LTCC Advanced Mathematics Series - Volume 3

Algebra, Logic and Combinatorics

Shaun Bullett
Tom Fearn
Frank Smith
editors

World Scientific

LTCC Advanced Mathematics Series - Volume 3

Algebra, Logic and Combinatorics

Editors

Shaun Bullett
Queen Mary University of London, UK

Tom Fearn
University College London, UK

Frank Smith
University College London, UK

World Scientific

NEW JERSEY · LONDON · SINGAPORE · BEIJING · SHANGHAI · HONG KONG · TAIPEI · CHENNAI · TOKYO

Published by

World Scientific Publishing Europe Ltd.

57 Shelton Street, Covent Garden, London WC2H 9HE

Head office: 5 Toh Tuck Link, Singapore 596224

USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601

Library of Congress Cataloging-in-Publication Data

Names: Bullett, Shaun, 1967– | Fearn, T., 1949– | Smith, F. T. (Frank T.), 1948–

Title: Algebra, logic, and combinatorics / [edited by]
Shaun Bullett (Queen Mary University of London, UK),
Tom Fearn (University College London, UK),
Frank Smith (University College London, UK).

Description: New Jersey : World Scientific, 2016. |
Series: LTCC advanced mathematics series ; volume 3

Identifiers: LCCN 2015049552| ISBN 9781786340290 (hc : alk. paper) |
ISBN 9781786340306 (pbk : alk. paper)

Subjects: LCSH: Algebra. | Logic, Symbolic and mathematical. | Combinatorial analysis. |
Differential equations.

Classification: LCC QA155 .A525 2016 | DDC 510--dc23

LC record available at http://lccn.loc.gov/2015049552

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

Desk Editors: R. Raghavarshini/Mary Simpson

Typeset by Stallion Press
Email: enquiries@stallionpress.com

Printed by FuIsland Offset Printing (S) Pte Ltd Singapore

Algebra, Logic and Combinatorics

LTCC Advanced Mathematics Series

Published

Vol. 2 Fluid and Solid Mechanics
edited by Shaun Bullett, Tom Fearn & Frank Smith

Vol. 3 Algebra, Logic and Combinatorics
edited by Shaun Bullett, Tom Fearn & Frank Smith

Forthcoming

Vol. 1 Advanced Techniques in Applied Mathematics
edited by Shaun Bullett, Tom Fearn & Frank Smith

Preface

The *London Taught Course Centre (LTCC) for PhD students in the Mathematical Sciences* has the objective of introducing research students to a broad range of advanced topics. For some students, these topics might include one or two in areas directly related to their PhD projects, but the relevance of most will be much less clear or even apparently non-existent. However, all of us involved in mathematical research have experienced that extraordinary moment when the penny drops and some tiny gem of information from outside one's immediate research field turns out to be the key to unravelling a seemingly insoluble problem, or to opening up a new vista of mathematical structure. By offering our students advanced introductions to a range of different areas of mathematics, we hope to open their eyes to new possibilities that they might not otherwise encounter.

Each volume in this series consists of chapters on a group of related themes, based on modules taught at the LTCC by their authors. These modules were already short (five two-hour lectures) and in most cases the lecture notes here are even shorter, covering perhaps three-quarters of the content of the original LTCC course. This brevity was quite deliberate on the part of the editors: we asked contributors to keep their chapters short in order to allow as many topics as possible to be included in each volume, whilst keeping the volumes digestible. The chapters are "advanced introductions", and readers who wish to learn more are encouraged to continue elsewhere. There has been no attempt to make the coverage of topics comprehensive. That would be impossible in any case — any book or series of books which included all that a PhD student in mathematics might need to know would be so large as to be totally unreadable. Instead, what we present in this series is a cross-section of some of the topics, both classical and new, that have appeared in LTCC modules in the nine years since it was founded.

The present volume covers the general area of algebra, logic and combinatorics. The main readers are likely to be graduate students and more experienced researchers in the mathematical sciences, looking for introductions to areas with which they are unfamiliar. The mathematics presented is intended to be accessible to first year PhD students, whatever their specialised areas of research, though we appreciate that how "elementary" or "advanced" any particular chapter appears to be will differ widely from reader to reader. Whatever your mathematical background, we encourage you to dive in, and we hope that you will enjoy reading these concise introductory accounts written by experts at the forefront of current research.

