

推動第五次工業革命 量子資訊時代即將來臨

●作者：張晏瑞、張慶瑞

作者簡介

張晏瑞目前就讀臺大物理博士班，臺灣大學—IBM 量子電腦中心擔任大學推廣課程講師，正努力讓量子計算在臺灣扎根。
張慶瑞是臺灣大學物理學系特聘教授。

Take Home Message

量子科學在 20 世紀被提出後，相關的研究發展蓬勃，也改變了後世人們對於自然的理解。同時，量子科學也進一步促成了兩次的量子革命。根據量子的特性，科學家製造出各種電子元件，促成半導體科技的發展。後續科學家藉由量子的疊加、糾纏等特性，發展出量子電腦、量子計算、量子通訊等科技。這些科技理論上可大幅超越目前古典電腦的運算能力，將成為第五次工業革命的關鍵，而臺灣也不落人後，開始培養相關領域的技術人員。

量子科學旨在了解「物質在微觀尺度中所遵循的規律」，而量子論的起源則要從黑體輻射（black-body radiation）實驗開始講起。

「黑體」（black body）是一個理想化的概念，電磁波照射於黑體都會被百分之百吸收，當黑體達熱平衡後會輻射出電磁波。科學家先從古典統計力學出發，而解釋黑體輻射頻譜分布的瑞利／金斯定律（Rayleigh-Jean's law）其結果在低頻符合實驗上的測量，但在高頻則相差甚大。而維恩位移定律（Wien's displacement law）則在短波範圍內和實驗數據相當符合，但在長波範圍內又有偏差。

1900 年，德國物理學家普朗克（Max Planck）從黑體輻射實驗觀察，引入「能量量子化」的參數概念，發表黑體輻射定律，則在全波段範圍內都和實驗結果符合。

1905 年，愛因斯坦將此概念應用於解釋金屬的光電效應原理，提出了「光量子」的概念解釋光電效應，並認為光具有波動性與粒子性。

之後丹麥物理學家波耳更提出角動量量子化，精確地解釋了氫原子的不連續光譜。1924 年，法國物理學家德布羅意（Louis de Broglie）在其博士學位論文中提出了物質波（matter wave）的概念，認為

電子也具有波的性質，之後的戴維森／革末實驗（Davisson-Germer experiment）成功以低速電子入射於鎳晶體，取得電子的繞射圖樣證明了物質的波動性質，確認了「波粒二象性」。

1925 年後發展出兩種描述量子現象的數學工具，分別是德國物理學家海森堡和波恩（Max Born）提出的「矩陣力學」（matrix mechanics），以及奧地利物理學家薛丁格（Erwin Schrödinger）利用「波動力學」（wave mechanics）提出「薛丁格方程式」（Schrödinger equation）。之後英國物理學家狄拉克（Paul Dirac）提出了著名的狄拉克方程式（Dirac equation），發展出量子力學的基本數學架構。這些新穎的量子力學的原理，徹底改變人們對於自然世界的觀點。

兩次的量子革命

隨著量子科學的發展，科學家更能掌握微觀尺度中依循的規則，也能從微觀的解釋理解固體材料的宏觀物理性質，進而發展出固態物理學。從氫原子能階到更複雜的原子軌域，再拓展到多原子有週期性排列的晶體結構，並整合量子力學、統計物理、

電動力學為理論基礎，應用薛丁格方程式描述固體物質的電子態，發展出能帶的概念，預測了半導體的存在，成功解釋導體、絕緣體、半導體的區別，並為電晶體的製造提供了基石。

世界上第一部電腦是用真空管組成，通過真空管放大電子信號，由於真空管製作困難、體積大、耗能高且使用壽命短，因此當時電腦無法普及。隨著對半導體材料的研究漸深，1947年貝爾實驗室三位科學家蕭克利（William Shockley）、巴丁（John Bardeen）、布拉頓（Walter Brattain）發明電晶體，之後以電晶體為主的技術便開始急速發展，也拉開了第一次量子科技革命的序幕。

電晶體可作為開關功能，在 0 與 1 之間快速進行切換，進行數位訊號的運算。隨著摩爾定律（Moore's law）的進展，元件尺寸越做越小，出現物體有限尺寸的量子效應，也使得量子穿隧效應（quantum tunnelling effect）與奈米科技越來越重要，這也是第一次量子科技革命的半導體科技的基石。

