



量子計算 不可迴避的挑戰

作者：黃琮暉

作者簡介

黃琮暉是臺灣大學物理學博士，現任職於中原大學資訊工程系與中原大學量子資訊中心，研究的領域是量子計算、量子資訊。

人類對於量子電腦或是量子計算的概念可以回溯到 20 世紀末期費曼提出利用量子特性來模擬自然界難解量子力學的問題，爾後更多的理論提出來量子計算在特定題目具有快速計算的能力，除了上述原子分子問題外還有：破解 RSA 加密（快速的質因數分解法）[1]、搜尋問題 [2] 等，因此科學家一直想實現量子計算進而增進計算能力，然而過去受限於硬體設備往往只能在實驗室做出原型機或是驗證量子計算的可行性。然而近年來量子電腦的硬體蓬勃發展，而且在各個目前的主要硬體包含：超導型量子電腦 [3]、離子阱量子電腦 [4]、光子型量子電腦 [5] 等在實現量子位元 (qubits) 都有快速的進步與突破，如在超導型量子電腦 IBM 已經具有 127 個量子位元的計算能力 [6]、離子阱型量子電腦具有百萬的量子體積 (quantum volume) [7]、光子型量子電腦能在室溫下運算等等。這代表人類實現量子計算的機會越來越大也越來越快。但不管何種硬體以目前的技術跟物理上的限制都會有量子退相干性 (quantum decoherence) 與量子退相位性 (quantum dephasing) 的問題 [8]，而這些線上在量子計算上就會造成錯誤以至於計算結果是錯誤的，因此除了發展更多的量子位元外，量子計算的另一個挑戰就是如何降低錯誤發生或是消除錯誤。前者通常是製作硬體的科學家或是工程師所考慮的，而後者是藉由理論與計算的原理來消除錯誤的發生，被稱為糾錯理論 (error-correction theory) [9]。而本文主要著重在於糾錯理論並拋磚引玉讓讀者有機會踏入量子糾錯理論的世界裡。

糾錯理論

糾錯理論並不是只發生在量子計算中，在古典通訊或是透過網路傳送資料時都需要做糾錯以保證傳遞資訊的正確性，在古典上可以利用三個位元代表一個位元的資訊，例如：000 代表一個 0。這樣的好處是當這三個位元只有一個錯誤，依然可以判別出正確的資訊。例如當透過網路接受到 001 或是 010 或是 100 還是可以知道該資訊應該為 0 而非 1。[10]

要考慮量子糾錯理論首先要從量子位元與古典位元 (bit) 的不同，單一個量子位元可以表示為

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle,$$

其中代表出現 0 (或 1) 的機率為

$$\left|\cos\frac{\theta}{2}\right|^2 \text{ (或 } \left|e^{i\phi}\sin\frac{\theta}{2}\right|^2 \text{)},$$

而其中的 θ 與 ϕ 可以對應到布洛赫球面 (Bloch sphere) 上如圖 1。其中 θ 的數值可以改變 0 與 1 的機率大小，而 ϕ 則被稱為相位 (phase)。因此最簡易的量子錯誤率 (此種錯誤率稱為相干錯誤 [coherent error]) 可以寫為

$$|\psi'\rangle = \cos\frac{\theta + \delta\theta}{2}|0\rangle + e^{i(\phi + \delta\phi)}\sin\frac{\theta + \delta\theta}{2}|1\rangle。$$

本文作者特別致謝科技部的支持，其計畫編號為 MOST111-2119-M-033-001-。