Introduction of **Mutually Unbiased Bases**

and

**Solution to the Mean King’s problem**

for arbitrary finite levels

Recent issues and prospects on quantum theory

2006. 3. 10,11 (KEK)

G. Kimura, H. Tanaka, M. Ozawa (Tohoku Univ.)
★ Prelude

Quantum Theory

Infinite or finite

© Realization ⋅⋅⋅ Approximation, System of Interest

© Application ⋅⋅⋅ Quantum Information Theory

→ Quantum Computer, Quantum Cryptography, et. al

© Foundation ⋅⋅⋅ To understand Quantum Mystery (?)

© Nonobviousness ⋅⋅⋅ Connections with various combinatorial problems

→ character in each dimension
Overview

★ 1 Mutually Unbiased Bases (MUBs)
   - Complementarity in d level quantum systems
   - State determination with d+1 MUBs
   - Optimal state determination
   - Open Problem with MUBs [Orthogonal Latin Squares (OLSs) ?]

★ 2 Mean King’s Problem
   - Introduction of Mean King’s problem
   - Review of HHH method [OLS]
   - Solution for arbitrary levels [Orthogonal Arrays]
   - Conclusion and discussion
1 Mutually Unbiased Bases (MUBs)
Mutually Unbiased Bases [Complementarity 1]

\[ \dim(\mathcal{H}) = \infty \]

\[ [x, p] = i\mathbb{I} \]

\[ \langle x|p \rangle = \exp(ipx) \]

\[ |\langle x|p \rangle|^2 = \text{const} \]

\[ \dim(\mathcal{H}) = d \]

Maximum degree of incompatibility !!

Mutually Unbiased Bases
**Mutually Unbiased Bases [Complementarity 2]**

Consider a level quantum system: $\mathcal{H}_d$

Two orthonormal bases $\{\psi_i\} \{\phi_j\}$ are said to be Mutually Unbiased if

$$p_j^{(i)} = |\langle \psi_i | \phi_j \rangle|^2 = \frac{1}{d}$$

for all $i, j = 1, \ldots, d$

Let $O_\psi$ and $O_\phi$ be observables with Mutually Unbiased eigenvectors $\{\psi_i\} \{\phi_j\}$

$O_\psi$ and $O_\phi$ are also called mutually unbiased

For any eigenstate of $O_\psi$, information of $O_\phi$ is most random!!

```
O_\psi \rightarrow \text{"Complementary" pair of observables}!!
```

Schwinger (1960)
Mutually Unbiased Bases [Entropic Uncertainty Relation]

Entropic Uncertainty Relation

\[ H(p) + H(q) \geq \ln(\min_{i,j} \frac{1}{|\langle \phi_i | \psi_j \rangle|^2}) \]

\[ = \ln d \quad \text{(Mutually Unbiased Obs)} \]

Mutually Unbiased Observables \iff maximum lower bound

★ Mutually Unbiased Bases [ state determination 1 ]

Consider a set of orthonormal bases: \( \mu = 1, \ldots, n \)

\[
\{ |\mu, i\rangle \}_{i=1}^{d}
\]

Set of orthonormal bases are said to be mutually unbiased bases (MUBs) if any pair of them are mutually unbiased!!

\[
|\langle \mu, i | \nu, j \rangle|^2 = \frac{1}{d} \quad (\mu \neq \nu)
\]

( \( \iff \) \( |\langle \mu, i | \nu, j \rangle|^2 = \delta_{\mu \nu} \delta_{ij} + (1 - \delta_{\mu \nu}) \frac{1}{d} \) )

Case \( n = d + 1 \) is important and intriguing!
Measurements of $d+1$ numbers of MUBs determine (unknown) quantum state $\rho$

\[ p_{\mu i} = \langle \mu, i | \rho | \mu, i \rangle \]

Corresponding Density Operator

\[ p \equiv (p_{\mu i}) \rightarrow \rho(p) = \sum_{\mu=1}^{d+1} \sum_{i=1}^{d} p_{\mu i} |\mu, i\rangle \langle \mu, i | - \mathbb{I} \]

[Example: $d=2$] 3 ($=2+1$) numbers of $x$, $y$ and $z$ Pauli Matrices are MUBs

\[ \cdots \] Connection with Bloch Vector

(Ivanovic 1981)
Mutually Unbiased Bases [optimal state determination]

$d+1$ numbers of MUBs provides an optimal state determination in the sense that the effects of statistical errors are minimized!!

