Linear Recurrences

An Introduction

Carlo Sanna

Politecnico di Torino

version 1.2 (Second Draft), November 30, 2025

How to cite this book:

Plaintext:
Carlo Sanna, Linear Recurrences, 2025, available at:
https://github.com/carlo-sanna-math/books/

BibTeX:
```
@misc{SannaLR2025,
    author       = {Sanna, Carlo},
    title        = {Linear {R}ecurrences},
    howpublished = {available at:
    \url{https://github.com/carlo-sanna-math/books/}},
    year         = {2025},
}
```

to Ansel

Contents

Preface

Subject

Linear recurrences occur across nearly every area of pure and applied mathematics.

In algebra and geometry, they appear as the entries of matrix powers and as the coefficients of power series representing rational functions, including Hilbert series, generating functions in group theory, and zeta functions of algebraic varieties.

In analysis and probability theory, linear recurrences include many important families of orthogonal polynomials, arise from evaluating solutions to differential equations, and describe probabilities associated with transitions between states of Markov chains.

In number theory, linear recurrences include well-studied integer sequences such as those of Fibonacci and Mersenne numbers, arise as solutions to Diophantine equations and as the sequences of partial quotients of continued fractions of quadratic irrational numbers.

In combinatorics, they count paths between vertices of directed graphs and, more generally, they are the counting sequences for a wide range of combinatorial classes.

In computer science, they make it possible to realize efficient pseudorandom number generators and count the number of words accepted by a finite automaton or described by a regular expression.

Purpose

The purpose of this book is to introduce the reader to the theory of linear recurrences in its most common and useful settings: over an arbitrary field, a finite field, a field of characteristic zero, and—for readers with a number-theoretic inclination—the ring of integers. Still, the subject is so vast that a complete account is impossible. Instead, this book provides a survey of the main results and proof methods. It may serve as a reference, a textbook for a short course, or a resource for self-study.

Some words about topics missing from this book. Except where particularly relevant, this book does not focus on special families of linear recurrences, such as polynomial sequences, Lucas sequences, Pierce sequences, and Lehmer sequences. The reason is that these sequences have distinctive properties that do not reflect the general behavior of linear recurrences. In addition, this book does not develop the theory of linear recurrences over an arbitrary commutative ring. The rationale is twofold. First, the theory over a commutative ring lacks the elegance found in the field case and involves numerous technical complications.

Second, including it might make the material less accessible to readers who are not deeply familiar with ring theory or commutative algebra.

Prerequisites

The prerequisites for an uninterrupted reading of this book are a basic knowledge of linear algebra (matrices, vector spaces, linear maps, ...), field theory (field extensions, trace, norm, ...), and algebraic number theory (ring of integers of a number field, S-integers, p-adic numbers, ...). These topics should be familiar to a graduate student in mathematics who has taken at least one course in algebraic number theory.

Structure

This book consists of six chapters.

Chapter 1 provides the basic definitions regarding linear recurrences and, as a motivation to the study of the subject, collects several examples of linear recurrences coming from many fields of pure and applied mathematics, such as number theory, algebra, analysis, graph theory, probability theory, computer science, group theory, and combinatorics.

Chapter 2 develops the theory of linear recurrences over an arbitrary field. It introduces the three main perspectives to approach the subject, that is, the *power-sum representation*, the *companion matrix*, and the correspondence with *rational functions*; and it provides the key results on linear recurrences and their operations.

Chapter 3 is devoted to a special class of linear recurrences: the *ultimately periodic sequences*. This short chapter provides the main results on this important class of linear recurrences.

Chapter 4 focuses on the rich theory of linear recurrences over a finite field. It provides the main results on the least period and the distribution of the values of such linear recurrences.

Chapter 5 deals with linear recurrences over fields of characteristic zero or, more specifically, number fields. The main topics are the important *Skolem–Mahler–Lech theorem* on the structure of the set of zeros, results on the growth of the terms, and the *Hadamard quotient theorem* about the ratio of two linear recurrences.

Chapter 6 concerns linear recurrences over the ring of integers and addresses results and questions of a number-theoretic nature. It examines the divisibility properties, the reductions modulo integers, the prime factors, the primality, and the compositeness of the terms of linear recurrences.

The Appendix, which is for the reader convenience, contains some results used sparsely through this book and not fitting in a precise chapter.

Except for Chapter 1, each chapter ends with two sections titled "Bibliographical notes" and "Exercises".

The "Bibliographical notes" section contains the references to the original books and papers on which the chapter's results are based. A special mention goes to the monumental monograph "Recurrence Sequences" by Everest, van der Poorten, Shparlinski, and Ward [55],

which was essential to the development of this book. In addition, the "Bibliographical notes" section provides historical context and highlights generalizations of the results and related research topics.

The "Exercises" section provides a list of exercises that the readers can use to test their comprehension of the material of the chapter. Software for symbolic computation is useful for solving some of the exercises. A very good option is SageMath [165], which is open source and released under the GNU General Public Licence GPLv2+,

Acknowledgments

The author is deeply grateful to Christian Ballot and Paolo Leonetti whose insightful suggestions have greatly enhanced the quality of this book.

Conventions

Italic font emphasizes technical terms, either when introducing a definition (e.g., A *linear recurrence* over $\mathcal{R}$ is…) or when referring to a term defined elsewhere (e.g., …from the theory of *Weierstrass elliptic functions*). Bold fonts are reserved for sequences, vectors, and matrices. The empty sum and the empty product are equal to 0 and 1, respectively.

The notation used throughout this book is largely standard. However, the following table provides a summary for easy reference. It may be skipped on a first reading and consulted later if needed.

$\mathbb{N}$	set of natural numbers, including 0
$\mathbb{Z}$	ring of integers
$\mathbb{Z}^+$	set of positive integers
$\mathbb{Q}$	field of rational numbers
$\mathbb{R}$	field of real numbers
$\mathbb{C}$	field of complex numbers
$\mathbb{F}_q$	a finite field of q elements
$\mathbb{Z}_p$	ring of p-adic integers
$\mathbb{Q}_p$	field of p-adic numbers
$\mathcal{R}$	a commutative ring with unity
$\mathbb{K}$	a field
$\mathrm{char}(\mathbb{K})$	characteristic of the field $\mathbb{K}$
$\mathcal{O}_{\mathbb{K}}$	ring of integers of the number field $\mathbb{K}$
$\mathcal{O}_S$	ring of S-integers of a number field
$\mathrm{N}_{\mathbb{L}/\mathbb{K}}$	field norm of the finite extension $\mathbb{L}/\mathbb{K}$
$\mathrm{tr}_{\mathbb{L}/\mathbb{K}}$	field trace of the finite extension $\mathbb{L}/\mathbb{K}$
$\mathcal{R}[x, y, \dots]$	ring of polynomials in the variables $x, y, \dots$ with coefficients in $\mathcal{R}$
$\mathcal{R}[[x, y, \dots]]$	ring of formal power series in $x, y, \dots$ with coefficients in $\mathcal{R}$
$\deg f$	degree of the polynomial f
$\mathrm{res}_x(f, g)$	resultant of the polynomials f and g with respect to the variable x
$\varnothing$	empty set
$\mathcal{A}^{\mathbb{N}}$	set of sequences $\boldsymbol{u} = (u_n)_{n\in\mathbb{N}}$ with elements in $\mathcal{A}$

$\mathcal{A}^{\mathbb{Z}}$	set of double infinite sequences $\boldsymbol{u} = (u_n)_{n\in\mathbb{Z}}$ with elements in $\mathcal{A}$
$\lvert\mathcal{A}\rvert$	cardinality of the finite set $\mathcal{A}$
$\mathcal{A} \setminus \mathcal{B}$	difference of the sets $\mathcal{A}$ and $\mathcal{B}$
$\mathcal{A} \times \mathcal{B}$	cartesian product of the sets $\mathcal{A}$ and $\mathcal{B}$
$\mathcal{R}^{m\times n}$	set of $m \times n$ matrices with entries in $\mathcal{R}$
$\boldsymbol{0}$	zero sequence, zero vector, or zero matrix
$\boldsymbol{I}$	identity matrix
$\delta_{i,j}$	Kronecker symbol, which is equal to 1 if $i = j$, and to 0 if $i \neq j$
$\boldsymbol{e}_i$	vector with all entries equal to 0 except for the ith entry, which is equal to 1 ($\boldsymbol{e}_i$ is a column or a row depending from the context)
$\boldsymbol{A}^{\intercal}$	transpose of the matrix $\boldsymbol{A}$
$\boldsymbol{A}_{i,j}$	entry of the ith row and jth column of the matrix $\boldsymbol{A}$
$\mathrm{tr}(\boldsymbol{A})$	trace of the square matrix $\boldsymbol{A}$
$\det(\boldsymbol{A})$	determinant of the square matrix $\boldsymbol{A}$
$\dim(V)$	dimension of the vector space V
$\lfloor x \rfloor$	the maximum integer less than or equal to x
$\lceil x \rceil$	the minimum integer greater than or equal to x
$\binom{n}{k}$	binomial coefficient, with $\binom{n}{k} := 0$ if $k < n$ or $k > n$
$a \mid b$	"a divides b"
gcd	greatest common divisor
lcm	least common multiple
$\mathbb{i}$	imaginary unit
$\mathrm{Re}(z)$	real part of the complex number z
$\mathrm{Im}(z)$	imaginary part of the complex number z
e	Neper number (base of the natural logarithm)
log	principal branch of the complex logarithm
$\log_b$	logarithm in base b
exp	exponential function
$\langle a, b, \dots \rangle$	subgroup generated by $a, b, \dots$
$\mathrm{ord}(a)$	multiplicative order of the element a of a group
ν_p	p-adic valuation (more generally $\nu_{\mathfrak{p}}$, for a prime ideal $\mathfrak{p}$)
$\lvert\cdot\rvert_p$	p-adic norm (more generally $\lvert\cdot\rvert_{\mathfrak{p}}$, for a prime ideal $\mathfrak{p}$)
μ	Möbius function
φ	Euler totient function
$f(n) \sim g(n)$	asymptotic notation for $\lim f(n)/g(n) = 1$
$f(n) = o\big(g(n)\big)$	asymptotic notation for $\lim f(n)/g(n) = 0$
$f(n) = O\big(g(n)\big)$	"there exists a constant $C > 0$ such that $\lvert f(n)\rvert < C\lvert g(n)\rvert$"

Chapter 1

Introduction

1.1 Basic definitions

Let $\mathcal{R}$ be a commutative ring. A *linear recurrence*[1] over $\mathcal{R}$ is a sequence $\boldsymbol{u} \in \mathcal{R}^{\mathbb{N}}$ for which there exist $a_1, \ldots, a_k \in \mathcal{R}$ such that

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k}, \tag{1.1}$$

for all integers $n \geq k$. The relation (1.1) is a *kth-order linear recurrence relation*. The elements $u_0, \ldots, u_{k-1}$ are the *initial values* of $\boldsymbol{u}$ with respect to the relation (1.1). Note that the initial values $u_0, \ldots, u_{k-1}$ and the coefficients $a_1, \ldots, a_k$ recursively determine every term of $\boldsymbol{u}$ via (1.1). The polynomial

$$f(x) := x^k - a_1 x^{k-1} - a_2 x^{k-2} - \cdots - a_k \tag{1.2}$$

is the *characteristic polynomial*[2] of the linear recurrence relation (1.1). For short, the polynomial f is also "the" characteristic polynomial of the linear recurrence $\boldsymbol{u}$. However, every linear recurrence satisfies infinitely many linear recurrence relations, and consequently it has infinitely many characteristic polynomials. The *order* of a linear recurrence $\boldsymbol{u} \neq \boldsymbol{0}$ is the minimal positive integer k such that $\boldsymbol{u}$ satisfies a kth-order linear recurrence relation; and the order of the zero sequence $\boldsymbol{0} \in \mathcal{R}^{\mathbb{N}}$ is equal to 0.

Some authors refer to (1.1) as a *homogeneous* kth-order linear recurrence relation and use the term *inhomogeneous* kth-order linear recurrence relation for a relation of the form

$$u_n = a_1 u_{n-1} + a_2 u_{n-2} + \cdots + a_k u_{n-k} + b, \tag{1.3}$$

for all integers $n \geq k$, where $b \in \mathcal{R} \setminus \{0\}$ is fixed. It is not difficult to check that if $\boldsymbol{u}$ satisfies the inhomogeneous kth-order linear recurrence relation (1.3) then $\boldsymbol{u}$ satisfies a homogeneous $(k+1)$th-order linear recurrence relation with characteristic polynomial $(x-1)f(x)$. Thus

[1] Alternative names are: *linear recurrence sequence* [55], *linear recurring sequence* [115], *linear recurrent sequence* [3], *linearly recurrent sequence* [191], *C-finite sequence* [91], and many others.

[2] Some authors call it the *companion polynomial* [57].

it suffices to study homogeneous linear recurrence relations. If $\boldsymbol{u} \in \mathcal{R}^{\mathbb{Z}}$ then $\boldsymbol{u}$ is a *linear recurrence* if (1.1) holds for every integer n.

This book focuses on linear recurrences over a field $\mathbb{K}$. This provides a sufficiently general setting for most applications and makes it possible to take advantage of linear algebra. Note that this setting also includes the case of linear recurrences over an integral domain $\mathcal{R}$, by taking $\mathbb{K}$ as the field of fractions of $\mathcal{R}$.

1.2 Examples

This section illustrates the ubiquity and broad relevance of linear recurrences by providing several examples drawn from different fields of pure and applied mathematics. Some examples are elementary, others rely on more advanced terminology and background theory (and might parenthetically refer to results of the next chapter), and yet others touch on concepts beyond the scope of this book.

1.2.1 Basic examples

Example 1.1 (Constant sequence)**.** Let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ be a *constant sequence*, that is, $u_n = u_0$ for all integers $n \geq 0$. Then $\boldsymbol{u}$ satisfies the first-order linear recurrence relation $u_n = u_{n-1}$ for each integer $n \geq 1$. Hence, the constant sequence $\boldsymbol{u}$ is a linear recurrence with initial value u_0 and characteristic polynomial $x - 1$.

Example 1.2 (Geometric progression)**.** Let $a, r \in \mathbb{K}$. The *geometric progression* with *initial value* a and *common ratio* r is the sequence $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ defined by $u_n := ar^n$ for each integer $n \geq 0$. It follows that $\boldsymbol{u}$ satisfies the first-order linear recurrence relation $u_n = ru_{n-1}$ for each integer $n \geq 1$. Hence, the geometric progression $\boldsymbol{u}$ is a linear recurrence with initial value a and characteristic polynomial $x - r$.

Example 1.3 (Arithmetic progression)**.** Let $a, d \in \mathbb{K}$. The *arithmetic progression* with *initial value* a and *common difference* (or *modulo*) d is the sequence $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ defined by $u_n := a + dn$ for every integer $n \geq 0$. It follows easily that $\boldsymbol{u}$ satisfies the first-order inhomogeneous linear recurrence relation $u_n = u_{n-1} + d$ for each integer $n \geq 1$. Hence, the arithmetic progression $\boldsymbol{u}$ is a linear recurrence with initial values $a, a + d$ and characteristic polynomial $(x - 1)^2$.

Example 1.4 (Polynomial sequence)**.** Let $f \in \mathbb{K}[x]$ and let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ be the *polynomial sequence* defined by $u_n := f(n)$ for all integers $n \geq 0$. Then $\boldsymbol{u}$ is a linear recurrence with characteristic polynomial $(x - 1)^k$, where $k := 0$ if f is the zero polynomial and $k := \deg(f) + 1$ otherwise (see Theorem 2.15).

Example 1.5 (Ultimately periodic sequence)**.** A sequence $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ is *ultimately periodic* if there exist integers $n_0 \geq 0$ and $t > 0$ such that $u_n = u_{n-t}$ for each integer $n \geq n_0 + t$. Hence, if $\boldsymbol{u}$ is ultimately periodic then $\boldsymbol{u}$ is a linear recurrence with initial values $u_0, \ldots, u_{n_0+t-1}$ and characteristic polynomial $x^{n_0}(x^t - 1)$.

1.2.2 Fibonacci numbers, Mersenne numbers, and Lucas sequences

Example 1.6 (Fibonacci numbers)**.** The most famous example of a linear recurrence is the sequence of *Fibonacci numbers* (F_n), which is defined by the initial values $F_0 = 0$, $F_1 = 1$, and the second-order linear recurrence relation $F_n = F_{n-1} + F_{n-2}$ for each integer $n \geq 2$. Fibonacci numbers are named after the Italian mathematician Leonardo Pisano (Leonardo of Pisa), also known as Leonardo Fibonacci (filius Bonacci, Latin for "son of Bonacci"), who introduced them in an exercise about addition in his 1202 book "Liber Abaci". However, Fibonacci numbers were known as early as 200 BC in ancient Indian mathematics. They have been, and continue to be, widely studied by both professional mathematicians and amateur enthusiasts. Fibonacci numbers appear in computer science, number theory, and combinatorics, as well as in art, literature, music, and movies. The "Fibonacci Association" [24], founded in 1962 [16, Section 2], is a mathematical organization entirely devoted to the study of Fibonacci numbers. It publishes its mathematical journal, the "Fibonacci Quarterly" [25], four times a year, and hosts an international conference every two years.

Example 1.7 (Mersenne numbers)**.** The sequence of *Mersenne numbers* (M_n) is defined by $M_n := 2^n - 1$ for every integer $n \geq 0$. It is named in honor of Marin Mersenne, a French monk and polymath who studied it in the early 17th century. It is easy to verify that $M_n = 3M_{n-1} - 2M_{n-2}$ for every integer $n \geq 2$. Thus (M_n) is a linear recurrence with characteristic polynomial $x^2 - 3x + 2$. Mersenne numbers have many interesting number-theoretic properties. A *Mersenne prime* is a Mersenne number that is prime. It can be proved that a necessary condition for M_n to be prime is that n is prime. (This condition is not sufficient, since $M_{11} = 23 \cdot 89$.) A *perfect number* is a positive integer that is equal to the sum of its proper divisors. For example, the number 6 is a perfect number since its proper divisors are $1, 2, 3$ and $6 = 1 + 2 + 3$. The *Euclid–Euler theorem* states that the even perfect numbers are exactly the integers of the form $2^{p-1}M_p$, where p is prime and M_p is a Mersenne prime. (On the other hand, it is unknown whether odd perfect numbers exist. This is likely the oldest unsolved problem in mathematics.) As to date, the largest known prime number is the Mersenne prime $M_{136,279,841}$ [64].

Example 1.8 (Lucas sequence)**.** A *Lucas sequence* is a linear recurrence $\boldsymbol{u}$ over $\mathbb{Z}$ with initial values $u_0 = 0$, $u_1 = 1$, and satisfying the second-order linear recurrence relation $u_n = a_1 u_{n-1} + a_2 u_{n-2}$ for every integer $n \geq 2$, where $a_1, a_2 \in \mathbb{Z}$ and $a_2 \neq 0$. Édouard Lucas introduced Lucas sequences in 1876. Both the sequence of Fibonacci numbers ($a_1 = a_2 = 1$) and the sequence of Mersenne numbers ($a_1 = 3$, $a_2 = -2$) are Lucas sequences. There is a rich theory on Lucas sequences, including their divisibility properties, the structure of the prime factorization of their terms, and their applications in primality testing and factorization algorithms. For these topics and more, see the book by Ballot and Williams [9].

1.2.3 Examples from number theory

Example 1.9 (Solutions to the Pell equation)**.** Let d be a positive integer that is not a square. The *Pell equation* of parameter d is the Diophantine equation

$$s^2 - dt^2 = 1 \tag{1.4}$$

where the unknowns s and t are restricted to be positive integers. Despite the name, the mathematician John Pell never studied this equation. Euler mistakenly attributed a solution method to Pell and the name stuck. The first result on Pell equation states that (1.4) has infinitely many solutions. The *fundamental solution* is the unique solution (s_1, t_1) for which $s_1 + t_1\sqrt{d}$ is minimal. The formulas

$$s_n = \frac{\left(s_1 + t_1\sqrt{d}\right)^n + \left(s_1 - t_1\sqrt{d}\right)^n}{2}, \qquad t_n = \frac{\left(s_1 + t_1\sqrt{d}\right)^n - \left(s_1 - t_1\sqrt{d}\right)^n}{2\sqrt{d}}, \tag{1.5}$$

where n is a positive integer, give every solution (s_n, t_n) to (1.4). It is convenient to set $s_0 := 1$ and $t_0 := 0$, so that the equations (1.5) hold also for $n = 0$. From (1.5) it follows (see Corollary 2.16) that (s_n) and (t_n) are linear recurrences with characteristic polynomial

$$\left(x - \left(s_1 + t_1\sqrt{d}\right)\right)\left(x - \left(s_1 - t_1\sqrt{d}\right)\right) = x^2 - 2s_1x + 1.$$

For an extensive treatise on the Pell equation, see the book by Jacobson and Williams [84].

Example 1.10 (Numerators and denominators of convergents of continued fractions of quadratic irrationals)**.** A *continued fraction* is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}}, \tag{1.6}$$

where a_0 is an integer and $a_1, a_2, \ldots$ are positive integers. The integers $a_0, a_1, \ldots$ are the *partial quotients* of (1.6). More precisely, define recursively the expressions $[a_0, \ldots, a_n]$ by

$$[a_0] := a_0 \quad \text{and} \quad [a_0, a_1, \ldots, a_{n+1}] := a_0 + \frac{1}{[a_1, a_2, \ldots, a_{n+1}]}$$

for each integer $n \geq 0$. The term $[a_0, \ldots, a_n]$ is the nth *convergent* of (1.6). The continued fraction (1.6) is the limit

$$\lim_{n \to +\infty} [a_0, a_1, \ldots, a_n],$$

which exists and is finite. In fact, every irrational real number α is equal to a unique continued fraction (1.6), where $a_0, a_1, \ldots$ are computed recursively by the formulas

$$\begin{aligned} a_0 &= \lfloor \alpha \rfloor, & t_0 &:= \alpha - a_0, \\ a_{n+1} &= \lfloor 1/t_n \rfloor, & t_{n+1} &:= 1/t_n - a_{n+1}, \end{aligned}$$

for every integer $n \geq 0$. Continued fractions play a fundamental role in the field of *Diophantine approximation*, which studies how well irrational real numbers can be approximated by rational numbers. Indeed, in a precise sense, the convergents $[a_0, \ldots, a_n]$ are the best rational approximations to α.

Let α be an irrational real number, let (a_n) be the sequence of the partial quotients of the continued fraction of α, and let (p_n) and (q_n) be the sequences of integers defined by

$[a_0, \dots, a_n] = p_n/q_n$, $q_n > 0$, and $\gcd(p_n, q_n) = 1$, for each integer $n \geq 0$. A famous theorem of Lagrange states that α is a quadratic irrational if and only if (a_n) is ultimately periodic. A lesser-known theorem due to Lenstra and Shallit [114] asserts that α is a quadratic irrational if and only if (p_n) is a linear recurrence; if and only if (q_n) is a linear recurrence. For a concise introduction to continued fractions, see the book by Hardy and Wright [78, Chapter X].

Example 1.11 (Ramanujan's τ function at powers of a prime)**.** The *Ramanujan τ function* is the function $\tau\colon \mathbb{Z}^+ \to \mathbb{Z}$ defined by the formal identity

$$\sum_{n=1}^{\infty} \tau(n) x^n = x \prod_{k=1}^{\infty} \bigl(1 - x^k\bigr)^{24}. \tag{1.7}$$

Its first values are

$$1,\ -24,\ 252,\ -1472,\ 4830,\ -6048,\ -16744,\ 84480,\ -113643,\ -115920,$$

for $n = 1, \dots, 10$. The formula (1.7) might appear to be cryptic, but it stems naturally from the theory of *modular forms*. Indeed, for $x = \mathrm{e}^{2\pi \mathbb{i} z}$ with $z \in \mathbb{C}$ and $\operatorname{Im}(z) > 0$, the right-hand side of (1.7) is the *modular discriminant* $\Delta(z)$, which is a cusp form of weight 12 coming from the theory of *Weierstrass elliptic functions*. For modular forms in number theory, see the book by Apostol [4].

Mordell [135] proved that τ is a multiplicative arithmetic function, that is,

$$\tau(mn) = \tau(m)\tau(n)$$

for all coprime positive integers m and n. He also showed that

$$\tau(p^n) = \tau(p)\tau\bigl(p^{n-1}\bigr) - p^{11}\tau\bigl(p^{n-2}\bigr),$$

for every prime number p and for each integer $n \geq 2$. (Ramanujan [155] had previously conjectured these properties.) Therefore, for every prime number p, the sequence $\bigl(\tau(p^n)\bigr)$ is a linear recurrence.

1.2.4 Examples from analysis

Example 1.12 (Linear differential equations)**.** Let $a_1, \dots, a_k \in \mathbb{C}$ and let $f\colon \mathbb{R} \to \mathbb{C}$ be a solution to the *kth-order homogeneous linear differential equation* with constant coefficients

$$f^{(k)} = a_1 f^{(k-1)} + \cdots + a_{k-1} f' + a_k f, \tag{1.8}$$

where $f^{(n)}$ is the nth derivative of f. Repeatedly differentiating both sides (1.8) and evaluating at a fixed $x_0 \in \mathbb{R}$ yields

$$f^{(n)}(x_0) = a_1 f^{(n-1)}(x_0) + \cdots + a_{k-1} f'(x_0) + a_k f(x_0),$$

for every integer $n \geq k$. Hence, the sequence $\bigl(f^{(n)}(x_0)\bigr)$ is a linear recurrence.

Example 1.13 (Basis of Fourier series)**.** Let $f\colon [0,2\pi] \to \mathbb{R}$ be an integrable function. The *Fourier series* of f at $\theta \in [0,2\pi]$ is the expression

$$\frac{a_0}{2} + \sum_{n=1}^{\infty} \big(a_n \cos(n\theta) + b_n \sin(n\theta)\big),$$

where

$$a_n := \frac{1}{\pi}\int_0^{2\pi} f(\theta)\cos(n\theta)\,\mathrm{d}\theta \quad \text{and} \quad b_n := \frac{1}{\pi}\int_0^{2\pi} f(\theta)\sin(n\theta)\,\mathrm{d}\theta.$$

A classic result states that if f is differentiable over $(0,2\pi)$ and its derivative is continuous then the Fourier series of f at $\theta \in (0,2\pi)$ converges to $f(\theta)$. The functions $\cos(n\theta)$ and $\sin(n\theta)$ form the *basis* of Fourier series. From the addition formulas for cosine and sine, it follows that both sequences of functions $\big(\cos(n\theta)\big)$ and $\big(\sin(n\theta)\big)$ are linear recurrences with characteristic polynomial $x^2 - (2\cos\theta)x + 1$. For a clear introduction to Fourier series, see the book by Folland [59, Chapter 2].

Example 1.14 (Chebyshev polynomials)**.** The sequence of *Chebyshev polynomials* (T_n) is a linear recurrence of polynomials in $\mathbb{Z}[y]$ defined by the initial values $T_0 = 1$, $T_1 = y$, and the linear recurrence relation $T_n = 2yT_{n-1} - T_{n-2}$ for every integer $n \geq 2$. Chebyshev polynomials play a fundamental role in interpolation theory, approximation theory, numerical integration, numerical analysis, and ergodic theory. They satisfy the trigonometric identity

$$T_n(\cos\theta) = \cos(n\theta),$$

for every integer $n \geq 0$ and every real number θ, and the orthogonality relation

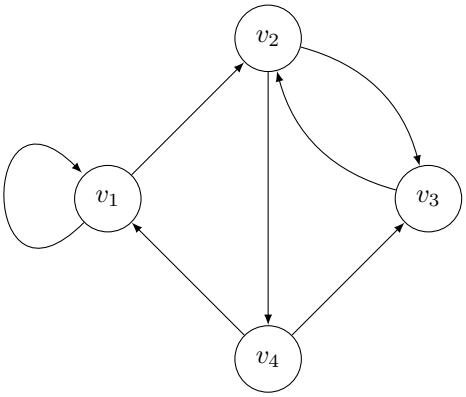
$$\frac{2}{\pi}\int_{-1}^{1} T_m(y)T_n(y)\frac{\mathrm{d}y}{\sqrt{1-y^2}} = \delta_{m,n}$$

for all positive integers m and n. The book by Rivlin [159] provides an excellent account of Chebyshev polynomials.

1.2.5 Examples from algebra

Example 1.15 (Trace of powers of algebraic numbers)**.** Let $\mathbb{L}/\mathbb{K}$ be a finite field extension, let $\alpha \in \mathbb{L}$, let $f \in \mathbb{K}[x]$ be the minimal polynomial of α over $\mathbb{K}$, and let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ be the sequence defined by $u_n := \mathrm{tr}_{\mathbb{L}/\mathbb{K}}(\alpha^n)$ for each integer $n \geq 0$. From the linearity of the trace function over $\mathbb{K}$, and from the fact that $f(\alpha) = 0$, it follows that $\boldsymbol{u}$ is a linear recurrence with characteristic polynomial f (cf. Theorem 2.20).

Example 1.16 (Entries of powers of matrices)**.** Let k be a positive integer, let $\boldsymbol{s} \in \mathbb{K}^{1\times k}$, $\boldsymbol{A} \in \mathbb{K}^{k\times k}$, $\boldsymbol{t} \in \mathbb{K}^{k\times 1}$, and let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ be the sequence defined by $u_n := \boldsymbol{s}\boldsymbol{A}^n\boldsymbol{t}$ for each integer $n \geq 0$. From the Cayley–Hamilton theorem, it follows that $\boldsymbol{u}$ is a linear recurrence (see Theorem 2.23). In particular, for fixed $i, j \in \{1,\ldots,k\}$, the sequence $\big(\boldsymbol{A}^n\big)_{i,j}$ is a linear recurrence.



$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

Figure 1.1: A directed graph and its adjacency matrix.

1.2.6 Examples for graph theory, probability theory, and computer science

Example 1.17 (Number of paths on directed graphs)**.** A *directed graph* $\mathcal{G}$ is a pair $(\mathcal{V}, \mathcal{E})$ consisting of a finite set $\mathcal{V}$ and a subset $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$. The elements of $\mathcal{V}$ are the *vertices* and the elements of $\mathcal{E}$ are the *edges* of the directed graph $\mathcal{G}$. Given two vertices $v, w \in \mathcal{V}$, a *path* of length ℓ from v to w is a sequence $v_1, \ldots, v_\ell$ of vertices of $\mathcal{G}$ such that $v_1 = v$, $(v_i, v_{i+1}) \in \mathcal{E}$ for each $i \in \{1, \ldots, \ell - 1\}$, and $v_\ell = w$. Let $v_1, \ldots, v_k$ be a fixed enumeration of the vertices of $\mathcal{G}$. The *adjacency matrix* of $\mathcal{G}$ is the $k \times k$ matrix $\boldsymbol{A}$ defined by $A_{i,j} := 1$ if $(v_i, v_j) \in \mathcal{E}$, and $A_{i,j} := 0$ if $(v_i, v_j) \notin \mathcal{E}$, for all $i, j \in \{1, \ldots, k\}$. Directed graphs are depicted diagrammatically representing each vertex by a node and each edge (v, w) by an arrow from the vertex v to the vertex w, see Figure 1.1. Directed graphs have countless applications. They provide a powerful model for network-like phenomena such as communication systems, transportation, social interactions, and biological processes. For an extensive introduction, see the book by Bang-Jensen and Gregory [10].

Fix $i, j \in \{1, \ldots, k\}$. Let $\boldsymbol{u}$ be the sequence such that u_n is the number of paths of length n from v_i to v_j, for every integer $n \geq 0$. From the definition of matrix product it follows easily that $u_n = (\boldsymbol{A}^n)_{i,j}$ for each integer $n \geq 0$. Hence, by Example 1.16, the sequence $\boldsymbol{u}$ is a linear recurrence.

Example 1.18 (Weights of paths on weighted directed graphs)**.** A *weighted directed graph* is a directed graph $\mathcal{G}$ such that each of its edges has attached a *weight*, which can be either a formal variable or a real number. The *weight* of a path $v_1, \ldots, v_\ell$ of $\mathcal{G}$ is the product of all the weights of the edges (v_i, v_{i+1}) for $i = 1, \ldots, \ell - 1$. Fix an enumeration $v_1, \ldots, v_k$ of the vertices of $\mathcal{G}$, and let $w_{i,j}$ be the weight of the edge (v_i, v_j), for all $i, j \in \{1, \ldots, k\}$. The *adjacency matrix* of $\mathcal{G}$ is the $k \times k$ matrix $\boldsymbol{W}$ defined by $W_{i,j} := w_{i,j}$ if (v_i, v_j) is an edge of $\mathcal{G}$, and $W_{i,j} := 0$ otherwise, for all $i, j \in \{1, \ldots, k\}$.

Fix $i, j \in \{1, \ldots, k\}$. Let $\boldsymbol{u}$ be the sequence such that u_n is the sum of the weights of all the paths of length n from v_i to v_j, for every integer $n \geq 0$. From the definition of matrix product it follows easily that $u_n = (\boldsymbol{W}^n)_{i,j}$ for each integer $n \geq 0$. Hence, by Example 1.16,

the sequence $\boldsymbol{u}$ is a linear recurrence.

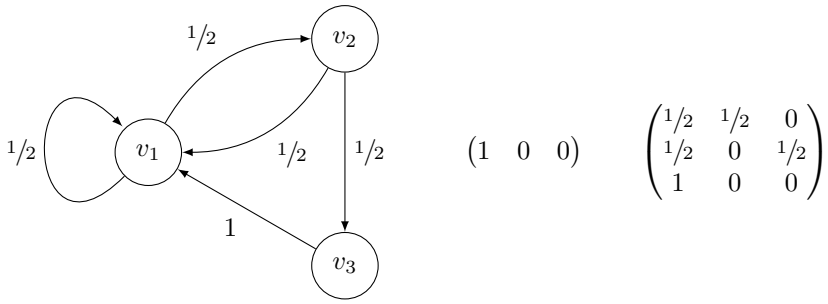


Figure 1.2: A Markov chain, its initial distribution, and its transition matrix. Starting from state v_1 at time $n = 0$, at each time step the random process moves from state v_i to state v_{i+1} (with $v_4 := v_1$) with probability $1/2$ and goes back to state v_1 with probability $1/2$.

Example 1.19 (Probability of reaching a state of a Markov chain)**.** A *(discrete time-homogeneous) Markov chain* is a weighted directed graph $\mathcal{G}$ with k vertices together with a vector $\boldsymbol{s} \in \mathbb{R}^{1\times k}$ such that:

(i) the weights of $\mathcal{G}$ and the entries of $\boldsymbol{s}$ belong to the real interval $[0, 1]$;

(ii) the sum of the entries of each row of the weighted adjacency matrix $\boldsymbol{W}$ of $\mathcal{G}$ is equal to 1 (that is, $\boldsymbol{W}$ is a *stochastic matrix*);

(iii) the sum of the entries of $\boldsymbol{s}$ is equal to 1.

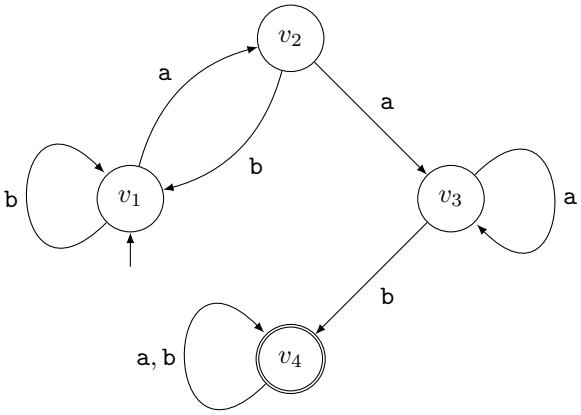
The vertices $v_1, \ldots, v_k$ of $\mathcal{G}$, the vector $\boldsymbol{s}$, and the matrix $\boldsymbol{W}$ are the *states*, the *initial distribution*, and the *transition matrix* of the Markov chain, respectively.

A Markov chain describes the behavior of a random process $\mathcal{P}$ that evolves at discrete times $n = 0, 1, 2, \ldots$, and at each time n it is in exactly one of the states $v_1, \ldots, v_k$. The ith entry of $\boldsymbol{s}$ is the probability that at the initial time $n = 0$ the process $\mathcal{P}$ is in the state v_i. The weight of each edge (v_i, v_j) of $\mathcal{G}$ is the probability that at the next time step $\mathcal{P}$ moves from state v_i to state v_j. Hence, the probability that $\mathcal{P}$ will move to a certain state at the next time step depends only on the current state of $\mathcal{P}$ (*Markov property*). See Figure 1.2 for an example.

Markov chains have a multitude of applications, including mathematical modeling, statistics, data science, and machine learning. For a clear introduction to the subject, see the book by Privault [152].

Fix $i \in \{1, \ldots, k\}$. Let $\boldsymbol{u}$ be the sequence such that u_n is the probability that $\mathcal{P}$ is in the state v_i after n time steps. Then, by Example 1.18, $u_n = \boldsymbol{s}\boldsymbol{W}^n\boldsymbol{e}_i$ for each integer $n \geq 0$. In turn, by Example 1.16, it follows that $\boldsymbol{u}$ is a linear recurrence.

Example 1.20 (Number of words accepted by a finite automaton)**.** An *alphabet* is a finite set Σ. The elements of Σ are the *letters* of Σ. A *(deterministic) finite automaton* $\mathcal{A}$ is a directed graph, whose vertices are called *states*, such that:



$$\begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

Figure 1.3: A finite automaton over the alphabet $\{\mathtt{a}, \mathtt{b}\}$ and its transition matrix. The initial state is v_1 (highlighted by the incoming arrow) and the accepting state is v_4 (highlighted by the double circle). The words accepted by this finite automaton are those containing the pattern `aab`.

(i) there is a unique state called the *initial state*;

(ii) some (possibly none) states are called *accepting states*;

(iii) each edge of $\mathcal{A}$ is labeled with one or more letters from Σ;

(iv) for each state a of $\mathcal{A}$ and each letter $\ell \in \Sigma$, there is at most one edge starting from a and whose label contain ℓ.

A *word* of length n over Σ is a finite sequence $w_1, \ldots, w_n$ of letters from Σ, including the *empty word*, which is denoted by ϵ. A word $w_1, \ldots, w_n$ is *accepted* by the finite automaton $\mathcal{A}$ if there exists a path $v_1, \ldots, v_n$ of $\mathcal{A}$ such that:

(a) v_1 is the initial state of $\mathcal{A}$;

(b) the letter w_i appears in the label of the edge (v_i, v_{i+1}) for each $i \in \{1, \ldots, n-1\}$;

(c) v_n is an accepting state of $\mathcal{A}$.

If $v_1, \ldots, v_k$ are the states of the finite automaton $\mathcal{A}$, then the *transition matrix* of $\mathcal{A}$ is the $k \times k$ matrix $\boldsymbol{T}$ such that $T_{i,j}$ is the number of letters $\ell \in \Sigma$ appearing in the label of (v_i, v_j) (0 if (v_i, v_j) is not an edge of $\mathcal{A}$). See Figure 1.3 for an example. Finite automata provide a model for simple computers with bounded memory and are of fundamental importance in computer science. See the book by Hopcroft, Motvani, and Ullman [82] for an introduction.

Assume that v_1 is the initial state. Let $\boldsymbol{t} \in \mathbb{R}^{k \times 1}$ be the vector such that $t_i := 1$ if v_i is an accepting state, and $t_i = 0$ otherwise, and let $\boldsymbol{u}$ be the sequence such that u_n is the number of words of length n that are accepted by $\mathcal{A}$. In a way similar to Examples 1.17, 1.18, and 1.19, it follows that $u_n = \boldsymbol{e}_1 \boldsymbol{T}^n \boldsymbol{t}$ for each integer $n \geq 0$. Hence, by Example 1.16, the sequence $\boldsymbol{u}$ is a linear recurrence.

Example 1.21 (Number of words described by a regular expression)**.** As in Example 1.20, let Σ be an alphabet. The *concatenation* of two (possibly empty) words $\boldsymbol{a} = a_1, \ldots, a_m$ and $\boldsymbol{b} = b_1, \ldots, b_n$ over Σ is the word $\boldsymbol{ab} = a_1, \ldots, a_m, b_1, \ldots, b_n$. A *language* over Σ is a set of words over Σ. *Regular expressions* over Σ are defined recursively as follows.

(i) The empty word ϵ is a regular expression representing the *empty language* $\varnothing$.

(ii) For each $a \in \Sigma$ the single-letter word a is a regular expression representing the *singleton language* $\{a\}$.

(iii) If R_1 and R_2 are two regular expressions representing the languages $\mathcal{L}_1$ and $\mathcal{L}_2$, respectively, then:

- $R_1 \mid R_2$ (*alternation*) is a regular expression representing the language $\mathcal{L}_1 \cup \mathcal{L}_2$;
- $R_1 R_2$ (*concatenation*) is a regular expression representing the language
$$\mathcal{L}_1 \mathcal{L}_2 := \{\boldsymbol{w}_1 \boldsymbol{w}_2 : \boldsymbol{w}_1 \in \mathcal{L}_1,\ \boldsymbol{w}_2 \in \mathcal{L}_2\};$$
- R_1^* (*Kleene star*) is a regular expression representing the language
$$\mathcal{L}_1^* := \{\epsilon\} \cup \{\boldsymbol{w}_1 \cdots \boldsymbol{w}_n : n \in \mathbb{Z}^+,\ \boldsymbol{w}_1, \ldots, \boldsymbol{w}_n \in \mathcal{L}_1\}.$$

By convention, the Kleene star has the highest priority, followed by concatenation, and then alternation. For example, if $\Sigma = \{\mathtt{a}, \mathtt{b}, \mathtt{c}\}$ then $\mathtt{a}(\mathtt{b} \mid \mathtt{c})^*$ is a regular expression representing the language
$$\mathcal{L} = \{\mathtt{a}, \mathtt{ab}, \mathtt{ac}, \mathtt{abb}, \mathtt{abc}, \mathtt{acb}, \mathtt{acc}, \ldots\}$$
containing each word whose first letter is equal to `a` and each subsequence letter is either equal to `b` or `c`. A language over Σ is a *regular language* if it can be represented by a regular expression. Regular languages have several important applications including text searching and pattern matching, lexical analysis in programming language compilation, and user-interface translations [202].

Kleene's theorem [100] states that a language $\mathcal{L}$ is regular if and only if there exists a finite automaton that accepts each word in $\mathcal{L}$ and rejects each word not in $\mathcal{L}$ (see [82, Section 3.2] for a modern treatise).

Let $\mathcal{L}$ be a regular language over Σ, and let $\boldsymbol{u}$ be the sequence such that u_n is the number of words in $\mathcal{L}$ of length equal to n. By Kleene's theorem and Example 1.20, it follows that $\boldsymbol{u}$ is a linear recurrence.

1.2.7 Coefficients of rational formal power series

Example 1.22 (Coefficients of a rational generating function)**.** Let $\mathbb{K}[[x]]$ be the ring of *formal power series* in the variable x, that is, the set of all infinite series of the form $\sum_{n=0}^{\infty} a_n x^n$ ($a_n \in \mathbb{K}$) with addition and multiplication defined in the natural way, without concern for convergence. An element of $\mathbb{K}[[x]]$ is a *rational function* if it can be written as the ratio of two polynomials. The *generating function* of a sequence $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ is the formal power series $\sum_{n=0}^{\infty} u_n x^n$. Then $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ is a linear recurrence if and only if its generating function is a rational function (see Theorem 2.47).

Example 1.23 (Coefficients of Hilbert series)**.** This example comes from commutative algebra (see, e.g., the book by Kemper [95, Chapter 11]). A *graded algebra* $\mathcal{A}$ over $\mathbb{K}$ is an algebra over $\mathbb{K}$ that admits a decomposition $\mathcal{A} = \bigoplus_{n\in\mathbb{N}} \mathcal{A}_n$, where $\mathcal{A}_n$ is a finite-dimensional vector space over $\mathbb{K}$, such that $\mathcal{A}_0 = \mathbb{K}$ and $\mathcal{A}_m\mathcal{A}_n \subseteq \mathcal{A}_{m+n}$ for all integers $m, n \geq 0$. The standard example is the ring of polynomials $\mathcal{A} = \mathbb{K}[x_1, \ldots, x_m]$ in the formal variables $x_1, \ldots, x_m$, which is a graded algebra with $\mathcal{A}_n$ being equal to the vector space of homogeneous polynomials of degree n. The *Hilbert series* of a graded algebra $\mathcal{A}$ is the formal power series

$$H_{\mathcal{A}}(x) := \sum_{n=0}^{\infty} \dim_{\mathbb{K}}(\mathcal{A}_n)x^n \in \mathbb{Z}[[x]].$$

Suppose that $\mathcal{A}$ is finitely-generated over $\mathbb{K}$. Then the *Hilbert–Serre theorem* asserts that $H_{\mathcal{A}}(x)$ is a rational function. Therefore, by Example 1.22, the sequence $\big(\dim_{\mathbb{K}}(\mathcal{A}_n)\big)$ is a linear recurrence.

Example 1.24 (Number of subgroups of index n)**.** Let $\mathcal{G}$ be a group such that the number $a_n(\mathcal{G})$ of index-n subgroups of $\mathcal{G}$ is finite for each positive integer n. The *zeta function* of $\mathcal{G}$ is the formal Dirichlet series

$$\zeta_{\mathcal{G}}(s) := \sum_{n=1}^{\infty} a_n(\mathcal{G})n^{-s}.$$

If $\mathcal{G}$ is nilpotent then $\zeta_{\mathcal{G}}(s)$ has the *Euler product*[3]

$$\zeta_{\mathcal{G}}(s) = \prod_{p} \zeta_{\mathcal{G},p}(s),$$

where p runs over the prime numbers and

$$\zeta_{\mathcal{G},p}(s) := \sum_{n=0}^{\infty} a_{p^n}(\mathcal{G})p^{-sn}.$$

Suppose that $\mathcal{G}$ is finitely generated, torsion-free, and nilpotent. Grunewald, Segal, and Smith [73] proved that $\zeta_{\mathcal{G},p}(s)$ is a rational function of p^{-s}. Hence, by Example 1.22, the sequence $\big(a_{p^n}(\mathcal{G})\big)$ is a linear recurrence. For more on zeta functions of groups, see the book by du Sautoy and Woodward [48]

Example 1.25 (Number of points of an algebraic variety over a finite field)**.** This example comes from algebraic geometry (see, e.g., the book by Silverman [176, Section V.2]). Let $\mathbb{F}_q$ be a finite field of q elements, for every positive integer n let $\mathbb{F}_{q^n}$ be an extension of $\mathbb{F}_q$ of degree n, and let V be a *projective variety* over $\mathbb{F}_q$, that is, the set of solutions to the system of equations

$$f_i(x_0, \ldots, x_N) = 0 \quad (i = 1, \ldots, m)$$

where $f_1, \ldots, f_m$ are homogeneous polynomials in $\mathbb{F}_q[x_0, \ldots, x_N]$ generating a prime ideal.

[3] In analogy with the Euler product of the *Riemann zeta function* $\sum_{n=1}^{\infty} n^{-s} = \prod_p (1 - 1/p^s)^{-1}$.

The *zeta function* of V is the formal power series

$$Z_V(x) := \exp\left(\sum_{n=1}^{\infty} \frac{|V(\mathbb{F}_{q^n})|}{n} x^n \right),$$

where $V(\mathbb{F}_{q^n})$ is the set of points of V with coordinates in $\mathbb{F}_{q^n}$. In 1949 Weil [198] conjectured that if V is smooth then $Z_V(x)$ is a rational function; and he proved this conjecture for curves and for abelian varieties. In 1960 Dwork [51] proved the general case. The rationality of $Z_V(x)$ implies that the *logarithmic derivative*

$$\frac{\frac{\mathrm{d}}{\mathrm{d}x} Z_V(x)}{Z_V(x)} = \frac{\mathrm{d}}{\mathrm{d}x} \log\big(Z_V(x)\big) = \sum_{n=0}^{\infty} |V(\mathbb{F}_{q^{n+1}})|\, x^n$$

is also a rational function. Hence, by Example 1.22, the sequence $\big(|V(\mathbb{F}_{q^{n+1}})|\big)$ is a linear recurrence.

Construction	Notation	Generating Function
Union	$\mathcal{A} \cup \mathcal{B}$	$A(x) + B(x)$
Product	$\mathcal{A} \times \mathcal{B}$	$A(x)B(x)$
Sequences	$\mathcal{A}^*$	$\dfrac{1}{1 - A(x)}$
Pointing	$\Theta\mathcal{A}$	$x\dfrac{\mathrm{d}}{\mathrm{d}x}A(x)$
Substitution	$\mathcal{A} \circ \mathcal{B}$	$A\big(B(x)\big)$

Table 1.1: Important combinatorial constructions and their translations into generating functions. Here $\mathcal{A}$ and $\mathcal{B}$ are combinatorial classes with generating functions $A(x)$ and $B(x)$, respectively.

Example 1.26 (Counting sequences of combinatorial classes)**.** This example provides an explanation of the widespreadness of linear recurrences in combinatorics. A *combinatorial class* is a countable set $\mathcal{A}$ equipped with a function $\mathcal{A} \to \mathbb{N}$ that maps each element of $\mathcal{A}$ to its *size* and such that for each integer $n \geq 0$ there are finitely many elements of $\mathcal{A}$ of size n. The *counting sequence* of $\mathcal{A}$ is the sequence (a_n) where a_n is the number of elements of $\mathcal{A}$ with size equal to n. The *generating function* of $\mathcal{A}$ is the formal power series $A(x) := \sum_{n=0}^{\infty} a_n x^n$. A *neutral element* is an element of size equal to 0, and it is usually denoted by ϵ. An *atom* is an element of size equal to 1. It is convenient to think of an element of positive size n as a "combination" of n atoms.

Let $\mathcal{A}$ and $\mathcal{B}$ be two combinatorial classes. The following are important constructions of new combinatorial classes.

(i) Assuming that $\mathcal{A} \cap \mathcal{B} = \varnothing$, the *union* of $\mathcal{A}$ and $\mathcal{B}$ is the combinatorial class $\mathcal{A} \cup \mathcal{B}$ where each element inherited the size from $\mathcal{A}$ or $\mathcal{B}$.

(ii) The *product* of $\mathcal{A}$ and $\mathcal{B}$ is the combinatorial class $\mathcal{A} \times \mathcal{B}$ where the size of each $(a, b) \in \mathcal{A} \times \mathcal{B}$ is the sum of the sizes of a and b.

(iii) Assuming that $\mathcal{A}$ has no neutral element, the set $\mathcal{A}^*$ of all finite sequences of elements of $\mathcal{A}$ (including the empty sequence) is a combinatorial class where the size of each sequence is the sum of the sizes of its elements. Note the analogy with the Kleene star of a regular expression (Example 1.21).

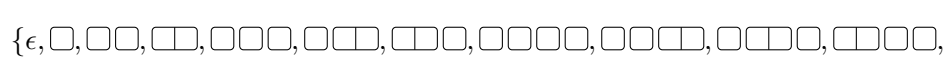
(iv) The *pointing* of $\mathcal{A}$ is a the combinatorial class $\Theta\mathcal{A}$ constructed by creating n copies of each size-n element a of $\mathcal{A}$, where each copy is distinguished by "pointing at" one of the atoms of a.

(v) The *substitution* of $\mathcal{B}$ into $\mathcal{A}$ is the combinatorial class $\mathcal{A} \circ \mathcal{B}$ obtained by substituting, in all possible ways, each atom of each element of $\mathcal{A}$ by an element of $\mathcal{B}$. The size of each element c of $\mathcal{A} \circ \mathcal{B}$ is the sum of the sizes of the elements of $\mathcal{B}$ that have been substituted to obtain c.

Each of the aforementioned constructions translates into an algebraic operation involving the generating functions of $\mathcal{A}$ and $\mathcal{B}$, see Table 1.1.

Note that if the generating functions of $\mathcal{A}$ and $\mathcal{B}$ are rational functions, then the generating function of each construction of Table 1.1 is a rational function. Therefore, by Example 1.22, repeated applications of these constructions yield combinatorial classes whose counting sequences are linear recurrences.

For instance, let ▢ denote a 1×1 domino of size 1, and let ▭ denote a 1×2 domino of size 2. Thus the combinatorial classes {▢} and {▭} have generating functions x and x^2, respectively. Their union {▢, ▭} has generating function $x + x^2$. The combinatorial class of all finite sequences of ▢ and ▭ is



(1.9)

and has generating function $1/(1 - x - x^2)$. The pointing of the combinatorial class (1.9) is

(1.10)

where each cross × marks the atom being pointed to. The generating function of the combinatorial class (1.10) is $(x + 2x^2)/(1 - x - x^2)^2$. Let ■ denote a black 1×1 domino, also of size 1. Hence the combinatorial class {▢, ■} has generating function $2x$. The substitution of {▢, ■} into the combinatorial class (1.9) is

and has generating function $1/(1 - 2x - 4x^2)$. All the counting sequences of these combinatorial classes are linear recurrences.

For an extensive example-driven introduction to combinatorial classes and their generating functions, see the book by Flajolet and Sedgewick [58].

Chapter 2

Linear Recurrences over a Field

2.1 Introduction

This chapter develops the theory of linear recurrences over an arbitrary field. The only prerequisites are a basic knowledge of linear algebra, along with occasional references to slightly more advanced results from the theory of field extensions. Essentially, Chapter 2 is a collection of results on linear recurrences that can be derived using exclusively algebraic methods, without employing analytic techniques.

This chapter provides the three main perspectives for studying linear recurrences: the *power-sum representation* (Section 2.3), the use of the *companion matrix* (Section 2.4), and the correspondence with *rational functions* (Section 2.8). None of these perspectives is better than the others. Each of them can be more or less convenient depending on the context, and switching from one to another is often useful.

Additionally, this chapter considers several operations involving linear recurrences, such as termwise addition, termwise multiplication, convolution, changing finitely many terms, reflection, and interleaving. Another key result of this chapter is the characterization of linear recurrences in terms of their *Hankel transform* (Section 2.10).

Finally, this chapter addresses several algorithmic considerations, including: efficient methods for computing the terms of a linear recurrence (Section 2.4), systematic techniques for proving algebraic identities involving linear recurrences (Section 2.9), and the fundamental *Berlekamp–Massey algorithm* for determining the minimal polynomial (Section 2.11).

Throughout this chapter, $\mathbb{K}$ is a field, all vector spaces are over $\mathbb{K}$, and all linear maps are $\mathbb{K}$-linear maps, unless stated otherwise. In particular, the spaces of sequences $\mathbb{K}^{\mathbb{N}}$ and $\mathbb{K}^{\mathbb{Z}}$ are vector spaces equipped with the usual termwise addition and scalar multiplication.

2.2 General facts

This section collects some general facts and definitions about linear recurrences.

2.2.1 Shift operator

Identify each polynomial $f(x) = \sum_{i=0}^{k} a_i x^i$ ($a_i \in \mathbb{K}$) with the linear map $\mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}}$ defined by

$$(f\boldsymbol{u})_n := \sum_{i=0}^{k} a_i u_{n+i}, \tag{2.1}$$

for every $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ and every integer $n \geq 0$. With this identification, the formal variable x is the *shift operator* of $\mathbb{K}^{\mathbb{N}}$ and satisfies $(x\boldsymbol{u})_n = u_{n+1}$, for every $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ and every integer $n \geq 0$. Moreover, for every integer $j \geq 0$, the power x^j is the jth iteration of the shift operator and satisfies $(x^j\boldsymbol{u})_n = u_{n+j}$, for every $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ and for every integer $n \geq 0$. In fact, extending by linearity this last equality leads to definition (2.1). It follows easily that

$$(f+g)\boldsymbol{u} = f\boldsymbol{u} + g\boldsymbol{u} \quad \text{and} \quad f(g\boldsymbol{u}) = (fg)\boldsymbol{u}, \tag{2.2}$$

for all $f, g \in \mathbb{K}[x]$. Hence the operation defined by (2.1) makes $\mathbb{K}^{\mathbb{N}}$ a $\mathbb{K}[x]$-module.

For every $f \in \mathbb{K}[x]$, let $\mathcal{L}(f) := \{\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}} : f\boldsymbol{u} = \boldsymbol{0}\}$ be the kernel of f as a linear map $\mathbb{K}^{\mathbb{N}} \to \mathbb{K}^{\mathbb{N}}$. In particular, $\mathcal{L}(f)$ is a vector space. If f is given by (1.2), then $\mathcal{L}(f)$ is the vector space of all linear recurrences satisfying (1.1) or, in other words, having characteristic polynomial f.

2.2.2 Impulse sequences

For every polynomial $f \in \mathbb{K}[x]$ of positive degree k, define the *impulse sequences*

$$\boldsymbol{\delta}^{(0)}(f), \ldots, \boldsymbol{\delta}^{(k-1)}(f) \in \mathbb{K}^{\mathbb{N}}$$

as the linear recurrences with characteristic polynomial f and initial values determined by

$$\big(\boldsymbol{\delta}^{(i)}(f)\big)_n = \delta_{i,n}$$

for every $i, n \in \{0, \ldots, k-1\}$. For short, write $\boldsymbol{\delta}^{(i)} := \boldsymbol{\delta}^{(i)}(f)$ when f is clear from the context. The importance of the impulse sequences is due to the following result.

Theorem 2.1. *Let $f \in \mathbb{K}[x]$ be nonzero and let $k := \deg(f)$. Then*

(i) $\dim\big(\mathcal{L}(f)\big) = k$;

(ii) for $k > 0$ the sequences $\boldsymbol{\delta}^{(0)}, \ldots, \boldsymbol{\delta}^{(k-1)}$ form a basis of $\mathcal{L}(f)$;

(iii) for $k > 0$ an isomorphism $\mathcal{L}(f) \to \mathbb{K}^{k\times 1}$ is given by the map $\boldsymbol{u} \mapsto (u_0 \cdots u_{k-1})^{\intercal}$ whose inverse is $(u_0 \cdots u_{k-1})^{\intercal} \mapsto \sum_{i=0}^{k-1} u_i \boldsymbol{\delta}^{(i)}$.

Proof. If $k = 0$ then $\mathcal{L}(f) = \{\boldsymbol{0}\}$ and (i) follows. Hence, assume that $k > 0$. By looking at their initial values, it follows that $\boldsymbol{\delta}^{(0)}, \ldots, \boldsymbol{\delta}^{(k-1)}$ are linearly independent. Moreover, for every $\boldsymbol{u} \in \mathcal{L}(f)$, it follows easily by induction on n that $u_n = \sum_{i=0}^{k-1} u_i \delta_n^{(i)}$ for every integer $n \geq 0$. In turn, this implies that $\boldsymbol{u} = \sum_{i=0}^{k-1} u_i \boldsymbol{\delta}^{(i)}$. Thus (i), (ii), and (iii) follow. □

The expression $\boldsymbol{u} = \sum_{i=0}^{k-1} u_i \boldsymbol{\delta}^{(i)}(f)$ in the proof of Theorem 2.1(iii) is the *impulsive representation* of the linear recurrence $\boldsymbol{u}$.

2.2.3 Minimal polynomial

Theorem 2.2. *Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$. Then there exists a unique monic polynomial $m_{\boldsymbol{u}} \in \mathbb{K}[x]$ such that $\boldsymbol{u} \in \mathcal{L}(f)$ if and only if $m_{\boldsymbol{u}}$ divides f, for every $f \in \mathbb{K}[x]$.*

Proof. Let $\mathcal{I} := \{f \in \mathbb{K}[x] : f\boldsymbol{u} = \boldsymbol{0}\}$. From (2.2) it follows that $\mathcal{I}$ is an ideal of the ring of polynomials $\mathbb{K}[x]$. Since $\mathbb{K}$ is a field, the ring $\mathbb{K}[x]$ is a principal ideal domain. Hence, the ideal $\mathcal{I}$ is generated by a unique monic polynomial $m_{\boldsymbol{u}}$. The claim follows. □

For every linear recurrence $\boldsymbol{u}$ over $\mathbb{K}$, the polynomial $m_{\boldsymbol{u}}$ from Theorem 2.2 is the *minimal polynomial* of $\boldsymbol{u}$. Note that $m_{\boldsymbol{u}}$ is the monic polynomial in $\mathbb{K}[x]$ of minimal degree such that $\boldsymbol{u} \in \mathcal{L}(m_{\boldsymbol{u}})$. Moreover, the degree of $m_{\boldsymbol{u}}$ is equal to the order of $\boldsymbol{u}$.

The *roots* of the linear recurrence $\boldsymbol{u}$ are the roots of its minimal polynomial $m_{\boldsymbol{u}}$, taken in the splitting field of $m_{\boldsymbol{u}}$ over $\mathbb{K}$, and their *multiplicities* are their multiplicities as roots of $m_{\boldsymbol{u}}$. The linear recurrence $\boldsymbol{u}$ is *simple* if it has no multiple roots. The roots of a linear recurrence appear in its *power-sum representation* (Section 2.3).

The following result is a useful criterion to determine if a polynomial is the minimal polynomial of a linear recurrence.

Theorem 2.3. *Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$ and let $f \in \mathbb{K}[x]$ be a monic polynomial of positive degree k. Then f is the minimal polynomial of $\boldsymbol{u}$ if and only if $x^0\boldsymbol{u}, \ldots, x^{k-1}\boldsymbol{u}$ form a basis of $\mathcal{L}(f)$.*

Proof. First, suppose that $x^0\boldsymbol{u}, \ldots, x^{k-1}\boldsymbol{u}$ form a basis of $\mathcal{L}(f)$. In particular, the linear recurrence $\boldsymbol{u}$ belongs to $\mathcal{L}(f)$. Moreover, the sequences $x^0\boldsymbol{u}, \ldots, x^{k-1}\boldsymbol{u}$ are linearly independent. Hence $\boldsymbol{u} \notin \mathcal{L}(g)$ for every nonzero polynomial $g \in \mathbb{K}[x]$ of degree less than k. This implies that f is the minimal polynomial of $\boldsymbol{u}$.

Conversely, suppose that f is the minimal polynomial of $\boldsymbol{u}$. Then all the sequences $x^0\boldsymbol{u}, \ldots, x^{k-1}\boldsymbol{u}$ belong to $\mathcal{L}(f)$, since $fx^i\boldsymbol{u} = x^i f\boldsymbol{u} = \boldsymbol{0}$ for every $i \in \{0, \ldots, k-1\}$. Furthermore, the sequences $x^0\boldsymbol{u}, \ldots, x^{k-1}\boldsymbol{u}$ are linearly independent, otherwise there would exist a nonzero polynomial $g \in \mathbb{K}[x]$ of degree less than k such that $\boldsymbol{u} \in \mathcal{L}(g)$, in contradiction with f being the minimal polynomial of $\boldsymbol{u}$. Thus, from Theorem 2.1(i), it follows that $x^0\boldsymbol{u}, \ldots, x^{k-1}\boldsymbol{u}$ form a basis of $\mathcal{L}(f)$. □

The following theorem shows that every monic polynomial is the minimal polynomial of some linear recurrence.

Theorem 2.4. *Let $f \in \mathbb{K}[x]$ be a monic polynomial of degree k. If $k = 0$ (that is, $f = 1$), then f is the minimal polynomial of the zero linear recurrence. If $k > 0$ then f is the minimal polynomial of $\boldsymbol{\delta}^{(k-1)}(f)$.*

Proof. If $k = 0$ then the claim is obvious. Hence, assume that $k > 0$. By definition, the impulse sequence $\boldsymbol{\delta}^{(k-1)}$ belongs to $\mathcal{L}(f)$. Consequently $x^i\boldsymbol{\delta}^{(k-1)} \in \mathcal{L}(f)$ for every integer $i \geq 0$. Moreover, by looking at their initial values, it follows easily that the linear recurrences $x^0\boldsymbol{\delta}^{(k-1)}, \ldots, x^{k-1}\boldsymbol{\delta}^{(k-1)}$ are linearly independent (essentially, this is an application of the isomorphism of Theorem 2.1(iii)). Hence, by Theorem 2.1(i), the sequences $x^0\boldsymbol{\delta}^{(k-1)}, \ldots, x^{k-1}\boldsymbol{\delta}^{(k-1)}$ form a basis of $\mathcal{L}(f)$. Therefore f is the minimal polynomial of $\boldsymbol{\delta}^{(k-1)}$ by Theorem 2.3. □

2.2.4 Spaces of linear recurrences

The next theorem determines how vector spaces of the form $\mathcal{L}(f)$, for a nonzero $f \in \mathbb{K}[x]$, behave with respect to the operations of intersection and addition of subspaces of $\mathbb{K}^{\mathbb{N}}$.

Theorem 2.5. *Let $f, g \in \mathbb{K}[x]$ be nonzero. Then*

(i) $\mathcal{L}(f) \subseteq \mathcal{L}(g)$ if and only if f divides g;

(ii) $\mathcal{L}(f) \cap \mathcal{L}(g) = \mathcal{L}((f, g))$;

(iii) $\mathcal{L}(f) + \mathcal{L}(g) = \mathcal{L}([f, g])$;

(iv) if $(f, g) = 1$ then $\mathcal{L}(f) + \mathcal{L}(g) = \mathcal{L}(fg)$ and $\mathcal{L}(f) \cap \mathcal{L}(g) = \{\mathbf{0}\}$ (direct sum);

where (f, g) and $[f, g]$ denote the greatest common divisor and the least common multiple of f and g, respectively.

Proof. Let (i′) be the claim: "if f divides g then $\mathcal{L}(f) \subseteq \mathcal{L}(g)$" (that is, one of the two implications of (i)). If f divides g then $g = hf$ for some $h \in \mathbb{K}[x]$. Hence, if $\boldsymbol{u} \in \mathcal{L}(f)$ then $g\boldsymbol{u} = h(f\boldsymbol{u}) = \mathbf{0}$, and so $\boldsymbol{u} \in \mathcal{L}(g)$. This proves (i′).

Since (f, g) divides each of f and g, it follows from (i′) that $\mathcal{L}((f, g)) \subseteq \mathcal{L}(f) \cap \mathcal{L}(g)$. Suppose that $\boldsymbol{u} \in \mathcal{L}(f) \cap \mathcal{L}(g)$. By Bézout's identity, there exist $a, b \in \mathbb{K}[x]$ such that $af + bg = (f, g)$. Therefore

$$(f, g)\boldsymbol{u} = (af + bg)\boldsymbol{u} = a(f\boldsymbol{u}) + b(g\boldsymbol{u}) = \mathbf{0} + \mathbf{0} = \mathbf{0},$$

so that $\boldsymbol{u} \in \mathcal{L}((f, g))$. Thus $\mathcal{L}(f) \cap \mathcal{L}(g) \subseteq \mathcal{L}((f, g))$. This proves (ii).

If $\mathcal{L}(f) \subseteq \mathcal{L}(g)$ then, by (ii),

$$\mathcal{L}(f) = \mathcal{L}(f) \cap \mathcal{L}(g) = \mathcal{L}((f, g)).$$

Hence $\deg(f) = \deg((f, g))$ by Theorem 2.1(i). This implies that f divides g, and together with (i′) proves (i).

Since both f and g divide $[f, g]$, it follows from (i′) that $\mathcal{L}(f)$ and $\mathcal{L}(g)$ are subspaces of $\mathcal{L}([f, g])$. Consequently $\mathcal{L}(f) + \mathcal{L}(g) \subseteq \mathcal{L}([f, g])$. Moreover, from Grassmann's formula, claim (ii), and Theorem 2.1(i), it follow that

$$\begin{aligned}\dim(\mathcal{L}(f) + \mathcal{L}(g)) &= \dim(\mathcal{L}(f)) + \dim(\mathcal{L}(g)) - \dim(\mathcal{L}(f) \cap \mathcal{L}(g)) \\ &= \dim(\mathcal{L}(f)) + \dim(\mathcal{L}(g)) - \dim(\mathcal{L}((f, g))) \\ &= \deg(f) + \deg(g) - \deg((f, g)) = \deg([f, g]) = \dim(\mathcal{L}([f, g])).\end{aligned}$$

Thus $\mathcal{L}(f) + \mathcal{L}(g) = \mathcal{L}([f, g])$. This proves (iii).

Finally, claim (iv) follows from (ii) and (iii). □

Corollary 2.6. *Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be linear recurrences over $\mathbb{K}$ of orders k and ℓ, respectively. Then $\boldsymbol{u} + \boldsymbol{v}$ is a linear recurrence of order at most $k + \ell$.*

Proof. The claim follows at once from Theorem 2.5(iii). □

The next result is a characterization of the subspaces of $\mathbb{K}^{\mathbb{N}}$ that are of the form $\mathcal{L}(f)$, for some nonzero polynomial $f \in \mathbb{K}[x]$.

Theorem 2.7. *Let V be a vector subspace of $\mathbb{K}^{\mathbb{N}}$. Then there exists a nonzero $f \in \mathbb{K}[x]$ such that $V = \mathcal{L}(f)$ if and only if V is finite-dimensional and closed with respect to the shift operator.*

Proof. First, suppose that $V = \mathcal{L}(f)$ for some nonzero $f \in \mathbb{K}[x]$. From Theorem 2.1(i), the dimension of V is finite. Furthermore, if $\boldsymbol{u} \in V$ then $fx\boldsymbol{u} = xf\boldsymbol{u} = \boldsymbol{0}$, so that $x\boldsymbol{u} \in V$. Hence, the vector subspace V is closed with respect to the shift operator.

