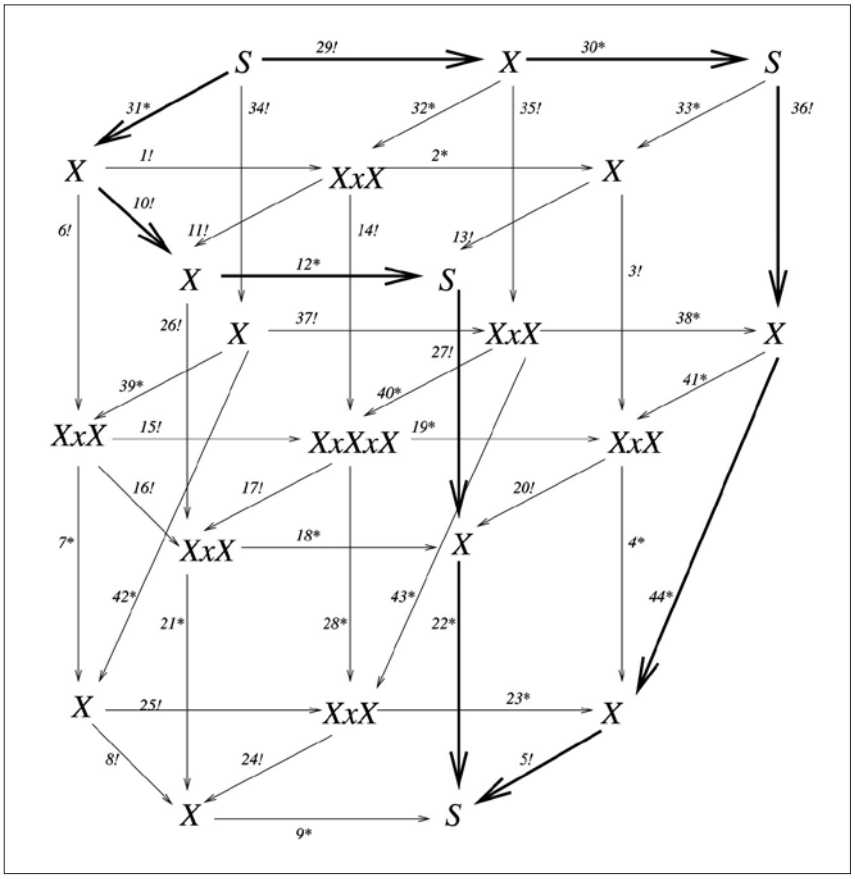
數學需要電腦與新數學基礎

用電腦輔證數學證明才能避免犯錯

作者：**渥伊沃茨基 Vladimir Voevodsky**　譯者：**周樹靜**

渥伊沃茨基是俄羅斯代數幾何學家，2002 年成為普林斯頓高等研究院教授。他以代數解形同倫理論與模諦上同調理論的研究獲得 2002 年的費爾茲獎。



渥伊沃茨基必須使用圖中三維圖式這類「公式」，才能支撐他 2 理論裡的論證。

格羅騰迪克（Alexandre Grothendieck）1984 年 1 月向法國國家科學研究中心（CNRS）遞交了名為〈計畫要覽〉（Esquisse d'un Programme）的研究計畫。這份文件的複印本很快在數學家之間流傳起來。幾個月後，作為莫斯科大學的第一年研究生，我也從沙巴（George Shabat）那裡拿到一份，他是我的第一位科學導師。為了閱讀這份文件，我還特地去學法文，之後就開始研究文件中所描繪的一些觀念。

1988 或 1989 年時，我遇到卡帕拉諾夫（Michael Kapranov）。我們受到範疇與 2- 範疇（2-categories）的理論啟迪，都被在數學裡發展新「高維」物件的想法強烈吸引。我們合作發表的第一篇論文是〈以 ∞ 廣群作為同倫範疇的模型〉（∞ -Groupoids as a Model for a Homotopy Category）。就格羅騰迪克連結兩類數學概念——∞ 廣群（∞ -Groupoid）與同倫型（homotopy type）——的想法，我們宣稱給出了嚴格的數學表述與證明。

之後我們決定將類似的想法應用到當時頂尖的數學問題，構造類似上同調理論的模諦上同調（motivic cohomology）理論，這個理論的存在性猜想來自 1987 年貝林森（Alexander Beilinson）、麥克弗森（Robert MacPherson）與謝特曼（Vadim Schechtman）合寫的論文。

