【基礎科研】Google的量子霸權是怎麼回事？

2019-09-25 06:25:00

原文网址：http://blog.udn.com/MengyuanWang/129678773

前天有讀者在訪客簿（順便提一下，請大家盡可能在文章下的留言欄做討論，只有在《UDN》的系統出問題，無法正常留言的前提下，才選擇訪客簿）上提問，說Google剛宣稱的“量子霸權”（“Quantum Supremacy”）是怎麼一回事？當時我說：“要嘛是謠言，要嘛是一個毫無實際意義的程序，專爲創紀錄而創紀錄。”

現在有了更清楚的消息（參見Scott Aaronson的博客https://www.scottaaronson.com/blog/?p=4317；Aaronson是知名的量子計算專家，並且參與了Google的這個研究計劃），我可以給出更精確的答案，也就是上述兩個可能中的後者。這是一個毫無實際意義的結果，而且有相當嚴重的假大空成分。

首先，我們先解釋一下什麼是“量子霸權”；它指的是量子計算機在某個程序上能比現有的古典電腦高效許多。請注意，這個定義並不要求那個程序有任何實際意義或價值，所以我一開始就疑心Google團隊鑽的是這個漏洞。

結果果然是如此。Google選擇的程序是先隨機產生一串長度為N（Aaronson說N大約為20）的量子位元串列，其間可能有各式各樣的量子糾纏，然後不斷複製這個串列，再讓複製版塌縮形成長度為N的古典位元，那麼這些古典位元就是隨機但並不完全獨立，而是有由量子糾纏來決定的複雜相關性（Correlation）。這有什麼用呢？一點用處都沒有，就像你隨便建造出一個複雜而沒有規律的機器，然後說它在產生獨特的噪音上，有無可比擬的效率。

事實上，Google的這個“成就”，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。現在的世界記錄是不到100個量子位元；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，完全無法驗證。

Google用了50-60個量子位元來儲存這個量子串列，並且不斷複製再塌縮。這顯然並沒有解決糾錯的基本難關，其結果自然無法確認量子態在程序過程中被正確保存了，還是純屬噪音。

所以Google團隊就先用古典電腦算出他們計劃中的量子糾纏應該會產生的相關性，接著反復地用量子計算機跑這個程序，一直到它產生同樣的相關性結果爲止。這時他們比較兩者跑單次程序所花的時間，然後宣稱量子計算機大獲全勝。

至此，理工科的讀者應該理解到問題有多大。首先，相關性關係裏的自由度（Degrees of

Freedom）遠低於原系統，所以只用相關性結果來驗證程序的正確性，完全可能是統計上的偶然。

但是更基本的毛病，在於Google的量子計算機並無法自行保證結果是正確的，只有在古典電腦已經給出結果之後，才能做比較。一個有相當大而且不可預知的可能性會輸出噪音的計算機，不止是沒有實用價值，根本就沒有任何意義。這是標準的假大空，不是學術界可以容許的做法。Google是一個商業機構，做虛僞廣告是本行，但是量子計算界不應該受商業資金的收買，學術道德也不能待價而沽。

【後註一】因爲Aaronson的博文對若干細節語焉不詳，我必須依照科學原理來做推測，現在有更新的文章，似乎是有一點差異，亦即Google的系統比我想象的還要簡單，連"複製"的那一步都做不到，而只是反復地隨機產生量子位元，然而塌縮。這對接下來的評論並沒有影響，Google仍然是先射箭、再畫靶，而且也沒有糾錯機制，如果沒有古典電腦的驗證，就不知道結果是否正確。

【後註二】有讀者用私信問我有關最近《Nature》上面批評中國在西部乾旱地區植樹的一篇論文。我的想法和這裏的正文有點關係，所以也節錄於下。

我覺得一般的中國群衆，因爲受傳統文化和社會結構的影響，對學術界有非理性的崇拜。事實上，現代學術界雖然整體來說還是有不斷的重要貢獻，但是其中欺世盜名的假大空已經佔了大多數，所以固然不須要拿任何個別論文來當真，即使是中位平均（Median）也可以鄙視的。這是因爲不能被複製的科學論文，就是假的，而假科學不但沒有任何正面價值，反而對人類社會能有重大的負面影響。

我以前已經提過，現代學術界正處在一個所謂的"可複製性危機"（Reproducibility Crisis），過去十年有很多研究，給出驚人的可複製比率（如11%，也就是大約1/9）。在2018年出版的一個新報告（參見https://www.sciencemag.org/news/2018/08/generous-approach-replication-confirms-many-high-profile-social-science-findings）專注在最頂尖的兩個科學期刊（亦即《Nature》和《Science》，這篇論文本身發表在《Nature》）上，結果是只有62%可以複製，而且即使在這62%裏，信號强度也顯著低於原本號稱的程度。

以上這些研究的對象，只限於實驗性的論文，所以至少還有幾分之幾的可複製性可談。如果我們考慮如高能物理理論這樣在過去40多年總進展為零的領域，就會明白他們在期間所發表的百多萬篇論文幾乎全都是假大空，那麼自然更加沒有什麼崇敬的必要。

---

7 条留言

leo369258 2019-09-25 10:18:00

王老师已经很久没有发有关军事的文章了，期待。。。。

> 最近比較沒有去注意新武器的發展。。。 不過我在過去很多年，一直詬病共軍居然還大批采用藍色的野戰迷彩服。現在總算要改了。

东湖人 2019-09-25 10:35:00

感谢王兄解惑，这个谷歌的量子霸权消息一出来，先让人吃惊，后来撤论文又搞得扑朔迷离。我内心一直是觉得此事应该不靠谱，因为听过科技猿人关于量子通信那一期的扫盲，所以完全不相信谷歌能突然放出个大卫星出来。这下明白了。另外，私以为搞基础性科技，什么公司都不可能干得过国家行为。

