一般社団法人

国際数理科学協会会報

No.74/ 2011.3

編集委員：藤井正俊(委員長)、藤井淳一

目次

＊ 理事および監事

先日行なわれました理事および監事の選挙の開票が 2 月 4 日所要で一名理事欠席のもとで行なわれました。その結果、次のようになりました。ご報告いたします。

設立時理事長：長尾壽夫　設立時理事：寺岡義伸、熊谷悦生
設立時監事：植松康祐

理事：中西シヅ、石井博昭、井関清志、長尾壽夫、寺岡義伸、佐藤優子、曽布川拓也、藤井正俊、熊谷悦生、高橋渉、藤井淳一　以上 11 名　(会員番号順)

監事：植松康祐

＊ SCMJ 投稿論文頁数の推移

年	投稿頁数（論文数）	受理頁数（論文数）	棄却頁数（論文数）	受理割合
2001	**1,746（176）**	**1,387（136）**	**348（45）**	**75%**
2002	**1,234（105）**	**1,199（103）**	**181（21）**	**83%**
2003	2,181（200）	**1,566（134）**	**197（23）**	**85%**
2004	**1,028（91）**	**1,051（92）**	**397（40）**	**70%**
2005	1,313（138）	**754（85）**	**260（29）**	**75%**
2006	**1,372（123）**	**1,417（123）**	**116（16）**	**88%**
2007	**824（80）**	**685（64）**	**210（21）**	**75%**
2008	**1,068（87）**	**918（73）**	**139（13）**	**85%**
2009	**850（75）**	**778（73）**	**95（5）**	**94%**
2010	**778（73）**	**678（68）**	**156（13）**	**84%**

上の表より投稿論文が最近すくなくなっています．会員の方の更なる投稿をお願い致します。受理の割合は 8 割前後になっています。

＊ 寄稿

量子鍵交換プロトコルをめぐって

藤井 淳一　（大阪教育大学 情報科学）

はじめに

最近、量子コンピュータ・量子情報理論が話題になっています。日本の企業が合同で、2010 年の 10 月に量子暗号ネットワークの試験運用を開始するとの報道がありました。しかしながら素人がとっつきにくい分野でもあり、実際出版されているテキストは、残念ながら必ずしも十分わかりやすいものであるとは言えません。また、「量子テレポーテーション」という刺激的な用語が使われたこともあって、この分野は誤解されたり理解されにくかったりすることもしばしばです。ここでは、E91 と呼ばれる量子鍵交換プロトコルを巡って、これらの話題を含んだ状況を明確にし、線形代数のみの知識で門外漢にもわかる形にする試みです。私自身量子力学を習ったことさえなく、素人の解釈で勘違いの可能性もありますが、一応整合的ですので恐れずに言い切ってみたいと思います。

1. 量子測定

通常認められている量子測定のコペンハーゲン解釈についてまず述べます。一般には無限次元のヒルベルト空間およびその上の作用素が必要ですが、ここでは有限次元モデルで十分なので、有限次元の話に限定します。その場合、**観測量**とも呼ばれる**物理量**はエルミット行列 A で、そのスペクトル分解を $A = \sum_k t_k E_k$ とします。物理的な**状態**は単位ベクトル ξ のことですが、しばしば**密度行列** $\xi \otimes \xi^*$（Dirac の記法では、$|\xi\rangle\langle\xi|$）と同一視されることからもわかるように、スカラー倍 $e^{i\theta}\xi$ は ξ と同一視されます。状態ベクトルが、$|\alpha|^2 + |\beta|^2 = 1$ として、$\xi = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ とかけるならば、密度行列は、$\xi \otimes \xi^* = \begin{pmatrix} |\alpha|^2 & \alpha\bar{\beta} \\ \bar{\alpha}\beta & |\beta|^2 \end{pmatrix}$ となります。絶対値 1 のスカラー倍を無視する理由は、状態といっても目に見えるものではなく、（実際作用素の分野では「ベクトル状態」といわれる）**エルミット形式**、それを状態の内積型と密度行列のトレース型で書くならば $\langle\xi|A\xi\rangle = \mathrm{tr}\,(\xi \otimes \xi^*)A$ のみが観測値としてやっと顔を見せるので、スカラー倍が無関係になるのです。

この状態 ξ で、観測量 A を観測したときは、**測定値**は A の**固有値** $\sigma(A) = \{t_k\}$ のいずれかとなり、測定値 t_k を得る確率は、$p_k = \langle\xi|E_k\xi\rangle$ であり、確率が 0 でない場合は、状態 ξ は $E_k\xi/\|E_k\xi\|$ に（状態の波束が）**収縮**してしまうというのが、**コペンハーゲン解釈**といわれているものです。このとき、**期待値**は、

$$E_A(\xi) = \sum_k t_k p_k = \sum_k t_k \langle\xi|E_k\xi\rangle = \left\langle \xi \middle| \sum_k t_k E_k \xi \right\rangle = \langle\xi|A\xi\rangle$$

