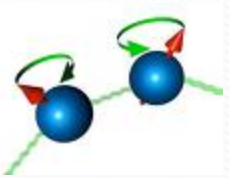
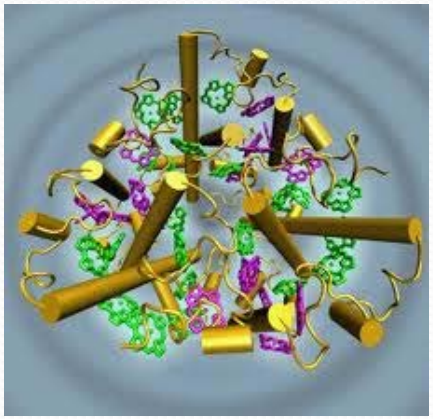
量子計算
神奇的數據處理方法

李志光 (Chi-Kwong Li)
The College of William and Mary
University of Hong Kong

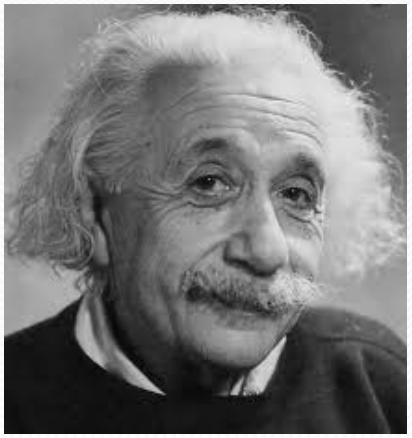
量子力學/理論是甚麼?

- 量子是能量的基本單位. (Planck, 1900).
- 輻射亦有相同現像. (Einstein, 1905).
- 量子理論發展成為瞭解微觀世界的工具. (Atomic, subatomic particle: 原子及亞原子粒子如質子, 中子, 電子等.)
- 近年更發現量子現像出現在其他系統如植物的光合作用過程之中.





量子理論的爭議



- God does not play dice.

Albert Einstein

- I think it is safe to say that no one understands Quantum Mechanics.

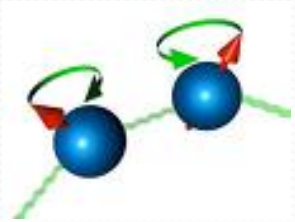
Richard Feynman

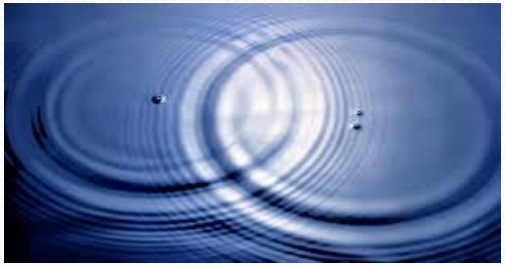
- Quantum mechanics is magic.

Daniel Greenberger

神奇的量子世界

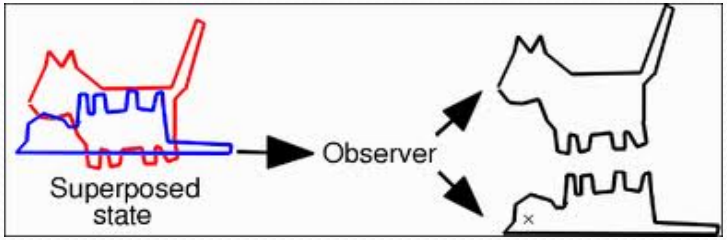
讓量子博士的解釋:



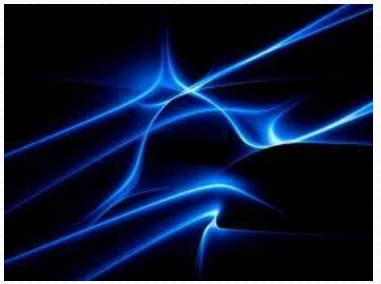


- 基本粒子有粒子和波的雙重性.

- 粒子運動遵從概率法則.



- 測量會影響/ 改變量子態.



- 量子態總會在疊加狀態. 且相互糾纏.
  Superposition and entanglement.

