数学机械化丛书

11

不等式机器证明与自动发现

杨 路 夏壁灿 著

科学出版社
www.sciencep.com

数学机械化丛书 11

不等式机器证明与自动发现

杨 路 夏壁灿 著

科学出版社
北京

内 容 简 介

本书主要介绍作者及其合作者近十年来在不等式机器证明与自动发现方面的工作，兼顾经典结果和方法. 全书共分 7 章，分别介绍和论述多项式的伪除与结式、相对单纯分解、多项式的实根、常系数半代数系统的实解隔离、参系数半代数系统的实解分类、不等式机器证明的降维算法与 BOTTEMA 程序以及不等式的明证. 除第 1 章及第 3 章、第 7 章的部分内容外，余皆作者及合作者的工作. 附录介绍了子结式理论和柱形代数分解算法，还包括了对作者自编软件包 BOTTEMA 的使用说明.

本书可作为高等院校、科研机构数学或计算机科学方向研究生的教材，也可作为相关专业研究人员和工程技术人员的参考书.

图书在版编目(CIP)数据

不等式机器证明与自动发现/杨路，夏壁灿著. —北京：科学出版社，2007
(数学机械化丛书；11)

ISBN 978-7-03-020721-0

Ⅰ.不… Ⅱ.①杨… ②夏… Ⅲ.不等式-机器证明 Ⅳ.O178-39

中国版本图书馆 CIP 数据核字(2007) 第 186181 号

责任编辑：赵彦超 吕 虹/责任校对：张怡君
责任印制：赵德静/封面设计：王 浩

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

中国科学院印刷厂印刷
科学出版社发行 各地新华书店经销
*
2008 年 1 月第 一 版 开本：B5(720×1000)
2008 年 1 月第一次印刷 印张：15
印数：1—3 000 字数：277 000

定价：45.00 元

(如有印装质量问题，我社负责调换〈科印〉)

前　言

自古以来, 物理量之间大小的比较为现实世界之必需, 这导致了数学不等式的产生和发展. 迄今, 不等式的重要应用已贯穿于当代科学技术和工程领域的多个学科分支.

不等式在数学中从来就不是一个二级或三级的相对独立的学科, 而是 "哪里不平哪里有我". 关于不等式的系统研究应该是近八十年之内的事情. 1929 年, Bohr 向 Hardy 抱怨说: "所有的分析学家都要花一半时间从文献中搜寻他们需用然而未能证明的不等式." 5 年之后, Hardy, Littlewood 和 Pólya 出版了系统研究不等式的经典名著 "*Inequalities*", 1952 年发行了第二版, 该书带有 Hardy 作品中一以贯之的漂亮的代数风格; 关于不等式的第二本重要著作当推 1965 年 Beckenbach 和 Bellman 的与上面同名的专著, 后者的部分内容与前者重叠, 但包含了许多较现代的题材和方法以及较多的应用; 第三本应该是 Mitrinović 于 1970 年出版的 "*Analytic Inequalities*", 这是一部近乎词典式的工具书, 包含了从别处不易获得的若干材料.

以上以及同类的工作, 虽然提供了不等式的大量研究成果和多种论证方法, 却不能适应数学机械化和推理自动化的需要. 由于没有建立强有力的判定算法, 不能对一些常见的不等式问题类作整体的解决, 更不可能对大量的在线问题作实时判定. Hardy 在他的书出版 5 年后被问及: 该书是否对 Bohr 提到的情况有所改善? Hardy 回答说, 从这本书里似乎从来都找不到我所需要的东西.

本书主题是如何用计算机证明和发现代数不等式, 着重研究实用的算法和程序, 固然不同于上面提到的不等式经典, 与国内外阐述实代数或实代数几何的理论性专著也有明显的区别. 但为了理论上做到自成体系以方便研读, 必须补充一些基础知识包括作者及其合作者的若干有关的理论工作作为铺垫. 这部分内容构成本书的前两章和附录 A、附录 B.

代数不等式问题的本质是多项式或多项式组实零点的存在和分类问题, 所以在接下来的三章讨论了多项式的实根、常系数半代数系统的实解隔离和参系数半代数系统的实解分类. 其中第 5 章介绍了实现参系数半代数系统的实解分类的程序 DISCOVERER, 并水到渠成地阐述了该程序自动发现不等式型定理的功能.

