量子計算不可迴避的挑戰

黃琮暐 [1,2]

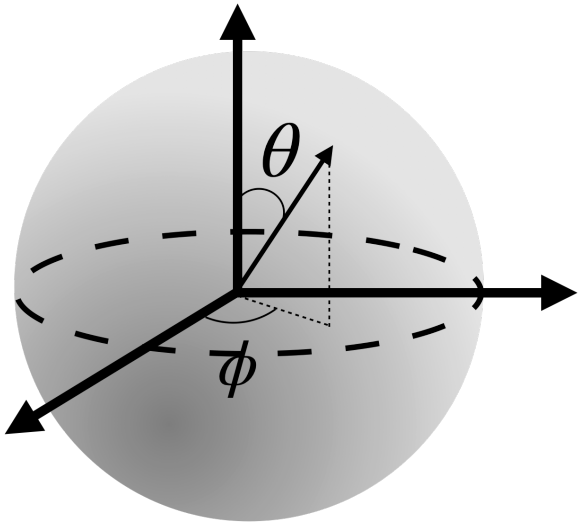
1. 中原大學資工系

2. 中原大學量子資訊中心

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]、搜尋問提[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（qubit）與古典位元的不同，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$\left|\cos\frac{\theta}{2}\right|^2$（或$\left|e^{i\phi}\sin\frac{\theta}{2}\right|^2$），而其中的$\theta$與$\phi$可以對應到布洛赫球面上如圖一。其中$\theta$的數值可以改變 0 與 1 的機率大小，而$\phi$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$|\psi'\rangle = \cos\frac{\theta+\delta\theta}{2}|0\rangle + e^{i\phi+\delta\phi}\sin\frac{\theta+\delta\theta}{2}|1\rangle$。從此可知量子糾錯理論將會比古典糾錯

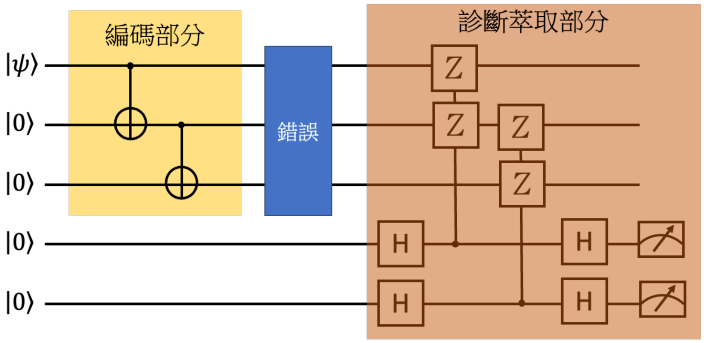


圖一：布洛赫球，在理想的量子計算上單一個量子位元的所有狀態可以用布洛赫球面描述。

理論困難許多。還好根據數學嚴格上的驗證，任何一種相干錯誤都可以利用包利矩陣展開，即$|\psi'\rangle = \cos\frac{\theta+\delta\theta}{2}|0\rangle + e^{i\phi+\delta\phi}\sin\frac{\theta+\delta\theta}{2}|1\rangle = \alpha_I I|\psi\rangle + \alpha_x X|\psi\rangle + \alpha_Z Z|\psi\rangle + \alpha_Y Y|\psi\rangle = \alpha_I I|\psi\rangle + \alpha_x X|\psi\rangle + \alpha_Z Z|\psi\rangle + \alpha_{XZ} XZ|\psi\rangle$，因此在相干錯誤下只需要針對X與Z所造成的錯誤做糾錯[11]。而X所造成的錯誤被稱為翻轉錯誤（flip error）、Z所造成的錯誤被稱為相位翻轉錯誤（phase flip error），其中X所類似像是古典的錯誤一樣會將位元所處的數值翻轉，然而Z所造成的錯誤沒有類似的古典錯誤。除了糾錯形式與古典糾錯有差異之外，在量子計算中還有兩個很重要的特性，在實現量子糾錯演算法必須知道：（1）不可克隆理論（No-clone theorem）即無法複製任意的量子態[12]；（2）量子量測，量測後量子狀態會崩塌（collapse）到古典態，即量測後量子態消失。

