【基礎科研】再談Google的量子霸權

2019-10-29 09:23:00

原文网址：http://blog.udn.com/MengyuanWang/130416352

上周應《觀察者網》的邀請，針對Google在十月23日正式發表的“量子霸權”論文寫了一篇評論。我基本上是基於上月寫的《Google的量子霸權是怎麼回事》一文，加入了新公開的技術細節，重新修飾整理，所以這篇新文章並不是後續或補充，而是早先文章的增訂版。

《觀察者網》最近稿子多，所以一直到今天（十月28日）才刊出，參見http://www.guancha.cn/wangmengyuan/2019_10_29_523101.shtml。

==========

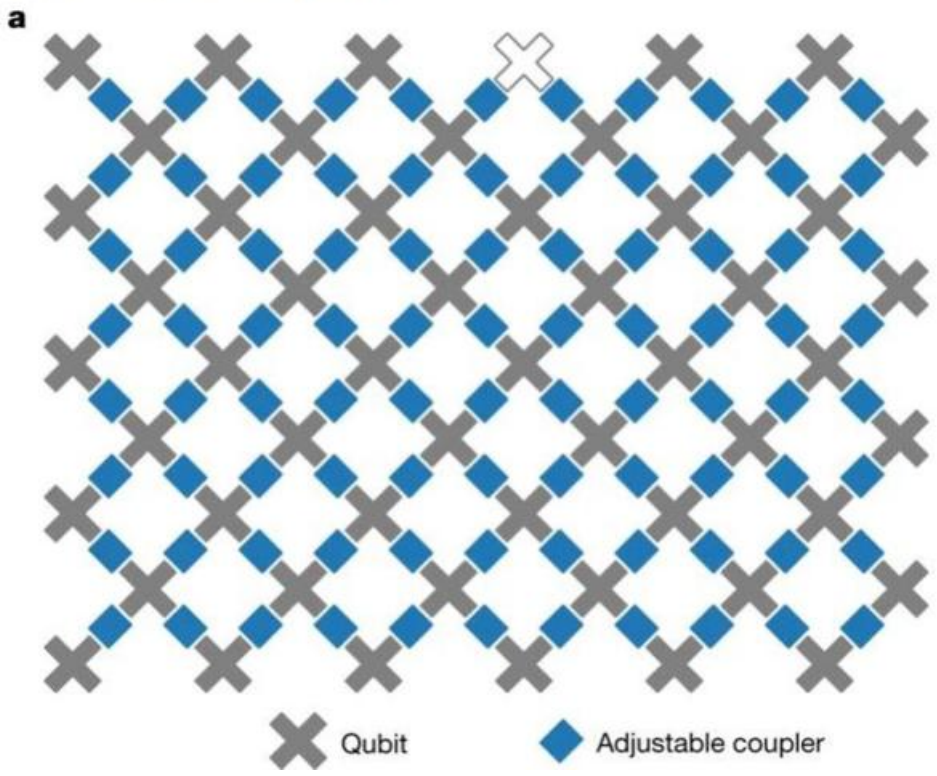
上個月，NASA大意提前泄露了Google的量子霸權論文，因爲違反了Google公關部門的計劃，所以很快就撤下。其後，Google遵循典型的商業炒作方案，始終三緘其口，一直到2019年十月23日，論文正式在《Nature》發表（參見https://www.nature.com/articles/s41586-019-1666-5），伴隨著各式各樣的公關吹噓，鋪天蓋地而來。

有趣的是，與其同時，IBM在官方博客公然唱反調，發表了一篇自己的論文稿，宣稱已經證明Google並沒有達到量子霸權。那麼到底誰是誰非呢？

首先，我們先回顧一下什麼是“量子霸權”；它指的是量子計算機在某個有實用價值的程序上能比現有的古典電腦高效許多。請注意，一般人往往忘記這個定義中要求有實用價值的那部分，所以我一開始就疑心Google團隊鑽的是這個漏洞，而且已經寫過一篇文章來推測其中的奧秘（參見前文《Google的量子霸權是怎麼回事？》）。現在因爲有了更詳細的消息，我可以更精確地解釋Google的這篇論文，希望讓理工科出身的讀者都能理解。

下面是Google所用的Sycamore（梧桐；名字純屬巧合，不要亂做聯想）量子處理器的示意圖；其中灰色的叉叉是個別量子位元，藍色的長方塊是耦合器，共有88個，它們負責將兩個相鄰的位元轉化為糾纏態。原本應該有54個量子位元，但是其中一個失效無法修復（白色叉叉），所以整個實驗只能用上53個位元；有效的耦合器也因而減少了兩個，剩下86個。

Fig. 1: The Sycamore processor.



