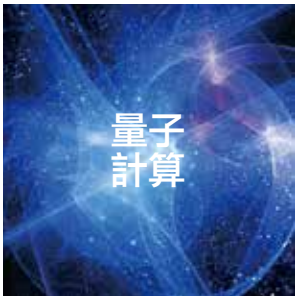


退火演算法、量子退火機與通用量子電腦簡介

作者：施佳妡、卓建宏

作者簡介

施佳妡是臺北市立第一女子高級中學學生，卓建宏是臺灣大學物理系博士班學生。

量子力學令即使是它的開創者們都驚奇不已。

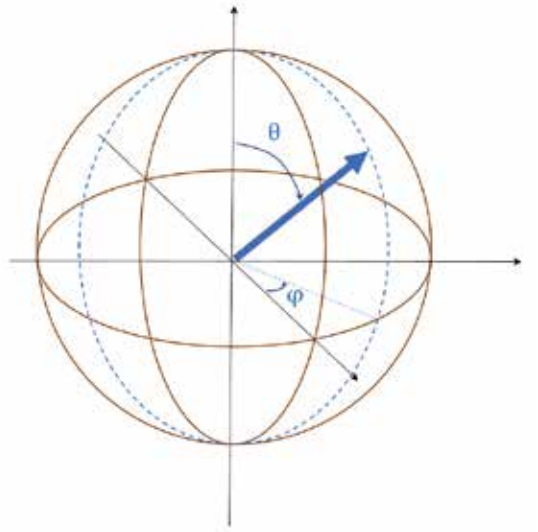
公元 1900 年，普朗克（Max Planck，1858 ～ 1947）以能階量子化的假設，成功推導出與實驗吻合的黑體輻射公式，標示了量子論的誕生。量子力學的發展徹底改變了人們對自然現象的認知，成爲探索微觀尺度下科學奧秘的鑰匙。這項發生在二十世紀初的重大理論發展被稱爲第一次量子革命，對次原子尺度現象的了解促進了科技的快速發展，我們所熟知的雷射、原子鐘、磁振造影（magnetic resonance imaging）、電晶體等，皆是由此而來。

然而這只應用了科學進展的一部份。隨著製程微縮與技術的突破，科技界正從對自然現象的詮釋和利用，設法跨越到能夠操縱量子系統，使其符合應用需求的境界。這就是此刻正在上演的第二次量子革命，預計在通訊、量測、計算等領域會帶來巨大影響。其中量子計算初步能夠實現的是量子退火機，長期技術願景則是製造出可編程的通用量子計算機。本文針對退火方法與不同量子計算機的實現進行概述。

量子退火機與一般稱爲「量子電腦」的通用型量子計算機都使用到量子位元的概念。如同傳統位元，量子位元也有 0 與 1，兩種狀態分別以 $|0\rangle$、$|1\rangle$ 描述。不同的是傳統位元只能落在 $|0\rangle$ 或 $|1\rangle$ 上，而量子位元的值可以是 $|0\rangle$ 或 $|1\rangle$ 的任意疊加 $\alpha|0\rangle + \beta|1\rangle$。在計算過程中，此一特性加上量子位

本篇文章的完成需感謝臺大物理系張慶瑞教授的協助與指導，特此致謝。

元間的糾纏，使平行計算成爲可能。不但如此，$|0\rangle$ 和 $|1\rangle$ 的係數只要符合 $|\alpha|^2+|\beta|^2=1$ 即可，因此 α 與 β 可以是複數，量測時量子態會塌縮，量測到 $|0\rangle$ 與 $|1\rangle$ 的機率分別由 $|\alpha|^2$ 與 $|\beta|^2$ 決定。



