你抓得到我嗎—非0非1的量子資訊

當孩子們看到科幻電影裡太空人由「時空隧道」從一個星球送到另一個星球時，一定會幻想自己也能身歷其境，樂在其中；當情人們透過網路卿卿我我時，也多麼希望資訊的傳遞能超越光的速度、資訊的容量能包含一切。這都已不再是遙遠的夢想，透過新崛起的資訊科技—量子資訊，在實驗室裡，真實世界的夢想正一步一步地實現…

張為民

在e世代的今天，幾乎每個人都已身不由己地被捲入資訊的漩渦中。網際網路成了我們了解世界、認識世界最有效的窗口，行動電話、電子郵件也已成為人們溝通最便利的橋樑。

資訊科學的快速發展，在提高人類生活質量和推動社會文明進步方面，發揮了令人驚嘆的作用，但人類對資訊的需求似乎是無止境的。 商業網路化、生活網路化、社會網路化、家庭網路化、…隨著對資訊需求的日益增加，人們必須不斷地推動資訊科技的進一步發展，但現有的資訊處理系統功能已接近極限。

在過去五十年中，幾乎每隔兩年，電腦的速度就加快了一倍，而每個晶片上集成的電晶體數目，在過去三十年中也隨時間呈指數增長。 這個稱為摩爾定律的經驗法則預示，到二〇一〇年，一個晶片上的電晶體數目將超過十億個。十多年以後，電腦存儲單元將是單個原子。在這樣微小的世界裡，將無可避免地造成電路間的相互干擾，系統溫度的急速升高及能量損耗的大量增加，這是現有資訊處理系統必須面對的危機。但正如我們常說的，危機即是轉機，當電腦越做越小，速度越來越快，量子力學的效應就不能不列入考慮，電子技術面臨的危機正是導致量子技術興起的轉機。

量子力學是二十世紀初發展起來與相對論力學並列的兩大近代物理理論之一。 量子力學描述原子世界的物理特性，而相對論力學則描述高速（接近光速）粒子的物理現象，二十世紀物理科學完全建立在這兩大理論上。它們為人類認識自然界—從小至構成物質最基本的夸克到大至整個宇宙的產生及演變—奠定了基礎，而量子力學對過去半個世紀的工業技術發展也發揮了不可忽視的作用。從半導體技術的發展，各種新材料的發現到最近奈米技術的產生，無一不是以量子力學為其基石。

如果說二十世紀是電子技術的全盛時期，則二十一世紀將會是量子技術創造成果的世紀。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必須借助於量子力學的原理和方法，而量子力學究竟會對資訊處理和電腦運算速度產生什麼樣的影響呢？

直觀地想像，電腦和各種數位影音設備能展現如此複雜的影像世界和動聽的音樂，其內部資訊處理一定非常複雜。但事實上，在電腦及數位器材內構成各種資訊的基本單位—位元，卻極為簡單，是用二進位制中的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。以開關為例，「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，這種用傳統位元存儲和處理資訊的手法稱為古典資訊。如果我們用量子力學中光子的兩個極化狀態，或電子、核子自旋的兩個自旋狀態，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>和 | 1> ），這樣的位元稱為量子位元，用量子位元來存儲和處理資訊，則稱為量子資訊。

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>和狀態 | 1 > 中。量子位元的這一特性來自量子力學的狀態疊加原理，即如果狀態 | 0>和 | 1>是兩個互相獨立的量子態，它們的任意線性疊加 |ψ> =α| 0 > +β | 1> 也是某一時刻的一個量子態，而係數 α 和 β 的絕對值的平方則描述系統分別處在 | 0>和 | 1>的機率。這使得每個量子位元的組態比古典位元多得多，量子位元能利用不同的量子疊加態記錄不同的資訊，在同一位置上可擁有不同的資訊。因此，同樣由二個狀態組成的物理裝置，量子位元的功能比古典位元強得多。然而量子態是非常不穩定的，並且根據量子力學的測量理論，任何觀測都會立刻改變系統的狀態，因此量子資訊的實際可行性一直受到懷疑。但令人驚訝的是，這正是保證量子資訊的絕對安全性，因為任何竊聽（測量）者都會被發現。

