數學傳播 43卷2期, pp. 3-14

有朋自遠方來——專訪 Ronald Graham 教授

策　劃：劉太平

訪　問：劉太平、葉永南

時　間：民國 104 年 10 月 7 日

地　點：中央研究院數學研究所

整　理：編輯室

Ronald Lewis “Ron” Graham 教授 1935 年 10 月 31 日出生於 Taft, California。1962 年在 UC Berkeley 獲 Ph.D. 學位。先後任職 Bell Labs 和 AT&T Labs, 並曾在 AT&T 擔任資訊科學所所長。1999 離開 AT&T, 現任教 UCSD, 同時也是 Cal-(IT)^2 首席科學家。他在 1993~1994 年擔任美國數學會會長。

Graham 教授在離散數學等核心領域有重要貢獻, 曾獲多項殊榮, 包括 2003 年美國數學會 Steele Prize 終生成就獎。本訪談中先生展現其寬闊的見識, 理論應用出入無礙的學術精神。

劉太平 (以下簡稱「劉」): 你常提到 Erdős[1], 我想請問一下: 什麼原因讓他選擇過那種獨特的生活方式?

Graham (以下簡稱「G」): 嗯 $\cdots$ 這可難說了。有一位匈牙利數學家名叫 László Babai[2], 目前在芝加哥大學。我第一次遇見他時, 他年方 19, 現在已年約 62。他曾寫過上百頁的 Erdős

[1] Paul Erdős (1913~1996), 匈牙利籍數學家, 研究領域涵蓋組合數學、圖論、數論、古典分析、逼近理論、集合論和機率論。

[2] László Babai (1950~), 匈牙利籍數學家, 芝加哥大學計算機科學暨數學系教授, 研究演算法、計算複雜性理論、組合數學和有限群, 並強調這些領域之間的相互作用。他於 2017 年提出圖同構問題的準多項式 (quasipolynomial) 時間演算法。

傳記。在 Erdős 求學時期, 匈牙利嚴格限制猶太大學生的人數。這個限制極爲嚴格, 而數學是一個容許你實際去學習的領域。Erdős 的兩個姊姊都在他出生前後過世, 因此母親對他百般呵護。他母親其實是一位數學老師, 因此 Erdős 大半時間在家自學。舉例來說, 他不知道如何把奶油塗在麵包上, 因爲他從來不需要做這種事, 媽媽總是爲他打點好。他在英國時, 才發現「原來我做得到!」。有一本很好的童書, 題爲「*The Boy Who Loved Math*」(「一個熱愛數學的男孩」), 述說 Erdős 的少年時期及成長歷程。這是本很迷人的小書, 而我的工作就是確認 Erdős 黑板上和其他地方隨興寫的數學是正確的。

Erdős 個性很獨特。有一個好故事: 一位名叫 Péter Frankl[3] 的數學家, 目前居住日本。他在匈牙利拿到學位後, 被徵召入伍, 但數學才華與他相若的朋友卻能免役, 逕赴數學研究所。Péter 覺得這是因爲他是猶太人, 於是請 Erdős 寫封信, 讓他可以離開軍隊。Erdős 寫了信, 但 Péter Frankl 一退伍, 立即自匈牙利叛逃。這讓 Erdős 震怒, 因爲他事先不知道 Péter 會這麼做。Erdős 告訴他:「你削弱了我的地位, 現在我無法用同樣的方式幫助其他人, 所以我兩年內不再對你說話。」在那段時間, Péter Frankl 到法國巴黎拿另一個博士學位, 而 Erdős 在授予學位的委員會裡。Erdős 提交報告時 (報告裡寫說: 這是篇傑出的論文), 真的沒對 Péter Frankl 正式說任何話, 甚至私下也不和他交談。兩年過去, 沒事, 他依然沒有任何改變, 在這方面他很固執。

話說, 匈牙利曾舉辦某會議, 是非正式的國際會議。Erdős 的幾位以色列同事想來參加, 但礙於以色列和匈牙利的關係不佳, 他們沒拿到簽證。依據法規, 召開國際會議時, 必須核發簽證給與會的科學家, 但那場會議是非正式的, 不發簽證。這讓 Erdős 震怒, 放話說:「在他們向我道歉前, 我都不回匈牙利!」結果他等了好幾年; 衆人十分錯愕, 對他喊話:「看吧, 沒人會向你道歉。你只會傷了我們這些在匈牙利的, 因爲你是我們當下國外數學資訊的主要來源。請重新考慮一下, 回來吧。」最後他回去了, 但他始終立場堅定。

1954年, 國際數學家大會 (International Congress of Mathematicians, 簡稱 ICM) 在阿姆斯特丹舉行, Erdős 很想參加。匈牙利當局告訴他: 一旦去了, 恐怕拿不到再次入境的簽證。Erdős 說:「聽著! 我不會讓任何政府官員告訴我哪裡可以去、哪裡不能去。我就要去了!」他赴會了, 在美國拿不到回程的簽證。之後多年, 大家寫信給國會議員和其他官員, 爲 Erdős 遊說及爭取。他最終拿到簽證回匈牙利, 但始終固守一些原則, 其中之一是不戀棧身外之物。他只有兩個行李箱, 一箱裝著信件和複印的資料, 另一箱只裝幾件衣服。

