcal{H}_B$. Such correlation of the outcomes is called quantum correlation. We discuss quantum correlation in 2-level quantum system in the next section, mentioning the particular example.

Now it seems natural to investigate a criterion that enables us to tell whether a given state is entangled or separable. This is the problem of separability criterion. Unfortunately, only for the very small quantum systems, the necessary and sufficient criterion is known. For instance, so-called Peres-Horodecki criterion [39, 40] works only for 2 × 2 or 2 × 3 dimensional bipartite quantum systems. Recently Hofmann and Takeuchi [41] proposed an interesting criterion using the uncertainty relation. Their original criterion was based on the Robertson-type uncertainty relation [42]. Moreover, several works [43, 44, 45] following it showed the possibility of using other kinds of the uncertainty relations. In particular, Vicente and Sánchez-Ruiz [45] proposed a criterion based on the Landau-Pollak uncertainty relation and examined its effectiveness in the 2×2 bipartite systems. Although their criterion is simple and works well in the low-dimensional case, they have not succeeded in obtaining a criterion that is effective in the higher dimensional systems. After their work, Miyadera and Imai [46] proposed a possible generalization of it to the higher dimensional systems by using their generalized Landau-Pollak uncertainty relation. We showed further investigation and improvement on this direction [47]. We obtained a strict Landau-Pollak type inequality for observables related with mutually unbiased bases [48, 49] in prime dimensional Hilbert spaces.

Foundation theory of entanglement such as the above discussion has been studied in many previous works. On the other hand, its applied technologies are also studies by many researchers and engineers. Especially, entanglement plays crucial roles in quantum communication. Quantum superdense coding [50, 51] is a technique to enable us to send 2^n bits by using only n quantum systems. In the coding scheme, firstly, a sender and a receiver share a entanglement constructed from two quantum systems. The sender encode the quantum state to a quantum code according to chosen two bits and sends the system to the receiver. The receiver measures the bipartite system with a relevant measurement and obtains an outcome expressing the two bits. Quantum teleportation [3, 52] is a scheme to enable us to teleport any quantum state by using only classical information. In the scheme, the sender and the receiver also share a bipartite system in a maximally entangled state. The sender measures a bipartite system constructed from one of the prepared bipartite system and a quantum system in a state teleported to the sender. After the measurement, the sender sends the outcome to the receiver. The receiver performs a relevant time evolution according to the outcome on one of the prepared bipartite system and obtain the state prepared by the sender. In both of two techniques, it is necessary that the sender and the receiver share pairs of entanglement in advance over a noisy quantum channel and a public channel. To attain this goal one may employ so called entanglement distillation protocols (purification protocols, or sharing protocols) [53, 54, 55, 56, 57]. Those protocols are closely related to quantum error-correcting codes.

3.4 Quantum Bit

In this section, we introduce quantum bit systems which play basic role in quantum information processing such as quantum cryptography, quantum computation, and so on. We call a quantum system described by 2 dimensional Hilbert space a quantum bit system (qubit system) and call a quantum state of a qubit system a qubit state. Any qubit state of a qubit $\mathcal{H} \simeq \mathbb{C}^2$ has the following form:

$$\alpha|0\rangle + \beta|1\rangle,$$

where $\alpha, \beta \in \mathbb{C}$ with $|\alpha|^2 + |\beta|^2 = 1$ and

$$|0\rangle := (1,0)^\top, |1\rangle := (0,1)^\top \in \mathbb{C}^2 .$$

In quantum computation, a bit string is corresponded to a qubits state of qubits (composite quantum bits). For $s = (s_1, s_2, \cdots, s_n) \in \mathbb{F}_2^n$ [12] , we define a corresponding pure state by $|s\rangle := |s_1\rangle \otimes |s_2\rangle \otimes \cdots \otimes |s_n\rangle \in \mathcal{H}^{\otimes n}$, where $\mathcal{H}^{\otimes n} := \mathcal{H} \otimes \mathcal{H} \otimes \cdots \otimes \mathcal{H}$ (n times tensor product Hilbert space). Then, any qubit state of $\mathcal{H}^{\otimes n}$ is uniquely represented as $\sum_{s \in \mathbb{F}_2^n} \alpha_s |s\rangle \in \mathcal{H}^{\otimes n}$, where $\alpha_s \in \mathbb{C}$ satisfying $\sum_s |\alpha_s|^2 = 1$.

We introduce basic observables on qubit so called Pauli matrices:

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix}, \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

[12] Define $\mathbb{F}_2^n := \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbb{F}_2\}$.

The Pauli matrices are decomposed into the following form:

$$\sigma_x = +1|+\rangle\langle+| - 1|-\rangle\langle-|,$$

$$\sigma_y = +1|+'\rangle\langle+'| - 1|-'\rangle\langle-'|,$$

$$\sigma_z = +1|0\rangle\langle 0| - 1|1\rangle\langle 1|,$$

where

$$|+\rangle := 1/\sqrt{2}(1,1)^\top, |-\rangle := 1/\sqrt{2}(1,-1)^\top,$$

$$|+'\rangle := 1/\sqrt{2}(1,\mathrm{i})^\top, |-'\rangle := 1/\sqrt{2}(1,-\mathrm{i})^\top.$$

Suppose that we measure a qubit in a state $|x\rangle$ with an observable $\sigma_J (J \in \{x, y, z\})$. We obtain an eigenvalue $i \in \{1, -1\}$ of σ_J as an outcome with probability 1 if $|x\rangle$ is an eigenvector of the eigenvalue i of σ_J. On the other hand, probability of obtaining an outcome i is equal to 0 if $|x\rangle$ is an eigenvector of the eigenvalue $i'(\neq i)$ of σ_J. For any J, probability of obtaining an eigenvalue i of σ_J is equal to 1/2 if $|x\rangle$ is an eigenvector of $\sigma_{J'}(J' \neq J)$.

Considering the Pauli matrices, those are not only Hermitian matrices but also unitary matrices. We often use the notations $X = \sigma_x, Y = \sigma_y$, $Z = \sigma_z$ as time evolutions. Note that $X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$ and $Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$ hold. The Pauli matrix X is called Pauli X gate and the matrix Z is called Pauli X gate [13] , and $Y = \mathrm{i}XZ$ holds. We can flip one bit ($|0\rangle \leftrightarrow |1\rangle$) by using Pauli X gate and can flip phase ($|1\rangle \leftrightarrow -|1\rangle$) by using Pauli Z gate.

We define the following qubits state:

$$|\Psi^+\rangle := \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle),$$
$$|\Psi^-\rangle := \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle),$$
$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle),$$
$$|\Phi^-\rangle := \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle).$$

The qubits states are called Bell states. Those are most useful entangled states in quantum information processing such as quantum cryptography, quantum teleportation, and quantum communication. Suppose that we measure two qubits in the Bell state $|\Psi^+\rangle$ separately with a projective measurement corresponding to the observable σ_z. According to the axiom, we

[13] In quantum error-correcting codes, X is called bit-flip error and Z is called phase-flip error.

obtain an outcome $i \in \{1, -1\}$ from one qubit if an outcome from the other is equal to i. In this case, the outcomes are correlated. By the way,

$$\frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|+\rangle \otimes |+\rangle + |-\rangle \otimes |-\rangle),$$

holds. From the construction above, outcomes with measurements of σ_x instead of σ_z are also correlated. In this way, we obtain correlated outcomes with measurement of several observables. The strongly correlation is called quantum correlation.

Chapter 4

Basics of Quantum Error-Correcting Codes

4.1 Modern Coding Theory

Modern coding theory [1] is closely related to Information theory. Shannon introduced channel coding theorem in 1948 [16]. To put it simply, the theorem showed that there exists a code such that error rate of the code converges zero for any coding rate which is less than or equal to channel capacity. Showing existence of such a code is an interesting point of this theorem. Therefore, coding theory was became brisk for constructing such a code.

We introduce a simple example of error-correcting codes. Let us consider that the noisy communication channel is an independent, identically distributed channel, i.e., each bit of the bit string is flipped with a priori probability p. Suppose that a sender sends bit 1 (length of the bit string 0) to a receiver on the channel. The receiver could determine the sent bit as 0 if the bit 1 is flipped. In this manner, they cannot communicate correctly. We add redundancy bit to sent bit string to settle the problem. The code is called a repetition code. For example, we add redundancy two bit to one bit such as

$$0 \in \mathbb{F}_2 \mapsto (000) \in \mathbb{F}_2^3, \quad 1 \in \mathbb{F}_2 \mapsto (111) \in \mathbb{F}_2^3.$$

Decision by a majority is a kind of very simple error-correcting methods. Suppose that the sent bit string 000 is changed to 001. Then, the number of symbol 0 is greater than the number of symbol 1. Therefore, the receiver guess the sent bit string as 000 according to majority decision. However, majority decision is not omnipotent error-correcting method. In fact, the receiver guess the sent bit string as 111 if that the sent bit string 000 is changed to 011.

[1] For more details, see Ref.[58, 59]

In general, we call a map $\mathrm{Enc} : \mathbb{F}_2^k \to C \subset \mathbb{F}_2^n$ $(k \leq n)$ an encoder. The domain and the range of Enc are called a source and a code, respectively. A element of a code is called a code word. We call a map $\mathrm{Dec} : \mathbb{F}_2^n \to \mathbb{F}_2^k$ a decoder. In particular, a k dimensional subspace of an n dimensional vector space $\mathbb{F}_2^n$ on $\mathbb{F}_2$ is called an $[n, k]$ linear code. In modern coding theory, we try to construct three tuple of a linear code, an encoder, and a decoder such that decoding error rate of the code is extremely small and the encoder and the decoder is operated in realistic time for finite and appropriate number n. That is, we try to construct optimal a code and a decoder satisfying channel codding theorem.

Let C be an $[n, k]$ linear code, i.e., C is a k dimensional subspace of $\mathbb{F}_2^n$. We define the dual code of C as orthogonal complement of C. We describe $C^{\perp}$ as the dual code. Let $\{e_i\}_{i=1}^{n-k}$ be a base of $C^{\perp}$. We define a parity check matrix $H_C = (h_{ij})_{i=1,j=1}^{n-k,n}$ of C as h_{ij} is equal to jth element of e_i for any i and j. We notice that $H_C \cdot c^{\top}$ so called a syndrome is equal to the zero vector of $\mathbb{F}_2^n$ for any $c \in C$ since any row of H_C is orthogonal to any codeword of C. If a syndrome for a received element c' of $\mathbb{F}_2^n$ is equal to the zero, c' is the sent code word. We notice that the sent code word is changed into a non code word if the syndrome is not equal to the zero vector. Therefore, we estimate bit flip effecting the sent code word by using the syndrome and try to correct the non code word with the estimation.

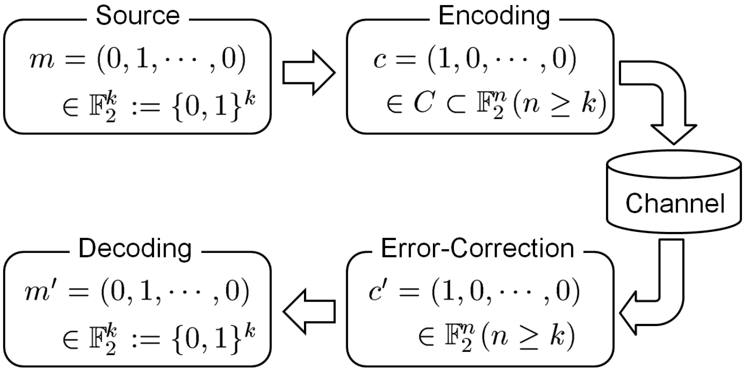
Source
$m = (0, 1, \cdots, 0)$
$\in \mathbb{F}_2^k := \{0, 1\}^k$
Encoding
$c = (1, 0, \cdots, 0)$
$\in C \subset \mathbb{F}_2^n\,(n \geq k)$
Channel
Error-Correction
$c' = (1, 0, \cdots, 0)$
$\in \mathbb{F}_2^n\,(n \geq k)$
Decoding
$m' = (0, 1, \cdots, 0)$
$\in \mathbb{F}_2^k := \{0, 1\}^k$

Figure 4.1: Model of error-correcting codes

4.2 General Quantum Error-Correcting Codes

We introduce an abstract of general quantum codes. In modern coding theory, we focus attention on bit flip error for bit strings. On the other hand, in quantum coding theory , we need to take account of many kinds of error since quantum systems are affected with any time evolution represented by unitary operators or TPCP maps, e.g., a qubit state is changed to another qubit state such like $\alpha|0\rangle + \beta|1\rangle \mapsto \alpha'|0\rangle + \beta'|1\rangle$, where $\alpha, \beta, \alpha', \beta' \in \mathbb{C}$ with $|\alpha|^2 + |\beta|^2 = 1$ and $|\alpha'|^2 + |\beta'|^2 = 1$. We introduced a model of a quantum communication over a noisy quantum channel. Let us consider that information source is a set of quantum systems and a quantum system in information source is encoded to a quantum system so called a code state in a quantum code [2]. A sender prepares a quantum system in a code state and sends it to a receiver over a noisy quantum channel described by a TPCP map. The receiver tries to corrects disturbance of the sent code state and decodes the system to the system in information source.

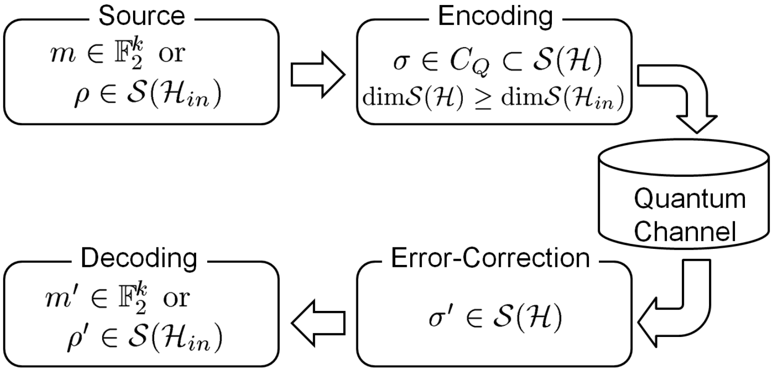
Source
$m \in \mathbb{F}_2^k$ or
$\rho \in \mathcal{S}(\mathcal{H}_{in})$
Encoding
$\sigma \in C_Q \subset \mathcal{S}(\mathcal{H})$
$\dim\mathcal{S}(\mathcal{H}) \geq \dim\mathcal{S}(\mathcal{H}_{in})$
Quantum Channel
Error-Correction
$\sigma' \in \mathcal{S}(\mathcal{H})$
Decoding
$m' \in \mathbb{F}_2^k$ or
$\rho' \in \mathcal{S}(\mathcal{H}_{in})$

Figure 4.2: Model of quantum error-correcting codes

We define quantum error operators and quantum error-correcting codes formally. Suppose that a quantum system $\mathcal{H}$ in a quantum state described by a density operator ρ is prepared and is sent over a noisy quantum channel. The state could be disturbed collapse by noise on the channel. The process is described by a Kraus representation of a TPCP map. A family of operators on $\mathcal{H}$ L which is a complex vector space is called the error. By using a subset $\{L_i\}_i \subset L$ satisfying

$$\sum_i L_i^\dagger L_i = \mathbb{I},$$

a quantum operation of disturbing the quantum stat ρ is represented by

$$\rho \mapsto \sum_i L_i \rho L_i^\dagger.$$

Note that each L_i is called an error operator.

Throughout this paper, we deal with quantum codes constructed from quantum systems in pure states.

[2] We can also consider that information source is a set of bit strings and a bit string of it is encoded to a quantum system in a code state.

Definition 15 *Let $\mathcal{H}$ be a d dimensional Hilbert space. An n dimensional subspace $C \subset \mathcal{H}$ is called a $[d, n]$ quantum code. A pure state of the quantum code C is called a code state.*

A quantum error-correcting code against error operators is, in a word, a pair of a quantum code and operators to correct the error.

Definition 16 *(Knill-Laflamme [60]). Let $C \subset \mathcal{H}$ be a $[d, n]$ quantum code, $L = \{\tilde{L}_i\}_i$ error on $\mathcal{H}$. C is called a quantum error-correcting code against L if there exists a set of operators on $\mathcal{H}$ $R = \{R_j\}_j$ satisfying*

$$\max_{|\psi\rangle \in C} \sum_{i,j} \|(R_j\tilde{L}_i - \langle\psi|R_j\tilde{L}_i|\psi\rangle)|\psi\rangle\|^2 = 0,$$

and $\sum_j R_j^\dagger R_j = \mathbb{I}$ Then, R is called recovery operators against L.

Knill and Laflamme also introduce necessary and sufficient condition for a pair of a quantum code and operators being a quantum error correcting code against given error operators. The condition is derived from the viewpoint of operator algebra.

Theorem 17 *(Knill-Laflamme [60]). Let C be a $[d, n]$ quantum code and L error on $\mathcal{H}$. There exists a set of recovery operators $R = \{R_j\}_j$ with $\sum_j R_j^\dagger R_j = \mathbb{I}$ such that C is a quantum error-correcting code against L if and only if*

$$E\tilde{L}_i^\dagger \tilde{L}_{i'} E = \lambda_{ii'} E,$$

holds for any $\tilde{L}_i, \tilde{L}_{i'} \in L$, where E is the projection operator onto C and $\lambda_{ii'} \in \mathbb{C}$.

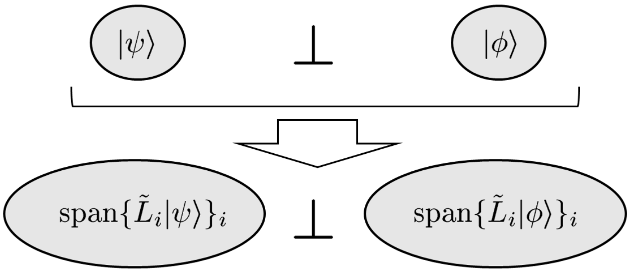
$|\psi\rangle$
$\perp$
$|\phi\rangle$
$\mathrm{span}\{\tilde{L}_i|\psi\rangle\}_i$
$\perp$
$\mathrm{span}\{\tilde{L}_i|\phi\rangle\}_i$

Figure 4.3: Orthogonality between a pair of code states

Lastly, we introduce examples of constructions of general quantum codes against several error. The codes are called stabilizer codes [61] and Calderbank-Shor-Steane (CSS) codes [62, 63]. It is known that CSS codes are a class of stabilizer codes. We call a group

$$\{a_1 A_1 \otimes a_2 A_2 \otimes \cdots \otimes a_n A_n \mid a_i \in \mathbb{C}, A_i \in \{X, Y, Z, \mathbb{I}\}\},$$

with multiple of matrices Pauli group. An abelian subgroup of Pauli group is called a stabilizer group. Let S be a stabilizer group. We define a stabilizer code by

$$C_S := \mathrm{span}\{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} \mid s|\psi\rangle = |\psi\rangle, \forall s \in S\},$$

where any $|\psi\rangle$ is normalized. For example, a subgroup generated by $\{Z \otimes Z \otimes \mathbb{I}, \mathbb{I} \otimes Z \otimes Z\}$ is a stabilizer group. Then, a stabilizer code for the stabilizer group is $\{\alpha|000\rangle + \beta|111\rangle \mid \alpha, \beta \in \mathbb{C}\}$.

CSS codes are a class of stabilizer codes and a CSS code is constructed from a pair of linear codes. Recall that a linear code is called an $[n, k]$ code if the code is a k dimensional vector space of a n dimensional vector space $\mathbb{F}_2^n$ over $\mathbb{F}_2$. Let C and D be $[n, k]$ linear codes over $\mathbb{F}_2$ satisfying $D^\perp \subset C$, where $D^\perp$ be the dual code of D under the standard inner product, i.e., $D^\perp$ is the orthogonal complement of D. A CSS code is defined as a subspace spanned by the collection of the following states

$$\sum_{d \in D^\perp} |d \oplus c\rangle \in (\mathbb{C}^2)^{\otimes n},$$

where $c \in C$ and $\oplus$ denotes bit wise exclusive OR. A twisted relation $D^\perp \subset C$ holds if and only if

$$H_C H_D^\top = \mathbf{0},$$

where H_C (resp. H_D) is an arbitrary parity-check matrix of C (resp. D) and $\mathbf{0}$ is a zero matrix. Performance of error correction of CSS codes depend on performance of error correction of linear codes from which the CSS codes are constructed.

