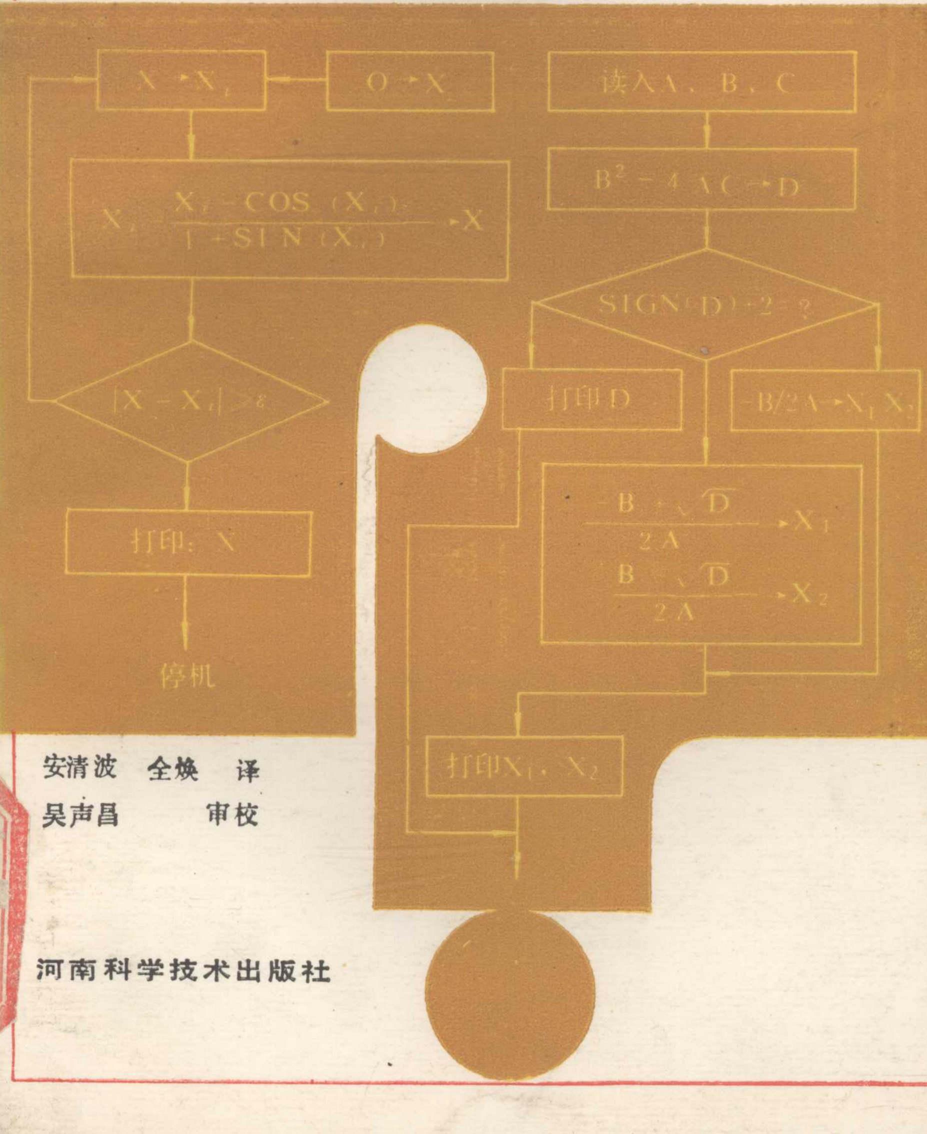
程序正确性的证明

CHENGXUZHENGQUEXINGDEZHENGMING

[美] ROBERT B·ANDERSON 著



安清波 全焕 译

吴声昌 审校

河南科学技术出版社

程序正确性的证明

〔美〕ROBERT B. ANDERSON 著

安清波　全　焕　译

吴声昌　审校

河南科学技术出版社

程序正确性的证明

〔美〕ROBERT B.ANDERSON著

安清波　全　焕译

吴声昌　审校

责任编辑　范云操

河南科学技术出版社出版

河南确山县印刷厂印刷

河南省新华书店发行

850×1168毫米　32开本　5.375印张　124千字

1987年8月第1版　1987年8月第1次印刷

印数1—5,000册

统一书号15245·83　定价1.35元

译 者 的 话

美国豪斯顿大学 ROBERT B. ANDERSON著的《程序正确性的证明》，是一本专门介绍如何验证程序正确性的专业书. 计算机的普及应用使得越来越多的人从事或接触程序编制工作. 然而,什么样的程序才算正确的呢?这确实是所有程序员共同关心的一个重大问题. 这本书通俗简明地介绍了一套易学实用的验证程序是否正确的方法. 每个程序员花费不长一段时间就可以学会这种方法. 掌握这种方法不仅可以证明自己的或别人的程序是否正确，更重要的是程序员在这种思想方法的影响下，编程工作中可以不犯或少犯错误. 很多人的实践证实了这一点. 显然，对所有计算机工作者尤其是程序员来说,掌握这一方法是很有意义的。

本书的序言及第一、二、四章由安清波同志翻译，第三、五章由全焕同志翻译，整个译本请中国科学院应用数学研究所研究员吴声昌老师审稿. 在译本出版过程中，孙建英老师、张发成同志曾给我们很大帮助. 张清海同志承担了全部绘图工作. 我们在此表示衷心的感谢.

序　言

