專輯前言：
量子資訊科學的發展與展望

文/張為民

一、緣起

量子資訊科學是物理學與資訊科學相結合的一個新興交叉領域，涉及物理、數學、電腦、通訊、工程和材料等多門學科。它的未來發展勢將對整個基礎科學和工程科學，包括電腦科技、通訊科技、材料工程、精密測量技術、量子基礎科學及資訊理論科學帶來一次巨大的變革。這個新興領域的原始構想起源於二十世紀八十年代，著名物理學家 Richard Feynman，美國阿貢國家實驗室 Paul Benioff 博士，英國牛津大學 David Deutsch 教授及美國 IBM 公司 Charles Bennett 博士等試探如何將量子力學的概念應用到電腦的建構中。而量子資訊科學取得突破性的進展則是發生在不到十年內的事。1994 年 AT&T 公司的 Peter Shor 博士証明，量子電腦(quantum computer)能非常快速地進行大因數分解，這在傳統資訊領域裡被認為是無法有效計算的一個 NP 問題。正是 Peter Shor 的開創性工作導致了今天量子計算(quantum computation)和量子資訊(quantum information) 的研究熱潮。

而迫使科學家們全力投入量子資訊科學這一新興領域的另一主要原因是現有資訊處理系統的功能已接近於極限。半導體工業在過去 30 年的發展告訴我們，幾乎每隔兩年的電腦 CPU 就增長一倍。而每個晶片上集成的電晶體數目也隨時間呈指數增長。 這個被稱為摩爾定律（Moor Law）的經驗法則預示，到 2010 年，一個晶片上的電晶體數目將超過 10 億個。10 多年以後電腦存儲單元將是單個原子及單個電子。在以原子為基石的微觀世界裡，光與電的行為將不再服從古典物理規律，取而代之的是量子物理規律。如何在原子尺度上設計和建構資訊處理的實用元件即是近年來最具有挑戰性的奈米科技 (nanoscience and nanotechnology)。然而，當前支配高科技發展的資訊處理及電腦運算仍以古典物理法則為基礎，毫無疑問，資訊科學的進一步發展勢必要借助於量子力學的原理和方法。

1999 年，美國國家科學基金會(National Science Foundation)為這一快速成長的領域舉辦了一次綜合物理、數學、電腦和資訊工程及工程學等部會的研討會，在此研討會上，人們以「新科學的誕生」(Birth of A New Science)來描述這一結合基礎科學和工程學研究與教學的新興交叉領域，並命名為「量子資訊科學」(Quantum

Information Science, 簡稱 QIS)。它是將量子力學與資訊理論和電腦科學相結合, 以量子力學的態疊加原理及量子子系統間量子態的糾纏性為基礎, 研究資訊處理和電腦運算的一門新科學。由於量子特性在資訊領域中的獨特功能, 在增大資訊容量、提高運算速度、確保資訊安全等方面將突破現有傳統資訊系統的極限, 量子資訊科學在過去幾年中的發展可以用突飛猛進來形容。

二、QIS 及其發展現況

傳統上, 構成各種資訊的基本單位, 位元(bit), 是由二進位制中的 0 和 1 表示。所有的信號都是由 0 與 1 來組成、儲存、運算及傳遞。物理上, 位元是用一個實際物理系統來實現。比如說用一個開關, `關'代表 0, `開'代表 1; 也可以用光纖中的光脈衝, 磁帶中的磁化性質等來實現。在傳統的電腦裡, 0 與 1 是由電位的高低來表示, 這種用古典位元存儲和處理資訊的手法稱為古典資訊(classical information)。如果我們用量子力學中兩個互相獨立正交的量子態, 如光子的兩個極化態、或電子、核子自旋的兩個自旋態、或原子的基態和激發態來實現資訊中 0 與 1 的兩個狀態(記為 $|0\rangle$ 和 $|1\rangle$), 這樣的位元稱為量子位元(quantum bit, 簡稱 qubit), 用量子位元來存儲和處理資訊則稱為量子資訊(quantum information)。