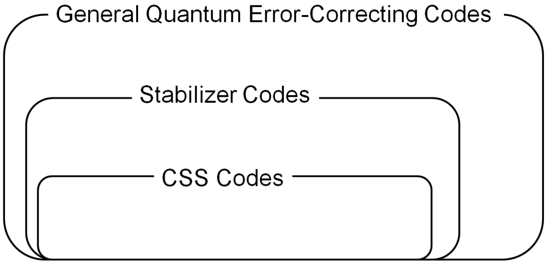

Figure 4.4: Classes of error-correcting codes

Chapter 5

Basics of Quantum Cryptography

5.1 Modern Cryptography

Cryptography is used for achieving untroubled information society [1] . For instance, internet shopping via communication channels between buyers and sellers is protected leaking of secret information to an outsider by using several cryptographic techniques. We call current cryptography modern cryptography. In the above instance, the buyer sends secret information such as personal information, credit card number, and so on, to the seller. Generally, the sender encrypts the secret information so called a plain text to a cipher text by using encryption key and sends the cipher text to the receiver over the public channel. The receiver decodes the cipher text to the plain text by using a decoding key. Let us consider that an eavesdropper obtains the cipher text on the channel. Then, the eavesdropper cannot gain secret information from the text easily since the cipher text cannot be decoded easily without using the decoding key. We often call the sender, the receiver, and the eavesdropper Alice, Bob, and Eve, respectively. The modern cryptography is often classified as public key cryptography and symmetric key cryptography.

- Public key cryptography:
  In public key cryptography, Bob generates a pair of a public key as a encryption key and a secret key as a decoding key firstly. He publishes the public key and keeps the secret key in secret. Alice encrypts a plain text to a cipher text by using the public key published by Bob. Bob receives the cipher text from Alice and decodes the text to the plain text by using the secret key kept by himself. In public key cryptography, every body obtaining the public key can encode a plain text by

[1] For more details, see Ref.[64]. Ref.[65] gives a detailed description of history of cryptography.

using the encoder. However, none but Bob having the secret key can decode by using the decoder. Digital signatures and authentication systems are constructed as applications of public key cryptography. The idea of public key cryptography is introduced by Diffie and Hellman [66] in 1976. Years later, RSA cryptosystem [67] and ElGamal cryptosystem [68] as representative public key cryptography are introduced. Those cryptosystems are constructed from several algorithms to applied properties of algebra.

- Symmetric key cryptography:
  In symmetric key cryptography, encryption key is equal to decoding key exactly and the keys as the secret key are prevented the leakage to a person other than Alice and Bob. Therefore, Alice and Bob share the secret key before using cryptography. This problem is called a key sharing problem. Now, we assume that they share the secret key in secret. Alice encrypts a plain text to a cipher text by using the secret key and sends it to Bob. He decodes it to the plain text by using the secret key. Lightweight computational cost is a peculiarity of symmetric key cryptography, although it is necessary to settle the key sharing problem. Most famous symmetric cryptosystem Deta Encryption Standard (DES) [69] is selected as Federal Information Processing Standard in 1977. Advanced Encryption Standard (AES) [70] is also selected as new standard cryptosystem in USA. MISTY [71] and FEAL [72] are developed in Japan.

We introduced the classification of modern cryptography from a viewpoint of its functions and constructions. In this section, we classify modern cryptography from a viewpoint of its security criteria.

- Computational security:
  We explain security of cryptosystem as an example of computation security. RSA cryptosystem is a kind of public key cryptography. Thus, a public key is published in public. On the other hand, a secret key is kept in secret. Consider that Eve gains the public key and calculates the secret key from the public key. In RSA cryptosystem, factorization of composite number included in the public key is one of methods of calculating the secret key from the public key. Key size of the public key which is now widely used is more than 1024 bits. The factorization of composite number included in such a large size public key is very hard in realistic time. Security guaranteed with hardness of computation is called computational security. It is not argued that cryptosystems with computational security cannot guarantee security without any condition. In the above example, Eve can gain the secret key with factorizing the public key if she can take unlimited computational time. Moreover, Shor proposed a quantum

algorithm [2], so called Shor's algorithm, to enable us to factorize large size number realistically by using a quantum computer. Therefore, cryptography which guarantees computational security is not secure in a long run if computers or algorithms can be improved dramatically.

- Unconditional security:
  We explain security of one-time pad which is a kind of symmetric key cryptography as an example of unconditional security. In one-time pad, calculations is very simple. For a plain text $m \in \mathbb{F}_2^n$ and a secret key $k \in \mathbb{F}_2^n$, a cipher text c has the following form: $c = m \oplus k \in \mathbb{F}_2^n$, where $\oplus$ denotes an operation of the bitwise exclusive OR. On the other hand, decoding of the cipher text is denoted by $m = c \oplus k$. Let M be a random variable relevant to plain texts, K a random variable relevant to secret keys, and C a random variable to cipher texts. Let M, K and C be random variables expressing plain texts, secret keys, and cipher texts, respectively. Then,

$$H(M) = H(M \mid C), \tag{5.1}$$

$$H(M \mid C, K) = 0, \tag{5.2}$$

  hold. Eq.(5.1) denotes that uncertainty of the plain text is not reduced even if we have the cipher text, i.e., Eve cannot gain information of the plain texts if she can gain the cipher texts on the communication channel and has unlimited computational power and time. On the other hand, eq.(5.2) denotes that we can decodes the cipher text to the plain text if we have the secret key, i.e., the legitimate users can decode by using the secret key. In this manner, one-time pad guarantees security by lack of information to decode the cipher text. We call this type of security unconditional security. Cryptography with unconditional security guarantees security for a long time since the security has nothing to do with computational power or time. However, length of the secret key should be grater than length of the plain text and we use the secret key once and then throw it away. In addition, we should resolve the key sharing problem if we use one-time pad in practical.

5.2 Quantum Cryptography

5.2.1 Abstract of Quantum Cryptography

As mentioned above, cryptography with computational security cannot guarantee longterm security if computational algorithms, computer, and so on are made remarkable progress. Therefore, we expect that cryptography with unconditional security is made progress. One-time pad is a kind of

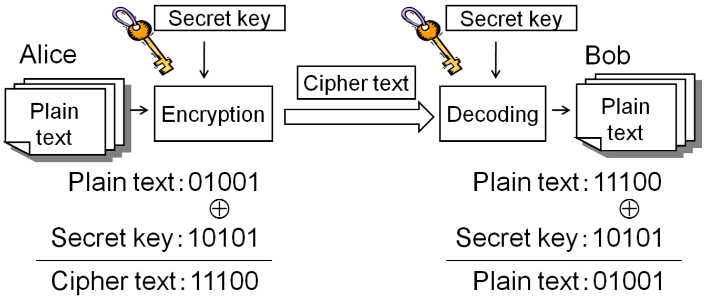

Figure 5.1: One-time pad cryptosystem

symmetric key cryptography with unconditional security. The encryption and the decryption algorithm of one-time pad take at a low computational cost. However, key sharing is a nasty problem. Quantum key distribution protocol (QKD protocol) is a solution for the problem and it is expected to guarantee "unconditional security". In typical QKD protocol, Alice prepares a qubit in a qubit state to which is encoded bit as a key and sends the qubit to Bob over a quantum channel. Bob measures it with an observable and obtains an outcome as a key. After Alice and Bob operate the above process a large number of times or repetitions, they try to detect an eavesdropper Eve with half of the keys. If they dose not detect Eve, secret key is generated by operating error-correction and privacy amplification on remaining the keys. Quantum cryptography is defined as a combination of one-time pad and QKD protocols.

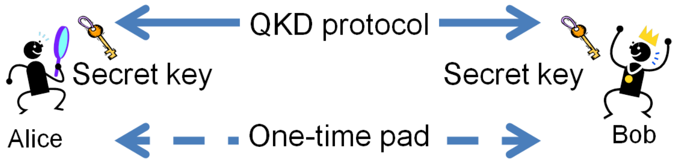

Figure 5.2: A combination of a quantum key distribution protocol and one-time pad

In 1984, Bennet and Brassard proposed original QKD protocol with noncommutative observable σ_x and σ_z. It is so called BB84 protocol [1]. In BB84 protocol, Alice and Bob try to share secret key by using two pairs of orthogonal qubit states realized by four kinds of polarizations of photon [2] and two measurements corresponding to noncommutative observables. A

[2] In practical, phase difference between photons is used for encoding bit instead of polarization of photon. QKD protocol using phase difference of photons for encoding is

generalization of BB84 protocol is discussed, i.e., σ_y in addition to σ_x and σ_z are employed by Alice and Bob, and three pairs of orthogonal qubit states are used for encoding. The general protocol is called six-state quantum key distribution protocol [74]. On the other hand, a QKD protocol which is more simpler than BB84 protocol was introduced. This QKD protocol is called B92 protocol [75]. In B92 protocol, random bit is encoded to one of two nonorthogonal qubit states. In 1991, Ekert proposed a QKD protocol by using the Bell state [76]. The QKD protocol is called E91 protocol. In the protocol, Alice prepares two qubits in the Bell state and sends one of the qubits to Bob. After that they perform one of measurements corresponding σ_x and σ_z randomly and separately on the each qubit. Same outcome as a key is shared if they choose same observable. Then, it is known that security notion of BB84 is equivalent to it of E91.

Several cryptographic techniques other than QKD protocols are introduced in the related works. Okamoto et al., introduced so called OTU cryptosystem [77] and Kawachi et al., introduced so called KKNY cryptosystem [78] in 2000 and 2005 respectively. Those cryptosystem are a kind of quantum public key cryptography. A quantum digital signature scheme was introduced by Gottesman and Chuang in 2001 [79]. The scheme is called GC signature scheme. Hillery et al., introduced a quantum secret sharing scheme so called HBB protocol in 1999 [80].

5.2.2 An Example: BB84 Protocol

We introduce BB84 protocol as an example of QKD protocols. BB84 protocol is constructed from the following steps:

1. Alice prepares a bit generated by random bit and sends qubit in a quantum state of her selecting to Bob over quantum channel. If a generated bit is equal to 0, $|0\rangle$ or $|+\rangle$ are selected randomly. If a generated bit is equal to 1, $|1\rangle$ or $|-\rangle$ are selected randomly. Alice also keeps Z (resp. X) if $|0\rangle$ or $|1\rangle$ (resp. $|+\rangle$ or $|-\rangle$) is selected.

2. Bob receives the qubit and carries out a measurement with respect to observable $Z(=\sigma_z)$ or $X(=\sigma_x)$ randomly on the qubit. Then, he keeps a measurement outcome and selected observable. He also obtains a bit from the outcome, i.e., bitwise transpose: $1 \mapsto 0$ and $-1 \mapsto 1$.

3. They repeat the above steps large times sufficient to generate a bit string with large length.

4. Alice publishes which of the X or Z she has selected to Bob over a public channel. They check the bit string and discard a bit if the bit is generated by X (resp. Z) and the observable Z (resp. X) is selected.

called a differential phase shift-quantum key distribution [73].

5. They calculate error rate of bits randomly chosen from the checked bits. They abort the protocol if the rate is grater than or equal to a preset rate. Otherwise, they perform error correction and privacy amplification on the left over bits to generate final secret key.

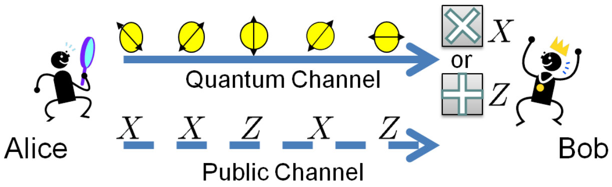

Figure 5.3: BB84 protocol

Table 5.1: The relationship between Alice's bit and Bob's bit

	X		Z	
	0	1	0	1
	$\vert +\rangle$	$\vert -\rangle$	$\vert 0\rangle$	$\vert 1\rangle$
$X = \sigma_x$	0	1	0 or 1	0 or 1
$Z = \sigma_z$	0 or 1	0 or 1	1	0

Table 5.1 denotes the relationship between Alice's bit preparation and bit obtained by Bob. Remark that calculation of the error rate in Step 5 plays a role of a function of detecting eavesdropping, i.e., Alice and Bob determine that Eve obtain large information if the rate is sufficient large. We can share same bit string with error correction and leakage information dose not make sense with privacy amplification [81].

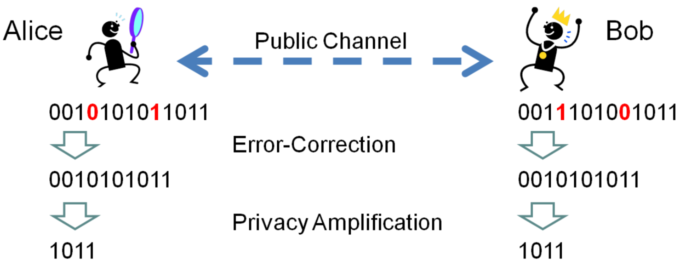

Figure 5.4: Error correction and privacy amplification

5.2.3 Consideration on Security for BB84 Protocol

It is expected that BB84 protocol guarantees “unconditional security”. Unfortunately, there are several definition of unconditional security in according to settings of equipments, channel, and so on. Suppose that equipments and channels employed by the user are ideally perfect, i.e., Alice can prepare the desired qubit, Bob can detect qubit and measure it without false detection and loss of performance of key generating, and noise derived from environment dose not occur on the quantum and public channels. Suppose that an attacker Eve with unconditional computational and physically power eavesdrops on both of the quantum and public channels in this setting. Then, unconditional security means that Eve cannot gain any information without being detected by the user. In this sense, leakage information is zero by using BB84 protocol. Mayers introduced first proof of unconditionally security for BB84 protocol in 1996 [82]. Then, Shor and Preskill proved it by using CSS codes in 2000 [53].

In 2000 [83], Biham et al. introduced a proof by using information disturbance theorem [83, 84]. We summarize the proof introduced by Biham et al. intuitively. Information disturbance theorem means that there is no quantum operation to gain information from a quantum system without disturbing the state. To applying the theorem to the setting of BB84 protocol, it is shown that Eve cannot gain information without disturbing the qubit states. Then, error rate of secret key shared by Alice and Bob is not equal to zero since Bob cannot obtain the desired outcomes from the disturbed state. Therefore, Eve is detected by gaining the information with any quantum operation.

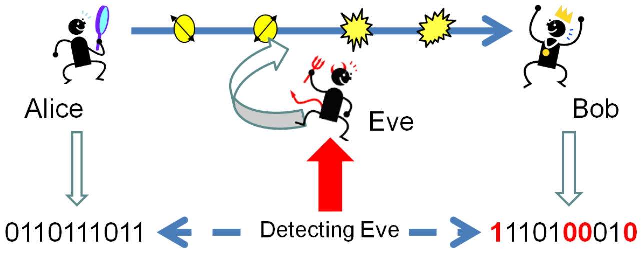

Figure 5.5: Inevitable disturbance of quantum states by eavesdropping

We can immediately see the fact against Eve’s simple attack. Suppose that Eve try to obtain secret key by performing randomly chosen X or Z projective measurement on each qubit on the quantum channel from Alice to Bob and sends the post measurement state to Bob. This attack is called intercept-resend attack. Eve dose not disturb the eigenstates of Z (resp. X) if Eve measures it with Z (resp. X). However, the eigenstates of Z (resp. X)

prepared by Alice is disturbed if Eve measures it with X (resp. Z), i.e., the eigenstate of Z is change to one of two eigenstates of X with probability $1/2$. Considering disagreement of bit string, probability that Alice and Bob share same bit in any element of the bit string is equal to $3/4$. This probability seems large value in oder to detecting Eve with error probability. However, we can make the probability of small value by choosing large number of pairs of bits. For instance, the probability is equal to $(3/4)^n$ for n pairs of bits, then, probability of occurring of disagreement for n pairs of bits is equal to $1-(3/4)^n$. Therefore, the lager number of checked bits, the lager probability of detecting Eve with error rate of bits.

Chapter 6

Mean King's Problem and Its Application

6.1 Mean King's Problem

Mean King's problem is formulated by Vaidman, Aharonov, and Albert [5]. The problem is told as a tale that mean King gives physicist Alice a retrodiction problem [85, 86, 87]. King asks Alice to prepare a qubit system in an arbitrary state. Then, King measures the system with one of observables σ_x, σ_y, and σ_z and obtains an outcome 1 or -1. After this measurement, King gives back Alice the system. Alice measures the post measurement system with an arbitrary measurement. After that King reveals the observable which he employed, then, Alice has to guess the outcome obtained by King immediately by using the outcome obtained by her and knowledge of the observable. The problem is to find the measurement employed by and the initial state prepared by Alice such that she guesses the outcome obtained by King perfectly. In Ref.[5], a solution to the problem is shown using the Bell state. Alice prepares the qubit system given to King and an ancillary qubit system kept by her in the Bell state, then Alice guesses the King's outcome perfectly by using a measurement derived from Aharonov-Bergmann-Lebowitz (ABL) rule [88] on the bipartite qubits system.

Let $\mathcal{H}_A \simeq \mathbb{C}^2$ be a qubit kept by Alice and $\mathcal{H}_K \simeq \mathbb{C}^2$ a qubit given by Alice to King. The bipartite system $\mathcal{H}_A \otimes \mathcal{H}_K$ is prepared in the Bell state $|\Psi^+\rangle = 1/\sqrt{2}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$. Alice gives only $\mathcal{H}_K$ to King, who measures it with one of the observables:

$$\begin{aligned}\sigma_x &= +1|+\rangle\langle+| - 1|-\rangle\langle-|,\\ \sigma_y &= +1|+'\rangle\langle+'| - 1|-'\rangle\langle-'|,\\ \sigma_z &= +1|0\rangle\langle0| - 1|1\rangle\langle1|.\end{aligned}$$

Recall that $|0\rangle = (1,0)^\top, |1\rangle = (0,1)^\top, |+\rangle = 1/\sqrt{2}(1,1)^\top, |-\rangle := 1/\sqrt{2}(1,-1)^\top, |+'\rangle := 1/\sqrt{2}(1,\mathrm{i})^\top$, and $|-'\rangle := 1/\sqrt{2}(1,-\mathrm{i})^\top$. King obtains

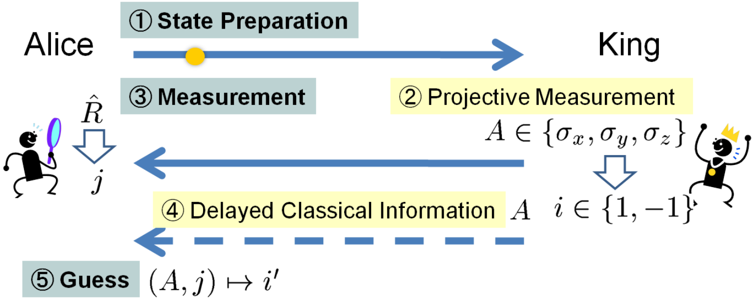

Figure 6.1: Mean King's problem

an outcome $i \in \{1, -1\}$. The measurement changes the state according to the projective (Lüders) postulate. For instance, if King chooses σ_x and obtains i, then, the initial King's state $\rho = \mathrm{tr}_A |\Psi^+\rangle\langle\Psi^+|$ is transformed into,

$$\frac{X_i \rho X_i}{\mathrm{tr}(X_i \rho X_i)},$$

where $X_1 = |+\rangle\langle+|$ and $X_{-1} = |-\rangle\langle-|$. After King measures the system, it is returned to Alice. Alice measures the bipartite system with a PVM [1]

$$\hat{R} := (R_j := |r_j\rangle\langle r_j|)_{j=0}^{3},$$

on $\mathcal{H}_A \otimes \mathcal{H}_K$ defined as

$$\begin{aligned}
|r_0\rangle &:= \frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{2}(|0\rangle|1\rangle e^{\mathrm{i}\pi/4} + |1\rangle|0\rangle e^{-\mathrm{i}\pi/4}),\\
|r_1\rangle &:= \frac{1}{\sqrt{2}}|0\rangle|0\rangle - \frac{1}{2}(|0\rangle|1\rangle e^{\mathrm{i}\pi/4} + |1\rangle|0\rangle e^{-\mathrm{i}\pi/4}),\\
|r_2\rangle &:= \frac{1}{\sqrt{2}}|1\rangle|1\rangle + \frac{1}{2}(|0\rangle|1\rangle e^{-\mathrm{i}\pi/4} + |1\rangle|0\rangle e^{\mathrm{i}\pi/4}),\\
|r_3\rangle &:= \frac{1}{\sqrt{2}}|1\rangle|1\rangle - \frac{1}{2}(|0\rangle|1\rangle e^{-\mathrm{i}\pi/4} + |1\rangle|0\rangle e^{\mathrm{i}\pi/4}).
\end{aligned}$$

and obtains an index of the operator as an outcome $j \in \{0, 1, 2, 3\}$. The relationship between Alice's outcome and King's outcome is denoted in Table 6.1. Using this correspondence, Alice can estimate King's outcome perfectly with her outcome and the knowledge of observable revealed by King. For instance, King employs σ_z and Alice obtains an outcome 2, then the outcome obtained by King is equal to -1.

