

由在IBM工作50余年的资深计算机专家撰写，Amazon全五星评价，算法领域最有影响力的著作之一
Google公司首席架构师、Jolt大奖得主Joshua Bloch和Emacs合作创始人、C语言畅销书作者Guy Steele倾情推荐
算法的艺术和数学的智慧在本书中得到了完美体现，书中总结了大量高效、优雅和奇妙的算法，并从数学角度剖析了其背后的原理

算法心得

高效算法的奥秘

(原书第2版)

(美) Henry S. Warren, Jr. 著

爱飞翔 译



Hacker's Delight

(Second Edition)



机械工业出版社
China Machine Press

算法心得

高效算法的奥秘

(原书第2版)

(美) Henry S. Warren, Jr. 著

爱飞翔 译

Hacker's Delight

(Second Edition)



机械工业出版社
China Machine Press

图书在版编目 (CIP) 数据

算法心得：高效算法的奥秘 (原书第2版) / (美) 沃伦 (Warren, Jr., H.S.) 著; 爱飞翔译. — 北京: 机械工业出版社, 2014.1

(名家经典系列)

书名原文: Hacker's Delight, Second Edition

ISBN 978-7-111-45356-7

I. 算… II. ①沃… ②爱… 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 (2014) 第 002804 号

版权所有·侵权必究

封底无防伪标均为盗版

本书法律顾问 北京市展达律师事务所

本书版权登记号: 图字: 01-2013-0212

Authorized translation from the English language edition, entitled *Hacker's Delight, Second Edition*, 9780321842688 by Henry S. Warren, Jr., published by Pearson Education, Inc., Copyright © 2013.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education, Inc.

Chinese Simplified language edition published by Pearson Education Asia Ltd., and China Machine Press Copyright © 2014.

本书中文简体字版由 Pearson Education (培生教育出版集团) 授权机械工业出版社在中华人民共和国境内 (不包括中国台湾地区和香港、澳门特别行政区) 独家出版发行。未经出版者书面许可, 不得以任何方式抄袭、复制或节录本书中的任何部分。

本书封底贴有 Pearson Education (培生教育出版集团) 激光防伪标签, 无标签者不得销售。

本书是算法领域最有影响力的著作之一, 与大师高德纳所著的《计算机程序设计艺术》共同被誉为所有程序员都应该阅读的计算机著作。它由在 IBM 工作 50 余年的资深计算机专家撰写, Amazon 全五星评价, Google 公司首席架构师、Jolt 大奖得主 Hoshua Bloch 和 Emacs 合作创始人、C 语言畅销书作者 Guy Steele 倾情推荐。书中总结了大量高效、优雅和奇妙的算法, 并从数学角度剖析了其背后的原理, 算法的艺术和数学的智慧在本书中得到了最好的体现。

本书共 18 章。第 1 章是概述; 第 2 章介绍了基础知识; 第 3~4 章介绍了 2 的幂边界和算术边界; 第 5 章讨论了位计数; 第 6~7 章讲解了在字组中搜索位串和重排位元与字节; 第 8~10 章分别介绍了乘法、整数除法和以除数为常量的整数除法; 第 11 章讲解了初等函数; 第 12 章介绍了以特殊值为底的数制; 第 13~15 章分别讲解了格雷码、循环冗余校验和纠错码; 第 16~18 章分别介绍了希尔伯特曲线、浮点数和素数公式。之后是各章习题的参考答案。附录分别介绍了计算机算术运算表、牛顿法和各种离散函数图像。



机械工业出版社 (北京市西城区百万庄大街 22 号 邮政编码 100037)

责任编辑: 关 敏

北京市荣盛彩色印刷有限公司印刷

2014 年 3 月第 1 版第 1 次印刷

186mm×240mm·27.25 印张

标准书号: ISBN 978-7-111-45356-7

定 价: 89.00 元

凡购本书, 如有缺页、倒页、脱页, 由本社发行部调换

客服热线: (010) 88378991 88361066

投稿热线: (010) 88379604

购书热线: (010) 68326294 88379649 68995259

读者信箱: hzsj@hzbook.com

译者序

写代码总会遇到难题，时而苦于乘法操作频繁溢出，时而苦于开方算法太过笨拙，于是，程序员之间口耳相传的那些代码秘籍，这些时候就该大显身手了。有些小程序，仅两三行代码即能解决平常数十行代码方能实现的功能；还有些小程序，只用0x24924925这般神奇的数字，即能成倍提升运算速度。读者若对此感兴趣，则本书定能令你开怀畅读。

作者从事计算机研发工作数十年，他将期间所得之大量技巧融于书中。本书不但讲授算法技巧，而且还会剖析背后的数学原理，令你在学会某个奇妙算法后，可举一反三，推出很多类似技巧，以运用于不同场合。

