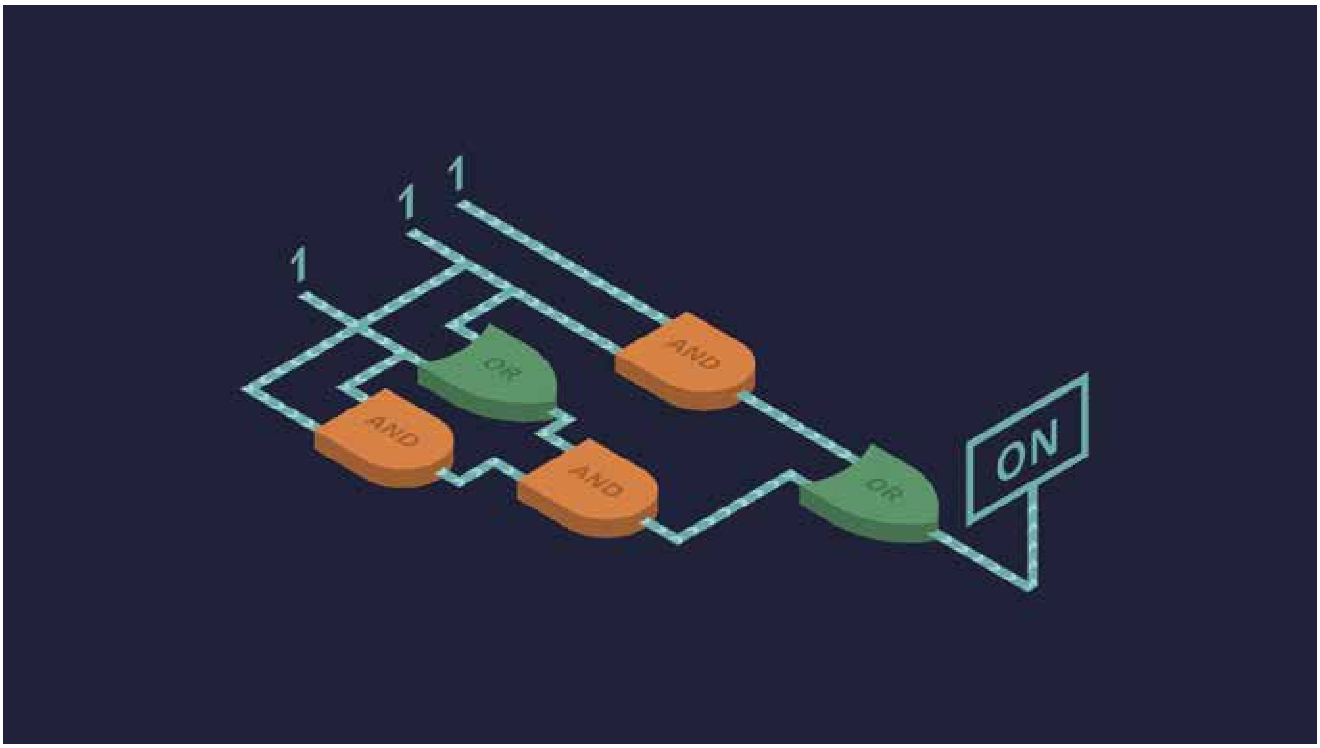
理

幾十年懸而未解計算機科學猜想的證明竟只需兩頁

再度窺見上帝的瑰寶

作者：蔻拉萊克（Erica Klarreich）
譯者：林武雄

作者簡介：蔻拉萊克是紐約石溪大學數學博士，她也獲有加州大學聖塔克魯茲分校科學傳播學程學位。從事數學與科學寫作十餘年，為許多科學雜誌或網站撰稿；文章收入於 2010、2011、與 2016 年的《數學領域最佳寫作評選》。



「靈敏度」猜想困住了許多頂級的資訊學家，然而新證明卻簡單到一個研究員用一條推文就能總結。（Dave Whyte 為 Quanta 雜誌繪製）

一篇於今年七月線上 [1] 發表的論文解決一個懸宕將近 30 年有關電路基本組件結構的猜想。「靈敏度」（sensitivity）猜想多年來困惑了許多最傑出的資訊學家，然而新證明卻簡單到一個研究員用一條推文（tweet）就能總結。