第 6 章介绍代数不等式机器证明的降维算法以及对应的程序 BOTTEMA, 这是一个简便快速的不等式证明器, 可以直接处理带多重根式的不等式. 最后两节讨论如何尝试将本章的算法和程序应用于 "高等问题", 即超出 Tarski 所界定的 "初等" 范围的问题. 譬如, 不等式中变量的个数是一个不确定的正整数 n. 读者会发现

这部分内容是富有吸引力的, 虽然探索可以说是刚刚开始.

第 7 章介绍几项探索式研究的进展, 其中包括 Hilbert 第 17 问题的构造性研究. 这些算法虽不完备, 但在实际中常能解决许多原本束手无策的问题. 特别是这些方法产生的证明是可读性很强的 "明证"(certificate), 它无需专家 "审稿", 普通读者即可 "核对" 无误.

由于本书读者包括不同的群体, 对理论部分暂时无暇顾及, 但对不等式机器证明的实用算法和程序有兴趣的读者可以直接阅读第 6 章、第 7 章和附录 C. 俟机再读其余部分.

本书系统地介绍作者及其合作者近十年来在不等式机器证明与自动发现方面的工作. 除第 1 章及第 3 章、第 7 章部分内容外, 余皆作者及合作者的工作.

值此书稿完成之际, 作者衷心感谢吴文俊先生、胡国定先生和吴文达先生多年的教诲和帮助.

深切怀念已经离去的程民德先生.

衷心感谢十年来从多方面对作者帮助和支持的亲人、同事和朋友们.

衷心感谢国家重点基础研究发展计划 "数学机械化方法及其在信息技术中的应用" 项目的鼎力支持, 使本书得以顺利出版.

作 者

2007 年 1 月 3 日

《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, 电子计算机已可开始有条件地代替一部分特定的脑力劳动, 因而人类已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, 就应对机器的作用, 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 Pascal, 利用齿轮传动造出了第一台机械计算机 —— 加法机, 并由 Leibniz 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

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.

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 Descartes 和 Leibniz 所具有. 只是直到 19 世纪末, Hilbert(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 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 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 Tarski 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个机械化方法, 用计算机证明了 Russell 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 Peano、Whitehead、Russell、Hilbert 以及 Turing 等人的梦想得以实现, 而且计算将成为科学的皇后, 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 Hanker 等人, 在高速计算机上用了 1200 小时的计算时间, 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, Hanker 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. 另一方面, 在真正的机械化证明方面, 虽然 Tarski 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 年时, 美国做了许多在计算机上证明定理的实验, 在 Tarski 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 Tarski 的定理之中. 但与 Tarski 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. 事实上数学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 Simson 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 Simson 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, 将是不可想像的. 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即是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, 则是今后需要探索的长期的理论性工作.

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 Hilbert 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与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 Hilbert 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. Hilbert 是以公理化的典范而著称于世的, 但我认为, 该书更重要处, 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 Hilbert 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事情, 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, 我们从事机械化定理证明工作获得成果之前, 对 Tarski 的已有工作并无接触, 更没有想到 Hilbert 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 Euclid 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成轻而易举. 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 Descartes 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 20 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 J. F. 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式式的问题. 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. 在本丛书的第一本书, 吴文俊的《数学机械化》一书中, 可以看到这些应用的实例. 在工程技术方面的应用, 在本丛书中已有高小山的《几何自动作图与智能 CAD》与陈发来和冯玉瑜的《代数曲面拼接》两本专著. 上述解多项式方程组的一般方法已推广至代微分方程的情形. 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的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, 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

目　录

第 1 章　多项式的伪除与结式 ····· 1
1.1　伪除 ····· 1
1.2　结式 ····· 4
1.3　子结式 ····· 7
1.4　三角列 ····· 9
第 2 章　相对单纯分解 ····· 11
2.1　多项式关于三角列的结式 ····· 11
2.2　多项式关于三角列的伪除 ····· 13
2.3　相对单纯分解算法 ····· 14
2.4　三角列的相关性 ····· 19
2.5　三角化的半代数系统 ····· 21
2.6　一般的半代数系统 ····· 25
第 3 章　多项式的实根 ····· 28
3.1　经典结果 ····· 28
3.2　多项式的判别系统 ····· 33
3.3　判别定理的证明 ····· 42
3.4　判别矩阵的某些性质 ····· 46
3.5　多项式的实根隔离 ····· 57
第 4 章　常系数半代数系统的实解隔离 ····· 65
4.1　单调性与第一算法 ····· 65
4.2　若干实例 ····· 70
4.3　区间算术 ····· 77
4.4　第二算法 ····· 78
4.5　讨论 ····· 82
第 5 章　参系数半代数系统的实解分类 ····· 84
5.1　边界多项式和判别多项式 ····· 84
5.2　基本算法 ····· 89
5.3　正维数与超定情形 ····· 93