在研究这些高效而优雅的算法时，作者还会如数家珍地列出许多变体，并旁征博引地讲述可以解决同一问题的其他思路，铺陈完毕后，更会将各自优劣娓娓道来。实际应用中，经常需要权衡各算法之轻重，嵌入式开发、硬件编程、图形渲染、游戏智能等领域尤其如此，若是平素能像作者这样勤于总结、善于对比，那么在需要用到相关技巧时必能信手拈来，左右逢源。

从培养兴趣、锻炼思维、付诸实践三个角度观之，本书皆为精彩而思辨的智慧书。既可静心品读代码之诗意，又能细致体味数学之美感，何其乐哉！

作者乃业界翘楚，学识渊博而思维开阔，文中部分词句与日常用语及数学、计算机等领域一般用法不甚相同，故译文或加注释或添引号，以强调其特殊含义。

翻译过程中，得到机械工业出版社华章公司诸君勉励，于此深表谢意。

本书主要由爱飞翔翻译，舒亚林、张军、王鹏亦参与部分翻译工作。小弟乐意与各位朋友通过个人网站（www.agilemobidev.com）及电子邮件（eastarstormlee@gmail.com）探讨算法问题。由于时间仓促，水平有限，错误与疏漏在所难免，敬请读者不吝赐教。

爱飞翔
2014年2月

序（第1版序）

三十年前的一个暑假，我在麻省理工学院的 Project MAC 实验室^①找到了首份工作。当时很喜欢操作那里的 DEC PDP-10 计算机^②。这台计算机有丰富且易于操控的指令集，可以做位测试和位屏蔽，并操作位段^③与整数，所以和其他计算机相比，拿它写汇编语言代码绝对要更顺手些。尽管已经停产多年，仍有一批狂热的粉丝还在玩 PDP-10，还有一些人拿家用电脑模拟 PDP-10 指令集，这样就可以执行以前的整个 PDP-10 操作系统及其附属软件了。这帮人甚至还在该平台上开发新的程序，比如说现在还有些网站用模拟的 PDP-10 平台来提供网页服务。（拜托，大家别笑，与那些爱开老爷车的人相比，这种怀旧方式也不算什么。）

1972 年夏天，还有一件事让我开心，那就是读到了一本全新的 MIT 研究备忘录：HAKMEM。这部秘籍收录了从电路到数论的各种技术细节^④，而最令我着迷的内容还是其中各项精妙的编程小技巧。通常每一条编程技巧都会讲一个貌似符合编程规范但是看上去却十分怪异的操作。这些整数或位串操作（bit string，例如计算某个字^⑤中值为 1 的

① “数学与计算研究计划”（Project on Mathematics and Computation）一词的缩写，是 1963 年设立于麻省理工学院（Massachusetts Institute of Technology, MIT）的一个研究项目，为当前“MIT 计算机科学与人工智能实验室”（MIT Computer Science and Artificial Intelligence Laboratory）的前身。详情参见：https://en.wikipedia.org/wiki/Project_MAC#Project_MAC。——译者注

② DEC 公司（Digital Equipment Corporation）于 20 世纪 60 至 80 年代推出的一系列大型计算机。详情参见：<https://en.wikipedia.org/wiki/PDP-10>。——译者注

③ field，在这里指 bit field，也叫“位域”，是一种数据结构，可将各个字段用若干个位元的形式紧密存储，以节省空间。详情参见：<https://zh.wikipedia.org/wiki/位域>。——译者注

④ “HAKMEM”是“hacks memo”的简称，为什么这样写呢？因为 PDP-10 平台的字（word）长度为 36 位，而每个字符占 6 个二进制位，这样，一个字就能容纳 6 个字符，所以很多 PDP-10 程序员用的名字都是 6 个字符，我们这帮人一看到 6 字符的缩写，立马就能还原出它的原意。所以，“HAKMEM”这个怪名字在那个时代是合理的，至少对程序员来说是这样。

⑤ word，在计算机领域里指由一定数量的二进制位（bit，比特）所构成的数据结构。为了与日常汉语中的“字”区别开，译文多以“字组”称之。详情参见：[https://zh.wikipedia.org/wiki/字_\(计算机\)](https://zh.wikipedia.org/wiki/字_(计算机))。此外，为了与十进制的“数位”（digit）和常用的“位置”等词相区分，译文将酌情以“位元”一词对应 bit。——译者注

二进制位共有多少个)，本来用一个较长但是约定俗成的机器指令序列或是循环就能轻松实现，然而秘籍中却用了一种极为巧妙的办法来完成：它只用三四个甚至两个精心选择的指令就够了。这些指令的意思很隐晦，需要有人给你解释，或是自己仔细研究才能搞清楚。品尝这份编程大餐，与吃花生豆或夹心软糖那种小零食一样，也令人欲罢不能。这些技巧内涵丰富，充满了深邃的智慧，体现了程序的美感，甚至让人读出了诗意。

