计算机科学 1994 Vol. 21 No. 5

计算理论中的重大难题
——P=? NP

赵沁平
(北京航空航天大学 北京 100083)

计算理论研究各种计算模型、可计算性和计算的复杂性等计算的固有性质，是计算机科学理论研究的核心。可计算理论研究的基本问题是，什么是计算，什么是可计算和不可计算，它可以使我们精确地区分有算法的问题和没有算法的问题，从而可以在抽象意义上回答计算机究竟能干什么，不能干什么的问题。计算复杂性理论研究在可利用的空间和时间范围内完成计算的问题，也就是研究现实可计算性问题。可计算理论和计算复杂性理论从不同出发点研究计算问题，共同构成了计算理论的基础。

在计算理论中有一个著名的重大难题，即：P=? NP。这一难题几十年来吸引了众多的计算机基础理论科学家和数学家们为之奋斗，产生了一系列新概念，新思想和新方法，推动了计算机科学的成熟与发展，但是至今仍未得到解决，成为一个跨世纪的难题。

在计算理论中，多项式时间算法可求解的问题类称为P类，不确定性多项式时间算法可求解的问题类称为NP类，许多尚不知道是否属于P类的现实问题都属于NP类。如果NP类的所有问题都能有效地归约到NP类中的某一个问题，则称这个问题是NP完全的。这样，如果某一个NP完全问题确实在P类中，则P类和NP类重合，即P=NP。这一概念的巨大意义在于现已证明装箱、路径、调度等许多组合问题以及不同科学领域中的一大批问题都是NP完全的。如果对于NP完全问题中的任意一个找到多项式时间算法，则所有NP完全问题就都有多项式时间算法。

由于P=?NP问题的重要性，它一直受到数学家和计算机理论科学家们的高度重视，取得了一些影响深远的成果。特别是七十年代初希尔伯特第十问题的解决(不存在求解丢番图方程的通用判定过程)，Cook定理的发现(所有NP问题都可用多项式时间归约为可满足性问题)以及空间P-NP问题的解决(空间NP问题是多项式时间可解的)，使人们对计算复杂性有了更为深刻的认识，推动了计算理论和整个计算机科学的研究。

进入八十年代，在P=?NP问题的研究领域逐步形成了三个流派。一是坚持沿着传统概念(图灵机、图灵可计算等)研究P=?NP。提出了一些新方法，新思路。例如关于布尔线路下界的研究、多项式时间分层、多项式时间归约，交互式证明系统、one-way函数和程序复杂性等。

下界问题是复杂性理论中最本质而又是难度最大的问题。P=?NP长期未能得到解决从某种意义上说就是未能得到NP完全问题在计算时间上有超多项式下界。研究下界问题有多种模型，许多人认为布尔线路模型是其中最为理想的，在下界研究中，近年来有两项引人注目的成果。一是苏联学者Razeborov证明了完全子图问题(NP-完全问题)对于计算它的单调布尔线路具有指数下界。二是Yao对于深度有界而又不限宽度的布尔线路的研究，得到了一系列函数计算问题的指数下界，从而整个多项式分层在相对化意义下被全部分开。

多项式时间分层PH是从非确定的多项式时间类NP诱导出来的。对PH的结构以及PH同其它复杂性类之间的关系的研究是当前结构复杂性研究中的主要课题，并由其派生出一些相关问题。例如由于分离P和NP两个复杂性类存在巨大困难，人们转而考虑复杂性类之间的相对化分离。这类相对化的结果告诉人们，现有的证明技术和工具存在着很大的局限。在关于NP-完全问题的结构上，Berman和Hartmanis提出了所有NP-完全集都是多项式时间同构的猜想，这一猜想引起了广泛的研究，丰富了结构复杂性的内容。