Google所做的程序是先從86個耦合器和53個位元中隨機選出部分，被選中的會被開啓而發生作用，叫做閘門（Gate）。位元的閘門（Single-Qubit Gate）作用是產生對應著隨機古典結果的量子態；耦合器的閘門（Two-Qubit Gate）作用則是將相鄰的位元糾纏起來。這些作用合起來，形成一個循環（Cycle）；全部總共有20多個循環被事先隨機確定，它們一起組成一個綫路（Circuit）。Google在實驗中所用的最複雜綫路，包含了1113個單位元閘門和430個雙位元閘門。

接下去是重複以下的這個程序圈子（Loop）：首先把所有的位元清零；接著讓事先選定的固定綫路發生作用，製造出新的量子態；然後全部位元進行塌縮，以便形成古典的0或1讀出。所以結果是一個看似隨機的53位元序列，但是內含量子糾纏，所以位元之間並非真正的統計獨立，而是有由量子糾纏來決定的複雜相關性（Correlation）。

經過小規模的試用之後，最終Google團隊用全部53個量子位元跑這個程序圈子3千萬次，這一共費時200秒。Google估計最新的古典超級電腦也要耗時10000年，所以可以自誇量子霸權。

IBM出來潑冷水的研究，是采用了更高效的古典超級電腦設置，結果只用了兩天半，大約比Google團隊的估計快了八個數量級，所以並非沒有意義的。

然而這個古典程序的運行時間（Runtime），可以在數學上證明是與2^n成正比，這裏n是量子位元的數目，亦即Google實驗中的53。所以即使在n=53的條件下古典電腦還可以一搏，到n=90左右的時候，也會重現量子霸權。這大概也就是三四年的研發時間。

IBM的算法（Algorithm）仍然是以蠻力（Brute Force）為主，如果未來發明了更巧妙的算法，可能會讓古典程序又再增速幾個數量級，不過這頂多是把門檻擡高到n=200。換句話說，最多最多也就是延遲Google的量子霸權十年左右罷了。

那麽我們的結論是量子霸權在2030年之前必然會發生嗎？不是的，Google這篇論文的真正問題，不在這些細節上，而在於整體設計，也就是我在本文開頭所提的，程序的實用價值。

要比較兩個不同工程方案的優劣，一個很重要的隱性前提是要達成同樣的、有實用價值的目標。Google的公關文稿，把他們的這個“成就”和100多年前Wright Brothers的首次飛行相比，就是故

