

量子資訊淺談

蘇正耀

國家高速電腦中心

zsu@nchc.gov.tw

量子資訊學是近年來快速成長的領域。限於時間，本文僅對早期幾個主要的發展，做最淺顯的介紹。

夢想與驚喜

始自第一個電子計算機開始運轉，構想能夠超越傳統所謂 Turing Machines 的計算模型，便是許多科學家努力的夢想。美國阿岡國家實驗室的 Paul Benioff 是第一位提出概念⁽¹⁾，認為利用量子物理的二態系統模擬數位 0 與 1，可以設計出更有效能的計算工具。此概念稍後又經 Feynman 的引申⁽²⁾，使得有更多的物理學家注意到量子力學與計算科學之間可能的關聯。直到 1985 年，在英國牛津的物理學家 David Deutsch 發表的一篇論文裡⁽³⁾，所謂 Quantum Church-Turing Machines 才正式開始略具數學型式。但此論文中所提示的量子計算範例，則過於簡易且不甚實際。

到了 1994 年，Bell Lab 的應用數學家 Peter Shor，於當年 IEEE 基礎計算理論年會發表突破性工作—快速整數因數分解方法（現今已被稱為 Shor's Algorithm）⁽⁴⁾，量子計算的潛在應用實力便迅速引起廣泛的注意。因為如果能對任意極大的整數快速作質數分解，就可以破解目前普遍採用的 RSA 密碼

系統。以傳統已知最快的方法對整數 N 做質數分解，其計算的複雜度（Complexity）是此整數位數（ $\log N$ ）的指數函數；此難以突破的鉅額計算複雜度保證了密碼系統的安全性。Shor 的方法卻可將此複雜度降為多項式函數（雖然僅是機率性的），使得快速破解 RSA 密碼系統成為可能。此工作所引起的震撼不難想像，自 94 年後有關量子計算、量子通訊或所謂量子資訊學的論文便疾速增加，也開始吸引大量研究經費的投入（特別是來自軍方與工業界）。目前在美國、歐洲、日本以及中國大陸，已經有許多專為此新領域而成立的研究團隊或研究機構。而 Shor 本人則於 98 年柏林舉行的國際數學大會，與 Andrew Wiles（費馬最後定理的證明者）一同獲獎表揚（雖然不是費爾茲獎，但與其對等）。

平行與糾纏

量子計算機的實現，不是為了取代傳統的計算機，實際上也無法取代。一個有效的量子計算方法，其成功在於巧妙的結合本身特徵優勢，以及可在傳統計算機快速執行的古典技巧，然後在特定極困難

問題上擊敗已知的傳統方法。這裡所指的特徵優勢主要有二——即所謂的量子平行 (Quantum Parallelism) 與量子纏結 (Quantum Entanglement)。量子平行簡而言之，就是只需 n 個運算 (酉變換, Unitary Transforms)，就可以準備出 2^n 個可能狀態，雖然這 2^n 個狀態是以線性組合的方式結為一個狀態；所以自然也可以再一起通過另外一個變換，就相當於同時對此 2^n 個狀態做了該變換。而為準備此 2^n 個狀態，也只需要 n 個量子位元 (Qubits, 由二態量子系統來實現) 即可。量子纏結指的是兩個或更多的量子系統彼此關聯，因而使得某些物理量無法由單一或少數的系統獨立決定。此纏結特徵幾乎在所有的量子運算中自然產生，也是計算所以加速的原因之一；但因為是自然產生，故往往不在過程中特別強調，待稍後範例再來說明量子纏結極其特殊的作用。

一個量子計算的過程可簡單視為將所有可能的 2^n 個輸入 (inputs)，以線性組合的方式“儲放”在 n 個量子位元上，再加上運算過程中輔助用的 m 個量子位元 ($m < p(n)$, p 是某一個多項式函數) 的資料，一起通過適當數目 (此數目也是 n 的某一個多項式函數) 特別設計的酉變換，之後 2^n 個 outputs 即同時現，雖然仍舊以某種線性組合的方式儲放在數個量子位元上。如何從這輸出的線性組合態“萃取”——即測量其中一個或數個量子位元——正確的答案，則完全取決於運算過程中酉變換的選擇與設計。至此已可看出量子計算能獲致正確答案，往往是機率性 (probabilistic or nondeterministic, 如同量子力學一般) 而非絕定性的 (deterministic)。

