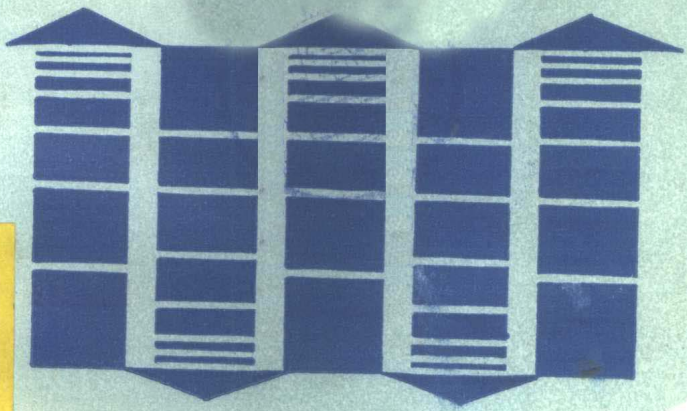
计算机科学丛书

可计算性理论导引

李 祥 编著



贵州人民出版社

JISUANJI KEXUE CONGSHU

计算机科学丛书

可计算性理论导引

李 祥 编著

中国科学院科学基金资助课题

贵州人民出版社

封面设计　石俊生
技术设计　荀新馨

可计算性理论导引

李　祥　编著

贵州人民出版社出版

（贵阳市延安中路5号）

贵州新华印刷厂印刷　　贵州省新华书店发行

787×1092毫米　32开本　5.25印张　106千字

1986年10月第1版　　1986年10月第1次印刷

印数1—2,860

书号 13115·73　　定价（平装）1.15元
（精装）2.35元

编者的话

为了加速发展我国的计算机科学技术，在贵州人民出版社的大力支持和协助下，中国科学院软件研究所、复旦大学、吉林大学、浙江大学、武汉大学、南京大学、上海交通大学、山东大学、哈尔滨科技大学、西北电讯工程学院、贵州大学等有关方面的同志经过多次磋商，组成了《计算机科学丛书》编委会。

这套《丛书》的作者，大多是长期从事计算机科学技术方面的科研、教学工作并在近几年内出国考察或学习过的中年同志。他们既有丰富的实践经验，又对国内外计算机科学的进展有比较清楚的了解。《丛书》将向读者介绍现代计算机科学方面的进展及其理论、方法和应用知识，每本书的内容也都自成体系，独立成册，集中介绍一个专题。为了便于学习，部分书后还列有少量习题，可供读者练习。在写作上，《丛书》力求做到篇幅短，内容新，重点突出，适于读者自学，并使读者在较短时间内对每一个专题的动向和发展趋势得到较为完整的了解。

这套《丛书》可作大专院校有关学科的教材和参考书。《丛书》以大学生、研究生为主要读者对象，也可供大专院校教师、科研工作者和计算机工作者参考。

我们相信，这套《丛书》的出版，将对广大读者了解和掌握计算机科学知识有所裨益。

《计算机科学丛书》
编 委 会
一九八六年一月

前　言

计算的数学理论是计算机科学的一个重要内容，可计算性与能行计算复杂性理论是其中的一个重要分支．在本世纪三十年代,由于数理逻辑学家Herbrand, Gödel, Post, Turing, Church等人的工作，建立了数理逻辑中的一个分支——递归论，从而奠定了可计算性与计算复杂性理论的基础．第二次世界大战后，计算机科学与技术蓬勃发展，可计算性与计算复杂性理论便在六十年代中建立并发展起来．如今，这门理论已成为计算机科学的一门重要理论．各大学计算机系纷纷为高年级学生或研究生开设这门课程，由于其应用的重要性，不仅从事于计算机科学的人，而且从事于数理逻辑与数学的人，也以极大的兴趣研究其中的课题．

本书是数理逻辑递归理论的导引，主要阐述可计算性理论的最基本知识．内容包括：递归函数，图灵可计算函数，计算模型与 Church 论题，递归论的基本定理，算术谱系，递归可枚举集，图灵归约与跃变算子，有穷延伸与有穷损害优先方法，计算复杂性等．根据笔者的学习体会和讲授经验，想用较短的篇幅与较简明扼要的方式，阐述可计算性理论的基础知识及其应用，并期望达到一定的深度与广度．

阅读本书不需要其他专门知识，稍具数理逻辑知识和一

定数学训练的读者即可看懂．本书可作高等院校“可计算性理论”、“递归论”等课程的参考教材，也可供有关人员自学与参考．

限于笔者水平，不足之处，尚望读者不吝赐教．

另外，我的研究生冉太模、许道云两同志，也为本书付出了辛勤的劳动，在此，谨表谢意．

作　者

1986年2月于贵州大学

目　录

第一章　函数、集合、关系与运算

本书假定读者知道一些关于集合与映射的简单知识.