Now suppose that V has finite dimension k and is closed with respect to the shift operator. If $k = 0$ then $V = \mathcal{L}(1)$ and the proof is complete. Hence, assume that $k > 0$.

Claim: every $\boldsymbol{v} \in V$ is a linear recurrence. Indeed, since V is closed with respect to the shift operator, the sequences $x^0\boldsymbol{v}, \ldots, x^k\boldsymbol{v}$ belong to V. Since $\dim(V) = k$, the sequences $x^0\boldsymbol{v}, \ldots, x^k\boldsymbol{v}$ are linearly dependent. Hence, there exists a monic $g \in \mathbb{K}[x]$ such that $g\boldsymbol{v} = \boldsymbol{0}$. Thus $\boldsymbol{v}$ is a linear recurrence, as claimed.

Let $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(k)}$ be a basis of V. By the previous reasoning, the sequences $\boldsymbol{v}^{(1)}, \ldots, \boldsymbol{v}^{(k)}$ are linear recurrences. For each $i \in \{1, \ldots, k\}$, let m_i be the minimal polynomial of $\boldsymbol{v}^{(i)}$ and put $k_i := \deg(m_i)$. On the one hand, since $\boldsymbol{v}^{(i)} \in \mathcal{L}(m_i)$ for each $i \in \{1, \ldots, k\}$, it follows that $V \subseteq \sum_{i=1}^{k} \mathcal{L}(m_i)$. On the other hand, since V is closed with respect to the shift operator, it follows that $x^j\boldsymbol{v}^{(i)} \in V$ for every $i \in \{1, \ldots, k\}$ and $j \in \{0, \ldots, k_i - 1\}$. Furthermore, by Theorem 2.3, the sequences $x^0\boldsymbol{v}^{(i)}, \ldots, x^{k_i-1}\boldsymbol{v}^{(i)}$ form a basis of $\mathcal{L}(m_i)$, for each $i \in \{1, \ldots, k\}$. Hence $\sum_{i=1}^{k} \mathcal{L}(m_i) \subseteq V$. Therefore $V = \sum_{i=1}^{k} \mathcal{L}(m_i)$. At last, from Theorem 2.5(iii) it follows that $V = \mathcal{L}(f)$, where f is the least common multiple of the polynomials $m_1, \ldots, m_k$. □

2.2.5 Reversibility

Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$ and let $f(x) = x^k - \sum_{i=1}^{k} a_i x^{k-i}$ $(a_i \in \mathbb{K})$ be its characteristic polynomial. If $f(0) \neq 0$, then $\boldsymbol{u}$ can be *extended backward* by defining

$$u_n := a_k^{-1} \left(u_{n+k} - \sum_{i=1}^{k-1} a_i u_{n+k-i} \right), \tag{2.3}$$

for every integer $n < 0$. In this way, the doubly infinite sequence $\boldsymbol{u} \in \mathbb{K}^{\mathbb{Z}}$ is a linear recurrence with characteristic polynomial f. In light of these considerations, if $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ is a linear recurrence with minimal polynomial $m_{\boldsymbol{u}}$ such that $m_{\boldsymbol{u}}(0) \neq 0$, then $\boldsymbol{u}$ is a *reversible* linear recurrence. Note that, by Theorem 2.2, the linear recurrence $\boldsymbol{u}$ is reversible if and only if $\boldsymbol{u}$ has a characteristic polynomial f such that $f(0) \neq 0$.

Theorem 2.8. *Let $\boldsymbol{u}$ be a reversible linear recurrence over $\mathbb{K}$. Then the backward extension of $\boldsymbol{u}$ to a linear recurrence in $\mathbb{K}^{\mathbb{Z}}$ does not depend on the particular choice of the characteristic polynomial of $\boldsymbol{u}$.*

Proof. Let $f(x) = x^k - \sum_{i=1}^{k} a_i x^{k-i}$ $(a_i \in \mathbb{K})$ be a characteristic polynomial of $\boldsymbol{u}$. Suppose that $f(0) \neq 0$. Extend backward $\boldsymbol{u}$ to a linear recurrence in $\mathbb{K}^{\mathbb{Z}}$ via (2.3). Let $m_{\boldsymbol{u}}$ be the

minimal polynomial of $\boldsymbol{u}$. Theorem 2.2 implies that $m_{\boldsymbol{u}}$ divides f. In particular $m_{\boldsymbol{u}}(0) \neq 0$. Let $\boldsymbol{v} \in \mathbb{K}^{\mathbb{Z}}$ be the linear recurrence obtained by extending backward $\boldsymbol{u}$ via $m_{\boldsymbol{u}}$. Hence, by construction, it follows that $u_n = v_n$ for every integer $n \geq 0$, and $(m_{\boldsymbol{u}}\boldsymbol{v})_n = 0$ for every integer n. Since $m_{\boldsymbol{u}}$ divides f, it follows that $(f\boldsymbol{v})_n = 0$ for every integer n. Thus the equality (2.3) holds for every integer $n < 0$ even if $\boldsymbol{u}$ is replaced by $\boldsymbol{v}$. Since $u_n = v_n$ for $n = 0, \ldots, k-1$, reasoning by induction gives that $u_n = v_n$ for every integer $n < 0$. Hence $\boldsymbol{u} = \boldsymbol{v}$. Thus the extension to $\mathbb{K}^{\mathbb{Z}}$ does not depend on f. □

Example 2.1 (Extension of Fibonacci numbers to negative integers)**.** The linear recurrence of Fibonacci numbers (F_n) is reversible and can be extended backward by defining

$$F_n := F_{n+2} - F_{n+1}$$

for every integer $n < 0$. It follows easily by induction that $F_{-n} = (-1)^{n+1}F_n$ for every integer $n < 0$.

The next result shows that, for most purposes, it is sufficient to consider only reversible linear recurrences.

Theorem 2.9. *Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$ and let $x^k f$ be its minimal polynomial, where $k \geq 0$ is an integer and $f \in \mathbb{K}[x]$ satisfies $f(0) \neq 0$. Then there exists a reversible linear recurrence $\boldsymbol{v}$ over $\mathbb{K}$ such that f is the minimal polynomial of $\boldsymbol{v}$ and $v_n = u_n$ for every integer $n \geq k$.*

Proof. Let $\boldsymbol{w} := x^k\boldsymbol{u}$. Since $x^k f$ is the minimal polynomial of $\boldsymbol{u}$, it follows easily that f is the minimal polynomial of $\boldsymbol{w}$. Since $f(0) \neq 0$, the sequence $\boldsymbol{w}$ is a reversible linear recurrence and can be extended backward to a linear recurrence $\boldsymbol{w} \in \mathbb{K}^{\mathbb{Z}}$. Let $\boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$ be defined by $v_n = w_{n-k}$ for every integer $n \geq 0$. Since $\boldsymbol{w}$ is a linear recurrence (in $\mathbb{K}^{\mathbb{Z}}$) with minimal polynomial f, and $w_n = u_{n+k}$ for every integer $n \geq 0$, it follows that $\boldsymbol{v}$ is a linear recurrence with minimal polynomial f and such that $v_n = u_n$ for every integer $n \geq k$. □

2.2.6 Changing finitely many terms

The following result, which is closely related to Theorem 2.9, says that every linear recurrence remains a linear recurrence if finitely many of its terms are changed.

Theorem 2.10. *Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$ with characteristic polynomial f, let $k \geq 0$ be an integer, and let $\boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$ be a sequence such that $v_n = u_n$ for every integer $n \geq k$. Then $\boldsymbol{v}$ is a linear recurrence with characteristic polynomial $x^k f$.*

Proof. Let $\boldsymbol{w} := \boldsymbol{v} - \boldsymbol{u}$. By the hypothesis, $w_n = 0$ for every integer $n \geq k$. Hence $\boldsymbol{w} \in \mathcal{L}(x^k)$. Thus, by Theorem 2.5(iii), it follows that $\boldsymbol{v} = \boldsymbol{u} + \boldsymbol{w}$ is a linear recurrence with characteristic polynomial $x^k f$. □

2.2.7 Reflection

For each sequence $\boldsymbol{u} \in \mathbb{K}^{\mathbb{Z}}$, the *reflection* of $\boldsymbol{u}$ is the sequence $\boldsymbol{u}^* \in \mathbb{K}^{\mathbb{Z}}$ defined by $u_n^* := u_{-n}$ for every integer n. For each polynomial $f(x) = \sum_{i=0}^{k} a_i x^i$ ($a_i \in \mathbb{K}$), with $a_k \neq 0$, the *reciprocal polynomial* of $f(x)$ is defined as $f^*(x) := \sum_{i=0}^{k} a_{k-i} x^i = x^k f(1/x)$.

The next theorem states that the reflection of a reversible linear recurrence is a linear recurrence.

Theorem 2.11. *Let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{Z}}$ be a reversible linear recurrence with characteristic polynomial f such that $f(0) \neq 0$. Then $\boldsymbol{u}^*$ is a linear recurrence with characteristic polynomial f^*.*

Proof. Write $f(x) = \sum_{i=0}^{k} a_i x^i$ ($a_i \in \mathbb{K}$), with $a_k \neq 0$. Then $\sum_{i=0}^{k} a_i u_{n+i} = 0$ for every integer n. Hence

$$\sum_{i=0}^{k} a_{k-i} u_{n+i}^* = \sum_{i=0}^{k} a_i u_{n+k-i}^* = \sum_{i=0}^{k} a_i u_{-n-k+i} = 0,$$

for every integer n. Thus $\boldsymbol{u}^*$ is a linear recurrence having $f^*(x) = \sum_{i=0}^{k} a_{k-i} x^i$ as its characteristic polynomial. □

2.2.8 Subsequences modulo m

The following theorem shows that the study of a linear recurrence can be reduced to the study of its subsequences whose indices run in the arithmetic progressions modulo m.

Theorem 2.12. *Let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$, let m be a positive integer, and for each $r \in \{0, \dots, m-1\}$ let $\boldsymbol{u}^{(r)} \in \mathbb{K}^{\mathbb{N}}$ be the sequence defined by $u_n^{(r)} := u_{mn+r}$ for every integer $n \geq 0$. Then $\boldsymbol{u}$ is a linear recurrence if and only if $\boldsymbol{u}^{(r)}$ is a linear recurrence for each $r \in \{0, \dots, m-1\}$.*

Proof. Suppose that $\boldsymbol{u}$ is a linear recurrence. Let $f \in \mathbb{K}[x]$ be the characteristic polynomial of $\boldsymbol{u}$. Put $k := \deg(f)$. Since $\mathbb{K}[x]/(f)$ is a vector space of dimension k, the $k+1$ polynomials $x^{0m}, \dots, x^{km}$ are linearly dependent modulo $f(x)$. Hence, there exists a monic polynomial $g \in \mathbb{K}[x]$ of degree at most k such that $f(x)$ divides $g(x^m)$. Thus, for each $r \in \{0, \dots, m-1\}$, Theorem 2.5(i) implies that $\boldsymbol{u} \in \mathcal{L}\big(x^r g(x^m)\big)$ and, consequently, that $\boldsymbol{u}^{(r)} \in \mathcal{L}\big(g(x)\big)$. In particular, the sequence $\boldsymbol{u}^{(r)}$ is a linear recurrence.

Suppose that, for each $r \in \{0, \dots, m-1\}$, the sequence $\boldsymbol{u}^{(r)}$ is a linear recurrence, and let $f^{(r)} \in \mathbb{K}[x]$ be its characteristic polynomial. Thus $\big(f^{(r)}(x^m)\boldsymbol{u}\big)_n = 0$ for every $r \in \{0, \dots, m-1\}$ and every integer $n \geq 0$ such that $n \equiv r \pmod m$. Consequently $\boldsymbol{u} \in \mathcal{L}(g)$, where $g(x) := \prod_{r=0}^{m-1} f^{(r)}(x^m)$. Thus $\boldsymbol{u}$ is a linear recurrence. □

Remark 2.13. One implication of Theorem 2.12 says that if $\boldsymbol{u}^{(0)}, \dots, \boldsymbol{u}^{(m-1)}$ are linear recurrences over $\mathbb{K}$ then their *interleaved sequence*

$$u_0^{(0)}, \dots, u_0^{(m-1)}, u_1^{(0)}, \dots, u_1^{(m-1)}, u_2^{(0)}, \dots, u_2^{(m-1)}, \dots$$

is a linear recurrence.

2.3 Power sums

Theorem 2.14. *Let $f(x) = \prod_{i=1}^{s}(x-\alpha_i)^{k_i}$, where $\alpha_1, \ldots, \alpha_s \in \mathbb{K}^*$ are pairwise distinct and $k_1, \ldots, k_s$ are positive integers. Then for every $\boldsymbol{u} \in \mathcal{L}(f)$ there exist unique coefficients $c_{i,j} \in \mathbb{K}$ such that*

$$u_n = \sum_{i=1}^{s} \sum_{j=0}^{k_i-1} c_{i,j} \binom{n}{j} \alpha_i^{n-j} \tag{2.4}$$

for every integer $n \geq 0$. Conversely, if $\boldsymbol{u}$ is a sequence of the form (2.4) then $\boldsymbol{u} \in \mathcal{L}(f)$.

The expression (2.4) is the *power-sum representation* of the linear recurrence $\boldsymbol{u}$. The next theorem and corollary show that, under some mild hypothesis, the power-sum representation takes a simpler form.

Theorem 2.15. *Let $f(x) = \prod_{i=1}^{s}(x-\alpha_i)^{k_i}$, where $\alpha_1, \ldots, \alpha_s \in \mathbb{K}^*$ are pairwise distinct and $k_1, \ldots, k_s$ are positive integers. If $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq \max\{k_1, \ldots, k_s\}$, then for every $\boldsymbol{u} \in \mathcal{L}(f)$ there exist unique polynomials $f_i \in \mathbb{K}[x]$, with $\deg(f_i) < k_i$ or $f_i = 0$, such that*

$$u_n = \sum_{i=1}^{s} f_i(n)\, \alpha_i^n \tag{2.5}$$

for every integer $n \geq 0$. Conversely, if $\boldsymbol{u}$ is a sequence of the form (2.5) then $\boldsymbol{u} \in \mathcal{L}(f)$ (note that this implication requires no hypothesis on the characteristic of $\mathbb{K}$).

Corollary 2.16. *Let $f(x) = \prod_{i=1}^{s}(x-\alpha_i)$, where $\alpha_1, \ldots, \alpha_s \in \mathbb{K}^*$ are pairwise distinct. Then for every $\boldsymbol{u} \in \mathcal{L}(f)$ there exist unique coefficients $c_i \in \mathbb{K}$ such that*

$$u_n = \sum_{i=1}^{s} c_i \alpha_i^n \tag{2.6}$$

for every integer $n \geq 0$. Conversely, if $\boldsymbol{u}$ is a sequence of the form (2.6) then $\boldsymbol{u} \in \mathcal{L}(f)$.

An expression of the form (2.5) is a *generalized power sum*. The values $\alpha_1, \ldots, \alpha_s$ are the *roots*, the integers $k_1, \ldots, k_s$ are their *multiplicities*, and the polynomials $f_1, \ldots, f_s$ are the *coefficients* of the generalized power sum. Observe that, with the notation of Theorem 2.15, if $\boldsymbol{u} \in \mathcal{L}(f)$ then the order of $\boldsymbol{u}$ is equal to $\sum(\deg(f_i)+1)$, where the sum is over the polynomials f_i that are nonzero.

Note that if $f \in \mathbb{K}[x]$ is a monic polynomial with $f(0) \neq 0$, and $\alpha_1, \ldots, \alpha_s \in \mathbb{L}^*$ are the pairwise distinct roots of f, where $\mathbb{L}$ is the splitting field of f over $\mathbb{K}$, then the first parts of Theorem 2.14 and Theorem 2.15 hold by taking $c_{i,j} \in \mathbb{L}$ and $f_i \in \mathbb{L}[x]$. In fact, the usual application of Theorem 2.14 and Theorem 2.15 takes f as the minimal polynomial of a reversible linear recurrence $\boldsymbol{u}$, so that $\alpha_1, \ldots, \alpha_s$ are the roots of $\boldsymbol{u}$ and belongs to $\mathbb{L}$.

The coefficients $c_{i,j}$ appearing in the power-sum representation (2.4) are determined from the initial values $u_0, \ldots, u_{k-1}$ of $\boldsymbol{u}$, where $k := \sum_{i=1}^{s} k_i$, by solving the linear system in the k unknowns $c_{i,j}$ and the k equations obtained by setting $n = 0, \ldots, k-1$ in (2.4). The polynomials f_i in (2.5), and the coefficients c_i in (2.6), are determined in a similar way. Section 2.5 explains this in detail.

Example 2.2 (Second-order linear recurrences)**.** Let $f(x) = x^2 - a_1 x - a_2$ with $a_1, a_2 \in \mathbb{K}$ and $a_2 \neq 0$, let $\mathbb{L}$ be the splitting field of f over $\mathbb{K}$, let $\alpha_1, \alpha_2 \in \mathbb{L}^*$ be the roots of f, and let $\boldsymbol{u} \in \mathcal{L}(f)$. From Theorem 2.15 it follows that

(i) if $\alpha_1 = \alpha_2$ then

$$u_n = \big(\alpha_1 u_0 + (u_1 - \alpha_1 u_0)n\big)\alpha_1^{n-1}$$

for every integer $n \geq 0$;

(ii) if $\alpha_1 \neq \alpha_2$ then

$$u_n = \frac{(u_1 - \alpha_2 u_0)\alpha_1^n - (u_1 - \alpha_1 u_0)\alpha_2^n}{\alpha_1 - \alpha_2},$$

for every integer $n \geq 0$.

Note that $\boldsymbol{u}$ is a second-order linear recurrence unless $u_1 = \alpha_1 u_0$ or $u_1 = \alpha_2 u_0$.

Example 2.3 (Binet's formula)**.** Specializing Example 2.2 to the sequence of Fibonacci numbers (F_n) yields

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \tag{2.7}$$

for every integer $n \geq 0$. Equation (2.7) is the *Binet formula* for the nth Fibonacci number. The constant $\big(1+\sqrt{5}\big)/2$ is the famous *golden ratio*, which appears naturally in geometry and number theory (see the beautifully illustrated book by Walser [194]). Alas, the golden ratio is also frequently subject to exaggerated—or entirely incorrect—claims about its significance in biology, psychology, ancient art, or finance. Equation (2.7) implies the asymptotic formula

$$F_n \sim \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n$$

as $n \to +\infty$. Section 5.5 studies the asymptotic growth of linear recurrences.

The proofs of Theorem 2.14, Theorem 2.15, and Corollary 2.16 require some notation and two lemmas. For every $\alpha \in \mathbb{K}^*$ and for every integer j, let $\boldsymbol{\psi}^{(j)}(\alpha)$ be the sequence in $\mathbb{K}^{\mathbb{N}}$ defined by

$$\big(\boldsymbol{\psi}^{(j)}(\alpha)\big)_n := \binom{n}{j}\alpha^{n-j}$$

for each integer $n \geq 0$. For the sake of brevity, put $\boldsymbol{\psi}^{(j)} := \boldsymbol{\psi}^{(j)}(\alpha)$ when α is clear from the context. Note that $\boldsymbol{\psi}^{(j)} = \mathbf{0}$ for every integer $j < 0$, while $\boldsymbol{\psi}^{(j)} \neq \mathbf{0}$ for every integer $j \geq 0$.

Lemma 2.17. *$(x - \alpha)\boldsymbol{\psi}^{(j)} = \boldsymbol{\psi}^{(j-1)}$ for every $\alpha \in \mathbb{K}^*$ and for every integer j.*

Proof. For every integer $n \geq 0$, recall that $\binom{n+1}{j} = \binom{n}{j} + \binom{n}{j-1}$, so that

$$\big((x-\alpha)\boldsymbol{\psi}^{(j)}\big)_n = \binom{n+1}{j}\alpha^{n+1-j} - \binom{n}{j}\alpha^{n+1-j} = \binom{n}{j-1}\alpha^{n-(j-1)} = \big(\boldsymbol{\psi}^{(j-1)}\big)_n.$$

The claim follows. □

Lemma 2.18. *Let $\alpha \in \mathbb{K}^*$ and let k be a positive integer. Then $\boldsymbol{\psi}^{(0)}, \dots, \boldsymbol{\psi}^{(k-1)}$ form a basis of $\mathcal{L}\big((x-\alpha)^k\big)$.*

Proof. Thanks to Lemma 2.17 and the fact that $\boldsymbol{\psi}^{(-1)} = \mathbf{0}$, the sequences $\boldsymbol{\psi}^{(0)}, \dots, \boldsymbol{\psi}^{(k-1)}$ belong to $\mathcal{L}\big((x-\alpha)^k\big)$. Suppose that there exist $c_0, \dots, c_{k-1} \in \mathbb{K}$ such that

$$c_0\boldsymbol{\psi}^{(0)} + \cdots + c_{k-1}\boldsymbol{\psi}^{(k-1)} = \mathbf{0}. \tag{2.8}$$

Multiplying successively (2.8) by $(x-\alpha)^{k-j}$ for $j = 1, \dots, k$, using Lemma 2.17 and the fact that $\boldsymbol{\psi}^{(i)} = \mathbf{0}$ for each negative integer i but $\boldsymbol{\psi}^{(0)} \neq \mathbf{0}$, it follows that $c_0 = \cdots = c_{k-1} = 0$. Hence, the sequences $\boldsymbol{\psi}^{(0)}, \dots, \boldsymbol{\psi}^{(k-1)}$ are linearly independent. By Theorem 2.1(i) the dimension of $\mathcal{L}\big((x-\alpha)^k\big)$ is equal to k. Thus $\boldsymbol{\psi}^{(0)}, \dots, \boldsymbol{\psi}^{(k-1)}$ form a basis of $\mathcal{L}\big((x-\alpha)^k\big)$, as desired. □

Now to the proofs of Theorem 2.14, Theorem 2.15, and Corollary 2.16.

Proof of Theorem 2.14. By Theorem 2.5(iv), the vector space $\mathcal{L}(f)$ is the direct sum of the subspaces $\mathcal{L}\big((x-\alpha_i)^{k_i}\big)$ for $i = 1, \dots, s$. Then the claim follows from Lemma 2.18. □

Proof of Theorem 2.15. Let $j \geq 0$ be an integer. Suppose that $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) > j$. Then the polynomial

$$\binom{x}{j} := \frac{1}{j!}\prod_{t=0}^{j-1}(x-t) \in \mathbb{K}[x]$$

is well defined and has degree equal to j. Consequently, the polynomials $\binom{x}{0}, \dots, \binom{x}{j}$ form a basis of the subspace of polynomials in $\mathbb{K}[x]$ of degree at most j. After changing from the basis $\binom{x}{0}, \dots, \binom{x}{j}$ to the basis $x^0, \dots, x^{j-1}$, from Theorem 2.14 it follows that every $\boldsymbol{u} \in \mathcal{L}(f)$ has a unique representation of the form (2.5).

Conversely, let $\boldsymbol{u}$ be a sequence of the form (2.5) (make no hypothesis on $\mathrm{char}(\mathbb{K})$). If $\alpha, \beta \in \mathbb{K}^*$ and $f \in \mathbb{K}[x]$ is a nonzero polynomial, then

$$(x-\alpha)\big(f(n)\,\beta^n\big)_{n\in\mathbb{N}} = \big(g(n)\,\beta^n\big)_{n\in\mathbb{N}} \tag{2.9}$$

where $g(x) := f(x+1)\beta - f(x)\alpha$. In particular, if g is nonzero, then $\deg(g) \leq \deg(f)$. Moreover, if $\alpha = \beta$ then the last inequality is strict. Hence, by repeatedly applying (2.9), it follows that multiplying $\boldsymbol{u}$ by $(x-\alpha_i)^{k_i}$, for $i \in \{1, \dots, s\}$, yields the zero sequence, that is, $f\boldsymbol{u} = 0$. Therefore $\boldsymbol{u} \in \mathcal{L}(f)$, as desired. □

Proof of Corollary 2.16. With the notation of Theorem 2.15, if $k_1 = \cdots = k_s = 1$ then it is clear that $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) \geq \max\{k_1, \dots, k_s\}$, and that the polynomials f_i are in fact constant polynomials. Thus the claim follows. □

Remark 2.19. Let $i, j \geq 0$ be integers. The *Stirling number of the first kind* $\left[{j \atop i}\right]$ is defined as the number of permutations of j elements with exactly i cycles, while the *Stirling number of the second kind* $\left\{{j \atop i}\right\}$ is defined as the number of partitions of a set of j elements into i nonempty subsets. Suppose that $\mathrm{char}(\mathbb{K}) = 0$ or $\mathrm{char}(\mathbb{K}) > j$. To convert between the

polynomial bases $\binom{x}{0}, \dots, \binom{x}{j}$ and $x^0, \dots, x^{j-1}$, appearing in the proof of Theorem 2.15, use the formulas

$$\binom{x}{j} = \frac{1}{j!} \sum_{i=0}^{j} (-1)^{j-i} \begin{bmatrix} j \\ i \end{bmatrix} x^i \quad \text{and} \quad x^j = \sum_{i=0}^{j} i! \begin{Bmatrix} j \\ i \end{Bmatrix} \binom{x}{i},$$

which hold as identities between polynomials in $\mathbb{K}[x]$. See for instance the book by Graham, Knuth, and Patashnik [70, p. 264].

The next theorem shows that, in the special case in which $f \in \mathbb{K}[x]$ is monic irreducible and separable over $\mathbb{K}$, it is possible to "parametrize" linear recurrences in $\mathcal{L}(f)$ by values in an extension of $\mathbb{K}$.

Theorem 2.20. *Let $f \in \mathbb{K}[x]$ be a monic irreducible and separable polynomial of positive degree k, and let α be a root of f in some field extension of $\mathbb{K}$. Then for every $\boldsymbol{u} \in \mathcal{L}(f)$ there exists a unique $\beta \in \mathbb{K}(\alpha)$ such that $u_n = \operatorname{tr}_{\mathbb{K}(\alpha)/\mathbb{K}}(\alpha^n \beta)$ for every integer $n \geq 0$. More precisely, the map $\boldsymbol{\tau} \colon \beta \mapsto \left(\operatorname{tr}_{\mathbb{K}(\alpha)/\mathbb{K}}(\alpha^n \beta)\right)_{n \in \mathbb{N}}$ is vector-space isomorphism $\mathbb{K}(\alpha) \to \mathcal{L}(f)$.*

Proof. Let $\beta \in \mathbb{K}(\alpha)$. First, from the definition of the trace, it follows that $\boldsymbol{\tau}(\beta) \in \mathbb{K}^{\mathbb{N}}$. Furthermore, the linearity of the trace and the fact that $f(\alpha) = 0$ imply that

$$f\boldsymbol{\tau}(\beta) = \left(\operatorname{tr}_{\mathbb{K}(\alpha)/\mathbb{K}}(f(\alpha)\alpha^n \beta)\right)_{n \in \mathbb{N}} = \mathbf{0},$$

so that $\boldsymbol{\tau}(\beta) \in \mathcal{L}(f)$. Thus $\boldsymbol{\tau}$ is indeed a map $\mathbb{K}(\alpha) \to \mathcal{L}(f)$ and, again from the linearity of the trace, it follows that $\boldsymbol{\tau}$ is linear.

Since f is irreducible over $\mathbb{K}$, the powers $\alpha^0, \dots, \alpha^{k-1}$ form a basis of $\mathbb{K}(\alpha)$. Moreover, since f is separable over $\mathbb{K}$, the extension $\mathbb{K}(\alpha)/\mathbb{K}$ is separable.

Recall that if $\mathbb{L}/\mathbb{K}$ is a separable extension of degree $k > 0$, then for every basis $\gamma_1, \dots, \gamma_k$ of $\mathbb{L}$ there exists a basis $\gamma_1', \dots, \gamma_k'$ of $\mathbb{L}$ such that $\operatorname{tr}_{\mathbb{L}/\mathbb{K}}(\gamma_i \gamma_i') = \delta_{i,j}$ for each $i, j \in \{1, \dots, k\}$ [110, Chapter 6, Corollary 5.3]. Therefore, there exists a basis $\beta_1, \dots, \beta_k$ of $\mathbb{K}(\alpha)$ such that $\operatorname{tr}_{\mathbb{K}(\alpha)/\mathbb{K}}(\alpha^{i-1}\beta_i) = \delta_{i,j}$ for every $i, j \in \{1, \dots, k\}$. This implies that $\boldsymbol{\tau}(\beta_i) = \boldsymbol{\delta}^{(i-1)}(f)$ for every $i \in \{1, \dots, k\}$. Hence, thanks to Theorem 2.1(ii), the map $\boldsymbol{\tau}$ is a linear isomorphism $\mathbb{K}(\alpha) \to \mathcal{L}(f)$. □

Example 2.4. From the Binet formula (2.7) it follows that

$$F_n = \operatorname{tr}_{\mathbb{Q}(\sqrt{5})/\mathbb{Q}}\left(\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n\right),$$

for every integer $n \geq 0$.

Remark 2.21. In Theorem 2.14, Theorem 2.15, and Corollary 2.16, the polynomial f satisfies $f(0) \neq 0$. Consequently, the linear recurrence $\boldsymbol{u}$ is reversible and can be extended backward to a linear recurrence in $\mathbb{K}^{\mathbb{Z}}$. In fact, it is possible to adapt the proofs of the aforementioned results to show that (2.4), (2.5), and (2.6) hold for every integer n. It is also possible to extend Theorem 2.20 to linear recurrences in $\mathbb{K}^{\mathbb{Z}}$ but, in order to ensure that $\boldsymbol{u}$ is reversible, it is necessary to add the hypothesis that $f \neq x$.

2.4 Companion matrix

For each monic polynomial $f(x) = x^k - \sum_{i=1}^{k} a_i x^{k-i}$ ($a_i \in \mathbb{K}$) of positive degree k, define the *companion matrix* of f as[1]

$$\boldsymbol{C}(f) := \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ a_k & a_{k-1} & a_{k-2} & \cdots & a_1 \end{pmatrix} \in \mathbb{K}^{k\times k}.$$

Note that $\boldsymbol{C}(f)$ is the matrix associated[2] to the shift operator as an endomorphism of $\mathcal{L}(f)$ with respect to the basis of the impulse sequences $\boldsymbol{\delta}^{(0)}, \dots, \boldsymbol{\delta}^{(k-1)}$ (recall Theorem 2.1(ii)). It is well known that the characteristic polynomial and the minimal polynomial[3] of $\boldsymbol{C}(f)$ are both equal to f, but this fact is not used here.

The following theorem provides the connection between the companion matrix $\boldsymbol{C}(f)$ and linear recurrences of characteristic polynomial f.

Theorem 2.22. *Let $f \in \mathbb{K}[x]$ be a monic polynomial of positive degree k and let $\boldsymbol{u} \in \mathcal{L}(f)$. Then*

(i) $\begin{pmatrix} u_{n+1} & \cdots & u_{n+k} \end{pmatrix}^\intercal = \boldsymbol{C}(f) \begin{pmatrix} u_n & \cdots & u_{n+k-1} \end{pmatrix}^\intercal$;

(ii) $\begin{pmatrix} u_n & \cdots & u_{n+k-1} \end{pmatrix}^\intercal = \boldsymbol{C}(f)^n \begin{pmatrix} u_0 & \cdots & u_{k-1} \end{pmatrix}^\intercal$;

(iii) $\left(\boldsymbol{C}(f)^n\right)_{i,j} = \left(\boldsymbol{\delta}^{(j-1)}(f)\right)_{n+i-1}$;

for every integer $n \geq 0$ and $i, j \in \{1, \dots, k\}$. Furthermore, if $f(0) \neq 0$ then $\boldsymbol{C}(f)$ is invertible and, after extending backward $\boldsymbol{u}, \boldsymbol{\delta}^{(0)}, \dots, \boldsymbol{\delta}^{(k-1)}$ to linear recurrences in $\mathbb{K}^{\mathbb{Z}}$, the statements (i), (ii), and (iii) hold for every integer n.

Proof. As already observed, by identifying $\mathcal{L}(f)$ with $\mathbb{K}^{k\times 1}$ via the isomorphism provided by Theorem 2.1(iii), the shift operator corresponds to pre-multiplication by the companion matrix $\boldsymbol{C}(f)$, which is exactly claim (i). Then (ii) follows easily from (i) by induction on n. At this point, claim (iii) follows from (ii) by pre-multiplying by $\boldsymbol{C}(f)^n$ the identity matrix $\boldsymbol{I}$ of $\mathbb{K}^{k\times k}$ and noticing that $\boldsymbol{I}_{i,j} = \left(\boldsymbol{\delta}^{(j-1)}(f)\right)_{i-1}$. Finally, if $f(0) \neq 0$ then it is easy to check that $\boldsymbol{C}(f)$ is invertible. More precisely, if $f(x) = x^k - \sum_{i=1}^{k} a_i x^{k-i}$ ($a_i \in \mathbb{K}$) then

$$\boldsymbol{C}(f)^{-1} = \frac{1}{a_k} \begin{pmatrix} -a_{k-1} & -a_{k-2} & \cdots & -a_1 & 1 \\ a_k & 0 & \cdots & 0 & 0 \\ 0 & a_k & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & a_k & 0 \end{pmatrix}.$$

[1] Some authors define the companion matrix as the transpose of the matrix defined here.

[2] Throughout, if a matrix $\boldsymbol{A}$ is associated to a linear map with respect to some bases, then $\boldsymbol{A}$ acts on column vectors $\boldsymbol{v}$ by pre-multiplication $\boldsymbol{v} \mapsto \boldsymbol{A}\boldsymbol{v}$.

[3] Of course, here "characteristic/minimal polynomial" refers to matrices and not to linear recurrences.

Hence, from relation (2.3) it follows that (i), (ii), and (iii) hold for every integer n, if the involved linear recurrences are extended backward. □

The vector $\begin{pmatrix} u_n & \cdots & u_{n+k-1} \end{pmatrix}^\mathsf{T}$ appearing in Theorem 2.22(ii) is known as the nth *state vector* of the linear recurrence $\boldsymbol{u}$.

Example 2.5. For the sequence of Fibonacci numbers, Theorem 2.22(ii) implies that

$$\begin{pmatrix} F_n \\ F_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

for every integer n.

Theorem 2.22(ii) shows that each linear recurrence can be expressed in terms of the powers of its companion matrix. The following theorem states that, in fact, linear recurrences are characterized in terms of powers of matrices.

Theorem 2.23. *Let $\boldsymbol{u} \in \mathbb{K}^\mathbb{N}$ and let k be a positive integer. Then the following statements are equivalent.*

(i) The sequence $\boldsymbol{u}$ is a linear recurrence of order at most k.

(ii) There exist $\boldsymbol{s} \in \mathbb{K}^{1\times k}$, $\boldsymbol{A} \in \mathbb{K}^{k\times k}$, and $\boldsymbol{t} \in \mathbb{K}^{k\times 1}$ such that $u_n = \boldsymbol{s}\boldsymbol{A}^n\boldsymbol{t}$ for each integer $n \geq 0$.

Proof. Suppose that $\boldsymbol{u}$ is a linear recurrence of order at most k. Let $f \in \mathbb{K}[x]$ be a monic polynomial of degree k such that $\boldsymbol{u} \in \mathcal{L}(f)$. Note that, by Theorem 2.2, the polynomial f can be obtained by multiplying the minimal polynomial of $\boldsymbol{u}$ by a monic polynomial of appropriate degree. Let $\boldsymbol{s} := \boldsymbol{e}_1$, $\boldsymbol{A} := \boldsymbol{C}(f)$, and $\boldsymbol{t} := \begin{pmatrix} u_0 & \cdots & u_{k-1} \end{pmatrix}^\mathsf{T}$. Then Theorem 2.22(ii) gives that $u_n = \boldsymbol{s}\boldsymbol{A}^n\boldsymbol{t}$ for every integer $n \geq 0$. Thus (i) implies (ii).

Suppose that there exist $\boldsymbol{s} \in \mathbb{K}^{1\times k}$, $\boldsymbol{A} \in \mathbb{K}^{k\times k}$, and $\boldsymbol{t} \in \mathbb{K}^{k\times 1}$ such that $u_n = \boldsymbol{s}\boldsymbol{A}^n\boldsymbol{t}$ for every integer $n \geq 0$. Let $f(x) = \sum_{i=0}^k a_i x^i$ $(a_i \in \mathbb{K})$ be the characteristic polynomial of $\boldsymbol{A}$. The Cayley–Hamilton theorem says that $f(\boldsymbol{A}) = \boldsymbol{0}$. Hence

$$(f\boldsymbol{u})_n = \sum_{i=0}^k a_i u_{n+i} = \sum_{i=0}^k a_i \boldsymbol{s}\boldsymbol{A}^{n+i}\boldsymbol{t} = \boldsymbol{s}\sum_{i=0}^k a_i \boldsymbol{A}^{n+i}\boldsymbol{t} = \boldsymbol{s}f(\boldsymbol{A})\boldsymbol{t} = 0,$$

for every integer $n \geq 0$. Therefore, the sequence $\boldsymbol{u}$ is a linear recurrence of order at most k. Thus (ii) implies (i). □

The next result shows that applying a linear functional to the sequence of powers of a matrix produces a linear recurrence.

Theorem 2.24. *Let k be a positive integer, let $\boldsymbol{A} \in \mathbb{K}^{k\times k}$, and let ℓ be a linear map $\mathbb{K}^{k\times k} \to \mathbb{K}$. Then the sequence $\big(\ell(\boldsymbol{A}^n)\big)$ is a linear recurrence.*

Proof. By the linearity of ℓ, the sequence $\big(\ell(\boldsymbol{A}^n)\big)$ is a linear combination of the sequences $\big(\boldsymbol{e}_i\boldsymbol{A}^n\boldsymbol{e}_j^\mathsf{T}\big)$, where $i, j \in \{1, \ldots, k\}$. In turn, by Theorem 2.23, each of these sequences is a linear recurrence. Therefore, the claim follows from Theorem 2.5(iii). □

Example 2.6. Let k be a positive integer and let $\boldsymbol{A} \in \mathbb{K}^{k\times k}$. Then the sequence $\big(\operatorname{tr}(\boldsymbol{A}^n)\big)$ is a linear recurrence.

2.5 Vandermonde matrix

Throughout this section, let $f(x) := \prod_{i=1}^{s}(x-\alpha_i)^{k_i}$, where $\alpha_1,\dots,\alpha_s \in \mathbb{K}^*$ are pairwise distinct and $k_1,\dots,k_s$ are positive integers. Put also $k := \deg(f) = \sum_{i=1}^{s} k_i$. The vector space $\mathcal{L}(f)$ has two important bases. The first is the basis of impulse sequences $\boldsymbol{\delta}^{(\ell)}(f)$, with $\ell \in \{0,\dots,k-1\}$, which appears in Theorem 2.1(i). The second is the basis of linear recurrences $\boldsymbol{\psi}^{(j)}(\alpha_i)$, with $i \in \{1,\dots,s\}$ and $j \in \{0,\dots,k_i-1\}$, which appears in Theorem 2.14.

The *Vandermonde matrix* $\boldsymbol{V}(f)$ associated to f is defined[4] as the matrix of change of basis from $\boldsymbol{\psi}^{(j)}(\alpha_i)$ to $\boldsymbol{\delta}^{(\ell)}(f)$. More precisely, the Vandermonde matrix $\boldsymbol{V}(f)$ is the (block) matrix defined by

$$\boldsymbol{V}(f) := \big(\boldsymbol{v}_{n,i}\big)_{\substack{0\le n<k\\ 1\le i\le s}} \in \mathbb{K}^{k\times k} \text{ where } \boldsymbol{v}_{n,i} := \Big(\big(\boldsymbol{\psi}^{(j)}(\alpha_i)\big)_n\Big)_{0\le j<k_i} \in \mathbb{K}^{1\times k_i}. \tag{2.10}$$

Note that $\boldsymbol{V}(f)$ does not depend only on f but, in fact, also on the order assigned to the roots $\alpha_1,\dots,\alpha_s$. This slight abuse of notation is not a problem. Since $\boldsymbol{V}(f)$ is a change-of-basis matrix, it follows that $\boldsymbol{V}(f)$ is invertible.

Let the *Jordan matrix* associated to f be defined as

$$\boldsymbol{J}(f) := \begin{pmatrix} \boldsymbol{J}_{\alpha_1,k_1} & & \\ & \ddots & \\ & & \boldsymbol{J}_{\alpha_s,k_s} \end{pmatrix} \in \mathbb{K}^{k\times k}, \quad \text{where} \quad \boldsymbol{J}_{\alpha,h} := \begin{pmatrix} \alpha & 1 & & & \\ & \alpha & 1 & & \\ & & \ddots & \ddots & \\ & & & \alpha & 1 \\ & & & & \alpha \end{pmatrix} \in \mathbb{K}^{h\times h}$$

for every $\alpha \in \mathbb{K}$ and for each positive integer h. Similarly to $\boldsymbol{V}(f)$, note that $\boldsymbol{J}(f)$ does not depend only on f but also on the order assigned to the roots.

Example 2.7. If $s=2$, $k_1=1$, and $k_2=2$, then

$$\boldsymbol{V}(f) = \begin{pmatrix} \big(\boldsymbol{\psi}^{(0)}(\alpha_1)\big)_0 & \big(\boldsymbol{\psi}^{(0)}(\alpha_2)\big)_0 & \big(\boldsymbol{\psi}^{(1)}(\alpha_2)\big)_0 \\ \big(\boldsymbol{\psi}^{(0)}(\alpha_1)\big)_1 & \big(\boldsymbol{\psi}^{(0)}(\alpha_2)\big)_1 & \big(\boldsymbol{\psi}^{(1)}(\alpha_2)\big)_1 \\ \big(\boldsymbol{\psi}^{(0)}(\alpha_1)\big)_2 & \big(\boldsymbol{\psi}^{(0)}(\alpha_2)\big)_2 & \big(\boldsymbol{\psi}^{(1)}(\alpha_2)\big)_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ \alpha_1 & \alpha_2 & 1 \\ 2\alpha_1^2 & 2\alpha_2^2 & \alpha_2 \end{pmatrix}$$

and

$$\boldsymbol{J}(f) = \begin{pmatrix} \alpha_1 & 0 & 0 \\ 0 & \alpha_2 & 1 \\ 0 & 0 & \alpha_2 \end{pmatrix}.$$

The next theorem states that the Vandermonde matrix $\boldsymbol{V}(f)$ is the matrix that transform the companion matrix $\boldsymbol{C}(f)$ into Jordan normal form.

Theorem 2.25. $\boldsymbol{V}(f)^{-1}\boldsymbol{C}(f)\boldsymbol{V}(f) = \boldsymbol{J}(f)$.

[4] Other authors call it the *confluent* Vandermonde matrix, and may or may not define it as $\boldsymbol{V}(f)^{\intercal}$.

The proof of Theorem 2.25 requires the following lemma.

Lemma 2.26. *Let $\alpha \in \mathbb{K}^*$ and let h be a positive integer. Then $\boldsymbol{J}_{\alpha,h}$ is the matrix associated to the shift operator as an endomorphism of $\mathcal{L}\big((x-\alpha)^h\big)$ with respect to the basis $\boldsymbol{\psi}^{(0)}, \ldots, \boldsymbol{\psi}^{(h-1)}$.*

Proof. Lemma 2.17 says that $x\boldsymbol{\psi}^{(j)} = \alpha\boldsymbol{\psi}^{(j)} + \boldsymbol{\psi}^{(j-1)}$ for each $j \in \{0, \ldots, h-1\}$. The claim follows. □

Proof of Theorem 2.25. Consider the shift operator as an endomorphism of $\mathcal{L}(f)$. The companion matrix $\boldsymbol{C}(f)$ is the matrix associated to the shift operator with respect to the basis $\boldsymbol{\delta}^{(\ell)}(f)$. Theorem 2.5(iv) says that $\mathcal{L}(f)$ is the direct sum of the subspaces $\mathcal{L}\big((x-\alpha_i)^{k_i}\big)$ where $i \in \{1, \ldots, s\}$. Hence, by Lemma 2.26, the Jordan matrix $\boldsymbol{J}(f)$ is the matrix associated to the shift operator with respect to the basis $\boldsymbol{\psi}^{(j)}(\alpha_i)$. The claim follows since $\boldsymbol{V}(f)$ is the matrix of change of basis from $\boldsymbol{\psi}^{(j)}(\alpha_i)$ to $\boldsymbol{\delta}^{(\ell)}(f)$. □

Remark 2.27. In light of Theorem 2.25, the following is a sketch of an alternative way to prove Theorem 2.14. The characteristic polynomial of $\boldsymbol{C}(f)$ is equal to f and so it splits into linear factors over $\mathbb{K}$. Hence, from the theorem on the existence of the Jordan normal form, it follows that $\boldsymbol{C}(f)$ is similar to $\boldsymbol{J}(f)$, and consequently $\boldsymbol{C}(f)^n$ is similar to $\boldsymbol{J}(f)^n$ for every integer $n \geq 0$, where the transformation matrix is independent from n. Furthermore, for every $\alpha \in \mathbb{K}^*$ and for all integers $h > 0$ and $n \geq 0$, the entry of the ith row and jth column of $\boldsymbol{J}_{\alpha,h}^n$ is equal to $\big(\boldsymbol{\psi}^{(j-i)}(\alpha)\big)_n$ (Lemma 3.4). Then Theorem 2.14 follows from Theorem 2.22(ii).

The following result concerns the computation of the coefficients of the power-sum representation of a linear recurrence.

Theorem 2.28. *Let $\boldsymbol{u} \in \mathcal{L}(f)$. Then the coefficients $c_{i,j}$ of (2.4) can be computed from f and $u_0, \ldots, u_{k-1}$ by solving the linear system*

$$\boldsymbol{V}(f)\,(\boldsymbol{c}_1 \ \cdots \ \boldsymbol{c}_k)^\intercal = (u_0 \ \cdots \ u_{k-1})^\intercal, \tag{2.11}$$

where $\boldsymbol{c}_i := (c_{i,0} \ \cdots \ c_{i,k_i-1})$ for each $i \in \{1, \ldots, s\}$.

Proof. Since $\boldsymbol{V}(f)$ is the matrix of change of basis from $\boldsymbol{\psi}^{(j)}(\alpha_i)$ to $\boldsymbol{\delta}^{(\ell)}(f)$, the claim follows. □

For every integer $j \geq 0$, let $\mathrm{D}^{(j)}$ be the jth *Hasse derivative*, that is, the linear map $\mathbb{K}[x] \to \mathbb{K}[x]$ defined by

$$\mathrm{D}^{(j)} x^n := \binom{n}{j} x^{n-j} \tag{2.12}$$

for every integer $n \geq 0$. (Note that if $j > n$ then $\binom{n}{j} = 0$ and the right-hand side of (2.12) is indeed a polynomial.) If $\mathrm{char}(\mathbb{K}) = 0$ then it follows easily that $\mathrm{D}^{(j)} = (j!)^{-1}(\mathrm{d}/\mathrm{d}x)^j$ for every integer $j \geq 0$, where $\mathrm{d}/\mathrm{d}x$ is the formal derivative of polynomials.

The *Hermite interpolation problem* asks to determine a polynomial $p \in \mathbb{K}[x]$ given the values $(\mathrm{D}^{(j)}p)(\alpha_i)$, where $i \in \{1, \dots, s\}$ and $j \in \{0, \dots, k_i - 1\}$. The special case in which $k_1 = \cdots = k_s = 1$ is the *Lagrange interpolation problem*.

The following theorem shows that the Vandermonde matrix $\boldsymbol{V}(f)$ is strictly related to the Hermite interpolation problem.

Theorem 2.29. *Let $y_{i,j} \in \mathbb{K}$ for every $i \in \{1, \dots, s\}$ and $j \in \{0, \dots, k_i - 1\}$. Then there exists a unique polynomial $p(x) := \sum_{i=0}^{k-1} b_i x^i$ $(b_i \in \mathbb{K})$ such that*

$$(\mathrm{D}^{(j)}p)(\alpha_i) = y_{i,j} \quad \text{for every } i \in \{1, \dots, s\} \text{ and } j \in \{0, \dots, k_i - 1\}. \tag{2.13}$$

More precisely, the coefficients b_i are given by the unique solution to the linear system

$$(b_0 \ \cdots \ b_{k-1})\, \boldsymbol{V}(f) = (\boldsymbol{y}_1 \ \cdots \ \boldsymbol{y}_k), \tag{2.14}$$

where $\boldsymbol{y}_i := (y_{i,0} \ \cdots \ y_{i,k_i-1}) \in \mathbb{K}^{1\times k_i}$ for each $i \in \{1, \dots, s\}$.

Proof. From definitions (2.10) and (2.12), the conditions (2.13) are equivalent to the linear system (2.14). The claim follows. □

It is perhaps interesting to note that, in light of Theorem 2.28 and Theorem 2.29, the problem of determining the coefficients of the power-sum representation of a linear recurrence and the problem of Hermite interpolation are "dual" to each other.

The entries of the inverse of the Vandermonde matrix $\boldsymbol{V}(f)$ do not have a simply expression. However, the following result holds.

Theorem 2.30. *Let $\ell, m \in \{1, \dots, k\}$ and let i, j be the unique integers such that*

$$\ell = \Big(\sum_{v=1}^{i-1} k_v\Big) + j + 1, \quad 1 \le i \le s, \quad 0 \le j < k_i.$$

Then the entry on the ℓth row and mth column of $\boldsymbol{V}(f)^{-1}$ is equal to the coefficient of x^{m-1} in the polynomial

$$\Big[(x-\alpha_i)^j \big(g_i(x)\big)^{-1} \bmod (x-\alpha_i)^{k_i}\Big] g_i(x),$$

where $g_i(x) := f(x)/(x-\alpha_i)^{k_i}$.

In particular, if $k_1 = \cdots = k_s = 1$ then the aforementioned entry is equal to the coefficient of x^{m-1} in the polynomial $g_\ell(x)/g_\ell(\alpha_\ell)$.

Proof. Proceed by solving the Hermite interpolation problem of Theorem 2.29. This gives a way to invert $\boldsymbol{V}(f)$ by employing (2.14). Let $y_{i,j} \in \mathbb{K}$ for every $i \in \{1, \dots, s\}$ and $j \in \{0, \dots, k_i - 1\}$, and let $p(x) := \sum_{i=0}^{k-1} b_i x^i$ $(b_i \in \mathbb{K})$ be the unique polynomial satisfying (2.13).

From definition (2.12) and the binomial theorem, it follows easily that

$$p(x) = \sum_{j=0}^{\infty} (\mathrm{D}^{(j)}p)(\alpha)\,(x-\alpha)^j, \tag{2.15}$$

for every $\alpha \in \mathbb{K}$. In turn, from (2.15) it follows that conditions (2.13) are equivalent to

$$p(x) \equiv r_i(x) \pmod{(x-\alpha_i)^{k_i}} \quad \text{for every } i \in \{1,\dots,s\}, \tag{2.16}$$

where $r_i(x) := \sum_{j=0}^{k_i-1} y_{i,j}(x-\alpha_i)^j$.

Hence, by the Chinese remainder theorem, the polynomial $p(x)$ is the unique solution modulo $f(x)$ of the system of congruences (2.16). More precisely

$$\begin{aligned} p(x) &= \sum_{i=1}^{s} r_i(x)\Big[\big(g_i(x)\big)^{-1} \bmod (x-\alpha_i)^{k_i}\Big] g_i(x) \\ &= \sum_{i=1}^{s} \sum_{j=0}^{k_i-1} y_{i,j}(x-\alpha_i)^j \Big[\big(g_i(x)\big)^{-1} \bmod (x-\alpha_i)^{k_i}\Big] g_i(x), \end{aligned}$$

where $g_i(x) := f(x)/(x-\alpha_i)^{k_i}$ for every $i \in \{1,\dots,s\}$.

At this point, the thesis follows from Theorem 2.29 by setting the values $y_{i,j}$ so that the vector $(\boldsymbol{y}_1 \ \cdots \ \boldsymbol{y}_k)$ has the ℓth entry equal to 1 and all the other entries equal to 0. □

Combining Theorem 2.28 and Theorem 2.30, it is possible to write explicit formulas for the coefficients of the power-sum representation of an arbitrary linear recurrence. However, these formulas involve quite unwieldy products and are not particularly useful, so they are not considered here. Instead, assuming that f has no multiple roots, the power-sum representation of the impulse sequence $\boldsymbol{\delta}^{(k-1)}(f)$ has a quite explicit formula.

Theorem 2.31. *Suppose that $k_1 = \cdots = k_s = 1$. Then*

$$\big(\boldsymbol{\delta}^{(k-1)}(f)\big)_n = \sum_{i=1}^{k} c_i \alpha_i^n, \qquad \textit{where} \qquad c_i := \prod_{\substack{j=1 \\ j\neq i}}^{k} \frac{1}{\alpha_i - \alpha_j}, \tag{2.17}$$

for every integer $n \geq 0$.

Proof. From Theorem 2.15 there exist some coefficients $c_1,\dots,c_k \in \mathbb{K}$ such that the first equality in (2.17) holds. Furthermore, since $\big(\boldsymbol{\delta}^{(k-1)}\big)_n = \delta_{k-1,n}$ for every $n \in \{0,\dots,k-1\}$, by Theorem 2.28 the coefficient c_i is equal to the entry of the ith row and kth column of $\boldsymbol{V}(f)^{-1}$. In turn, according to Theorem 2.30, this entry is equal to the coefficient of x^{k-1} in the polynomial

$$\prod_{\substack{j=1 \\ j\neq i}}^{k} \frac{x-\alpha_j}{\alpha_i - \alpha_j},$$

and this coefficient is clearly equal to the expression for c_i provided in (2.17). □

Note that Theorem 2.31 can be used to determine the power-sum representation of every simple linear recurrence $\boldsymbol{u}$ with minimal polynomial f, after having written $\boldsymbol{u}$ as a linear combination of the basis $x^0\boldsymbol{\delta}^{(k-1)},\dots,x^{k-1}\boldsymbol{\delta}^{(k-1)}$ (recall Theorem 2.3 and Theorem 2.4).

2.6 Computing the nth term

Given the initial values $u_0, \ldots, u_{k-1}$ and the characteristic polynomial f of a linear recurrence $\boldsymbol{u}$ over $\mathbb{K}$, there are several methods to compute the nth term of $\boldsymbol{u}$.

2.6.1 By the linear recurrence relation

The simplest method consists in employing the linear recurrence relation (1.1) to compute $u_k, u_{k+1}, \ldots$ up to u_n. This is the most inefficient method and requires about kn multiplications in $\mathbb{K}$. It makes sense if it is needed to compute not only u_n but also all the previous terms of the linear recurrence.

2.6.2 By powers of the companion matrix

A better method is to use Theorem 2.22(ii) and compute u_n by taking the nth power of the companion matrix $\boldsymbol{C}(f)$. If $\boldsymbol{C}(f)^n$ is computed using *binary exponentiation* [102, Section 4.6.3], then this method requires about $\log_2 n$ multiplications of $k \times k$ matrices with entries in $\mathbb{K}$, which is no more than $(\log_2 n)k^3$ multiplications in $\mathbb{K}$.

2.6.3 By powers of the Jordan matrix

Another method consists in computing u_n via its power-sum representation involving the roots $\alpha_1, \ldots, \alpha_s$ of f, taken in the splitting field $\mathbb{L}$ of f over $\mathbb{K}$. In fact, as already observed in Remark 2.27, this is equivalent to computing the nth power of the Jordan matrix $\boldsymbol{J}(f)$. Again using binary exponentiation, the computational complexity of this method is dominated by $s \log_2 n$ multiplications in $\mathbb{L}$, so it can be more or less efficient than the previous method depending on the degree of the extension $\mathbb{L}/\mathbb{K}$.

2.6.4 By powers of x modulo the characteristic polynomial

Theorem 2.32. *Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$ with characteristic polynomial $f(x)$ of positive degree k. Then $u_n = \sum_{i=0}^{k-1} r_i u_i$ for every integer $n \geq 0$, where $r(x) = \sum_{i=0}^{k-1} r_i x^i$ $(r_i \in \mathbb{K})$ is the remainder of the division of x^n by $f(x)$.*

Proof. Note that $x^n = q(x)f(x) + r(x)$ for some polynomial $q(x) \in \mathbb{K}[x]$. Since $f\boldsymbol{u} = \boldsymbol{0}$, it follows that

$$x^n \boldsymbol{u} = (qf + r)\boldsymbol{u} = q(f\boldsymbol{u}) + r\boldsymbol{u} = r\boldsymbol{u}. \tag{2.18}$$

Thus the 0th terms of the sequences on the left- and right-hand side of (2.18) are equal, which means that $u_n = \sum_{i=0}^{k-1} r_i u_i$, as claimed. □

Using binary exponentiation, this method requires about $\log_2 n$ polynomial multiplications modulo $f(x)$.

Remark 2.33. If $\mathbb{K}$ is an infinite field then it is necessary to refine the analysis in this section by taking into account that the computational cost of each multiplication is not fixed but increases with the "size" of the operands. For instance, the nth term of a general linear

recurrences over the integers grows exponentially in n (see Section 5.5). Hence, computing it for very large n is unfeasible simple because too much memory is required to store the result.

2.7 Product of linear recurrences

For every two sequences $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$, define the *(termwise) product* $\boldsymbol{uv} \in \mathbb{K}^{\mathbb{N}}$ as the sequence such that $(\boldsymbol{uv})_n = u_n v_n$ for every integer $n \geq 0$. It follows easily that $\mathbb{K}^{\mathbb{N}}$ equipped with the termwise addition and the termwise multiplication of sequences is a $\mathbb{K}$-algebra.

Corollary 2.6 says that the sum of two linear recurrences is a linear recurrence. The following theorem shows that also the product of two linear recurrences is a linear recurrence. Therefore, linear recurrences form a subalgebra of $\mathbb{K}^{\mathbb{N}}$.

Theorem 2.34. *Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be two linear recurrences over $\mathbb{K}$ of orders k and ℓ, respectively. Then $\boldsymbol{uv}$ is a linear recurrence of order at most $k\ell$.*

For all vector subspaces U and V of $\mathbb{K}^{\mathbb{N}}$, let UV be the vector subspace spanned by all the products $\boldsymbol{uv}$ with $\boldsymbol{u} \in U$ and $\boldsymbol{v} \in V$.

Proof of Theorem 2.34. Let f and g be the minimal polynomials of $\boldsymbol{u}$ and $\boldsymbol{v}$, respectively. Theorem 2.1(i) says that $\mathcal{L}(f)$ and $\mathcal{L}(g)$ are vector spaces of dimensions k and ℓ, respectively. Hence, it follows easily that $V := \mathcal{L}(f)\mathcal{L}(g)$ is a vector space of dimension at most $k\ell$. Let $\boldsymbol{v} \in V$. Then $\boldsymbol{v} = \sum_{i=1}^{s} \boldsymbol{w}_i \boldsymbol{z}_i$ for some $\boldsymbol{w}_1, \dots, \boldsymbol{w}_s \in \mathcal{L}(f)$ and $\boldsymbol{z}_1, \dots, \boldsymbol{z}_s \in \mathcal{L}(g)$. Theorem 2.7 gives that $x\boldsymbol{w}_i \in \mathcal{L}(f)$ and $x\boldsymbol{z}_i \in \mathcal{L}(g)$ for each $i \in \{1, \dots, s\}$. Consequently $x\boldsymbol{v} = \sum_{i=1}^{s} (x\boldsymbol{w}_i)(x\boldsymbol{z}_i) \in V$. Thus V is closed with respect to the shift operator. Therefore, Theorem 2.7 and Theorem 2.1(i) imply that there exists a nonzero $h \in \mathbb{K}[x]$ such that $\deg(h) \leq k\ell$ and $V = \mathcal{L}(h)$. Since $\boldsymbol{uv} \in V$, the product $\boldsymbol{uv}$ is a linear recurrence of order at most $k\ell$. □

Remark 2.35. Suppose that $\operatorname{char}(\mathbb{K}) = 0$ and that $\boldsymbol{u}$ and $\boldsymbol{v}$ are reversible linear recurrences over $\mathbb{K}$. Then an alternative way to prove Theorem 2.34 is the following. By Theorem 2.15, reversible linear recurrences are generalized power sums (in some extension of $\mathbb{K}$). Then it is easy to check that the product of two generalized power sums of orders k and ℓ is a generalized power sums of order at most $k\ell$.

The explicit determination of the polynomial h in the proof of Theorem 2.34 is nontrivial. In fact, the rest of this section is devoted to such a task.

For all positive integers k and h, define

$$k \vee h := \max\left\{ i + j + 1 : i, j \in \mathbb{N},\ i < k,\ j < h,\ \binom{i+j}{i} \neq 0 \text{ in } \mathbb{K} \right\}. \tag{2.19}$$

Note that $k \vee h$ depends only on k, h and the characteristic of $\mathbb{K}$. In particular, $k \vee h$ does not change if $\mathbb{K}$ is replaced by a subfield or an extension field. Moreover

$$\max(k, h) \leq k \vee h \leq k + h - 1. \tag{2.20}$$

The lower bound in (2.20) follows since $\binom{(k-1)+0}{k-1} = \binom{0+(h-1)}{h-1} = 1$, while the upper bound is straightforward and it is always attained if the characteristic of $\mathbb{K}$ is equal to zero.

Let $f, g \in \mathbb{K}[x]$ be nonconstant polynomials. Define the *Zierler–Mills polynomial* $Z(f,g)$ of f and g as follows. Let $\mathbb{L}$ be the splitting field of fg over $\mathbb{K}$, let $\alpha_1, \dots, \alpha_s \in \mathbb{L}$ be the pairwise distinct roots of f and let $k_1, \dots, k_s$ be their multiplicities; let $\beta_1, \dots, \beta_t \in \mathbb{L}$ be the pairwise distinct roots of g and let $h_1, \dots, h_t$ be their multiplicities. Furthermore, let $\gamma_1, \dots, \gamma_r$ be all the pairwise distinct products $\alpha_i\beta_j$, with $i \in \{1, \dots, s\}$ and $j \in \{1, \dots, t\}$, and let

$$e_\ell := \max\{k_i \vee h_j : \alpha_i\beta_j = \gamma_\ell\}$$

for each $\ell \in \{1, \dots, r\}$. Then the Zierler–Mills polynomial is defined as

$$Z(f,g) := \prod_{\ell=1}^{r} (x - \gamma_\ell)^{e_\ell}.$$

The main theorem of this section is the following.

Theorem 2.36. *Let $f, g \in \mathbb{K}[x]$ be monic nonconstant polynomials with $f(0) \neq 0$ and $g(0) \neq 0$. Then $Z(f,g) \in \mathbb{K}[x]$ and*

$$\mathcal{L}(f)\mathcal{L}(g) = \mathcal{L}\big(Z(f,g)\big).$$

The proof of Theorem 2.36 requires several lemmas. First, the following results regard the linear recurrences $\boldsymbol{\psi}^{(j)}(\alpha)$ introduced in Section 2.3.

Lemma 2.37. *Let $\alpha \in \mathbb{K}^*$ and let $i, j \geq 0$ be integers. Then the minimal polynomial of the linear recurrence $x^i\boldsymbol{\psi}^{(j)}$ is equal to $(x-\alpha)^{j+1}$.*

Proof. From Lemma 2.17 it follows that

$$(x-\alpha)^j(x^i\boldsymbol{\psi}^{(j)}) = x^i\boldsymbol{\psi}^{(0)} \neq \mathbf{0} \quad \text{and} \quad (x-\alpha)^{j+1}(x^i\boldsymbol{\psi}^{(j)}) = x^i\boldsymbol{\psi}^{(-1)} = \mathbf{0}.$$

The claim follows from Theorem 2.2. □

Lemma 2.38. *Let $\alpha \in \mathbb{K}^*$ and let $k > 0$, $i_1, \dots, i_k \geq 0$ be integers. Then the sequences $x^{i_1}\boldsymbol{\psi}^{(0)}, \dots, x^{i_k}\boldsymbol{\psi}^{(k-1)}$ form a basis of $\mathcal{L}\big((x-\alpha)^k\big)$.*

Proof. The proof proceeds exactly as the proof of Lemma 2.18, but replacing $\boldsymbol{\psi}^{(j)}$ with $x^{i_{j+1}}\boldsymbol{\psi}^{(j)}$, and noticing that $x^{i_{j+1}}\boldsymbol{\psi}^{(0)} \neq \mathbf{0}$. □

Lemma 2.39. *Let $\alpha, \beta \in \mathbb{K}^*$ and let $i, j \geq 0$ be integers. Then*

$$\boldsymbol{\psi}^{(i)}(\alpha)\, x^j\boldsymbol{\psi}^{(j)}(\beta) = \beta^i \binom{i+j}{i} x^j\boldsymbol{\psi}^{(i+j)}(\alpha\beta).$$

Proof. For every integer $n \geq 0$, thanks to the identity $\binom{n}{i}\binom{n+j}{j} = \binom{i+j}{i}\binom{n+j}{i+j}$,

$$\begin{aligned}\big(\boldsymbol{\psi}^{(i)}(\alpha)\, x^j \boldsymbol{\psi}^{(j)}(\beta)\big)_n &= \binom{n}{i}\alpha^{n-i}\binom{n+j}{j}\beta^n = \beta^i\binom{n}{i}\binom{n+j}{j}(\alpha\beta)^{n-i} \\ &= \beta^i\binom{i+j}{i}\binom{n+j}{i+j}(\alpha\beta)^{n-i} = \beta^i\binom{i+j}{i}\binom{n+j}{i+j}(\alpha\beta)^{n+j-(i+j)} \\ &= \beta^i\binom{i+j}{i}\big(x^j\boldsymbol{\psi}^{(i+j)}(\alpha\beta)\big)_n.\end{aligned}$$

The claim follows. □

The next lemma provides the first connection between the operation $\vee$ and the product of linear recurrences.

Lemma 2.40. *Let $\alpha, \beta \in \mathbb{K}^*$ and let k, h be positive integers. Then*

$$\mathcal{L}\big((x-\alpha)^k\big)\mathcal{L}\big((x-\beta)^h\big) = \mathcal{L}\big((x-\alpha\beta)^{k\vee h}\big).$$

Proof. Lemma 2.38 states that $\boldsymbol{\psi}^{(0)}(\alpha), \dots, \boldsymbol{\psi}^{(k-1)}(\alpha)$ form a basis of $\mathcal{L}\big((x-\alpha)^k\big)$ and $x^0\boldsymbol{\psi}^{(0)}(\beta), \dots, x^{h-1}\boldsymbol{\psi}^{(h-1)}(\beta)$ form a basis of $\mathcal{L}\big((x-\beta)^h\big)$. From Lemma 2.39, Lemma 2.37, and (2.19) it follows that

$$\boldsymbol{\psi}^{(i)}(\alpha)\, x^j\boldsymbol{\psi}^{(j)}(\beta) = \beta^i\binom{i+j}{i}x^j\boldsymbol{\psi}^{(i+j)}(\alpha\beta) \in \mathcal{L}\big((x-\alpha\beta)^{k\vee h}\big),$$

for every $i \in \{0, \dots, k-1\}$ and $j \in \{0, \dots, h-1\}$. Therefore

$$\mathcal{L}\big((x-\alpha)^k\big)\mathcal{L}\big((x-\beta)^h\big) \subseteq \mathcal{L}\big((x-\alpha\beta)^{k\vee h}\big). \tag{2.21}$$

From (2.19) there exist $i_0 \in \{0, \dots, k-1\}$ and $j_0 \in \{0, \dots, h-1\}$ such that $k \vee h = i_0 + j_0 + 1$ and $\binom{i_0+j_0}{i_0} \neq 0$ in $\mathbb{K}$. On the one hand, by Lemma 2.37, the minimal polynomial of

$$\boldsymbol{u} := \beta^{i_0}\binom{i_0+j_0}{i_0}x^{j_0}\boldsymbol{\psi}^{(i_0+j_0)}(\alpha\beta)$$

is equal to $(x-\alpha\beta)^{k\vee h}$. Hence, Theorem 2.3 implies that $x^0\boldsymbol{u}, \dots, x^{k\vee h-1}\boldsymbol{u}$ form a basis of $\mathcal{L}\big((x-\alpha\beta)^{k\vee h}\big)$. On the other hand, by Lemma 2.39 and Theorem 2.7,

$$x^\ell\boldsymbol{u} = \big(x^\ell\boldsymbol{\psi}^{(i_0)}(\alpha)\big)\big(x^j\boldsymbol{\psi}^{(j_0)}(\beta)\big) \in \mathcal{L}\big((x-\alpha)^k\big)\mathcal{L}\big((x-\beta)^h\big),$$

for every integer $\ell \geq 0$, since $\mathcal{L}\big((x-\alpha)^k\big)$ is closed with respect to the shift operator. Therefore

$$\mathcal{L}\big((x-\alpha\beta)^{k\vee h}\big) \subseteq \mathcal{L}\big((x-\alpha)^k\big)\mathcal{L}\big((x-\beta)^h\big). \tag{2.22}$$

The claim follows from (2.21) and (2.22). □

The following two lemmas concern some properties of the operation $\vee$.