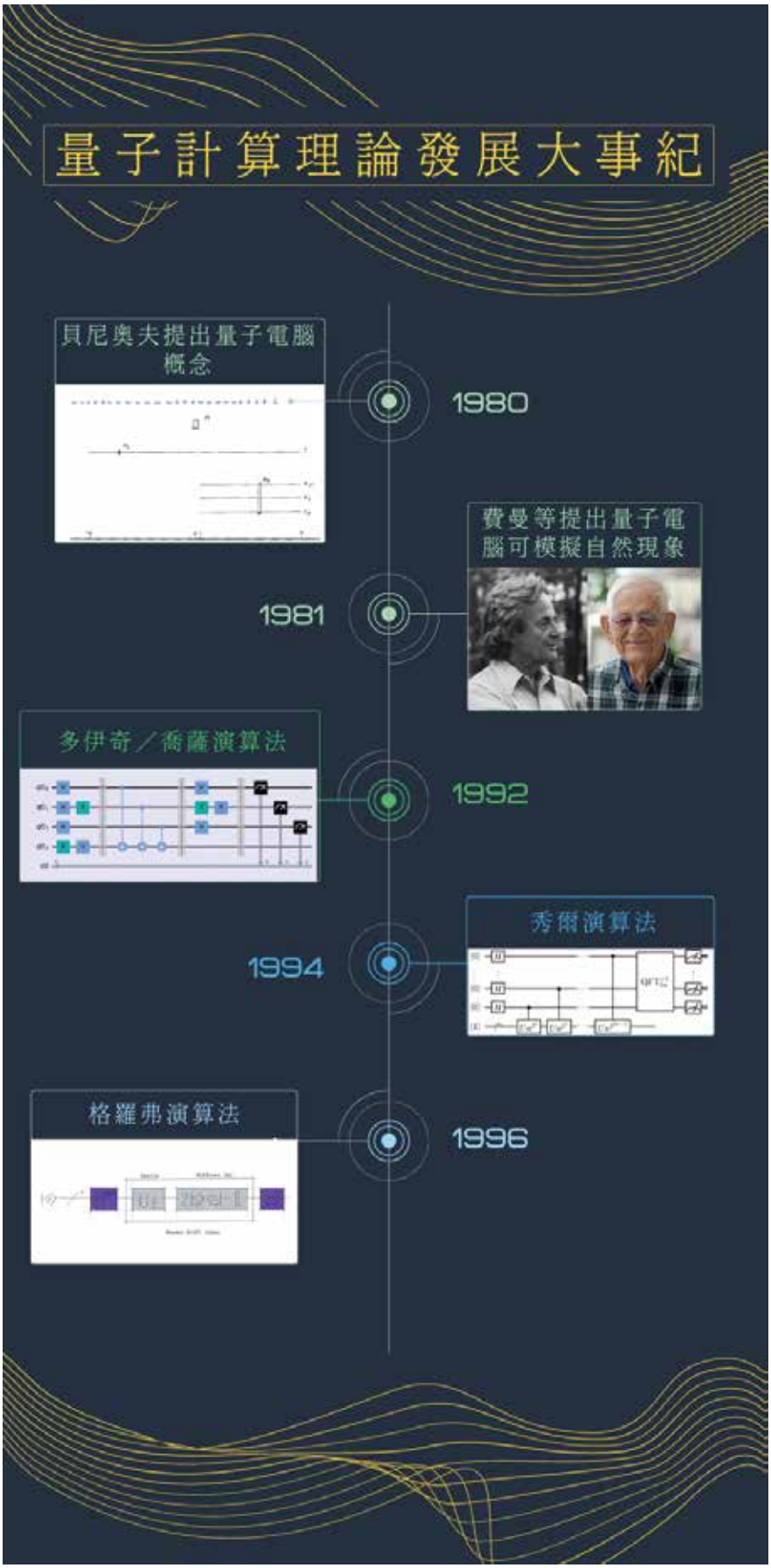
用來圖像化量子位元的布洛赫球面。將 $\alpha|0\rangle+\beta|1\rangle$ 寫成 $\cos\frac{\theta}{2}|0\rangle+e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$ 的形式，用球面上的一點描述。

