数学机械化丛书 5

# 近世计算理论导引

## ——NP难度问题的背景、前景及其求解算法研究

黄文奇 许如初 著

科学出版社
www.sciencep.com

数学机械化丛书　　5

# 近世计算理论导引

## ——NP难度问题的背景、前景及其求解算法研究

黄文奇　许如初　著

科 学 出 版 社

北 京

# 内 容 简 介

本书对迄今为止有关计算理论的实质性成果作了深刻、严格而又直观的论述，为计算机科学的实质性难题 NP 难度问题的实现求解提出了一条现实的高效的求解途径. 它在透彻讲解图灵机的基础上，阐明了为什么会有计算机不可解的问题，会有计算机难解的问题；然后为当代实质性的计算机难解问题，即 NP 难度问题指明了得出高性能求解算法的现实途径——拟物、拟人途径；最后为设计算法与分析问题的复杂度提供了一个强有力的工具——有穷损害优先方法.

本书的内容经过不同组合可作为大学生、硕士生、博士生的教材，也可供有关的科技人员参考。

**图书在版编目(CIP)数据**

近世计算理论导引：NP 难度问题的背景、前景及其求解算法研究/黄文奇，许如初著.—北京：科学出版社，2004

(数学机械化丛书；5)

ISBN 7-03-012617-3

Ⅰ. 近… Ⅱ. ①黄… ②许… Ⅲ. 电子计算机－算法理论 Ⅳ. TP301.6

中国版本图书馆 CIP 数据核字(2003)第 125395 号

责任编辑：吕 虹/责任校对：柏连海

责任印制：钱玉芬/封面设计：黄华斌

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

新蕾印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2004 年 6 月第 一 版 开本：B5(720×1000)

2004 年 6 月第一次印刷 印张：6 1/2

印数：1—3 000 字数：105 000

**定价：20.00 元**

(如有印装质量问题，我社负责调换〈新欣〉)

中国科学院科学出版基金资助出版

《数学机械化丛书》获国家基础研究发展规划项目“数学机械化与自动推理平台”与“数学机械化应用推广专项经费”资助

# 《数学机械化丛书》编委会

# 《数学机械化丛书》前言[①]

十六七世纪以来,人类历史上经历了一场史无前例的技术革命,出现了各种类型的机器,取代各种形式的体力劳动,使人类进入一个新时代.几百年后的今天,电子计算机已可以有条件地代替一部分特定的脑力劳动,因而人类面临另一场更宏伟的技术革命,处在又一个新时代的前夕.数学是一种典型的脑力劳动,它在这一场新的技术革命中,无疑地将扮演一个重要的角色.为了了解数学在当前这场革命中所扮演的角色,应对机器的作用,以及作为数学的脑力劳动的方式,进行一定的分析.

**1. 什么是数学的机械化**

不论是机器代替体力劳动,或是计算机代替某种脑力劳动,其所以成为可能,关键在于所需代替的劳动已经“机械化”,也就是说已实现了刻板化或规格化.正因为割麦、刈草、纺纱、织布的动作已经是机械化刻板化了的,因而可据此造出割麦机、刈草机、纺纱机、织布机来.也正因为加减乘除开方等运算这一类脑力劳动,几千年来就已经是机械地刻板地进行的,才有可能使得 17 世纪的法国数学家帕斯卡,利用齿轮传动造出了第一台机械计算机——加法机,并由莱布尼茨改进成为也能进行乘法的机器.数学问题的机械化,就要求在运算或证明过程中,每前进一步之后,都有一个确定的、必须选择的下一步,这样沿着一条有规律的、刻板的道路,一直达到结论.