1986 年在中國濟南有一個會議, 我們一同從北京搭火車, 車上喧鬧且悶熱。半夜時, Erdős 說:「我得下車了, 太熱了, 我睡不著!」我說:「Paul, 我們現在是在從北京到山東的火車上, 你不能就這樣下車啊! 你不能啊!」到天津時, 我買了些絲襪給他。他皮膚極敏感, 但他可能會去沒賣絲襪的地方, 所以我買了一些給他。有好多關於 Erdős 的好故事。

[3]Péter Frankl (1935∼), 匈牙利數學家, 熱衷於街頭表演藝術, 曾與 Paul Erdős 合寫 7 篇論文, 目前居住於日本。日本名爲富蘭平太。

劉: 你把他當家人一般地照顧。

G: 是的。當時我們的房子特別留有 Erdős 的房間。他需要有自己的浴室、電話, 也要會用冰箱, 半夜才有食物吃。關於這些, 還真是有許多好故事。

劉: 這是出自你對他由衷的敬意。你喜歡他, 也尊敬他的數學, 對吧?

G: 是的。他心腸很好, 有顆好大的心。

葉永南 (以下簡稱「葉」): 他真的很好。

G: 有這樣一個好故事: 有次他和某人住在一起。淸晨四點時, 浴室傳出巨大聲響。他一早去用早餐時, 隻字未提, 最後才說:「你知道的, 早上你的浴室裡沒有發生什麼意外, 只是有一大瓶碘酒破了, 灑了一地。但別擔心, 我找到足夠的毛巾, 把它們都吸了起來。」你可能知道, 碘漬是幾乎不可能淸除的。Erdős 用意良善, 但他的用心並不是都能奏效。

劉: 但你了解他, 你說他「好心 (good heart)」。

G: 他最珍貴的一項財產, 是他每天寫的數學日誌, 裡頭記錄他當時在思考些什麼。他過世時, 這些日記都放在他的鄰居兼親密數學同事 Vera T. Sós[4] 那裡。她持有這些日記, 卻不讓其他人過目。我們問:「爲什麼呢?」而她說:「喔, 我就是不想要。」很多人都想了解 Erdős 過去思考些什麼。Erdős 會把數學筆記寫在右邊, 而後經常性地回顧, 並在左邊加上其他註記, 像是:「喔! 我知道了, 這是我之前想過的其他問題的一個特例。」我很想了解: 他在從事質數定理 (prime number theorem) 的初等證明[5] (elementary proof) 時, 想了些什麼。

劉: 所以日記仍然存在, 但沒有人可以過目。

G: 對, 她擁有這些日記。共約 20 冊, 我複印了其中兩冊, 但它們都是用匈牙利語寫的, 我看不懂。幾年前, 他百歲誕辰, 舉辦了 800 人的大型會議。我想他不曾到過台灣。

劉: 說到這個, 今天早上我跟同事劉豐哲提到這次訪談時, 他告訴我: 你很久以前來過台灣, 1971 年吧。

G: 沒錯, 我來過。我在香港待了一個夏天, 適逢當地首條隧道開通。我記得, 時值李小龍[6]亡故。我去台大給了一場排定的演講, 我還保存著報導這場演講的報紙。我四處旅行, 金芳蓉[7]在此地, 1970~74年間。

[4]Vera T. Sós (1930~), 匈牙利數學家, 研究數論和組合數學。

[5]意指只用到基本技巧的證明。特別是在數論中, 意指沒有用到複分析的證明。

[6]李小龍 (1940~1973), 出生於香港, 武術家暨國際武打巨星。

[7]金芳蓉 (1949~), Graham 教授的夫人, 加州大學聖地牙哥分校教授, 研究譜圖學 (Spectral Graph Theory)。

葉: 對, 她是張聖容[8]、李文卿[9]和吳徵眉[10]的同學。

G: 陳省身爲她們那班的四朵「金花」寫了一篇文章[11]。某份數學雜誌的編輯聲稱要把它翻譯成英文, 但應該還沒動工。其實班上有五位才華洋溢的女性, 但其中一位早逝, 所以實際上有五朵金花。

劉: 雜誌名稱是「傳記文學」。你和很多人交往, 在多方向做研究。可否問個問題: 什麼研究帶給你最大的快樂? 或是說什麼工作對你來說最難完成?

G: 嗯, 我想數學是很特殊的。小時候, 我喜歡的其實是天文學, 覺得星星很有意思, 但之後發現天文學家不光是看星星; 他們不是看望遠鏡, 而是用電腦去分析從望遠鏡得到的數據。不過這仍令人驚嘆!