我心里当时就在想：“这种技巧不会只有这么几条吧？”我把这些年来在各种场合发现的编程心得总结了一下，果然数量非常多。所以我又想，“是不是该有一本专著来谈谈这个问题呢？”

看到 Hank Warren 先生的原稿时，我实在太高兴了：他将这些编程小技巧系统地收集起来，按主题分类，并清晰地讲解其意义。虽说有些技巧是用机器指令描述的，但是这本书可不是只写给汇编语言程序员看的。本书主题是探讨计算机中整数与位串的基本结构关系，以及如何才能更为高效地操作它们。汇编语言中能用的技巧，放在 C 或 Java 语言里照样适用。

很多算法和数据结构的书都在讲排序和搜索这些复杂的技术，告诉你如何维护哈希表和二叉树，怎样操作记录和指针等，然而它们都没有讲到二进制位及位元数组这种微型数据结构的功用。单用二进制加减法和位操作就能实现很多强大的功能。由于进位链 (carry chain) 机制，改变一个位元的值有可能会影响到它左方的所有二进制位。某些利用此机制的二进制加法技巧不为人熟知，然而它们却是操作数据的利器。

的确该有一本书来总结这些技巧了。你手中捧着的这本就是，而且写得非常好。要想优化编译器或编写高效代码，那非读它不可。也许这些技巧不是每天都能用到，但在遇到困难时，还是会派上用场的。有时我们要遍历一个字中的位元，有时要执行某些不太好实现的整数操作，有时为了让运行速度加倍，还要优化内循环[⊖]中那些棘手的整数或位元运算——如果真碰到上述情况，那就得求助此书啦。当然了，有时也不必想那么多，直接翻开来读，就必能体会到个中乐趣。

Guy L. Steele, Jr.

2002 年 4 月于马萨诸塞州伯灵顿

⊖ inner loop，指两重循环中内部的那一层，通常优化程序时应首先考虑减少内层循环体的执行时间。详情参见：https://en.wikipedia.org/wiki/Inner_loop。——译者注

前言

程序员创造力第一定律：软件维护成本与程序员创造力的平方成正比。

——Robert D. Bliss, 1992 年

本书收集了笔者多年来总结的一些编程小技巧，其中大部分都必须运行在以二进制补码来表示整数的电脑^①上。尽管本书假设寄存器长度是 32 位，但在寄存器长度不是 32 位的电脑中，这些技巧基本上仍能适用。

本书不打算讲高深的排序算法或是编译器的优化技术等大话题，而是着重来谈涉及单个计算机字组或指令的小技巧，比如怎样统计字组中值为 1 的位元数。此类技巧通常需要混用算术与逻辑指令。

我们还需假定整数溢出^②中断已经屏蔽，这样的话，就算整数运算溢出了，也不会出问题。C、Fortran、Java 等程序都是如此，但使用 Pascal 与 Ada 语言的程序员一定要注意这一点！

书中以通俗的语言来讲述各技巧，只有算法含义不明显时才会给出证明，有时甚至略去证明。算法中将会出现计算机算术指令、“地板”函数^③、算术与逻辑操作混搭等内容，它们要证明起来通常比较困难，而且也不易表述。

笔者把很多算法都写成了程序代码，在电脑上执行并验证，以减少笔误及疏忽。用实际存在的编程语言来描述算法，就有这个好处；然而即便如此，每一种计算机语言也还是各有其缺陷。我使用很多人能看懂的 C 代码来描述高级语言部分，因为它可以直接

① 在本书语境中，电脑、计算机（computer）、机器（machine）、处理器（processor）等词常常都指代中央处理器（CPU），故译文在不致混淆的情况下，将其视为互相通用的概念。——译者注

② integer overflow，指算术运算时由于结果过大或过小而超出存储范围的情形。详情参见：https://en.wikipedia.org/wiki/Integer_overflow。——译者注

③ floor function，又叫向下取整函数或最低值函数，返回不大于自变量的最大整数，也常称为“高斯函数”。详情参见：<https://zh.wikipedia.org/wiki/地板函数>。——译者注

把整数与位串操作写在一起，而且很多 C 语言编译器都能产生高质量的目标代码^㉔。

书中偶尔也会用到机器语言，它们都以“三地址格式”^㉕出现，这样读起来更方便。其中的汇编语言是笔者参照当下的 RISC 指令集^㉖虚构出来的。

大家应该尽量编写没有分支的代码（branch-free code），因为分支代码会拖慢很多电脑的指令获取速度，并阻止 CPU 并发执行。此外，它还会妨碍一些编译器优化措施^㉗，如指令调度^㉘、重复子表达式消除^㉙、寄存器分配^㉚等。也就是说，编译器优化大段的简单代码要比优化很多小代码块的效果更好。