1990 夏天，在卡帕拉諾夫的安排下，我不需申請直接進入哈佛大學的博士班。不過他當時人在康乃爾，幾個月後，我們的數學道路就開始分歧。我專心研究模諦上同調理論，後來更著重於模諦同倫論（motivic homotopy theory）。在我 1991 年 3 月 29 日的筆記上，一開頭就寫下這個問題：「代數解形（algebraic variety）或概形（scheme）的同倫論是什麼？」

渥伊沃茨基正在演講「如果目前的數學基礎並不一致？」（What if Current Foundations of Mathematics are Inconsistent?）。這是 2010 年高等研究院慶祝數學所和自然科學所 80 週年的演講。（Cliff Moore 攝，感謝 IAS 提供）

險象環生的錯誤

當時許多人認為模諦上同調這個領域還相當空泛，缺乏堅實的基礎。1986 年布洛克（Spencer Bloch）的突破性論文〈代數閉鏈和高階 K 理論〉（Algebraic Cycles and Higher K-theory）出版後，蘇斯林（Andrei Suslin）很快就發現其中引理 1.1 的證明有錯，而且這個錯誤無法修正，因此整篇文章大部分的宣稱便缺乏支持的根據。

一直到 1993 年，新證明才公諸於世，並將原文的一個段落，換成 30 頁左右的複雜論證。然後還要再經過許多年，才被接受是正確的。有趣的是，新證明是基於史匹瓦科夫斯基（Mark Spivakovsky）的舊結果。而史匹瓦科夫斯基大概就在那時，發表了奇點分解（resolution of singularities）猜想的證明。此後數年裡，大家都相信史匹瓦科夫斯基奇點分解證明的正確性，後來才發現錯誤，目前這個猜想依然未解決。

我和蘇斯林、弗萊蘭德（Eric Friedlander）一起發展的模諦上同調進路，則避開布洛克引理，改運用我論文〈具轉移之預層的上同調理論 〉（Cohomological Theory of Presheaves with Transfer）的結果。這是我 1992-1993 擔任高等研究院研究員時的研究。到了 1999-2000 年，也是在高等研究院裡，我有一系列演講機會，數學所教授德利涅（Pierre Deligne）幫我記錄並檢查每一道步驟。直到那時，我才發現論文中有個關鍵的引理證明有誤，而且就該引理的字面敘述是無法挽回的。幸好我能夠證明一個比較弱但更複雜的引理，結果足以應付所有的應用。這一系列修正過的論證發表於 2006 年。

這段往事把我嚇壞了。因為打從 1993 年開始，就有許多組數學家在各討論班內研究我的論文，並運用於他們的研究，但是卻沒有一個人注意到這項錯誤。很顯然這不是偶發事件。由可信任的作者給出的專業論證，如果既不易檢查，看起來又類似已知的正確論證，就幾乎沒有人會去檢查細節。不過，這並不是數學文本中錯誤持續存在的唯一問題。

1998 年 10 月，辛普森（Carlos Simpson）在 arXiv 預印本網站遞交一篇名為〈嚴 3 廣群的同倫型〉（Homotopy Types of Strict 3-groupoids）的論文。他宣稱文中有段論證，足以推翻我和卡帕拉諾夫 1989 年「∞廣群」論文的主要結果。但是，先前卡帕拉諾夫和我已經自行考慮過類似的批評，並且彼此確信這樣的疑問並不成立。我很確定我們是對的，一直到 2013 年秋天（！！）。

對於這個令人訝憾的局面，我覺得有兩個因素致此。辛普森所宣稱的是他構造了一個反例，但是他無法指出我們的錯誤所在。因此，到底是我們的論文某處有誤，還是他的反例有錯，情況並不明朗。近來的數學研究依賴一個基於名聲的複雜互信系統。在辛普森論文出現時，卡帕拉諾夫和我都已有深厚的名望。辛普森的論文激起對我們研究的懷疑，導致其他研究人士不再運用我們的結果。但是卻沒有人接近我們直接質疑。

電腦輔助的需求

大概在我發現模諦論文錯誤的時候，我正在發展一種新理論，稱為 2- 理論（2-theories）。在我研究這些概念的過程裡，卻逐漸無法確定該如何繼續進行。2- 理論中的數學，正是卡帕拉諾夫和我 1989 年所夢想的那種高維數學的範例。我真的很喜歡發現這類並非出自低維推廣的新結構。