According to the ABL rule, a probability of obtaining an outcome $i \in \{1, -1\}$ with an observable $\sigma_J (J \in \{x, y, z\})$ between King's measurement

[1] Recall that an n-tuple of operators $(P_i)_{i=1}^n$ is called a projection-valued measure (PVM) if $\sum_{i=1}^n P_i = \mathbb{I}$ and $P_i^2 = P_i^\dagger = P_i$ hold for any i.

Table 6.1: The relationship between King's observables and $\hat{R}$

	0	1	2	3
σ_x	1	-1	1	-1
σ_y	1	-1	-1	1
σ_z	1	1	-1	-1

and Alice's measurement is described by

$$p(\sigma_J = i \mid R_j, |\Psi^+\rangle) = \frac{|\langle r_j| \, \mathbb{I} \otimes P_{\sigma_J = i} |\Psi^+\rangle|^2}{\sum_i |\langle r_j| \, \mathbb{I} \otimes P_{\sigma_J = i} |\Psi^+\rangle|^2},$$

where $P_{\sigma_J=i}$ denotes the projection into the eigenspace of the eigenvalue i of σ_J. For J, i, and j, Alice estimate King's outcome with probability 1 if and only if

$$p(\sigma_J = i \mid R_j, |\Psi^+\rangle) = 1,$$

holds.

6.2 Quantum Key Distribution Using Mean King's Problem

In 2001, Bub [6] proposed a quantum key distribution protocol using Mean King's problem. In the protocol, Alice prepares a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_K \simeq \mathbb{C}^2 \otimes \mathbb{C}^2$ in the Bell state. She gives the system $\mathcal{H}_K$ to King and keeps the system $\mathcal{H}_A$ with her. King measures the system $\mathcal{H}_K$ with one of observables [2],

$$\hat{X} := (X_0 := |\bar{0}\rangle\langle\bar{0}|, X_1 := |\bar{1}\rangle\langle\bar{1}|),$$
$$\hat{Z} := (Z_0 := |0\rangle\langle 0|, Z_1 := |1\rangle\langle 1|),$$

and returns the system to Alice [3]. He keeps the outcome as a secret key. Alice measures the bipartite system exactly with an observable $\hat{R} = \{R_j = |r_j\rangle\langle r_j|\}_{j=1}^4$ on $\mathcal{H}_A \otimes \mathcal{H}_K$ defined in Sec.6.1 that solves Mean King's problem for $\sigma_x(=\hat{X}), \sigma_y(=\hat{Y})$, and $\sigma_z(=\hat{Z})$, and estimates King's outcome. If there is no eavesdropper, Alice and King are able to share the key as $\hat{R}$ solves Mean King's problem for $\sigma_x(=\hat{X})$ and $\sigma_z(=\hat{Z})$ [4]. An eavesdropper called Eve has opportunities to gain information of the secret key on a quantum channel from Alice to King and it from King to Alice.

[2] Note that this notation is slightly different for indexes: $\sigma_x \leftrightarrow \hat{X}, \sigma_z \leftrightarrow \hat{Z}$ $|\bar{0}\rangle\langle\bar{0}| \leftrightarrow |+\rangle\langle+|$, and $|\bar{1}\rangle\langle\bar{1}| \leftrightarrow |-\rangle\langle-|$.

[3] In a similar way $\hat{Y}$ consists of projections derived from σ_y.

[4] It has been shown in Sec.6.1.

The quantum key distribution using Mean King's problem is described as follows:

1. Alice prepares the bipartite system $\mathcal{H}_A \otimes \mathcal{H}_K$ in the Bell state $|\Psi^+\rangle$. She gives $\mathcal{H}_K$ to King and keeps $\mathcal{H}_A$ by herself.

2. King measures $\mathcal{H}_K$ with an observable $\hat{X}$ or $\hat{Z}$ and obtains an outcome 0 or 1 as a sifted key [5]. He returns the system to Alice.

3. Alice measures the bipartite system $\mathcal{H}_A \otimes \mathcal{H}_K$ with a PVM $\hat{R}$ and obtains an outcome $j \in \{1, 2, 3, 4\}$.

4. King announces the observable ($\hat{X}$ or $\hat{Z}$) which he employed.

5. Alice estimates King's outcome with her outcome and knowledge of King's observable.

6. They repeat the above steps $2n$ times to share $2n$ sifted keys and calculate two kinds of error probabilities of sifted keys generated by $\hat{X}$ and $\hat{Z}$ with randomly chosen n sifted keys.

7. If the error probabilities are greater than or equal to a preset $\epsilon(\geq 0)$, they abort the protocol. Otherwise, they perform the leftover n sifted keys to make final keys with errorcorrection and privacy amplification.

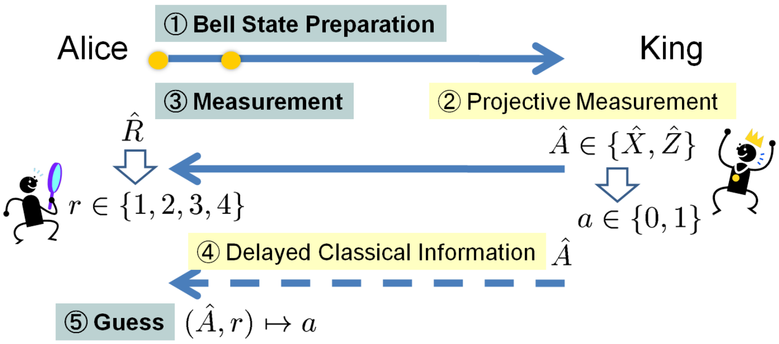

Figure 6.2: Quantum key distribution using Mean King's problem

6.3 Historical Notes

Mean King's problem has been generalized concerning the prepared quantum system and King's measurements [85, 86, 87, 89, 90, 91, 92, 93, 94, 95].

[5] We construct a bit $i \in \{0, 1\}$ from an outcome $i' \in \{1, -1\}$ by using transpose $1 \mapsto 0$ and $-1 \mapsto 1$.

Table 6.2: The relationship between King's observables and $\hat{R}$

	R_1	R_2	R_3	R_4
$\hat{X}$	0	1	0	1
$\hat{Z}$	0	0	1	1

In particular, it has been proved [89, 90, 91] 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 bases [48, 49]. On the other hand, Alice cannot retrodict the outcome with certainty without using entangled states in the setting [92, 93]. In the reference, an upper bound of the success probability is also introduced. In case of King's measurements constructed from biased bases, the problem is also investigated [94, 95].

In QKD protocol using Mean King's problem, Eve try to gain information with measurement on the quantum channel from King to Alice and sends the post measurement state to Alice, i.e., Eve employs an intercept resend attack on the quantum channel from King to Alice. Then, it was shown that error probability, which means bit error rate of a secret key simply, is greater than or equal to 3/8 for the intercept resend attack [6]. Werner et al., [100] showed that Eve cannot gain information about secret key without being detected even if Eve can attack qubits twice on the channels in an arbitrary way. That is, they showed that the information gain by Eve inevitably disturbs the outcomes obtained by the legitimate users. While this result is important, in order to full security proof one has to derive a quantitative trade-off relationship between the information gain by Eve and the error probability of secret key obtained by Alice and Bob. Therefore, in the next section, we drive such a trade-off for several attacks as a first step of obtaining full security proof of the protocol.

Chapter 7

A Solution Using Quantum Error-Correcting Codes

7.1 General Mean King's Problem

We suppose that Alice can prepare an ancillary system in secret in addition to the system given to King. Then, she answers the problem to King by using correlation between the systems. Let d dimensional Hilbert space $\mathcal{H}_K$ be the system given to King and d' dimensional Hilbert space $\mathcal{H}_A$ the ancillary system kept by Alice. King measures the system with one of projective measurements in the conventional setting of Mean King's problem. In this paper, we deal with more general setting with respect to the measurements. King measures the system $\mathcal{H}_K$ with one of the measurements described by families of measurement operators $M^{(J)} = (M_i^{(J)})_i (J = 1, 2, \ldots, m)$ satisfying $\sum_i M_i^{(J)\dagger} M_i^{(J)} = \mathbb{I}$. Suppose that the system in a state ρ is measured with the measurement operators $(M_i^{(J)})_i$, then, recall that the probability of obtaining ith outcome corresponding to $M_i^{(J)}$ is given by $p_i = \mathrm{tr} M_i^{(J)\dagger} M_i^{(J)} \rho$ and the post measurement state is represented as

$$\frac{M_i^{(J)} \rho M_i^{(J)\dagger}}{p_i}.$$

In this setting, the general Mean King's problem is described as the follows:

1. Alice prepares the bipartite system $\mathcal{H}_A \otimes \mathcal{H}_K$ in an initial state. She gives the system $\mathcal{H}_K$ to King and keeps the ancillary system $\mathcal{H}_A$.

2. King measures the system with one of the measurements described by

$$M^{(J)} = (M_i^{(J)})_i \quad (J = 1, 2, \ldots, m),$$

then, King obtains ith outcome. The system is returned to Alice after he measures it.

3. Alice measures the bipartite system $\mathcal{H}_A \otimes \mathcal{H}_K$ with a suitable Positive Operator Valued Measure (POVM) $P = (P_j)_j$, i.e., $P_j \geq 0$ and $\sum_j P_j = \mathbb{I}$ hold, and she obtains jth outcome.

4. King announces the measurement $M_i^{(J)}$ which he employed.

5. Alice estimates the ith outcome obtained by King immediately by using the jth outcome and the measurement $M^{(J)}$.

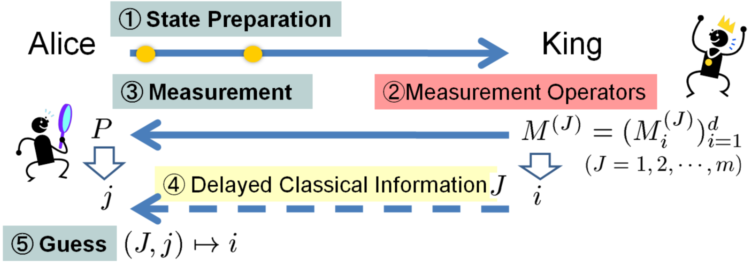

Figure 7.1: General Mean King's problem

With given d and measurements $M^{(J)} = (M_i^{(J)})_i$, we say that a solution to 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.

7.2 A Solution to the Problem

In this section, we introduce a solution of the general Mean King's problem by using the relationship between the problem and quantum error-correcting codes. Note that the following theorem is a solution to Mean King's problem. In the next section, we prove existence of the solution in prime power dimensional case.

Theorem 18 *Let $C \subset \mathcal{H}_A \otimes \mathcal{H}_K$ be an n dimensional subspace (i.e., C is a $[dd', n]$ quantum code) and E the projection operator onto C. If there exists l-tuple of Kraus operators $(L_k)_{k=1}^l$ on $\mathcal{H}_K$ with $\sum_k L_k^\dagger L_k = \mathbb{I}_K$ and non-empty index sets $X^{(J,i)} \subset \{1, 2, \ldots, l\}$ satisfying*

$$\mathbb{I}_A \otimes M_i^{(J)} = \textstyle\sum_{k \in X^{(J,i)}} \mathbb{I}_A \otimes L_k \text{ on } C, \tag{7.1}$$

$$X^{(J,i)} \cap X^{(J,i')} = \emptyset, \quad \forall J, \forall i \neq i', \tag{7.2}$$

$$E(\mathbb{I}_A \otimes L_k)^\dagger (\mathbb{I}_A \otimes L_{k'}) E = \lambda_{kk'} \delta_{kk'} E, \tag{7.3}$$

for some $\lambda_{kk'} \in \mathbb{C}$, then

(i) Alice can solve King's problem for any initial state in C,

(ii) C is a quantum error-correcting code against $\mathrm{span}\{\mathbb{I}_A \otimes L_k\}_{k=1}^{l}$.

Condition (7.1) denotes the relationship between the measurement operators employed by King and the error operators. Condition (7.2) denotes that a set of operators belong to ith outcome with the measurement is distinct from one belong to $i'(\neq i)$th outcome with the same measurement. Condition (7.3) is a sufficient condition for distinguishing kinds of the error operators perfectly.

Proof

(i) Let $|\Phi\rangle \in C$ be an initial state prepared by Alice. If King chooses Jth measurement and obtains ith outcome, then the post measurement state is proportional to [1]

$$\mathbb{I}_A \otimes M_i^{(J)}|\Phi\rangle \in \bigoplus_{k\in X^{(J,i)}} K_k,$$

where $K_k := \mathrm{span}\{\mathbb{I}_A \otimes L_k|\psi\rangle \mid |\psi\rangle \in C\}(k = 1, 2, \ldots, l)$. Note that K_k is orthogonal to $K_{k'}$ for $k \neq k'$ from condition (7.3). Let P_k be the projection operator onto K_k, then $\mathcal{P} := (P_1, P_2, \ldots, P_l, P^{\perp})$ forms a (discrete) projection valued measure (PVM), where $P^{\perp} := \mathbb{I}_A \otimes \mathbb{I}_K - \sum_{k=1}^{l} P_k$.

Let Alice performs the PVM measurement $\mathcal{P}$ and obtains kth outcome $(k = 1, 2, \ldots l, \perp)$. With a revealed J and the outcome k, Alice is assured that King's outcome i satisfied $k \in X^{(J,i)}$. However, from condition (7.2), such i is uniquely determined, and thus Alice can correctly guess the King's outcome.

(ii) For any $\tilde{L}_\alpha = \sum_{k=1}^{l} \alpha_k(\mathbb{I}_A \otimes L_k), \tilde{L}_\beta = \sum_{k'=1}^{l} \beta_{k'}(\mathbb{I}_A \otimes L_{k'}) \in \mathrm{span}\{\mathbb{I}_A \otimes L_k\}_{k=1}^{l}$,

$$E\tilde{L}_\alpha^\dagger \tilde{L}_\beta E = \left(\sum_{k,k'=1}^{l} \overline{\alpha_k}\beta_{k'}\lambda_k\right)E,$$

holds, where $\alpha_k, \beta_k \in \mathbb{C}$. By using the above equation and the Theorem 17, it is shown that C is a quantum error-correcting code against $\mathrm{span}\{\mathbb{I}_A \otimes L_k\}_{k=1}^{l}$. ■

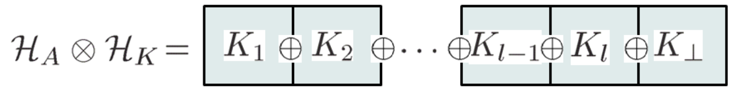

Figure 7.2: Decomposition of the bipartite system into orthogonal subspaces

Thus, it is a solution of Mean King's problem that Alice prepares a code state of a quantum error-correcting code against errors into decomposed

[1] $\bigoplus$ denotes direct sum of several subspaces.

the measurement operators and distinguishes a kind of the error operators belong to the measurement perfectly. Note that the error operators (Kraus operators) $(L_k)_{k=1}^{l}$ denotes not the measurement process performed by King on $\mathcal{S}(\mathcal{H}_K)$. but the quantum operation as adding the error to the system.

7.3 Existence of Solutions in Prime-Power Dimensions

In this section, we show existence of the our solution of Mean King's problem owing to the previous works [89] in prime-power dimensions, i.e., we show a construction of Kraus operators and index sets satisfying all conditions of Theorem 18. We also show a concrete example of the solution by using the above construction in the case of 2 dimensions.

We denote by $\mathcal{L}(\mathcal{H})$ the set of all linear operators on d dimensional Hilbert space $\mathcal{H}$. Note that $\mathcal{L}(\mathcal{H})$ is a d^2 dimensional Hilbert space with respect to the Hilbert-Schmidt inner product:

$$\langle A|B\rangle_{HS} := \mathrm{tr}\, A^\dagger B.$$

In the following, we consider the case where $C \subset \mathcal{H}_A \otimes \mathcal{H}_K$ is a one dimensional subspace spanned by a maximal entangled state

$$|\Psi\rangle := \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |\psi_i\rangle \otimes |\phi_i\rangle \tag{7.4}$$

with orthonormal bases $\{|\psi_i\rangle\}_i$ and $\{|\phi_i\rangle\}_i$ of $\mathcal{H}_A = \mathcal{H}_K = \mathcal{H}$. This includes all conventional models of Mean King's problem.

Proposion 19 *Let $\{L_k\}_{k=1}^{d^2}$ be an ortho"normal"base of $\mathcal{L}(\mathcal{H})$ with $\langle L_k|L_{k'}\rangle_{HS} = \frac{1}{d}\delta_{kk'}$. Then, $\{L_k\}_{k=1}^{d^2}$ satisfies $\sum_{k=1}^{d^2} L_k^\dagger L_k = \sum_{k=1}^{d^2} L_k L_k^\dagger = \mathbb{I}$ and condition (7.3) irrespective of the choice of orthonormal bases $\{|\psi_i\rangle\}_i$ and $\{|\phi_i\rangle\}_i$.*

Lemma 20 *Let $\{L_k\}_{k=1}^{d^2}$ be an ortho"normal"base of $\mathcal{L}(\mathcal{H})$ with $\langle L_k|L_{k'}\rangle_{HS} = \frac{1}{d}\delta_{kk'}$. Then,*

$$\sum_{k=1}^{d^2} L_k^\dagger L_k = \sum_{k=1}^{d^2} L_k L_k^\dagger = \mathbb{I},$$

holds.

Proof

Since $\langle L_k|L_{k'}\rangle_{HS} = \operatorname{tr} L_k^\dagger L_{k'} = \operatorname{tr} L_{k'}L_k^\dagger = \langle L_{k'}^\dagger|L_k^\dagger\rangle_{HS}$, $\{L_k^\dagger\}_{k=1}^{d^2}$ also forms an ortho“normal”bases and $A = d\sum_{k=1}^{d^2} \operatorname{tr}(L_k A)L_k^\dagger$ for any $A \in \mathcal{L}(\mathcal{H})$. With $A = |\psi\rangle\langle\phi|$, we have $|\psi\rangle\langle\phi| = d\sum_k \langle\phi|L_k\psi\rangle L_k^\dagger$ and

$$\langle\phi|\phi\rangle|\psi\rangle = d\sum_k \langle\phi|L_k\psi\rangle L_k^\dagger|\phi\rangle,$$

for any $|\psi\rangle, |\phi\rangle \in \mathcal{H}$. From this, we obtain

$$\sum_{j=1}^{d}\langle\phi_j|\phi_j\rangle|\psi\rangle = \sum_{j=1}^{d}(d\sum_{k=1}^{d^2}\langle\phi_j|L_k\psi\rangle L_k^\dagger|\phi_j\rangle).$$

The above equation holds if and only if,

$$|\psi\rangle = (\sum_{k=1}^{d^2} L_k^\dagger L_k)|\psi\rangle,$$

holds for any $|\psi\rangle$. Thus $\sum_k L_k^\dagger L_k = \mathbb{I}$. By exchanging L_k and $L_k^\dagger$, we also have $\sum_k L_k L_k^\dagger = \mathbb{I}$. ■

Proof of Proposition 19

From Lemma 20, we only have to show condition (7.3) with arbitrary orthonormal bases $\{|\psi_i\rangle\}_i$ and $\{|\phi_i\rangle\}_i$. Notice that

$$\begin{aligned}\langle(\mathbb{I}_A \otimes L_k)\Psi|(\mathbb{I}_A \otimes L_{k'})\Psi\rangle &= \frac{1}{d}\sum_{i=1}^{d}\langle\phi_i|(L_k^\dagger L_{k'})\phi_i\rangle\\ &= \frac{1}{d}\operatorname{tr} L_k^\dagger L_{k'}\\ &= \frac{1}{d^2}\delta_{kk'},\end{aligned}$$

holds for arbitrary $\{|\psi_i\rangle\}_i$ and $\{|\phi_i\rangle\}_i$. Since C is a one dimensional subspace spanned by $|\Psi\rangle$, condition (7.3) holds with $\lambda_k = 1/d^2$. ■

We consider the following correspondence (which is similar to Choi-Jamiołkowski isomorphisim [96, 97, 98]) between operators on $\mathcal{H}$ and vectors of $\mathcal{H}\otimes\mathcal{H}$:

$$L \in \mathcal{L}(\mathcal{H}) \mapsto \mathbb{I}\otimes L|\Psi\rangle \in \mathcal{H}\otimes\mathcal{H}. \tag{7.5}$$

This gives an isomorphism between Hilbert spaces $\mathcal{L}(\mathcal{H})$ and $\mathcal{H}\otimes\mathcal{H}$ since

$$L = L' \quad \text{if and only if} \quad \mathbb{I}\otimes L|\Psi\rangle = \mathbb{I}\otimes L'|\Psi\rangle, \tag{7.6}$$

$$\forall|\psi\rangle \in \mathcal{H}\otimes\mathcal{H},\ \exists! L \in \mathcal{L}(\mathcal{H}) \text{ s.t. } |\psi\rangle = \mathbb{I}\otimes L|\Psi\rangle, \tag{7.7}$$

$$\forall L, M \in \mathcal{L}(\mathcal{H}),\ \frac{1}{d}\langle L|M\rangle_{HS} = \langle(\mathbb{I}\otimes L)\Psi|(\mathbb{I}\otimes M)\Psi\rangle. \tag{7.8}$$

Let C be the one dimensional subspace of $\mathcal{H}\otimes\mathcal{H}$ spanned by $|\Psi\rangle$:

- **Remark 1**: From (7.6), condition (7.1) reduces to the operator-equality: $M_i^{(J)} = \sum_{k \in X^{(J,i)}} L_k$.
- **Remark 2**: From (7.8), condition (7.3) reduces to the orthogonality-condition of $\{L_k\}_k$: $\langle L_k | L_{k'} \rangle_{HS} = 1/d \delta_{kk'}$.
- **Remark 3**: Let $\{|\Phi_i\rangle\}_{i=1}^{d^2}$ be an orthonormal bases on $\mathcal{H} \otimes \mathcal{H}$. Define operators $\{N_i\}_{i=1}^{d^2}$ by $|\Phi_i\rangle = (\mathbb{I} \otimes dN_i)|\Psi\rangle$, then $\langle N_i | N_j \rangle_{HS} = 1/d\delta_{ij}$ holds.

