(15)「量子統計とその周辺」に関する研究報告

局所的観測量による量子推定

堀田昌寛 小澤正直 (東北大)

Based on our recent paper,
"Quantum Estimation by Local Observables",
PRA,**70** 022327(2004).

これまで量子推定理論はあらゆる観測量が使用できるという前提の下で定式化されてきたが、現実の量子系においては必ずしもこの暗黙の条件は満たされていない。現在の実験技術の限界など様々な制約の中に置かれて、限られた観測量のみを用いて推定を行うこともしばしば強要される。これを踏まえて我々は、限定された観測量（局所的観測量）の集合のみを用いた場合にも推定が可能となるように、理論の拡張を行なった。局所的密度行列

$$\rho := P\rho_{tot}(t)P + (1 - Tr[P\rho_{tot}(t)P])|B\rangle\langle B| \tag{1}$$

に対して

$$\partial_g \rho = \frac{1}{2}(\tilde{L}\rho + \rho\tilde{L}), \tag{2}$$

$$\tilde{L}^\dagger = \tilde{L} \tag{3}$$

で定まる対称対数微分から得られるフィッシャー情報量 J の逆数はクラメール・ラオ不等式の平均２乗誤差の下限となる。また藤原-長岡の純粋状態量子推定理論を局所的観測量による推定に適用できるように拡張を行なった。規格化されない純粋状態：

$$\rho_{\|}(t,g) = |\Psi(t,g)\rangle\langle\Psi(t,g)| \tag{4}$$

に対して情報量は

$$J = 4\left(\langle\partial_g\Psi|\partial_g\Psi\rangle - \frac{|Im\langle\Psi|\partial_g\Psi\rangle|^2}{\langle\Psi|\Psi\rangle}\right) + 4\frac{|Re\langle\Psi|\partial_g\Psi\rangle|^2}{1-\langle\Psi|\Psi\rangle} \tag{5}$$

で与えられる。更に多体系における量子推定を論じ、２つのフィッシャー情報量が導入できることを述べる。その１つの情報量の計算評価は簡単であるがその大きさは他方の情報量に比べて小さい。もうひとつの情報量は大きな値をもち前者より良い推定を与えるが、その計算解析は多体系が大きくなるほど複雑となり、異なる初期条件の下で解かれた多数の密度作用素の時間発展を解くことが要求される。

我々の局所的観測量による推定理論は、より現実に沿った推定を可能とする。また量子コンピュータの素子設計においても、量子計算に不要な準位の及ぼす影響の解析精密化等に役立つ可能性があると考えられる。

Free Analogues of Cramer-Rao Inequality and Powers Factors

Fumio Hiai
Graduate School of Information Sciences, Tohoku University

1. Free analogue of Cramer-Rao inequality

Most simply, assume that X is a real random variable having a smooth density function p. The (classical) Fisher information $I(X)$ is defined by

$$I(X) := \int_{-\infty}^{\infty} \left(\frac{d}{dx} \log p(x) \right)^2 p(x)\, dx = \int_{-\infty}^{\infty} \frac{p'(x)^2}{p(x)}\, dx.$$

The (classical) Cramer-Rao inequality is given (in this simplest case) as

$$I(X) \geq \frac{1}{V(X)},$$

where $V(X) := \int_{-\infty}^{\infty} x^2 p(x)\, dx$ is the variance of X. Equality occurs in the inequality only when p is a normal (or Gaussian) law:

$$p(x) = \frac{1}{\sqrt{2\pi}\sigma} \exp\left(-\frac{(x-m)^2}{2\sigma^2} \right).$$

Based on random matrix heuristics, in 1993 Voiculescu found that the free analogue of the Fisher information is

$$\Phi(X) := \frac{4\pi^2}{3} \|p\|_3^3 = \frac{4\pi^2}{3} \int_{-\infty}^{\infty} p(x)^3\, dx = 4 \int_{-\infty}^{\infty} (Hp)(x)^2 p(x)\, dx,$$

where Hp is the Hilbert transform of p:

$$(Hp)(x) := \lim_{\varepsilon \searrow 0} \int_{|x-t|>\varepsilon} \frac{p(t)}{x-t}\, dt.$$

The free analogue of the Cramer-Rao inequality holds as follows:

$$\Phi(X) \geq \frac{1}{V(X)}$$

and equality holds if and only if p is a semicircle (or Wigner) law:

$$p(x) = \frac{2}{\pi r^2} \sqrt{r^2 - (x-m)^2}\, \chi_{[m-r,m+r]}(x).$$

Voiculescu further introduced the free Fisher information $\Phi^*(X_1, \ldots, X_n)$ for n-tuples of noncommutative random variables $(X_1, \ldots, X_n)$ in a tracial noncommutative probability space $(\mathcal{M}, \tau)$. The free Cramer-Rao inequality for noncommutative multivariables is given as

$$\Phi^*(X_1, \ldots, X_n) \geq \frac{1}{\tau(X_1^2 + \cdots + X_n^2)}$$

and equality holds if and only if $X_1, \ldots, X_n$ are freely independent semicirculars with $\tau(X_j) = 0$.

In my talk I explain these free Cramer-Rao inequalities and also a recent progress on free Logarithmic Sobolev inequalities; the latter is concerned with inequalities between free entropy and free Fisher information.

2. Free analogue of Powers factors

For $0 \leq \lambda \leq 1$ let ψ_λ be a state on $M_2(\mathbb{C})$ (the 2×2 matrix algebra) with the density matrix $\begin{bmatrix} \lambda(1+\lambda) & 0 \\ 0 & 1/(1+\lambda) \end{bmatrix}$. Consider the tensor product state $\varphi := \bigotimes_1^\infty \psi_\lambda$ on the infinite tensor product C^*-algebra $\mathcal{A} := \bigotimes_1^\infty M_2(\mathbb{C})$ (the so-called CAR algebra) and construct the von Neumann algebra

$$\mathcal{M}_\lambda := \pi_\varphi(\mathcal{A})'' = \bigotimes_1^\infty \{M_2(\mathbb{C}), \psi_\lambda\}$$

via the GNS representation π_φ associated with φ. This $\mathcal{M}_\lambda$ becomes a factor. For extreme cases $\lambda = 0$ and $\lambda = 1$, the factors constructed are the I_∞ factor $B(\mathcal{H})$ and the hyperfinite type II_1 factor, respectively. When $0 < \lambda < 1$, the factor $\mathcal{M}_\lambda$ is the Powers factor that is a unique hyperfinite (or AFD) type III_λ factor.

The above factors $\mathcal{M}_\lambda$ $(0 \leq \lambda \leq 1)$ are among more general Araki-Woods factors

$$\bigotimes_{n=1}^\infty \{M_{k_n}(\mathbb{C}), \psi_n\}.$$

Araki-Woods factors (in particular, the Powers factors) can be also constructed by use of Fermion (or CAR) Fock space models. In 1977 Shlyakhtenko constructed free analogues of Araki-woods factors

$$\Gamma(\mathcal{H}_\mathbb{R}, U_t)''$$

associated with a separable real Hilbert space $\mathcal{H}_\mathbb{R}$ and a strongly continuous one-parameter group of orthogonal transformations U_t on $\mathcal{H}_\mathbb{R}$; here the tensor product is replaced by the free product and the Fermion Fock space is replaced by the full Fock space. He proved that $T_\lambda := \Gamma(\mathbb{R}^2, U_t)''$ with $U_t := \begin{bmatrix} \cos(t\log\lambda) & -\sin(t\log\lambda) \\ \sin(t\log\lambda) & \cos(t\log\lambda) \end{bmatrix}$ (the rotation with period $2\pi/\log\lambda$) is a unique type III_λ free Araki-Woods factor, regarded as the free analogue of the type III_λ Powers factor.

In my talk I explain the Powers factors, their free analogues and moreover q-deformed algebras due to Bożejko and Speicher constructed in the q-Fock space $(-1 < q < 1)$ interpolating Fermion $(q = -1)$, free $(q = 0)$ and Boson $(q = 1)$.

2次元ユニタリ通信路の漸近推定問題における量子クラメル・ラオ型の評価

今井寛*†, 藤原彰夫*‡

2次元ヒルベルト空間を用いて記述される量子状態 ρ が, 外界との接触を持たず孤立的に変化する状況を考える. 状態の変化は Lie 群 $SU(2)$ に属する作用素 g を用いて $\Gamma_g : \rho \mapsto g\rho g^*$ と記述される. Γ_g は2次元ユニタリ通信路と呼ばれ, 量子ユニタリゲート等がその例である.

今, 未知の2次元ユニタリ通信路 Γ_g が在り, Γ_g を特徴付ける未知パラメタ $g \in SU(2)$ を特定したいとしよう. この時, 入力状態 ρ を適当に選んで通信路 Γ_g に入力し, 出力状態 $\Gamma_g(\rho)$ に対して何らかの測定 M を行なう事で, g に関する情報を得る事が出来る.

それではどのような ρ と M を用いた時に, g に関する情報を最大限引き出す事が可能なのか. また, 引き出す事が出来る情報の限界はどの様に定まるのか. こういった問題を量子統計学的な立場から議論するのが, 量子通信路の統計的推定問題である.

本研究で扱う, 2次元ユニタリ通信路の漸近的推定問題は, Bagan et al., Chiribella et al. および林によりベイズ統計的な手法による研究が行なわれているが, 我々は非ベイズ的な立場からより詳細な解析を行なう.

Lie 環 $su(2)$ の表現論を利用して, 通信路の出力モデルに対する量子 SLD クラメル・ラオ下界が局所的に達成可能となる為の必要十分条件を与え, さらに分散・共分散行列の重み付きトレース $\mathrm{Tr}\, \mathrm{GV}_g[M]$ を最小化するという基準での, 最適な推定方式を議論する.

*大阪大学理学研究科数学教室
†himai@gaia.math.wani.osaka-u.ac.jp
‡fujiwara@math.wani.osaka-u.ac.jp

Conclusion

- $\mathrm{Tr}\, G\, \mathcal{V}_\theta[M,\theta] = \mathcal{O}(J^{-2})$ for most admissible input states.
- The explicit formula of

$$\min_{M,\tau} \mathrm{Tr}\, G\, \mathcal{V}_\theta[M,\tau]$$

for $X_i = \sqrt{-1}\sigma_i, G = I$ and a construction scheme of the optimal (M,τ) for any X_i, G are provided. The main tools we used are:

- information geometrical consideration
- the representation theory of $su(2)$

51

Statistical Estimation of a Quantum Channel

Enlarged SU(2) channel:

$$\varepsilon_\theta : \tau \mapsto (\mathrm{I}\otimes U_\theta)^{\otimes N}\,\tau\,(\mathrm{I}\otimes U_\theta^*)^{\otimes N}$$

Output states form a quantum statistical model:

$$\left\{(\mathrm{I}\otimes U_\theta)^{\otimes N}\,\tau\,(\mathrm{I}\otimes U_\theta^*)^{\otimes N} \mid U_\theta \in \mathrm{SU}(2)\right\}$$

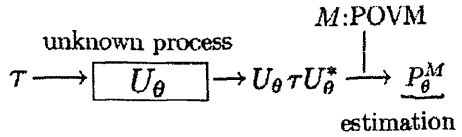
$\downarrow M$: POVM

$$\left\{P_\theta^{M,\tau} \mid \theta \in \Theta\right\}$$

(M,τ)-doubly optimization problem.

18

Identification Scheme of Unknown Quantum Channel



4

- How about SU(d) (d ≥ 3)?
  - Lemma 2 does not hold.
  - Take ψ^{ME} as maximally entangled in $\mathbf{C}^3 \otimes \mathcal{H}^{[N,0]}$.

$$\min_M \mathcal{V}_\theta[M,\psi^{\mathrm{ME}}] = \mathcal{O}(J^{-2})$$

SU(d) case will be reported elsewhere.

52

Main Result

Construction scheme of the optimal (M,ψ) for any $\{X_i\}_{1\le i\le 3}$ is provided.

Corollary

When $X_i = \sqrt{-1}\,\sigma_i$ (HS bases up to const.),

$$\min_{M,\psi} \mathrm{Tr}\, \mathcal{V}_\theta[M,\psi] = \frac{9}{16j(j+1)}$$

where $j = \frac{1}{2}(\dim \mathcal{H}_j - 1)$.