在中小学数学的范围里,就有着不少已经机械化了的课题.除了四则、开方等运算外,解线性联立方程组就是一个很好的例子.在中学用的数学课本中,往往介绍解线性方程组的各种“消去法”,其求解过程是一个按一定程序进行的计算过程,也就是一种机械的、刻板的过程.根据这一过程编成程序,由电子计算机付诸实施,就可以不仅机器化而且达到自动化,在几分钟甚至几秒钟之内求出一个未知数多至上百个的线性方程组的解答来,这在手工计算几乎是不可能的.如

① 20 世纪七八十年代之交,我尝试用计算机证明几何定理取得成功,由此并提出了数学机械化的设想.先后在一些通俗报告与写作中,解释数学机械化的意义与前景,例如 1978 年发表于《自然辩证法通讯》的“数学机械化问题”以及 1980 年发表于《百科知识》的“数学的机械化”.二文都重载于 1995 年由山东教育出版社出版的《吴文俊论数学机械化》一书.经过 20 多年众多学者的努力,数学机械化在各个方面都取得了丰富多彩的成就,并已出版了多种专著,汇集成现在的数学机械化丛书.现据 1980 年的《百科知识》的“数学的机械化”一文,稍加修改并作增补,以代丛书前言.

果用手工计算,即使是解只有三四个未知数的方程组,也将是繁琐而令人厌烦的.现代化的国防、经济建设中,大量出现的例如网络一类的问题,往往可归结为求解很多未知数的线性方程组.这使得已经机械化了的线性方程组解法在四个现代化中起着一种重要作用.

即使是不专门研究数学的人们,也大都知道,数学的脑力劳动有两种主要形式:数值计算与定理证明(或许还应包括公式推导,但这终究是次要的).著名的数理逻辑学家美国洛克菲勒大学教授王浩先生在一篇有名的"向机械化数学前进"的文章中,曾列举了这两种数学脑力劳动的若干不同之点,我们可以简略而概括地把它们对比一下:

| 计　算 | 证　明 |
| --- | --- |
| 易 | 难 |
| 繁 | 简 |
| 刻板 | 灵活 |
| 枯燥 | 美妙 |

计算,如已经提到过的加、减、乘、除开方与解线性方程组,其所以虽繁而易,根本原因正在于它已经机械化.而证明的巧而难,是大家都深有体会的,其根本原因也正在于它并没有机械化.例如,我们在中学初等几何定理的证明中,就经常要依靠诸如直观、洞察、经验,以及其他一些模糊不清的原则,去寻找捷径.

## 2. 从证明的机械化到机器证明

一个值得提出的问题是:定理的证明是不是也能像计算那样机械化,因而把巧而难的证明,化为计算那样虽繁而易的劳动呢? 事实上,这一证明机械化的设想,并不始自今日,它早就为 17 世纪时的大哲学家、大思想家和大数学家笛卡儿和莱布尼茨所具有.只是直到 19 世纪末,希尔伯特(德国数学家,1862～1943)等创立并发展了数理逻辑以来,这一设想才有了明确的数学形式.又由于 20 世纪 40 年代电子计算机的出现,才使这一设想的实现有了现实可能性.

从 20 世纪二三十年代以来,数理逻辑学家们对于定理证明机械化的可能性,进行了大量的理论探讨,他们的结果大都是否定的.例如哥德尔(Gödel)等的一条著名定理就说,即使看来最简单的初等数论这一范围,它的定理证明的机械化也是不可能的.另一方面,1950 年波兰数学家塔斯基(Tarski)则证明了初等几何(以及初等代数)这一范围的定理证明,却是可以机械化的.只是塔斯基的结果近于例外,在初等几何及初等代数以外的大量结果都是反面的,即机械化是不可能的.1956 年以来美国开始了利用电子计算机做证明定理的尝试.1959 年王浩先生设计了一种机械化方法,用计算机证明了罗素等著的《数学原理》这一经典著作中的几百条定理,只用了 9 分钟,在数学与数理逻辑学界引起了轰动.一时

间，机器证明的前景似乎非常乐观.例如 1958 年时就有人曾经预测:在 10 年之内计算机将发现并证明一个重要的数学新定理.还有人认为，如果这样，则不仅许多著名哲学家与数学家，如皮亚诺、怀特海、罗素、希尔伯特以及图灵等人的梦想得以实现，而且计算机将成为科学的皇后，人类的主人!

