機器證明的回顧與展望

張景中
中國科學院成都計算機應用研究所

編輯室註：本文係九月十七日張景中教授在國立台灣師範大學數學系講稿，並獲張教授同意本刊發表。

機器證明及其應用，是我國攀登計劃項目之一。項目核心內容主要是幾何定理機器證明和非線性代數方程組理論、算法和應用。實際上，機器證明研究領域的範圍要廣泛得多。在國外更一般地叫做自動推理。我們把幾何定理機器證明和非線性代數方程組作爲主攻方向，一方面是因爲吳文俊先生在七十年代的突出工作，使我國在此方向有領先的優勢；另一方面，這兩個方向有鮮明的應用背景，近年來在機器證明領域也確是十分活躍，值得重視。本文只涉及這兩個方向，特別是幾何定理的機器證明。

由於傳統的興趣和多種原因，幾何定理的機器證明在自動推理的研究中占有重要的地位。近二十年來，幾何定理機器證明的研究和實踐有了很大的進展。

從古老的夢想到驚人的突破

能否建立一個通用的幾何解題方法，成批地解決問題，以至萬理一證，是歷史上一些卓越的科學家的夢想。

爲此，笛卡爾發明了坐標系；萊布尼茲設想過推理機器；希爾伯特在其名著《幾何基礎》中給出了一類幾何命題的機械化定理。電子計算機的出現推動了數學機械化。五十年代，塔斯基用代數方法證明了初等幾何的機械化的可能性。到六十年代，斯拉格和莫色斯實現了符號積分，代數與分析計算問題的機械化已經初具規模，而幾何定理的機器證明看來仍遙遙無期。接著，格蘭特等提出用邏輯方法建立幾何推理機，科林斯等改進了塔斯基的代數方法。直到1975年，仍找不到能用計算機判定非平凡幾何命題的有效算法。正當這一領域的熱情由於發展緩慢而趨於冷落之際，吳文俊方法的提出[W77]，給定理機器證明的研究帶來勃勃生機。用吳法可在微機上很快地證明困難的幾何定理。周咸青發展了吳法並把它實現爲有效的通用程序，證明了512條非平凡定理，寫成英文專著[C88]。這一進展是自動推理領域一大突破。被國際同行譽爲革命性的工作。

從機器判定到可讀證明的自動生成

吳法的成功使一度冷落的幾何定理機器證明研究活躍起來。用代數方法證明幾何定理的方向受到重視。新的代數方法接連出現。在國外，周咸青等提出了用Grobner基方法構作幾何定理機器證明的算法和程序並得到成功[CS86]。在國內，洪家威提出了單點例證方法的理論設想，但因複雜度太大不能實現[H86]。張景中、楊路則提出數值並行方法，在低擋微機（甚至計算器）上實現了非平凡幾何定理的機器證明和機器發明[ZYD90]。數值並行方法的優點是所需內存極小，且易於並行化。所有這些方法都屬於代數方法。它們的提出和實現豐富了幾何定理機器證明的研究。但與吳法相比，沒有大的新突破。

代數方法不能使人滿意的是，它所給出的〝證明〞是關於大多項式的繁複的計算，人難於理解其幾何意義，也難於檢驗其是否正確。能否讓計算機生成人能理解和易於檢驗的簡明巧妙的證明，所謂可證明，是對自動推理和人工智能領域的一個挑戰性的課題。一些著名的科學家認爲，機器證明的基本思想是以量的複雜取代質的困難，這就很難想像用機器生成可讀證明。國外一些學者從60年代即致力於幾何定理可讀證明自動生成的研究，三十多年來進展不大，未能給出哪怕是一小類非平凡幾何定理的機器證明的有效算法和程序。

作者以他多年所發展的幾何新方法爲基本工具，並提出了消點思想，和周咸青、高小山合作，於1992年突破了這一困難，實現了幾何定理可讀證明的自動生成[CGZ94]，這一新方法既不以坐標爲基礎，也不同於傳統的綜合方法，而是一個以幾何不變量爲工具，把幾何、代數、邏輯和人工智能方法結合起來所形成的開放系統。它選擇幾個基本的幾何不變量和一套作圖規則，並且建立一系列與這些不變量和作圖規則有關的消點公式。當命題的前提以作圖語句的形式輸入時，程序可調用適當的消點公式把結論中的約束點逐個消去，最後達到水落石出。消點的過程紀錄與消點公式相結合，就是一個具有幾何意義的證明。此算法對可構造等式型幾何命題的是完全的，但其應用範圍不限於這一類命題。基於此法所編的程序，已在微機上對數以百計的困難的幾何定理完全自動地生成了簡短的可讀證明，其效率也比其他方法爲高。隨所用的幾何量的不同，它能生成面積法、向量法、複數法和全角法等多種風格的證明，也能用於立體幾何。楊路、高小山、周咸青與作者合作，把消點法用於非歐幾何可讀證明的自動生成也得到成功，並得到一批非歐幾何新定理。消點法也可用於幾何計算和公式推導。基於幾何量和消點思