量子電腦與傳統電腦的區別在於運用量子位元獨有的疊加（superposition）、干涉（interference）與糾纏性（entanglement），實現平行計算。常見的誤解是量子電腦會是更快速的「新一代電腦」，實際上量子電腦主要的優勢在於能實現應用量子物理特性的量子演算法，解決特定問題，是傳統電腦所不能在合理時間內解決的，而量子電腦適合何種問題的相關理論已有非常豐富的發展，本文不深入探討。除此之外，目前的通用電腦計算過程會擦除資訊，遺失的資訊（熵）以熱能形式逸散。學界期待透過可逆計算（reversible computing）的實現，能突破此一計算機能量消耗的下限。量子計算屬於可逆計算，在計算過程中不會遺失資訊，具有落實可逆計算的潛力，也是它吸引人的原因之一。

量子計算理論的發展

量子計算的概念 1968 年首次由貝尼奧夫（Paul Benioff）提出。至 1980 年代相關概念逐漸成形，費曼等物理學家於 1980 年代意識到量子電腦具有模擬許多自然現象的能力，這些現象若要以傳統電腦模擬，將耗費過多計算資源而不具實用性。1989 年量子退火可能優於古典模擬退火的想法被提出。1992 年科學家發現了第一個量子電腦能快於古典電腦的問題，並提出多伊奇／喬薩演算法（Deutsch–Jozsa algorithm）。儘管此演算法適用的問題應用空間有限，它仍具有高度代表性，而成爲了量子計算發展史的里程碑。用於解決質因數分解問題的量子演算法 —— 秀爾演算法（Shor's algorithm）於 1994 年提出，在足夠大（數千個量子位元）的量子電腦上可以破解當前 RSA 加密所用的質因數乘積，引起了各界關注。這是危機也是轉機，有鑑於量子科技發展可能帶來的重大突破，各國均挹注資源促進這方面的研究。1996 年格羅弗（Lov Grover）發明了量子搜尋演算法 —— 格羅弗演算法（Grover's algorithm），其較古典搜尋演算法的優勢雖不如秀爾演算法顯著，可應用的範圍卻十分廣大。至此量子運算主要幾個理論皆已被提出。

儘管基礎的理論堪稱完備，如許多專家所預測的，較大規模量子電腦的實現還需要一段時日。這是由於量子態顧名思義牽涉到的能量級十分微小，



量子計算理論發展示意圖。

圖片來源：由上至下，左一：Benioff, P. (1980). The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. Journal of statistical physics, 22(5), 563-591.

左二：by Saptashwa Bhattacharyya https://medium.com/a-bit-of-qubit/deutsch-jozsa-algorithm-quantum-computing-basics-708df8c4caf7.

左三：https://qiskit.org/textbook/ch-algorithms/images/grover_circuit_high_level.png

右一左圖：https://commons.wikimedia.org/wiki/File:RichardFeynman-PaineMansionWoods1984_copyrightTamikoThiel_bw.jpg

右一右圖：By Justinhsb - Own work, CC BY 4.0, https://commons.wikimedia.org/w/index.php?curid=83268462

右二：by Bender2k14 https://upload.wikimedia.org/wikipedia/commons/6/6b/Shor%27s_algorithm.svg

很容易因外界環境擾動造成雜訊。如何建立更穩定的量子電腦系統，並修復無可避免的雜訊干擾，正是當前大家努力的方向。相較之下，目前發展較快的是量子退火機（以 D-Wave 公司爲代表），主要訴求是用於求解以無約束二元二次優化模型（QUBO）描述的問題。雖然所能解決的問題與通用量子電腦有本質上的差異，應用不如量子電腦廣泛，仍不失爲了解和探索量子計算一個好的開始。

QUBO

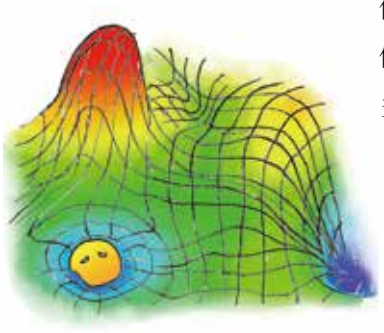
QUBO 是一種組合優化問題模型，由於與物理上的易辛模型（一種量子系統的模型）相對應，適合以量子系統呈現並求解。在資訊科學中，QUBO 屬於 NP 完備（NP-complete）問題，任何 NP 問題皆可以該形式描述，比如包含貨運、排班、包裝等，對企業非常重要的組合最佳化問題，因此 QUBO 模型在討論量子退火機應用性時，扮演著舉足輕重的角色。