量子態ψ可以同時處在狀態 | 0>和 | 1>之中，即為 | 0>和 | 1>的任意線性疊加。

http://www.qubit.org/intros/comp/comp.html

由於量子力學具有這些特性，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將突破現有傳統資訊系統的極限，一門新的科學分支—量子資訊科學也就應運而生。它是將量子力學與資訊學相結合，以量子力學的狀態疊加原理為基礎，研究資訊處理的一門新興科學。量子資訊科學包括量子計算（量子電腦）和量子資訊（量子通訊和量子密碼）兩大方面，近年來在理論和實驗上都取得重大的突破。可以預見，一旦量子資訊實用化，將再一次改變我們今天的產業結構和生活方式。

量子計算

很多人都讀過名物理學家費曼（R. P. Feynman）的故事，但也許沒有很多人知道他生前（二十世紀八十年代初）曾認真地研究過用量子力學理論、實現量子計算並建構量子電腦。費曼的構想雖然在當時引起了部分科學家很大的興趣，但大家對量子計算的概念基本上停留在「原則上可行」的狀態，原因之一是由於量子態的測不準特性和量子系統容易受環境雜訊干擾，使量子運算很容易出錯。因此，在八十年代，這股熱潮並沒有對新科技的發展產生很大的衝擊。

直到一九九四年，量子計算的基本問題取得突破性的進展。美國電話電報公司（AT&T）電腦專家蘇爾（P. Shor）證明量子電腦能非常快速地進行大因數分解，他還發展出第一套量子算法編碼。而這兩項成果在資訊領域裡靠傳統電腦是無法有效實現的，從而使量子電腦的研究進入實驗時代。目前，已有許多國家建立了量子電腦的研究中心和實驗室，並投入相當可觀的研究經費。簡單地說，量子計算就是利用量子態進

http://www.phy.hr/~dpaar/fizicari/feynman.html

行資訊處理的方法，其實體裝置稱為量子電腦，是一類遵循量子力學規律進行高速數學和邏輯運算、儲存及處理量子資訊的物理裝置。基本原理就是透過量子力學的運用，將電晶體壓縮到原子般大小，然後在極小的面積上放入數十億顆量子電晶體，進而利用量子態的疊加性和相干性進行資訊運算、儲存及處理。

在傳統電腦中，運算對象是各種位元序列，在量子電腦中，運算對象是量子位元序列，所不同的是，量子位元序列可以處在各種正交態的疊加態上。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每次只能記錄這八個數字中的一個，但量子暫存器可以在同一時刻以量子態疊加同時記錄這八個不同的數字。

這一簡單結果顯示量子電腦所具有的無窮潛力，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十六個不同的數字，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，量子電腦記錄資訊的速度是目前傳統電腦的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，正是人類夢寐以求的。

另一方面，電腦運算是由邏輯閘做基本元件，量子電腦則由量子邏輯閘構成其運算元件。與傳統電腦不同的是，量子電腦中的量子邏輯元件對應於數學上的一個么正變換矩陣，例如，量子邏輯閘不僅可以將 | 0>態和 | 1>態做交換，還可以將 | 0>態和 | 1>態變為它們的任意疊加態。

更為關鍵的是，量子運算會將暫存器內的量子位元變換為糾纏態。量子糾纏指的是兩個或多個量子系統之間具有在非古典的強關聯，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時，也決定了糾纏態內所有其它位元狀態的相應變化，這類特殊量子態提供了量子平行處理的可行性。量子平行處理就是對量子態每一疊加分量進行么正變換，所有這些變換在同一時刻一次完成，並按一定的機率幅疊加起來得出結果。