Lemma 2.41. *Suppose that* $p := \mathrm{char}(\mathbb{K}) > 0$. *Let* k *and* h *be positive integers. Then*

$$k \vee h = p^{\ell_0} + \sum_{\ell=\ell_0}^{\infty} (k_\ell + h_\ell) p^\ell,$$

where $k_\ell, h_\ell \in \{0, \ldots, p-1\}$ $(\ell \in \mathbb{N})$ *are uniquely determined by*

$$k - 1 = \sum_{\ell=0}^{\infty} k_\ell p^\ell \quad \text{and} \quad h - 1 = \sum_{\ell=0}^{\infty} h_\ell p^\ell, \tag{2.23}$$

and ℓ_0 *is minimal nonnegative integer such that* $k_\ell + h_\ell < p$ *for all integers* $\ell \geq \ell_0$.

Proof. Let $i, j \geq 0$ be integers such that $i < k$, $j < h$, $\binom{i+j}{j} \not\equiv 0 \pmod{p}$, and $i + j + 1$ is maximum. *Kummer's theorem* (Theorem A.33) asserts that the highest power of p that divides $\binom{i+j}{i}$ is equal to p^c, where c is the number of carries in the base-p addition of i and j. Consequently, since $\binom{i+j}{j} \not\equiv 0 \pmod{p}$, writing

$$i = \sum_{\ell=0}^{\infty} i_\ell p^\ell \quad \text{and} \quad j = \sum_{\ell=0}^{\infty} j_\ell p^\ell,$$

where $i_\ell, j_\ell \in \{0, \ldots, p-1\}$ $(\ell \in \mathbb{N})$, implies that $i_\ell + j_\ell < p$ for every integer $\ell \geq 0$.

Moreover, the bounds $i < k$ and $j < h$ and the maximality of $i + j + 1$ imply that $(i_\ell, j_\ell) = (k_\ell, h_\ell)$ if $\ell \geq \ell_0$, and $i_\ell + j_\ell = p - 1$ if $\ell < \ell_0$, for every integer $\ell \geq 0$.

Hence, from (2.19) it follows that

$$\begin{aligned} k \vee h = i + j + 1 &= \sum_{\ell=0}^{\infty} (i_\ell + j_\ell) p^\ell + 1 \\ &= \sum_{\ell=0}^{\ell_0 - 1} (p-1) p^\ell + \sum_{\ell=\ell_0}^{\infty} (k_\ell + h_\ell) p^\ell + 1 = p^{\ell_0} + \sum_{\ell=\ell_0}^{\infty} (k_\ell + h_\ell) p^\ell, \end{aligned}$$

as desired. □

Lemma 2.42. *Suppose that* $p := \mathrm{char}(\mathbb{K}) > 0$. *Let* k *and* h *be positive integers. Then*

$$\nu_p(k \vee h) \geq \max\{\nu_p(k), \nu_p(h)\},$$

where ν_p *is the* p*-adic valuation.*

Proof. Since $\binom{i+j}{i} = \binom{i+j}{j}$ for all integers $i, j \geq 0$, it follows easily that $k \vee h = h \vee k$. Hence, without loss of generality, assume that $\nu_p(k) \leq \nu_p(h)$.

Let k_ℓ, h_ℓ $(\ell \in \mathbb{N})$ and ℓ_0 as in Lemma 2.41. If $\ell_0 \geq \nu_p(h)$ then Lemma 2.41 implies that $\nu_p(k \vee h) \geq \ell_0 \geq \nu_p(h)$, and the proof is complete. Hence, assume that $\ell_0 < \nu_p(h)$. From (2.23) it follows that $h_\ell = p - 1$ for every integer ℓ with $0 \leq \ell < \nu_p(h)$. In turn, by

the definition of ℓ_0, this implies that $k_\ell + h_\ell = p - 1$ for every integer ℓ with $\ell_0 \le \ell < \nu_p(h)$. Thus Lemma 2.41 implies that

$$k \vee h = p^{\ell_0} + \sum_{\ell=\ell_0}^{\nu_p(h)-1} (p-1)p^\ell + \sum_{\ell=\nu_p(h)}^{\infty} (k_\ell + h_\ell)p^\ell = p^{\nu_p(h)} + \sum_{\ell=\nu_p(h)}^{\infty} (k_\ell + h_\ell)p^\ell,$$

which implies that $\nu_p(k \vee h) \ge \nu_p(h)$, as desired. □

Now it is time to establish that the Zierler–Mills belongs to $\mathbb{K}[x]$.

Lemma 2.43. *Let $f, g \in \mathbb{K}[x]$ be monic nonconstant polynomials. Then $Z(f,g) \in \mathbb{K}[x]$.*

Proof. Let $\mathbb{L}$ be the splitting field of fg over $\mathbb{K}$, let $\gamma \in \mathbb{L}$ be a root of $Z(f,g)$ of multiplicity e, and let e_0 be the multiplicity of γ as a root of its minimal polynomial over $\mathbb{K}$. Recall that two elements $\alpha, \beta \in \mathbb{L}$ are said to be *conjugate* (over $\mathbb{K}$) if there exists a field automorphism $\sigma\colon \mathbb{L} \to \mathbb{L}$ that fixes $\mathbb{K}$ and sends α to β; or, equivalently, if α and β have the same minimal polynomial over $\mathbb{K}$. In order to prove that $Z(f,g) \in \mathbb{K}[x]$, it suffices to show that

(i) every conjugate of γ is a root of $Z(f,g)$ of multiplicity e;

(ii) e_0 divides e.

Indeed, by the arbitrariness of the root γ, from (i) and (ii) it follows that $Z(f,g)$ is the product of powers of the minimal polynomials of its roots, and so $Z(f,g) \in \mathbb{K}[x]$.

Proof of (i): Let $\sigma\colon \mathbb{L} \to \mathbb{L}$ be a field automorphism that fixes $\mathbb{K}$. Since γ is a root of $Z(f,g)$, from the definition of $Z(f,g)$ it follows that $\gamma = \alpha\beta$, where α and β are roots of f and g of, say, multiplicities k and h, respectively; and e is the maximum of $k \vee h$ over all the aforementioned α and β. Thus $\sigma(\gamma) = \sigma(\alpha)\sigma(\beta)$ and, since $f, g \in \mathbb{K}[x]$, the images $\sigma(\alpha)$ and $\sigma(\beta)$ are roots of f and g of multiplicities k and h, respectively. Hence, since σ permutes the roots of f and the roots of g, from the definition of $Z(f,g)$ it follows that $\sigma(\gamma)$ is a root of $Z(f,g)$ of multiplicity e, as desired.

Proof of (ii): If $\operatorname{char}(\mathbb{K}) = 0$ then $e_0 = 1$ and (ii) follows. Hence, suppose that $p := \operatorname{char}(\mathbb{K}) > 0$. Since γ is a root of $Z(f,g)$ of multiplicity e, from the definition of $Z(f,g)$ it follows that there exist roots α and β of f and g of multiplicities k and h, respectively, such that $\gamma = \alpha\beta$ and $e = k \vee h$. Let p^a and p^b, where $a, b \ge 0$ are integers, be the multiplicities of α and β, respectively, as roots of their minimal polynomials over $\mathbb{K}$. Thus α^{p^a} and β^{p^b} are separable over $\mathbb{K}$. Since the product of separable elements is separable, if $m := \max\{a, b\}$ then γ^{p^m} is separable over $\mathbb{K}$. In turn, this implies that e_0 divides p^m. Since $f, g \in \mathbb{K}[x]$, it follows that p^a divides k and p^b divides h. Hence, thanks to Lemma 2.42, the power p^m divides $e = k \vee h$. Consequently, the integer e_0 divides e, as desired. □

The next lemma shows that the product of subspaces of $\mathbb{K}^{\mathbb{N}}$ obeys the distributive law.

Lemma 2.44. *Let U, V, W be vector subspaces of $\mathbb{K}^{\mathbb{N}}$. Then $(U+V)W = UW + VW$.*

Proof. On the one hand $(U+V)W \subseteq UW + VW$. On the other hand $UW \subseteq (U+V)W$ and $VW \subseteq (U+V)W$, which implies that $UW + VW \subseteq (U+V)W$. The claim follows. □

If $\mathbb{L}$ is a field extension of $\mathbb{K}$ and $f \in \mathbb{L}[x]$, then let $\mathcal{L}_{\mathbb{L}}(f) := \{\boldsymbol{u} \in \mathbb{L}^{\mathbb{N}} : f\boldsymbol{u} = \boldsymbol{0}\}$.

Lemma 2.45. *Let $\mathbb{L}$ be a finite extension of $\mathbb{K}$ and let $f, g \in \mathbb{K}[x]$ be nonzero. Then*

$$\mathcal{L}(f)\mathcal{L}(g) = \mathcal{L}_{\mathbb{L}}(f)\mathcal{L}_{\mathbb{L}}(g) \cap \mathbb{K}^{\mathbb{N}}. \tag{2.24}$$

Proof. It is easy to check that the left-hand side of (2.24) is contained in the right-hand side. It remains to prove the converse.

Let $e_1, \dots, e_s$ form a basis of $\mathbb{L}$ over $\mathbb{K}$ with $e_1 := 1$. Then, for every $\boldsymbol{u} \in \mathbb{L}^{\mathbb{N}}$, it follows easily that

(i) $\boldsymbol{u} = \sum_{i=1}^{s} \boldsymbol{u}^{(i)} e_i$, where $\boldsymbol{u}^{(i)} \in \mathbb{K}^{\mathbb{N}}$ for each $i \in \{1, \dots, s\}$;

(ii) $\boldsymbol{u} \in \mathcal{L}_{\mathbb{L}}(f)$ if and only if $\boldsymbol{u}^{(i)} \in \mathcal{L}(f)$ for each $i \in \{1, \dots, s\}$ (and similarly for g);

(iii) $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ if and only if $\boldsymbol{u}^{(i)} = \boldsymbol{0}$ for each $i \in \{2, \dots, s\}$.

From (i) and (ii) it follows that the elements of $\mathcal{L}(f)$ span $\mathcal{L}_{\mathbb{L}}(f)$ over $\mathbb{L}$, and similarly the elements of $\mathcal{L}(g)$ span $\mathcal{L}_{\mathbb{L}}(g)$ over $\mathbb{L}$. In turn, this implies that the elements of $\mathcal{L}(f)\mathcal{L}(g)$ span $\mathcal{L}_{\mathbb{L}}(f)\mathcal{L}_{\mathbb{L}}(g)$ over $\mathbb{L}$. From Theorem 2.5(i) it follows that $\mathcal{L}(f)$ and $\mathcal{L}(g)$ have finite dimensions. Hence $\mathcal{L}(f)\mathcal{L}(g)$ has finite dimension. Pick $\boldsymbol{z}_1, \dots, \boldsymbol{z}_t \in \mathbb{K}^{\mathbb{N}}$ that form a basis of $\mathcal{L}(f)\mathcal{L}(g)$ over $\mathbb{K}$.

Let $\boldsymbol{w} \in \mathcal{L}_{\mathbb{L}}(f)\mathcal{L}_{\mathbb{L}}(g) \cap \mathbb{K}^{\mathbb{K}}$. Recalling that the elements of $\mathcal{L}(f)\mathcal{L}(g)$ span $\mathcal{L}_{\mathbb{L}}(f)\mathcal{L}_{\mathbb{L}}(g)$ over $\mathbb{L}$, it follows that $\boldsymbol{w} = \sum_{j=1}^{t} c_j \boldsymbol{z}_j$, where $c_j \in \mathbb{L}$ for each $j \in \{1, \dots, t\}$. Furthermore, $c_j = \sum_{i=1}^{s} d_{i,j} e_i$ for every $j \in \{1, \dots, t\}$, where $d_{i,j} \in \mathbb{K}$. Hence

$$\boldsymbol{w} = \sum_{i=1}^{s} \left(\sum_{j=1}^{t} d_{i,j} \boldsymbol{z}_j \right) e_i.$$

Since $\boldsymbol{w} \in \mathbb{K}^{\mathbb{N}}$, from (iii) it follows that $\sum_{j=1}^{t} d_{i,j} \boldsymbol{z}_j = \boldsymbol{0}$ for each $i \in \{2, \dots, s\}$. Therefore, recalling that $e_1 = 1$, it follows that

$$\boldsymbol{w} = \sum_{j=1}^{t} d_{1,j} \boldsymbol{z}_j \in \mathcal{L}(f)\mathcal{L}(g),$$

as desired. □

Now to the proof of Theorem 2.36.

Proof of Theorem 2.36. Lemma 2.43 states that $Z(g, f) \in \mathbb{K}[x]$. Let $\mathbb{L}$ be the splitting field of fg, let $\alpha_1, \dots, \alpha_s \in \mathbb{L}^*$ be the pairwise distinct roots of f and let $k_1, \dots, k_s$ be their multiplicities; and let $\beta_1, \dots, \beta_t \in \mathbb{L}^*$ be the pairwise distinct roots of g and let $h_1, \dots, h_t$ be their multiplicities. Thus $f(x) = \prod_{i=1}^{s} (x - \alpha_i)^{k_i}$ and $g(x) = \prod_{j=1}^{t} (x - \beta_j)^{h_j}$.

From Theorem 2.5(iv), Lemma 2.44, Lemma 2.40, and again Theorem 2.5(iv), it follows that

$$\mathcal{L}_{\mathbb{L}}(f)\mathcal{L}_{\mathbb{L}}(g) = \Big(\sum_{i=1}^{s} \mathcal{L}_{\mathbb{L}}\big((x - \alpha_i)^{k_i}\big) \Big) \Big(\sum_{j=1}^{t} \mathcal{L}_{\mathbb{L}}\big((x - \beta_j)^{h_j}\big) \Big)$$

$$
\begin{aligned}
&= \sum_{i=1}^{s}\sum_{j=1}^{t} \mathcal{L}_{\mathbb{L}}\big((x-\alpha_i)^{k_i}\big)\mathcal{L}_{\mathbb{L}}\big((x-\beta_j)^{h_j}\big) \\
&= \sum_{i=1}^{s}\sum_{j=1}^{t} \mathcal{L}_{\mathbb{L}}\big((x-\alpha_i\beta_i)^{k_i\vee h_j}\big) \\
&= \mathcal{L}_{\mathbb{L}}\big(Z(f,g)\big). \qquad (2.25)
\end{aligned}
$$

Therefore, from Lemma 2.45, equation (2.25), and Lemma 2.43, it follows that

$$\mathcal{L}(f)\mathcal{L}(g) = \mathcal{L}_{\mathbb{L}}(f)\mathcal{L}_{\mathbb{L}}(g)\cap\mathbb{K}^{\mathbb{N}} = \mathcal{L}_{\mathbb{L}}\big(Z(f,g)\big)\cap\mathbb{K}^{\mathbb{N}} = \mathcal{L}\big(Z(f,g)\big),$$

as desired. □

The Zierler–Mills polynomial $Z(f,g)$ has no simple expression in terms of f and g; especially if $\mathbb{K}$ has positive characteristic p, since in such a case, by Lemma 2.41, the multiplicities of the roots of $Z(f,g)$ depend on the base-p digits of the multiplicities of the roots of f and g. However, the next theorem provides a multiple of $Z(f,g)$ that has a relatively simple expression. Given two matrices $\boldsymbol{A}\in\mathbb{K}^{\ell\times m}$ and $\boldsymbol{B}\in\mathbb{K}^{n\times r}$, their *Kronecker product* $\boldsymbol{A}\otimes\boldsymbol{B}$ is defined as the block matrix $(A_{i,j}\boldsymbol{B})\in\mathbb{K}^{\ell n\times mr}$.

Theorem 2.46. *Let $f,g\in\mathbb{K}[x]$ be monic nonconstant polynomials and put*

$$R(f,g)(x) := \operatorname{res}_y\big(f(y), y^{\deg(g)}g(x/y)\big).$$

Then $R(f,g)\in\mathbb{K}[x]$ and $Z(f,g)$ divides $R(f,g)$. Moreover, the polynomial $R(f,g)$ is the characteristic polynomial of $\boldsymbol{C}(f)\otimes\boldsymbol{C}(g)$.

Proof. Since $y^{\deg(g)}g(x/y)\in\big(\mathbb{K}[x]\big)[y]$, it follows easily that $R(f,g)\in\mathbb{K}[x]$. Let $\mathbb{L}$ be the splitting field of fg, let $\alpha_1,\dots,\alpha_s\in\mathbb{L}$ be the pairwise distinct roots of f and let $k_1,\dots,k_s$ be their multiplicities; let $\beta_1,\dots,\beta_t\in\mathbb{L}$ be the pairwise distinct roots of g and let $h_1,\dots,h_s$ be their multiplicities. Thus $f(x)=\prod_{i=1}^{s}(x-\alpha_i)^{k_i}$ and $g(x)=\prod_{j=1}^{t}(x-\beta_j)^{h_j}$. Let $\gamma_1,\dots,\gamma_r$ be all the pairwise distinct products of the form $\alpha_i\beta_j$ with $i\in\{1,\dots,s\}$ and $j\in\{1,\dots,t\}$. The definition of the resultant gives that

$$R(f,g)(x) = \prod_{i=1}^{s}\big(\alpha_i^{\deg(g)}g(x/\alpha_i)\big)^{k_i} = \prod_{i=1}^{s}\prod_{j=1}^{t}(x-\alpha_i\beta_j)^{k_ih_j} = \prod_{\ell=1}^{r}(x-\gamma_\ell)^{r_\ell}, \qquad (2.26)$$

where

$$r_\ell := \sum_{\alpha_i\beta_j=\gamma_\ell} k_ih_j \geq \sum_{\alpha_i\beta_j=\gamma_\ell}(k_i+h_j-1) \geq \max_{\alpha_i\beta_j=\gamma_\ell}(k_i\vee h_j),$$

for each $\ell\in\{1,\dots,r\}$, also thanks to the upper bound in (2.20). Thus, from the definition of $Z(f,g)$, it follows that $Z(f,g)$ divides $R(f,g)$.

Given two matrices $\boldsymbol{A}$ and $\boldsymbol{B}$ over $\mathbb{K}$, the roots of the characteristic polynomial of $\boldsymbol{A}\otimes\boldsymbol{B}$ are all the products of a root of the characteristic polynomial of $\boldsymbol{A}$ and a root of the characteristic polynomial of $\boldsymbol{B}$, counted with their multiplicities [69, p. 27]. Equation (2.26) says that $R(f,g)$ is the monic polynomial having as roots all the products of a root of f and a root of g, counted with their multiplicities. Thus it follows that $R(f,g)$ is the characteristic polynomial of $\boldsymbol{C}(f)\otimes\boldsymbol{C}(g)$. □

2.8 Rational functions

Let $\mathbb{K}[[x]]$ be the ring of *formal power series* in the variable x, that is, the set of infinite series of the form $\sum_{n=0}^{\infty} a_n x^n$ ($a_n \in \mathbb{K}$) with addition and multiplication defined in the natural way, without concern for convergence. An element of $\mathbb{K}[[x]]$ is a *rational function* if it can be written as the ratio of two polynomials. The *generating function* of a sequence $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ is the formal power series $\sum_{n=0}^{\infty} u_n x^n$.

Linear recurrences and rational functions are intimately connected. Indeed, the next two theorems show that a sequence in $\mathbb{K}^{\mathbb{N}}$ is a linear recurrence if and only if its generating function is a rational function. Recall that f^* denotes the reciprocal polynomial of a given nonzero polynomial $f \in \mathbb{K}[x]$.

Theorem 2.47. *Let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$, let $U(x) := \sum_{n=0}^{\infty} u_n x^n$ be the generating function of $\boldsymbol{u}$, and let $f(x) := -\sum_{i=0}^{k} a_i x^{k-i}$ ($a_i \in \mathbb{K}$), with $a_0 := -1$. If $\boldsymbol{u}$ is a linear recurrence, then $U(x)$ is a rational function. More precisely, if $\boldsymbol{u} \in \mathcal{L}(f)$ then*

$$U(x) = \frac{g(x)}{f^*(x)}, \tag{2.27}$$

where

$$g(x) := -\sum_{j=0}^{k-1} \left(\sum_{i=0}^{j} a_i u_{j-i} \right) x^j \tag{2.28}$$

Conversely, if $g \in \mathbb{K}[x]$ is a polynomial such that (2.27) holds, and $g = 0$ or $\deg(g) < k$, then $\boldsymbol{u} \in \mathcal{L}(f)$ and g is given by (2.28).

Proof. For the sake of notation, put $u_n := 0$ for every integer $n < 0$. Thus

$$f^*(x)U(x) = \left(-\sum_{i=0}^{k} a_i x^i \right) \left(\sum_{n=0}^{\infty} u_n x^n \right) = -\sum_{j=0}^{\infty} \left(\sum_{i=0}^{k} a_i u_{j-i} \right) x^j. \tag{2.29}$$

Suppose that $\boldsymbol{u} \in \mathcal{L}(f)$. Hence $\sum_{i=0}^{k} a_i u_{j-i} = 0$ for every integer $j \geq k$. Therefore, from (2.29) it follows that

$$f^*(x)U(x) = -\sum_{j=0}^{k-1} \left(\sum_{i=0}^{k} a_i u_{j-i} \right) x^j = -\sum_{j=0}^{k-1} \left(\sum_{i=0}^{j} a_i u_{j-i} \right) x^j = g(x),$$

and (2.27) follows.

Suppose that $g \in \mathbb{K}[x]$ is a polynomial such that (2.27) holds, and $g = 0$ or $\deg(g) < k$. Thus (2.29) implies that $\sum_{i=0}^{k} a_i u_{j-i} = 0$ for every integer $j \geq k$, which in turn implies that $\boldsymbol{u} \in \mathcal{L}(f)$. At this point, that g is given by (2.28) follows from the part of Theorem 2.47 proved in the previous paragraph. □

Theorem 2.48. *Let $U(x)$ be a formal power series that is also a rational function. Then there exist $f, g \in \mathbb{K}[x]$, such that f is monic, $g = 0$ or $\deg(g) < \deg(f)$, and $U(x) = g(x)/f^*(x)$.*

Proof. If $U(x) = 0$ then the claim is obvious. Hence, assume that $U(x) \neq 0$. Since $U(x)$ is a rational function, there exist $g, h \in \mathbb{K}[x]$, with $g, h \neq 0$, such that $U(x) = g(x)/h(x)$. Moreover, since $U(x)$ is a formal power series, the function $U(x)$ is defined at $x = 0$. Consequently, after eventually factoring out a multiple of a power of x from both g and h, assume that $h(0) = 1$. Thus write $h(x) = \sum_{i=0}^{k} h_i x^i$ ($h_i \in \mathbb{K}$) with $h_0 = 1$ and $h_k \neq 0$. Let $d := \deg(g)$ and $f(x) := \sum_{i=0}^{k+d+1} h_i x^{k+d+1-i}$, where $h_i := 0$ if $i > k$. Then f is monic, $\deg(f) = k + d + 1 > \deg(g)$, and $f^*(x) = h(x)$. Hence $U(x) = g(x)/f^*(x)$, where f is monic and $\deg(g) < \deg(f)$, as desired. □

Example 2.8 (Generating function of Fibonacci numbers)**.** From Theorem 2.47 it follows that the generating function of the sequence of Fibonacci numbers is

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

Example 2.9 (Generating function of Chebyshev polynomials)**.** From Theorem 2.47 it follows that the generating function of the sequence of Chebyshev polynomials is

$$\sum_{n=0}^{\infty} T_n(y) x^n = \frac{1 - xy}{1 - 2xy + x^2}.$$

A first consequence of Theorem 2.47 is a representation of each linear recurrence in terms of the partial fraction decomposition of its generating function.

Theorem 2.49. *Let $f(x) = \prod_{i=1}^{s} (x - \alpha_i)^{k_i}$, where $\alpha_1, \ldots, \alpha_s \in \mathbb{K}^*$ are pairwise distinct and $k_1, \ldots, k_s$ are positive integers, and let $\boldsymbol{u} \in \mathcal{L}(f)$. Then*

$$u_n = \sum_{i=1}^{s} \sum_{j=0}^{k_i - 1} c_{i,j} \binom{n+j}{j} \alpha_i^n \tag{2.30}$$

for every integer $n \geq 0$, where the coefficients $c_{i,j}$ belong to $\mathbb{K}$ and are uniquely determined by the partial fraction decomposition

$$\frac{g(x)}{f^*(x)} = \sum_{i=1}^{s} \sum_{j=0}^{k_i - 1} \frac{c_{i,j}}{(1 - \alpha_i x)^{j+1}} \tag{2.31}$$

where $g(x)$ is given by (2.28).

Proof. Note that the identity of formal power series

$$\frac{1}{(1-x)^{j+1}} = \sum_{n=0}^{\infty} \binom{n+j}{j} x^n \tag{2.32}$$

holds for each integer $j \geq 0$. (This is a special case of the binomial series. Alternatively, to prove (2.32) proceed by induction on j; and to prove the inductive step take the formal derivative of both sides of (2.32).)

From Theorem 2.47, (2.31), and (2.32) it follows that

$$\sum_{n=0}^{\infty} u_n x^n = \frac{g(x)}{f^*(x)} = \sum_{i=1}^{s} \sum_{j=0}^{k_i-1} \frac{c_{i,j}}{(1-\alpha_i x)^{j+1}} = \sum_{n=0}^{\infty} \sum_{i=1}^{s} \sum_{j=0}^{k_i-1} c_{i,j} \binom{n+j}{j} \alpha_i^n x^n. \tag{2.33}$$

Therefore (2.30) follows by equating the coefficients of x^n in the left- and right-hand side of (2.33). □

Remark 2.50. Every representation of the form (2.30) can be converted into a power-sum representation of the form (2.4), and vice versa, by employing the identities

$$\binom{n+j}{j} = \sum_{i=0}^{j} \binom{j}{i}\binom{n}{i} \quad \text{and} \quad \binom{n}{j} = \sum_{i=0}^{j} (-1)^{i+j} \binom{j}{i}\binom{n+i}{i},$$

which hold for all integers $n, j \geq 0$. These identities are related to the *Pascal matrix* and its inverse, that is, the matrices

$$\left(\binom{i}{j}\right)_{0 \leq i,j \leq n} \quad \text{and} \quad \left((-1)^{i+j}\binom{i}{j}\right)_{0 \leq i,j \leq n};$$

and more generally to the *binomial transform* of a sequence. See the article by Call and Velleman [29] and the book by Mező [131, Section 2.3].

Remark 2.51. Here a sketch of yet another way to prove Theorem 2.14 (cf. Remark 2.27). From Theorem 2.47, for every linear recurrence $\boldsymbol{u}$ the generating function $U(x)$ of $\boldsymbol{u}$ is a rational function. From the existence of the partial fraction decomposition of $U(x)$, and employing Theorem 2.49, it follows that $\boldsymbol{u}$ can be written in the form (2.30). In turn, by Remark 2.50, this representation can be converted into the power-sum representation (2.4).

Remark 2.52. Theorem 2.47 provides a method to determine the minimal polynomial of a linear recurrence from the initial values and the characteristic polynomial. First, using Theorem 2.47, write the generating function $U(x)$ of the linear recurrence $\boldsymbol{u}$. Second, reduce the rational function $U(x)$ to the lowest terms. Then, the denominator of $U(x)$ is the reciprocal of the minimal polynomial of $\boldsymbol{u}$.

From Theorem 2.47 it follows an explicit (although unwieldy) formula for the nth term of a linear recurrence in terms of the coefficients of the characteristic polynomial.

Theorem 2.53. *Let $f(x) := -\sum_{i=0}^{k} a_i x^{k-i}$ $(a_i \in \mathbb{K})$, with $a_0 := -1$, and let $\boldsymbol{u} \in \mathcal{L}(f)$. Then, for every integer $n \geq 0$,*

$$u_n = -\sum \left(\sum_{i=0}^{j} a_i u_{j-i}\right) \binom{j_1 + \cdots + j_k}{j_1 \cdots j_k} a_1^{j_1} \cdots a_k^{j_k}, \tag{2.34}$$

where the outer sum runs over all integers $j, j_1, \ldots, j_k \geq 0$ such that $j + \sum_{i=1}^{k} i j_i = n$ and $j < k$. Here $\binom{j_1+\cdots+j_k}{j_1 \cdots j_k}$ denotes a multinomial coefficient.

Proof. From the formula for the geometric series and from the multinomial theorem, it follows that

$$\begin{aligned}\frac{1}{f^*(x)} &= \frac{1}{1-\sum_{i=1}^{k} a_i x^i} = \sum_{j=0}^{\infty}\left(\sum_{i=1}^{k} a_i x^i\right)^j \\ &= \sum_{j_1,\dots,j_k\geq 0} \binom{j_1+\cdots+j_k}{j_1\cdots j_k} a_1^{j_1}\cdots a_k^{j_k}\, x^{\sum_{i=1}^{k} i j_i}. \end{aligned} \tag{2.35}$$

Hence, from Theorem 2.47 and (2.35) it follows that

$$\begin{aligned}\sum_{n=0}^{\infty} u_n x^n &= -\sum_{j=0}^{k-1}\left(\sum_{i=0}^{j} a_i u_{j-i}\right) x^j \cdot \frac{1}{f^*(x)} \\ &= -\sum_{j=0}^{k-1}\sum_{j_1,\dots,j_k\geq 0}\left(\sum_{i=0}^{j} a_i u_{j-i}\right)\binom{j_1+\cdots+j_k}{j_1\cdots j_k} a_1^{j_1}\cdots a_k^{j_k}\, x^{j+\sum_{i=1}^{k} i j_i}, \end{aligned} \tag{2.36}$$

and (2.34) follows by equating the coefficients of the corresponding powers of x in the left- and right-hand side of (2.36). □

Given two sequence $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$, their *convolution* $\boldsymbol{u} * \boldsymbol{v}$ is defined as the sequence in $\mathbb{K}^{\mathbb{N}}$ such that

$$(\boldsymbol{u} * \boldsymbol{v})_n := \sum_{j=0}^{n} u_{n-j} v_j,$$

for every integer $n \geq 0$.

The following theorem shows that for linear recurrences the convolution is a more natural operation than the termwise multiplication.

Theorem 2.54. *Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be two linear recurrences over $\mathbb{K}$ with characteristic polynomials f and g, respectively. Then $\boldsymbol{u} * \boldsymbol{v}$ is a linear recurrence with characteristic polynomial fg.*

Proof. Let $U(x) := \sum_{n=0}^{\infty} u_n x^n$ and $V(x) := \sum_{n=0}^{\infty} v_n x^n$ be the generating functions of $\boldsymbol{u}$ and $\boldsymbol{v}$, respectively. Theorem 2.47 says that $U(x) = r(x)/f^*(x)$ and $V(x) = s(x)/g^*(x)$ for some $r, s \in \mathbb{K}[x]$ with $r = 0$ or $\deg(r) < \deg(f)$, and $s = 0$ or $\deg(s) < \deg(g)$. Thus

$$\sum_{n=0}^{\infty} (\boldsymbol{u} * \boldsymbol{v})_n\, x^n = \sum_{n=0}^{\infty}\sum_{m=0}^{n} u_m v_{n-m} x^n = U(x)V(x) = \frac{r(x)s(x)}{f^*(x)g^*(x)} = \frac{g(x)s(x)}{(f(x)g(x))^*}. \tag{2.37}$$

Hence, from (2.37) and Theorem 2.47, it follows that $\boldsymbol{u} * \boldsymbol{v}$ is a linear recurrence having characteristic polynomial fg. □

Given two formal power series $U(x) = \sum_{n=0}^{\infty} u_n x^n$ and $V(x) = \sum_{n=0}^{\infty} v_n x^n$ in $\mathbb{K}[[x]]$, their *Hadamard product* is defined as $(U \odot V)(x) := \sum_{n=0}^{\infty} u_n v_n x^n$.

Theorem 2.55. *If U and V are rational functions in $\mathbb{K}[[x]]$, then $U \odot V$ is a rational function.*

Proof. The claim follows at once from Theorem 2.34 and Theorem 2.47. □

Note that the connection between linear recurrences and rational functions given by Theorem 2.47 significantly benefits the study of both subjects. Indeed, on the one hand, from simple manipulations of rational functions it is possible to prove nontrivial results about linear recurrences (Theorem 2.54). On the other hand, from relatively simple properties of linear recurrences it is possible to prove nontrivial results about rational functions (Theorem 2.55).

2.9 Proving identities

Finding and proving identities involving linear recurrences is an old but still very active area of research. For instance, the journal "Fibonacci Quarterly" [25], founded in 1962, is mostly devoted to identities involving Fibonacci numbers and other linear recurrences.

While finding beautiful identities remains an art—once an identity is found, it is often possible to prove it by employing systematic methods.

This section is devoted to *algebraic identities*, that is, identities involving finitely many products and sums of linear recurrences. There are essentially three systematic methods to prove such identities: by induction, by algebraic manipulations, and "by cases." Departing from the style of the previous sections, instead of giving a formal presentation of these methods, this section shows how to apply each of them to prove a specific identity.

Throughout this section, let $a_1, a_2 \in \mathbb{K}$ with $a_2 \neq 0$, let $f(x) := x^2 - a_1x - a_2$, and let $\boldsymbol{u} \in \mathcal{L}(f)$. For the sake of example, the goal is to prove identity

$$u_{n+1}^2 - u_n u_{n+2} = (-a_2)^n (u_1^2 - u_0 u_2), \tag{2.38}$$

for every integer $n \geq 0$.

2.9.1 By induction

This is the conceptually easier method, but often the more tiresome. It simply consists of proceeding by induction on a suitable base and applying the linear recurrence relation (1.1) when needed.

First, prove that (2.38) holds for $n = 0$. This is obvious, since

$$u_1^2 - u_0 u_2 = (-a_2)^0 (u_1^2 - u_0 u_2)$$

Thus (2.38) holds for $n = 0$.

Assuming that (2.38) holds for an integer $n \geq 0$, prove that it holds also for $n+1$. Some computation yields that

$$\begin{aligned} u_{n+2}^2 - u_{n+1}u_{n+3} &= u_{n+2}^2 - u_{n+1}(a_1u_{n+2} + a_2u_{n+1}) = u_{n+2}^2 - a_1u_{n+1}u_{n+2} - a_2u_{n+1}^2 \\ &= (u_{n+2} - a_1u_{n+1})u_{n+2} - a_2u_{n+1}^2 = a_2u_nu_{n+2} - a_2u_{n+1}^2 \\ &= (-a_2)(u_{n+1}^2 - u_nu_{n+2}) = (-a_2)^{n+1}(u_1^2 - u_0u_2) \end{aligned}$$

thanks to the relations $u_{n+3} = a_1u_{n+2} + a_2u_{n+1}$ and $a_2u_n = u_{n+2} - a_1u_{n+1}$, which are due to (1.1), and the inductive hypothesis. Thus (2.38) holds for $n+1$. Therefore, it follows by induction that (2.38) is true for every integer $n \geq 0$.

2.9.2 By algebra

Another method consists in writing each linear recurrence as its power-sum representation and then checking the identity by performing algebraic manipulations.

For the sake of simplicity, assume that $\mathrm{char}(\mathbb{K}) = 0$. Note that, without loss of generality, it can be assumed that f has distinct roots. Indeed, first assume that a_1, a_2 are formal variables and work in $\mathbb{Q}(a_1, a_2)$ instead of $\mathbb{K}$. In this way, the roots of f are distinct by construction. Once the identity is proved in $\mathbb{Q}(a_1, a_2)$, pick $a_1, a_2 \in \mathbb{K}$, and the identity remains true in $\mathbb{K}$ regardless of whether f has distinct roots.

Let $\mathbb{L}$ be the splitting field of f, and let $\alpha_1, \alpha_2 \in \mathbb{L}$ be the two distinct roots of f. Then, by Corollary 2.16, there exist $c_1, c_2 \in \mathbb{L}$ such that

$$u_n = c_1\alpha_1^n + c_2\alpha_2^n,$$

for every integer $n \geq 0$. (Example 2.2 provides explicit formulas for c_1 and c_2 in terms of α_1, α_2 and u_0, u_1, but this is not necessary here.) Moreover

$$a_1 = \alpha_1 + \alpha_2, \quad a_2 = -\alpha_1\alpha_2, \quad u_0 = c_1 + c_2, \quad u_1 = c_1\alpha_1 + c_2\alpha_2. \tag{2.39}$$

Let $n \geq 0$ be an integer. On the one hand,

$$\begin{aligned} u_{n+1}^2 - u_nu_{n+2} &= (c_1\alpha_1^{n+1} + c_2\alpha_2^{n+1})^2 - (c_1\alpha_1^n + c_2\alpha_2^n)(c_1\alpha_1^{n+2} + c_2\alpha_2^{n+2}) \\ &= c_1^2\alpha_1^{2n+2} + 2c_1c_2\alpha_1^{n+1}\alpha_2^{n+1} + c_2^2\alpha_2^{2n+2} \\ &\qquad - (c_1^2\alpha_1^{2n+2} + c_1c_2\alpha_1^{n+2}\alpha_2^n + c_1c_2\alpha_1^n\alpha_2^{n+2} + c_2^2\alpha_2^{2n+2}) \\ &= 2c_1c_2\alpha_1^{n+1}\alpha_2^{n+1} - c_1c_2\alpha_1^{n+2}\alpha_2^n - c_1c_2\alpha_1^n\alpha_2^{n+2}. \end{aligned} \tag{2.40}$$

On the other hand,

$$\begin{aligned} (-a_2)^n(u_1^2 - u_0u_2) &= (\alpha_1\alpha_2)^n\big((c_1\alpha_1 + c_2\alpha_2)^2 - (c_1 + c_2)(c_1\alpha_1^2 + c_2\alpha_2^2)\big) \\ &= (\alpha_1\alpha_2)^n\big((c_1^2\alpha_1^2 + 2c_1c_2\alpha_1\alpha_2 + c_2^2\alpha_2^2) - (c_1^2\alpha_1^2 + c_1c_2\alpha_1^2 + c_1c_2\alpha_2^2 + c_2^2\alpha_2^2)\big) \\ &= (\alpha_1\alpha_2)^n\big(2c_1c_2\alpha_1\alpha_2 - c_1c_2\alpha_1^2 - c_1c_2\alpha_2^2\big) \\ &= 2c_1c_2\alpha_1^{n+1}\alpha_2^{n+1} - c_1c_2\alpha_1^{n+2}\alpha_2^n - c_1c_2\alpha_1^n\alpha_2^{n+2}. \end{aligned} \tag{2.41}$$

Therefore, the identity (2.38) follows from (2.40) and (2.41).

The computations in (2.40) and (2.41) might seem tedious, but in reality they can be performed easily and quickly by employing a software for symbolic computation [165]. Moreover, there is no need to explicitly compute $c_1, c_2, \alpha_1, \alpha_2$, but it suffices to employ the relations (2.39) or, in other words, work in the quotient ring $\mathbb{K}[x]/(f)$.

2.9.3 "By cases"

Algebraic identities involving linear recurrences can be proved by checking that they are true for a sufficiently large number of cases. This method stems from the obvious consideration that if a linear recurrence of order at most k has its first k terms equal to zero, then the linear recurrence is identically zero. Hence, the strategy to prove an identity is the following. First, upper bound the order of the appropriate linear recurrence by a constant k. Then, check that the identity is true for the first k cases.

Rewrite (2.38) as

$$u_{n+1}^2 - u_n u_{n+2} - (-a_2)^n (u_1^2 - u_0 u_2) = 0 \tag{2.42}$$

for every integer $n \geq 0$. Let $\boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$ be the sequence having the nth term equal to the left-hand side of (2.42). Since $\boldsymbol{u} \in \mathcal{L}(f)$, it follows that $\boldsymbol{u}$ has order at most 2. Moreover, the linear recurrences $(u_{n+1}) = x\boldsymbol{u}$ and $(u_{n+2}) = x^2\boldsymbol{u}$ belong to $\mathcal{L}(f)$ (Theorem 2.7), and so they have order at most 2. Hence, by Theorem 2.34, each of the linear recurrences $(u_{n+2}u_n)$ and (u_{n+1}^2) has order at most 4. The linear recurrence $(-a_2)^n(u_1^2 - u_0u_2)$ is already written as a generalized power sum having the single root $-a_2$, thus it has order at most 1. Therefore, the sequence $\boldsymbol{v}$ is the sum of three linear recurrences of orders at most 4, 4, and 1, respectively. Corollary 2.6 implies that $\boldsymbol{v}$ is a linear recurrence of order at most 9. At this point, a quick computation shows that $v_n = 0$ for $n = 0, 1, \ldots, 8$. Therefore $\boldsymbol{v} = \boldsymbol{0}$. This proves the identity (2.38).

Note that, despite the systematic methods presented in this section, clever ideas can lead to surprisingly short and nice proofs. For instance, from Theorem 2.22(ii) it follows that

$$\begin{pmatrix} u_{n+1} & u_n \\ u_{n+2} & u_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ a_2 & a_1 \end{pmatrix}^n \begin{pmatrix} u_1 & u_0 \\ u_2 & u_1 \end{pmatrix} \tag{2.43}$$

for every integer $n \geq 0$. Taking the determinants of both sides of (2.43), and using the fact that the determinant is multiplicative, yields the identity (2.38).

2.10 Hankel transform

This section is devoted to an important characterization of linear recurrences in terms of a sequence of determinants. For every $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ and every positive integer k, let

$$\boldsymbol{H}_k(\boldsymbol{u}) := (u_{i+j})_{0 \leq i,j < k} = \begin{pmatrix} u_0 & u_1 & \cdots & u_{k-1} \\ u_1 & u_2 & \cdots & u_k \\ \vdots & \vdots & \ddots & \vdots \\ u_{k-1} & u_k & \cdots & u_{2k-2} \end{pmatrix} \in \mathbb{K}^{k \times k}$$

be a *Hankel matrix* and let $H_k(\boldsymbol{u}) := \det\big(\boldsymbol{H}_k(\boldsymbol{u})\big)$ be its *Hankel determinant*. Put also $H_0(\boldsymbol{u}) := 1$, which makes sense if $\boldsymbol{H}_0(\boldsymbol{u})$ is the empty matrix, whose determinant is equal to 1. The sequence $\big(H_k(\boldsymbol{u})\big)_{k \in \mathbb{N}}$ is the *Hankel transform* of $\boldsymbol{u}$.

The next theorem states that a sequence is a linear recurrence if and only if its Hankel transform is ultimately equal to zero.

Theorem 2.56. *Let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ and let $k \geq 0$ be an integer. Then $\boldsymbol{u}$ is a linear recurrence of order k if and only if $H_k(\boldsymbol{u}) \neq 0$ and $H_h(\boldsymbol{u}) = 0$ for every integer $h > k$.*

In such a case, if $k > 0$ then the minimal polynomial of $\boldsymbol{u}$ is equal to $x^k - \sum_{i=1}^{k} a_i x^{k-i}$, where $a_1, \ldots, a_k \in \mathbb{K}$ are given by

$$(a_k \ \cdots \ a_1)^{\intercal} = \boldsymbol{H}_k(\boldsymbol{u})^{-1}(u_k \ \cdots \ u_{2k})^{\intercal}. \tag{2.44}$$

The proof of Theorem 2.56 requires two lemmas. For brevity, put $\boldsymbol{H}_k := \boldsymbol{H}_k(\boldsymbol{u})$, $H_k := H_k(\boldsymbol{u})$, $\boldsymbol{H}_k^{(n)} := \boldsymbol{H}_k(x^n\boldsymbol{u})$, and $H_k^{(n)} := H_k(x^n\boldsymbol{u})$, for every $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ and for all integers $k, n \geq 0$.

Lemma 2.57. *Let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ and let $k > 0$ and $n \geq 0$ be integers. If $H_k^{(n)} = H_{k+1}^{(n)} = 0$ then $H_k^{(n+1)} = 0$.*

Proof. First, note that

$$\boldsymbol{H}_{k+1}^{(n)} = \left(\begin{array}{|ccc:c|}\hline u_n & u_{n+1} & \cdots & u_{n+k-1} & u_{n+k} \\ \hdashline u_{n+1} & u_{n+2} & \cdots & u_{n+k} & u_{n+k+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ u_{n+k-1} & u_{n+k} & \cdots & u_{n+2k-2} & u_{n+2k-1} \\ \hdashline u_{n+k} & u_{n+k+1} & \cdots & u_{n+2k-1} & u_{n+2k} \\ \hdashline \end{array}\right), \tag{2.45}$$

where the matrix in the continuous rectangle is equal to $\boldsymbol{H}_k^{(n)}$ and the two matrices in the dashed rectangles are both equal to $\boldsymbol{H}_k^{(n+1)}$.

Suppose that $H_k^{(n)} = H_{k+1}^{(n)} = 0$. If the first k columns of $\boldsymbol{H}_{k+1}^{(n)}$ are linearly dependent then, since the left-most dashed rectangle in (2.45) is equal to $\boldsymbol{H}_k^{(n+1)}$, it follows that also the first k columns of $\boldsymbol{H}_k^{(n+1)}$ are linearly dependent. Hence $H_k^{(n+1)} = 0$, as desired.

If instead the first k columns of $\boldsymbol{H}_{k+1}^{(n)}$ are linearly independent, then $H_{k+1}^{(n)} = 0$ implies that the last column of $\boldsymbol{H}_{k+1}^{(n)}$ is a linear combination of the previous k columns. Hence, since the continuous and the right-most dashed rectangles in (2.45) are equal to $\boldsymbol{H}_k^{(n)}$ and $\boldsymbol{H}_k^{(n+1)}$, respectively, it follows that the last column of $\boldsymbol{H}_k^{(n+1)}$ is a linear combination of the columns of $\boldsymbol{H}_k^{(n)}$. In fact, again looking at the continuous and the right-most dashed rectangles in (2.45), it follows that each column of $\boldsymbol{H}_k^{(n+1)}$ is a linear combination of the columns of $\boldsymbol{H}_k^{(n)}$. Moreover, since $H_k^{(n)} = 0$, the columns of $\boldsymbol{H}_k^{(n)}$ generate a subspace of dimension less than k. Therefore $H_k^{(n+1)} = 0$, as desired. □

Lemma 2.58. *Let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$, and suppose that there exist integers $k, n_0 \geq 0$ such that $H_{k+1}^{(n)} = 0$ for every integer $n \geq n_0$. Then $\boldsymbol{u}$ is a linear recurrence.*

Proof. If $k = 0$ then $u_n = H_1^{(n)} = 0$ for every integer $n \geq n_0$. Hence $\boldsymbol{u}$ is a linear recurrence with characteristic polynomial x^{n_0}. Assume that $k > 0$.

Without loss of generality, assume that k is the minimal integer such that there exists an integer $n_1 \geq 0$ for which $H_{k+1}^{(n)} = 0$ for all integers $n \geq n_1$.

Suppose that there exists an integer $n_1 \geq n_0$ such that $H_k^{(n_1)} = 0$. From Lemma 2.57 and the fact that $H_{k+1}^{(n)} = 0$ for every integer $n \geq n_0$, it follows that $H_k^{(n)} = 0$ for each integer $n \geq n_1$, which contradicts the minimality of k. Hence $H_k^{(n)} \neq 0$ for each integer $n \geq n_0$.

Pick an integer $n \geq n_0$. Since $H_k^{(n)} \neq 0$, the columns of $\boldsymbol{H}_k^{(n)}$ are linearly independent. Hence, also the first k columns of $\boldsymbol{H}_{k+1}^{(n)}$ are linearly independent. Thus, from $H_{k+1}^{(n)} = 0$ it follows that the last column of $\boldsymbol{H}_{k+1}^{(n)}$ is a linear combination of the previous k columns.

Let V be the subspace of $\mathbb{K}^{(k+1)\times 1}$ generated by the first k columns of $\boldsymbol{H}_{k+1}^{(n_0)}$. From the previous paragraph, reasoning by induction on n, it follows easily that $(u_{n+k} \ \cdots \ u_{n+2k})^\intercal$ belongs to V for every integer $n \geq n_0$.

Since $\dim(V) = k$, there exists a nonzero vector $(c_0 \ \cdots \ c_k) \in \mathbb{K}^{1\times k}$ such that

$$(c_0 \ \cdots \ c_k)\boldsymbol{v}^\intercal = 0 \quad \text{ if and only if } \quad \boldsymbol{v} \in V,$$

for every $\boldsymbol{v} \in \mathbb{K}^{k\times 1}$. In particular

$$(c_0 \ \cdots \ c_k)(u_{n+k} \ \cdots \ u_{n+2k})^\intercal = 0, \tag{2.46}$$

for every integer $n \geq n_0$. From (2.46) it follows easily that $\boldsymbol{u}$ is a linear recurrence. □

The setup for the proof of Theorem 2.56 is complete.

Proof of Theorem 2.56. First, suppose that $\boldsymbol{u}$ is a linear recurrence of order k. If $k = 0$ then $\boldsymbol{u} = \boldsymbol{0}$, $H_0 := 1$, and $H_h = \det(\boldsymbol{0}) = 0$ for every integer $h > 0$, as desired. Assume that $k > 0$. From Theorem 2.3 it follows that the sequences $x^0\boldsymbol{u}, \cdots, x^{k-1}\boldsymbol{u}$ are linearly independent. Then Theorem 2.1(iii) implies that the columns of $\boldsymbol{H}_k$ are linearly independent and consequently $H_k \neq 0$. Let $x^k - \sum_{i=1}^{k} a_i x^{k-i}$ $(a_i \in \mathbb{K})$ be the minimal polynomial of $\boldsymbol{u}$. Hence

$$u_{h-1} = \sum_{i=1}^{k} a_i u_{h-i-1}, \tag{2.47}$$

for every integer $h > k$. This means that, for every integer $h > k$, the last $k+1$ columns of $\boldsymbol{H}_h$ are linearly dependent, and so $H_h = 0$. Furthermore, from (2.47) with $h = k+1$, it follows that

$$\boldsymbol{H}_k(a_k \ \cdots \ a_1)^\intercal = (u_k \ \cdots \ u_{2k})^\intercal.$$

and (2.44) follows. This proves one implication.

Suppose that $H_k \neq 0$ and $H_h = 0$ for every integer $h > k$. Claim: $\boldsymbol{u}$ is a linear recurrence of order k. From Lemma 2.57, it follows by induction that $H_k^{(n)} = 0$ for all integers $h > k$ and $n \geq 0$. In particular, $H_{k+1}^{(n)} = 0$ for every integer $n \geq 0$. Thus Lemma 2.58 implies that $\boldsymbol{u}$ is a linear recurrence. The first part of the proof showed that if $\boldsymbol{u}$ is a linear recurrence

of order t then $H_t \neq 0$ and $H_h = 0$ for every integer $h > t$. Since $H_k \neq 0$ and $H_h = 0$ for every integer $h > k$, it follows easily that $\boldsymbol{u}$ is a linear recurrence of order k. □

The following result provides a useful relation between the Hankel matrix and the companion matrix of a linear recurrence.

Theorem 2.59. *Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$, let $k > 0$ be the order of $\boldsymbol{u}$, and let f be the minimal polynomial of $\boldsymbol{u}$. Then*

$$\boldsymbol{H}_k^{(n)}(\boldsymbol{u}) = \boldsymbol{C}(f)^n \boldsymbol{H}_k(\boldsymbol{u}),$$

for every integer $n \geq 0$.

Proof. The claim follows from the definition of the Hankel matrix and Theorem 2.22(ii). □

2.11 Berlekamp–Massey algorithm

For every finite sequence $\boldsymbol{s} = s_0, \ldots, s_{n-1}$ of n elements in $\mathbb{K}$, the *linear complexity* $\ell(\boldsymbol{s})$ of $\boldsymbol{s}$ is the minimal integer $k \geq 0$ such that there exists a linear recurrence $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ of order k satisfying $u_j = s_j$ for every $j \in \{0, \ldots, n-1\}$. In other words, the linear complexity $\ell(\boldsymbol{s})$ is the minimal integer $k \geq 0$ such that there exist coefficients $c_0, \ldots, c_k \in \mathbb{K}$, with $c_0 = 1$, satisfying $\sum_{i=0}^{k} c_i s_{j-i} = 0$ for every integer j such that $k \leq j < n$. Note that the linear complexity is well defined: pick $\boldsymbol{u}$ as an arbitrary linear recurrence with initial values $s_0, \ldots, s_{n-1}$ or, equivalently, take $k = n$ so that there are no integers j such that $k \leq j < n$ and the condition is satisfied vacuously. This also implies that $\ell(\boldsymbol{s}) \leq n$.

Input: $N \in \mathbb{Z}^+$ and $\boldsymbol{s} = s_0, \ldots, s_{N-1} \in \mathbb{K}$.
Output: the linear complexity k of $\boldsymbol{s}$, and $c_0, \ldots, c_k \in \mathbb{K}$ such that $c_0 = 1$ and $\sum_{i=0}^{k} c_i s_{j-i} = 0$ for $j = k, \ldots, N-1$.

```
1 : g ← 1, k ← 0, m ← −1, g_pre ← 1, d_pre ← 1
2 : for n = 0, ..., N − 1 do
3 :   d ← Σ_{i=0}^{k} c_i s_{n−i}   // where g(x) = Σ_{i=0}^{k} c_i x^i.
4 :   if d ≠ 0 then
5 :     g_tmp ← g, g ← g − d d_pre^{−1} x^{n−m} g_pre
6 :     if 2k ≤ n then
7 :       k ← n + 1 − k, m ← n, g_pre ← g_tmp, d_pre ← d
8 :     end if
9 :   end if
10 : end for
11 : return k, c_0, ..., c_k   // where g(x) = Σ_{i=0}^{k} c_i x^i.
```

Algorithm 2.1: Berlekamp–Massey algorithm.

n	k	m	g	g_{pre}	d	d_{pre}
0	0	-1	1	1		1
1	1	0	$x+1$	1	1	1
2	1	0	$x+1$	1	0	1
3	2	2	x^2+x+1	$x+1$	1	1
4	2	2	x^2+x+1	$x+1$	0	1
5	3	4	x^3+x+1	x^2+x+1	1	1
6	3	4	x^2+1	x^2+x+1	1	1
7	3	4	x^2+1	x^2+x+1	0	1
8	3	4	x^2+1	x^2+x+1	0	1
9	3	4	x^2+1	x^2+x+1	0	1
	3	4	x^2+1	x^2+x+1	0	1

Table 2.1: Steps of the Berlekamp–Massey algorithm (Algorithm 2.1) when applied to the sequence $\boldsymbol{s} = 1,1,0,1,0,1,0,1,0,1$ over $\mathbb{F}_2$. The output is $k = 3$, $c_0 = 1$, $c_1 = 0$, $c_2 = 1$, and $c_3 = 0$.

Given a finite sequence $\boldsymbol{s}$, the linear complexity of $\boldsymbol{s}$, as well as the coefficients of the shortest linear recurrence relation satisfied by $\boldsymbol{s}$, can be efficiently computed by the celebrated *Berlekamp–Massey algorithm*, which is given as Algorithm 2.1. See Table 2.1 for an example.

Theorem 2.60. *The Berlekamp–Massey algorithm (Algorithm 2.1) is correct.*

The rest of this section is devoted to the proof of Theorem 2.60. Hereafter, let $\boldsymbol{s} \in \mathbb{K}^{\mathbb{N}}$ be fixed, and let ℓ_n be the linear complexity of $s_0, \ldots, s_{n-1}$, for every positive integer n. If $\boldsymbol{s} \neq \boldsymbol{0}$ then let $n_0 \geq 0$ be minimal integer such that $s_{n_0} \neq 0$.

Lemma 2.61. *The following properties hold.*

(i) *The sequence $(\ell_n)_{n\in\mathbb{N}}$ is monotone nondecreasing.*

(ii) *If $\boldsymbol{s} = \boldsymbol{0}$ then $\ell_n = 0$ for every integer $n \geq 0$.*

(iii) *If $\boldsymbol{s} \neq \boldsymbol{0}$ then $\ell_n = 0$ for every nonnegative integer $n \leq n_0$, while $\ell_{n_0+1} = n_0 + 1$.*

Proof. Claim (i) is a straightforward consequence of the definition of linear complexity. Since the zero sequence $\boldsymbol{0} \in \mathbb{K}^{\mathbb{N}}$ is a linear recurrence of order 0, it follows that every finite zero sequence has linear complexity equal to 0. This gives (ii) and the part on $n \leq n_0$ of (iii). For the part on $\ell_{n_0+1} = n_0+1$ of (iii), it suffices to consider that it cannot be $\ell_{n_0+1} < n_0+1$ since the term s_{n_0}, which is nonzero, cannot be a linear combination of $s_0, \ldots, s_{n_0-1}$, which are all equal to zero. Thus $\ell_{n_0+1} = n_0 + 1$, since $\ell_n \leq n$ for every positive integer n. □

Lemma 2.62. *Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$ of order ℓ_n. Suppose that $u_j = s_j$ for every nonnegative integer $j < n$, while $u_n \neq s_n$. Then $\ell_{n+1} \geq \max\{\ell_n, n+1-\ell_n\}$.*

Proof. From Lemma 2.61(i) it follows that $\ell_{n+1} \geq \ell_n$. Thus it suffices to prove that

$$\ell_{n+1} \geq n + 1 - \ell_n. \tag{2.48}$$

Let $\boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$ be a linear recurrence of order ℓ_{n+1} such that $v_j = s_j$ for every nonnegative integer $j \leq n$. Moreover, let $\boldsymbol{w} := \boldsymbol{u} - \boldsymbol{v}$, and let $m_{\boldsymbol{u}}, m_{\boldsymbol{v}}, m_{\boldsymbol{w}}$ be the minimal polynomials of $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w}$, respectively. Note that $\deg(m_{\boldsymbol{u}}) = \ell_n$ and $\deg(m_{\boldsymbol{v}}) = \ell_{n+1}$. Since $w_j = 0$ for every nonnegative integer $j < n$, while $w_n \neq 0$, it follows that $\deg(m_{\boldsymbol{w}}) \geq n + 1$. Furthermore, from Theorem 2.5(i) and (iii) it follows that $m_{\boldsymbol{w}}$ divides $m_{\boldsymbol{u}} m_{\boldsymbol{w}}$. Therefore

$$n + 1 \leq \deg(m_{\boldsymbol{w}}) \leq \deg(m_{\boldsymbol{u}}) + \deg(m_{\boldsymbol{v}}) = \ell_n + \ell_{n+1},$$

which implies (2.48), as desired. □

Define a sequence of nonnegative integers $(k_n)_{n\in\mathbb{N}}$ and a sequence $(g_n)_{n\in\mathbb{N}}$ of polynomials in $\mathbb{K}[x]$ as follows. For every integer $n \geq 0$, write $g_n(x) = \sum_{i=0}^{k_n} c_{n,i} x^i$, where $c_{n,i} \in \mathbb{K}$ and $c_{n,0} := 1$ (note that $\deg(g_n) \leq k_n$), and let $d_n := \sum_{i=0}^{k_n} c_{n,i} s_{n-i}$. Put also $g_{-1}(x) := 1$, $k_{-1} := -1$, and $d_{-1} := 1$. Then $(k_n)_{n\in\mathbb{N}}$ and $(g_n)_{n\in\mathbb{N}}$ are recursively defined by

$$k_0 := 0, \quad k_{n+1} := \begin{cases} k_n & \text{if } d_n = 0; \\ \max\{k_n, n + 1 - k_n\} & \text{if } d_n \neq 0; \end{cases} \tag{2.49}$$

and

$$g_0(x) := 1, \quad g_{n+1}(x) := \begin{cases} g_n(x) & \text{if } d_n = 0; \\ g_n(x) - d_n d_m^{-1} x^{n-m} g_m(x) & \text{if } d_n \neq 0; \end{cases} \tag{2.50}$$

for each integer $n \geq 0$, where $m = m(n)$ is the maximal integer such that $-1 \leq m < n$ and $k_m < k_n$.

It is not obvious that $(g_n)_{n\in\mathbb{N}}$ is well defined. The next lemma clarifies this.

Lemma 2.63. *The sequence $(g_n)_{n\in\mathbb{N}}$ is well defined. Moreover*

(i) if $\boldsymbol{s} = \boldsymbol{0}$ then $k_n = 0$ and $g_n(x) = 1$ for every integer $n \geq 0$;

(ii) if $\boldsymbol{s} \neq \boldsymbol{0}$ then $k_n = 0$ and $g_n(x) = 1$ for every nonnegative integer $n \leq n_0$, while $k_{n_0+1} = n_0 + 1$ and $g_{n_0+1} = 1 - s_{n_0} x^{n_0+1}$;

(iii) if $\boldsymbol{s} \neq \boldsymbol{0}$ then $m \geq 0$ and $k_{n+1} = \max\{k_n, n - m + k_m\}$ for every integer $n \geq n_0 + 1$ such that $d_{m(n)} \neq 0$.

Proof. Proving that $(g_n)_{n\in\mathbb{N}}$ is well defined requires to show that, for every integer $n \geq 0$,

(a) $m = m(n)$ exists;

(b) if $d_n \neq 0$ then $d_m \neq 0$, so that the inverse d_m^{-1} exists;

(c) $\deg(g_n) \leq k_n$, so that writing $g_n(x) = \sum_{i=0}^{k_n} c_{n,i} x^i$ makes sense.

First, from (2.49) it follows easily that (k_j) is a monotone nondecreasing sequence of nonnegative integers. Thus, since $k_{-1} := -1$, the existence of m is guaranteed. This proves (a).

Let $n \geq 0$ be an integer such that $d_n \neq 0$. If $m(n) = -1$ then $d_m = d_{-1} := 1 \neq 0$. Suppose that $m \geq 0$. Since m is maximal such that $m < n$ and $k_m < k_n$, and since (k_j) is monotone nondecreasing, it follows that $k_m < k_{m+1}$. Thus (2.49) implies that $d_m \neq 0$. This proves (b).

If $\boldsymbol{s} = \mathbf{0}$ then (i) follows at once from (2.49) and (2.50), and in turn it implies (c). Hereafter, suppose that $\boldsymbol{s} \neq \mathbf{0}$, and recall that n_0 is the minimal nonnegative integer such that $s_{n_0} \neq 0$. Hence $d_n = 0$ for every nonnegative integer $n < n_0$, while $d_{n_0} = s_{n_0} \neq 0$. Thus (ii) follows easily from (2.49) and (2.50), also noticing that $m(n_0) = -1$.

Let $n \geq n_0 + 1$ be an integer such that $d_{m(n)} \neq 0$. By (ii) and the monotonicity of the sequence (k_j), it follows that $k_n \geq k_{n_0+1} = n_0 + 1 > k_0$, so that $m \geq 0$. Since m is maximal such that $m < n$ and $k_m < k_n$, and since (k_j) is monotone nondecreasing, it follows that $k_m < k_{m+1} = k_n$. Moreover, from $m \geq 0$, $k_m < k_{m+1}$, and (2.49), it follows that $k_{m+1} = m + 1 - k_m$. Hence $k_n = k_{m+1} = m + 1 - k_m$ and, consequently, from (2.49) it follows that

$$k_{n+1} = \max\{k_n, n + 1 - k_n\} = \max\{k_n, n - m + k_n\}.$$

This proves (iii).

It remains to prove (c). From (ii) it follows that (c) is true for every nonnegative integer $n \leq n_0 + 1$. The proof of (c) is completed by using strong induction on n. Let $n' \geq n_0 + 1$ and suppose that (c) is true for all nonnegative integers $n \leq n'$. The goal is to prove that (c) is true for $n = n' + 1$. Let $m = m(n')$.

If $d_m = 0$ then (2.49) and (2.50) imply that $k_{n'+1} = k_{n'}$ and $g_{n'+1}(x) = g_{n'}(x)$. Hence, since by the inductive hypothesis $\deg(g_{n'}) \leq k_{n'}$, it follows that $\deg(g_{n'+1}) \leq k_{n'+1}$.

If $d_m \neq 0$ then (2.50) gives that

$$g_{n'+1}(x) = g_{n'}(x) - d_{n'} d_m^{-1} x^{n'-m} g_m(x).$$

Hence, from the inductive hypothesis and (iii), it follows that

$$\deg(g_{n'+1}) \leq \max\{\deg(g_{n'}), n' - m + \deg(g_m)\} \leq \max\{k_{n'}, n' - m + k_m\} = k_{n'+1},$$

as desired. The proof of (c) is complete. □

Lemma 2.64. *For every positive integer n, the following statements are true.*

(i) $k_n = \ell_n$.

(ii) $\sum_{i=0}^{k_n} c_{n,i} s_{j-i} = 0$ *for every integer j such that* $k_n \leq j < n$.

Proof. If $\boldsymbol{s} = \mathbf{0}$ then the claims follow easily from Lemma 2.61(ii) and Lemma 2.63(i). Hence, assume that $\boldsymbol{s} \neq \mathbf{0}$. Then, from Lemma 2.61(iii) and Lemma 2.63(ii), it follows that (i) and (ii) are true for every positive integer $n \leq n_0 + 1$ (note that (ii) is true for $n = n_0 + 1$ simply because there are no integers j such that $k_n \leq j < n$). It remains to prove that (i) and (ii) are true also for every integer $n > n_0 + 1$.

Proceed by strong induction on n. Let $n' \geq n_0 + 1$ be an integer. Suppose that (i) and (ii) are true for every positive integer $n \leq n'$. The goal is to prove that they are true also for $n = n' + 1$.

Suppose that $d_{n'} = 0$. Hence $\sum_{i=0}^{k_{n'}} c_{n',i} s_{n'-i} = 0$. Moreover, from (2.49) and (2.50), it follows that $k_{n'+1} = k_{n'}$ and $g_{n'+1}(x) = g_{n'}(x)$. Therefore, also employing the inductive hypothesis, it follows that

$$\sum_{i=0}^{k_{n'+1}} c_{n'+1,i} s_{j-i} = \sum_{i=0}^{k_{n'}} c_{n',i} s_{j-i} = 0,$$

for every integer j with $k_{n'+1} \leq j < n'+1$. This proves (ii) for $n = n'+1$, and it shows that

$$\ell_{n'+1} \leq k_{n'+1} = k_{n'} = \ell_{n'}, \tag{2.51}$$

also thanks to the inductive hypothesis. Then Lemma 2.61(i) and (2.51) give that $\ell_{n'+1} = \ell_{n'}$ and $k_{n'+1} = \ell_{n'+1}$. Thus (i) is true for $n = n' + 1$.

Suppose that $d_{n'} \neq 0$. Let $m = m(n')$. Lemma 2.63(iii) implies that $m \geq 0$ and

$$k_{n'+1} = \max\{k_{n'}, n' - m + k_m\}. \tag{2.52}$$

Furthermore, from (2.50) it follows that

$$g_{n'+1}(x) = g_{n'}(x) - d_{n'} d_m^{-1} x^{n'-m} g_m(x). \tag{2.53}$$

Let j be an integer such that $k_{n'+1} \leq j < n' + 1$. Note that (2.52) implies that

$$k_{n'} \leq j \leq n' \quad \text{and} \quad k_m \leq j - n' + m \leq m. \tag{2.54}$$

Hence, from (2.53) and (2.54), it follows that

$$\begin{aligned} \sum_{i=0}^{k_{n'+1}} c_{n'+1,i} s_{j-i} &= \sum_{i=0}^{k_{n'}} c_{n',i} s_{j-i} - d_{n'} d_m^{-1} \sum_{i=n'-m}^{k_m+n'-m} c_{n',i-n'+m} s_{j-i} \\ &= \sum_{i=0}^{k_{n'}} c_{n',i} s_{j-i} - d_{n'} d_m^{-1} \sum_{i=0}^{k_m} c_{n',i} s_{j-n'+m-i}. \end{aligned} \tag{2.55}$$

On the one hand, if $j < n'$ then, from the inductive hypothesis, which can be applied because $m \geq 0$ and (2.54) holds, it follows that the last two sums in (2.55) are both equal to 0. On the other hand, if $j = n'$ then the right-hand side of (2.55) is equal to

$$d_{n'} - d_{n'} d_m^{-1} d_m = 0.$$

Therefore (ii) is true for $n = n' + 1$.

It remains to prove that that (i) holds for $n = n'+1$. Let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ be the linear recurrence with initial values $s_0, \ldots, s_{k_{n'}-1}$ and satisfying $u_j = \sum_{i=0}^{k_{n'}} c_{n',i} u_{j-i}$ for every integer $j \geq k_{n'}$.

Then, by the inductive hypothesis and the fact that $d_{n'} \neq 0$, it follows that $u_j = s_j$ for every nonnegative integer $j < n'$, while $u_{n'} \neq s_{n'}$. Moreover, the linear recurrence $\boldsymbol{u}$ has order at most $k_{n'}$. In fact, since $k_{n'} = \ell_{n'}$ by the inductive hypothesis, the order of $\boldsymbol{u}$ is equal to $\ell_{n'}$. Therefore, Lemma 2.62 gives that

$$\max\{\ell_{n'}, n' + 1 - \ell_{n'}\} \leq \ell_{n'+1}. \tag{2.56}$$

Furthermore, from (2.49) and the inductive hypothesis, it follows that

$$k_{n'+1} = \max\{k_{n'}, n' + 1 - k_{n'}\} = \max\{\ell_{n'}, n' + 1 - \ell_{n'}\}. \tag{2.57}$$

On the one hand, putting together (2.56) and (2.57) it follows that $k_{n'+1} \leq \ell_{n'+1}$. On the other hand, since (ii) is true for $n = n' + 1$, it follows that $k_{n'+1} \geq \ell_{n'+1}$. Thus $k_{n'+1} = \ell_{n'+1}$ and (i) is true for $n = n' + 1$, as desired. □

Now to the proof of the correctness of the Berlekamp–Massey algorithm.