- In principle, ensembles are finite no matter how they are large
- In each measurement $A,B,\ldots$, statistical errors appear
- Estimated state are in the intersection of their error ranges
- Find a set of observables with minimum intersection of error ranges

$\rightarrow$ MUBs provides minimum int.

(Wootters & Fields 1989)
Mutually Unbiased Bases [open problem]

Existence of \( d+1 \) numbers of MUBs?

\begin{itemize}
  \item at most \( d + 1 \) numbers!!
  \item when \( d = p^m \), \( d+1 \) numbers of MUBs do exist!!
  \item Otherwise, unknown so far, even \( d = 6 \)!!
\end{itemize}

http://www.imaph.tu-bs.de/qi/problems/

Orthogonal Latin Squares (OLSs)

\begin{itemize}
  \item at most \( d - 1 \) numbers!!
  \item when \( d = p^m \), \( d-1 \) numbers of OLSs do exist!!
  \item There are some \( d \), e.g., \( d = 6 \) and 10, less than \( d-1 \)
\end{itemize}

Are there really some mathematical connection between MUB problem and OLS problem?

2 Mean King’s Problem, with MUBs
★ Mean King’s Problem [ Introduction 1 ]

★ Alice has to guess King’s output, otherwise she will be executed !!

★ HHH found under the assumption of d+1 MUBs

Solution for Alice to survive with certainty

⇔ d-1 Maximum Numbers of OLSs

→ Alice might be executed in e.g., d=6 or 10 level systems !!!

Our Goal:
find solutions for Alice to survive with certainty for arbitrary dimension !!

Connection with Orthogonal Arrays !!

Hayashi, Horibe, & Hashimoto (2005)
Once upon a time,

there lived a mean King who loved cats.

The King hated physicists

since he heard what had happened to Schroedinger's cat.
One day, a terrible storm came on, and Alice, a physicist, got stranded on the island that was ruled by the King.

The King called Alice to the royal laboratory and gave her a challenge.

poor Alice …
Mean King’s Problem [Introduction 2]

1. King orders Alice to prepare a $d$ level quantum system and hand it over to the King.

2. The King will then secretly measure it with respect to one of $d+1$ MUBs and return it to Alice.

3. Alice is then allowed to perform one more measurement on the system.

4. Afterwards, the King reveals his measurement basis and Alice must immediately guess the correct output of the King’s measurement, or she will be executed ...

L. Vaidman et al. (1987), Y. Aharonov & Englert (2001), etc..
**Mean King's Problem [ HHH method 1 ]**

**Alice has to guess King's output \( i \), with her Output \( I \) and post information \( \mu \)**

\[ s(I, \mu): \text{Estimation Function} \]

**No ways to survive with Prob. 1, without entangling to some object**

→ **Use entanglement at the state preparation !!!**

**HHH method**

\[ \mathbb{C}^d \otimes \mathbb{C}^d \text{ use the same d level system} \]

\[ |\Phi\rangle \equiv \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A \otimes |i\rangle_K \in \mathbb{C}^d \otimes \mathbb{C}^d \text{ maximal entangled state !!!} \]

Allow Alice only **projective measurement**

→ **Existence-Equivalence between Alice's way to survive with certainty and d-1 OLSs**

Hayashi, Horibe, & Hashimoto (2005)
★ Mean King’s Problem [ Our method 1 ]

@ She can perform not only projective measurement, but also POVMs !!
[ Notice: She can use another ancilla with higher dimension $d'$ to realize the POVMs ]

Theorem 1 [G.K., H. Tanaka, M. Ozawa] For any $d$ level system, By using maximal entangled state, Alice can find a POVM to guess King’s output with probability 1 !

with a certain mathematical connection with Orthogonal Arrays

Alice can survive with certainty !!
★ Mean King’s Problem [ Proof ]

