逻辑与形而上学教科书系列

递归论

算法与随机性基础

郝兆宽 杨睿之 杨 跃 著

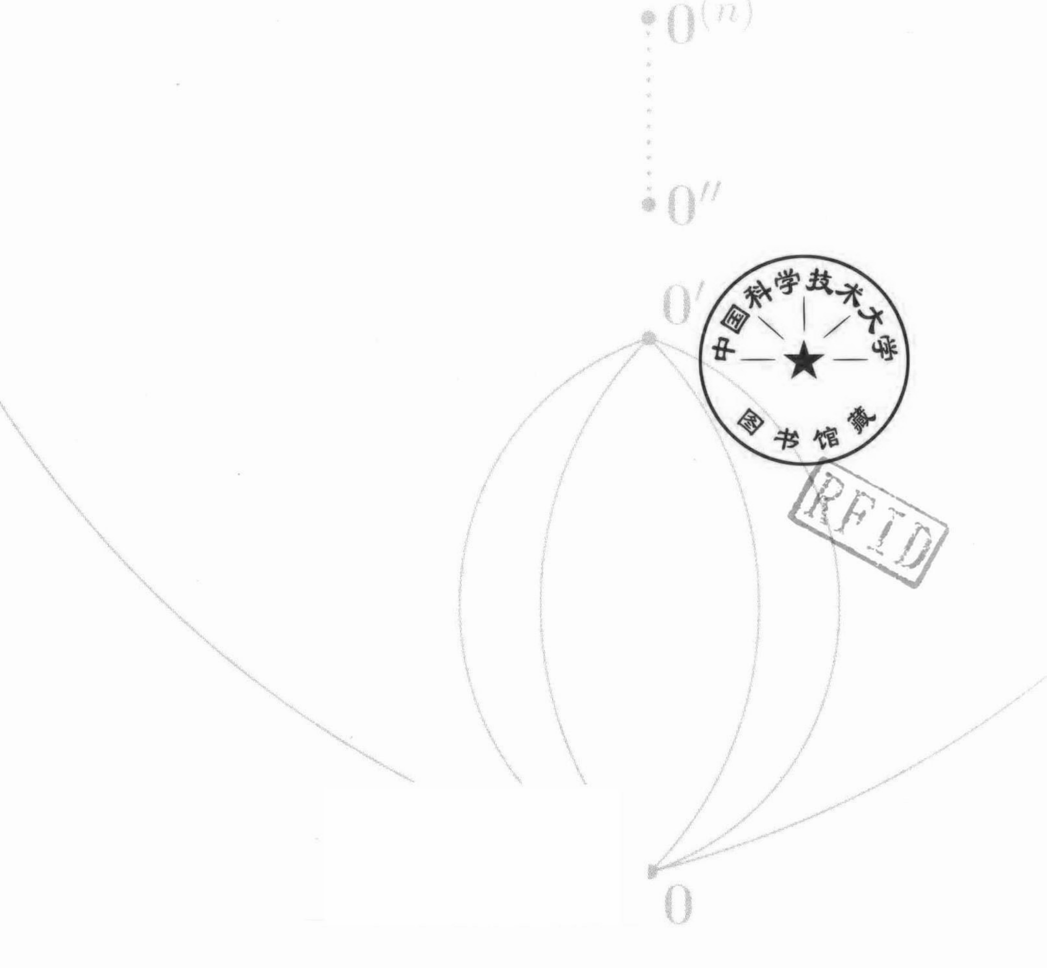
复旦大学出版社

逻辑与形

递归论

算法与随机性基础

郝兆宽 杨睿之 杨 跃 著



复旦大学出版社

图书在版编目(CIP)数据

递归论:算法与随机性基础/郝兆宽,杨睿之,杨跃著. —上海:复旦大学出版社, 2018.10
逻辑与形而上学教科书系列
ISBN 978-7-309-14018-7

Ⅰ.①递… Ⅱ.①郝…②杨…③杨… Ⅲ.①递归论-高等学校-教材 Ⅳ.①O141.3

中国版本图书馆 CIP 数据核字(2018)第 241285 号

递归论:算法与随机性基础
郝兆宽 杨睿之 杨 跃 著
责任编辑/梁 玲

复旦大学出版社有限公司出版发行
上海市国权路 579 号 邮编:200433
网址:fupnet@fudanpress.com http://www.fudanpress.com
门市零售:86-21-65642857 团体订购:86-21-65118853
外埠邮购:86-21-65109143
上海盛通时代印刷有限公司

