2025 年【科學探究競賽-這樣教我就懂】

大專/社會組　科學文章格式

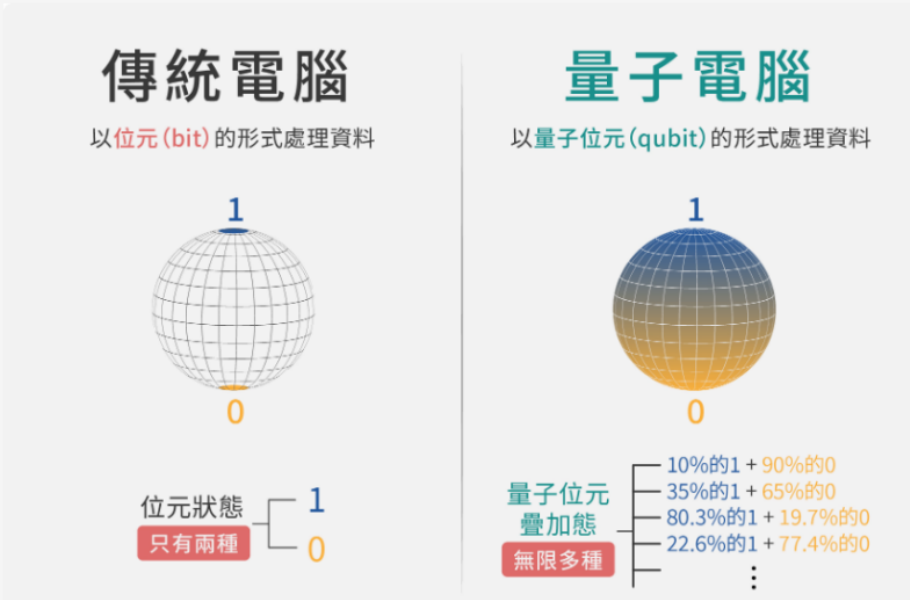
文章題目：　打破 0 與 1 的世界:量子電腦的奇異革命

摘要：在社會大眾所熟知的(傳統)電腦中，皆是以「位元」0 和 1 為基礎做運算，然而量子電腦則是運用「量子位元」，一個可以同時處於 0 和 1 兩種狀態的特殊位元作運算，這是量子電腦具有比傳統電腦更強大計算能力的原因之一。因此本文將介紹何謂量子位元、並講述量子電腦可能帶來的利與弊。

文章內容：（限 500 字~1,500 字）

位元 vs.量子位元

傳統電腦以位元(bit)為基本單位處理資料，每一個位元狀態會被標示為 0 或 1；而量子電腦則應用量子位元(qubit)，為了使量子位元能夠被應用，量子需具有量子疊加態(quantum superposition)和量子糾纏(quantum entanglement)的特性，即單一量子需同時處於兩種物理狀態，且兩個量子間需形成聯結，使得兩個量子即使處於不同的空間，仍然可以互相影響。由於量子位元的疊加和糾纏特性，使得量子位元能夠同時為 0 和 1，並使運算能力增加。