此外，编码时还应该多用数值较小的常量^㉛，多与 0 比较（少与非 0 值比较），尽量写出易于并发执行的指令序列^㉜。如果改写书里很多代码，让它们从内存中查表，其结果会更精确，然而笔者通常不提这种做法。因为与算术指令相比，从内存中加载数据反而更耗时。虽说查表法的确很实用，但是一般来说都比较乏味。当然还有些特例不属于上述情况。

最后要说的是，本书书名^㉝中的“hacker”用的是本意，也就是指痴迷于计算机的人。这种人喜欢拿电脑开发点新玩意儿，或是用新潮而有创意的办法来实现原有的功能。

- ㉔ object code，又叫“目的码”，是编译器处理源代码后的产物，一般由机器码或近于机器语言的代码组成。存放此类代码的文件叫目标文件（object code），也叫二进制文件。详情参见：<https://zh.wikipedia.org/wiki/目标代码>。——译者注
- ㉕ three-address format，即 three address code，缩写为 TAC 或 3AC，又叫“三位址码”、“三地址码”。它把通常的算式“运算结果=操作数 1 操作符 操作数 2”写成“操作符 操作数 1，操作数 2，运算结果”的形式，因其中牵涉 3 个变量（即操作数 1、操作数 2、运算结果）而得名。例如 $z=x+y$ 用 TAC 格式来写就是 add x, y, z。详情参见：https://en.wikipedia.org/wiki/Three_address_code。——译者注
- ㉖ RISC, Reduced Instruction Set Computing 的缩写，是一种设计 CPU 的模式，该设计思路精简了指令数目及定址方式，使 CPU 的制作更为容易，也有助于提升其并行能力与执行效率。使用此种指令集的 CPU 目前主要应用于智能手机和平板电脑等移动设备上，与之相对的是 x86 等处理器所用的“复杂指令集”（CISC，C 表示 Complex）。详情参见：<https://zh.wikipedia.org/wiki/精简指令集>。——译者注
- ㉗ 常见的编译器优化技法请参考：https://en.wikipedia.org/wiki/Category:Compiler_optimizations。——译者注
- ㉘ instruction scheduling，是通过指令流水线（instruction pipeline）技术提升指令并发执行效果的优化手法。详情参见：https://en.wikipedia.org/wiki/Instruction_scheduling。——译者注
- ㉙ commoning，即 common subexpression elimination（CSE），是通过消减重复的表达式来提升执行速度的优化技术。详情参见：https://en.wikipedia.org/wiki/Common_subexpression_elimination。——译者注
- ㉚ register allocation，该技术让众多变量共用一个 CPU 寄存器，以优化执行速度。详情参见：https://en.wikipedia.org/wiki/Register_allocation。——译者注
- ㉛ immediate value，也叫“立即值”。——译者注
- ㉜ instruction-level parallism，缩写为 ILP，意为指令级并行度，用于度量指令序列的并发执行程度。例如某段指令在非并发方式下需要 3 个时间单位来执行，而并发执行只需 2 个时间单位，那么其 ILP 就是 3/2。详情参见：https://en.wikipedia.org/wiki/Instruction-level_parallelism。书中还用该词表示 CPU 并发执行指令的能力。——译者注
- ㉝ 本书英文书名为 Hacker's Delight。——译者注

他们都挺会用电脑，但却很可能不是一名专职电脑程序员或设计师，这些电脑极客^①开发出来的东西，有些有用，有些只是玩玩而已。说到此类纯属玩乐的戏作，让我想起很多资深编程票友都写过一段小程序，它可以把自己照原样打印出来^②。这才是我使用“hacker”一词的初衷，在书里可别想找到教你怎样入侵他人电脑的把戏哦。

致谢

首先要感谢 Bruce Shriver 与 Dennis Allison 两位先生鼓励我写作本书，然后还要对 IBM 诸位同仁致意，参考文献中也提到了其中一些同事的名字。尤其感谢 Martin E. Hopkins 先生，他可谓 IBM 的“活编译器”（Mr. Compiler）。Hopkins 先生在编码工作中一丝不苟，认真优化每一个循环——这种敬业精神深深感染了我。仰赖 Addison-Wesley 各位评审，本书内容有了极大改观。他们的姓名笔者大多不了解，我唯一记住的是大名鼎鼎的 Guy L. Steele, Jr.。在 50 页书评中，Guy 补充了一些我当时没有谈到的新问题，如位元的打乱与复原，“绵羊与山羊分离操作”（分羊法，sheep and goats operation），等等，而且他提出的一些算法也比我原来用的更高明。Guy 是个非常仔细的人，比方说，我曾把十六进制数 AAAAAAAAA 的质因子分解式错写为 $2 \times 3 \times 17 \times 257 \times 65\,537$ ，而他发现其中的 3 应该是 5。此外，他还提了一些旨在改善写作风格的建议，并且从不回避书里的细节问题。读者若发现文中有疑似他人捉刀之处^③，那恐怕得归功于 Guy 了。