Movies and demonstrations:

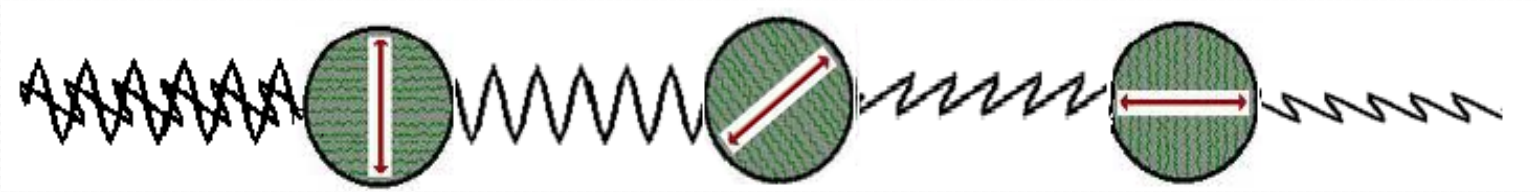
1. Two slit experiment explained by Dr. Quantum
   http://www.youtube.com/watch?v=DfPeprQ70Gc

2. Entanglement explained by Dr. Quantum
   http://www.youtube.com/watch?v=Jh8uZUzuRhk&feature=related

3. Demonstration of interference using green laser pointer, and photon states using polarization filters.

光子(photon)

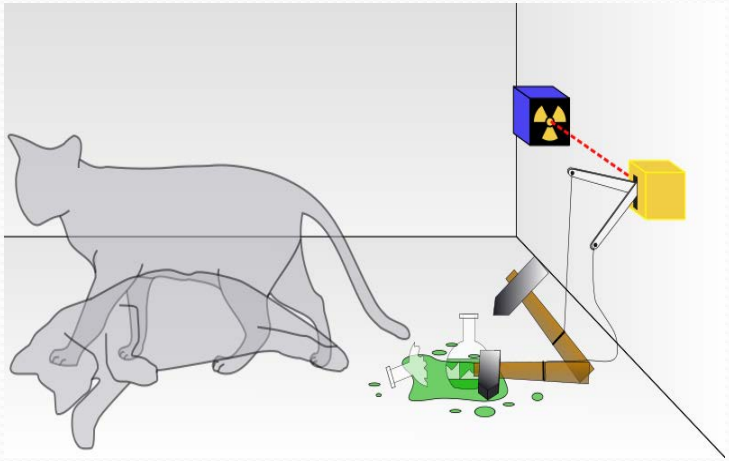
垂直/ 平行　　垂直　　黑暗



垂直/ 平行　　垂直　(測量)　45°　　平行

Schrodinger's cat (薛丁格之貓)

- 在日常生活中, 貓祇有生和死兩種 狀態.
- 若放一隻小貓在一密封箱中, 裡面的裝置在特定時限內,有一半機會放出毒氣.
- 在時限過後, 打開箱子, 理應有一半機會看到生/死貓.
- 但如果小貓在量子世界裡面...



- 儘管量子世界有很多神奇之處, 為何要考慮量子計算?

- 讓我們先看看現代的計算方法和限制.

- Alan Turing (1912-1954) 於 1936 年提出 Turing machine 的概念引發了電子計算機 (電腦)的誕生.

$$0 \vee 0 = 0$$
$$0 \vee 1 = 1$$
$$1 \vee 0 = 1$$
$$1 \vee 1 = 1$$

- 用 Boolean 代數法則處理 0,1 數列. 作二進制的高速計算.

- 改進了圖像與文書處理、資料儲存與搜尋、訊息傳遞的效率、保密和精確度.

信息／資訊科學迅速發展

- Computing - 計算.
  (數據的儲存和處理.)

- Communication - 資訊交流.

- Complexity - 複雜性.
  - 計算程序的複雜性.
    (Polynomial /exponential time.)
  - 信息的重要和精確性.
    (Shannon entropy.)

電腦的改進和限制

- 用平行(並行) 計算提高效率.

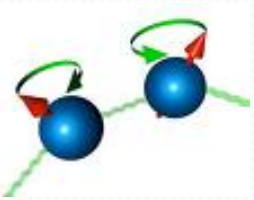
- 改進計算機的精密度. (Moore's Law.)
  晶體管上面的集成電路約於每兩年增加一倍.
  (The number of transistors on an integrated circuit doubles approximately every two years.)

- 長此下去,無可避免地會出現量子效應.

- Feynman (1982) 指出傳統電腦不能處理量子系統. 簡單的量子系統或可加速計算和模擬複雜的系統.
- Benioff 於 1981 亦提議發展量子計算.
- 九十年代, 有很多理論上的突破.
- 2000 年以後, 理論 和實驗都有飛躍的進展.