开本 787×960 1/16 印张 14 字数 245 千
2018 年 10 月第 1 版第 1 次印刷

ISBN 978-7-309-14018-7/O·664
定价:39.00 元

郝兆宽
复旦大学哲学学院教授。主要研究方向为数学哲学、哥德尔思想。

杨睿之
复旦大学哲学学院副教授。主要研究方向为数理逻辑与数学哲学。

杨　跃
新加坡国立大学数学系教授。主要研究方向为数理逻辑，尤其是递归论、皮亚诺算术模型。

逻辑与形而上学教科书系列

集合论 对无穷概念的探索	郝兆宽 杨 跃/著
数理逻辑 证明及其限度（第二版）	郝兆宽 杨睿之 杨 跃/著
作为哲学的数理逻辑	杨睿之/著
初等模型论	姚宁远/著
递归论 算法与随机性基础	郝兆宽 杨睿之 杨 跃/著

责任编辑 梁 玲
封面设计 杨睿之
责任美编 路 静

引言

递归论是数理逻辑的四大分支之一，创立于 20 世纪 30 年代。促使递归论产生的一个重要因素是想要解决数学中的判定问题，即：是否存在一个算法统一地解决某类数学问题。例如，数理逻辑中有“一个语句是否为谓词演算的定理”这样的判定问题，这里人们关心的不是哪一个具体的语句（如 $\forall x \exists y(x \neq y)$）是不是定理，而是关心是否有一个统一的算法，无论我们将哪一个语句输入给它，它都能回答我们该语句是否是定理。对判定问题的回答（特别是否定的回答）直接导致了对算法和对相对可计算性的严格定义。

随着研究的深入，从 20 世纪 50 年代起，递归论的研究范围逐渐扩大，关注点从可计算性扩展到对一般意义上的复杂性、构造性和可定义性等。如今的递归论与逻辑学的其他分支（如集合论、模型论和证明论）和理论计算机科学都有紧密的联系。它的影响也渐渐深入到数学各个分支中与构造性有关的部分。在哲学中有关心灵与机器、人工智能和认识论方面的讨论，也越来越多地涉及递归论里的概念，如图灵机和丘奇论题等。

递归论简介

算法及其严格定义

人们对算法的研究由来已久。在古代中国和古希腊就有了算法概念，并且给出了算法的例子，如欧几里得求最大公约数的辗转相除法。但是有些问题经过了长时期的研究，还是找不到解决它们的算法。例如，希尔伯特第

十问题、群的字问题，以及上面提到的谓词演算中的任一语句是否为一定理的问题，等等。因此数学家们猜想可能根本不存在解决这些问题的算法。但要想证明这一点，却不能依赖朴素直观的算法概念。只有一个严格定义的、能作为数学对象处理的算法概念，才有可能回答“某类问题的算法不存在”这样的问题。

在 20 世纪 30 年代，人们成功地找到了算法的数学定义，而且是多个。这些定义背后的思想各不相同，表述方式也不一样，但令人惊奇的是它们所定义的是同一个函数类。这些定义方式背后的概念有递归函数、λ-演算、图灵机、正规算法等。

递归函数的概念源于哥德尔，如今的递归函数类的定义也含有厄布朗和克林尼的一些深刻想法。递归论（recursion theory）就是递归函数论（theory of recursive functions）的简称。λ-演算由丘奇在 1928 年引入，经过（包括克林尼和罗瑟在内，他们当时是丘奇的研究生）一系列修正和改进，在 20 世纪 30 年代中叶形成了 λ-可定义函数的概念。丘奇认为 λ-可定义函数就是算法可计算函数的精确数学描述，这一观点被称之为“丘奇论题”。不久克林尼证明了递归函数和 λ-可定义函数的等价性，这对丘奇论题是一个支持。但由于λ-演算从表面上看不很自然，所以这一论题没能立即得到包括哥德尔在内的多数人的认同。

1936 年，英国数学家图灵引进了著名的图灵机来描述算法，继而证明了图灵可计算函数和递归函数的等价性。由于图灵机的定义起源于图灵对算法直观经验的精确分析，这就大大增强了丘奇论题的说服力，哥德尔就是在见到图灵机的定义后才接受了丘奇论题的。今天，人们普遍认同丘奇论题，即一切直观上算法可计算的函数都是递归函数。另外值得一提的是，图灵的想法直接导致了现代计算机的产生。在本书的第一章，我们会仔细介绍递归函数、图灵机和丘奇论题。