QUBO 模型變數兩兩之間以耦合係數互相關聯。係數由懲罰函數決定，懲罰函數必須滿足「若且唯若當變數間滿足限制時懲罰最小」。利用二元變數 0 與 1 與自己的任意次方相等的性質，可以將懲罰函數皆以二次方多項式與常數表示。幾個常見限制條件轉爲懲罰函數的慣用方法舉例如表 1。

最佳化與退火的具體關聯

最佳化與退火的具體關聯爲何呢？最佳化問題在數學上即求函數極值，只不過這些函數沒有分析方法求極值，若要決定性的求得，必須透過窮舉，或稱暴力搜索法（brute-force method），而這樣做的運算成本太高了。因此在資訊有限，運算資源也有限的情況下，如何有效率的在搜尋空間中找到極值，是資訊科學的一個重要問題。

若要找極值最單純的想法如下：以尋找最小值爲例，演算法在目標函數某點上，計算相鄰所有點的函數值，如果小於目前的值，就移動到該點；如果相鄰的點函數值皆大於當前點，則不移動，並宣布已找到解。這適用於單一極小值的情形。在大部分情況下，函數在變數域內有數個局部極小值，除非起始條件幸運的落在全域最小值附近，否則演算法所求出的值將會被困在某個局部極小值。如果局部極小值數量不多，這個演算法進行幾次就能找到最佳解，也算可行。但若「坑洞」數量多怎麼辦呢？



在複雜的搜尋空間中，演算法可能會被困住。

表 1

限制條件	懲罰函數
$x_1 = 1$	$(x_1 - 1)^2$
$x_1 = x_2$	$(x_1 - x_2)^2$
$x_1 + x_2 \leq 1$	$x_1 x_2$
$x_1 + x_2 + x_3 \leq 1$	$(x_1 + x_2 + x_3 + s - 1)^2$, s 爲輔助變數

這時必須借助隨機的力量。既然不知道往哪邊走比較好（無法有一個決定性的方法判斷下一步怎麼走最好），透過一定程度的隨機決定，可以提高找到正確解的機會。機率演算法的概念皆是在原本單純「往下走」的大方向之上，加上某些隨機性的選擇往上，如何決定往上的機率就是不同機率演算法之間的差異。

退火演算法

退火演算法即是靈感取自自然現象，奠基於機率的一種演算法。此方法在優化問題有非常廣泛的應用，以下就退火概念進行簡介。

模擬退火演算法（simulated annealing algorithm）的名稱取自金屬緩慢冷卻時的結晶現象。原子按照晶格規律排列時，系統能量有最小值，因此各原子相對位置與系統總位能有一對應關係；同時原子熱運動具有隨機性，與周遭原子試圖建構的規律相抗衡，因此系統並非單調的演化到起始條件所決定的局部極小值狀態，而是因熱運動的動能，有可能隨機發展到位能較高的狀態，而過渡到其他局部極小值的「領域」內。如此系統便有機會跳脫位能的局部極小值陷阱，找到眞正的全域最小值。隨著溫度緩慢降低，系統組成隨機熱運動的能力也越來越低，退火結束時系統所在的狀態就是所求出的解。