不過，第一次量子革命僅利用有限尺寸的量子特性製作元件，許多量子科學真正有趣的量子性質並未進一步發展。因此，第二次量子科技革命就是利用之前未能使用的量子特性，並開發創新的工具與技術。

1980年，美國阿貢國家實驗室（Argonne National Laboratory）的物理學家貝尼奧夫（Paul Benioff）提出涂林機（Turing Machine）的基礎，首度將量子力學與電腦科學結合。1982年，美國著名物理學家費曼（Richard Feynman）提出可逆計算的量子電腦模型。1985年，英國牛津大學的物

理學家杜奇（David Deutsch）提出杜奇 / 涂林機（Deutsch-Turing Machine），量子計算才具備了數學的基本型式。

而量子資訊科學取得突破性的進展，則是發生在1994年AT&T貝爾實驗室的修爾（Peter Shor）提出第一套量子演算法：量子因數分解演算法，證明運用量子電腦能快速地進行大數的因數分解。大數的因數分解被應用RSA非對稱加密演算法（Rivest-Shamir-Adleman）上^①，在傳統的資訊領域中，理論上只要數字夠大，即使是使用全世界性能最強大的超級電腦，也需要上萬年才能破解。1996年美國計算機科學家格羅弗（Lov Grover）提出另一個量子搜尋演算法，可以在巨量而雜亂的資料中快速搜尋到正確資料，可大幅減少搜尋資料的次數。

量子計算的基礎—量子位元

資訊的基本單位是位元（bit），現在古典電腦由二進位制中的 0 或 1 表示，利用半導體技術靠控制電晶體以 0 與 1 來運算資訊，所有的資訊都是由多個位元以 0 或 1 狀態來組成、儲存、運算、傳遞。

而量子電腦則藉由控制原子、小分子、光子等的量子狀態，以量子力學原理中的疊加及糾纏態為基礎，進而同時表達 0 與 1 的線性組合狀態，用機率

^① 註：RSA 非對稱加密演算法是一種加密演算法，主要應用於公開金鑰加密與商業範疇中。RSA 取自三位發明人的名字，分別為美國密碼學家李維斯特（Ron Rivest）、以色列密碼學加薩莫爾（Adi Shamir）、美國電腦科學家阿德曼（Leonard Adleman）。

的概念來儲存和運算 0 和 1 的資訊，需要量測時才能確定結果，這樣的位元稱為量子位元（quantum bit, qubit），物理上以布洛赫球（Bloch sphere）來展示這樣的現象。布洛赫球的性質可想像成一個漂浮在空中且不斷旋轉的硬幣，不斷轉動的過程就像量子態組合出正面和反面的機率；古典位元則對應到當旋轉硬幣最後落地停止的結果，即正面或反面。



量子計算與量子通訊

由於量子計算是以量子位元狀態的組合來表示，若古典和量子位元一樣多，則量子位元的可表示的組態會比古典位元更多。以 3 個位元為例，3 個古典位元可以表示出 8 個組態（000,001,010,……,111），但卻只能儲存 8 個數字

中其中一個。若同樣是 3 個量子位元，由於量子疊加的性質，所以可以同時將 8 個不同組態都同時儲存在量子位元中。

這也意味著，更多的量子位元組成的儲存器，其儲存量子資訊的組態數量將呈指數增加帶來龐大的運算威力。若由 n 個量子位元組成的暫存器在同一個量子態可一次儲存 2^n 個組態。由格羅弗所發明的格羅弗演算法（Grover's algorithm）主要就是依賴此性質，使得量子電腦在搜尋上有巨大的優勢。

由於量子態有糾纏的性質，每一個操作可以同時改變所有互相糾纏一起的量子疊加態，這是在執行量子計算時可以達成比古典計算機快指數級倍的主要原因。兩量子系統一旦形成糾纏狀態，之後這兩個量子系統不管分隔多遠，只要糾纏態不破壞，系統間就可維持量子關聯性。修爾演算法（Shor's algorithm）就是利用此性質破解目前 RSA 加密系統，這也是實現量子通訊的主要原理。