27

$$\tau \longrightarrow \boxed{U_\theta} \longrightarrow \rho_\theta$$

$$\hat{\tau} \longrightarrow \boxed{(\mathrm{I}\otimes U_\theta)^{\otimes N}} \longrightarrow \rho_\theta^{[N]}$$

$$\hat{\tau} \in \mathcal{S}\left((\mathcal{H}\otimes\mathcal{H})^{\otimes N}\right)$$

- role of entanglement?
- asymptotic order?

5

Outline of The Proof

- Calculate $J_\theta^S(\psi)|_{\theta=0}$ using $su(2)$ representation theory.
- Concentrate on "admissible" input states.

$$\min_{M,\psi} \mathrm{Tr}\, \mathcal{V}_\theta[M,\psi] = \min_{M,\psi\,:\,\underline{\text{admissible}}} \mathrm{Tr}\, \mathcal{V}_\theta[M,\psi]$$

- The following equalities hold:

$$\min_{M,\psi} \mathrm{Tr}\, \mathcal{V}_\theta[M,\psi] = \min_{M,\psi\ \text{admissible}} \mathrm{Tr}\, \mathcal{V}_\theta[M,\psi] = \min_{\psi\,:\,\text{admissible}} \mathrm{Tr}\, J_\theta^S(\psi)^{-1}$$

- Minimize $\mathrm{Tr}\, J_\theta^S(\psi)^{-1}$ over admissible ψ's.

32

Related Researches

Baysian	Peres et al.	
	Bagan et al.	
	Chiribella et al.	
	Hayashi	
Cramér-Rao	Fujiwara	$N = 1$
	Ballestar	phase estimation

⇒ Our approach is Cramér-Rao type ($^\forall N$)

7

Estimation of $SU(d)$ action using entanglement

Manuel A. Ballester*
Department of Mathematics, University of Utrecht, Box 80010, 3508 TA Utrecht, The Netherlands

In recent papers (Refs [1, 2, 3, 4]) it is shown that if N copies of an $SU(2)$ gate are available, one can estimate it with a square error that goes to 0 as $1/N^2$ (instead of $1/N$ as one normally expects in statistics). This is achieved by using an Nfold entangled state as input to $U^{\otimes N}$. In my talk I will try to show that this is also possible for $SU(d)$ with $d > 2$.

Consider we have N copies of a $d \times d$ unknown unitary U at the same time. We'll prepare an N-partite input state $|\psi_0\rangle$.

Let $V = U^{\otimes N}$, the output density matrix is

$$\rho = (\mathbb{1}_D \otimes V)|\psi_0\rangle\langle\psi_0|(\mathbb{1}_D \otimes V^\dagger),$$

where $|\psi_0\rangle \in \mathbb{C}^D \otimes \mathbb{C}^{d^{\otimes N}}$.

The Quantum Crámer-Rao bound (QCRB) tells us that for a class of "reasonable" estimators, the mean square error (MSE) is bounded from below by the quantum Fisher information (QFI), furthemore from Ref. [5] we have conditions for achievability of the QCRB. The strategy therefore is to find an input state that satisfies the conditions for achievability of the QCRB and so that its QFI scales like N^2.

Let

$$|\psi_0\rangle = \sum_{K=1}^{\min(D,d^N)} \sqrt{p_K}\, |\psi_K^A\rangle \otimes |\psi_K^B\rangle,$$

where $|\psi_K^A\rangle$ ($|\psi_K^B\rangle$) is a system of orthonormal vectors in $\mathbb{C}^D$ (respectively $\mathbb{C}^{d^{\otimes N}}$),let

$$\rho_B = \sum_K p_K |\psi_K^B\rangle\langle\psi_K^B|,$$

be the reduced density matrix on $\mathbb{C}^{d^{\otimes N}}$.

Let us define $\overline{\rho}_1$ as the average one-copy reduced density matrix of ρ, i.e.,

$$\overline{\rho}_1 = \frac{1}{N}\sum_{s=1}^{N} \mathrm{tr}_{\bar{s}}\, \rho, \tag{1}$$

where $\mathrm{tr}_{\bar{s}}$ means partial trace with respect to all copies except the s^{th} one. In the same way, let us define $\overline{\rho}_2$ as the average symmetrized two-copy reduced density matrix of ρ, i.e.,

$$\overline{\rho}_2 = \frac{2}{N(N-1)}\sum_{s\neq r}^{N} (\mathrm{tr}_{\overline{sr}}\, \rho + W\, \mathrm{tr}_{\overline{sr}}\, \rho W), \tag{2}$$

where $\mathrm{tr}_{\overline{sr}}$ means partial trace with respect to all copies except the r^{th} and the s^{th}, and W is the exchange operator

$$\begin{aligned} W &= \sum_{kl} |kl\rangle\langle lk| \\ &= \frac{\mathbb{1}\otimes\mathbb{1}}{d} + \sum_{\alpha=1}^{d^2-1} t_\alpha \otimes t_\alpha. \end{aligned} \tag{3}$$

With these definitions, we get that the condition for achievability of the QCRB becomes $\overline{\rho_{B1}} = \mathbb{1}/d$. Then $\overline{\rho_{B2}}$ must be of the form

$$\overline{\rho_{B2}} = \frac{\mathbb{1}\otimes\mathbb{1}}{d^2} + \sum_{\alpha\beta} c_{\alpha\beta} t_\alpha \otimes t_\beta,$$

---

*Electronic address: ballester@math.uu.nl; URL: http://www.math.uu.nl/people/balleste/

here $c_{\alpha\beta} = c_{\beta\alpha}$. With these choices, the QFI becomes

$$H_{\alpha\beta} = 4[\frac{N}{d}\delta_{\alpha\beta} + N(N-1)c_{\alpha\beta}].$$

If we want to ewstimate all parameters with the same accuracy, the best we can hope for is a state of the form

$$\begin{aligned}\overline{\rho_{B}}_2 &= \frac{\mathbb{1}\otimes\mathbb{1}}{d^2} + \frac{1}{d(d+1)}\sum_{\alpha} t_\alpha \otimes t_\alpha \\ &= \frac{1}{d(d+1)}(\mathbb{1}\otimes\mathbb{1} + W).\end{aligned} \tag{4}$$

The QFI corresponding to this state is

$$H_{\alpha\beta} = 4\frac{N(N+d)}{d(d+1)}\delta_{\alpha\beta},$$

which has the desired N^2 behaviour.

Let

$$|n_1,\ldots,n_d\rangle = \frac{|1\rangle^{\otimes n_1}\otimes\ldots\otimes|d\rangle^{\otimes n_d} + \text{non-equivalent permutations}}{\sqrt{\frac{N!}{n_1!n_2!\ldots n_d!}}},$$

where $\sum_{k=1}^{d} n_k = N$.

Let $N = dn + m$, $n_k = n + m$, $n_l = n$, $l \neq k$ and $|\phi_{Nmk}\rangle = |n,\ldots,n_k = n+m,\ldots,n\rangle$, we get that an input state of the form

$$|\psi_0(m)\rangle = \frac{1}{\sqrt{d}}\sum_{k=1}^{d}|k\rangle\otimes\left(\sqrt{\frac{(d+1)m^2-N^2}{(d+1)m^2}}\,|\phi_{N1k}\rangle + \sqrt{\frac{N^2}{(d+1)m^2}}\,|\phi_{Nmk}\rangle\right),$$

will do the required job. Linear combinations of these states would work as well.

---

[1] M. Hayashi, (2004), quant-ph/0407053.
[2] E. Bagan, M. Baig, and R. Munoz-Tapia, Phys. Rev. A **69**, 050303 (2004), quant-ph/0303019.
[3] E. Bagan, M. Baig, and R. Munoz-Tapia, Phys. Rev. A **70**, 030301 (2004), quant-ph/0405082.
[4] G. Chiribella, G. D'Ariano, P. Perinotti, and M. Sacchi, (2004), quant-ph/0405095.
[5] K. Matsumoto, J. Phys. A **35**, 3111 (2002), quant-ph/9711008.

Query Complexity and Quantum Estimation

Keiji Matsumoto[1,2]
keiji@nii.ac.jp

February 23, 2005

I review the results in quantum query complexity, a famous tool in computational complexity theory, and show these are in fact statistical estimation theoretic problems. I also comment on the defference of the formulation of the problem between these communities.

Phase estimation problem had been also studied in quantum measurement theory, in relation with phase-number uncertainty. After the appearance of quantum computation, this problem was related to Abelian hidden subgroup problems, with Shor's algorithm and Simon's period finding problem being special examples. Earlier than that, researchers in state estimation theory considered parallel query version of this problem. There are several proof of the optimality of square root speed up, and here I add yet one more, which seems to me easier and thus might be applicable to derive unknown results.

1 Optimality of Grover's Algorithm

Grover's problem is to find a x such that $f(x) = 1$, under the assumption $|f^{-1}(1)| = 1$. Grover suggested an algorithm which solves this problem at most $(\sqrt{d}t)$, with $\log d$ being the length of the input of the function f. This algorithm realizes square root speed up, and known to be optimal algorithm. There are several proofs already, here I add yet one more, which I think is simpler than any other existing proofs.

Following preceding authors, we describe all the processes other than last measurement by unitary operation. Let U_f be a unitary operator which computes the function f, and V be a unitary operator which describes information processing between queries. For simplicity, we write $\Lambda_U(\rho) = U\rho U^\dagger$. After n steps, will be $\Lambda^n_{U_f V}(\rho)$, where ρ is the inital states. For the final mesurement can extract the information about f, $\|\Lambda^n_{U_f V}(\rho) - \Lambda^n_{U_{f'} V}(\rho)\|$ should be large enough

[1]Quantum Computation Group, National Institute of Informatics, Japan.
[2]Quantum Computation and Information Project, ERATO, JST, 5-28-3 Hongo, Bunkyo-ku, Tokyo 113-0033, Japan.

for all $f \neq f'$. we have,

$$\frac{1}{d(d-1)} \sum_{f \neq f'} \|\Lambda^n_{U_f V}(\rho) - \Lambda^n_{U_{f'} V}(\rho)\| \leq \frac{1}{d(d-1)} \sum_{f \neq f'} \sum_{t=1}^{n} \|\Lambda^{n-t}_{U_f V}(\Lambda_{U_f V} - \Lambda_{U_{f'} V})(\Lambda^{t-1}_{U_{f'}}(\rho))\|$$
$$\leq \frac{n}{d(d-1)} \max_{\rho} \sum_{f \neq f'} \|(\Lambda_{U_f V} - \Lambda_{U_{f'} V})(\rho)\| \tag{1}$$

Without loss of generality, the initial state can be assumed to be pure state. Hence, this is furthuer evaluated as,

$$\frac{n}{d(d-1)} \max_{\phi} \sum_{f \neq f'} \sqrt{1 - |\langle \phi | U_f^\dagger U_{f'} | \phi \rangle|^2} \leq n \max_{\phi} \sqrt{1 - (\frac{1}{d(d-1)} \sum_{f \neq f'} |\langle \phi | U_f^\dagger U_{f'} | \phi \rangle|)^2}. \tag{2}$$

Let $\{|i\rangle\}$ be an orthonormal basis in the space of input of the function f, and $\{|\phi_i\rangle\}$ be a set of states satisfying $|\phi\rangle = \sum_i \alpha_i |i\rangle |\phi_i\rangle$. Then, we can evaluate the quantity (2) is equal to

$$n \max_{\alpha} \sqrt{1 - (\frac{1}{d(d-1)} \sum_{j'} \sum_{j : j \neq j'} \sum_{i : i \neq j, j'} |\alpha_i|^2)^2}$$
$$= n \max_{\alpha} \sqrt{1 - \frac{(d-2)^2 (d-1)^2}{d^2 (d-1)^2}} \sim n\sqrt{2/d}. \tag{3}$$

For $\frac{1}{d(d-1)} \sum_{f \neq f'} \|\Lambda^n_{U_f V}(\rho) - \Lambda^n_{U_{f'} V}(\rho)\|$ should close to 1, we have n should be at least in the order of $\sqrt{d}$.