Proof of Theorem 2.60. It suffices to notice that Algorithm 2.1 computes the sequences (k_n) and (g_n) via (2.49) and (2.50). More precisely, at the nth iteration of the loop, $g = g_n$, $k = k_n$, $m = m(n)$, $d = d_n$, $g_{\text{pre}} = g_m$, and $d_{\text{pre}} = d_m$. Note also that the equality $k_{n+1} = \max\{k_n, n+1-k_n\}$ is equivalent to $k_{n+1} = n+1-k_n$ if $2k_n \leq n+1$, and $k_{n+1} = k_n$ otherwise. □

2.12 Bibliographical notes

Sections 2.2–2.4, 2.8 and 2.10

The results of these sections are well known and most of them appear, for instance, in the book by Lidl and Niederreiter [115, Chapter 6]. There they are proved assuming that $\mathbb{K}$ is a finite field, but almost all the proofs work as they are even if $\mathbb{K}$ is an arbitrary field. For the theory of linear recurrences over rings and modules, see the monograph by Kurakin, Kuzmin, Mikhalev, and Nechaev [109]; and for the case of linear recurrences with indeterminate coefficients and values in a module, see the books by Gatto [61] and Gatto–Salehyan [62, Chapter 2].

The characterization of linear recurrences in terms of the Hankel transform is usually attributed to Kronecker [106, p. 27]. The Hankel transform has amazing connections with generating functions, continued fractions, orthogonal polynomials, and lattice paths. See the surveys on advanced determinant calculus by Krattenthaler [104, Section 2.7], [105, Section 5.4].

Section 2.5 "Vandermonde matrix"

The results of this section are all standard results of linear algebra. However, locating them in the literature, stated and proved for fields of arbitrary characteristic, is quite challenging. For instance, a proof of Theorem 2.25 for $\mathbb{K} = \mathbb{C}$ can be found in the book by Dym [52, Theorem 8.3].

Sections 2.6 and 2.9

The content of these sections belongs to the folklore. The reader interested in automatic methods to prove identities in discrete mathematics must read the book by Petkovšek, Wilf, and Zeilberger [144].

Section 2.7 "Product of linear recurrences"

This section is based on the papers by Zierler–Mills [203], and Göttfert–Niederreiter [67]. More precisely, Theorem 2.36 was first proved in 1973 by Zierler and Mills [203]. They defined $Z(f, g)$ as the least common multiple of certain polynomials in $\mathbb{K}[x]$. On the one hand, this definition is convenient since it does not require to prove that $Z(f, g) \in \mathbb{K}[x]$. On the other hand, it makes some parts of the proof quite involved. In any case, their definition of $Z(f, g)$ is easily seen to be equivalent to the definition given in Section 2.7. In 1995 Göttfert and Niederreiter [67] provided a simpler proof of Theorem 2.36, using the same definition of $Z(f, g)$ given in Section 2.7. The exposition of Section 2.7 mostly follows the proof of Göttfert and Niederreiter, except that in some parts they employed rational functions instead of the results of Section 2.2. In their paper, Göttfert and Niederreiter also determine a polynomial $A(f, g)$ that divides the minimal polynomial of $\boldsymbol{uv}$, where $\boldsymbol{u}$ and $\boldsymbol{v}$ are linear recurrences with minimal polynomials f and g, respectively. Çakçak [35] (see also [36]) improved their result. Kauers and Zeilberger [92] provided an algorithm to decide

if a given polynomial is the Zierler–Mills polynomial of some polynomial pair. Cerruti and Vaccarino [37] proved a generalization of Theorem 2.46 that holds for linear recurrences over an arbitrary commutative ring.

Section 2.11 "Berlekamp–Massey algorithm"

Massey [128] invented the Berlekamp–Massey algorithm in 1969, after recognizing that an algorithm developed by Berlekamp [14] in 1967 for decoding BCH codes could be generalized to efficiently find the shortest linear recurrence relation satisfied by a finite sequence. Later, several authors [38, 47, 60, 133, 199] noticed that the Berlekamp–Massey algorithm can be interpreted as an application of the extended Euclidean algorithm to the computation of the *Padé approximant* of the generating function of a sequence. Section 2.11 is based on the original paper of Massey, but the proofs are more detailed. There are algorithms analogous to the Berlekamp–Massey algorithm that operate on linear recurrences over rings that are not fields. For example, the Reed–Sloane algorithm [157] works over the ring of integers modulo m.

2.13 Exercises

Exercise 2.1. Let $\boldsymbol{u}$ be the linear recurrence over $\mathbb{Q}$ with initial values $1, 2, -2, -34$ and characteristic polynomial $(x-1)(x-2)^2(x-3)$. Determine

(i) the minimal polynomial f of $\boldsymbol{u}$;

(ii) the companion matrix of f;

(iii) the power-sum representation of $\boldsymbol{u}$;

(iv) the generating function of $\boldsymbol{u}$.

Exercise 2.2. Let $\alpha \in \mathbb{F}_4$ be a root of $x^2+x+1 \in \mathbb{F}_2[x]$, and let $\boldsymbol{u}$ be the linear recurrence over $\mathbb{F}_4$ with initial values $1, \alpha, 0, 1+\alpha$ and characteristic polynomial $(x-1)(x-\alpha)^3$. Determine

(i) the minimal polynomial f of $\boldsymbol{u}$;

(ii) the companion matrix of f;

(iii) the power-sum representation of $\boldsymbol{u}$;

(iv) the generating function of $\boldsymbol{u}$.

Exercise 2.3. Implement the Berlekamp–Massey algorithm in your favorite programming language (over $\mathbb{Q}$ and over a finite field $\mathbb{F}_q$).

Exercise 2.4. For each of the following finite sequences $\boldsymbol{s}$ of length ℓ, compute the linear complexity k of $\boldsymbol{s}$, and find the coefficients $c_1, \ldots, c_k$ such that $s_j + \sum_{i=1}^{k} c_i s_{j-i} = 0$ for every integer j with $k \le j < \ell$.

(i) $\boldsymbol{s} = 3, 1, 1, 0, 8, 3, 10, 11, 29, 27$ over $\mathbb{Q}$.

(ii) $\boldsymbol{s} = 2, 1, 1, 0, 1, 2, 2, 0, 2, 1$ over $\mathbb{F}_3$.

(iii) $\boldsymbol{s} = 2, 2, 2, 1, 1, 3, 1, 2, 0, 4, 0, 3, 4$ over $\mathbb{F}_5$.

Exercise 2.5. Let $\boldsymbol{u}$ be the linear recurrence over $\mathbb{Q}$ with initial values $23, 69, 289, 1337$ and characteristic polynomial $(x-1)(x-2)(x-4)^2$, and let $\boldsymbol{v}$ be the linear recurrence over $\mathbb{Q}$ with initial values $3, 27, 87$ and characteristic polynomial $(x-1)(x-2)^2$. Determine the minimal polynomial of each of the following linear recurrences.

(i) The sum $\boldsymbol{u} + \boldsymbol{v}$.

(ii) The product $\boldsymbol{u}\boldsymbol{v}$.

(iii) The convolution $\boldsymbol{u} * \boldsymbol{v}$.

(iv) The reflection $\boldsymbol{u}^*$.

(v) The interleaved sequence $u_0, v_0, u_1, v_1, u_2, v_2, \ldots$

Exercise 2.6. Let $\mathbb{K}$ be a field of characteristic zero, let $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{K}^*$, and let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$ with initial values u_0, u_1, u_2 and characteristic polynomial $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$. Determine the power-sum expression of $\boldsymbol{u}$ in terms of u_0, u_1, u_2 and $\alpha_1, \alpha_2, \alpha_3$.

Exercise 2.7. Determine the Zierler–Mills polynomial $Z(f, g)$ for each of the following pairs of polynomials f, g.

(i) $f = x^2 + 2x + 4$ and $g = x^3 + 2$ over $\mathbb{Q}$.

(ii) $f = x^3 + x + 1$ and $g = x^3 + x^2 + 1$ over $\mathbb{F}_2$.

(iii) $f = (x^2 + x + 2)^3$ and $g = (x-1)^5(x-2)^7$ over $\mathbb{F}_3$.

Exercise 2.8. Let $\boldsymbol{u}, \boldsymbol{v}$ be linear recurrences over $\mathbb{K}$ of order at most $k > 0$, and let $\boldsymbol{u} \bullet \boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$ be the sequence defined by

$$(\boldsymbol{u} \bullet \boldsymbol{v})_n = \sum_{i=0}^{k-1} u_{n+i} v_{n+i}$$

for each integer $n \geq 0$. Prove that $\boldsymbol{u} \bullet \boldsymbol{v}$ is a linear recurrence of order at most k.

Exercise 2.9. Given two sequences $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$, their *binomial convolution* is the sequence $\boldsymbol{u} \star \boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$ defined by

$$(\boldsymbol{u} \star \boldsymbol{v})_n = \sum_{j=0}^{n} \binom{n}{j} u_{n-j} v_j,$$

for every integer $n \geq 0$. Prove that if $\boldsymbol{u}$ and $\boldsymbol{v}$ are linear recurrences then $\boldsymbol{u} \star \boldsymbol{v}$ is a linear recurrence.
(This result is due to Kurakin [108] and has applications in the theory of Hopf algebras.)

Exercise 2.10. Let $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$ be sequences with $v_0 = 0$. The *composition* of $\boldsymbol{u}$ and $\boldsymbol{v}$ is the sequence $\boldsymbol{u} \circ \boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$ defined by

$$(\boldsymbol{u} \circ \boldsymbol{v})_n = \sum_{n_1, \ldots, n_k} u_k v_{n_1} \cdots v_{n_k}$$

for every integer $n \geq 0$, where the sum runs over all the integers $k \geq 0$ and $n_1, \ldots, n_k \geq 1$ such that $\sum_{i=0}^{k} n_i = k$. Prove that if $\boldsymbol{u}$ and $\boldsymbol{v}$ are linear recurrences then $\boldsymbol{u} \circ \boldsymbol{v}$ is a linear recurrence.

Exercise 2.11. Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$ of order $k > 0$. Prove that there exist coefficients $a_{i,j} \in \mathbb{K}$, depending only on $u_0, \ldots, u_{2k-1}$, such that the *addition formula*

$$u_{m+n} = \sum_{i=0}^{k-1} \sum_{j=0}^{k-1} a_{i,j} u_{m+i} u_{n+j}$$

holds for all integers $m, n \geq 0$.

Exercise 2.12. Let $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{Q}^{\mathbb{N}}$ be defined by

$$\sum_{n=0}^{\infty} a_n x^n = \frac{9x^2 + 53x + 1}{x^3 - 82x^2 - 82x + 1},$$
$$\sum_{n=0}^{\infty} b_n x^n = \frac{-12x^2 - 26x + 2}{x^3 - 82x^2 - 82x + 1},$$
$$\sum_{n=0}^{\infty} c_n x^n = \frac{-10x^2 + 8x + 2}{x^3 - 82x^2 - 82x + 1}.$$

Prove that $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \mathbb{Z}^{\mathbb{N}}$ and $a_n^3 + b_n^3 = c_n^3 + (-1)^n$ for every integer $n \geq 0$.
(This amazing identity is due to Ramanujan [156, p. 341] (cf. [80]).)

Exercise 2.13. Let $u_0, u_1, a_1, a_2 \in \mathbb{K}$, and let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ be the sequence defined by

$$u_n := \begin{vmatrix} u_0 & -1 & & & & & \\ u_1 & 0 & 1 & & & & \\ & -a_2 & a_1 & 1 & & & \\ & & -a_2 & a_1 & 1 & & \\ & & & \ddots & \ddots & \ddots & \\ & & & & -a_2 & a_1 & 1 \end{vmatrix} \tag{2.58}$$

for each integer $n \geq 0$, where the matrix appearing in the determinant of (2.58) is tridiagonal of size $(n+1) \times (n+1)$.

(i) Prove that $\boldsymbol{u}$ is a linear recurrence of order at most 2.

(ii) Generalize to linear recurrences of arbitrary order.

Exercise 2.14. Let $a_1, \ldots, a_k \in \mathbb{C}$. Proceed as follows to determine all the solutions $f : \mathbb{R} \to \mathbb{C}$ to the kth-order homogeneous linear differential equation with constant coefficients

$$f^{(k)} = a_1 f^{(k-1)} + \cdots + a_{k-1} f' + a_k f,$$

where $f^{(n)}$ is the nth derivative of f.

(i) Prove that $\left(f^{(n)}(0)\right)_{n \in \mathbb{N}}$ is a linear recurrence.

(ii) Write $f^{(n)}(0)$ as a generalized power sum.

(iii) Substitute the expression for $f^{(n)}(0)$ in the Taylor series for $f(x)$ around $x = 0$.

Exercise 2.15. Complete the proof sketched in Remark 2.27.

Exercise 2.16. Complete the proof sketched in Remark 2.51.

Exercise 2.17. Prove that

$$F_{n+1} = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n-j}{j}$$

for every integer $n \geq 0$, where F_n is the nth Fibonacci number.

Exercise 2.18. Let (T_n) be the sequence of Chebyshev polynomials (Example 1.14). Prove that the sequence of derivatives (T_n') is a linear recurrence and find its minimal polynomial.

Chapter 3

Periodic Sequences

3.1 Introduction

This short chapter studies ultimately periodic sequences from the point of view of the theory of linear recurrences. The prerequisites are the same as those for Chapter 1.

The first result of this chapter characterizes ultimately periodic sequences over a field as linear recurrences whose minimal polynomials satisfy a specific condition (Section 3.2).

The second result consists of three formulas for the *least period* of an ultimately periodic sequence; and the last result provides the relation between the least period of ultimately periodic sequences with minimal polynomial f and ultimately periodic sequences with characteristic polynomial f (Section 3.3).

3.2 Periodic sequences are linear recurrences

Let $\mathcal{A}$ be a nonempty set. A sequence $\boldsymbol{s} \in \mathcal{A}^{\mathbb{N}}$ is *ultimately periodic* if there exist integers $n_0 \geq 0$ and $t > 0$ such that $s_{n+t} = s_n$ for every integer $n \geq n_0$. In such a case, the integer n_0 is a *preperiod* of $\boldsymbol{s}$ and the integer t is a *period* of $\boldsymbol{s}$. The minimal preperiod of $\boldsymbol{s}$ is the *least preperiod* of $\boldsymbol{s}$ and the minimal period of $\boldsymbol{s}$ is the *least period* of $\boldsymbol{s}$. It is not difficult to prove that, if $\boldsymbol{s}$ is an ultimately periodic sequence, then the least period of $\boldsymbol{s}$ divides every period of $\boldsymbol{s}$. Sometimes, the terms *preperiod* and *period* refer to the finite sequences $s_0, \ldots, s_{n_0-1}$ (which is empty if $n_0 = 0$) and $s_{n_0}, \ldots, s_{n_0+t-1}$, where n_0 and t are the least preperiod and the least period of an ultimately periodic sequence $\boldsymbol{s}$, respectively. An ultimately periodic sequence having least preperiod equal to zero is *(purely) periodic*.

For the rest of this chapter, let $\mathbb{K}$ be a field. Ultimately periodic sequences over $\mathbb{K}$ are in fact a special family of linear recurrences.

Theorem 3.1. *Let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$. Then $\boldsymbol{u}$ is an ultimately periodic sequence if and only if $\boldsymbol{u}$ is a linear recurrence over $\mathbb{K}$ and there exist integers $n_0 \geq 0$ and $t > 0$ such that the minimal polynomial $f(x)$ of $\boldsymbol{u}$ divides $x^{n_0}(x^t - 1)$. In such a case, the sequence $\boldsymbol{u}$ has preperiod n_0 and period t; and $\boldsymbol{u}$ is periodic if and only if $f(0) \neq 0$.*

Proof. Suppose that $\boldsymbol{u}$ is ultimately periodic. Hence, there exist integers $n_0 \geq 0$ and $t > 0$ such that $u_{n+t} = u_n$ for every integer $n \geq n_0$. This means that $x^{n_0}(x^t - 1)\boldsymbol{u} = \boldsymbol{0}$, so that $\boldsymbol{u}$ is a linear recurrence and, by Theorem 2.2, its minimal polynomial divides $x^{n_0}(x^t - 1)$.

Vice versa, if $\boldsymbol{u}$ is a linear recurrence whose minimal polynomial divides $x^{n_0}(x^t - 1)$ for some integers $n_0 \geq 0$ and $t > 0$, then $x^{n_0}(x^t - 1)\boldsymbol{u} = \boldsymbol{0}$, which means that $u_{n+t} = u_n$ for every integer $n \geq n_0$. Hence, the linear recurrence $\boldsymbol{u}$ is ultimately periodic with preperiod n_0 and period t.

Suppose that $\boldsymbol{u}$ is an ultimately periodic sequence with least preperiod n_0 and least period t. From the first paragraph it follows that $\boldsymbol{u}$ is a linear recurrence. Let $f(x)$ be the minimal polynomial of $\boldsymbol{u}$. Again from the first paragraph, the minimal polynomial $f(x)$ divides $x^{n_0}(x^t - 1)$. If $\boldsymbol{u}$ is periodic, then $n_0 = 0$ and so $f(0) \neq 0$. If $f(0) \neq 0$ then it is possible to extend $\boldsymbol{u}$ backward to a sequence $\boldsymbol{u} \in \mathbb{K}^{\mathbb{Z}}$ that satisfies $u_{n+t} = u_n$ for every integer n. Thus $\boldsymbol{u}$ is periodic. □

In light of Theorem 3.1, if $\boldsymbol{u}$ is an ultimately periodic sequence over $\mathbb{K}$ then $\boldsymbol{u}$ is a linear recurrence over $\mathbb{K}$. Hence, it makes sense to speak of the minimal polynomial and the roots of $\boldsymbol{u}$, as well as any other property of linear recurrences. Hereafter, this occurs without referring to Theorem 3.1.

Corollary 3.2. *Let $\boldsymbol{u}$ be a nonzero periodic sequence over $\mathbb{K}$. Then the roots of $\boldsymbol{u}$ are roots of unity. Moreover, if $\operatorname{char}(\mathbb{K}) = 0$ then $\boldsymbol{u}$ is a simple linear recurrence.*

Proof. Let $f(x)$ be the minimal polynomial of $\boldsymbol{u}$. From Theorem 3.1, there exists a positive integer t such that $f(x)$ divides $x^t - 1$. Hence, the roots of $f(x)$ are roots of unity. If $\operatorname{char}(\mathbb{K}) = 0$ then the polynomial $x^t - 1$ has no multiple root. Hence, the roots of $f(x)$ are simple and so $\boldsymbol{u}$ is a simple linear recurrence. □

3.3 Formulas for the least period

Let $f \in \mathbb{K}[x]$ be a polynomial such that $f(0) \neq 0$. The *period* of f is the minimal positive integer t such that f divides $x^t - 1$, if such a positive integer exists. Equivalently, the period of f is the multiplicative order of x modulo f, if such a multiplicative order exists. Let $\operatorname{per}(f)$ denote the period of f.

The next theorem provides three formulas for the least period of a periodic sequence in terms of its minimal polynomial. Each formula can be more or less convenient depending on the context.

Theorem 3.3. *Let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ be a nonzero periodic sequence with minimal polynomial f (note that $\deg(f) > 0$ and $f(0) \neq 0$). Then the least period of $\boldsymbol{u}$ is equal to*

(i) the multiplicative order of $\boldsymbol{C}(f)$;

(ii) the period of f;

(iii)

$$\operatorname{lcm}\{\operatorname{ord}(\alpha_1),\dots,\operatorname{ord}(\alpha_s)\}\cdot\begin{cases}p^{\lfloor\log_p \max\{k_1,\dots,k_s\}\rfloor} & \text{if } p:=\operatorname{char}(\mathbb{K})>0;\\ 1 & \text{otherwise;}\end{cases}$$

where $\alpha_1,\dots,\alpha_s$ are the pairwise distinct roots of f (in the splitting field of f over $\mathbb{K}$) and $k_1,\dots,k_s$ are their respective multiplicities.

The proof of Theorem 3.3 needs a preliminary lemma.

Lemma 3.4. *Let $\alpha\in\mathbb{K}^*$, let $h>0$ and $n\geq 0$ be integers, and let $i,j\in\{1,\dots,h\}$. Then the entry of the ith row and jth column of the Jordan block $\boldsymbol{J}^n_{\alpha,h}$ is equal to $\big(\boldsymbol{\psi}^{(j-i)}(\alpha)\big)_n$.*

Proof. Lemma 2.17 says that

$$x\boldsymbol{\psi}^{(j)}=\alpha\boldsymbol{\psi}^{(j)}+\boldsymbol{\psi}^{(j-1)}. \tag{3.1}$$

From (3.1) it follows by induction on n that

$$x^n\boldsymbol{\psi}^{(j)}=\sum_{\ell=0}^{n}\binom{n}{\ell}\alpha^{n-\ell}\boldsymbol{\psi}^{(j-\ell)},$$

which in turn implies that

$$x^n\boldsymbol{\psi}^{(j)}=\sum_{\ell=0}^{n}\big(\boldsymbol{\psi}^{(\ell)}\big)_n\boldsymbol{\psi}^{(j-\ell)}. \tag{3.2}$$

Since $\boldsymbol{\psi}^{(\ell)}=\mathbf{0}$ for every negative integer ℓ, from (3.2) it follows that

$$x^n\boldsymbol{\psi}^{(j)}=\sum_{i=0}^{h}\big(\boldsymbol{\psi}^{(j-i)}\big)_n\boldsymbol{\psi}^{(i)} \tag{3.3}$$

The claim follows from (3.3) and Lemma 2.26. □

Proof of Theorem 3.3. Let $k:=\deg(f)$. The least period of $\boldsymbol{u}$ is the minimal positive integer t such that $u_{n+t}=u_n$ for every integer $n\geq 0$. By Theorem 2.59, this last condition is equivalent to $\boldsymbol{C}(f)^{n+t}\boldsymbol{H}_k(\boldsymbol{u})=\boldsymbol{C}(f)^n\boldsymbol{H}_k(\boldsymbol{u})$ for every integer $n\geq 0$. Since $f(0)\neq 0$ and k is the order of $\boldsymbol{u}$, from Theorem 2.22 and Theorem 2.56 it follows that $\boldsymbol{C}(f)$ and $\boldsymbol{H}_k(\boldsymbol{u})$ are both invertible. Hence t is the minimal positive integer such that $\boldsymbol{C}(f)^t=\boldsymbol{I}$. Consequently t is the multiplicative order of $\boldsymbol{C}(f)$. This proves (i).

The least period of $\boldsymbol{u}$ is the minimal positive integer t such that $(x^t-1)\boldsymbol{u}=\mathbf{0}$. By Theorem 2.2, this is equivalent to x^t-1 being divisible by the minimal polynomial f. Hence $t=\operatorname{per}(f)$. This proves (ii).

From Theorem 2.25, the matrices $\boldsymbol{C}(f)$ and $\boldsymbol{J}(f)$ are similar. Thus $\boldsymbol{C}(f)$ and $\boldsymbol{J}(f)$ have the same multiplicative order. From Lemma 3.4 the entry of the ith row and jth column of $\boldsymbol{J}^t_{\alpha_v,k_v}$ is equal to $\big(\boldsymbol{\psi}^{(j-i)}(\alpha_v)\big)_t$, for every positive integer t and each $v\in\{1,\dots,s\}$. Therefore, the multiplicative order of $\boldsymbol{J}(f)$ is the minimal positive integer t such that $\alpha_v^t=1$

and $\binom{t}{h} = 0$ in $\mathbb{K}$ for every $v \in \{1, \dots, s\}$, and $h \in \{1, \dots, k_v - 1\}$. Hence t must be a multiple of $\ell := \operatorname{lcm}\{\operatorname{ord}(\alpha_1), \dots, \operatorname{ord}(\alpha_s)\}$.

If $\operatorname{char}(\mathbb{K}) = 0$ then, since $k_1 = \cdots = k_s = 1$ (Corollary 3.2), the condition on the binomial coefficients is vacuously satisfied. Thus $t = \ell$.

If $p := \operatorname{char}(\mathbb{K}) > 0$ then, by Kummer's theorem (Theorem A.33), the condition on the binomial coefficients is equivalent to t being a multiple of $q := p^{\lfloor \log_p \max\{k_1, \dots, k_s\} \rfloor}$. Since the multiplicative order of each root is coprime to p, it follows that $t = q\ell$.

At this point, claims (iii) follows from (i). □

The following result is a consequence of Theorem 3.3.

Theorem 3.5. *Let $f \in \mathbb{K}[x]$ be a monic polynomial of positive degree. Then*

(i) all the periodic sequences with minimal polynomial f have the same least period t;

(ii) if $\boldsymbol{u}$ is a periodic sequence with characteristic polynomial f, then the least period of $\boldsymbol{u}$ divides t.

Proof. Claim (i) follows at once from Theorem 3.3, which says that the least period depends only on the minimal polynomial. If $\boldsymbol{u}$ is a periodic sequence with characteristic polynomial f, then Theorem 2.22(ii) and Theorem 3.3(i) imply that t is a period of $\boldsymbol{u}$. Hence, the least period of $\boldsymbol{u}$ divides t, and (ii) is proved. □

3.4 Bibliographical notes

The results of this chapter are well known and can be found (for the case of finite fields, but the proofs generalize naturally) in the book by Lidl and Niederreiter [115, Chapter 6].

3.5 Exercises

Exercise 3.1. Let $\boldsymbol{u}$ be a reversible linear recurrence over $\mathbb{K}$ and let f be the minimal polynomial of $\boldsymbol{u}$. Prove that if $\boldsymbol{u}$ is periodic then $f(0)$ is a root of unity. Then show that the converse implication is false.

Exercise 3.2. Prove that there exist no periodic sequence over $\mathbb{C}$ with characteristic polynomial $x^4 + 2x^3 + 2x^2 + 2x + 1$.

Exercise 3.3. Let k and t be positive integers. Prove that there exists a periodic sequence over $\mathbb{Q}$ of order k and least period t if and only if there exist positive integers $d_1 < \cdots < d_s$ such that $k = \varphi(d_1) + \cdots + \varphi(d_s)$ and $t = \operatorname{lcm}(d_1, \ldots, d_s)$.

Exercise 3.4. Let $\boldsymbol{u}, \boldsymbol{v}$ be periodic sequences over $\mathbb{K}$ with minimal polynomials f, g and least periods s, t, respectively. Prove that if f and g are coprime then the least period of $\boldsymbol{u} + \boldsymbol{v}$ is equal to $\operatorname{lcm}(s, t)$.

Chapter 4

Linear Recurrences over Finite Fields

4.1 Introduction

This chapter focuses on the study of linear recurrences over a finite field. The prerequisites are the same as those for Chapter 2.

The first topic of this chapter concerns the fact that, over a finite field, linear recurrences coincide with ultimately periodic sequences; and it is interesting to study their least period (Section 4.2).

The second topic of this chapter is an interlude on *primitive polynomials* and their basic properties, which are fundamental for the subsequent results (Section 4.3).

The third topic is the study of linear recurrences that achieve maximal periods, that is, *maximal-period sequences*. A key result is the characterization of maximal-period sequences as those having minimal polynomials that are primitive polynomials. Other results concern several properties of maximal-period sequences, such as the regularity of the distribution of their values (Section 4.4).

The fourth topic is an upper bound on a *character sum* involving the terms of a linear recurrence (Section 4.5), which is preliminary to the next topic.

The fifth topic of this chapter regards the distribution of the values of linear recurrences, including: estimates for the number of solutions to systems of equations involving linear recurrences, an upper bound on the number of zeros of a simple linear recurrence, and lower bounds on the number of distinct values taken by a linear recurrence (Section 4.6).

The last topic of this chapter is the generation of the terms of a linear recurrence over $\mathbb{F}_2$ via a *linear-feedback shift register* (Section 4.7).

Throughout this chapter, $\mathbb{F}_q$ is a finite field of q elements and characteristic p.

4.2 Periodicity

Over a finite field, linear recurrences coincide with ultimately periodic sequences.

Theorem 4.1. *Let $\boldsymbol{u} \in \mathbb{F}_q^{\mathbb{N}}$. Then $\boldsymbol{u}$ is a linear recurrence over $\mathbb{F}_q$ if and only if $\boldsymbol{u}$ is an ultimately periodic sequence. Furthermore, if $\boldsymbol{u}$ is a linear recurrence with minimal*

polynomial f, order $k > 0$, least preperiod n_0, and least period t, then $n_0 + t \leq q^k - 1$; and $\boldsymbol{u}$ is periodic if and only if $f(0) \neq 0$.

Proof. Suppose that $\boldsymbol{u}$ is a linear recurrence. If $\boldsymbol{u} = \mathbf{0}$ then it is clear that $\boldsymbol{u}$ is periodic. Assume that $\boldsymbol{u} \neq \mathbf{0}$ and let k be the order of $\boldsymbol{u}$. Hence $(u_n, \ldots, u_{n+k-1}) \in \mathbb{F}_q^k \setminus \{\mathbf{0}\}$ for every integer $n \geq 0$. Moreover, since $|\mathbb{F}_q^k \setminus \{\mathbf{0}\}| = q^k - 1$, the pigeonhole principle implies that there exist integers $n_0 \geq 0$ and $t > 0$ such that $n_0 + t \leq q^k - 1$ and

$$(u_{n_0}, \ldots, u_{n_0+k-1}) = (u_{n_0+t}, \ldots, u_{n_0+t+k-1}).$$

Thus it follows easily by induction on n that $u_{n+t} = u_n$ for every integer $n \geq n_0$. Hence $\boldsymbol{u}$ is an ultimately periodic sequence. Moreover, from Theorem 3.1 it follows that $\boldsymbol{u}$ is periodic if and only if $f(0) \neq 0$, where f is the minimal polynomial of $\boldsymbol{u}$.

Conversely, if $\boldsymbol{u}$ is an ultimately periodic sequence, then from Theorem 3.1 it follows that $\boldsymbol{u}$ is a linear recurrence. □

Remark 4.2. The statement and the proof of Theorem 4.1 generalize naturally to finite rings. Let $\mathcal{R}$ be a finite ring and let $\boldsymbol{u} \in \mathcal{R}^{\mathbb{N}}$. Then $\boldsymbol{u}$ is a linear recurrence over $\mathcal{R}$ if and only if $\boldsymbol{u}$ is an ultimately periodic sequence. Furthermore, if $\boldsymbol{u}$ is a linear recurrence with characteristic polynomial f of positive degree k, least preperiod n_0, and least period t, then $n_0 + t < |\mathcal{R}|^k$; and $\boldsymbol{u}$ is periodic if $f(0)$ is invertible.

Remark 4.3. From Theorem 3.3, if $\mathbb{K}$ is an arbitrary field and $\boldsymbol{u}$ is a nonzero periodic linear recurrence over $\mathbb{K}$ with minimal polynomial f, then the least period of $\boldsymbol{u}$ is equal to the multiplicative order of the companion matrix $\boldsymbol{C}(f)$ and also to the period of f. Note that if $f \in \mathbb{F}_q[x]$ is a nonconstant monic polynomial with $f(0) \neq 0$, then the multiplicative order of $\boldsymbol{C}(f)$ exists (since $\boldsymbol{C}(f)$ is an invertible matrix over $\mathbb{F}_q$) and the period of f exists (since x is an invertible element in the finite ring $\mathbb{F}_q[x]/(f)$), coherently with Theorem 4.1.

For every $f \in \mathbb{F}_q[x]$, let $\mathcal{L}(f) := \{\boldsymbol{u} \in \mathbb{F}_q^{\mathbb{N}} : f\boldsymbol{u} = \mathbf{0}\}$, and let $\mathcal{L}^*(f)$ be the set of all linear recurrences over $\mathbb{F}_q$ having minimal polynomial f.

The following theorem provides the number of linear recurrences having prescribed characteristic polynomial or prescribed minimal polynomial.

Theorem 4.4. *Let $f \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree k. Then*

(i) $|\mathcal{L}(f)| = q^k$;

(ii) $|\mathcal{L}^*(f)| = q^k \prod'_{g|f} \left(1 - q^{-\deg(g)}\right)$;

where the product is over all the irreducible factors g of f.

Proof. From Theorem 2.1(i) it follows that $\mathcal{L}(f)$ is a vector space over $\mathbb{F}_q$ of dimension k. This proves (i). Theorem 2.2 implies that $\boldsymbol{u} \in \mathcal{L}^*(f)$ if and only if $\boldsymbol{u} \in \mathcal{L}(f)$ and $\boldsymbol{u} \notin \mathcal{L}(f/g)$ for every irreducible polynomial g in $\mathbb{F}_q[x]$ that divides f. Hence, from the inclusion-exclusion principle and (i), it follows that

$$|\mathcal{L}^*(f)| = \sum_{g_1,\ldots,g_s} (-1)^s \left|\mathcal{L}\left(f(g_1 \cdots g_s)^{-1}\right)\right|$$

$$= \sum_{g_1,\dots,g_s} (-1)^s q^{k-\sum_{i=1}^s \deg(g_i)} = q^k \prod_{g\,|\,f}{}' \big(1 - q^{-\deg(g)}\big),$$

where the sums are over the unordered s-tuples (including the empty tuple) of pairwise distinct monic irreducible polynomials $g_1, \dots, g_s$ in $\mathbb{F}_q[x]$ such that $g_1 \cdots g_s$ divides f. This proves (ii). □

Remark 4.5. In Theorem 4.4(ii), the product $q^k \prod'_{g|f} \big(1 - q^{-\deg(g)}\big)$ is the function field analog of the Euler function and is equal to the number of monic polynomials in $\mathbb{F}_q[x]$ that are coprime to f and have degree less than $\deg(f)$. See, e.g., the book by Rosen [160, Proposition 1.7]. This is due to the fact that Theorem 4.4(ii) can be proved by employing Theorem 2.47 and showing that the linear recurrences in $\mathcal{L}^*(f)$ are exactly those with generating function of the form g/f^*, where g is a polynomial in $\mathbb{F}_q[x]$ having degree less than $\deg(f)$ and being coprime to f^*.

The next result provides the number of linear recurrences having prescribed characteristic polynomial and least period.

Theorem 4.6. *Let $f \in \mathbb{F}_q[x]$ be a monic polynomial of positive degree k such that $f(0) \neq 0$. Put $t := \mathrm{per}(f)$. Then*

(i) every sequence in $\mathcal{L}^*(f)$ has least period equal to t;

(ii) the least period of every sequence in $\mathcal{L}(f)$ divides t;

(iii) the number of sequences in $\mathcal{L}(f)$ having least period T, where T divides t, is equal to

$$\sum_{d\,|\,T} \mu(T/d)\, q^{\deg\left(\gcd(f,\, x^d - 1)\right)},$$

where μ is the Möbius function.

Proof. Claims (i) and (ii) follow at once from Theorem 3.3 and Theorem 3.5. It remains to prove claim (iii). Let T be a positive integer dividing t, let $\boldsymbol{u} \in \mathcal{L}(f)$ and let $m_{\boldsymbol{u}}$ be the minimal polynomial of $\boldsymbol{u}$. Then, by Theorem 2.2 and Theorem 3.3, the least period of $\boldsymbol{u}$ is equal to T if and only if $m_{\boldsymbol{u}}$ divides $\gcd(f, x^T - 1)$ but does not divide $\gcd\big(f, x^{T/s} - 1\big)$ for every prime factor s of T. Consequently, the sequence $\boldsymbol{u}$ has least period T if and only if $\boldsymbol{u} \in \mathcal{L}\big(\gcd(f, x^T - 1)\big)$ and $\boldsymbol{u} \notin \mathcal{L}\big(\gcd(f, x^{T/s} - 1)\big)$ for every prime factor s of T. Therefore, by the inclusion-exclusion principle and by Theorem 4.4(i), the number of sequences in $\mathcal{L}(f)$ having least period T is equal to

$$\sum_{d\,|\,T} \mu(d)\, \big|\mathcal{L}\big(\gcd(f,\, x^{T/d} - 1)\big)\big| = \sum_{d\,|\,T} \mu(d)\, q^{\deg\left(\gcd(f,\, x^{T/d} - 1)\right)} = \sum_{d\,|\,T} \mu(T/d)\, q^{\deg\left(\gcd(f,\, x^d - 1)\right)},$$

which proves (iii). □

4.3 Primitive polynomials

Let $f \in \mathbb{F}_q[x]$ be a polynomial of positive degree k. Then f is a *primitive polynomial* if f is the minimal polynomial over $\mathbb{F}_q$ of a primitive $(q^k - 1)$th root of unity.

Primitive polynomials are fundamental in the study of linear recurrences over $\mathbb{F}_q$ that achieve maximum period length (Section 4.4).

The following theorem provides some basic facts on primitive polynomials.

Theorem 4.7. *Let $f \in \mathbb{F}_q[x]$ be a polynomial of positive degree k. Then the following statements are equivalent.*

(i) f is a primitive polynomial.

(ii) $f(x) = \prod_{i=0}^{k-1}(x - \alpha^{q^i})$ where α is a primitive $(q^k - 1)$th root of unity.

(iii) f is monic, $f(0) \neq 0$, and $\operatorname{per}(f) = q^k - 1$.

Corollary 4.8. *For every positive integer k, there are exactly $\varphi(q^k - 1)/k$ primitive polynomials of degree k.*

The proofs of Theorem 4.7 and Corollary 4.8 require the following lemma.

Lemma 4.9. *Let $f, g \in \mathbb{F}_q[x]$ be nonconstant polynomials such that $f(0) \neq 0$ and $g(0) \neq 0$.*

(i) If f is irreducible, then $\operatorname{per}(f)$ divides $q^{\deg(f)} - 1$.

(ii) If f is irreducible and m is a positive integer, then $\operatorname{per}(f^m) = p^{\lceil \log_p m \rceil} \operatorname{per}(f)$.

(iii) If f and g are coprime, then $\operatorname{per}(fg) = \operatorname{lcm}\big(\operatorname{per}(f), \operatorname{per}(g)\big)$.

Proof. If f is irreducible and $k := \deg(f)$, then $\mathbb{F}_q[x]/(f)$ is a finite field of q^k elements. Hence, the multiplicative order of x modulo f divides $q^k - 1$. Thus claim (i) follows.

Suppose that f is irreducible and let m be a positive integer. Also, let $t := \operatorname{per}(f)$ and $\ell := \lceil \log_p m \rceil$. Note that t divides $\operatorname{per}(f^m)$, since f divides f^m. Moreover f^m divides $(x^t - 1)^{p^\ell} = x^{p^\ell t} - 1$, since f divides $x^t - 1$ and $p^\ell \geq m$. Thus $\operatorname{per}(f^m)$ divides $p^\ell t$. Hence $\operatorname{per}(f^m) = p^i t$ for some integer i such that $0 \leq i \leq \ell$. If $\ell = 0$, then claim (ii) follows. Suppose that $\ell > 0$. From claim (i) it follows that p does not divide t. Hence, the polynomial $x^t - 1$ has no multiple root. Consequently, the multiplicity of each root of $(x^t - 1)^{p^{\ell-1}}$ is equal to $p^{\ell-1}$. Thus, since $p^{\ell-1} < m$, the polynomial f^m cannot divide $(x^t - 1)^{p^{\ell-1}} = x^{p^{\ell-1}t} - 1$. It follows that $\operatorname{per}(f^m) = p^\ell t$, which is claim (ii).

Suppose that f and g are coprime. The Chinese remainder theorem implies that

$$\mathbb{F}_q[x]/(fg) \cong \big(\mathbb{F}_q[x]/(f)\big) \times \big(\mathbb{F}_q[x]/(g)\big).$$

Hence, the multiplicative order of x in $\mathbb{F}_q[x]/(fg)$ is the least common multiple of the multiplicative orders of x in $\mathbb{F}_q[x]/(f)$ and $\mathbb{F}_q[x]/(g)$. Claim (iii) follows. □

Proof of Theorem 4.7. Suppose that f is a primitive polynomial. Then f is the minimal polynomial over $\mathbb{F}_q$ of a primitive (q^k-1)th root of unity α. Consequently, the powers $\alpha^{q^0}, \ldots, \alpha^{q^{k-1}}$ are pairwise distinct roots of f. Since f is monic and has degree k, it follows that $f(x) = \prod_{i=0}^{k-1}(x - \alpha^{q^i})$. Thus (i) implies (ii).

Suppose that (ii) holds. Note that, by applying the Frobenius automorphism to f, it follows easily that indeed $f \in \mathbb{F}_q[x]$ and that f is irreducible over $\mathbb{F}_q$. Furthermore, the polynomial f is monic and $f(0) \neq 0$. Since the field $\mathbb{F}_q[x]/(f)$ is isomorphic to $\mathbb{F}_q(\alpha)$ via the isomorphism that sends x to α, the multiplicative order of x in $\mathbb{F}_q[x]/(f)$ is equal to the multiplicative order of α in $\mathbb{F}_q$, which in turn is equal to $q^k - 1$. So the period of f is equal to $q^k - 1$. Thus (ii) implies (iii).

Suppose that (iii) holds. Claim: f is irreducible over $\mathbb{F}_q$. Suppose that $f = g^m$ for some irreducible polynomial $g \in \mathbb{F}_q[x]$ and some integer $m \geq 2$. From Lemma 4.9(ii), it follows that

$$q^k - 1 = \operatorname{per}(f) = \operatorname{per}(g^m) = p^{\lceil \log_p m \rceil} \operatorname{per}(g),$$

which in turn implies that $\lceil \log_p m \rceil = 0$. Hence $m = 1$, which is a contradiction. Suppose that $f = gh$ for some coprime nonconstant polynomials $g, h \in \mathbb{F}_q[x]$. From Lemma 4.9(iii) and Lemma 4.9(i), it follows that

$$\begin{aligned} q^k - 1 &= \operatorname{per}(f) = \operatorname{lcm}\big(\operatorname{per}(g), \operatorname{per}(h)\big) \\ &\leq (q^{\deg(g)} - 1)(q^{\deg(h)} - 1) < q^{\deg(g)+\deg(h)} - 1 = q^k - 1, \end{aligned}$$

which is again a contradiction. Therefore, the polynomial f is irreducible, as claimed.

Let α be a root of f. Since the field $\mathbb{F}_q(\alpha)$ is isomorphic to $\mathbb{F}_q[x]/(f)$ via the isomorphism that sends α to x, the multiplicative order of α is equal to the multiplicative order of x in $\mathbb{F}_q[x]/(f)$, which in turn is equal to the period of f, that is, to $q^k - 1$. Thus α is a primitive (q^k-1)th root of unity. Hence f is the minimal polynomial over $\mathbb{F}_q$ of a primitive (q^k-1)th root of unity, which means that f is a primitive polynomial. Thus (iii) implies (i). □

Proof of Corollary 4.8. The claim follows from Theorem 4.7, by partitioning the $\varphi(q^k - 1)$ primitive (q^h-1)th roots of unity into pairwise disjoint sets of the form $\{\alpha^{q^0}, \ldots, \alpha^{q^{k-1}}\}$, □

4.4 Maximal-period sequences

Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{F}_q$ of positive order k. Then, by Theorem 4.1, the least period of $\boldsymbol{u}$ does not exceed $q^k - 1$. The sequence $\boldsymbol{u}$ is a *maximal-period sequence*[1] if $\boldsymbol{u}$ is periodic with least period equal to $q^k - 1$.

The next theorem provides a necessary and sufficient condition for a linear recurrence to be a maximal-period sequence.

Theorem 4.10. *Let $\boldsymbol{u}$ be a nonzero linear recurrence over $\mathbb{F}_q$ with minimal polynomial f. Then $\boldsymbol{u}$ is a maximal-period sequence if and only if f is a primitive polynomial.*

[1] Some authors use the term *maximum-length sequence* [66].

Proof. The claim follows from Theorem 3.3 and Theorem 4.7. □

Thus the construction of maximal-period sequences is equivalent to the construction of primitive polynomials, which is an important and difficult problem; see for instance the book by Shparlinski [174, Chapter 2].

The next theorem shows that maximal-period sequences exhibit peculiar regularities. A finite sequence $s_1, \ldots, s_n$ is a *cyclic sequence* if the element after s_n is s_1, and the element before s_1 is s_n. In other words: think of $s_1, \ldots, s_n$ as if they were arranged on a circle.

Theorem 4.11. *Let $\boldsymbol{u} \in \mathbb{F}_q^{\mathbb{N}}$ be a maximal-period sequence of order k, let $\boldsymbol{s}$ be the cyclic sequence $u_0, \ldots, u_{q^k-2}$, and let ℓ be an integer with $0 < \ell \leq k$. Then each nonzero sequence $a_1, \ldots, a_\ell$ ($a_i \in \mathbb{F}_q$) appears exactly $q^{k-\ell}$ times as a contiguous subsequence of $\boldsymbol{s}$, while the zero sequence $0, \ldots, 0$ (ℓ times 0) appears exactly $q^{k-\ell} - 1$ times as a contiguous subsequence of $\boldsymbol{s}$.*

Proof. Let $\boldsymbol{a} = a_1, \ldots, a_\ell$ be a sequence in $\mathbb{F}_q$ of length ℓ. Since $\boldsymbol{u}$ has least period equal to $q^k - 1$, the pigeonhole-principle argument in the proof of Theorem 4.1 implies that each tuple in $\mathbb{F}_q^k \setminus \{\mathbf{0}\}$ appears exactly once in the sequence $\big((u_n, \ldots, u_{n+k-1})\big)_{n=0,\ldots,q^k-2}$. Hence, the number of times that $\boldsymbol{a}$ appears as a contiguous subsequence of $\boldsymbol{s}$ is equal to the number of tuples in $\mathbb{F}_q^k \setminus \{\mathbf{0}\}$ whose first elements are $a_1, \ldots, a_\ell$. If $\boldsymbol{a} \neq \mathbf{0}$ then this number is $q^{k-\ell}$, since there are q possible values for each of the remaining $k - \ell$ elements of the tuple. If $\boldsymbol{a} = \mathbf{0}$ then this number is $q^{k-\ell} - 1$, since the zero tuple has to be excluded. □

The following theorem shows that all maximal-period sequences of order k can be generated by a single one.

Theorem 4.12. *Let k be a positive integer, let $\mathcal{R}_k \subseteq \{1, \ldots, q^k - 1\}$ be a complete set of representatives of the group $\big(\mathbb{Z}/(q^k-1)\mathbb{Z}\big)^*/\langle q \rangle$, and let $\boldsymbol{u} \in \mathbb{F}_q^{\mathbb{N}}$ be a maximal-period sequence of order k. Then the sequences $(u_{an+b})_{n\in\mathbb{N}}$, where a and b are integers such that $a \in \mathcal{R}_k$ and $0 \leq b \leq q^k - 2$, are pairwise distinct and constitute the set of all maximal-period sequences of order k.*

Proof. Let f be the minimal polynomial of $\boldsymbol{u}$. Theorem 4.10 says that f is a primitive polynomial of degree k. Hence, Theorem 4.7 implies that $f(x) = \prod_{i=0}^{k-1}(x - \alpha^{q^i})$, where α is a primitive $(q^k - 1)$th roots of unity.

Let a and b be integers such that $a \in \mathcal{R}_k$ and $0 \leq b \leq q^k - 2$. Claim: $(u_{an+b})_{n\in\mathbb{N}}$ is a maximal-period sequence of order k. Since $\gcd(a, q^k - 1) = 1$, the power α^a is a primitive $(q^k - 1)$th root of unity. Hence, Theorem 4.7 implies that $g(x) := \prod_{i=0}^{k-1}(x - \alpha^{aq^i})$ is a primitive polynomial of degree k. Note that the sequence $(u_{an+b})_{n\in\mathbb{N}}$ is nonzero and, by Corollary 2.16, its minimal polynomial is equal to g. Hence Theorem 4.10 implies that $(u_{an+b})_{n\in\mathbb{N}}$ is a maximal-period sequence of order k, as claimed.

Let $\boldsymbol{v} \in \mathbb{F}_q^{\mathbb{N}}$ be a maximal-period sequence of order k. Claim: there exist unique integers a and b such that $a \in \mathcal{R}_k$, $0 \leq b \leq q^k - 2$, and $v_n = u_{an+b}$ for every integer $n \geq 0$. Let g be the minimal polynomial of $\boldsymbol{v}$. From Theorem 4.10 it follows that g is a primitive polynomial. Furthermore, Theorem 4.7 implies that $g(x) = \prod_{i=0}^{k-1}(x - \beta^{q^i})$, where β is a

primitive (q^k-1)th root of unity. Hence, there exists an integer a such that $1 \le a \le q^k-1$, $\gcd(a, q^k-1) = 1$, and $\beta = \alpha^a$. In fact, by eventually replacing β with one of the other roots of g, assume that $a \in \mathcal{R}_k$. Then, by Corollary 2.16, the linear recurrence $(u_{an+c})_{n\in\mathbb{N}}$ has characteristic polynomial equal to g, for every integer $c \ge 0$. Moreover, from Theorem 4.11 it follows that there exists a unique integer b such that $0 \le b \le q^k-2$ and $(u_b, \dots, u_{b+k-1}) = (v_0, \dots, v_{k-1})$. Hence, the linear recurrences $\boldsymbol{v}$ and $(u_{an+b})_{n\in\mathbb{N}}$ are identical, since they have the same initial values and the same characteristic polynomial. Thus $v_n = u_{an+b}$ for every integer $n \ge 0$.

It remains to prove that a and b are unique. Suppose that $a' \in \mathcal{R}_k$ and $b' \in \mathbb{Z}$ are such that $0 \le b' \le q^k-2$ and $v_n = u_{a'n+b'}$ for every integer $n \ge 0$. Hence, by Corollary 2.16, the roots of $\boldsymbol{v}$ are the a'th powers of the roots of $\boldsymbol{u}$. In particular $\beta = \alpha^{a'q^i}$ for some $i \in \{1, \dots, k\}$. Recalling that $\beta = \alpha^a$, and that α is a primitive (q^h-1)th root of unity, it follows that $a \equiv a'q^i \pmod{(q^k-1)}$. In turn, since $a, a' \in \mathcal{R}_k$, this implies that $a' = a$. Thus $u_{an+b} = u_{an+b'}$ for every integer $n \ge 0$. Since $\boldsymbol{u}$ has period q^k-1, and a is invertible modulo q^k-1, it follows that $u_{n+b} = u_{n+b'}$ for every integer $n \ge 0$. Then, from Theorem 4.11, it follows easily that $b = b'$. This proves the uniqueness of a and b, □

Corollary 4.13. *Let k be a positive integer. Then there are exactly $\big(\varphi(q^k-1)/k\big) \cdot (q^k-1)$ maximal-period sequences of order k.*

Proof. The claim follows from Theorem 4.12, since there are $|\mathcal{R}_k| = \varphi(q^k-1)/k$ choices for a and q^k-1 choices for b. □

The next theorem is another characterization of maximal-period sequences.

Theorem 4.14. *Let k be a positive integer and let $\boldsymbol{u} \in \mathbb{F}_q^{\mathbb{N}}$ be a periodic sequence. Then $\boldsymbol{u}$ is a maximal-period sequence of order k if and only if $V := \{\mathbf{0}\} \cup \{x^i\boldsymbol{u} : i \in \mathbb{N}\}$ is a $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{\mathbb{N}}$ of dimension k.*

Proof. Let f be the minimal polynomial of $\boldsymbol{u}$. Since $\boldsymbol{u}$ is periodic, from Theorem 4.1 it follows that $f(0) \neq 0$. Let t be the period of f.

Claim: $|V| = t+1$. Let i and j be integers such that $i \ge j \ge 0$. Suppose that $x^i\boldsymbol{u} = x^j\boldsymbol{u}$. Hence $(x^{i-j}-1)x^j\boldsymbol{u} = \mathbf{0}$ and, recalling that f is the minimal polynomial of $\boldsymbol{u}$ and $f(0) \neq 0$, it follows that $x^{i-j} \equiv 1 \pmod f$. Thus $i \equiv j \pmod t$. Conversely, if $i \equiv j \pmod t$ then it follows easily that $x^i\boldsymbol{u} = x^j\boldsymbol{u}$. Therefore, the sequences $x^0\boldsymbol{u}, \dots, x^{t-1}\boldsymbol{u}$, and $\mathbf{0}$ are the pairwise distinct elements of V. Thus $|V| = t+1$, as claimed.

Suppose that $\boldsymbol{u}$ is a maximal-period sequence of order k. From Theorem 4.10 it follows that f is a primitive polynomial. Let $\mathbb{K} := \mathbb{F}_q[x]/(f)$ and note that $\mathbb{K}$ is a finite field of q^k elements. By Theorem 4.7, $t = q^k-1$ and consequently x is a generator of $\mathbb{K}^*$. Hence, for every $a, b \in \mathbb{F}_q$, either $ax^i + bx^j \equiv 0 \pmod f$ or $ax^i + bx^j \equiv x^k \pmod f$ for some integer $k \ge 0$. Since $f\boldsymbol{u} = \mathbf{0}$, this implies that every $\mathbb{F}_q$-linear combination of elements of V belongs to V. Therefore V is a $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{\mathbb{N}}$. Moreover, since $|V| = t+1 = q^k$, it follows that $\dim(V) = k$. Thus one implication is proved.

Suppose that V is a $\mathbb{F}_q$-linear subspace of $\mathbb{F}_q^{\mathbb{N}}$ of dimension k. Hence $|V| = q^k$, which implies that the period of f is equal to q^k-1. From Theorem 4.7 and Theorem 4.10 it follows that $\boldsymbol{u}$ is a maximal-period sequence of order k. This proves the other implication. □

The next result shows that every maximal-period sequence has a unique shift that satisfies a special relation.

Theorem 4.15. *Let $\boldsymbol{u} \in \mathbb{F}_q^{\mathbb{N}}$ be a maximal-period sequence of order k. Then there exists a unique integer i such that $0 \le i < (q^k-1)/(q-1)$ and $u_{qn+i} = u_{n+i}$ for every integer $n \ge 0$.*

Proof. First, the proof of the existence of i. Let f be the minimal polynomial of $\boldsymbol{u}$. From Theorem 4.10 it follows that f is a primitive polynomial. Thus f is the minimal polynomial over $\mathbb{F}_q$ of a primitive (q^k-1)th root of unity α. Hence, from Theorem 2.20, there exists $\beta \in \mathbb{F}_q(\alpha)$ such that $u_n = \operatorname{tr}(\alpha^n\beta)$ for every integer $n \ge 0$, where $\operatorname{tr} := \operatorname{tr}_{\mathbb{F}_q(\alpha)/\mathbb{F}_q}$. Since $\boldsymbol{u} \ne \boldsymbol{0}$, it follows that $\beta \in \mathbb{F}_q(\alpha)^*$. Moreover, since α generates $\mathbb{F}_q(\alpha)^*$, there exists an integer $i \ge 0$ such that $\beta = \alpha^{-i}$. Therefore

$$u_{qn+i} = \operatorname{tr}(\alpha^{qn+i}\beta) = \operatorname{tr}(\alpha^{qn}) = \operatorname{tr}(\alpha^n) = \operatorname{tr}(\alpha^{n+i}\beta) = u_{n+i}, \tag{4.1}$$

for every integer $n \ge 0$. Put $Q := (q^k-1)/(q-1)$. If $i < Q$ then the proof of the existence of i is complete. Suppose that $i \ge Q$. Since $\boldsymbol{u}$ has period q^k-1, from $Q \equiv qQ \pmod{(q^k-1)}$ and (4.1), it follows that

$$u_{qn+(i-Q)} = u_{q(n-Q)+i} = u_{n+(i-Q)},$$

for every integer $n \ge Q$. Thus (4.1) still holds if i is replaced by its remainder modulo Q. In other words, it is possible to assume that $i < Q$. This proves the existence of i.

Now to the proof of the uniqueness of i. Suppose that there exists an integer $j \ge 0$ such that $u_{qn+j} = u_{n+j}$ for every integer $n \ge 0$. Hence

$$\operatorname{tr}\bigl(\alpha^{n+q^{k-1}(j-i)}\bigr) = \operatorname{tr}\bigl(\alpha^{qn+q^k(j-i)}\bigr) = \operatorname{tr}(\alpha^{qn+j-i}) = u_{qn+j} = u_{n+j} = \operatorname{tr}(\alpha^{n+j-i}),$$

for every integer $n \ge 0$, where the facts that $\operatorname{tr}(\gamma) = \operatorname{tr}(\gamma^q)$ for each $\gamma \in \mathbb{F}_q(\alpha)$ and $\alpha^{q^k} = \alpha$ were employed. Then, Theorem 2.20 implies that $\alpha^{q^{k-1}(j-i)} = \alpha^{j-i}$. Thus, since α is a primitive (q^k-1)th root of unity, $(q^{k-1}-1)(j-i) \equiv 0 \pmod{(q^k-1)}$. In turn, it is easy to check that $\gcd(q^{k-1}-1, q^k-1) = q-1$, so that $j \equiv i \pmod{Q}$. This proves the uniqueness of i. □

4.5 Character sums

An *additive character* of $\mathbb{F}_q$ is a group homomorphism $\mathbb{F}_q \to \mathbb{C}^*$. In other words, an additive character of $\mathbb{F}_q$ is a function $\chi\colon \mathbb{F}_q \to \mathbb{C}^*$ that satisfies $\chi(a+b) = \chi(a)\chi(b)$ for every $a, b \in \mathbb{F}_q$. The *trivial additive character* of $\mathbb{F}_q$ is the additive character that is identically equal to 1.

The main result of this section is the following important upper bound for a *character sum* over the terms of a linear recurrence.

Theorem 4.16. *Let $f \in \mathbb{F}_q[x]$ be a nonconstant monic polynomial such that $f(0) \ne 0$, put $k := \deg(f)$ and $t := \operatorname{per}(f)$, let $\boldsymbol{u} \in \mathcal{L}^*(f)$, let N be an integer such that $0 < N < t$, and let χ be a nontrivial additive character of $\mathbb{F}_q$. Then*

$$\left|\sum_{n=0}^{N-1} \chi(u_n)\right| \le \begin{cases} q^{k/2}(\log t + 1) & \text{if } N < t; \\ q^{k/2} & \text{if } N = t. \end{cases} \tag{4.2}$$

In Section 4.6, an application of Theorem 4.16 yields an approximation for the number of solutions to a system of equations with linear recurrences (Theorem 4.23).

The proof of Theorem 4.16 needs some basic lemmas on character and exponential sums.

Lemma 4.17. *Let χ be a nontrivial additive character of $\mathbb{F}_q$ and let $b \in \mathbb{F}_q$. Then*

$$\frac{1}{q}\sum_{a\in\mathbb{F}_q}\chi(ab) = \begin{cases} 1 & \text{if } b = 0; \\ 0 & \text{if } b \neq 0. \end{cases}$$

Proof. If $b = 0$ then $\chi(ab) = \chi(0) = 1$ for every $a \in \mathbb{F}_q$, and the claim follows. Suppose that $b \neq 0$. Let $S := \sum_{a\in\mathbb{F}_q}\chi(a)$. Since χ is nontrivial, there exists $a_0 \in \mathbb{F}_q$ such that $\chi(a_0) \neq 0$. Hence

$$\chi(a_0)S = \sum_{a\in\mathbb{F}_q}\chi(a_0)\chi(a) = \sum_{a\in\mathbb{F}_q}\chi(a_0+a) = \sum_{c\in\mathbb{F}_q}\chi(c) = S,$$

which implies that $\big(1-\chi(a_0)\big)S = 0$, and so $S = 0$. Therefore

$$\sum_{a\in\mathbb{F}_q}\chi(ab) = \sum_{c\in\mathbb{F}_q}\chi(c) = S = 0,$$

as claimed. □

Let $\mathrm{e}(t) := \mathrm{e}^{2\pi \mathrm{i} t}$ for each $t \in \mathbb{R}$, where i is the imaginary unit.

Lemma 4.18. *Let $t > 0$ and n be integers. Then*

$$\frac{1}{t}\sum_{a=0}^{t-1}\mathrm{e}(an/t) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod t; \\ 0 & \text{if } n \not\equiv 0 \pmod t. \end{cases}$$

Proof. If $n \equiv 0 \pmod t$, then $\mathrm{e}(an/t) = 1$ for every integer a, and the claim follows. If $n \not\equiv 0 \pmod t$, then $\mathrm{e}(n/t) \neq 1$, and consequently

$$\sum_{a=0}^{t-1}\mathrm{e}(an/t) = \sum_{a=0}^{t-1}\big(\mathrm{e}(n/t)\big)^a = \frac{\big(\mathrm{e}(n/t)\big)^t - 1}{\mathrm{e}(n/t) - 1} = \frac{1-1}{\mathrm{e}(n/t)-1} = 0,$$

as claimed. □

Remark 4.19. The similarity of Lemma 4.17 and Lemma 4.18 is no coincidence. Each of them is the orthogonality relation for the characters of a finite abelian group ($\mathbb{F}_q$ for Lemma 4.17, and $\mathbb{Z}/t\mathbb{Z}$ for Lemma 4.18). See, e.g., the book by Nathanson [140, Section 4.2].

The next lemma is an upper bound for the average of some incomplete exponential sums.

Lemma 4.20. *Let t and N be positive integers. Then*

$$\frac{1}{t}\sum_{a=1}^{t-1}\left|\sum_{n=0}^{N-1}\mathrm{e}(an/t)\right| \leq \log t$$

Proof. Note that $\mathrm{e}(a/t) \neq 1$ for every $a \in \{1, \dots, t-1\}$. Consequently

$$\left|\sum_{n=0}^{N-1} \mathrm{e}(an/t)\right| = \left|\frac{\big(\mathrm{e}(a/t)\big)^N - 1}{\mathrm{e}(a/t) - 1}\right| \leq \frac{2}{|\mathrm{e}(a/t) - 1|} = \frac{1}{\sin(a\pi/t)} \leq \frac{t}{2\min\{a, t-a\}},$$

also thanks to the inequality $\sin(\pi x) \geq 2\min\{x, 1-x\}$, which holds for every $x \in [0,1]$. Hence

$$\sum_{a=1}^{t-1} \left|\sum_{n=0}^{N-1} \mathrm{e}(an/t)\right| \leq \frac{t}{2} \sum_{a=1}^{t-1} \frac{1}{\min\{a, t-a\}} = t \sum_{a=1}^{\lfloor t/2 \rfloor} \frac{1}{a} - \begin{cases} 1 & \text{if } t \text{ is even;} \\ 0 & \text{if } t \text{ is odd.} \end{cases} \tag{4.3}$$

If $t \leq 9$, then a computation shows that the right-hand side of (4.3) is not exceeding $t \log t$. If $t \geq 10$, then

$$\sum_{a=1}^{\lfloor t/2 \rfloor} \frac{1}{a} = \sum_{a=1}^{5} \frac{1}{a} + \int_5^{\lfloor t/2 \rfloor} \frac{\mathrm{d}x}{x} \leq \frac{137}{60} - \log 5 + \log(t/2) < \log t.$$

Therefore, in any case, the desired upper bound follows. □

The following result is an important formula for the average of the squared absolute values of some incomplete character sums involving linear recurrences.

Lemma 4.21. *Let $f \in \mathbb{F}_q[x]$ be a nonconstant monic polynomial such that $f(0) \neq 0$, put $k := \deg(f)$ and $t := \mathrm{per}(f)$, let N be a positive integer such that $N \leq t$, let a be an integer, and let χ be a nontrivial additive character of $\mathbb{F}_q$. Then*

$$\frac{1}{q^k} \sum_{\boldsymbol{u} \in \mathcal{L}(f)} \left|\sum_{n=0}^{N-1} \chi(u_n)\, \mathrm{e}(an/t)\right|^2 = N.$$

Proof. Pick $\boldsymbol{v} \in \mathcal{L}^*(f)$. From Theorem 2.3 it follows that $x^0\boldsymbol{v}, \dots, x^{k-1}\boldsymbol{v}$ form a basis of $\mathcal{L}(f)$. Hence, also employing Lemma 4.17, it follows that

$$\begin{aligned}
S &:= \sum_{\boldsymbol{u} \in \mathcal{L}(f)} \left|\sum_{n=0}^{N-1} \chi(u_n)\, \mathrm{e}(an/t)\right|^2 = \sum_{c_0, \dots, c_{k-1} \in \mathbb{F}_q} \left|\sum_{n=0}^{N-1} \chi\left(\sum_{i=0}^{k-1} c_i v_{n+i}\right) \mathrm{e}(an/t)\right|^2 \\
&= \sum_{c_0, \dots, c_{k-1} \in \mathbb{F}_q} \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} \mathrm{e}\big(a(m-n)/t\big)\, \chi\left(\sum_{i=0}^{k-1} c_i (v_{m+i} - v_{n+i})\right) \\
&= \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} \mathrm{e}\big(a(m-n)/t\big) \sum_{c_0, \dots, c_{k-1} \in \mathbb{F}_q} \prod_{i=0}^{k-1} \chi\big(c_i(v_{m+i} - v_{n+i})\big) \\
&= \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} \mathrm{e}\big(a(m-n)/t\big) \prod_{i=0}^{k-1} \left(\sum_{c_i \in \mathbb{F}_q} \chi\big(c_i(v_{m+i} - v_{n+i})\big)\right)
\end{aligned}$$

$$= q^k \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} \mathrm{e}\big(a(m-n)/t\big)\, N_{m,n}, \tag{4.4}$$

where

$$N_{m,n} := \begin{cases} 1 & \text{if } v_{m+i} = v_{n+i} \text{ for each } i \in \{0,\dots,k-1\}; \\ 0 & \text{otherwise;} \end{cases}$$

for all $m, n \in \{0,\dots,N-1\}$. Since $\boldsymbol{v} \in \mathcal{L}^*(f)$, from Theorem 4.4(i), it follows that the least period of $\boldsymbol{v}$ is equal to t. In turn, since $N \le t$, this implies that $N_{m,n} = 1$ if and only if $m = n$, for all $m, n \in \{0,\dots,N-1\}$. Thus from (4.4) it follows that $S = Nq^k$, as claimed. □

Now to the proof of Theorem 4.16.

Proof of Theorem 4.16. Let a be an integer and put

$$S_a := \sum_{n=0}^{t-1} \chi(u_n)\, \mathrm{e}(an/t).$$

From Theorem 3.3 it follows that the least period of $\boldsymbol{u}$ is equal to t. Consequently, the sequences $x^0\boldsymbol{u},\dots,x^{t-1}\boldsymbol{u}$ are t pairwise distinct linear recurrences belonging to $\mathcal{L}(f)$. Furthermore,

$$\left|\sum_{n=0}^{t-1} \chi(u_{n+i})\, \mathrm{e}(an/t)\right| = \left|\sum_{n=0}^{t-1} \chi(u_n)\, \mathrm{e}(an/t)\right| \big|\mathrm{e}(-ai/t)\big| = |S_a|, \tag{4.5}$$

for every integer $i \ge 0$. Thus, from (4.5) and Lemma 4.21 with $N = t$, it follows that

$$t|S_a|^2 = \sum_{i=0}^{t-1} \left|\sum_{n=0}^{t-1} \chi(u_{n+i})\, \mathrm{e}(an/t)\right|^2 \le \sum_{\boldsymbol{v} \in \mathcal{L}(f)} \left|\sum_{n=0}^{t-1} \chi(v_n)\, \mathrm{e}(an/t)\right|^2 = tq^k.$$

Hence $|S_a| \le q^{k/2}$. If $N = t$ then letting $a = 0$ in this last inequality yields the upper bound (4.2).

Suppose that $N < t$. From Lemma 4.18, Lemma 4.20, and the inequality $|S_a| \le q^{k/2}$, it follows that

$$\begin{aligned} \left|\sum_{n=0}^{t-1} \chi(u_n)\right| &= \left|\sum_{n=0}^{t-1} \chi(u_n) \sum_{m=0}^{N-1} \frac{1}{t} \sum_{a=0}^{t-1} \mathrm{e}\big(a(n-m)/t\big)\right| \\ &= \frac{1}{t} \left|\sum_{a=0}^{t-1} \sum_{m=0}^{N-1} \mathrm{e}(-am/t) \sum_{n=0}^{t-1} \chi(u_n)\, \mathrm{e}(an/t)\right| \\ &\le \frac{1}{t} \sum_{a=0}^{t-1} \left|\sum_{m=0}^{N-1} \mathrm{e}(-am/t)\right| |S_a| \\ &\le (\log t + 1) q^{k/2}, \end{aligned}$$

which is (4.2). □

Remark 4.22. Improvements of Theorem 4.16 are possible (see the bibliographical notes). Note that, thanks to Lemma 4.21, for every nontrivial additive character χ of $\mathbb{F}_q$ and for each fixed real number $\varepsilon > 0$,

$$\left|\sum_{n=0}^{N-1} \chi(u_n)\right| \le N^{1/2+\varepsilon}$$

for all linear recurrences $\boldsymbol{u} \in \mathcal{L}(f)$ but at most $q^k N^{-2\varepsilon}$ exceptions.

4.6 Distribution

This section collects some results on the distribution of the values of linear recurrences over finite fields. The first is a theorem providing an approximation for the number of solutions to a system of equations with linear recurrences.