というエルミット形式で与えられることは自明です。

2. 量子もつれ — EPR 状態

粒子が増えるたびに記述上必要となってくる概念は、**テンソル積**（行列では**クロネッカー積**）です（物理の本ではしばしば「直積」と書かれていますが、数学用語の誤用です）。行列とベクトルのテンソル積の性質（A 側 1 粒子目、B 側 2 粒子目）

$$(A\otimes B)(C\otimes D)=AC\otimes BD,\ (A\otimes B)\xi\otimes\eta=A\xi\otimes B\eta,\ \langle\xi\otimes\eta|\xi'\otimes\eta'\rangle=\langle\xi|\xi'\rangle\langle\eta|\eta'\rangle$$

は、各粒子個別の測定の様子をよく表しています。2 粒子（以上）で、A, B それぞれの正規直交状態 $\{\xi(A)_j\}, \{\xi(B)_j\}$ について、密度行列 $\xi^*\otimes\xi$ では、凸和で書ける状態

$$\xi=\sum_j p_j\big(\xi(A)_j\otimes\xi(A)_j^*\big)\otimes\big(\xi(B)_j\otimes\xi(B)_j^*\big)$$

を**分離可能状態 (separable state)** といい、そのような表現を持たない状態を**量子もつれ状態 (entangled state)** といいます。もちろん、一つのテンソル積で書けるような状態 $\xi=\xi_1\otimes\xi_2$ の場合には分離可能状態ですので、量子もつれ状態でも、後述のように測定を一度行うと分離可能状態になってしまいます。

その中でも今回取り上げる典型的な量子もつれ状態は、2-4 次元モデルでは、

$$\Psi=\frac{1}{\sqrt{2}}\left(\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}-\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right)=\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$$

と解釈できる **EPR 状態**と呼ばれる特別なものです。EPR は Einstein-Podolsky-Rosen の頭文字をとったもので、量子力学の解釈の誤りを指摘するために Einstein らが挙げた例と同等のものですが、皮肉なことに実験結果は彼らの方が間違っているという結論を下すことになった、いわくつきの「状態」です。これによって、後述するように 2 つの不等式が問題となり、その「不等式の違いによって、暗号の安全性を保とう」という戦略が今回の話のキーポイントとなっています。しかし、不思議なことに [2, 10] などのような代表的な良質なテキストでさえ、2 つ目の不等式を導くのに Einstein の誤った解釈に基づき、素人目からするとどうしてもアドホックに見える（局所原理に基づく）「隠れた変数理論」のようなものを使用しています。学生ならばテキストに大事そうに書いてあると（特に Einstein の名前に屈して）、これは正しいものだと思い込んでしまって自己矛盾に陥って混乱してしまいます。素人の私には理解できない事情があるのでしょうが、そんなものに頼らない証明を後述しましょう。

この EPR 状態は顕著な性質を持っています。直交単位ベクトル ξ, η を

$$\xi=\begin{pmatrix}\alpha\\\beta\end{pmatrix},\ \eta=\begin{pmatrix}-\bar\beta\\\bar\alpha\end{pmatrix}\qquad(|\alpha|^2+|\beta|^2=1)$$

とするとき、テンソル積では、

$$\xi\otimes\eta-\eta\otimes\xi=\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\otimes\begin{pmatrix}-\bar{\beta}\\ \bar{\alpha}\end{pmatrix}-\begin{pmatrix}-\bar{\beta}\\ \bar{\alpha}\end{pmatrix}\otimes\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=\begin{pmatrix}-\alpha\bar{\beta}\\ |\alpha|^2\\ -|\beta|^2\\ \beta\bar{\alpha}\end{pmatrix}-\begin{pmatrix}-\bar{\beta}\alpha\\ -|\beta|^2\\ |\alpha|^2\\ \beta\bar{\alpha}\end{pmatrix}$$

$$=\begin{pmatrix}0\\ |\alpha|^2+|\beta|^2\\ -(|\alpha|^2+|\beta|^2)\\ 0\end{pmatrix}=\begin{pmatrix}0\\ 1\\ -1\\ 0\end{pmatrix}=\sqrt{2}\Psi$$

となって、Ψ はあらゆる 2 つの単位直交ベクトルの組に対し、同じ形式で

$$\Psi=\frac{1}{\sqrt{2}}\left(\xi\otimes\eta-\eta\otimes\xi\right)$$

とかけてしまうのです。それで、A 側の測定は、上記のことからあらゆる直交状態で同じなので、$\xi=\begin{pmatrix}1\\ 0\end{pmatrix}$, $\eta=\begin{pmatrix}0\\ 1\end{pmatrix}$ として、観測量は常に ±1 を取るように

$$A_\xi=(\xi\otimes\xi^*-\eta\otimes\eta^*)\otimes I=\left(\begin{pmatrix}1&0\\ 0&0\end{pmatrix}-\begin{pmatrix}0&0\\ 0&1\end{pmatrix}\right)\otimes I=\begin{pmatrix}1&0\\ 0&-1\end{pmatrix}\otimes I$$

としておきましょう。すると、測定値が 1 のとき、A 側では ξ に収縮するので、Ψ 自体は、$\xi\otimes\eta$ に収縮せざるを得ず、B 側で、

$$B_\xi=I\otimes(\xi\otimes\xi^*-\eta\otimes\eta^*)=I\otimes\begin{pmatrix}1&0\\ 0&-1\end{pmatrix}$$