2 Query complexity of estimation of unitary matrices

Note that in previous proof, we didn't use the property of U_f up to (2). Hence, this inequality can be for any other estimation problem. Especially, here we assume that $U_f = e^{\imath H_f t}$, with t being very small and $[H_f, H_{f'}] = 0$. Then, (2) is,

$$n \max_{\phi} \frac{t}{d(d-1)} \sum_{f \neq f'} |\langle \phi | (H_f - H_{f'}) | \phi \rangle| + O(t^2). \tag{4}$$

Further more, assume that the eigenvalues of H_f is of the form $E\delta_{j,f} (j = 0, \cdots, d)$. Then, this simplifies to,

$$n \max_{\alpha} \frac{Et}{d(d-1)} \sum_{f \neq f'} ||\alpha_f|^2 - |\alpha_{f'}|^2| + O(t^2) = O(nEt/d) + O(t^2). \tag{5}$$

Hence, to solve this query complexity problem, at least $O(d/nEt)$ times queries are necessary.

This seemingly artificial problem is derived from estimation of d-level unitary matrices which commutes with each other. If we can estimate a unitary matrix with the accuracy of t, we can easily solve the problem analyzed above. Hence, to estimate unitary matrix with given accuracy t, we need $O(d/nEt)$ times queries at least.

有限個のPOVMによる純粋状態の最適量子推定

林明久、橋本貴明、堀邊稔
福井大学工学部　物理工学科

I. 目的 - 結果

d 次元空間の純粋状態 $\rho = |\phi\rangle\langle\phi|$ のコピーが N 個与えられたとしよう。状態 ρ が全く未知であるとして、系 $\rho^{\otimes N}$ を測定することにより、ρ をできるだけ正確に推定したいとする。ここでは、正確さの目安としてフィデリティ $\mathrm{tr}[\rho\rho']=|\langle\phi|\phi'\rangle|^2$ を採用する。純粋状態 $\rho'=|\phi'\rangle\langle\phi'|$ は入力 ρ に対する推定である。さて、どのような測定が平均フィデリティ $F(N,d)$ を最大にするだろうか、また最大値は N と d の関数としてどのようになるだろうか？

Qubit（d=2）の場合には、$F_{\max}(N,2)=(N+1)/(N+2)$ となることが分かっている [1]。更に一般的な次元 d や評価関数の場合について、共変的測定を用いて林正人によって調べられた [2]。特に平均フィデリティーについては、$F_{\max}(N,d)=(N+1)/(N+d)$ を得ている。また、純粋状態の量子状態推定を、N 個の状態コピーから $M=\infty$ 個のコピーへの最適クローニングと関係づけることにより、同じ最大平均フィデリティーが得られている [3]。

この研究 [4] では、最大平均フィデリティーが有限個の要素からなる POVM 測定で実現できる事を示す。そのため、先ず測定の共変性や最適クローニングとの関連を使わずに最大平均フィデリティーを導く。なぜなら、この問題のように全く未知の状態は連続的なパラメータで指定されており、共変的な POVM は無限個の要素を必要とするからである。そして、最適な有限 POVM は超球面上の正確な求積法（quadrature）で与えられることを示す。

また共変的な POVM は、フィデリティーが入力状態に依存しないという意味でユニバーサルであり、必然的にフィデリティーの最小値を最大にする（ミニマックス法）解でもある [2]。この事は我々の有限 POVM については一般に保証されない。しかし、$N+1$ 個の状態コピーに対する最適な有限 POVM は、N 個の状態コピーに対してユニバーサルであり、ミニマックス法の解にもなっていることが示される。

II. 平均フィデリティーの最大値と有限な最適 POVM

平均フィデリティーの最大値と、それを与える有限な最適 POVM にたいする条件は次のように導かれる。入力 $\rho^{\otimes N}$ に対して、POVM 測定 $\{E_a\}_{a=1,\cdots,A}$, $\sum_a E_a=\mathcal{S}_N$ を行う。ここで、$\mathcal{S}_N$ は N 体系の完全対称空間への射影演算子である。測定結果 a に対して状態が $\rho_a\in\{\rho_a\}_{a=1,\cdots,A}$ であったと推定することにすると、平均フィデリティーは次のように与えられる。

$$F(N,d)=\sum_{a=1}^{A}\left\langle \mathrm{tr}\left[E_a\rho^{\otimes N}\right]\mathrm{tr}\left[\rho_a\rho\right]\right\rangle=\sum_{a=1}^{A}\left\langle \mathrm{tr}\left[E_a\rho^{\otimes(N+1)}\rho_a(N+1)\right]\right\rangle. \tag{1}$$

ここで、$<\cdots>$ は入力の純粋状態 ρ に関する平均を表し、ρ の分布が一体の任意のユニタリー変換に対して不変であると仮定すると、$\rho^{\otimes N}$ の平均に対して次の強力な関係式が成立する。

$$\left\langle\rho^{\otimes N}\right\rangle=\frac{\mathcal{S}_N}{d_N}, \tag{2}$$

ただし、$d_N=\mathrm{tr}[\mathcal{S}_N]={}_{N+d-1}C_{d-1}$ である。これを使って平均を実行し、仮想的に導入した $(N+1)$ 番目の系をトレースアウトすれば

$$F(N,d)=\frac{1}{(N+1)d_{N+1}}\sum_{a=1}^{A}\mathrm{tr}\left[E_a\left(1+\sum_{n=1}^{N}\rho_a(n)\right)\right]. \tag{3}$$

さて、$\rho_a\le 1$ に注意すれば、平均フィデリティーの上限は

$$F(N,d)\le\frac{d_N}{d_{N+1}}=\frac{N+1}{N+d}, \tag{4}$$

で与えられ、等号は $E_a \propto \rho_a^{\otimes N}$ の時にのみ成立することが分かる。さらに POVM の完全性と関係式 (2) を使うと有限 POVM が最適であるための必要充分条件は

$$\sum_{a=1}^{A} w_a \rho_a^{\otimes N} = \left\langle \rho^{\otimes N} \right\rangle , \tag{5}$$

であることが分かる。重み w_a は非負であり、$\sum_a w_a = 1$ でなければならない。

さて、条件 (5) の右辺は $2d-1$ 次元超球面上の積分であり、左辺は A 個の超球面上の点 ρ_a についての重み付の有限和である。すなわち、正の重みを持つ有限個の点からなる超球面上のある求積法が関数 $\rho^{\otimes N}$ に対して正確な結果を与えるということを意味する。そのような求積法の存在を示すためには、超球面上の任意の $2N$ 次多項式まで正確な値を与える求積法があることを言えば充分である。実際、超球面上の積分を角度変数の多重積分で表すことによりそのような求積法を構成することができる（詳細は [4])。さらに、すべての重みが定数である求積法は spherical $2N$-design と呼ばれ、その存在は示されている。しかし、その実際の構成は一般には難しいようである。

いずれにせよ、条件 (5) を満たす解はあり、従って上限 (4) は有限個の POVM で実現できる最大値 $F_{\max}(N,d)$ である。

つぎに、最適な有限 POVM のユニバーサリティーについて調べてみよう。最適な POVM は条件 (5) を満たす $E_a = d_N w_a \rho_a^{\otimes N}$ で与えられるので、入力状態について平均する前のフィデリティーは、

$$\sum_{a=1}^{A} \mathrm{tr}\left[E_a \rho^{\otimes N}\right] \mathrm{tr}\left[\rho_a \rho\right] = d_N \sum_{a=1}^{A} w_a \mathrm{tr}\left[\rho_a^{\otimes (N+1)} \rho^{\otimes (N+1)}\right], \tag{6}$$

となる。これが入力に依存しないためには

$$\sum_{a=1}^{A} w_a \rho_a^{\otimes (N+1)} = \left\langle \rho^{\otimes (N+1)} \right\rangle , \tag{7}$$

でなければならない事がわかる。これは $N+1$ 個の状態コピーの場合の最適性の条件であり、N 個のコピーに対する条件 (5) より強い条件である。したがって、有限個の POVM は一般にはユニバーサルではないが、$N+1$ 個のコピーに対する最適な推定法を N 個のコピーに対して用いるとユニバーサルとなり、必然的にミニマックス法の最適測定でもある事がわかる。

この事は例えば、具体的に次のようにしても実現できるだろう。すなわち、N 個の状態コピーが与えられたとき、先ず N 個のコピーから $M(>N)$ 個のコピーへ最適なクローニングを行う。その後、M 個の状態コピーに対する最適有限 POVM で状態推定を行う。すると、この状態推定はユニバーサルであり平均フィデリティーと最小フィデリティーを最大にすることを示すことができるのである。

---

[1] S. Massar and S. Popescu, Optimal Extraction of Information from Finite Quantum Ensembles, Phys. Rev. Lett., **74**, 1259 (1995)

[2] Masahito Hayashi, Asymptotic estimation theory for a finite dimensional pure state model, J. Phys. **A31**, 4633 (1998)

[3] Dagmar Bruß and Chiara Macchiavello, Optimal state estimation for d-dimensional quantum systems, Phys. Lett., **A253**, 249 (1999)

[4] A. Hayashi, T. Hashimoto, and M. Horibe, Optimal quantum state estimation of pure states revisited, quant-ph/0410207

[5] A. Hayashi, T. Hashimoto, and M. Horibe, Extended Quantum Color Coding, Phys. Rev., **A71**, (2005) (in press),(quant-ph/0409173)

Quantum entanglement and Bell inequalities

L. C. Kwek[1]

[1]*Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542. National Institute of Education, Nanyang Technological University, 1 Nanyang Walk, Singapore 639798*

We look briefly at the development of Bell inequalities in higher dimensions with larger number of particles under two settings. We briefly describe some of the recent work done to connect Bell inequalities to game theoretic formulation. **Talk presented at the Workshop on Quantum Statistics and Related Topics, Tokyo, 27 to 28 January, 2005.**

PACS numbers: 03.65.Ud, 03.67.-a,42.50.-p

INTRODUCTION

In their classic paper in 1934, Einstein, Podolsky and Rosen did not question the validity of quantum mechanics. However, they claimed that quantum mechanics is an incomplete description of physical reality. Essentially, they showed that the wave function alone cannot describe physical reality, another variable, which is not measurable nor calculable, is required. This hidden variable, often denoted by λ is needed to supplement quantum mechanics. Over the years, many hidden variable models have been formulated. In 1964, John Bell showed that any local hidden variable theory is incompatible with quantum mechanics.

To describe Bell's argument, we can consider, for simplicity, two particles emitted from a common source and flying towards two people, typically labeled as Alice and Bob. Alice and Bob then measured some observables associated with the particles, for example, its spin or polarization. For simplicity, let us assume that they record their measurements as ± 1 corresponding to up and down spin (or vertical and horizontal polarization). Suppose also that the corresponding observables are $\vec{n}\cdot\vec{\sigma}$ where $\vec{n}$ is some direction corresponding to the measurement and $\vec{\sigma}$ is the vector of Pauli matrices. By looking at the correlation of the results, E_{ij} of their measurements, it can be shown that

$$\begin{aligned} E_{ij} &= E(\vec{n},\vec{m}) \\ &= p(+1,+1)+p(-1,-1)-p(+1,-1)-p(-1,+1) \\ &= \langle\psi|\vec{n}\cdot\vec{\sigma}\otimes\vec{m}\cdot\vec{\sigma}|\psi\rangle \end{aligned} \quad (1)$$

where the i-th and j-th measurements are aligned with the vectors $\vec{n}$ and $\vec{m}$

For a hidden variable model, we suppose that the "complete" state of system is characterized by some hidden variable λ which may be chosen by Bob (or Alice) just before Alice's (or Bob's) measurement. In other words, there exist some functions $A(\vec{a},\lambda)$ and $B(\vec{b},\lambda)$ such that

$$E(\vec{a},\vec{b}) = \int \rho(\lambda)A(\vec{a},\lambda)B(\vec{b},\lambda)d\lambda, \quad (2)$$

where $rho(\lambda)$ is the probability density for the hidden variable. Without any loss in generality, one may assume that the detectors are perfectly aligned so that $A(\vec{a},\lambda) = -B(\vec{a},\lambda)$ and that $A(\vec{a},\lambda) = \pm 1$ although the latter assumption may be stronger than needed. In this way, Eq. (3) may be written as

$$E(\vec{a},\vec{b}) = -\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)d\lambda. \quad (3)$$

Thus, we have

$$\begin{aligned} & |E(\vec{a},\vec{b}) - E(\vec{a},\vec{c})| \\ = & \left|\int \rho(\lambda)A(\vec{a},\lambda)\left(A(\vec{b},\lambda) - A(\vec{c},\lambda)\right)d\lambda\right| \\ = & \left|\int \rho(\lambda)A(\vec{a},\lambda)A(\vec{b},\lambda)\left(1 - A(\vec{b},\lambda)A(\vec{c},\lambda)\right)d\lambda\right| \\ \leq & \left|\int \rho(\lambda)\left(1 - A(\vec{b},\lambda)A(\vec{c},\lambda)\right)d\lambda\right| \\ \leq & \; 1 + E(\vec{b},\vec{c})| \end{aligned} \quad (4)$$

As given in Eq. 1, quantum mechanically, $E(\vec{a},\vec{b}) = -\vec{a}\cdot\vec{b}$. So it is possible to choose the vectors $\vec{a}$, $\vec{b}$ and $\vec{c}$ appropriately so that $\vec{a}\cdot\vec{b} = \vec{b}\cdot\vec{c} = \frac{1}{2}$ while $\vec{a}\cdot\vec{c} = -\frac{1}{2}$. These values do not satisfy the inequality 4.