然而，事情的发展却并不如预期那样美好.尽管在 1976 年，美国的哈肯等人，在高速计算机上用了 1200 小时的计算机时间，解决了数学家们 100 多年来所未能解决的一个著名难题——四色问题，因此而轰动一时，但是，这只能说明计算机作为定理证明的辅助工具有着巨大潜力，还不能认为这样的证明就是一种真正的机器证明.用王浩先生的说法，哈肯等关于四色定理的证明是一种使用计算机的特例机证，它只适用于四色这一特殊的定理，这与所谓基础机器证明之能适用于一类定理者有别.后者才真正体现了机械化定理证明，进而实现机器证明的实质.另一面，在真正的机械化证明方面，虽然塔斯基在理论上早已证明了初等几何的定理证明是能机械化的，还提出了据以造判定机也即是证明机的设想，但实际上他的机械化方法非常繁，繁到不可收拾，因而远远不是切实可行的.1976 年，美国做了许多在计算机上证明定理的实验，在塔斯基的初等几何范围内，用计算机所能证明的只是一些近于同义反复的“儿戏式”的“定理”.因此，有些专家曾经发出过这样悲观的论调:如果专依靠机器，则再过 100 年也未必能证明出多少有意义的新定理来.

**3. 一条切实可行的道路**

1976 年冬，我们开始了定理证明机械化的研究.1977 年春取得了初步成果，证明初等几何主要一类定理的证明可以机械化.在理论上说来，我们的结果已包括在塔斯基的定理之中.但与塔斯基的结果不同，我们的机械化方法是切实可行的，即使用手算，依据机械化的方法逐步进行，虽然繁复，也可以证明一些艰深的定理.

我们的方法主要分两步，第一步是引进坐标，然后把需证定理中的假设与终结部分都用坐标间的代数关系来表示.我们所考虑的定理局限于这些代数关系都是多项式等式关系的范围，例如平行、垂直、相交、距离等关系都是如此.这一步可以叫做几何的代数化.第二步是通过代表假设的多项式关系把终结多项式中的坐标逐个消去，如果消去的结果为零，即表明定理正确，否则再作进一步检查.这一步完全是代数的，即用多项式的消元法来验证.

上述两步都可以机械与刻板地进行.根据我们的机械化方法编成程序，以在计算机上实现机器证明，并无实质上的困难.事实上中国科学院数学研究所某些同志以及国外的王浩先生都曾在计算机上试行过.我们自己也曾在国产的长城 203 台式机上证明了像西摩松线那样不算简单的定理.1978 年初我们又证明了

初等微分几何中主要的一类定理证明也可以机械化. 而且这种机械化方法也是切实可行的,并据此用手算证明了不算简单的一些定理.

从我们的工作中可以看出,定理的机械化证明,往往极度繁复,与通常既简且妙的证明形成对照,这种以量的复杂来换取质的困难,正是利用计算机所需要的.

在电子计算机如此发展的今天,把我们的机械化方法在计算机上实现不仅不难,而且有一台微型的台式机也就够了. 就像我们曾经使用过的长城 203,它的存数最多只能到 234 个 10 进位的 12 位数,就已能用以证明西摩松线那样的定理. 随着超大规模集成电路与其他技术的出现与改进,微型机将愈来愈小型化而内存却愈来愈大,功能愈来愈多,自动化的程度也愈来愈高. 进入 21 世纪以后,这一类方便的小型机器将为广大群众普遍使用. 它们不仅将成为证明一些不很简单的定理的武器,而且还可用以发现并证明一些艰深的定理,而这种定理的发现与证明,在数学研究手工业式的过去,将是不可想象的. 这里我们应该着重指出,我们并不鼓励以后人们将使用计算机来证明甚至发现一些有趣的几何定理. 恰恰相反,我们希望人们不再从事这种虽然有趣却对数学甚至几何学本身也已意义不大的工作,而把自己从这种工作中解放出来,把自己的聪明才智与创造能力贯注到更有意义的脑力劳动上去.

还应该指出,目前我们所能证明的定理,局限于已经发现的机械化方法的范围,例如初等几何与初等微分几何之内. 而如何超出与扩大这些机械化的范围,则是今后需要长期探索的理论性工作.