有人問我爲什麼玩那麼多雜耍 (juggling)? 玩雜耍的人很多是來自數學界或電腦科學界, 歷史和哲學領域裡玩雜耍的較少。何以致此? 箇中關聯似乎是, 數學時或被描述成模式 (pattern) 的科學, 我們是在追尋模式。雜耍是一門在時間和空間中掌控模式的藝術。常言道: 雜耍的癥結是, 球確實到達的位置, 取決於你如何扔出, 而非依照你的期望。電腦運作程式時, 完全遵照你的囑咐, 但不會有指令說 :「喔, 你應當知道我的意向。」它不知道你的意向是如何, 你必須告訴它! 數學裡有無窮無盡的挑戰, 你永遠解決不完所有的問題。每當你寫了篇論文, 就會有所延伸, 諸如去探詢更高的維度。雜耍也總會有越來越難的花招。很有趣的是, 過去耍七顆球是非常困難的技巧, 現在則已司空見慣, 難度持續上升中。

YouTube 上有段耍九顆球的影片, 雜耍者一面耍球、一面將九顆球拋到背後, 難以想像。這看似不可能, 但總有堅定有毅力之士。一旦你目擊一些事情是可能的, 心裡就有所領會。好比當年出現首位四分鐘內跑完一英里的人。那成績看來無法企及, 但一旦有人做到了, 就會有更多人達成。

劉: 我記得有位名叫 Bannister[12] 之類的人物, 相當晚近, 似乎在 70 年代 $\cdots$

G: 我認爲 Roger Bannister 是第一個做到的, 目前紀錄大概是 3:45 左右。現在普遍認爲會有人可以在兩小時內跑完馬拉松, 但幾年前這聽來似乎不可能。

葉: 你也曾是專業的彈翻床[13]選手?

G: 是的, 彈翻床也是一種的雜耍形式, 以你自己爲拋彈的主體, 所以不可拋丟! 我父母在造船廠造船, 因此我小時候經常搬家, 每年念不同的學校, 從來沒真的好好念高中或國中。我跳

---

[8]張聖容 (1948∼), 研究幾何分析, 普林斯頓大學數學系教授; 參見本刊 153、154 期 (2015 年第 36 卷第 1 及第 2 期) 專訪。

[9]李文卿 (1948∼), 賓州州立大學數學系教授, 研究數論。

[10]吳徵眉, 伊利諾大學厄巴納-香檳分校數學系教授, 研究複分析、機率論及偏微分方程。

[11]陳省身, 記幾位中國的女數學家, 傳記文學, 66 卷第 5 期 (1995)。

[12]Roger Gilbert Bannister (1929∼2018), 英國著名賽跑運動員和神經學專家, 是第一位於 4 分鐘內跑完 1 英里的人。

[13]彈翻床爲體操項目, 2000 年雪梨奧運正式列入比賽項目之一。

過級, 沒念過 12 年級, 15 歲就去上芝加哥大學, Carl Sagan[14]是我的同學。我在那裡接觸到體操和雜耍。芝加哥大學有個社團, 每週聚會數次, 學習各種不同的馬戲技巧, 像是雜耍、單輪車、體操 $\cdots$ 等。到高中巡迴表演, 展示芝加哥大學是個多麼有趣的地方, 成了一個招生的手法。彈翻床是其中一部分。我到現在還保有一個彈翻床。如今世界水準急劇上升。彈翻床在澳洲奧運會上被引介, 成爲奧運項目。中國眼見彈翻床成爲奧運項目, 企圖成爲世界第一。中國有了最好的教練、最好的設備、及最好的運動員, 如今舉世無匹。毫無疑問地, 他們是世界第一。

劉: 而且他們很小就開始訓練。

G: 是的, 但要有好的訓練。他們有大量人口可供挑選, 再加上精良的訓練技巧, 有些表演技藝真令人嘆爲觀止。表演者經常彈跳 10 公尺高。以往, 彈翻床上有人時, 你站到床附近, 在他飛過時, 試著從下方抓住他。現在如果有人從 10 公尺高墜落, 你再也不用這樣做了; 取而代之的是, 你扔一個防護墊, 然後說:「祝你好運!」另外, 彈翻床上還有框架墊, 落到上面安全無虞; 即使有些閃失, 也無妨, 大命可保。

我們談到這些事物, 有一個基本原則: 要理解一項複雜的東西時, 你可以把它分解成幾個小的部分; 掌握小的部分後, 再它們湊合在一起。舉個例子, 我正在研究這個方塊。想想當你長途飛行時, 有什麼事情可以做? 有這個魔術方塊 (Rubik's cube)。

葉: 這是 $9 \times 9 \times 9$ 的?

G: 不是, 是 $7 \times 7 \times 7$ 的。如今已製作出各種不同的尺寸。四十年前魔術方塊初問世時, 是 $3 \times 3 \times 3$。之後希臘有位人士, 習得製作技術, 做出更大的魔術方塊, 最大可達 7 階左右, 但轉起來不很順暢。中國大陸有更好的建構技術, 目前尺寸可達 17 階。這些立方體的每個面, 都有很多像素 (pixels)。去年夏天, MAA (Mathematical Association of America) 百週年紀念會議上, 我將「 MAA」和「100」的字樣印在 $13 \times 13 \times 13$ 立方體的面上, 致贈他們。