量子位元基本性質—疊加、糾纏

量子疊加（quantum superposition）：

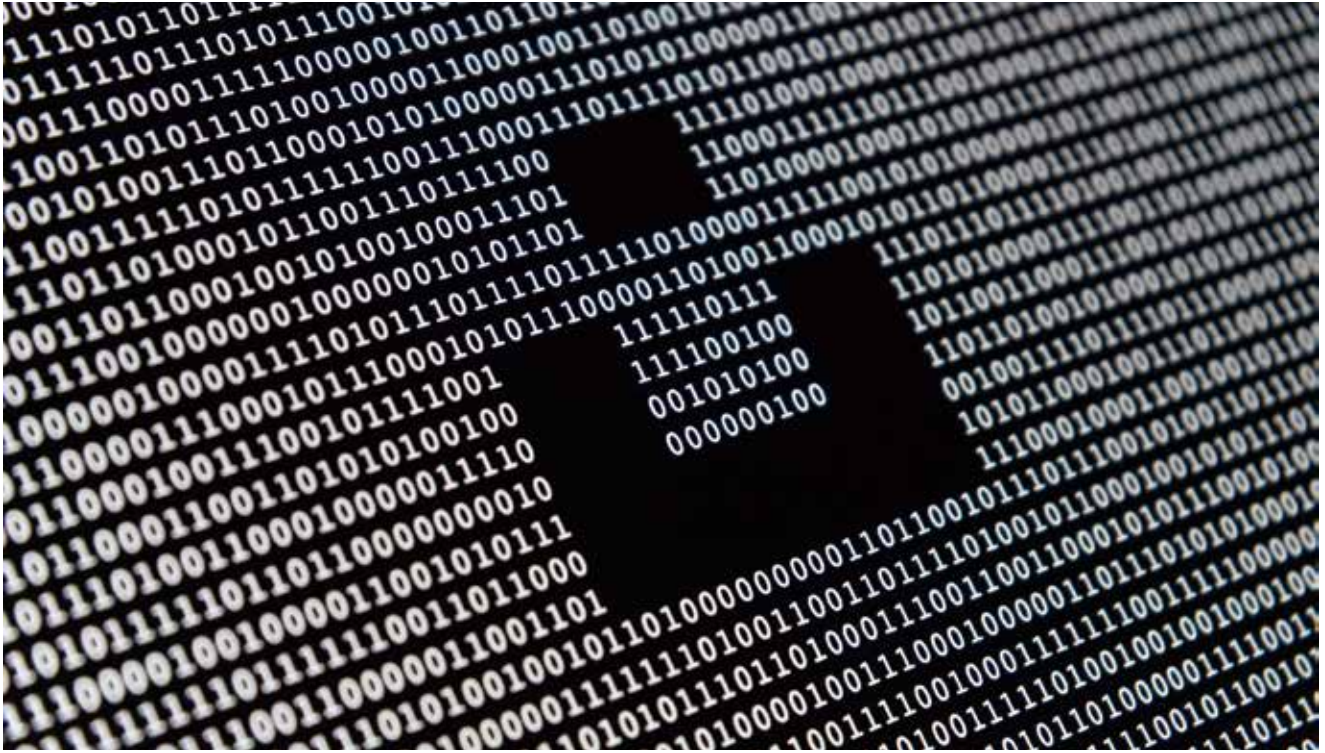
表現 0 與 1 所有可能的狀態組合機率。

量子糾纏（quantum entanglement）：

以量子位元的干涉展現出量子狀態間的關聯性。

各種類型的量子電腦

現今發展量子計算機分成四大類：



(Photo by Alexander Sinn on Unsplash)

- 1 **通用量子電腦**：利用疊加與糾纏態性質和量子邏輯閘運算。
- 2 **量子退火計算器**：利用量子元件解決特定數學最佳化問題。
- 3 **量子啟發式計算機**：利用古典數位或類比電子元件模擬量子穿隧的原理，專門處理最佳化的問題。
- 4 **教育型量子電腦**：提供學習者實際體會和操作硬體。

在量子電腦中，量子位元要克服的問題至少有三個，包含穩定且容易量測二能階系統；穩定的糾纏態；以及足夠多的糾纏態量子位元。敏感的量子狀態很容易受到外界的熱擾動和電磁影響而破壞，目前主流的做法是將量子系統放置在接近絕對零度的環境中，隔絕外界的影響，以維持量子疊加態，以及延長相干時間。

目前主要的量子位元製作技術有超導迴路（superconducting loops）、離子阱（ion-trapped）、鑽石氮／空缺中心（nitrogen-vacancy center in

diamond）、量子點（quantum dot）、矽基量子位元（Si-based qubits）、拓模量子（topological qubits）、光子積體電路（photonics integrated circuit）、核磁共振（NMR）等。以下向讀者介紹較為常見的超導迴路與離子阱技術。