想的新原理的建立，像是打開了幾何定理機器求解的一個礦床。它也使幾何定理機器證明的成果在數學教育中的應用有了現實可能。這一成果被國際同行譽爲使計算機能像處理算術那樣處理幾何的發展道路上的里程碑，是自動推理領域三十年來最重要的工作。

在多數情形下，消點法也可用筆紙證明不平凡的定理。它結束了兩千年來幾何證題無定法的局面，把初等幾何解法從四則雜題的層次推進到代數方程的階段。

機器證明與人工證明媲美的新階段

但是，比起人類在幾千年間積累起來的豐富多彩的幾何知識來，計算機目前所能做的仍是十分有限。應當把幾何學家所掌握的方法更多地〝教給〞計算機，使計算機產生的解決可以與幾何學家相比。爲此，要分析幾何學家有哪些解題方法，計算機已經學會了哪些，以確定下一步應當做什麼和如何做。幾何學家常用下列四種手段：

W1. 檢驗：對具體圖形作觀察和計算，以確信命題爲眞。

W2. 搜索：依據常用的引理和已知條件去找尋題圖中更多的幾何性質。這樣做如達不到目的。得到的訊息就是進一步工作的基礎。

W3. 歸約：從結論出發，利用已知訊息消去依賴的幾何量或幾何元素，使結論的眞假趨於顯然或易於檢驗。

W4. 轉化：改變命題的形式。如幾何變換、反證法、輔助線等。

手段W1的機器模擬已經實現。手段W3的機械化研究得到了最大的成功。吳法、GB法、面積法和向量法均屬此類。手段W4充分體現了人的思維活動的靈活性與豐富性，尙難以機械化。手段W2，搜索，是傳統幾何證明活動中的常規方法，是歸約的補充和轉化的基礎。我們基於前推模式設計並實現了一個〝幾何訊息搜索系統〞(GISS)。由於適當選擇幾何工具，合理組織數據和優化推理的過程，效果極好。文獻中曾提出的用搜索法處理涉及圓的命題，以及找出所有可能推出的幾何性質（達到推理不動點）的問題，均爲我們的算法完滿回答。我們的程序用C語言在NeXT工作站上實現，用於161個非平凡幾何命題，均在合理的時間內達到不動點，並能發現新定理，證得其它方法不能證明的結果(ZGC)。程序已具有添加某些輔助線的功能。

非線性代數方程組的研究

機器生成可讀證明的實現並不使代數方法失去價值。一些特殊問題及代數曲線、曲面的幾何問題仍需用代數方法。代數方法與非線性代數方程組的理論和符號求解密切相

關，有廣泛應用，是自動推理的一大熱點。數學、物理和工程技術中的許多問題，歸根結底要靠解代數方程組。線性方程組還好辦，非線性方程組就成了難關。特別是非線性方程組的符號求解，更難，理論上也更重要。

對非線性代數方程組的研究，十九世紀就提出了各種結式方法。由於結式法涉及大行列式的計算，算不動，研究就冷下來。本世紀有了計算機，人們又研究新的算法。在60年代，國外提出了GB法和Ritt方法。GB方法是完全方法。Ritt方法經吳文俊先生改進後，也成了一種完全方法，叫Ritt-Wu方法，在我國簡稱吳法。（把Ritt-Wu方法用於幾何定理的機器證明，也叫吳法。國外有人把機器證明的吳法，叫做Ritt-Wu方法，是不確切的。Ritt和幾何定理機器證明沒有關係。）兩個方法哪個更好，目前還沒有定論。用於幾何定理機器證明，吳法確實比GB法強。我國學者還用吳法解決了許多重要問題，涉及理論物理、微分方程、樣條理論和機器人。

雖已有了吳法、GB法等優秀的完全方法，但是道高一尺，魔高一丈，更難的問題要求更有力的新方法。近年來國外一再提出新的思路和算法，歐共體還投資數百萬美元組織項目專門研究非線性代數方程組的解法，但均無突破性進展。

最近，基於我們在[ZY89]中提出，在[ZYH89, ZYH93, 竹ZYH95]等文中加以完善的新的理論和算法—結式矩陣法，符紅光編寫了代數方程組符號求解和機器證明MAPLE程序。新算法的特點是：