で測定すると、確率 1 で η（測定値 -1）が得られることになります。実際、-1 に対する射影は、$I\otimes\begin{pmatrix}0&0\\ 0&1\end{pmatrix}$ なので、

$$p(\{B=-1\})=\left\langle\xi\otimes\eta\middle|\left(I\otimes\begin{pmatrix}0&0\\ 0&1\end{pmatrix}\right)\xi\otimes\eta\right\rangle=\langle\xi|\xi\rangle\langle\eta|\eta\rangle=1$$

になります。A 側の測定値 -1 の時も同様で、B 側では確率 1 で 1 が測定値となります。このように完全に反相関の関係にあるので、結果を逆転して考えることで相手の情報が確実に伝わることになります。もし量子もつれの状態にある 2 つの粒子を十分離すことができるなら（km オーダーで、実験が成功していると聞いています）、瞬時に情報伝

達が可能になりますので、光速を超えた瞬間移動の情報伝達ということで**「量子テレポーテーション」**と名づけられました。「波束の収縮」という量子力学特有の解釈が、瞬時に情報伝達できるという結論を導きますから、これは物理学上ありえないということで、またまた量子力学解釈の論争になりそうですが、実際には、「測定したかどうか」の確認が何らかの別の形で情報伝達されないといけないので、解釈上そんなことはありません。しかし、誤解を生みそうなネーミングであることは確かです。

3. スピンモデルでの測定

スピンの概念自体に疎いために、実際に一番解釈に苦労した部分なのですが、結果が適合しているのでこのまま述べていきます。ここでは、スピン $\frac{1}{2}$ のフェルミ粒子の設定で話をします。**Pauli のスピン行列**と呼ばれる

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

というまさに固有値 ± 1 を有した観測量（したがってユニタリ行列でもあります。作用素論ではシンメトリーと呼ばれています）があります。スピンの測定値 $\pm 1/2$ に合わせ、全体を 2 で割っておくことが多いようですが、ここではこのままにしておきます。これらの組み合わせでスピンが観測されます。（「スピンの方向をあらわすベクトル」と解釈され、**Bloch ベクトル**あるいは **Pauli ベクトル**とも呼ばれる）3 次元の実単位ベクトル $\begin{pmatrix} x \\ y \\ z \end{pmatrix}$ について、$\Omega = \{x, y, z\}$ という記号を導入して、

$$\sum_{a \in \Omega} a\sigma_a = x\sigma_x + y\sigma_y + z\sigma_z = \begin{pmatrix} z & x - yi \\ x + yi & -z \end{pmatrix}$$

となりますので、固有方程式

$$0 = \det(x\sigma_x + y\sigma_y + z\sigma_z - \lambda I) = (\lambda^2 - z^2) - (x^2 + y^2) = \lambda^2 - 1$$

を解くと、やはり固有値 ± 1 のユニタリ・エルミット行列が得られます。Bloch ベクトル $\xi_k = \begin{pmatrix} x_k \\ y_k \\ z_k \end{pmatrix}$ に対応する 2 粒子のスピンの同時観測量は

$$\begin{aligned} C_{1,2} &= \left(\sum_{a \in \Omega} a_1\sigma_a\right) \otimes \left(\sum_{b \in \Omega} b_2\sigma_b\right) = \sum_{a,b \in \Omega} a_1 b_2 \sigma_a \otimes \sigma_b \\ &= x_1x_2\sigma_x \otimes \sigma_x + y_1y_2\sigma_y \otimes \sigma_y + z_1z_2\sigma_z \otimes \sigma_z \\ &+ x_1y_2\sigma_x \otimes \sigma_y + x_1z_2\sigma_x \otimes \sigma_z + y_1z_2\sigma_y \otimes \sigma_z \\ &+ y_1x_2\sigma_y \otimes \sigma_x + z_1z_x\sigma_z \otimes \sigma_x + z_1y_2\sigma_z \otimes \sigma_y \end{aligned}$$

と解釈します。この時、EPR 状態 Ψ を観測すると、

$$\langle\Psi|\sigma_a\otimes\sigma_b\Psi\rangle=\begin{cases}-1 & (a=b)\\ \\ 0 & (a\neq b).\end{cases}$$

なので、その期待値は、2 つの単位ベクトルの角度を $\theta_{1,2}$ とするとき、期待値は

$$E_{1,2}=\langle\Psi|C_{1,2}\Psi\rangle=-x_1x_2-y_1y_2-z_1z_2=-\cos\theta_{1,2}$$

となり、測定角度のコサインのマイナスという結果になります。この公式は、**スピン 1 重項**（[2, 7]）または**全スピン 0**（[10]）と呼ばれる状態の顕著な性質です。

4. Cirel'son の不等式

4 つの Bloch ベクトル ξ_{jk} について、2 方向の測定を対称的に（$\theta_{11,22}-\theta_{11,21}=\theta_{12,21}-\theta_{12,22}$ となるように）追加して、$S=E_{11,21}-E_{11,22}+E_{12,21}+E_{12,22}$ という 4 方向の期待値を考えます。観測量は、$C_{11,21}-C_{11,22}+C_{12,21}+C_{12,22}$ ですが、マイナス部分は、各方向を少しずらして、角度順に ξ_{11}, ξ_{21}, ξ_{12}, ξ_{22} とするとき、最も離れた ξ_{11}, ξ_{22} を $\pi/2$ 以上離すので、ここだけコサインの符号が変わるので最小値実現のためです [10]：

$$S=-\cos\theta_{11,21}+\cos\theta_{11,22}-\cos\theta_{12,21}-\cos\theta_{12,22}.$$