近年來 IBM、英特爾（Intel）、Google 等科技巨頭都在超導迴路技術上投入龐大的資源研發。超導迴路是將超導材料線迴路冷卻至接近絕對零度時，在沒有電阻的情況下，使線路形成二能階狀態的人工原子，作為量子位元。Google 在 2019 年利用 Sycamore 53 量子位元在 200 秒內取樣 1 個量子電路 100 萬次，計算速度遠遠超過古典電腦，進而宣稱達到量子霸權（quantum supremacy），並在去（2020）年用 12 個量子位元成功模擬目前最大規模的化學量子反應。而 IBM 則宣布推出代號為 IBM Quantum Hummingbird 的 65 位元量子電腦處理器，透露了未來量子電腦發展藍圖。預計在今（2021）年推出 127 位元的處理器「IBM Quantum Eagle」，明（2022）年推出 433 位元的處理器「IBM

Quantum Osprey」，2023 年推出 1121 位元的處理器「IBM Quantum Condor」。

離子阱則是以雷射冷卻捕捉離子，利用電場或磁場將離子限制在一定範圍內，藉由電荷與電磁場間的交互作用力控制離子的運動作為量子位元。去年初，美國的 Honeywell 集團首次推出了以離子阱為量子位元基礎的量子計算機，到了 10 月又公布了新一代的 Model H1 量子電腦，由 10 個完全連接的量子位元組成。此外，新創公司 IonQ 近期也發表了 32 量子位元量子電腦，後續將於紐約證券交易所上市，成為首家專注於量子運算的上市公司。

臺灣量子計算的未來展望

世界各國都已經積極的投入量子科技的研發，全球的量子競賽早已開始，利用量子電腦未來有機會處理當今古典電腦無法處理的部分複雜運算。除了量子電腦的硬體的開發之外，新穎的量子演算法則是臺灣可以積極投入發展的領域。

現在正處於生產力再次創新的時刻，回顧歷史，第一次工業革命蒸汽機的發明，用機械取代人力及獸力，工學院也孕育而生；第二次工業革命因為光和電的發明讓生活更便利，引發了電機學院創立；第三次工業革命也稱為數位化革命，資訊數位化之後徹底改變了整個社會的運作模式，減少了工作成本，又出現資訊學院，也創造了電腦工業。而隨著社會資訊數位化，大量的訊息各處充斥，第四次工業革命——物聯網革命也隨之而生，將巨量資訊建構成為智慧型意識的世界，使資源，人和機械可以協同合作。

超導迴路 VS. 離子阱

超導迴路的優勢在於許多科技公司都熟悉基本超導元件製作，與現在晶片技術相似；而離子阱則有其他許多的潛在優勢。一般來說，當量子位元越多，計算能力越強，但位元數量並不是唯一影響的因素。要比較量子電腦優缺點，有以下幾個因素需要考慮。