以下我們提及一個比較容易理解的量子糾錯過程。首先將三個量子位元當作一個邏輯量子位元（logical qubit，意指沒有錯誤的量子為元。）也就是當需要傳遞一個任意量子位元資訊$|\psi\rangle$利用三個量子位元描述，其中創建的方法如圖二中編碼器部分：$|\psi\rangle \to \alpha|0\rangle_L + \beta|1\rangle_L = \alpha|000\rangle + \beta|111\rangle$。這邊要注意的因為量子態無法複製且測量後該量子狀態就消失了，所以無法像古典糾錯一樣一個一個比對去找出事否有誤，而檢測的方法可以如圖二中診斷萃取部分。舉個例子如果整個錯誤造成第二個量子位元翻轉錯誤（及造成X誤差），這樣經過編碼部分並且通過錯誤區域前三個量子位元的量子態為：$|\overline{\psi}\rangle = \alpha|010\rangle + \beta|101\rangle$而整個系統（包含兩個診斷萃取的輔助位元）狀態變為：$|j\rangle|\overline{\psi}\rangle = (\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle))(\alpha|010\rangle + \beta|101\rangle)$；再經由兩個 controlled-ZZ 操作將得到 $\frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)\ (\alpha|010\rangle + \beta|101\rangle)$；最後讓兩個輔助位元透過 Hadarmad 操作將得到$|11\rangle(\alpha|010\rangle + \beta|101\rangle$，此時經由測量輔助位元可以知道第

二個位元被翻轉了。同樣的方法可以驗證出不同錯誤有不同的測量結果，所有的結果如下表一：



圖二：三位元的糾錯演算法，在此方法中需要利用三個量子位元當作一個邏輯量子位元與兩個輔助位元。黃色區域為編碼部分可以將想保存的資料轉成三個量子位元的型態；藍色違過程中可能造成的錯誤；橘色區域為診斷萃取部分用來判定那個位元發生錯誤。

錯誤型態	診斷結果	錯誤型態	診斷結果
$I_3I_2I_1$	00	$I_3X_2X_1$	10
$I_3I_2X_1$	01	$X_3X_2I_1$	01
$I_3X_2I_1$	11	$X_3I_2X_1$	11
$X_3I_2I_1$	10	$X_3X_2X_1$	00

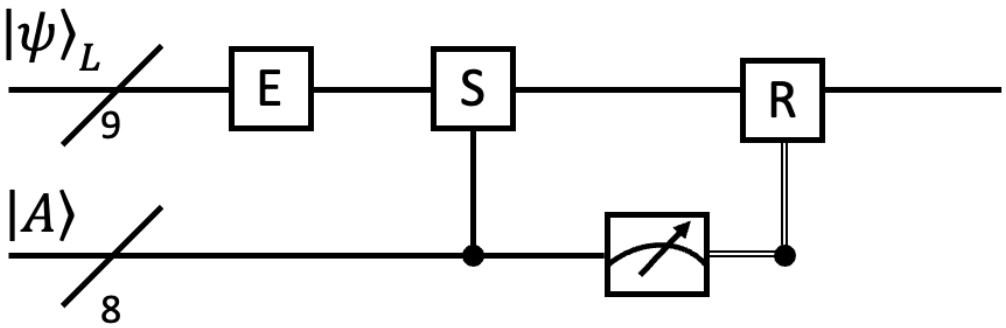
表一：在不同位置中發生翻轉錯誤下診斷部分的量測結果。

根據上表（左半邊）跟測量結果可以知道可以透過輔助位元的測量知道哪個量子位元具有翻轉錯誤。然而當錯誤在兩個以上這種方式依然會判斷錯誤如表一右半邊。然而如前面所說量子糾錯除了翻轉錯誤還有相位翻轉錯誤，在相位翻轉錯誤可以將考慮的基底換成$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$與$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$，在這種基底下可以清楚分辨出相位翻轉造成的誤差，也就是$Z|+\rangle = |-\rangle$與$Z|-\rangle = |+\rangle$。依照上面的方法將三個量子位元當作一個邏輯量子位元，即$|+\rangle_L = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$與$|-\rangle_L = \frac{1}{\sqrt{2}}(|000\rangle - |111\rangle)$，其實當其中任何一個量子位元的錯誤是相位翻轉都會讓這種編碼方式$|+\rangle_L \leftrightarrow |-\rangle_L$因此這種編碼方式無法有效的糾錯相位翻轉的錯誤。雖然這個例子無法完美的修正量子錯誤，但是一種比較容易理解的例子。而歷史上第一個有用的量子糾錯演算法是秀爾九量子位元糾錯（Shor nine-qubit code）[9]，其中利用 9 個量子位元當作一個邏輯量子位元，訂為