### 4. 历史的启示与中国古代数学

我们发现几何定理证明的机械化方法是在 1976 至 1977 年之间. 约在两年之后,我们发现早在 1899 年出版的希尔伯特的经典名著《几何基础》中,就有着一条真正的正面的机械化定理:初等几何中只涉及从属于平行关系的定理证明可以机械化. 当然,原来的叙述并不是以机械化的语言来表达的,也许就连希尔伯特本人也并没有对这一定理的机械化意义有明确的认识,自然更不见得有其他人提到过这一定理的机械化内容. 希尔伯特是以公理化的典范而著称于世的,但我认为,该书更重要之处,是在于提供了一条从公理化出发,通过代数化以到达机械化的道路. 自然,处于希尔伯特以及其后数学的一张纸一支笔的手工作业时代里,公理化的思想与方法得到足够的重视与充分的发展,而机械化的方向与意义受到数学家的忽视是完全可以理解的. 但在电子计算机已日益普及,因而繁琐而重复的计算已成为不足道的现代,机械化的思想应比公理化思想受到更大重视,似乎是合乎实际的.

其次应该着重指出,我们在从事机械化定理证明工作获得成果之前,对塔斯

基的已有工作并无接触,更没有想到希尔伯特的《几何基础》会与机械化有任何关系.我们是在中国古代数学的启发之下提出问题并想出解决办法来的.

说起来道理也很简单:中国的古代数学基本上是一种机械化的数学.四则运算与开方的机械化算法由来已久.汉初完成的《九章算术》中,对开平、立方与解线性联立方程组的机械化过程,都有详细说明.宋代更发展到高次代数方程求数值解的机械化算法.

总之,各个数学领域都有定理证明的问题,并不限于初等几何或微分几何.这种定理证明肇始于古希腊的欧几里得传统,现已成为近代纯粹数学或核心数学的主流.与之相异,中国的古代学者重视的是各种问题特别是来自实际要求的具体问题的解决.各种问题的已知数据与要求的数据之间,很自然地往往以多项式方程的形式出现.因之,多项式方程的求解问题,也就自然成为中国古代数学家研究的中心问题.从秦汉以来,所研究的方程由简到繁,不断有所前进,有所创新.到宋元时期,更出现了一个思想与方法的飞跃:天元术的创立.

"天元术"到元代朱世杰时又发展成四元术,所引入的天元、地元、人元、物元实际上相当于近代的未知元或未知数.将这些未知元作为通常的已知数那样加减乘除,就可得到与近代多项式与有理函数相当的概念与相应的表达形式与运算法则.一些几何性质与关系很容易转化成这种多项式或有理函数的形式及其关系.这使得过去依题意列方程这种无法可循需要高度技巧的工作从此变得轻而易举.朱世杰 1303 年的《四元玉鉴》又给出了解任意多至四个未知元的多项式方程组的方法.这里限于 4 个未知元只是由于所使用的计算工具(算筹和算板)的限制.实质上他解方程的思想路线与方法完全可以适用于任意多的未知元.

不问可知,在当时的具体条件下,朱世杰的方法有许多缺陷.首先,当时还没有复数的概念,因之朱世杰往往限于求出(正)实值.这无可厚非,甚至在 17 世纪笛卡儿的时代也还往往如此.但此外朱世杰在方法上也未臻完善.尽管如此,朱世杰的思想路线与方法步骤是完全正确的,我们在上世纪 70 年代之末,遵循朱世杰的思想与方法的基本实质,采用美国数学家里特(Ritt)在 1932,1950 年关于微分方程代数研究书中所提供的某些技术,得出了解任意复多项式方程组的一般算法,并给出了全部复数解的具体表达形式.此后又得出了实系数时求实解的方法,为重要的优化问题提供了一个具体的方法.

由于多种问题往往自然导致多项式方程组的求解,因而我们解方程的一般方法可被应用于形形色色的问题.这些问题可以来自数学自身,也可以来自其他自然科学或工程技术.在本丛书的第一本,吴文俊的《数学机械化》一书中,可以看到这些应用的实例.工程技术方面的应用,在本丛书中有高小山的《几何自动作图与智能 CAD》与陈发来和冯玉瑜等的《代数曲面造型》两本专著.上述解多项式方程组的一般方法已推广至微分方程的情形.许多应用以及相应论著正在

酝酿之中.