「這個猜想一直是所有組合學和理論計算機科學中最令人灰心與尷尬的未解問題之一，」德州大學奧斯汀分校的亞倫森（Scott Aaronson）在部落格這麼寫著。「挑戰失敗者的名單就像是離散數學和理論計算機科學的名人錄。」他在一封電子郵件中追述。

這個猜想涉及布林函數（Boolean function）[2]

[1] 編註：Hao Huang，“Induced subgraphs of hypercubes and a proof of the Sensitivity Conjecture”，http://arxiv.org/abs/1907.00847v2。
[2] 編註：命名自英國數學家布爾（George Boole），因其所創布林代數系統奠定數理邏輯的基礎，同時也應用到其他領域。

Quanta Magazine 是西蒙斯基金會（Simons Foundation）出版但編輯獨立之網路科普雜誌（http://www.quantamagazine.org/），希望能提高數學、物理與生命科學前沿研究進展的公眾能見度。本文譯自：
https://www.quantamagazine.org/mathematician-solves-computer-science-conjecture-in-two-pages-20190725/
本刊感謝 Quanta magazine 與主編 Thomas Lin 同意翻譯轉載，翻譯之文責由本刊自負。

—— 將一串（0 和 1 構成的）輸入元轉換爲一個輸出元的規則。有的是：只要任一輸入元是 1 就輸出 1，否則爲 0；或者是：有偶數個輸入元是 1 就輸出 0，否則爲 1。每個電路都是布林函數的某種組合，把它們變成「你在計算機科學裡所做的一切的實體，」 哥倫比亞大學的塞爾維迪奧（Rocco Servedio）如此說道。

多年來，資訊學家已經開發出許多方法來測量一個給定的布林函數的複雜度（complexity）。一個輸入串中的資訊是怎麼樣決定輸出元，每種測度（measure）都從其中擷取了一種不同的面向。例如，布林函數的「靈敏度」，粗略來說就是在追蹤當反轉單一輸入元後會改變輸出元的可能性；「查詢複雜度」（query complexity）則是在計算可以確定輸出結果之前所需要詢問的輸入元數量。

每種測度都爲通往布林函數的結構開了一扇獨特的窗口。然而，資訊學家早已發現幾乎所有的測度都適用於一個統一的框架，因此其中任何一種的數值都是其他測度值的粗略量尺。但似乎只有一種複雜度測度不適用：靈敏度。

1992 年，耶路撒冷希伯來大學的奈森（Noam Nisan）和（現任職於羅格斯大學）塞格狄（Mario Szegedy）提出了靈敏度會確實適用此框架的猜想。但是沒人能證明。塞爾維迪奧這麼說：「我想，這可能是布林函數的研究中懸而未解的重要問題。」

卡內基梅隆大學的奧唐納（Ryan O'Donnell）說道：「人們寫了冗長而複雜的論文，試圖取得些許的進展。」

現在，艾默利大學（Emory University）的數學家黃皓（Hao Huang），用一個巧妙而基本，有關於立方體上點的組合學的兩頁論證，就證明了靈敏度猜想。法國國家科學研究中心（Centre National de la Recherche Scientifique，CNRS）的馬蒂厄（Claire Mathieu）在透過 Skype 採訪時寫道：「就像顆貴重的珍珠，美極了！」