Shaun Bullett, Tom Fearn, Frank Smith

Contents

Chapter 1

Enumerative Combinatorics

Peter J. Cameron

School of Mathematical Sciences,
*Queen Mary University of London, London E1 4NS, UK**
pjc20@st-andrews.ac.uk

This chapter presents a very brief introduction to enumerative combinatorics. After a section on formal power series, it discusses examples of counting subsets, partitions and permutations; techniques for solving recurrence relations; the inclusion–exclusion principle; the Möbius function of a poset; q-binomial coefficients; and orbit-counting. A section on the theory of species (introduced by André Joyal) follows. The chapter concludes with a number of exercises, some of which are worked.

1. Introduction

Combinatorics is the science of arrangements. We want to arrange objects according to certain rules, for example, digits in a sudoku grid. We can break the basic question into three parts:

- Is an arrangement according to the rules possible?
- If so, how many different arrangements are there?
- What properties (for example, symmetry) do the arrangements possess?

Enumerative combinatorics provides techniques for answering the second of these questions.

Unlike the case of sudoku, we are usually faced by an infinite sequence of problems indexed by a natural number n. So if a_n is the number of solutions to the problem with index n, then the solution of the problem is a sequence $(a_0, a_1, \ldots)$ of natural numbers. We combine these into a single

*Current address: School of Mathematics and Statistics, University of St Andrews, North Haugh, St Andrews KY16 9SS, UK.

object, a formal power series, sometimes called the *generating function* of the sequence. In the next section, we will briefly sketch the theory of formal power series.

For example, consider the problem:

Problem 1. *How many subsets of a set of size n are there?*

Of course, the answer is 2^n. The generating function is

$$\sum_{n\geq 0} 2^n x^n = \frac{1}{1-2x}.$$

Needless to say, in most cases we cannot expect such a complete answer!

In the remainder of the chapter, we examine some special cases, treating some of the important principles of combinatorics (such as counting up to symmetry and inclusion–exclusion).

An important part of the subject involves finding good asymptotic estimates for the solution; this is especially necessary if there is no simple formula for it. Space does not permit a detailed account of this; see Flajolet and Sedgewick [4] or Odlyzko [10].

The chapter concludes with some suggestions for further reading.

To conclude this section, recall the definition of the binomial coefficients:

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 1}.$$

A familiar problem of elementary combinatorics asks for the number of ways in which k objects can be chosen from a set of n, under various combinations of sampling rules:

	Without replacement	With replacement
Order significant	$n(n-1)\dots(n-k+1)$	n^k
Order not significant	$\binom{n}{k}$	$\binom{n+k-1}{k}$

2. Formal Power Series

2.1. *Definition*

It is sometimes said that formal power series were the 19th-century analogue of random-access memory.

Suppose that $(a_0, a_1, a_2, \dots)$ is an infinite sequence of numbers. We can wrap up the whole sequence into a single object, the *formal power series*

$A(x)$ in an indeterminate x given by

$$A(x) = \sum_{n \geq 0} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots .$$

We have not lost any information, since the numbers a_n can be recovered from the power series:

$$a_n = \frac{1}{n!} \frac{\mathrm{d}^n}{\mathrm{d}x^n} A(x)\Big|_{x=0}.$$

Of course, we will have to think carefully about what is going on here, especially if the power series doesn't converge, so that we cannot apply the techniques of analysis.

In fact, it is very important that our treatment should not depend on using analytic techniques. We define formal power series and operations on them abstractly, but at the end it is legitimate to think that formulae like the above are valid, and questions of convergence do not enter. So operations on formal power series are not allowed to involve infinite sums, for example; but finite sums are legitimate. The "coefficients" will usually be taken from some number system, but may indeed come from any commutative ring with identity.

Here is a brief survey of how it is done.

A *formal power series* is defined as simply a sequence $(a_n)_{n \geq 0}$; but keep in mind the representation of it as a formal sum $\sum a_n x^n$. Now:

- Addition and scalar multiplication are defined term-by-term:

$$\left(\sum a_n x^n\right) + \left(\sum b_n x^n\right) = \sum (a_n + b_n) x^n,$$
$$c\left(\sum a_n c^n\right) = \sum (c a_n) x^n.$$

- Multiplication of series is by the *convolution rule* (mysterious in the abstract, but clear in the series representation)

$$\left(\sum a_n x^n\right)\left(\sum b_n x^n\right) = \sum c_n x^n,$$

where

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

- Differentiation of series (which will be denoted by D rather than $\mathrm{d}/\mathrm{d}x$) is term-by-term, using the rule that $\mathrm{D}(x^n) = n x^{n-1}$:

$$\mathrm{D}\left(\sum_{n \geq 0} a_n x^n\right) = \sum_{n \geq 1} n a_n x^{n-1} = \sum_{n \geq 0} (n+1) a_{n+1} x^n.$$

Note that, in the rule for product, the expression for c_n is a finite sum.