但是想在我認為必要的嚴格與精確層次進行研究，需要耗費大量的精神，寫出來的文章也難以卒讀。而且如果連在更簡單論證裡的錯誤都要耗上好幾年才被發現，誰能擔保我有沒有漏掉什麼，有沒有犯錯？我想就是在這個時刻，我大量停止了所謂的「基於好奇的研究」，開始嚴肅思考未來的對策。因為我缺乏工具去探索好奇心帶領我前往的領域，探索我認為有價值、有趣又優美的課題。

於是我開始研究要如何發明這樣的工具，很快我就明白，唯一的長期解決方案，就是盡可能運用電腦來檢驗我那些抽象、邏輯、數學的構造。從 1960 年代，可以執行這類工作的軟體就已經開始發展，但是到 2000 年左右，在我尋求實用的證明輔助工具時，卻找不到任何可用的軟體。當時有好幾個團隊正發展這類系統，但是沒有任何一個適合我這類數學理論。

當我開始摸索這些可能性時，電腦證明檢驗（computer proof verification）在數學家之間是近乎禁忌的話題。關於電腦證明輔助的話題，總是流向哥德爾不完備定理（這跟實際問題毫不相干），或是現存證明檢驗的一兩個案例，但其目的只是要展示這整個想法有多麼不實際。

渥伊沃茨基在午餐談笑。攝於 2014 年春。（Andrea Kane 攝，感謝 IAS 提供）

只有少數數學家，持續在數學界嘗試推動電腦檢驗，像是赫爾斯（Tom Hales）和辛普森。但是今日，才相隔幾年之後，對許多研究單型數學基礎（univalent foundations）與同倫型論（homotopy type theory）的人來說，以電腦檢驗證明或更廣泛的數學推理，似乎已經是完全實際可行的方法。

其中，我必須提出的主要挑戰論題是，現在的數學基礎並不足以應付這項工作的需求。以電腦能理解的精確語言來表述數學推理，意味著所用的數學基礎系統不只是建立幾項基礎定理的一致性標準，而是要成為日常數學研究能夠使用的工具。

如今的數學基礎系統有兩個不恰當的缺陷。首先，現在的數學基礎是基於謂詞邏輯（predicate logic），但這類語言有很大的侷限。其次，現存基礎系統無法直接表述某些如我 2- 理論研究中的敘述。

儘管如此，一般人很難接受數學需要全新基礎的想法。即使許多與推動同倫型論有關的學者，也還在和這個想法奮鬥。箇中理由很充分，因為現在的數學基礎—— ZFC ◐ 和範疇論——非常成功。克服想把範疇論當作新數學基礎候選理論的籲求，就我個人而言是最大的挑戰。

故事得從 ZFC 說起。自從 20 世紀前葉開始，數學就已經被目為基於 ZFC 的理論，而 ZFC 則是謂詞邏輯中的特殊理論。因此，想要理解數學基層的人有一條簡單的路徑——先學謂詞邏輯，接著是稱

在午餐討論會中的渥伊沃茨基，右為歷史所退休教授 Jonathan Israel。（Dan Komoda 攝，感謝 IAS 提供）

為 ZFC 的特殊理論，再學習如何將包含幾個基本數學概念的命題轉換為 ZFC 中的公式，然後透過一些範例，學著相信剩下的數學都可以化約到這些少數的數學概念。

這種情勢讓數學獲益甚大，也是讓抽象數學在 20 世紀能獲得巨大成功的真實理由。但從歷史來看，ZFC 的第一個困難，顯現於早期布巴基學派（Bourbaki）大業的衰頹。這個現象起因於 20 世紀後葉，數學的主要組織性概念轉以範疇論為基礎，然而以 ZFC 來呈現範疇論並不妥適。範疇論的成功鼓舞了把「範疇」視為「下一個維度的『集合』」的想法，而新數學基礎則應該是基於範疇論或者它更高維度的類比理論。將範疇視為「下個維度的集合」的想法，正是我最大的絆腳石。

當我理解上述想法其實是錯誤的當下，那種突破性的感受體驗，至今仍歷歷在目。範疇不是「下個維度的集合」，而是「下個維度的偏序（partially ordered）集合」，正確的「下個維度的集合」是廣群（groupoid）。這個關於「廣群」與「範疇」的新觀點，讓我自己調適了好一陣子。因為我記得教我數學的人經常強調，格羅騰迪克代數幾何進路之所以如此成功的原因之一，是他和老學派決裂，堅持考慮所有態射（morphism）的重要性，而不是只考慮同構（isomorphism，可逆的態射）。❷