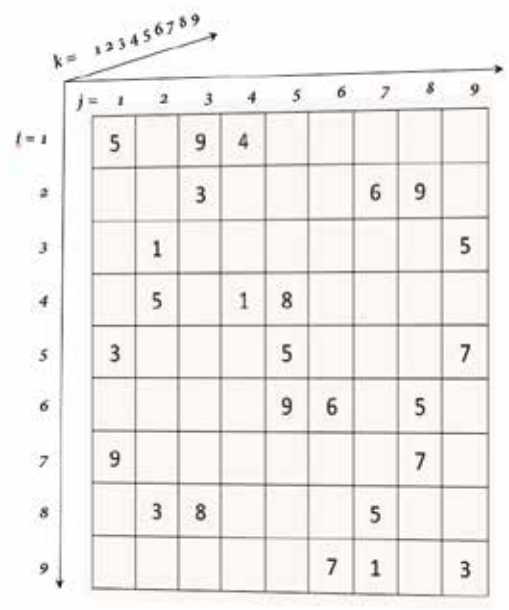
模擬退火演算法用電腦運算模擬此一現象，設置一個緩慢減小的溫度參數，並定義鄰近狀態，即與當前點稍有不同的狀態，做爲可能的下一步。計算該鄰近狀態的能量，並透過一個準則決定是否移動，常用的準則是：如果低於當前狀態的能量，則移動到該狀態；否則依波茲曼分布（Boltzmann distribution）$e^{-\frac{\Delta E}{kT}}$ 隨機決定是否移動到該狀態。此演算法理論上被證明，只要溫度參數減小的速度足夠慢，總是可以找到最小值。然而就實用層面而言，退火演算法主要的價值在於用較少的時間，有一定機會可以給出最佳解，或近似最佳解。

一般的最佳化問題考慮的是無約束的情形，亦即系統狀態可以是定義域內的任意值。若變數之間必須滿足特定關聯，則稱約束問題。約束問題也可以轉成無約束問題的形式，而使用針對無約束問題的方法求解之。轉換是藉由設置懲罰函數，在無約束地求解極小值時，懲罰函數作用在不符合約束條件的潛在解上提高其函數值，使這些不可行的解被選中的機率微乎其微，藉此達成約束。甚至連不屬於最佳化問題的某些約束問題，也能透過此方式，以最佳化方法求解。

實作例子

在此分享筆者以筆記型電腦實作的一個例子。問題是我們熟悉的數獨遊戲：玩家以 1 ～ 9 的數字填入劃分成九個 3×3 大格的 9×9 方格，在已給予的初始條件限制之下，須滿足同行、同列、同大格不能重複出現同一數字，將 81 個方格都填入。一個正規的數獨應恰有一解，因此數獨屬於約束問題的一類（約束滿足問題，constraint satisfaction problem），但不屬於最佳化問題。將其以懲罰函數形式表示，並轉換成 QUBO 模型，以模擬退火演算法求解。爲了用二進位制描述 9×9 數獨問題，使用 729 個變數，編號 ijk 的變數對應第 i 列第

j 行填數字 k 的眞值。使用的懲罰函數如表 2。



數獨 QUBO 模型變數的設置。

調整提示數與提示所對應的懲罰函數倍數，兩項變因造成的影響簡述如下：對於提示較多，且分布較隨機的數獨，退火演算求得正解的機會較高。而其中提示數、分布形式與解答成功率關係如圖 1 所示。

