【庖丁篇】— 刊於《經濟日報》，2021 年 9 月 30 日

量子計算有望突破摩爾定律極限

黃 昊
科大商學院會計學系副教授、商學院副院長

本月初，中國科學技術大學潘建偉、朱曉波團隊在 arXiv 提交了論文《60 量子比特 24 層循環隨機電路採樣的量子計算優越性》(Quantum Computational Advantage via 60-Qubit 24-Cycle Random Circuit Sampling)。 文章報道了超導量子計算系統祖冲之 2.1，與祖冲之 2.0 相比，量子比特數量仍為 66，但是完成了更大規模的隨機電路採樣。照文章估計，祖冲之 2.1 只需約 4.2 小時即可實現如果使用傳統計算機，即便使用最先進的經典算法（張量網絡）和超級計算機 (Summit) ，也需耗時長達數萬年(約 4.8 萬年)，才能完成的經典模擬隨機電路採樣實驗。即量子運算的速度快了近 1 億倍，大大提高了量子計算優越性（即量子霸權）。

究竟量子計算機和量子計算技術在商業應用上的前景如何，的確是一個引人入勝的議題，很值得一談。

量子理論和計算其實已經有一段時間。可以說，量子理論是 20 世紀一項偉大的科學發現和成就；而量子計算機在上世紀 80 年代亦已經出現和應用，只是當時的設置相對簡單。很顯然，量子計算機何以出現，其肇端可以從經典物理學和量子物理學的區別之中得到了解。

電子計算機與摩爾定律

普通的計算機，是以電子作為基本載體，通過 0、1 的二進制系統進行運算。無論是數子、文字、圖片等所有訊息，都使用一系列 0 與 1 表示並進行儲存。最小儲存單元稱為「位元」(bit)。在採用二進制的數字電子方式進行運算時，二進制整體處於 0 或 1 的確定狀態。

經典電子計算機一路發展，經過上世四十、五十年代，按照摩爾定律，積體電路可容納的電晶體數目，每隔 18 個月增加一倍，回頭去看，電晶體的數目的確不斷增加，體積愈來愈細，如今已然到了「納米」級水平，而摩爾定律所描述

電晶體以倍數增加的速度，近年不僅在邏輯上也在現實上無法保証會持續下去。在受到物理上的限制，要再發展下去，很自然考慮進入量子計算和應用量子計算機的新紀元。事實上，量子計算被認為是突破摩爾定律極限最有前景的技術之一，為社會發展帶來進步和改變的力量。

薛定諤的貓

量子計算技術與二進制電子計算技術不同，量子計算是按照量子力學的規律調控量子信息單元進行計算。扼要言之，量子計算是利用量子力學的叠加特性，能夠在計算狀態下進行叠加，亦即不只包含 0 和 1，而且還可以包含 0 和 1 混合同時存在的「叠加態」（superposition）。換言之，電子計算機每個「位元」是 0 或者 1，但量子計算機，有 0 和 1「混合物」的儲存單位，稱之為「量子位元」（qubits）。

談到「叠加態」，值得補充解釋量子力學上著名「薛定諤的貓」（Schrodinger's cat）的思想實驗。把貓放到一個盒子裡，盒內接連到一個包含一個放射性原子核和一個裝有毒性氣體的實驗裝置。如果這個放射性原子核發生衰變，便觸發實驗裝置打開，毒死這隻貓。按照量子力學，未進行觀察時，亦即盒子不打開，這個原子核處於已衰變和未衰變的叠加態，這隻貓在盒內處於生存、又處於死亡的叠加狀態，即「又是生又是死」；但如果把盒打開進行觀察，叠加態瓦解，便會看到「衰變的原子核和死貓」，或者，是「未衰變的原子核和活貓」兩種情況。換言之，一進行觀察，就會確認貓是生是死。未觀察，便處於「又是生又是死」的叠加態。

量子計算叠加態倍增算力

量子計算另一個特徵是量子糾纏（quantum entanglement），即個別粒子在彼此相互作用後，之間雖然相隔很遠距離，但彼此有連繫，相互有所反應，而且在相互作用後所形成的系統整體性質，使得量子計算機較經典的電子計算機，在處理很多具體問題上，取得更快速和更強大的處理算力。

「叠加態」加上量子糾纏，導致的結果是可以進行併行的運算，譬如 2 個 qubits，可以進行 4 個運算（2 的 2 次方）；3 個 qubits，可以進行 8 個運算（2 的 3 次方）。可以像想，100 個 qubits 以至 1000 個 qubits，理論上，1000 個 qubits 可以進行 2 的 1000 次方的運算，如此巨大的併行運算能力，是電子計算機所無法比擬的。

目前，量子計算機還未普及商業化，有其硬件和軟件的原因。先說硬件，這種量子計算機的硬件要求很高，並且容易受到其他外來的干擾。可編程的量子芯片，在材料、工藝、設計、製造和封測等方面的要求，都同經典集成電路芯片有異。在軟件方面，需要有新的編程語言。

用秀爾算法破解密碼

誠然，量子計算機和普通電子計算機比較，前者並非每一處都比電子計算機更為先進，但由於量子計算技術是可以同時併行多種運算，因而對某一些問題，特別適宜用量子計算機來運算。不過，應用者要找得到問題，並能夠用量子計算機讀得懂的語言來編程。

在九十年代中，美國計算機科學家比得・秀爾（Peter Shor）提出在量子計算機應用上的「秀爾算法」（又稱為量子質因數分解演算）。計算的基礎方法，是把一個整數分解為幾個約數的乘積。秀爾算法之所以重要，因為它代表使用量子計算機，我們可以用來破解已被廣泛使用的公開密鑰加密方法，也就是 RSA 加密算法。換言之，RSA 加密算法的基礎，是假設了我們不能有效率地分解一個已知的整數，而秀爾算法明晰地展示了分解這個問題，可以在量子計算機上有效得到解決。雖然，傳統的電子計算機也可以進行運算解密，但需要的時間很長。基於量子計算機可以同時作併行計算，據此能夠更有效地快速解決。

近幾年量子計算機的發展特別快速，原因何在？可以說，一方面，是硬件方面取得可觀發展，進步神速。事實上，谷歌、IBM 和不少科研公司近年投入大量資源在這方面，尤其是美國和中國，近年投入大量資源開發量子計算機的硬件材料，上文提到國防科技大學計算機學院牽頭研製的銀河鯤騰 QW2020 量子計算系統，見微可知中國在這方面的投入；另一方面，在軟件方面，即算法方面有很大提高。

給人類帶來無限想像和憧憬

誠然，量子計算機和量子技術在商業和金融應用上，近年受到銀行和金融機構投入資源，不斷進行研究和開發。除了金融應用的潛在領域，譬如，在交通運輸行業上來說，在什麼情況下，如何選擇最優的運輸路線，車輛可以用最短的時間和成本，把貨物運輸到目的地，量子計算技術可以輕易取得最優的選擇方案。

在上世紀四十、五十年代，電子計算機的運算能力有限，但機體的體積幾乎佔用了整個房間。能夠擁有一部電子計算機，人數不多。但有誰料到，目前不論海內外世界各地，幾乎每個人都擁有至少一部手機，而手機的體積可以在手握之中，且功能之多，已同每個人的生活牽連一起，無論購物、交易支付，進行社交活動，掌握世界大事的發生，都可盡在手機中有效率地得到實現，當中所蘊含的商機，是當年無法想像的！如今量子計算機和量子計算技術的研究和開發，在未來商業上的應用，無疑也給人類社會帶來無限的想像和憧憬！