⑴是非線性代數方程組符號求解和相容性判定的完全方法。

⑵不依賴於多項式的因式分解。

⑶用我們提出的弱非退化條件作零點分解，減少多餘分支。

⑷子結式計算與數值檢驗配合，進行大範圍消元。

⑸將所給方程組分解爲三角列，便於機器證明和最終求解。

經許多例子的演算，它比已知的各種方法有更好的效果[YZH]。此法能在PC486機上解六量循環方程，反解各種類型的六關節機器人問題，這是其它方法做不到的。

非線性代數方程組研究的又一新進展是楊路等提出的實系數代數方程的判別式系統[YHZ95]。這不但徹底解決了幾世紀懸而未決的關於代數方程一個基本問題，也使幾何不等式機器證明的難題得到了突破。楊路等最近所寫的程序，能快速地證明許多幾何不等式，根據已給條件推出幾何不等式，並已改正和改進了國外一些關於幾何不等式的結果。

展望與建議

預計在未來十年中初等幾何等式型問題的機器求解將基本完成，並進入實用階段。在前述成果的基礎上，會出現新的熱點：

⑴在幾何定理可讀證明自動生成工作的影響下，用幾何不變量爲工具進行機器求解的研究會有新的進展。例如作圖的機器求解、幾何推理數據庫的研究及微分幾何可讀證明的研究。

⑵幾何不等式的機器求解，會隨著實代數研究的進展而出現新的突破。

⑶非線性代數方程組的理論與算法，仍將是熱點。結式法和插值方法等利於並行的算法會得到更多重視。

⑷微分多項式的機器推導研究將得到開展。

⑸機器證明的成果，特別是非線性代數方程組理論與算法的研究成果，將在數學、物理和工程技術中得到更多的應用。

目前，在幾何定理機器證明方面，我國處於國際領先地位。在非線性代數方程組研究領域，競爭激烈，我國已進入先進行列，但還不能說領先。在數學機械化軟件開發方面，由於起步晚，隊伍小和資金不足等原因，我國遠不及歐美先進國家。我們不應滿足於某些方向上的領先地位。在繼續進行幾何定理機器證明研究，保持領先的同時，要把力量集中到非線性代數方程組的方向上來，特別應加強對實用而有效的算法的研究。數學機械化推廣應用方面，也應投入力量，發揮我們理論與算法方向的優勢，在軟件開發方面趕超先進。在幾何定理機器證明成果的基礎上，開發高智能的教育軟件和自主版權的符號演算數學軟件，爲我國科技教育事業做出貢獻。

參考文獻

[W77] 吳文俊，初等幾何判定問題與機械化證明。中國科學，7:507-516. 1977.

[H86] 洪加威，能用例證法證明幾何定理嗎。中國科學，16:225-233. 1986.

[ZGC] 張景中、高小山、周咸青，基於前推法的幾何訊息搜索系統。計算機學報（已接受，待發表）

[ZYH93] 張景中、楊路、侯曉榮：代數方程組相關性判準及其在定理機器證明中的應用。中國科學，23:1036-1042, 1993.

[ZYH95] 張景中、楊路、侯曉榮，幾何定理機器證明的結式矩陣法。系統科學與數

學，15:10-15 , 1995.

[YZH] 楊路、張景中、侯曉榮，《非線性代數方程組與機器證明》。上海科技教育出版社（待出版）。

[C88] S.C.Chou, Mechanical geometry theorem proving.
Dordrecht, Netherlands: d.Reidel Pub. Company, 1988.

[CS86] S.C.Chou & W.Schelter, Proving geometry theorem with rewrite rules, J. of Automated Reasoning 1986, 4:253-273.

[CGZ94] S.C.Chou, X.S.Gao & J.Z.Zhang, 《Machine Proofs in Geometry》. Singapore: World Scientific, 1994.

[YHZ95] L.Yang, X.R.Hou & Z.B.Zeng: A complete discrimination system for polynomials. IMS-70（數理科學），1995.

[ZY89] J.Z.Zhang, L.Yang: A method to overcome the reducibility difficulty in mechanical theorem proving.
IC/89/263, 1989.

[ZYD90] J.Z Zhang、L.Yang & M.K.Deng, The parallel numerical method of mechanical theorem proving. Theoretical Computer Science, 74:253-271. 1990.

[ZYH89] J.Z.Zhang, L.Yang & X.R.Hou: A note on Wu Wen-tsrn's non-degenerate conditions. IC/89/160, 1989.