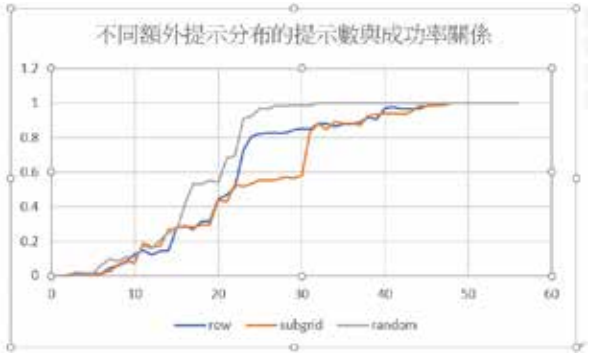


圖 1：對於同樣提示數，隨機分布的提示提高成功率的效果，比起有規律分布的提示更好。

將提示的懲罰函數倍數設置爲普遍性數獨規則的數倍，也能提高解答成功的機會，在五倍左右有最好效果。懲罰函數倍數與解答成功率關係如圖 2。

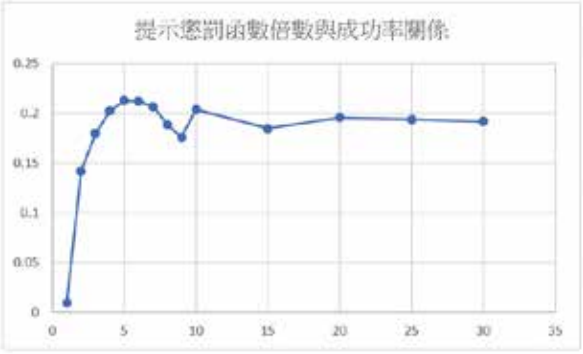


圖 2：在提示懲罰函數倍數較小時，提高其倍數能明顯提高成功率。在超過五倍之後，再提高倍數則無顯著效果。

表 2

規則	數學限制式	轉換後的懲罰函數
一格應恰填一個數字	$\sum_k x_{ijk} = 1$	$\alpha \sum_{(i,j)} (\sum_k x_{ijk} - 1)^2$
同一個數字在同一行應恰出現一次	$\sum_j x_{ijk} = 1$	$\alpha \sum_{(i,k)} (\sum_j x_{ijk} - 1)^2$
同一個數字在同一列應恰出現一次	$\sum_i x_{ijk} = 1$	$\alpha \sum_{(j,k)} (\sum_i x_{ijk} - 1)^2$
同一個數字在一大格應恰出現一次	$\sum_{i=1}^{3}\sum_{j=1}^{3} x_{(u+i)(v+j)k} = 1,$ $u, v \in \{0, 3, 6\}$	$\alpha(\sum_{i=1}^{3}\sum_{j=1}^{3} x_{(u+i)(v+j)k} - 1)^2,$ $u, v \in \{0, 3, 6\}$
題目	$x_{ijk} = 1, (i, j, k) \in hint$	$\alpha \sum_{hint} (1 - x_{ijk})$

透過這兩項觀察，推測一般退火演算法解組合問題的應用中，提供更多限制（資訊）與提高約束條件的懲罰函數倍數，都是能提高求解效果的方法。

量子退火的優勢

量子退火與古典退火概念上十分相似，關鍵差異在於前者運用了量子力學中的穿隧現象，使得演算法穿越能量障壁的機率除了與障壁高度有關外，同時也與其厚度有關。穿隧現象係指量子力學中，物質波即使在位能高於其總能量的「古典禁區」，仍能以指數虛數形態傳遞其影響，此一影響隨深入禁區的距離而以指數衰減。若能在足夠近的距離內脫離禁區，使衰減程度不太大，波動將能「穿過」禁區，以實數形式出現在另一端，此即穿隧現象，也是前述量子退火方法中，越過能量障壁的機率除了與高度有關，也取決於寬度的原因。

直觀來說，量子退火在某些問題能夠較古典退火有優勢，例如搜尋空間中包含高而薄能量障壁的問題。事實上量子退火被證明能夠在較少的步驟內，達到與古典退火相同的成功率。儘管兩種退火都能以古典演算法模擬，在某些問題中，使用眞正的量子硬體，即量子退火機，能夠提供模擬量子退火所不能提供的優勢。

在量子退火機之外，遠大的量子夢想所追求的，是能實現通用計算的量子電腦。這必須透過與傳統電腦同樣概念的量子邏輯閘完成。能透過排列組合實現任意計算操作的邏輯閘組合稱爲通用邏輯閘（universal gate set），是製造通用量子電腦的基礎之一。實現通用量子電腦的技術必須至少滿足五個

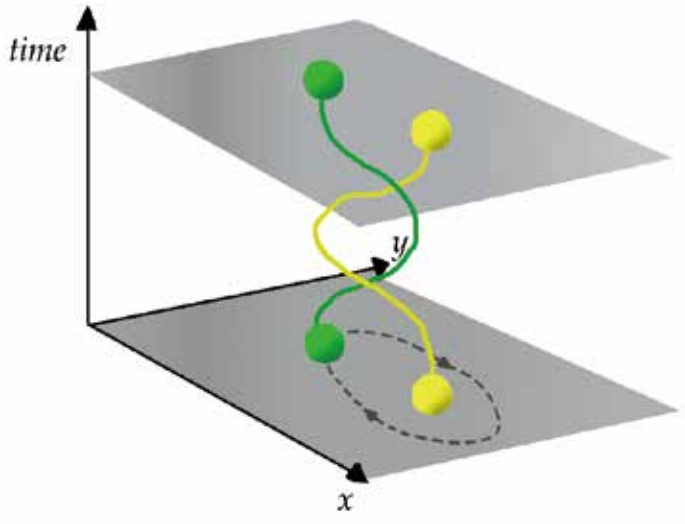
IBM 的量子電腦。
（Ron Gilbert 攝，flickr，https://www.flickr.com/photos/23161425@N08/39677430701）

