量子資訊科學：
可能成為二十一世紀工業發展的核心

成功大學物理系　張爲民

一、引言

眾所周知，二十世紀的工業(以半導體工業及資訊工業爲核心)是依賴於十九世紀已發展完備的古典物理學，特別是古典電磁理論爲其基礎。今天，我們已進入二十一世紀，自然地，二十一世紀工業發展的核心將成爲人們普遍所關心的問題。

當今最受世界各國政府及工業界重視的，也是學術界和產業界研究探討最熱門的課題是在過去二十年中發展起來的奈米科技。毫無疑問，在未來的一段時間內，奈米科技仍將是學術界與產業界全力推動的一個主要領域。但一個有趣且也是值得深思的問題是，奈米科技會將二十一世紀的工業發展帶向一個什麼樣的遠景？

奈米科技是以奈米尺度(十的負九次方米)爲基本物質結構進行材料加工及元件製造的新科技。作爲一位物理研究工作者，我們必須自問，奈米科技的基礎理論是什麼？

奈米結構是介於宏觀結構(服從古典物理規則)與微觀結構(遵守量子物理規則)之間的一種過度物質結構，其本身並沒有相應的一套完整的基礎理論爲其支柱。以個人觀點，我認爲奈米科技應該是進入下一個工業時代的過度階段。而下一個工業時代(即二十一世紀工業的核心)將會是以原子爲其基本結構，以量子物理爲其基礎理論的量子科技和量子工業。

其實，過去二十年來奈米科技的發展已使我們學會如何改變及重組材料內部的原子結構，製造由有限個原子或分子組成的奈米元件。自然地，下一步的科技突破將是如何操控單個原子本身的微觀狀態(即原子的量子態)，這就是量子科技的核心問題。二十世紀我們已學會成熟地搬動物質表面單個原子技術，但卻未能掌握操控量子態的有效方法。

除了奈米科技以原子爲其最基本的構造元素外，光電科技最基本的構造元素是光子與電子。目前的光電科技(包括半導體科技)所處理的是巨量光子與巨量電子的效應，如何操控和處理單個光子及單個電子的行爲同樣是量子科技的主要研究課題。

因此，簡單地說，量子科技就是如何操控單個原子，單個電子及單個光子的量子態行爲。而二十一世紀工業發展的核心將是由量子科技主導的量子工業，其中用原子、電子及光子的量子態來處理資訊科學是當前最爲熱門的量子科技之一，被稱之爲「量子資訊科學」(Quantum Information Science, 簡稱 QIS)。由二十世紀資訊工業帶給我們的影響力可以預見，量子資訊科學將是二十一世紀工業發展的核心。本文將著重介紹這一新領域的發展現況及未來展望。

二、量子資訊科學的起源

量子資訊科學這個新興領域的原始構想起源於二十世紀八十年代初，美國阿貢國家實驗室 Paul Benioff 博士，著名物理學家 Richard Feynman，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近十年內的事。1994 年 AT&T 公司的 Peter Shor 博士証明，量子電腦(quantum computer)能有效快速地進行大因數分解，這在傳統資訊領域裡被認爲是一個無法有效計算(NP)的問題。正是 Shor 對量子計算的開創性工作導致了今天量子計算(quantum computation)和量子資訊(quantum information)的迅速發展。

而迫使科學家們投入量子資訊科學這一新興領域的研究的另一主要原因是現有資訊處理系統的功能已逐漸接近於極限。半導體工業在過

去 30 年的發展告訴我們，幾乎每隔兩年(嚴格的說每十八個月)，微處理速度就增快一倍。而每個晶片上集成的電晶體數目也隨時間呈指數增長。這個被稱爲摩爾定律(Moor Law)的經驗法則預示，到 2015 年，一個晶片上的電晶體數目將超過 10 億個，而電腦的存儲及處理單元將是單個原子及單個電子。在以原子爲基石的微觀世界裡，光與電的行爲將不再服從古典物理規律，取而代之的是量子物理規律。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基本原理和方法。這是產生量子資訊科學的另一個原動力。

概括的說，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、電腦、通訊、工程和材料等多門學科。它是以量子態疊加原理及量子子系統間量子態的糾纏性爲其理論基礎，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遠遠突破現有傳統資訊系統的極限，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。

三、量子位元

爲了更直接的了解量子資訊科學，我們有必要對傳統資訊與量子資訊作一比較。資訊的基本單位是位元(bit)，數學上是由二進位制中的 0 或 1 來表示;物理上位元是由一個實際物理系統所處的非 0 即 1 的狀態來實現;在傳統的電腦裡，0 與 1 是由電位的高低來表示。所有的信號都是由多個位元之 0 或 1 狀態來組成、儲存、運算及傳遞。這種用古典位元存儲和處理資訊的手法就是我們熟知的古典資訊(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(記爲|0〉和|1〉)，這樣的位元稱爲量子位元 (quantum bit，簡稱 qubit)，用量子位元來存儲和處理資訊則稱爲量子資訊(quantum information)。