利用算法的精确定义，我们可以把可判定问题等同于自然数的一类子集，称为“递归集”；把算法可产生集精确描述为“递归可枚举集”（见第一章 1.6 节）。可以证明，一切递归集都是递归可枚举集。但是存在不是递归集的递归可枚举集。例如，停机问题所对应的集合

$$K = \{e : \text{第 } e \text{ 台图灵机对输入 } e \text{ 停机}\}$$

就是非递归的递归可枚举集。通过将 K 归约到上面提到的几个长期未能找出算法的问题，人们就证明了它们是不可判定的。因为如果有判定它们的算法，通过归约就能改造成判定停机问题的算法，而这是不可能的。这些都是递归论的重要成就。

不可解的度及其结构

既然存在算法不可判定的集合，那么自然会问这些不可判定集合的复杂程度是否都是一样的？这就需要给出度量不可解程度的办法。换句话说，对集合 A 和 B，我们想依照某种标准 r 来比较它们之间的复杂程度，即研究在 r 的意义下 A 是否比 B 更容易计算。粗略地说，如果在 r 的意义下 A 比 B 容易计算，则称"A 可以 r-归约到 B"，记作 $A \leq_r B$。在 r 的意义下，计算复杂度相同的集合就形成了所谓的"r-度"。由于标准不同，递归论中研究了很多不同的归约以及相应的度，如多一归约 $\leq_m$、一一归约 $\leq_1$、真值表归约 $\leq_{tt}$、弱真值表归约 $\leq_{wtt}$、图灵归约 $\leq_T$、枚举归约 $\leq_e$、超算术归约 $\leq_h$ 等。但其中最经典的是图灵归约。因此，人们通常谈论的不可解度一般指的就是"图灵度"。在第三章里我们会介绍多一度和图灵度。

图灵在 1939 年利用带信息源的图灵机严格定义了相对可计算性的概念 (Turing, 1939)。考察自然数的子集 A 和 B，我们称"A 图灵归约于 B"(或"A 递归于 B"，或"A 相对于 B 可计算")，如果有一台带信息源 B 的图灵机，对输入 x，该图灵机在计算过程中，可以随时向信息源询问"y 是否属于 B"这样的问题，并根据信息源的回答来决定下一步计算怎样进行，最终在有限步内给出 x 是否属于 A 的答案。我们用"$A \leq_T B$"表示"A 图灵归约于 B"，用"$A \equiv_T B$"表示"$A \leq_T B$ 且 $B \leq_T A$"。容易看出 $\equiv_T$ 是一个等价关系，集合 A 所在的等价类称为 A 的图灵度，记作 $\deg(A)$。所有图灵度的集合记为 $\mathcal{D}$。$\leq_T$ 自然诱导出度上的一个偏序关系 $\leq$，即：如果 $A \leq_T B$，则定义 $\deg(A) \leq \deg(B)$；自然我们也有定义：如果 $A \leq_T B$ 且 $B \not\leq_T A$，则 $\deg(A) < \deg(B)$。如果集合 A 具有某某性质，则称 $\deg(A)$ 为某某度。例如，如果 A 是递归可枚举的，则称 $\deg(A)$ 为一递归可枚举度。一切递归集形成一个度，用 $\mathbf{0}$ 表示，它是最小的图灵度。停机问题 K 的图灵度用 $\mathbf{0}'$ 表示，我们称 $\deg(K)$ 为完全的递归可枚举度。因为 K 不是递归集，故有 $\mathbf{0} < \mathbf{0}'$。

1944 年波斯特在美国数学会做了题为“正整数上的递归可枚举集及其判定问题”的讲演，同年成文发表（Post, 1944）。波斯特在文章中提出了是否存在既不递归也不完全的递归可枚举图灵度这一问题，后来被称为“波斯特问题”。波斯特讨论了几种典型的归约方法，例如，多一归约 $\leq_m$，真值表归约 $\leq_{tt}$ 和图灵归约 $\leq_T$。他证明了在这几种归约下，停机问题 K 在递归可枚举集中都具有最大的不可解度。通过构造单集和超单集，波斯特找到了既不递归又与 K 的度不同的递归可枚举多一度和真值表度。但他没能找到这样的递归可枚举图灵度。波斯特问题直接影响了接下来十几年递归论的发展。在本书的第三章，我们会仔细介绍多一归约、波斯特单集的构造，以及图灵度和递归可枚举度的基本性质。

