Daniel H. Greene
Donald E. Knuth

Mathematics for the Analysis of Algorithms

Daniel H. Greene
Donald E. Knuth

Mathematics for the Analysis of Algorithms

1981

Birkhäuser
Boston • Basel • Stuttgart

Authors:

Daniel H. Greene
Department of Computer Science
Stanford University
Stanford, California 94305, USA

Donald E. Knuth
Department of Computer Science
Stanford University
Stanford, California 94305, USA

Library of Congress Cataloging in Publication Data

Greene, David H., 1955-
  Mathematics for the analysis of algorithms.
  (Progress in Computer Science ; v. 1)
  Bibliography: p.
  Includes index.
  1. Electronic digital computers--Programming.
2. Algorithms. I. Knuth, Donald E. II. Title.
III. Series.
QA76.6.G7423 519.4 81-38484
ISBN 3-7643-3046-5 AACR2

CIP - Kurztitelaufnahme der Deutschen Bibliothek

Greene, Daniel H.:
Mathematics for the analysis of algorithms/
Daniel H. Greene ; Donald E. Knuth.-
Boston ; Basel ; Stuttgart : Birkhäuser, 1981.
  (Progress in Computer Science ; Vol. 1)
  ISBN 3-7643-3046-5
NE: Knuth, Donald E.:; GT

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without prior permission of the copyright owner.

©Birkhäuser Boston, 1981

ISBN 3-7643-3046-5
Printed in USA

Table of Contents

此为试读,需要完整PDF请访问: www.ertongbook.com

Preface

This monograph assembles the handouts for Computer Science 255 at Stanford University, an advanced course on the analysis of algorithms. The course presents examples of the major paradigms used in the precise analysis of algorithms, emphasizing some of the more difficult ones. Much of the material is drawn from the starred sections of *The Art of Computer Programming*, Volume 3 [Knuth III].

Analysis of algorithms, as a discipline, relies heavily on both computer science and mathematics. This report is a mathematical look at the synthesis—emphasizing the mathematical perspective, but using motivation and examples from computer science. It covers binomial identities, recurrence relations, operator methods and asymptotic analysis, hopefully in a format that is terse enough for easy reference and yet detailed enough to be of use to those who have not attended Computer Science 255. However, it is assumed that the reader is familiar with the fundamentals of complex variable theory and combinatorial analysis.

Winter 1980 was the fourth offering of Computer Science 255 and credit is due to the previous teachers and staff—Leo Guibas, Scott Drysdale, Sam Bent, Andy Yao and Phyllis Winkler—for their detailed contributions to the documentation of the course. Portions of earlier handouts are incorporated in this monograph. Harry Mairson, Andrei Broder, Ken Clarkson, and Jeff Vitter contributed helpful comments and corrections, and the preparation of these notes was also aided by the facilities of Xerox corporation and the support of NSF and Hertz graduate fellowships. The material itself was typeset with the TEX composition system, using the Computer Modern family of fonts recently developed with the **METAFONT** system.

Table of Contents

Chapter 1

Binomial Identities

1.1 Summary of Useful Identities

So that the identities themselves do not become buried on an obscure page, we summarize them immediately:

$$(x+y)^n = \sum_k \binom{n}{k} x^k y^{n-k}, \qquad \begin{array}{c}\text{integer } n \\ \text{or } n \text{ real and } |x/y| < 1\end{array} \tag{1.1}$$

$$\binom{r}{k} = \binom{r-1}{k} + \binom{r-1}{k-1}, \qquad \begin{array}{c}\text{real } r \\ \text{integer } k\end{array} \tag{1.2}$$

$$\binom{n}{k} = \binom{n}{n-k}, \qquad \begin{array}{c}\text{integer } n \geq 0 \\ \text{integer } k\end{array} \tag{1.3}$$

$$\binom{r}{k} = \frac{r}{k}\binom{r-1}{k-1}, \qquad \begin{array}{c}\text{real } r \\ \text{integer } k \neq 0\end{array} \tag{1.4}$$

$$\sum_{k=0}^{n} \binom{r+k}{k} = \binom{r+n+1}{n}, \qquad \begin{array}{c}\text{real } r \\ \text{integer } n \geq 0\end{array} \tag{1.5}$$

$$\sum_{k=0}^{n} \binom{k}{m} = \binom{n+1}{m+1}, \qquad \text{integer } m, n \geq 0 \tag{1.6}$$