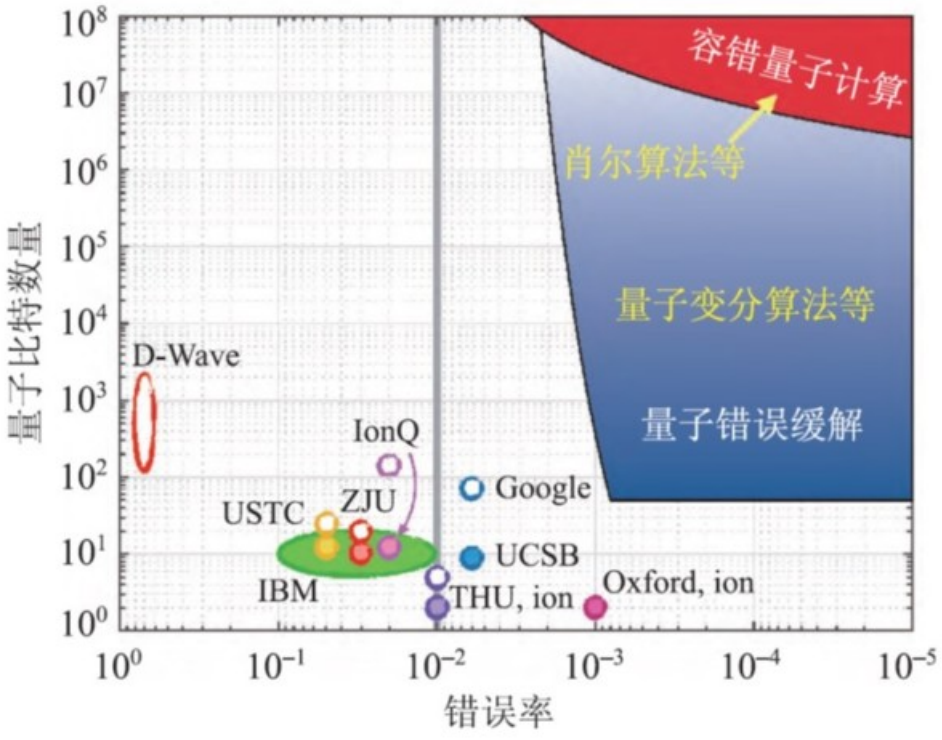
意混肴視聽：Wright Brothers的飛機是圍繞著一個歷史長久、公認有價值的目標（亦即動力飛行）而設計製造的成品；Google的Sycamore卻執行了一個一點用處都沒有的程序。真正類似的，是建造出一個複雜而沒有實用性的機器，然後說它在產生獨特的噪音上，有無可比擬的效率。換句話說，他們是先射箭、再畫靶，Sycamore自己隨便動一動，然後叫古典電腦來做模擬；如果這樣也算量子霸權，那麼隨便找一個有53個原子的系統，要求古典電腦來模擬它歷時200秒的演變，同樣也會需要萬年以上。

事實上，Google的這個結果，比毫無實用價值還要糟糕。要理解這一點，我們先回顧一下當前量子計算界的處境。現在的世界記錄是大約100個量子位元（DWave的量子計算機是假的）；但是這些位元很不穩定，非常容易與周圍的巨觀環境起作用而喪失量子態，這是我以前詳細討論過的量子退相干過程（Quantum Decoherence）。要知道計算的輸出（Output）是程序邏輯的結果，而不是量子噪音的後果，就必須有糾錯機制。

目前人類所知的量子糾錯機制，必須用上80-10000個原始的量子位元，才能產生1個穩定可靠的位元（叫做邏輯位元，Logical Bit）。世界記錄是連1個邏輯位元都沒有的。

Google的這個“突破”，第一個巧妙之處在於用的是內生的（Endogenous）隨機量子態，而不是事先指定的（亦即Exogenous，外源性的）串列。雖然Google團隊可以試圖去影響這些原始量子位元之間的糾纏，實際上是否成功，並不能絕對精確地驗證。換句話說，他們根本沒有解決糾錯的基本難關，而只估計出Sycamore保持量子態的半衰期大約是10微秒，那麼因爲每一輪程序圈子費時不到7微秒（=200秒/30000000輪），大部分時候量子退相干還沒有發生。然後又再巧妙地只考慮統計結果，那麼少部分的噪音就可以遮蓋住了。

這裏最基本的毛病，在於Google的量子計算機並無法自行保證結果是正確的，事實上我們知道它不可能是絕對正確的，頂多只能是近似正確。相對的，古典電腦給出的結果卻是絕對精確可靠的。這時硬要比較兩者所費的時間，顯然不是公平的。



其實要有丁點實用價值的量子計算，至少也必須達到上圖（来自孙昌璞院士等作者的论文）的藍色區域。目前量子計算被吹捧並獲得各國政府極度重視的真正原因，是能夠破解通信上的公開碼，那麼就必須達到上圖中的紅色區域。Google的量子計算機雖然算是先進，但距離實用目標還有至少九個數量級之遙；現在就宣稱勝利，純屬忽悠大衆的商業宣傳。

【後註】Google量子計算機團隊負責硬件的主管John Martinis上周忽然宣佈離職，昨天（2020年四月30日）《Forbes》登出對他的采訪（參見https://www.forbes.com/sites/moorinsights/2020/04/30/googles-top-quantum-scientist-explains-in-detail-why-he-resigned/#6afdfb986983），內容是標準的八股，不過有一個有趣的細節，可能解釋這位Martinis教授真正被排斥的原因：他說他堅決要求整個團隊投入量子霸權項目，受到多數研究人員的反對。嗯...Google量子計算機的團隊成員反對搞這個項目，我不知道是否與它是假大空有關...