この絶対値の最大値を求めるため、$\alpha=(\theta_{11,22}+\theta_{11,21})/2$, $\beta=(\theta_{12,22}+\theta_{12,21})/2$ と置き、各角度の差は π より大きくないとすると、対称性より

$$0<2\gamma=\theta_{11,22}-\theta_{11,21}=\theta_{12,21}-\theta_{12,22}<\pi,$$

$$\begin{aligned}|S|&\leqq|-\cos\theta_{11,21}+\cos\theta_{11,22}|+|\cos\theta_{12,21}+\cos\theta_{12,22}|\\ &=\left|2\sin\alpha\sin\left(\frac{\theta_{11,22}-\theta_{11,21}}{2}\right)\right|+\left|2\cos\beta\cos\left(\frac{\theta_{12,21}-\theta_{12,22}}{2}\right)\right|\\ &\leqq 2\left|\sin\left(\frac{\theta_{11,22}-\theta_{11,21}}{2}\right)\right|+2\left|\cos\left(\frac{\theta_{12,21}-\theta_{12,22}}{2}\right)\right|\\ &=2\left(\sin\gamma+\cos\gamma\right)=2\sqrt{2}\left(\sin\left(\gamma+\frac{\pi}{4}\right)\cos\left(\gamma+\frac{\pi}{4}\right)\right)\leqq 2\sqrt{2}\end{aligned}$$

となります。この不等式 $|S|\leqq 2\sqrt{2}$ は、**Cirel'son の不等式**（最近の表記では、Tsirelson に変わっているようです, cf.[9]，本人の解説もあります [11]）と呼ばれています。実際にこの不等式が最良であることは、6 節でわかります。

5. CHSH 不等式

さて、（盗聴者などが）一度測定してしまった場合を考えてみましょう。この場合、A, B 同時の測定を行うわけですから、一番細かい波束収縮については、$P_A\otimes Q_B$ という、2 つの射影のテンソル積によるものと考えられるでしょう。すると、その収縮によって、Ψ でさえも、ξ_1, ξ_2 を、P_A, Q_B の固有ベクトルとして、$\Phi=\zeta_1\otimes\zeta_2$ という「分離可能状態」にならざるを得なくなります。この場合に前節の不等式は、（通常の古典的な因果関係と同じになって）

上記の $|S|$ の値が 2 以下になってしまいます。この不等式を **CHSH 不等式**（研究者名 Clauser-Horne-Shimony-Holt の略）といい、（厳密には少し違うようですが）量子力学の顕著な性質を示す有名な **Bell の不等式**の特別な場合と解釈されます。これを通常のテキストに逆らって「隠れた変数理論」を使わずに示してみましょう：

$$\zeta_1 = \begin{pmatrix} \alpha_1 \\ \\ \beta_1 \end{pmatrix}, \quad \zeta_2 = \begin{pmatrix} \alpha_2 \\ \\ \beta_2 \end{pmatrix}$$

としておきます。すると、

$$t_{jx} \equiv \langle \zeta_j | \sigma_x \zeta_j \rangle = 2 \operatorname{Re} \alpha_j \overline{\beta_j},\ t_{jy} \equiv \langle \zeta_j | \sigma_y \zeta_j \rangle = 2 \operatorname{Im} \alpha_j \overline{\beta_j},\ t_{jz} \equiv \langle \zeta_j | \sigma_x \zeta_j \rangle = |\alpha_j|^2 - |\beta_j|^2$$

となって、$|t_{jx}|^2 + |t_{jy}|^2 + |t_{jz}|^2 = (|\alpha_j|^2 + |\beta_j|^2)^2 = 1$ がわかります。Bloch ベクトル ξ_{jk} の各座標を $x_{jk},\ y_{jk},\ z_{jk}$ としておくと、Schwarz 不等式により

$$\left| \sum_{a_\in \Omega} a_{jk} t_{ja} \right| = |x_{jk} t_{jx} + y_{jk} t_{jy} + z_{jk} t_{jz}| \leqq \sqrt{x_{jk}^2 + y_{jk}^2 + z_{jk}^2} \sqrt{t_{jx}^2 + t_{jy}^2 + t_{jz}^2} = 1$$

となります。この場合の観測量は

$$C = C_{11,21} - C_{11,22} + C_{12,21} + C_{12,22} = \sum_{a,b \in \Omega} \left(a_{11}(b_{21} - b_{22}) + a_{21}(b_{21} - b_{22}) \right) \sigma_a \otimes \sigma_b$$

ですから、その期待値は

$$\begin{aligned} S &= \sum_{a,b \in \Omega} \big(a_{11}(b_{21} - b_{22}) + a_{21}(b_{21} - b_{22}) \big) t_{1a} t_{2b} \\ &= \left(\sum_{a \in \Omega} a_{11} t_{1a} \right) \left(\sum_{b \in \Omega} b_{21} t_{2b} - \sum_{b \in \Omega} b_{22} t_{2b} \right) + \left(\sum_{a \in \Omega} a_{12} t_{1a} \right) \left(\sum_{b \in \Omega} b_{21} t_{2b} + \sum_{b \in \Omega} b_{22} t_{2b} \right) \end{aligned}$$