$$\binom{-r}{k} = (-1)^k \binom{r+k-1}{k}, \qquad \begin{array}{c}\text{real } r \\ \text{integer } k\end{array} \tag{1.7}$$

$$\binom{r}{m}\binom{m}{k}=\binom{r}{k}\binom{r-k}{m-k}, \qquad \begin{array}{c}\text{real } r\\ \text{integer } m, k\end{array} \tag{1.8}$$

$$\sum_k \binom{r}{k}\binom{s}{n-k}=\binom{r+s}{n}, \qquad \text{integer } n \tag{1.9}$$

$$\sum_k \binom{r}{k}\binom{s}{n+k}=\binom{r+s}{r+n}, \qquad \begin{array}{c}\text{integer } n\\ \text{integer } r \geq 0\end{array} \tag{1.10}$$

$$\sum_k \binom{r}{k}\binom{s+k}{n}(-1)^k=(-1)^r\binom{s}{n-r}, \qquad \begin{array}{c}\text{integer } n\\ \text{integer } r \geq 0\end{array} \tag{1.11}$$

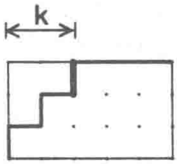
$$\sum_{k=0}^{r} \binom{r-k}{m}\binom{s+k}{n}=\binom{r+s+1}{m+n+1}, \qquad \begin{array}{c}\text{integer } m, n, r, s \geq 0\\ n \geq s\end{array} \tag{1.12}$$

One particularly confusing aspect of binomial coefficients is the ease with which a familiar formula can be rendered unrecognizable by a few transformations. Because of their chameleon character there is no substitute for practice of manipulations with binomial coefficients. The reader is referred to Section 1.2.6 of [Knuth I] for an explanation of the formulas above and for a useful collection of exercises. A large catalog of sums of binomial coefficients, arranged according to the number of terms in the numerator and denominator of the summand, appears in [Gould 72].

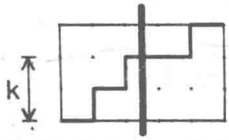
此为试读，需要完整PDF请访问：www.ertongbook.com

1.2 Deriving the Identities

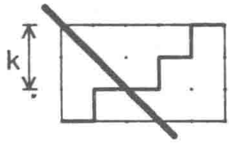
Here is an easy way to remember many of the identities that do not include an alternating -1. The number of paths through a rectangular lattice with sides m and n is $\binom{m+n}{m}$. By cutting the lattice along different axes, and counting the paths according to where they cross the cut, the identities are derived. The pictures below show different ways of partitioning the paths and the parameter k used in the sum.



A sum based on when the path hits the top edge derives identity (1.5)



Counting paths according to when they cross a vertical line derives identity (1.12)



Similarly, a sum based on a slanted line derives identity (1.9)

More complicated identities can be derived by successive applications of the identities given on pages 5 and 6. One example appears in "A trivial algorithm whose analysis isn't," by A. Jonassen and D. E. Knuth [Jonassen 78]. The sum

$$S = \sum_k \binom{m}{k} \left(-\frac{1}{2}\right)^k \binom{2k}{k} \tag{1.13}$$

is evaluated by a lengthy series of elementary transformations. Rather than include their derivation, we give instead a derivation suggested by I. Gessel. He attributes this elegant technique, the "method of coefficients," to G. P. Egorychev.

First replace k by $m-k$, giving

$$S=\sum_k \binom{m}{k}\left(-\frac{1}{2}\right)^{m-k}\binom{2m-2k}{m-k}. \tag{1.14}$$

Using $\langle x^n\rangle f(x)$ for the coefficient of x^n in $f(x)$ we can express portions of the sum with generating functions:

$$\binom{m}{k}\left(-\frac{1}{2}\right)^{-k}=\langle x^k\rangle(1-2x)^m \tag{1.15}$$

$$\binom{2m-2k}{m-k}=\langle y^{m-k}\rangle(1+y)^{2m-2k}. \tag{1.16}$$

The whole sum is

$$S=\left(-\frac{1}{2}\right)^m\sum_k\langle x^k\rangle(1-2x)^m\langle y^{m-k}\rangle(1+y)^{2m-2k}. \tag{1.17}$$

We can remove $\langle y^{m-k}\rangle$ from the sum by noting that $\langle y^{m-k}\rangle=\langle y^m\rangle y^k$:

$$S=\left(-\frac{1}{2}\right)^m\langle y^m\rangle(1+y)^{2m}\sum_k\langle x^k\rangle(1-2x)^m\left(\frac{y}{(1+y)^2}\right)^k. \tag{1.18}$$