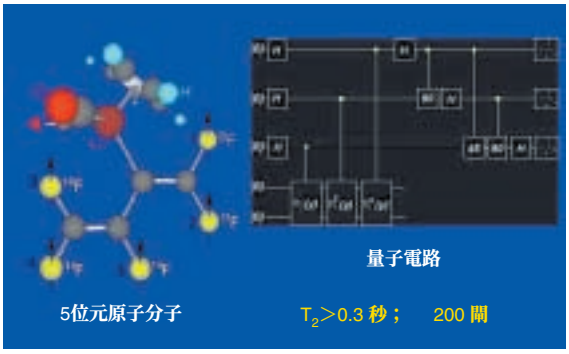
因此，量子運算完全摒棄傳統運算法則，其大量瞬間計算的能力是傳統電腦望塵莫及的。一台三十二個量子位元的電腦，其能力相當於四十億部傳統電腦作平行運算。如用量子電腦做因數分解，以目前最快速的電腦而言，大概要花上數十億年的時間，才能求出一個四百位的數字的所有質因數，而量子電腦可能只需要一小時甚至幾分鐘的時間。

除了進行平行計算外，量子電腦的另一重要用途是模擬量子系統。雖然現在的電腦已被廣泛用來解各種複雜的量子力學問題，但正如費曼先生生前指出，用傳統電腦模擬真實的量子演化過程是不切實際的，因為用一般電腦模擬量子系統所需的時間隨系統的大小呈指數增長。另一方面，傳統電腦中的隨機變數都是虛假的，而量子態是一種真正的隨機分布，量子電腦內的運算過程本身就是量子態的一個變換過程，因此只有量子電腦能瞬間模擬量子系統的演化。

不管是量子平行計算還是量子模擬計算，本質上都是利用量子糾纏態特有的相干性，但在實際系統中，量子糾纏態很難維持。在量子電腦中，由於量子位元是由原子或其它微粒子系統所構成，很容易受外部環境雜訊影響，導致量子相干性的消失，稱為消相干，從而使運算容易產生錯誤結果。

要使量子計算成為現實，最重要的問題就是克服這種消相干。其最有效的方法是在發生消相干前完成運算，或用誤差修正的方法消去因消相干引起的錯誤。前者依賴糾纏態的壽命，一般說來，一個量子資訊由產生到消失的時間只有十億分之一秒。而後者是同時做幾種相同的運算，並不斷對相應狀態做比較，發生偏差時及時修正，但這樣的方法會降低運算效率。如何保持糾纏態不衰減，或當糾纏態發生偏差時及時修正，是目前量子資訊研究中最基本且亟待解決的問題。

至今，世界上還沒有建構成有實用價值的量子電腦。但是，科技發達的國家都已投入大量的經費尋求實現這個夢想。自一九九五年以來，已提出各種方案，主要包括利用冷束縛離子阱、原子和光腔相互作用、電子或核自旋共振、量子點操縱、超導約瑟芬森結等量子系統，並且在過去幾年中，已成功地在實驗室中實現二量子位元、三量子位元、四量子位元的糾纏態。二〇〇〇年美國國際商業機器公司（IBM）阿曼頓實驗室和美國哈佛大學及德國慕尼黑技術大學的科學家分別建構出五個量子位元的離子阱量子電腦和核磁共振量子電腦。二〇〇一年，美國國際商業機器公司又建構了七位元的量子電腦。到能建構十五至十六位元的量子電腦時，就可以超過目前傳統電腦的功能了。



美國國際商業機器公司的科學家在二〇〇〇年建構的五位元215赫茲量子處理器。二〇〇一年，他們又建構了七位元的量子電腦。到能建構十五至十六位元的量子電腦時，就可以超過目前傳統電腦的功能了。