條件：可擴展性（scalability），即理論上能夠製造足夠大的計算系統；可控制的量子位元初始化；執行操作所需時間與系統去相干時間（decoherence time）相比足夠短；運算結果能被量測；系統能實現至少一組通用邏輯閘。量子閘作用在量子位元上，因此與傳統電腦的邏輯閘有些不同（表 3）。

量子電腦的建構目前有利用超導量子位元（transmon qubit）、鑽石空缺（diamond vacancy）、量子點（quantum dot）、離子阱（ion trap）或拓樸量子位元（topological qubit）等技術（表 4）。

常見的量子邏輯閘	矩陣形式	
Pauli Gates	$X=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}; Y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}; Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix};$	單一位元閘
Rotation Gates	$R_X(\theta)=\begin{bmatrix}\cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2})\\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\end{bmatrix}$ $R_Y(\theta)=\begin{bmatrix}\cos(\frac{\theta}{2}) & \sin(\frac{\theta}{2})\\ \sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2})\end{bmatrix}$ $R_z(\theta)=\begin{bmatrix}e^{-i(\frac{\theta}{2})} & 0\\ 0 & e^{i(\frac{\theta}{2})}\end{bmatrix}$	
Hadamard	$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$	
Phase shift	$P(\phi)=\begin{bmatrix}1 & 0\\ 0 & e^{i\phi}\end{bmatrix}$	
Swap	$\text{SWAP}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\end{bmatrix}$	雙位元閘
Controlled NOT(Controlled X)	$\text{CNOT}=\begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0\end{bmatrix}$	

表 3



二維準粒子透過交換位置，形成拓樸纏結。

結語

隨著第二次量子革命的浪潮襲來，世界將會完全不一樣。現今量子科技的發展還在摸索階段，有許多挑戰等待克服；不過正是由於這如同新大陸一般的契機與廣大潛能，使各國願意投注資源，以求在新科技的世界中，能占得一席之地。現在正是量子科技新賽局的開始，希望這篇文章能夠提供各位讀者有用的資訊，讓我們一起迎接無限可能的未來！∞

延伸閱讀

▶宇津木健 (Takeru Utsugi)、德永裕己 (Yuuki Tokunaga) 監修，莊永裕翻譯，《圖解量子電腦入門》，臉譜出版社（2020）。本書以深入淺出透過圖像化的說明量子電腦的各類知識。