分離與追尋

Shor 整數因數分解方法的成功，在於精巧的結合了古典數論技巧與量子傅利葉變換 (QFT, Quantum Fourier Transform)。這裡的古典數論技巧主要指的是計算一特定模數函數的週期 (故須引用傅利葉變換來求得此週期)，再利用孰知的輾轉相除法即可獲得該整數 N 的因數。此技巧早在 70 年代已被應用在數論與資訊科學研究上⁽⁵⁾，本身即是機率性的方法。而量子傅利葉變換是由 IBM 的 Coppersmith 首先給出⁽⁶⁾，數學上可視為快速傅利葉變換 (FFT, Fast Fourier Transform) 的量子計算版本 (量子計算中基本的 Hadamard Transform 即是 2-point FFT)。由於量子平行的特性，使得變換的複雜度由 FFT 的 $O(N \log N)$ 降為 QFT 的 $O(\log N \log N)$ 。雖然是機率性的方法，但由於每次嘗試的計算複雜度已大為降低，所以整體而言仍保證了因數分解的快速取得⁽⁷⁾。固然熟練的運用諸多數論與分析的技巧，Shor 的方法真正揭示給人們的是量子傅利葉變換的快速與實用。受此啟發，已有許多文獻報告了 QFT 在不同問題的推廣與應用⁽⁸⁾。

繼 Shor 的快速因數分解方法後，另外一個較重要的量子計算研究成果，是於 96 年由 IBM 的 Lov Grover 所提出的量子資料庫搜尋 (Quantum Seaching)，如今已稱作 Grover's Algorithm⁽⁹⁾。此方法所針對的命題為：在一個有 N ($N=2^n$) 個物件的資料庫中，若且惟若有一個物件合乎所指定的要求，請搜尋出此物件。以古典的方法做搜尋其複雜度 (搜尋的步數) 為 $O(N)$ ，而量子搜尋的複雜度則減為 $O(\sqrt{N})$ 。此方法的原理是首先將每一個物件視為一個單位正交基底向量，遂形成了一個 2^n 維數的 (希爾伯特) 空間 (所以需要 n 個量子位元)；暫以 $|x\rangle$ 為代表被搜尋物件的基底向量。然後將所有

基底以相等振幅相加做為初始向量，將此向量暫記為 $|V\rangle$ 。所謂的量子搜尋其實就是盡量放大此向量 ($|V\rangle$) 中代表被搜尋物件基底 ($|x\rangle$) 分量的振幅，而當在此分量振幅達到最大時做測量，就有最高的機率攫取到此被搜尋物件。代數上 $|x\rangle$ 分量振幅的放大，就等同於幾何上將 $|V\rangle$ 盡量移至 $|x\rangle$ 的方向。雖然是處於一個 2^n 維數的高維空間，將 $|V\rangle$ 移至 $|x\rangle$ 最便捷的路線就是沿著此二向量所張成的平面做旋轉；Grover 的方法就是找出對應此旋轉的酉變換。雖然數學結構上遠不如 Shor 方法的精巧與困難，但 Grover 搜尋有更廣泛的實用價值，因此也引發了許多後續研究。很快的被推廣改進，Grover's Algorithm 已拓展到可搜尋多物件的情況⁽¹⁰⁾。

春嬌與志明

早於 70 年代，Stephen Wiesner 已提出量子通訊的相關想法，但由於此類概念對當時而言過於先進，所以其原始論文遲遲未獲發表。直到 92 年與 Charles Bennett 合作關於超密加碼 (Superdense Coding) 的論文⁽¹¹⁾，才使此概念正式見諸於世。也是該論文將量子纏結的特徵優勢，首次應用到通訊技巧上。

到了第二年，Bennett 與合作者又更進一步援用量子纏結態，提出了量子隱傳 (Quantum Teleportation) 的構想⁽¹²⁾。就數學原理，超密加碼與量子隱傳是兩個互為對偶 (Dual) 的概念。首先假設春嬌 (Alice) 與志明 (Bob) 是一對相隔甚遠的戀人，春嬌想把手邊的一個單一量子位元“隱形傳遞”給志明當禮物。但春嬌完全不知道此位元處於何型式的量子態，當然她不能去測量它，因為一

旦測量此位元就崩毀了。因為修過量子力學，事前他們已準備了一副老字號的 EPR 纏結對，將此量子對的第一個位元由春嬌帶走，第二個位元由志明保留。當春嬌想把手上的禮物量子位元隱傳給志明時，她只須將此位元與原先帶來的位元(得自於 EPR 纏結對) 同時一起做“貝爾測量”(Bell Measurement)。由於是對兩個量子位元同時做測量，所以一定是量到四個正交量子態(即所謂的 Bell's states) 的其中一態。然後春嬌再根據測量的結果，以電話指示志明對他手上的量子位元做對應的酉變換後(包括單位變換或三個鮑立矩陣的其中之一)，志明手上的位元就完全轉換至原先春嬌的隱傳(禮物)位元量子態——換句話說，未經實際距離上的傳遞，春嬌已將手上的禮物量子位元送給了志明，一個科幻電影中常見的情節。