Theorem 4.23. *Let $f \in \mathbb{F}_q[x]$ be a nonconstant monic polynomial such that $f(0) \neq 0$, put $t := \operatorname{per}(f)$, let $\boldsymbol{u}^{(1)}, \dots, \boldsymbol{u}^{(s)} \in \mathcal{L}^*(f)$ be linearly independent, let $y_1, \dots, y_s \in \mathbb{F}_q$, let N be a positive integer such that $N \le t$, and let S be the number of integers n such that $0 \le n < N$ and $u_n^{(i)} = y_i$ for each $i \in \{1, \dots, s\}$. Then*

$$\left|S - N/q^s\right| \le \left(1 - \frac{1}{q^s}\right) \cdot \begin{cases} q^{k/2}(\log t + 1) & \text{if } N < t; \\ q^{k/2} & \text{if } N = t. \end{cases}$$

Proof. Let χ be a nontrivial additive character of $\mathbb{F}_q$. From Lemma 4.17 it follows that

$$\begin{aligned} S &= \sum_{n=0}^{N-1} \prod_{i=1}^{s} \left(\frac{1}{q} \sum_{c_i \in \mathbb{F}_q} \chi\big(c_i(u_n^{(i)} - y_i)\big) \right) = \frac{1}{q^s} \sum_{n=0}^{N-1} \sum_{c_1, \dots, c_s \in \mathbb{F}_q} \prod_{i=1}^{s} \chi\big(c_i(u_n^{(i)} - y_i)\big) \\ &= \frac{1}{q^s} \sum_{c_1, \dots, c_s \in \mathbb{F}_q} \sum_{n=0}^{N-1} \chi\left(\sum_{i=1}^{s} c_i u_n^{(i)} \right) \chi\left(-\sum_{j=1}^{s} c_j y_j \right). \end{aligned} \tag{4.6}$$

If $c_1 = \cdots = c_s = 0$ then the second sum in the right-hand side of (4.6) is equal to N. Hence, recalling that $\boldsymbol{u}^{(1)}, \dots, \boldsymbol{u}^{(s)}$ are linearly independent, it follows that

$$\begin{aligned} \left|S - N/q^s\right| &\le \frac{1}{q^s} \left| \sum_{(c_1, \dots, c_s) \in \mathbb{F}_q^s \setminus \{\mathbf{0}\}} \sum_{n=0}^{N-1} \chi\left(\sum_{i=1}^{s} c_i u_n^{(i)} \right) \chi\left(-\sum_{j=1}^{s} c_j y_j \right) \right| \\ &\le \frac{1}{q^s} \sum_{(c_1, \dots, c_s) \in \mathbb{F}_q^s \setminus \{\mathbf{0}\}} \left| \sum_{n=0}^{N-1} \chi\left(\sum_{i=1}^{s} c_i u_n^{(i)} \right) \right| \le \left(1 - \frac{1}{q^s}\right) \max_{\substack{\boldsymbol{u} \in \mathcal{L}(f) \\ \boldsymbol{u} \neq \mathbf{0}}} \left| \sum_{n=0}^{N-1} \chi(u_n) \right|. \end{aligned}$$

At this point, the claim follows from Theorem 4.16. □

Remark 4.24. The upper bound of Theorem 4.23 is nontrivial only when f has a large period, say $t > q^{k/2+\varepsilon}$ for some fixed real number $\varepsilon > 0$.

The following theorem is an upper bound for the number of zeros of a simple linear recurrence (cf. Corollary 2.16).

Theorem 4.25. *Let $k \geq 2$ be an integer, let $c_1, \ldots, c_k, \alpha_1, \ldots, \alpha_k \in \mathbb{F}_q^*$, and let R be the number of integers n such that $0 \leq n < q-1$ and $\sum_{i=1}^{k} c_i \alpha_i^n = 0$. Then*

$$R \leq 2(q-1)\, T^{-1/(k-1)},$$

where

$$T := \max_{1 \leq i \leq k} \min_{j \neq i} \operatorname{ord}(\alpha_j/\alpha_i).$$

The proof of Theorem 4.25 requires a technical lemma.

Lemma 4.26. *Let $r_1, \ldots, r_k, m, T$ be integers such that $m > 0$ and $T > 1$. Then there exist a positive integer $\ell < T$ and integers $s_1, \ldots, s_k$ such that $s_i \equiv r_i \ell \pmod{m}$ and $|s_i| \leq m/T^{1/k}$ for each $i \in \{1, \ldots, k\}$.*

Proof. For $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{R}^k$, let $\|\boldsymbol{x}\|_\infty := \max\{|x_1|, \ldots, |x_k|\}$ be the ∞-norm of $\boldsymbol{x}$, and let

$$\|\boldsymbol{x}\|_m := \min_{\boldsymbol{z} \in (m\mathbb{Z})^k} \|\boldsymbol{x} - \boldsymbol{z}\|_\infty \quad \text{and} \quad \mathrm{d}_m(\boldsymbol{x}, \boldsymbol{y}) := \|\boldsymbol{x} - \boldsymbol{y}\|_m.$$

It follows easily that d_m is a pseudometric on $\mathbb{R}^k$, which becomes a metric on $(\mathbb{R}/m\mathbb{Z})^k$.

For each $i \in \{1, \ldots, T\}$, let $\boldsymbol{x}_i := (r_1 i, \ldots, r_k i) \in (\mathbb{R}/m\mathbb{Z})^k$. Moreover, put

$$d := \min_{1 \leq i < j \leq T} \mathrm{d}_m(\boldsymbol{x}_i, \boldsymbol{x}_j)$$

and let

$$\mathcal{B}_i := \left\{\boldsymbol{x} \in (\mathbb{R}/m\mathbb{Z})^k : \mathrm{d}_m(\boldsymbol{x}, \boldsymbol{x}_i) < d/2\right\},$$

for every $i \in \{1, \ldots, T\}$. Thus, by construction, the balls $\mathcal{B}_1, \ldots, \mathcal{B}_T$ are T pairwise disjoint subsets of $(\mathbb{R}/m\mathbb{Z})^k$, and each of them has measure equal to d^k. Therefore, since the measure of $(\mathbb{R}/m\mathbb{Z})^k$ is equal to m^k, it follows that $d \leq m/T^{1/k}$.

At this point, pick $i, j \in \{1, \ldots, T\}$ such that $i > j$ and $\mathrm{d}_m(\boldsymbol{x}_i, \boldsymbol{x}_j) = d$. Setting $\ell := i - j$, it follows that ℓ is a positive integer such that $\ell < T$ and

$$\|\boldsymbol{x}_\ell\|_m = \|\boldsymbol{x}_i - \boldsymbol{x}_j\|_m = \mathrm{d}_m(\boldsymbol{x}_i, \boldsymbol{x}_j) = d \leq m/T^{1/k}.$$

This implies that there exist integers $s_1, \ldots, s_k$ such that $s_i \equiv r_i \ell \pmod{m}$ and $|s_i| \leq m/T^{1/k}$ for each $i \in \{1, \ldots, k\}$, as desired. □

Proof of Theorem 4.25. Put $M := (q-1)\, T^{-1/(k-1)}$. The claim to prove is that $R \leq 2M$. If $T = 1$ then the claim follows. Hence, assume that $T > 1$. Up to reordering $\alpha_1, \ldots, \alpha_k$, assume that

$$T := \min_{2 \leq j \leq k} \operatorname{ord}(\alpha_j/\alpha_1).$$

Let g be a generator of $\mathbb{F}_q^*$. Thus there exist integers $r_1, \ldots, r_{k-1}$ such that $\alpha_j/\alpha_k = g^{r_j}$ for each $j \in \{1, \ldots, k-1\}$. Furthermore, by Lemma 4.26, there exist a positive integer

$\ell < T$ and integers $s_1, \ldots, s_{k-1}$ such that $s_j \equiv r_j \ell \pmod{(q-1)}$ and $|s_j| \le M$ for each $j \in \{1, \ldots, k-1\}$. Put also $s_k := 0$.

Claim: $s_1 \notin \{s_2, \ldots, s_k\}$. If $s_1 = s_j$ for some $j \in \{2, \ldots, k-1\}$, then $(r_j - r_1)\ell \equiv 0 \pmod{(q-1)}$, and so $(\alpha_j/\alpha_1)^\ell = 1$, which is impossible since $\ell < T$ and $\mathrm{ord}(\alpha_j/\alpha_1) \ge T$. If $s_1 = s_k$, then $r_1 \ell \equiv 0 \pmod{(q-1)}$, and so $(\alpha_k/\alpha_1)^\ell = 1$, which is impossible since $\ell < T$ and $\mathrm{ord}(\alpha_k/\alpha_1) \ge T$. This proves the claim.

Let $c'_1, \ldots, c'_k \in \mathbb{F}_q^*$, and let R' be the number of integers n such that $0 \le n < q-1$ and $\sum_{i=1}^k c'_i \alpha_i^{\ell n} = 0$. Claim: $R' \le 2M$. Let $f(x) := \sum_{i=1}^k c'_i x^{s_i + M}$. Since $s_1 \notin \{s_2, \ldots, s_k\}$ and $|s_i| \le M$ for each $i \in \{1, \ldots, k\}$, it follows that $f(x)$ is a nonzero polynomial of degree at most $2M$. Hence $f(x)$ has at most $2M$ roots. It follows easily that $\sum_{i=1}^k c'_i \alpha_i^{\ell n} = 0$ if and only if $f(g^n) = 0$, for every integer n. Thus $R' \le 2M$, as claimed.

Now to the proof of the upper bound on R. Let $d := \gcd(\ell, q-1)$. From the fact that $\gcd\big(\ell, (q-1)/d\big) = 1$, it follows that for every integer n, with $0 \le n < q-1$, there exist unique integers n_1, n_2, with $0 \le n_1 < d$ and $0 \le n_2 < (q-1)/d$, such that $n \equiv n_1 + \ell n_2 \pmod{(q-1)}$. Hence

$$\begin{aligned} R &= \sum_{n_1=0}^{d-1} \big|\big\{n_2 \in \mathbb{N} : 0 \le n_2 < (q-1)/d,\ \textstyle\sum_{i=1}^k c_i \alpha_i^{n_1} \alpha_i^{\ell n_2} = 0\big\}\big| \\ &= \frac{1}{d} \sum_{n_1=0}^{d-1} \big|\big\{n \in \mathbb{N} : 0 \le n < q-1,\ \textstyle\sum_{i=1}^k c_i \alpha_i^{n_1} \alpha_i^{\ell n} = 0\big\}\big| \\ &\le \frac{1}{d} \sum_{n_1=0}^{d-1} 2M = 2M, \end{aligned}$$

also thanks to the upper bound on R' with $c'_i := c_i \alpha_i^{n_1}$. □

The next result is a lower bound for the cardinality of the set of values of a tuple of linear recurrences over an interval of integers.

Theorem 4.27. *Let $f \in \mathbb{F}_q[x]$ be a nonconstant monic polynomial such that $f(0) \ne 0$, put $k := \deg(f)$ and $t := \mathrm{per}(f)$, let $\boldsymbol{u}^{(1)}, \ldots, \boldsymbol{u}^{(s)} \in \mathcal{L}^*(f)$ be linearly independent (note that $s \le k$ by Theorem 2.1(i)), let N be an integer with $k \le N \le t$, and let*

$$\mathcal{V}_N := \big\{(u_n^{(1)}, \ldots, u_n^{(s)}) : n \in \mathbb{N},\ n < N\big\}.$$

If $s = 1$, or if $s \ge 2$ and f is irreducible over $\mathbb{F}_q$, then

$$|\mathcal{V}_N| \ge \begin{cases} (N - k + s)^{1/(k-s+1)} & \text{if } N < t; \\ t^{1/(k-s+1)} & \text{if } N = t. \end{cases}$$

Proof. First, assume that $s = 1$ and let $\boldsymbol{u} := \boldsymbol{u}^{(1)}$. Recall that, from Theorem 3.3, the least period of $\boldsymbol{u}$ is equal to t. If $N < t$ then the $N - k + 1$ tuples $(u_n, \ldots, u_{n+k-1})$, where $n \in \{0, \ldots, N-k\}$, are pairwise distinct and belong to the Cartesian product $\big(\mathcal{V}_N\big)^k$. Hence

$|\mathcal{V}_N| \geq (N-k+1)^{1/k}$, as desired. If $N = t$ then the t tuples $(u_n, \ldots, u_{n+k-1})$, where $n \in \{0, \ldots, t-1\}$, are pairwise distinct and, since $u_{m+t} = u_m$ for every integer $m \geq 0$, belong to $\big(\mathcal{V}_N\big)^k$. Hence $|\mathcal{V}_N| \geq t^{1/k}$, as desired.

Now assume that $s \geq 2$ and f is irreducible over $\mathbb{F}_q$. Let $\mathbb{L}$ be the splitting field of f over $\mathbb{F}_q$, and let $\alpha_1, \ldots, \alpha_k \in \mathbb{L}^*$ be the pairwise distinct roots of f. Note that f has no multiple root, since f is irreducible over $\mathbb{F}_q$. From Theorem 2.15 it follows that $u_n^{(i)} = \sum_{j=1}^{k} c_j^{(i)} \alpha_j^n$ for each $i \in \{1, \ldots, s\}$ and for every integer $n \geq 0$, for some coefficients $c_j^{(i)} \in \mathbb{L}$. Moreover, since $\boldsymbol{u}^{(1)}, \ldots, \boldsymbol{u}^{(s)}$ are linearly independent, the matrix $\boldsymbol{C} := (c_j^{(i)}) \in \mathbb{L}^{s \times k}$ has rank equal to s. Hence, there exists $\boldsymbol{\lambda} := (\lambda_i) \in \mathbb{L}^{1 \times s}$ such that the vector $\boldsymbol{\lambda C}$ is nonzero and has at most $k - s + 1$ nonzero entries. This implies that $\boldsymbol{u} := \sum_{i=1}^{s} \lambda_i \boldsymbol{u}^{(i)} \in \mathbb{L}^{\mathbb{N}}$ is a nonzero linear recurrence of order at most $k - s + 1$. Let $g \in \mathbb{L}[x]$ be the minimal polynomial of $\boldsymbol{u}$. Thus the roots of g belong to $\{\alpha_1, \ldots, \alpha_k\}$. Since f is irreducible, the roots $\alpha_1, \ldots, \alpha_k$ have the same multiplicative order. Thus $\mathrm{per}(g) = t$ by Theorem 3.3. Therefore, by using the lower bound for the case $s = 1$, it follows that

$$|\mathcal{V}_N| \geq \big|\{u_n : n \in \mathbb{N},\, n < N\}\big| \geq \begin{cases} (N-k+s)^{1/(k-s+1)} & \text{if } N < t; \\ t^{1/(k-s+1)} & \text{if } N = t; \end{cases}$$

as desired. □

4.7 Linear-feedback shift registers

A *linear-feedback shift register* (LFSR) is an electronic circuit that, at each clock cycle, outputs a bit corresponding to the next term of a linear recurrence $\boldsymbol{u}$ over $\mathbb{F}_2$.

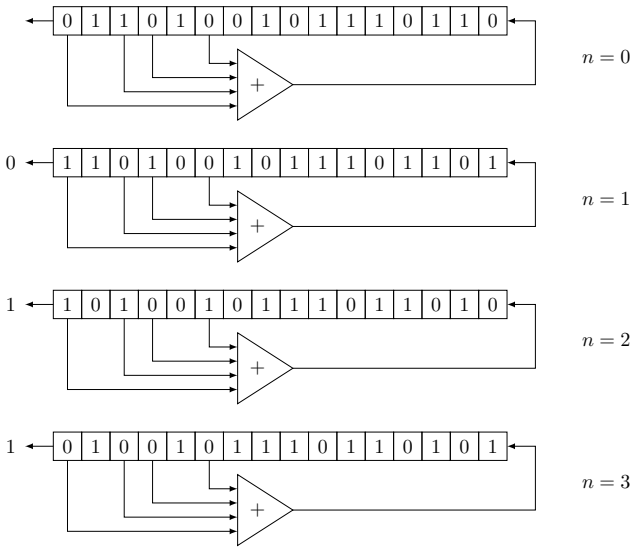


Figure 4.1: Three clock cycles of a 16-bit LFSR whose characteristic polynomial is the primitive polynomial $x^{16} + x^5 + x^3 + x^2 + 1$.

Without going too much into detail, an LFSR consists of

(i) a *shift register* of k bits, whose content at the nth clock cycle represents the state vector $\begin{pmatrix} u_n & \cdots & u_{n+k-1} \end{pmatrix}^\mathsf{T}$ of the kth-order linear recurrence $\boldsymbol{u}$ (recall Theorem 2.22);

(ii) an *adder* that computes u_{n+k} by performing the addition in $\mathbb{F}_2$ of the bits of the shift register corresponding to the terms u_{n+i}, where $i \in \{0, \cdots, k-1\}$ is such that $a_i = 1$ and $f(x) = \sum_{i=0}^{k} a_i x^i$ ($a_i \in \mathbb{F}_2$) is the minimal polynomial of $\boldsymbol{u}$.

At each clock cycle, the content of the shift register is shifted to the left, with the first bit being returned as output and the new last bit being provided by the output of the adder. The shift register is initialized with any nonzero state vector. See Figure 4.1 for an illustration.

Usually, the minimal polynomial f is a primitive polynomial, so that $\boldsymbol{u}$ is a maximal-period sequence, and the output sequence of the LFSR has period $2^k - 1$ (recall Theorem 4.10).

```c
#include <stdio.h>
#include <stdint.h>

int main() {
    uint16_t n = 1, s = 0x6E96, b;

    while (n) {
        printf("%d", s & 1);
        b = s ^ (s >> 2) ^ (s >> 3) ^ (s >> 5);
        s = (s >> 1) | (b << 15);
        n++;
    }

    return 0;
}
```

Figure 4.2: The C source code of a program that prints the full period of an LFSR having characteristic polynomial $x^{16} + x^5 + x^3 + x^2 + 1$.

LFSRs can also be implemented in software, by leveraging CPU bitwise and shift operations. See Figure 4.2 for a simple implementation in the C programming language.

LFSRs have many important applications in fields that require the fast generation of bit sequences that are very uniformly distributed (Theorem 4.11) and have a long period. These applications include fast counters, white noise generation, digital communications, error-detecting codes, circuit testing, pseudorandom number generators, and stream ciphers. With regard to cryptographic applications, note that the output of an LFSR cannot be used directly as a source of cryptographically secure pseudorandom bits. Indeed, given only $2k$ output bits of an LFSR, the Berlekamp–Massey algorithm (Algorithm 2.1) makes it possible to efficiently reconstruct the characteristic polynomial and thereby predict all subsequent bits. However, cryptographically secure pseudorandom bits can be generated from an LFSR

by employing various techniques, such as applying a nonlinear function to the bits in the shift register. For more on the applications of LFSRs, see the book by Jetzek [87, Chapter 6].

4.8 Bibliographical notes

The material of this chapter is mostly inspired by the related chapters of the book of Everest, van der Poorten, Shparlinski, and Ward [55, Chapters 3, 5, and 7].

Sections 4.2–4.4

The results of these sections appear, in more or less the same form, in the books by Golomb [66, Chapter IV] and Lidl–Niederreiter [115, Chapters 3, 6, and Section 4 of Chapter 7]. For Theorem 4.6, see the paper by Pinch [146, Proposition 8]. A *de Bruijn sequence* of order ℓ over an alphabet $\mathcal{A}$ of m letters is a cyclic sequence $\boldsymbol{s}$ such that each sequence $a_1, \ldots, a_\ell$ ($a_i \in \mathcal{A}$) appears exactly once as a contiguous subsequence of $\boldsymbol{s}$. From Theorem 4.11, it is clear that maximal-period sequences and de Brujin sequences are closely related. For an extensive treatise on de Brujin sequences, see the book of Etzion [54].

Section 4.5 "Character sums"

Korobov [103] was the first to prove Theorem 4.16. Shparlinski [175] and Ali [134] provided some improvements. Shparlinski [171] gave upper bounds for sums of *multiplicative characters* of $\mathbb{F}_q^*$ over linear recurrences. These bounds make possible to improve the case $s = 1$ of Theorem 4.23 (see [171, Lemma 4, Theorem 3]).

Section 4.6 "Distribution"

Shparlinski [171, 173] and Kamlovskii [88, 89, 90] gave improvements and generalizations of Theorem 4.23.

Canetti et al. [30, Lemma 7] proved a slightly weaker form of Theorem 4.25. Later, Kelley [94, Theorem 2.3 and Proposition 2.4] proved a more precise upper bound that implies Theorem 4.25. Canetti et al. and Kelley stated their results in terms of sparse polynomials, but it is not difficult to translate them in terms of linear recurrences.

Mullen and Shparlinski [137, Theorem 3] proved Theorem 4.27 and several other lower bounds for the cardinality of $\mathcal{V}_N$.

Section 4.7 "Linear-feedback shift registers"

The books by Golomb [66], Lidl–Niederreiter [115, Chapter 6], and Jetzek [87] provide the general theory of LFSRs.

4.9 Exercises

Exercise 4.1. Let $\mathcal{S}$ be a finite set, let k be a positive integer, let $f\colon \mathcal{S}^k \to \mathcal{S}$, and let $\boldsymbol{u} \in \mathcal{S}^{\mathbb{N}}$ be the sequence defined recursively by

$$u_n := f(u_{n-1}, \dots, u_{n-k}),$$

for every integer $n \geq k$.

(i) Prove that $\boldsymbol{u}$ is ultimately periodic.

(ii) State a condition on f under which $\boldsymbol{u}$ is periodic.

(This is a wide, but not deep, generalization of one of the implications of Theorem 4.1.)

Exercise 4.2. Determine the number of periodic linear recurrences over $\mathbb{F}_7$ with least period equal to 4.

Exercise 4.3. Prove Theorem 4.4(ii) using rational functions as hinted in Remark 4.5.

Exercise 4.4. Prove Theorem 4.4(ii) as follows.

(i) Prove that

$$|\mathcal{L}^*(f^k)| = q^{k \deg(f)}\big(1 - q^{-\deg(f)}\big),$$

for every irreducible polynomial $f \in \mathbb{F}_q[x]$ and for every positive integer k.

(ii) Use Theorem 2.5(iv).

Exercise 4.5. Let k be an integer such that $2^k - 1$ is a prime number (in fact, a Mersenne prime). Prove that every polynomial $f \in \mathbb{F}_q[x]$ of degree k is primitive if and only if it is irreducible.

Exercise 4.6. Let $f \in \mathbb{F}_q[x]$ be a primitive polynomial. Prove that $f^*(x)/f(0)$ is a primitive polynomial.

Exercise 4.7. Determine all prime powers q and all primitive polynomials $f \in \mathbb{F}_q[x]$ such that $f^* = f$.

Exercise 4.8. Let $\boldsymbol{u}$ be a maximal-period sequence over $\mathbb{F}_q$ of order k, let Φ be the function $\mathbb{Z}/(q^k - 1)\mathbb{Z} \to \mathbb{F}_q$ defined by $\Phi(n) := (u_n, \dots, u_{n+k-1})$ for every integer n, and define a product over $\mathbb{F}_q^k$ by

$$\boldsymbol{a} \cdot \boldsymbol{0} := \boldsymbol{0} \cdot \boldsymbol{a} := \boldsymbol{0} \cdot \boldsymbol{0} := \boldsymbol{0} \quad \text{and} \quad \boldsymbol{a} \cdot \boldsymbol{b} := \Phi\big(\Phi^{-1}(\boldsymbol{a}) + \Phi^{-1}(\boldsymbol{b})\big)$$

for every $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_q^k \setminus \{\boldsymbol{0}\}$.

(i) Prove that Φ is well defined.

(ii) Prove that Φ is a bijection (so that the product is well defined).

(iii) Prove that $\mathbb{F}_q^k$ with termwise addition and the product defined by (4.8) is a field.

Exercise 4.9. Let $\boldsymbol{u}$ be a maximal-period sequence over $\mathbb{F}_q$ of order k and let χ be a nontrivial additive character of $\mathbb{F}_q$. Compute the complete character sum

$$\sum_{n=0}^{q^k-2} \chi(u_n).$$

Exercise 4.10. Let q be a fixed prime power, let $k \to +\infty$ be a prime number, and let $\boldsymbol{u} \in \mathbb{F}_q^{\mathbb{N}}$ be a kth-order maximal-period sequence. Prove that the number of zeros of $\boldsymbol{u}$ over its period is asymptotic to q^{k-1}, while the upper bound for the number of zeros of $\boldsymbol{u}$ provided by Theorem 4.25 is asymptotic to $2q^{k-1}$. (Hence, Theorem 4.25 is asymptotically optimal up to a factor of 2.)

Exercise 4.11. Design a LFSR whose output sequence has least period $2^7 - 1$, using the minimum number of wires.

Chapter 5

Linear Recurrences in Characteristic Zero

5.1 Introduction

This chapter is devoted to linear recurrences over a field of characteristic zero or, more specifically, a number field. The prerequisites are the same as those of the previous chapters, plus a basic knowledge of algebraic number theory and p-adic analysis.

This chapter begins with some preliminary facts: the *Cassels' embedding theorem*, which provides embeddings of a finitely-generated extension of the rational numbers into the field of p-adic numbers for infinitely many primes p (Section 5.2); and the important notion of *nondegenerate* linear recurrence (Section 5.3).

The first topic of this chapter is the study of the set of zeros of a linear recurrence. This includes the important *Skolem–Mahler–Lech theorem*, which says that the set of zeros of a linear recurrence is the union of finitely many arithmetic progressions and a finite set; the related *Skolem problem*, which is still unsettled; and an upper bound on the number of zeros of a nondegenerate linear recurrence (Section 5.4).

The second topic is the growth of terms of linear recurrences, that is, upper and lower bounds for the absolute values of the terms of a linear recurrence over a number field. The proofs of some of these results employ tools from Baker's theory of lower bounds for linear forms in logarithms (Section 5.5).

The third topic of this chapter is the factorization in the ring of generalized power sums, which (under mild hypotheses) turns out to be a unique factorization domain (Section 5.6).

Finally, this chapter deals with the important *Hadamard quotient theorem*, along with some related results (Section 5.7).

Remark 5.1. Let $\mathbb{K}$ be a field of characteristic zero and let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$. Then each term of $\boldsymbol{u}$ belongs to a finitely-generated subring $\mathcal{R}$ of $\mathbb{K}$. Indeed, if $f(x) = x^k - \sum_{i=1}^{k} a_i x^{k-i}$ $(a_i \in \mathbb{K})$ is the minimal polynomial of $\boldsymbol{u}$, then it suffices to take

$$\mathcal{R} = \mathbb{Z}[u_0, \ldots, u_{k-1}, a_1, \ldots, a_k].$$

This also implies that there is no loss of generality in assuming that $\mathbb{K}$ is a finitely-generated extension of $\mathbb{Q}$.

5.2 Cassels' embedding theorem

The purpose of this section is to prove the following important result of Cassels [34], which gives special p-adic embeddings for finitely-generated extensions of $\mathbb{Q}$.

Theorem 5.2 (Cassels' embedding theorem)**.** *Let $\mathbb{K}$ be a finitely-generated extension of $\mathbb{Q}$, and let $\mathcal{C}$ be a finite subset of $\mathbb{K}^*$. Then there are infinitely many prime numbers p such that there exists an embedding $\sigma_p\colon \mathbb{K} \to \mathbb{Q}_p$ satisfying $|\sigma_p(c)|_p = 1$ for every $c \in \mathcal{C}$.*

Theorem 5.2 is an extremely useful tool that makes possible to employ p-adic techniques to prove results in arbitrary fields of characteristic zero. It is used in part of the proof of the Skolem–Mahler–Lech theorem (Theorem 5.10) on the zeros of linear recurrences.

The proof of Theorem 5.2 requires some preliminary lemmas.

Lemma 5.3. *Let m, n be positive integers and, for each $i \in \{1, \dots, m\}$, let f_i be a nonzero polynomial in $\mathbb{Z}[x_1, \dots, x_n]$. Then there exist integers $a_1, \dots, a_n$ such that $f_i(a_1, \dots, a_n) \neq 0$ for each $i \in \{1, \dots, m\}$.*

Proof. The proof proceeds by induction on n. If $n = 1$ then it suffices to pick some integer a_1 that is distinct from all the finitely many roots of $f_1, \dots, f_m$. Suppose that the claim is proved for n. The goal is to prove it for $n + 1$. For each $i \in \{1, \dots, m\}$, the polynomial $f_i \in \mathbb{Z}[x_1, \dots, x_{n+1}]$ can be written as $f_i = \sum_{j=0}^{k_i} f_{i,j} x_{n+1}^j$, where $k_i \in \mathbb{N}$ and $f_{i,j} \in \mathbb{Z}[x_1, \dots, x_n]$. Since f_i is a nonzero polynomial, there exists a nonnegative integer $j_i \leq k_i$ such that f_{i,j_i} is nonzero. Hence, by the inductive hypothesis, there exist integers $a_1, \dots, a_n$ such that $f_{i,j_i}(a_1, \dots, a_n) \neq 0$ for every $i \in \{1, \dots, m\}$. Thus it suffices to pick some integer a_{n+1} that is distinct from all the finitely many roots of the nonzero polynomials $f_1(a_1, \dots, a_n, x_{n+1}), \dots, f_m(a_1, \dots, a_n, x_{n+1})$. □

Lemma 5.4. *Let $f \in \mathbb{Z}[x]$ be a nonconstant polynomial. Then there exist infinitely many primes p such that p divides $f(n)$ for some integer n.*

Proof. The proof is an adaptation of Euclid's proof of the infinitude of prime numbers. Write $f(x) = \sum_{i=0}^{k} a_i x^i$ ($a_i \in \mathbb{Z}$), where k is a positive integer and $a_k \neq 0$. If $a_0 = 0$ then the claim follows, since p divides $f(p)$ for every prime number p. Hence, assume that $a_0 \neq 0$. Let $\mathcal{P}$ be a finite set of prime numbers, and put $P := \prod_{p \in \mathcal{P}} p$. Since f is nonconstant, there exists a sufficiently large integer n such that $|f(a_0 P n)| > |a_0|$. Furthermore,

$$f(a_0 P n) = \sum_{i=0}^{k} a_i (a_0 P n)^i = a_0 \left(1 + P \sum_{i=1}^{k} a_i (a_0 P)^{i-1} n^i \right), \tag{5.1}$$

where the term in the parentheses of the right-hand side of (5.1) is an integer with absolute value greater than 1 and not divisible by any prime in $\mathcal{P}$. Thus $f(a_0 P n)$ has a prime factor that does not belong to $\mathcal{P}$. The claim follows. □

Lemma 5.5. *Let p be a prime number, let $f \in \mathbb{Z}_p[x]$, let D be the discriminant of f, and let $a \in \mathbb{Z}_p$. Suppose that $|f(a)|_p < |D|_p^2$. Then there exists $\alpha \in \mathbb{Q}_p$ such that $f(\alpha) = 0$ and $|\alpha - a|_p < 1$.*

Proof. Note that f must be nonzero. Recall that $D = a^{-1}(-1)^{n(n-1)/2}\operatorname{res}(f, f')$, where a is the leading coefficient of f and $n := \deg(f)$. By the properties of the resultant, there exist $g, h \in \mathbb{Z}_p[x]$ such that $D = fg + f'h$. Since

$$|f(a)g(a)|_p = |f(a)|_p|g(a)|_p \leq |f(a)|_p < |D|_p^2 \leq |D|_p,$$

it follows that

$$|D|_p = |D - f(a)g(a)|_p = |f'(a)h(a)|_p = |f'(a)|_p|h(a)|_p \leq |f'(a)|_p,$$

and so $|f(a)|_p < |D|_p^2 \leq |f'(a)|_p^2$. Thus Hensel's lemma (Lemma A.29) implies that there exists $\alpha \in \mathbb{Q}_p$ such that $f(\alpha) = 0$ and $|\alpha - a|_p < 1$, as claimed. □

Now to the proof of Theorem 5.2.

Proof of Theorem 5.2. By enlarging $\mathcal{C}$, assume that $c^{-1} \in \mathcal{C}$ for each $c \in \mathcal{C}$. Hence, it suffices to prove the existence of infinitely many prime numbers p and corresponding embeddings σ_p such that $|\sigma_p(c)|_p \leq 1$ for each $c \in \mathcal{C}$.

Let $\alpha_1, \ldots, \alpha_n$ be a (possibly empty) transcendence basis of $\mathbb{K}$ over $\mathbb{Q}$. Thus $\mathbb{K} = \mathbb{Q}(\alpha_1, \ldots, \alpha_n, \beta)$ for some $\beta \in \mathbb{K}$ that is algebraic over $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Hence, for every $c \in \mathcal{C}$ there exist $U_c \in \mathbb{Z}[x_1, \ldots, x_n, y]$ and $V_c \in \mathbb{Z}[x_1, \ldots, x_n]$, with $V_c \neq 0$, such that

$$c = U_c(\alpha_1, \ldots, \alpha_n, \beta)/V_c(\alpha_1, \ldots, \alpha_n). \tag{5.2}$$

Since β is algebraic over $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, there exists a polynomial $G \in \mathbb{Q}(\alpha_1, \ldots, \alpha_n)[y]$ such that $G(\beta) = 0$ and G is irreducible over $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. Indeed, without loss of generality, assume that $G(y) = H(\alpha_1, \ldots, \alpha_n, y)$ for some $H \in \mathbb{Z}[x_1, \ldots, x_n, y]$. Let s be the degree of y in H, and let $H_0 \in \mathbb{Z}[x_1, \ldots, x_n]$ be the coefficient of y^s in H, so that $H_0 \neq 0$. The discriminant of H as a polynomial in y is equal to $D(\alpha_1, \ldots, \alpha_n)$, where $D \in \mathbb{Z}[x_1, \ldots, x_n]$ is a nonzero polynomial. From Lemma 5.3 it follows that there exist integers $a_1, \ldots, a_n$ such that

$$D(a_1, \ldots, a_n) \neq 0, \tag{5.3}$$
$$H_0(a_1, \ldots, a_n) \neq 0, \tag{5.4}$$
$$V_c(a_1, \ldots, a_n) \neq 0 \quad \text{for each } c \in \mathcal{C}. \tag{5.5}$$

From (5.4) it follows that $H(a_1, \ldots, a_n, y)$ is a nonzero polynomial in $\mathbb{Z}[y]$. Hence, Lemma 5.4 implies the existence of an infinite set of prime numbers $\mathcal{P}$ such that, for each $p \in \mathcal{P}$, there exists an integer b_p satisfying

$$H(a_1, \ldots, a_n, b_p) \equiv 0 \pmod{p}. \tag{5.6}$$

From (5.3), (5.4), and (5.5), by removing finitely many primes from $\mathcal{P}$, assume that

$$D(a_1, \ldots, a_n) \not\equiv 0 \pmod{p}, \tag{5.7}$$
$$H_0(a_1, \ldots, a_n) \not\equiv 0 \pmod{p}, \tag{5.8}$$
$$V_c(a_1, \ldots, a_n) \not\equiv 0 \pmod{p}, \text{ for each } c \in \mathcal{C} \text{ and } p \in \mathcal{P}. \tag{5.9}$$

Let $p \in \mathcal{P}$ and $c \in \mathcal{C}$ be fixed. Recall that $\mathbb{Q}_p$ has infinite transcendence degree over $\mathbb{Q}$. (Indeed, the field $\mathbb{Q}_p$ is uncountable, while every extension of $\mathbb{Q}$ of finite transcendence degree is countable). Hence, there exist n algebraic independent numbers $\theta_1, \ldots, \theta_n \in \mathbb{Q}_p$ that are transcendental over $\mathbb{Q}$. Moreover, by eventually replacing θ_i with $p^k\theta_i$ for some large integer k, assume that $|\theta_i|_p < 1$ for each $i \in \{1, \ldots, n\}$. Let $\zeta_i := a_i + \theta_i$ for each $i \in \{1, \ldots, n\}$. Then $\zeta_1, \ldots, \zeta_n$ are algebraic independent numbers in $\mathbb{Q}_p$ that are transcendental over $\mathbb{Q}$ and satisfy

$$|\zeta_i - a_i|_p < 1, \tag{5.10}$$

for each $i \in \{1, \ldots, n\}$. From (5.6), (5.7), and (5.10), it follows that

$$H(\zeta_1, \ldots, \zeta_n, b_p) \equiv 0 \pmod{p}, \quad \text{and} \quad D(\zeta_1, \ldots, \zeta_n) \not\equiv 0 \pmod{p}.$$

Thus Lemma 5.5 implies that there exists $\eta_p \in \mathbb{Q}_p$ such that $|\eta_p - b_p|_p < 1$ and

$$H(\zeta_1, \ldots, \zeta_n, \eta_p) = 0.$$

Noting that $\mathbb{K} \cong \mathbb{Q}(\alpha_1, \ldots, \alpha_n)/(G)$ and $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) \cong \mathbb{Q}(\zeta_1, \ldots, \zeta_n)$, there exists an embedding $\sigma_p \colon \mathbb{K} \to \mathbb{Q}_p$ that is defined by $\sigma_p(\beta) = \eta_p$ and $\sigma_p(\alpha_i) = \zeta_i$ for each $i \in \{1, \ldots, n\}$. Furthermore, on the one hand,

$$|U_c(\zeta_1, \ldots, \zeta_n, \eta_p)|_p \leq 1, \tag{5.11}$$

since $U_c \in \mathbb{Z}[x_1, \ldots, x_n, y]$, $|\eta_p|_p \leq 1$, and $|\zeta_i|_p \leq 1$ for each $i \in \{1, \ldots, n\}$. On the other hand,

$$|V_c(\zeta_1, \ldots, \zeta_n)|_p = 1, \tag{5.12}$$

since $V_c \in \mathbb{Z}[x_1, \ldots, x_n]$, (5.9), and (5.10). In conclusion, from (5.2), (5.11), and (5.12), it follows that $|\sigma_p(c)|_p \leq 1$, as desired. □

5.3 Degeneracy

Let $\mathbb{K}$ be a field, let $f \in \mathbb{K}[x]$ be a nonconstant polynomial such that $f(0) \neq 0$, and let $\mathbb{L}$ be the splitting field of f over $\mathbb{K}$. If f has two distinct roots $\alpha, \beta \in \mathbb{L}^*$ such that α/β is a root of unity, then f is *degenerate*. Otherwise, the polynomial f is *nondegenerate*. Let $\boldsymbol{u}$ be a nonzero reversible linear recurrence over $\mathbb{K}$. If the minimal polynomial of $\boldsymbol{u}$ is degenerate, then $\boldsymbol{u}$ is *degenerate*. Otherwise, the linear recurrence $\boldsymbol{u}$ is *nondegenerate*. Note that if $\mathbb{K}$ is a finite field then every nonzero reversible linear recurrence over $\mathbb{K}$ having at least two distinct roots is degenerate. Hence, degeneracy is interesting only when $\mathbb{K}$ is an infinite

field. The concept of degeneracy is fundamental in the study of the set of zeros of linear recurrences over fields of characteristic zero, which is the topic of Section 5.4.

The next theorem shows that, in characteristic zero, every reversible linear recurrence can be "partitioned" into finitely many subsequences that are either nondegenerate or the zero sequence.

Theorem 5.6. *Let $\mathbb{K}$ be a field of characteristic zero, and let $\boldsymbol{u}$ be a reversible linear recurrence over $\mathbb{K}$. Then there exists a positive integer m such that each of the sequences $(u_{mn+r})_{n\in\mathbb{N}}$, where $r \in \{0, \dots, m-1\}$, is either a nondegenerate linear recurrence or the zero sequence.*

Proof. If $\boldsymbol{u}$ is the zero sequence then the claim follows by taking $m = 1$. Hence, assume that $\boldsymbol{u}$ is nonzero. Let f be the minimal polynomial of $\boldsymbol{u}$ and let $\mathbb{L}$ be the splitting field of f over $\mathbb{K}$. Note that $f(0) \neq 0$, since $\boldsymbol{u}$ is reversible. Let $\alpha_1, \dots, \alpha_s \in \mathbb{L}^*$ be the pairwise distinct roots of $\boldsymbol{u}$, let Γ be the multiplicative group generated by them, and let m be the order of the torsion part of Γ. Hence $\Gamma^m := \{g^m : g \in \Gamma\}$ is a torsion-free group. Let $r \in \{0, \dots, m-1\}$. From Theorem 2.15 it follows easily that the sequence $(u_{mn+r})_{n\in\mathbb{N}}$ is a linear recurrence whose roots belong to Γ^m. Therefore, each sequence $(u_{mn+r})_{n\in\mathbb{N}}$ is either nondegenerate or the zero sequence. □

Remark 5.7. As it is clear from its proof, Theorem 5.6 remains true if "nondegenerate linear recurrence" is replaced by "generalized power sum whose roots generate a torsion-free group".

The following theorem states the existence of an algorithm to establish if a given polynomial is degenerate. A *computable field* is a field $\mathbb{K}$ such that each element of $\mathbb{K}$ has a finite representation (say, as a finite binary string), and, in terms of this representation, the field operations (addition, subtraction, multiplication, and division) can be computed, and the equality of two elements of $\mathbb{K}$ can be decided. For example, the field of rational numbers $\mathbb{Q}$ is computable, and more generally every number field is computable.

Theorem 5.8. *Let $\mathbb{K}$ be a computable field of characteristic zero. Then there exists an algorithm that, given as input a polynomial $f \in \mathbb{K}[x]$, establishes if f is degenerate or not.*

The proof of Theorem 5.8 needs the following lemma.

Lemma 5.9. *Let $\mathbb{K}$ be a field of characteristic zero, let $f \in \mathbb{K}[x]$ be a polynomial of positive degree k such that $f(0) \neq 0$, and let $r(x) := \operatorname{res}_y\big(f(y), f(xy)\big) \in \mathbb{K}[x]$. Then the following statements are equivalent.*

(i) *$f(x)$ is degenerate.*

(ii) *$r(x)$ has a root $\zeta \neq 1$ that is a root of unity.*

(iii) $\gcd\big(r(x), (x^n-1)/(x-1)\big) \neq 1$ *for some positive integer n such that*

$$\varphi(n) \leq (k^2)!\,[\mathbb{K} : \mathbb{Q}],$$

where φ is the Euler totient function.

Proof. By the definition of the resultant, it follows that γ is a root of $r(x)$ if and only if the polynomials $f(y)$ and $f(\gamma y)$ have a common root. Hence, since $f(0) \neq 0$, the roots of $r(x)$ are given by all the ratios α/β where α, β are roots of $f(x)$. Thus the equivalence of (i) and (ii) follows.

Since $f(x)$ has degree equal to k, the polynomial $r(x)$ has degree equal to k^2. Let $\mathbb{L}$ be the splitting field of $r(x)$ over $\mathbb{K}$. Suppose that $\zeta \in \mathbb{L}$ is a root of $r(x)$, and that ζ is a primitive nth root of unity. Then, since $\mathbb{Q}(\zeta) \subseteq \mathbb{L}$,

$$\varphi(n) = [\mathbb{Q}(\zeta) : \mathbb{Q}] \leq [\mathbb{L} : \mathbb{Q}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{Q}] \leq (k^2)! \, [\mathbb{K} : \mathbb{Q}].$$

Since every primitive nth root of unity $\zeta \neq 1$ is a root of $(x^n - 1)/(x - 1)$, the equivalence of (ii) and (iii) follows. □

Proof of Theorem 5.8. Note that $\varphi(2^h) = 2^{h-1} \geq 2^{(h-1)/2}$ and $\varphi(p^h) = p^{h-1}(p-1) > p^{h/2}$, for every positive integer h and for every odd prime number p. Hence, the multiplicativity of φ implies that $\varphi(n) \geq (n/2)^{1/2}$ for every positive integer n. Therefore, from Lemma 5.9 it follows that to test if f is degenerate or not it suffices to check if

$$\gcd\big(r(x), (x^n - 1)/(x - 1)\big) \neq 1$$

for some positive integer $n \leq 2\big(\big(\deg(f)^2\big)! \, [\mathbb{K} : \mathbb{Q}]\big)^2$, where $r(x) := \operatorname{res}_y\big(f(y), f(xy)\big)$. □

The algorithm proposed in the proof of Theorem 5.8 is very inefficient. Cipu, Diouf, and Mignotte [39] proposed much more efficient algorithms for testing the degeneracy of a polynomial.

5.4 Zeros

The following result is the celebrated Skolem–Mahler–Lech theorem on the set of zeros of a linear recurrence over a field of characteristic zero. For every sequence $\boldsymbol{u}$, let $\mathcal{Z}_{\boldsymbol{u}}$ be the set of integers $n \geq 0$ such that $u_n = 0$.

Theorem 5.10 (Skolem–Mahler–Lech theorem)**.** *Let $\mathbb{K}$ be a field of characteristic zero and let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$. Then $\mathcal{Z}_{\boldsymbol{u}}$ is the union of a finite set and finitely many arithmetic progressions. Moreover, if $\boldsymbol{u}$ is nondegenerate then $\mathcal{Z}_{\boldsymbol{u}}$ is finite.*

Proof. If $\boldsymbol{u} = \boldsymbol{0}$ then the claim is obvious. Hence, suppose that $\boldsymbol{u} \neq \boldsymbol{0}$. By Remark 5.1, assume that $\mathbb{K}$ is a finitely-generated extension of $\mathbb{Q}$. Let $f \in \mathbb{K}[x]$ be the minimal polynomial of $\boldsymbol{u}$. By Theorem 2.9, assume that $f(0) \neq 0$. Let $\mathbb{L}$ be the splitting field of f over $\mathbb{K}$. From Theorem 2.15 it follows that

$$u_n = \sum_{i=1}^{s} f_i(n) \, \alpha_i^n \tag{5.13}$$

for every integer $n \geq 0$, where $\alpha_1, \ldots, \alpha_s \in \mathbb{L}^*$ are the pairwise distinct roots of f and $f_1, \ldots, f_s \in \mathbb{L}[x]$ are nonzero polynomials.

By Theorem 5.2, there exist an arbitrary large prime number p and an embedding $\sigma_p\colon \mathbb{L} \to \mathbb{Q}_p$ such that $|\sigma_p(\alpha_i)|_p = 1$ for each $i \in \{1,\dots,s\}$.

To simplify the notation, identify $\mathbb{L}$ with the image of σ_p, so that $\mathbb{L} \subseteq \mathbb{Q}_p$. Note that $|\alpha_i|_p = 1$ for every $i \in \{1,\dots,s\}$, and so α_i is a p-adic integer that is invertible modulo p. By Fermat's little theorem in $\mathbb{Z}_p$, it follows that $\alpha_i^{p-1} \equiv 1 \pmod{p}$, and so Hence

$$|\alpha_i^{p-1} - 1|_p \le p^{-1} < p^{-1/(p-1)}.$$

From the properties of the p-adic logarithm and p-adic exponential (Theorem A.30(i) and (iii)) it follows that

$$\alpha_i^{(p-1)n} = \operatorname{Exp}_p\Big(n \operatorname{Log}_p\big(\alpha_i^{p-1}\big)\Big)$$

for every integer $n \ge 0$.

Hence, for each integer $r \ge 0$, the function

$$U_r(z) := \sum_{i=1}^{s} f_i\big((p-1)z + r\big)\, \alpha_i^r \operatorname{Exp}_p\Big(z \operatorname{Log}_p\big(\alpha_i^{p-1}\big)\Big) \tag{5.14}$$

is a p-adic analytic and defined for every $z \in \mathbb{Z}_p$. From (5.13) and (5.14), it follows that

$$u_{(p-1)m+r} = U_r(m) \tag{5.15}$$

for every integer $m \ge 0$ and each $r \in \{0,\dots,p-2\}$.

Since, for each $r \in \{0,\dots,p-2\}$, the function U_r is p-adic analytic over $\mathbb{Z}_p$, either U_r has finitely many zeros in $\mathbb{Z}_p$ or U_r vanishes identically (this is as a consequence of the Strassmann theorem (Theorem A.31)). From (5.15) it follows that $\mathcal{Z}_{\boldsymbol{u}}$ is the union of a finite set and some of the arithmetic progressions

$$\big\{(p-1)m + r : m \in \mathbb{N}\big\},$$

where $r \in \{0,\dots,p-2\}$.

It remains to prove the claim on the finiteness of $\mathcal{Z}_{\boldsymbol{u}}$. Suppose that $\mathcal{Z}_{\boldsymbol{u}}$ is infinite. Hence, by the previous reasoning, there exists $r \in \{0,\dots,p-2\}$ such that $u_{(p-1)m+r} = 0$ for every integer $m \ge 0$. Then, from Theorem 2.15, it follows easily that $\alpha_i^{p-1} = \alpha_j^{p-1}$ for some $i, j \in \{1,\dots,s\}$ with $i \ne j$. Thus $\boldsymbol{u}$ is degenerate, as claimed. □

Remark 5.11. Theorem 5.10 is optimal in the following sense. Let $\mathcal{S}$ be a subset of $\mathbb{N}$ that is the union of a finite set and finitely many arithmetic progressions. From Theorem 2.10 and Theorem 2.12, it follows that there exists a linear recurrence $\boldsymbol{u}$ over $\mathbb{Q}$ such that $\mathcal{Z}_{\boldsymbol{u}} = \mathcal{S}$.

Remark 5.12. If the hypothesis that $\operatorname{char}(\mathbb{K}) = 0$ is dropped, then Theorem 5.10 does not hold anymore. For instance, let $\mathbb{K} := \mathbb{F}_p(x,y)$ for some prime number p and formal variables x, y and let $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}}$ be the linear recurrence having power-sum representation

$$u_n = (x+y)^n - x^n - y^n \quad (n \in \mathbb{N}).$$

Then $\mathcal{Z}_{\boldsymbol{u}} = \{p^k : k \in \mathbb{N}\}$, which is not the union of a finite set and finitely many arithmetic progressions.

In light of Theorem 5.10, it is natural to pose the following problem.

Problem 5.1 (Skolem Problem)**.** Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$. Determine if there exists an integer $n \geq 0$ such that $u_n = 0$.

The decidability of the Skolem problem, that is, if there exists an algorithm solving the Skolem problem, is currently unknown. For linear recurrences of order at most 4, the Skolem problem is decidable thanks to the results of Mignotte, Shorey, Tijdeman [132], and Vereshchagin [190] (see also the result of Bacik [5] and the expository paper by Bilu [17]). However, for linear recurrences of order 5 the decidability of the Skolem problem is unknown [117]. Assuming the *Skolem conjecture* and the *p-adic Schanuel conjecture*, Bilu, Luca, Nieuwveld, Ouaknine, Purser, and Worrell [18] provided an algorithm that solves the Skolem problem for simple linear recurrences. Notably, their conjectural assumptions are needed only to ensure that the algorithm always terminates; when it does, it outputs all the zeros of the linear recurrence together with an unconditional certificate that all zeros have been found. An open source implementation of their algorithm is available online at the SKOLEM tool website [153].

Despite the decidability of the Skolem problem being an open question, it is possible to prove upper bounds for the number of zeros of a nondegenerate linear recurrence in a field of characteristic zero. Currently, the best general result is the following theorem due to Amoroso and Viada [2, Theorem 1.2].

Theorem 5.13. *Let $\mathbb{K}$ be a field of characteristic zero, let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{K}$ whose minimal polynomial has s pairwise distinct roots each with multiplicity at most m. Then $|\mathcal{Z}_{\boldsymbol{u}}| \leq (8s^m)^{8s^{6m}}$. In particular, the number of zeros of $\boldsymbol{u}$ is effectively upper bounded in terms of the order of $\boldsymbol{u}$.*

The case of second-order linear recurrences is pretty simple.

Theorem 5.14. *Let $\mathbb{K}$ be a field of characteristic zero and let $\boldsymbol{u}$ be a nondegenerate second-order linear recurrence over $\mathbb{K}$. Then $\boldsymbol{u}$ has at most one zero.*

Proof. Let $\mathbb{L}$ be the splitting field of the minimal polynomial of $\boldsymbol{u}$, and let $\alpha_1, \alpha_2 \in \mathbb{L}^*$ be the two (possibly equal) roots of $\boldsymbol{u}$. From Theorem 2.15 (cf. Example 2.2) it follows that there exist $c_1, c_2 \in \mathbb{L}^*$ such that either

(i) $u_n = \big(c_1 + c_2 n\big)\alpha_1^n$ for all integers $n \geq 0$, or

(ii) $u_n = c_1\alpha_1^n + c_2\alpha_2^n$ for all integers $n \geq 0$.

In case (i), if $u_n = 0$ for some integer $n \geq 0$, then $n = -c_1/c_2$. In case (i), if $u_m = u_n = 0$ for some integers $m, n \geq 0$, then $(\alpha_2/\alpha_1)^m = (\alpha_2/\alpha_1)^n = -c_1/c_2$, and so $(\alpha_2/\alpha_1)^{m-n} = 1$. Since $\boldsymbol{u}$ is nondegenerate, the ratio α_2/α_1 is not a root of unity. Hence, it must be $m = n$. The claim follows. □

5.5 Growth

This section investigates the growth of the terms of a linear recurrence over a number field, providing upper bounds, lower bounds, and asymptotic formulas.

5.5.1 Effective upper bound and asymptotic formula

Let $\mathbb{K}$ be a field whose algebraic closure is equipped with an absolute value $|\cdot|$ and let $\boldsymbol{u}$ be a nonzero linear recurrence over $\mathbb{K}$ with pairwise distinct roots $\alpha_1, \dots, \alpha_s$. Every root α_i such that $|\alpha_i| = \max_{j\in\{1,\dots,s\}} |\alpha_j|$ is called a *dominant root* of $\boldsymbol{u}$ (with respect to $|\cdot|$).

The next two theorems show that the dominant roots play a fundamental role in estimating the growth of a linear recurrence.

Theorem 5.15. *Let $\mathbb{K}$ be a field of characteristic zero whose algebraic closure is equipped with an absolute value $|\cdot|$ and let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$. Suppose that $\boldsymbol{u}$ has a nonzero dominant root α. Then*

$$|u_n| < Cn^{k-1}|\alpha|^n, \tag{5.16}$$

for every positive integer n, where $C > 0$ is an effectively computable constant depending only on $\boldsymbol{u}$, and k is the maximum of the multiplicities of the dominant roots of $\boldsymbol{u}$.

Proof. In light of Theorem 2.9, assume that $\boldsymbol{u}$ is reversible. Let $\alpha_1, \dots, \alpha_s$ be the pairwise distinct roots of $\boldsymbol{u}$, and let $k_1, \dots, k_s$ be their respective multiplicities. From Theorem 2.15 it follows that

$$u_n = \sum_{i=1}^{s} f_i(n)\,\alpha_i^n,$$

for every integer $n \geq 0$, where $f_1, \dots, f_s$ are nonzero polynomials such that $\deg(f_i) = k_i - 1$ for each $i \in \{1, \dots, t\}$. Up to reordering the roots, assume that $\alpha_1, \dots, \alpha_t$ $(t \leq s)$ are all the dominant roots of $\boldsymbol{u}$. For each $i \in \{1, \dots, s\}$, let c_i be the coefficient of x^{k_i-1} in $f_i(x)$. Hence

$$u_n = \sum_{i=1}^{s} c_i n^{k_i-1}\alpha_i^n + \sum_{j=1}^{s} \left(f_j(n) - c_j n^{k_j-1}\right)\alpha_j^n,$$

for each integer $n \geq 0$. Since $|\alpha_i| = |\alpha| > |\alpha_j|$ for each $i \in \{1, \dots, t\}$ and $j \in \{t+1, \dots, s\}$, the upper bound (5.16) follows easily. □

Theorem 5.16. *Let $\mathbb{K}$ be a field of characteristic zero whose algebraic closure is equipped with an absolute value $|\cdot|$ and let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{K}$. Suppose that $\boldsymbol{u}$ has a single nonzero dominant root α. Let k be the multiplicity of α. Then*

$$|u_n| = Cn^{k-1}|\alpha|^n + O\big(|\alpha|^{\delta n}\big), \tag{5.17}$$

as $n \to +\infty$, where $C > 0$, $\delta \in (0, 1)$, and the implied constant in the Big-O notation are effectively computable and depend only on $\boldsymbol{u}$.

Proof. Proceeding as in the proof of Theorem 5.15 yields that

$$u_n = c_1 n^{k-1}\alpha^n + \sum_{j=1}^{s} \left(f_j(n) - c_j n^{k_j-1}\right)\alpha_j^n,$$

for every integer $n \geq 0$. Since $|\alpha| > |\alpha_j|$ for each $j \in \{2, \dots, s\}$, the asymptotic (5.17) follows easily. □

5.5.2 Ineffective lower bound

Evertse [56] and van der Poorten and Schlickewei [188] (see also [186]) independently proved the following theorem (cf. [55, Theorem 2.3]), which shows that the upper bound provided by Theorem 5.15 is essentially the best possible.

Theorem 5.17. *Let $\mathbb{K}$ be a number field, let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{K}$, let α be one of the dominant roots of $\boldsymbol{u}$, and let $\varepsilon > 0$. Then*

$$|u_n| > |\alpha|^{(1-\varepsilon)n}$$

for every integer $n \geq C$, where $C > 0$ is a constant depending only on ε and $\boldsymbol{u}$.

Actually, Theorem 5.17 is a corollary of more general statements on S-unit equations, whose proofs are too advanced to be incluced here. Unfortunately, the proof of Theorem 5.17 is ineffective, meaning that it does not provide an explicit value for C in terms of ε and $\boldsymbol{u}$.

In fact, proving an effective lower bound for the absolute value of the terms of a linear recurrence is an open problem.

Problem 5.2. Let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{Z}$. Provide an effective lower bound for the absolute value of u_n. More precisely, provide an effectively computable function $f\colon \mathbb{N} \to \mathbb{N}$ such that $|u_n| > t$ for all integers $t > 0$ and $n > f(t)$.

Note that Problem 5.2 is at least as difficult as the decidability of the Skolem problem (Problem 5.1), since a solution to the former yields a solution to the latter.

5.5.3 Interlude: Lower bounds for linear forms in logarithms

The proof of the next theorem on lower bounds for terms of linear recurrences (Theorem 5.20) requires some results from the theory of *lower bounds for linear forms in logarithms*, which was initiated by Baker in the 1960s. Actually, the results stated here are stronger than what is strictly necessary at this stage, as they are required in a stronger form in Chapter 6.

For every algebraic number α, let $\mathrm{h}(\alpha)$ denote the *absolute logarithmic height* of α, which is defined as

$$\mathrm{h}(\alpha) := \frac{1}{d}\left(\log|a_0| + \sum_{i=1}^{d} \log\max\{1, |\alpha_i|\}\right),$$

where $a_0 \prod_{i=1}^{d}(x - \alpha_i) \in \mathbb{Z}[x]$, with $a_0 \in \mathbb{Z}^+$ and $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$, is the minimal polynomial of α over $\mathbb{Q}$.

Matveev [129] proved the following theorem, which provides an effective lower bound for a linear form of logarithms of algebraic numbers.

Theorem 5.18. *Let $\mathbb{K}$ be a number field, let $\alpha_1, \ldots, \alpha_n \in \mathbb{K}^*$, let $\ell_1, \ldots, \ell_n \in \mathbb{C}^*$ such that $\alpha_i = \exp(\ell_i)$ for each $i \in \{1, \ldots, n\}$, let $b_1, \ldots, b_n$ be integers, and let $\Lambda := \sum_{i=1}^{n} b_i \ell_i$. Then either $\Lambda = 0$ or*

$$|\Lambda| > \exp\bigl(-C^n D^2 A_1 \cdots A_n \log(\mathrm{e}D)\log(\mathrm{e}B)\bigr),$$

where $C > 1$ is an absolute constant, D is the degree of $\mathbb{K}$ over $\mathbb{Q}$,

$$A_i := \max\bigl\{D\,\mathrm{h}(\alpha_i), |\ell_i|, 0.16\bigr\}$$

for each $i \in \{1,\dots,n\}$, and $B := \max\bigl\{|b_1|,\dots,|b_n|\bigr\}$.

Proof. The claim follows easily from [129, Corollary 2.3]. □

It is more convenient to work with the following multiplicative version of Theorem 5.18.

Theorem 5.19. *Let $\mathbb{K}$ be a number field, let $\alpha_1,\dots,\alpha_n \in \mathbb{K}^*$, let $b_1,\dots,b_n$ be integers, and let $\Omega := \prod_{i=1}^n \alpha_i^{b_i} - 1$. Then either $\Omega = 0$ or*

$$|\Omega| > \exp\bigl(-C^n D^2 A_1 \cdots A_n \log(\mathrm{e}D)\log(enB)\bigr)\,, \tag{5.18}$$

where $C > 1$ is an absolute constant, D is the degree of $\mathbb{K}$ over $\mathbb{Q}$,

$$A_i := \max\bigl\{D\,\mathrm{h}(\alpha_i), |\log\alpha_i|, 0.16\bigr\}$$

for each $i \in \{1,\dots,n\}$, and $B := \max\bigl\{|b_1|,\dots,|b_n|\bigr\}$. Furthermore, if $\alpha_1,\dots,\alpha_n \in \mathbb{R}$, then either $\Omega = 0$ or

$$|\Omega| > \exp\bigl(-C^n D^2 A_1 \cdots A_n \log(\mathrm{e}D)\log(\mathrm{e}B)\bigr)\,. \tag{5.19}$$

Proof. Recall that $\log z = \sum_{n=1}^{\infty}(-1)^{n+1}(z-1)^n/n$ for every $z \in \mathbb{C}$ such that $|z-1| < 1$. Hence $|\log z| < 2|z-1|$ for every $z \in \mathbb{C}$ such that $|z-1| < 1/2$.

Put $z := \prod_{i=1}^n \alpha_i^{b_i}$ so that $\Omega = z - 1$. Suppose that $\Omega \neq 0$. Hence $z \neq 1$. If $|z-1| \geq 1/2$ then the claim follows. Hence, assume that $|z-1| < 1/2$. By the previous paragraph, it follows that

$$|\Omega| = |z-1| > \frac{|\log z|}{2}. \tag{5.20}$$

Note that, for every $x, y \in \mathbb{C}^*$,

$$\log(xy) = \log x + \log z + k_{x,y}\pi\mathrm{i}$$

for some $k_{x,y} \in \{-1,0,1\}$. Therefore, there exists an integer k such that $|k| \leq nB$ and

$$\Lambda := \log z = \log\left(\prod_{i=1}^{n} \alpha_i^{b_i}\right) = \sum_{i=1}^{n} b_i \log\alpha_i + k\pi\mathrm{i} = \sum_{i=1}^{n+1} b_i \log\alpha_i,$$

where $\alpha_{n+1} := -1$ and $b_{n+1} := k$. Note that $\Lambda \neq 0$ since $z \neq 1$. Thus by applying Theorem 5.18 with $n+1$ in place of n, and $\ell_i := \log\alpha_i$ for each $i \in \{1,\dots,n+1\}$, and by noticing that

$$A_{n+1} = \max\bigl\{D\,\mathrm{h}(-1), |\log(-1)|, 0.16\bigr\} = \pi,$$

it follows that

$$|\Lambda| > \exp\bigl(-C^n D^2 A_1 \cdots A_n \log(\mathrm{e}D)\log(enB)\bigr)\,, \tag{5.21}$$

for some absolute constant $C > 1$. Putting together (5.20) and (5.21) yields (5.18), as desired.

Finally, suppose that $\alpha_1, \dots, \alpha_n \in \mathbb{R}$. Thus there exists $h \in \{0, 1\}$ such that

$$\Lambda := \log z = \log\left(\prod_{i=1}^{n} \alpha_i^{b_i}\right) = \sum_{i=1}^{n} b_i \log|\alpha_i| + h\pi\mathrm{i} = \sum_{i=1}^{n+1} b_i \log\beta_i,$$

where $\beta_i := |\alpha_i|$ for each $i \in \{1, \dots, n\}$, while $\beta_{n+1} = -1$ and $b_{n+1} = h$. At this point, the bound (5.19) follows by applying Theorem 5.18 with $n+1$ and β_i in place of n and α_i, respectively, and $\ell_i := \log\beta_i$ for each $i \in \{1, \dots, n+1\}$. □

5.5.4 Effective lower bounds

The following result is an effective version of Theorem 5.17 for the special case of linear recurrences of order at most 2.

Theorem 5.20. *Let $\mathbb{K}$ be a number field, let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{K}$ of order at most 2, and let α be one of the dominant roots of $\boldsymbol{u}$. Then*

$$|u_n| > \frac{|\alpha|^n}{n^{C_1}} \tag{5.22}$$

for every integer $n > C_2$, where $C_1, C_2 > 0$ are effectively computable constants depending only on $\boldsymbol{u}$.

Proof. If $\boldsymbol{u}$ has a unique dominant root, then the claim follows from Theorem 5.16. Hence, it remains to prove the claim in the case in which $\boldsymbol{u}$ is a second-order linear recurrence with distinct roots α_1, α_2 such that $|\alpha_1| = |\alpha_2|$. From Theorem 2.15 it follows that

$$u_n = c_1\alpha_1^n + c_2\alpha_2^n$$

for every integer $n \geq 0$, where c_1, c_2 are nonzero algebraic numbers. Thus

$$|u_n| = |c_2|\,|\alpha_2|^n\,|\gamma_1\gamma_2^n - 1|, \tag{5.23}$$

for every integer $n \geq 0$, where $\gamma_1 := -c_1/c_2$ and $\gamma_2 := \alpha_1/\alpha_2$. As a consequence of Theorem 5.14, $\gamma_1\gamma_2^n \neq 1$ for all sufficiently large integers n. Thus (5.22) follows from Theorem 5.19 and (5.23). □

The next theorem provides an effective lower bound for the absolute values of almost all the terms of a linear recurrence over a number field.

Theorem 5.21. *Let $\mathbb{K}$ be a number field, let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{K}$, let α be one of the dominant roots of $\boldsymbol{u}$, let $\varepsilon > 0$, and let $X \geq 2$ be a real number. Suppose that $|\alpha| > 1$. Then*

$$|u_n| > |\alpha|^{(1-\varepsilon)n}$$

for every nonnegative integer $n \leq X$ but at most $C \log X$ exceptions, where $C > 0$ is an effectively computable constant depending only on ε and $\boldsymbol{u}$.

The proof of Theorem 5.21 needs the following preliminary lemma.

Lemma 5.22. *Let $\mathbb{K}$ be a number field, let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{K}$, let α be one of the dominant roots of $\boldsymbol{u}$, and let $X \geq Y \geq 0$ be real numbers. Suppose that $|\alpha| > 1$. Then, the number of integers $n \in [Y, X]$ such that*

$$|u_n| \leq |\alpha|^{X - C_1(X-Y)}$$

is at most C_2, where $C_1, C_2 > 0$ are effectively computable constants depending only on $\boldsymbol{u}$.

Proof. Throughout the proof, let $C_1, C_2, \ldots$ be effectively computable constants depending only on $\boldsymbol{u}$. Let $U \geq 0$ be a real number, put $Z := X - Y$, $M := \lceil Y \rceil$, and

$$\mathcal{E} := \big\{ n \in \mathbb{N} : n \leq Z,\, |u_{M+n}| \leq U \big\}.$$

Then, it suffices to prove that there exist constants $C_1, C_2 > 0$ such that if $|\mathcal{E}| > C_2$ then $U > |\alpha|^{X - C_1 Z}$. Without loss of generality, assume that $Z \geq 1$.

Let f be the minimal polynomial of $\boldsymbol{u}$, put $k := \deg(f)$ (note that $k > 0$ since $\boldsymbol{u}$ is nondegenerate), and let $\mathbb{L}$ be the splitting field of f over $\mathbb{K}$. By Theorem 5.13, there exists a constant $C_4 > 0$ such that every nondegenerate linear recurrence in $\mathbb{L}^{\mathbb{N}}$ with order not exceeding k has at most C_4 zeros. Put $C_2 := k + C_4$.

In light of Theorem 2.9, assume that $f(0) \neq 0$. Let $\alpha_1, \ldots, \alpha_s \in \mathbb{L}^*$, with $\alpha_1 := \alpha$, be the pairwise distinct roots of f, and let $k_1, \ldots, k_s$ be their respective multiplicities. From Theorem 2.15 it follows that

$$u_n = \sum_{i=1}^{s} f_i(n)\, \alpha_i^n$$

for every integer $n \geq 0$, where $f_1, \ldots, f_s \in \mathbb{L}[x]$ are nonzero polynomials such that $\deg(f_i) = k_i - 1$ for each $i \in \{1, \ldots, s\}$. Consequently

$$u_{M+n} = \sum_{i=1}^{s} \sum_{j=0}^{k_i - 1} \left(\frac{f_i^{(j)}(M)\, \alpha_i^M}{j!} \right) n^j \alpha_i^n, \tag{5.24}$$

where $f_i^{(j)}$ denotes the jth derivative of the polynomial f_i.

Let $t_1, \ldots, t_k$ be an enumeration of the k functions $n \mapsto n^j \alpha_i^n$, where $i \in \{1, \ldots, s\}$ and $j \in \{0, \ldots, k_i - 1\}$. For each $h \in \{1, \ldots, k\}$ and for all integer $n_1, \ldots, n_h$, define the determinant

$$D_h(n_1, \ldots, n_h) := \det\Big(\big(t_j(n_i)\big)_{1 \leq i,j \leq h} \Big).$$

Claim: there exist pairwise distinct integers $n_1, \ldots, n_k \in \mathcal{E}$ such that

$$D_k(n_1, \ldots, n_k) \neq 0.$$

Proceed by induction on h. First, since $|\mathcal{E}| > 1$, it is possible to pick $n_1 \in \mathcal{E} \setminus \{0\}$ such that $D_1(n_1) = t_1(n_1) \neq 0$. Suppose that, for a positive integer $h < k$, there are pairwise distinct $n_1, \ldots, n_h \in \mathcal{E}$ such that $D_h(n_1, \ldots, n_h) \neq 0$. Note that, by the Laplace expansion with

respect to the last column, the determinant $D_{h+1}(n_1,\dots,n_h,n)$ ($n\in\mathbb{N}$) is a nondegenerate linear recurrence over $\mathbb{L}$ of order at most k (in particular, it is nonzero since its power-sum expansion contains the term $t_{h+1}(n)$). Hence, since $|\mathcal{E}|>h+C_4$, it is possible to pick $n_{h+1}\in\mathcal{E}\setminus\{n_1,\dots,n_h\}$ such that $D_{h+1}(n_1,\dots,n_{h+1})\neq 0$. Thus the claim follows.