本书旨在解释和阐明一些证明计算机程序正确性的基本方法．近几年来，这个课题已经有了大量的研究成果．这方面研究的最终目的是使这样的证明格式化和机械化．然而，我们的重点在于研究有点非正式的正确性证明，使用这种方法，程序员可以确信他们的程序的正确性．当然，我们十分清楚，非正式的正确性证明容易包含错误，而且没有防止和发现程序错误的灵丹妙药．然而，我们坚信这种非正式的正确性证明将给程序员提供一个系统而又基本的检查程序的方法．同时，我们认为这种应用于程序正确性证明中的基本方法，将能够增加我们对于最基本的程序结构、循环以及递归的洞察力．由于这些原因，我们认为所有的程序员都应该掌握好这种证明程序正确性的基本方法．

读懂本书的唯一要求是具有应用高级程序设计语言编制程序的经验和一些数学证明的知识，而几乎无须专门的数学知识．第一章详尽地介绍了数学归纳法，它是奠定正确性证明基础的一个主要的数学方法．第二章主要讨论了归纳断言法，它是适用于迭代程序正确性证明的最通用的方法；这一章包含着最基础的材料．第三章进一步阐述适用于 FORTRAN 和 PL/1 程序的归纳断言法，利用归纳断言法简要地介绍了证明的控制思想及其等价形式．第四章论述了结构归纳法，它是证明递归程序正确性的最通用的方法，这种方法在证明迭代程序的正确性方面是非常有

用的．所谓迭代程序，基本上是用于完成递归过程的．第五章是一个非常简短的与当前程序正确性证明有关的研究介绍．最后还为有志于这个专题研究的读者提供了一个范围相当广泛的文献目录（此部分略去未译——译者注）．

这本书可以作为大学生和一年级研究生的关于计算理论课程的辅助教材，还可以用作程序设计第二课程的辅助教材，以强调这种程序设计的风格和程序的正确性．显而易见，它还适用于具有一定数学证明知识和编程序经验的人们自学．

ROBERT B. ANDERSON

目　录

第一章　数学归纳法

1.1　引言

数学归纳法是数学证明的一般方法。虽然这种方法并不总是给出代数表达式，但它却是计算机程序正确性证明的基本方法。在这一章里，我们准备使读者充分地熟悉这个基本的证明方法。

数学归纳法通常被认为是一种关于正整数的证明方法，在下一节中，我们将对这一方法的最基本形式进行描述。在1.3节中，我们将给出这一方法的较强的形式。1.4节，我们将给出适用于一些良序集的、而不仅仅是正整数的方法的一般形式。在本章里，仅仅1.2节对于本书大部分章节来说是必要的内容。所以，读者可以跳过1.3节和1.4节而仅当以后需要时再回头读这两部分。1.4节比1.2节和1.3节更加抽象，对于缺乏数学系统训练的读者，可以略去这一部分。