Finally, this seemingly aimless wandering comes to a glorious finish. The sum in the last formula is a simple substitution for x:

$$S=(-2)^{-m}\langle y^m\rangle(1+y)^{2m}\left(1-\frac{2y}{(1+y)^2}\right)^m; \tag{1.19}$$

$$S=(-2)^{-m}\langle y^m\rangle(1+y^2)^m. \tag{1.20}$$

The solution follows immediately:

$$S=\begin{cases}2^{-m}\binom{m}{m/2}, & m \text{ even};\\ 0, & m \text{ odd}.\end{cases} \tag{1.21}$$

From a theoretical standpoint, it would be nice to unify binomial identities in one coherent scheme, much as the physicist seeks a unified field theory. Unfortunately no single scheme covers everything. There are however several "meta" concepts that explain the existence of large classes of binomial identities. We will briefly describe two of these: inverse relations and operator calculus.

1.3 Inverse Relations

One of the simplest set of inverse relations is the pair

$$a_n = \sum_k (-1)^k \binom{n}{k} b_k, \qquad b_n = \sum_k (-1)^k \binom{n}{k} a_k, \tag{1.22}$$

which follows from the orthogonal relation

$$\delta_{nk} = \sum_{j=k}^{n} (-1)^{j+k} \binom{n}{j} \binom{j}{k}. \tag{1.23}$$

And this is just a specialization of equation (1.11) with s equal to zero. In general an inverse relation will pair two series so that individual terms of one can be computed from the terms of the other. There will always be an associated orthogonal relation.

In his book *Combinatorial Identities*, John Riordan devotes several chapters to inverse relations. Since inverse relations are even more likely to change appearance than the binomial identities we have seen already, care must be taken to recognize relations that are basically the same. For this purpose Riordan describes several transformations and then groups equivalent inverse pairs into broad categories. His transformations and classifications are summarized below.

Since we are working with a pair of equations, we can move terms from one equation to another by replacements like $b'_k = (-1)^k b_k$, obtaining a new pair

$$a_n = \sum_k \binom{n}{k} b'_k, \qquad b'_k = \sum_k (-1)^{k+n} \binom{n}{k} a_k. \tag{1.24}$$

An inverse relation corresponds to a pair of lower triangular matrices whose product is the identity. By reflecting across the diagonal we can derive yet another pair

$$a_n = \sum_{k \geq n} \binom{k}{n} b_k, \qquad b_n = \sum_{k \geq n} (-1)^{k+n} \binom{k}{n} a_k. \tag{1.25}$$

Finally, note that we can multiply both sides of the orthogonal relation (1.23) by almost any function that is unity when $n = k$, without affecting the orthogonal character of the equation.

The last equation, (1.25), has an extremely useful combinatorial significance. Suppose we have a large collection of random events. Let b_n be the probability that *exactly* n events occur, and let a_n be the sum of the probability of n simultaneous events taken over all selections of n events. Roughly speaking a_n can be viewed as a sloppy way of computing the probability that exactly n events occur since it makes no allowance for the possibility of more than n events. The left side of (1.25) shows how a_n is inflated. However, a_n is often easier to compute and the right hand side of equation (1.25), the "principle of inclusion and exclusion," provides a practical way of obtaining b_n.

Equations (1.22), (1.24) and (1.25) are in the simplest class of inverse relations. [Riordan 68] lists several other classes like the Chebyshev-type:

$$a_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{k} b_{n-2k}, \qquad b_n = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{n}{n-k} \binom{n-k}{k} a_{n-2k}. \quad (1.26)$$

Not surprisingly the inverse relations are often associated with their namesakes among the orthogonal polynomials used in interpolation.