Plugging $n=n_1,\dots,n_k$ into (5.24) yields a linear system of k equations in the k unknowns $f_i^{(j)}(M)\,\alpha_i^M/j!$, where $i\in\{1,\dots,s\}$ and $j\in\{0,\dots,k_i-1\}$. Since α_1 is a root of $\boldsymbol{u}$, there exists $j_1\in\{0,\dots,k_1-1\}$ such that $f_1^{(j_1)}(M)\neq 0$. Without loss of generality, assume that $t_1(x)=x^{j_1}\alpha_1^x$. Hence, recalling that $\alpha_1=\alpha$, the Cramer rule gives that

$$\frac{f_1^{(j_1)}(M)\,\alpha^M}{j_1!}=\frac{1}{D_k(n_1,\dots,n_k)}\begin{vmatrix} u_{M+n_1} & t_2(n_1) & \cdots & t_k(n_1)\\ \vdots & \vdots & \ddots & \vdots\\ u_{M+n_s} & t_2(n_k) & \cdots & t_k(n_k)\end{vmatrix}. \tag{5.25}$$

Since $n_1,\dots,n_k\in\mathcal{E}$, it follows that

$$|u_{M+n_i}|\le U \quad\text{and}\quad |t_j(n_i)|\le Z^k|\alpha|^Z, \tag{5.26}$$

for every $i,j\in\{1,\dots,k\}$. Thus, from (5.25) and (5.26), it follows that

$$\left|\frac{f_i^{(j_1)}(M)\,\alpha^M}{j_1!}\right|\le\frac{k!\,U\big(Z^k|\alpha|^Z\big)^{k-1}}{|D_k(n_1,\dots,n_k)|}.$$

Moreover, since $|f_1^{(j_1)}(M)/(j_1!k!)|>C_5$ for some constant $C_5>0$, while $M\ge Y$,

$$U>C_5\,|D_k(n_1,\dots,n_k)|\,Z^{-k(k-1)}\,|\alpha|^{Y-(k-1)Z}. \tag{5.27}$$

Since $\alpha_1,\dots,\alpha_s$ are algebraic integers, it follows that $D_k(n_1,\dots,n_k)$ is an algebraic integer. Thus $\big|\mathrm{N}_{\mathbb{L}/\mathbb{Q}}(D_k(n_1,\dots,n_k))\big|\ge 1$. Moreover, since $n_1,\dots,n_k\in\mathcal{E}$, each algebraic conjugate of $D_k(n_1,\dots,n_k)$ over $\mathbb{Q}$ has absolute value not exceeding $k!Z^{k^2}A^{kZ}$, where A is the maximum of the absolute values of $\alpha_1,\dots,\alpha_k$ and their algebraic conjugates over $\mathbb{Q}$. Hence

$$|D_k(n_1,\dots,n_k)|\ge(k!Z^{k^2}A^{kZ})^{1-[\mathbb{L}:\mathbb{Q}]}\ge(k!Z^{k^2}A^{kZ})^{1-k!}. \tag{5.28}$$

Putting together (5.27) and (5.28), it follows that

$$U>C_5(k!)^{-(k!-1)}Z^{-k(k-1)-k^2(k!-1)}A^{-k(k!-1)Z}\,|\alpha|^{Y-(k-1)Z}>|\alpha|^{Y-C_6Z},$$

for some constant $C_6>0$. Hence, letting $C_1:=C_6+1$, gives that $U>|\alpha|^{X-C_1Z}$, as desired. □

Proof of Theorem 5.21. Let C_1 and C_2 be the constants of Lemma 5.22. Without loss of generality, assume that $\varepsilon<C_1$. Let $C_3:=1-\varepsilon/C_1$, $L:=\lfloor\log X/\log(1/C_3)\rfloor$, $X_0:=X$, and $X_{i+1}:=C_3X_i$ for every integer $i\ge 0$. Note that $C_3\in(0,1)$, $L\ge 0$, $X_i>X_{i+1}$, and

$$X_i-C_1(X_i-X_{i+1})=(1-\varepsilon)X_i,$$

for every integer $i \geq 0$. Hence, from Lemma 5.22, it follows that

$$\begin{aligned}
&\left|\left\{n \in \mathbb{N} : n \leq X,\, |u_n| \leq |\alpha|^{(1-\varepsilon)n}\right\}\right| \\
&\qquad \leq 1 + \sum_{i=0}^{L} \left|\left\{n \in \mathbb{N} : X_{i+1} \leq n \leq X_i,\, |u_n| \leq |\alpha|^{(1-\varepsilon)X_i}\right\}\right| \\
&\qquad \leq 1 + \sum_{i=0}^{L} \left|\left\{n \in \mathbb{N} : X_{i+1} \leq n \leq X_i,\, |u_n| \leq |\alpha|^{X_i - C_1(X_i - X_{i+1})}\right\}\right| \\
&\qquad \leq 1 + C_2(1+L) \leq 1 + C_2 + \frac{C_2 \log X}{\log(1/C_3)} \leq C \log X,
\end{aligned}$$

where $C > 0$ is a an effectively computable constant depending only on ε and $\boldsymbol{u}$. The claim follows. □

5.6 Factorization of generalized power sums

Linear recurrences over a field of characteristic zero are generalized power sums, and vice versa (Theorem 2.15); while the product of linear recurrences is still a linear recurrence (Theorem 2.34). This section investigates how generalized power sums can be factored into the product of other generalized power sums.

For every field of characteristic zero $\mathbb{K}$ and for each subgroup Γ of $\mathbb{K}^*$, let

$$\mathfrak{S}_{\mathbb{K}}(\Gamma) := \left\{ \left(\textstyle\sum_{i=1}^{s} f_i(n)\, \alpha_i^n \right)_{n \in \mathbb{N}} : s \in \mathbb{Z}^+,\, f_1, \ldots, f_s \in \mathbb{K}[x],\, \alpha_1, \ldots, \alpha_s \in \Gamma \right\} \tag{5.29}$$

be the set of generalized powers sums with coefficients in $\mathbb{K}[x]$ and roots in Γ. It follows easily that $\mathfrak{S}_{\mathbb{K}}(\Gamma)$ equipped with termise addition and termwise product is a subring of the ring of sequences $\mathbb{K}^{\mathbb{N}}$.

Theorem 5.23. *Let $\mathbb{K}$ be a field of characteristic zero, let Γ be a finitely-generated torsion-free subgroup of $\mathbb{K}^*$, and let $\gamma_1, \ldots, \gamma_s$ be multiplicatively independent generators of Γ. Then*

(i) the ring $\mathfrak{S}_{\mathbb{K}}(\Gamma)$ is isomorphic to $\mathbb{K}[x, y_1, y_1^{-1} \ldots, y_s, y_s^{-1}]$, where $x, y_1, \ldots, y_s$ are formal variables, via the unique ring homomorphism Φ such that

$$\Phi\big((n)_{n\in\mathbb{N}}\big) = x \quad \text{and} \quad \Phi\big((\gamma_i^n)_{n\in\mathbb{N}}\big) = y_i, \tag{5.30}$$

for each $i \in \{1, \ldots, s\}$;

(ii) $\mathfrak{S}_{\mathbb{K}}(\Gamma)$ is a unique factorization domain;

(iii) each unit of $\mathfrak{S}_{\mathbb{K}}(\Gamma)$ is of the form $(c\,\alpha^n)_{n\in\mathbb{N}}$, where $c \in \mathbb{K}^*$ and $\alpha \in \Gamma$;

(iv) each irreducible element of $\mathfrak{S}_{\mathbb{K}}(\Gamma)$ is equal to a unit multiplied by $\Phi^{-1}(f)$, for some irreducible polynomial $f \in \mathbb{K}[x, y_1, \ldots, y_s]$ with $f \notin \{y_1, \ldots, y_s\}$.

Proof. Let $G := \langle y_1, \dots, y_s \rangle$, let $\mathcal{R} := \mathbb{K}[x, y_1, \dots, y_s]$, and let $\mathcal{R}' := \mathbb{K}[x, y_1, y_1^{-1}, \dots, y_s, y_s^{-1}]$. Since Γ is a torsion-free group with multiplicatively independent generators $\gamma_1, \dots, \gamma_s$, there exists a unique group isomorphism $\phi\colon \Gamma \to G$ such that $\phi(\gamma_i) = y_i$ for each $i \in \{1, \dots, s\}$. From (5.29) every $\boldsymbol{u} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$ can be written as

$$\boldsymbol{u} = \Big(\sum_{i=1}^{s} f_i(n)\, \alpha_i^n \Big)_{n \in \mathbb{N}}, \tag{5.31}$$

where $f_1, \dots, f_s \in \mathbb{K}[x]$ and $\alpha_1, \dots, \alpha_s \in \Gamma$. Moreover, thanks to Theorem 2.15, the representation (5.31) is unique except for the order of the roots α_i such that the corresponding polynomials f_i are nonzero.

Therefore, it is well defined the map $\Phi\colon \mathfrak{S}_{\mathbb{K}}(\Gamma) \to \mathcal{R}'$ such that

$$\Phi(\boldsymbol{u}) := \sum_{i=1}^{s} f_i(x)\, \phi(\alpha_i),$$

for every $\boldsymbol{u} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$ of the form (5.31). Since ϕ is a group homomorphism, it follows easily that Φ is a ring homomorphism and in fact the unique ring homomorphism that satisfies (5.30). Moreover, again by the considerations on (5.29) and Theorem 2.15, the map Φ is injective and surjective. This proves (i).

Since $\mathbb{K}$ is a field, the polynomial ring $\mathcal{R}$ is a unique factorization domain. Moreover, since $\mathcal{R}'$ is the localization of $\mathcal{R}$ with respect to the multiplicatively closed set G, it follows that $\mathcal{R}'$ is a unique factorization domain. This and (i) imply (ii).

At last, since $\mathcal{R}'$ is the localization of $\mathcal{R}$ with respect to the G, the units of $\mathcal{R}'$ are generated by the units of $\mathcal{R}$ and the elements of G, while the irreducible elements of $\mathcal{R}'$ are the irreducible elements of $\mathcal{R}$ except those in G. These facts and (i) imply (iii) and (iv). □

Note that, in Theorem 5.23, the hypothesis that Γ is torsion-free is not a significant restriction for most applications, thanks to Remark 5.7.

The next theorem shows that, in the ring of generalized power sums, if a generalized power sum $\boldsymbol{u}$ is divisible by a generalized power sum $\boldsymbol{v}$, then the roots of the quotient belong to the group generated by the roots of $\boldsymbol{u}$ and $\boldsymbol{v}$. For the sake of brevity, for every generalized power sum $\boldsymbol{u}$, let $\Gamma_{\boldsymbol{u}}$ be the multiplicative group generated by the roots of $\boldsymbol{u}$.

Theorem 5.24. *Let $\mathbb{K}$ be a field of characteristic zero and let $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in \mathfrak{S}_{\mathbb{K}}(\mathbb{K}^*)$. Suppose that $\boldsymbol{u} = \boldsymbol{v}\boldsymbol{w}$. Then $\Gamma_{\boldsymbol{w}} \subseteq \langle \Gamma_{\boldsymbol{u}}, \Gamma_{\boldsymbol{v}} \rangle$.*

Proof. Let $\Gamma := \langle \Gamma_{\boldsymbol{u}}, \Gamma_{\boldsymbol{v}}, \Gamma_{\boldsymbol{w}} \rangle$. The proof begins with some preliminary facts on Γ. Since Γ is a finitely-generated commutative group, $\Gamma \cong (\mathbb{Z}/d\mathbb{Z}) \times \mathbb{Z}^s$ for some integers $d > 0$ and $s \geq 0$. Hence, from the lexicographical order on $\mathbb{Z}^s$, it is possible to define a strict preorder on Γ that is invariant with respect to the group multiplication. Explicitly, let ζ and $g_1, \dots, g_s$ be multiplicatively independent generators of the torsion and torsion-free parts of Γ, respectively. Define a binary relation "$<$" on Γ by writing

$$\zeta^{a_0} g_1^{a_1} \cdots g_s^{a_s} < \zeta^{b_0} g_1^{b_1} \cdots g_s^{b_s}$$

if and only if there exists $i \in \{1, \dots, s\}$ such that $a_i < b_i$ and $a_j = b_j$ for every positive integer $j < i$ (note that a_0 and b_0 play no role). It is easy to prove that

(i) $\alpha \not< \alpha$;

(ii) $\alpha < \beta$ and $\beta < \gamma$ implies that $\alpha < \gamma$;

(iii) $\alpha < \beta$ or $\beta < \alpha$ or α/β is a power of ζ, with each alternative excluding the others;

(iv) $\alpha < \beta$ implies that $\alpha\gamma < \beta\gamma$;

for every $\alpha, \beta, \gamma \in \Gamma$. In particular, from (i) and (ii), it follows that every nonempty finite subset $\mathcal{S} \subseteq \Gamma$ has a (possibly not unique) *maximal element*, that is, an element $\alpha \in \mathcal{S}$ such that $\alpha < \beta$ implies that $\beta \notin \mathcal{S}$, for every $\beta \in \Gamma$. Moreover, if G is a torsion-free subgroup of Γ, then (iii) implies that

(v) $\alpha < \beta$ or $\beta < \alpha$ or $\alpha = \beta$, with each alternative excluding the others;

for every $\alpha, \beta \in G$. Consequently, from (v) it follows that every nonempty finite subset $\mathcal{S} \subseteq G$ has a unique maximal element.

Now to the proof of the theorem. First, assume that $\Gamma_{\boldsymbol{v}}$ is torsion-free. Then there exists a unique maximal root β of $\boldsymbol{v}$. For the sake of contradiction, suppose that $\Gamma_{\boldsymbol{w}}$ is not contained in $\langle \Gamma_{\boldsymbol{u}}, \Gamma_{\boldsymbol{v}} \rangle$. Hence, there exists a root γ of $\boldsymbol{w}$ such that $\gamma \notin \langle \Gamma_{\boldsymbol{u}}, \Gamma_{\boldsymbol{v}} \rangle$. Assume that γ is a maximal root of $\boldsymbol{w}$ such that $\gamma \notin \langle \Gamma_{\boldsymbol{u}}, \Gamma_{\boldsymbol{v}} \rangle$. Note that γ is not necessarily the unique maximal root of $\boldsymbol{w}$ with such a property, but this is not a problem.

Suppose that there exist a root β_0 of $\boldsymbol{v}$ and a root γ_0 of $\boldsymbol{w}$ such that $\beta_0 \neq \beta$ and $\beta_0\gamma_0 = \beta\gamma$. Since $\beta_0 \neq \beta$ and β is the unique maximal root of $\boldsymbol{v}$, from (v) it follows that $\beta_0 < \beta$. Hence, multiplying by γ, from (iv) it follows that $\beta_0\gamma < \beta\gamma = \beta_0\gamma_0$. In turn, multiplying by β_0^{-1}, from (iv) it follows that $\gamma < \gamma_0$. Thus, from the maximality of γ, it follows that $\gamma_0 \in \langle \Gamma_{\boldsymbol{u}}, \Gamma_{\boldsymbol{v}} \rangle$. Hence $\gamma = \beta^{-1}\beta_0\gamma_0 \in \langle \Gamma_{\boldsymbol{u}}, \Gamma_{\boldsymbol{v}} \rangle$, which is a contradiction.

Therefore, $\beta_0\gamma_0 \neq \beta\gamma$ for every root $\beta_0 \neq \beta$ of $\boldsymbol{v}$ and every root γ_0 of $\boldsymbol{w}$. This implies that in the product $\boldsymbol{vw}$ the term containing the root $\beta\gamma$ does not cancel out. Thus, since $\boldsymbol{u} = \boldsymbol{vw}$, the product $\beta\gamma$ is a root of $\boldsymbol{u}$. Consequently $\gamma \in \langle \Gamma_{\boldsymbol{u}}, \Gamma_{\boldsymbol{v}} \rangle$, which is again contradiction. This proves that $\Gamma_{\boldsymbol{w}} \subseteq \langle \Gamma_{\boldsymbol{u}}, \Gamma_{\boldsymbol{v}} \rangle$, as desired.

Now suppose that $\Gamma_{\boldsymbol{v}}$ is not torsion-free. Let d be the order of the torsion part of $\Gamma_{\boldsymbol{v}}$, so that $\Gamma_{\boldsymbol{v}}$ contains a primitive dth root of unity ζ_d. For every $\boldsymbol{z} \in \mathbb{K}^{\mathbb{N}}$ and every group G, let $\boldsymbol{z}^{(d)} := (z_{dn})_{n\in\mathbb{N}}$ and $G^{(d)} := \{g^d : g \in G\}$. Note that $\Gamma_{\boldsymbol{z}^{(d)}} = \Gamma_{\boldsymbol{z}}^{(d)}$ for every $\boldsymbol{z} \in \mathfrak{S}_{\mathbb{K}}(\mathbb{K}^*)$. From $\boldsymbol{u} = \boldsymbol{vw}$ it follows that $\boldsymbol{u}^{(d)} = \boldsymbol{v}^{(d)}\boldsymbol{w}^{(d)}$. Since $\Gamma_{\boldsymbol{v}}^{(d)}$ is torsion-free, the previous part of the proof implies that $\Gamma_{\boldsymbol{w}}^{(d)} \subseteq \langle \Gamma_{\boldsymbol{u}}^{(d)}, \Gamma_{\boldsymbol{v}}^{(d)} \rangle$. This means that for every $\gamma \in \Gamma_{\boldsymbol{w}}$ there exist $\alpha \in \Gamma_{\boldsymbol{u}}$ and $\beta \in \Gamma_{\boldsymbol{v}}$ such that $\gamma^d = \alpha^d\beta^d$. Hence $\gamma = \alpha\beta\zeta_d^k \in \langle \Gamma_{\boldsymbol{u}}, \Gamma_{\boldsymbol{v}} \rangle$ for some integer $k \geq 0$. Therefore $\Gamma_{\boldsymbol{w}} \subseteq \langle \Gamma_{\boldsymbol{u}}, \Gamma_{\boldsymbol{v}} \rangle$, as claimed. □

The next result is an upper bound on the order of each divisor of a given generalized power sum. Let $\deg_y(f)$ denote the degree of the variable y in the multivariate Laurent polynomial f, and set $\deg_y(f) := 0$ if y does not appear in f.

Theorem 5.25. *Let $\mathbb{K}$ be a field of characteristic zero, let Γ be a finitely-generated torsion-free subgroup of $\mathbb{K}^*$, and let $\boldsymbol{u}, \boldsymbol{v} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$ such that $\boldsymbol{u} \neq \boldsymbol{0}$ and $\boldsymbol{u}$ is divisible by $\boldsymbol{v}$ in $\mathfrak{S}_{\mathbb{K}}(\Gamma)$. Then the order of $\boldsymbol{v}$ is at most equal to*

$$\prod_{i=1}^{s} \Big(\deg_{y_i}(\Phi(\boldsymbol{u})) + \deg_{y_i^{-1}}(\Phi(\boldsymbol{u})) + 1 \Big),$$

where $y_1, \ldots, y_s$ and Φ are as in Theorem 5.23.

Proof. Employing Theorem 5.23, identify $\mathfrak{S}_{\mathbb{K}}(\Gamma)$ with $\mathbb{K}[x, y_1, y_1^{-1}, \ldots, y_s, y_s^{-1}]$ via the isomorphism Φ. Moreover, put $\mathsf{d}_i^+(\boldsymbol{s}) := \deg_{y_i}(\boldsymbol{s})$ and $\mathsf{d}_i^-(\boldsymbol{s}) := -\deg_{y_i^{-1}}(\boldsymbol{s})$ for each $i \in \{1, \ldots, s\}$ and for every nonzero $\boldsymbol{s} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$. Note that the order of $\boldsymbol{v}$ is at most equal to the number N of monomials $y_1^{a_1} \cdots y_s^{a_s}$ where the exponents $a_1, \ldots, a_s$ are integers such that $\mathsf{d}_i^-(\boldsymbol{v}) \leq a_i \leq \mathsf{d}_i^+(\boldsymbol{v})$ for each $i \in \{1, \ldots, s\}$. Furthermore, by a simple counting argument, it follows that

$$N = \prod_{i=1}^{s} \big(\mathsf{d}_i^+(\boldsymbol{v}) - \mathsf{d}_i^-(\boldsymbol{v}) + 1 \big). \tag{5.32}$$

Since $\boldsymbol{u}$ is divisible by $\boldsymbol{v}$, there exists $\boldsymbol{w} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$ such that $\boldsymbol{u} = \boldsymbol{v}\boldsymbol{w}$. Hence, for each $i \in \{1, \ldots, s\}$,

$$\mathsf{d}_i^+(\boldsymbol{u}) = \mathsf{d}_i^+(\boldsymbol{v}) + \mathsf{d}_i^+(\boldsymbol{w}) \quad \text{and} \quad \mathsf{d}_i^-(\boldsymbol{u}) = \mathsf{d}_i^-(\boldsymbol{v}) + \mathsf{d}_i^-(\boldsymbol{w}),$$

which in turn imply that

$$\mathsf{d}_i^+(\boldsymbol{v}) - \mathsf{d}_i^-(\boldsymbol{v}) = \big(\mathsf{d}_i^+(\boldsymbol{u}) - \mathsf{d}_i^-(\boldsymbol{u}) \big) - \big(\mathsf{d}_i^+(\boldsymbol{w}) - \mathsf{d}_i^-(\boldsymbol{w}) \big) \leq \mathsf{d}_i^+(\boldsymbol{u}) - \mathsf{d}_i^-(\boldsymbol{u}). \tag{5.33}$$

Hence, putting together (5.32) and (5.33), the claim follows. □

5.7 Hadamard quotient theorem

The product of two linear recurrences is itself a linear recurrence (Theorem 2.34). A natural question is whether this result can be somehow inverted, that is, under which conditions the ratio of two linear recurrences is a linear recurrence. This problem has a long history (see the bibliographical notes). By Remark 5.1, a necessary condition for the ratio to be a linear recurrence is that its terms belong to a finitely-generated ring. Pisot conjectured that this condition is in fact sufficient. van der Poorten [189] settled this conjecture by proving the *Hadamard quotient theorem* below. (It is slightly more convenient to work with generalized power sums instead of linear recurrences, so that it is possible to employ the results of Section 5.6. This is not a restriction in light of Theorem 2.9.)

Given two sequences $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{K}^{\mathbb{N}}$, let $\boldsymbol{u}/\boldsymbol{v}$ denote the sequence $(u_n/v_n)_{n \in \mathbb{N}}$, by tacitly assuming that $v_n \neq 0$ for every integer $n \geq 0$.

Theorem 5.26 (Hadamard quotient theorem)**.** *Let $\mathbb{K}$ be a field of characteristic zero, let $\mathcal{R}$ be a finitely-generated subring of $\mathbb{K}$, and let $\boldsymbol{u}, \boldsymbol{v} \in \mathfrak{S}_{\mathbb{K}}(\mathbb{K}^*)$. If $u_n/v_n \in \mathcal{R}$ for every integer $n \geq 0$, then $\boldsymbol{u}/\boldsymbol{v} \in \mathfrak{S}_{\mathbb{K}}(\mathbb{K}^*)$.*

The proof of Theorem 5.26 involves some ingenious constructions of p-adic nature and it is not provided here.

Corollary 5.27. *Let $\mathbb{K}$ be a field of characteristic zero, let Γ be a subgroup of $\mathbb{K}^*$, and let $\boldsymbol{u}, \boldsymbol{v} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$. Then the terms of the sequence $\boldsymbol{u}/\boldsymbol{v}$ belong to a finitely-generated subring of $\mathbb{K}$ if and only if $\boldsymbol{u}$ is divisible by $\boldsymbol{v}$ in the ring $\mathfrak{S}_{\mathbb{K}}(\Gamma)$.*

Proof. Suppose that the terms of $\boldsymbol{u}/\boldsymbol{v}$ belong to a finitely-generated subring of $\mathbb{K}$. From Theorem 5.26 it follows that $\boldsymbol{u} = \boldsymbol{v}\boldsymbol{w}$ for some $\boldsymbol{w} \in \mathfrak{S}_{\mathbb{K}}(\mathbb{K}^*)$. Then, since $\boldsymbol{u}, \boldsymbol{v} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$, Theorem 5.24 implies that $\boldsymbol{w} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$. Thus $\boldsymbol{u}$ is divisible by $\boldsymbol{v}$ in the ring $\mathfrak{S}_{\mathbb{K}}(\Gamma)$.

Vice versa, if $\boldsymbol{u}$ is divisible by $\boldsymbol{v}$ in the ring $\mathfrak{S}_{\mathbb{K}}(\Gamma)$, then $\boldsymbol{u}/\boldsymbol{v} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$. Hence, by Remark 5.1, the terms of $\boldsymbol{u}/\boldsymbol{v}$ belong to finitely-generated subring of $\mathbb{K}$. □

Note that, by Remark 5.7 and Theorem 5.23, it is possible to verify the divisibility condition in Corollary 5.27 in a purely algebraic way.

The following important theorem is due to Corvaja and Zannier [41] and shows that in Theorem 5.26 the condition "for every integer $n \geq 0$" can be relaxed to "for infinitely many integers $n \geq 0$" provided that the conclusion is slightly changed.

Theorem 5.28. *Let $\mathbb{K}$ be a field of characteristic zero, let Γ be a torsion-free subgroup of $\mathbb{K}^*$, let $\mathcal{R}$ be a finitely-generated subring of $\mathbb{K}$, and let $\boldsymbol{u}, \boldsymbol{v} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$. If $u_n/v_n \in \mathcal{R}$ for infinitely many integers $n \geq 0$, then there exists a nonzero polynomial $g(x) \in \mathbb{K}[x]$ such that $\big(g(n)u_n/v_n\big)_{n\in\mathbb{N}}$ and $\big(v_n/g(n)\big)_{n\in\mathbb{N}}$ belong to $\mathfrak{S}_{\mathbb{K}}(\Gamma)$.*

Remark 5.29. Corvaja and Zannier [41] stated and proved Theorem 5.28 for the field of complex numbers, but the case of an arbitrary field of characteristic zero $\mathbb{K}$ follows easily. Indeed, by Remark 5.1, assume that $\mathbb{K}$ is a finitely-generated extension of $\mathbb{Q}$, and then embed $\mathbb{K}$ into $\mathbb{C}$.

Remark 5.30. In light of Remark 5.7, in Theorem 5.28 the hypothesis that Γ is torsion-free is not a loss of generality.

Remark 5.31. The polynomial g in Theorem 5.28 can be effectively determined [41, p. 434]. If $v_n = \sum_{i=1}^{t} g_i(n)\,\beta_i^n$ for every integer $n \geq 0$, where $g_1, \ldots, g_t \in \mathbb{K}[x]$ are nonzero polynomials and $\beta_1, \ldots, \beta_t \in \Gamma$, then g can be taken as $\gcd(g_1, \ldots, g_t)$.

Remark 5.32. There are cases in which the polynomial $g(x)$ of Theorem 5.28 cannot be constant. For example, if $\mathbb{K} = \mathbb{Q}$, $\mathcal{R} = \mathbb{Z}$, $u_n = 2^n$ and $v_n = n$ for every integer $n \geq 0$, then it must be $g(x) = ax$ for an arbitrary $a \in \mathbb{Q}^*$.

The proof of Theorem 5.28 makes a clever and heavy use of the *Schmidt subspace theorem*, and it is too advanced to be included here.

Let $\mathcal{S}$ be a set of nonnegative integers. The *natural density*, *upper density*, and *lower density* of $\mathcal{S}$ are the limit (if it exists), limit superior, and limit inferior of $\big|\mathcal{S} \cap [0, X]\big|/X$ as $X \to +\infty$, respectively.

Theorem 5.33. *Let $\mathbb{K}$ be a number field, let Γ be a torsion-free subgroup of $\mathbb{K}^*$, let $\mathcal{R}$ be a finitely-generated subring of $\mathbb{K}$, and let $\boldsymbol{u}, \boldsymbol{v} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$. Suppose that $\boldsymbol{u}/\boldsymbol{v} \notin \mathfrak{S}_{\mathbb{K}}(\Gamma)$. Then the set of integers $n \geq 0$ such that $u_n/v_n \in \mathcal{R}$ has natural density zero.*

The proof of Theorem 5.33 requires a lemma regarding the multiplicative order of a fixed algebraic number modulo some prime ideals.

Lemma 5.34. *Let $\mathbb{K}$ be a number field, let $\alpha \in \mathbb{K}^*$ with α not a root of unity, let $\kappa \in (0,1)$, let $\mathcal{P}$ be the set of prime numbers p such that, for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ lying above p, the multiplicative order of α modulo $\mathfrak{p}$ is less than p^κ, and let $X \geq 2$ be a real number. Then*

$$\big|\mathcal{P} \cap [1, X]\big| < \frac{CX^{2\kappa}}{\log X},$$

where $C > 0$ is a constant depending only on α and $\mathbb{K}$.

Proof. It is well known that there exist $\beta \in \mathcal{O}_{\mathbb{K}}$ and a positive integer b such that $\alpha = \beta/b$. Let p be a prime number, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{\mathbb{K}}$ lying above p, and let n be a positive integer. If $\alpha^n \equiv 1 \pmod{\mathfrak{p}}$ then $\beta^n - b^n$ is a nonzero algebraic integer in $\mathfrak{p}$, and consequently $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\beta^n - b^n)$ is a nonzero integer that is divisible by p. Moreover,

$$\big|\mathrm{N}_{\mathbb{Q}(\beta)/\mathbb{Q}}(\beta^n - b^n)\big| \leq \prod_{\beta'} \big|(\beta')^n - b^n\big| \leq \prod_{\beta'} \big(|\beta'|^n + b^n\big) \leq \prod_{\beta'} \big(\max\{|\beta'|, b\}\big)^n,$$

where the product is over all the algebraic conjugates β' of β over $\mathbb{Q}$. Thus

$$\big|\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\beta^n - b^n)\big| = \big|\mathrm{N}_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\beta^n - b^n)\big|^{[\mathbb{K}\,:\,\mathbb{Q}(\beta)]} \leq e^{C_1 n},$$

where $C_1 > 0$ is a constant depending only on α and $\mathbb{K}$. Hence, it follows that

$$\prod_{\substack{p \in \mathcal{P} \\ p \leq X}} p \leq \prod_{n \leq X^\kappa} \big|\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\beta^n - b^n)\big| \leq \exp\Big(C_1 \sum_{n \leq X^\kappa} n\Big) \leq \exp(C_1 X^{2\kappa}). \tag{5.34}$$

Let $N := \big|\mathcal{P} \cap [1, X]\big|$, and let $(p_i)_{i \in \mathbb{Z}^+}$ be the monotone increasing sequence of prime numbers. Without loss of generality, assume that $N \geq 2$. From the prime number theorem (Corollaries A.38 and A.39), it follows that

$$\prod_{\substack{p \in \mathcal{P} \\ p \leq X}} p \geq \prod_{i=1}^{N} p_i > \mathrm{e}^{C_2 p_N} > \mathrm{e}^{C_3 N \log N}, \tag{5.35}$$

where $C_2, C_3 > 0$ are absolute constants. Therefore, from (5.34) and (5.35), it follows that

$$C_3 N \log N < C_1 X^{2\kappa},$$

and thus $N < CX^{2\kappa}/\log X$, where $C > 0$ is a constant that depends only on α and $\mathbb{K}$. □

Proof of Theorem 5.33. Let $\mathcal{N}$ be the set of integers $n \geq 0$ such that $u_n/v_n \in \mathcal{R}$. If $\mathcal{N}$ is finite, then the claim follows. Assume that $\mathcal{N}$ is infinite. Then Theorem 5.28 implies that there exists a nonzero polynomial $g(x) \in \mathbb{K}[x]$ such that the sequence $\widetilde{\boldsymbol{u}} \in \mathbb{K}^{\mathbb{N}}$, defined by $\widetilde{u}_n := g(n)u_n/v_n$ for every integer $n \geq 0$, belongs to $\mathfrak{S}_{\mathbb{K}}(\Gamma)$. Furthermore, it follows that $\mathcal{N}$ is the set of integers $n \geq 0$ such that $\widetilde{u}_n/g(n) \in \mathcal{R}$.

Since $\widetilde{\boldsymbol{u}} \in \mathfrak{S}_{\mathbb{K}}(\Gamma)$, it follows that

$$\widetilde{u}_n = \sum_{i=1}^{s} f_i(n)\,\alpha_i^n, \tag{5.36}$$

for every integer $n \geq 0$, where $f_1, \ldots, f_s \in \mathbb{K}[x]$ are nonzero polynomials and $\alpha_1, \ldots, \alpha_s \in \Gamma$. The fact that $\big(\widetilde{u}_n/g(n)\big)$ is not a linear recurrence implies that g does not divide $\gcd(f_1, \ldots, f_s)$. In particular, it follows that g is nonconstant. Moreover, factoring out $\gcd(g, f_1, \ldots, f_s)$, assume that $\gcd(g, f_1, \ldots, f_s) = 1$. By Bézout's lemma, this implies that there exist $a_0, \ldots, a_s \in \mathbb{K}[x]$ such that

$$a_0 g + a_1 f_1 + \cdots + a_s f_s = 1. \tag{5.37}$$

Pick a finite set of absolute values S, containing all the archimedian absolute values, and such that $\mathcal{R} \subseteq \mathcal{O}_S$, $\alpha_1, \ldots, \alpha_s \in \mathcal{O}_S^*$, and the polynomials $a_0, \ldots, a_s$, $f_1, \ldots, f_s$, and g all belong to $\mathcal{O}_S[x]$.

Let $\mathcal{P}$ be the set of prime numbers p such that

(i) p is not a S-unit;

(ii) p splits completely in $\mathcal{O}_{\mathbb{K}}$;

(iii) for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_{\mathbb{K}}$ lying above p, the multiplicative order modulo $\mathfrak{p}$ of each ratio α_i/α_j, where $i, j \in \{1, \ldots, s\}$ and $i \neq j$, is at least $p^{1/4}$.

From a corollary of the *Chebotarev density theorem* (Corollary A.40), and from Lemma 5.34, it follows that there exist constants $C_1, C_2 > 0$ such that

$$\big|\mathcal{P} \cap [1, X]\big| > \frac{C_1 X}{\log X}, \tag{5.38}$$

for every real number $X > C_2$.

Fix an arbitrary $\varepsilon > 0$. It suffices to prove that the upper density of $\mathcal{N}$ is less than ε. In light of (5.38), fix two sufficiently large real numbers $X > Y$, depending only on $\boldsymbol{u}$, $\boldsymbol{v}$, $\mathbb{K}$, and ε, such that

$$\sum_{n \geq Y} \frac{1}{n^{1+1/(4s)}} < \frac{\varepsilon}{4} \tag{5.39}$$

and

$$\prod_{\substack{p \in \mathcal{P} \\ Y \leq p \leq X}} \left(1 - \frac{1}{p}\right) < \frac{\varepsilon}{2}. \tag{5.40}$$

By enlarging $\mathbb{K}$, assume that all the roots of g belong to $\mathbb{K}$. Let $z \in \mathbb{K}$ be a root of g. For each $p \in \mathcal{P}$, pick a prime ideal $\mathfrak{p}_p$ of $\mathcal{O}_S$ lying above p, and pick $z_p \in \mathbb{Z}$ such that $z \equiv z_p \pmod{\mathfrak{p}_p}$. Split $\mathcal{N}$ into two subsets:

$$\mathcal{N}' := \big\{n \in \mathcal{N} : n \equiv z_p \pmod{p} \text{ for some } p \in \mathcal{P} \cap [Y, X]\big\}$$
$$\mathcal{N}'' := \mathcal{N} \setminus \mathcal{N}'.$$

Claim: the upper density of $\mathcal{N}'$ is less than $\varepsilon/2$. Let $n \in \mathcal{N}'$. Then there exist $p \in \mathcal{P}$ and an integer $m \geq 0$ such that $p \geq Y$ and $n = z_p + mp$. Hence

$$g(n) \equiv g(z_p + mp) \equiv g(z) \equiv 0 \pmod{\mathfrak{p}_p}.$$

Moreover, since $\widetilde{u}_n/g(n) \in \mathcal{O}_S$, it follows that $\widetilde{u}_n \equiv 0 \pmod{\mathfrak{p}_p}$. From (5.36) it follows that

$$\sum_{i=1}^{s} \big(f_i(z_p)\alpha_i^{z_p}\big)(\alpha_i^p)^m \equiv \sum_{i=1}^{s} f_i(n)\,\alpha_i^n \equiv \widetilde{u}_n \equiv 0 \pmod{\mathfrak{p}_p}. \tag{5.41}$$

Note that $f_1(z_p), \ldots, f_s(z_p)$ cannot be all equal to zero modulo $\mathfrak{p}_p$, because $g(z_p) \equiv 0 \pmod{\mathfrak{p}_p}$ and (5.37). In particular, from (5.41) it follows that $s \geq 2$. Moreover, from (ii) it follows that $\mathcal{O}_S/\mathfrak{p}_p$ is a finite field of p elements; and (iii) implies that the multiplicative order modulo $\mathfrak{p}_p$ of each $(\alpha_i/\alpha_j)^p$, where $i, j \in \{1, \ldots, s\}$ and $i \neq j$, is at least $p^{1/4}$. Thus Theorem 4.25 implies that the possible values of m modulo $p-1$ are at most $2(p-1)/p^{1/(4s)}$. Hence, also using (5.39), the upper density of $\mathcal{N}'$ is at most

$$\sum_{\substack{p \in \mathcal{P} \\ p \geq Y}} \frac{2(p-1)p^{-1/(4s)}}{p(p-1)} \leq 2 \sum_{n \geq Y} \frac{1}{n^{1+1/(4s)}} < \frac{\varepsilon}{2},$$

as claimed.

Claim: the upper density of $\mathcal{N}''$ is less than $\varepsilon/2$. If $n \notin \mathcal{N}''$ then $n \not\equiv z_p \pmod{p}$ for every $p \in \mathcal{P} \cap [Y, X]$. Hence, by the Chinese remainder theorem and (5.40), it follows that the upper density of $\mathcal{N}''$ is at most $\varepsilon/2$, as claimed.

Therefore, the upper density of $\mathcal{N}$ is less than ε. □

Theorem 5.33 is related to the following difficult open problem.

Problem 5.3. Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$ and let $\boldsymbol{v} \in \mathbb{Z}^{\mathbb{N}}$ be a polynomial sequence. Determine if the set $\mathcal{N} := \{n \in \mathbb{N} : u_n/v_n \in \mathbb{Z}\}$ is infinite or finite.

The following are some particular instances of Problem 5.3.

Example 5.1. If $u_n := 2^n - 2$ and $v_n := n$, then it follows from Fermat's little theorem that $p \in \mathcal{N}$ for every prime number p. Hence $\mathcal{N}$ is infinite.

Example 5.2. If $u_n := 4^n + 1$ and $v_n := 4n + 3$, then it follows easily that $\mathcal{N}$ is finite. In fact, the set $\mathcal{N}$ is empty, since v_n has a prime factor p that is equal to 3 modulo 4, and -1 is not a square modulo p.

Example 5.3. If $u_n := 2^n - 2$ and $v_n := n(2n-1)$, then it is not known if $\mathcal{N}$ is infinite. However, it is easy to check that if p is a prime number such that $p \equiv 1 \pmod 4$ and $2p-1$ is a prime number, then $p \in \mathcal{N}$. Hence, assuming the *Schinzel hypothesis H* on simultaneous prime values of polynomials, it follows that $\mathcal{N}$ is infinite.

Example 5.4. A *Wieferich prime* is a prime number p such that p^2 divides $2^{p-1} - 1$. Currently, the only known Wieferich primes are 1093 and 3511. Whether there exists infinitely many Wieferich primes is an open problem [138]. If $u_n := 2^n - 2$ and $v_n := n^2$, then it is possible to prove that $\mathcal{N}$ is infinite if and only if there are infinitely many Wieferich primes.

5.8 Bibliographical notes

Section 5.2 "Cassels' embedding theorem"

This section follows the original paper of Cassels [34]. Lech [111] proved implicitly a weaker form of Theorem 5.2, in which $\mathbb{Q}_p$ is replaced by an algebraic extension of $\mathbb{Q}_p$. Cassels [34] used Theorem 5.2 to provide a simple proof of a theorem of Selberg [170] (see also [23]), which says that every finitely-generated group of matrices over a field of characteristic zero contains a normal torsion-free subgroup of finite index. In the case in which $\mathbb{K}$ is a number field, Dubickas, Sha, and Shparlinski [50] provided an upper bound for the least prime number p for which the embedding σ_p of Theorem 5.2 exists.

Section 5.3 "Degeneracy"

This section is inspired by a paper of Cipu, Diouf, and Mignotte [39], in which the authors propose some algorithms to establish if a given polynomial with integer coefficients is degenerate.

Section 5.4 "Zeros"

Skolem [177] gave the first proof of Theorem 5.10 for generalized power sums over $\mathbb{Q}$. Subsequently, Mahler [126] provided an extension to number fields; and then Lech [111] established the general case of arbitrary fields of characteristic zero. Hansel [76] provided an elementary proof that does not rely on p-adic analysis.

For a number field $\mathbb{K}$ and a nondegenerate linear recurrence $\boldsymbol{u}$ over $\mathbb{K}$ of order k, Schlickewei [169] gave the first upper bound on the number of zeros of $\boldsymbol{u}$ that depends only on k and $[\mathbb{K} : \mathbb{Q}]$. Later, Amoroso and Viada [2] (Theorem 5.13) strengthened this result.

Assuming the Skolem conjecture (a central hypothesis in Diophantine analysis, also known as the *exponential local-global principle*), Lipton, Luca, Nieuwveld, Ouaknine, Purser, and Worrell [117] proved that the Skolem problem for linear recurrences of order 5 is decidable; and exhibited a concrete procedure for solving it. Furthermore, unconditionally, they proved that the Skolem problem is decidable for every linear recurrences of order at most 7 whose minimal polynomial has constant term equal to ± 1. Kenison [96] gave an alternative proof by employing a powerful result of Dubickas and Smyth [49] concerning Galois conjugates that lie on two concentric circles.

Bilu, Luca, Nieuwveld, Ouaknine, Purser, and Worrell [18] proved the decidability of the Skolem problem for simple linear recurrences conditionally to the Skolem conjecture and the p-adic Schanuel conjecture. More precisely, they provided an algorithms that computes the set of zeros of a simple nondegenerate linear recurrence together with an unconditional certificate that its output is correct, that is, that all zeros have been found. The conjectural aspect of their result solely concerns the proof that the algorithm terminates on all inputs. An open source implementation of their algorithm is available online at the Skolem tool website [153].

A *Universal Skolem Set* is an infinite set $\mathcal{S}$ of nonnegative integers such that there exists an algorithm that takes as input a linear recurrence $\boldsymbol{u}$ over $\mathbb{Z}$ and decides whether $u_n = 0$ for some $n \in \mathcal{S}$. Evidently, establishing the decidability of the Skolem problem is equivalent to showing that $\mathbb{N}$ is a Universal Skolem Set. Luca, Ouaknine, and Worrell [120] introduced the notion of Universal Skolem Set an exhibited the first explicit example of such a set. This first example has natural density zero. Subsequently, Luca, Ouaknine, and Worrell [121] produced a set $\mathcal{S} \subseteq \mathbb{N}$ of positive lower density and an effective procedure that, given a simple nondegenerate linear recurrence $\boldsymbol{u}$ over $\mathbb{Z}$, computes the set $\{n \in \mathcal{S} : u_n = 0\}$. Luca, Maynard, Noubissie, Ouaknine, and Worrell [119] constructed a Universal Skolem Set that has lower density at least 0.29 and showed that this set has natural density 1 subject to the Bateman–Horn conjecture [12]. Finally, Luca, Ouaknine, and Worrell [122] unconditionally constructed a Universal Skolem Set of natural density 1. They achieved this by introducing the following notion. A *large zero* of a nondegenerate linear recurrence $\boldsymbol{u}$ is an integer n such that $u_n = 0$ and (roughly speaking) n exceeds a sixth-fold exponential in the size of the data that define the linear recurrence $\boldsymbol{u}$. Then they showed that the set of positive integers that can possibly arise as large zeros of some linear recurrence has natural density zero; hence its complement is a Universal Skolem Set. Furthermore, they provided a heuristic argument, based on the *Cramér conjecture* on gaps between consecutive primes, for the nonexistence of large zeros and, consequently, the decidability of the Skolem problem.

Kenison, Lipton, Ouaknine, and Worrell [97] considered the following problem. Given a linear recurrence $\boldsymbol{u}$ over $\mathbb{Z}$ and an integer c, determine whether there exist a prime number p and positive integers $\ell, k \leq c$ such that $\boldsymbol{u}_{\ell p^k} = 0$. Note that the case $c = 1$ corresponds to the Skolem problem restricted to the set of prime numbers. They solved this problem for some classes of linear recurrences including those of the form $u_n = \sum_{i=1}^{m} c_i \alpha_i^n$ $(n \in \mathbb{N})$, where $c_1, \ldots, c_m$ are integers and $\alpha_1, \ldots, \alpha_m$ are algebraic integers.

Regarding the computational complexity of the Skolem problem, Blondel and Portier proved that the Skolem problem is *NP-hard* [20].

Derksen [45] proved a version of Theorem 5.10 for fields of positive characteristic. In this case, the set of zeros is no longer the union of a finite set and finitely many arithmetic progressions (recall Remark 5.12); instead, it is a *p-normal set* and can be effectively computed. Dong and Shafrir [46] extended the result of Derksen to linear recurrence over commutative rings of positive characteristic.

Section 5.5 "Growth"

Loxton and van der Poorten [118, Conjecture 2] conjectured Theorem 5.17. Evertse [56] and van der Poorten and Schlickewei [188] (see also [186]) independently proved it. It is difficult to overstate the impact that Baker's theory on lower bounds for linear forms in logarithms has had on number theory. For results and applications of lower bounds for linear forms in logarithms, see the books by Baker [6] and Bugeaud [27].

Section 5.6 "Factorization of generalized power sums"

This section is based on the paper of Rumely and van der Poorten [164] and follows their original proofs.

Section 5.7 "Hadamard quotient theorem"

Pisot was the first to conjecture Theorem 5.26 (see the paper of Benzaghou [13, p. 233]). Pólya [147], Cantor [31, 32], and Uchiyama [185] already proved the special case in which $\boldsymbol{v}$ is a polynomial sequence. Moreover, Cantor [32, Lemma 2] proved the case in which $\boldsymbol{v}$ has a single dominant root. Pourchet [149] announced a proof of the general case, but this proof contained some gaps. van der Poorten [189] gave the first complete proof of Theorem 5.26. He stated that: "In retrospect, however, it is plain that the present proof is that implied in [Pourchet's] announcement." See also the notes of Rumely [163] for a more detailed argument. van der Poorten [187, Section 6.6.1] suggested the possibility of considering the much weaker assumption that $u_n/v_n \in \mathcal{R}$ for infinitely many integers $n \geq 0$, instead of all integers $n \geq 0$. Corvaja and Zannier [41] (see also [40]) then proved Theorem 5.28. This was a breakthrough result that used Schmidt subspace theorem to overcome the absence of a single dominant root. For a survey on Schmidt subspace theorem and its applications, see the article of Bilu [19]. The proof of Theorem 5.33 comes from the paper by Corvaja and Zannier [41, Corollary 2], as well as some of the examples after Problem 5.3. Sanna [166] gave a quantitative version of Theorem 5.33 and showed that, under the *Hardy–Littlewood k-tuple conjecture*, the result is nearly optimal. There is some literature about the nth values of a polynomial sequence dividing the nth value of a linear recurrence, see for instance the works of Alba González et al. [1], Luca and Tron [123], and Sanna [167].

5.9 Exercises

Exercise 5.1. Determine all monic second-degree degenerate polynomials in $\mathbb{Q}[x]$.

Exercise 5.2. Determine the set of zeros of each of the following linear recurrences $\boldsymbol{u}$ over $\mathbb{Z}$.

(i) $u_0 = 169$, $u_1 = -70$, and $u_n = 2u_{n-1} + u_{n-2}$ for $n \geq 2$.

(ii) $u_0 = 1$, $u_1 = 1$, and $u_n = u_{n-1} - 2u_{n-2}$ for $n \geq 2$.

(iii) $u_0 = 3$, $u_1 = 9$, and $u_n = 3u_{n-1} - 3u_{n-2}$ for $n \geq 2$.

(iv) $u_0 = 4$, $u_1 = 3$, $u_2 = -7$, and $u_n = u_{n-2} + u_{n-3}$ for $n \geq 3$.

(v) $u_0 = 0$, $u_1 = 1$, $u_2 = 2$, and $u_n = 5u_{n-1} - 9u_{n-2} + 5u_{n-3}$ for $n \geq 3$.

(vi) $u_0 = u_1 = 0$, $u_2 = 2$, $u_3 = -1$, and $u_n = 2u_{n-1} - 11u_{n-2} - 10u_{n-3} - 25u_{n-4}$ for $n \geq 4$.

Exercise 5.3. Let τ be the Ramanujan τ function (Example 1.11). Prove that

(i) for every integer $n \geq 0$,

$$\tau(p^n) = \frac{p^{11/2}\sin\big((n+1)\theta_p\big)}{\sin\theta_p},$$

where $\theta_p \in \mathbb{R}$ satisfies $\cos\theta_p = p^{11/2}\tau(p)/2$;

(ii) if $\tau(m) = 0$ for some positive integer m, then m is a prime number.

(Lehmer [113] proved (ii) in 1947. The *Lehmer conjecture* assert that $\tau(m) \neq 0$ for every positive integer m.)

Exercise 5.4. Consider the following two versions of the Skolem problem (Problem 5.1).

(i) (Decision version) Given a nondegenerate linear recurrence $\boldsymbol{u}$ over $\mathbb{Z}$, determine if there exists an integer $n \geq 0$ such that $u_n = 0$.

(ii) (Search version) Given a nondegenerate linear recurrence $\boldsymbol{u}$ over $\mathbb{Z}$, find all integers $n \geq 0$ such that $u_n = 0$.

Prove that from an algorithm to solve (i) it is possible to build an algorithm to solve (ii), and vice versa.

Exercise 5.5. Find an asymptotic formula for the nth term of each of the following linear recurrences $\boldsymbol{u}$ over $\mathbb{Z}$.

(i) $u_n = 1$, $u_1 = 2$, and $u_n = 4u_{n-1} - u_{n-2}$ for $n \geq 2$.

(ii) $u_n = 0$, $u_1 = 4$, $u_2 = 12$, and $u_n = 5u_{n-1} - 5u_{n-2} - 3u_{n-3}$ for $n \geq 3$.

(iii) $u_n = 3$, $u_1 = 15$, $u_2 = 73$, and $u_n = 11u_{n-1} - 40u_{n-2} + 48u_{n-3}$ for $n \geq 3$.

Exercise 5.6. Let $f \in \mathbb{C}[x]$ be a nonconstant monic polynomial with a single dominant root α. Prove that

$$\alpha = \lim_{n \to +\infty} \frac{u_{n+1}}{u_n},$$

for every linear recurrence $\boldsymbol{u}$ with minimal polynomial f, such as the impulse sequence $\boldsymbol{\delta}(f)$. (This is the *Bernoulli method* to find the largest root of a polynomial [154, Section 8.10-3].)

Exercise 5.7. Let $\mathbb{K}$ be a field of characteristic zero whose algebraic closure is equipped with an absolute value $|\cdot|$, let $\boldsymbol{u}$ be a nonzero linear recurrence over $\mathbb{K}$, let f be the minimal polynomial of $\boldsymbol{u}$, and put $k := \deg(f)$. Suppose that $|f(0)| > 1$. Prove that

$$\max\left\{|u_n|, \ldots, |u_{n+2k-2}|\right\} > C|f(0)|^{n/k},$$

for every integer $n \geq 0$, where $C > 0$ is an effectively computable constant depending on $\boldsymbol{u}$.

Exercise 5.8. Find the factorization into irreducibles of each of the following generalized power sums $\boldsymbol{u}$ in the ring $\mathfrak{S}_{\mathbb{Q}}(\Gamma)$.

(i) $u_n = 4^n + 3 \cdot 6^n + 2 \cdot 9^n + 12^n - 16^n$ for $\Gamma = \langle 2, 3 \rangle$.

(ii) $u_n = (1 + 2n + n^2)4^n - 4^{-n}$ for $\Gamma = \langle 2 \rangle$.

(iii) $u_n = 2^n + n3^n + 4^n$ for $\Gamma = \langle 2, 3 \rangle$.

Exercise 5.9. Determine for which of the following generalized power sums $\boldsymbol{u}$ and $\boldsymbol{v}$ the ratio $\boldsymbol{u}/\boldsymbol{v}$ is a generalized power sum over $\mathbb{Q}$.

(i) $u_n = 4^n - 9^n + 2 \cdot 10^n + 2 \cdot 15^n$ and $v_n = 2^n + 3^n$.

(ii) $u_n = n4^n + n^2 6^n + 8^n + n12^n$ and $v_n = n2^n + 4^n$.

(iii) $u_n = 2^n - 4^n + 6^n$ and $v_n = 2^n + 2 \cdot 3^n$.

Exercise 5.10. Determine the cardinality of each of the following sets of positive integers n.

(i) n such that n divides $2^n - 1$.

(ii) n such that n divides $2^n + 1$.

(iii) n such that n^2 divides $2^n + 1$. (This set appears in Problem 3 of IMO 1990 [83].)

(iv) n such that $n + 2$ divides $2^n - 1$. (Rotkiewicz [162] studied this set.)

Exercise 5.11. A *Wieferich prime* is a prime number p such that $2^{p-1} \equiv 1 \pmod{p^2}$. The only known Wieferich primes are 1093 and 3511. It is believed that there are infinitely many Wieferich primes, but proving so is an open problem [138].

Prove the following statements.

(i) If n be a positive integer such that $2^{n-1} \equiv 1 \pmod{n^2}$, and p is a prime factor of n, then p is a Wieferich prime and $\nu_p(n) \leq \nu_p(2^{p-1} - 1)/2$.

(ii) The ratio u_n/v_n of the linear recurrences $u_n := 2^n - 2$ and $v_n := n^2$ is an integer for infinitely many positive integers n if and only if there exist infinitely many Wieferich primes.

Chapter 6

Linear Recurrences over the Integers

6.1 Introduction

This chapter focuses on the study of linear recurrences over the ring of integers and considers results and questions of a number-theoretic nature. The prerequisites are the same as those of the previous chapter.

The first topic of this chapter is the family of *linear divisibility sequences*, which consists of linear recurrences enjoying a particularly nice divisibility property (Section 6.2).

The second topic is the problem of establishing if a linear recurrence has infinitely many prime terms. This problem is wide open, but there are many heuristic considerations that find support in data (Section 6.3).

The third topic concerns linear recurrences modulo a positive integer m. This includes periodicity properties (Section 6.4) and bounds for the number of zeros modulo m over an interval (Section 6.5).

The fourth topic of this chapter regards the prime factors of terms of linear recurrences. In particular, the number of primes dividing the first terms of a linear recurrence (Section 6.6) and lower bounds for the greatest prime factor of the term of a linear recurrence (Section 6.7).

Finally, the last topic concerns composite values of terms of linear recurrences. The main result says that if a linear recurrence is a *Cullen sequence* then almost all its terms are composite (Section 6.8).

Throughout this chapter, the letters p and q are reserved for prime numbers.

6.2 Divisibility sequences

A *divisibility sequence* is a sequence $\boldsymbol{u} \in \mathbb{Z}^{\mathbb{N}}$ such that, for all positive integers m and n, if m divides n then u_m divides u_n. A *strong divisibility sequence* is a sequence $\boldsymbol{u} \in \mathbb{Z}^{\mathbb{N}}$ such that $\gcd(u_m, u_n) = |u_{\gcd(m,n)}|$ for all positive integers m and n. (Note that u_0 is immaterial to the previous two definitions.) Since a divides b if and only if $\gcd(a, b) = |a|$, for all integers a and b, it follows that every strong divisibility sequence is a divisibility sequence.

A *linear divisibility sequence*, respectively a *strong linear divisibility sequence*, is a linear recurrence that is also a divisibility sequence, respectively a strong divisibility sequence.

Linear divisibility sequences play a special role in the study of the prime values of linear recurrences over the ring of integers (Section 6.3).

Example 6.1. Every constant sequence of integers is a strong linear divisibility sequence.

Example 6.2. The linear recurrence of natural numbers $0, 1, 2, \ldots$ is a strong linear divisibility sequence.

Example 6.3. Every first-order linear recurrence over $\mathbb{Z}$ (that is, every geometric progression) is a divisibility sequence, which in general is not a strong divisibility sequence.

Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree $s \geq 2$ having no multiple root and satisfying $f(0) \neq 0$. The *resultant sequence* $\boldsymbol{r}$ associated to f is defined by

$$r_n := \prod_{1 \leq i < j \leq s} \frac{\alpha_i^n - \alpha_j^n}{\alpha_i - \alpha_j} \tag{6.1}$$

for every integer $n \geq 0$, where $\alpha_1, \ldots, \alpha_s$ are the roots of f. Note that (6.1) does not depend on the order of the roots $\alpha_1, \ldots, \alpha_s$. Hence $\boldsymbol{r}$ is well defined.

The next theorem says that resultant sequences are linear divisibility sequences.

Theorem 6.1. *Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree $s \geq 2$ having no multiple root and satisfying $f(0) \neq 0$. Then the resultant sequence $\boldsymbol{r}$ associated to f is a linear divisibility sequence.*

Proof. Let $\alpha_1, \ldots, \alpha_s$ be the roots of f. First, from (6.1) and Theorem 2.15, it follows that $\boldsymbol{r}$ is a linear recurrence. Second, for every integer $n \geq 0$, from (6.1) it follows that

$$r_n = \prod_{1 \leq i < j \leq s} \frac{\alpha_i^n - \alpha_j^n}{\alpha_i - \alpha_j} = \prod_{1 \leq i < j \leq s} \left(\sum_{\ell=0}^{n-1} \alpha_i^{n-\ell} \alpha_j^{\ell} \right)$$

is a symmetric polynomial in the roots $\alpha_1, \ldots, \alpha_k$. Thus r_n is an integer. At last, if m and n are positive integers such that m divides n, then

$$\frac{r_n}{r_m} = \prod_{1 \leq i < j \leq s} \frac{\alpha_i^n - \alpha_j^n}{\alpha_i^m - \alpha_j^m} = \prod_{1 \leq i < j \leq k} \left(\sum_{\ell=0}^{n/m-1} \alpha_i^{(n/m-\ell)m} \alpha_j^{\ell m} \right)$$

is a symmetric polynomial of the roots $\alpha_1, \ldots, \alpha_k$. Hence r_n/r_m is an integer, which means that r_m divides r_n. Thus $\boldsymbol{r}$ is a linear divisibility sequence. □

Remark 6.2. In general, resultant sequences are not strong linear divisibility sequences. For example, the resultant sequence $\boldsymbol{r}$ of $(x-1)(x-2)(x-3)$ is not a strong divisibility sequence since $\gcd(r_3, r_4) = \gcd(1729, 39000) = 13$ but $r_{\gcd(3,4)} = r_1 = 1$.

Barbero [11] proved the following theorem, which states that, essentially, each linear divisibility sequence divides a resultant sequence.

Theorem 6.3. *Let $\boldsymbol{u}$ be a simple nondegenerate linear recurrence over $\mathbb{Z}$ of order $s \geq 2$, let f be the minimal polynomial of $\boldsymbol{u}$, and let $\boldsymbol{r}$ be the resultant sequence associated to f. Suppose that $u_0 = 0$ and $u_1 = 1$. If $\boldsymbol{u}$ is a divisibility sequence then u_n divides r_n for every integer $n \geq 0$.*

The proof of Theorem 6.3 is elementary but involves some technical determinant identities and so it is not included here. Barbero [11, Theorem 2] provided also a generalization for linear recurrences with multiple roots (of which Theorem 6.3 is in fact a corollary).

Recall that a *Lucas sequence* is a linear recurrence $\boldsymbol{u}$ over $\mathbb{Z}$ with initial values $u_0 = 0$, $u_1 = 1$, and characteristic polynomial $f(x) = x^2 - a_1x - a_2$, where $a_1, a_2 \in \mathbb{Z}$ and $a_2 \neq 0$ (Example 1.8). From Example 2.2 it follows that if f has distinct roots then the Lucas sequence $\boldsymbol{u}$ is the resultant sequence associated to f.

The next result says that every Lucas sequence is a divisibility sequence and, under a certain condition, a strong divisibility sequences.

Theorem 6.4. *Let $\boldsymbol{u}$ be a Lucas sequence with characteristic polynomial $x^2 - a_1x - a_2$ ($a_i \in \mathbb{Z}, a_2 \neq 0$). Then $\boldsymbol{u}$ is a linear divisibility sequence. If $\gcd(a_1, a_2) = 1$ then $\boldsymbol{u}$ is a strong linear divisibility sequence.*

In particular, Theorem 6.4 implies that the sequences of Fibonacci numbers and Mersenne numbers are strong divisibility sequences.

Proof of Theorem 6.4. Let m and n be integers with $0 \leq m < n$. Any of the methods of Section 2.9 proves that

$$u_n = u_{m+1}u_{n-m} + a_2u_mu_{n-m-1}.$$

As a consequence

$$u_n \equiv u_{m+1}u_{n-m} \pmod{u_m}. \tag{6.2}$$

If m divides n then n/m applications of (6.2) give

$$u_n \equiv u_{m+1}u_{n-m} \equiv u_{m+1}^2u_{n-2m} \equiv \cdots \equiv u_{m+1}^{n/m}u_0 \equiv 0 \pmod{u_m},$$

since $u_0 = 0$. Hence $\boldsymbol{u}$ is a linear divisibility sequence.

Suppose that $\gcd(a_1, a_2) = 1$. Claims:

(i) $\gcd(a_2, u_n) = 1$;

(ii) $\gcd(u_{n-1}, u_n) = 1$.

Proceeding by induction proves both claims. Claim (i) is true for $n = 1$ since $u_1 = 1$. Suppose that claim (i) is true for a positive integer n. Then

$$\gcd(a_2, u_{n+1}) = \gcd(a_2, a_1u_n + a_2u_{n-1}) = \gcd(a_2, a_1u_n) = \gcd(a_2, u_n) = 1,$$

where the third equality holds since $\gcd(a_1, a_2) = 1$. Thus claim (i) follows by induction. Claim (ii) is true for $n = 1$ since $u_0 = 0$ and $u_1 = 1$. Suppose that claim (ii) is true for a positive integer n. Then

$$\gcd(u_n, u_{n+1}) = \gcd(u_n, a_1u_n + a_2u_{n-1}) = \gcd(u_n, a_2u_{n-1}) = \gcd(u_n, u_{n-1}) = 1,$$

where the third equality is a consequence of claim (i). Hence claim (ii) follows by induction.

At this point (ii) implies that $\gcd(u_m, u_{m+1}) = 1$, and so (6.2) implies

$$\gcd(u_m, u_n) = \gcd(u_m, u_{m+1}u_{n-m}) = \gcd(u_m, u_{n-m}). \tag{6.3}$$

Since $\gcd(m, n) = \gcd(m, n-m)$, it follows from (6.3) that $\gcd(u_m, u_n) = |u_{\gcd(m,n)}|$. Hence $\boldsymbol{u}$ is a strong linear divisibility sequence. □

It is natural to ask if—beside resultant sequences and Lucas sequences—there are other interesting families of linear divisibility sequences and strong linear divisibility sequences. Using Theorem 2.34, it is easy to verify that the termwise multiplication of linear divisibility sequences is a linear divisibility sequence. Hence, for instance, the product of two Lucas sequences is a fourth-order linear divisibility sequence. But there are also higher-order linear divisibility sequences that do not come as products of Lucas sequences. The following examples are given without proofs.

Example 6.4. Let $f \in \mathbb{Z}[x]$ be a monic polynomial and let $\alpha_1, \ldots, \alpha_k$ be the roots of f. The *Pierce sequence* $\boldsymbol{u}$ associated to f is the sequence defined by

$$u_n := \prod_{i=1}^{k} (\alpha_i^n - 1)$$

for every integer $n \geq 0$. The Pierce sequence $\boldsymbol{u}$ is a linear divisibility sequence.

Example 6.5. Let α and β be nonzero complex numbers such that $(\alpha + \beta)^2$ and $\alpha\beta$ are nonzero coprime integers and α/β is not a root of unity. The *Lehmer sequence* $\boldsymbol{\ell}$ associated to α and β is defined by

$$\ell_n := \begin{cases} (\alpha^n - \beta^n)/(\alpha^2 - \beta^2) & \text{if } n \text{ is even;} \\ (\alpha^n - \beta^n)/(\alpha - \beta) & \text{if } n \text{ is odd;} \end{cases}$$

for every integer $n \geq 0$. The Lehmer sequence is a strong linear divisibility sequence and satisfies the fourth-order linear recurrence relation

$$\ell_n = (\alpha^2 + \beta^2)\ell_{n-2} + (\alpha\beta)^2\ell_{n-4}$$

for every integer $n \geq 4$.

Granville [72] has recently classified all linear divisibility sequences and strong linear divisibility sequences (see the bibliographical notes for more information).

6.3 Prime terms

Problem 6.1. Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$. Are there infinitely many integers $n \geq 0$ such that u_n is a prime number?

A general answer to Problem 6.1 is currently out of reach. Already the "easier" case in which $\boldsymbol{u}$ is a polynomial sequence leads to the the following open conjecture.

Conjecture 6.1 (Bunyakovsky conjecture)**.** Let $f \in \mathbb{Z}[x]$ be a nonconstant polynomial. Suppose that

(i) the leading coefficient of f is positive;

(ii) f is irreducible over $\mathbb{Q}$;

(iii) $\gcd\{f(n) : n \in \mathbb{N}\} = 1$.

Then there are infinitely many integers $n \geq 0$ such that $f(n)$ is a prime number.

It is easy to verify that (i)–(iii) in Conjecture 6.1 are necessary conditions in order for $f(n)$ to be prime for infinitely many integers $n \geq 0$. Conjecture 6.1 says that (i)–(iii) are also sufficient conditions.

The only proved case of the Bunyakovsky conjecture is that of first-degree polynomials, which corresponds to the important *Dirichlet theorem* on primes in arithmetic progressions.

Theorem 6.5 (Dirichlet theorem)**.** *Let a and b be relatively prime integers with $a > 0$. Then $an + b$ is a prime number for infinitely many integers $n \geq 0$.*

The proof of Theorem 6.5 is a milestone in analytic number theory, introducing powerful tools such as *Dirichlet characters* and *L-functions*. For a modern treatment, see the book by Tenenbaum [184, Chapter II.8].

6.3.1 Obstructions to primality

Hereafter, the focus is on linear recurrences that are not polynomial sequences. Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$. Assume that $\boldsymbol{u}$ is nondegenerate. This is not a restriction in light of Theorem 2.9 and Theorem 2.12. If $\boldsymbol{u}$ has a single root α, then α must be an integer and, by Theorem 2.15, there exists $f \in \mathbb{Q}[x]$ such that $u_n = f(n)\alpha^n$ for every integer $n \geq 0$. Hence, if u_n is prime for infinitely many integers $n \geq 0$, then $|\alpha| = 1$ and $f(n)$ is prime for infinitely many integers $n \geq 0$. In other words, the primality of the terms of $\boldsymbol{u}$ boils down to the primality of the terms of a polynomial sequence. Thus assume that $\boldsymbol{u}$ has at least two distinct roots.

It seems likely that $\boldsymbol{u}$ has infinitely many prime terms, unless it is prevented by some of the following "obstructions".

(a) $u_n < 1$ for all sufficiently large integers n.

(b) The linear recurrence $\boldsymbol{u}$ factorizes as the product of two linear recurrences (Section 5.6). For example, if $\boldsymbol{u}$ is the linear recurrence defined by $u_n := 4^n - 1$ for each integer $n \geq 0$, then u_n is prime only for $n = 1$. Indeed $u_n = (2^n - 1)(2^n + 1)$ for every integer $n \geq 0$.

(c) There exists a finite set of prime numbers $\mathcal{P}$ such that, for each sufficiently large integer n, there exists $p \in \mathcal{P}$ for which p divides u_n. For example, let $\boldsymbol{u}$ be the linear

recurrence defined by $u_n := 4^{n+1} + 11^n$ for every integer $n \geq 0$. Then $u_0 = 5$ is the only prime term of $\boldsymbol{u}$. Indeed $u_n \equiv 0 \pmod 3$ if n is odd, and $u_n \equiv 0 \pmod 5$ is n is even.

(d) The linear recurrence $\boldsymbol{u}$ has some kind of "divisibility property", such as being a divisibility sequence. For instance, if $\boldsymbol{u}$ is the sequence of Fibonacci numbers or Mersenne numbers, then u_n can be prime only if n is prime. This restriction does not necessarily prevent the infinitude of prime terms of $\boldsymbol{u}$, but it must somehow be taken into account (more about this in Section 6.3.3 and Section 6.3.4).