从 1944 年波斯特的文章开始，递归论的中心就是研究各种不可解度，尤其是研究图灵度$(\mathcal{D}, \leq)$ 这一偏序结构。这既包括对所谓整体结构（对 $\mathcal{D}$ 本身），也包括对局部结构（研究 $\mathcal{D}$ 的某一部分，如递归可枚举度等）的研究。

我们在此顺便介绍一下图灵度方面的研究现状。整体结构研究中比较重要的问题及结果有：

(1) 图灵度理论的可判定性问题。令 $\mathrm{Th}(\mathcal{D})$ 表示图灵度的理论，即所有在 $(\mathcal{D}, \leq)$ 成立的偏序语言上的语句的集合。1977 年辛普森证明了 $\mathrm{Th}(\mathcal{D})$ 与二阶算术的理论是递归同构的，从而完全刻画了图灵度整体结构理论的复杂性。对于图灵度结构理论的片段，施梅尔证明了图灵度的 Σ_3 理论是不可判定的。莱尔曼和肖尔独立证明了 Σ_2 理论是可判定的（Lerman, 1983, 157–159）。

(2) 图灵度上的齐性问题。通过计算的相对化，任何一个图灵度的问题都能自然转换成一个图灵度大于某个度 $\mathbf{a}$ 的问题。这样自然产生了图灵度是否齐性的问题，即是不是对所有的图灵度$\mathbf{a}$，$\mathcal{D}$ 限制在 $\mathbf{a}$ 之上的结构都是一样的。1979 年，肖尔证明了如果一个度 $\mathbf{a}$ 是足够复杂的（如大于克林尼的 $\mathcal{O}$），则 $\mathcal{D}$ 限制在 $\mathbf{a}$ 之上与 $\mathcal{D}$ 本身不仅不同构，甚至不是初等等价的（Shore, 1979）。

(3) 图灵度中哪些集合是可以（仅用偏序的语言）定义的？1984 年约库什和肖尔证明了算术度构成的理想在图灵度中是可定义的。斯莱曼和肖

尔于 1999 年在斯莱曼和武丁工作的基础上证明了图灵跃迁算子在图灵度结构中是可定义的。

(4) 图灵度是否是刚性的，即是否存在图灵度的非平凡自同构？斯莱曼和武丁证明了图灵度结构的自同构群至多有可数多个元素，并且任何自同构在 $\mathbf{0}''$ 之上都是恒同的。刚性问题迄今为止依然悬而未决，可以说是递归论中最重要的尚未解决的问题。

局部结构研究的结果因关注点的不同而不同。我们这里只列举一些关于递归可枚举度的重要结果：

(1) 穆奇尼克（1956）与弗里德伯格（1957）独立证明了存在既不递归也不完全的递归可枚举度，从而肯定地回答了波斯特问题。他们在证明中创造了（有穷损害）优先方法。

(2) 萨克斯（1964）证明了递归可枚举度的稠密性；于是引发了肖恩菲尔德猜想（1965），认为递归可枚举度是一个具有最大和最小元的“稠密”上半格，用精确的模型论语言来说就是可数饱和的上半格。肖恩菲尔德猜想一定程度上代表了当时对递归可枚举度结构的认识，即它是简单且分布均匀的，除了最小和最大的度之外，其他的度都没有多大差别。后来结果证明实际情形完全不像最初想象的那样。

(3) 1966 年，拉赫兰和耶茨独立证明了极小对的存在，即存在下确界是 $\mathbf{0}$ 的非零递归可枚举度 $\mathbf{a}$ 和 $\mathbf{b}$，从而，否定了肖恩菲尔德的猜想。他们的证明利用了无穷损害优先方法。

(4) 1966 年，拉赫兰和耶茨独立证明了递归可枚举度不形成一个格。

(5) 1975 年，拉赫兰证明了非分裂定理，创造了 $\mathbf{0}'''$-损害方法。

(6) 1982 年，哈林顿和沙拉赫证明了递归可枚举图灵度结构的理论是不可判定的，从他们的结果开始，人们渐渐认为递归可枚举度会是一个非常复杂的结构。兰普、尼茨和斯莱曼在 1998 年证明了递归可枚举度的 Σ_3 理论是不可判定的。关于递归可枚举图灵度的 Σ_2 理论是否可判定仍然未知。