H. S. Warren, Jr.

2012 年 6 月于纽约州约克镇

本书英文版相关资料请查阅
[www. HackersDelight. org](http://www.HackersDelight.org)

① 本书语境中的“hacker”可理解成“电脑极客”、“程序玩家”、“编程票友”、“编程达人”、“技术发烧友”等意思，以便与容易引发歧义的“骇客”、“黑客”等通俗叫法区分开。本来 hacker 指计算机技术狂热爱好者，而 cracker 指破坏计算机安全的人，但后者的词义逐渐侵蚀了前者，导致 cracker、hacker 及“骇客、黑客、怪客、剑客”等译名全都成了“计算机安全破坏者”，令 hacker 一词丧失了原意。详情参见：<https://zh.wikipedia.org/wiki/骇客>。——译者注

② 比方说，下面这段用 C 语言写的程序代码：

```
main () {char * p="main () {char * p=%c%s%c; (void) printf (p, 34, p, 34, 10);} %c"; (void) printf (p, 34, p, 34, 10);}
```

③ 原文为 parallel prefix，意为“并行前置式算法”、“平行前缀算法”，是一套分组归并形式的速算流程。详情参见：https://www.wikipedia.org/wiki/Prefix_sum。作者在此处以之比喻他与 Guy 四手联弹的佳话。——译者注

目 录

译者序	
序 (第 1 版序)	
前言	
第 1 章 概述	1
1.1 记法	1
1.2 指令集与执行时间模型	5
1.3 习题	10
第 2 章 基础知识	11
2.1 操作最右边的位元	11
2.1.1 德摩根定律的推论	12
2.1.2 从右至左的可计算性	
测试	13
2.1.3 位操作的新式用法	14
2.2 结合逻辑操作的加减运算	16
2.3 逻辑与算术表达式中的	
不等式	17
2.4 绝对值函数	18
2.5 两数平均值	19
2.6 符号扩展	20
2.7 用无符号右移模拟带符号右移	
操作	20
2.8 符号函数	21
2.9 三值比较函数	21
2.10 符号传递函数	22
2.11 将值为 0 的位段解码为 2 的 n	
次方	22
2.12 比较谓词	23
2.12.1 利用进位标志求比较	
谓词	26
2.12.2 计算机如何设置比较	
谓词	27
2.13 溢出检测	28
2.13.1 带符号的加减法	28
2.13.2 计算机执行带符号数	
的加减法时如何设置	
溢出标志	31
2.13.3 无符号数的加	
减法	31
2.13.4 乘法	32
2.13.5 除法	34
2.14 加法、减法与乘法的	
特征码	36
2.15 循环移位	37
2.16 双字长加减法	38
2.17 双字长移位	38
2.18 多字节加减法与求绝对值	39
2.19 doz、max、min 函数	41
2.20 互换寄存器中的值	44

2.20.1 交换寄存器中相应的 位段	45	的位元数	82
2.20.2 交换同一寄存器内的 两个位段	46	5.1.4 应用	86
2.20.3 有条件的交换	47	5.2 奇偶性	87
2.21 在两个或两个以上的值之间 切换	47	5.2.1 计算字组的奇偶性 ...	87
2.22 布尔函数分解公式	50	5.2.2 将表示奇偶性的位元 添加到7位量中	89
2.23 实现16种二元布尔操作	51	5.2.3 应用	90
2.24 习题	54	5.3 前导0计数	90
第3章 2的幂边界	56	5.3.1 浮点数算法	94
3.1 将数值上调/下调为2的 已知次幂的倍数	56	5.3.2 比较两个字组前导0的 个数	96
3.2 调整到上一个/下一个 2的幂	57	5.3.3 与对数函数的关系 ...	96
3.2.1 向下舍入	58	5.3.4 应用	97
3.2.2 向上舍入	59	5.4 后缀0计数	97
3.3 判断取值范围是否跨越了 2的幂边界	59	5.5 习题	105
3.4 习题	61	第6章 在字组中搜索位串	106
第4章 算术边界	63	6.1 寻找首个值为0的字节	106
4.1 检测整数边界	63	6.1.1 0值字节位置函数的 一些简单推广	110
4.2 通过加减法传播边界	65	6.1.2 搜索给定范围内 的值	110
4.3 通过逻辑操作传播边界	69	6.2 寻找首个给定长度的全1 位串	111
4.4 习题	73	6.3 寻找最长全1位串	114
第5章 位计数	74	6.4 寻找最短全1位串	115
5.1 统计值为“1”的位元数	74	6.5 习题	115
5.1.1 两个字组种群计数的 和与差	80	第7章 重排位元与字节	117
5.1.2 比较两个字组的种群 计数	80	7.1 反转位元与字节	117
5.1.3 统计数组中值为“1” 的位元数	82	7.1.1 位元反转算法的 推广	122
		7.1.2 奇特的位元反转 算法	122
		7.1.3 递增反转后的整数 ...	124