归约同复杂性理论中的完全性概念交织地联系在一起，不同的归约很可能对应着不同的完全集类。所以归约既是联系不同集合的纽带，也是沟通复杂

赵沁平 教授，副校长。

性类的桥梁。目前，已经提出了许多种不同的归约，不同的归约呈现出不同的性质，它们在复杂性理论的研究中发挥着重要作用。

交互式证明系统是近几年发展起来的一种理论体系，它同密码学有着深刻的联系，零知识系统就是从这里引出的。利用这套理论工具有人证明了图同构问题不太可能是NP-完全的，否则PH将会倒塌。最近Shamir又证明了IP＝Pspace，这大大加深了人们对Pspace的认识。对交互式证明系统的研究又同伴随着随机算法出现的概率复杂性类交织在一起，深刻地利用了概率的理论和方法，扩大了计算理论的研究疆域。

one-way函数是这样一种函数，它是多项式时间算法可计算的，而它的逆函数是不确定性多项式时间算法可计算的。只要找到这样的函数，就可解决P＝？NP问题，这一方法提供了一种新的思路，但并未降低问题的难度。

程序复杂性又称为"描述复杂性"。这个方向起源于对有限字符串中所含信息量大小的度量，它从算法的角度找到了有限字符串中信息量的度量方法。传统的对复杂性的度量是以程序运行中消耗的时间或空间等动态概念作为尺度的，而程序复杂性则以程序长短这一静态概念作为尺度。

一般说来，一个长的程序可以解决的问题，如果用短的程序解决，则计算的时间可能会指数增长，甚至完全变成不可计算。计算的复杂性和程序复杂性之间应该有着密切的联系。把计算机做为封闭系统，把程序的长度看成一个常数，对计算的复杂性进行孤立的研究，只应该是理论研究的一个方面。程序复杂性理论的建立为人们认识计算复杂性增添了一个新角度。

上述研究途径和方法引出了一系列新概念，取得了一些新成果，扩展了人们的思路，并在一定程度上增加了人们解决P＝？NP问题的信心，是研究P＝？NP问题的主流。

第二个流派主张避开NP完全问题。由于大多数求解组合最优解算法都是NP完全的，在现实的存储资源和时间条件下很难或根本得不到最优解。另一方面，对于大量的具体应用，比如推销员旅行问题等，令人满意的解往往并非一定要最优解。所以这一流派放弃寻求最优解，转而研究各种启发式搜索算法以及与之相适应的概率分析方法。从本质上说，这是牺牲完全性来换取高效率和满意解。这种方法在许多领域特别是人工智能应用中取得了良好效果，成为人工智能的基本技术之一。近年来又有人在更为深刻和更为宽广的意义上提出了启发式程序设计的思想，从而把启发式方法的研究提高到一个新水平。启发式方法将对今后的计算机科学和人工智能产生重大影响。

第三个流派是变革性的。由于机器智能和认知科学研究的不断深入，P＝？NP问题又长期未得到满意的解决，因此引起人们对传统的"计算"、"图灵可计算"等概念进行"反思"。

传统的所谓"计算"是从一离散的符号行得到另一符号行的变换。但从一般意义上说，任何物理过程中的信息活动都是某种计算，都和其它运动形式中的信息活动有某种共性，计算的本质是一种模拟。计算富里叶变换最快的方法是用一块透镜，计算最小曲面最快的方法是肥皂膜。因而Clark提出不能把计算归结为符号变换，应该弄清形式符号系统和连续信号处理系统之间的异同。我国也有学者尝试通过将递归函数的自然数基扩充到实数来突破图灵计算模型，还有人认为人脑是一个开放系统，计算机也应是开放的，应该用开放的模型去刻划计算。总之，这一流派试图从更广义的角度刻划可计算与不可计算之间的界线，进而把计算理论置于一种新的基础之上。这种对计算本质的再认识对计算机科学具有现实的和深远的意义。

P＝？NP是涉及计算机科学根本性问题的一个重大难题，对它的研究派生出了一系列新概念、新方法和新观点。它的最终解决将导致整个计算机科学技术的突破和巨大发展。

参考文献

[1]美国计算机研究报告，模式识别与人工智能，1990年第4期，1-35

[2]NASA91-1 SBIR Technical Topics and Subtopics, 1991

[3]Faculty Research Guide 1990-1991, Computer Science Department, CMU

[4]自然科学学科发展战略研究报告—计算机科学技术，1993

[5]Martin Dietzfelbinger & Wolfgang Maass, The complexity of matrix transposition on one-tape off-line Turing machines with output tape, Theoretical Computer Science 108(1993)271-290