

# 簡介量子非局部性的應用與度量

黃顯棟

東華大學應用數學系

email: [siendong@server.am.ndhu.edu.tw](mailto:siendong@server.am.ndhu.edu.tw)

## 摘要

非局部性 (nonlocality) 並不是一個新的主題，但近十年來，新的應用不斷被發展出來。對於量子狀態非局部性的進一步研究日益重要，尤其是如何度量非局部性的大小。本文介紹了一些主要的應用方向及解釋度量非局部性的大小的原則。

## I. 非局部性的發現

科學的發展，往往令人無法預測。就當人們以為對量子狀態的非局部性十分了解，認為它只具有純粹學術研究上的價值與興趣時，它卻和電腦，資訊，通訊等學科結合在一起，漸漸形成了一門新的領域，展現了量子理論一個嶄新的應用範圍。

1935 年 Einstein, Podolsky and Rosen (EPR) 為了探討量子力學的完備性(completeness)，提出了一個量子狀態，這個量子狀態具有非局部性，也就是說我們在 A 地測量的結果可以完全決定在 B 地測量的結果。進一步而言，在一些局部性非常強的量子狀態中，如量子場論的真空狀態，我們在地球上只要作“足夠充分”的測量與實驗，我們可以知道宇宙空間任一時空區域的量子狀態。

EPR 原來想利用這個量子狀態來論證量子力學的不完備性。他們使用以下“合理”的假設：在一粒子上做測量並不會影響在另一粒子上作測量的結

果。據此他們認為量子力學是不完備的。然而就是此一特性讓量子世界有別於的古典世界。

由於位置和動量的本徵值都是連續的，EPR 的量子狀態難以用數學式子表示出來。後來 Bohm 以 spin-1/2 的電子對來取代 EPR state，因為 spin-1/2 的電子對在 Z 軸方向只有 +、- 兩個本徵值，這樣大大降低了數學討論的困難度，也使量子狀態的非局部性更容易表現出來。

1964 年，Bell 找到古典機率的相關函數 (correlation function) 的限制條件，意即如果系統可以被古典機率來描述，那麼在相關函數之間存在一些關係，它們必須滿足所謂的 Bell's inequality。然而不管是 EPR 系統中利用粒子的位置或動量所建立的量子態，或 Bohm 利用 spin-1/2 電子對所建立的量子狀態，都無法滿足這不等式。也就是說存在著一些量子狀態，它們的相關函數是無法用古典機率來描述的，這些量子狀態就具有非局部性。

## I. 非局部性的應用

### II.1 量子計算機

1982年 Feynman 討論如何利用計算機來模擬物理世界時，也遇到相同的情況。既然實際物理世界有隨機現象，我們就必須放棄使用決定性型 (deterministic) 計算機，改用古典機率型 (probabilistic) 計算機。假設有一 Bohm spin-1/2 電子對從同一系統朝 A, B 兩地射出。我們在 A, B 兩地分別對電子自旋沿不同的軸 ( $\eta_A, \eta_B$ ) 作測量 ( $\sigma_{\eta_A}, \sigma_{\eta_B}$ )。根據量子力學，測量值是  $\sigma_{\eta_A}$  及  $\sigma_{\eta_B}$  的本徵值，即  $\pm 1$ 。因此我們可以得到 (+, +) (+, -) (-, +) (-, -) 的機率分佈。如在 A, B 兩地測量值是 (+, +) 或 (-, -) 的機率是  $\sin^2((\varphi_B - \varphi_A)/2)$ ，其中  $\varphi_A$  ( $\varphi_B$ ) 是  $\eta_A$  ( $\eta_B$ ) 與 Z 軸的夾角。Feynman 試著利用古典機率理論，建立了這些機率分佈所必須滿足的條件。然而，我們卻找不到一個機率分佈，一方面滿足 Feynman 所建立了條件，同時又滿足  $\sin^2((\varphi_B - \varphi_A)/2)$  給出的限定條件，如在  $\varphi_A = \varphi_B$  時， $\sin^2((\varphi_B - \varphi_A)/2)=0$ ，可以確定測量值是 (+, -) (-, +)，在  $\varphi_A = \varphi_B + 180^\circ$  時， $\sin^2((\varphi_B - \varphi_A)/2)=1$ ，可以確定測量值是 (+, +) (-, -)，在  $\varphi_B - \varphi_A = 120^\circ$ ，有  $\sin^2(120^\circ/2)=3/4$  的機會是 (+, +) (-, -)。藉此 Feynman 否定了用古典機率型計算機來模擬物理世界的可能性。