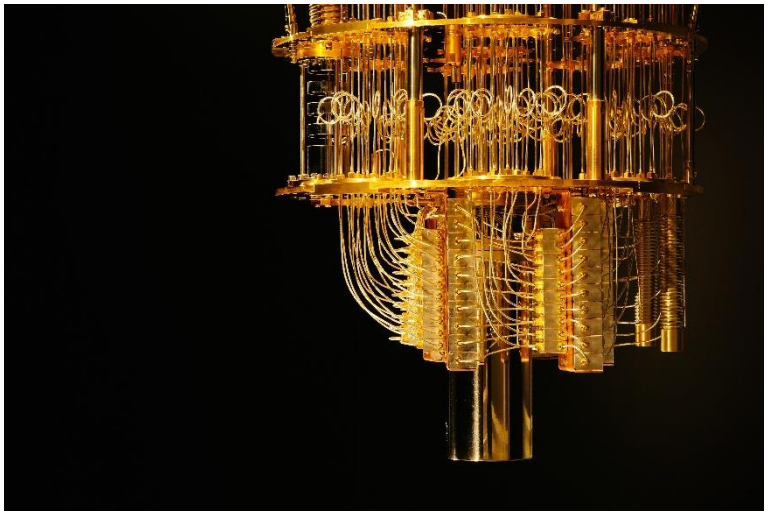


(圖一)　傳統電腦與量子電腦的位元差別

量子電腦的利與弊

如前所述，量子電腦不像傳統電腦，因其量子位元具有疊加和糾纏特性，使量子電腦同時間可以進行多個平行處理計算，在運算速度上遠比任何超級電腦都快得多，因此將在解決大量運算的代數問題、模擬蛋白質和化學結構、醫學與製藥等領域具備潛力，然而這項技術卻也衍伸出了風險，特別是在資訊安全領域，目前普遍的加密演算法有 RSA 與 ECC(Elliptic Curve Cryptography)等，分別是建立在大質數分解和離散對數問題上，而對量

子電腦來說卻很容易，一旦量子電腦具有足夠的量子位元，現有的加密技術恐將失去防護能力。



(圖二) Quantum computers and accelerated discovery

後量子時代的應對之法

隨著量子運算技術的快速發展，世界開始關注以密碼學為基礎的後量子密碼學(Post-Quantum Ctyptography, PQC)，PQC 指的是設計能夠抵禦量子電腦攻擊的加密演算法，其原理是避開量子電腦擅長處理的數學問題，使其無法發揮其優勢；目前美國國家標準與技術研究院 NIST(National Institute of Standards and Technology)已展開相關標準制定並公布數種候選演算法，其中格密碼學(Lattice-based Cryptography)被視為最具潛力之一。

參考資料

1. 科技大觀園:超乎想像的運算力：量子電腦時代來臨，幾件你需要知道的事 https://scitechvista.nat.gov.tw/Article/c000003/detail?ID=f059f6ab-a1be-4684-a1e8-b2d3ff72eed3
2. 國家實驗研究室:量子電腦的原理、挑戰與未來衝擊 https://www.niar.org.tw/xcscience/cont?xsmsid=0I148638629329404252&sid=0M103505917643100370&sq=%E9%87%8F%E5%AD%90%E9%9B%BB%E8%85%A6
3. 科學月刊:零與一之間的威力 量子電腦的原理 https://www.scimonth.com.tw/archives/5158
4. 量子開放學院:量子電腦的基本單元-不同的量子位元 Qubit https://qt.ntu.edu.tw/qoa/202204-qt-qubit/
5. 科技大觀園:【專家領進門】只有幾個國家做得出來?! 臺灣第一台 5 位元超導量子電腦 https://scitechvista.nat.gov.tw/Article/C000008/detail?ID=42b7f735-caaf-4cdb-a74c-21bdcfe8336b
6. 科技大觀園:【科普 3 分鐘】認識通訊的最強之盾「量子加密通訊」 https://scitechvista.nat.gov.tw/Article/C000008/detail?ID=1b639e9c-cab4-4a30-8e0b-

97a9a10b1f59
7. 科技大觀園:量子電腦問世後的密碼學主力戰場「後量子加密技術」
https://scitechvista.nat.gov.tw/Article/C000003/detail?ID=f9093947-6062-46d4-858a-3d16824edc95
8. NIST PQC
https://csrc.nist.gov/projects/post-quantum-cryptography
9. (圖一) 來自科技大觀園
https://scitechvista.nat.gov.tw/Article/c000003/detail?ID=f059f6ab-a1be-4684-a1e8-b2d3ff72eed3
10. (圖二) 來自 IBM
https://newsroom.ibm.com/media-quantum-innovation?keywords=quantum&l=100

註：

1. 未使用本競賽官網提供「科學文章表單」格式投稿，**將不予審查**。
2. 字數沒按照本競賽官網規定之限 500 字~1,500 字，**將不予審查。**
   PS.摘要、參考資料與圖表說明文字不計入。
3. 建議格式如下：
   - 中文字型：微軟正黑體；英文、阿拉伯數字字型：Times New Roman
   - 字體：12pt 為原則，若有需要，圖、表及附錄內的文字、數字得略小於 12pt，不得低於 10pt
   - 字體行距，以固定行高 20 點為原則
   - 表標題的排列方式為向表上方置中、對齊該表。圖標題的排列方式為向圖下方置中、對齊該圖