催生新數學基礎

單型數學基礎比較像基於 ZFC 的數學基礎理論而非範疇論，它是一個完備的數學基礎系統，但是又和 ZFC 非常不同。為了提供比較的準則，我得先預設適合人類推理與電腦驗證的數學基礎理論，必須包含底下三項要件。

第一項要件是形式演繹系統（formal deduction system），包括一個語言與處理該語言語句的規則。其中這些規則必須是純粹形式的，如此電腦才可以檢驗這些語句的處理紀錄。第二項要件是某種結構，藉由人類可理解的心智物件，提供這個語言中語句的意義所指。第三項要件是某種結構，讓人類能將數學概念藉以編碼成與語言直接相連的物件。

在ZFC數學基礎裡。第一項要件有兩個「層次」，第一層是稱為謂詞邏輯的一般演繹系統；第二層則是稱為 ZFC 的特殊演繹系統，將第一層的謂詞邏輯應用於一組運算與公設。ZFC 的第二項要件是基於人類能直覺理解的階序（hierarchy），事實上 ZFC 的公設可以視為所有階序都滿足的性質，再加上假設存在無窮階序的無窮公設。ZFC 的第三項要件是將數學概念藉由階序加以編碼的方法，首先是將集合數學性質編碼的規則。這正是通常稱 ZFC 為集合論的原因。

---

❶ 譯註：ZFC 是廣被接受的數學基礎系統縮寫，ZF 表示哲美羅 / 弗蘭科集合論（Zermelo–Fraenkel set theory）公設系統，C 則表示選擇公設（axiom of choice）。

❷ 廣群和範疇都包含集合層次的對象（object），但廣群要求對象間的同構，而範疇則只要求對象間的態射。

單型數學基礎的原初形式演繹系統稱為歸納構造演算（calculus of inductive construction，簡稱 CIC）。這是柯康（Thierry Coquand）和林尼（Christine Pauline）在 1988 年左右發展的理論，其根據是關連到構造數學（constructive mathematics）概念的電腦語言中一些理論和實務想法的組合。和這些想法有關的關鍵人士包括德布倫（Nicolaas Govert de Bruijn）、馬丁洛夫（Per Martin-Löf）、吉哈德（Jean-Yves Girard）。證明輔證工具 Coq 的形式演繹系統就是直接傳承自 CIC。

單型數學基礎的第二項要件——提供 CIC 語句直接意義的結構——是以單型模型（univalent model）為本的結構。單型模型中直接關連到 CIC 語句意義的物件稱為同倫型（homotopy type）。同倫型的世界分成許多層次，稱為 h 層級（h-levels）。其中，h 層級 1 的同倫型對應到邏輯命題，h 層級 2 的同倫型則對應到集合。而我們對於更高層級同倫型的直覺，大部分來自它們與多維度形體的連結，在 ZFC 數學裡，這些已經被研究了數十年。

單型數學基礎的第三項要件——將一般數學概念藉由同倫型來編碼的方法，奠基於反轉格羅騰迪克在 1970 年代末的想法，我們曾在「∞廣群」那篇文章討論過。就數學和哲學兩方面來看，這都是整個故事中最深刻，卻也最乏人理解的部分。

從 2005 年開始，我就開始發展這些想法，從而發現了單型模型。我對這項主題的首次演講發表於 2009 年 11 月德國慕尼黑大學（Ludwig-Maximilians-Universität München，LMU）。當我在獨立研究我的模型時，這個方向的進展其實最早在 1995 年就已出現，相關的研究學者包括賀夫曼（Martin Hofmann）、史采策（Thomas Streicher）、歐代（Steve Awodey）、華倫（Michael Warren）。2010 年春，我建議高等科學院數學所，在 2012-2013 年度由我籌組一個研討數學新基礎的特別計畫。儘管這個領域是否能成熟到配合這項計畫，當時其實還在未定之天。

現在的我研究數學時會使用證明輔助工具。對於這個證明輔助工具，我有許多想法，希望它能運作得更好。但是，至少現在我不必回家後還要擔心研究有錯。我知道一旦我做出什麼，那就是對的，我既不用回頭考慮這些問題，也不用煩惱自己的論證太複雜，不必憂心如何讓別人信服論證是正確的。我只要信任電腦就可以。電腦科學領域裡有很多人為這個程式做出貢獻，但是大部分數學家還不相信這是個好主意。我認為他們錯得離譜。