這看起來極其複雜, 但其實並不複雜, 因爲有標準技巧如下述: 首先讓各個面的中央區[15]呈單色。這是個奇數尺寸的立方體, 所以中央區始終置中。這是第一步, 花了我半小時左右來確實完成每一面。然後你讓周邊的顏色一致[16], 但周邊的內部不需要與面的中心部分同色, 很快地, 所有面的中央區呈單色, 且所有周邊的顏色布局一致。接著, 你可以想像你有個 $3 \times 3 \times 3$ 魔術方塊, 其中央層非常肥厚, 於是 $7 \times 7 \times 7$ 方塊等價於 $3 \times 3 \times 3$ 方塊, 而你接下來就可以套用 3 階的演算法。

[14] Carl Edward Sagan (1934∼1996), 美國天文學家、宇宙學家、科普作家。小行星 2709 及火星上的一個撞擊坑以他的名字命名。他因撰寫多部科普著作及電視影集而享譽全球, 曾獲普利茲獎。

[15] 不在周邊的部分。

[16] 亦即, 在角落方格外的部分有單一顏色。

這個想法就是: 把看似複雜的東西, 簡化成許多較小且較單純的區塊。這就真的數學化了。通常當立方體漸趨完成, 你的任何動作都會破壞之前完成的部分; 你不想如此, 因此需要一些步驟來移動少量的方格。這裡有各種等價類 (equivalence class): 邊上的任何方格都和內部的方格不同類, 我不能把這裡的方格放在那裡; 角落上的八個方格等價, 我可以把它們放在這八個角落的其中任何一個位置上, 但不能把它們放在非角落的區域。所以這兩個方格是等價的。舉例來說, 我想把這個方格放在這裡, 於是我開始填補白色這面, 想把這個方格放在這裡。現在的想法是: 這方格即將放在這位置, 所以我把這個方格移上來這裡, 接著旋轉這個面, 而後回復成之前的樣子; 這過程形成代數上所謂的3-cycle(長度爲三的環)。所以 ⋯ 我要做的就是 ⋯ 這方格 ⋯ 現在放在上方; 接著我旋轉這個面, 而後再把它轉回去; 現在我把它放到底部。我所做的就是處理這三個方格, 重新排列它們, 恰好是 3-cycle。

葉: 還記得四十年前, 我玩魔術方塊, 玩到有點瘋狂, 無法停止思考, 就是停不下來。我年紀很小時就試著自己搞定它, 而後就著迷了。我無法停止也無法入睡, 一心一意只想著這些。我真是太瘋狂了, 兄弟姐妹都叫我停下, 但我就是無法停下。最後, 我到郊外山區某處, 大吼大叫地跑著, 最後覺得非常、非常地累, 昏昏睡去, 才終於停下來。

G: 嗯! 我無時無刻不在想它。如果你勇於挑戰, 會發現這裡有個方格。這是第二層的第 3、5 和 6 號方格。嗯, 你看這面, 3、5、6, 第二層的, 這三個可以換到這裡。有個步驟可以同時把這三個移到那裡, 3、5 和 6 ⋯ 回到上方, 轉個面, 然後 ⋯ 3、5、6, 現在我把它們換到那裡了。所以我簡單地說, 一旦你完成了面和邊的部分, 還有一些事 ⋯ 可能發生的是, 雖然有一個群結構在, 因此你可以任意移位, 但有時還是會陷入棘手的狀況: 一切都完美, 就差了個亂糟糟的邊! 這就是所謂的宇稱性問題 (parity problem), 只會發生在偶數階的魔術方塊上。有些複雜的步驟可以解決這樣的狀況。正如跳彈翻床, 當你持續注視立方體, 一切了然於心; 當我看著它, 我凝視著我打算移動的方格, 不看其它方格。

當今人類的能力極限讓人驚嘆, 譬如競速賽的最佳比賽記錄是 8 秒。還有個競賽, 先把數個魔術方塊打亂, 而後讓你逐一端詳, 接著戴上眼罩去解它們; 目前的紀錄是 50。

葉: 50 秒嗎?

G: 不是, 50 個! 戴上眼罩時, 你只知道目前在解第 37 個、第 38 個、第 39 個等等, 由其他人總計你解決了幾個。YouTube 影片上的某玩家, 解了 50 個魔術方塊中的 49 個, 不過我認爲他其實是可以搞定全部 50 個。你必須記得每個魔術方塊。

有個 3 階魔術方塊的問題是: 若想解決任意打亂的魔術方塊, 至少需要多少步驟? 必要的步驟多達幾個? Google 伺服器列舉了所有可能的位置, 發現你在 20 個步驟內, 一定可以還原任何被打亂的魔術方塊。事實上, 通常 17 個步驟就夠了, 只有少數情況需要 20 個步驟。但競速的選手通常不會使用最少步驟的演算法, 因爲這要花過長的時間去心算。

葉: 你對拉姆齊數 (Ramsey number) $R(5,5)$ 的值有何看法? 15 年前, 有人聲稱這個問題會在幾年內被解出來。

G: 我認識的人都沒說這個問題會被解決。Erdős 有個好故事: 一些外星人要求我們算出拉姆齊數 $R(5,5)$, 否則要摧毀我們。好吧, 世人通力合作個幾年, 可能算得出它。但如果他們要的是 $R(6,6)$, 那就只好攻擊他們, 因爲我們無法計算它。

葉: 那是個廣爲流傳的故事, 沒錯!

