4

Rational Generating Functions

4.1 Rational Power Series in One Variable

The theory of binomial posets developed in the previous chapter sheds considerable light on the "meaning" of generating functions and reduces certain types of enumerative problems to a routine computation. However, it does not seem worthwhile to attack more complicated problems from this point of view. The remainder of this book will for the most part be concerned with other techniques for obtaining and analyzing generating functions. We first consider the simplest general class of generating functions, namely, the *rational* generating functions. In this chapter we will concern ourselves primarily with rational generating functions in one variable; that is, generating functions of the form $F(x) = \sum_{n\geq 0} f(n)x^n$ that are rational functions in the ring $K[[x]]$, where K is a field. This means that there exist polynomials $P(x), Q(x) \in K[x]$ such that $F(x) = P(x)Q(x)^{-1}$ in $K[[x]]$. Here it is assumed that $Q(0) \neq 0$, so that $Q(x)^{-1}$ exists in $K[[x]]$. The field of all rational functions in x over K is denoted $K(x)$, so the ring of rational power series is given by $K[[x]] \cap K(x)$. For our purposes here it suffices to take $K = \mathbb{C}$ or sometimes $\mathbb{C}$ with some indeterminates adjoined.

The fundamental property of rational functions in $\mathbb{C}[[x]]$ from the viewpoint of enumeration is the following.

4.1.1 Theorem. *Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be a fixed sequence of complex numbers, $d \geq 1$ and $\alpha_d \neq 0$. The following conditions on a function $f : \mathbb{N} \to \mathbb{C}$ are equivalent:*

i.
$$\sum_{n\geq 0} f(n)x^n = \frac{P(x)}{Q(x)}, \tag{4.1}$$
where $Q(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_d x^d$ and $P(x)$ is a polynomial in x of degree less than d.

ii. For all $n \geq 0$,
$$f(n+d) + \alpha_1 f(n+d-1) + \alpha_2 f(n+d-2) + \cdots + \alpha_d f(n) = 0. \tag{4.2}$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

iii. For all $n \geq 0$,

$$f(n) = \sum_{i=1}^{k} P_i(n)\gamma_i^n, \tag{4.3}$$

where $1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_d x^d = \prod_{i=1}^{k}(1-\gamma_i x)^{d_i}$, *the* γ_i*'s are distinct and nonzero, and* $P_i(n)$ *is a polynomial of degree less than* d_i.

Proof. Fix $Q(x) = 1 + \alpha_1 x + \cdots + \alpha_d x^d$. Define four complex vector spaces as follows:

$V_1 = \{f : \mathbb{N} \to \mathbb{C}$ such that (i) holds$\}$,

$V_2 = \{f : \mathbb{N} \to \mathbb{C}$ such that (ii) holds$\}$,

$V_3 = \{f : \mathbb{N} \to \mathbb{C}$ such that (iii) holds$\}$,

$V_4 = \{f : \mathbb{N} \to \mathbb{C}$ such that $\sum_{n\geq 0} f(n)x^n = \sum_{i=1}^{k}\sum_{j=1}^{d_i} \beta_{ij}(1-\gamma_i x)^{-j}$, for some $\beta_{ij} \in \mathbb{C}$, where γ_i and d_i have the same meaning as in (iii)$\}$.

We first claim that $\dim V_4 = d$ (all dimensions are taken over $\mathbb{C}$). Now V_4 is spanned over $\mathbb{C}$ by the rational functions $R_{ij}(x) = (1-\gamma_i x)^{-j}$, where $1 \leq i \leq k$ and $1 \leq j \leq d_i$. There are $\sum d_i = d$ such functions, so $\dim V_4 \leq d$. It remains to show that the $R_{ij}(x)$'s are linearly independent. Suppose to the contrary that we have a linear relation

$$\sum c_{ij} R_{ij}(x) = 0, \tag{4.4}$$

where $c_{ij} \in \mathbb{C}$ and not all $c_{ij} = 0$. Let i be such that some $c_{ij} \neq 0$, and then let j be the largest integer for which $c_{ij} \neq 0$. Multiply equation (4.4) by $(1-\gamma_i x)^j$ and set $x = 1/\gamma_i$. We obtain $c_{ij} = 0$, a contradiction, proving that $\dim V_4 = d$.