A refinement of Bell inequality 4 was subsequently proposed by Clauser, Holt, Shimony and Horne (CHSH) in the late sixties in the form

$$|E(\vec{a},\vec{b}) + E(\vec{a},\vec{b'})| + |E(\vec{a'},\vec{b}) - E(\vec{a'},\vec{b'})| \leq 2. \quad (5)$$

This inequality was subsequently generalized by Clauser and Horne (CH) by replacing the correlations by probabilities

$$P_{12}(\vec{a},\vec{b}) - P_{12}(\vec{a},\vec{b'}) + P_{12}(\vec{a'},\vec{b}) + P_{12}(\vec{a'},\vec{b'}) - p_1(\vec{a'}) - p_2(\vec{b'}) \leq 0. \quad (6)$$

EXTENSION TO THREE THREE-DIMENSIONAL SYSTEMS

In a recent paper[1], we generalize CH inequality to three three-dimensional systems. To be specific we consider a Bell-type gedanken experiment with three observers each measuring two observables on some quantum state $\hat{\rho}$. We denote the observables by $\hat{A}_1, \hat{A}_2$ for the first observer (Akira), $\hat{B}_1, \hat{B}_2$ for the second observer (Bento) and $\hat{C}_1, \hat{C}_2$ for the third one (Chiko). The measurement of each observable yields three distinct outcomes (numbers) which we denote by a_1^i, a_2^i, a_3^i for Akira's measurement of the observable $\hat{A}_i$, b_1^j, b_2^j, b_3^j for Bento's measurement of the observable $\hat{B}_j$ and c_1^k, c_2^k, c_3^k for Chiko's measurement of the observable $\hat{C}_k$ $(i,j,k = 1,2)$. Specifically, the observable $\hat{A}_i$ has the spectral decomposition $\hat{A}_i = a_1^i\hat{P}_1^i + a_2^i\hat{P}_2^i + a_3^i\hat{P}_3^i$, where $\hat{P}_1^i, \hat{P}_2^i, \hat{P}_3^i$ are mutually orthogonal projectors. Similarly, the observable $\hat{B}_j$ has the spectral decomposition $\hat{B}_j = b_1^j\hat{Q}_1^j + b_2^j\hat{Q}_2^j + b_3^j\hat{Q}_3^j$ and the observable $\hat{C}_k = c_1^k\hat{R}_1^k + c_2^k\hat{R}_2^k + c_3^k\hat{R}_3^k$ where $\hat{Q}_\zeta^j$ as well as $\hat{R}_\zeta^k$ $(\zeta = 1,2,3)$ are mutually orthogonal projectors.

The probability of obtaining the set of three numbers $(a_{l_i}^i, b_{m_j}^j, c_{n_k}^k)$ in a simultaneous measurement of observables $\hat{A}_i, \hat{B}_j, \hat{C}_k$ on the state ρ is denoted by $P_{QM}(a_{l_i}^i, b_{m_j}^j, c_{n_k}^k)$, where l_i, m_j, n_k assumes the values $1,2,3$, and is given by the standard formula

$$P_{QM}(a_{l_i}^i, b_{m_j}^j, c_{n_k}^k) = Tr(\rho\hat{P}_{l_i}^i \otimes \hat{Q}_{m_j}^j \otimes \hat{R}_{n_k}^k). \quad (7)$$

According to quantum theory, everything that can be measured in this gedanken experiment is given by the set of these $8 \times 27 = 216$ probabilities.

Local realistic (classical) description of the above experiment is equivalent to the existence of a joint probability distribution from which the quantum probabilities $P_{QM}(a_{l_i}^i, b_{m_j}^j, c_{n_k}^k)$ can be derived as the marginals. Let us denote this hypothetical joint probability distribution by $W_{LR}(a_{l_1}^1, a_{l_2}^2; b_{m_1}^1, b_{m_2}^2; c_{n_1}^1, c_{n_2}^2)$. Thus, a local realistic description of the experiment exists *if and only if* the following marginals

$$P_{LR}(a_{l_i}^i, b_{m_j}^j, c_{n_k}^k) = \sum_{l_{i+1}=1}^{3} \sum_{m_{j+1}=1}^{3} \sum_{n_{k+1}=1}^{3} P_{LR}(a_{l_1}^1, a_{l_2}^2; b_{m_1}^1, b_{m_2}^2; c_{n_1}^1, c_{n_2}^2) \quad (8)$$

are equal to the quantum probabilities, i.e., $P_{LR}(a_{l_i}^i, b_{m_j}^j, c_{n_k}^k) = P_{QM}(a_{l_i}^i, b_{m_j}^j, c_{n_k}^k)$ where the addition on the indices is computed using modulo 2 arithmetics.

Owing to (8), $P_{LR}(a_l^i, b_m^j, c_n^k)$ must obey the following inequality

$$-\Gamma_{221} - \Gamma_{111} + 2\Gamma_{122} + \Gamma'_{121} - \Gamma'_{212} + \Gamma''_{211} + \Gamma''_{222} + \Gamma''_{112} \leq 3, \quad (9)$$

where

$$\Gamma_{ijk} = \sum_{l+m+n=1 \ mod\ 3} P_{LR}(a_l^i, b_m^j, c_n^k)$$
$$\Gamma'_{i'j'k'} = \sum_{l+m+n=0 \ mod\ 3} P_{LR}(a_1^{i'}, b_1^{j'}, c_2^{k'})$$
$$\Gamma''_{i''j''k''} = \sum_{l+m+n=2 \ mod\ 3} P_{LR}(a_1^{i''}, b_1^{j''}, c_2^{k''}), \quad (10)$$

and $(i,j,k) = (221,111,122)$, $(i',j',k') = (121,212)$, $(i'',j'',k'') = (211,222,112)$. This is the Clauser-Horne-Bell inequality for three qutrits. It must be obeyed by any local realistic theory that claims to reproduce the correlations generated by three qutrits.

To prove the inequality in (10), we first replace the marginals in the left hand side of the inequality in (10) by the appropriate sums of joint probabilities given in (8). Naturally, we get an extremely long expression in which the joint probabilities $P_{LR}(a_{l_1}^1, a_{l_2}^2; b_{m_1}^1, b_{m_2}^2; c_{n_1}^1, c_{n_2}^2)$

appear only with coefficients -3, 0 or 3 and nothing else. Since the sum of all joint probabilities adds to one, i.e., $\sum_{a_{l_1}^1,a_{l_2}^2,b_{m_1}^1,b_{m_2}^2,c_{n_1}^1,c_{n_2}^2=1}^{3} P_{LR}(a_{l_1}^1,a_{l_2}^2;b_{m_1}^1,b_{m_2}^2;c_{n_1}^1,c_{n_2}^2)$ $=1$, it follows immediately that the entire expression is less than or equal to 3.

We should stress at this point that the above inequality is a member of the set of inequalities that can obtained from (10) by permutations of indices enumerating the outcomes of the measurements as well as the permutations of indices enumerating the observables.

Suppose Akira, Bento and Chiko measure observables defined by unbiased symmetric six-port beamsplitters [8] on the maximally entangled state of three qutrits $|\psi\rangle = \frac{1}{\sqrt{3}}(|111\rangle + |222\rangle + |333\rangle)$.

The matrix elements of an unbiased symmetric six-port beamsplitter are given by $U_{kl}(\vec{\phi}) = \frac{1}{\sqrt{3}}\alpha^{(k-1)(l-1)}\exp(i\phi_l)$, where $\vec{\phi} = (\phi_1,\phi_2,\phi_3)$ and ϕ_l $(k,l=1,2,3)$ are the settings of the appropriate phase shifters (for convenience we denote them as a three dimensional vector $\vec{\phi}$) and $\alpha = \exp(\frac{2i\pi}{3})$.

The observables measured by Akira, Bento and Chiko are now defined as follows. The set of projectors for Alice's i-th experiment is given by $\hat{P}_l^i = U_A^\dagger(\vec{\phi}_i)|l\rangle\langle l|U_A(\vec{\phi}_i)$ $(l=1,2,3)$, where $U_A(\vec{\phi}_i)$ is the matrix of Akira's unbiased symmetric six-port beamsplitter defined by the set of phases $\vec{\phi}_i = (\phi_1^i,\phi_2^i,\phi_3^i)$, Bento's set of projectors j-th experiment is given by $\hat{Q}_m^j = U_B^\dagger(\vec{\psi}_j)|m\rangle\langle m|U_B(\vec{\psi}_j)$, where $\vec{\psi}_j = (\psi_1^j,\psi_2^j,\psi_3^j)$ is a set of Bento's phases defining his unbiased symmetric six-port beamsplitter, whereas Chiko's projectors in the k-th experiment is given by $\hat{R}_n^k = U_C^\dagger(\vec{\delta}_k)|n\rangle\langle n|U_C(\vec{\delta}_k)$, where $\vec{\delta}_k = (\delta_1^k,\delta_2^k,\delta_3^k)$ is a set of Chiko's phases defining her unbiased symmetric six-port beamsplitter.

To each result of the measurement of the projectors $\hat{P}_n^i, \hat{Q}_n^j, \hat{R}_n^k$ for any i,j,k we ascribe the complex number α^n $(n=1,2,3)$, namely $a_{l_1}^1, a_{l_2}^2, b_{m_1}^1, \ldots$ have been assigned the values $\alpha^{l_1},\alpha^{l_2},\alpha^{m_1},\ldots$ respectively. This special assignment was first used in Ref. [8] to generalize the Bell experiment for higher dimensions.

In this way, the probability of getting the set of three numbers $(a_{l_i}^i, b_{m_j}^j, c_{n_k}^k)$ can now be computed using the formula (7). However, note that we need to use the following property regarding these probabilities. All the probabilities $W_{QM}(a_{l_i}^i, b_{m_j}^j, c_{n_k}^k)$ can be sorted into three groups consisting of nine equal probabilities. The first group consists of the probabilities for which $l_i + m_j + n_k = 1 \bmod 3$, the second one consists of the probabilities for which $l_i + m_j + n_k = 2 \bmod 3$ and the third one consists of the probabilities for which $l_i + m_j + n_k = 0 \bmod 3$. Let us denote each probability (they are equal, so it suffices to take an arbitrary one as a representative of the whole group) from the first group by $P_{QM}^1(ijk)$, from the second one by $P_{QM}^2(ijk)$ and from the third one by $P_{QM}^3(ijk)$. It is obvious that we have $P_{QM}^1(ijk) + P_{QM}^2(ijk) + P_{QM}^3(ijk) = \frac{1}{9}$ for any triple i,j,k.