G: 譬如, 這個立方體有超過 10^{160} 種布局, 你無法確實列出每一種, 來找出最少步驟的解。10^{160} 已超出我們所能計算的範圍了。

如同許多領域, 在組合數學, 無法解出原來的問題時, 你可以將問題一般化, 而後去解不同的特例。思考原來的拉姆齊數問題時, 你可以著眼於 m 個頂點的完全圖 K_m, 把它的邊上色, 得到 5 或 6 個頂點的單色子圖。你不會得到紅色 K_5 和藍色 K_5, 但或許能得到單色的紅色 K_5 或藍色 K_3, 這是對角線外的情況。衆人對這些已有較多了解; 一旦完全理解它們, 或可計算出 $R(5,5)$。

70 年代, Kenneth Appel[17] 和 Wolfgang Haken[18] 藉助電腦解決四色問題。Haken 認爲不存在人類可審視的簡短證明; 這是問題的本質使然。四色猜想是對的, 因爲它在很多特殊情況是對的; 如果該猜想在某情況下不成立, 定理就不成立。你可以對一些算術系統證明: n 個符號足以陳述的某定理, 其最短證明的長度爲 n 的雙重指數[19], 因此你永遠無法將該證明寫下, 儘管它證明的是定理。

數論有個後設猜想 (meta-conjecture): 若要證明一個數 n 是質數, 則符號用量的成長速度至少是 $\log n$。若真如此, 則無法證明形如 $10^{10^{73}+3}$ 的數是質數。你或可援用機率測試 (probabilistic test): 如果它是合成數, 一半時間會說它是合成數, 而另一半時間不置可否。這並不表示它是合成數; 這是證據, 但卻稱不上是證明。

有一個可能: 我們所熟悉的數學定理, 或許正好都有很短的證明, 讓人類可以確實寫下, 比如說一百頁之內。有限單群 (finite simple groups) 的分類呢? 你可以用一頁紙來陳述這個問題, 但最短的證明會是如何? 可以在一百頁內完成嗎? 我不這麼認爲。一千頁呢? 或許吧! 那個證明被分成好幾個小部分, 不同的部份由不同的人擔綱。Conway[20] 那時還希望在這群人宣布證明後, 能找到其中遺漏的某個單群, 但他說:「不, 他們可能提出完整的分類了。」我想, 當時他們之中有些作者仍盼著自己是最後完成的人; 如果你是最後完成的人, 就

[17] Kenneth Appel (1932∼2013), 生於美國, 1976 年與 Wolfgang Haken 提出四色定理的首個電腦輔助證明。

[18] Wolfgang Haken(1928∼), 德國數學家, 除參與四色定理的證明工作外, 對三維流形理論有重要貢獻, 曾引介 Haken 流形及 Kneser-Haken 有限性等概念, 並曾提出演算法以檢驗結能否打開。

[19] 形如 $f(n)=a^{b^n}$ 的函數, 其指數是另一個指數冪的指數冪。

[20] John Horton Conway (1937∼), 生於英國, 普林斯頓大學榮譽退休教授, 在有限群的分類、結理論、組合賽局論曾做出傑出貢獻, 且曾發明自動細胞機 Game of the Life。

可以說:「我終於完成它了!」

克卜勒猜想[21] (Kepler conjecture) 的證明, 雖被 *Annals of Mathematics* 接受, 卻附帶一則免責聲明: 衆多審稿人審查了這篇文章, 但它如此繁複, 而且需要依賴如此大量的電腦計算, 因此這個證明無法完全被驗證。但他們 95% 相信它是對的。據我所知, 目前已有人提出形式化的證明[22](formal proof)。

當電腦聲稱某事是對的時, 你相信它嗎? 一百頁的證明? 我較相信電腦, 較不相信人! 即使 Feit-Thompson 關於奇數階群的論文[23], 原稿的第一版也有一些錯誤, 但 Thompson[24]說:「別擔心, 我們會修正它們。」事實上, Appel 和 Haken 發表論文[25]後, 還有篇後續論文, 名爲「四色證明足矣」(「the four color proof suffices」)[26]。重點是, 論文的首版往往不完美, 但我們總希望學界的其他人能參與其事, 協力找到完整簡潔的證明。我們很失望學界沒這麼做。順帶一提, 四色定理也有形式化的證明了。

劉: 你曾在貝爾實驗室 (Bell Labs) 多年, 那是你數學生涯的一段重要章節。

G: 當時貝爾實驗室有個很強的團隊。貝爾實驗室曾是 AT& T 的一部分, 而 AT& T 執掌美國電話網絡。貝爾實驗室比較像是一所大學, 但你不用授課, 又有實際問題可以探討。電晶體在那裡被發明, 資訊理論的奠基者 Claude Shannon[27]也在那裡任職。此外, 舉例來說, Unix 作業系統是在那裡創建的。我們有個非常強大的數學團隊, 金芳蓉隸屬其中; 我和她的指導老師 Herb Wilf[28]初結識時, 是在貝爾實驗室, 而不是在 Wilf 執教的費城。

但世局多變, 變動速度與日俱增, 我剛去那裡時, 其他人告訴我, 我的研究成果在未來一、二十年還無法應用, 我想這倒無妨, 反正之後他們仍會在那裡, 可以利用我的成果。而今, 三年就被認爲是非常長的時段了, 因爲電腦世界三年已歷經兩代。我正在用的 iPhone 6+, 已經落伍了。

葉: 他們說最新的版本是 iPhone 6s, 很快就要出 iphone 7 了!