Now in (i) we may choose the d coefficients of $P(x)$ arbitrarily. Hence, $\dim V_1 = d$. In (ii) we may choose $f(0), f(1), \ldots, f(d-1)$ and then the other $f(n)$'s are uniquely determined. Hence, $\dim V_2 = d$. In (iii) we see that $f(n)$ is determined by the d coefficients of the $P_i(n)$'s, so $\dim V_3 \leq d$. (It is not so apparent, as it was for (i) and (ii), that different choices of $P_i(n)$'s will produce different $f(n)$'s.) Now for $j \geq 0$ we have

$$\frac{1}{(1-\gamma x)^j} = \sum_{n\geq 0}(-\gamma)^n \binom{-j}{n} x^n = \sum_{n\geq 0} x^n \gamma^n \binom{j+n-1}{j-1}.$$

Since $\binom{j+n-1}{j-1}$ is a polynomial in n of degree j, we get $V_4 \subseteq V_3$. Since $\dim V_4 = d \geq \dim V_3$, we have $V_3 = V_4$.

If $f \in V_1$, then equate coefficients of x^n in the identity $Q(x)\sum_{n\geq 0} f(n)x^n = P(x)$ to get $f \in V_2$. Since $\dim V_1 = \dim V_2$, there follows $V_1 = V_2$.

By putting the sum $\sum_{i=1}^{k}\sum_{j=1}^{d_i} \beta_{ij}(1-\gamma_i x)^{-j}$ over a common denominator, we see that $V_4 \subseteq V_1$. Since $\dim V_1 = \dim V_4$, there follows $V_1 = V_2 = V_3\,(= V_4)$, so the proof is complete. □

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Before turning to some interesting variations and special cases of Theorem 4.1.1, we first give a couple of examples of how a rational generating function arises in combinatorics.

4.1.2 Example. The prototypical example of a function $f(n)$ satisfying the conditions of Theorem 4.1.1 is given by $f(n) = F_n$, a Fibonacci number. The recurrence $F_{n+2} = F_{n+1} + F_n$ yields the generating function $\sum_{n\geq 0} F_n x^n = P(x)/(1-x-x^2)$ for some polynomial $P(x) = a + bx$. The initial conditions $F_0 = 0, F_1 = 1$ imply that $P(x) = x$. Hence,

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

Now $1 - x - x^2 = (1-\varphi x)(1-\bar{\varphi}x)$, where

$$\varphi = \frac{1+\sqrt{5}}{2}, \quad \bar{\varphi} = \frac{1-\sqrt{5}}{2} = 1-\varphi = -\frac{1}{\varphi}.$$

Hence, $F_n = \alpha\varphi^n + \beta\bar{\varphi}^n$. Setting $n = 0, 1$ yields the linear equations

$$\alpha + \beta = 0, \quad \varphi\alpha + \bar{\varphi}\beta = 1,$$

with solution $\alpha = 1/\sqrt{5}$ and $\beta = -1/\sqrt{5}$. Hence,

$$F_n = \frac{\varphi^n - \bar{\varphi}^n}{\sqrt{5}}. \tag{4.5}$$

Although equation (4.5) has no direct combinatorial meaning, it still has many uses. For instance, since $-1 < \bar{\varphi} < 0$, it is easy to deduce that F_n is the nearest integer to $\varphi^n/\sqrt{5}$. Thus, we have a very accurate expression for the rate of growth of F_n. Moreover, the explicit formula (4.5) often gives a routine method for proving various identities and formulas involving F_n, though sometimes there are more enlightening combinatorial or algebraic proofs. An instance is mentioned in Example 4.7.16.

4.1.3 Example. Let $f(n)$ be the number of paths with n steps starting from $(0,0)$, with steps of the type $(1,0)$, $(-1,0)$, or $(0,1)$, and never intersecting themselves. For instance, $f(2) = 7$, as shown in Figure 4.1 (with the initial point at $(0,0)$ circled). Equivalently, letting $E = (1,0)$, $W = (-1,0)$, $N = (0,1)$, we want the number of words $A_1A_2\cdots A_n$ ($A_i = E, W$, or N) such that EW and WE never appear as factors. Let $n \geq 2$. There are $f(n-1)$ words of length n ending in N. There are $f(n-1)$ words of length n ending in EE, WW, or NE. There are $f(n-2)$ words of length n ending in NW. Every word of length at least 2 ends in exactly one of N, EE, WW, NE, or NW. Hence,

$$f(n) = 2f(n-1) + f(n-2), \quad f(0) = 1, \quad f(1) = 3.$$

By Theorem 4.1.1, there are numbers A and B for which $\sum_{n\geq 0} f(n)x^n = (A + Bx)/(1-2x-x^2)$. By, for example, comparing coefficients of 1 and x, we obtain