The Gould-type class of inverse relations,

$$f_n = \sum_k (-1)^k \binom{n}{k} \binom{a+bk}{n} g_k, \quad (1.27)$$

$$g_n \binom{a+bn}{n} = \sum_k (-1)^k \frac{a+bk-k}{a+bn-k} \binom{a+bn-k}{n-k} f_k, \quad (1.28)$$

has a very curious property. A Chinese mathematician L. Hsu recently discovered that the binomial coefficients containing a and b are inessential to the functioning of the inversion. In fact if we choose $\{a_i\}$ and $\{b_i\}$ to be any two sequences of numbers such that

$$\psi(x,n) = \prod_{i=1}^{n} (a_i + b_i x) \neq 0, \qquad \text{integer } x, n \geq 0, \quad (1.29)$$

we obtain a general inversion:

$$f_n = \sum_k (-1)^k \binom{n}{k} \psi(k,n)\, g_k, \quad (1.30)$$

$$g_n = \sum_k (-1)^k \binom{n}{k} (a_{k+1} + k\, b_{k+1}) \psi(n,k+1)^{-1} f_k. \quad (1.31)$$

Stirling numbers are used in another well known pair of inverse relations:

$$a_n = \sum_{k=0}^{n} (-1)^{n-k} \begin{bmatrix} n \\ k \end{bmatrix} b_k, \quad \left[{n \atop k}\right] \equiv \text{Stirling numbers of the first kind;} \tag{1.32}$$

$$b_n = \sum_{k=0}^{n} \begin{Bmatrix} n \\ k \end{Bmatrix} a_k, \quad \left\{{n \atop k}\right\} \equiv \text{Stirling numbers of the second kind.} \tag{1.33}$$

Here a_n is usually $x^{\underline{n}}$ and b_n is x^n, so that these formulas convert between factorials and powers of x.

We cannot explore all the inverse relations here, but it is worth noting that many generating functions can be converted to inverse relations. A pair of power series $z(x)$ and $z^*(x)$ such that $z(x)\,z^*(x) = 1$ provide a pair of relations:

$$a(x) = z(x)\,b(x), \quad \text{and} \quad b(x) = z^*(x)\,a(x). \tag{1.34}$$

For example, we can let $z(x) = (1-x)^{-p}$ and $z^*(x) = (1-x)^p$; clearly $z(x)\,z^*(x) = 1$, so we can proceed to compute formulas for the coefficients in $a(x)$ and $b(x)$:

$$a_n = \sum_k (-1)^k \binom{-p}{k} b_{n-k}, \qquad b_n = \sum_k (-1)^k \binom{p}{k} a_{n-k}. \tag{1.35}$$

This pair is a member of the Gould class of inverse relations.

Inverse relations are partially responsible for the proliferation of binomial identities. If one member of an inverse pair can be embedded in a binomial identity, then the other member of the pair will often provide a new identity. Inverse relations can also enter directly into the analysis of an algorithm. The study of radix exchange sort, for example, uses the simple set of relations (1.22) introduced at the beginning of this section. For details see [Knuth III; exercises 5.2.2–36 and 5.2.2–38].

1.4 Operator Calculus

Here are several common operators, and their effects on functions:

The shift operator E:

$$E^a p(x) = p(x+a) \tag{1.36}$$

The derivative operator D:

$$D\,p(x) = p'(x) \tag{1.37}$$

The difference operator $\Delta = E^1 - I$:

$$\Delta\,p(x) = p(x+1) - p(x) \tag{1.38}$$

Following [Rota 75] we will find it useful to define a D-type operator to be any operator that behaves like the derivative operator. Specifically, an operator Q is D-type if it is shift invariant ($Q\,E^a = E^a\,Q$) and if $Q\,x$ is a nonzero constant. From these two properties it is possible to show that Q operators resemble the derivative:

i) $Q\,a = 0$ for every constant a

ii) Q(nth degree polynomial) = (($n-1$)st degree polynomial).

We can push this resemblance even further by defining a sequence of basic polynomials for Q as follows:

$$\begin{aligned} &\text{i)}\ \ p_0(x) = 1 \\ &\text{ii)}\ \ p_n(0) = 0, \quad n > 0 \\ &\text{iii)}\ Q\,p_n(x) = n\,p_{n-1}(x). \end{aligned}$$

The third property means that whenever Q is applied to its basic polynomials the result is similar to D applied to $1, x, x^2 \ldots.$ For example, Δ is a D-type operator with basic polynomials $x^{\underline{n}} = x(x-1)\ldots(x-n+1)$.

It turns out that D-type operators are a very useful generalization of the derivative. Taylor's expansion theorem can be cast in the general form

$$T = \sum_k \frac{a_k}{k!} Q^k \tag{1.39}$$

where

T is any shift invariant operator;

Q is a D-type operator with basic polynomials $p_k(x)$;

$a_k = [T\,p_k(x)]_{x=0}$.

此为试读,需要完整PDF请访问: www.ertongbook.com