淺談量子計算

葉丙成／臺大電機系教授
鄭子宇／臺大電機系大三

自二次大戰之後計算機的雛形出現，科技日新月異，甚至像摩爾定律（Moore's Law）預測的成指數增長。隨著人們要求更大的計算量，也開始發掘這樣新奇的可能性：利用量子位元（qubit）儲存，並以量子力學預測的行為來操弄他們。量子電腦真能在眨眼間處理天文數字，還是另一個不切實際的幻想？筆者將和讀者介紹纏結的概念，然後定性的說明兩個演算法。接著，討論它與傳統計算機有什麼不同，或注定的限制。

幾條公理

量子力學是 20 世紀一群物理學家發展出來的，描述微觀世界的一套計算方式。我們用一個內積空間（inner-product space, 就是歐氏空間裡面向量的推廣）計算，並以單位向量（波函數）來表示系統的狀態（state）。這裡我們關心的是二維空間，其中 | 0 >, |1 > 這兩個位元是基底（basis, 類似座標軸），至於我們要用什麼實體的東西來代表他們，則暫且不論。【注：尖角括號在量子力學代表列向量】

當一段時間經過，可以乘上一個么正矩陣 U（unitary matrix, 類似歐氏空間的剛體轉動），來代表系統的改變。簡單的說，就是把 | 0 >, | 1 > 的組合作某種規律的重新組合。

測量的時候，也可以用矩陣 M 表示。如果 M 代表測量到 m 的結果這件事，那把 M 乘上目前的波函數，再取「長度」（範）就可以知道測量到 m 的機率 p_m 了。但是波函數也會改變，要重新計算。事實上，它本來是多重的狀態以加權混合，這時候會變成單一的值。

如何解釋這個式子的物理意義呢？依照主流觀點（Copenhagen interpretation），原來系統各有某種機率事何種狀態，現在，經過觀測，只可能是確定的值了。我們說波函數塌縮（collapse）了。

量子纏結

現在，可以介紹纏結（entanglement）的概念了，這可以充分展示量子物理的奇特，以至於瞬間運輸資訊，在某種意義上，是可能的。

詳言之，如果有 u, v, w 三個量子位元，現在將 v, w 通過一個「邏輯閘」（某種矩陣），輸出之後，v, w 不再無關，也就是纏結了。將 w 運送到遠方，依然不改變他們的纏結。這時考慮 u, v, w 的合成系統（現在 u 並未和 v, w 纏結），我們可以測量此合成的波函數 $|\phi>$，透過把他們重新以某種新「基底」（座標軸）表示，可以知道 w 原來的值，即使它在很遠的地方，而且 v, w 也沒有接觸。

事實上，根據狹義相對論，資訊傳播的速度不可能超過光速 c，故起初有人（包括愛因斯坦）為了調和量子力學的「矛盾」，認為有某些變數並未在量子力學被考慮；如果這樣作，就可以完整描述系統，物理事件也不是機率性的。但是這並未被廣泛接受。

Deutsch-Jozsa 演算法

為了舉例，我們再考慮一個硬幣，它的機率 f: {0,1} → {0,1} 可能是「永遠給出梅花或人頭」或是「給出梅花或人頭的機率都是 1/2」；傳統上，我們似乎要實驗很多次，仍不能確定它是哪一種。

但是這個機率函數 f 的性質與它的兩個值都相關，暗示我們可以利用波函數可疊加的能力。可是，當我們得到兩個結果的疊加，卻不能同時取得，因為測量會造成塌縮，使量子位元回到古典位元。

其實這個問題並未要求我們取得兩個值。如果用聰明的辦法把兩個可能的結果干涉（interfere），就通過特殊的矩陣來獲得答案。

Shor 演算法

RSA，一個非常普遍的密碼系統，的安全性依賴於，「將很大的數字 N 作質因數分解是困難的」這件事。古典的方法需要的步驟數約與指數成正比，但運用量子演算法只與 N^3 成正比。

關鍵在，這個過程需要針對很多不同的 x 計算指數 a^x，並觀查函數 $f = a^x$ 的周期。量子位元允許了同時計算許多值，並透過一連串「干涉」，讓我們知道 f 取值是否有重複出現的樣式。

偵測誤差

真實世界中，有許多不可避免的噪音（資訊的擾動）使傳輸資訊不同調（decoherence, 與環境交互作用）。古典系統中，最簡單的辦法就是把一個位元重複多次，使他們「投票」決定哪個是正確的，因為大部分的位元訛誤，比起少部分位元訛誤來的不可能。遺憾的是，有人證明（不可複製定理 , No-cloning theorem）量子系統不可能被完整複製。

可是 Shor 在 1995 年提出這個演算法：假如我們有 x, y, z, 量子位元，透過一些「邏輯閘」可以直接比較（XOR）x 和 y 是否不同 , 以及 y 和 z 是否不同。這樣就不難推敲之中有哪些由 $|0>$ 變 $|1>$（或反過來）了。

極限？

如果一個問題能在少於 Nk 的時間（N 是某個參數）內被解決，說它是 P（polynomial）問題。若不能在少於 N^k 之內被解決，但能在極短的時間被驗證，就說它是 NP。上述的 Shor 演算法是一例，在

古典運算是 NP，在量子運算卻是 P。NP 完全（NP-complete）是 NP 問題，而且如果找到快速的演算法，就能對所有 NP 問題都適用。量子電腦還沒解決任何一個 NP 完全問題。

何況，因為量子位元的機率性，還有測量造成的困難，我們要聰明的利用目標問題的特殊情況，來獲得全域的（和許多狀態都相關的）性質，就像方才的例子說明的。

也有人認為，量子電腦可以提供對量子力學的有史以來最嚴苛的測試。更何況，NP 完全問題的不可解，說不定能被當成計算機的公理，就像「熱機不可作淨功從低溫熱庫輸熱到高溫熱庫」是一個熱力學公理一樣。總之量子運算的未來還是令人振奮！

參考資料

1. Scott Aaronson. “The Limits of Quantum Computers.” Scientific American, March 2008.
   (Retrieved from: http://www.scottaaronson.com/writings/limitsqc-draft.pdf)
2. Samuel J. Lomonaco, Jr. “Lecture 1: A Rosetta Stone for Quantum Computing.”
   (Retrieved from: http://www.csee.umbc.edu/~lomonaco/conf/uva2003/lecture1.pdf)
3. “Lecture 2: Three Quantum Algorithms.”
   (Retrieved from: http://www.csee.umbc.edu/~lomonaco/conf/uva2003/lecture2.pdf)
4. Mark Oskin. “Quantum Computing - Lecture Notes.”
   (Retrieved from: http://www.cs.washington.edu/homes/oskin/quantum-notes.pdf)
5. 科學人 — 聚焦物理世界。台北：遠流 , 2011。