(7) 哈林顿和斯莱曼、斯莱曼和武丁、尼茨和肖尔以及斯莱曼先后用不同的编码方法证明了递归可枚举度的理论与一阶算术理论是递归同构的，因此完全刻画了递归可枚举度理论的复杂性。

(8) 尼茨、肖尔和斯莱曼证明了递归可枚举度中除了低度之外的跃迁类都是可定义的。但递归可枚举度低度是否在递归可枚举图灵度中可定义仍然未知。

与 20 世纪 60 年代完全相反，人们现在猜测递归可枚举度的理论可以与一阶算术互释。如果真是这样，则说明递归可枚举度结构的复杂程度是它所能达到的最高程度，但这一猜想尚未得到证明。

回到递归论的历史。波斯特问题促使人们寻找构造递归可枚举集和其他可定义集的新方法。1952 年波斯特和克林尼创造了带信息源的递归构造办法，部分地解决了波斯特问题。他们的方法是后来集合论中力迫法的先声。之后不久，弗里德伯格（1957）和穆奇尼克（1956）各自独立地创造了有穷损害优先方法，肯定地回答了波斯特问题。从 60 年代开始，算术中的力迫法和优先方法经过人们的不断的改进，渐渐成为整体图灵度和递归可枚举度研究中最有利的工具。在第四章，我们会介绍波斯特和克林尼以及弗里德伯格和穆奇尼克的证明。

经典递归论之外的内容

经典递归论主要研究自然数子集的可计算性和度。除此之外，递归论还有很多很有趣的其他研究方向。但由于牵涉术语太多，我们在此只能点到为止。可以说递归论从诞生开始，它的研究范围就超出了经典递归论。例如，图灵就研究过实数上的计算。20 世纪 50 年代末，斯佩克特、萨克斯和克林尼等人将递归论研究的论域以及可计算性的概念进一步拓展，拓展后的领域可以笼统地称为广义递归论（generalized recursion theory），其中很大一部分可以称为高远递归论（higher recursion theory）。一方面，人们将研究的论域推向更高的类型，考虑实数上的或者泛函的可计算性；或者将论域从自然数集 ω 拓展到可容许序数（admissible ordinal）上，α-递归论就是研究可容许序数上的可计算性和 α-度的性质；另一方面，人们从二阶

算术或集合论的角度重新审视自然数子集的性质，从新的角度看，算术分层或图灵归约等就显得太细了，我们需要离研究对象远一些，才能从宏观的角度看到更多的东西。这方面经典的例子是克林尼证明了超算术集实际上就是 Δ_1^1 集，从而在更大的尺度上建立了可计算性与可定义性的对应。超算术集、解析集和投影集是递归论和描述集合论研究对象的交集。在高远递归论的领域内，萨克斯和他的弟子们在 20 世纪 70 和 80 年代做了大量开创性的工作，形成了萨克斯学派。

在递归论的应用方面，递归论学界也一直不停地试图用递归论的工具来解决其他数学领域的问题，如同当年解决希尔伯特第十问题那样。随着计算机的发展，以及对构造性证明的兴趣要求把古典数学能行化。以尼罗德为首的递归论学家在这方面做了大量的工作。他们把古典数学的基本概念算法化，然后考虑哪些数学定理可以成立，哪些无法成立。递归模型论也可以看作是同一主题的变奏。递归论在计算机科学里的应用主要是用于计算复杂性理论。起初是把图灵机作为研究计算复杂性的模型考虑计算的时间、空间复杂性。继而基于递归论，再加上适当的公理，又建立了抽象计算复杂性理论。虽然到现在为止，这些努力尚未取得所期待的成果，但 21 世纪以来递归论在反推数学、算法随机性以及丢番图逼近上的成果又令人燃起新的希望。值得一提的是，递归论在不同领域中的应用为递归论本身注入了新的活力。在第五章我们会以算法随机性为例，看看递归论与其他学科是怎样相互促进、共同发展的。