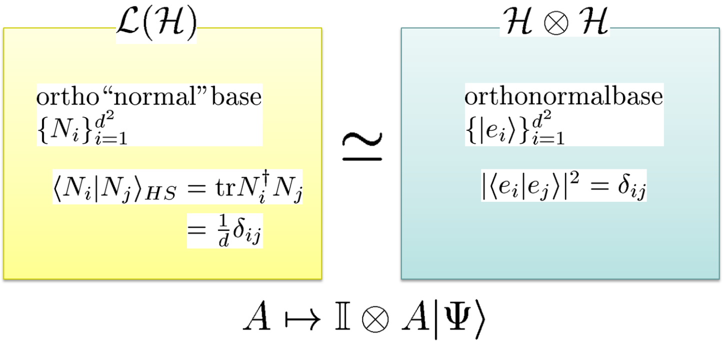
$\mathcal{L}(\mathcal{H})$
ortho“normal”base
$\{N_i\}_{i=1}^{d^2}$
$\langle N_i | N_j \rangle_{HS} = \mathrm{tr} N_i^\dagger N_j$
$= \frac{1}{d}\delta_{ij}$
$\simeq$
$\mathcal{H} \otimes \mathcal{H}$
orthonormalbase
$\{|e_i\rangle\}_{i=1}^{d^2}$
$|\langle e_i | e_j \rangle|^2 = \delta_{ij}$
$A \mapsto \mathbb{I} \otimes A|\Psi\rangle$

Figure 7.3: An isomorphism between $\mathcal{L}(\mathcal{H})$ and $\mathcal{S}(\mathcal{H} \otimes \mathcal{H})$

In the following, we prove the existences of Kraus operators $\{L_k\}_k$ and index set $X^{(J,i)}$ in Theorem 18 for the case of mutually unbiased bases (MUBs). Let $\{|J,i\rangle\}_{i=1}^{d}$ $(J = 1, 2, \ldots, d+1)$ be complete sets of MUBs:

$$|\langle J, i | J', i' \rangle|^2 = \delta_{JJ'}\delta_{ii'} + \frac{1}{d}(1 - \delta_{JJ'}),$$

and let

$$M_i^{(J)} := |J, i\rangle\langle J, i|.$$

Let $s(k, J) \in \{1, 2, \ldots, d\}$ be a decision function of Alice so that Alice will predict King's output to be $s(k, J)$ if she gets outcome k and King's bases is J. In Ref.[89], it was proved that there exists a decision function $s(k, J)$ and an orthonormal bases $\{|k\rangle\}_{k=1}^{d^2}$ of $\mathcal{H} \otimes \mathcal{H}$ if and only if there exists the maximal number $d + 1$ of orthogonal Latin squares: note that the latter is known to exist when d is a power prime, but does not exist, e.g., for $d = 6, 10$. In particular, $s(k, J)$ and $\{|k\rangle\}_k$ satisfy

$$\langle \Phi_{J,i} | k \rangle = \frac{1}{\sqrt{d}} \delta_{i,s(k,J)}, \tag{7.9}$$

where

$$|\Phi_{J,i}\rangle := \overline{|J,i\rangle} \otimes |J,i\rangle \ (\ \overline{|J,i\rangle} := \sum_j \overline{\langle \phi_j | J, i \rangle} |\psi_j\rangle).$$

Indeed,

$$|k\rangle := \frac{1}{\sqrt{d}} \sum_{J=1}^{d+1} |\Phi_{J,s(k,J)}\rangle - |\Phi\rangle,$$

satisfies eq.(7.9).
(See eq.(7.9) in Ref.[89]: note that our notation is slightly different for indexes: $J \leftrightarrow A$, $i \leftrightarrow a$, $k \leftrightarrow I$.)

Notice that

$$\frac{1}{\sqrt{d}} |\Phi_{J,i}\rangle = \mathbb{I} \otimes M_i^{(J)} |\Psi\rangle, \tag{7.10}$$

holds. Now, we define Kraus operators $\{L_k\}_{k=1}^{d^2}$ by

$$|k\rangle = (\mathbb{I} \otimes dL_k)|\Psi\rangle, \tag{7.11}$$

and an index set by

$$X^{(J,i)} := \{k \in \{1, \dots, d^2\} \mid i = s(k, J)\}. \tag{7.12}$$

Then, from eq.(7.8), $\{L_k\}_k$ forms an ortho"normal"bases of $\mathcal{L}(\mathcal{H})$: $\langle L_k|L_{k'}\rangle_{HS} = 1/d\delta_{kk'}$. From Proposition 19, we have $\sum_k L_k^\dagger L_k = \mathbb{I}$ and condition (7.3). From definition eq.(7.12), $X^{(J,i)}$ satisfies condition eq.(7.2). Applying eq.(7.8) with eq.(7.10) and eq.(7.11), we have the following equation from eq.(7.9)

$$d\langle M_i^{(J)}|L_k\rangle_{HS} = \delta_{i,s(k,J)}.$$

Indeed,

$$\begin{aligned}
\langle M_i^{(J)}|L_k\rangle_{HS} &= d\langle (\mathbb{I} \otimes M_i^{(J)})\Psi|(\mathbb{I} \otimes L_k)\Psi\rangle \\
&= \langle (\mathbb{I} \otimes M_i^{(J)})\Psi|(\mathbb{I} \otimes dL_k)\Psi\rangle \\
&= \frac{1}{\sqrt{d}}\langle \Phi_{J,i}|k\rangle \\
&= \frac{1}{\sqrt{d}}\frac{1}{\sqrt{d}}\delta i, s(k, J) \\
&= \frac{1}{d}\delta i, s(k, J),
\end{aligned}$$

holds. Thus, we obtain condition (7.1):

$$M_i^{(J)} = d\sum_k \langle L_k|M_i^{(J)}\rangle_{HS} L_k = \sum_k \delta i, s(k, J) L_k = \sum_{k \in X^{(J,i)}} L_k.$$

Therefore, we have shown the existence of Kraus operators $\{L_k\}_{k=1}^{d^2}$ and index set $X^{(J,i)}$ satisfying all the conditions in Theorem 18 provided that there exists the maximal number $d + 1$ of orthogonal Latin squares. We also reconsider the result given by Ref.[89] from a viewpoint of the quantum error-correcting codes.

7.4 An Example: A Solution in Two Dimensions

Suppose that Alice prepares qubit systems described by $\mathcal{H}_A \otimes \mathcal{H}_K \simeq \mathbb{C}^2 \otimes \mathbb{C}^2$ in a Bell state $|\Psi^+\rangle = 1/\sqrt{2}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$, where $|0\rangle = (1,0)^\top$ and $|1\rangle = (0,1)^\top$. King chooses one of measurement operators constructed from MUBs in 2 dimensional Hilbert space:

$$\begin{aligned} M^{(1)} &:= (M_1^{(1)} := |+\rangle\langle+|, M_2^{(1)} := |-\rangle\langle-|), \\ M^{(2)} &:= (M_1^{(2)} := |+'\rangle\langle+'|, M_2^{(2)} := |-'\rangle\langle-'|), \\ M^{(3)} &:= (M_1^{(3)} := |0\rangle\langle 0|, M_2^{(3)} := |1\rangle\langle 1|), \end{aligned}$$

where $|+\rangle = 1/\sqrt{2}(1,1)^\top, |-\rangle = 1/\sqrt{2}(1,-1)^\top, |+'\rangle = 1/\sqrt{2}(1,\mathrm{i})^\top$, and $|-'\rangle = 1/\sqrt{2}(1,-\mathrm{i})^\top$. Let us define

$$\begin{aligned} L_1 &:= \frac{1}{4}\begin{pmatrix} 0 & -1-\mathrm{i} \\ -1+\mathrm{i} & 2 \end{pmatrix}, \\ L_2 &:= \frac{1}{4}\begin{pmatrix} 2 & -1+\mathrm{i} \\ -1-\mathrm{i} & 0 \end{pmatrix}, \\ L_3 &:= \frac{1}{4}\begin{pmatrix} 0 & 1+\mathrm{i} \\ 1-\mathrm{i} & 2 \end{pmatrix}, \\ L_4 &:= \frac{1}{4}\begin{pmatrix} 2 & 1-\mathrm{i} \\ 1+\mathrm{i} & 0 \end{pmatrix}, \end{aligned}$$

by using eq.(7.11) and the measurement employed by Alice in Ref.[89] generalized from Ref.[5]. As mentioned in the previous, we find that $\sum_{k=1}^4 L_k^\dagger L_k = \mathbb{I}_K$ and

$$\begin{aligned} M_1^{(1)} &= L_3 + L_4, \quad M_2^{(1)} = L_1 + L_2, \\ M_1^{(2)} &= L_1 + L_4, \quad M_2^{(2)} = L_2 + L_3, \\ M_1^{(3)} &= L_2 + L_4, \quad M_2^{(3)} = L_1 + L_3, \end{aligned}$$

hold for the measurement operators performed by King and $(L_k)_{k=1}^4$. That is, the operators $(L_k)_{k=1}^4$ and the index sets $X^{(J,i)}$ (see Table 7.1) satisfy conditions (7.1) and (7.2) of Theorem 18. For the Bell state $|\Psi^+\rangle$,

$$\langle (\mathbb{I}_A \otimes L_k)\Psi^+ | (\mathbb{I}_A \otimes L_{k'})\Psi^+ \rangle = \frac{1}{4}\delta_{kk'},$$

holds, i.e., condition (7.3) is satisfied by the above equation. Remark that Alice's measurement $\hat{L}$, which consists of projections into $\mathrm{span}\{(\mathbb{I}_A \otimes L_k)|\Psi^+\rangle\}$ for any k, in the above setting is equal to the proposed measurement $\hat{R}$ proposed in the original work.

Therefore, we can reconsider the solution in Ref.[5, 89] in the case of qubit systems from the viewpoint of quantum error-correcting codes.

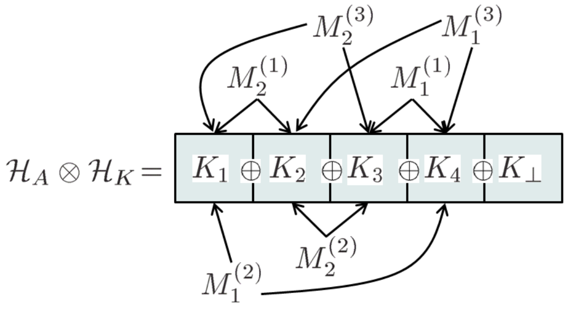
$M_2^{(3)}$
$M_1^{(3)}$
$M_2^{(1)}$
$M_1^{(1)}$
$\mathcal{H}_A \otimes \mathcal{H}_K =$
$K_1 \oplus K_2 \oplus K_3 \oplus K_4 \oplus K_\perp$
$M_2^{(2)}$
$M_1^{(2)}$

Figure 7.4: Decomposition of qubit systems $\mathcal{H}_A \otimes \mathcal{H}_K$ into five orthogonal subspaces

Table 7.1: The relationship between the measurement operators and index sets in 2 dimensions

J	i	$X^{(J,i)}$	J	i	$X^{(J,i)}$
1	1	3, 4	1	2	1, 2
2	1	1, 4	2	2	2, 3
3	1	2, 4	3	2	1, 3

7.5 Construction of Mean King's Problem with Proposal

In this section, we introduce a setting of Mean King's problem which is solved by using our proposal, then, measurement operators employed by King is defined by any orthonormal bases and an initial state is a 1 dimensional quantum code spanned by a maximal entangled state.

First we define Kraus operators on d dimensional Hilbert space $\mathcal{H}_K$. Let $\{|f_i\rangle\}_{i=1}^d$ be an orthonormal base. Define operators on $\mathcal{H}_K$ $(L_{ij})_{i,j=1}^d$ by

$$(\mathbb{I} \otimes dL_{ij})|\Psi\rangle = |f_i\rangle \otimes |f_j\rangle \in \mathcal{H}_A \otimes \mathcal{H}_K, \tag{7.13}$$

where $|\Psi\rangle := 1/\sqrt{d}\sum_{i=1}^d |f_i\rangle \otimes |f_i\rangle$. We find that (i) $\{L_{ij}\}_{i,j=1}^d$ be an ortho"normal"base of $\mathcal{L}(\mathcal{H}_\mathcal{K})$, i.e., $\langle L_{ij}|L_{i'j'}\rangle_{HS} = 1/d\delta_{ij,i'j'}$ holds, since the linear transpose Eq.(7.13) is the isomorphism between $\mathcal{L}(\mathcal{H}_\mathcal{K})$ and $\mathcal{H}_A \otimes \mathcal{H}_K$, (ii) $\sum_{i,j=1}^d L_{ij}^\dagger L_{ij} = \mathbb{I}$ holds since $\{L_{ij}\}_{i,j=1}^d$ is the ortho"nomal" base.

Define index sets $X^{(J,i)} := \{(1, J^{(i)}(1)), (2, J^{(i)}(2)), \ldots, (d, J^{(i)}(d))\} \subset [d] \times [d]$ $(i = 1, 2, \ldots, d$ and $J = 1, 2, \ldots, m)$ as $J^{(i)}(l) \neq J^{(i')}(l)$ for any $i \neq i', l$ and $\{J^{(i)}(l) \mid l \in [d]\} = [d]$ holds, where $[d] := \{1, 2, \ldots, d\}$.

- **Remark 4**: A size $d \times d$ matrix $\hat{J} = (J_{il} := J^{(i)}(l))_{1 \leq i,l \leq d}$ is a Latin square, i.e., $\hat{J}$ has d different symbols, each occurring exactly once in each row and each column.

Define an index set $X^{(0,i)} := \{(i,m)\}_{m=1}^{d} \subset [d] \times [d]$ $(i \in [d])$. We find that $X^{(J,i)} \cap X^{(J,i')} = \emptyset$ holds for any J and $i \neq i'$.

Lemma 21 *Define a family of operators* $M^{(0)} := (M_i^{(0)})_{i=1}^{d}$ *as* $M_i^{(0)} := \sum_{j=1}^{d} L_{ij}$ *and define* $M^{(J)} := (M_i^{(J)})_{i=1}^{d}$ *(*$J = 1, 2, \ldots, m$*) as* $M_i^{(J)} := \sum_{(j,k)\in X^{(J,i)}} L_{jk}$*, then,* $|M_i^{(0)} f_l\rangle = \frac{\delta_{il}}{\sqrt{d}}|f\rangle$ *and* $|M_i^{(J)} f_l\rangle = \frac{1}{\sqrt{d}}|f_{J^{(i)}(l)}\rangle$ *hold for any* $i, J \in [d]$*, where* $|f\rangle := \sum_{j=1}^{d} |f_j\rangle$.

Proof For any $j, k \in [d]$,

$$\sum_{l=1}^{d} |f_l\rangle \otimes |L_{jk} f_l\rangle = \frac{1}{\sqrt{d}}|f_j\rangle \otimes |f_k\rangle, \tag{7.14}$$

holds from eq.(7.13). Form eq.(7.14),

$$\begin{aligned}
\sum_{l=1}^{d}(\mathbb{I} \otimes M_i^{(0)})|f_l\rangle \otimes |f_l\rangle &= \sum_{l,j=1}^{d} |f_l\rangle \otimes |L_{ij} f_l\rangle \\
&= \sum_{j=1}^{d} \frac{1}{\sqrt{d}}|f_i\rangle \otimes |f_j\rangle \\
&= |f_j\rangle \otimes \sum_{j=1}^{d} \frac{1}{\sqrt{d}}|f_j\rangle \\
&= \sum_{l=1}^{d} |f_l\rangle \otimes \frac{\delta_{il}}{\sqrt{d}} \sum_{j=1}^{d} |f_j\rangle,
\end{aligned}$$

holds, therefore, we have $|M_i^{(0)} f_l\rangle = \delta_{il}/\sqrt{d}|f\rangle$. For any $i, J \neq 0$,

$$\begin{aligned}
\sum_{l=1}^{d}(\mathbb{I} \otimes M_i^{(J)})|f_l\rangle \otimes |f_l\rangle &= \sum_{l=1}^{d} \sum_{(j,k)\in X^{(J,i)}} |f_l\rangle \otimes |L_{jk} f_l\rangle \\
&= \sum_{(j,k)\in X^{(J,i)}} \frac{1}{\sqrt{d}}(\mathbb{I} \otimes d L_{jk})|\Psi\rangle \\
&= \sum_{(j,k)\in X^{(J,i)}} \frac{1}{\sqrt{d}}|f_j\rangle \otimes |f_k\rangle \\
&= \sum_{j=1}^{d} |f_j\rangle \otimes \frac{1}{\sqrt{d}}|f_{J^{(i)}(j)}\rangle,
\end{aligned}$$

holds from eq.(7.14), therefore, we have $|M_i^{(J)} f_l\rangle = 1/\sqrt{d}|f_{J^{(i)}(l)}\rangle$. ■

Corollary 22 *$M^{(J)}$ is a set of measurement operators for any J with $\sum_{i=1}^{d} {M_i^{(J)}}^{\dagger} M_i^{(J)} = \mathbb{I}$.*

Proof We find that

$$\begin{aligned}
\langle f_l|\sum_{i=1}^{d} {M_i^{(0)}}^{\dagger} M_i^{(0)}|f_{l'}\rangle &= \langle f_l|\sum_{i=1}^{d} {M_i^{(0)}}^{\dagger} \sum_{k=1}^{d} |f_k\rangle\langle f_k|M_i^{(0)}|f_{l'}\rangle \\
&= \sum_{i,k=1}^{d} \langle f_l|{M_i^{(0)}}^{\dagger}|f_k\rangle\langle f_k|M_i^{(0)}|f_{l'}\rangle \\
&= \sum_{i,k=1}^{d} \overline{\langle f_k|M_i^{(0)}|f_l\rangle}\langle f_k|M_i^{(0)}|f_{l'}\rangle \\
&= \sum_{i,k=1}^{d} \overline{\langle f_k|\frac{1}{\sqrt{d}}\delta_{il}|f\rangle}\langle f_k|\frac{1}{\sqrt{d}}\delta_{il'}|f\rangle \\
&= \sum_{i,k=1}^{d} \frac{1}{d}\delta_{il}\delta_{il'}\overline{\langle f_k|f\rangle}\langle f_k|f\rangle \\
&= \frac{1}{d}\sum_{i=1}^{d} \delta_{il}\delta_{il'}\langle f|f\rangle \\
&= \sum_{i=1}^{d} \delta_{il}\delta_{il'} = \delta_{ll'},
\end{aligned}$$

holds. For any $J \neq 0$,

$$\begin{aligned}
\langle f_l|\sum_{i=1}^{d} {M_i^{(J)}}^{\dagger} M_i^{(J)}|f_{l'}\rangle &= \langle f_l|\sum_{i=1}^{d} {M_i^{(J)}}^{\dagger} \sum_{k=1}^{d} |f_k\rangle\langle f_k|M_i^{(J)}|f_{l'}\rangle \\
&= \sum_{i,k=1}^{d} \langle f_l|{M_i^{(J)}}^{\dagger}|f_k\rangle\langle f_k|M_i^{(J)}|f_{l'}\rangle \\
&= \sum_{i,k=1}^{d} \overline{\langle f_k|M_i^{(J)}|f_l\rangle}\langle f_k|M_i^{(J)}|f_{l'}\rangle \\
&= \sum_{i,k=1}^{d} \overline{\langle f_k|\frac{1}{\sqrt{d}}|f_{J^{(i)}(l)}\rangle}\langle f_k|\frac{1}{\sqrt{d}}|f_{J^{(i)}(l')}\rangle \\
&= \frac{1}{d}\sum_{i,k=1} \langle f_{J^{(i)}(l)}|f_k\rangle\langle f_k|f_{J^{(i)}(l')}\rangle \\
&= \frac{1}{d}\sum_{i=1}\langle f_{J^{(i)}(l)}|f_{J^{(i)}(l')}\rangle = \delta_{ll'},
\end{aligned}$$

holds. Therefore, we have $\sum_{i=1}^{d} {M_i^{(J)}}^{\dagger} M_i^{(J)} = \mathbb{I}$. ■

Consequently, by using our proposal method, Alice can solve Mean King's problem which consists of sets of measurement operators $M^{(J)}$ for the 1 dimensional quantum code spanned by the maximal entangled state.