---

7 条留言

4a3c6572 2019-11-01 09:50:00

很多科學家相信未來人工智慧能超越真實人類智慧，所謂超越真實人類智慧是指比真實人類更能理解人性愛恨情欲個性自尊，我常懷疑這點是否已違反了最基本的常識邏輯，正如同量子力學相信時間能倒流一樣違反了祖父悖論此種最基本的常識邏輯，量子電腦離不開量子力學理論，依據量子力學相信時間能倒流的邏輯可以導出量子電腦能促使未來人工智慧超越真實人類智慧的結論，如果量子電腦能超越真實人類智慧，那就等同於人類能創造出高於自己智慧(不是智商而是理解人性)的產物，而且這產物還是沒有生命的無生物，沒有生命的無生物比真實人類更理解人性的前提應是它比人類大腦更複雜，人類能創造出比自己大腦(再強調不是智商而是理解人性)更複雜的東西合乎最基本的常識邏輯嗎？如果量子力學相信時間能倒流的理論不成立，量子電腦還能超越人類大腦嗎？

> 我無法斷言在長遠的未來，人工智能是否會超越人類智力水平的上限，這是因爲目前根本沒有足夠的事實來做推斷。然而正因如此，我可以明確地告訴你，任何一個下斷言的人都是在胡扯；你所看到的那些對量子計算機做無限聯想的，連量子計算機的細節都不懂，邏輯亂七八糟，我們沒有必要去理他們。 當然，這些人正在主動拉低人類智力水平的下限，所以人工智能超越他們是必然的，至少電腦不會故意去胡扯。

無知者，無畏 2019-11-01 18:57:00

到底什麼應用需要用到量子計算？ 王兄的上一篇文章就沒有看得太明白這一篇出來以後，大致明白了。 古典計算機的運行機制是LPS(load-process-save)，即「載入->處理->存放」機制。不管CPU做得多麼複雜，也都是在執行這個邏輯，其中其實最核心的是ALU（算術邏輯單元），現實應用計算中的各種實際需求，比如加減乘除和邏輯判斷等，都是根據不同的算法（Algorithm）固化在電子電路中，也就是說由具體的電子電路來完成，CPU中的ALU完成這些具體的處理時間非常短，實際上大量的時間是消耗在算元「載入」和處理結果「存放」這兩個步驟上，因為這兩個過程需要訪問寄存器（Registers）或內存(RAM)，片面加快CPU中的ALU實際效果到底有多大？就算快到飛起的量子ALU又能怎麼樣？此其一。 其二，正如王兄所說，google的這個例子有何意義？現實世界中要用到超算的應用，主要是： 1.天量數據庫的訪問， 2.基本粒子（源自內部的基本粒子）間的相互作用， 3.定量空間內分子級別熱力學和空氣動力學計算， 4.海量的3D圖形rendering，模型，氣象，海象等。 5.化學和分子生物學方面的分子級別解算 如果新的量子計算不能在這些方面幫忙？用它來做什麼？ 目前已知的古典計算機的發展方向是，類神經元處理機制的處理器（nPU）和有助於AI應用的專用處理器。其中神經元處理器，實際上是仿人類大腦的處理的分任務處理器，這個方向最有前途，也會最先取得突破。所謂AI的專用處理器，需要依據高速的天量數據訪問和猜測學習，各行各業的需求都不一樣，非常難形成一個通用處理器，但是在某些特定方面取得進展是有可能的。 但是所有的這些新的方向，並沒有改變計算機的LPS機制。請恕我才疏學淺，我實在是想像不到這個量子計算機將用什麼方式來取代古典計算機而發生革命性的改變？？否則，意義何在？？

> 是的，即使在最樂觀的假設下，量子計算機頂多只是輔助古典電腦，在少數幾個特定領域有優勢。 實際上，我覺得很可能只有破解公開碼這種數論上的問題才會有效益，但是還距