7.2	乱序排列位元	126	9.4.1	用硬件实现移位并相 减算法	172
7.3	转置位矩阵	128	9.4.2	用短除法实现无符号 长除法	174
7.4	压缩算法 (广义提取 算法)	136	9.5	用长除法实现双字除法	176
7.4.1	用“插入”、“提取” 指令实现压缩操作 ...	140	9.5.1	无符号双字除法	176
7.4.2	向左压缩	141	9.5.2	带符号双字除法	179
7.5	展开算法 (广义插入 算法)	141	9.6	习题	180
7.6	压缩与展开操作的硬件 算法	142			
7.6.1	压缩	142	第 10 章 除数为常量的整数 除法	181	
7.6.2	展开	144	10.1	除数为 2 的已知次幂的 带符号除法	181
7.7	通用置换算法及分半操作	145	10.2	求与 2 的已知次幂相除的 带符号余数	182
7.8	重排与下标变换	149	10.3	在除数不是 2 的幂时求 带符号除法及余数	183
7.9	LRU 算法	150	10.3.1	除以 3	183
7.10	习题	153	10.3.2	除以 5	184
			10.3.3	除以 7	185
第 8 章 乘法	154		10.4	除数大于等于 2 的带符号 除法	185
8.1	多字乘法	154	10.4.1	算法	187
8.2	64 位积的高权重部分	156	10.4.2	算法可行性证明 ...	187
8.3	无符号与带符号的高权重 互化	157	10.4.3	证明乘积正确	188
8.4	与常数相乘	157	10.5	除数小于等于 -2 的带符号 除法	191
8.5	习题	160	10.6	将除法算法集成至编译 器中	193
第 9 章 整数除法	162		10.7	其他主题	196
9.1	预备知识	162	10.7.1	唯一性	196
9.2	多字除法	165	10.7.2	可生成最佳程序 代码的除数	197
9.3	用带符号除法计算无符号短 除法	169	10.8	无符号除法	199
9.3.1	用带符号长除法计算 无符号短除法	169	10.8.1	除数为 3 的无符号	
9.3.2	用带符号短除法计算 无符号短除法	169			
9.4	无符号长除法	171			

除法	199	10.17.2 除数大于等于 2 的带符号除法 ...	219
10.8.2 除数为 7 的无符号 除法	200	10.18 不使用 Multiply High 指令 的除法算法	220
10.9 除数大于等于 1 的无符号 除法	201	10.18.1 无符号除法	221
10.9.1 无符号版算法	202	10.18.2 带符号除法	226
10.9.2 算法可行性证明 ...	202	10.19 合计各数位求余数	229
10.9.3 证明无符号版算法的 乘积正确	203	10.19.1 求无符号除法的 余数	229
10.10 将无符号除法算法集成至 编译器中	203	10.19.2 求带符号除法的 余数	232
10.11 与无符号除法相关的其他 话题	205	10.20 用乘法及右移位求 余数	234
10.11.1 可生成最佳无符号 除法代码的 除数	205	10.20.1 求无符号除法的 余数	234
10.11.2 带符号乘法与无 符号乘法互化 ...	206	10.20.2 求带符号除法的 余数	237
10.11.3 更简单的无符号 除法生成算法 ...	206	10.21 将普通除法化为精确 除法	239
10.12 余数非负式除法与向下取 整式除法的适用性	207	10.22 计时测试	240
10.13 类似算法	208	10.23 用电路计算除数为 3 的 除法	241
10.14 神奇数字示例	209	10.24 习题	242
10.15 用 Python 语言编写的 简单代码	210	第 11 章 初等函数	243
10.16 除数为常量的精确除法	211	11.1 整数平方根	243
10.16.1 用欧几里得算法计 算乘法逆元素 ...	212	11.1.1 用牛顿法开 平方	243
10.16.2 用牛顿法计算乘法 逆元素	215	11.1.2 二分查找	246
10.16.3 乘法逆元素 示例	217	11.1.3 硬件算法	247
10.17 检测除以常数后是否 余 0	217	11.2 整数立方根	249
10.17.1 无符号除法	218	11.3 求整数幂	250
		11.3.1 用 n 的二进制分解式 计算 x^n	250
		11.3.2 用 Fortran 语言	