量子資訊與古典資訊最大的不同在於: 古典資訊中, 位元只能處在一個狀態, 非 0 即 1; 而在量子資訊中, 量子位元(量子系統)可以同時處在狀態 $|0\rangle$ 和狀態 $|1\rangle$ 中。量子位元的這一特性來自量子力學的狀態疊加原理: 即如果 $|A\rangle$ 和 $|B\rangle$ 是兩個互相獨立正交的量子態, 它們的任意線性疊加也是一個量子態。這使得每個量子位元的組態比傳統位元多得多, 量子位元能利用不同的量子疊加態記錄不同的資訊, 即同一位元可擁有各種不同的資訊。因此, 同樣由二個狀態組成的物理裝置, 量子位元的功能比普通位元強得多。

另一方面, 在古典的資訊存儲器(register)中, 資訊是用各種位元序列來表示的。類似地, 在量子資訊存儲器中, 資訊則是用量子位元序列態來表示。所不同的是, 多個量子位元序列態可以用各個量子位元序列正交態的一個線性疊加態來表示。以一個由三位元組成的序列為例, 可以用八個二進制組態表示: 000, 001, 010, …, 111, 分別代表 0 到 7 這八個數字。由這三位元序列構成的古典暫存器(register)每次只能記錄這八個數字中的一個, 但對應的量子暫存器可以在同一時刻(instant time)以量子位元序列正交態的線性疊加同時記錄這八個不同的數字。這一簡單結果顯示量子資訊處理器所具有的無窮潛力, 因為它意味著用更多的量子位元組成的暫存器, 其存儲量子資訊的速度將呈指數增加。四個量子位元可同時存儲 16 個不同的數字, n 個量子位元可同時存儲 2 的 n 次方個數字。換句話說, 在相同位元數下, 量子資訊存儲器記錄資訊的速度是目前古典資訊存儲器的 2 的 n 次方。用 500 量子位元就能在瞬間存儲比已知宇宙中所有原子的總數還要多的數字。隱藏在量子資訊中如此驚人的功能正是量子電腦所夢寐以求的。

更進一步地, 資訊運算是由邏輯閘(logical gate)作為其基本元件來實現。量子資訊則由量子邏輯閘構成其運算元件。與古典資訊不同, 量子資

訊處理器中的量子邏輯元件對應於數學上的一個么正變換矩陣(unitary matrix)，是一個可逆過程，即過程本身無能量耗損。更為重要的是量子運算還提供了量子平行處理(quantum parallelism)的一個可行性方案。所謂量子平行處理就是對所求函數與對應自變量的各種取值通過量子態疊加原理及量子態間的糾纏特性進行一么正變換(即一量子邏輯運算)，在同一時刻一次完成。量子資訊中的量子糾纏(quantum entanglement)指的是兩個或多個量子位元之間存在的非古典關聯。例如兩個量子位元可構成糾纏態(|00□+|11□)，其特性是它不能被分解為兩個單獨量子位元態的乘積。因此糾纏態內量子位元間具有很強的相干性或關聯性，其中一個量子位元狀態被改變或測量同時決定了糾纏態內所有其它位元狀態的相應變化。由此，量子運算完全摒棄古典運算法則，其大容量平行計算的能力是傳統電腦望塵莫及的。一台 32 個量子位元的電腦其能力相當於數十億部傳統電腦作平行運算。如用量子電腦做因數分解，以目前最快速的電腦而言，大概要花上數十億年的時間，才能求出一個 400 位的數字的所有質因數，而量子電腦可能只需要幾小時甚至幾分鐘的時間就能完成。

量子糾纏不僅為量子運算提供最有效的平行處理方法，它同時也是實現量子通訊所必備的工具。這是因為量子糾纏具有另一重要特性，就是它的非定域性(Non-locality)。量子力學中的非定域性是指一旦兩量子系統的狀態(比如是兩光子的極化態)構成糾纏態(例如|00□+|11□)，則不管後來這兩個量子系統間的距離被分隔多遠，並且它們之間可能不再存在力學上的交互作用，只要它們仍保持在糾纏態，它們之間超強的量子關聯性不會改變。量子糾纏態的這種非定域性是實現量子遠距(隱形)傳輸(quantum teleportation)、超密集編碼(superdense coding)及量子密鑰分佈(quantum cryptography key distribution)的理論基礎。