> 目前Google爲什麼撤稿，有不同説法，包括他們的公關預定的時間還沒有到，事先泄露是個別人員的失誤。 如果有精幹的管理人，國家的力量當然大於企業。問題是中共的官僚體系，對專業議題並不擅長。

大一統理論 2019-09-25 22:41:00

量子通用計算領域的量子計算距離實用化還很遠，距離建造一個有效的量子邏輯位元都還很遠，而量子計算目前只有量子保密通訊的應用被中國工程師實用化而已，但是對大多數對計算機科學理解不深的人來說看到新聞還以為量子計算都快要普及了量子電腦快要出了，他們不清楚這兩者的分別.....因為他們沒學過演算法和計算複雜度理論、程式設計等相關課程，結果就是一些非理性投資人買進股票Google達到宣傳效果....

> 是的，量子計算目前可見唯一的實用目的，是破解使用公開碼（Public Key）的密信，它不但對私碼（Private Key）毫無作用，連下一代的公開碼都不一定會有效。所以它真正的意義，只在於有點可能會對大國之間的互相監聽有影響。 要破解現有的公開碼，至少要有幾千個邏輯位元，顯然這不是能很快發生的事。

大一統理論 2019-09-26 16:27:00

(抱歉我底下打錯字)回王博士量子電腦用來解決目前的通常的應用，因為這些應用通常已經被優化成多項式時間的複雜度能完成的並不會比古典電腦更快(看要解決什問題)，但是量子通用計算如果在工程上有突破並不是只能應用在RSA加密演算法的破解上面，秀爾演算法只是其中一種量子演算法而已，還有一大堆的應用是非多項式時間的，而且量子演算法也不只一種，計算機科學裡將計算規模的成長和所需資源的關係用「計算複雜度」大寫O(括弧)表示，例如演算法導致的計算規模每增長N倍 如果是需要指數倍的時間 這樣的算法就稱謂指數複雜度O(C^N) 大寫的O，而比如說許多人如果學過基本的程式設計會知道例如收尋排序所使用的"氣泡排序演算法"通常只要O(log N)對數時間納就能找到結果，而演算法並不是什麼高大上的稱呼，只不過是處理問題的數學方法和邏輯而已，但是就是這個處理問題的方法和邏輯過程影響程式執行的效率，如果計算規模和計算所花的時間呈線性相關就是O(N)大致上如果規模成長N倍所需的資源只會增長N倍，但是有一些應用例如風洞模擬、新藥開發、材料科學，是基本上找不到什麼好的數學方法能夠降低計算複雜度的，用古典電腦計算式和計算規模成指數相關的O(C^N)，這就是量子電腦的妙處，如果量子通用計算實現就能把原本需要和計算規模成長成指數倍時間的擴張的演算法降低成只需要多項式時間，在這些領域如材料科學、可能都會有重大突破的..... 但是如果數學方法(演算法)上有重大突破同樣也能在古典電腦上達成突然的突飛猛進，並不是一定需要量子電腦，例如這個神童有找到針對特定應用的特定問題的解決方法造成「用古典電腦就能夠達成量子演算法的計算性能 https://buzzorange.com/techorange/2018/08/02/18-prodigy/ 新聞：18 歲台裔神童只花一年，就讓傳統電腦演算法效率也能逼近「量子電腦」 以上完全是有可能的，只要數學方法上有改進或有重大突破 針對特定問題的解決方案完全有可能突然之間變得比量子電腦更快...

> 我指的是在量子計算的經濟成本、時間耗費以及失敗的可能性都很大的背景下，這裏一點、那裏一點的小優勢根本不足以交待爲什麼國家必須做出這麼大的投入，唯一勉强説得過去的，是在互相監聽上可以得到的戰略利益。

lbboy 2019-09-27 11:45:00

請問公開密鑰保密性受到打擊的影響層面 請問這種對公開密鑰的保密性破壞的方法出來之後，會不會對像比特幣等加密貨幣等金融記帳系統產生重大的衝擊？ 謝謝

> 有可能。Bitcoin的電子簽名用的是橢圓曲綫加密法（詳細來説是ECDSA算法），這是現有公開碼的一種。

K. 2019-09-27 16:47:00

. 我覺得現在大國搞量子計算就是一個囚徒困境，搞成的可能性也許非常低，但說不準哪個國家哪一天突然做出了革命性突破，如果這種情況發生，不研究這個的國家就會非常被動，所以必須研究，即使投資浪費了也是大家一起浪費，總比發生上面那種情況要好，再說萬一自己國家研究出來了呢

> 是的，我一直說量子計算和量子通訊的意義只限於大國競爭，就是這個意思。

大一統理論 2019-09-29 00:32:00

光是量子計算可能讓材料科學、新藥物合成、量子化學等領域有巨大突破，怎麼會是這裡一點點、那裡一點底的小優勢呢? 只要量子通用計算能夠真正實用，就能夠讓隨計算規模成長古典電腦在指數倍時間才能做完的事情再多項式時間裡做完間，量子計算的研究可以算是高風險高報酬的投入，怎麼會是一點點小優勢呢? 我並不否認他的投入失敗可能性很大 但是1%成功率可能完全改變在材料科學、量子化學大分子藥物合成等領域的巨大突破就足以讓他繼續研發了....

> 這不只是成功機會小的問題，主要是在民生用途上，不須要第一個去吃螃蟹，像是LCD是美國人發明的，但是賺錢的是日本、韓國、台灣和大陸。如此一來，投資風險和報酬的平衡公式就不一樣。 軍用的就會絕對保密，所以只好自己開發。

返回索引页