1.2　简单归纳法

简单归纳法原理

假定 S(n) 是关于正整数n的某个命题，我们希望证明 S(n) 对于一切正整数n为真。简单归纳法可表达为：为了证明这个问题，我们只需要证明

(i)　S(1)为真。

(ii) 对于一切正整数n，如果S(n)为真，则 S(n+1) 也真。

事实上，这两个语句已经表明 $S(n)$ 对于一切正整数 n 为真。这是很直观的（虽然在正整数的公理化处理中，这个原理的某些形式必须假定为公理），如果我们证明了 (i) 和 (ii) 都正确，由 (i) 我们知道 $S(1)$ 为真，由 (ii) 我们知道当 $S(1)$ 为真时 $S(2)$ 也为真。因 $S(1)$ 为真，所以 $S(2)$ 也必然为真。由 (ii) 我们又可以知道如果 $S(2)$ 为真，则 $S(3)$ 也为真。于是我们从 $S(2)$ 为真可以推出 $S(3)$ 也为真，…等等。于是直观地据 (i) 和 (ii) 可知，$S(1)$，$S(2)$，$S(3)$，…，$S(n)$ 都为真。

现在，我们给出一些应用简单归纳法的例子。

例1·2·1

我们来证明对于一切正整数 n，从 1 起的前 n 个正整数的和是 $n\cdot(n+1)/2$。换句话说，对于一切正整数 n，有 $1+2+3+\cdots+n=n\cdot(n+1)/2$。如果使用简单归纳法证之，则只要证明：

(i) 从 1 起的 1 个正整数的和是 $1\cdot(1+1)/2$，即 $1=1\cdot(1+1)/2$。

显然，(i) 为真。

(ii) 如果从 1 起的前 n 个正整数的和是 $n\cdot(n+1)/2$，那么，从 1 起的前 $n+1$ 个正整数的和是 $(n+1)\cdot[(n+1)+1]/2$。于是，我们假定 $1+2+3+\cdots+n=n(n+1)/2$ 为真，这就是所谓的归纳假设。下面我们必须由此设法证明 $1+2+3+\cdots+n+(n+1)=(n+1)\cdot[(n+1)+1]/2$ 也为真。

注意到：

$$\begin{aligned}
&1+2+\cdots+n+(n+1)\\
&=(1+2+\cdots+n)+(n+1)\\
&=[n\cdot(n+1)/2]+(n+1)\\
&=[(n^2+n)/2]+(n+1)
\end{aligned}$$

$$=[(n^2+n)/2]+[(2n+2)/2]$$
$$=(n^2+3n+2)/2$$
$$=(n+1)\cdot(n+2)/2$$
$$=(n+1)\cdot[(n+1)+1]/2$$

由此，我们得到了(ii)的证明．由于(i)和(ii)都已被证明，由简单归纳法可知，对于一切正整数n，有：

$$1+2+\cdots+n=n\cdot(n+1)/2$$

改进的简单归纳法

有时我们希望证明命题 S(n) 对于一切整数 $n\geqslant n_0$ 时为真．简单归纳法可以稍微作如下的改进．为了证明 S(n) 对于一切整数 $n\geqslant n_0$ 时为真，我们只需证明

(i) $S(n_0)$为真．

(ii) 对于一切整数 $n\geqslant n_0$，如果 S(n) 为真，则 S(n+1) 也为真．

特别地，如果我们要证明某个命题S(n)对于一切非负整数（即 $n\geqslant 0$）为真，我们只需证明

(i) S(0)为真．

(ii) 对于一切整数 $n\geqslant 0$，如果S(n)为真，那么S(n+1)也为真．

例1·2·2

对于一切非负整数n，我们来证明

$$2^0+2^1+2^2+\cdots+2^n=2^{n+1}-1$$

为了用简单归纳法证明这个等式，我们证明

(i) $2^0=2^{0+1}-1$．这是很显然的，因为

$$2^0=1=2^{0+1}-1=2^1-1=2-1=1$$

(ii) 对于一切非负整数n，如果

$$2^0+2^1+2^2+\cdots+2^n=2^{n+1}-1$$

为真，那么

$$2^0+2^1+2^2+\cdots+2^n+2^{n+1}=2^{(n+1)+1}-1$$

也为真.

$2^0+2^1+2^2+\cdots+2^n=2^{n+1}-1$称为归纳假设.