**5. 未来的技术革命与时代的使命**

宋元时代天元术与四元术的创造,把许多问题特别是几何问题转化成代数方程与方程组的求解问题.这一方法用于几何可称为几何的代数化.12 世纪的刘益将新法与“古法”比较,称“省功数倍”.这可以说是减轻脑力劳动使数学走上机械化道路的一项伟大的成就.

与天元术的创造相伴,宋元时代的数学又引进了相当于现代多项式的概念,建立了多项式的运算法则和消元法的有关代数工具,使几何代数化的方法得到了有系统的发展,俱见于宋元时代幸以保存至今的杨辉、李冶、朱世杰的许多著作之中.几何的代数化是解析几何的前身,这些创造使我国古代数学达到了又一个高峰.可以说,当时我国已到达了解析几何与微积分的大门,具备了创立这些数学关键领域的条件,但是各种原因使我们数学的雄伟步伐就在这些大门之前停顿下来.几百年的停顿,使我们这个古代的数学大国在近代变成了数学上的纯粹入超国家.然而,我国古代机械化与代数化的光辉思想和伟大成就是无法磨灭的.本人关于数学机械化的研究工作,就是在这些思想与成就启发之下的产物,它是我国自《九章算术》以迄宋元时期数学的直接继承.

恩格斯曾经指出,枪炮的出现消除了体力上的差别,使中世纪的骑士阶级从此销声匿迹,为欧洲从封建时代进入到资本主义时代准备了条件.近年有些计算机科学家指出,个人用计算机的出现,其冲击作用可与枪炮的出现相比.枪炮使人们在体力上难分强弱,而个人用计算机将使人们在智力上难分聪明愚鲁.又有人对数学的未来提出看法,认为计算机的出现,将使数学现在一张纸一支笔的方法,在历史的长河中,无异于石器时代的手工方法.今天的数学家们,不得不面对计算机的挑战,但是,也不必妄自菲薄.大量繁复的事情交给计算机去做了,人脑将仍然从事富有创造性的劳动.

我国在体力劳动的机械化革命中曾经掉队,以致造成现在的落后状态.在当前新的一场脑力劳动的机械化革命中,我们不能重蹈覆辙.数学是一种典型的脑力劳动,它的机械化有着许多其他类型脑力劳动所不及的有利条件.它的发扬与实现对我国的数学家是一种时代的使命.我国古代数学的光辉,鼓舞着我们为实现数学的机械化,在某种意义上也可以说是真正的现代化而勇往直前.

吴文俊

2002 年 6 月于北京

# 序　　言

教学经验说明,严格的逻辑证明能使学生将事物把握得十分确切.但长期囿于严格逻辑证明的人往往会失去直觉的功能,进而失去创造性.他们只能检验出错误和虚伪的东西,而不善于发现和创造出真实、美好的东西.

另一方面,经验也说明,直觉能使学生将事物看得很自然很亲切,最终会导致对事物透彻的理解与把握.但同样地,只喜欢直观领悟而没有经过系统严格的逻辑证明的训练的人,最终有可能变成口才很好的事后诸葛亮.在微妙复杂的形势下,他们往往无力辨别事物的真伪,将一些似是而非的感想当成科学的事实,一旦碰到困难问题,就感到茫然,拿不出真实有用的解决办法.尤其是,他们不具有把一件事情从头到尾彻底做完的能力,在工作中不能真正解决具体问题.

更为重要的是,教师本人,有必要成为严格逻辑与生动直观这两方面的典范.在进行严格证明时,不能避重就轻,将容易的问题仔细证明而将困难的问题一带而过.对于困难的问题更应当正面对待,将它仔细地全面铺展开来,证得一清二楚,并且证明的过程中还要能将符号式子的含义形象地显示出来,防止证明的过程成为被动的验证符号式子搬家演变的合法性的过程.在进行直观解释时,要能把握事物的实质性的形象与来龙去脉,而不能只涉及看来生动却属表面的那些现象.尤其是要不时地考察从似是而非的直观中得出的错误结论,从而不断地校正自己的直观,使其变得更为真实深刻和准确.