1.1 笛卡儿积　以$\omega=\{0,1,2,\cdots\}$表示非负整数集. 设A_1，…，A_n为ω的子集，以$A_1\times A_2\times\cdots\times A_n$表示笛卡儿积集合，即

$A_1\times A_2\times\cdots\times A_n=\{(x_1,x_2,\cdots,x_n):x_1\in A_1$且$x_2\in A_2$且…且$x_n\in A_n\}$. 若$A_1=A_2=\cdots=A_n=A$，则把$A_1\times A_2\times\cdots\times A_n$记为$A^n$，约定$A^1$为$A$.

1.2 函数与部分函数　本书中，一个n元函数($n>0$)是一个从ω^n到ω里的映射. 一个n元部分函数是一个从$A\subseteq\omega^n$到ω里的映射. 若f为函数或部分函数，则dom f与range f分别表示f的定义域与值域.

1.3 集合与关系　若$R\subseteq\omega^n(n\geqslant 1)$，则称$R$为一个$n$元关系. 若$R$与$Q$为两个$n$元关系，则用：

$R(x_0,\cdots,x_{n-1})$ 表示 $(x_0,\cdots,x_{n-1})\in R$;

$\neg R(x_0,\cdots,x_{n-1})$ 表示 $(x_0,\cdots,x_{n-1})\notin R$;

$R(x_0,\cdots,x_{n-1})\vee Q(x_0,\cdots,x_{n-1})$ 表示

$(x_0,\cdots,x_{n-1})\in R\cup Q$;

$R(x_0,\cdots,x_{n-1})\&Q(x_0,\cdots,x_{n-1})$ 表示

$(x_0,\cdots,x_{n-1})\in R\cap Q$;

$R(x_0,\cdots,x_{n-1})\Rightarrow Q(x_0,\cdots,x_{n-1})$ 表示

$\neg R(x_0,\cdots,x_{n-1})\vee Q(x_0,\cdots,x_{n-1})$;

$(\exists y)R(x_0,\cdots,x_{n-2},y)$表示有一个$y$使$R(x_0,\cdots,x_{n-2},y)$成立；$(\forall y)R(x_0,\cdots,x_{n-2},y)$表示一切$y$都有$R(x_0,\cdots,x_{n-2},y)$；依定义，一元关系就是$\omega$的一个子集合．用$\phi$表示空集合．

1.4 常用的函数、关系与集合

（1）和函数$x+y$．

（2）算术差函数$x\dot{-}y$，定义为：

$$x\dot{-}y=\begin{cases}0, & \text{若 } x<y,\\ x-y, & \text{若 } x\geqslant y.\end{cases}$$

（3）积函数$x\cdot y$．

（4）算术商函数$[x/y]$，定义为：

$$[x/y]=\begin{cases}\text{不大于}x/y\text{的最大整数}, & \text{若 } y\neq 0,\\ 0, & \text{若 } y=0.\end{cases}$$

（5）n元$(n>0)$常函数C_m^n，定义为：对一切$x_0,x_1,\cdots,x_{n-1}$，$C_m^n(x_0,x_1,\cdots,x_{n-1})=m$．

（6）后继函数$s(x)=x+1$．

（7）前承函数$q(x)=x\dot{-}1$．

（8）符号函数$\mathrm{sg}(x)$与$\overline{\mathrm{sg}}(x)$，定义为：

$$\mathrm{sg}(x)=\begin{cases}0, & \text{若 } x=0,\\ 1, & \text{若 } x\neq 0.\end{cases}$$

$$\overline{\mathrm{sg}}(x)=\begin{cases}1, & \text{若 } x=0,\\ 0, & \text{若 } x\neq 0.\end{cases}$$

（9）指数函数$\exp(x,y)$，定义为：

$$\exp(x,y)=\begin{cases}x^y, & \text{若 } x\neq 0 \text{ 或 } y\neq 0,\\ 1, & \text{若 } x=0 \text{ 且 } y=0.\end{cases}$$

（10）射影函数U_i^n，其中$n>0$，$i<n$，定义为：对一

切 x_0，…，x_{n-1}，$U_i^n(x_0, \cdots, x_{n-1}) = x_i$。

（11）二元关系 $x \leqslant y$，$x < y$，$x \geqslant y$，$x > y$，$x = y$，$x \neq y$ 如通常的意义。

（12）PM 表示素数集合{2，3，5，…}。

（13）以 P_0 记第一个素数 2，以 P_i 记第 $i+1$ 个素数。

（14）以 $x|y$ 表示 y 被 x 整除。

1.5 运算 一个从函数（或关系）的子类到函数类里的映射叫运算。下面列举一些本书常用的运算：

（1）复合运算 K_n^m。设 f 为 m 元函数，g_0，…，g_{m-1} 为 m 个 n 元函数，定义函数 h 为：对一切 x_0，…，$x_{n-1} \in \omega$