为了证明 (ii)，我们注意到

$$\begin{aligned}
&2^0+2^1+2^2+\cdots+2^n+2^{n+1}\\
&=(2^0+2^1+2^2+\cdots+2^n)+2^{n+1}\\
&=(2^{n+1}-1)+2^{n+1}\\
&=(2^{n+1}+2^{n+1})-1\\
&=2\cdot 2^{n+1}-1\\
&=2^{n+2}-1\\
&=2^{(n+1)+1}-1
\end{aligned}$$

有时我们希望证明命题S(n)对于一切整数 $n_0\leqslant n\leqslant m_0$为真. 由于$n_0$到$m_0$之间的整数是有限的，我们仅用检验所有不同情况的方法就可以来证明S(n)对于这一切不同的情况为真. 然而，用简单归纳法来证明S(n)仍然常常是一种比较容易的、有时也是必要的方法（例如，当我们不知道n_0或m_0的特定值时）. 在这种情况下，两种形式的简单归纳法都可以用来证明 S(n)对于一切 $n_0\leqslant n\leqslant m_0$均为真.

向上的简单归纳法

(i) 证明$S(n_0)$为真.

(ii) 证明（对于一切整数$n_0\leqslant n\leqslant m_0-1$）如果 S(n) 为真，那么S(n+1)也为真.

向下的简单归纳法

(i) 证明$S(m_0)$为真.

(ii) 证明（对于一切整数$n_0+1 \leqslant n \leqslant m_0$）如果 S(n) 为真，则S(n−1)也为真.

读者可以明显看出，这两种方法中的任一种对于证明 S(n)（对于一切$n_0 \leqslant n \leqslant m_0$）为真来说都是充分的.

证明计算机程序的命题

证明S(n)对于一切n为真，因而使得S(n)对于$n_0 \leqslant n \leqslant m_0$为真，或是对于$n_0 \leqslant n$为真，有时并无明确区别. 在这种情况下，我们常常可以证明这一结果而勿须知道涉及到哪一种情况. 例如，在证明程序的正确性时，有时我们想证明命题S对于每次操作到达程序中的某一点时都为真. 这时我们便可以利用关于操作到达该点次数n的归纳法来证明它. 但我们不能精确地知道操作到达该点有多少次——这可以由运行的程序所使用的数据来确定. 或者操作到达该点的次数是有限数字m_0,或者如果程序不停止的话操作到达该点的次数会达到无限次. 这样，我们可以证明S(n)对于一切的n为真，从而使得S(n)对于$1 \leqslant n \leqslant m_0$或者$1 \leqslant n$都为真. 然而，我们可以证明这一结果而不必考虑实际上是哪一种情况. 如果能够作出如下证明，那么我们就证明了每次操作达到该点时论断S(n)都为真：

(i) S(1)为真（即操作第一次到达该点时S为真）.

(ii) 如果S(n)为真（即当操作第n次达到该点时S为真），那么当操作第n+1次到达该点时，S(n+1)也为真（即操作第n+1次到达该点时S也为真）.

如果操作仅仅到达该点m_0次，那么只有使归纳前提(ii)可能为真的n的值才是满足$1 \leqslant n \leqslant m_0-1$的所有的n的值，而操作再次达到该点就是第n+1次. 另一方面，如果操作达到该点无限次，则使归纳前提(ii)为真的n的值都是$1 \leqslant n$的. 于是，如果我们能够证

明(i)和(ii)，那么我们就通过向上的简单归纳法，或者简单归纳法证明了S(n)对于所有n的有关的值为真，而不必考虑是这两种情况中的哪一种情况。

练　习

1. 证明对于所有的正整数n，有

$$\frac{1}{(1)\cdot(2)}+\frac{1}{(2)\cdot(3)}+\cdots+\frac{1}{n\cdot(n+1)}=\frac{n}{n+1}$$

2. 证明对于所有的非负整数n，有

$$3^0+3^1+3^2+\cdots+3^n=\frac{3^{n+1}-1}{2}$$

3. 证明对于所有的正整数n，有

$$1^3+2^3+3^3+\cdots+n^3=\frac{n^2\cdot(n+1)^2}{4}$$

(注意：上述等式和例1·2·1一起可以证明下述显著的事实

$$1^3+2^3+\cdots+n^3=(1+2+\cdots+n)^2)$$

4.