$$|0\rangle_L = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$

$$|1\rangle_L = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)$$

除了利用 9 個量子位元之外，還需要 8 個輔助位元來作為診斷萃取的量子位元，簡易的量子電路圖如下圖三。



圖三：秀爾九量子位元糾錯演算示意圖。其中 E 為過程中造成的錯誤， S 為萃取錯物的方法， R 為根據萃取結果修正錯誤。

在這裡將不仔細推導詳細過程，而利用秀爾糾錯演算法萃取出來的錯誤表入下表二：

錯誤型態	診斷結果	錯誤型態	診斷結果
X_1	10000000	Z_1	00000010
X_2	11000000	Z_2	00000010
X_3	01000000	Z_3	00000010
X_4	00100000	Z_4	00000011
X_5	00110000	Z_5	00000011
X_6	00010000	Z_6	00000011
X_7	00001000	Z_7	00000001
X_8	00001100	Z_8	00000001
X_9	00000100	Z_9	00000001

表二：在不同位置中發生翻轉錯誤與相位翻轉下診斷部分的量測結果。

雖然在本文中沒有仔細探討如何實現上表，然而重點是在使用秀爾九量子位元糾錯演算法可以同時針對翻轉錯誤與相位翻轉錯誤做糾錯，這便使得量子糾錯演算法是可能實現的。然而在這裡有更多可以做的包括是否有可能在使用更少的量子位元實現量子糾錯，這方面讀者可以參考。而在使用量子糾錯的機率限制可以參考。另外根據上述兩個問題可以延展出來議題—故障容許度的量子電腦（Fault tolerance quantum computer）可以參考。總括來說量子糾錯是量子電腦不可迴避挑戰，也是一個重要且嶄新的領域，依然有非常多的可能，也是值得投入的領域。

致謝：
本文特別致謝科技部的支持其計畫編號為 MOST111-2119-M-033-001-。
Reference:

1. Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing. 1997;26(5):1484–1509.
2. Grover LK. A fast quantum mechanical algorithm for database search. In: STOC; 1996.
3. Wendin G. Quantum information processing with superconducting circuits: a review. Reports on Progress in Physics. 2017;80(10):106001. Available from: https://doi.org/10.1088/1361-6633/aa7e1a.
4. Ballance C, Harty T, Linke N, et al. High-fidelity quantum logic gates using trapped-ion hyperfine qubits. Physical Review Letters. 2016;117(6).
5. Qiang X, Zhou X, Wang J, et al. Large-scale silicon quantum photonics implement- ing arbitrary two-qubit processing. Nature Photonics. 2018;12(9):534–539. Available from: https://doi.org/10.1038/s41566-018-0236-y.
6. https://www.hpcwire.com/2021/12/13/ibm-breaks-100-qubit-qpu-barrier-marks-milestones-on-ambitious-roadmap/
7. https://www.nextbigfuture.com/2021/03/ionq-quantum-computer-4-million-quantum-volume-and-16x-error-correction.html
8. Gardiner C W 1991 Quantum Noise (Springer Series in Synergetics vol 56) (Berlin: Springer)
9. Shor P W 1995 Scheme for reducing decoherence in quantum computer memory Phys. Rev. A 52 R2493
10. MacKay DJ. Information theory, inference and learning algorithms. Cambridge University Press; 2003.
11. Knill E, Laflamme R. Theory of quantum error-correcting codes. Physical Review A. 1997;55(2):900– 911.
12. Wootters WK, Zurek WH. A single quantum cannot be cloned. Nature. 1982; 299 (5886) :802–803.