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

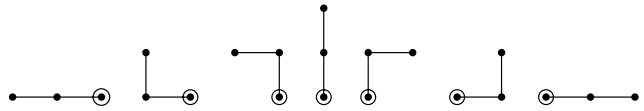

Figure 4.1 Some non-self-intersecting lattice paths.

$A = B = 1$, so

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

We have $1-2x-x^2 = (1-(1+\sqrt{2})x)(1-(1-\sqrt{2})x)$. Again by Theorem 4.1.1 we have $f(n) = a(1+\sqrt{2})^n + b(1-\sqrt{2})^n$ for some numbers a and b. By, for example, setting $n = 0, 1$, we obtain $a = \frac{1}{2}(1+\sqrt{2})$ and $b = \frac{1}{2}(1-\sqrt{2})$. Hence,

$$f(n) = \frac{1}{2}\left((1+\sqrt{2})^{n+1} + (1-\sqrt{2})^{n+1}\right). \tag{4.6}$$

Note that without the restriction that the path doesn't self-intersect, there are 3^n paths with n steps. With the restriction, the number has been reduced from 3^n to roughly $(1+\sqrt{2})^n = (2.414\cdots)^n$. Note also that since $-1 < 1-\sqrt{2} < 0$, it follows from equation (4.6) that

$$f(n) = \begin{cases} \left\lfloor \frac{1}{2}(1+\sqrt{2})^{n+1} \right\rfloor, & n \text{ even}, \\ \left\lceil \frac{1}{2}(1+\sqrt{2})^{n+1} \right\rceil, & n \text{ odd}. \end{cases}$$

4.2 Further Ramifications

In this section, we will consider additional information that can be gleaned from Theorem 4.1.1. First, we give an immediate corollary that is concerned with the possibilities of "simplifying" the formulas (4.1), (4.2), (4.3).

4.2.1 Corollary. *Suppose that $f : \mathbb{N} \to \mathbb{C}$ satisfies any (or all) of the three equivalent conditions of Theorem 4.1.1, and preserve the notation of that theorem. The following conditions are equivalent.*

i. $P(x)$ and $Q(x)$ are relatively prime. In other words, there is no way to write $P(x)/Q(x) = P_1(x)/Q_1(x)$, where P_1, Q_1 are polynomials and $\deg Q_1 < \deg Q = d$.

ii. There does not exist an integer $1 \leq c < d$ and complex numbers $\beta_1, \ldots, \beta_c$ such that

$$f(n+c) + \beta_1 f(n+c-1) + \cdots + \beta_c f(n) = 0$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

for all $n \geq 0$. In other words, equation (4.2) is the homogeneous linear recurrence with constant coefficients of least degree satisfied by $f(n)$.

iii. $\deg P_i(n) = d_i - 1$ *for* $1 \leq i \leq k$.

Next we consider the coefficients of *any* rational function $P(x)/Q(x)$, where $P, Q \in \mathbb{C}[x]$, not just those with $\deg P < \deg Q$. Write $\mathbb{C}^* = \mathbb{C} - \{0\}$.

4.2.2 Proposition. *Let $f : \mathbb{N} \to \mathbb{C}$ and suppose that $\sum_{n\geq 0} f(n)x^n = P(x)/Q(x)$, where $P, Q \in \mathbb{C}[x]$. Then there is a unique finite set $E_f \subset \mathbb{N}$ (called the* exceptional set *of f) and a unique function $f_1 : E_f \to \mathbb{C}^*$ such that the function $g : \mathbb{N} \to \mathbb{C}$ defined by*

$$g(n) = \begin{cases} f(n), & \text{if } n \notin E_f, \\ f(n) + f_1(n), & \text{if } n \in E_f. \end{cases}$$

satisfies $\sum_{n\geq 0} g(n)x^n = R(x)/Q(x)$ where $R \in \mathbb{C}[x]$ and $\deg R < \deg Q$. Moreover, assuming $E_f \neq \emptyset$ (i.e., $\deg P \geq \deg Q$), define $m(f) = \max\{i : i \in E_f\}$. Then

i. $m(f) = \deg P - \deg Q$.