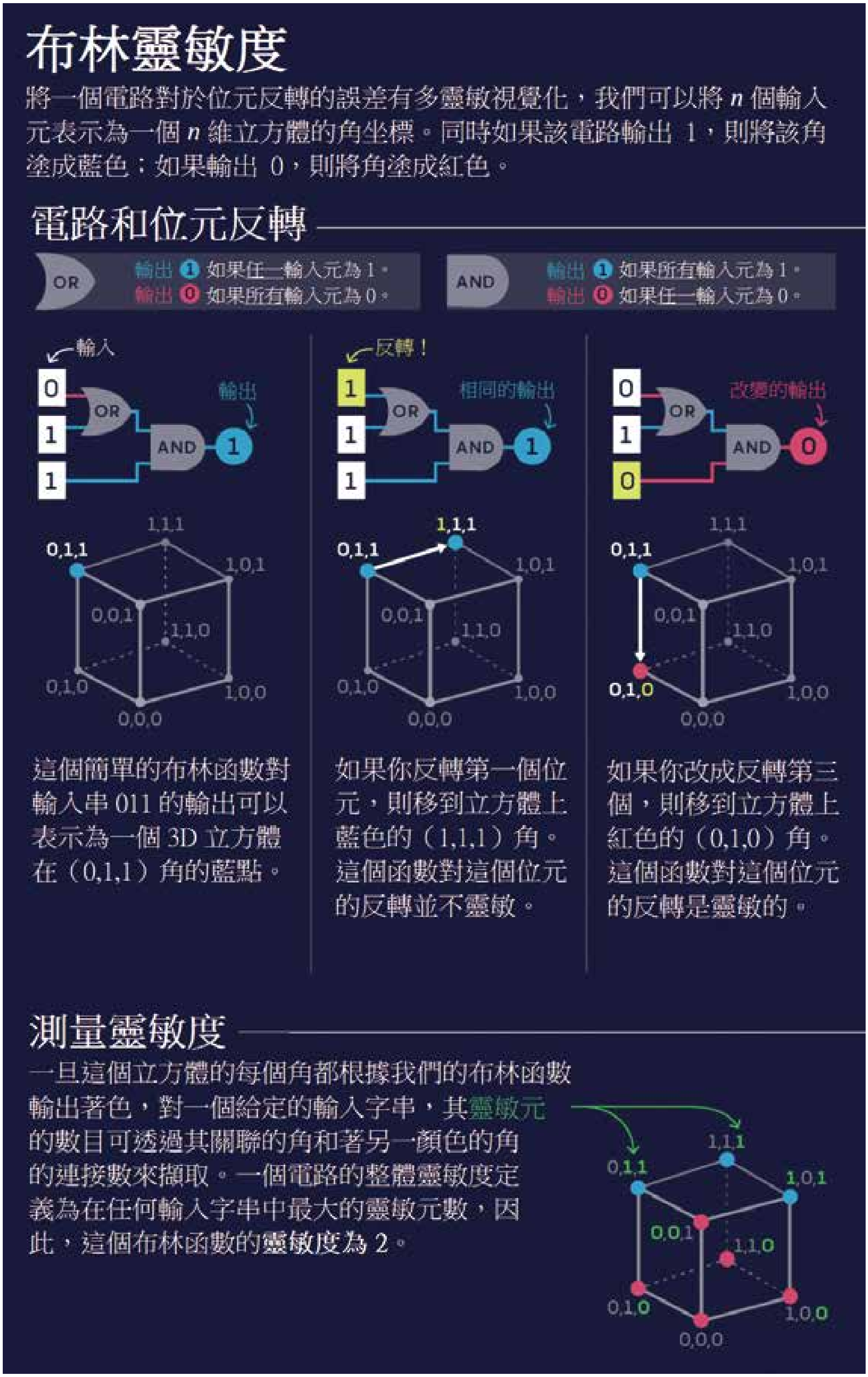
亞倫森和奧唐納讚譽黃皓的靈敏度猜想證明論文實屬於書中的證明。這裡，書指的是艾狄胥（Paul Erdős）的一個概念 —— 有一本天書，上帝在這本書中寫下每個定理的完美證明。亞倫森在他的部落格中評道：「我覺得即使上帝知道如何證明靈敏度猜想，也很難想像有比這還簡單的方法。」

一個靈敏的問題

馬蒂厄說道：「想像一下，當你填寫完成銀行貸款申請書上一連串的是非題問卷後，行員會對你的問卷答案進行評分，並告訴你是否有資格獲得貸款。這整個過程就是一個布林函數：你的答案是輸入元，而行員的決定是輸出元。」