5.4 DISCOVERER 与例子 ····· 96
5.5 几何不等式的自动发现 ····· 99
5.6 生物系统稳定性的代数分析 ····· 106
5.7 混成系统的可达性 ····· 111
第 6 章 不等式机器证明的降维算法与 BOTTEMA 程序 ····· 117
6.1 半代数系统的不相容性 ····· 117
6.2 基本定义 ····· 119
6.3 降维算法 ····· 122
6.4 关于三角形的不等式 ····· 124
6.5 BOTTEMA 程序及若干实例 ····· 126
6.6 全局优化的符号算法与有限核原理 ····· 131
6.7 借助 BOTTEMA 模拟数学归纳法 ····· 138
6.8 Tarski 模型外的一类机器可判定问题 ····· 142
第 7 章 不等式的明证 ····· 152
7.1 平方和表示 ····· 152
7.2 Schur 分拆 ····· 156
7.3 差分代换 ····· 163
参考文献 ····· 176
附录 A 子结式 ····· 186
A.1 Habicht 定理 ····· 186
A.2 子结式链定理 ····· 190
A.3 子结式多项式余式序列 ····· 196
附录 B 柱形代数分解算法 ····· 201
B.1 基本概念 ····· 201
B.2 基本算法 ····· 204
附录 C BOTTEMA 简易使用指南 ····· 209
C.1 如何安装和运行 BOTTEMA ····· 209
C.2 关于三角形中几何不变量的约定记号列表 (可扩充) ····· 209
C.3 证明不等式型定理的主要指令及其例解 ····· 210
C.4 关于全局优化的主要指令及其例解 ····· 212
附录 D 六次多项式根的分类 ····· 216
索引 ····· 221

第 1 章　多项式的伪除与结式

多项式的伪除与结式是 *消去法* 的两个基本工具, 也是本书许多算法中的常用操作. 我们就从简单介绍相关概念和结论开始.

本章中如非特别指明, $\mathcal{R}$ 表示整环, 一元多项式皆指 $\mathcal{R}[x]$ 中的多项式.

1.1　伪　　除

域 $\mathcal{K}$ 上的多项式环 $\mathcal{K}[x]$ 中多项式的带余除法 (又称长除法) 是人们熟知的. 如果 $\mathcal{R}$ 为整环, 那么带余除法不再适用于 $\mathcal{R}[x]$ 上的多项式, 因为这样的除法会产生 "分式"(系数不再属于 $\mathcal{R}$). 为了避免分式的出现, 对 $\mathcal{R}[x]$ 中的多项式可以使用所谓 *伪除法*.

设

$$F=\sum_{i=0}^{m}a_ix^i,\quad G=\sum_{i=0}^{l}b_ix^i$$

是 $\mathcal{R}[x]$ 中多项式且 $m\geqslant l$. 构造矩阵

$$M=\begin{pmatrix} b_l & \cdots & b_1 & b_0 & & & \\ & b_l & \cdots & b_1 & b_0 & & \\ & & \ddots & & \ddots & & \\ & & & b_l & \cdots & b_1 & b_0 \\ a_m & a_{m-1} & \cdots & \cdots & \cdots & a_1 & a_0 \end{pmatrix},$$

除了 F 和 G 的系数所处的位置外, 别的元素都是零. 矩阵 M 的第 i 列对应着相应多项式关于 x^{m-i+1} 的系数, 具体地说,

$$M\cdot\begin{pmatrix} x^m \\ x^{m-1} \\ \vdots \\ x \\ 1 \end{pmatrix}=\begin{pmatrix} x^{m-l}G \\ x^{m-l-1}G \\ \vdots \\ G \\ F \end{pmatrix}.$$

如果系数在一个域中, 那么对矩阵 M 做高斯消去化为阶梯形, 最后一行的元素就是 F 除以 G 的余式的系数, 即如果 M 最终可通过高斯消去化为

$$\begin{pmatrix} b_l & \cdots & b_1 & b_0 & & & \\ & b_l & \cdots & b_1 & b_0 & & \\ & & \ddots & & \ddots & & \\ & & & b_l & \cdots & b_1 & b_0 \\ 0 & \cdots & \cdots & 0 & r_{l-1} & \cdots & r_0 \end{pmatrix}, \tag{1.1.1}$$

那么, $R=\sum_{i=0}^{l-1} r_i x^i$ 就是 F 除以 G 的余式, 记作 $R=\mathrm{rem}(F,G)$.