7.6 An Example: A Construction from Computational Bases

We show an example of measurement operators constructed from the computational base by using the above construction method. Let $\{|i\rangle\}_{i=0}^{d-1}$ be the computational bases of d dimensional Hilbert space $\mathcal{H}_K \simeq \mathbb{C}^d$, i.e., $i+1$th element of $|i\rangle$ is equals to 1 and the others are equal to 0 for any i. Define a d^2-tuple of Kraus operators $(L_{ij} = (L_{kl}^{(ij)})_{0\le k,l\le d-1})_{i,j=0}^{d-1}$ by $(\mathbb{I} \otimes d L_{ij})|\Psi\rangle = |i\rangle \otimes |j\rangle$. Remark that $L_{kl}^{(ij)} = 1/\sqrt{d}\delta_{(k,l),(i,j)}$ holds. we show three kinds of sets of measurement operators constructed from Kraus operators $(L_{ij})_{i,j}$ as an instance in 3 dimensional case:

$$M_1^{(0)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, M_2^{(0)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$
$$M_3^{(0)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

$$M_1^{(1)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, M_2^{(1)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$
$$M_3^{(1)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$M_1^{(2)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, M_2^{(2)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
$$M_3^{(2)} = \frac{1}{\sqrt{3}} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Table 7.2 denotes index sets related with the relationship between the measurement operators and Kraus operators.

Table 7.2: The relationship between measurement operators and index sets

J	i	$X^{(J,i)}$
0	1	$(1,1),(1,2),(1,3)$
0	2	$(2,1),(2,2),(2,3)$
0	3	$(3,1),(3,2),(3,3)$
1	1	$(1,1),(2,2),(3,3)$
1	2	$(1,2),(2,3),(3,1)$
1	3	$(1,3),(2,1),(3,2)$
2	1	$(1,1),(2,3),(3,2)$
2	2	$(1,2),(2,1),(3,3)$
2	3	$(1,3),(2,2),(3,1)$

7.7 Higher Dimensional Quantum Codes for Bipartite System

We show a setting of Mean King's problem which is solved by using 3 dimensional quantum error-correcting code toward higher dimensional quantum codes. First, we construct a Mean King's problem which consists of two projective measurements in 2 dimensional Hilbert space, then, our proposal solution of the problem is a 1 dimensional quantum code spanned by the Bell state. Let $\mathcal{H}_A, \mathcal{H}_K$ be 2 dimensional Hilbert spaces. Define Kraus operators $(\hat{L}_i)_{i=1}^4$ with $\sum_{i=1}^4 \hat{L}^\dagger \hat{L}_i = \mathbb{I}$ as

$$\begin{aligned}\hat{L}_1 &:= X_0 Z_0, \quad \hat{L}_2 := X_1 Z_0,\\ \hat{L}_3 &:= X_0 Z_1, \quad \hat{L}_4 := X_1 Z_1,\end{aligned}$$

where $X_0 := |+\rangle\langle+|, X_1 := |-\rangle\langle-|, Z_0 := |0\rangle\langle 0|$, and $Z_1 := |1\rangle\langle 1|$. For projective measurements $\hat{M}^{(1)} := (X_0, X_1), \hat{M}^{(2)} := (Z_0, Z_1)$, and the Bell state $|\Psi^+\rangle$,

$$\begin{aligned}X_0 &= \hat{L}_1 + \hat{L}_3, \quad X_1 = \hat{L}_2 + \hat{L}_4,\\ Z_0 &= \hat{L}_1 + \hat{L}_2, \quad Z_1 = \hat{L}_3 + \hat{L}_4,\end{aligned}$$

and

$$\langle(\mathbb{I}_A \otimes \hat{L}_k)\Psi^+|(\mathbb{I}_A \otimes \hat{L}_{k'})\Psi^+\rangle = \frac{1}{4}\delta_{kk'},$$

hold, where we used a property $(\mathbb{I} \otimes Z_i)|\Psi^+\rangle = (Z_i \otimes \mathbb{I})|\Psi^+\rangle$. Therefore all the conditions of Theorem 18 are satisfied for Kraus operators $(\hat{L}_i)_i$

with respect to King's measurement $\hat{M}^{(1)}, \hat{M}^{(2)}$ and a $[4,1]$ quantum code spanned by $|\Psi^+\rangle$.

Lastly, we construct a Mean King's problem from the above discussion, then, our solution of the problem is 3 dimensional quantum code. Let $\mathcal{H}_A, \mathcal{H}_K$ be 3 dimensional Hilbert spaces and $\{|i\rangle\}_{i=0}^2$ the computational base of $\mathcal{H}_A$ and $\mathcal{H}_K$. Define

$$\tilde{X_0} := \begin{pmatrix} \multicolumn{2}{c}{\multirow{2}{*}{X_0}} & 0 \\ & & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \tilde{X_1} := \begin{pmatrix} \multicolumn{2}{c}{\multirow{2}{*}{X_1}} & 0 \\ & & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

$$\tilde{Z_0} := \begin{pmatrix} \multicolumn{2}{c}{\multirow{2}{*}{Z_0}} & 0 \\ & & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \tilde{Z_1} := \begin{pmatrix} \multicolumn{2}{c}{\multirow{2}{*}{Z_1}} & 0 \\ & & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Define Kraus operators $\tilde{L}_1 := \tilde{X_0}\tilde{Z}_0, \tilde{L}_2 := \tilde{X_1}\tilde{Z}_0, \tilde{L}_3 := \tilde{X_0}\tilde{Z}_1, \tilde{L}_4 := \tilde{X_1}\tilde{Z}_1, \tilde{L}_5 := |2\rangle\langle 2|$, then $\sum_i \tilde{L}_i^\dagger \tilde{L}_i = \mathbb{I}$ holds. Define measurement operators $\tilde{M}^{(J)} := (\tilde{M}_1^{(J)}, \tilde{M}_2^{(J)})$ $(J = 1,2)$ as

$$\begin{aligned}
\tilde{M}_1^{(1)} &:= \tilde{L}_1 + \tilde{L}_2 = |0\rangle\langle 0|, \\
\tilde{M}_2^{(1)} &:= \tilde{L}_3 + \tilde{L}_4 + \tilde{L}_5 = |1\rangle\langle 1| + |2\rangle\langle 2|, \\
\tilde{M}_1^{(2)} &:= \tilde{L}_1 + \tilde{L}_2 + \tilde{L}_5 = |0\rangle\langle 0| + |2\rangle\langle 2|, \\
\tilde{M}_2^{(2)} &:= \tilde{L}_3 + \tilde{L}_4 = |1\rangle\langle 1|,
\end{aligned}$$

and a $[9,3]$ quantum code $\tilde{C}$ spanned by

$$\{|i\rangle \otimes (|0\rangle + |2\rangle) \mid i \in \{0,1,2\}\} \subset \mathcal{H}_A \otimes \mathcal{H}_K,$$

then,

$$\langle i|(\langle 0| + \langle 2|)(\mathbb{I} \otimes \tilde{L}_k)^\dagger (\mathbb{I} \otimes \tilde{L}_{k'})|j\rangle(|0\rangle + |2\rangle) = \lambda_{ijkk'}\delta_{kk'}\delta_{ij},$$

holds for some $\lambda_{ijkk'} \in \mathbb{C}$. All the conditions of the Theorem 18 hold for $(\tilde{L}_i)_i$ and $\tilde{C}$. Therefore, by using our proposal method, Alice can solve Mean King's problem which consists of measurement operators performed by King $\tilde{M}^{(1)}$ and $\tilde{M}^{(2)}$ for any initial state in the $[9,3]$ quantum code $\tilde{C}$.

7.8 Higher Dimensional Quantum Codes for Composite System

Let us consider that Alice prepares not bipartite system but composite system consisted from qubit systems, i.e., she can prepare and keep many qubit systems secretly. Define $|\bar{0}\rangle := |1\rangle, |\bar{1}\rangle := |0\rangle$. We call

$$\frac{1}{\sqrt{2}}(|i_1 i_2 \cdots i_n\rangle + |\bar{i_1}\bar{i_2}\cdots\bar{i_n}\rangle) \in \mathbb{C}^{\otimes n},$$

Greenberg-Horne-Zeilinger (GHZ) state [99], where $n \geq 3$ and $i_l \in \{0, 1\}$ for any l. Note that the states are equal to the Bell states if we permit $n = 2$. Alice prepares a GHZ state gives jth qubit system to Bob. Then, the remnants are kept by Alice in secret. Let

$$\hat{Z}^j = (Z_0^j := |0\rangle\langle 0|, Z_1^j := |1\rangle\langle 1|),$$

$$\hat{X}^j = (X_0^j := |+\rangle\langle +|, X_1^j := |-\rangle\langle -|),$$

be projective measurements employed by King [2] on jth qubit system. We show that we can construct higher dimensional quantum error-correcting code, which is a solution of Mean King's problem with the above setting, constructed from GHZ states against error constructed from the measurements employed by King.

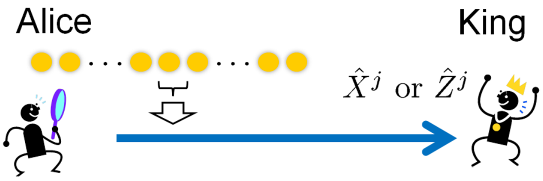

Figure 7.5: Preparing a GHZ state and sending one qubit system

Define $L^j := \{X_a^j Z_b^j\}_{a,b}$. Then, $\sum_{a,b} (X_a^j Z_b^j)^\dagger X_a^j Z_b^j = \mathbb{I}_j$ holds. Furthermore, we obtain

$$X_0^j = X_0^j Z_0^j + X_0^j Z_1^j, \quad X_1^j = X_1^j Z_0^j + X_1^j Z_1^j,$$

$$Z_0^j = X_0^j Z_0^j + X_1^j Z_0^j, \quad Z_1^j = X_0^j Z_1^j + X_1^j Z_1^j.$$

Therefore, conditions (7.1) and (7.2) of Theorem 18 hold for $\hat{Z}^j, \hat{X}^j$, and L^j.

Let $|\psi\rangle$ be a GHZ states on $\mathbb{C}^{\otimes n}$. We use a short notation:

$$Z_a^j \leftrightarrow \mathbb{I}_1 \otimes \cdots \otimes \mathbb{I}_{j-1} \otimes Z_a^j \otimes \mathbb{I}_{j+1} \otimes \cdots \otimes \mathbb{I}_n,$$

$$X_a^j \leftrightarrow \mathbb{I}_1 \otimes \cdots \otimes \mathbb{I}_{j-1} \otimes X_a^j \otimes \mathbb{I}_{j+1} \otimes \cdots \otimes \mathbb{I}_n,$$

for any j and a. Using the following equations $Z_a^j|\psi\rangle = Z_a^k|\psi\rangle$ and $X_{a'}^j Z_a^k = Z_a^k X_{a'}^j$ for any a, a' and $j \neq k$, we obtain

$$\begin{aligned} \langle\psi|Z_{b_1}^j X_{a_1}^j X_{a_2}^j Z_{b_2}^j|\psi\rangle &= \langle\psi|Z_{b_1}^k Z_{b_2}^k X_{a_1}^j X_{a_2}^j|\psi\rangle \\ &= \delta_{a_1 a_2}\delta_{b_1 b_2}\langle\psi|Z_{b_1}^j X_{a_1}^j|\psi\rangle. \end{aligned}$$

[2] Z_0^j and Z_1^j are projections corresponding to a Pauli matrix σ_z. X_0^j and X_1^j are projections corresponding to a Pauli matrix σ_x.

We try to find GHZ state $|\phi\rangle \neq |\psi\rangle$ such that

$$\langle\psi|Z^j_{b_1}X^j_{a_1}X^j_{a_2}Z^j_{b_2}|\phi\rangle = 0, \tag{7.15}$$

holds. From the above discussion, we obtain the following the equation:

$$\langle\psi|Z^j_{b_1}X^j_{a_1}X^j_{a_2}Z^j_{b_2}|\phi\rangle = \delta_{a_1a_1}\lambda_{b_1b_2}\langle\psi|Z^j_{b_1}X^j_{a_1}|\phi\rangle,$$

where $\lambda_{b_1b_2} = \delta_{b_1b_2}, \delta_{\bar{b}_1b_2}$, or $\delta_{b_1\bar{b}_2}$ holds according to jth and kth states. We show that there exist GHZ states such that eq.(7.15) holds by observing the following forms:

$$\begin{aligned} Z^j_{b_1}|\psi\rangle &= \frac{1}{\sqrt{2}}(|i_1i_2\cdots i_{j-1}\rangle Z^j_{b_1}|i_j\rangle|i_{j+1}\cdots i_n\rangle \\ &\quad +|\bar{i}_1\bar{i}_2\cdots \bar{i}_{j-1}\rangle Z^j_{b_1}|\bar{i}_j\rangle|\bar{i}_{j+1}\cdots \bar{i}_n\rangle), \end{aligned} \tag{7.16}$$

and

$$\begin{aligned} X^j_{a_1}|\phi\rangle &= \frac{1}{\sqrt{2}}(|l_1l_2\cdots l_{j-1}\rangle X^j_{a_1}|l_j\rangle|l_{j+1}\cdots l_n\rangle \\ &\quad +|\bar{l}_1\bar{l}_2\cdots \bar{l}_{j-1}\rangle X^j_{a_1}|\bar{l}_j\rangle|\bar{l}_{j+1}\cdots \bar{l}_n\rangle). \end{aligned} \tag{7.17}$$

Indeed, eq.(7.15) holds if there exist uth qubit states of eq.(7.16) and eq.(7.17) such that $\langle i_u|l_u\rangle = 0$ holds. Define a subset of GHZ states $\Theta := \{|\phi\rangle \mid \langle\psi|Z^j_{b_1}X^j_{a_1}X^j_{a_2}Z^j_{b_2}|\phi\rangle = 0, \forall a_1, a_2, b_1, b_2\}$ and $C :=$ span$(\{|\psi\rangle \cup \Theta\}$. Note that the number of elements of C is equal to 2^{n-2}. Let E be the projection from $\mathbb{C}^{\otimes n}$ into C. Then, condition (7.3) of Theorem 18 holds since

$$EZ^j_{b_1}X^j_{a_1}X^j_{a_2}Z^j_{b_2}E = \lambda_{a_1b_1}\delta_{a_1a_2}\delta_{b_1b_2}E,$$

holds. Therefore, Alice can estimate King's outcome with probability 1 by using any state of C and C is a $[2^n, 2^{n-2}]$ quantum error-correcting code against spanL^j.

Chapter 8

Re-formulation of the Problem Using Entropy

8.1 Re-formulation of the Problem

We reformulate the general Mean King' problem introduced in Sec.7.1. In the setting, with given $d(=\dim\mathcal{H}_K)$ and measurements $M^{(k)} = (M_j^{(k)})_{j=0}^{m}(k = 0, 1, \ldots, m')$ [1], we say that a solution to 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 and chooses an appropriate entangled state on the bipartite system. In step 3, she performs a POVM measurement $P = (P_i)_{i=0}^{n}$ on the bipartite system. In this section, we reformulate the problem using conditional Shannon entropy.

Let K, J, and 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 P, respectively. Then, we can reformulate Mean King's problem using the conditional entropy as follows:

Find an initial state ρ and a measurement P such that

$$H(J \mid I, K) = 0, \tag{8.1}$$

where $H(\cdot \mid \cdot)$ denotes conditional Shannon entropy.

Note that $H(J \mid I)$ is generally strictly positive, otherwise Alice can guess King's outcome without a delayed information K. By the chain rule of the conditional entropy, eq.(8.1) is equivalent to the following relation:

$$H(K, J \mid I) = H(K \mid I), \tag{8.2}$$

[1] Note that this notation is slightly different for indexes in Sec.7.1: $J \leftrightarrow k$.

Let $P_{K,J,I}(k,j,i)$ be a joint probability of K,J,I, and let $P_{K,I}(k,i) = \sum_j P_{K,J,I}(k,j,i)$ be the marginal joint probability of K and I. We find that eq.(8.2) holds if and only if

$$P_{K,J,I}(k,j,i) = 0 \quad \text{or} \quad P_{K,J,I}(k,j,i) = P_{K,I}(k,i), \tag{8.3}$$

holds for each k,j, and i. Indeed, by the definition of conditional entropy, we can rewrite eq.(8.2) as follow:

$$-\sum_{k,j,i} P_{K,J,I}(k,j,i) \log P_{K,J,I}(k,j \mid i) = -\sum_{k,i} P_{K,I}(k,i) \log P_{K,I}(k \mid i), \tag{8.4}$$

where $P(\cdot \mid \cdot)$ denotes a conditional probability corresponding to the random variables. If $P_I(i)(= \sum_{k,j} P_{K,J,I}(k,j,i)) \neq 0$ holds, using the monotonically increasing property $\log P_{K,J,I}(k,j,i) \leq \log P_{K,I}(k,i)$, eq.(8.4) holds if and only if

$$P_{K,J,I}(k,j,i) \log P_{K,J,I}(k,j,i) = P_{K,J,I}(k,j,i) \log P_{K,I}(k,i), \tag{8.5}$$

holds for any k,j, and i. Nothing that $P_I(i) = 0$ holds if and only if $P_{K,J,I}(k,j,i) = 0$ for any k and j, eq.(8.4) holds if and only if eq.(8.5) holds also in this case. Therefore, we have obtained the equivalence between eq.(8.2) and eq.(8.3). In our setting, a solution to Mean King's problem is to find an initial state ρ and a measurement P such that condition eq.(8.1), eq.(8.2), or eq.(8.3) holds.

8.2 An Application: Nonexistence of Solutions in Qubit Setting

In this section, we give an alternate proof [2] 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 $\mathbb{C}^2$. King employs one of three projective measurements,

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

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

$$P_{K,J,I}(k,j,i) = P_K(k)\langle\psi_j^k|\rho|\psi_j^k\rangle\langle\psi_j^k|P_i|\psi_j^k\rangle, \tag{8.6}$$

[2] The previous proofs are shown in Ref.[92, 93].

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 A, B, and C of the joint probabilities satisfying eq.(8.6) 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 $P_{K,J,I}(k, j', i) \neq 0$ hold for $i \neq i'$ and $j \neq j'$.

In Figure 8.1, we show a complete classification of probability for each type, where the number of kinds of the probabilities type A, B, and C is 8. Now, we try to find ρ and P such that each three joint probabilities for $k = 0, 1, 2$ satisfies any of the above 8 kinds of the probabilities.

By using eq.(8.6), we obtain the equivalent relations for each type and the joint probability $P_{K,J,I}(k, j, i)$ as follows:

- The joint probability satisfies **type A** if and only if
  $(\rho = M_0^{(k)}, P_0 = M_0^{(k)}, P_1 = M_1^{(k)})$ or
  $(\rho = M_0^{(k)}, P_0 = M_1^{(k)}, P_1 = M_0^{(k)})$ or
  $(\rho = M_1^{(k)}, P_0 = M_0^{(k)}, P_1 = M_1^{(k)})$ or
  $(\rho = M_1^{(k)}, P_0 = M_1^{(k)}, P_1 = M_0^{(k)})$.