となります。したがって、

$$|S| \leqq \left| \sum_{b \in \Omega} b_{21} t_{2b} - \sum_{b \in \Omega} b_{22} t_{2b} \right| + \left| \sum_{b \in \Omega} b_{21} t_{2b} + \sum_{b \in \Omega} b_{22} t_{2b} \right|$$

が得られます。一般に、実数 v, w について

$$|v + w| + |v - w| \leqq 2 \max\{|v|, |w|\}$$

が、次の事実からわかることに注意しましょう：

$$v + w + |v - w| = 2 \max\{v, w\} \quad \text{and} \quad v + w - |v - w| = 2 \min\{v, w\}.$$

以上のことより、

$$\begin{aligned} |S| &\leqq \left| \sum_{b \in \Omega} b_{21} t_{2b} - \sum_{b \in \Omega} b_{22} t_{2b} \right| + \left| \sum_{b \in \Omega} b_{21} t_{2b} + \sum_{b \in \Omega} b_{22} t_{2b} \right| \\ &\leqq 2 \max \left\{ \left| \sum_{b \in \Omega} b_{21} t_{2b} \right|, \left| \sum_{b \in \Omega} b_{22} t_{2b} \right| \right\} = 2 \max \left\{ \left| \sum_{a \in \Omega} a_{21} t_{2a} \right|, \left| \sum_{a \in \Omega} a_{22} t_{2a} \right| \right\} \leqq 2, \end{aligned}$$

となって、「分離可能状態を測定することで CHSH 不等式が得られる」ことがわかります（たぶんオリジナルな証明だと思います)。さらに、測定ペアが直交している場合には $\sqrt{2}$ 以下になることも確かめられます。

6. E91 プロトコル

前節までのことを利用して、量子鍵交換を考えます。ここでは y 成分を省いて 2 次元方向の Bloch ベクトルを

$$\xi_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \xi_2 = \xi_{21} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \xi_3 = \xi_{21} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \xi_{21} = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

と配置します。すると、直交している 1 と 3 の同時スピン測定の期待値は、

$$S_{1,3} = -\cos\frac{\pi}{4} + \cos\frac{3\pi}{4} - \cos\frac{\pi}{4} - \cos\frac{\pi}{4} = -2\sqrt{2}$$

となって、Cirel'son の不等式が最良であり、この場合に最も離れていることがわかります。したがって、これらの観測を十分含むような長さのメッセージを、上記の各 3 種類の測定について、EPR 状態 Ψ のもとで行います。すると、盗聴（他人による量子測定）がなければ上記の値を保ちますが、盗聴があれば CHSH 不等式の範囲ですから、上記の値は -2 以上（ここでは実際には $-\sqrt{2}$ 以上）になってしまいます。したがってお互いにすべての測定の方向を十分多くランダムに選んで公開し、すべて測定したのち、方向が違っている部分の測定結果（上記の測定平均値計算に必要）のみを公開して、盗聴がなければ、方向が一致している部分の測定結果により（結果は真逆になるので、その意をくんで）お互いに秘密鍵を安全に共有するというのが、**E91** と呼ばれる鍵交換プロトコルです（これは、A.K.Ekert が 1991 年に発表したものなので、この略称で呼ばれています)。採用された使い捨ての鍵は、**ワンタイムパッド** と呼ばれています。

おわりに

実は卒業研究の指導からこのようなことを思いついたのですが、このように書いてあれば指導しやすいのにという思いがこの文章にこもっています。局所原理と呼ばれる哲学的な考察に基づいて、「隠れた確率変数」があるはずだという議論の流れよりも、測定によって量子もつれ状態が解消し、「分離可能状態」になるため、そのまま測定すれば、CHSH 不等式が成り立つという話の方が、物理の素人にはより納得しやすいものだと思うのは私だけでしょうか。残念ながらこの方向で CHSH 不等式を示しているものが見当たらなかったので、特にここで詳説しておきました。

なお最近この不等式の差異の話の発展が作用素環論の方に及んでいる事を、東北大の日合文雄先生からお聞きましたが（[5]）、CHSH 不等式については（Bell 不等式と呼んでいますが）作用環論でのすっきりとした証明 [1] があることも同時にわかりましたので、書き留めておきます。

参考文献

[1] J.Baez: Bel's inequality for C*-algebras, Lett. in Math. Phys., **13**(1987), 135–136.
http://www.springerlink.com/content/k6v6w76028711615/

[2] D. バウミースター・A. エカート・A. ツァイリンガー（西野哲朗・井元信之 訳）: 量子情報の物理—量子暗号、量子テレポーテーション、量子計算—, 共立出版, 2007.

[3] G. ベネンティ・G. カザーティ・G. ストゥリーニ：量子計算と量子情報の原理, シュプリンガー・ジャパン, 2009.

[4] 古澤　明, 量子光学と量子情報科学, 数理工学社, 2005.

[5] M.Junge et.al.: Connes's embedding problem and Tsirelson's problem, arXiv:1008.1142v1.
http://arxiv4.library.cornell.edu/abs/1008.1142v1

[6] 小芦雅斗・小柴健史：量子暗号理論の展開, サイエンス社, 2008.

[7] N.D. マーミン（木村 元 訳）: 量子コンピュータ科学の基礎, 丸善, 2009.