如果系数在整环中, 我们可以对 M 施行所谓无分式高斯消去法 (fraction-free Gaussian elimination): 首先, 用最后一行乘以 b_l 减去第一行乘以 a_m; 假设计算的第 i 步 $(1\leqslant i\leqslant m-l+1)$ 最后一行的第 i 个系数是 c_i, 则用最后一行乘以 b_l 减去第 i 行乘以 c_i. 这样经过 $m-l+1$ 次上述操作后, M 变成了形如 (1.1.1) 的矩阵, 那么 $R=\sum_{i=0}^{l-1} r_i x^i$ 称作 F伪除 以 G 的 伪余式, 记作 $\mathrm{prem}(F,G,x)$ 或 $\mathrm{prem}(F,G)$. 它满足

$$b_l^{m-l+1}F=QG+R, \tag{1.1.2}$$

这里 $Q\in\mathcal{R}[x]$ 称作 伪商, 记作 $\mathrm{pquo}(F,G,x)$ 或 $\mathrm{pquo}(F,G)$. 公式 (1.1.2) 称作 伪余公式.

如果上述步骤中某个 $c_i=0$, 那么伪余公式的两端会有公因子 b_l. 我们可以在施行无分式高斯消去法时对最后一行少乘一次 b_l 来降低伪余公式中 b_l 的方次.

例 1.1.1　设多项式

$$F=2x^3-x^2+1,\quad G=3x^2+x-1.$$

我们来考查 F 除以 G 的余式和伪余式. 构造矩阵

$$M=\begin{pmatrix} 3 & 1 & -1 & 0 \\ 0 & 3 & 1 & -1 \\ 2 & -1 & 0 & 1 \end{pmatrix}.$$

容易计算矩阵 M 在通常的高斯消去和无分式高斯消去下分别化为

$$M_1=\begin{pmatrix} 3 & 1 & -1 & 0 \\ 0 & 3 & 1 & -1 \\ 0 & 0 & 11/9 & 4/9 \end{pmatrix}\quad 和\quad M_2=\begin{pmatrix} 3 & 1 & -1 & 0 \\ 0 & 3 & 1 & -1 \\ 0 & 0 & 11 & 4 \end{pmatrix}.$$

所以

$$\mathrm{rem}(F,G,x)=\frac{11}{9}x+\frac{4}{9},\quad \mathrm{prem}(F,G,x)=11x+4.$$

多项式的伪余式还可以用显式表达出来. 为简便起见, 我们引入如下定义.

设 M 为 $\mathcal{R}$ 上的 $r\times s$ 矩阵, 这里 $r\leqslant s$. 定义 M 的 行列式多项式 为

$$\mathrm{detpol}(M)=|M^{(r)}|x^{s-r}+|M^{(r+1)}|x^{s-r-1}+\cdots+|M^{(s)}|,$$

其中 $M^{(j)}$ 是由 M 的前 $r-1$ 列和第 j 列构成的 $r\times r$ 阶子矩阵.

设

$$A_i=\sum_{j=0}^{n_i}a_{ij}x^{n_i-j},\quad 1\leqslant i\leqslant k$$

为一列多项式, 而 $t=1+\max(n_1,\cdots,n_k)$. 我们用 $\mathrm{mat}(A_1,\cdots,A_k)$ 记矩阵 $(m_{ij})_{k\times t}$, 其中 m_{ij} 是 A_i 关于 x^{t-j} 项的系数.