经验说明,一个好的理论,一个好的定理,其最原始的创造性部分绝不可能从什么高级的体系经由单纯的逻辑推演而来,而只能是先朦朦胧胧地感觉出来或说是看出来,然后才寻求道理将它说清楚.因此教师教书时最重要的事情是要能向学生描述这个理论或这个定理是如何被想到的,同学生讨论能否很自然地就看出这个理论与定理来.否则教师治学再严谨,论述推理的逻辑再严格学生还是不懂,学生当时被迫于逻辑,承认了理论的正确性,甚至也建立了信仰,并且随之也正确地演算了大量的习题,但是事隔不久他们还是会遗忘,没有留下什么体会,没有形成自己的独立能力,遇到有关的新问题时仍然解决不了.这样的痛苦疲惫要经过很长的反复过程才有可能缓解,学生对事物的领悟水平和独立的思考能力才有可能稍有提高.更有甚者,对于有些深刻的理论,包括定理和算法,大多数学生虽然能照猫画虎地套用并且能得出正确的结果,但是毕其终生对于这些理论本身却没有达到真实的理解,没有领悟到要害,没有形成自己的体会.

许多大师们的教学经验说明,在一段时间内,学生学的东西太多,不但无益,

反而有害,那些东西对实质性的应该牢靠掌握的东西的理解不但没有帮助反而形成了干扰.特别是那些无穷无尽的细小技巧,永远也学不完,而且一旦陷入之后,学生往往会忘记事物的本质和主流,最后成为精巧的工匠和事务主义者.学生们在掌握数量并非十分庞大的最本质的理论和最基本的技巧之后应立即从事世界前沿的科学研究,在这种真实的研究工作中进行有选择性的深入细致的思考和试验,以提高自己的理论水平和实际工作能力.在这一过程中用功细心的学生自然会自己创造发明出许多细小的技巧并有能力自觉地学会过去在学校没有学过的相关的有用理论和技术.

在现代科学技术中有一个令人十分向往的领域,那就是人类思维劳动的机械化.虽然全人类对此问题已思考了数千年之久,但是直到19世纪末才产生了颇具规模的有关科学技术.然而,至20世纪70年代,这方面的科学技术已有了长足的发展和进步.由于微型电脑的出现,由于电脑在各种控制工程中的应用,特别是电脑在现代通信网络中的管理与控制的作用,计算机科学技术已深深地渗入到人类生活的各个方面.

本书的目的是希望对人类的思维劳动机械化的有关哲学从科学与技术的角度加以表述,以期望有关学生提高自己的科学素养并获得若干基本的实用技术.希望本书的表述能做到既严格又直观,尽量浅显易懂,内容则在保存本质的条件下尽量精简.作者估计,不管学生毕业后将来从事什么样的工作,这种素养和技术对他们都是有益有用的.

由任课教师作不同方式的讲授和发挥,选择本书的不同章节可以构成大学各类院系的教本或参考书.学生的对象可以是本科生也可以是硕士生或博士生.学生专业的门类可以是计算机科学技术、哲学、数学、自动控制、无线电通信、工商管理等,也可是任何其他的理科和工科专业.

本书第一章描述作为计算的数学模型的Turing机,包括它的严格数学定义与直观形象.第二章说明世上确实有许多事情是无法办到的,然后严格证明停机问题的不可解性及Gödel不完全性定理.第三章讲解NP完全理论,显示并论证在现实生活中频繁地出现的大量问题——NP难度问题对于数学家与计算机科学家来说是困难的,并指出这种困难的现象与根源.第四章介绍对于NP难度问题获得高性能求解算法的一个有效途径——拟物拟人.此章为本书的核心,它可供具有不同优势的学者单独阅读.特别地,可供稍具物理知识的数学家阅读,也可供对数学有点兴趣的物理学家阅读.在作者看来,计算机科学家也就是数学家,因为计算机科学事实上就是数学科学中的一个特殊门类,它是侧重于时间的数学,不像20世纪中叶以前的数学那样侧重于空间.第五章介绍一种有用的工具——有穷损害优先方法.这是一个来自于纯粹数学的方法,它对设计算法与研究计算复杂度的结构十分有用.然而由于行业的隔阂,当今世上计算机科学的专

家多不了解这一方法,而少数了解这一方法的数学家中也乏人参与计算机算法的设计.