> 離九個數量級，這說不定永遠做不到，就算做得到，也很可能是50年之後了，現在拼命圈錢實在沒有意義（除了為圈錢大師們收集退休金）。

無知者，無畏 2019-11-02 05:12:00

可能的應用領域 可能的應用領域，誠如王兄所說，如果用來破解公開碼（所謂解密鑰）可能會是一個應用領域。 在數字通訊的加解密領域，不管是DES,SHA,MD5,RSA,DSA,還是AES，都有固定的加/解密算法，量子計算可能唯一有優勢的方向，就是根據這些特定的解密算法設計出固定的量子routing來高速解密。可是老問題還在，不管你多快的量子ALU，你還是需要大量的時間來訪問寄存器或內存，更有甚者，你絕大部分時間其實是耗在等待通訊通道的響應。而且這還是你已經解決了真正實現了物化量子處理單元的條件下，也就是說，你已經把量子處理器做出來了，而且可以可靠使用。 量子處理器的另外一個可能的應用，是礦機，也就是說，可能可以用在高速解算bit幣的專用處理器上，因為bit幣的解算是固定算法，有可能為此設計出專用的量子routing。 我這裡多說幾句礦機（為解算bit幣而設計的專用計算機，號稱礦機），如果把bit幣的解算看成是挖礦，那麼現在的bit幣的挖取幾乎到了極貧礦，數十數百台專用挖礦機，數月也未必可以挖一枚bit幣。近幾年，大量的挖礦（bit幣）公司因為付不出礦機運行的電費而破產，礦機被當成廢鐵賣掉。 礦機的處境其實跟加解密一樣，確認挖礦是否成功的服務端，要應答每秒數十億的挖礦客戶機（挖礦機）結果查詢，極大地耗費了寶貴的網際通訊資源，挖礦機的絕大部分時間其實都是在等待服務端的答覆響應。 就算是上述兩個可能的應用領域，量子計算也未必就一定比古典計算機高明多少，對吧？而且加解密這個領域，一旦全面進入量子通訊，就變得不可為了，礦機應用，大家都破產了，誰來做這個？我還真想不到！

> 有關BitCoin挖礦的評論我同意，但是你確定量子計算機解密須要消耗大部分時間“等待通訊通道的響應”嗎？這和我既有的理解不同，不過我不是這方面的專家。

無知者，無畏 2019-11-04 07:07:00

CPU的運行時效成本 喔，好，先說說的學術背景。我在大學專門修讀過（師從：John G. Cleary 教授）《計算機架構》這門課，這是大學四年級的課程，每屆學生不超過10人，我是1999年選讀的，John說，多年來，第一次有中國人選這門課，因為這門課非常不容易通過考試。我那年獲得了他的年度最佳程序片段獎，不過獎品是三條巧克力fish。 這門課重點是講解計算機CPU的內部機制，包括ALU的算法設計及實施，CPU對外設的訪問機制，等待機制，鎖定機制，指令對列等非常底層的邏輯和技術。 我這裡重點回應王兄有關CPU等待數據通訊響應問題。 由於CPU中ALU的底層實現都是具體的電路（不同算法所對應的晶體管及與非門陣列），所以CPU在執行指令上消耗的時間極短（跟CPU的內部時鐘頻率相關），不同的指令，所消耗的時長差異巨大，比如一個算元平移（整數加減運算），只需一個時鐘循環，但是一個浮點除法，則需要10-40個時鐘循環（很多線路內循環），很多複雜的指令（比如Intel的CISC指令集中的一些指令），則需耗時超過150個時鐘循環。 訪問寄存器（Register）大致在一個時鐘循環，但是訪問緩存（Cache）一二三級（L1,L2,L3）則耗時3-70個時鐘循環，如果需要通過總線（BUS）訪問主內存（Main RAM），則需要耗時100-150個時鐘循環。 訪問數據接口（socket）則需要100-300個時鐘循環，而這僅僅是通訊端口到達，也就是說，從CPU touch到通訊端口，就需要這麼多時長。如果再加上本地數據接口到遠程（Remote）數據接口，再等待對方發送response回來，通常耗時10的三次方到六次方量級個時長（這是對方計算機立刻就回覆的理想狀態），但是通常對方遠程計算機都要等待處理，也就是說，對方在服務遠程請求的時候，是實行隊列管理，你的請求被Put in queue,請耐心等待。 你或許有打電話給電話公司查詢的經驗，你的電話接入以後，你可能需要花半個小時等待對方CRM員工處理排在你前面的打入電話，計算機遠程服務的機制，跟這個一模一樣。 所以我說，遠程應用的計算機，“絕大部分時間其實是耗在等待通訊通道的響應”。就是這個意思。 總體來說，從計算機運行機制來看，計算機的性能瓶頸根本就不在CPU的先進程度，時鐘，邏輯上面，而是在通訊上面。中國的超算能夠迅速地進入全球頂級超算行列，一個最主要的成就，就是他們突破了計算機遠程通訊的瓶頸，讓CPU可以更加快速地訪問主內存和網絡設備。這跟中國的文化和文明有關，中國人就算小屁孩都知道“要想富，先修路！”這個道理。這裡所謂「路」就是「骨干通訊網絡」，隨著中國5G的部署加快，中國區域間的骨干網絡的更新也在加快，這才是未來奪取計算機遠程應用和人工智能的那條「路」。 注：時長，clock cycle,也稱「時鐘循環」。