[8] M.A. ニールセン・I.L. チャン：量子コンピュータと量子通信 III—量子通信・情報処理と誤り訂正—, オーム社, 2005.

[9] 大矢雅則・渡辺昇：量子暗号と量子テレポーテーション, 共立出版, 2006.

[10] 佐川弘幸・吉田宣章：量子情報理論（第 2 版）, シュプリンガー・ジャパン, 2009.

[11] Boris Tsirelson's home page: http://www.tau.ac.il/~tsirel/

＊ 在庫雑誌の案内

協会事務の部屋が海外からの雑誌で手狭になってきています。そこで希望の会員または所属する大学等に、**無償**でお分けすることにしています。一度配布が決まりましたらその後もお送りいたします。ただし、**送料は負担**していただきます。下にある申込用紙にご記入のうえ協会あて、pbls@jams.jp にご連絡下さい。番号の欠となっているのはすでに希望者のあった雑誌です。

雑誌（a）

1. Serdica mathematical journal
2. Colloquium mathematicum
3. Monatshefte fur mathematik
4. Milan journal of mathematics
5. Naval research logistics NRL a journal dedicated to advances in operations and logistics research
6. Rendiconti del seminario matematico universita e politecnico torino
7. Analytic function spaces properties of operation and duality
8. Iranian Journal of fuzzy systems
9. Publicationes mathematicae Debrecen

11.Annali dell'universita di ferrara scienze matematiche

雑誌 (b)

2. Numerical mathematics　A journal of Chinese universities
3. University of istanbull faculty of science　the journal of mathematics, physics and Astronomy
4. Academie serbe des sciences et des arts bulletin T.CXXXI—sciences mathematique
6. Annali dell'universita di ferrara nuova serie　scienze matematiche
7. Divulgaciones matematicas
8. Dirasat engineering sciences
9. Tamkang journal of mathematics
10. Annals de L'institute Fourier
11. Bollettino della unione mathematica italiana sezione (A, B)

雑誌 (c)

1. Annales universitatis scientiarum budapestinesis de Rolando eotvos nominatae
2. Bulletin mathematique de la societe des sciences mathematiques de roumanie
3. Ion beam science solved and unsolved
4. Annals of the university of Craiova mathematics and computer science series
5. Mathematicae notae
6. Statistica sinica

7. IBM journal of research and development
8. Analeles stintifice ale universitatii Alexandru ioan cuza din iasi (serie noua) matematica
9. Scientific annals of computer science
10. Atti della academia nazionale dei lince rendiconti lincei scienze fisiche e naturali
11. Tohoku Mathematical Journal 東北数学雑誌

雑誌（d）

1. Rivista di matematica della universita di parma
2. Bolletino della unione mathematica italiana (sezione A, B)
3. Revista tecnica
4. Matematica contemporanea
5. Studia universitatis babes-bolyai mathematica cluj-napoca
6. Academie roumaine filiale de cluj-napoca
7. Bolletino di storia delle scienze matematiche
8. Analele universitatii de vest din Timisoara seriamathematica-informatica
9. Relatorio de pesquisa
10. Annals de L'institute Fourier
11. Allosteric proteins
12. Changing models

雑誌 (R)

1. у к р а ё н с ь к и й м а м е м а м ц ч н и й ы с н ц к (Ukrainian Mathematical Bulletin)

2. Т Е О Р И Я В Е Р О Я Т Н О С Т Е Й
3. З А П И К И Н А У Ч Н Ы Х С Е М И Н А Р О В П О М И
4. М А Т Е М А Т И К А (Izvestiya NAN Armenii, Matematika)
5. **К И Б Е Р Н Е Т И К А И С И С Т Е М Н Ы Й А Н А Л И З**

希望雑誌申込書

氏名		所属		電話番号	
				e-mail	
送り先					
雑誌名					
例えば 1）a-3 題目 2）R-1 題目 ・・・・・・・・・・・・・・・・・・・・・ のように記入して下さい。					

＊　機関会員募集

機関会員の特典としては

(1)本屋より SCMJ を購入すると、print 版 45,000 円ですが、機関会員になると、print 版 33,000 円で **online も見ることができます。**

(2)会員でない 2 名の方を準会員（会費不要）として登録することができます。これにより、page charge（別刷代金）が会員と同じ扱いになります。

(3)上の準会員 2 名は online で SCMJ を見る事ができます。

(4) Net を用いて国際研究集会を催す時、アナウンス、アブストラクトの作成などお助けいたします。

大学、研究所等が協会から SCMJ 誌の直接購入すると、今年から online も無料で見ることができるようになりました。機関会員の申込用紙です。適当にお使い下さい。

上にも書きましたように、2006 年より発効の機関会員制度により各機関会員に所属の研究者 2 名を会費無料で準会員として登録しますと、準会員が SCMJ に accept された論文を掲載するときの page charge（別刷代金）は会員と同額とすることにしました。

この新しい制度の機関会員の P.R.を、日本国内外（BRICS 諸国など）400 大学に向けて、昨年 1 月から始めています。同時に今迄の SCMJ 投稿者で会員でない方、また、個人会員および（機関会員の）準会員加入の P.R.も始めています。

＊ Application for Academic and Institutional Member of ISMS

Subscription of SCMJ	□Print ＋ Online (¥33,000, US$300)
University (Institution)	
Department	
Postal Address where SCMJ should be sent.	
E-mail address	
Person in charge	Name: Signature:
Payment Check one of the two.	□Bank transfer □Credit Card (Visa, Master)
Name of Associate Members	1.
	2.