定义 1.1.1　多项式列 $A_1,\cdots,A_k$ 的 行列式多项式 定义为

$$\mathrm{detpol}(A_1,\cdots,A_k)=\mathrm{detpol}(\mathrm{mat}(A_1,\cdots,A_k)).$$

例 1.1.2　设

$$A_1=x^3+2x+5,\quad A_2=3x^2-x-6,\quad A_3=-x^4+x^3$$

是三个多项式, 那么 $t=5,k=3$, 而

$$\mathrm{mat}(A_1,A_2,A_3)=\begin{pmatrix}0&1&0&2&5\\0&0&3&-1&-6\\-1&1&0&0&0\end{pmatrix}.$$

于是

$$\begin{aligned}&\mathrm{detpol}(A_1,A_2,A_3)\\=&\begin{vmatrix}0&1&0\\0&0&3\\-1&1&0\end{vmatrix}x^2+\begin{vmatrix}0&1&2\\0&0&-1\\-1&1&0\end{vmatrix}x+\begin{vmatrix}0&1&5\\0&0&-6\\-1&1&0\end{vmatrix}\\=&-3x^2+x+6.\end{aligned}$$

容易验证如下命题.

命题 1.1.1　设多项式 F 和 G 如上所示, 且 $m\geqslant l>0$, 则

$$\mathrm{detpol}(x^{m-l}G,\cdots,G,F)=\mathrm{prem}(F,G,x).$$

其实这是容易理解的, 因为从高斯消去法的过程可以看出, 伪余式 R 的 x^i $(0 \leqslant i \leqslant l-1)$ 的系数显然只与矩阵 M 的前 $m-l+1$ 列及第 $m-i+1$ 列有关, 而与别的列无关. 上述命题进一步指出这个系数就是这 $m-l+2$ 列构成的矩阵之行列式.

特别地, 如果 F, G 是 $\mathcal{R}[\boldsymbol{x}]$ 中的多项式 (这里 $\boldsymbol{x}$ 代表 $x_1, \cdots, x_n$), 我们可以视其为某个事先确定的主变元—— 比如 x_k 的多项式. 记 $\tilde{\mathcal{R}} = \mathcal{R}[x_1, \cdots, x_{k-1}, x_{k+1}, \cdots, x_n]$, 那么 $\tilde{\mathcal{R}}$ 也是整环, F, G 都是 $\tilde{\mathcal{R}}[x_k]$ 中的多项式. 于是, 可以如上施行关于 x_k 的伪除, 得到伪余式和伪商.

1.2 结　　式

两个一元多项式 $F, G \in \mathcal{R}[x]$ 的结式是关于 F 和 G 的系数的一种形式, 该形式为零将为这两个多项式关于 x 有公共零点提供某种条件. 这里 F 和 G 的公共零点 $\bar{x}$ 是指 $\mathcal{R}$ 之商域的某一扩域中的元素, 使得 $F(\bar{x}) = G(\bar{x}) = 0$.

结式理论是经典的消去理论, 有多种形式的结式, 比如 Sylvester 结式、Bézout 结式、Dixon 结式、Macaulay 结式等. 从本书的内容出发, 我们仅介绍 Sylvester 结式. 它不仅结论优美, 而且充分展示了经典消去法的技巧和思想. 建立在 Sylvester 矩阵之上的子结式理论更是把余式和结式联系起来了.

设 F 和 G 关于 x 的次数分别为 m 和 l, 并将 F 与 G 写成如下形式

$$\begin{aligned} F &= a_0 x^m + a_1 x^{m-1} + \cdots + a_{m-1} x + a_m, \\ G &= b_0 x^l + b_1 x^{l-1} + \cdots + b_{l-1} x + b_l. \end{aligned} \tag{1.2.1}$$

我们构造一个 $m+l$ 阶方阵

$$\boldsymbol{S} = \begin{pmatrix} a_0 & a_1 & \cdots & a_m & & & \\ & a_0 & a_1 & \cdots & a_m & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_0 & a_1 & \cdots & a_m \\ b_0 & b_1 & \cdots & b_l & & & \\ & b_0 & b_1 & \cdots & b_l & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_0 & b_1 & \cdots & b_l \end{pmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} l \\ \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \end{matrix}, \tag{1.2.2}$$

其中, 除 F, G 的系数所处位置外别的元素都为 0. 称该方阵为 F 和 G 关于 x 的 Sylvester 矩阵.

定义 1.2.1　称 Sylvester 矩阵 S 的行列式为 F 和 G 关于 x 的 Sylvester 结式, 记作 $\operatorname{res}(F, G, x)$.