课程大纲

本教材可以提供一学期课程的容量，构成递归论的入门课程。着重点在于介绍概念，而将递归论中技术性强的内容留给后续课程。在本课程中，我们将介绍可计算性和算法随机性的概念。有趣的是，每个概念都有若干个截然不同然而又相互等价的定义。我们也介绍基本的递归可枚举集的性质，以及不可解度的知识。

第一章　可计算性

在这一部分，我们将介绍递归论的基本概念：可计算性。这一部分与

《数理逻辑：证明及其限度》（郝兆宽，杨睿之，杨跃，2014）一书的第七章有重复。只是为了内容的完整性才将它写入。读过《数理逻辑：证明及其限度》一书的读者，可以只看“递归定理”和“递归可枚举集”这两节。

第二章 不可判定问题

在这一章，我们首先讨论了停机问题，这是最为典型的不可判定问题。借助将停机问题“归约到”某一问题 **Q**，我们可以证明很多问题的不可判定性。随后我们引入了指标集的概念，并证明了莱斯定理。

这一章其余部分全部用来讲述希尔伯特第十问题，这也许是数学史上最著名的一个不可判定问题。我们给出了马季亚谢维奇定理（定理 2.2.11）的完整证明，供有兴趣的读者参考。

第三章 归约、度和算术分层

我们在第二章已经引入了多一对约和一一归约的概念，本章开始部分是对这两者基本性质的研究，核心是迈希尔的两个定理，一个是一一等价与递归同构的等价性，另一个是一一完全与多一完全的等价性。在这一过程中我们引入了创造集和产生集的概念。随后我们讨论了关于多一度的波斯特问题，并借助单集概念给出了肯定的回答。

本章第二个内容是介绍图灵归约和图灵度的概念。在证明了这个递归论核心概念的基本性质后，我们还讨论了跃迁算子，以及一些常见的不可判定集合的度。

本章最后讨论了算术分层问题，证明了波斯特分层定理和肖恩菲尔德极限引理（定理3.3.8），并讨论了 Σ_2 和 Σ_3 完全集的例子。

第四章 典型构造

在这一章我们借助讨论关于图灵度的波斯特问题，给出了递归论中经典的几个实例。首先是克林尼和波斯特的尾节扩张，本质上是力迫法的前驱。借助这一方法，我们可以构造一个 Δ_2^0 的中间度，部分回答了波斯特问题。其次是弗里德伯格和穆奇尼克的定理：存在中间的递归可枚举度。除了完整回答了波斯特问题外，他们发明的有穷损害优先方法是经典递归论最为重要的方法之一。最后一节讨论了萨克斯的进一步的结果：每个递归可

枚举集都可拆分为两个互相不能归约的递归可枚举集。萨克斯的构造同样使用了有穷损害方法，只是比弗里德伯格和穆奇尼克的更为复杂。它的损害集是有穷的，但却没有一个递归的上界。

第五章 算法随机性初步

在这一章中，我们将介绍递归论中一个相对年轻的领域——算法随机性。随机性与可计算性一样，都是关于自然数集的性质。对随机性概念的刻画依赖于可计算性概念，而随机性概念又提供了划分自然数集的另一种维度。我们在本章中介绍了 3 种刻画随机性概念的方式：基于不可压缩性的刻画、基于测试的刻画和基于不可预测性的刻画，以及各自的核心概念：柯尔莫哥洛夫复杂度、马丁-洛夫测试以及鞅。我们证明了对“马丁-洛夫随机”的 3 种刻画的等价性。

同数理逻辑一样，递归论现在也已是非常成熟的学科，本书中的大部分内容都是经典的成果。作者仅仅根据教学经验，将经典内容理顺，以期减少同学们学习的阻力而已。在写作过程中，作者从已有的众多的中外教科书中受益匪浅。其中对作者影响最大的是索阿的经典教材《递归可枚举集和度》(Soare, 1987) 以及它的新版《图灵可计算性：理论和应用》(Soare, 2016)。除此之外，我们还参考了罗杰斯和库特兰德的经典著作 (Rogers, 1967); (Cutland, 1980)。算法随机性一节的内容则参考了唐尼和希施费尔德的《算法随机性与复杂性》(Downey and Hirschfeldt, 2010) 以及尼茨的《可计算性与随机性》(Nies, 2009)。

在编写过程中，中山大学王玮教授、南京大学喻良教授、南开大学彭程博士等对初稿提出了宝贵的修改意见，在此表示深深的感谢。

目录