超密加碼的過程也極為類似，只是更為簡單。春嬌選取上面四種之一的酉變換，作用在自己手上的位元(來自 EPR 纏結對)，然後將此作用後的量子位元傳給志明。志明接到此位元後就與自己原先手上的位元(EPR 纏結對的第二個位元)一起做貝爾測量，其結果也一定是落在四個正交量子態的其中之一，至此即可得知春嬌原先所選擇的酉變換——也就是說僅靠一個量子位元就可以傳遞兩個古典位元的資訊。進一步的推廣，利用 K 個 EPR 纏結對，可以隱傳任意 K 個量子位元；而 $2K$ 個古典位元資訊的傳遞，只需藉由 K 個量子位元的運載。就數學上而言，過程中所牽涉到的酉變換，實際上是在進行所謂量子錯碼修正，而 EPR 纏結對則扮演著量子修正密碼(Quantum Error Correcting Code)的角色。

只是正開始

自 Shor 與 Grover 的貢獻之後，量子計算的進展就略顯停滯。原始催生此研究的基本疑問：“是否存在量子技巧 (Quantum Algorithms) 可對古典極度困難問題^[13] (Intractable or NP-Complete Problems) 提供多項式時間解 (Polynomial-Time Solutions),”也一直尚未有明確的答案。但在量子通訊方面，卻已累積了可觀的成果。基於量子力學本身的特性，使得在傳訊過程中具有“凡竊聽必留下線索” (No Disturbance, No Information Gained) 的優勢，因而大大刺激了量子密碼學 (Quantum Cryptography) 的蓬勃發展^[14]。

爲了對抗量子計算與通訊過程中不可避免的消相干 (Decoherence) 效應所造成的錯誤，Shor、Steane 等人引申古典線性群密碼 (Linear Group Code) 的概念，建立了量子修正密碼 (Quantum Error Correcting Code) 的理論架構^[15]。量子與古典修正密碼除了要修正位元的失誤外 (如 0 與 1 的互變)，前者比後者更多了修正相位失誤的功能 (因古典密碼沒有相位的差異)。看似增加複雜度，實際上此功能提昇了量子密碼的傳訊效率；也就是可以用較短的密碼傳送較多的資訊。完全根據群生成子 (Group Generators) 的交換與反交換特性，D. Gottesman 發展的 Stabilizer Codes^[16]，是量子修正密碼選擇中數學結構最優美，也最具推廣潛能的探索方向。

在上面所提及的諸多研究中，產生各式各樣不同的量子纏結態是隨處可見。如何對這些纏結態加以分類、量化，可能是目前此領域最富挑戰性，也最引人入勝的研究課題^[17]。由於此課題的基礎性，使我們不得不說——其實量子資訊學的研究才正開始。

參考文獻

1. P. Benioff, J. Stat. Phys. 22, 563 (1980); Phys. Rev. Lett. 48, 1581 (1982).
2. R. P. Feynman, Int. J. Theor. Phys. 21, 467 (1982).
3. D. Deutsch, Proc. Roy. Soc. A400, 97 (1985).
4. P. W. Shor, in Proc. 35th IEEE FOCS, 124 (1994).
5. D. E. Knuth, Seminumerical Algorithms 3rd ed., vol. 2 of The Art of Computer Programming, Addison-Wesley, Reading, MA (1997).
6. R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, Proc. Roy. Soc. A454, 339 (1998).
7. D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill, Phys. Rev. A 54, 1034 (1996).
8. A. Y. Kitaev, quant-ph/9511026 (1995); A. Ekert and R. Jozsa, quant-ph/9803072 (1998); M. Mosca and A. Ekert, quant-ph/9903071 (1999).
9. L. Grover, in Proc. 28th ACM STOC, 212 (1996).
10. R. Jozsa, quant-ph/9901021 (1999); G. Chen, S. A. Fulling, and M. A. Scully, quant-ph/9909040 (1999).
11. C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. 69, 2881 (1992).
12. C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wothers, Phys. Rev. Lett. 70, 1895 (1993).
13. M. R. Garey and D. S. Johnson, Computers and Intractability, Freeman, NY (1979).
14. C. H. Bennett and G. Brassard, in Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing, 175 (1984); A. Ekert, Phys. Rev. Lett. 67, 661 (1991).
15. A. R. Calderbak and P. W. Shor, quant-ph/9512032 (1995); A. Steane, quant-ph/9601029 (1996).
16. D. Gottesman, Stabilizer Codes and Quantum Error Correction, Ph.D. thesis, Caltech (1997).
17. V. Vedral and M. Plenio, quant-ph/9707035 (1997); W. K. Wothers, quant-ph/9709029 (1997); M. Horodecki, P. Horodecki, and R. Horodecki, quant-ph/9801069 (1998).