1 量子邏輯閘執行計算速度：超導迴路 > 離子阱

超導迴路約十億分之一秒內執行的基本邏輯閘運算，約是離子阱運算速度的千分之一。

2 糾纏態時間：離子阱 > 超導迴路

離子阱能夠維持數秒的時間，甚至能夠達到數分鐘或數小時；超導迴路僅有約數微秒。

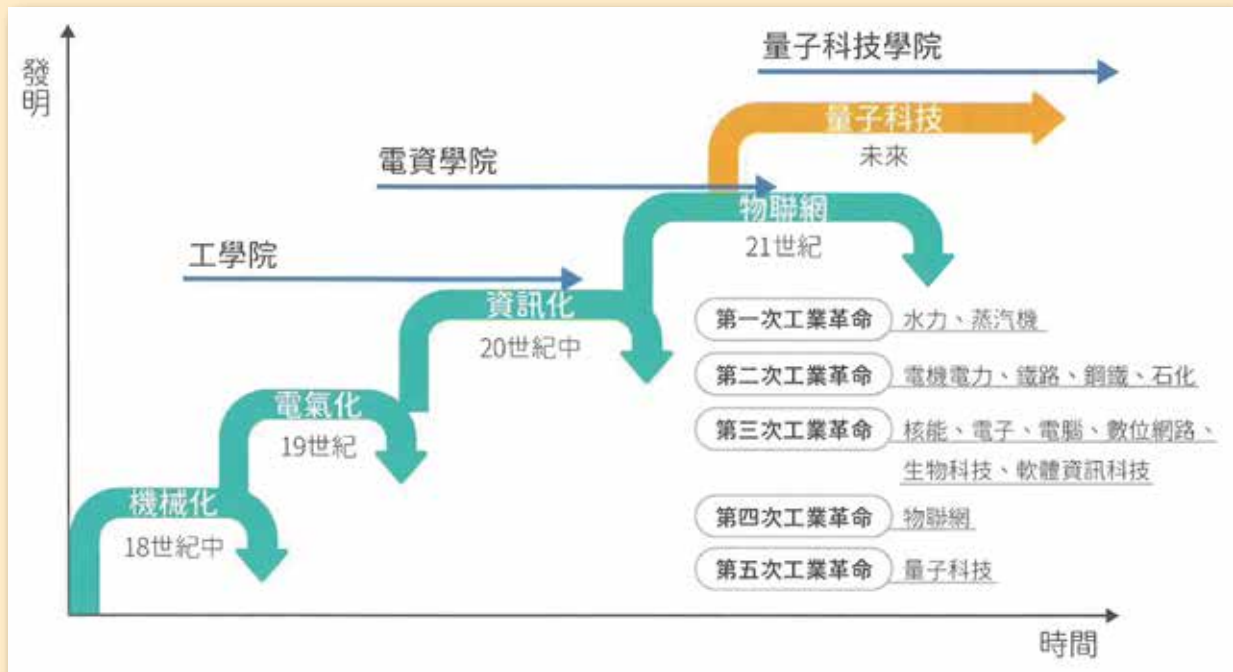
3 糾錯能力：離子阱 > 超導迴路

超導迴路通常只和相鄰的糾纏；而離子阱可以和很多個其他離子糾纏，更能執行複雜的計算，達到低量子閘錯誤。

4 操作溫度：離子阱 > 超導迴路

離子阱操作溫度約數 K，是液態氦就可以達到的溫度；超導迴路則需要利用特殊的製冷技術，在趨近絕對零度的狀態下才能進行操作。

歷史上的生產力創新週期



從 18 世紀中葉起，生產開始朝向機械化發展，並在 18 世紀末開啟了第一次工業革命。而 19 世紀則進入了電氣化生產階段，帶動第二次工業革命。20 世紀中則朝向資訊化發展，第三次工業革命隨之展開。目前因物聯網的快速發展，進入第四次工業革命階段。未來當量子技術成熟發展後，也將帶動第五次工業革命。

目前很明顯的趨勢，第五次工業革命的泉源必然是量子科技。隨著物聯網的發展，人、資訊、機器的合作越加緊密，應用也越來越多元。然而該如何最佳化龐雜的資訊，這正是未來量子計算可以展現的優勢所在，而量子科技學院也必將迅速在大學體系中出現。培養優秀的量子科技人才必須從教育開始，讓更多人理解量子計算的特性，以提供未來量子產業中最重要量子技術相關人才庫，才能加速將臺灣量子基礎研究成果擴展至各領域的量子技術應用上。

目前政府由科技部補助成立「臺灣大學—IBM 量子電腦中心」，負責提供給臺灣各領域中對量子技術有興趣的單位入門課程。而「台灣量子電腦暨資訊科技協會」也時常舉辦各種量子技術交流的會議，讓企業單位可更容易踏入量子計算的領域，增進臺灣在未來科技的發展能量。以臺灣過去在矽產業的成功與領先經驗，只要集中現有的量子人力，

在目前的量子生態環境中，找尋臺灣的專長，大力投入，必將再度在未來建立出矽產業之後更龐大的「量子科技護國神山群」。[∞](#)

本文出處

原刊於科學月刊 05 月號 /2021 第 617 期。本刊感謝作者與《科學月刊》同意轉載。

延伸閱讀

- Morten Kjaergaard et al., "Superconducting Qubits: Current State of Play", *Annual Review of Condensed Matter Physics*, 11, 2020, 369-395。
- Yu-Ching Shen and Guin-Dar Lin, "Scalable quantum computing stabilised by optical tweezers on an ion crystal", *New Journal of Physics*, 22, 2020。
- Ching-Ray Chang et al., "The Second Quantum revolution with Quantum Computers", *AAPPS Bulletin*, 30(1), 2020, 9-22。