由於量子態的疊加性(quantum superposition)及量子各系統量子態間的糾纏性(quantum entanglement)的獨特功能，使得量子資訊在增大資訊容量、提高運算速度、確保資訊安全等方面大大地突破現有古典資訊系統的極限。簡單地說，量子資訊的研究主要包括量子計算、量子通訊及量子資訊理論等三大發展方向，近年來在理論和實驗上都取得重大的突破。其中在量子算法(quantum algorithm)研究方面，Peter Shor 於 1994 年提出大整數質數分解的第一個量子算法，隨後 AT&T Bell 實驗室 Lov Grover 在 1996 年提出了量子搜尋算法，從而開創了量子計算的熱潮。而在量子電腦(quantum computer)研究方面，自 1995 以來，已提出量子電腦的多種方案，主要包括利用原子和光腔相互作用(Cavity QED)、冷束縛離子系統(Trapped Ions)、電子或核自旋共振(NMR)、量子點(Quantum Dots)、超導約瑟芬森結(Josephson-Junction)及光子晶格(Photonic Lattice)等量子系統，2001 年美國 IBM 公司阿曼頓實驗室的科學家已建構了七位元的核磁共振量子電腦。到能建構二十多個量子位元的量子電腦時，就可以超過目前高速電腦的功能。在量子密碼學(quantum cryptography)研究上，西歐和美國進展最快。英國於 1993 年首先在光纖傳輸長度為 10 公里中實現光子相位編碼量子解碼鑰分發。1997 年，美國洛斯阿拉莫斯(Los Alamos)國家實驗室創造了光纖量子密碼通訊距離的新紀錄，成功地在長

達 48 公里的地下光纜中傳送量子密碼本。1999 年，瑞典和日本合作，在光纖中成功地進行了 40 公里長的量子密碼通訊實驗。2000 年中國大陸在 850 奈米的單模光纖中也完成了量子密碼通訊示範性實驗。現在人們已開始計劃在人造衛星與地球間建立量子密碼通訊實驗。在量子隱形傳輸(quantum teleportation)方面，1997 年，奧地利學者在國際上首次實現了未知量子態的遠距傳輸，成功地將一個量子態從甲地的極化光子傳送到乙地的極化光子上，1998 年，美國加州理工學院的 H.J.Kimble 和合作者用光的壓縮態(squeezed state)，成功地將一束光從一個房間轉移到另一個房間，為量子隱形傳輸跨出了革命性的一步。這些成就使人們認識到用量子態作為資訊載體，通過量子態完成大容量資訊的瞬間傳輸，並為實現原則上不可破解的量子保密通訊提供了可行性的示範，同時也開闢了量子科技更為廣泛，前景更為誘人的應用領域。而量子資訊理論本身，也開創一個全新的資訊理論研究，包括計算的複雜性問題的分析，編碼糾錯理論及量子通道之數學模型的發展等等，都必須在量子力學的框架上進行重新的定義及研究。

本期我們邀請到國內九位專家撰寫量子資訊各個領域的專文，包括成功大學李建二教授對量子隱形傳輸的討論、盧炎田教授關於量子點量子電腦的研究、國家高速電腦中心蘇正耀教授對量子計算，特別是量子算法的概述、中研院陳啟東研究員關於超導微結構量子電腦的討論、國立中正大學韓殿君教授關於利用光子晶格實現量子電腦的構想、國立東華大學鄭王曜教授對量子控制方面的研究、彰化師大郭西川教授對於冷束縛離子量子電腦的討論及國家理論科學中心徐立義博士對量子密碼學的討論及目前就讀伊利諾大學的魏子傑先生對量子光學在量子通訊方面的應用的探討等等，幾乎涵蓋了目前量子資訊各個不同方面的研究。