如果你的申請被拒絕，你可能會想「是不是只要就單一問題上說個小謊就能改變結果呢？即使沒有，也宣稱自己收入超過 50,000 美元。」也許吧！如果這個謊言會反轉結果，資訊學家就說這個布林函數對此特定元的值是「靈敏的」。比方說，如果有七個你原本可以撒的不同謊言，分別都會反轉結果，那麼對於你的貸款資料來說，這個布林函數的靈敏度就是 7。

在看過所有的貸款資料後，資訊學家將布林函數的整體靈敏度定義爲「最大靈敏度值」。從某種意義上來說，這個測度值計算出在最灰色地帶的搖擺



（Lucy Reading-Ikkanda 製，Quanta 雜誌。）

案例中，有多少問題是眞正重要的 —— 如果這些問題的答案稍有不同，那麼這些申請案最容易被擺到另一邊。

靈敏度通常是最容易計算複雜度的測度之一，但它絕非測度的唯一明燈。例如，與其給你一張申請表，行員可以經由對話，從第一個問題開始問起，然後根據你的答案決定接下來要問的問題。在做出決定之前，行員需要提出的最多問題數就是布林函數的查詢複雜度。

這種測度出現在許多情境中 —— 例如，醫生會想要在做出診斷前給患者儘可能的少做檢查，或者機器學習專家會想要演算法在把一個物體分類之前儘可能的少檢驗其特徵。「在很多情況下 —— 診斷情況或學習情況 —— 如果基本原則……你會眞的很高興，有低的查詢複雜度。」奧唐納說。

其他的測度包括尋找將布林函數寫成數學式的最簡單方法，或者計算行員要向老闆展示多少答案來證明他們有做出正確的貸款決定。甚至還有量子物理學版本的查詢複雜度，其中行員還可以同時詢問好幾個問題的「疊加狀態（superposition）」。弄清楚這個測度如何與其他複雜度測度有關，就已經幫助研究人員理解量子演算法的侷限。

除了靈敏度這個僅有的例外，資訊學家證明所有這些測度都是緊密相連的。具體來說，它們之間具有多項式的關係 —— 例如，一個測度可能大致是另一個測度的平方、立方、或平方根。只有靈敏度頑固拒絕適用這種簡潔的特徵。許多研究人員認爲它有可能確實屬於這個圈子，但他們無法證明不會有個奇怪的布林函數，其靈敏度與其他測度具有指數型的而非多項式型的關係，在這種情境下，意味著靈敏度測度遠小於其他的測度。

「這個問題成爲人們的心頭大患有 30 年了，」亞倫森是這麼評論的。

轉「角」遇到解法

2012 年底，黃皓在高等研究院（當時他在那擔任博士後研究員）與數學家沙克斯（Michael Saks）共進午餐時聽聞了靈敏度猜想。他立刻被這個猜想的簡潔和優雅所吸引。「從那一刻起，我開始沉迷於思考它，」他說。

黃皓將靈敏度猜想加進他感興趣問題的「秘密列表」中，每當他學到新的數學工具時，他都會思量是否能有幫助。「每次我發表新論文後，我都會回到這個問題，」他說。「當然，在一段時間後我就會放棄，而去著手一些更現實的問題。」

正如廣大的研究社群所知，黃皓也知道，如果數學家們可以證明一個簡單陳述著關於不同維度立方體上的點集合的猜想，那麼靈敏度猜想就可以得到解決。n 個 0 和 1 的字串與 n 維立方體上的頂點之間有一種自然的對應方式：只要用這 n 位元作爲點的坐標。

例如，四個二位字串 —— 00，01，10 和 11 —— 對應於二維平面中正方形的四個角：$(0,0)$，$(0,1)$，$(1,0)$ 和 $(1,1)$。同樣的，八個三位字串對應於三維立方體的八個角，更高的維度依此類推。反過來，一個布林函數可以想成是把這些角賦予兩種不同顏色的規則（例如，紅色表示 0，藍色表示 1）。