> 古典電腦的架構，我也略有涉獵，所以計算核心常常等Data我是知道的。 我不確定的，是量子計算機在破解公開碼的例子，也會有同樣的問題嗎？我猜測未來這型量子計算機的設計，不會是像現有古典電腦的通用計算格局，而是針對一個程序從底到上來設計建構，那麼這種瓶頸可能是從一開始就必須重點消除的對象。

無知者，無畏 2019-11-04 14:21:00

深挖量子計算機 此文純屬跟王兄商榷。如果可能，請王兄賜教！ 從前面兩篇有關古典計算機中的核心部分之討論，我們知道CPU之ALU(算術邏輯單元)由根據不同算術邏輯的實際需求，配合相關算法而通過電子線路集群來完成ALU之處理任務這架構中，我們知道，非常神秘的ALU實際上就是一群有不同輸入/輸出端的，由二三極管和與/非門陣列所組成的電子電路集群。完成這個工作的核心媒體，是電子，也就是說，是一個電子技術的實際應用。 再往下想一步，如果未來是量子計算機，那麼將會使用量子作為媒體來完成這個任務。我們假定，取代電子線路出現在未來量子計算機中的，將是量子Routing，亦即，由量子routing來替代電子線路。 那麼我的問題是，有沒有人真正明白量子和量子routing?就算真的能夠做出來，做出來以後，會是多大？會不會整棟樓都裝不下一個簡單的ALU單元？ 另，據我所知，量子不像電子，會無緣無故消失。量子的產生，捕獲和控制都非常困難，在人類對量子的了解如此之少的情況下，大勢鼓吹，意義何在？

> 我想我們已經扯得太遠了。正文中提過，量子計算機距離實用，還有八九個數量級；回顧古典CPU的發展歷史，1970年的第一代微處理器4004到現在剛好也是進步了八九個數量級。我們討論未來量子計算機的技術細節，就好像在1970年考慮EUV光刻一樣，純屬空談。

schrodingjier‘s cat 2019-11-06 03:00:00

Google的宣传，特别是ceo的言论，确实有很重的商业吹嘘的成分，上篇文章的回复里我就这么说过。不过quantum supremacy本身只是说能比classical computer更快的解决问题，是没有规定问题本身有意义或者实用价值。在这一点上我对文中要求有实用价值的观点表示异议。 论文本身我上周末看了一遍，内容丰富论证严谨，没有受到商业吹嘘的影响，读起来还是很畅快的。反倒是IBM的反击有些乏力，即使按照ibm的结论，只需要数天而不是若干年的计算就能得到结果，quantum supremacy仍然成立，无非是吹嘘起来没有那么impressive。 另外关于量子计算的application的问题，我觉得科技发展的规律普遍是技术和需求往往互相促进，现在空谈量子计算无应用是站不住脚的。 现有所有的所谓量子计算机都还是量子模拟器，在达成通用量子计算机之前还有很远的路要走，个人觉得如何有效操作量子态的问题会是最大障碍。但在此之前能够模拟某些特定系统的specialized quantum simulator还是可能有实用价值的，希望这能早日实现。