量子通訊

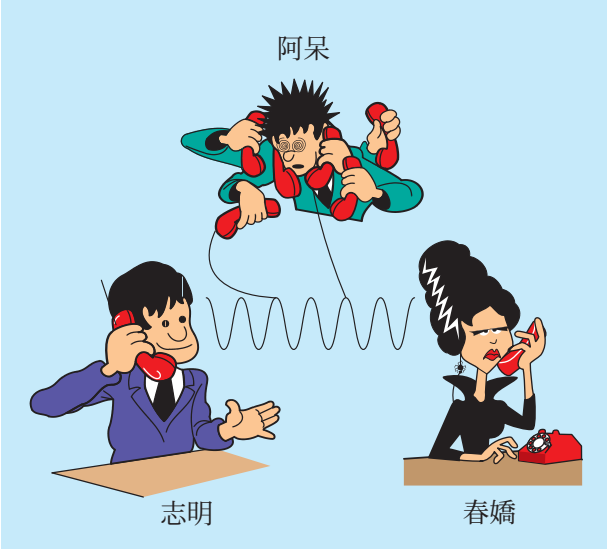
電腦或量子電腦本身是處理資訊的工具，而資訊本身更吸引人的產業市場是資訊的傳輸，即通訊。隨著網路和數位時代的來臨，人類生活將越來越依賴資訊的傳輸，如電話、電視、電子郵件、電子媒體、電子交易等。而確保資訊傳遞的安全性和隱密性是通訊技術的另一大學問，稱為密碼學。一九九〇年代開始研究的量子通訊和量子密碼學，可能為資訊傳輸提供一套更有效且更安全的保密方法。

量子通訊系統是由量子態產生器、量子通道和量子接收裝置而成。它可以說是光纖通訊技術的一種，只不過其量子通道係利用光的量子特性，讓一個個光子傳輸0和1的資訊。量子通訊技術按其所傳輸的信息是古典還是量子而分為兩類，前者主要用於量子解碼鑰匙的傳輸，開發無法破譯的密碼；後者則是量子隱形傳送，一種令人難以置信但在量子世界裡確實可行的瞬間遠距「實物」傳輸技術。因此，資訊量子化不僅為我們建構新一代的電腦提供了基礎，更為現代通訊技術開闢一條新的途徑。

量子密碼學是量子通訊技術裡研究得最久且也是目前最為成熟的領域，它是密碼學與量子力學結合的產物。密碼的關鍵在於解碼鑰匙（密鑰），早期是暗密鑰，即傳送者和接收者要事先知道密鑰才能閱讀對方的資訊，例如，銀行提款用的密碼。其缺點是在傳輸過程中，密碼可能被第三者不留痕跡地竊看而破解。而現今常採行的加密裝置，像網路的安全密碼，通常用一較大的質數做公用密鑰，它沒有被竊取的可能，其破解的關鍵在於求一個很大整數的質因數。正如前面已指出，以一個四百位數的超大整數來說，想要求得其質因數，最快的超級電腦大概要花上數十億年的時間。因此，這樣的安全機制幾乎被視為是無法破解的。然而，利用量子電腦能夠在短時間內找出超大整數的質因數。這樣，一旦研發出量子電腦，對現代的金融甚至國防安全體系就會帶來很大的威脅。

如何使資訊傳輸快速、方便而又安全，是通訊科學的主要課題。早在一九七〇年，美國科學家威斯納（S. Wiesner）就提出如何將量子特性用於密碼術，利用單量子態製造不可偽造的「電子鈔票」。這個構想因量子態的壽命極短而無法實現，但卻讓美國國際商業機器公司的貝內特（C. Bennett）博士和加拿大學者布拉薩德（G. Brassard）想到可將單量子態用於傳送資訊。量子密碼術並不用於傳輸密文，而是用於建立、傳送解碼本。根據量子力學的測量理論，任何觀測都會立刻改變系統的狀態，因此，任何竊聽者的存在都會被發現，從而保證解碼本的絕對安全，也就保證了加密資訊的絕對安全性。