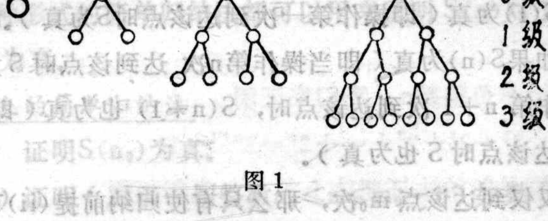


图1

上图是0，1，2以及3级的完全二元树的例子．n级的完全二元树是一个象上面那样的图，树的所有节点除n级上的以外都有两个分支．树的n级节点没有任何分支，因而被称为树的

末端节点或叶节点．通过关于级n的归纳法，证明n级的完全二元树的末端节点数是2^n．找出这种树的节点（末端节点和非末端节点）总数公式，并用归纳法证明之．

5．

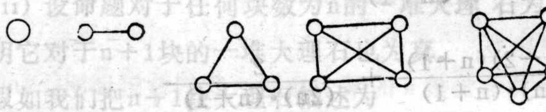


图 2

上图是一个包含 1，2，3，4 和 5 个节点的完全图的例子．n个节点的完全图是一个象上面那样的图，它包含n个节点而且具有连接每一对节点的支路（或者说是链节）．找出 n 个节点的完全图中的支路或者说是链节的个数的公式，并用关于n的归纳法证明之．

6． 找出下述证明中的错误，并希望证明

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{(n-1)\cdot n}=\frac{3n-2}{2n}$$

对于一切正整数n成立．关于n的归纳法证明如下：

(i) 对于$n=1$，公式为真．因为

$$\frac{1}{1\cdot 2}=\frac{3\cdot 1-2}{2\cdot 1}=\frac{3-2}{2}=\frac{1}{2}$$

(ii) 设公式对于n为真，即

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{(n-1)\cdot n}=\frac{3n-2}{2n}$$

同时由于

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{(n-1)\cdot n}+\frac{1}{n\cdot (n+1)}$$

$$=\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\cdots+\frac{1}{(n-1)\cdot n}+\frac{1}{n\cdot(n+1)}$$

$$=\frac{3n-2}{2n}+\frac{1}{n\cdot(n+1)} \quad \text{（归纳假设）}$$

$$=\frac{(3n-2)(n+1)}{(2n)\cdot(n+1)}+\frac{2}{(2n)\cdot(n+1)}$$

$$=\frac{3n^2+n-2+2}{(2n)\cdot(n+1)}$$

$$=\frac{3n^2+n}{(2n)\cdot(n+1)}$$

$$=\frac{n(3n+1)}{(2n)\cdot(n+1)}$$

$$=\frac{3n+1}{2(n+1)}$$

$$=\frac{3(n+1)-2}{2(n+1)}$$

于是公式关于$n+1$也为真．

虽然这个证明似乎是有根据的，但是由于$n=4$时我们有

$$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}=\frac{6}{12}+\frac{2}{12}+\frac{1}{12}=\frac{9}{12}=\frac{3}{4}$$

而

$$\frac{3n-2}{2n}=\frac{3\cdot 4-2}{2\cdot 4}=\frac{10}{8}\neq\frac{3}{4}，$$ 所以证明是不正确的．

7．找出下面证明中的错误．我们希望证明的命题是任一堆大理石仅包含同一种颜色．下面给出大理石块数为n的归纳 法证

明.

(i) 当$n=1$时，是很明显的，因为任何仅有一块的一堆大理石明显地仅包含有同一种颜色的大理石.

(ii) 设命题对于任何块数为n的一堆大理石为真，让我们证明它对于$n+1$块的一堆大理石也为真.

假如我们把$n+1$块大理石描述为

○ ○ … ○ ○

1 2 … n $n+1$

如果我们从中移走第$n+1$块，那么剩下的是n块大理石：

○ ○ … ○

1 2 … n

根据归纳假设，这n块大理石一定都是同一种颜色的. 现在我们假定从中移走的不是第$n+1$块，而是第1块，那么剩下的大理石是

○ ○ … ○ ○

2 3 … n $n+1$

但这也是块数为n的一堆大理石，由此可根据归纳假设，这n块大理石也是同一种颜色. 这就是说$n+1$块大理石全都是同一种颜色的，因为我们知道大理石

○ ○ … ○

1 2 … n

全都是同一种颜色的，而且第$n+1$块大理石也是和第n块大理石同一种颜色（事实上，它不仅和第n块大理石是同一种颜色，而且它和第2，3，…，n块大理石都是同一种颜色）. 于是，所有$n+1$块大理石都是同一种颜色的.