量子系統的複雜性

- 設有一簡單的量子系統, 每一量子態祇有兩種可測量態.



$$|\uparrow\rangle \qquad |\downarrow\rangle$$

- 每一疊加量子態可以表示為二階向量:

$$|\psi\rangle = a\,|\uparrow\rangle + b\,|\downarrow\rangle = \begin{pmatrix} a \\ b \end{pmatrix}, \qquad |a|^2 + |b|^2 = 1.$$

a, b 為複數; |a|, |b| 為複數的絕對值.

- 若有兩個這樣的量子態組成一量子系統,
  則其可測量態及糾纏態可以表示為:

$$|\uparrow\uparrow\rangle, \quad |\uparrow\downarrow\rangle, \quad |\downarrow\uparrow\rangle, \quad |\downarrow\downarrow\rangle,$$

- 其糾纏態可以表示為:

$$|\psi\rangle = a\,|\uparrow\uparrow\rangle + b\,|\uparrow\downarrow\rangle + c\,|\downarrow\uparrow\rangle + d\,|\downarrow\downarrow\rangle = \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1.$$

- 若有 100 個這樣的態子態組成一量子系統. 則有 2^{100} 可測量態, 需要用 2^{100} 維的向量來表示量子態.

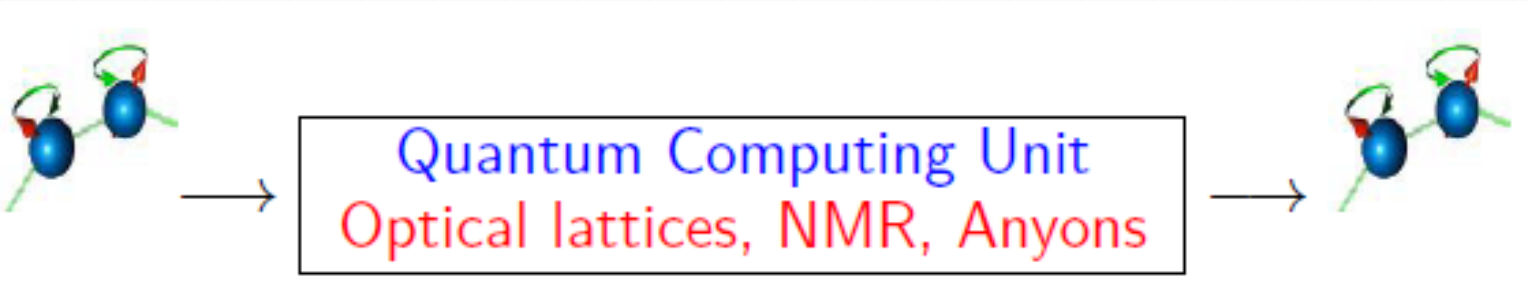
$$|\psi\rangle = a_1 \left|\uparrow\cdots\uparrow\right\rangle + \cdots + a_{2^{100}} \left|\downarrow\cdots\downarrow\right\rangle, \qquad |a_1|^2 + \cdots + |a_{2^{100}}|^2 = 1.$$

- 如果電腦能以每秒處理 10^{15} 個數據. 檢測/模擬一個量子態需時:

$2^{100}/(10^{15}\text{x}60\text{x}60\text{x}24\text{x}365) > 40,000,000$ 年 ！

(四千萬)

量子計算的基本原理



- 先預備好一堆糾纏的量子態.
- 讓它經過一特定的環境中按量子法則自由轉化.
- 小心選擇測量方法, 取出有用資料.

量子計算的數學方法

1. 把多個量子態纏結 得出纏結量子態:

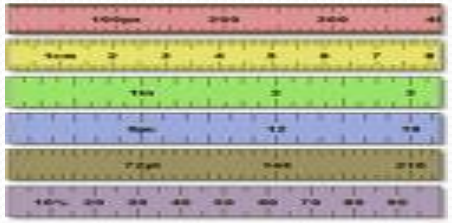
$$|x\rangle = \frac{1}{\sqrt{2^n}}\{|\uparrow\cdots\uparrow\rangle + \cdots + |\downarrow\cdots\downarrow\rangle\}$$

2. 作一次性的 運算.

$$f(|x\rangle) = \frac{1}{\sqrt{2^n}}\{f(|\uparrow\cdots\uparrow\rangle) + \cdots + f(|\downarrow\cdots\downarrow\rangle)\}$$