> 我的正文已經說得很清楚了，做工程比較必須是有用的目的。這不是任何人能主觀選擇的事，否則可以簡單要求古典電腦來模擬自己系統的自然演化，那麼如果照你所說的邏輯，世界早就有無數的量子系統是古典電腦無法在萬年內精確仿真出來的，這個定義下的“量子霸權”在宇宙誕生就已經達到了，哪還輪得到Google。 正文已經講清楚的事，你還來胡扯，嚴重警告一次。

4a3c6572 2019-11-06 14:34:00

版主王孟源給我、5樓的“無知者，無畏”、schrodingjier‘s cat的回應「你所看到的那些對量子計算機做無限聯想的，連量子計算機的細節都不懂」、「我們討論未來量子計算機的技術細節，就好像在1970年考慮EUV光刻一樣，純屬空談」、「那麼如果照你所說的邏輯，世界早就有無數的量子系統是古典電腦無法在萬年內精確仿真出來的，這個定義下的“量子霸權”在宇宙誕生就已經達到了」這三句話，可以總而言之變成一個問題：科技發展是有極限或無窮無盡？很多科學家將科學當成全能上帝當然相信科技發展進步一定是無窮無盡，科技進步無窮無盡的願望潛意識讓這些科學家無視於祖父悖論等最基本的常識邏輯，所以愛因斯坦相對論才會被某些人推導出時間能倒流以及平行宇宙的結論，只要時間能倒流就能回到宇宙大霹靂去改變物理定律進而創造出一個等同於人間天堂的平行宇宙，與其說這些科學家胡扯倒不如說他們反映了人性弱點，他們如同西遊記當中想吃唐僧肉的妖怪一樣期待長生不老，或許他們不應該將科學當成全能上帝而應去信奉真正的宗教。如果科技進步真能無窮無盡，推翻祖父悖論實現時間倒流即使一萬年做不到也可等到一百萬年後再實現，實現時間倒流創造出同於人間天堂的平行宇宙不過是時間遲早的問題，人類總有一天不必吃唐僧肉也能長生不老，不必信上帝也能進天堂，創造出平行宇宙天堂的長生不老人類就是上帝，平行宇宙天堂的長生不老人類可以靠著時間倒流如同上帝一樣向廿一世紀的無知人類顯靈，以上所述是否胡扯？若是胡扯，科技進步就是有極限，也代表量子電腦在理解人性上無法超越真實人類。

> 我對兩三百年之後的事，無法置喙，但是在可見的未來幾代人生命中，除非發生如全面核戰之類毀滅人類經濟和文明的大災難，整體科技的不斷進步是必然的。 一般常見的誤解，是把整體的進步，誤認為個別專業的永恆發展。其實每一個領域都有極限，一旦低垂的果

子被摘光之後，就會停滯不前，例如民用飛機的氣動造型，頭60年進步飛速，但是在噴射客機出現之後，逼近了音速障礙，在其後的60年，就基本沒有改進，這也是爲什麼Boeing會想要繼續沿用737的原始機體設計，以避免重新設計新機的費用與時間。 另一個例子，當然是高能物理，自從1974年確立QCD之後，理論上的進步不大於零，這也是我解釋過很多次的事實。 量子計算是一個新領域，倒不像傳統的Si基半導體那樣已經接近黃昏，但是全新的科技有更大的危險，就是絕大多數都沒有實用性，這一點我也寫過幾篇文章來討論了。例如現在的所謂第四代核裂變反應器有十幾種，30年後頂多有兩種能存活下來；核聚變反應堆的設計種類更多，但是50年後仍然可能是無一成功。 我覺得這類成功機率很小的新科技，如果有特殊背景考慮，例如量子計算對大國之間的鬥爭可能有巨大影響，可以適度投資，至少保持不落後太遠；但是絕對應該量力而爲，避免蘇聯被忽悠進科幻武器軍備競賽的窘境。

返回索引页