- The joint probability satisfies **type B** if and only if
  $(\rho = M_0^{(k)}, P_0 \neq M_0^{(k)}, M_1^{(k)}, P_1 \neq M_0^{(k)}, M_1^{(k)})$ or
  $(\rho = M_1^{(k)}, P_0 \neq M_0^{(k)}, M_1^{(k)}, P_1 \neq M_0^{(k)}, M_1^{(k)})$.

- The joint probability satisfies **type C** if and only if
  $(\rho \neq M_0^{(k)}, M_1^{(k)}, P_0 = M_0^{(k)}, P_1 = M_1^{(k)})$ or
  $(\rho \neq M_0^{(k)}, M_1^{(k)}, P_0 = M_1^{(k)}, P_1 = M_0^{(k)})$.

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) [3] . This fact is also derived from construction of P_0 and P_1. In a similar way, we cannot construct the probability satisfying any of pairs of types (type B, type B), (type C, type C), (type A, type B), (type B, type

[3] $P_{K,J,I}(k, j, i)$ satisfies type A and $P_{K,J,I}(k, j, i)$ satisfies type A, then, we use a notation (type A, type A).

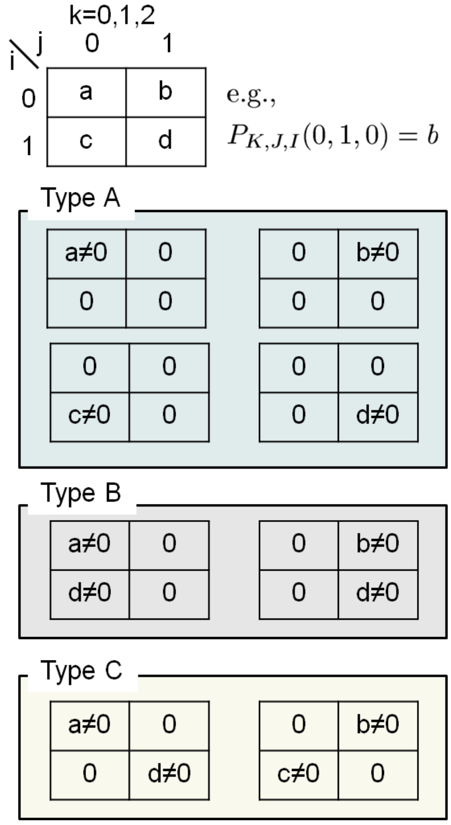

Figure 8.1: A classification of probability for each type

A), (type C, type A), and (type A, type C). On the other hand, there are ρ and P such that the probabilities satisfy any of pairs of (type B, type C) and (type C, type B). For instance, $(\rho = M_0^{(k)}, P_0 = M_0^{(k')}, P_1 = M_1^{(k')})$ satisfies (type B, type C). According to the above fact, we obtain $H(J \mid I, K) = 0$ 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) [4] 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 P. Thus, we can conclude that $H(J \mid I, K) = 0$ dose not hold for three kinds of the measurements.

[4] $P_{K,J,I}(0, j, i), P_{K,J,I}(1, j, i)$, and $P_{K,J,I}(2, j, i)$ satisfy type B, type C, and type B, respectively. Then, we use a notation (type B, type C, type B).

Chapter 9

Security Analysis of Quantum Key Distribution

9.1 Modified Measurement Schemes

In Mean King's problem introduced in Sec.6.1, King measures the system with one of the observables $\hat{X}, \hat{Y}$, and $\hat{Z}$, and Alice measures the bipartite system with $\hat{R}$. On the other hand, in the quantum key distribution protocol using Mean King's problem proposed by Bub, King uses only $\hat{X}$ and $\hat{Z}$, while Alice measures $\hat{R}$. It should be noted that $\hat{R}$ is not a unique solution for Mean King's problem for these two observables. In addition, it is difficult to realize the measurement of $\hat{R}$, as it has projections on to the entangled bases $|r_j\rangle$ $(j = 1, 2, 3, 4)$ [1]. In the following, by using the solution introduced in Section 7.2, we show three observables employed by Alice that also solve Mean King's problem for $\hat{X}$ and $\hat{Z}$. These observables are rather simple compared with $\hat{R}$. We apply them to the quantum key distribution and study their security.

Measurement $\hat{M}$

Define a family of operators $\{E_k\}_k$ on $\mathcal{H}_K$ by $E_1 := X_0Z_0, E_2 := X_0Z_1, E_3 := X_1Z_0$, and $E_4 := X_1Z_1$. This family satisfies $\sum_k E_k^\dagger E_k = \mathbb{I}$ and is called Kraus operators. Remark that

$$\begin{aligned} &\langle\Psi^+|(\mathbb{I}\otimes E_k)^\dagger(\mathbb{I}\otimes E_k')|\Psi^+\rangle = \frac{1}{4}\delta_{kk'}, \qquad (9.1)\\ &X_0 = E_1 + E_2, \quad X_1 = E_3 + E_4,\\ &Z_0 = E_1 + E_3, \quad Z_1 = E_2 + E_4, \end{aligned}$$

hold for the Bell state as an initial state $|\Psi^+\rangle$ and King's measurements $\hat{X}, \hat{Z}$, where we used a property $(\mathbb{I}\otimes X_iZ_j)|\Psi^+\rangle = (Z_j \otimes X_i)|\Psi^+\rangle$. If King measures the system $\mathcal{H}_K$ with $\hat{X}$, a post measurement state is proportional

[1] See in Sec.6.1.

to

$$(\mathbb{I}\otimes X_0)|\Psi^+\rangle \in K_1 \oplus K_2,\ \ (\mathbb{I}\otimes X_1)|\Psi^+\rangle \in K_3 \oplus K_4, \tag{9.2}$$

in accordance with an outcome 0 or 1, where K_k is defined as a subspace spanned by $(\mathbb{I}\otimes E_k)|\Psi^+\rangle$. Note that K_k are orthogonal to $K_{k'}$ on $\{|\Psi^+\rangle\}$ for any $k \neq k'$ owing to eq.(9.1). Similarly, if he chooses $\hat{Z}$, a post measurement state is proportional to

$$(\mathbb{I}\otimes Z_0)|\Psi^+\rangle \in K_1 \oplus K_3,\ \ (\mathbb{I}\otimes Z_1)|\Psi^+\rangle \in K_2 \oplus K_4. \tag{9.3}$$

The projection operator M_k onto K_k for each k is defined by

$$M_1 := Z_0 \otimes X_0,\ \ M_2 := Z_1 \otimes X_0,$$

$$M_3 := Z_0 \otimes X_1,\ \ M_4 := Z_1 \otimes X_1.$$

These operator define a PVM $\hat{M} := (M_k)_{k=1}^4$ on $\mathcal{H}_A \otimes \mathcal{H}_K$. Alice measures the post measurement state with $\hat{M}$ and obtains an outcome $k \in \{1,2,3,4\}$. She can estimate King's outcome by using the relationship (see Table 9.1) between King's observables and her outcome obtained from eq.(9.2) and (9.3), e.g., if King chooses $\hat{X}$ and Alice obtains an outcome 2, she estimates King's outcome as 0.

Note that this observable $\hat{M}$ does not contain any entangled PVM element and is much simpler than $\hat{R}$.

Measurement $\hat{N}$

Define Kraus operators $\{E'_k\}_k$ as $E'_1 := Z_0X_0, E'_2 := Z_1X_0, E'_3 := Z_0X_1$, and $E'_4 := Z_1X_1$. We obtain a PVM measurement $\hat{N} = (N_k)_{k=1}^4$ on $\mathcal{H}_A \otimes \mathcal{H}_K$ in a similar way:

$$N_1 := X_0 \otimes Z_0,\ \ N_1 := X_0 \otimes Z_1,$$

$$N_3 := X_1 \otimes Z_0,\ \ N_4 := X_1 \otimes Z_1.$$

Note that Table 9.2 denotes the relationship between King's observables and $\hat{N}$.

Measurement $\hat{L}$

Lastly, we define a POVM $\hat{L} := (L_k)_{k=1}^4$ on $\mathcal{H}_A \otimes \mathcal{H}_K$ by

$$L_1 := \frac{1}{2}(Z_0 \otimes X_0 + X_0 \otimes Z_0),\ \ L_2 := \frac{1}{2}(Z_1 \otimes X_0 + X_0 \otimes Z_1),$$

$$L_3 := \frac{1}{2}(Z_0 \otimes X_1 + X_1 \otimes Z_0),\ \ L_2 := \frac{1}{2}(Z_1 \otimes X_1 + X_1 \otimes Z_1).$$

In Table 9.3, the relationship between King's observables and $\hat{L}$ is denoted. While this POVM seems complicated than $\hat{M}$ and $\hat{N}$, it can be realized by probabilistically choosing $\hat{M}$ and $\hat{N}$ and is simple as well.

Table 9.1: The relationship between King's observables and $\hat{M}$

	M_1	M_2	M_3	M_4
$\hat{X}$	0	0	1	1
$\hat{Z}$	0	1	0	1

Table 9.2: The relationship between King's observables and $\hat{N}$

	N_1	N_2	N_3	N_4
$\hat{X}$	0	0	1	1
$\hat{Z}$	0	1	0	1

Table 9.3: The relationship between King's observables and $\hat{L}$

	L_1	L_2	L_3	L_4
$\hat{X}$	0	0	1	1
$\hat{Z}$	0	1	0	1

9.2 Setting of Attack Models

We study security of the quantum key distribution protocol with modified measurement schemes. We introduce three attack models.

We call a quantum channel from Alice to King AK-channel and a quantum channel from King to Alice KA-channel. An eavesdropper Eve attacks a qubit with unlimited quantum resource on the quantum channels. A purpose of Eve's attack is to obtain information of the secret key without being detected by Alice and King. Eve can use all the public classical information.

- **Attack model 1**:
  Eve attacks only KA-channel.

- **Attack model 2**:
  Eve attacks only AK-channel.

- **Attack Model 3**:
  There are two eavesdroppers Eve1 and Eve2 who do not communicate with each other. Eve1 attacks only AK-channel and Eve2 attacks only KA-channel.

Note that model 3 is the strongest in such a sense that this model can be reduced to the other models if one of the eavesdroppers does nothing.

We first consider model 1 and show that the protocols using $\hat{M}$ and $\hat{N}$ are insecure even against this weak attack. Then we introduce our previous result on the protocol using $\hat{R}$ in the model 2. Model 3 is considered with respect to the modified protocol with $\hat{L}$. By showing a nontrivial information-disturbance trade-off inequality, we conclude that only this protocol could be secure in the models introduced above.

Before we consider security of the protocol, we define the following conditional probabilities. Let ρ_k be a state of the bipartite system after King measures $\mathcal{H}_K$ with $\hat{B} \in \{\hat{X}, \hat{Z}\}$ and obtains an outcome k.

$$\mathrm{P}(\hat{A} = i \vee \hat{A} = j \mid \hat{B} = k) := \mathrm{tr}\, \rho_k A_i + \mathrm{tr}\, \rho_k A_j,$$

denotes a probability that Alice measures $\mathcal{H}_A \otimes \mathcal{H}_K$ in the post measurement state ρ_k with $\hat{A} = \{A_i\}_i \in \{\hat{R}, \hat{M}, \hat{N}, \hat{L}\}$ and obtains i or j. We define an error probability which means that Alice dose not estimate King's outcome perfectly, e.g.,

$$\mathrm{P}(\mathrm{error}_{\hat{M}} \mid \hat{Z} = 0) := 1 - \mathrm{P}(\hat{M} = 1 \vee \hat{M} = 3 \mid \hat{Z} = 0).$$

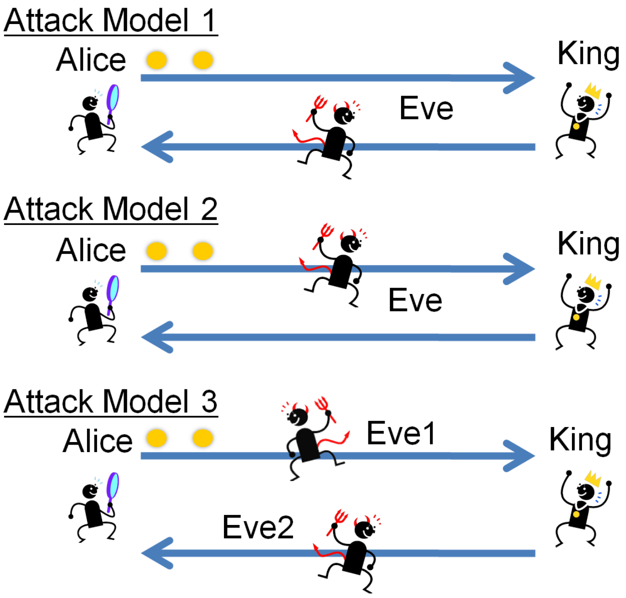

Figure 9.1: Three attack models

9.3 Security Analysis for Attack Model 1

9.3.1 Measurements $\hat{M}$ and $\hat{N}$

In the attack model 1, Eve makes the system $\mathcal{H}_K$ interact with her own system $\mathcal{H}_E$ on KA-channel. King measures $\mathcal{H}_K$ which is not performed the attack by Eve with one of projective measurements. The post measurement state on $\mathcal{H}_K$ is $|i\rangle\langle i|$ or $|\bar{j}\rangle\langle\bar{j}|$ according to King's projective measurement. Eve prepares a system $\mathcal{H}_E$ in a state σ_0 and performs unitary evolution

W_{KE} on $\mathcal{H}_K \otimes \mathcal{H}_E$. We denote by Λ a completely-positive map (CP map) [2] describing the general attack. Then it can be written

$$\Lambda^*(|i\rangle\langle i|) := W_{KE}(|i\rangle\langle i| \otimes \sigma_0)W_{KE}^\dagger,$$

$$\Lambda^*(|\bar{j}\rangle\langle\bar{j}|) := W_{KE}(|\bar{j}\rangle\langle\bar{j}| \otimes \sigma_0)W_{KE}^\dagger.$$

Define

$$\Lambda_K^*(\rho) := \mathrm{tr}_E(\Lambda^*(\rho)),$$

$$\Lambda_E^*(\rho) := \mathrm{tr}_K(\Lambda^*(\rho)),$$

for any state ρ with partial trace restricted by $\mathcal{H}_E$ and $\mathcal{H}_K$ respectively. Remark that Eve has the state $\Lambda_E^*(|i\rangle\langle i|)$ or $\Lambda_E^*(|\bar{j}\rangle\langle\bar{j}|)$ on $\mathcal{H}_E$ and sends Alice one of two states

$$\rho_i' := \Lambda_K^*(|i\rangle\langle i|),$$

$$\rho_{\bar{j}}' := \Lambda_K^*(|\bar{j}\rangle\langle\bar{j}|),$$

on $\mathcal{H}_K$. Alice takes the bipartite system $\mathcal{H}_A \otimes \mathcal{H}_K$ in the state $|i\rangle\langle i| \otimes \rho_i'$ or $|\bar{j}\rangle\langle\bar{j}| \otimes \rho_{\bar{j}}'$.

Suppose that Alice measures the system with measurement $\hat{M}$. The state of $\mathcal{H}_A \otimes \mathcal{H}_K$ is $|i\rangle\langle i| \otimes \rho_i'$ if King chooses $\hat{Z}$ and obtains an outcome i, then, probability that Alice estimates the outcome correctly are

$$\mathrm{P}(\hat{M} = 1 \vee \hat{M} = 3 \mid \hat{Z} = 0) = \mathrm{tr}(|0\rangle\langle 0| \otimes \rho_0'(M_1 + M_3)) = 1,$$

and

$$\mathrm{P}(\hat{M} = 2 \vee \hat{M} = 4 \mid \hat{Z} = 1) = \mathrm{tr}(|1\rangle\langle 1| \otimes \rho_1'(M_2 + M_4)) = 1.$$

Therefore, even if Eve gains information of a secret key generated by $\hat{X}$, the error probability of the secret keys generated by $\hat{Z}$ is zero, i.e., she is not detected.

Let us consider that Alice employs $\hat{N}$. The state of $\mathcal{H}_A \otimes \mathcal{H}_K$ is $|\bar{j}\rangle\langle\bar{j}| \otimes \rho_{\bar{j}}'$ if King chooses $\hat{X}$ and obtains j, then, the probabilities are

$$\mathrm{P}(\hat{N} = 1 \vee \hat{N} = 2 \mid \hat{X} = 0) = \mathrm{tr}(|\bar{0}\rangle\langle\bar{0}| \otimes \rho_{\bar{0}}'(N_1 + N_2)) = 1,$$

and

$$\mathrm{P}(\hat{N} = 3 \vee \hat{N} = 4 \mid \hat{X} = 1) = \mathrm{tr}(|\bar{1}\rangle\langle\bar{1}| \otimes \rho_{\bar{1}}'(M_3 + M_4)) = 1.$$

Therefore, even if Eve gains information of a secret key generated by $\hat{Z}$, the error probability of the secret keys generated by $\hat{X}$ is zero.

Consequently, Eve gains information of the secret keys without being detected if $\hat{M}$ or $\hat{N}$ is applied to the protocol.

[2] Remind that a CP map $\Lambda : \mathcal{S}(\mathcal{H}_1) \to \mathcal{S}(\mathcal{H}_2)$ takes two property: completeness and positivity. For more details in Sec.3.2.

9.3.2 Measurements $\hat{L}$ and $\hat{R}$

Firstly, we suppose that $\hat{L}$ is applied to the protocol. We have probabilities of estimating King's outcome perfectly on condition that King chooses $\hat{Z}$:

$$\begin{aligned}\mathrm{P}(\hat{L}=1 \vee \hat{L}=3 \mid \hat{Z}=0) &= \frac{1}{2}(1+\langle 0|\rho'_0|0\rangle),\\ \mathrm{P}(\hat{L}=2 \vee \hat{L}=4 \mid \hat{Z}=1) &= \frac{1}{2}(1+\langle 1|\rho'_1|1\rangle).\end{aligned}$$

An error probability of the sifted key generated by the measurement $\hat{Z}$ is

$$\mathrm{P}(\mathrm{error}_{\hat{L}} \mid \hat{Z}=i) = \frac{1}{2}(1-\langle i|\rho'_i|i\rangle). \tag{9.4}$$

We estimate Eve's information gain by using the relationship between trace norm and fidelity.

Definition 23 *Trace norm is defined as*

$$\|\rho-\sigma\|_1 := \sup_{\|E\|_{op}=1} |\mathrm{tr}((\rho-\sigma)E)|,$$

for density operators ρ and σ, where $\|\cdot\|_{op}$ denotes operator norm [3]*.*

Remark that $0 \leq \|\rho-\sigma\|_1 \leq 1$ holds and $\|\rho-\sigma\|_1 = 0$ holds if $\rho=\sigma$. That is, the trace norm is regarded as distinguishability of two states.

Definition 24 *(Ref.[101, 102]). Fidelity is defined as*

$$F(\rho,\sigma) := \sqrt{\rho^{1/2}\sigma\rho^{1/2}},$$

for density operators ρ and σ.

Remark that $0 \leq F(\rho,\sigma) \leq 1$, and $F(\rho,\sigma)=1$ holds if and only if $\rho=\sigma$. Its value is a kind closeness of two state. The following equation related with the fidelity is introduced.

Lemma 25 *(Ref.[103, 104]).*

$$F(\rho,\sigma) = \inf_{\{E_\alpha\}_\alpha:\mathrm{POVM}} \sum_\alpha \sqrt{p_\rho(\alpha)p_\sigma(\alpha)}, \tag{9.5}$$

holds for density operator ρ and σ, where $p_\rho(\alpha) := \mathrm{tr}(E_\alpha\rho)$ and $p_\sigma(\alpha) := \mathrm{tr}(E_\alpha\sigma)$.

We obtain the following theorem.

[3] Define $\|A\|_{op} := \sup\{\|Ax\|/\|x\| \mid x \in \mathcal{H} \text{ s.t. } x \neq \mathbf{0}\}$ for $A : \mathcal{H} \to \mathcal{H}$.

Theorem 26 *If Alice employs the measurement $\hat{L}$,*

$$\|\Lambda_E^*(|+\rangle\langle+|) - \Lambda_E^*(|-\rangle\langle-|)\|_1 \leq 2\sqrt{2} \sum_{i\in\{0,1\}} \sqrt{\mathrm{P}(\mathrm{error}_{\hat{L}} \mid \hat{Z} = i)}, \qquad (9.6)$$

holds for the attack model 1.