Let us now define the following correlation function (for details see [8]) for each triple of experiments that we denote by Q_{ijk}

$$Q_{ijk} = \sum_{l_i,m_j,n_k=1}^{3} \alpha^{l_i+m_j+n_k} P_{QM}(a_{l_i}^i, b_{m_j}^j, c_{n_k}^k) \quad (11)$$

Using the explicit form of the probabilities, it can be shown easily that such correlation function acquires the following symmetric form

$$Q_{ijk} = \frac{1}{3}(\exp(\phi_1^i - \phi_2^i + \psi_1^j - \phi_2^j + \delta_1^k - \delta_2^k) + \exp(\phi_2^i - \phi_3^i + \psi_2^j - \phi_3^j + \delta_2^k - \delta_3^k)$$
$$+ \exp(\phi_3^i - \phi_1^i + \psi_3^j - \phi_1^j + \delta_3^k - \delta_1^k)). \quad (12)$$

The splitting of the probabilities into the three groups implies that this correlation function conveys as much information about the experiment as the probabilities themselves. In fact, there is a one-to-one mapping between the correlation function and the probabilities so that the following equations hold

$$P_{QM}^1(ijk) = \frac{1}{27}(1 - \Re Q_{ijk} + \sqrt{3}\Im Q_{ijk})$$
$$P_{QM}^2(ijk) = \frac{1}{27}(1 - \Re Q_{ijk} - \sqrt{3}\Im Q_{ijk})$$
$$P_{QM}^3(ijk) = \frac{1}{9} - P_{QM}^1(ijk) - P_{QM}^2(ijk). \quad (13)$$

Putting the probabilities expressed by the equations (13) into the Clauser-Horne-Bell inequality (10), we obtain the following inequality (which is totally equivalent to (10) in the case considered here)

$$\Re[Q_{121} - Q_{212} + \alpha\,(Q_{112} + Q_{211} + Q_{222}) + \alpha^2\,(2Q_{122} - Q_{111} - Q_{221})] \leq 3 \qquad (14)$$

For an appropriate choice of phase shifts: $\vec{\phi}_1 = (0, 0, \frac{2\pi}{3}), \vec{\phi}_2 = (0, 0, 0), \vec{\psi}_1 = (0, 0, \pi), \vec{\psi}_2 = (0, 0, \frac{5\pi}{3}), \vec{\delta}_1 = (0, \frac{\pi}{3}, 0), \vec{\delta}_2 = (0, \pi, 0)$, the values of the correlation function computed using the above phase shifts read $Q_{111} = \frac{1}{3}(1 + \alpha^2), Q_{112} = \frac{2}{3}\alpha^2, Q_{121} = \frac{2}{3}, Q_{122} = -\frac{2}{3}(1 + \alpha^2), Q_{211} = \frac{2}{3}\alpha^2, Q_{212} = -\frac{1}{3}, Q_{221} = -\frac{1}{3}\alpha, Q_{222} = \frac{2}{3}\alpha^2$. Putting them into the left hand side of the inequality in (14) we arrive at a violation of the inequality in which the left hand side is equal to 5.

In Ref. [2], a proposal was made to measure the strength of violation of local realism by the minimal amount of noise that must be added to the system in order to hide the non-classical character of the observed correlations. This is equivalent to a replacement of the pure state $|\psi\rangle\langle\psi|$ by the mixed state $\rho(F)$ of the form $\rho(F) = (1 - F)|\psi\rangle\langle\psi| + \frac{F}{27} I \otimes I \otimes I$, where I is an identity matrix and where F $(0 \leq F \leq 1)$ is the amount of noise present in the system.

It can be checked immediately that such addition of the noise in the gedenken experiment considered here changes the correlation function Q_{ijk} to $Q^F_{ijk} = (1 - F)Q_{ijk}$. Therefore, the minimal amount of noise F_{min} that must be added to the system to conceal the non-classicality of quantum correlations is $F_{min} = \frac{4}{10}$, which is consistent with the numerical results presented in Ref. [6].

THREE TWO-DIMENSIONAL SYSTEM THAT GENERALIZES GISIN'S THEOREM

In 1991 Gisin presented a theorem, which states that *any* pure entangled state of two particles violates a Bell inequality for two-particle correlation functions [9][10]. Bell's inequalities for systems of more than two qubits are the object of renewed interest, motivated by the fact that entanglement between more than two quantum systems is becoming experimentally feasible. Recent investigations show a surprising result that there exists a family of pure entangled $N > 2$ qubit states that do not violate any Bell inequality for N-particle correlations for the case of a standard Bell experiment on N qubits [11]. By a standard Bell experiment we mean the one in which each local observer is given a choice between two dichotomic observables [12][13]. This family is the generalized GHZ states given by

$$|\psi\rangle_{GHZ} = \cos\xi|0\cdots0\rangle + \sin\xi|1\cdots1\rangle \qquad (15)$$

with $0 \leq \xi \leq \pi/4$. The GHZ states [?] are for $\xi = \pi/4$. In 2001, Scarani and Gisin noticed that for $\sin 2\xi \leq 1/\sqrt{2^{N-1}}$ the states (15) do not violate the Mermin-Ardehali-Belinskii-Klyshko (MABK) inequalities. Based on which, Scarani and Gisin wrote that "this analysis suggests that MK [in Ref. [12], MABK] inequalities, and more generally the family of Bell's inequalities with two observables per qubit, may not be the 'natural' generalizations of the CHSH inequality to more than two qubits" [11]. In Ref. [13] Żukowski and Brukner (and Werner and Wolf))have derived a general Bell inequality, also known as ZB inequality, for correlation functions for N qubits. The ZB inequalities include MABK inequalities as special cases. Ref. [12] shows that (a) For N = even, although the generalized GHZ state (15) does not violate MABK inequalities, it violates the ZB inequality and (b) For $\sin 2\xi \leq 1/\sqrt{2^{N-1}}$ and N = odd, the correlations between measurements on qubits in the generalized GHZ state (15) satisfy all Bell inequalities for correlation functions, which involve two dichotomic observables per local measurement station.

We next study a three-qubit system, whose corresponding generalized GHZ state reads $|\psi\rangle_{GHZ} = \cos\xi|000\rangle + \sin\xi|111\rangle$. Up to now, there is no Bell inequality violated by this pure entangled state for the region $\xi \in (0, \pi/12]$ based on the standard Bell experiment. Can Gisin's theorem be generalized to 3-qubit pure entangled states? Can one find a Bell inequality that violates $|\psi\rangle_{GHZ}$ for the whole region?

To see this we need to consider the classification of N-qubit entanglement via quadratic Bell inequality consisting of MABK polynomials has been presented in Ref. [?]. For $N = 3$, there are three types of 3-qubit states: i) totally separable states denoted as (1_3)={ mixtures of states of form $\rho_A \otimes \rho_B \otimes \rho_C$}; ii) 2-entangled states which are denoted as $(2, 1)$={mixtures of states of form $\rho_A \otimes \rho_{BC}, \rho_{AC} \otimes \rho_B, \rho_{AB} \otimes \rho_C$}; iii) fully entangled states which are denoted as $(3) = \{\rho_{ABC}\}$ including the GHZ state. Ref. [?] has drawn an ancient Chinese coin (ACC) diagram for the classification of 3-qubit entanglement. However, for the four points located on the four corners of the square, some of the above three types of 3-qubit states coexist. For instance, the totally separable states and the generalized GHZ states for $\xi \in (0, \pi/12]$ coexist at these four corners, it looks somehow that these four points are "degenerate".

There are two different entanglement classes for 3-qubit states, namely, 2-entangled states and fully entangled states. Why MABK inequalities as well as ZB inequalities fail for the region $\xi \in (0, \pi/12]$ maybe due to the reason that their inequalities contain only fully 3-particle correlations. If one expands $\hat{P}(a_i = m) \otimes \hat{P}(b_j = n) \otimes \hat{P}(c_k = l)$ and substitutes them into the Bell quan-

tity $\mathcal{B}$, one will find that $\mathcal{B}$ contains not only the terms of fully 3-particle correlations, such as $\hat{n}_{a_i}\cdot\vec{\sigma}\otimes\hat{n}_{b_j}\cdot\vec{\sigma}\otimes\hat{n}_{c_l}\cdot\vec{\sigma}$, but also the terms of 2-particle correlations, such as $\hat{n}_{a_i}\cdot\vec{\sigma}\otimes\hat{n}_{b_j}\cdot\vec{\sigma}\otimes\mathbf{1}$. The above theorem implies that 2-particle correlations may make a contribution to the quantum violation of Bell inequality.

We introduce a Bell inequality with all possible probabilities:

$$\begin{aligned}
&P(a_1+b_1+c_1=1)+2P(a_2+b_2+c_2=1)\\
&+P(a_1+b_2+c_2=2)+P(a_2+b_1+c_2=2)+P(a_2+b_2+c_1=2)\\
&-P(a_1+b_1+c_2=0)-P(a_1+b_2+c_1=0)-P(a_2+b_1+c_1=0)\\
&-P(a_1+b_1+c_2=3)-P(a_1+b_2+c_1=3)-P(a_2+b_1+c_1=3)\le 3. \qquad (16)
\end{aligned}$$

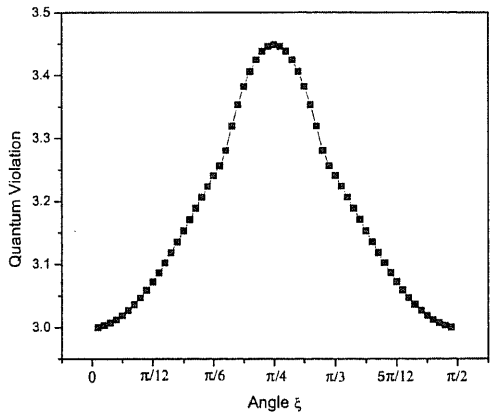


FIG. 1: Numerical results for the generalized GHZ states $|\psi\rangle_{GHZ}=\cos\xi|000\rangle+\sin\xi|111\rangle$, which violate Bell inequality for probabilities (16) except $\xi=0$ and $\pi/2$. For the GHZ state with $\xi=\pi/4$, the Bell quantity reaches its maximum value $\frac{3}{8}(4+3\sqrt{3})$.

This inequality is symmetric under the permutations of three observers Alice, Bob and Charlie. Pure states of three qubits constitute a five-parameter family, with equivalence up to local unitary transformations. This family has the representation [1]

$$\begin{aligned}
|\psi\rangle &= \sqrt{\mu_0}|000\rangle+\sqrt{\mu_1}e^{i\phi}|100\rangle+\sqrt{\mu_2}|101\rangle\\
&\quad+\sqrt{\mu_3}|110\rangle+\sqrt{\mu_4}|111\rangle \qquad (17)
\end{aligned}$$

with $\mu_i\ge 0$, $\sum_i\mu_i=1$ and $0\le\phi\le\pi$. Numerical results show that this Bell inequality for probabilities is violated by all pure entangled states of three-qubit system. However, it is difficult to provide an analytic proof.

In Fig.1, we show the numerical results for the generalized GHZ states $|\psi\rangle_{GHZ}=\cos\xi|000\rangle+\sin\xi|111\rangle$, which violate the above symmetric Bell inequality for

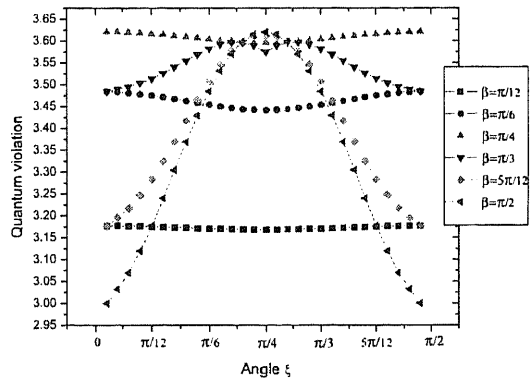


FIG. 2: Numerical results for the family of generalized W states $|\psi\rangle_W=\sin\beta\cos\xi|100\rangle+\sin\beta\sin\xi|010\rangle+\cos\beta|001\rangle$ with the cases $\beta=\pi/12,\pi/6,\pi/4,\pi/3,5\pi/12$ and $\pi/2$.

probabilities except $\xi=0$ and $\pi/2$. For the measuring angles $\theta_{a_1}=\theta_{a_2}=\theta_{b_1}=\theta_{b_2}=\theta_{c_1}=\theta_{c_2}=\pi/2,\phi_{a_1}=-5\pi/12,\phi_{a_2}=\pi/4,\phi_{b_1}=-5\pi/12,\phi_{b_2}=\pi/4,\phi_{c_1}=-\pi/3,\phi_{c_2}=\pi/3$, all the probability terms with positive signs in Bell inequality (16) are equal to $\frac{3}{16}(2+\sqrt{3})$, while the terms with negative signs are equal to $\frac{1}{8}$, so the quantum violation of Bell quantity for the GHZ state (where $\xi=\pi/4$) is obtained as $6\times\frac{3}{16}(2+\sqrt{3})-6\times\frac{1}{8}=\frac{3}{8}(4+3\sqrt{3})>3$. In Fig.2, we show the numerical results for the family of generalized W states $|\psi\rangle_W=\sin\beta\cos\xi|100\rangle+\sin\beta\sin\xi|010\rangle+\cos\beta|001\rangle$ with the cases $\beta=\pi/12,\pi/6,\pi/4,\pi/3,5\pi/12$ and $\pi/2$, which show the quantum violation of $|\psi\rangle_W$ except the product cases with $\beta=\pi/2,\xi=0$ and $\pi/2$. For the standard W state $|\psi\rangle_W=(|100\rangle+|010\rangle+|001\rangle)/\sqrt{3}$, the quantum violation is 3.55153. We now proceed to present the second theorem.