正会員の特典としては(1)online で SCMJ をみることが出来ます。(2)論文の掲載時に page charge(別刷代金)が随分と安くなる。
(3) Net を用いて国際研究集会を催す時、アナウンス、アブストラクトの作成などお助けいたします。6,000 円を支払うと、hard-copy の SCMJ が一年を通じて手に入ります。
(4) 10 年間個人会員を続けると、国内会員は 70,000 円、外国会員は US$600、途上会員は US$500 を支払うと生涯会員となれます。

2008 年度からの会費

Categories	国内会員	海外会員	途上国会員
単年度 A 会員	¥9,000	US$75, €60	US$117, €93
3 年 A 会員	¥24,000	US$200, €160	US$117, €93
単年度 S 会員	¥5,000	US$40, €32	US$27, €21
3 年 S 会員	¥12,000	US$100, €80	US$71, €57
生涯会員	¥90,000	US$740, €592	US$616, €493

日本語が出来る方の入会の申込用紙です。また、英語版も書いて頂くことになります。近く Net 上で申し込み可能となるようにしますので、入会しようとする方はそれをご利用下さい。

＊　正会員申込用紙

正会員入会申込書

<table>
<tr><td>氏名</td><td colspan="2"></td><td>英語名</td><td></td></tr>
<tr><td colspan="5">次の２つのうち会報等を送付先とする方に○を付けてお書き下さい。</td></tr>
<tr><td>所属先
住所</td><td colspan="4">〒</td></tr>
<tr><td>住所</td><td colspan="4">〒</td></tr>
<tr><td>専門分野</td><td colspan="4">表 f *より選んで○で囲って下さい
f-1, f-2, f-3, f-4, f-5, f-6, f-7, f-8, f-9, f-10, f-11, f-12, f-13, f-14</td></tr>
<tr><td rowspan="2">E-mail
address</td><td colspan="2" rowspan="2"></td><td>電話番号</td><td></td></tr>
<tr><td>Fax 番号</td><td></td></tr>
<tr><td>会員区分
該当部分にチェック</td><td colspan="4">□A1 一般 1 年　□ A3 一般 3 年　　□ S-A1 高齢者又は学生 1 年
□　S-A3 高齢者又は学生 3 年　　□ 生涯会員</td></tr>
<tr><td>所属先の
施設</td><td colspan="4">□ ビデオ会議可能　　□ 遠隔会議可能　　□ コンピューターセンター</td></tr>
<tr><td>所属先の
通信システム</td><td colspan="4">□　ISDN　　□ IP</td></tr>
<tr><td>所属大学等が
機関会員</td><td colspan="4">□　会員である　　□　会員でない</td></tr>
<tr><td colspan="5">SCMJ のプリント版の購入</td></tr>
<tr><td colspan="3">□　希望　1 年に付き
１年会員 9,000 円、3 年会員 8,000 円**</td><td colspan="2">□ 希望しない</td></tr>
<tr><td>高齢会員を申し込む場合</td><td colspan="2">生年月日</td><td colspan="2">学生会員の場合は在学証を添付</td></tr>
<tr><td>日付</td><td colspan="4"></td></tr>
<tr><td colspan="3">私は ISMS 会員になり、国際数理科学協会に送り状に記載された年会費を払います。ISMS 会員として受け取った Scientiae Mathematicae Japonicae のコピーは個人使用とし、機関、大学または図書館やその他の組織の中に置かず、閲覧目的で会員購読することもしません。</td><td>署名</td><td colspan="2"></td></tr>
</table>

* Notices from the ISMS March 2008 p.25 を御参照下さい。**ただし、３年間一括の場合は 24,000 円です。
この申込みの内容は会との連絡以外には使用いたしません。

Application form for an individual member of ISMS

Family Name		First &Middle Name	
Check one of the following addresses to which "Notices from the ISMS" should be sent.			
Address of your institution (university)	□		
Home address	□		
Special fields*	f-1 f-2 f-3 f-4 f-5 f-6 f-7 f-8 f-9 f-10 f-11 f-12 f-13 f-14		
E-mail address		Tel.	
		Fax	
Membership category** (Circle one)	A1, A3, SA1, SA3, F1, F3, SF1, SF3, D1, D3, SD1, SD3, AL, FL, DL		
Check the facilities your institution has.	☐ Conference room(s) for video conference ☐ Computer center		
Communication system of your institution	□ ISDN □ IP		
Is your institution (university) an Institutional Member of ISMS?	□ Yes □ No		
☐ I subscribe to the printed version of SCMJ.	□¥6,000 (US$60, €48) per year for those members of A1, SA1, F1, and SF1 , D1 and SD1. □¥5,500 (US$55. €44) per year for those members of A3, SA3, F3, SF3, D3, SD3, AL, FL, and DL. □In case A3, SA3, F3, SF3, D3, SD3, AL, FL, or DL members make the payment at a time in advance, the price for 3 years is ¥15,000 (US$150, €120).		
For the aged member, write your birth year.		For the student member, student registration certificate should be attached.	
Date of Application			
I wish to enroll as a member of ISMS and will pay to International Society for Mathematical Sciences the annual dues upon presentation of an invoice. Copies of Scientiae Mathematicae Japonicae received as an ISMS member will be for my personal use only and shall not be placed in institutional, university or other libraries or organizations, nor can membership subscriptions be used for library purposes.			
Signature			