With the above addition and multiplication, the set $R[[x]]$ of all formal power series over a commutative ring R with identity is a commutative ring with identity. The third operation makes it a *differential ring*. This just says that differentiation is R-linear and that *Leibniz' law*

$$\mathrm{D}(AB) = A(\mathrm{D}B) + (\mathrm{D}A)B,$$

holds.

Other operations on formal power series are possible. For example, we can form infinite sums and products, provided these only involve finite sums and products of coefficients. For example, if $(a_n^{(i)})$ are sequences with the property that, for any n, there exists m such that $a_n^{(i)} = 0$ for all $i > m$, then we can form $\sum_{i\geq 0} A_i$, where $A_i = \sum_{n\geq 0} a_n^{(i)} x^n$. For the coefficient of x^n in this infinite sum is the *finite* sum

$$\sum_{i=0}^{m} a_n^{(i)}.$$

We can substitute a formal power series $B(x)$ for x in another formal power series $A(x)$ provided that the constant term of B is zero. For the series $B(x)^i$ has the coefficients of $1, x, x^2, \ldots, x^{i-1}$ all zero; so by the preceding paragraph,

$$A(B(x)) = \sum_{i\geq 0} a_i B(x)^i$$

is well-defined.

You are invited to formulate a sufficient condition for the infinite product $\prod A_i(x)$ to be defined.

A formal power series $A(x)$ in $R[[x]]$ is invertible if and only if its constant term a_0 is invertible in R. To see this, consider the equation

$$\left(\sum a_n x^n\right)\left(\sum b_n x^n\right) = 1.$$

The constant term shows that $a_0 b_0 = 1$, so it is necessary that a_0 is invertible. But if a_0 is invertible, then the equation for the coefficient of x^n is

$$\sum_{k=0}^{n} a_k b_{n-k} = 0,$$

so that

$$b_n = -a_0^{-1}\left(\sum_{k=1}^{n} a_k b_{n-k}\right),$$

so b_n can be found recursively as a linear combination of $b_0, \ldots, b_{n-1}$.

An important special case is: a formal power series with constant term 1 is invertible (and its inverse also has constant term 1).

2.2. *Classical examples*

If the coefficients of a formal power series are numbers (as they will almost always be), then the series may or may not converge for a particular value of x. Recall from complex analysis that, for any power series with complex coefficients, there is a number $R \in [0, \infty]$ (a non-negative real number or infinity) with the properties

- If $|x| < R$, then $\sum a_n x^n$ converges;
- If $|x| > R$, then $\sum a_n x^n$ diverges.

We say that R is the *radius of convergence*; the behaviour of the series for $|x| = R$ is not specified. The interpretation of the extreme values is that, if $R = \infty$, then the series converges for all x, while if $x = 0$, then the series diverges for all $x \neq 0$.

If a series has non-zero radius of convergence, then it defines a complex analytic function inside its circle of convergence. This gives us several more techniques that can be used. For example,

- We can use Cauchy's integral formulae to evaluate the derivatives at the origin (the coefficients of the series);
- If some identity between power series is known for analytic reasons, then it holds in the ring of formal power series.

There are three very important series:

- The *exponential series*

$$\exp(x) = \sum_{n \geq 0} \frac{x^n}{n!}.$$

(We usually write $\exp(x)$ rather than e^x.)

- The *logarithmic series*

$$\log(1+x) = \sum_{n \geq 1} \frac{(-1)^{n-1} x^n}{n}.$$

- The *binomial series*, for any complex number a:

$$(1+x)^a = \sum_{n \geq 0} \binom{a}{n} x^n,$$

where $\binom{a}{n}$ is the *binomial coefficient*

$$\binom{a}{n} = \frac{a(a-1)\dots(a-n+1)}{n!}.$$

Note that the binomial series has only finitely many terms if a is a non-negative integer, since in that case if $n > a$ then the numerator of the binomial coefficient $\binom{a}{n}$ contains a factor $a - a = 0$. However, in all other cases, it is an infinite series.