本书的雏形曾于1991年在吴文俊先生主持、由中国国家自然科学基金委员会支持的南开数学研究所计算机数学年的系列活动中作为博士生课程"计算复杂性理论导引"的讲义由黄文奇作过系统的讲授.在1991年至今的10余年中余新国先生、宋恩民博士、金人超博士及作者黄文奇、许如初曾用此书的初稿为华中科技大学及其前身华中理工大学计算机科学技术领域的硕士生、博士生作过近20次的系统讲授.其间偶有外系、外校及科学院所的青年学子参与听课.

本书的部分章节曾被作者在国内外的一些大学与科学院所作为讲义讲演过,其中包括北京大学、清华大学、中国人民解放军长沙国防科技大学、北京航空航天大学、武汉大学、哈尔滨工业大学、重庆大学、兰州大学及郑州大学;包括中国科学院数学研究所,系统科学研究所,自动化研究所及软件研究所;包括香港大学,香港中文大学,香港城市大学及香港浸会大学;包括美国康乃尔大学,新加坡国立大学及法国比卡地·朱尔丝文尼大学.有听讲者反映本书对计算理论的最实质性部分都讲到了,但比已有的其他书籍通俗好懂,并且某些章节在当今还有其实用价值;缺点是对某些有用的理论与技术没有提及,有的提及了又不够深入细致.为了补充本书的不足,建议使用本书的教师和学生参考以下四本教科书和专著:

1　Martin D. Davis and Elaine J. Weyuker, Computability, Complexity, and Language (fundamentals of theoretical computer science), Academic Press, INC., 1983.[中译本:戴维斯与维俞克,可计算性,复杂性和语言(理论计算机科学基础),张立昂,陈进元,耿素云译,清华大学出版社,北京,1989.]

2　Robert I. Soare, Recursively Enumerable Sets and Degrees —— A Study of Computable Functions and Computably Generated Sets, Springer-Verlag, Berlin Heidelberg New York London Paris Tokyo, 1987

3　Harry R. Lewis and Christos H. Papadimitriou, Elements of the Theory of Computation, Prentice-Hall, Inc. and 清华大学出版社,北京,1999.[中译本:勒维斯与帕帕蒂米特里欧,计算理论基础,张立昂,刘田译,清华大学出版社,北京,2000.]

4　张健,逻辑公式的可满足性判定——方法、工具及应用,科学出版社,北京,2000.

本书许多根本的思想、感觉和技术都是来源于作者的老师与学长,没有他们几十年来的熏陶、教诲、指导与帮助,作者对有关的世界不可能达到目前的认识.他们是周培源、李学英、朱九思、程民德、余家荣、吴文俊、王浩(Hao Wang)、王世强、黄敦、陆钟万、陈廷槐、陈耀松、涅罗德(Anil Nerode)、杨东屏、陶仁骥、董韫

美、陈火旺、石赫、李慧陵、黄泽权(C. K. Wong)、杨乐、黄且圆、索阿(Rorbert I. Soare)、李未、葛可一(K. I. Ko)、堵丁柱、唐守文.

作者进入 SAT 问题非完整求解算法领域的研究是源于李未的启发与激励，在此研究的初期阶段，研究工作是在他的领导之下并与他合作进行的.

对于原苏联的物理学家 Л. Д. ЛаНДау，作者虽无缘面见，但已被他的著作所深深感动. 相关的读者会察觉到本书的正文是明显地受到了他的影响，只不过有些表述远不及他的美丽、清晰和简单.

作者的青年同事李初民(Chumin Li)、柳渝(Yu Li)和吴有亮(Yu-Liang W)，依他们的学识见地对作者的研究工作给予了大的激励并开阔了作者的眼界. 青年同事詹叔浩，依其才能与勤奋，同作者一道在拟物算法的最初形成阶段完成了因试探而动荡不定的艰苦的计算工作.