★ prepare $\mathbb{C}^{d'} \otimes \mathbb{C}^{d}$ systems $d' \geq d$

with the same maximal entanglement state

$$|\Phi\rangle \equiv \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle_A \otimes |i\rangle_K \in \mathbb{C}^{d'} \otimes \mathbb{C}^{d}$$

$$= \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |\mu, i\rangle_A \otimes |\mu, i\rangle_K, \quad (|\mu, i\rangle_A \equiv \sum_{i=0}^{d-1} \langle i| \mu\rangle_K |i\rangle_A)$$

post measurement state

$$\mu \quad \frac{1}{\mu} \rightarrow \quad |\Phi_{\mu, i}\rangle \equiv |\mu, i\rangle_A \otimes |\mu, i\rangle_K$$

$$\langle \Phi_{\mu, i} | \Phi_{\nu, j} \rangle = \langle \mu, i | \nu, j \rangle_K^2 \quad \text{MUB cond.}$$
★ Mean King’s Problem [Proof]

❤ Find a projective measurement $\{ |I\rangle \}_{I=0}^{dd'-1}$ on $\mathbb{C}^{d'} \otimes \mathbb{C}^d$

and an estimation function $s(I, \mu) \in \{0, \ldots, d - 1\}$

\[
(\ast) \quad \langle I | \Phi_{\mu,i} \rangle = 0 \quad \text{whenever} \quad s(I, \mu) \neq i
\]

Lemma 1

Given $s(I, \mu)$, there exists an orthonormal basis $\{ |I\rangle \}$ satisfying (\ast)

iff there is a $dd' \times d(d+1)$ matrix $H(I; \mu, i)$ s.t.

\[
(\ast 1) \quad H(I; \mu, i) = 0 \quad \text{whenever} \quad s(I, \mu) \neq i.
\]

\[
(\ast 2) \quad H^\dagger H(\mu, i; \nu, j) = \delta_{\mu\nu}\delta_{ij} + (1 - \delta_{\mu\nu})\frac{1}{d}
\]
⋆ Mean King’s Problem [ Orthogonal Array ]

© Orthogonal Array \( O\mathcal{A}_n(k, d) \)

(degree \( k \), order \( d \) and index \( n \)) \( \iff \)

an \( nd^2 \times k \) array with entries from \( \{0, 1, \ldots, d-1\} \)
s.t. in each (ordered) pair of distinct columns, every (ordered) pair occurs exactly \( n \) times.

⋆ every symbol occurs \( nd \) times in each column

For any \((k,d)\), we can always find a suitable \( n \) and \( O\mathcal{A}_n(k, d) \)

Let \( s(I, \mu) \) form an \( O\mathcal{A}_n(k, d) \)

\[
\frac{1}{nd} \sum_{I=0}^{nd^2-1} \delta_{i,s(I,\mu)}\delta_{j,s(I,\nu)} = \delta_{\mu,\nu}\delta_{i,j} + (1 - \delta_{\mu,\nu}) \frac{1}{d}
\]
★ Mean King's Problem [Proof]

◎ Let Alice prepare $d' = nd$ Ancila

◎ Set

$$H(I; \mu, i) = \frac{1}{\sqrt{nd}} \delta_{i,s(I,\mu)}$$

where Alice use the estimation function $s(I, \mu)$ which forms an $OAn(d+1,d)$

Condition in Lemma 1 holds

(*) 1) $H(I; \mu, i) = 0$ whenever $s(I, \mu) \neq i$.

(*) 2) $H^\dagger H(\mu, i; \nu, j) = \delta_{\mu \nu} \delta_{ij} + (1 - \delta_{\mu \nu}) \frac{1}{d}$

From Lemma 1, Alice finds a suitable measurements $\{|I\rangle\}_{I=0}^{nd^2-1}$ and estimation function $s(I, \mu)$, from which she can guess King's output with certainty!!
★ Mean King's Problem  [ Proof ]

Let $P : \mathbb{C}^{d'} \otimes \mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^d$

and $M_I \equiv P|I\rangle\langle I|P$

Positive Operator Valued Measure in $\mathbb{C}^d \otimes \mathbb{C}^d$

(I) positivity $M_I \geq 0$

(II) normalization $\sum_{i=0}^{dd'-1} M_I = P^2 = P$

Q.E.D
★ Mean King’s Problem  [ Conclusion ]

We showed a solution of Mean King’s problem always exists for any $d$

Using maximal entangled state and
a suitable POVM in $d \times d$ system

Mathematical connection between MUB
and Orthogonal Array

Unfortunately, this result tells nothing about
the existence of maximum numbers of MUBs

Possible Application: Quantum Cryptography
If it is safe, our protocol provides an efficient scheme for QC
References