G: 下一代的產品通常較優質, 但不會比較便宜, 而且總會在不久之後問世; 何必現在購入呢? 我們通常用 Apple 的產品, 決定試試看 Android 手機, 買了 Galaxy 6, 很不錯; 它和

---

[21]克卜勒猜想 (Kepler conjecture), 1611 年由德國天文學家克卜勒 (Johannes Kepler) 提出, 關乎三維歐氏空間中留下最小空隙的的裝球方式。

[22]以形式化的數學語言書寫而成的證明, 不同於以自然語言書寫的非形式化證明。

[23]Feit-Thompson theorem, 亦稱奇階定理 (odd order theorem), 聲稱: 每一個奇階有限群都可解, 由 Walter Feit (1930∼2004) 和 John Griggs Thompson (1932∼) 於 1963 年提出證明。

[24]John Griggs Thompson (1932∼), 美國數學家, 1963 年與 Walter Feit 證明奇階定理, 之後在分類不可解集及逆 Galois 問題有根本性貢獻, 證明怪獸群爲 Galois 群, 且發現命名爲 Thompson 群的散在有限單群。1970、1986、2008 年分別獲頒費爾茲獎、Wolf 獎、Abel 獎。

[25]Research Announcement : Every planar map is four colorable. *Bull. Amer. Math. Soc.*, 1976, 82 (5): 711-712.

[26]Kenneth Appel 和 Wolfgang Haken 於 1986 年發表於 *The Mathematical Intelligencer*, 8(1): 10-20 的文章。

[27]Claude Elwood Shannon (1916∼2001), 出生於美國。1948 年發表的論文「通訊的數學原理」, 以機率論爲重要工具, 並提出資訊熵的概念, 奠定了現代資訊理論。二戰期間, 他爲密碼破譯和保密通訊做出巨大貢獻。

[28]Herbert Saul Wilf (1931∼2012), 美國數學家, 專精圖論, 生前任教於賓州大學。

iPhone 稍有不同 ，但有些很好的特性。這些公司必須競爭, 精益求精。這有點像在學習; 做符號計算[29](Symbolic Computation) 時, 我通常使用 Maple, 儘管大家都用 Mathematica、Matlab 和 Sage。最麻煩的是轉換軟體, 要經歷一番學習過程, 譬如: 用什麼方式宣告列表 (list)、字串或向量? 要把小括號、中括號、大括號放在那裡? 什麼時候應該要用分號終止指令? 不變不換較爲省事 (Apple 產品又是另一回事)。但世界很大, 你應該多體驗。我在貝爾實驗室的工作, 容許我四處旅行, 因此有時我整學期到外地授課。我也到實驗室附近的西東大學 (Seton Hall University) 學中文。

大自然的運行致使你接觸到許多好問題。來自大自然的某些東西, 可能正好促成某些事情。舉例來說, 我們曾遇到過一個涉及雷射的問題, 希望雷射中有某些光的介質, 好讓光經過時吸收能量; 我們的構想是在每一端放一面鏡子, 讓光束來回多次, 汲取大量能量。但你必須讓光束離開雷射, 所以你在一端放個小洞, 好讓光束逃逸。光束的影像在每一端都由小圓圈組成。最終要找的, 是這些圓圈所覆蓋的區域範圍。我們爲這些圓圈找到極佳的模式。組裝好配置後, 我們希望看到它運作。麻煩的是, 光束落在紅外線光譜, 所以我們無法看到任何東西。嗯, 不論如何, 它可以運作。

劉: 數學有許多面向。你認爲來日的數學研究本質上會是如何?

G: 這問題很有意思。菲爾茲獎得主 Timothy Gowers[30]近日在一篇文章[31]中談到: 2099 年之前, 電腦或可完成所有重要的數學。電腦會提出猜想、找到證明。而數學家的工作, 是試著去理解和運用其中的一些結果。

電腦不斷地進步。我在日前的演講[32] 提到, 某位人工智慧的研究員編寫了程式「Graffiti」[33], 從而提出圖論方面的諸多猜想, 目前猜想個數已達六千; 金芳蓉幾年前對其中一個猜想找到一個不很顯然的證明。編寫它的研究員表示, 最困難的是去判斷各個猜想是否有趣。目前的電腦並不是那麼擅長找證明, 但它們至少還善於做猜想。