這一結果迫我們必須考慮量子計算機的可能性。一方面在理論上我們面臨以上的問題，另一方面，一旦我們晶片製作技術日益進步，量子效應也隨著晶片的縮小，而隨之增強，我們終究要面臨如何處理這些量子效應的問題。

發展量子計算機還有其他優點，它比古典計算

機 (不管是決定性型或機率型) 更有效率。所謂有效率是指當輸入  $N$  位數時，解決問題所需的步驟大約是  $P(\log N)$  次，其中  $P$  是一個固定的多項式。1985年 Deutsch 提出了第一個 Quantum algorithm，來決定一個由  $\{0, 1\}$  到  $\{0, 1\}$  的函數  $f$  是否為常數，亦即  $f$  是否為  $f(0)=f(1)=0$ ，或  $f(0)=f(1)=1$ 。由於問題簡單，並不能完全表現量子計算機的效率。但它卻表現了量子力學的特性：superposition 及 linearity。

1994年 Shor 提出了一個利用量子計算機做因數分解的方法。因數分解 (亦即給定一自然數  $N$ ，我們要尋找兩自然數  $p, q$ ，使得  $pq=N$ )，是一個很重要的問題。在所謂 RSA 公開密鑰系統 (public-key cryptosystem) 中，是否能很快地作出因數分解，決定了破解密碼的快慢。然而在古典計算機中，不管是決定性的或是機率性的，都無法提供有效率的 algorithm 來解決它。而 Shor 的 quantum algorithm 卻能有效率地做因數分解。這顯示量子計算機的效率遠大於古典計算機。

### II.2 量子密碼學

另一非局部性的應用在於量子密碼學。1984年 Bennett 與 Brassard 提出一個如何利用量子力學測量的特性，(即當我們對量子狀態作測量時，我們所得到的是測量作用子的本徵值，並且系統的量子狀態轉變成測量作用子的本徵向量。) 在 A, B 兩地建構一個密鑰分佈 (key distribution)。由於量子測量的特性，使得第三者很難竊取密鑰 (一旦第三者作了測量，就改變了量子狀態)，藉此保證密鑰的安全性。但是如何儲藏卻未解決。1991年 Ekert 建議利用 EPR state 的特性，來作量子密鑰。在 A, B 兩地 Alice 及 Bob 分別擁有 EPR 電子對中的一個電子。當要建

立量子密鑰時，他們可以藉著測量電子自旋，然後公開比對結果（但不公開測量自旋的方向），得到密鑰分佈，因而解決了量子密鑰儲藏的問題。

### II.3 量子資訊學

除了量子計算及量子密碼學外，量子理論與資訊理論的結合也形成了另一種具應用潛力的學科：量子資訊學 (quantum information)。簡而言之，在古典資訊理論中，我們所處理的基本對象是 bit，它是值域是  $\{0,1\}$ ，但是在量子資訊學中，我們所處理的基本對象是 quantum bit，簡稱 qubit，它代表了一個  $C^2$  上的一個向量，亦即古典中的 0 與 1 被我們視為兩個基底作標  $|0\rangle$  與  $|1\rangle$ ，而 qubit 就是  $|0\rangle + |1\rangle$ ，其中  $c_0, c_1 \in C$ 。而在  $C^2$  上的么正變換 (即  $UU^+ = U^+U = \mathbf{1}$ ) 則被稱作 quantum gate。許多 quantum gate 聯合起來則是 quantum networks。邏輯運算則被視為一個在 Hilbert space 的么正轉換。如

$$\text{Not gate} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|$$

$$\text{Controlled Not gate} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 11| + |10\rangle\langle 11|$$

一個有趣的事實是我們無法建構一部量子拷貝機 (quantum copy machine)。所謂拷貝機 (copy machine) 就是一部機器，其狀態是固定在  $|0\rangle$  (空白紙)，當我們輸入量子狀態  $|i\rangle$  時，經過拷貝的程序 (一個么正變換)，我們得到輸出狀態是  $|ii\rangle$

$|i\rangle$ ，亦即  $U(|i\rangle|0\rangle) = |i\rangle|i\rangle$ ，而當我們輸入狀態  $|i\rangle$  時 ( $|i\rangle|0\rangle$ )，輸出狀態是  $|i\rangle|i\rangle$ 。因此當我們考慮輸入狀態是  $|i\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$  時，根據么正變換的特性

$$U(|i\rangle|0\rangle) = U(1/\sqrt{2}(|0\rangle + |1\rangle)|0\rangle) = 1/\sqrt{2}(|0\rangle|0\rangle + |1\rangle|1\rangle)$$