(e) Any "combination" of the preceding obstructions. For example, let $\boldsymbol{u}$ be the linear recurrence defined by $u_n := 24^n + 6^n + 4^n + (-1)^n$, for every integer $n \geq 0$. Then every u_n is composite. Indeed, if n is even then $u_n = (4^n + 1)(6^n + 1)$, while if n is odd then $u_n \equiv 0 \pmod 3$.

If none of (a)–(e) occurs, then $\boldsymbol{u}$ is believed to have infinitely many prime terms. Note that conditions (a) and (b) are analogous to conditions (i) and (ii) of Conjecture 6.1; condition (c) is already more involved than (iii), while (d) and (e) are peculiar of linear recurrences.

6.3.2 Heuristic for the counting function of prime terms

For every real number X, let $P_{\boldsymbol{u}}(X)$ be the number of positive integers $n \leq X$ such that u_n is prime. Heuristically, by the prime number theorem (Theorem A.37), the "probability" that a large integer N is prime is about $1/\log N$. Moreover, in general u_n grows exponentially (Section 5.5). Say $u_n \sim C\alpha^n$, as $n \to +\infty$, for some constant $C, \alpha > 0$ (Theorem 5.16). Hence, it should be

$$P_{\boldsymbol{u}}(X) \approx \sum_{2 \leq n \leq X} \frac{1}{\log u_n} \approx \frac{1}{\log \alpha} \sum_{2 \leq n \leq X} \frac{1}{n} \approx \frac{\log X}{\log \alpha}, \tag{6.4}$$

as $X \to +\infty$. From numerical experiments, the quantity $P_{\boldsymbol{u}}(X)$ does in fact seem to grow as $\log X$, but with a multiplicative constant different from the factor $1/\log \alpha$ appearing in (6.4).

6.3.3 Mersenne primes

Let $\boldsymbol{M} := (M_n)$ be the sequence of Mersenne numbers. Theorem 6.4 says that $\boldsymbol{M}$ is a divisibility sequence. Hence, for every positive integer n, the Mersenne number M_n can be prime only if n is prime. (The converse is false, since $M_{11} = 23 \cdot 89$.) Thus the argument of Section 6.3.2 must be adapted to consider only prime indices. This implies that

$$P_{\boldsymbol{M}}(X) \approx \sum_{p \leq X} \frac{1}{\log(2^p - 1)} \approx \frac{1}{\log 2} \sum_{p \leq X} \frac{1}{p} \approx \frac{\log \log X}{\log 2}, \tag{6.5}$$

as $X \to +\infty$, also thanks to Mertens' second theorem (Theorem A.35). But (6.5) is not compatible with numerical data. One reason could be that each prime factor of M_p is guaranteed to be greater that p. Indeed, if q is a prime factor of M_p, then $2^p \equiv 1 \pmod q$.

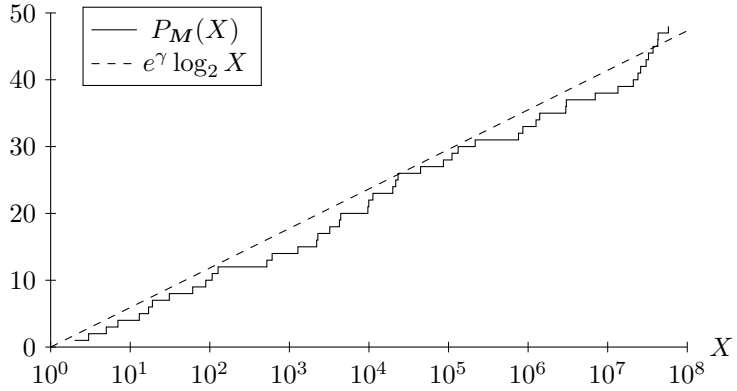


Figure 6.1: Number $P_{\boldsymbol{M}}(X)$ of positive integers $n \leq X$ such that $2^n - 1$ is a prime, and the estimate $e^{\gamma} \log_2 X$ from the Lenstra–Pomerance–Wagstaff conjecture.

Hence the multiplicative order of 2 modulo q is equal to p. In turn, by Fermat's little theorem, this implies that p divides $q - 1$, and in particular $q > p$. By the prime number theorem and Mertens' third theorem (Theorem A.36), the "probability" that a large integer N is not divisible by a prime greater than p is about

$$\frac{1}{\log N} \prod_{q \leq p} \left(1 - \frac{1}{q}\right)^{-1} \approx \frac{\mathrm{e}^{\gamma} \log p}{\log N},$$

where γ is the Euler–Mascheroni constant. With this adjustment (6.5) becomes

$$P_{\boldsymbol{M}}(X) \approx \sum_{p \leq X} \frac{\mathrm{e}^{\gamma} \log p}{\log(2^p - 1)} \approx \frac{\mathrm{e}^{\gamma}}{\log 2} \sum_{p \leq X} \frac{\log p}{p} \approx \frac{\mathrm{e}^{\gamma} \log X}{\log 2}, \tag{6.6}$$

as $X \to +\infty$, also thanks to Mertens' first theorem (Theorem A.34). Approximation (6.6) is the *Lenstra–Pomerance–Wagstaff conjecture* and seems to fit with numerical data, see Figure 6.1.

6.3.4 Fermat primes

Let $\boldsymbol{u}$ be the linear recurrence defined by $u_n := 2^n + 1$ for every integer $n \geq 0$. Despite the similarity with the sequence of Mersenne numbers, the primality of the terms of $\boldsymbol{u}$ is drastically different. If m and n are positive integers such that m divides n, and n/m is odd, then u_m divides u_n. Indeed

$$u_n = 2^n + 1 \equiv (2^m)^{n/m} + 1 \equiv (-1)^{n/m} + 1 \equiv -1 + 1 \equiv 0 \pmod{u_m}.$$

It follows that, for all positive integers n, a necessary condition for u_n to be prime is that n is a power of 2. Thus it is more convenient to move to the corresponding subsequence of $\boldsymbol{u}$.

The sequence of *Fermat numbers* (F_n) is defined by $F_n := 2^{2^n} + 1$ for every integer $n \geq 0$. (Caution: the notation F_n collides with that for the Fibonacci number.) A *Fermat prime* is

a Fermat number that is prime. The first five Fermat numbers

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537$$

are prime numbers, while

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417$$

is composite. Indeed $F_0, \ldots, F_4$ are the only known Fermat primes.

Reasoning as in the previous heuristics, the expected number of Fermat primes should be about

$$\sum_{n=0}^{\infty} \frac{1}{\log(2^{2^n}+1)} \approx \frac{1}{\log 2} \sum_{n=0}^{\infty} \frac{1}{2^n} < +\infty.$$

In other words, there should be only finitely many Fermat primes.

6.4 Periodicity modulo m

Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$, let f be the minimal polynomial of $\boldsymbol{u}$, and let m be a positive integer. Then $\boldsymbol{u}$ modulo m is a linear recurrence over the ring of integers modulo m. Consequently, by Remark 4.2, the sequence $\boldsymbol{u}$ modulo m is ultimately periodic. Let $\rho_{\boldsymbol{u}}(m)$ and $\tau_{\boldsymbol{u}}(m)$ be the least preperiod and the least period of $\boldsymbol{u}$ modulo m, respectively.

Theorem 6.6. *Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$ of positive order k, let f be the minimal polynomial of $\boldsymbol{u}$, and let m be a positive integer. Then $\rho_{\boldsymbol{u}}(m) + \tau_{\boldsymbol{u}}(m) < m^k$. Furthermore, the sequence $\boldsymbol{u}$ modulo m is periodic, that is $\rho_{\boldsymbol{u}}(m) = 0$, if and only if m and $f(0)$ are coprime.*

Proof. The claim follows easily from Remark 4.2. □

The following theorem provides some basic properties of the least period and the least preperiod of a linear recurrence modulo m.

Theorem 6.7. *Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$ and let m_1 and m_2 be coprime positive integers. Then*

(i) $\tau_{\boldsymbol{u}}(m_1 m_2) = \operatorname{lcm}\big(\tau_{\boldsymbol{u}}(m_1), \tau_{\boldsymbol{u}}(m_2)\big)$;

(ii) $\rho_{\boldsymbol{u}}(m_1 m_2) = \max\big(\rho_{\boldsymbol{u}}(m_1), \rho_{\boldsymbol{u}}(m_2)\big)$.

Proof. From the definitions of $\tau_{\boldsymbol{u}}(m_1 m_2)$ and $\rho_{\boldsymbol{u}}(m_1 m_2)$, it follows that

$$u_{n+\tau_{\boldsymbol{u}}(m_1 m_2)} \equiv u_n \pmod{m_1 m_2},$$

for every integer $n \geq \rho_{\boldsymbol{u}}(m_1 m_2)$. Hence

$$u_{n+\tau_{\boldsymbol{u}}(m_1 m_2)} \equiv u_n \pmod{m_i}$$

for each $i \in \{1,2\}$ and for every integer $n \geq \rho_{\boldsymbol{u}}(m_1 m_2)$. This implies that

$$\tau_{\boldsymbol{u}}(m_i) \mid \tau_{\boldsymbol{u}}(m_1 m_2) \quad \text{and} \quad \rho_{\boldsymbol{u}}(m_i) \leq \rho_{\boldsymbol{u}}(m_1 m_2),$$

for each $i \in \{1,2\}$, which in turn implies that

$$\operatorname{lcm}\big(\tau_{\boldsymbol{u}}(m_1), \tau_{\boldsymbol{u}}(m_2)\big) \mid \tau_{\boldsymbol{u}}(m_1 m_2) \quad \text{and} \quad \max\big(\rho_{\boldsymbol{u}}(m_1), \rho_{\boldsymbol{u}}(m_2)\big) \leq \rho_{\boldsymbol{u}}(m_1 m_2). \tag{6.7}$$

Vice versa, from the definitions of $\tau_{\boldsymbol{u}}(m_i)$ and $\rho_{\boldsymbol{u}}(m_i)$, it follows that

$$u_{n+\tau_{\boldsymbol{u}}(m_i)} \equiv u_n \pmod{m_i},$$

for each $i \in \{1,2\}$ and for every integer $n \geq \rho_{\boldsymbol{u}}(m_i)$. Thus

$$u_{n+\operatorname{lcm}(\tau_{\boldsymbol{u}}(m_1), \tau_{\boldsymbol{u}}(m_2))} \equiv u_n \pmod{m_1 m_2},$$

for every integer $n \geq \max\big(\rho_{\boldsymbol{u}}(m_1), \rho_{\boldsymbol{u}}(m_2)\big)$, which implies that

$$\tau_{\boldsymbol{u}}(m_1 m_2) \mid \operatorname{lcm}\big(\tau_{\boldsymbol{u}}(m_1), \tau_{\boldsymbol{u}}(m_2)\big) \quad \text{and} \quad \rho_{\boldsymbol{u}}(m_1 m_2) \leq \max\big(\rho_{\boldsymbol{u}}(m_1), \rho_{\boldsymbol{u}}(m_2)\big). \tag{6.8}$$

Putting together (6.7) and (6.8), claims (i) and (ii) follow. □

Theorem 6.7 implies the following corollary.

Corollary 6.8. *Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$ and let $m \geq 2$ be an integer. Then*

(i) $\tau_{\boldsymbol{u}}(m) = \operatorname{lcm}_{p \mid m} \tau_{\boldsymbol{u}}\big(p^{\nu_p(m)}\big)$;

(ii) $\rho_{\boldsymbol{u}}(m) = \max_{p \mid m} \rho_{\boldsymbol{u}}\big(p^{\nu_p(m)}\big)$.

Proof. The claim follows by repeated applications of Theorem 6.7. □

In light of Corollary 6.8, the least period and the least preperiod of a linear recurrence modulo m are completely determined by its least periods and least preperiods modulo prime powers. The following theorem provides a description of the least period and the least preperiod of a linear recurrence modulo prime powers. If $\boldsymbol{u}$ is a linear recurrence of positive order k and minimal polynomial f, the companion matrix of $\boldsymbol{u}$ is $\boldsymbol{C}(f)$ (Section 2.4) and the Hankel matrix of $\boldsymbol{u}$ is $\boldsymbol{H}_k(\boldsymbol{u})$ (Section 2.10).

Theorem 6.9. *Let $\boldsymbol{u}$ be a nonzero linear recurrence over $\mathbb{Z}$, let $\boldsymbol{H}$ be the Hankel matrix of $\boldsymbol{u}$, let p be a prime number, let $h := \nu_p\big(\det(\boldsymbol{H})\big)$ (recall that $\det(\boldsymbol{H}) \neq 0$ by Theorem 2.56), and let $v > h$ be an integer. Then*

(i) $\tau_{\boldsymbol{u}}(p^{v+1}) = \tau_{\boldsymbol{u}}(p^v)$ *or* $\tau_{\boldsymbol{u}}(p^{v+1}) = p\,\tau_{\boldsymbol{u}}(p^v)$;

(ii) $\rho_{\boldsymbol{u}}(p^{v+1}) \leq \rho_{\boldsymbol{u}}(p^v) + \rho_{\boldsymbol{u}}(p^{h+1})$;

(iii) $\tau_{\boldsymbol{u}}(p^v)$ *divides* $p^{v-h-1}\tau_{\boldsymbol{u}}(p^{h+1})$;

(iv) $\rho_{\boldsymbol{u}}(p^v) \leq (v-h)\rho_{\boldsymbol{u}}(p^{h+1})$;

(v) *if $p > 2$ or $v > h + 1$, and $\tau_{\boldsymbol{u}}(p^{v+1}) \neq \tau_{\boldsymbol{u}}(p^v)$, then $\tau_{\boldsymbol{u}}(p^{v+2}) = p\,\tau_{\boldsymbol{u}}(p^{v+1})$.*

(vi) *if $p > 2$ or $v > h + 1$, and $\tau_{\boldsymbol{u}}(p^{v+1}) \neq \tau_{\boldsymbol{u}}(p^v)$, then $\tau_{\boldsymbol{u}}(p^s) = p^{s-v}\tau_{\boldsymbol{u}}(p^v)$ for every integer $s \geq v$.*

Remark 6.10. The condition "$p > 2$ or $v > h + 1$" in Theorem 6.9(v) is a bit annoying but it cannot be removed. Indeed, with the notation of Theorem 6.9, let $\boldsymbol{u}$ be the linear recurrence such that $u_0 = 0$, $u_1 = 1$, and $u_n = u_{n-1} + 3u_{n-2}$ for every integer $n \geq 2$; and let $p := 2$, so that $h = 0$. Then $\tau_{\boldsymbol{u}}(2) = 3$, and $\tau_{\boldsymbol{u}}(2^2) = \tau_{\boldsymbol{u}}(2^3) = 6$.

Example 6.6. Let $\boldsymbol{F}$ be the linear recurrence of Fibonacci numbes and let m be a positive integer. Then $\tau_{\boldsymbol{F}}(m)$ is the *Pisano period* of m. ("Leonardo Pisano" was another name of Fibonacci, and "Pisano" is Italian for "from the city of Pisa"). For instance, from Theorem 6.9(vi) it follows that

$$\tau_{\boldsymbol{F}}(2^v) = 3 \cdot 2^{v-1}, \quad \tau_{\boldsymbol{F}}(3^v) = 8 \cdot 3^{v-1}, \quad \tau_{\boldsymbol{F}}(5^v) = 4 \cdot 5^v,$$

for every positive integer v.

The proof of Theorem 6.9 requires the following lemma.

Lemma 6.11. *Let $\boldsymbol{u}$ be a nonzero linear recurrence over $\mathbb{Z}$ with companion matrix $\boldsymbol{C}$ and Hankel matrix $\boldsymbol{H}$, and let $t > 0$, $n_0 \geq 0$, and $m > 0$ be integers. Then $\boldsymbol{u}$ modulo m has period t and preperiod n_0 if and only if $\boldsymbol{C}^{n_0}(\boldsymbol{C}^t - \boldsymbol{I})\boldsymbol{H} \equiv \boldsymbol{0} \pmod{m}$.*

Proof. By definition, the sequence $\boldsymbol{u}$ modulo m has period t and preperiod n_0 if and only if

$$u_{n+t} \equiv u_n \pmod{m} \qquad \text{for all integers } n \geq n_0. \tag{6.9}$$

It follows easily that (6.9) is equivalent to

$$u_{n+t} \equiv u_n \pmod{m} \qquad \text{for each } n \in \{n_0, \ldots, n_0 + 2k - 2\}. \tag{6.10}$$

From Theorem 2.59 it follows that (6.10) is equivalent to

$$\boldsymbol{C}^{n_0+t}\boldsymbol{H} \equiv \boldsymbol{C}^{n_0}\boldsymbol{H} \pmod{m},$$

which in turn is equivalent to $\boldsymbol{C}^{n_0}(\boldsymbol{C}^t - \boldsymbol{I})\boldsymbol{H} \equiv \boldsymbol{0} \pmod{m}$, as claimed. □

Now to the proof of Theorem 6.9.

Proof of Theorem 6.9. For the sake of brevity, let $\tau_i := \tau_{\boldsymbol{u}}(p^i)$ and $\rho_i := \rho_{\boldsymbol{u}}(p^i)$ for every positive integer i. Let w be an integer such that $h < w \leq v$. From Lemma 6.11 it follows that

$$\boldsymbol{C}^{\rho_w}(\boldsymbol{C}^{\tau_w} - \boldsymbol{I})\boldsymbol{H} \equiv \boldsymbol{0} \pmod{p^w}. \tag{6.11}$$

Multiplying (6.11) on the right by the adjugate of $\boldsymbol{H}$ yields that

$$\boldsymbol{C}^{\rho_w}(\boldsymbol{C}^{\tau_w} - \boldsymbol{I}) \det(\boldsymbol{H}) \equiv \boldsymbol{0} \pmod{p^w}. \tag{6.12}$$

In turn, recalling that $h := \nu_p\big(\det(\boldsymbol{H})\big)$ and $w > h$, from (6.12) it follows that

$$\boldsymbol{C}^{\rho_w}(\boldsymbol{C}^{\tau_w} - \boldsymbol{I}) \equiv \boldsymbol{0} \pmod{p^{w-h}}. \tag{6.13}$$

Furthermore, since $w \le v$, it follows easily that τ_w divides τ_v, and consequently $\boldsymbol{C}^{\tau_w} - \boldsymbol{I}$ divides $\boldsymbol{C}^{\tau_v} - \boldsymbol{I}$. Hence (6.13) implies that

$$\boldsymbol{C}^{\rho_w}(\boldsymbol{C}^{\tau_v} - \boldsymbol{I}) \equiv \boldsymbol{0} \pmod{p^{w-h}}. \tag{6.14}$$

From the binomial theorem, it follows that

$$\boldsymbol{C}^{p\tau_v} - \boldsymbol{I} = \big((\boldsymbol{C}^{\tau_v} - \boldsymbol{I}) + \boldsymbol{I}\big)^p - \boldsymbol{I} = \sum_{i=1}^{p} \binom{p}{i} (\boldsymbol{C}^{\tau_v} - \boldsymbol{I})^i,$$

which in turn implies that

$$\boldsymbol{C}^{\rho_v+\rho_w}(\boldsymbol{C}^{p\tau_v} - \boldsymbol{I})\boldsymbol{H} = \left(p\boldsymbol{C}^{\rho_w} + \sum_{i=2}^{p} \binom{p}{i} \boldsymbol{C}^{\rho_w}(\boldsymbol{C}^{\tau_v} - \boldsymbol{I})^{i-1}\right) \boldsymbol{C}^{\rho_v}(\boldsymbol{C}^{\tau_v} - \boldsymbol{I})\boldsymbol{H}. \tag{6.15}$$

From the fact that p divides $\binom{p}{i}$ for each $j \in \{1, \ldots, p-1\}$, and from (6.14), it follows that

$$\binom{p}{i} \boldsymbol{C}^{\rho_w}(\boldsymbol{C}^{\tau_v} - \boldsymbol{I})^{i-1} \equiv \boldsymbol{0} \pmod{p^2} \quad \text{for each } i \in \{2, \ldots, p-1\} \tag{6.16}$$

and

$$\boldsymbol{C}^{\rho_w}(\boldsymbol{C}^{\tau_v} - \boldsymbol{I})^{p-1} \equiv \boldsymbol{0} \pmod{p}. \tag{6.17}$$

Furthermore, from Lemma 6.11 it follows that

$$\boldsymbol{C}^{\rho_v}(\boldsymbol{C}^{\tau_v} - \boldsymbol{I})\boldsymbol{H} \equiv \boldsymbol{0} \pmod{p^v}. \tag{6.18}$$

Putting together (6.15), (6.16), (6.17), and (6.18) yields that

$$\boldsymbol{C}^{\rho_v+\rho_w}(\boldsymbol{C}^{p\tau_v} - \boldsymbol{I})\boldsymbol{H} \equiv \boldsymbol{0} \pmod{p^{v+1}},$$

which by Lemma 6.11 implies that $\rho_v + \rho_{h+1}$ and $p\,\tau_v$ are a preperiod and a period of $\boldsymbol{u}$ modulo p^{v+1}, respectively. Hence $\rho_{v+1} \le \rho_v + \rho_{h+1}$ and τ_{v+1} divides $p\,\tau_v$. This proves (i) and (ii). Then claims (iii) and (iii) follow easily by induction from (i) and (ii).

It remains to prove (v) and (vi). Suppose that $p > 2$ or $v > h + 1$, and $\tau_{v+1} \neq \tau_v$. Set $w := h + 2$ if $p = 2$, and $w := h + 1$ if $p > 2$ (note that $w \le v$ in any case). From (6.14) it follows that

$$\boldsymbol{C}^{2\rho_w}(\boldsymbol{C}^{\tau_v} - \boldsymbol{I})^{p-1} \equiv \boldsymbol{0} \pmod{p^2}. \tag{6.19}$$

Thus from (6.15), (6.16), and (6.19) if follows that

$$\boldsymbol{C}^{\rho_v+2\rho_w}(\boldsymbol{C}^{p\tau_v} - \boldsymbol{I})\boldsymbol{H} \equiv p\boldsymbol{C}^{\rho_v+2\rho_w}(\boldsymbol{C}^{\tau_v} - \boldsymbol{I})\boldsymbol{H} \pmod{p^{v+2}}. \tag{6.20}$$

Since $\tau_{v+1} \neq \tau_v$, from (i) it follows that $\tau_{v+1} = p\,\tau_v$. The goal is to prove that $\tau_{v+2} = p\,\tau_{v+1}$. For the sake of contradiction, suppose that $\tau_{v+2} \neq p\,\tau_{v+1}$. Hence $\tau_{v+2} = \tau_{v+1} = p\,\tau_v$ by claim (i). Then Lemma 6.11 implies that

$$\boldsymbol{C}^{\rho_{v+2}}(\boldsymbol{C}^{p\tau_v} - \boldsymbol{I})\boldsymbol{H} \equiv \boldsymbol{0} \pmod{p^{v+2}}. \tag{6.21}$$

From (6.20) and (6.21) it follows that

$$\boldsymbol{C}^{\rho_v+\rho_{v+2}+2\rho_w}(\boldsymbol{C}^{\tau_v} - \boldsymbol{I})\boldsymbol{H} \equiv \boldsymbol{0} \pmod{p^{v+1}}.$$

Hence, Lemma 6.11 implies that τ_v is a period of $\boldsymbol{u}$ modulo p^{v+1}, and so τ_{v+1} divides τ_v. But this is impossible, since $\tau_{v+1} = p\,\tau_v$. Thus $\tau_{v+2} = p\,\tau_{v+1}$. This proves (v). Now (vi) follows by induction from (i) and (v). □

The following theorem is an explicit upper bound for the period of a linear recurrence modulo a prime power.

Theorem 6.12. *Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$ of positive order k, let $\boldsymbol{H}$ be the Hankel matrix of $\boldsymbol{u}$, and let p be a prime number not dividing* $\det(\boldsymbol{H})$. *Then $\tau_{\boldsymbol{u}}(p^v) \leq p^{v-1}(p^k - 1)$ for every positive integer v.*

Proof. By Theorem 6.6, $\tau_{\boldsymbol{u}}(p) \leq p^k - 1$. The claim follows from Theorem 6.9(iii). □

Theorem 6.12 motivates the following definition. Let p be a prime number and let v be a positive integer. A linear recurrence $\boldsymbol{u}$ over $\mathbb{Z}$ of positive order k is a *maximal-period sequence modulo p^v* if $\tau_{\boldsymbol{u}}(p^v) = p^{v-1}(p^k - 1)$ (cf. Section 4.4).

The following theorem provides a construction of a maximal-period sequences modulo a prime power.

Theorem 6.13. *Let $p > 2$ be a prime number and let $f \in \mathbb{Z}[x]$ be a polynomial of positive degree k. Suppose that f modulo p is a primitive polynomial in $\mathbb{F}_p$. Put $f_0(x) := f(x)$ and $f_1(x) := f(x) + p$. Then, for at least one $i \in \{0, 1\}$, the impulse sequence $\boldsymbol{\delta}^{(k-1)}(f_i)$ (Section 2.2.2) is a maximal-period sequence modulo p^v for every positive integer v.*

Proof. Let $i \in \{0, 1\}$, put $\boldsymbol{u}_i := \boldsymbol{\delta}^{(k-1)}(f_i)$, and let $\boldsymbol{C}_i$ and $\boldsymbol{H}_i$ be the companion matrix and the Hankel matrix of $\boldsymbol{u}_i$, respectively. Since f modulo p is a primitive polynomial in $\mathbb{F}_p$, from Theorem 4.10 it follows that $\boldsymbol{u}_i$ is a maximal-period sequence modulo p. Hence $\tau_{\boldsymbol{u}_i}(p) = p^k - 1$. Furthermore $\det(\boldsymbol{H}_i) = 1$, since $\boldsymbol{u}_i$ is an impulse sequence.

Suppose that $\tau_{\boldsymbol{u}_i}(p^2) \neq \tau_{\boldsymbol{u}_i}(p) = p^k - 1$. From Theorem 6.9(vi) it follows that

$$\tau_{\boldsymbol{u}_i}(p^v) = p^{v-1}\tau_{\boldsymbol{u}_i}(p) = p^{v-1}(p^k - 1),$$

for every positive integer v. Thus $\boldsymbol{u}_i$ is a maximal-period sequence modulo p^v for every positive integer v, as desired.

Suppose that $\tau_{\boldsymbol{u}_i}(p^2) = \tau_{\boldsymbol{u}_i}(p) = p^k - 1$. From Lemma 6.11, it follows that

$$\boldsymbol{C}_i^{\rho_{\boldsymbol{u}}(p^2)}(\boldsymbol{C}_i^{p^k-1} - \boldsymbol{I})\boldsymbol{H}_i \equiv \boldsymbol{0} \pmod{p^2}. \tag{6.22}$$

Since $\det(\boldsymbol{C}_i) = f_i(0)$ and $\det(\boldsymbol{H}_i) = 1$, the matrices $\boldsymbol{C}_i$ and $\boldsymbol{H}_i$ are both invertible modulo p. Thus (6.22) implies that $\boldsymbol{C}_i^{p^k-1} \equiv \boldsymbol{I} \pmod{p^2}$. In turn, this gives that

$$f_i(0)^{p^k-1} \equiv \det(\boldsymbol{C}_i)^{p^k-1} \equiv \det(\boldsymbol{C}_i^{p^k-1}) \equiv \det(\boldsymbol{I}) \equiv 1 \pmod{p^2},$$

because the determinant of a matrix is a polynomial of its entries. But

$$f_1(0)^{p^k-1} \equiv (f_0(0)+p)^{p^k-1} \equiv f_0(0)^{p^k-1} + (p^k-1)pf_0(0)^{p^k-2} \not\equiv f_0(0)^{p^k-1} \pmod{p^2}.$$

Hence $\tau_{\boldsymbol{u}_i}(p^2) \neq \tau_{\boldsymbol{u}_i}(p)$ for at least one $i \in \{0,1\}$, and so $\boldsymbol{u}_i$ is a maximal-period sequence modulo p^v for every positive integer v. □

6.5 Number of zeros modulo m

Throughout this section, let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{Z}$ of order $k \geq 2$. For all integers $M \geq 0$ and $N, m > 0$, let $R_{\boldsymbol{u}}(M, N, m)$ be the number of integers n such that $M \leq n < M+N$ and $u_n \equiv 0 \pmod{m}$.

The goal of this section is to provide an upper bound for $R_{\boldsymbol{u}}(M, N, m)$. This is useful in several situations, such as estimating the number of prime factor of u_n (Section 6.6) and lower bounding the greatest prime factor of u_n (Section 6.7).

It is necessary to introduce some notation. Let f be the minimal polynomial of $\boldsymbol{u}$, let $\mathbb{K}$ be the splitting field of f over $\mathbb{Q}$, let $\alpha_1, \ldots, \alpha_s \in \mathcal{O}_{\mathbb{K}}$ be the pairwise distinct roots of f, and let $k_1, \ldots, k_s$ be their respective multiplicities.

Let $t_1, \ldots, t_k$ be a fixed enumeration of the k functions $n \mapsto n^j \alpha_i^n$, where $i \in \{1, \ldots, s\}$ and $j \in \{0, \ldots, k_i - 1\}$. Assume that $t_1(n) = \alpha_1^n$. From Theorem 2.15, there exist a positive integer Δ and coefficients $c_i \in \mathcal{O}_{\mathbb{K}}$ such that

$$u_n = \frac{1}{\Delta} \sum_{j=1}^{k} c_j t_j(n) \tag{6.23}$$

for every integer $n \geq 0$.

For each $h \in \{1, \ldots, k\}$ and for all integers $n_1, \ldots, n_h$, define the determinant

$$D_h(n_1, \ldots, n_h) := \det\Big(\big(t_j(n_i)\big)_{1 \leq i,j \leq h}\Big).$$

(This determinant occurred earlier in the proof of Lemma 5.22.) Let $T(m)$ be the supremum of the positive integers t such that m does not divide

$$\max\Big\{1, \big|\mathrm{N}_{\mathbb{K}/\mathbb{Q}}\big(D_k(n_1, \ldots, n_k)\big)\big|\Big\}$$

for all integers $n_1, \ldots, n_k \in [0, t)$.

Finally, in light of Theorem 5.13, let Z_k be the maximum number of zeros of a nondegenerate linear recurrence over $\mathbb{K}$ of order at most k.

The main result of this section is the following theorem.

Theorem 6.14. *Let $M \geq 0$ and $N > 0$ be integers, and let m be a positive integer coprime to Δ and to infinitely many terms of $\boldsymbol{u}$. Then*

$$R_{\boldsymbol{u}}(M, N, m) \leq (Z_k + k - 1)\left(\frac{N}{T(m)} + 1\right) \tag{6.24}$$

with the convention that $N/+\infty := 0$.

The proof of Theorem 6.14 requires several lemmas.

Lemma 6.15. *Let $n_1, \dots, n_h$ be integers with $h < k$. Suppose that $D_h(n_1, \dots, n_h) \neq 0$. Then there are at most Z_k integers $n \geq 0$ such that $D_{h+1}(n_1, \dots, n_h, n) = 0$.*

Proof. By the Laplace expansion with respect to the last column, the determinant

$$D_{h+1}(n_1, \dots, n_h, n)$$

is a nondegenerate linear recurrence over $\mathbb{K}$ of order at most k (in particular, it is nonzero since its power-sum expansion contains the term $t_{h+1}(n)$). Hence the claim follows from the definition of Z_k. □

Lemma 6.16. *Let $M, n_1, \dots, n_k \geq 0$ be integers, and let m be a positive integer coprime to Δ and to infinitely many terms of $\boldsymbol{u}$. Suppose that $u_{M+n_i} \equiv 0 \pmod{m}$ for each $i \in \{1, \dots, k\}$. Then $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}\big(D_k(n_1, \dots, n_k)\big) \equiv 0 \pmod{m}$.*

Proof. From (6.23) it follows that there exist $c'_1, \dots, c'_k \in \mathcal{O}_{\mathbb{K}}$ such that

$$u_{M+n} = \frac{1}{\Delta}\sum_{j=1}^{k} c'_j t_j(n) \tag{6.25}$$

for every integer $n \geq 0$. Let $\mathcal{I}$ be the ideal of $\mathcal{O}_{\mathbb{K}}$ generated by $c'_1, \dots, c'_k$. Since $\mathcal{I} \cap \mathbb{Z}$ is a nonzero ideal of $\mathbb{Z}$, there exists a unique positive integer ℓ such that $\mathcal{I} \cap \mathbb{Z} = \ell\mathbb{Z}$. From (6.25) it follows that ℓ divides Δu_{M+n} for every integer $n \geq 0$. Since m is coprime to Δ and to infinitely many terms of $\boldsymbol{u}$, it follows that ℓ is coprime to m. As a consequence $\mathcal{I}$ is coprime to $m\mathcal{O}_{\mathbb{K}}$. Recalling that $u_{M+n_i} \equiv 0 \pmod{m}$ for each $i \in \{1, \dots, k\}$, from (6.25) it follows that

$$\sum_{j=1}^{k} c'_j t_j(n_i) \equiv 0 \pmod{m\mathcal{O}_{\mathbb{K}}} \tag{6.26}$$

for each $i \in \{1, \dots, k\}$. Let $\boldsymbol{A} := \big(t_j(n_i)\big)_{1 \leq i,j \leq k}$ and $\boldsymbol{c} = \begin{pmatrix} c'_1 & \cdots & c'_k \end{pmatrix}^{\mathsf{T}}$. Then (6.26) is equivalent to

$$\boldsymbol{A}\boldsymbol{c} \equiv \boldsymbol{0} \pmod{m\mathcal{O}_{\mathbb{K}}}. \tag{6.27}$$

Multiplying (6.27) on the left by the adjugate of $\boldsymbol{A}$ yields that

$$\det(\boldsymbol{A})\boldsymbol{c} \equiv \boldsymbol{0} \pmod{m\mathcal{O}_{\mathbb{K}}}. \tag{6.28}$$

Since $\mathcal{I}$ is coprime to $m\mathcal{O}_{\mathbb{K}}$, there exists $\boldsymbol{b} \in \mathcal{O}_{\mathbb{K}}^{1\times k}$ such that $\boldsymbol{bc} \equiv 1 \pmod{m\mathcal{O}_{\mathbb{K}}}$. Multiplying (6.28) on the left by $\boldsymbol{b}$ gives that

$$\det(\boldsymbol{A}) \equiv 0 \pmod{m\mathcal{O}_{\mathbb{K}}},$$

that is,

$$D_k(n_1, \dots, n_k) \equiv 0 \pmod{m\mathcal{O}_{\mathbb{K}}},$$

Hence $m\mathcal{O}_{\mathbb{K}}$ divides the ideal of $\mathcal{O}_{\mathbb{K}}$ generated by $D_k(n_1, \dots, n_k)$. Thus $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(m)$, which is equal to $m^{[\mathbb{K}:\mathbb{Q}]}$, divides $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}\big(D_k(n_1, \dots, n_k)\big)$. This implies that

$$\mathrm{N}_{\mathbb{K}/\mathbb{Q}}\big(D_k(n_1, \dots, n_k)\big) \equiv 0 \pmod{m},$$

as claimed. □

Everything is ready for the proof of Theorem 6.14.

Proof of Theorem 6.14. It suffices to prove that

$$R_{\boldsymbol{u}}(M, T(m), m) \le Z_k + k - 1. \tag{6.29}$$

Indeed, the general upper bound (6.24) follows from (6.29) since

$$R_{\boldsymbol{u}}(M, N, m) \le \sum_{i=0}^{\lfloor N/T(m)\rfloor} R_{\boldsymbol{u}}(M + T(m)i, T(m), m) \le (Z_k + k - 1)\left(\frac{N}{T(m)} + 1\right).$$

For the sake of contradiction, suppose that (6.29) is false. Hence the set

$$\mathcal{S} := \big\{n \in \mathbb{N} : n < T(m),\ u_{M+n} \equiv 0 \pmod{m}\big\}$$

has at least $Z_k + k$ elements. Claim: there exist integers $n_1, \dots, n_k \in \mathcal{S}$ such that

$$D_k(n_1, \dots, n_k) \neq 0. \tag{6.30}$$

Indeed, construct $n_1, \dots, n_k$ as follows. First, pick an arbitrary $n_1 \in \mathcal{S}$. Thus $D_1(n_1) = \alpha_1^{n_1} \neq 0$. Then, assuming that $n_1, \dots, n_h \in \mathcal{S}$ $(h < k)$ such that $D_h(n_1, \dots, n_h) \neq 0$ have been constructed, pick $n_{h+1} \in \mathcal{S} \setminus \{n_1, \dots, n_h\}$ such that $D_{h+1}(n_1, \dots, n_{h+1}) \neq 0$. This is possible thanks to Lemma 6.15, since

$$\big|\mathcal{S} \setminus \{n_1, \dots, n_h\}\big| \ge |\mathcal{S}| - h \ge Z_k + k - h > Z_k.$$

This proves the claim. Furthermore, from Lemma 6.16 it follows that

$$\mathrm{N}_{\mathbb{K}/\mathbb{Q}}\big(D_k(n_1, \dots, n_k)\big) \equiv 0 \pmod{m}. \tag{6.31}$$

But (6.30) and (6.31) contradict the definition of $T(m)$. This proves (6.29). □

Theorem 6.14 has the disadvantage of involving $T(m)$, whose definition is a bit convoluted. The next theorem provides a more explicit upper bound.

Theorem 6.17. *Let $M \geq 0$ and $N > 0$ be integers, and let $m \geq 2$ be an integer coprime to Δ and with infinitely many terms of $\boldsymbol{u}$. Then*

$$R_{\boldsymbol{u}}(M, N, m) < C\left(\frac{N}{\log m} + 1\right) \tag{6.32}$$

where $C > 0$ is an effectively computable constant depending only on $\boldsymbol{u}$.

Remark 6.18. Without further hypotheses, Theorem 6.17 is optimal. Indeed, let $\boldsymbol{u} = 2^n - 1$ be the sequence of Mersenne numbers and take $m := u_r$ for some integer $r \geq 2$. Since $\boldsymbol{u}$ is a divisibility sequence (Theorem 6.4), it follows easily that

$$R_{\boldsymbol{u}}(M, N, m) \geq \left\lfloor \frac{N}{r} \right\rfloor > C\left(\frac{N}{\log m} + 1\right)$$

for all integers $M \geq 0$ and $N \geq r$, where $C > 0$ is an absolute constant.

The proof of Theorem 6.17 needs the following lemma.

Lemma 6.19. *Let $m \geq 2$ be an integer. Then $T(m) > C \log m$, where $C > 0$ is an effectively computable constant depending only on $\boldsymbol{u}$.*

Proof. Let $A > 1$ be a constant greater than the absolute values of the roots $\alpha_1, \ldots, \alpha_s$ and all their algebraic conjugates, let d be the degree of $\mathbb{K}$ over $\mathbb{Q}$, and put

$$C := \tfrac{1}{2}\left(d \log\left(k!\, \mathrm{e}^{k^2} A^k\right)\right)^{-1} \quad \text{and} \quad U := C \log m.$$

Then, for all integers $n_1, \ldots, n_k \in [0, U]$,

$$\begin{aligned} \left|\mathrm{N}_{\mathbb{K}/\mathbb{Q}}\big(D_k(n_1, \ldots, n_k)\big)\right| &\leq \left(k!\,(n_1+1)^k \cdots (n_k+1)^k A^{n_1+\cdots+n_k}\right)^d \\ &\leq \left(k!\,(U+1)^{k^2} A^{kU}\right)^d \leq \left(k!\,\mathrm{e}^{k^2} A^k\right)^{dU} \leq m^{1/2} < m. \end{aligned}$$

The claim follows. □

Proof of Theorem 6.17. The claim follows at once from Theorem 6.14 and Lemma 6.19. □

Both Theorem 6.14 and Theorem 6.17 require the positive integer m to be coprime to infinitely many terms of $\boldsymbol{u}$. The next result states that the set of prime numbers that are not coprime to infinitely many terms of $\boldsymbol{u}$ is finite and effectively computable.

Theorem 6.20. *Let $\boldsymbol{u}$ be a reversible linear recurrence over $\mathbb{Z}$ of positive order k, and let $\mathcal{P}$ be the set of prime numbers p for which there exists an integer $n_p \geq 0$ such that p divides u_n for every integer $n \geq n_p$. Then $\mathcal{P}$ is finite and effectively computable in terms of the initial values and the minimal polynomial of $\boldsymbol{u}$.*

Proof. Let f be the minimal polynomial of $\boldsymbol{u}$, and let p be a prime number. If p does not divide $f(0)$ then, by Theorem 6.6, the linear recurrence $\boldsymbol{u}$ modulo p is periodic. Hence $p \in \mathcal{P}$ if and only if $u_0 \equiv \cdots \equiv u_{k-1} \equiv 0 \pmod{p}$. If p does divide $f(0)$ then, again by Theorem 6.6, the linear recurrence $\boldsymbol{u}$ modulo p is ultimately periodic with preperiod $\rho_{\boldsymbol{u}}(p) < p^k$. Hence $p \in \mathcal{P}$ if and only if $u_{p^k} \equiv \cdots \equiv u_{p^k+k-1} \equiv 0 \pmod{p}$. Thus $\mathcal{P}$ is the set of the prime factors of

$$\gcd(u_0, \dots, u_{k-1}) \prod_{p \,|\, f(0)} \gcd(f(0), u_{p^k}, \dots, u_{p^k+k-1}),$$

and so $\mathcal{P}$ is finite and effectively computable. □

6.6 Number of prime factors

For all nonzero integers n, let $\omega(n)$ be the number of prime factors of n. For each sequence $\boldsymbol{u} \in \mathbb{Z}^{\mathbb{N}}$ and for all integers $M \geq 0$ and $N > 0$, let

$$\omega_{\boldsymbol{u}}(M, N) := \omega\Big(\prod_{\substack{M \leq n < M+N \\ u_n \neq 0}} u_n \Big).$$

In other words, the quantity $\omega_{\boldsymbol{u}}(M, N)$ is the number of primes that divides at least a nonzero term u_n for some integer n such that $M \leq n < M + N$.

The next theorem provides a lower bound for $\omega_{\boldsymbol{u}}(M, N)$ when $\boldsymbol{u}$ is a nondegenerate linear recurrence.

Theorem 6.21. *Let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{Z}$ of order $k \geq 2$. Then*

$$\omega_{\boldsymbol{u}}(M, N) > C_1 \min\left\{ N, \frac{M+N}{\log N} \right\}, \tag{6.33}$$

for all integers $M \geq 0$ and $N > C_2$, where $C_1, C_2 > 0$ are effectively computable constants depending only on $\boldsymbol{u}$.

Proof. Hereafter, let $C_1, C_2, \dots$ denote positive effectively computable constants depending only on $\boldsymbol{u}$. Let $M \geq 0$ and $N > C_2$ be integers, and define

$$\Pi := \prod_{\substack{M \leq n < M+N \\ u_n \neq 0}} |u_n|.$$

Let Δ be defined as in Section 6.5. Hereafter, ignore the prime numbers p that divides Δ and that are not coprime to infinitely many terms of $\boldsymbol{u}$. By Theorem 6.20, there are only finitely many, and effectively computable, such primes; and so they do not effect the coming bounds. Theorem 5.15 implies that $|u_n| < \mathrm{e}^{C_3(n+1)}$ for every integer $n \geq 0$. Let p be a prime number and put $a_p := C_3(M+N)/\log p$. Then, for all integers $n \in [M, M+N)$ and

$v \geq 0$, if p^v divides u_n then either $u_n = 0$ or $v < a_p$. As a consequence, also thanks to Theorem 6.17, for every prime factor p of Π,

$$\nu_p(\Pi) \leq \sum_{v=1}^{a_p} R_{\boldsymbol{u}}(M, N, p^v) \leq \sum_{v=1}^{a_p} C_4\left(\frac{N}{\log(p^v)} + 1\right) = C_4\left(\frac{N}{\log p}\sum_{v=1}^{a_p}\frac{1}{v} + a_p\right)$$
$$< C_4\left(\frac{N\log(a_p\mathrm{e})}{\log p} + a_p\right) < C_5\frac{M + N\log(M+N)}{\log p}.$$

Hence, if $p_1, \ldots, p_r$ are all the prime factors of Π, then

$$\log\Pi = \sum_{i=1}^{r} \nu_{p_i}(\Pi)\log p_i < C_5\big(M + N\log(M+N)\big)r. \tag{6.34}$$

From Theorem 5.21, $|u_n| > \mathrm{e}^{C_6 n}$ for all integers $n \in [M, M+N)$ but at most $\lceil N/2\rceil + 1$ exceptions. Then

$$\log\Pi > C_6 \sum_{n=M}^{M+\lceil N/2\rceil} n > \tfrac{1}{8}C_6 N(M+N). \tag{6.35}$$

Putting together (6.34) and (6.35) yields

$$r > \frac{C_7 N(M+N)}{M + N\log(M+N)}. \tag{6.36}$$

If $(M+N)/\log N < N$, then $M + N\log(M+N) < 3N\log N$. Thus (6.36) implies (6.33). If $(M+N)/\log N \geq N$, then

$$\frac{M + N\log(M+N)}{M+N} < 1 + \frac{N\log(M+N)}{M+N} < 1 + \frac{N\log(N\log N)}{N\log N} < 3. \tag{6.37}$$

Hence (6.36) and (6.37) imply (6.33). □

For every real number X, and for each sequence $\boldsymbol{u} \in \mathbb{Z}^{\mathbb{N}}$, let $\pi_{\boldsymbol{u}}(X)$ be the number of primes $p \leq X$ such that p divides a nonzero term u_n for some integer $n \geq 0$.

Theorem 6.22. *Let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{Z}$ of order $k \geq 2$. Then*

$$\pi_{\boldsymbol{u}}(X) > \frac{C_1\log X}{\log\log X},$$

for all real numbers $X > C_2$, where $C_1, C_2 > 0$ are effectively computable constants depending only on $\boldsymbol{u}$.

Proof. From Theorem 5.15 it follows that there exists an effectively computable constant $C_3 > 0$, depending only on $\boldsymbol{u}$, such that $|u_n| < \mathrm{e}^{C_3(n+1)}$ for every integer $n \geq 0$. Put $N := \lfloor C_3^{-1}\log X\rfloor$. Hence, if p is a prime number such that p divides a nonzero term u_n, for some integer $n \in [0, N)$, then $p < X$. This consideration and Theorem 6.21 imply that

$$\pi_{\boldsymbol{u}}(X) \geq \omega_{\boldsymbol{u}}(0, N) > \frac{C_4 N}{\log N} > \frac{C_1\log X}{\log\log X},$$

for all real numbers $X > C_2$, where $C_1, C_2, C_4 > 0$ are effectively computable constants depending only on $\boldsymbol{u}$. □

It is believed that the bound of Theorem 6.22 can be strengthened to

$$\pi_{\boldsymbol{u}}(X) > \frac{C_1 X}{\log X},$$

for all real numbers $X > C_2$, where $C_1, C_2 > 0$ are effectively computable constants depending only on $\boldsymbol{u}$ (see the bibliographical notes).

6.7 Greatest prime factor

For every integer n such that $|n| > 1$, let $P(n)$ be the greatest prime factor of n. Put also $P(0) := 0$ and $P(\pm 1) := 1$ (these values are immaterial).

Theorem 6.23. *Let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{Z}$ with at least two distinct roots. Then $P(u_n) \to +\infty$ as $n \to +\infty$.*

The proof of Theorem 6.23 is not included here. It employs the same results on S-unit equations used in the proof of Theorem 5.17. As for Theorem 5.17, the lower bound of Theorem 6.23 is ineffective. (An effective lower bound would solve Problem 5.2).

The following theorem provides an effective lower bound for the greatest prime factor of the terms of a linear recurrence having a single dominant root.

Theorem 6.24. *Let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{Z}$ with a single dominant root α_1 and at least another root $\alpha_2 \neq \alpha_1$. Then there exists an effectively computable constant $C > 0$, depending only on $\boldsymbol{u}$, such that*

$$P(u_n) > \frac{C \log n \log\log n}{\log\log\log n}$$

for every integer $n \geq 3$.

Theorem 6.24 is a consequence of the following more general statement.

Lemma 6.25. *Let α be an algebraic number such that $|\alpha| > 1$, let f be a nonzero polynomial with coefficients that are algebraic numbers, let $\delta \in (0, 1)$, let $C > 0$ be a real number, and let $\boldsymbol{u} \in \mathbb{Z}^{\mathbb{N}}$ be a sequence. Suppose that*

$$0 < |u_n - f(n)\alpha^n| < |\alpha|^{\delta n} \tag{6.38}$$

for every integer $n > C$. Then there exists an effectively computable constant $C_1 > 0$, depending only on α, f, δ, and C, such that

$$P(u_n) > \frac{C_1 \log n \log\log n}{\log\log\log n} \tag{6.39}$$

for every integer $n \geq 3$.

Proof. Hereafter, let $C_1, C_2, \dots$ denote positive effectively computable constants depending only on α, f, δ, and C. Let $\mathbb{K}$ be the number field obtained by adjoining α and the coefficients of f to $\mathbb{Q}$, and put $D := [\mathbb{K} : \mathbb{Q}]$. Let $n > C_2$ be an integer and write $u_n = (-1)^{b_0} p_1^{b_1} \cdots p_k^{b_k}$, where $b_0 \in \{0, 1\}$, $b_1, \dots, b_k$ are positive integers and $p_1 < \cdots < p_k$ are prime numbers. From (6.38) it follows that

$$\max\{b_0, \dots, b_k\} < C_3 n.$$

From the properties of the absolute logarithmic height (Theorem A.41), it follows that $\mathrm{h}(f(n)) < C_4 \log n$. Therefore, Theorem 5.19 implies that

$$\begin{aligned} |u_n f(n)^{-1} \alpha^{-n} - 1| &= |(-1)^{b_0} p_1^{b_1} \cdots p_k^{b_k} f(n)^{-1} \alpha^{-n} - 1| \\ &> \exp\left(-C_5^k \log p_1 \cdots \log p_k (\log n)^2\right). \end{aligned} \tag{6.40}$$

Hence, from (6.38) and (6.40), it follows that

$$\prod_{i=1}^{k} \log p_i > \frac{C_6 n}{C_5^k (\log n)^2}.$$

Furthermore, from the arithmetic-geometric mean inequality, it follows that

$$\sum_{i=1}^{k} \log p_i \geq k \left(\prod_{i=1}^{k} \log p_i \right)^{1/k} > \frac{k}{C_5} \left(\frac{C_6 n}{(\log n)^2} \right)^{1/k}. \tag{6.41}$$

In turn, by the prime number theorem (Corollary A.39) and (6.41),

$$P(u_n) = p_k > C_7 \sum_{p \leq p_k} \log p \geq C_7 \sum_{i=1}^{k} \log p_i > C_8 k \left(\frac{C_6 n}{(\log n)^2} \right)^{1/k}. \tag{6.42}$$

Let $L := \log n \log\log n / \log\log\log n$. If $k \geq L$, then (6.39) follows at once from (6.42). Hence, suppose that $k < L$. Note that, for fixed n, the right-hand side of (6.42) as a function of k is monotone decreasing over the interval $\left[1, \log\left(C_6 n/(\log n)^2\right)\right]$. Since $L < \log\left(C_6 n/(\log n)^2\right)$, from (6.42) it follows that

$$P(u_n) > C_8 L \left(\frac{C_6 n}{(\log n)^2} \right)^{1/L} = C_8 L \exp\left(\frac{1}{L} \log\left(\frac{C_6 n}{(\log n)^2} \right) \right) > C_8 L,$$

which is (6.39). □

Proof of Theorem 6.24. The claim follows at once from Theorem 5.16 and Lemma 6.25. □

The following result is a lower bound for $P(u_n)$ that holds for almost all integers $n \geq 0$.

Theorem 6.26. *Let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{Z}$ of order $k \geq 2$ and let f be a monotone increasing function $[0, +\infty) \to [2, +\infty)$ such that $f(X) = o(X)$ as $X \to +\infty$. Then*

$$P(u_n) > f(n)$$

for all integers $n \in [0, X]$ but at most $o(X)$ exceptions, as $X \to +\infty$.

Proof. The proof is quite similar to the proof of Theorem 6.21. Hereafter, let $C_1, C_2, \dots$ denote positive effectively computable constants depending only on $\boldsymbol{u}$. Let $\mathcal{E}$ be the set of integers $n \in [0, X]$ such that $P(u_n) \le f(n)$, and let

$$\Pi' := \prod_{n \in \mathcal{E}} |u_n|.$$

A slight adaptation of the reasoning leading to (6.34) (again ignoring finitely many prime factors of Π') yields that

$$\log \Pi' = \sum_{p \le f(X)} \nu_p(\Pi') \log p < C_1 X (\log X) \sum_{p \le f(X)} 1 < \frac{C_2 X (\log X) f(X)}{\log f(X)}, \tag{6.43}$$

for all real numbers $X > C_3$, where the last inequality is due to the prime number theorem (Theorem A.37).

From Theorem 5.21, $|u_n| > \mathrm{e}^{C_4 n}$ for all integers $n \in [0, X]$ but at most $C_5 \log X$ exceptions. Let $\mathcal{E}'$ be the set of integers $n \in [0, X]$ such that $|u_n| \le \mathrm{e}^{C_4 n}$.

If $|\mathcal{E} \setminus \mathcal{E}'| \le |\mathcal{E}|/2$ then

$$|\mathcal{E}| \le |\mathcal{E} \setminus \mathcal{E}'| + |\mathcal{E}'| \le \tfrac{1}{2}|\mathcal{E}| + |\mathcal{E}'|$$

and consequently

$$|\mathcal{E}| \le 2|\mathcal{E}'| \le 2C_5 \log X = o(X),$$

as $X \to +\infty$. Thus the claim follows.

Hence, assume that $|\mathcal{E} \setminus \mathcal{E}'| > |\mathcal{E}|/2$. Then

$$\log \Pi' \ge \sum_{n \in \mathcal{E} \setminus \mathcal{E}'} \log |u_n| > C_4 \sum_{n \in \mathcal{E} \setminus \mathcal{E}'} n > C_4 \sum_{n=0}^{|\mathcal{E} \setminus \mathcal{E}'|} n > C_4 \sum_{n=0}^{\lfloor |\mathcal{E}|/2 \rfloor} n > C_5 |\mathcal{E}|^2. \tag{6.44}$$

Putting together (6.43) and (6.44) yields that

$$|\mathcal{E}| < C_6 \left(\frac{X (\log X) f(X)}{\log f(X)} \right)^{1/2}. \tag{6.45}$$

If $f(X) > X/(\log X)^2$ then $\log f(X) > (\log X)/2$, and from (6.45) it follows that

$$|\mathcal{E}| < C_5 \big(2X f(X)\big)^{1/2} = o(X),$$

as $X \to +\infty$. If $f(X) \le X/(\log X)^2$ then from (6.45) it follows that

$$|\mathcal{E}| < C_6 \left(\frac{X^2}{(\log 2)(\log X)} \right)^{1/2} = o(X),$$

as $X \to +\infty$. Thus in any case $|\mathcal{E}| = o(X)$, which is the claim. □

6.8 Composite terms

Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$ and let $\mathcal{P}_{\boldsymbol{u}}$ be the set of integers $n \geq 0$ such that u_n is a prime number. The takeaways of Section 6.3 are that establishing if $\mathcal{P}_{\boldsymbol{u}}$ is infinite (Problem 6.1) is beyond current techniques and that heuristic arguments suggest that $\mathcal{P}_{\boldsymbol{u}}$, even if infinite, should be quite sparse (Section 6.3.2). Hence, it is tempting to hope that a solution to the following problem is attainable.

Problem 6.2. Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$. Is u_n composite for all integers $n \geq 0$ but a set of natural density zero?

Unfortunately, in a somehow ironic way, Problem 6.2 is also open. For instance, the answer is unknown even for the seemingly innocent linear recurrence $u_n = 2^n + 5$. However, there exists a small family of linear recurrences for which Problem 6.2 is known to have an affirmative answer.

A *Cullen sequence* is a linear recurrence $\boldsymbol{u}$ over $\mathbb{Z}$ whose power-sum representation has the form

$$u_n = c_0 n a_0^n - \sum_{i=1}^{k} c_i a_i^n, \tag{6.46}$$

for every integer $n \geq 0$, where $a_0, \ldots, a_k$ $(k \geq 2)$ are pairwise distinct nonzero integers and $c_0, c_1, \ldots, c_k$ are nonzero rational numbers.

Example 6.7 (Cullen numbers)**.** The sequence of *Cullen numbers* (C_n) is defined by $C_n := n2^n + 1$ for every integer $n \geq 0$. Its name honors James Cullen [42], a Jesuit priest that in 1905 observed that C_n is composite for every integer $n \in [2, 100]$ with the possible exception of $n = 53$. Shortly later, Cunningham [43] showed that C_{53} is composite. A *Cullen prime* is a Cullen number that is prime. As to date, the only known Cullen primes C_n are those for n equal to

$$\begin{aligned} &1,\ 141,\ 4713,\ 5795,\ 6611,\ 18496,\ 32292,\ 32469,\ 59656,\\ &90825,\ 262419,\ 361275,\ 481899,\ 1354828,\ 6328548,\ 6679881; \end{aligned}$$

and the PrimeGrid project [150] showed that there are no others for $n < 26,897,819$. For more on the early history of Cullen numbers, see the article by Keller [93].

Example 6.8 (Woodall numbers)**.** The sequence of *Woodall numbers* (W_n) is defined by $W_n := n2^n - 1$ for every integer $n \geq 0$. Cunningham and Woodall [44] studied Woodall numbers after been inspired by the similarly defined Cullen numbers.

Example 6.9. The linear recurrence $\boldsymbol{u}$ defined by $u_n = 11^n + n$ for every integer $n \geq 0$ does not have a name, but it has a peculiar property: none of its first $1,181,716$ terms is prime [143, A093324]. (Note that, by the arguments of Section 6.3, the sequence $\boldsymbol{u}$ is expected to have infinitely many prime terms.) It is unknown if $u_{1,181,716}$ (which has $1,230,631$ decimal digits) is a prime number. Shenton [116] checked that it has a very high probability of being prime, in the sense that it passes many probabilistic primality tests.

The following theorem says that almost all terms of a Cullen sequence are composite.

Theorem 6.27. *Let $\boldsymbol{u}$ be a Cullen sequence. Then u_n is composite for all integers $n \geq 0$ but a set of natural density zero.*

The rest of this section is devoted to the proof of Theorem 6.27. Hereafter, let $\boldsymbol{u}$ be the Cullen sequence satisfying (6.46), let $\boldsymbol{v}$ be the linear recurrence defined by

$$v_n = \sum_{i=1}^{k} c_i a_i^n, \tag{6.47}$$

for every integer $n \geq 0$, and let A be the product of $a_0, \dots, a_k$ and the denominators of $c_0, \dots, c_k$. For the sake of brevity, write (a, b) and $[a, b]$ for the greatest common divisor and the least common multiple, respectively, of the integers a and b. Note that, by Euler's theorem, if d is a positive integer coprime to A, then the linear recurrence $\boldsymbol{v}$ modulo d and the geometric progression (a_0^n) modulo d have both period $\varphi(d)$; while the linear recurrence $\boldsymbol{u}$ modulo d has period $\big[d, \varphi(d)\big]$.

The following lemma is the key to the proof of Theorem 6.27 and provides an exact formula for the number of zeros of $\boldsymbol{u}$ modulo d over a period.

Lemma 6.28. *Let d be a positive integer coprime to A. Then there are exactly*

$$\frac{\varphi(d)}{\big(d, \varphi(d)\big)}$$

integers n such that $0 \leq n < \big[d, \varphi(d)\big]$ and $u_n \equiv 0 \pmod{d}$.

Proof. Let (d_i) be the sequence of integers defined by $d_0 := d$ and $d_{i+1} := \big(d_i, \varphi(d_i)\big)$ for every integer $i \geq 0$. Moreover, let N_i be the number of integers n such that $0 \leq n < \big[d_i, \varphi(d_i)\big]$ and $u_n \equiv 0 \pmod{d_i}$, for each integer $i \geq 0$. The goal is to prove that $N_0 = \varphi(d_0)/d_1$.

Let $i, n, n_1 \geq 0$ be integers. From (6.46) and (6.47) it follows that the system

$$\begin{cases} n \equiv n_1 & \pmod{\varphi(d_i)} \\ u_n \equiv 0 & \pmod{d_i} \end{cases}$$

is equivalent to

$$\begin{cases} n \equiv n_1 & \pmod{\varphi(d_i)} \\ n \equiv c_0^{-1} a_0^{-n_1} v_{n_1} & \pmod{d_i}. \end{cases} \tag{6.48}$$

Furthermore, the system (6.48) has a solution if and only if

$$n_1 \equiv c_0^{-1} a_0^{-n_1} v_{n_1} \pmod{d_{i+1}}$$

that is, if and only if $u_{n_1} \equiv 0 \pmod{d_{i+1}}$. In such a case, the solution is unique modulo $\big[d_i, \varphi(d_i)\big]$. Therefore

$$N_i = \sum_{\substack{0 \leq n < [d_i, \varphi(d_i)] \\ u_n \equiv 0 \pmod{d_i}}} 1 = \sum_{0 \leq n_1 < \varphi(d_i)} \sum_{\substack{0 \leq n < [d_i, \varphi(d_i)] \\ n \equiv n_1 \pmod{\varphi(d_i)} \\ u_n \equiv 0 \pmod{d_i}}} 1 = \sum_{\substack{0 \leq n_1 < \varphi(d_i) \\ u_{n_1} \equiv 0 \pmod{d_{i+1}}}} 1$$

$$= \frac{\varphi(d_i)}{\big[d_{i+1}, \varphi(d_{i+1})\big]} \sum_{\substack{0 \le n_1 < [d_{i+1}, \varphi(d_{i+1})] \\ u_{n_1} \equiv 0 \pmod{d_{i+1}}}} 1 = \frac{\varphi(d_i) d_{i+2}}{\varphi(d_{i+1}) d_{i+1}} N_{i+1}, \tag{6.49}$$

also since $\big[d_{i+1}, \varphi(d_{i+1})\big]$ divides $\varphi(d_i)$. In turn, repeated applications of (6.49) yield that

$$N_0 = \frac{\varphi(d_0)}{d_1} \frac{d_{i+1}}{\varphi(d_i)} N_i. \tag{6.50}$$

The definition of d_{i+1} implies that d_{i+1} divides d_i. If $d_i > 1$ then, letting p be the greatest prime factor of d_i, it follows that $\nu_p(d_{i+1}) \le \nu_p(\varphi(d_i)) < \nu_p(d_i)$, and so $d_{i+1} < d_i$. Hence $d_i = 1$ for every sufficiently large integer i. This fact together with (6.50) implies that $N_0 = \varphi(d_0)/d_1$, as desired. □

Now to the proof of Theorem 6.27.

Proof of Theorem 6.27. Let $\varepsilon > 0$. By Merten's third theorem (Theorem A.36), there exists a finite set of prime numbers $\mathcal{P}$ such that each $p \in \mathcal{P}$ does not divide A and

$$\prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right) < \varepsilon. \tag{6.51}$$

Let P be the product of the primes in $\mathcal{P}$ and let $\mathcal{S}$ be the set of positive integers n such that u_n is coprime to P.

By (6.46), both the linear recurrences (u_{2n}) and (u_{2n+1}) have a single dominant root. Hence, by Theorem 5.16, $|u_n| \to +\infty$ as $n \to +\infty$. For each positive integer n, if u_n is prime then either $u_n \in \mathcal{P}$ or $u_n \in \mathcal{S}$. The first case is possible only for finitely many positive integers n, since $|u_n| \to +\infty$ as $n \to +\infty$. Hence, in order to prove Theorem 6.27, it suffices to show that the natural density of $\mathcal{S}$ is at most equal to ε.

Let d be a squarefree divisor of P and let $X > 1$ be a real number. Since u_n modulo d has period $\big[d, \varphi(d)\big]$, from Lemma 6.28 it follows that

$$\begin{aligned} \sum_{\substack{1 \le n \le X \\ u_n \equiv 0 \pmod{d}}} 1 &= \left\lfloor \frac{X}{\big[d, \varphi(d)\big]} \right\rfloor \frac{\varphi(d)}{\big(d, \varphi(d)\big)} + O\Big(\big[d, \varphi(d)\big]\Big) \\ &= \left(\frac{X}{\big[d, \varphi(d)\big]} + O(1) \right) \frac{\varphi(d)}{\big(d, \varphi(d)\big)} + O\big(d^2\big) = \frac{X}{d} + O\big(d^2\big). \end{aligned} \tag{6.52}$$

From the inclusion-exclusion principle and (6.52) it follows that

$$\begin{aligned} \big|\mathcal{S} \cap [1, X]\big| &= \sum_{d \,|\, P} \mu(d) \sum_{\substack{1 \le n \le X \\ u_n \equiv 0 \pmod{d}}} 1 = \sum_{d \,|\, P} \mu(d) \left(\frac{X}{d} + O\big(d^2\big) \right) \\ &= X \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right) + O\Big(P^2 2^{|\mathcal{P}|}\Big). \end{aligned} \tag{6.53}$$

Finally, letting $X \to +\infty$, from (6.51) and (6.53) it follows that the natural density of $\mathcal{S}$ is at most equal to ε, as desired. □

6.9 Bibliographical notes

Section 6.2 "Divisibility sequences"

The fact that Lucas sequences are strong linear divisibility sequences dates back at least to Lucas [125, Section XI]. Lehmer [112] and Pierce [145] introduced other linear divisibility sequences. Hall [75] started the classification of linear divisibility sequence by partially characterizing those of order three. Bézivin, Pethő, and van der Poorten [15] made the first important progress by showing that every linear divisibility sequence must divide a resultant sequence, as Ward speculated [197]. Later Barbero [11] provided a more elementary proof. Finally, Granville [72] provided a complete classification of all linear divisibility sequences and strong linear divisibility sequences. Browning and Verzobio [26] gave results on terms of strong divisibility sequences that are prime, or that have a somewhat large prime factor. In particular, these results apply to strong linear divisibility sequences.

Section 6.3 "Prime terms"

Bunyakovsky [28] formulated the Bunyakovsky conjecture in 1857. The *Schinzel hypothesis H* [168] is a generalization of the Bunyakovsky conjecture that provides conditions for the infiniteness of the integers $n \geq 0$ such that $f_1(n), \ldots, f_k(n)$ are all primes, where $f_1, \ldots, f_k$ are fixed polynomials in $\mathbb{Z}[x]$. In turn, the *Bateman–Horn conjecture* [12] is a strengthening of the Schinzel hypothesis H that not only predicts the infiniteness but also an asymptotic for the counting function. The *Hardy–Littlewood k-tuple conjecture* [77, p. 61] is the special case of the Bateman–Horn conjecture in which all the involved polynomials are of first degree. All these conjectures are open.

Grantham and Granville [71] provided a heuristic that is more precise than that of Section 6.3.2. In particular, their argument gives a multiplicative constant for $\log X$ that seems compatible with numerical data.

Gillies [63] provided the argument for the estimate (6.5). Lenstra, Pomerance [148], and Wagstaff [192], giving slightly different arguments, independently stated the Lenstra–Pomerance–Wagstaff conjecture. The Great Internet Mersenne Prime Search (GIMPS) [65] is a collaborative project of volunteers who use distributed computation to search for Mersenne prime numbers.

Fermat conjectured that all Fermat numbers are prime, and Euler was the first to confute that by showing that F_5 is composite. As to date, all Fermat numbers F_n for $n = 5, \ldots, 33$ are known to be composite. The *Gauss–Wantzel theorem* [127, p. 46] states that a regular n-gon can be constructed with compass and straightedge if and only if n is the product of a power of 2 and some (possibly none) pairwise distinct Fermat primes. The argument for the finiteness of Fermat primes is due to Hardy and Wright [78, Section 2.5]. Boklan and Conway [21, 22] provided a more precise heuristic suggesting that the probability that there exists a Fermat prime beyond F_4 is less than one in a billion.

Section 6.4 "Periodicity modulo m"

Carmichael [33], Engstrom [53], and Ward [195, 196] initiated the systematic study of the least period of a linear recurrence over the integers modulo m. Earlier investigations of the subject trace back at least to Lucas [125, Section XXVI]. Theorem 6.7 and Theorem 6.9 are well-known and several authors independently discovered them. Everest, van der Poorten, Shparlinski, and Ward [55, Theorem 3.4] provided a slightly more general version of Theorem 6.13, which they attribute to the folklore.

Let $\boldsymbol{F}$ be the sequence of Fibonacci numbers. Wall [193] noticed that $\tau_{\boldsymbol{F}}(p) < \tau_{\boldsymbol{F}}(p^2)$ for every prime number $p < 10^4$. He called the hypothesis that $\tau_{\boldsymbol{F}}(p) < \tau_{\boldsymbol{F}}(p^2)$ for every prime number p the "most perplexing problem [...] met in this study", and was open the possibility of a negative answer. A prime number p such that $\tau_{\boldsymbol{F}}(p) = \tau_{\boldsymbol{F}}(p^2)$ is a *Wall–Sun–Sun prime* or a *Fibonacci–Wieferich prime*. McIntosh and Roettger [130] verified that there are no Wall–Sun–Sun primes less than $2 \cdot 10^{14}$. (This range was later extended by the PrimeGrid volunteer computing project [151], but the result had not been double-checked.) Sun and Sun [183] proved that if the first case of *Fermat's last theorem* is false for an odd prime p (that is, there exist integers a, b, c such that $a^p + b^p = c^p$ and p does not divide abc) then p must be a Wall–Sun–Sun prime. Thus, before Wiles' proof of Fermat's last theorem [200], the search for Wall–Sun–Sun primes was motivated also by the search for a potential counterexample to Fermat's last theorem. Klaška [98] provided a heuristic suggesting that there are infinitely many Wall–Sun–Sun primes. For more on Wall–Sun–Sun primes, see the survey of Klaška [99].