计算 2^n	251	15.2.2 校验位个数的最 小值	290
11.4 整数对数	252	15.2.3 小结	290
11.4.1 以 2 为底的整数 对数	253	15.3 适用于 32 位信息的软件 SEC-DED 算法	292
11.4.2 以 10 为底的整数 对数	253	15.4 广义错误修正	297
11.5 习题	257	15.4.1 汉明距离	298
第 12 章 以特殊值为底的数制 ...	258	15.4.2 编码论的主要 问题	299
12.1 以 -2 为底的数制	258	15.4.3 n 维球面	301
12.2 以 $-1+i$ 为底的数制	264	15.5 习题	305
12.3 以其他数为底的数制	266	第 16 章 希尔伯特曲线	307
12.4 最高效的底是什么	267	16.1 生成希尔伯特曲线的递归 算法	308
12.5 习题	267	16.2 根据希尔伯特曲线上从起点 到某点的途经距离求其坐标 ...	311
第 13 章 格雷码	269	16.3 根据希尔伯特曲线上的坐标 求从起点到某点的途经距离 ...	317
13.1 简介	269	16.4 递增希尔伯特曲线上点的 坐标	319
13.2 递增格雷码整数	271	16.5 非递归的曲线生成算法	321
13.3 负二进制格雷码	272	16.6 其他空间填充曲线	321
13.4 格雷码简史及应用	273	16.7 应用	322
13.5 习题	275	16.8 习题	324
第 14 章 循环冗余校验	276	第 17 章 浮点数	325
14.1 简介	276	17.1 IEEE 格式	325
14.2 理论	277	17.2 整数与浮点数互化	327
14.3 实现	279	17.3 使用整数操作比较浮点数 大小	331
14.3.1 硬件实现	281	17.4 估算平方根倒数	332
14.3.2 软件实现	283	17.5 前导数位的分布	334
14.4 习题	285	17.6 杂项数值表	336
第 15 章 纠错码	286	17.7 习题	338
15.1 简介	286		
15.2 汉明码	287		
15.2.1 SEC-DED 码	289		

第 18 章 素数公式	339	18.5 习题	350
18.1 简介	339	参考答案	351
18.2 Willans 公式	341	附录 A 4 位计算机算术运算表	395
18.2.1 Willans 第二 公式	342	附录 B 牛顿法	400
18.2.2 Willans 第三 公式	342	附录 C 各种离散函数图像	402
18.2.3 Willans 第四 公式	343	参考文献	412
18.3 Wormell 公式	344		
18.4 用公式来描述其他难解的 函数	345		

第 1 章

概述

1.1 记法

本书既不是普通的数学算式教程，也不是单纯的电脑程序算法手册，它讲的是“计算机算术”（computer arithmetic），参与运算的数是长度固定的位串与位元数组^①。计算机算术中的表达式与普通的数学表达式近似，不同之处在于其中的变量指代的是 CPU 寄存器中的内容，而且计算机算术表达式的值是一串不具备特定符号性的位元。在此类表达式中，操作符可能会以不同方式解读其操作数，例如“比较操作符”（comparison operator）有时会将其操作数当成有正负号的二进制整数，有时却把它视为无符号的二进制整数。为避免混淆，本书所列计算机算式以不同的符号来区分上述两种情况。

计算机算式与数学算式的主要差别在于：无论是加减法还是乘法，计算机算式的结果总是要跟 2 的 n 次方取模， n 是指当前机器的字长^②。此外，计算机算式的运算种类也远多于数学算式：除了基本的四则运算外，还有逻辑与、异或、比较、左移，等等。