For pure 2-entangled states of three-qubit system, we need to consider the following: $|\psi_{AB}\rangle\otimes|\psi_C\rangle$, $|\psi_{AC}\rangle\otimes|\psi_B\rangle$

and $|\psi_{BC}\rangle \otimes |\psi_A\rangle$. It is however sufficient to consider only one of them, say $|\psi_{AB}\rangle \otimes |\psi_C\rangle$, since Bell inequality (16) is symmetric under the permutations of A, B and C. Moreover, one can always have $|\psi_{AB}\rangle \otimes |\psi_C\rangle = (\cos\xi|00\rangle_{AB} + \sin\xi|11\rangle_{AB}) \otimes |0\rangle_C$ due to local unitary transformations. For the measuring angles $\theta_{a_1} = \theta_{a_2} = \theta, \phi_{a_1} = 2\pi/3, \phi_{a_2} = -\pi/3, \theta_{b_1} = \theta_{c_1} = 0, \phi_{b_1} = \phi_{c_1} = 0, \theta_{b_2} = \pi/2, \theta_{c_2} = \pi, \phi_{b_2} = \pi/3, \phi_{c_2} = 0$, we obtain from the left-hand side of Bell inequality (16) that

$$\begin{aligned} \mathcal{B} &= \frac{3}{2}(1 - \cos\theta + \sin(2\xi)\sin\theta) \\ &\geq \frac{3}{2}(1 + \sqrt{1 + \sin^2(2\xi)}), \end{aligned} \tag{18}$$

the equal sign occurs at $\theta = -\tan^{-1}[\sin(2\xi)]$. Obviously the Bell inequality is violated for any $\xi \neq 0$ or $\pi/2$. This ends the proof. Indeed, the quantum violation of the state $|\psi_{AB}\rangle \otimes |\psi_C\rangle$ corresponds to the curve with $\beta = \pi/2$ as shown in Fig.2, because $|\psi_{AB}\rangle \otimes |\psi_C\rangle$ is equivalent to $|\psi\rangle_W$ for $\beta = \pi/2$ up to a local unitary transformation.

There is a simpler and more intuitive way to show that 2-entangled states violate the three-qubit Bell inequality: the symmetric Bell inequality (16) can be reduced to a CHSH-like inequality for two qubits and then from Gisin's theorem for two qubits one easily deduce the result. Indeed, by taking $c_1 = 0, c_2 = 1$, we have from Eq. (16) that

$$\begin{aligned} &P(a_1 + b_1 = 1) + 2P(a_2 + b_2 = 0) \\ &+P(a_1 + b_2 = 1) + P(a_2 + b_1 = 1) + P(a_2 + b_2 = 2) \\ &-P(a_1 + b_1 = -1) - P(a_1 + b_2 = 0) - P(a_2 + b_1 = 0) \\ &-P(a_1 + b_1 = 2) - P(a_1 + b_2 = 3) - P(a_2 + b_1 = 3) \leq 2 \end{aligned} \tag{19}$$

Since $a_1, a_2, b_1, b_2 = 0, 1$, the probabilities $P(a_1 + b_1 = -1)$, $P(a_1 + b_2 = 3)$ and $P(a_2 + b_1 = 3)$ will be equal to zero, by using $P(a_2 + b_2 = 0) + P(a_2 + b_2 = 2) = 1 - P(a_2 + b_2 = 1)$, we arrive at the following Bell inequality for two-qubit:

$$\begin{aligned} &P(a_1 + b_1 = 1) + P(a_1 + b_2 = 1) + P(a_2 + b_1 = 1) + P(a_2 + b_2 = 0) \\ &-P(a_1 + b_1 = 2) - P(a_1 + b_2 = 0) - P(a_2 + b_1 = 0) - P(a_2 + b_2 = 1) \leq 2. \end{aligned} \tag{20}$$

This Bell inequality is symmetric under the permutations of Alice and Bob, it is an alternative form for CHSH inequality of two qubits. For the two-qubit state $|\psi\rangle = \cos\xi|00\rangle + \sin\xi|11\rangle$ and the projector as shown in Eq.(??), one can have the quantum probability

$$\begin{aligned} &P^{QM}(a_i = m, b_j = n) \\ &= \frac{1}{4}\cos^2\xi[1 + (-1)^m\cos\theta_{a_i}][1 + (-1)^n\cos\theta_{b_j}] \\ &+\frac{1}{4}\sin^2\xi[1 - (-1)^m\cos\theta_{a_i}][1 - (-1)^n\cos\theta_{b_j}] \\ &+\frac{1}{4}\sin(2\xi)(-1)^{m+n}\sin\theta_{a_i}\sin\theta_{b_j}\cos(\phi_{a_i} + \phi_{b_j}) \end{aligned} \tag{21}$$

For the measuring angles $\theta_{a_1} = \theta_{a_2} = \theta, \phi_{a_1} = \pi - \phi, \phi_{a_2} = -\phi, \theta_{b_1} = 0, \phi_{b_1} = 0, \theta_{b_2} = \pi/2, \phi_{b_2} = \phi$, the left-hand side of Bell inequality (20) becomes $\mathcal{B} = \frac{1}{2} + \frac{3}{2}(-\cos\theta + \sin(2\xi)\sin\theta) \geq \frac{1}{2}(1 + 3\sqrt{1 + \sin^2(2\xi)})$, the equal sign occurs at $\theta = -\tan^{-1}[\sin(2\xi)]$. Obviously the Bell inequality (20) is violated for any $\xi \neq 0$ or $\frac{\pi}{2}$, just the same as CHSH inequality violated by the 2-qubit state $|\psi\rangle = \cos\xi|00\rangle + \sin\xi|11\rangle$. For the Werner state $\rho_W = V|\psi\rangle\langle\psi| + (1 - V)\rho_{\text{noise}}$, where $|\psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is the maximally entangled state. The maximal value of V that a local realism is still possible by this Bell inequality is $V_{max} = 1/\sqrt{2}$, just the same as the case for CHSH inequality. Actually, if one denotes the left-hand side of Bell inequality (20) by $\mathcal{B}$ and redefines a new Bell quantity $\mathcal{B}' = \frac{4}{3}(\mathcal{B} - \frac{1}{2})$, he still has the Bell inequality $\mathcal{B}' \leq 2$. For quantum mechanics, $\mathcal{B}'_{max} = 2\sqrt{1 + \sin^2(2\xi)}$, which reaches $2\sqrt{2}$ and then $\mathcal{B}'$ recovers the usual CHSH inequality.

In summary, (i) since all pure entangled states (including pure 2-entangled states) of three-qubit system violate Bell inequality (16), thus we have Gisin's theorem for 3-qubit system; (ii) the Bell inequality (16) can be reduced to an alternative form of the CHSH inequality (in terms of probabilities), thus it can be viewed as a good candidate for a"natural" generalization of the usual CHSH inequality. (iii) MABK inequalities and ZB inequalities are binary correlation Bell inequalities. However, one may notice that Bell inequalities (4) and (16) are both ternary Bell inequalities, i.e., where the inequalities are "modulo 3". Note that the three-qutrit inequality [1] can be connected to Bell inequality (16), which is for three qubits, if one restricts the initial three possible outcomes of each measurement to only two possible outcomes.

FINAL REMARKS

In this talk, we have summarized some of the recent work done on extending Bell inequalities to three particles.

ACKNOWLEDGMENT

L.C. Kwek would like to thank Prof. Keiji Matsumoto for the invitation to the Quantum Statistics workshop and the organizing committee for their hospitality during his stay in Japan.

---

[1] A. Acin, J.L. Chen, N. Gisin, D. Kaszlikowski, L.C. Kwek, C.H. Oh and M. Zukowski, Phys. Rev. Lett., **92**, 250404 (2004)

[2] D. Kaszlikowski, P. Gnaciński, M. Żukowski, W. Miklaszewski and A. Zeilinger, Phys. Rev. Lett. **85**, 4418 (2000).

[3] T. Durt, D. Kaszlikowski and M. Żukowski, Phys. Rev. A **64** 024101 (2001).

[4] D. Kaszlikowski, L.C. Kwek, J.L. Chen, M. Żukowski and C.H. Oh, quant-ph//0106010 (To be published in Phys. Rev. A).

[5] D. Collins, N. Gisin, N. Linden, S. Massar and S. Popescu, quant-ph//0106024.

[6] D. Kaszlikowski, D. Gosal, E.J. Ling, L.C. Kwek, M. Żukowski and C.H. Oh, quant-ph/0202019.

[9] A. Acin, T. Durt, N. Gisin and J. I. Latorre, quant-ph//0111143.

[8] M. Żukowski, A. Zeilinger, M. A. Horne, Phys. Rev. A **55**, 2564 (1997).

[9] N. Gisin, Phys. Lett. A **154**, 201 (1991); N. Gisin and A. Peres, Phys. Lett. A **162**, 15-17 (1992).

[10] S. Popescu and D. Rohrlich, Phys. Lett. A **166**, 293 (1992).

[11] V. Scarani and N. Gisin, J. Phys. A **34** 6043 (2001).

[12] M. Żukowski, Č. Brukner, W. Laskowski, and M. Wiesniak, Phys. Rev. Lett. **88**, 210402 (2002).

[13] M. Żukowski and Č. Brukner, Phys. Rev. Lett. **88**, 210401 (2002).