另外，作者过去有幸带了许多天赋很好的学生，其中有的直接参与了作者所进行的科学研究的主流工作中具体问题的思考和计算. 本书某些部分事实上隐含着他们的智慧与劳动. 他们是余向东、陈亮、金人超、朱虹、许向阳、陈广华、赵孝武、陈卫东、张德富、康雁.

一个多少带有偶然性的喜剧性事件是，以本书第四章的哲学和技术为基础的 Solar 算法在“第三届 SAT 问题快速算法国际竞赛”上获金奖(第 1 名). 这届竞赛于 1996 年 3 月 15 日至 17 日在中国北京举行. 第二届与第一届是分别于 1993 年，1992 年在美国与德国举行. 预计类似的科学测量性质的国际竞赛今后还会不断地在世界大都市举行.

自 1985 年至今，18 年来，作者的研究工作持续地得到了中国政府和研究机构的资助，它们是：国家自然科学基金，国家高技术研究发展计划(863)，国家重点基础研究发展规划(973)，中国高等学校博士学科点专项科研基金，中国科学院软件研究所计算机科学开放实验室课题基金.

作者热诚欢迎海内外专家学者及青年学生指出书中的错误与不足之处，提出改正或改进的建议，也欢迎他们就有关问题的看法作更深入细致的思辨. 作者的通信地址是：

武汉市洪山区华中科技大学计算机学院(邮政编码：430074)

黄文奇　许如初

2003 年 10 月于武汉

# 目　　录

# 第一章　计算的数学模型——Turing 机

什么是计算机？它是帮助人们进行脑力劳动的工具.因为当今的计算机皆以“电”作为物质载体，所以有许多人称其为电脑，这也是颇有道理的.至于说“电脑这个词汇即暗示着计算机可以完全取代人脑进行思维”，那是一种误会，不难澄清，也不会导致太实际的消极的影响.

自古以来，人体的手指、脚趾，以及绳结、算筹、算盘、手摇计算机、电动计算机等都是处于某种发展阶段的计算机.但是只有在物质硬件上将“判断”和“选择执行”串通起来，使得视格局情况而进行有限的循环计算成为现实以后，计算机才在真正的“自动化”上迈出了第一步.这就是现代电子计算机的产生，以后发展的路还很长很长.

为了能够精确、系统地对计算和计算机进行研究，需要以人类高度文明的产物——严格精致且十分明白的数学作为工具，这就产生了一个数学模型的问题，即研究什么是计算，什么是计算机，如何能十分明白地将它说清楚.为了有一个明白的表述，我们不得不在真实性和永恒性上做一些牺牲，即我们的概念只能覆盖人类过去数千年的认识，只能涉及到有关事物在今后数百年至多几万年以内的发展，而决不能预料多少万万年以后和离银河系十分遥远的地方发生的事情.有趣的是，虽然人类关于“计算”的概念是发源于纯粹数学的“整数”，但是，“计算”本身却不是一个纯粹数学的概念，不能从纯粹数学得到.从根本上讲它与物质材料及其运动有关.

在人类使用、观察并制造了许许多多的计算机之后，在近代电子计算机诞生的前夜，英国人 Alan Turing(1912～1954)为计算机和计算定义了它们的数学模型——Turing 机.或者说 Turing 设计出了能够作为计算和计算机的统一的数学模型的机器——Turing 机.

Turing 机有两大特点.第一，极为简单明白.它十分好懂，十分亲近于人.学过一点算术的中等程度的小学高年级学生是完全能理解的.Turing 机已经明白和确切到了纯粹数学的程度，它已完全成了一个数学的结构，可以用确切的数学概念来对它进行描述和深入系统的研究.Turing 机的第二个特点是它的包容性.Turing 机，实际上不是一台机器，而是一类机器，是可数无穷台具体的机器.

自 20 世纪初至今严肃的数学家的研究证明，从可计算性的角度来看，即不计时间、空间开销的具体大小，则对于世上任何一件事，只要有一台计算机能做到，则必有一台 Turing 机，它也能做到.这就是所谓 Church-Turing 论题.