$h(x_0, \cdots, x_{n-1}) = f(g_0(x_0, \cdots, x_{n-1}), \cdots, g_{m-1}(x_0, \cdots, x_{n-1}))$，则称 h 为从 f 对 $g_0, \cdots, g_{m-1}$ 运用复合运算 K_n^m 而得，把函数 h 记为 $K_n^m(f; g_0, \cdots, g_{m-1})$。

（2）带参数的原始递归运算 R^m。设 f 为 m 元函数，$m>0$，h 为 $m+2$ 元函数，定义函数 g 为：

$$\begin{cases} g(x_0, \cdots, x_{m-1}, 0) = f(x_0, \cdots, x_{m-1}), \\ g(x_0, \cdots, x_{m-1}, y+1) = h(x_0, \cdots, x_{m-1}, y, \\ \qquad\qquad g(x_0, \cdots, x_{m-1}, y)). \end{cases}$$

则称 g 是从 f 与 h 运用带参数的原始递归运算而得，并记 $g = R^m(f, h)$。

（3）不带参数的原始递归运算 R_a^0。设 $a \in \omega$ 且 h 为二元函数，定义 g 为：

$$\begin{cases} g(0) = a, \\ g(y+1) = h(y, g(y)). \end{cases}$$

则称 g 是从 h 运用不带参数的原始递归运算 R_a^0 而得，并记 $g = R_a^0(h)$。

（4）Σ运算．设f为m元函数($m>0$)，定义m元函数g为：

$$g(x_0,\cdots,x_{m-1})=\begin{cases}\Sigma_{y<x_{m-1}}f(x_0,\cdots,x_{m-2},y), & \text{若}x_{m-1}\neq 0,\\ 0, & \text{若}x_{m-1}=0.\end{cases}$$

g称为从f运用Σ运算而得，记为$g=\Sigma f$．

（5）Π运算．设f为m元函数（$m>0$)，定义m元函数g为：

$$g(x_0,\cdots,x_{m-1})=\begin{cases}\Pi_{y<x_{m-1}}f(x_0,\cdots,x_{m-1},y), & \text{若}x_{m-1}\neq 0,\\ 1, & \text{若}x_{m-1}=0.\end{cases}$$

称g是从f运用Π运算而得，记为$g=\Pi f$．

1.6 能行可计算函数 对于函数f，一个颇为重要而有趣的问题是：有没有能行方法使得给定了自变元x的值后可以在有穷步内把相应的函数值$f(x)$计算出来．这种能行方法应由有穷条指令组成，依据于这些指令进行计算的过程应是机械地一步步地进行，其间不靠人的思维控制．这种能行方法又称为算法或程序．如果存在这种能行方法来计算函数f，则把f称为是能行可计算函数或简称为可计算函数．

不难看出，1.4节中的函数都是能行可计算函数，计算它们的能行方法是中小学数学里的方法；此外，如果对可计算函数用1.5节中的运算所获得的函数仍然是能行可计算函数．

现举一个能行可计算函数如下：定义f为

$$f(n)=\begin{cases}0, & \text{若}n\text{是哥德巴赫素数},\\ 1, & \text{若不是}.\end{cases}$$

则f是能行可计算函数，计算f的能行方法如下：

（1）给定n；

（2）用筛法检查 n 是不是素数，若不是则 $f(n)=1$，若是则继续（3）；

（3）用筛法列出 $\leqslant n$ 的所有素数；

（4）将（3）中所得的素数两两相加，若有两个素数之和为 n，则 $f(n)=0$，不然 $f(n)=1$.

不难看出：由指令（1）—（4）确定的算法必可在有穷步内算出 $f(n)$，故 f 是能行可计算函数.

习　题

说明对可计算函数施行 1.5 节中的运算，结果仍得出可计算函数.

第二章　递归函数类

本章首先定义一类直观上看是可计算的函数类——原始递归函数类.证明许多常见的函数都是原始递归函数,但并非每个可计算函数都是原始递归函数；进而定义一类比原始递归函数类更大的可计算函数类——递归函数类．在第三章中要证明这个递归函数类与该章所给出的图灵可计算函数类是相同的.

2.1 定义　满足下述条件的所有函数类A的交被称为原始递归函数类，原始递归函数类中的函数被称为原始递归函数：

（1）类A中有后继函数$s(x)=x+1$；

（2）对一切$n>0, j<n$，类A中有射影函数U_j^n；

（3）对每个自然数m，$n>0$，类A在复合运算K_n^m下封闭；

（4）对每个自然数$m>0$，类A在带参数的原始递归运算R^m下封闭；

（5）对每个自然数$n\geqslant 0$，类A在不带参数的原始递归运算R_n^0下封闭.