最大エンタングルメント状態検出についての一次漸近論について

First order asymptotic theory of testing for maximally entangled state

科学技術振興事業団 ERATO 今井量子計算機構プロジェクト
東京大学大学院 情報理工学系研究科 21 世紀 COE「情報科学技術戦略コア」
林 正人 [1]

現在様々な量子情報処理が提案されているが，その中には，リソースとして最大エンタングルメント状態を必要とするものが多い．したがって，実験的に最大エンタングルメント状態を生成することが望まれることが多い．しかし，実験的に生成された状態が本当に所望の最大エンタングルメント状態であるか否か判断するには，統計的手法が不可欠である．

現在，entanglement witness という手法が用いられることが多いが，これらの方法は必ずしも，統計的視点から見て必ずしも最適な手法とは言えない．一方，数理統計学では与えられた仮説が真であるか否か判断する問題は統計的仮説検定と呼ばれ，系統的に研究がなされている．それゆえ，与えられた量子状態が所望の最大エンタングルメント状態であることを判定する問題についても統計的仮説検定の枠組みで取り扱うことが望まれる．統計的仮説検定では事前に 2 つの仮説（帰無仮説，対立仮説）を仮定し，少なくともどちらかが真であると仮定する．その上で，得られたデータから，どちらの仮説が正しいか判断することになる．これまで，量子状態についての仮説検定では量子ネイマンピアソンの定理，量子 Stein の定理についてのみ扱われたのみであった．これらの設定では帰無仮説，対立仮説がともに 1 つの量子状態からなる場合（単純な場合）のみを扱っていた．

ここで扱っている問題では，双方の仮説を 1 つの量子状態と特定することは不自然である．したがって，量子ネイマンピアソンの定理や量子 Stein の定理をそのままの形で用いることはできず，少なくとも片方の仮説が複数の量子状態からなる場合（composite hypothesis）を扱う必要がある．同時に，取り扱う量子状態が最大エンタングルメント状態であるため，検定のために行える測定を LOCC に限る必要もある．

本研究では帰無仮説，対立仮説の選び方に以下の 3 通りの設定を考える．1) 帰無仮説が所望の最大エンタングルメント状態であり，対立仮説がそれ以外の状態からなる．2) 帰無仮説が所望の最大エンタングルメント状態との fidelity が ϵ 以下の状態であり，対立仮説がその fidelity が ϵ を超える状態である．3) 帰無仮説が所望の最大エンタングルメント状態との fidelity が ϵ を超える状態であり，対立仮説がその fidelity が ϵ 以下の状態である．設定 1) はやや人工的な設定で，他の 2 つに比べると実用的でない．しかし，解析が最も容易であり，多くの場合，この設定での解析を用いて，他の場合での解析が可能となる．

さらに，本稿ではサンプルが複数ある場合では独立性に加えて，サンプルの同一性の a) ある場合 b) 無い場合の双方の設定も検討した．すなわち，本稿では 6 通りの仮説の取り方を扱った．さらに，検定のために行う測定に対する制約についても，複数検討し，扱った．そして，これらの設定の下で，対立仮説の全ての要素に渡って一様に最適な検定方式（一様最強力検定）の有無を調べ，最適な場合での検定の性能について調べた．

具体的には検定のために用いる測定に全く条件を課さない場合を扱う．ここで扱う議論は，後の節の議論のための準備となるので重要である．そして，独立かつ同一に量子状態（サンプル）が

[1]E-mail: masahito@qci.jst.go.jp

準備された設定を考えた．特に，遠隔にある二者（Alice,Bob）間に跨る量子操作のみ禁止されており，独立に準備された状態間の操作は許されている設定を漸近論の枠組みで扱った．ただ，漸近論といっても少なくとも2通りの設定がある．1つは大偏差理論と呼ばれるものであり，対立仮説の形を独立に準備される状態数 n に依存せずに，極限を考えるものである．この場合，誤り確率は指数的に減少する．一方，小偏差理論では，状態数 n に依存して，対立仮説である量子状態を帰無仮設である最大エンタングルメント状態に近づけながら，誤り確率の極限を考えるものである．これらの2つの設定の下でともに漸近的に一様最強力検定が存在することを示した．特に小偏差理論では，与えられたサンプル数が $2n$ である場合，漸近的に一様最強力な検定は，全サンプルを2つのサンプルからなる n 個の組に分け，個々の組から2粒子系について Alice, Bob で同一のベル測定を行うという操作を n 個の組について繰り返すことで実現できることを示した．なお，このプロトコルに必要な測定は local operation のみで実現できる．

次にサンプル数が1または2の場合について扱った．これらの場合では，Alice, Bob 間について LOCC の制限を課すと，一様最強力な検定は存在しない．しかし，LOCC の制限に加え，対立仮説が持つ対称性に注目し，対立仮説を不変にする群の作用に注目し，これらの群の作用に関する不変性を検定にも課すことにした．その結果，サンプルが1つの場合には，一様に最強力な検定が存在することが示せる．この議論は本質的に Virmani&Plenio の議論と同じである．一方，サンプルが2つの場合では，少なくとも4つの問題設定を考えることが出来る．1つは対称性に関する議論であり，サンプルに対して独立性のみを仮定した場合での対称性についての不変性を検定に課した場合と独立性に加えて同一性まで課した場合での対称性についての不変性を検定に課す場合の2通り不変性に関する設定がある．この場合，後に詳しく述べるが，前者が $SU(d) \times SU(d)$ 群の作用を考えることになり，後者が $SU(d)$ 群の作用を考えることになる．（なお，d は空間の次元である．）さらに，Alice, Bob 間について LOCC の制限を考えているが，これに加えて，2つのサンプル間についての LOCC の制限を課すか否かで2通りの設定を考えることができる．したがって，サンプル間の LOCC の制限の有無と，対立仮説に対する仮定として，同一性の仮定の有無で，4通りの設定を考えることができる．

その結果，$SU(d) \times SU(d)$ 群の不変性を課した場合，サンプル間の LOCC の制限の有る場合，無い場合の双方の場合について，一様最強力検定が存在することを示した．一方，$SU(d)$ 群の不変性を課した設定では一般次元での解析は困難であるので，本稿では $d = 2$ の場合のみを扱った．その結果，サンプル間の LOCC の制限が無い場合では，一様最強力検定が存在することを示した．一方，サンプル間の LOCC の制限が有る場合では極めて解析が難しいので，より強い仮定を置くことで，一様最強力検定が存在することを示した．

なお，本研究は津田美幸，松本啓史氏との共同研究を一部含む．

Hypothesis Testing for Entanglement

Yoshiyuki Tsuda*, Bao-Sen Shi‡, Akihisa Tomita‡,
Masahito Hayashi‡, Keiji Matsumoto‡,§, and Yun Kun Jiang†
*COE, Chuo University, Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan
†Imai Quantum Computation and Information Project, ERATO,
Japan Science and Technology Agency (JST), Tokyo 113-0033, Japan
‡National Institute of Informatics, Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

(Dated: January 6, 2005)

We propose a practical procedure to test performance of a device which produces entangled photon pairs by SPDC. Our new test is demonstrated in an optical experiment.

最近, 量子力学的性質を活用して情報処理系の古典的限界を打破しようとする量子情報科学の研究が注目されている. 量子情報において量子的状態の非局所性 (entanglement) は重要な役割を担っている. 光子偏光は量子情報処理を実装する物理系として最も有望な候補の一つであり, SPDC は高度に entangle した光子対を生成する標準的な手法である. 本稿では, SPDC で生成した状態の entanglement に関する仮説検定を考え, 高精度で実用的な検定方式を提案し, 物理実験によりその有効性を確かめる.

SPDC で生成される状態は

$$\bigoplus_{n=0}^{\infty} \exp(-\lambda t)\frac{(\lambda t)^n}{n!}\rho^{\otimes n}$$

で記述される. ただし, λ は生成される光子対の単位時間当たりの平均数で, t は光の生成時間, ρ は 2 光子偏光状態の密度作用素である. λ は既知, t は選択可能, ρ は未知とする. 系の entanglement を表す指標として,

$$\theta = \langle \Phi^+ | \rho | \Phi^+ \rangle$$

を用いる. ただし, $|\Phi^+\rangle = 2^{-1/2}(|H\rangle|H\rangle + |V\rangle|V\rangle)$ (最大 entangled 状態ベクトル) である. 適切な有意水準 α に対して, 仮説

$$H_0 : \theta \leq \theta_0 \text{ versus } H_1 : \theta > \theta_0$$

を検定する. ただし, 系の測定は以下の基底に関する coincidence 測定に限る:

$$|HV\rangle, |VH\rangle, |DX\rangle, |XD\rangle, |RR\rangle, |LL\rangle.$$

ここで,

$$|D\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}},\ |X\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}},$$
$$|R\rangle = \frac{|H\rangle + \sqrt{-1}|V\rangle}{\sqrt{2}},\ |L\rangle = \frac{|H\rangle - \sqrt{-1}|V\rangle}{\sqrt{2}}$$

とする. すると我々の問題は, 6つの独立なPoisson分布のモデル

$$X_{xy} \sim \mathrm{Poi}(t_{xy}\mu_{xy})$$

$(x, y \in \{H, V, D, X, R, L\})$ において, 単位時間当たりの平均個数 μ_{xy} の和

$$\mu = \mu_{HV} + \mu_{VH} + \mu_{DX} + \mu_{XD} + \mu_{RR} + \mu_{LL}$$

に関する仮説

$$H_0 : \mu \geq \mu_0 \text{ versus } H_1 : \mu < \mu_0$$

を検定する問題になる. ただし, $\mu_{xy} = \langle x|\langle y|\rho|x\rangle|y\rangle\eta\lambda$ であり, η は光子検出器の量子効率に依存する量である. η は既知とする. θ と μ の関係は

$$\eta\lambda\frac{1-\theta}{3} = \mu$$

で与えられる. 各測定基底を利用する時間の配分が定まれば, 尤度比検定がPitman効率を最大にするという意味で漸近的に最適である. その検出力を最大にする時間配分はNeyman配分で与えられる. しかし, そのNeyman配分は未知の ρ に依存する. そこで, 2段階法を用いて, 漸近的にNeyman配分に基づく測定を行い, 検定する. すなわち, 利用可能な全時間 t のうち, 初めの $\log t$ を用いてNeyman配分を推定し, 残りの $t - \log t$ を推定された配分に基づく測定にあてる.

実験では, $t = 240$ 秒とした.

まず, Neyman配分を用いない場合, 各 t_{xy} は40秒とするのが自然である. この場合, 最尤法による μ の95%片側信頼区間は $\mu < 72.6$ となった.

一方, 各基底を1秒ずつ測定すると, 残りの時間 $240 - 6 = 234$ のNeyman配分の推定値は

HV	VH	DX	XD	RR	LL
25	19	48	45	49	48

となった. これに基づいた測定による μ の95%片側信頼区間は $\mu < 71.7$ となった.

$\theta_0 = 0.75$ とすると $\mu_0 = 72.5$ である. この場合, Neyman配分によらない検定では H_0 を棄却できないが, Neyman配分による検定は H_0 を棄却する.

Quantum state discrimination and estimation via linear optics

Peter van Loock
Quantum Information Science Group,
National Institute of Informatics (NII),
2-1-2 Hitotsubashi, Chiyodaku, Tokyo, Japan
email: vanloock@nii.ac.jp
fax: +81 (3) 4212 2568

We propose a set of sufficient conditions for implementing unambiguous discrimination of two nonorthogonal states. The implementation is assumed to be based upon a static array of linear optics without feedforward. These conditions are then sufficient for the linear-optics implementation of a POVM that contains at least one conclusive element corresponding to the error-free identification of either of the two states. Such a POVM may be either that for the optimal unambiguous state discrimination or one that approximates the optimal scheme. Only in the case of orthogonal states, the conditions become necessary and sufficient for optimality. In general, these criteria are necessary and sufficient for any implementation based upon an inconclusive (failure) POVM element that is represented by at most one photon number pattern. A scheme with only one failure pattern corresponds to the simplest extension of the exact discrimination of orthogonal states, requiring zero failure pattern, to the unambiguous discrimination of states with some finite overlap. We further investigate the linear-optics implementation of POVMs for quantum state estimation.

PACS numbers: 03.67.Hk, 42.25.Hz, 42.50.Dv

keywords: linear-optics quantum information processing, quantum state discrimination

As for the implementation of a given task in quantum information processing, for instance, the application of a unitary gate in a quantum computation or the generalized measurement (POVM) of a set of signal states in quantum communication, there are two different types of approaches. On the one hand, one may ask what the minimal requirements in terms of physical resources are when the goal is unit efficiency, i.e., perfect performance. On the other hand, a very important scenario concerning implementation is when the set of physical resources is fixed and limited, and the question is how well and to what extent one may fulfil the quantum information task in an approximative scheme.

In an optical implementation, as for the former case, in order to perform a given quantum information task perfectly, for example a general entangling gate or a general POVM, normally a nonlinear interaction (described by a Hamiltonian at least cubic in the optical mode operators [1]) is needed. At present, however, these nonlinear processes are hard to realize on the level of single photons. Alternatively, as a resource, one may build more or less expensive entangled single-photon states off-line, and for performing the task on-line, one can exclusively use linear optics including photon counting and conditional dynamics (feedforward) [2–4]. In the case of the implementation of particular POVMs, namely projection measurements, there are general criteria to decide whether, in principle, unit efficiency is possible using only linear optics [5].