* Notices from the ISMS March 2008 p.25 を御参照下さい。
**Notices from the ISMS March 2008 p.28 を御参照下さい。

ISMS　(JAMS の継続) 会員募集

ISMS の出版物：ISMS は、創刊より約 60 年、国際的に高い評価を得ている Mathematica Japonica (M.J.)と、その姉妹誌で電子 Journal と Paper 誌とを持つ、Scientiae Mathematicae (SCM) とを発行してきました。両誌は合併して、“21 世紀 MJ/SCM New Series, Scientiae Mathematicae Japonicae (SCMJ) ”として、電子版は 2000 年 9 月より発行してきました。印刷版は、1978 年 1 月より、年間 6 冊、700～1200 頁を出版しています。全体として 230 巻を超える、日本で最大量を誇る数理科学の雑誌です。その特長は、下の 1)～７)です。

1) Editorial Board には、国内だけでなく、海外 15 カ国の著名な研究者 40 名が参加している。
2) 世界の research group に論文が紹介され、積極的な交流が推進されている。
3) Editor を窓口として直接論文を投稿できて、迅速な referee 及び出版が得られる。
4) 有名な数理科学者の original paper や、研究に役立つ survey が、毎号載せられている。
5) SCMJ は、世界の有名数理科学者による、極めて興味ある expository paper を、毎号 International Plaza 欄に掲載している。世界各国の図書館へ、広く配布されている。
6) 投稿論文は、accept 後 (又は組版後) 待ち時間０で発行されます。
7) Mathematical Review, Zentralblatt に from cover to cover で review されている。

ISMS の研究集会：(1)研究仲間がゆっくり時間をかけて発表、討論をする、特色ある参集型研究集会が毎年行われ、非会員も含む多数の参加者の、活発な研究交流の場となっている。(2)ISMS には内外の著名な研究者が多数入っておられる。近いうちに内外を結ぶ高い level の研究会が online で行われる事を期待している。（本誌 45 号　3p 及び Notices　March　2006　9p　を御参照下さい）

ISMS の学術賞：会員の優れた論文を広く世界に紹介し、更なる研究を奨励するために、ISMS 賞、JAMS 賞、Shimizu 賞、Kunugui 賞、Kitagawa 賞を設けている。（詳しくは本誌 45 号 2p 会則 13 条を御参照下さい）

＜ISMS の会員の特典＞１．SCMJ 電子版の購読 (print out も含む) 無料。２．SCMJ print 版の少額での購読 (下表１)。３．Page charge(別刷代金)の discount (下表２)。

＜機関購読会員の特典＞1. 機関内の 2 名の方を準会員として会費無料で登録することが出来る。２．準会員は会員と同じ page charge(別刷代金)の discount を受けることが出来る。

表１
【雑誌購読費】

	正会員（1 年）	正会員（3 年）	機関会員	定価
Print	￥6,000 US$ 60, €48	￥5,500* US$ 55, €44	￥33,000 US$ 300, €240	￥45,000 US$ 400, €320
Online	Free	Free		
Online+print	￥6,000 US$ 60, €48	￥5,500 US$ 55, €44	￥33,000 US$ 300, €240	￥45,000 US$ 400, €320

*３年会員のみ、雑誌購読費 3 年分前払いの場合は￥15,000 になります。

著者の方には、SCMJ を１冊送料込みで 1,200 円または US＄12 で購入できます。

表２
【ページチャージ】

	ISMS members	Non-members
p	￥3,500 (US$35, € 23)	￥4,000 (US$40, €27)
Tex	￥2,000 (US$20, € 14)	￥2,500 (US$25, €17)
LateX2e, LaTeX	￥　700 (US$ 7,　€　4)	￥1,000 (US$10, € 7)
Js (ISMS style file)	￥　500 (US$ 5,　€　3)	￥　800 (US$ 8,　€ 5)

別刷作成について、次の費用の分担をお願いします。原稿の組版についての連絡費、抜刷送料等の事務処理として、一編について￥1,000、及び上表の各原稿の種類による組版費を請求させて頂きます。

（2008 年　Vol.67　から実施）

表３
【2008 年の会費】

Categories	国内会員	海外会員	途上国会員
単年度 A 会員	¥9,000	US$ 75,　€60	US$ 45 ,　€36
3 年 A 会員	¥24,000	US$ 200,　€160	US$ 117,　€93
単年度 S 会員	¥5,000	US$ 40,　€32	US$ 27,　€21
3 年 S 会員	¥12,000	US$ 100,　€80	US$ 71,　€57
生涯会員**	¥90,000	US$ 740, €592	US$ 616, €493

**過去 10 年以上、正会員であった方に限る。

A 会員は正会員を指し、S 会員は、学生会員と高齢会員(70 歳以上)を指します。

国際数理科学協会
International Society for Mathematical Sciences
〒590-0075　堺市堺区南花田口町 2-1-18　新堺東ビル内
Tel：(072)222-1850　/　Fax：(072) 222-7987　　URL：http://www.jams.or.jp