最初的量子密碼通訊利用的是光子的極化特性，目前主要的實驗方案則用光子的相位（糾纏態）特性進行編碼。簡單地說，如果傳送者（春嬌）先傳送一



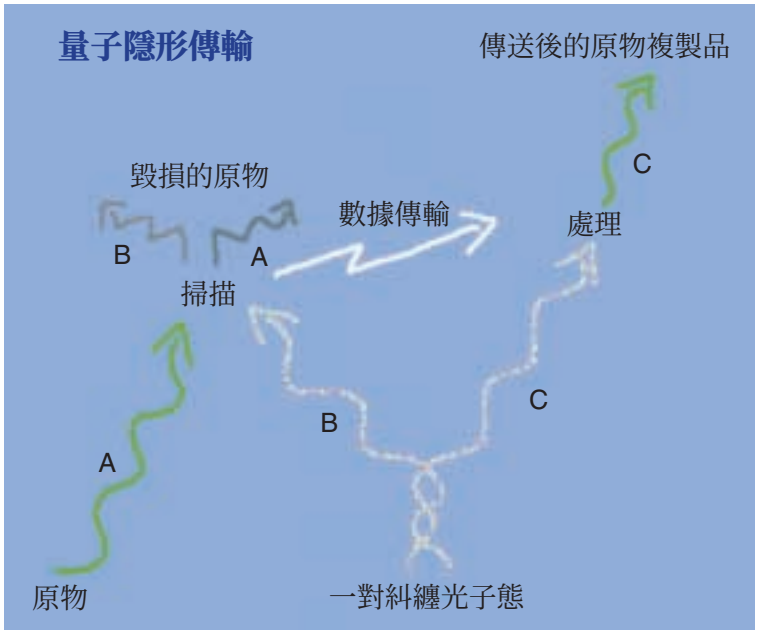
量子資訊具有原則上不可破解的保密通訊特性，即如阿呆想要竊聽志明和春嬌的通訊時，一定會被發現。

組隨機位元序列給接收者（志明），此隨機位元序列是以偏極光子或糾纏態光子來表示，隨後春嬌再與志明溝通，以便確立解碼本。在後來的溝通過程中，即使被竊聽者阿呆聽到，阿呆亦無法知道光子的狀態。如果阿呆試圖去攔截光子，由於他不知道光子之狀態，會得到錯誤訊息。更甚者，光子之狀態會因為阿呆的觀測而改變，這時，春嬌與志明便會察覺阿呆之存在。解碼本確立之後，便可依照解碼本來加密資料並傳送。

量子密碼的優點是可查知解碼本是否被盜用，當然，環境雜訊也有可能破壞解碼本中的位元而留下痕跡，因此量子密碼必須以所有機器正常運作為前提，如何在光源有雜訊的環境下也能正常運作，是量子密碼實用化所面臨的最大難題。

目前，西歐和美國在量子密碼術實驗研究上進展最快。英國於一九九三年首先在光纖傳輸長度為10公里中實現相位編碼量子解碼本的分發，到一九九五年，已能在30公里長的光纖傳輸中成功地實現量子解碼本的分發。同年，瑞士在日內瓦湖底鋪設的23公里長民用光通訊光纜中進行實地表演。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。一九九九年，瑞典和日本合作，在光纖中成功地進行了40公里的量子密碼通訊實驗。二〇〇〇年，中國大陸在850奈米的單模光纖中也完成了量子密碼通訊的示範性實驗。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。

量子資訊在通訊領域最奇妙的應用應該是量子隱形傳輸，即脫離實物的一種實物資訊傳送，就像在星際大戰故事裡所看到的，將太空人通過「時空隧道」，從一個星球傳送到另一個星球的科幻技術，其基本想法是：先提取原物所有的資訊，類似掃描一樣，在這過程中同時將原物毀掉，然後將這些資訊傳送到接收地點，接收者依據這些資訊製造出完全相同（具相同微觀結構）的三維空間原物。其效果就像郵局快遞一樣，但不同於現在用的傳真，後者只是近似的平面複製品。但是，根據量子力學的測不準原理，越精確的測量或掃描，越容易在掃描過程中改變原物微觀粒子的量子狀態，這樣在提取原物的全部資訊前，原物可能已面目全非了。因此，長期以來，量子隱形傳送不



量子隱形傳輸是將原物的資訊分成古典資訊和量子資訊兩部分，古典資訊是發送者對原物進行某種測量（掃描）而提取原物的一部分資訊並經古典通道傳送；量子資訊是發送者在掃描中留下未測量的資訊並由一對糾纏光子態B從A送到C，接收者在獲得這兩種資訊後，就可以備製出原物量子態的完美複製品。