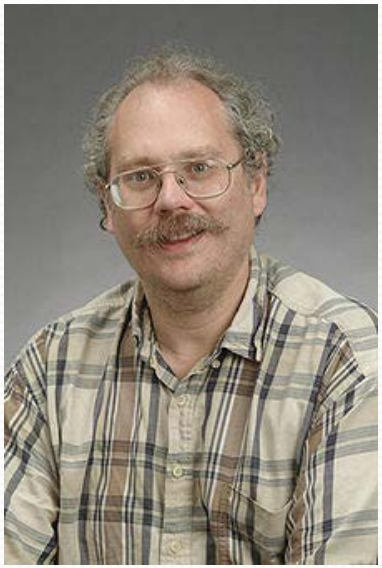
3. 重組纏結量子態的概率分佈. 作出適當的測量.

$$R \circ f(|x\rangle) = |y\rangle|z\rangle \longrightarrow |z\rangle$$



- Peter Shor 於 1994 年設計一個 效率為 $O((\log N)^3)$ 的量子程式分解 N = pq 的因子.

  (N = 1,000,000, $(\log N)^3 = 6^3 = 216$.)



- 14 = 2 x 7, 15 = 3 x 5 , 749 = 7 x 107.

- 如果: N = 89020836818747907956831989272091600303613
  26460379424703263764762563155496163835 1,
  p = 92810132054041315184759024472769733389 69,
  q = 95917153492371949995470500687189305142 79.

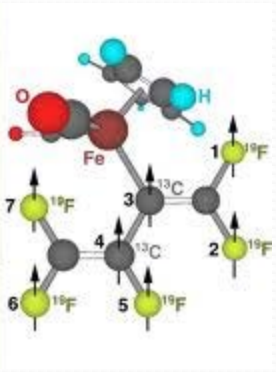
- 傳統電腦最佳的效率為: $O\left(e^{(\log N)^{1/3}(\log\log N)^{2/3}}\right)$

- 這對 被廣泛應用的RSA (Rivest, Shamir , Adleman) 密碼系統做成威脅.

1. 用3233 = 53 x 61 處理(傳送) 52 x 60 = 3120 以下的正整數.
2. 選取 e = 17, d = 2753.
3. 公開 (3233, 17), 私人解碼鑰匙 (3233, 2753).
4. Alice要傳遞 m = 0065 給朋友 Bob.
5. 先把它改成 $c = 65^{17} = 3233\ r + 2790 = 2790 \pmod{3233}$.
6. Bob 計算 $m = 2790^{2753} = 3233\ s + 65 = 0065 \pmod{3233}$.

- 問題是:若知道 3233 = 53 x 61 和 17, 則很容易算出 2753.

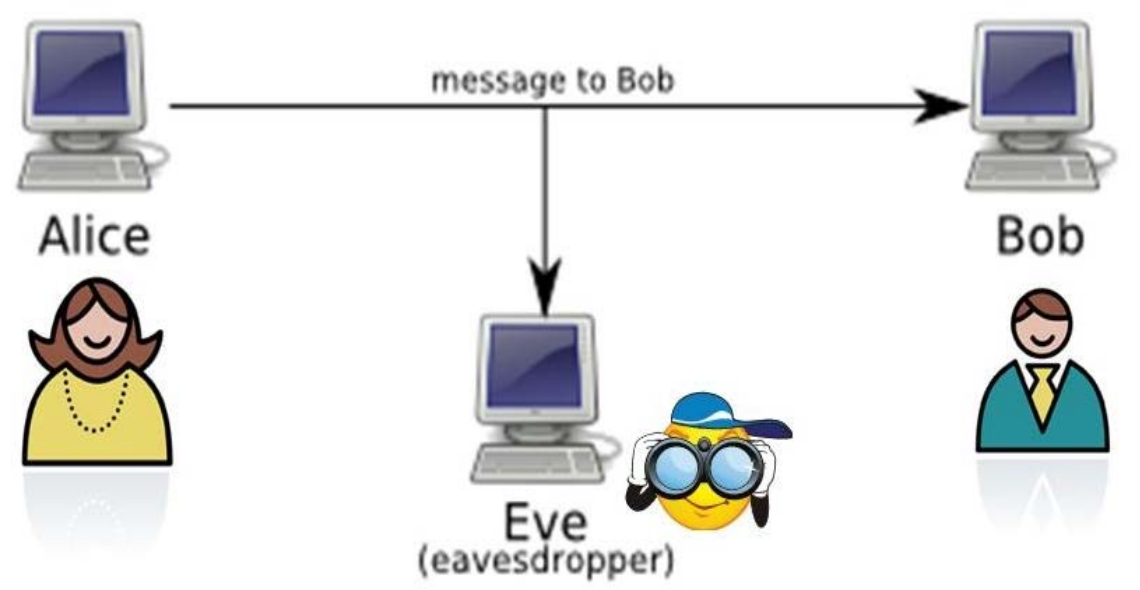
- IBM 於2001 年用NMR 的量子計算機驗証了Shor 的方法可以分解 15 為 3 x 5.