三、展望

目前量子資訊的研究在國際上剛剛起步。為因應量子資訊這一新科學的到來，近年來世界各地相繼成立了以量子資訊及量子電腦為主體的研究中心、研究所及研究實驗室，包括英國的量子計算研究中心(Center for Quantum Computation)及由 NSF 資助的加州理工學院的量子資訊研究所(Institute for Quantum Information)。2000 年美國將量子電腦列為美國的國家科技戰略目標。2001 年日本開始將量子資訊研究作為新的五年科技基本計畫的四大重點之一，投入大量的研究經費。世界各主要大學間也都成立了量子資訊與量子電腦的研究群。像美國加州理工學院、麻省理工學院與北加州大學組成的量子資訊合作群，及史丹福大學、伯克萊大學、麻省理工學院與 IBM 公司組成的 NMR 量子電腦研究群。中國大陸也有十多所大學成立了相應的研究中心及實驗室，並將量子資訊列為國家自然科學基金優先資助領域。 歐洲各國在歐盟的資助下成立許多整合型的研究群體。

臺灣目前在量子資訊方面的研究才剛引起人們的關注。國立成功大學一年前創立了國內第一個涵蓋理論與實驗的量子資訊研究團隊，並於今年成立了台灣第一個量子資訊科學研究中心，同時從今年八月開始將取得奈米國家型科技計劃支助的第一個以奈米元件研究量子資訊的學術卓越計畫。無論在理論或實驗上，國際間開始重視與投入量子資訊發展只是近幾年的事，而且此研究領域的切入，

並不特別需要在某些領域已很有經驗，我們完全站在與其他國家同等開始的立足點上，現在加入這一令人興奮的科學研究，我們有很大機會，即使不是站在最領導的地位，至少與世界最尖端的研究同步。為使臺灣在這一新領域的研究趕上和超越國際研究水準，我們應結合物理、數學、資訊工程和奈米材料科學等學科，建構一支跨學科、跨領域的理論和實驗研究隊伍，朝設立類似美國加州理工學院的量子資訊研究所(Institute for Quantum Information)這樣一個研究機構的方向發展，積極有效地參與量子資訊這一新興領域的國際競爭。

如果說二十世紀的第三次工業革命是結合微電子學技術、超大規模積體電路製造技術與電腦技術和通訊網路技術而形成今天的「電子工業」(即半導體工業)，那麼毫無疑問，現在的第四次工業革命將是結合奈米技術、奈米元件製造技術與量子計算技術和量子通訊技術而形成未來的「量子工業」(Quantum Industry)。想要在二十一世紀擠身世界先進工業國的行列，開發對量子資訊的研究已是刻不容緩。

參考資料：

[1] R. P. Feynman, Int. J. Theor. Phys. **21**, 467 (1982).

[2] P. Benioff, J. Stat. Phys. **22**, 563 (1980).

[3] C. H. Bennett, Int. J. Theor. Phys. **21**, 905 (1982).

[4] D. Deutsch, Proc. R. Soc. Lond **A400**, 97 (1985).

[5] P. W. Shor, in proceedings, 35th annual symposium on foundations of computers science, IEEE Press, Los Alamitos, US. (1994).

[6] NSF report: Quantum Information Science, http://www.nsf.gov/pubsys/ods/getpub.cfm?nsf00101. (1999)

[7] 更詳盡的關於量子資訊科學的討論可參閱本期各位作者的專題討論及 M. A. Nielsen and I. L. Chuang 的專著：“Quantum Computation and Quantum Information”, Cambridge University Press (2000).

執編簡介

張為民，美國德克塞爾大學物理博士，現為國立成功大學物理系教授，國內研究量子資訊的奈米國家型學術卓越計劃主持人。研究專長：粒子物理與場論、凝態物理多體理論，非線性動力學與量子混沌，原子核物理理論、數學物理。目前專致於量子資訊的研究與發展。

Email:wzhang@mail.ncku.edu.tw