In the second scenario, the set of physical resources is assumed to be fixed and limited, and one accepts that only a finite efficiency is possible. For example, one may be restricted to solely using linear optical elements, reasonably cheap auxiliary states, and postselection *without feedforward*. In some linear-optics proposals, this is exactly the setting for generating the off-line resources via non-deterministic quantum gates. However, it appears to be hard to express such approximative schemes in terms of simple criteria like those of Ref. [5]. More generally, so far, there is no solution to the problem of deciding whether a given POVM, including non-projective ones, can be implemented with linear optics. Here, we will consider a particular example for a non-projective POVM, namely the unambiguous state discrimination (USD) of two nonorthogonal states. It is well-known that two nonorthogonal states cannot be discriminated in a deterministic fashion. However, there is an optimal POVM for the nondeterministic discrimination. In this optimal scheme, the successful measurement outcomes unambiguously refer to either of the signal states, whereas the failure POVM element leads to an inconclusive result. Optimality here means that the probability for obtaining an inconclusive result is as small as allowed by quantum theory. This minimum failure probability is just given by the overlap of the two signal states.

Here we are interested in the question whether USD can be performed with a static array of linear optics. For this purpose, we propose a set of sufficient conditions for

implementing USD of two nonorthogonal states. These conditions are then sufficient for the linear-optics implementation of a POVM that contains at least one conclusive element corresponding to the error-free identification of either of the two states. Such a POVM may be either that for the optimal USD or one that approximates the optimal scheme. Only in the case of orthogonal states, the conditions become necessary and sufficient for optimality. In general, these criteria are necessary and sufficient for any implementation based upon an inconclusive (failure) POVM element that is represented by at most one photon number pattern. A scheme with only one failure pattern corresponds to the simplest extension of the exact discrimination of orthogonal states, requiring zero failure pattern, to the unambiguous discrimination of states with some finite overlap. We further investigate the linear-optics implementation of POVMs for quantum state estimation.

---

[1] S. Lloyd and S. L. Braunstein, Phys. Rev. Lett. **82**, 1784 (1999).

[2] E. Knill, R. Laflamme, and G. J. Milburn, Nature **409**, 46 (2001).

[3] M. A. Nielsen, LANL arXive quant-ph/0402005 (2004).

[4] D. E. Browne and T. Rudolph, LANL arXive quant-ph/0405157 (2004).

[5] P. van Loock and N. Lütkenhaus, Phys. Rev. A **69**, 012302 (2004).

Estimating Quantum Optical States and Processes

W. J. Munro,[1] D. F. V. James,[2] A. G. White,[3] P. G. Kwiat,[4] and A. Gilchrist[3]

[1]*Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS34 8QZ, United Kingdom*
[2]*Theory Division, T-4, Los Alamos National Laboratory, Los Alamos, New Mexico, USA*
[3]*Special Research Centre for Quantum Computer Technology, University of Queensland, Brisbane, Australia*
[4]*Dept. of Physics, University of Illinois, Urbana-Champaign, Illinois, USA.*

(Dated: January 30, 2005)

One of the distinguishing features of quantum mechanics, not found in classical physics, is the possibility of entanglement between subsystems. It lies at the core of many applications in the emerging field of quantum information science, such as quantum teleportation[1] and quantum error correction[2]. Quantum entanglement refers to correlations between the results of measurements made on component subsystems of a larger physical system which cannot be explained in terms of correlations between local classical properties inherent in those same subsystems. Alternatively, an entangled state cannot be prepared by local operations and local measurements on each subsystem. Thus one often says that an entangled composite system is nonseparable.

The nonclassical nature of quantum entanglement has been recognized for many years[3, 4] but only recently has considerable attention been focused on trying to understand and characterize its properties precisely. We now have a good understanding of entanglement for a pair of qubits[5], however, how does one determine the extent to which a real physical few qubit system is entangled? What measurements are actually required? There are a number of possible techniques but arguably the simplest (if not the most efficient) is to perform appropriate measurements to reconstruct the density matrix and then use the theoretical measures currently known. Tomographic techniques, in which the density matrix of a quantum state have been applied to experiments such as the homodyne measurement of the Wigner function of a single mode of light [6] and of the density matrix of the polarization degrees of freedom of a pair of entangled photons[7, 8].

For the characterization of a few qubit quantum computer, quantum state and process tomography provides invaluable information on the system. For quantum states the degree of entanglement and the degree of mixture can be calculated. If one were to consider quantum process tomography (tomography associated with the evolution of the state) then the entangling power of a gate could be determined as well as effects such as decoherence. Two caveats must be made: firstly, there must be a large enough number of copies of an identically prepared quantum system to allow to a reasonable approximation the reconstruction of the state (this may be time consuming in many architectures where the system must be re-initialized after each measurement); secondly, more measurements are preformed in the reconstruction that what is likely to be needed to get the degree of entanglement. However we believe these disadvantages are outweighed by the other information one can obtain from the reconstructed states.

Let us consider an arbitrary n qubit state (shown schematically in Figure (1)).

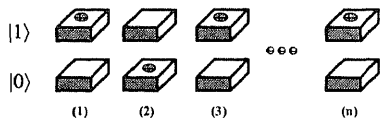


FIG. 1: Schematic representation of an n qubit state.

This n qubit state can be mathematically described by a density matrix of the form,

$$\rho = \frac{1}{2^n} \sum_{i_1,\ldots,i_n=0}^{3} c_{i_1,\ldots,i_n} \lambda_{i_1}^{(1)} \otimes \lambda_{i_2}^{(2)} \otimes \ldots \otimes \lambda_{i_n}^{(n)}, \quad (1)$$

where the λ_i matrices[9] are given by $\lambda_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\lambda_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\lambda_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\lambda_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and the j superscript in $\lambda_i^{(j)}$ labels the qubit. The $c_{i_1,\ldots,i_n}$ are the coefficients that specify the state. There are 4^n of these that need to be determined however the normalization criterion ($Tr(\rho) = 1$) ensures that $c_{0,\ldots,0} = 1$ leaving $4^n - 1$ parameters to be determined or specified . Noting that,

$$\langle \lambda_{i_1}^{(1)} \lambda_{i_2}^{(2)} \ldots \lambda_{i_n}^{(3)} \rangle = \frac{1}{2^n} \quad c_{i_1,\ldots,i_n}, \quad (2)$$

we now observe the procedure to reconstruct the state. By measuring all the expectation values $\langle \lambda_{i_1} \lambda_{i_2} \ldots \lambda_{i_n} \rangle$, for $i_1, i_2, \ldots, i_n = 0, 1, 2, 3$ one determines the coefficients $c_{i_1,\ldots,i_n}$ and hence the state. How we actually measure these expectation values $\langle \lambda_{i_1} \lambda_{i_2} \ldots \lambda_{i_n} \rangle$ depends heavily on the physical architecture. However one can always measure the probability of the system being in the ground state $|0\rangle$. From such measurements we can then calculate expectation values like $\langle \lambda_{i_1} \lambda_{i_2} \ldots \lambda_{i_n} \rangle$ (for $i_i = 0$ *or* 3). With appropriate single qubit rotations: $\hat{U}_j^k(\phi) = \exp\left[-ik\frac{\pi}{2}\left(|1\rangle_j\langle 0|e^{-i\phi} + |0\rangle_j\langle 1|e^{i\phi}\right)\right]$, on the individual qubits (where j label the particular qubit, $k\pi$

is the length of the pulse and ϕ the polarization) followed by the ground state measurement, all the expectation values $\langle \lambda_{i_1} \lambda_{i_2} ... \lambda_{i_n} \rangle$ (for $i_i = 0, 1, 2, 3$) can be determined and hence the state reconstructed. It is easy also to write the reconstructed state directly in terms of these single qubit rotations and ground measurements.

In any real situations, the information used to reconstruct the state will contain uncertainties due to small experimental errors. This errors make it possible that this reconstruction procedure for the state will not produce a physically acceptable state. While the resulting density matrix will be trace preserving and Hermitian, it may process small negative eigenvalues. Using a maximum likelihood technique[10] physically acceptable density matrices can be obtained. Let us now illustrate this procedure with two examples.

A single qubit density matrix can be written as $\rho = \frac{1}{2}\left(I_2 + \sum_{i=1}^{3} c_i \lambda_i\right)$, where I_2 is the 2×2 identity matrix, and the coefficients c_i are given by the measured expectation values $c_i = 2\langle \lambda_i \rangle$. In matrix form this is written as,

$$\rho = \frac{1}{2}\begin{pmatrix} 1 + \langle \lambda_3 \rangle & \langle \lambda_1 \rangle - i\langle \lambda_2 \rangle \\ \langle \lambda_1 \rangle + i\langle \lambda_2 \rangle & 1 - \langle \lambda_3 \rangle \end{pmatrix}. \qquad (3)$$

Let us consider the simplest states that may contain entanglement, namely two qubit states. Such states can be expressed in the form,

$$\rho = \frac{I_2 \otimes I_2}{4} + \sum_{\substack{i_1, i_2 = 0 \\ i_1 = i_2 \neq 0}}^{3} c_{i_1, i_2} \quad \lambda_{i_1}^{(1)} \otimes \lambda_{i_2}^{(2)}. \qquad (4)$$

So by measuring the moments $\langle \lambda_{i_1}^{(1)} \lambda_{i_2}^{(2)} \rangle$, the coefficients c_{i_1, i_2} are determined and hence the density matrix specified. As an example consider the result of the measurement of $\langle \lambda_{i_1}^{(1)} \lambda_{i_2}^{(2)} \rangle$ where the only nonzero zero measurements are given by $\langle \lambda_1^{(1)} \lambda_1^{(2)} \rangle = -\langle \lambda_2^{(1)} \lambda_2^{(2)} \rangle = \langle \lambda_3^{(1)} \lambda_3^{(2)} \rangle = \gamma/4$ and $\langle \lambda_0^{(1)} \lambda_0^{(2)} \rangle = 1/4$. The state is then the Werner state[11] given by,

$$\rho = \begin{pmatrix} \frac{1+\gamma}{4} & 0 & 0 & \frac{\gamma}{2} \\ 0 & \frac{1-\gamma}{4} & 0 & 0 \\ 0 & 0 & \frac{1-\gamma}{4} & 0 \\ \frac{\gamma}{2} & 0 & 0 & \frac{1+\gamma}{4} \end{pmatrix}.$$

With this reconstructed state properties like the degree of entanglement and entropy can now be calculated. For systems with several more qubits the tomography procedure can be easily implemented however the number of measurements increases as 4^n.

To summarize, we have shown a simple method by which the state of a few qubit quantum architecture can be reconstructed and hence the degree of entanglement determined. This characterization will be essential for early proof of principle quantum computation experiments.

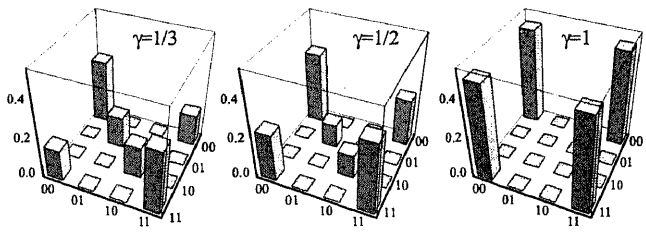


FIG. 2: Graphical representation of the two qubit state reconstruction for the Werner state. For $\gamma = 1/3$ the state is separable, while for $\gamma = 1/2, 1$ the state is entangled with $\gamma = 1$ corresponding to the maximally entangled Bell state.

[1] C. H. Bennett, *et. al*, Phys. Rev. Lett.**70**, 1895 (1993).
[2] P. W. Shor, Phys. Rev. A **52**, R2493 (1995).
[3] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[4] J. S. Bell, Physics (N.Y.) **1**, 195 (1965).
[5] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998).
[6] D. T. Smithey, M. Beck, M. G. Raymer and A. Faridani, Phys. Rev. Lett. **70**, 1244 (1993).
[7] A. G. White, D. F. V. James, P. H. Eberhard, P. G. Kwiat, Phys. Rev. Lett. **83**, 3103 (1999).
[8] A. G. White, D. F. V. James, W. J. Munro and P. G. Kwiat, Phys. Rev. A **65**, 012301 (2002)
[9] We have used λ matrix notation, which is the same as 2-dimensional Pauli matrices, but allows generalisation to *qunits*.
[10] D. F. V. James, W. J. Munro, A. G. White, P. G. Kwiat, "Characterising multiple qubits",in preparation (2001).
[11] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).
[12] C.H. Bennett, D.P. Vincenzo, J.A. Smolin and W.K. Wootters, Phys. Rev. A **54**, 3824 (1996).