我要感謝所有試著理解單型數學基礎想法的人、發展這些想法的人，以及嘗試傳播這些想法的人。

本文出處

本文出自渥伊沃茨基 2014 年 3 月的演講 " Univalent Foundations: New Foundations of Mathematics"。並發表於 2014 年夏的 *The Institute Letter*（《研究院簡訊》）。網頁版可見

https://www.ias.edu/ideas/2014/voevodsky-origins

錄影網頁為

https://video.ias.edu/voevodsky14/

譯者簡介

周樹靜為臺灣數學科普譯者。

延伸閱讀

▶ Hartnett, Kevin “Will Computers Redefine the Roots of Math?”。這是 *Quanta* 雜誌 2015 年 5 月 19 日關於這個主題的科普報導。

https://goo.gl/HFtiMK

▶作者用的程式 Coq，可以在下面網頁找到：https://coq.inria.fr

他們使用與撰寫中的主程式庫是 UniMath：https://github.com/UniMath

▶ Univalent Foundations Program, *Homotopy Type Theory: Univalent Foundations of Mathematics*（2013）, https://homotopytypetheory.org/book。本文中提到的 2012-13 年高等研究院特別計畫，結果號召了 24 位數學家（即作者群 Univalent Foundations Program），以不到半年的時間寫下這部 600 頁的大書。可以各種形式閱讀：

http://homotopytypetheory.org/book/

渥伊沃茨基答客問

渥伊沃茨基熱心回答譯者的疑問，翻譯於下以饗識者。

問：為什麼用 univalent 這個詞作為新基礎命名？我理解這應該和「一」有關，但我想知道採用這個詞的脈絡。

答：univalent 本來是宇系（universe）恆真纖形（tautological fibration）的性質。其意義大致如下，在恆真纖形裡所有對象都恰為纖維一次。但在代數幾何裡有所謂「多泛纖形」（versal fibration）的概念，意指所有對象至少成為纖維一次。而我需要一個詞描述另一類纖形，其中所有對象至多成為纖形一次。於是我採用 univalent 這個詞，稱之為單型纖形。後來我發現，老一代俄文著作曾用這個詞翻譯如今稱為「忠實函子」（faithful functor）的概念，稱為單型函子，這讓「單型」和「忠實」兩詞產生關聯。

一些數學家知之甚詳的理論裡，則認為需要建立「不變」基礎理論（invariant foundation）。馬凱（Michael Makkai）1995 年的論文〈具依賴類的一階邏輯〉（First order logic with dependent sorts，FOLDS）清楚表達這個概念。

就固有數學習慣，univalent 這個詞當然和「不變」有關。如果要我以簡單刻畫單型基礎，我會這樣說—任何在其形式語言中能表述的語句，在某種意義下，就是在該語句所指所有對象之等價關係下是不變的。

問：文中提到「……而我們對於更高層級同倫型的直覺，大部分來自它們與高維形體的連結。」什麼是古典高維形體的具體例子，高維流形或解形是例子嗎？

答：「高維形體」的確是針對幾何意義而言，也就是能在高維空間產生的幾何形體。數學家有豐富的知識，知道如何以同倫等價（homotopy equivalence）分類這些形體。正是這些知識啟發我們對高階 h 層級的直覺。只是同倫結構簡單的形體，可能具有無窮幾何維度（如無窮維歐氏空間），而低維形體則常常具有複雜同倫結構（如二、三維球面等）。因此出現在單型範疇論中相對簡單的型（type），其幾何表現維度可能是無窮的。但即使是這種表現，往往還是能提供有用的直覺。

問：在單型基礎系統中，「排中律」（law of excluded middle）的地位如何。這樣問是因為文中提及形式演繹系統 CIC，至少字面上和「構造數學」（constructive mathematics）有關。是否得加入什麼才能保住古典數學？

答：CIC 的確是構造的，包括我最常使用的形式數學 UniMath 程式庫也是。若要將古典數學形式化，可以把排中律當作公設加入。事實上，正是因為有了 h 層級的概念才讓這些變成可能。因為在我們的理論裡，h 層級 1 扮演了命題（或「真值」）的角色，因此可以放心在這些類型中加入排中律，不會造成理論矛盾（當然是相對於 ZFC 的一致性）。我們也可以在扮演集合角色的 h 層級 2 類型中加入選擇公設。

令人驚訝的是，我們可以把許多有趣的數學形式化，卻完全不需要引入排中律或選擇公設。