過是一種幻想而已。

直到一九九〇年代初，包括貝內特博士在內的六位科學家提出了利用經典與量子相結合的方法來實現量子隱形傳輸：將原物的資訊分成古典資訊和量子資訊兩部分，古典資訊是發送者對原物進行某種測量（掃描）而提取原物的一部分資訊，量子資訊是發送者在掃描中留下未測量的資訊；古典資訊和量子資訊分別經古典通道和量子通道傳送，接收者在獲得這兩種資訊後，就可以備製出原物量子態的完美複製品。該方案中最關鍵的地方是量子資訊部分的傳送，發送者甚至對這部分量子資訊一無所知。因此，量子資訊部分的傳送，是接收者利用一對糾纏光子態，透過將其中的一個光子備製到原物的量子態上，而提取原物的資訊，並非由發送者傳送給接收者，從而保證資訊的完整性。

利用一對糾纏態光子實現隱形傳輸的物理基礎在於量子力學（糾纏態）的非定域特性，這一在量子力學發展過程中曾令多少物理學家困惑已久的量子性質，沒想到今天卻成為開發隱形傳輸的科學基石。量子力學的非定域性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 $|00\rangle+|11\rangle$），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有力學上的交互作用，只要仍保持在糾纏態，它們之間超強的量子關聯性不會改變。

早在二十世紀三十年代，偉大的科學家愛因斯坦對量子態的這種遠距關聯性就提出了質疑，即著名的愛因斯坦－波渡斯基－羅遜（Einstein－Podolsky－Rosen, EPR）謬論，他認為自然界不可能存在這種非定域的現象，一定是量子力學在某個地方出錯了。直到三十年後，貝爾（J. S. Bell）證明愛因斯坦的定域性觀念與量子力學是不相容的（貝爾定理），七十年代許多實驗進一步證實了量子態的非定域性。但即使量子態的這種非定域性確實存在，人們認為這種超距離的量子關聯特性並不具真正的實用意義，因為這種非定域關聯並不直接傳送資訊。直到量子隱形傳輸實現後，人們對量子力學的非定域性所展現出來的神奇效應才有了更深入的認識。

量子隱形傳輸不僅對人們認識量子力學的神秘規律具有重要意義，而且可以用量子態做為資訊載體，透過量子態完成大容量資訊的瞬間傳輸，並具有原則上無法破解的量子保密通訊功能。

一九九七年，奧地利學者塞林革（A. Zeilinger）和合作者在國際上首次完成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。實驗中傳送的只是表達量子資訊的「狀態」，做為資訊載體的光子本身並不被傳送。隨後，美國加州理工學院的肯保（H. J. Kimble）教授和合作者用光的壓縮態，成功地將一束光從一個房間轉移到另一個房間。為了進行遠距離的量子態隱形傳輸，必須讓相距遙遠的傳送和接收兩系統一直保持在糾纏狀態。但由於各種不可避免的環境雜訊，使量子糾纏態的糾纏性，隨傳輸距離的增加而變得越來越差。因此，如何保持量子糾纏態的純度是目前量子通訊研究中的難題。近年來，國際上許多研究小組都對此進行研究，相信在不遠的將來，科幻般的量子隱形傳輸將給人類帶來真正「隔空取物」的新通訊技術。

總而言之，量子資訊技術在運算速度、通訊安全、資訊容量等方面，可遠遠突破傳統資訊系統的極限。量子電腦具有超強的平行計算能力，能夠解決傳統電腦難以解決的許多重要問題。量子資訊為未來資訊科學的工業發展，特別是量子元件及奈米技術的開發提供了可靠的物理基礎和應用前景。

雖然當前量子資訊無論在理論上，或是實驗上，都不斷地獲得重要的突破。但是想要有效地備製和操作宏觀或介觀尺度上的實用量子資訊系統，還是相當困難。歐美、日本和大陸的學者們目前都致力於這方面的研究，估計在二〇一五年左右，量子通訊和量子電腦技術將會達到實用階段。我們也應積極致力於量子資訊技術的開發，才能讓科學研究和技術的發展不落人後。 □

張為民
成功大學物理系