Sections 6.5 and 6.6

These sections are based on the article by Shparlinski [172]. In the case in which $\boldsymbol{u}$ is a nondegenerate second-order linear recurrence over $\mathbb{Z}$, Murty, Séguin, and Stewart [139] improved Theorem 6.21 by showing that $\omega_{\boldsymbol{u}}(0, N) > C_1 N$ for every integer $N > C_2$, where $C_1, C_2 > 0$ are effectively computable constants. In turn, this implies that $\pi_{\boldsymbol{u}}(X) > C_1 \log X$ for every real number $X > C_2$, which improves upon Theorem 6.22.

For a wide class of second-order linear recurrences $\boldsymbol{u}$, assuming the *Generalized Riemann Hypothesis (GRH)*, Stephens [178] proved that $\pi_{\boldsymbol{u}}(X) \sim C_{\boldsymbol{u}} X/\log X$ as $X \to +\infty$, where $C_{\boldsymbol{u}} > 0$ is an explicit constant depending on $\boldsymbol{u}$. For Lucas sequences, Moree and Stevenhagen [136] gave asymptotic formulas of the same form unconditionally. In fact, for many second-order order linear recurrences the same asymptotic formula holds unconditionally, see the book [7] and the more recent article [8] by Ballot. Under a generalization of *Artin conjecture* for primitive roots in number fields, Roskam [161] proved that $\pi_{\boldsymbol{u}}(X) > CX/\log X$ as $X \to +\infty$. Under the GRH, Järviniemi [85] proved that if $\boldsymbol{u}$ is a linear recurrence of order $k \geq 2$ whose minimal polynomial has full Galois group S_k, then

$$\pi_{\boldsymbol{u}}(X) > \left(\frac{1}{k-1} + o(1)\right) \frac{X}{\log X},$$

as $X \to +\infty$.

Section 6.7 "Greatest prime factor"

Evertse [56, Theorem 3] proved Theorem 6.23. Stewart [180] proved the lower bound of Theorem 6.24; while Shparlinski [172, Theorem 2] gave that of Theorem 6.26. It is important to remark that for second-order linear recurrences, or more specifically Lucas sequences, much better lower bounds appear in the literature. For instance, let $\boldsymbol{u}$ be a nondegenerate second-order linear recurrence over $\mathbb{Z}$. Yu and Hung [201, Theorem 2] showed that

$$P(u_n) > C_1 n^{1/3}$$

for all integers $n > C_2$, where $C_1, C_2 > 0$ are effectively computable constants depending on $\boldsymbol{u}$. Stewart [181, Theorem 2] proved that

$$P(u_n) > n \exp\left(\frac{\log n}{104 \log\log n}\right),$$

for all integers $n \geq 3$ but a set of natural density zero. He also showed [182, Theorem 1.1] that if $\boldsymbol{u}$ is a Lucas sequence then the previous bound holds for all sufficiently large integers n. For more on the greatest prime factor of terms of linear recurrences, see the survey by Stewart [179].

Section 6.8 "Composite terms"

In his book on sieve theory [81, Chapter VII], Hooley proved that the set of positive integers n such that the Cullen number C_n is prime has natural density zero. By refining Hooley's method, Rieger [158] and Heppner [79] showed that, for every real number $X > 1$, the number of positive integers $n \leq X$ such that C_n is prime is at most $CX/\log X$, and the number of primes $p \leq X$ such that C_p is prime is at most $CX/(\log X)^2$, where $C > 0$ is an effectively computable constant. Actually, whether there exists a prime number p such that C_p is prime is an open problem. Guy [74, B20] attributed this problem to Conway. The proof of Theorem 6.27 is a straightforward generalization of the technique of Heppner [79] (omitting the precise upper bound for the counting function).

Let $a > 1$ and b be integers. Under the GRH and an essentially self-serving hypothesis, Hooley [81, Chapter VII] proved that $2^n - b$ is composite for all positive integers n but a set of natural density zero. Recently, assuming GRH and a substantially more natural hypothesis in place of Hooley's technical hypothesis, Järviniemi and Terävänen [86] proved that $a^n - b$ is composite for all positive integers n but a set of natural density zero. In particular, they showed that the *pair correlation conjecture* implies their technical hypothesis.

6.10 Exercises

Exercise 6.1. Let $\boldsymbol{u}$ be a linear divisibility sequence with minimal polynomial f. Suppose that $u_0 \neq 0$ and $f(0) \neq 0$. Prove that:

(i) for each integer $n \geq 0$, if p is a prime factor of u_n then p divides $u_0 f(0)$;

(ii) $\boldsymbol{u}$ is either degenerate or first-order.

Exercise 6.2. Let $\boldsymbol{u}$ be a nondegenerate second-order linear divisibility sequence. Prove that (u_n/u_1) is a Lucas sequence.

Exercise 6.3. Prove that every Pierce sequence (Example 6.4) is a linear divisibility sequence.

Exercise 6.4. Prove that every Lehmer sequence (Example 6.5) is a strong linear divisibility sequence.

Exercise 6.5. Prove that each of the following linear recurrences $\boldsymbol{u}$ has only finitely many prime terms.

(i) $u_n = 4 \cdot 81^n + 1$.

(ii) $u_n = 2^n + 15^n - (-17)^n$.

(iii) $u_n = 2^{n+1} - n^2$.

(iv) $F_n + 1$, where F_n is the nth Fibonacci number.

Exercise 6.6. Let $n \geq 2$ be an integer. Suppose that p is a prime factor of the Fermat number $2^{2^n} + 1$. Prove that

(i) 2 is a square modulo p;

(ii) $p \equiv 1 \pmod{2^{n+2}}$.

(This result is due to Lucas [124, p. 280].)

Exercise 6.7. Adjust the heuristic for the finiteness of Fermat primes given in Section 6.3.4 to take into account Exercise 6.7(ii).

Exercise 6.8. Fix a prime number p. Let $\boldsymbol{u}$ be the linear recurrence defined by

$$u_n := \sum_{j=0}^{p-1} 2^{jn}$$

for every integer $n \geq 0$. Prove that if n is a positive integer such that u_n is prime then n must be a power of p.
(This generalizes the fact that $2^n + 1$ is prime only if n is a power of 2.)

Exercise 6.9. Construct a third-order linear recurrence over $\mathbb{Z}$ that is a maximal-period sequence modulo 5^v for every positive integer v.

Exercise 6.10. Let $\boldsymbol{u} \in \mathbb{Z}^{\mathbb{N}}$ be a sequence and let m be a positive integer. Then $\boldsymbol{u}$ is *uniformly distributed modulo* m if for every integer r the limit

$$\lim_{X \to +\infty} \frac{\left|\{n \in \mathbb{N} : n < X,\, u_n \equiv r \pmod{m}\}\right|}{X}$$

exists and is independent from r.

Prove that the sequence of Fibonacci numbers is uniformly distributed modulo 5^v for every positive integer v.
(Niederreiter [142] proved this result. Kuipers and Shiue [107] showed that the powers of 5 are the only moduli for which the sequence of Fibonacci numbers is uniformly distributed.)

Exercise 6.11. Let a, b, and m be integers such that $m > 0$ and $0 \leq a, b < m$; and let $\boldsymbol{u}$ be the linear recurrence satisfying $u_n = au_{n-1} + b$ for each integer $n \geq 1$. Prove that $\boldsymbol{u}$ modulo m has least period equal to m if and only if

(i) b is coprime to m;

(ii) if p is a prime factor of m then p divides $a - 1$;

(iii) if 4 divides m then 4 divides a.

(This is a classic theorem in the theory of *linear congruential generators*, see the book by Knuth [102, p. 17, Theorem A].)

Exercise 6.12. Fix $\delta \in (0, 1)$ and employ the notation of Section 6.5. Prove that, for every real number $X > 1$, the bound $T(p) > p^{\delta}$ holds for all prime numbers $p \leq X$ but at most $CX^{\delta k}/\log X$ exceptions, where $C > 0$ is an effectively computable constant depending on δ and $\boldsymbol{u}$.

Exercise 6.13. Let $\boldsymbol{u}$ be a linear recurrence over $\mathbb{Z}$. Prove that

$$\omega_{\boldsymbol{u}}(0, N) < \frac{CN^2}{\log N}$$

for every integer $N \geq 2$, where $C > 0$ is an effectively computable constant depending on $\boldsymbol{u}$.

Exercise 6.14. For every nonzero integer n, let $Q(n) := \prod_{p|n} p$. Put also $Q(0) := +\infty$. Let $\boldsymbol{u}$ be a nondegenerate linear recurrence over $\mathbb{Z}$ with a single dominant root α_1 and at least another root $\alpha_2 \neq \alpha_1$. Prove that

$$Q(u_n) > \exp\left(\frac{C_1 \log n \log\log n}{\log\log\log n}\right)$$

for every integer $n > C_2$, where $C_1, C_2 > 0$ are effectively computable constants depending only on $\boldsymbol{u}$.
(This bound is due to Stewart [180].)

Exercise 6.15. Let (F_n) be the sequence of Fibonacci numbers. Prove that $F_n + n$ is composite for all integers $n \geq 0$ but a set of natural density zero.

Hints and Solutions

Chapter 2

Solution to Exercise 2.1.

(i) $(x-2)^2(x-3)$.

(ii) $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 12 & -16 & 7 \end{pmatrix}$.

(iii) $(7+3n)2^n - 6\cdot 3^n$.

(iv) $(1-5x)/\big((1-3x)(1-2x)^2\big)$. ■

Solution to Exercise 2.2.

(i) $(x-1)(x-\alpha)^3$.

(ii) $\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & \alpha & 1 & 1+\alpha \end{pmatrix}$.

(iii) $(1+\alpha) + \big(\alpha\binom{n}{0} + \binom{n}{1} + (1+\alpha)\binom{n}{2}\big)\,\alpha^n$.

(iv) $\big(1+x+(1+\alpha)x^3\big)/\big((1-x)(1-\alpha x)^3\big)$. ■

Solution to Exercise 2.4.

(i) $k=4$, $c_1=0$, $c_2=-1$, $c_3=-1$, $c_4=-2$.

(ii) $k=2$, $c_1=1$, $c_2=2$.

(iii) $k=4$, $c_1=4$, $c_2=2$, $c_3=1$, $c_4=2$. ■

Solution to Exercise 2.5.

(i) $(x-2)^2(x-4)^2$.

(ii) $(x-1)(x-2)^2(x-8)^3$.

(iii) $(x-1)^2(x-2)^3(x-4)^2$.

(iv) $(x-1)(x-1/2)(x-1/4)^2$.

(v) $(x+1)(x-2)^2(x+2)^2(x^2-2)^2$. ■

Solution to Exercise 2.6. If $\alpha_1 = \alpha_2 = \alpha_3$ then

$$u_n = \frac{1}{2\alpha_1^3}\big(2\alpha_1^3u_0 + (-3\alpha_1^3u_0 + 4\alpha_1^2u_1 - \alpha_1u_2)n + (\alpha_1^3u_0 - 2\alpha_1^2u_1 + \alpha_1u_2)n^2\big)\alpha_1^n$$

for each $n \in \mathbb{N}$.

If $\alpha_1 \neq \alpha_2 = \alpha_3$ then

$$\begin{aligned} u_n = \frac{1}{(\alpha_1-\alpha_2)^2\alpha_2}\Big((\alpha_2^3u_0 - 2\alpha_2^2u_1 + \alpha_2u_2)\alpha_1^n + \big((\alpha_1^2\alpha_2 - 2\alpha_1\alpha_2^2)u_0 + 2\alpha_2^2u_1 - \alpha_2u_2 \\ + \big((\alpha_1\alpha_2^2 - \alpha_1^2\alpha_2)u_0 + (\alpha_1^2 - \alpha_2^2)u_1 - (\alpha_1-\alpha_2)u_2\big)n\big)\alpha_2^n\Big) \end{aligned}$$

for each $n \in \mathbb{N}$; and the cases $\alpha_2 \neq \alpha_1 = \alpha_3$ and $\alpha_3 \neq \alpha_1 = \alpha_2$ are similar.

If $\alpha_1, \alpha_2, \alpha_3$ are pairwise distinct then

$$\begin{aligned} u_n = \frac{1}{(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)}\Big(\big((\alpha_2\alpha_3^2 - \alpha_2^2\alpha_3)u_0 + (\alpha_2^2 - \alpha_3^2)u_1 - (\alpha_2-\alpha_3)u_2\big)\alpha_1^n \\ + \big((\alpha_1^2\alpha_3 - \alpha_1\alpha_3^2)u_0 - (\alpha_1^2 - \alpha_3^2)u_1 + (\alpha_1-\alpha_3)u_2\big)\alpha_2^n \\ + \big((\alpha_1\alpha_2^2 - \alpha_1^2\alpha_2)u_0 + (\alpha_1^2 - \alpha_2^2)u_1 - (\alpha_1-\alpha_2)u_2\big)\alpha_3^n\Big) \end{aligned}$$

for each $n \in \mathbb{N}$. ■

Solution to Exercise 2.7.

(i) $x^3 + 16$.

(ii) $(x+1)(x^3+x+1)(x^3+x^2+1)$.

(iii) $(x^2+x+2)^6(x^2+2x+2)^9$. ■

Solution to Exercise 2.8. Use Theorem 2.22 and Theorem 2.23. ■

Solution to Exercise 2.9. Suppose that $\mathrm{char}(\mathbb{K}) = 0$. Consider the *exponential generating functions* $U(x) := \sum_{n=0}^{\infty} u_n x^n/n!$ and $V(x) := \sum_{n=0}^{\infty} v_n x^n/n!$ in $\mathbb{K}[[x]]$ and the formal series of their product $U(x)V(x)$. ■

Solution to Exercise 2.10. Consider the generating functions $U(x) := \sum_{n=0}^{\infty} u_n x^n$ and $V(x) := \sum_{n=0}^{\infty} v_n x^n$ in $\mathbb{K}[[x]]$ and their composition $U\big(V(x)\big)$. ■

Solution to Exercise 2.11. Begin by proving the identity $\boldsymbol{H}_k^{(n)}(\boldsymbol{u}) = \boldsymbol{C}^n \boldsymbol{H}_k(\boldsymbol{u})$, where $\boldsymbol{H}_k^{(n)}(\boldsymbol{u})$ and $\boldsymbol{H}_k(\boldsymbol{u})$ are the Hankel matrices associated to $\boldsymbol{u}$ (Section 2.10) and $\boldsymbol{C}$ is the companion matrix of $\boldsymbol{u}$. ■

Solution to Exercise 2.12. Let $\boldsymbol{v} \in \mathbb{Q}^{\mathbb{N}}$ be defined by $v_n := a_n^3 + b_n^3 - c_n^3 - (-1)^n$ for each $n \in \mathbb{N}$. Upper bound the orders of the linear recurrences $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$, and $\boldsymbol{v}$. Then check that $a_n, b_n, c_n \in \mathbb{Z}$ and $v_n = 0$ for sufficiently many values of n. ■

Solution to Exercise 2.17. The claim follows from Theorem 2.53. ■

Solution to Exercise 2.18. Example 2.9 says that

$$\sum_{n=0}^{\infty} T_n(y) x^n = \frac{1 - xy}{1 - 2xy + x^2}.$$

Take the derivative with respect to y of both sides. ■

Chapter 3

Solution to Exercise 3.1. Note that $f(0) = \det\big(\boldsymbol{C}(f)\big)$. ■

Solution to Exercise 3.2. Note that

$$x^4 + 2x^3 + 2x^2 + 2x + 1 = (x - \mathbb{i})(x + \mathbb{i})(x + 1)^2$$

has a double root and so, by Corollary 3.2, it cannot be the minimal polynomial of a periodic sequence. ■

Solution to Exercise 3.3. Use the factorization $x^t - 1 = \sum_{d|t} \Phi_d(x)$, where $\Phi_d(x)$ is the dth *cyclotomic polynomial*, which is defined as the minimal polynomial over $\mathbb{Q}$ of a primitive dth root of unity and has degree equal to $\varphi(d)$ (see, e.g., [110, Chapter 6, Section 3]). ■

Solution to Exercise 3.4. First, prove that the minimal polynomial of $\boldsymbol{u}+\boldsymbol{v}$ is fg. Then apply one of the formulas for the least period in terms of the minimal polynomial (Theorem 3.3). ■

Chapter 4

Solution to Exercise 4.2. Let $\boldsymbol{u}$ be a periodic linear recurrence over $\mathbb{F}_7$ with least period equal to 4, and let f be the minimal polynomial of $\boldsymbol{u}$. From Theorem 4.1 it follows that f divides $x^4 - 1$, which in turn factorizes over $\mathbb{F}_7$ as $(x-1)(x+1)(x^2+1)$, and the periods of the three factors are 1, 2, and 4, respectively. Hence f can be only one of the following

$$f_1 := x^4 - 1, \quad f_2 := (x-1)(x^2+1), \quad f_3 := (x+1)(x^2+1), \quad f_4 := x^2 + 1.$$

Thus the number of linear recurrences over $\mathbb{F}_7$ with least period equal to 4 is

$$|\mathcal{L}^*(f_1)| + |\mathcal{L}^*(f_2)| + |\mathcal{L}^*(f_3)| + |\mathcal{L}^*(f_4)| = 1728 + 288 + 288 + 48 = 2352,$$

also employing Theorem 4.4(ii). ■

Solution to Exercise 4.7. The only possibilities are $q = 2$, $f = x + 1$, $f = x^2 + x + 1$; or $q = 3$ and $f = x + 1$. ■

Solution to Exercise 4.10. To count the number of zeros, use Theorem 4.11. ■

Solution to Exercise 4.11. The best choice is using one of the only three primitive trinomials of degree 7 over $\mathbb{F}_2$, which are $x^7 + x + 1$, $x^7 + x^3 + 1$, $x^7 + x^4 + 1$, and $x^7 + x^6 + 1$. ■

Chapter 5

Solution to Exercise 5.1. Suppose that $x^2 + ax + b$ $(a, b \in \mathbb{Q})$ is a degenerate polynomial, and let α, β be its roots. Then $\alpha \neq \beta$ and $\zeta := \alpha/\beta$ is a root of unity. Note that

$$\xi := \zeta + \zeta^{-1} = \frac{\alpha}{\beta} + \frac{\beta}{\alpha} = \frac{\alpha^2 + \beta^2}{\alpha\beta} = \frac{a^2 - 2b}{b}$$

is an algebraic integer that is also a rational integer. Hence ξ is an integer. Furthermore,

$$|\xi| \leq |\zeta| + |\zeta^{-1}| \leq 1 + 1 = 2.$$

Thus $\xi \in \{-2, -1, 0, 1, 2\}$. Studying each of these five cases (case $\xi = 2$ is impossible because it implies $\alpha = \beta$), it turns out that the monic second-degree degenerate polynomials in $\mathbb{Q}[x]$ are

$$x^2 + t, \quad x^2 + tx + t^2, \quad x^2 + 2tx + 2t^2, \quad x^2 + 3tx + 3t^2,$$

where t runs over the nonzero rational numbers. ■

Solution to Exercise 5.2.

(i) $n = 7$ is the only zero.

(ii) There are no zeros.

(iii) The set of zeros is the arithmetic progression $\{6k + 5 : k \in \mathbb{N}\}$.

(iv) Since $\boldsymbol{u}$ has a single dominant root, it is possible to provide an effective lower bound for $|u_n|$. This bound implies that the zeros are $n = 5, 14, 18, 19, 21$.

(v) $n = 0$ is the only zero. This case is more difficult since $\boldsymbol{u}$ is a third-order linear recurrence with two dominant roots. The power-sum representation of $\boldsymbol{u}$ is

$$u_n = \tfrac{1}{2}(2+\mathbb{i})^n + \tfrac{1}{2}(2-\mathbb{i})^n - 1 \quad (n \in \mathbb{N}).$$

Hence $u_n = 0$ if and only if $(2+\mathbb{i})^n$ is a root of $f_n(x) := x^2 - 2x + 5^n$, which can happen only if the splitting field of $f_n(x)$ contains $\mathbb{i}$.

(vi) The only zeros are $n = 0, 1$. Note that $\boldsymbol{u}$ is the product of two nondegenerate second-order linear recurrences, each having at most one zero. ■

Solution to Exercise 5.5.

(i) $u_n \sim \frac{1}{2}\big(2+\sqrt{3}\big)^n$.

(ii) $u_n \sim 2 \cdot 3^n$.

(iii) $u_n \sim n \cdot 4^n$. ■

Solution to Exercise 5.7. In the identity of Theorem 2.59, take the determinant of both sides. ■

Solution to Exercise 5.5.

(i) $u_n = \big(2^n + 2 \cdot 3^n - 4^n\big)\big(2^n + 3^n + 4^n\big)$.

(ii) $u_n = \big((1+n)2^n - 2^{-n}\big)\big((1+n)2^n + 2^{-n}\big)$.

(iii) Irreducible. ■

Solution to Exercise 5.9.

(i) $\boldsymbol{u}/\boldsymbol{v}$ is the generalized power sums $2^n - 3^n + 2 \cdot 5^n$.

(ii) $\boldsymbol{u}/\boldsymbol{v}$ is the generalized power sums $2^n + n3^n$.

(iii) $\boldsymbol{u}/\boldsymbol{v}$ is not a generalized power sums. ■

Solution to Exercise 5.10.

(i) The only positive integer n such that n divides $2^n - 1$ is $n = 1$. In order to prove that, suppose that $n > 1$ divides $2^n - 1$, let p be the smallest prime factor of n, and deduce a contradiction by considering the multiplicative order of 2 modulo p.

(ii) There are infinitely many positive integers n such that n divides $2^n + 1$. For instance, it follows by induction that 3^k divides $2^{3^k} + 1$ for every integer $k \geq 0$.

(iii) The only positive integer n such that n^2 divides $2^n - 1$ is $n = 1$.

(iv) There are infinitely many positive integers n such that $n+2$ divides 2^n+1. ■

Chapter 6

Solution to Exercise 6.1.

(i) Let p be a prime factor of u_n that does not divide $f(0)$. Then Theorem 6.6 states that $\boldsymbol{u}$ is periodic modulo p. Let t be a period of $\boldsymbol{u}$ modulo p. Periodicity implies that $u_0 \equiv u_{nt} \pmod{p}$. Since p divides u_n, and $\boldsymbol{u}$ is a divisibility sequence, $u_{nt} \equiv 0 \pmod{p}$. Hence p divides u_0.

(ii) The claim follows from (i) and Theorem 6.22. ■

Solution to Exercise 6.2. From Exercise 6.1(ii) it follows that $u_0 = 0$. Since $\boldsymbol{u}$ is a divisibility sequence, the term u_1 divides u_n for every positive integer n. The claim follows. ■

Solution to Exercise 6.3. The proof proceeds similarly to that of Theorem 6.1. ■

Solution to Exercise 6.4. The proof proceeds similarly to that of Theorem 6.4. ■

Solution to Exercise 6.5.

(i) $u_n = (2\cdot 9^n + 2\cdot 3^n + 1)(2\cdot 9^n - 2\cdot 3^n + 1)$.

(ii) $u_n \equiv 0 \pmod{3}$ if $n > 1$ is even, and $u_n \equiv 0 \pmod{17}$ if n is odd.

(iii) $u_n \equiv 0 \pmod{2}$ if n is even, and $u_n = \big(2^{(n+1)/2} - n\big)\big(2^{(n+1)/2} + n\big)$ if n is odd.

(iv) Let (L_n) be the linear recurrence defined by $L_0 = 2$, $L_1 = 1$, and $L_n = L_{n-1} + L_{n-2}$ for every integer $n \geq 2$. Then, for every integer $k \geq 0$,

$$F_{4k+1} + 1 = F_{2k+1}L_{2k}, \qquad F_{4k+2} + 1 = F_{2k+2}L_{2k},$$
$$F_{4k+3} + 1 = F_{2k+1}L_{2k+2}, \qquad F_{4k+4} + 1 = F_{2k+1}L_{2k+3}.$$

■

Solution to Exercise 6.6.

(i) $2 \equiv a^2 \pmod{p}$ where a is an arbitrary integer such that $a \equiv 2^{2^{n-2}} + 2^{-2^{n-2}} \pmod{p}$.

(ii) $2^{2^n} \equiv -1 \pmod{p}$ and so $a^{2^{n+2}} \equiv 2^{2^{n+1}} \equiv 1 \pmod{p}$. Thus $p \equiv 1 \pmod{2^{n+2}}$. ■

Solution to Exercise 6.8. Note that, if m is a positive integer coprime with p, then the polynomial $(x^p-1)/(x-1)$ divides $(x^{pm}-1)/(x^m-1)$. Indeed, the roots of the first polynomial are the $p-1$ primitive pth roots of unity; and if ζ is a primitive pth roots of unity so it is ζ^m. Since $u_n = (2^{pn}-1)/(2^n-1)$, if n has a divisor m that is coprime with p, then $u_{n/m}$ divides u_n. Then claim follows. ■

Solution to Exercise 6.9. $u_0 = 0$, $u_1 = 0$, $u_2 = 1$, and $u_n = 2u_{n-2} + 3u_{n-3}$ for $n \geq 3$. ■

Solution to Exercise 6.12. Adapt the proof of Lemma 5.34. ■

Solution to Exercise 6.13. Compare the growth of $\prod_{n<N,\, u_n \neq 0} |u_n|$ with that of the product of the first K prime numbers. ■

Appendix

The appendix collects some miscellaneous results that are used sparsely through this book, and that do not fit in a precise chapter.

Lemma A.29 (Hensel's lemma)**.** *Let p be a prime number, let $f \in \mathbb{Z}_p[x]$, and let $a \in \mathbb{Z}_p$. Suppose that $|f(a)|_p < |f'(a)|_p^2$. Then there exists $\alpha \in \mathbb{Q}_p$ such that $|\alpha - a|_p < 1$ and $f(\alpha) = 0$.*

Proof. See, e.g., the book by Knapp [101, Theorem 6.28]. □

Let p be a prime number. The *p-adic exponential function* Exp_p is defined by the series

$$\mathrm{Exp}_p(z) := \sum_{n=0}^{\infty} \frac{z^n}{n!},$$

which converges for every $z \in \mathbb{Q}_p$ such that $|z|_p < p^{-1/(p-1)}$. The *p-adic logarithm function* Log_p is defined by the series

$$\mathrm{Log}_p(z) := -\sum_{n=1}^{\infty} \frac{(1-z)^n}{n},$$

which converges for every $z \in \mathbb{Q}_p$ such that $|z-1|_p < 1$.

The following theorem collects the basic properties of the p-adic exponential and the p-adic logarithm.

Theorem A.30. *Let p be a prime number and let $z, w \in \mathbb{Q}_p$.*

(i) If $|z|_p < p^{-1/(p-1)}$ and $|w|_p < p^{-1/(p-1)}$, then $|z+w|_p < p^{-1/(p-1)}$ and

$$\mathrm{Exp}_p(z+w) = \mathrm{Exp}_p(z)\,\mathrm{Exp}_p(w).$$

(ii) If $|z-1|_p \le p^{-1}$ and $|w-1|_p \le p^{-1}$, then $|zw-1|_p < 1$ and

$$\mathrm{Log}_p(zw) = \mathrm{Log}_p(z) + \mathrm{Log}_p(w).$$

(iii) If $|z-1|_p < p^{-1/(p-1)}$ then $\big|\mathrm{Log}_p(z)\big|_p < p^{-1/(p-1)}$ and

$$\mathrm{Exp}_p\big(\mathrm{Log}_p(z)\big) = z.$$

(iv) If $|z|_p < p^{-1/(p-1)}$ *then* $\left|\operatorname{Exp}_p(z) - 1\right|_p < 1$ *and*

$$\operatorname{Log}_p\bigl(\operatorname{Exp}_p(z)\bigr) = z.$$

Proof. See, e.g., the book by Gouvêa [68, Section 5.7]. □

Theorem A.31 (Strassmann's theorem)**.** *Let* $f(x) = \sum_{n=0}^{\infty} a_n x^n$ $(a_n \in \mathbb{Q}_p)$ *be a nonzero power series such that* $a_n \to 0$ *as* $n \to +\infty$*, so that* $f(x)$ *converges over* $\mathbb{Z}_p$*. Let* N *be the unique nonnegative integer such that* $|a_N| = \max_{n\in\mathbb{N}} |a_n|$ *and* $|a_n| < |a_N|$ *for every integer* $n > N$*. Then the function* $f\colon \mathbb{Z}_p \to \mathbb{Q}_p$ *has at most* N *zeros.*

Proof. See, e.g., the book by Gouvêa [68, Theorem 5.6.1]. □

Theorem A.32 (Legendre–de Polignac formula)**.** *Let* $n \geq 0$ *be an integer and let* p *be a prime number. Then*

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Proof. A quick computation yields that

$$\nu_p(n!) = \sum_{k=1}^{n} \nu_p(k) = \sum_{k=1}^{n} \sum_{i=1}^{\nu_p(k)} 1 = \sum_{i=1}^{\infty} \sum_{\substack{k=1 \\ \nu_p(k)\geq i}}^{n} 1 = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor,$$

as desired. □

Theorem A.33 (Kummer's theorem)**.** *Let* $m \geq n \geq 0$ *be integers and let* p *be a prime number. Then the* p*-adic valuation of* $\binom{m+n}{n}$ *is equal to the number of carries in the base-*p *addition of* m *and* n*.*

Proof. Let $m = \sum_{i=0}^{\infty} m_i p^i$ $(m_i \in \{0, \ldots, p-1\})$ and $n = \sum_{i=0}^{\infty} n_i p^i$ $(n_i \in \{0, \ldots, p-1\})$ be the base-p representations of m and n. For each integer $i \geq 0$, let $c_i \in \{0, 1\}$ be the carry occurring at the ith digit in the base-p addition of m and n. Put also $c_{-1} := 0$. Hence the base-p representation of $m + n$ is

$$m + n = \sum_{i=0}^{\infty} \ell_i p^i \quad (\ell_i \in \{0, \ldots, p-1\}),$$

where $\ell_i := m_i + n_i + c_{i-1} - pc_i$ for every integer $i \geq 0$. Moreover, it is easy to verify that

$$\left\lfloor \frac{m}{p^i} \right\rfloor = \sum_{j=0}^{\infty} m_{i+j} p^j, \quad \left\lfloor \frac{n}{p^i} \right\rfloor = \sum_{j=0}^{\infty} n_{i+j} p^j, \quad \left\lfloor \frac{m+n}{p^i} \right\rfloor = \sum_{j=0}^{\infty} \ell_{i+j} p^j, \tag{A.54}$$

for each positive integer i. From Theorem A.32 and (A.54) it follows that

$$\nu_p\left(\binom{m+n}{m}\right) = \nu_p\bigl((m+n)!\bigr) - \nu_p(m!) - \nu_p(n!) = \sum_{i=1}^{\infty} \left(\left\lfloor \frac{m+n}{p^i} \right\rfloor - \left\lfloor \frac{m}{p^i} \right\rfloor - \left\lfloor \frac{n}{p^i} \right\rfloor \right)$$

$$= \sum_{i=1}^{\infty} \sum_{j=0}^{\infty} (\ell_{i+j} - m_{i+j} - n_{i+j}) p^j = \sum_{i=1}^{\infty} \sum_{j=0}^{\infty} (c_{i+j-1} - p c_{i+j}) p^j = \sum_{i=0}^{\infty} c_i,$$

since the last sum over j is telescopic. This proves the claim. □

Theorem A.34 (Merten's first theorem)**.** *For all real numbers $X \geq 2$,*

$$\sum_{p \leq X} \frac{\log p}{p} = \log X + O(1),$$

where p runs over the prime numbers.

Theorem A.35 (Merten's second theorem)**.** *For all real numbers $X \geq 2$,*

$$\sum_{p \leq X} \frac{1}{p} = \log \log X + M + O\left(\frac{1}{\log X}\right),$$

where p runs over the prime numbers and $M \approx 0.261$ is the Meissel–Mertens constant*.*

Theorem A.36 (Merten's third theorem)**.** *For all real numbers $X \geq 2$,*

$$\prod_{p \leq X} \left(1 - \frac{1}{p}\right) = \frac{1}{\mathrm{e}^{\gamma} \log X} \left(1 + O\left(\frac{1}{\log X}\right)\right)$$

where p runs over the prime numbers and $\gamma \approx 0.577$ is the Euler–Mascheroni constant*.*

Proofs of Theorems A.36, A.35, and A.36. See for instance the book by Tenenbaum [184, Chapter I.1, Theorems 1.8, 1.10, and 1.12]. □

For every real number X, let $\pi(X)$ be the number of primes that do not exceed X.

Theorem A.37 (Prime number theorem)**.** $\pi(X) \sim X/\log X$ *as* $X \to +\infty$*.*

Corollary A.38. *If p_n is the nth prime number, then*

$$p_n \sim n \log n,$$

as $n \to +\infty$.

Corollary A.39. *As $X \to +\infty$,*

$$\sum_{p \leq X} \log p \sim X.$$

Proofs of Theorem A.37 and Corollaries A.38 and A.39. Again, see for instance the book by Tenenbaum [184, Chapter II.4]. □

The following is an important corollary of the *Chebotarev density theorem*.

Corollary A.40. *Let $\mathbb{K}$ be a number field. Then the number of (rational) primes not exceeding X and splitting completely in $\mathbb{K}$ is at least*

$$\frac{1+o(1)}{[\mathbb{K}:\mathbb{Q}]} \cdot \frac{X}{\log X},$$

as $X \to +\infty$.

Proof. See, e.g., the book by Neukirch [141, Chapter VII, Corollary 13.6]. □

Theorem A.41. *Let $\alpha_1, \dots, \alpha_s$ be algebraic numbers. Then*

(i) $\mathrm{h}(\alpha_1 + \cdots + \alpha_s) \le \log s + \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_s)$;

(ii) $\mathrm{h}(\alpha_1 \cdots \alpha_s) \le \mathrm{h}(\alpha_1) + \cdots + \mathrm{h}(\alpha_s)$.

Proof. See, e.g., the book by Evertse and Győry [57, Lemma 1.9.2]. □

Bibliography

[1] J. J. Alba González, F. Luca, C. Pomerance, and I. E. Shparlinski, *On numbers n dividing the nth term of a linear recurrence*, Proc. Edinb. Math. Soc. (2) **55** (2012), no. 2, 271–289. [p. 117]

[2] F. Amoroso and E. Viada, *On the zeros of linear recurrence sequences*, Acta Arith. **147** (2011), no. 4, 387–396. [pp. 98 and 115]

[3] D. Andrica and O. Bagdasar, *Recurrent sequences—key results, applications, and problems*, Problem Books in Mathematics, Springer, Cham, [2020] ©2020. [p. 1]

[4] T. M. Apostol, *Modular functions and Dirichlet series in number theory*, second ed., Graduate Texts in Mathematics, vol. 41, Springer-Verlag, New York, 1990. [p. 5]

[5] P. Bacik, *Completing the picture for the Skolem Problem on order-4 linear recurrence sequences*, https://arxiv.org/abs/2409.01221. [p. 98]

[6] A. Baker, *Transcendental number theory*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 2022, With an introduction by David Masser, Reprint of the 1975 original [0422171]. [p. 116]

[7] C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. **115** (1995), no. 551, viii+102. [p. 150]

[8] C. Ballot, *Prime density of Lehmer sequences*, Integers **23** (2023), Paper No. A85, 14. [p. 150]

[9] C. J.-C. Ballot and H. C. Williams, *The Lucas sequences—theory and applications*, CMS/CAIMS Books in Mathematics, vol. 8, Springer, Cham, [2023] ©2023. [p. 3]

[10] J. Bang-Jensen and G. Gutin, *Digraphs*, second ed., Springer Monographs in Mathematics, Springer-Verlag London, Ltd., London, 2009, Theory, algorithms and applications. [p. 7]

[11] S. Barbero, *Generalized Vandermonde determinants and characterization of divisibility sequences*, J. Number Theory **173** (2017), 371–377. [pp. 124, 125, and 149]

[12] P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. **16** (1962), 363–367. [pp. 116 and 149]

[13] B. Benzaghou, *Algèbres de Hadamard*, Bull. Soc. Math. France **98** (1970), 209–252. [p. 117]

[14] E. Berlekamp, *Nonbinary BCH decoding (Abstr.)*, IEEE Transactions on Information Theory **14** (1968), no. 2, 242–242. [p. 56]

[15] J.-P. Bézivin, A. Pethő, and A. J. van der Poorten, *A full characterisation of divisibility sequences*, Amer. J. Math. **112** (1990), no. 6, 985–1001. [p. 149]

[16] M. Bicknell-Johnson, *The Fibonacci Association: historical snapshots*, Fibonacci Quart. **52** (2014), no. 5, 1–4. [p. 3]

[17] Y. Bilu, *Skolem Problem for linear recurrence sequences with 4 dominant roots (after Mignotte, Shorey, Tijdeman, Vereshchagin and Bacik)*, https://arxiv.org/abs/2501.16290. [p. 98]

[18] Y. Bilu, F. Luca, J. Nieuwveld, J. Ouaknine, D. Purser, and J. Worrell, *Skolem meets Schanuel*, 47th International Symposium on Mathematical Foundations of Computer Science, LIPIcs. Leibniz Int. Proc. Inform., vol. 241, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2022, pp. Art. No. 20, 15. [pp. 98 and 115]

[19] Y. F. Bilu, *The many faces of the subspace theorem [after Adamczewski, Bugeaud, Corvaja, Zannier...]*, Astérisque (2008), no. 317, Exp. No. 967, vii, 1–38, Séminaire Bourbaki. Vol. 2006/2007. [p. 117]

[20] V. D. Blondel and N. Portier, *The presence of a zero in an integer linear recurrent sequence is NP-hard to decide*, Linear Algebra Appl. **351/352** (2002), 91–98, Fourth special issue on linear systems and control. [p. 116]

[21] K. D. Boklan and J. H. Conway, *Expect at most one billionth of a new Fermat prime! (arXiv version)*, https://arxiv.org/abs/1605.01371. [p. 149]

[22] K. D. Boklan and J. H. Conway, *Expect at most one billionth of a new Fermat prime!*, Math. Intelligencer **39** (2017), no. 1, 3–5. [p. 149]

[23] A. Borel, *Compact Clifford-Klein forms of symmetric spaces*, Topology **2** (1963), 111–122. [p. 115]

[24] A. Brousseau and V. E. Hoggatt Jr., *The Fibonacci Association*, https://www.fibonacciassociation.org. [p. 3]

[25] A. Brousseau and V. E. Hoggatt Jr., *The Fibonacci Quarterly*, https://www.fq.math.ca. [pp. 3 and 44]

[26] T. Browning and M. Verzobio, *Strong divisibility sequences and sieve methods*, Mathematika **70** (2024), no. 4, Paper No. e12269, 26. [p. 149]

[27] Y. Bugeaud, *Linear forms in logarithms and applications*, IRMA Lectures in Mathematics and Theoretical Physics, vol. 28, European Mathematical Society (EMS), Zürich, 2018. [p. 116]

[28] V. Bunyakovsky, *Sur les diviseurs numériques invariables des fonctions rationnelles entiéres*, Mémoires de l'Académie Impériale des Sciences de Saint-Pétersbourg, 6th series **7** (1857), 305–329. [p. 149]

[29] G. S. Call and D. J. Velleman, *Pascal's matrices*, Amer. Math. Monthly **100** (1993), no. 4, 372–376. [p. 42]

[30] R. Canetti, J. Friedlander, S. Konyagin, M. Larsen, D. Lieman, and I. Shparlinski, *On the statistical properties of Diffie-Hellman distributions*, Israel J. Math. **120** (2000), 23–46. [p. 87]

[31] D. G. Cantor, *On arithmetic properties of coefficients of rational functions*, Pacific J. Math. **15** (1965), 55–58. [p. 117]

[32] D. G. Cantor, *On arithmetic properties of the Taylor series of rational functions. II*, Pacific J. Math. **41** (1972), 329–334. [p. 117]

[33] R. D. Carmichael, *On sequences of integers defined by recurrence relations*, Quart. J. Pure Appl. Math. **48** (1920), 343–372. [p. 150]

[34] J. W. S. Cassels, *An embedding theorem for fields*, Bull. Austral. Math. Soc. **14** (1976), no. 2, 193–198. [pp. 92 and 115]

[35] E. Çakçak, *A remark on the minimal polynomial of the product of linear recurring sequences*, Finite Fields Appl. **4** (1998), no. 1, 87–97. [p. 55]

[36] E. Çakçak, *A note on the minimal polynomial of the product of linear recurring sequences*, Finite fields and applications (Augsburg, 1999), Springer, Berlin, 2001, pp. 57–69. [p. 55]

[37] U. Cerruti and F. Vaccarino, *R-algebras of linear recurrent sequences*, J. Algebra **175** (1995), no. 1, 332–338. [p. 56]

[38] U. Cheng, *On the continued fraction and Berlekamp's algorithm*, IEEE Trans. Inform. Theory **30** (1984), no. 3, 541–544. [p. 56]

[39] M. Cipu, I. Diouf, and M. Mignotte, *Testing degenerate polynomials*, Appl. Algebra Engrg. Comm. Comput. **22** (2011), no. 4, 289–300. [pp. 96 and 115]

[40] P. Corvaja and U. Zannier, *Diophantine equations with power sums and universal Hilbert sets*, Indag. Math. (N.S.) **9** (1998), no. 3, 317–332. [p. 117]

[41] P. Corvaja and U. Zannier, *Finiteness of integral values for the ratio of two linear recurrences*, Invent. Math. **149** (2002), no. 2, 431–451. [pp. 109 and 117]

[42] J. Cullen, *Question 15897*, Dec. 1, 1905. [p. 144]

[43] A. J. C. Cunningham, *Solution of Question 15897*, Math. Quest. Educ. Times **10** (1906), 44–47. [p. 144]

[44] A. J. C. Cunningham and H. J. Woodall, *Factorisation of* $Q = (2^q \mp q)$ *and* $(q \cdot 2^q \mp 1)$, Messenger **47** (1917), 1–38 (English). [p. 144]

[45] H. Derksen, *A Skolem–Mahler–Lech theorem in positive characteristic and finite automata*, Invent. Math. **168** (2007), no. 1, 175–224. [p. 116]

[46] R. Dong and D. Shafrir, *The Skolem Problem in rings of positive characteristic*, https://arxiv.org/abs/2510.27603. [p. 116]

[47] J.-L. Dornstetter, *On the equivalence between Berlekamp's and Euclid's algorithms*, IEEE Trans. Inform. Theory **33** (1987), no. 3, 428–431. [p. 56]

[48] M. du Sautoy and L. Woodward, *Zeta functions of groups and rings*, Lecture Notes in Mathematics, vol. 1925, Springer-Verlag, Berlin, 2008. [p. 11]

[49] A. Dubickas and C. J. Smyth, *On the Remak height, the Mahler measure and conjugate sets of algebraic numbers lying on two circles*, Proc. Edinb. Math. Soc. (2) **44** (2001), no. 1, 1–17. [p. 115]

[50] A. Dubickas, M. Sha, and I. Shparlinski, *Explicit form of Cassels' p-adic embedding theorem for number fields*, Canad. J. Math. **67** (2015), no. 5, 1046–1064. [p. 115]

[51] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648. [p. 12]

[52] H. Dym, *Linear algebra in action*, third ed., Graduate Studies in Mathematics, vol. 232, American Mathematical Society, Providence, RI, [2023] ©2023. [p. 55]

[53] H. T. Engstrom, *Periodicity in sequences defined by linear recurrence relations.*, Proc. Natl. Acad. Sci. USA **16** (1930), 663–665 (English). [p. 150]

[54] T. Etzion, *Sequences and the de Bruijn Graph*, first ed., Academic Press, 2024. [p. 87]
[55] G. Everest, A. van der Poorten, I. Shparlinski, and T. Ward, *Recurrence sequences*, Mathematical Surveys and Monographs, vol. 104, American Mathematical Society, Providence, RI, 2003. [pp. viii, 1, 87, 100, and 150]
[56] J.-H. Evertse, *On sums of S-units and linear recurrences*, Compositio Math. **53** (1984), no. 2, 225–244. [pp. 100, 116, and 151]
[57] J.-H. Evertse and K. Győry, *Unit equations in Diophantine number theory*, Cambridge Studies in Advanced Mathematics, vol. 146, Cambridge University Press, Cambridge, 2015. [pp. 1 and 166]
[58] P. Flajolet and R. Sedgewick, *Analytic combinatorics*, Cambridge University Press, Cambridge, 2009. [p. 13]
[59] G. B. Folland, *Fourier analysis and its applications*, The Wadsworth & Brooks/Cole Mathematics Series, Wadsworth & Brooks/Cole Advanced Books & Software, Pacific Grove, CA, 1992. [p. 6]
[60] S. B. Gashkov and I. B. Gashkov, *The Berlekamp–Massey algorithm, continued fractions, Padé approximants, and orthogonal polynomials*, Mat. Zametki **79** (2006), no. 1, 45–59. [p. 56]
[61] L. Gatto, *Generic linear recurrent sequences and related topics*, Publicações Matemáticas do IMPA. [IMPA Mathematical Publications], Instituto Nacional de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 2015, 30º Colóquio Brasileiro de Matemática. [30th Brazilian Mathematics Colloquium]. [p. 55]
[62] L. Gatto and P. Salehyan, *Hasse–Schmidt derivations on Grassmann algebras*, IMPA Monographs, vol. 4, Springer, [Cham], 2016, With applications to vertex operators. [p. 55]
[63] D. B. Gillies, *Three new Mersenne primes and a statistical theory*, Math. Comp. **18** (1964), 93–97. [p. 149]
[64] GIMPS, *GIMPS Discovers Largest Known Prime Number:* $2^{136,279,841} - 1$, https://www.mersenne.org/primes/?press=M136279841. [p. 3]
[65] GIMPS, *Great Internet Mersenne Prime Search*, https://www.mersenne.org. [p. 149]
[66] S. W. Golomb, *Shift register sequences. Secure and limited-access code generators, efficiency code generators, prescribed property generators, mathematical models*, 3rd revised edition ed., Hackensack, NJ: World Scientific, 2017 (English). [pp. 73 and 87]
[67] R. Göttfert and H. Niederreiter, *On the minimal polynomial of the product of linear recurring sequences*, Finite Fields Appl. **1** (1995), no. 2, 204–218, Special issue dedicated to Leonard Carlitz. [p. 55]
[68] F. Q. Gouvêa, *p-adic numbers*, third ed., Universitext, Springer, Cham, [2020] ©2020, An introduction. [p. 164]
[69] A. Graham, *Kronecker products and matrix calculus: with applications*, Ellis Horwood Series in Mathematics and its Applications, Ellis Horwood Ltd., Chichester; Halsted Press [John Wiley & Sons, Inc.], New York, 1981. [p. 39]
[70] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics*, second ed., Addison-Wesley Publishing Company, Reading, MA, 1994, A foundation for computer science. [p. 25]

[71] J. Grantham and A. Granville, *Fibonacci primes, primes of the form 2^n-k and beyond*, J. Number Theory **261** (2024), 190–219. [p. 149]

[72] A. Granville, *Classifying linear division sequences*, https://arxiv.org/abs/2206.11823. [pp. 126 and 149]

[73] F. J. Grunewald, D. Segal, and G. C. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. **93** (1988), no. 1, 185–223. [p. 11]

[74] R. K. Guy, *Unsolved problems in number theory*, third ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004. [p. 151]

[75] M. Hall, *Divisibility Sequences of Third Order*, Amer. J. Math. **58** (1936), no. 3, 577–584. [p. 149]

[76] G. Hansel, *Une démonstration simple du théorème de Skolem–Mahler–Lech*, Theoret. Comput. Sci. **43** (1986), no. 1, 91–98. [p. 115]

[77] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), no. 1, 1–70. [p. 149]

[78] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles. [pp. 5 and 149]

[79] E. Heppner, *über Primzahlen der Form $n2^n+1$ bzw. $p2^p+1$*, Monatsh. Math. **85** (1978), no. 2, 99–103. [p. 151]

[80] M. D. Hirschhorn, *An amazing identity of Ramanujan*, Math. Mag. **68** (1995), no. 3, 199–201. [p. 59]

[81] C. Hooley, *Applications of sieve methods to the theory of numbers*, Cambridge Tracts in Mathematics, No. 70, Cambridge University Press, Cambridge-New York-Melbourne, 1976. [p. 151]

[82] J. E. Hopcroft, R. Motvani, and J. D. Ullman, *Introduction to automata theory, languages, and computation*, Addison-Wesley Series in Computer Science, Pearson Addison-Wesley, 2007. [pp. 9 and 10]

[83] IMO, *International Mathematical Olympiad*, https://www.imo-official.org. [p. 120]

[84] M. J. Jacobson, Jr. and H. C. Williams, *Solving the Pell equation*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, Springer, New York, 2009. [p. 4]

[85] O. Järviniemi, *Positive lower density for prime divisors of generic linear recurrences*, Math. Proc. Cambridge Philos. Soc. **175** (2023), no. 3, 467–478. [p. 150]

[86] O. Järviniemi and J. Teräväinen, *Composite values of shifted exponentials*, Adv. Math. **429** (2023), Paper No. 109187, 48. [p. 151]

[87] U. Jetzek, *Galois fields, linear feedback shift registers and their applications*, Hanser, 2018. [pp. 85 and 87]

[88] O. V. Kamlovskii, *Frequency characteristics of linear recurrent sequences over Galois rings*, Mat. Sb. **200** (2009), no. 4, 31–52. [p. 87]

[89] O. V. Kamlovskii, *Improving bounds for the number of occurrences of elements in linear recurrent sequences over Galois rings*, Fundam. Prikl. Mat. **17** (2011/12), no. 7, 97–115. [p. 87]

[90] O. V. Kamlovskii, *The Sidel'nikov method for estimating the number of signs on segments of linear recurrence sequences over Galois rings*, Math. Notes **91** (2012), no. 3-4, 354–363, Translation of Mat. Zametki **91** (2012), no. 3, 371–382. [p. 87]

[91] M. Kauers and P. Paule, *The concrete tetrahedron*, Texts and Monographs in Symbolic Computation, SpringerWienNewYork, Vienna, 2011, Symbolic sums, recurrence equations, generating functions, asymptotic estimates. [p. 1]

[92] M. Kauers and D. Zeilberger, *Factorization of C-finite sequences*, Advances in computer algebra, Springer Proc. Math. Stat., vol. 226, Springer, Cham, 2018, pp. 131–147. [p. 55]

[93] W. Keller, *New Cullen primes*, Math. Comp. **64** (1995), no. 212, 1733–1741, S39–S46, With a biographical sketch of James Cullen by T. G. Holt and a supplement by Keller and Wolfgang Niebuhr. [p. 144]

[94] Z. Kelley, *Roots of sparse polynomials over a finite field*, LMS J. Comput. Math. **19** (2016), 196–204. [p. 87]

[95] G. Kemper, *A course in commutative algebra*, Graduate Texts in Mathematics, vol. 256, Springer, Heidelberg, 2011. [p. 11]

[96] G. Kenison, *On the Skolem Problem for reversible sequences*, 47th International Symposium on Mathematical Foundations of Computer Science, LIPIcs. Leibniz Int. Proc. Inform., vol. 241, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2022, pp. Art. No. 61, 15. [p. 115]

[97] G. Kenison, R. Lipton, J. Ouaknine, and J. Worrell, *On the Skolem problem and prime powers*, ISSAC'20—Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation, ACM, New York, [2020] ©2020, pp. 289–296. [p. 116]

[98] J. Klaška, *Short remark on Fibonacci–Wieferich primes*, Acta Math. Univ. Ostrav. **15** (2007), no. 1, 21–25. [p. 150]

[99] J. Klaška, *Donald Dines Wall's conjecture*, Fibonacci Quart. **56** (2018), no. 1, 43–51. [p. 150]

[100] S. C. Kleene, *Representation of events in nerve nets and finite automata*, Automata studies, Ann. of Math. Stud., vol. no. 34, Princeton Univ. Press, Princeton, NJ, 1956, pp. 3–41. [p. 10]

[101] A. W. Knapp, *Advanced algebra*, Cornerstones, Birkhäuser Boston, Inc., Boston, MA, 2007, Along with a companion volume *Basic algebra*. [p. 163]

[102] D. E. Knuth, *The art of computer programming. Vol. 2*, third ed., Addison-Wesley, Reading, MA, 1998, Seminumerical algorithms. [pp. 32 and 154]

[103] N. M. Korobov, *The distribution of non-residues and of primitive roots in recurrence series*, Doklady Akad. Nauk SSSR (N.S.) **88** (1953), 603–606. [p. 87]

[104] C. Krattenthaler, *Advanced determinant calculus*, Sém. Lothar. Combin. **42** (1999), Art. B42q, 67, The Andrews Festschrift (Maratea, 1998). [p. 55]

[105] C. Krattenthaler, *Advanced determinant calculus: a complement*, Linear Algebra Appl. **411** (2005), 68–166. [p. 55]

[106] L. Kronecker, *Zur Theorie der Elimination einer Variabeln aus zwei algebraischen Gleichungen.*, Berl. Monatsber. **1881** (1881), 535–600 (German). [p. 55]

[107] L. Kuipers and J. S. Shiue, *A distribution property of the sequence of Fibonacci numbers*, Fibonacci Quart. **10** (1972), no. 4, 375–376, 392. [p. 154]

[108] V. L. Kurakin, *Convolution of linear recurrent sequences*, Uspekhi Mat. Nauk **48** (1993), no. 4(292), 235–236. [p. 58]

[109] V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev, and A. A. Nechaev, *Linear recurring sequences over rings and modules*, J. Math. Sci. **76** (1995), no. 6, 2793–2915, Algebra, 2. [p. 55]

[110] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. [pp. 25 and 157]

[111] C. Lech, *A note on recurring series*, Ark. Mat. **2** (1953), 417–421. [p. 115]

[112] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. (2) **31** (1930), no. 3, 419–448. [p. 149]

[113] D. H. Lehmer, *The vanishing of Ramanujan's function $\tau(n)$*, Duke Math. J. **14** (1947), 429–433. [p. 119]

[114] H. W. Lenstra, Jr. and J. O. Shallit, *Continued fractions and linear recurrences*, Math. Comp. **61** (1993), no. 203, 351–354. [p. 5]

[115] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, first ed., Cambridge University Press, Cambridge, 1994. [pp. 1, 55, 65, and 87]

[116] H. Lifchitz and R. Lifchitz, *PRP records*, http://www.primenumbers.net/prptop/prptop.php. [p. 144]

[117] R. Lipton, F. Luca, J. Nieuwveld, J. Ouaknine, D. Purser, and J. Worrell, *On the Skolem problem and the Skolem conjecture*, Proceedings of the 37th Annual ACM/IEEE Symposium on Logic in Computer Science, ACM, New York, [2022] ©2022, pp. [Article 5], 9. [pp. 98 and 115]

[118] J. H. Loxton and A. J. van der Poorten, *On the growth of recurrence sequences*, Math. Proc. Cambridge Philos. Soc. **81** (1977), no. 3, 369–376. [p. 116]

[119] F. Luca, J. Maynard, A. Noubissie, J. Ouaknine, and J. Worrell, *Skolem meets Bateman–Horn*, https://arxiv.org/abs/2308.01152. [p. 116]

[120] F. Luca, J. Ouaknine, and J. Worrell, *Universal Skolem sets*, 2021 36th Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), IEEE, [Piscataway], NJ, [2021] ©2021, p. [6 pp.]. [p. 116]

[121] F. Luca, J. Ouaknine, and J. Worrell, *A universal Skolem set of positive lower density*, 47th International Symposium on Mathematical Foundations of Computer Science, LIPIcs. Leibniz Int. Proc. Inform., vol. 241, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2022, pp. Art. No. 73, 12. [p. 116]

[122] F. Luca, J. Ouaknine, and J. Worrell, *On large zeros of linear recurrence sequences*, 50th International Symposium on Mathematical Foundations of Computer Science, LIPIcs. Leibniz Int. Proc. Inform., vol. 345, Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2025, pp. Art. No. 71, 11. [p. 116]

[123] F. Luca and E. Tron, *The distribution of self-Fibonacci divisors*, Advances in the theory of numbers, Fields Inst. Commun., vol. 77, Fields Inst. Res. Math. Sci., Toronto, ON, 2015, pp. 149–158. [p. 117]

[124] E. Lucas, *Théorèmes D'Arithmétique*, Atti R. Acc. Sc. Torino **13** (1877–1878), 271–284. [p. 153]

[125] E. Lucas, *Theorie des Fonctions Numeriques Simplement Periodiques. [Continued]*, Amer. J. Math. **1** (1878), no. 3, 197–240. [pp. 149 and 150]

[126] K. Mahler, *Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen*, Proc. Akad. Wet. Amsterdam **38** (1935), 50–60 (German). [p. 115]

[127] G. E. Martin, *Geometric constructions*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1998. [p. 149]

[128] J. L. Massey, *Shift-register synthesis and BCH decoding*, IEEE Trans. Inform. Theory **IT-15** (1969), 122–127. [p. 56]

[129] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), no. 6, 125–180 (Russian), Translation in Izv. Math. **64** (2000), no. 6, 1217–1269. [pp. 100 and 101]

[130] R. J. McIntosh and E. L. Roettger, *A search for Fibonacci–Wieferich and Wolstenholme primes*, Math. Comp. **76** (2007), no. 260, 2087–2094. [p. 150]

[131] I. Mező, *Combinatorics and number theory of counting sequences*, Discrete Mathematics and its Applications (Boca Raton), CRC Press, Boca Raton, FL, [2020] ©2020. [p. 42]

[132] M. Mignotte, T. N. Shorey, and R. Tijdeman, *The distance between terms of an algebraic recurrence sequence*, J. Reine Angew. Math. **349** (1984), 63–76. [p. 98]

[133] W. H. Mills, *Continued fractions and linear recurrences*, Math. Comp. **29** (1975), 173–180. [p. 56]

[134] A. Mohammadi, *Improved bounds on Gauss sums in arbitrary finite fields*, Int. J. Number Theory **15** (2019), no. 10, 2027–2041. [p. 87]

[135] L. J. Mordell, *On Mr. Ramanujan's empirical expansions of modular functions*, Proc. Camb. Philos. Soc. **19** (1917), 117–124. [p. 5]

[136] P. Moree and P. Stevenhagen, *Prime divisors of Lucas sequences*, Acta Arith. **82** (1997), no. 4, 403–410. [p. 150]

[137] G. L. Mullen and I. Shparlinski, *Values of linear recurring sequences of vectors over finite fields*, Acta Arith. **65** (1993), no. 3, 221–226. [p. 87]

[138] M. R. Murty and F. Séguin, *Prime divisors of sparse values of cyclotomic polynomials and Wieferich primes*, J. Number Theory **201** (2019), 1–22. [pp. 113 and 120]

[139] M. R. Murty, F. Séguin, and C. L. Stewart, *A lower bound for the two-variable Artin conjecture and prime divisors of recurrence sequences*, J. Number Theory **194** (2019), 8–29. [p. 150]

[140] M. B. Nathanson, *Elementary methods in number theory*, Graduate Texts in Mathematics, vol. 195, Springer-Verlag, New York, 2000. [p. 77]

[141] J. Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. [p. 166]

[142] H. Niederreiter, *Distribution of Fibonacci numbers* mod 5^k, Fibonacci Quart. **10** (1972), no. 4, 373–374. [p. 154]

[143] OEIS Foundation Inc., *The On-Line Encyclopedia of Integer Sequences*, http://oeis.org. [p. 144]

[144] M. Petkovšek, H. S. Wilf, and D. Zeilberger, $A = B$, A K Peters, Ltd., Wellesley, MA, 1996, With a foreword by Donald E. Knuth, With a separately available computer disk. [p. 55]

[145] T. A. Pierce, *The numerical factors of the arithmetic forms* $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$, Ann. of Math. (2) **18** (1916), no. 2, 53–64. [p. 149]

[146] R. G. E. Pinch, *Recurrent sequences modulo prime powers*, Cryptography and coding, III (Cirencester, 1991), Inst. Math. Appl. Conf. Ser. New Ser., vol. 45, Oxford Univ. Press, New York, 1993, pp. 297–310. [p. 87]

[147] G. Pólya, *Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen*, J. Reine Angew. Math. **151** (1921), 1–31. [p. 117]

[148] C. Pomerance, *Recent developments in primality testing*, Math. Intelligencer **3** (1980/81), no. 3, 97–105. [p. 149]

[149] Y. Pourchet, *Solution du problème arithmétique du quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sci. Paris Sér. A-B **288** (1979), no. 23, A1055–A1057. [p. 117]

[150] PrimeGrid, *Subproject status*, https://www.primegrid.com/server_status_subprojects.php. [p. 144]

[151] PrimeGrid, *Welcome to the Wieferich and Wall–Sun–Sun Prime Search*, https://www.primegrid.com/forum_thread.php?id=9436. [p. 150]

[152] N. Privault, *Discrete stochastic processes—tools for machine learning and data science*, Springer Undergraduate Mathematics Series, Springer, Cham, [2024] ©2024. [p. 8]

[153] D. Purser, P. Bacik, and J. Nieuwveld, *SKOLEM Tool – Solver for the Skolem Problem on Integer LRS*, 2022, https://skolem.mpi-sws.org. [pp. 98 and 115]

[154] A. Ralston and P. Rabinowitz, *A first course in numerical analysis*, second ed., Dover Publications, Inc., Mineola, NY, 2001. [p. 120]

[155] S. Ramanujan, *On certain arithmetical functions [Trans. Cambridge Philos. Soc.* **22** *(1916), no. 9, 159–184]*, Collected papers of Srinivasa Ramanujan, AMS Chelsea Publ., Providence, RI, 2000, pp. 136–162. [p. 5]

[156] S. Ramanujan, *The lost notebook and other unpublished papers*, Springer-Verlag, Berlin; Narosa Publishing House, New Delhi, 1988, With an introduction by George E. Andrews. [p. 59]

[157] J. A. Reeds and N. J. A. Sloane, *Shift-register synthesis (modulo m)*, SIAM J. Comput. **14** (1985), no. 3, 505–513. [p. 56]

[158] G. J. Rieger, *Über Primzahlen und dünne Folgen*, Arch. Math. (Basel) **28** (1977), no. 6, 600–602. [p. 151]

[159] T. J. Rivlin, *Chebyshev polynomials—from approximation theory to algebra and number theory*, second ed., Dover Publications, Inc., Mineola, NY, 2020. [p. 6]

[160] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. [p. 71]

[161] H. Roskam, *Prime divisors of linear recurrences and Artin's primitive root conjecture for number fields*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 303–314, 21st Journées Arithmétiques (Rome, 2001). [p. 150]

[162] A. Rotkiewicz, *On the congruence* $2^{n-2} \equiv 1 (\mathrm{mod}\, n)$, Math. Comp. **43** (1984), no. 167, 271–272. [p. 120]

[163] R. Rumely, *Notes on van der Poorten's proof of the Hadamard quotient theorem. I, II*, Séminaire de Théorie des Nombres, Paris 1986–87, Progr. Math., vol. 75, Birkhäuser Boston, Boston, MA, 1988, pp. 349–382, 383–409. [p. 117]

[164] R. S. Rumely and A. J. van der Poorten, *Remarks on generalised power sums*, Bull. Austral. Math. Soc. **36** (1987), no. 2, 311–329. [p. 117]

[165] SageMath developers, *SageMath — a free open-source mathematics software system licensed under the GPL*, https://www.sagemath.org. [pp. ix and 45]

[166] C. Sanna, *Distribution of integral values for the ratio of two linear recurrences*, J. Number Theory **180** (2017), 195–207. [p. 117]

[167] C. Sanna, *On numbers n dividing the nth term of a Lucas sequence*, Int. J. Number Theory **13** (2017), no. 3, 725–734. [p. 117]

[168] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208; erratum 5 (1959), 259. [p. 149]

[169] H. P. Schlickewei, *Multiplicities of recurrence sequences*, Acta Math. **176** (1996), no. 2, 171–243. [p. 115]

[170] A. Selberg, *On discontinuous groups in higher-dimensional symmetric spaces*, Contributions to function theory (Internat. Colloq. Function Theory, Bombay, 1960), Tata Inst. Fund. Res., Bombay, 1960, pp. 147–164. [p. 115]

[171] I. E. Shparlinski, *Distribution of nonresidues and primitive roots in recurrent sequences*, Math. Notes **24** (1979), 823–828 (English). [p. 87]

[172] I. E. Shparlinski, *The number of different prime divisors of recurrent sequences*, Mat. Zametki **42** (1987), no. 4, 494–507, 622. [pp. 150 and 151]

[173] I. E. Shparlinski, *Distribution of values of recurrent sequences*, Problemy Peredachi Informatsii **25** (1989), no. 2, 46–53. [p. 87]

[174] I. E. Shparlinski, *Finite fields: theory and computation*, Mathematics and its Applications, vol. 477, Kluwer Academic Publishers, Dordrecht, 1999, The meeting point of number theory, computer science, coding theory and cryptography. [p. 74]

[175] I. E. Shparlinski, *Bounds of Gauss sums in finite fields*, Proc. Amer. Math. Soc. **132** (2004), no. 10, 2817–2824. [p. 87]

[176] J. H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. [p. 11]

[177] T. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, 8. Skand. Mat.-Kongr., 163-188 (1935)., 1935. [p. 115]

[178] P. J. Stephens, *Prime divisors of second-order linear recurrences. I*, J. Number Theory **8** (1976), no. 3, 313–332. [p. 150]

[179] C. L. Stewart, *On the greatest prime factor of terms of a linear recurrence sequence*, Rocky Mountain J. Math. **15** (1985), no. 2, 599–608, Number theory (Winnipeg, Man., 1983). [p. 151]

[180] C. L. Stewart, *On the greatest square-free factor of terms of a linear recurrence sequence*, Diophantine equations, Tata Inst. Fund. Res. Stud. Math., vol. 20, Tata Inst. Fund. Res., Mumbai, 2008, pp. 257–264. [pp. 151 and 154]

[181] C. L. Stewart, *On prime factors of terms of binary recurrence sequences*, Acta Arith. **209** (2023), 173–189. [p. 151]

[182] C. L. Stewart, *On divisors of Lucas and Lehmer numbers*, Acta Math. **211** (2013), no. 2, 291–314. [p. 151]

[183] Z. H. Sun and Z. W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), no. 4, 371–388. [p. 150]

[184] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, third ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015. [pp. 127 and 165]

[185] S. Uchiyama, *On a theorem of G. Pólya*, Proc. Japan Acad. **41** (1965), 517–520. [p. 117]

[186] A. J. van der Poorten, *Additive relations in number fields*, Seminar on number theory, Paris 1982–83 (Paris, 1982/1983), Progr. Math., vol. 51, Birkhäuser Boston, Boston, MA, 1984, pp. 259–266. [pp. 100 and 116]

[187] A. J. van der Poorten, *Some facts that should be better known, especially about rational functions*, Number theory and applications (Banff, AB, 1988), NATO Adv. Sci. Inst. Ser. C: Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 497–528. [p. 117]

[188] A. J. van der Poorten and H. P. Schlickewei, *Additive relations in fields*, J. Austral. Math. Soc. Ser. A **51** (1991), no. 1, 154–170. [pp. 100 and 116]

[189] A. J. van der Poorten, *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sci. Paris Sér. I Math. **306** (1988), no. 3, 97–102. [pp. 108 and 117]

[190] N. K. Vereshchagin, *The problem of the appearance of a zero in a linear recursive sequence*, Mat. Zametki **38** (1985), no. 2, 177–189, 347. [p. 98]

[191] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, third ed., Cambridge University Press, Cambridge, 2013. [p. 1]

[192] S. S. Wagstaff, Jr., *Divisors of Mersenne numbers*, Math. Comp. **40** (1983), no. 161, 385–397. [p. 149]

[193] D. D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly **67** (1960), 525–532. [p. 150]

[194] H. Walser, *The golden ratio—geometric and number theoretical considerations*, Springer, Berlin, 2024. [p. 23]

[195] M. Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc. **33** (1931), no. 1, 153–165. [p. 150]

[196] M. Ward, *The arithmetical theory of linear recurring series*, Trans. Amer. Math. Soc. **35** (1933), no. 3, 600–628. [p. 150]

[197] M. Ward, *The law of apparition of primes in a Lucasian sequence*, Trans. Amer. Math. Soc. **44** (1938), no. 1, 68–86. [p. 149]

[198] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508. [p. 12]

[199] L. R. Welch and R. A. Scholtz, *Continued fractions and Berlekamp's algorithm*, IEEE Trans. Inform. Theory **25** (1979), no. 1, 19–27. [p. 56]

[200] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. [p. 150]

[201] K. R. Yu and L.-k. Hung, *On binary recurrence sequences*, Indag. Math. (N.S.) **6** (1995), no. 3, 341–354. [p. 151]

[202] S. Yu, *Regular languages*, Handbook of formal languages, Vol. 1, Springer, Berlin, 1997, pp. 41–110. [p. 10]

[203] N. Zierler and W. H. Mills, *Products of linear recurring sequences*, J. Algebra **27** (1973), 147–157. [p. 55]

Index