下述事实给出了原始递归函数的另一等价定义：

2.2 定理　函数f是原始递归函数的充分必要条件是：存在函数的有穷序列$(g_0,\cdots,g_{k-1})$使$f=g_{k-1}$且对每个$i<k$，下述条件至少有一个能成立：

（1）$g_i = s$；

（2）对某个 $n > 0$，$j < n$，有 $g_i = U_j^n$；

（3）g_i 是 n 元函数且对某个 $m > 0$ 有 $j < i$ 及 $k_0, \cdots, k_{m-1} < i$ 使得 g_j 是 m 元的，$g_{k_0}, \cdots, g_{k_{m-1}}$ 是 n 元的，且有 $g_i = K_n^m(g_j;\ g_{k_0}, \cdots, g_{k_{m-1}})$；

（4）存在 $j, k < i$ 及 $m \in \omega$，$m \neq 0$ 使得 g_j 是 m 元的，g_k 是 $(m+2)$ 元的，且有 $g_i = R^m(g_j, g_k)$；

（5）存在 $j < i$ 及 $n \in \omega$ 使得 g_j 是 2 元的且有 $g_i = R_n^0(g_j)$.

证 设 A 是由具有定理所述的序列的函数 f 所成的集合；为证必要性，只需证明每个原始递归函数都在此 A 中即可. 因有长为 1 的序列 $\langle s \rangle$ 与 $\langle U_j^n \rangle$，故后继函数 s 与射影函数 U_j^n 在 A 中. 假定 m 元函数 $f \in A$，n 元函数 $h_0 \cdots, h_{m-1} \in A$，由 A 的定义知有有穷序列 $\langle g_0, \cdots, g_{k-1} \rangle$ 使得 $g_{k-1} = f$ 而且对于每个 $i < k$，条件（1）—（5）中至少有一个对 g_i 成立. 对每个 $j < m$，取有穷序列 $\langle r_0^j, \cdots, r_{n_j-1}^j \rangle$ 使得 $r_{n_j-1}^j = h_j$，且对每个 $i < n_j$ 条件（1）至（5）至少有一个对 r_i^j 成立，则序列

$$\langle g_0, \cdots, g_{k-1},\ r_0^0, \cdots, r_{n_0-1}^0, \cdots r_0^{m-1}, \cdots, r_{a_{m-1}-1}^{m-1}$$

$$K_n^m(f;\ h_0, \cdots, h_{m-1}) \rangle$$

证实了 $K_n^m(f;\ h_0, \cdots, h_{m-1}) \in A$，即 A 在复合运算下封闭.

充分性：只须证 A 中的每个函数是原始递归函数. 对此，设 $f \in A$ 且有 $(g_0, \cdots, g_{k-1})$，如所述，对 i 进行归纳可知对每个 $i < k$，g_i 是原始递归的，特别得 $f = g_{k-1}$ 是原始递归的.

我们常常通过变元置换、代入等方法获得新函数. 例如，由三元函数 $f(x,y,z)$ 可得一元、二元与三元、四元函数如下：$h_1(x)=f(x,x,x)$，$h_2(x,y)=f(x,y,x)$，$h_3(x,y,z)=f(x,z,y)$，$h_4(x,y,z,t)=f(x,y,z)$. 对于原始递归函数的变元置换、代入等，下述定理2.3—2.5是很有用的.

2.3 定理（变元置换） 设 f 是 m 元原始递归函数，π 是 $\{0,1,\cdots,m-1\}$ 的一个置换，则

$$g(x_0,x_1,\cdots,x_{m-1})=f(x_{\pi(0)},x_{\pi(1)},\cdots,x_{\pi(m-1)})$$

也是 m 元原始递归函数.

证 容易看出

$$g=K^m_m(f;\ U^m_{\pi(0)},\cdots,U^m_{\pi(m-1)})$$

故 g 是原始递归函数.

2.4 定理（减少变元） 若 f 是 m 元原始递归函数，$m>1$，则如下定义的 $m-1$ 元函数 g

$$g(x_0,\cdots,x_{m-2})=f(x_0,\cdots,x_{m-2},\ x_0)$$

也是原始递归函数.

证 $g=K^m_{m-1}(f;\ U^{m-1}_0,\cdots,U^{m-1}_{m-2},U^{m-1}_0)$.

2.5 定理 设 f 是 m 元原始递归函数，则 $m+1$ 元函数 g

$$g(x_0,\cdots,x_m)=f(x_0,\cdots,x_{m-1})$$

也是原始递归函数.

证 $g=K^m_{m+1}(f;\ U^{m+1}_0,\cdots,U^{m+1}_{m-1})$.

以上关于原始递归函数的变元置换、代入与增加的事实在下面关于原始递归性的许多证明中都常常用到，我们不再详尽地指明.

现在转到证明一些具体的函数是原始递归函数上来.