The inequality shows that Eve cannot distinguish a secret key generated by $\hat{X}$ without increasing the error probability of the secret key generated by $\hat{Z}$.
Proof

We use the following inequality [105] to obtain a trade-off between Eve's distinguishability and the error probability:

$$\|\Lambda_E^*(|+\rangle\langle+|) - \Lambda_E^*(|-\rangle\langle-|)\|_1 \leq 2F(\Lambda_K^*(|0\rangle\langle 0|), \Lambda_K^*(|1\rangle\langle 1|)). \qquad (9.7)$$

For $\rho_0' = \Lambda_K^*(|0\rangle\langle 0|)$ and $\rho_1' = \Lambda_K^*(|1\rangle\langle 1|)$,

$$\begin{aligned} F(\rho_0', \rho_1') &= \inf_{\{E_\alpha\}_\alpha:\mathrm{POVM}} \sum_\alpha \sqrt{\mathrm{tr}(\rho_0' E_\alpha)\mathrm{tr}(\rho_1' E_\alpha)} \\ &\leq \sqrt{\mathrm{tr}(\rho_0'|0\rangle\langle 0|)\mathrm{tr}(\rho_1'|0\rangle\langle 0|)} + \sqrt{\mathrm{tr}(\rho_0'|1\rangle\langle 1|)\mathrm{tr}(\rho_1'|1\rangle\langle 1|)} \\ &= \sqrt{\langle 0|\rho_0'|0\rangle\langle 0|\rho_1'|0\rangle} + \sqrt{\langle 1|\rho_0'|1\rangle)\langle 1|\rho_1'|1\rangle} \\ &= \sqrt{\langle 0|\rho_0'|0\rangle(1 - \langle 1|\rho_1'|1\rangle)} + \sqrt{(1 - \langle 0|\rho_0'|0\rangle)\langle 1|\rho_1'|1\rangle} \\ &\leq \sqrt{2} \sum_{i\in\{0,1\}} \sqrt{\mathrm{P}(\mathrm{error}_{\hat{L}} \mid \hat{Z} = i)}, \qquad (9.8) \end{aligned}$$

holds, where we use $\langle i|\rho_i'|i\rangle = 2\mathrm{P}(\mathrm{error}_{\hat{L}} \mid \hat{Z} = i) - 1$ owing to eq.(9.4). Therefore, eq.(9.6) holds owing to eq.(9.7) and eq.(9.8). ■

Suppose that $\hat{L}$ is applied to the protocol. We have probabilities of estimating King's outcome perfectly on condition that King chooses $\hat{Z}$:

$$\mathrm{P}(\hat{R} = 1 \vee \hat{R} = 2 \mid \hat{Z} = 0) = \frac{1}{2}(1 + \langle 0|\rho_0'|0\rangle),$$
$$\mathrm{P}(\hat{R} = 3 \vee \hat{R} = 4 \mid \hat{Z} = 1) = \frac{1}{2}(1 + \langle 1|\rho_1'|1\rangle).$$

An error probability of the sifted key generated by the measurement $\hat{Z}$ is

$$\mathrm{P}(\mathrm{error}_{\hat{R}} \mid \hat{Z} = i) = \frac{1}{2}(1 - \langle i|\rho_i'|i\rangle). \qquad (9.9)$$

Eq.(9.4) is equal to eq.(9.9). Therefore, we obtain the following theorem by substituting eq.(9.9) to eq.(9.8).

Theorem 27 *If Alice employs the measurement $\hat{R}$,*

$$\|\Lambda_E^*(|+\rangle\langle+|) - \Lambda_E^*(|-\rangle\langle-|)\|_1 \leq 2\sqrt{2} \sum_{i\in\{0,1\}} \sqrt{\mathrm{P}(\mathrm{error}_{\hat{R}} \mid \hat{Z} = i)}, \qquad (9.10)$$

holds for the attack model 1.

9.4 Security Analysis for Attack Model 2

In this section, we analyze security of the protocol to applied $\hat{R}$ and $\hat{L}$ since the protocol to applied $\hat{M}$ and $\hat{N}$ is not secure against the attack model 1. Suppose that the measurement $\hat{R}$ is applied to the protocol. For the attack model 2, we obtain the following theorem.

Theorem 28 *If Alice employs the measurement $\hat{R}$,*

$$I(X;\tilde{X}_E) \leq \sum_{i\in\{0,1\}} P^i_{\hat{Z}} f(\mathrm{P}(\mathrm{error}_{\hat{R}} \mid \hat{Z}=i)),$$

holds, where $I(\cdot;\cdot)$ is mutual information, X denotes a random variable expressing the outcomes of $\hat{X}$, $\tilde{X}_E$ denotes a random variable expressing results of the attack, $P^i_{\hat{Z}}$ denotes a probability for King to obtain an outcome i with $\hat{Z}$, $\mathrm{P}(\mathrm{error}_{\hat{R}}|\hat{Z}=i)$ denotes an error probability of the secret keys generated by $\hat{Z}$, and $f(x) := -(1-2x)\log(1-2x) - 2x\log 2x$ for $0 \leq x \leq 1/2$.

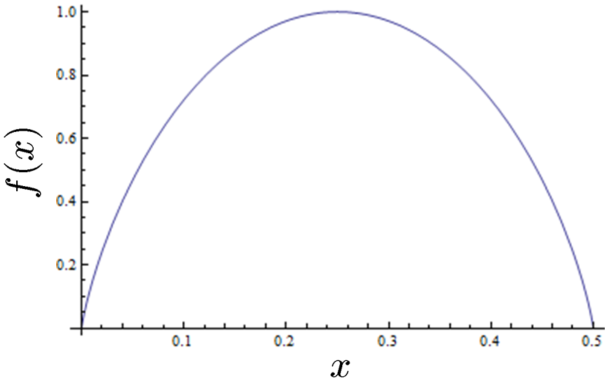

Figure 9.2: Function f defined in Theorem 28

The inequality shows that Eve cannot gain information of a secret key generated by $\hat{X}$ without increasing the error probability of the secret keys generated by $\hat{Z}$.

Proof

This proof is similar to a kind of security proofs of BB84 protocol. Let $\mathcal{H}_{E'}$ be an ancillary system prepared by Eve. Eve performs a quantum operation $V_{KE'}$ on bipartite system $\mathcal{H}_K \otimes \mathcal{H}_{E'}$:

$$\begin{aligned} V_{KE'} : \mathcal{H}_K \otimes \mathcal{H}_{E'} &\to \mathcal{H}_K \otimes \mathcal{H}_{E'} \\ |i\rangle \otimes |E_1\rangle &\mapsto \sum_j |E_{ij}\rangle \otimes |j\rangle, \end{aligned}$$

where $|E_1\rangle$ is a pure state which is prepared by Eve, and $|E_{ij}\rangle$ satisfies $\sum_j \langle E_{ij}|E_{kj}\rangle = \delta_{ik}$. Eve sends the system $\mathcal{H}_K$ to King after she operates on the bipartite system. A state on $\mathcal{H}_A \otimes \mathcal{H}_K \otimes \mathcal{H}_{E'}$ after Eve performs the operation is given by $|\Psi_{AKE'}\rangle := (\mathbb{I}_A \otimes V_{KE'})(|\Psi^+\rangle|E_1\rangle)$. Probability that King measures the system $\mathcal{H}_K$ with the measurement $\hat{Z}$ and obtains an outcome i is given by $P^i_{\hat{Z}} := \mathrm{tr}(\mathbb{I}_A \otimes Z_i \otimes \mathbb{I}_{E'} |\Psi_{AKE'}\rangle\langle\Psi_{AKE'}|)$. Then, a post measurement state of $\mathcal{H}_K$ is $|i\rangle\langle i|$, and let $\tilde{\rho}^i_{\hat{Z}}$ be a state of $\mathcal{H}_A$. King returns the system to $\mathcal{H}_K$ in the post measurement state to Alice. Probabilities that Alice estimates King's outcome with probability 1 by measuring the $\mathcal{H}_A \otimes \mathcal{H}_K$ in the state $\tilde{\rho}^i_{\hat{Z}} \otimes |i\rangle\langle i|$ with the measurement $\hat{R}$ are

$$\mathrm{P}(\hat{R} = 1 \vee \hat{R} = 2 \mid \hat{Z} = 0) = \frac{1}{2}(\langle 0|\tilde{\rho}^0_{\hat{Z}}|0\rangle + 1),$$

$$\mathrm{P}(\hat{R} = 3 \vee \hat{R} = 4 \mid \hat{Z} = 1) = \frac{1}{2}(\langle 1|\tilde{\rho}^1_{\hat{Z}}|1\rangle + 1).$$

Therefore, error probability is given by

$$\mathrm{P}(\mathrm{error}_{\hat{R}} \mid \hat{Z} = i) = \frac{1}{2}(1 - \langle i|\tilde{\rho}^i_{\hat{Z}}|i\rangle). \tag{9.11}$$

We consider a virtual setting which Eve (resp. Alice) measures the system $\mathcal{H}_{E'}$ (resp. $\mathcal{H}_A$) in the state $|\Psi_{AKE'}\rangle$ with an arbitrary (possibly optimal) POVM measurement. Let $\tilde{Z} = (\tilde{Z}_j)_j$ and $\tilde{X} = (\tilde{X}_\alpha)_\alpha$ be POVMs employed by Alice and Bob, respectively. Then, let $\rho_{j\alpha}$ be a post measurement state on $\mathcal{H}_K$ after Alice and Eve obtain outcomes j and α, respectively. Let $\hat{Z}(\rho_{j\alpha})$ (resp. $\hat{X}(\rho_{j\alpha})$) be a probability mass function of obtaining the outcomes with measurement $\hat{Z}$ (resp. $\hat{X}$) on the state $\rho_{j\alpha}$. By using entropic entropic uncertainty relation [106] for $\hat{Z}(\rho_{j\alpha})$ and $\hat{X}(\rho_{j\alpha})$,

$$H(\hat{Z}(\rho_{j\alpha})) + H(\hat{X}(\rho_{j\alpha})) \geq -2\log_e(\max_{i,j} \|Z_i^{1/2} X_j^{1/2}\|_{op}) = 1,$$

holds. We exchange notations and obtain the following inequality:

$$H(Z \mid \tilde{Z}_A, \tilde{X}_E) + H(X \mid \tilde{Z}_A, \tilde{X}_E) \geq 1$$

where $Z, X, \tilde{Z}_A$, and $\tilde{X}_E$ are random variables expressing outcomes of $\hat{Z}, \hat{X}, \tilde{Z}$, and $\tilde{X}$, respectively. By using a property of conditional entropy,

$$H(Z \mid \tilde{Z}_A) + H(X \mid \tilde{X}_E) \geq 1, \tag{9.12}$$

holds. Let us consider $\tilde{Z} = \hat{Z}$, then, joint probability that King obtains j by measuring the system with $\hat{Z}$ and King obtains l by measuring the system with $\tilde{Z}$ is given by $P_{\tilde{Z}_A Z}(j, l) = P_Z(l) P_{\tilde{Z}_A Z}(j \mid l) = P^l_{\hat{Z}} \langle j|\tilde{\rho}^l_{\hat{Z}}|j\rangle$, where $P(\cdot, \cdot), P(\cdot \mid \cdot)$, and $P(\cdot)$ are joint probability, conditional probability, and probability, respectively, corresponding to random variables. Then,

$$P_{\tilde{Z}_A Z}(j, l) = \langle\Psi_{AKE'}|(Z_j \otimes Z_l \otimes \mathbb{I}_{E'})|\Psi_{AKE'}\rangle,$$

holds. We obtain

$$\begin{aligned} P_{\tilde{Z}_A}(j) &= \sum_l P_{\tilde{Z}_A Z}(j,l) \\ &= \sum_l \langle \Psi_{AKE'}|(Z_j \otimes Z_l \otimes \mathbb{I}_{E'})|\Psi_{AKE'}\rangle \\ &= \langle \Psi_{AKE'}|(Z_j \otimes \mathbb{I}_K \otimes \mathbb{I}_{E'})|\Psi_{AKE'}\rangle = \frac{1}{2}, \end{aligned}$$

where we use a property of projections $\sum_l Z_l = \mathbb{I}$ and simple calculations [4]. Then,

$$P_{Z\tilde{Z}_A}(l \mid j) = \frac{P_{\tilde{Z}_A Z}(j \mid l)}{P_{\tilde{Z}_A}(j)} = 2P^l_{\hat{Z}}\langle j|\tilde{\rho}^l_{\hat{Z}}|j\rangle,$$

holds. Therefore, we obtain

$$\begin{aligned} H(Z \mid \tilde{Z}_A) &= \sum_j P_{Z\tilde{Z}_A}(l \mid j) H(Z \mid \tilde{Z}_A = j) \\ &= \sum_j \frac{1}{2} \sum_j -2P^l_{\hat{Z}}\langle j|\tilde{\rho}^l_{\hat{Z}}|j\rangle \log(2P^l_{\hat{Z}}\langle j|\tilde{\rho}^l_{\hat{Z}}|j\rangle) \\ &= -\sum_{j,l} P^l_{\hat{Z}}\langle j|\tilde{\rho}^l_{\hat{Z}}|j\rangle \log(2P^l_{\hat{Z}}\langle j|\tilde{\rho}^l_{\hat{Z}}|j\rangle) \end{aligned} \tag{9.13}$$

Substituting $\langle j|\tilde{\rho}^j_{\hat{Z}}|j\rangle = 1 - 2\mathrm{P}(\mathrm{error}_{\hat{R}} \mid \hat{Z} = j)$ obtained from eq.(9.11) to eq.(9.13),

$$H(Z \mid \tilde{Z}_A) = -1 + H(Z) + \sum_i P^i_{\hat{Z}} f(\mathrm{P}(\mathrm{error}_{\hat{R}} \mid \hat{Z} = i)),$$

holds. Substituting the above equation to eq.(9.12),

$$\begin{aligned} H(X \mid \tilde{X}_E) &\geq 2 - H(Z) - \sum_i P^i_{\hat{Z}} f(\mathrm{P}(\mathrm{error}_{\hat{R}} \mid \hat{Z} = i)) \\ &\geq 1 - \sum_i P^i_{\hat{Z}} f(\mathrm{P}(\mathrm{error}_{\hat{R}} \mid \hat{Z} = i)), \end{aligned}$$

holds, where we use a property of binary entropy $0 \leq H(Z) \leq 1$. By definition of mutual information $I(X;\tilde{X}_E) = H(X) - H(X \mid \tilde{X}_E)$,

$$\begin{aligned} I(X;\tilde{X}_E) &\leq H(X) - 1 + \sum_i P^i_{\hat{Z}} f(\mathrm{P}(\mathrm{error}_{\hat{R}} \mid \hat{Z} = i)) \\ &\leq \sum_i P^i_{\hat{Z}} f(\mathrm{P}(\mathrm{error}_{\hat{R}} \mid \hat{Z} = i)), \end{aligned}$$

[4] Thanks to $\langle \Psi_{AKE'}|(Z_j \otimes \mathbb{I}_K \otimes \mathbb{I}_{E'})|\Psi_{AKE'}\rangle = \langle \Psi^+|\langle E_1|(\mathbb{I}_A \otimes V^\dagger_{KE'})(Z_j \otimes \mathbb{I}_K \otimes \mathbb{I}_{E'})(\mathbb{I}_A \otimes V_{KE'})|E_1\rangle|\Psi^+\rangle = \langle \Psi^+|(Z_j \otimes \mathbb{I}_K)|\Psi^+\rangle\langle E_1|E_1\rangle = 1/2$.

holds, where we use the property $0 \leq H(X) \leq 1$ once more. It ends the proof. ■

Suppose that Alice measures the system in the state $\tilde{\rho}^i_{\hat{Z}} \otimes |i\rangle\langle i|$ with the measurement $\hat{L}$, then, probabilities in which Alice estimates King's outcome perfectly are

$$\mathrm{P}(\hat{L} = 1 \vee \hat{L} = 3 \mid \hat{Z} = 0) = \frac{1}{2}(\langle 0|\tilde{\rho}^0_{\hat{Z}}|0\rangle + 1),$$
$$\mathrm{P}(\hat{L} = 2 \vee \hat{L} = 4 \mid \hat{Z} = 1) = \frac{1}{2}(\langle 1|\tilde{\rho}^1_{\hat{Z}}|1\rangle + 1).$$

An error probability is

$$\mathrm{P}(\mathrm{error}_{\hat{L}} \mid \hat{Z} = i) = \frac{1}{2}(1 - \langle i|\tilde{\rho}^i_{\hat{Z}}|i\rangle).$$

The probability is equal to the error probability with the measurement $\hat{R}$ eq.(9.11). Therefore, we obtain the following theorem.

Theorem 29 *If Alice employs the measurement $\hat{L}$,*

$$I(X; \tilde{X}_E) \leq \sum_{i \in \{0,1\}} P^i_{\hat{Z}} f(\mathrm{P}(\mathrm{error}_{\hat{L}} \mid \hat{Z} = i)),$$

holds.

9.5 Security Analysis for Attack Model 3

The model 3 is the most general one among the three attack models. Eve1 takes the system $\mathcal{H}_K$ on AK-channel. She prepares a system $\mathcal{H}_{E'}$ in a state $|E'\rangle$ and performs unitary evolution $V_{KE'}$ on $\mathcal{H}_K \otimes \mathcal{H}_{E'}$ as $(\mathbb{I}_A \otimes V_{KE'})|\Psi^+\rangle \otimes |E'\rangle$, King measures the system $\mathcal{H}_K$ with $\hat{Z}$ or $\hat{X}$, then, a post measurement state of $\mathcal{H}_K$ is an eigenstate of $\hat{Z}$ or it of $\hat{X}$. On the other hand, a post measurement state of $\mathcal{H}_A$ may or may not be an eigenstate of them. Let ρ^i_A be a post measurement state of the system $\mathcal{H}_A$ when King chooses $A \in \{\hat{X}, \hat{Z}\}$ and obtains an outcome $i \in \{0, 1\}$. Eve2 takes the system $\mathcal{H}_K$ in the eigenstate on KA-channel and performs the unitary evolution W_{KE} on $\mathcal{H}_K \otimes \mathcal{H}_E$ similar to the attack model 1. Therefore, Alice takes the bipartite system $\mathcal{H}_A \otimes \mathcal{H}_K$ in the state $\rho^i_{\hat{Z}} \otimes \rho'_i$ or $\rho^j_{\hat{X}} \otimes \rho'_{\bar{j}}$ with the measurement $\hat{L}$ or $\hat{R}$.

Firstly, we consider that Alice employs $\hat{L}$. We have conditional probabilities of estimating King's outcome perfectly when King chooses $\hat{Z}$:

$$\mathrm{P}(\hat{L} = 1 \vee \hat{L} = 3 \mid \hat{Z} = 0) = \frac{1}{2}\langle 0|(\rho^0_{\hat{Z}} + \rho'_0)|0\rangle,$$
$$\mathrm{P}(\hat{L} = 2 \vee \hat{L} = 4 \mid \hat{Z} = 1) = \frac{1}{2}\langle 1|(\rho^1_{\hat{Z}} + \rho'_1)|1\rangle.$$

An error probability of the sifted key generated by the measurement $\hat{Z}$ is

$$\mathrm{P}(\mathrm{error}_{\hat{L}} \mid \hat{Z} = i) = 1 - \frac{1}{2}\langle i|(\rho^i_{\hat{Z}} + \rho'_i)|i\rangle. \tag{9.14}$$

By substituting ρ'_0, ρ'_1, and eq.(9.14) to eq.(9.5), we obtain the following inequality:

$$\begin{aligned}
F(\rho'_0, \rho'_1) &= \inf_{\{E_\alpha\}_\alpha:\mathrm{POVM}} \sum_\alpha \sqrt{\mathrm{tr}(\rho'_0 E_\alpha)\mathrm{tr}(\rho'_1 E_\alpha)} \\
&\leq \sqrt{\mathrm{tr}(\rho'_0|0\rangle\langle 0|)\mathrm{tr}(\rho'_1|0\rangle\langle 0|)} + \sqrt{\mathrm{tr}(\rho'_0|1\rangle\langle 1|)\mathrm{tr}(\rho'_1|1\rangle\langle 1|)} \\
&= \sqrt{\langle 0|\rho'_0|0\rangle(1 - \langle 1|\rho'_1|1\rangle)} + \sqrt{(1 - \langle 0|\rho'_0|0\rangle)\langle 1|\rho'_1|1\rangle} \\
&\leq \sqrt{2} \sum_{i\in\{0,1\}} \sqrt{\mathrm{P}(\mathrm{error}_{\hat{L}} \mid \hat{Z} = i) + \frac{1}{2}(\langle i|\rho^i_{\hat{Z}}|i\rangle - 1)} \\
&\leq \sqrt{2} \sum_{i\in\{0,1\}} \sqrt{\mathrm{P}(\mathrm{error}_{\hat{L}} \mid \hat{Z} = i)},
\end{aligned}$$

where we use $\langle i|\rho^i_{\hat{Z}}|i\rangle - 1 \leq 0$. We have the following theorem.