- 一旦實用的量子計算機面世, 對現代人的生活會做成很大的影響.

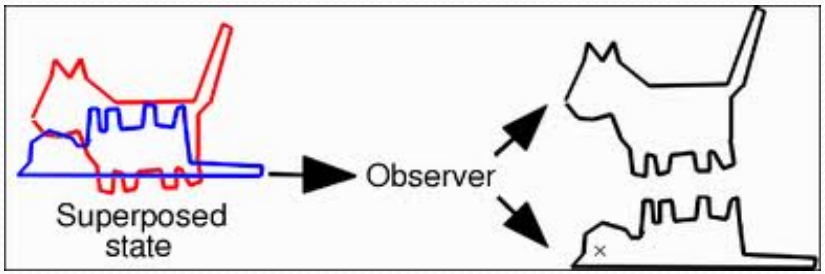
信息傳遞

- 重點在於精確,保密和效率.



量子方法對保密方面的優點

- 測量會影響/ 改變量子態.
- 量子系統不能複制.
  (No cloning theorem.)



BB84 Protocol

Charles Bannett 和 Gilles Brassard 提出BB84 Protocol 的傳遞密件方案.

- 通常這方法會用來傳近私人保密鑰匙.

例如: 要送出 2753, 可以把它化成二進位數 101011000001

$(2^{11}+2^{9}+2^{7}+2^{6}+1 = 2753.)$

1. Alice 和 Bob 各人用兩種不同的量子系統 送出 和接收 4N 個 0, 1 信號.

2. 約有 2N 個用同樣系統. 得到有用訊息.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

3. 測試其中 N 個信號. 判定有沒有人竊聽.

4. 確定之後, 用餘下的 N 個信號作解碼用途.

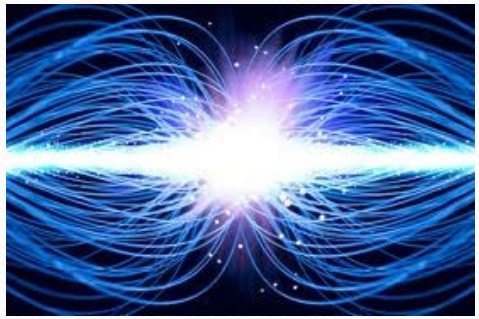
其他量子信息處理方法

- 量子傳輸 (Teleportation)

  http://www.youtube.com/watch?v=_qmSdC7aQpY

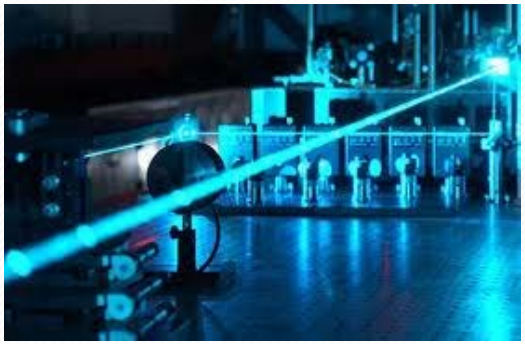
- 超密編碼 (Super Dense Coding)

- 量子糾錯 (Quantum Error Correction)
  對抗量子態跟周圍環境交互作用產生的消相干(Decoherence) 效應.