你可以在多項式時間內分解整數嗎? 如今有了所謂的量子運算; 如果你造出真的量子電腦, 就可以在多項式時間內分解整數。那麼, 有任何造不成它的理由嗎? 物理學家起初預期會有難以克服的天然障礙, 但目前普遍認同打造成功的可能性。困難的是, 纏結的 (entangled) 量子位元 (qubits) 要夠多, 且要孤立夠久, 方可做出有趣的事。近千個量子位元可能就夠用, 但目前的系統僅有數十個位元。不過, 實驗學家十分聰明機智, 我們且拭目以待, 等個幾年。

---

[29]意指用電腦推導數學公式。

[30]Sir William Timothy Gowers (1963∼), 英國數學家, 研究領域涵蓋泛函分析及組合學, 1998 年獲頒菲爾茲獎。他發起網上 Polymath Project, 集結衆人之才智解決數學難題。

[31]W. T. Gowers, Rough Structure and Classification, *Geom. Func. Anal.*, Special Vol. 2000, 79-117.

[32]Ronald Graham, 電腦與數學 : 問題與展望, 數學傳播 42 卷第 2 期, 3-24。

[33]休士頓大學的 Siemion Fajtlowicz。

葉: 南京大學的孫智偉是計算數論 (Computational number theory) 學家, 提出了很多很多組合數論方面的猜想。對第 n 個質數的性質, 他總能提出出人意表的猜想。

G: 他做了許多電腦實驗。幾年前, 他實地走訪加州一學期。當年六月在溫哥華有個會議, 他和姚期智等多人與會, Don Knuth[34]也在那裡待了五天, 十分難得!

葉: 正如你所言, 許多人在用電腦。

G: 沒錯。質數看似隨機出現, 很多很多的猜想植基於此。但事實上質數不是隨機的。正因爲它們不隨機, 所以有諸多讓人驚嘆的性質。它們實際上是確定的 (deterministic), 但有些性質讓它們看似隨機。如果它們確爲隨機, 許多猜想就會有明顯的答案。舉例來說, 有個我懸賞一千元的猜想, 是關於二項式係數的中間項 $\binom{2n}{n}$, $2n$ 取 n; 在巴斯卡三角形, 它是每一行的中央項。這一項始終是偶數 (這很容易證明)。有個問題是: 二項式係數的中間項 $\binom{2n}{n}$ 是否和 3 互質? 例如當 $n=3$ 時, 也就是 6 取 3, 結果爲 20。嗯, 它會和 5 爲互質嗎? 再舉個例, 當 $n=7$, 也就是 14 取 7, 等於 3432, 與 5、7 互質。這個值 \$1000 元的問題是: 對於 $2n$ 取 n, 是否有無限多個 n, 使得 $\binom{2n}{n}$ 和 3、5、7 都互質? 換句話說, 它和 105 互質。我想答案是肯定的。

理由如下述。任取質數 p, 你或許會問: 二項式係數中間項 $\binom{2n}{n}$ 可以被 p 的幾次方整除? 嗯, 有個方式可得到答案。將 n 寫成 p 進位展式, 接著加 n, 這麼一加導致 p 增加的冪數, 就是整除 $\binom{2n}{n}$ 的 p的冪數。意即, $\binom{2n}{n}$ 不被 p 整除, 若且唯若把 n 加上 n 時 p 的冪數未增加; 此時, n 以 p 爲基底展開的各個係數, 都小於 $p/2$; 譬如, 當你把 n 寫成 3 進位, 係數只會是 0 或 1; 寫成 5 進位, 係數只會是 0、1 或 2; 寫成 7 進位, 係數只會是 0、1、2、3。那麼, 這三件事會同時發生嗎? 想像你用 3 進位和 5 進位寫一個很大的數字, 它們的係數應該互不相關 (可能會相關嗎?) 你可以用機率估計: 有多少個不大於 x 的 n 會讓上述三件事同時發生。答案約爲 x 的 0.01 次方。冪數爲正的事實告訴你, n 應該有無限多, 但沒有人能證明這答案。

Erdős、Rusza 和我證明了這種狀況會發生於任意兩個質數。那麼, 對 3、5、7、11 這四個質數呢? 現在你進行相同的機率計算, 比 x 小且與這四個質數都互質的數, 個數是 x 的負數次方 (此負數很小), 因此其個數是有限的。3160 似乎是最大的了。至少到 10 的 10000 次方, 它是最大的, 在 3160 到 10^{10000} 之間沒有其他的, 所以 3160 大概是最大的。如果你相信它們的行爲具有類隨機性, 則理應如此。但如果你試圖證明它, 情況可能與正規數[35](normal numbers) 的證明相若。數字 n 對 b 進位是正規的, 若且唯若 b 進位的所有可能數字都 (漸近地) 出現相同的次數, 更一般地說, 對所有 k, b 進位的所有可能數字

[34]Donald Ervin Knuth (1938∼), 出生於美國, 史丹福大學電腦系榮譽退休教授, 對演算法的複雜度理論有重要貢獻, 且曾發明排版軟體 TEX。1974 年獲頒圖靈獎。

[35]數字隨機分布且每個數字出現機會均等的實數。

在所有 k-元組 (k-tuple) 都 (漸近地) 出現相同次數。絕對正規數 (abosolutely normal number) 是那些對每個 b, 它的 b 進位都是正規的數。幾乎所有數字都是絕對正規, 但沒人可確實舉出一個實際例子。這顯示我們還有很多東西要了解。

劉: 這就像幾乎所有數都是超越 數, 卻很難證明特定一個是如此。

葉: 隨機的事物廣受關注。我聽說你正在研究準隨機性 (quasi-randomness); 那是什麼?