Now various familiar properties hold, for example:

- $\exp(\log(1+x)) = 1+x$, $\log(1+(\exp(x)-1)) = x$ (the series $\exp(x)-1$ has constant term zero and so can be substituted into the logarithmic series);
- More generally, $\exp(a\log(1+x)) = (1+x)^a$;
- The laws of exponents hold, for example $(1+x)^a(1+x)^b = (1+x)^{a+b}$, or $((1+x)^a)^b = (1+x)^{ab}$. (For the second, we have to write $(1+x)^a = 1 + A(x)$ for some power series $A(x)$.)

As said above, all these facts have analytic proofs, and therefore hold for the power series. However, we have the possibility of either finding proofs of the identities by combinatorial manipulations, or alternatively, of unpacking the combinatorial content of the equations to prove combinatorial identities.

Here is a simple example. Consider the identity

$$(1+x)^a(1+x)^b = (1+x)^{a+b}.$$

Calculating the coefficient of x^n on both sides, and using the formula for multiplication of formal power series, we obtain our first example of a *binomial coefficient identity*:

Theorem 1 (Vandermonde convolution).

$$\sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k} = \binom{a+b}{n}.$$

An even simpler example is the one discussed in the introduction:

$$(1-2x)^{-1} = \sum_{n\geq 0} (2x)^n,$$

an example of a geometric series.

2.3. *Generalisations*

The simple notion of formal power series described here can be extended in several ways. Here are a few:

- We will often represent a sequence (a_n) by its *exponential generating function*

$$\sum_{n\geq 0} \frac{a_n x^n}{n!}.$$

  We will see that this arises naturally in counting "labelled" objects.
- A *Laurent series* can admit a finite number of negative powers of x:

$$A(x) = \sum_{n\geq n_0} a_n x^n,$$

  where n_0 may be negative. Of course, we could allow arbitrary negative as well as positive powers of x; but then the sum in the convolution rule for the product of two series would be infinite, so this doesn't work.
- We can consider formal power series in more than one variable, expressions of the form

$$A(x,y) = \sum_{m,n\geq 0} a_{m,n} x^m y^n.$$

  We see that a formal power series in two variables is the generating function for a two-dimensional array of numbers. Nothing new is required, since $A(x,y)$ belongs to the ring of formal power series in the indeterminate y over the ring $R[[x]]$.
- We can even allow infinitely many indeterminates (as long as each term only involves finitely many of them).
- There are other completely different kinds of series. Number theorists like the *Dirichlet series* which represents a sequence $(a_n)_{n\geq 1}$ by the series

$$\sum_{n\geq 1} \frac{a_n}{n^s}.$$

  There is a framework which includes both kinds of series, but that is beyond the scope of this chapter.

3. Subsets, Partitions, Permutations

We have met very little combinatorics yet. The most important combinatorial objects are subsets, partitions, and permutations, and these provide many counting problems, to which we now turn.

3.1. *Subsets*

The Binomial Theorem for non-negative integers n states:

Theorem 2 (Binomial Theorem).

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

This is a polynomial in x. Substituting $x = 1$, we obtain

$$2^n = \sum_{k=0}^{n} \binom{n}{k}.$$

The left-hand side of this equation is the number of subsets of the set $\{1, 2, \ldots, n\}$. On the right-hand side, we use a familiar interpretation of the binomial coefficients: $\binom{n}{k}$ is the number of k-element subsets of $\{1, 2, \ldots, n\}$. Since every subset has a unique cardinality in the range $0, \ldots, n$, we see why the equation is true. Indeed, once we have verified the counting interpretation of the binomial coefficients, we have given a bijective proof of the Binomial Theorem for non-negative integer exponents. (The term "bijective proof" refers to an argument which shows that two expressions are equal by finding a bijection or matching between sets counted by the two expressions.)

There is a huge industry of finding and verifying *binomial coefficient identities*. In the preceding section, we met the Vandermonde convolution (written here with different variables)

$$\sum_{l=0}^{k} \binom{n}{l}\binom{m}{k-l} = \binom{n+m}{k}.$$

Here is a bijective proof. Take a class of $n + m$ children, of whom n are girls and m are boys. We wish to pick a team made up of k of the children in the class. This can obviously be done in $\binom{n+m}{k}$ ways. Alternatively, we could choose a number l between 0 and k, and select l of the n girls,