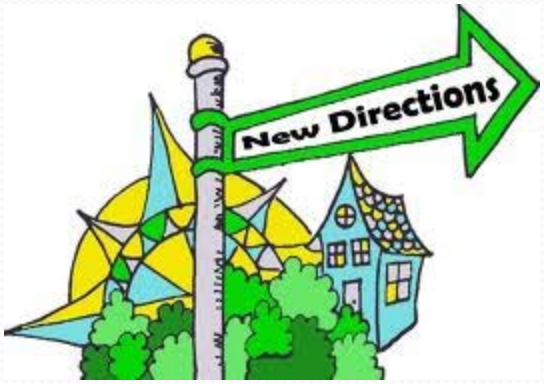
量子計算研究的現狀

- 量子傳訊已經被應用.

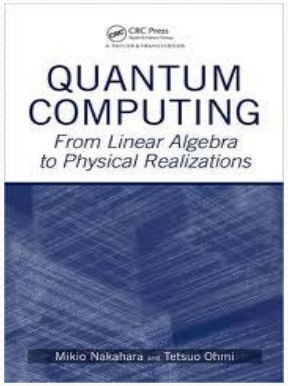


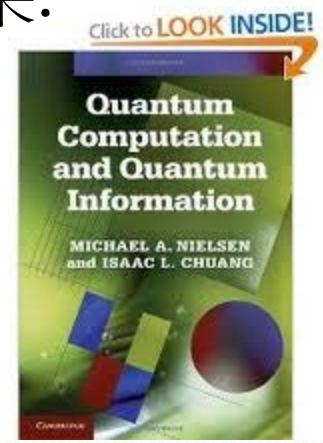
- 量子方法可以大大減低計算問題的複雜性.

- 怎樣把問題的複雜性分類？
- 怎樣設計高效率的量子計算程序?
- 如何製造實用的量子計算機?
- 都是活躍的研究題目.
- 刺激很多新的研究方向.



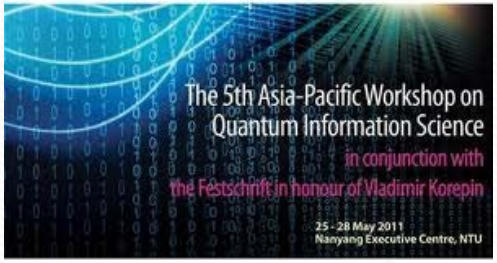
- 這些活動導致很多實驗成果.



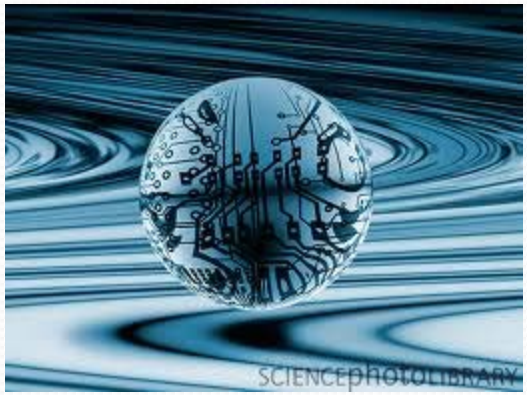


- 學術論文和書本.

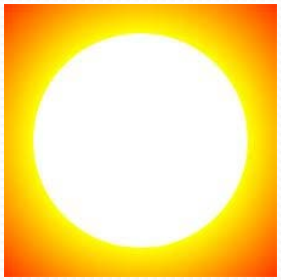
- 學術會議.



- 量子計算的理論和實踐, 需要大量的投資.
- 很多國家和私人機構都朝這個方向進發.
  Canada, China, Germany, UK, USA, IBM, Microsoft, ...
- 希望很快有重大突破, 實用的量子計算機可以面世!



量子計算的哲理



- 自然界蘊藏無窮的資源和變化, 人力不容易全面控制.

- 若能順應和善用自然規律, 則可以做出強力的(計算)工具.

- 所以「格物致知」是十分重要的!

結語

- 有人相信量子計算的前途無限.

- 有人對量子計算抱著保留的態度.

- 無論如何, 量子計算的研究, 凝聚了很多不同 領域學者的力量, 讓他們 以開明的態度, 獨立的研究精神,追逐共同的夢想, 已經是「功德無量」了!
  (應該說「功德有量」!)

Bright Futures

More Quantum Mechanics Quotes

- Those who are not shocked when they first come across quantum theory cannot possibly have understood it**.**

  Niels Bohr.

- Everything we call real is made of things that cannot be regarded as real. **Niels Bohr.**
- Quantum mechanics makes absolutely no sense.

  Roger Penrose.

- If you are not completely confused by quantum mechanics, you do not understand it. **John Wheeler.**