如未特别指明，则默认字长为 32 位，且带符号的整数均以“2 补码”^③形式表示。

-
- ① bit vector，即 bit array，也写作 bitmap、bitset、bit string 等，是由若干位元排列而成的数组，又叫“位向量”、“位矢量”等，详情参见：https://en.wikipedia.org/wiki/Bit_array。译文在不致混淆时，均以“位元数组”称之。——译者注
 - ② word size，就是字组中所含的位元个数，也称 word length、word width。在不致混淆的情况下，“字长”、“字宽”均指这一概念。——译者注
 - ③ two's complement，也叫“2 的补码”、“二补数”，是一种用二进制表示带符号数字的方式。整数和零的补码表示法与其二进制写法相同，只是左方要补足 0，而要表示负数，则需先将其绝对值按位取反，也就是求绝对值的一补数（也称反码），然后再加 1。例如用 8 位二进制表示数字时，5 可以表示为 0000 0101，而要表示 -5，则需先求其绝对值 5，写成二进制形式 0000 0101，然后对其按位取反得到 1111 1010，再加 1。最终的结果 1111 1011 就是 -5 的补码表示。详情参见：<https://zh.wikipedia.org/wiki/补码>。带符号整数与无符号整数的英文分别为 signed integer 与 unsigned integer，其中“带符号”与“无符号”是计算机处理二进制数的两种不同方式。前者会根据最高有效位来判定数字的正负，0 为非负，1 为负，而后者则一律将其视为非负数。以上面的 1111 1011 来说，若视为带符号整数，则其值为 -5（因最高位为 1，故是负数。先将其按位取反得 0000 0100，再加 1 得 0000 0101，即十进制的 5，再添上负号得 -5），若视为无符号整数，则其值为 251（最高位的 1 不再表示负数，而当做 128 来算）。详情参见：<https://zh.wikipedia.org/wiki/有符号数处理>。——译者注

计算机算式与数学算式的书写方式相同，只是其中指代 CPU 寄存器中内容的变量会以粗体标出。为了和位元数组运算的通则一致，我们把电脑中的字组也视为由一串位元构成的数组。若某常量表示 CPU 寄存器中的值，那么它也会以粗体字出现。（这种情况在位元数组运算中找不到对应物，如果要在位元数组算式里书写常量，只能逐个列出其中的每个位元。）然而常量如果作为 shift 等指令的操作数，则不加粗。

对于“+”这样的操作符，若其操作数为粗体，则表明执行的是计算机加法，也就是“向量加法”，否则意味着执行的是纯数字加法。如果操作数未加粗，则其对应的操作符就是纯数学运算中的含义。要是我们想拿原来做计算机运算的粗体 x 值做数学运算的话，那就会把它写成不加粗的 x ，其符号性应该能够从上下文中推出。假如 $x = 0x8000\ 0000$ ， $y = 0x8000\ 0000$ ，那么在做带符号的整数运算时， $x = y = -2^{31}$ ， $x + y = -2^{32}$ ，而 $x + y = 0^{\ominus}$ 。此处的 $0x8000\ 0000$ 是用十六进制表示的位串，它最左边的位元是“1”，后面跟着 31 个“0”。

位元的序号从右侧算起，最右方的位元（也就是最低有效位）叫做 0 号位元。术语“位”、“半字节”、“字节”、“半字组”、“字组”、“双字”^㉔所对应的位元数量分别是 1、4、8、16、32、64。

简短的代码段用的都是计算机算式，并以左箭头表示赋值操作，偶尔还会用 if 语句。在这种情况下，它只是以一种与电脑平台无关的方式编写汇编语言代码罢了。

过长或过于复杂的计算机算式则用 C 语言来写，其代码遵循 ISO 1999 标准^㉕。

完整描述 C 语言不是本书该做的事，不过书中用到的大部分 C 语言基本表达式 [H & S] 都总结到表 1.1 中了，用过程序语言编程但是不熟悉 C 语言的读者应该看看。表中也列出了笔者在计算机算式中用到的对应操作符，它们按照优先级从高到低的顺序排列（高者先算），在优先级这一列中，L 表示左结合，比如乘号就是左结合的运算符： $a \cdot b \cdot c = (a \cdot b) \cdot c$ ，而 R 则表示右结合^㉖。本书计算机算式里的运算符，其优先级与结合性同 C 语言一致。

表 1.1 C 语言与计算机算术表达式对照表

优先级	C	计算机算式	含义
	0x...	0x... , 0b...	十六进制常数，二进制常数

⊖ 不加粗的 $x + y$ 是普通的数学运算，故结果为 -2^{32} ，而粗体的 $x + y$ 则是按照计算机算术规则做二进制加法，其结果为 1 00000000 00000000 00000000 00000000，也就是 1 后面 32 个零。宽度为 32 的字组无法容纳这个 33 位元的数，故而最高有效位的“1”会被舍去，留下 32 个 0，因此最终的运算结果就是 0。——译者注

㉔ 对应英文写法分别为：bit、nibble、byte、halfword、word、doubleword。——译者注

㉕ 该标准的正式名称是 ISO/IEC 9899:1999，俗称 C99，详情参见：<https://zh.wikipedia.org/wiki/C语言#C99>。C 语言的最新标准是 2011 年发布的 ISO/IEC 9899:2011，俗称 C11。——译者注

㉖ 左结合与右结合的英文分别是 left-associative 与 right-associative，结合性指的是遇到两个相邻的同优先级运算符时，要从左先算还是从右先算。详情参见：https://en.wikipedia.org/wiki/Operator_associativity。——译者注