所以這個么正變換不存在，亦即量子拷貝機不存在。這個現象稱為 no cloning theorem。

量子資訊學是一門正在蓬勃發展的領域，許多古典資訊理論的定理，在量子資訊學中有相應的定理，如古典中我們有 Shannon's data compression theorem，在量子資訊學中則有 quantum data compression theorem。但是由於量子理論的特性，我們有一些古典資訊理論所沒有的現象，如上述的 no cloning theorem。

根據量子力學，任何系統都無法從周圍的環境中，孤立出來。由於與周遭環境交互作用的結果，量子狀態的非局部性會改變，使得上述所提的所有過程無法有效的進行。對量子狀態的非局部性的進一步瞭解，可以幫助我們解決這個問題。

### III. 什麼是量子纏繞(quantum entanglement)

為了對量子狀態的非局部性作定量的分析，我們企圖找出一個函數，以這個函數值的大小來表示非局部性的強弱。

考慮一個由 A, B 兩個部分所組成的系統。  $H_A$  與  $H_B$  分別是代表 A 與 B 系統的 Hilbert space。(在量子計算機等應用上，我們所面臨的都是有限維數的 Hilbert space，如  $C^2$  等。) 假設  $\{|i\rangle_A\}$  ( $i=1, 2, \dots$ ) 代表  $H_A$  中一組相互垂直歸一化的基底，而

$\{ |i\rangle_B \}$  代表  $H_B$  中一組相互垂直歸一化的基底，整個系統則是由  $H_A \otimes H_B$  來代表， $\{ |i\rangle_A |j\rangle_B \}$  則為  $H_A \otimes H_B$  的一個相互垂直歸一化的基底。

一個量子狀態，可以是一個純態 (pure state)

$|\psi\rangle$ ,

$$|\psi\rangle_{AB} = \sum_{ij} C_{ij} |i\rangle_A |j\rangle_B$$

其中  $C_{ij}$  是複數係數，而且  $\sum_{ij} |C_{ij}|^2 = 1$ 。也可以是混態 (mixed state)

$$\rho_{AB} = \sum_{ij, i'j'} C_{ij} C_{i'j'}^* |i\rangle_A |j\rangle_B \langle i'|_A \langle j'|_B$$

$\rho_{AB}$  的本徵值都是介於 0 與 1 之間，其總和是 1。

如同古典狀態，在有些量子狀態中，在 A 所作的測量與 B 中的測量是互相獨立的。例如我們在 A 中找一個狀態

$$|\psi\rangle_A = \sum_i C_i^{(A)} |i\rangle_A$$

在 B 中也找一個狀態

$$|\psi\rangle_B = \sum_j C_j^{(B)} |j\rangle_B$$

那麼他們張量相乘作出的積態 (product state)

$$|\psi\rangle_{AB} = |\psi\rangle_A |\psi\rangle_B = \sum_{ij} C_i^{(A)} C_j^{(B)} |i\rangle_A |j\rangle_B$$

就是這樣的一個狀態。如果  $O_A$  ( $O_B$ ) 是在部分系統  $H_A$  ( $H_B$ ) 中的一個觀測作用子 (observable)，那麼同時在 A 及 B 做測量的結果是

$$O_{AB} \langle \psi | O_A O_B | \psi \rangle_{AB} = \langle \psi | O_A | \psi \rangle_A \langle \psi | O_B | \psi \rangle_B$$

$$\langle \psi | O_A O_B | \psi \rangle_{AB} = \langle \psi | O_A | \psi \rangle_A \langle \psi | O_B | \psi \rangle_B$$

即測量結果是彼此獨立。

很明顯的，並不是所有量子狀態都具有這樣的性質。如果一個純態是積態，那麼具有這樣的性質，我們稱它作 separable，否則我們稱它作 entangled。對混態而言，如果其本徵態都是 separable，那它也稱為 separable，否則是 entangled。如 EPR state  $1/\sqrt{2} ( |1\rangle_A |1\rangle_B + |2\rangle_A |2\rangle_B )$  不是

separable，而是一個 maximally entangled 的量子狀態。量子狀態的非局部性就是由 entangled states 所表現出來的。

每一量子態 entanglement 的情形並不相同。我們希望對量子狀態找出一個度量 entanglement 的函數。所根據的原則是我們把量子狀態視為一資訊資源，而加以操作，當我們的操作都是局部性時，並不會使量子狀態 entanglement 的情況增加。所謂局部性的操作是指不對整個系統作操作，而只是對部分系統 A 或 B 作操作，如我們測量 EPR state 中的一個電子自旋的情形。