	簡述	優	缺	主要發展公司
超導量子位元	在超導體中，電子形成庫柏對（Cooper pairs）並發生玻色 - 愛因斯坦凝聚（Bose-Einstein condensation），構成巨觀量子態，足夠穩定而能進行操作。以微波訊號在能階之間轉換，並利用約瑟夫森結（Josephson junction），使操作頻率能透過外加磁場調整。	運算操作快速；與已發展多年的傳統積體電路較相近，可以應用現有技術	去相干時間短，造成錯誤率較高；需要小於 100mK 的低溫	**Google** **IBM**
鑽石空缺	緊鄰氮原子的鑽石晶格空缺與捕捉在其中的電子共同形成一個 NV 中心，可視爲一個量子點。其基態有三種，利用三者發生躍遷的機率差異，能夠初始化到其中 $m_s = 0$ 的能階。利用鑽石晶體價帶 - 導帶能差大而難導電，與強共價鍵的特性，達成量子系統與外界的隔離，有效排除自由電子與晶格震動造成之雜訊。	能在室溫下操作	目前製造相似環境的鑽石空缺量子位元仍是技術挑戰	
矽量子點	量子點是人造的量子系統，展現出類似原子的能階，因此也被稱爲人造原子。在半導體材料中，被侷限的自由電子構成一個可操作的量子點。透過外加磁場分裂電子兩種自旋的能階，作爲計算使用的 $\|0\rangle$ 與 $\|1\rangle$。可在數 K 的溫度下運作。	亦可應用傳統積體電路技術基礎	目前成功達到糾纏的位元數較低	**Intel**
離子阱	用恰當頻率的振動電場將雷射冷卻的離子近乎固定在眞空中。離子阱只能侷限兩個維度的離子運動，因此透過將離子在第三個方向上直線排列，可以達成三維空間中的固定。使用雷射操作。是最早發展的量子位元技術。	位元容易糾纏，能執行較準確的運算操作	只能以一維陣列形式排列，不利積體電路製造；操作需時較長；需在眞空環境	**IonQ** **Honeywell**
拓樸量子位元	因二維平面不同於三維空間的拓樸特性，使得被稱爲任意子（anyon）的二維準粒子彼此間交換位置的次數可以被記錄，在時空中構成形似辮子的結構。量測時將準粒子融合（fuse），不同交換情形下的準粒子融合結果不同，因此透過交換可以實現邏輯閘。這種量子位元的量子態只與系統拓樸性有關，不受局部微擾的影響，因此能達到幾乎無雜訊。	穩定、準確度高	二維準粒子的實現仍在初期發展階段	**Microsoft**

表 4

《數理人文》訂購單

（請填妥資料後傳真至 03-5731915 或郵寄至交通大學丘成桐中心）

數理人文為半年刊，固定於每年之 1 月及 7 月各出版一期。

訂閱方案	優惠價
一年2期（印刷品）	450元
一年2期（掛號）	490元
二年4期（印刷品）	900元
二年4期（掛號）	980元

☐ 自_____年_____月號開始訂閱。
（未填寫期數者，將由最新一期寄發）
☐ 續訂依原訂閱到期後續寄送。

客服專線：03-5731915
客服信箱：alicefsy@math.nctu.edu.tw
yushan.deng@intlpress.com

■ 基本資料（請以雜誌收件者之資料為主）

姓　名：_____　　性　別：☐先生　☐小姐
電　話：日（　）_____　夜（　）_____　手　機：_____
E-mail：_____
收件地址：☐☐☐_____

■ 付款資料

付款總金額：優惠價_____元 × 份數_____ ＝ _____元

☐ **郵政劃撥**（劃撥帳號：50422323　戶名：馮肅媛）

您可以使用本頁所附之劃撥單訂購，並將交易憑證傳真至 03-5731915，或使用郵局之劃撥單訂購，並請在劃撥單上寫明訂閱方案、聯絡方式及 E-mail。

☐ **網路訂購**（https://yaucenter.web.nctu.edu.tw/?page_id=78&lang=tw）期刊之網站提供電子平台的訂購連結

■ 發票資料

抬頭：_____　統一編號：_____

98-04-43-04　郵政劃撥儲金存款單

收款帳號：5 0 4 2 2 3 2 3　金額（阿拉伯數字）：億 仟萬 佰萬 拾萬 萬 仟 佰 拾 元

通訊欄（限與本次存款有關事項）

☐ 自　年　月號訂閱
☐ 續訂依原到期數接續寄送
☐ 一年2期（印刷品）450元
☐ 一年2期（掛號）490元
☐ 二年4期（印刷品）900元
☐ 二年4期（掛號）980元

訂戶姓名：_____
連絡電話：_____
E - mail ：_____
統一編號：_____
發票抬頭：_____

收款戶名：馮肅媛

寄款人　☐他人存款　☐本戶存款

姓名：申請人請於瞭解「郵政儲金匯兌個人資料直接蒐集告知聲明」內容後，填妥本單據交郵局辦理。

地址與電話：☐☐☐－☐☐

經辦局收款章戳

主管：

虛線內備供機器印錄用請勿填寫

◎寄款人請注意背面說明
◎本收據由電腦印錄請勿填寫

郵政劃撥儲金存款收據

收款帳號戶名

存款金額

電腦記錄

經辦局收款章戳