Theorem 30 *If Alice employs the measurement $\hat{L}$,*

$$\|\Lambda^*_E(|+\rangle\langle +|) - \Lambda^*_E(|-\rangle\langle -|)\|_1 \leq 2\sqrt{2} \sum_{i\in\{0,1\}} \sqrt{\mathrm{P}(\mathrm{error}_{\hat{L}} \mid \hat{Z} = i)}, \tag{9.15}$$

holds for the attack model 3.

The inequality also denotes a trade-off relationship between information gain for Eve1 and error rate.

Secondly, we discuss effect of the operation of Eve1 in this case. In the case of the model 1, i.e., Eve1 does not perform any operation on $\mathcal{H}_K$ on AK-channel, the error probability is represented as eq.(9.4). On the other hand, the error probability is eq.(9.14) if Eve1 performs an operation. As eq.(9.14) $-$ eq.(9.4) $= 1/2(1 - \langle i|\rho^i_{\hat{Z}}|i\rangle) \geq 0$ holds, Eve1 cannot decrease the error probability with any quantum operation.

Finally, we consider a case of employing the measurement $\hat{R}$ by Alice. In this case, probabilities of estimating King's outcome perfectly when King chooses $\hat{Z}$:

$$\begin{aligned}
\mathrm{P}(\hat{R} = 1 \vee \hat{R} = 2 \mid \hat{Z} = 0) &= \frac{1}{2}\langle 0|(\rho^0_{\hat{Z}} + \rho'_0)|0\rangle + \frac{\mathrm{i}}{2}(\langle 1|\rho^0_{\hat{Z}}|0\rangle - \langle 0|\rho'_0|1\rangle), \\
\mathrm{P}(\hat{R} = 3 \vee \hat{R} = 4 \mid \hat{Z} = 1) &= \frac{1}{2}\langle 1|(\rho^1_{\hat{Z}} + \rho'_1)|1\rangle + \frac{\mathrm{i}}{2}(\langle 0|\rho^1_{\hat{Z}}|1\rangle - \langle 1|\rho'_1|0\rangle).
\end{aligned}$$

holds. For the measurement $\hat{R}$, an error probability corresponding to $\mathrm{P}(\mathrm{error}_{\hat{R}} \mid \hat{Z} = i)$ is equal to eq.(9.14) if second terms of the above equations is equal to 0. However, the second terms is generally non zero values. Therefore, eq.(9.15) may or may not hold for $\hat{R}$.

Remark that the role of $\hat{X}$ is symmetrically with respect to the role of $\hat{Z}$ in Theorems 26,27,28,29, and 30.

Chapter 10

Summary

In this thesis, we obtained three main results about Mean King's problem and the quantum key distribution using the problem. The thesis consists of not only topics of the main results but also introductions of basics of quantum information theory and so on. We reviewed basics of quantum information theory in Chapter 3, quantum error-correcting codes in Chapter 4, quantum cryptography in Chapter 5. We introduced conventional setting of Mean King's problem and quantum key distribution protocol as its application in Chapter 6, and showed the main results after Chapter 6.

In Chapter 7, we proposed a solution to Mean King's problem generalized with respect to arbitrary families of measurement operators by using quantum error-correcting codes. We showed existence of the solution to the problem in the case that King employs measurements constructed from mutually unbiased basis of prime-power dimension, then it was show that the previous work in the same case can be considered from the viewpoint of quantum error-correcting codes. By constructing settings of the problem which are different from previous setting and are solved by our solution, we also expanded the class of settings of the problem a solution is existent. In Chapter 8, we reformulated Mean King's problem using Shannon entropy. As its application, we gave an alternative proof of nonexistence of solutions to qubit setting without using entanglement. As a result, we gave informational insight to the problem. In Chapter 9, we applied measurements $\hat{M}, \hat{N}$, and $\hat{L}$ which solve Mean King's problem for two observables to the quantum key distribution protocol. We analyzed security of the protocols to show that the protocols using $\hat{M}$ and $\hat{N}$ are insecure under a rather simple attack model. This result implies that measurements solving the Mean King's problem for two observables are necessary but are not sufficient to construct secure quantum key distribution protocols.

Finally, we expect that new insights from viewpoints of a combination of quantum estimation problem, quantum error-correcting codes, and quantum key distribution will be given to quantum information theory, physics, and information science. As a result, we hope that quantum information theory is recognized as a bridge between physics and information science, and we also hope that quantum information theory progresses and has good effect on not only science but also engineering.

References

[1] C. H. Bennett, and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” Proc. of IEEE Int. Conf. on Comp. Sys. and Signal Proc., pp.175-179, 1984.

[2] P. W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring,” Proc. of 35th IEEE FOCS, pp.124-134, 1994.

[3] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” Phys. Rev. Lett., vol. 70, pp.1895-1899, 1993.

[4] A. Einstein, B. Podolsky, and N. Rosen, “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?,” Phys. Rev., vol. 47, pp.777-780, 1935.

[5] L. Vaidman, Y. Aharonov, and D. Z. Albert, “How to ascertain the values of σ_x, σ_y, and σ_z of a spin-1/2 particle,” Phys. Rev. Lett., vol. 58, pp.1385-1387, 1987.

[6] J. Bub, “Secure key distribution via pre- and postselected quantum states,” Phys. Rev. A, vol. 63, 032309, 2001.

[7] F. Hiai, and K. Yanagi, *HILBERT SPACES AND LINEAR OPERATORS*, Makino Shoten, 1995. (in Japanese)

[8] H. Umegaki, M. Ohya, and F. Hiai, *An introduction to to operator algebra*, Kyoritsu Shuppan, 1985. (in Japanese)

[9] T. Saito, *An introduction to linear algebra*, University of Tokyo Press, 1966. (in Japanese)

[10] G. Nishida, *Linear algebra*, Kyoto University Press, 2009. (in Japanese)

[11] O. Bratteli, and D. W. Robinson, *Operator Algebras and Quantum Statistical Mechanics 1*, Springer-Verlag Berlin Heidelberg, Second Edit., 1987.

[12] O. Bratteli, and D. W. Robinson, *Operator Algebras and Quantum Statistical Mechanics 2*, Springer-Verlag Berlin Heidelberg, Second Edit., 1997.

[13] T. M. Cover, and J. A. Thomas, *Elements of Information Theory*, Wiley-Interscience, Second Edit., 2006.

[14] D. J. C. MacKay, *Information Theory, Inference and Learning Algorithms*, Cambridge University Press, 2003.

[15] H. Imai, *Information theory*, Shokodo, 1984. (in Japanese)

[16] C. E. Shannon, "A mathematical theory of communication," Bell System Tech. J., vol. 27, pp.379-423, 623-656, 1948.

[17] C. E. Shannon, and W. Weaver, *A mathematical theory of communication*, translated by T. Uyematsu, Chikuma Shobo, 2009. (in Japanese)

[18] S. Tomonaga, *Quantum Physics 1*, Misuzu Shobo, Second Edit., 1969. (in Japanese)

[19] S. Tomonaga, *Quantum Physics 2*, Misuzu Shobo, Second Edit., 1997. (in Japanese)

[20] C. J. Isham, *Lectures on Quantum Theory: Mathematical and Structural Foundations*, World Scientific Pub., 1995.

[21] A. Shimizu, *Foundation of quantum theory*, SAIENSU-SHA, 2003. (in Japanese)

[22] A. Holevo, *Probabilistic and Statistical Aspects pf Quantum Theory*, Edizioni Della Normale, 2011.

[23] M. Ohya, amd D. Petz, *Quantum Entropy and Its Use*, Springer-Verlag Berlin Heidelberg, 1993.

[24] M. Ozawa, "An Operational Approach to Quantum State Reduction," Ann. Phys., vol. 259, pp.121-137, 1997.

[25] M. Ozawa, "Uncertainty relations for noise and disturbance in generalized quantum measurements," Ann. Phys., vol. 311, pp.350-416, 2004.

[26] G. Kimura, T. Miyadera, and H. Imai, "Optimal state discrimination in general probabilistic theories," Phys. Rev. A, vol. 79, 062306, 2009.

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

[28] M. Hayashi, *Quantum Information An Introduction*, Springer-Verlag Berlin Heidelberg, 2006.

[29] S. Ishizaka, T. Ogawa, A. Kawachi, G. Kimura, and M. Hayashi, *Introduction to Quantum Information Science*, Kyoritsu Shuppan, 2012. (in Japanese)

[30] O. Hirota, *THE FOUNDATION OF QUANTUM INFORMATION SCIENCE Approach to quantum computer*, Morikita Pub., 2002.

[31] N. D. Mermin, *Quantum Computer Science An Introduction*, Cambridge University Press, 2007.

[32] J. Gruska, *QUANTUM COMPUTING*, Mcgraw Hill Book, 1999.

[33] J. K. Pachos, *Introduction to Topological Quantum Computation*, Cambridge University Press, 2012.

[34] R. P. Feynman, and A. Hey, *FEYNMAN LECTURES ON COMPUTATION*, Westview Press, 1996.

[35] A. Hosoya, *Lectures on Quantum Computation*, SAIENSU-SHA, 1999. (in Japanese)

[36] M. Ohya, and N. Watanabe, *Quantum Cryptography and Quantum Teleportation*, Kyoritsu Shuppan, 2006. (in Japanese)

[37] K. Kraus, *States, Effects, and Operations*, Lecture Notes in Physiscs, vol. 190, Springer, Berlin, 1983.

[38] W. F. Stinespring, "Uncertainty relations for noise and disturbance in generalized quantum measurements," Proc. of am. Math. Soc., vol. 6, pp.211-216, 1995.

[39] A.Peres, "Separability Criterion for Density Matrices," Phys. Rev. Lett., vol. 77, pp.1413-1415, 1996.

[40] M. Horodecki, P. Horodecki, and R. Horodecki, "Separability of Mixed States: Necessary and Sufficient Conditions," Phys. Lett., A, vol. 223, pp.1-8, 1996.

[41] H. F. Hofmann, and S. Takeuchi, "Violation of local uncertainty relations as a signature of entanglement," Phys. Rev. A, vol. 68, 032103, 2003.

[42] H. P. Robertson, "The Uncertainty Principle," Phys. Rev., vol. 34, pp.163-164, 1929.

[43] V. Giovannetti, "Separability conditions from entropic uncertainty relations," Phys. Rev. A, vol. 70, 012102, 2004.

[44] O. Gühne, and M. Lewenstein, "Entropic uncertainty relations and entanglement," Phys. Rev. A, vol. 70, 022316, 2004.

[45] J. I. de Vicente, and J. Sánchez-Ruiz, "Separability conditions from the Landau-Pollak uncertainty relation," Phys. Rev. A, vol. 71, 052325, 2005.

[46] T. Miyadera, and H. Imai, "Generalized Landau-Pollak Uncertainty Relation," Phys. Rev. A, vol. 76, 062108, 2007.

[47] M. Yoshida, T. Miyadera, and H. Imai, "Separability Criterion in prime dimensions based on Landau-Pollak Uncertainty Relation," Proc. of ISITA2008, pp.467-472, 2008.

[48] I. D. Ivanović, "Geometrical description of quantal state determination," J. Phys. A, vol. 14, pp.3241-3245, 1981.

[49] W. K. Wootters, and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," Ann. Phys. vol. 191, issue 2, pp.363-381, 1988.

[50] C. H. Bennerr, and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," Phys. Rev. Lett., vol. 69, pp.2881-2884, 1992.

[51] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense Coding in Experimental Quantum Communication," Phys. Rev. Lett., vol. 76, pp.4656-4659, 1996.

[52] X.-S. Ma, T. Herbst, T. Scheidl, D. Wang, S. Kropatschek, W. Naylor, B. Wittmann, A. Mech, J. Kofler, E. Anisimova, V. Makarov, T. Jennewein, R. Ursin, and A. Zeilinger, "Quantum teleportation over 143 kilometres using active feed-forward," Nature, vol. 489, pp.269-273, 2012.

[53] P. W. Shor, and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Phys. Rev. Lett., vol. 85, pp.441-444, 2000.

[54] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels," Phys. Rev. Lett., vol. 76, pp.722-725, 1996.

[55] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," Phys. Rev. A, vol. 54, pp.3824-3851, 1996.

[56] R. Matsumoto, “Conversion of a general quantum stabilizer code to an entanglement distillation protocol,” J. Phys. A: Math. Gen., vol. 36, no. 29, pp.8113-8127, 2003.

[57] M. Yoshida, M. Hagiwara, T. Miyadera, and H. Imai, “A Numerical Evaluation of Entanglement Sharing Protocols Using Quantum LDPC CSS Codes,” IEICE Trans. Fund., vol. E95-A, no. 9, 2012.

[58] H. Imai, *Coding theory*, The Institute of Electronics, Information and Communication Engineers, 1990. (in Japanese)

[59] M. Hagiwara, *Coding theory*, Nippon Hyoron Sha, 2012. (in Japanese)

[60] E. Knill, and R. Laflamme, “Theory of Quantum Error-Correcting Codes,” Phys. Rev. A, vol.55, pp.900-911, 1997.

[61] D. Gottesman, “Class of quantum error-correcting codes saturating the quantum Hamming bound,” Phys. Rev. A, vol.54, pp.1862-1868, 1996.

[62] A. R. Calderbank, and P. W. Shor, “Good quantum error-correcting codes exist,” Phys. Rev. A, vol.54, 1098, 1996.

[63] A. Steane, “Multiple particle interference and quantum error correction,” Proc. of Roy. Soc. Lond. A, 452, pp.2492-2495, 1996.

[64] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, Chapman and Hall/CRC, 2008.

[65] S. Singh, *The Code Book*, Fourth Estate, 2012.

[66] W. Diffie, and M. Hellman, “New Disrections in Cryptography,” IEEE Trans. on Information Theory, IT-22, 6, pp.644-654 1976.

[67] R. L. Rivest, A. Shamir, and L. Adelman, “A Method for Obtaining Digital Signature and Public-key Cryptsystems,” Technical Memo LCS/TM82; Apr. 4, 1977.

[68] T. ElGamal, “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms,” Proc. of CRYPTO84, pp.10-18, Springer-Verlag. 1984.

[69] National Bureau of Standards (U.S.): Data Encryption Standard, Federal Information Processing Standards Publication 46, National Technical Information Services, Springfield VA, 1977.

[70] Federal Information Processing Standards Publication 197, “Announcing the Advanced Encryption Standard (AES),” 2001.

[71] M. Matsui, "Block Encryption Algorithm MISTY," Proc. of ISEC96-1, pp.35-48, Jul. 1996. (in Japanese)

[72] A. Shimizu, and S. Miyaguchi, "Fast Date Encipherment Algorithm FEAL," Trans. on IEICE, Inf. and Sys.:D vol.J70-D no. 7, pp.1413-1423, 1987. (in Japanese)

[73] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," Phys. Rev. A, vol. 68, no.2, 022317, 2003.

[74] D. Bruß, "Optimal Eavesdropping in Quantum Cryptography with Six States," Phys. Rev. Lett., vol.81, pp.3018-3021, 1998.

[75] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," Phys. Rev. Lett., vol. 68, pp.3121-3124, 1992.

[76] A. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett., vol. 67, pp.661-663, 1991.

[77] T. Okamoto, K. Tanaka, and S. Uchiyama, "Quantum public-key cryptosystems," Proc. of CRYPTO2000, Lecture Notes in Computer Science, vol.1880, pp.147-165, 2000.

[78] A. Kawachi, T. Koshiba, H. Nishiyama, and T. Yamakami, "Computational indistinguishability between quantum states and its cryptographic application," Proc. of EUROCRYPT2005, Lecture Notes in Computer Science, vol. 3494, pp.268-284, 2005.

[79] D. Gottesman, and I. Chuang, "Quantum digital signatures," arXiv, quant-ph/0103032v2, 2001.

[80] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," Phys. Rev. A, vol.59, pp.1829-1834, 1999.

[81] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized Privacy Amplification," IEEE Trans. on Information Theory, vol. 41, no.6, pp.1915-1923, 1995.

[82] D. Mayers, "Unconditional security in Quantum Cryptography," JACM, vol. 48, no.3, pp.351-406, 2001.

[83] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," Proc. of 32nd Ann. ACM Symposium on the Theory of Computing, pp.715-724, ACM press, 2000.

[84] T. Miyadera, and H. Imai, "Information-disturbance theorem for mutually unbiased observables," Phys. Rev. A, vol. 73, 042317, 2006.

[85] Y. Aharonov, and B.-G. Englert, "The mean king's problem: Spin 1," Z. Naturforsch., A:Phys. Sci., 56a, 16, 2001.

[86] B.-G. Englert, and Y. Aharonov, "The mean king's problem: Prime degrees of freedom," Phys. Lett., A, 284, 1, 2001.

[87] A. Klappenecker, and M. Roetteler, "New Tales of the Mean King," arXiv, quant-ph/0502138, 2005. 1

[88] Y. Aharonov, P. G. Bergmann, and J. L. Lebowitz, "Time Symmetry in the Quantum Process of Measurement," Phys. Rev., vol. 134, pp.B1410-B1416, 1964.

[89] A. Hayashi, M. Horibe, and T. Hashimoto, "Mean king's problem with mutually unbiased bases and orthogonal Latin squares," Phys. Rev. A, vol. 71, 052331, 2005.

[90] G. Kimura, H. Tanaka, and M. Ozawa, "Solution to the mean king's problem with mutually unbiased bases for arbitrary levels," Phys. Rev. A, vol. 73, 050301(R), 2006.

[91] M. Reimpell, and R. F. Werner, "A Meaner King uses Biased Bases," Phys. Rev. A, vol. 75, 062334, 2007.

[92] G. Kimura, H. Tanaka, and M. Ozawa, "Comments on "Best conventional solutions to the King's problem"," Z. Naturforsch. vol. 62a, pp.152-156, 2007.

[93] P. K. Aravind, "Best conventional solutions to the King's Problem," Z. Naturforsch. vol. 58a, pp.682-690, 2003.

[94] S. Ben-Menahem, "Spin-measurement retrodiction," Phys. Rev. A, vol. 39, pp.1621-1627, 1989.

[95] M. Horibe, A, Hayashi, and T. Hashimoto, "Solution to the king ' s problem with observables that are not mutually complementary," Phys. Rev. A, vol. 71, 032337, 2005.

[96] A. Jamiołkowski, "Linear transformations which preserve trace and positive semidefiniteness of operators," Rep. Math. Phys., vol. 3, pp.275-278, 1972.

[97] M.-D. Choi, "Positive linear maps on C^*-algebras," Canad. J. Math., vol. 24, no. 3, pp.520-529, 1972.

[98] M.-D. Choi, "Completely positive linear maps on complex matrices," Linear Algebra and its Applications, vol. 10, pp.285-290, 1975.

[99] D. M. Greenberger, M. A. Horne, and A. Zeilinger, *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos, Kluwer Academic Pub., pp.73-76, 1989.

[100] A. H. Werner, T. Franz, and R. F. Werner, "Quantum cryptography as a retrodiction problem," Phys. Rev. Lett., vol. 103, 220504, 2009.

[101] A. Uhlmann, "The "transition probability" in the state space of a $*$-algebra," Rep. Math. Phys., vol. 9, pp.273-279, 1976.

[102] R. Jozsa, "Fidelity for Mixed Quantum States," J. Mod. Opt., vol. 41, pp.2315-2323, 1994.

[103] C. A. Fuchs, and C. M. Caves, "Mathematical techniques for quantum communication theory," Open Sys. Info. Dyn., vol. 3, pp.345-356, 1995.

[104] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, "Noncommuting Mixed States Cannot Be Broadcast," Phys. Rev. Lett., vol. 76, pp.2818-1821, 1996.

[105] T. Miyadera, and H. Imai, "State collapse in Information Transfer and its applications," Proc. of SCIS2008, 2D2-4, 2008.

[106] M. Krishna, and K. R. Parthasarathy, "An Entropic Uncertainty Principle For Quantum Measurements," Sankhya Series A, vol. 64 no. 3, pp.842-851, 2002.