那些操作是我們可以在部分系統上操作的呢？這些操作可以分成二大類：

第一類是局部量子作用 (local quantum operations, LO)，這是我們對於部分系統所能做的量子操作。

(1) 系正轉變：

$$\rho \rightarrow U\rho U^\dagger$$

其中  $U = U_A \otimes I$  或  $I \otimes U_B$ ， $U_A$  ( $U_B$ ) 是在  $H_A$  ( $H_B$ ) 上的么正變換。

(2) Von Neumann 測量：

$$\rho \rightarrow \{ \rho_K, p_K \}$$

我們對 A 或 B 系統作測量，有  $p_K$  機率，其結果是  $\rho_K$ ，其中  $p_K$  不一定要等於 1。

(3) 與一輔助的量子態  $\rho_c$  作積：

$$\rho \rightarrow \rho \otimes \rho_c$$

其中  $\rho_c$  是一無相關系統上 Q 的量子態。

(4) 遮去全系統中某個部分系統 Q

$$\rho \rightarrow \text{Tr}_Q \rho$$

其中 Q 是 A 或 B 的部分系統， $\text{Tr}_Q$  表示對 Q 部分求 trace。

第二類是古典通訊 (classical communication,

CC), 意即在 A 或 B 所得的操作結果可藉古典的方法, 由 A 傳到 B 或由 B 傳到 A。藉此 B (或 A) 可以知道在 A (或 B) 的操作結果。因此當我們在操作 LO 時, 會依據上一次我們在部分系統上作 LO 的結果來繼續作操作。這樣一來, 我們能更有效地操作量子狀態。

這二大類操作綜合稱作 LOCC。我們希望找到一個度量函數, 能在 LOCC 操作下, 不會增加。這一點很類似於熱力學第二定律。Peres 據此推論, 如同熱力學中有唯一的溫度函數, 在量子態中也存在唯一的 entanglement 的度量函數。目前我們所能掌握的只有對純態 (pure state) entanglement 的了解。對於混態 (mixed states) 存在許多不同的度量函數。這當然是不夠的, 因為一般的情形是系統處於混態中。

以下我們列出一些 entanglement 度量函數的定義。 $\rho$  是一個量子狀態。

(1) entanglement of distillation  $E_D$ : 我們可以從  $\rho^{\otimes n}$  中, 利用 LOCC, 萃取出 k 個 EPR state (即 maximally entangled states), 在 n 趨于無限大時, 那麼 k/n 的極限值, 稱為  $E_D$ 。

(2) entanglement of formation  $E_F$ : 我們可以 k 個 EPR state 中, 利用 LOCC 產生  $\rho^{\otimes n}$ , 那麼當 n 趨於無限大時, k/n 的極限值, 稱為  $E_F$ 。

(3) relative entropy of entanglement  $E_R(\rho)$ : 令  $S(\rho|\sigma)$  代表  $\rho$  對於  $\sigma$  的相對熵, 即

$$S(\rho|\sigma) = -\text{tr}(\rho \log_2 \rho) - \text{tr}(\rho \log_2 \sigma)$$

它代表統計上  $\rho$  與  $\sigma$  的一種距離。那麼我們定義

$$E_R(\rho) := \inf_{\sigma \in \text{separable}} S(\rho|\sigma)$$

其中  $\sigma$  屬於 separable state, 而 inf 是在這個 separable

states 的集合上取。 $E_R$  代表  $\rho$  到 separable states 所成集合的距離。

由定義可以看出  $E_D$  和  $E_F$  是互補的操作型定義, 而  $E_R$  則是從理論上考量所得的定義。對於純態而言, 這三者都是一樣, 然而對混態而言三者不一定一樣。

有人認為 von Neumann entropy 在關於混態 entanglement 的討論中並不適用, 原因在於, 它是古典資訊理論中 Shannon entropy 的推廣。而 Shannon entropy 是用來描述古典機率的不確定性, 但是具有非局部性的量子狀態是無法用古典機率來描述, 因此 von Neumann entropy 必須作修正。

有人認為  $E_D, E_F$  所考慮的都是 asymptotic 的行為 ( $n \rightarrow \infty$ ), 但實際上, 我們處理的都是有限個數的行為, 這兩者不一定相同。另外也有人認為當 A 與 B 系統不一樣時, 由 A 所測的 entanglement 也不一定與 B 所測得的 entanglement 一樣。

這些討論指出 entanglement 複雜的行為。從物理的角度, 我們更希望藉著對 entanglement 度量函數的尋找, 來更了解量子狀態的非局部性行為, 為其他應用領域提供更多的可能性。