G: 對於行爲類同隨機事物的對象, 你樂於找到它們的明確構造, 但如果你可以建構出它們, 就會更了解它們的性質。若以 1/2 的機率決定各對頂點是否以邊相連, 會形成一個圖, 而後你幾乎可確定某些事情。舉例來說, 如果你著眼於一半的頂點, 那麼你預期多少邊會形成呢? 沒錯, 你會預期半數的邊出現。或者, 你考慮其鄰接矩陣 (adjacency matrix), i 頂點和 j 頂點有邊相連時 (i, j) 爲 1, 否則 (i, j) 爲 0。接著你觀察其特徵值; 對稱矩陣特徵值爲實數, 所以最大的特徵值大約是 $n/2$, 而其他特徵值爲 $o(n)$。

這是準隨機性。有幾十個這類性質是等價的; 你的圖如果具備其中一個性質, 必定也會有其他所有性質。這種行爲很像隨機圖 (random graph)。Szemerédi[36] 正則性引理 (regularity lemma) 說的其實是: 你把任意一個圖分解成有限數量的子圖, 而後任取兩個子圖, 它們組成的二分圖 (bipartite graphs) 幾乎可以確定是準隨機的。

2017年, Simons 計算理論研究所 (Simons Institute for the Theory of Computing) 舉辦擬隨機 (pseudo-randomness) 和準隨機 (quasi-randomness) 的特別半年, 我和金芳蓉都在那裡 ⋯

劉: 在何地?

G: 柏克萊。

劉: 嗯嗯, MSRI[37]?

G: MSRI 在山上, 而這是校園內的新大樓。很高興去年能待在那裡幾個月! James Simons[38] 是我在柏克萊的同學。他賺了大錢, 大量回饋給數學。有個很好的線上雜誌 Quanta, 你們讀過嗎? 那是 Simons 基金會發行的, 刊登數學、物理、生物等學科的好文章和人物訪談。

劉: 看得出來你從數學中得到許多樂趣, 非常好!

G: 如果它無趣, 何必做它? 是吧? 我告訴學生, 無論你選擇什麼爲職業, 最好確實喜歡它; 因爲不論你選擇了什麼, 都將長時間從事它。

---

[36] Endre Szemerédi(1940∼), 任教於 Rutgers 大學, 2012 年獲 Abel 獎。他對組合數論、重合幾何及圖論都有重大貢獻。以他命名的 Szemerédi 正則性引理, 在理論電腦科學界廣被使用。

[37] 全名是 Mathematical Sciences Reasearch Institute, 位於美國加州柏克萊。

[38] James Harries Simons (1938∼), 曾與陳省身提出三維流形的 Chern-Simons 特徵類, 1982 年轉行成立 Rennaisance Technology, 運作對沖基金, 身家財產達數十億美元。

你讀過 ICCM[39] Notices 嗎? 幾年前, 我首次在那裡發表文章。
許多演講內容經年累積, 而後再參酌最近的成果。譬如談到張益唐, 目前確認的質數間隙 (prime gap) 已降至 246, 但上次我給演講時是 270, 所以昨天改成 246。有個網站會登載當前記錄。再如當前所知的最大質數[40]是 $2^{77,232,917}-1$, 這似乎每隔幾年就會改變。

劉: 有些猜想, 在直觀上很容易掌握, 感受上又令人興奮, 譬如孿生質數猜想, 你可以講給任何懂乘法表的人聽。基本上, 還有其他需要花時間解釋的猜想。你提到未來的數學研究, 其中一項或可倖存的, 我想是易於解釋又讓人興奮的猜想, 它們顯然會讓人振奮。譬如孿生質數, 或是 Goldbach 猜想: 任意大於 2 的偶數都是兩個質數的總和。

葉: 沒錯, 兩個質數的總和。

G: 每個大於 2 的數。最近的結果才剛證明, 每個大於 5 的數都是三個質數的總和。衆人持續推動進展, 不過要搞定孿生質數, 我認爲需要更多東西。
我喜歡張益唐的故事。我剛從維基百科得知他現在是 Santa Barbara 的教授。有部關於他人生的電影, 非常不錯, 一小時而已, 很平靜, 我喜歡。他的夫人在加州, 非常活躍又愛跳舞。我倒不覺得張益唐是個愛跳舞的人。

劉: 我想我們可能要就此打住, 我們聊了一個半小時, 很有意思, 非常感謝你。希望不久的將來在台北見到你。

—本文訪問者劉太平任職中央研究院數學研究所, 葉永南任職中央研究院數學研究所—

[39]世界華人數學家聯盟 (International Consortium of Chinese Mathematicians)。

[40]截至 2019 年一月, 最大已知質數爲 $2^{82,589,933}-1$。