1992 年，現在就職於紐澤西理工學院的戈特斯曼（Craig Gotsman）和耶路撒冷希伯來大學的利尼爾

數學家黃皓攝於里斯本度假期間。（Yao Yao 攝）

（Nati Linial）指出 [3] ，可以把靈敏度猜想的證明簡化為回答不同維度立方體上的簡單問題：如果你選擇立方體上任何超過一半的角並將它們染成紅色，是否總有一些紅點與許多其他紅點相連？（這裡，「相連」的意思是這兩個點共用立方體上的邊，而不是跨越對角線。）

如果你遴選剛好一半立方體上的角，有可能它們不會相連。例如，在三維立方體的八個角中，這四

[3] 編註：Craig Gotsman and Nati Linial，“The Equivalence of Two Problems on the Cube”，Journal of Combinatorial Theory, Series A, Volume 61 Issue 1, Sept. 1992 Pages 142-146。

個角 $(0,0,0)$ ，$(1,1,0)$ ，$(1,0,1)$ 和 $(0,1,1)$ 彼此對角而坐。但是只要把立方體上任何超過一半的點塗成紅色，某些紅點之間的相連必定浮現。問題是：這些連接是如何分布的？是否至少會有一個點具有高度的連接？

最初在 2013 年時，黃皓思考到：要理解這個問題的最佳途徑，可能就是要透過使用追蹤點之間連接的矩陣來表示網路的標準方法，然後檢查一組稱爲矩陣特徵值（eigenvalue）的數字。五年間他不斷的反覆審視這個想法，但總行不通。「但至少許多夜裡想著它（幫）我快速睡著，」他在亞倫森的部落格文章中給出這個評論。

到了 2018 年，黃皓突然想到要用一個有 200 年歷史，被稱爲柯西交錯定理（Cauchy interlace theorem）的數學，它將矩陣的特徵值與其子矩陣的特徵值聯繫起來，使其成爲研究立方體與立方體上角的子集之間關係的利器。黃皓決定申請美國國家科學基金會（National Science Foundation，NSF）補助來進一步探索這個想法。

一直到了上個月，當他坐在馬德里（Madrid）的一家旅館裡寫他的補助計畫時，他突然意識到：藉由切換矩陣中某些數字的正負號，就可以簡單的一路由此途徑落實想法。用這個方法他就能夠證明：在 n 維立方體上任何超過一半的點集合中，必定存在某個點與其他至少 $\sqrt{n}$ 個點相連 —— 同時靈敏度猜想隨即依此結果得證。

當黃皓的論文送抵馬蒂厄的信箱時，她的第一反應是「喔哦，」她說道「一個問題已經存在了 30 年左右，而且每個人又都聽過這個問題時，那麼它的證明如果不是很冗長、乏味又複雜，就是很深奧。」她不抱期待的開封這篇論文。

但是對於馬蒂厄和許多其他研究人員來說，這個證明簡單到一口氣就可以消化。她在 Skype 發出「我希望今年秋天就能夠在每個碩士班的組合學課程裡用一堂課講授這個證明。」這訊息。

黃皓所得到的結果甚至比證明靈敏度猜想所需的結果更強，而這個結果的強度勢必會促進對於複雜度測度有新的見解。塞爾維迪奧說道「它放進了我們會用來嘗試解答布林函數分析裡的其他問題的工具包。」

然而，最重要的是，黃皓的結果讓人們不再擔心靈敏度會是複雜度測度世界裡的某個離群怪客，塞爾維迪奧評論到：「我想很多人在聽到這個消息之後的那個晚上會睡得更香甜了。」∞

本文出處

Quanta Magazine July 25, 2019。本刊特別感謝艾默利大學的黃浩教授授權刊登他的照片。

譯者簡介

林武雄為國立交通大學應用數學系助理教授。

延伸閱讀

▶有關靈敏度猜想被證明的更多故事與討論，可見亞倫森的部落格，該篇底下還有黃皓本人的回應：https://www.scottaaronson.com/blog/?p=4229
▶Martin Aigner and Gunter M. Ziegler，“Proofs from THE BOOK”，6th ed.，2018，Springer。