四、量子態疊加原理與量子資訊

量子資訊與古典資訊最大的不同在於: 古典位元只能處在一個狀態，非 0 即 1；而量子位元(量子系統)可以同時處在狀態|0〉和狀態|1〉中，即|0〉和|1〉的任意線性疊加也是一個量子態，這就是量子力學中的量子態疊加原理(superposition principle of quantum states)。從而一個量子位元可擁有記載各種不同資訊的無窮多方式。因此，同樣由二個狀態組成的物理裝置，量子位元的功能比古典位元強得多。

另一方面，在資訊暫存器(register)中，資訊是用各種位元序列來表示的。類似地，在量子資訊暫存器中，資訊則是用量子位元序列態來表示。形式上，多個量子位元的組態序列數與傳統位元的同樣多，但不同的是，量子位元的組態空間比古典組態空間大得多，原因是一個多量子位元系統的任一量子態可以用量子位元序列正交態的一個線性疊加來表示，而古典位元無此特性。以一個由三位元組成的序列爲例，可以用八個基本的組態表示: 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將這八個不同的數字同時記錄在同一個量子態中。這一簡單結果顯示量子資訊處理器所具有的無窮潛力，因爲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呈指數增加。一個由 n 個量子位元組成的暫存器在同一個量子態可一次存儲 2 的 n 次方個符號。 換句話說，在相同位元數下，量子資訊暫存器記錄資訊的速度是目前古典資訊暫存器的 2 的 n 次方。一個有 32 個量子位元組成的存儲器的存儲速度是傳統電腦的數十億倍;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。

五、量子糾纏與量子資訊

更進一步地，資訊運算是由邏輯閘(logical gate)作爲其基本元件來實現的。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。更爲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可能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(即一次量子運算)，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爲兩個單獨量子位元態的乘積，其中一個量子位元狀態決定了糾纏態內另一個量子位元的狀態，因此糾纏態內量子位元間具有很強的相干性或關聯性。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。這就是 shor 所告訴我們的量子電腦的威力，也是用量子電腦破解目前網路 RSA 加密系統的主要原理。

量子糾纏不僅爲量子計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依賴的主要工具。這是因爲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)及量子密鑰分拆(quantum cryptography key distribution)的理論基礎。

六、量子資訊之主要研究領域

據以上特性，量子資訊的研究被主要分類爲量子計算、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 年提出了搜尋龐大無序資料庫的量子搜尋算法，從而開創了量子計算的熱潮，尋找新的量子算法是這個研究領域的主要目標，其中以發展量子模擬的量子算法最具挑戰性。

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操控光腔中原子的超精細態(Cavity QED)、利用光電控制離子精細態的冷束縛離子系統(Trapped Ions)、利用磁場操控固態或液態系統中某些原子核自旋共振(NMR)、光電控制下量子點(Quantum Dots)中電子的自旋態或電子空電對的激子態、超導約瑟芬森結(Josephson-Junction)中的電荷、相位或磁通量自由度及利用雷射光束建構光子晶格(Photonic Lattice)並操控置於其中之中性原子等量子系統。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爲 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。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，爲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爲資訊載體，通過量子態完成大容量資訊的瞬間傳輸，並爲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爲廣泛，前景更爲誘人的應用領域。

而對資訊理論本身，也開創一個全新的量子資訊理論研究，包括量子計算和量子通訊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。而量子資訊的研究又進一步促進對量子基礎理論的認識及發展，包括多體系統內在的量子糾纏性的理論發展、量子系統的精密量測、特別是無破壞性量測的技術發展及量子控制方法的研究等等，開辟了許多新的研究方向

七、未來展望

目前量子資訊的研究在國際上剛剛起步。爲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爲主體的研究中心、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)及由美國 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爲美國的國家科技戰略目標。 2001 年日本也將量子電腦研究作爲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，並將量子資訊列爲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。成功大學於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，同時從今年八月開始取得奈米國家型科技計劃支助的第一個以奈米元件(量子點)研究量子資訊的學術卓越計畫，並成爲國內第一個量子資訊研究中心。國科會工程處資訊學門最近也成立了「量子計算」研究的推動小組。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，現在加入這一領城的研究，我們有很大機會，即使不是站在最領導的地位，至少也與世界最尖端的研究同步。爲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、資訊、工程和材料科學等學科，建構一支跨學科、跨領域的理論和實驗研究隊伍，積極有效地參與量子資訊這一新興領域的國際競爭。

最後，我想指出，如果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，第四次工業革命將是結合量子技術及量子資訊而形成未來的「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，開發對量子資訊科學的研究已是刻不容緩。

參考資料：

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

[2] 更詳盡的關於量子資訊科學的討論可參閱 M. A. Nielsen and I. L. Chuang 的專著：*"Quantum Computation and Quantum Information",* Cambridge University Press (2000).