ii. *$m(f)$ is the largest integer n for which equation (4.2) fails to hold.*

iii. *Writing $Q(x) = \prod_{i=1}^{k}(1 - \gamma_i x)^{d_i}$ as in Theorem 4.1.1(iii), there are unique polynomials $P_1, \ldots, P_k$ for which equation (4.3) holds for all n sufficiently large. Then $m(f)$ is the largest integer n for which* (4.3) *fails.*

Proof. By the division algorithm for polynomials in one variable, there are unique polynomials $L(x)$ and $R(x)$ with $\deg R < \deg Q$ such that

$$\frac{P(x)}{Q(x)} = L(x) + \frac{R(x)}{Q(x)}. \tag{4.7}$$

Thus, we must define E_f, $g(n)$, and $f_1(n)$ by

$$\sum_{n\geq 0} g(n)x^n = \frac{R(x)}{Q(x)}, \quad E_f = \{i : [x^i]L(x) \neq 0\}, \quad \sum_{n\in E_f} f_1(n)x^n = -L(x).$$

The rest of the proof is then immediate. □

We next describe a fast method for computing the coefficients of a rational function $P(x)/Q(x) = \sum_{n\geq 0} f(n)x^n$ by inspection. Suppose (without loss of generality) that $Q(x) = 1 + \alpha_1 x + \cdots + \alpha_d x^d$, and let $P(x) = \beta_0 + \beta_1 x + \cdots + \beta_e x^e$ (possibly $e \geq d$). Equating coefficients of x^n in

$$Q(x)\sum_{n\geq 0} f(n)x^n = P(x)$$

yields

$$f(n) = -\alpha_1 f(n-1) - \cdots - \alpha_d f(n-d) + \beta_n, \tag{4.8}$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

where we set $f(k) = 0$ for $k < 0$ and $\beta_k = 0$ for $k > e$. The recurrence (4.8) can easily be implemented by inspection (at least for reasonably small values of d and α_i). For instance, let

$$\frac{P(x)}{Q(x)} = \frac{1 - 2x + 4x^2 - x^3}{1 - 3x + 3x^3 - x^3}.$$

Then

$$\begin{aligned}
f(0) &= \beta_0 = 1,\\
f(1) &= 3f(0) + \beta_1 = 3 - 2 = 1,\\
f(2) &= 3f(1) - 3f(0) + \beta_2 = 3 - 3 + 4 = 4,\\
f(3) &= 3f(2) - 3f(1) + f(0) + \beta_3 = 12 - 3 + 1 - 1 = 9,\\
f(4) &= 3f(3) - 3f(2) + f(1) = 27 - 12 + 1 = 16,\\
f(5) &= 3f(4) - 3f(3) + f(2) = 48 - 27 + 4 = 25,
\end{aligned}$$

and so on. The sequence of values $1, 1, 4, 9, 16, 25, \ldots$ looks suspiciously like $f(n) = n^2$, except for $f(0) = 1$. Indeed, the exceptional set $E_f = \{0\}$, and

$$\frac{P(x)}{Q(x)} = 1 + \frac{x + x^2}{(1 - x)^3} = 1 + \sum_{n \geq 0} n^2 x^n.$$

We will discuss in Section 4.3 the situation when $f(n)$ is a polynomial, and in particular the case $f(n) = n^k$.

Proposition 4.2.2(i) explains the significance of the number $\deg P - \deg Q$ when $\deg P \geq \deg Q$. What about the case $\deg P < \deg Q$? This is best explained in the context of a kind of duality theorem. If $\sum_{n \geq 0} f(n)x^n = P(x)/Q(x)$ with $\deg P < \deg Q$, then the formulas (4.2) and (4.3) are valid. Either of them may be used to extend the domain of f to *negative* integers. In (4.2) we can just run the recurrence backwards (since by assumption $\alpha_d \neq 0$) by successively substituting $n = -1, -2, \ldots$. It follows that there is a *unique* extension of f to all of $\mathbb{Z}$ satisfying (4.2) for all $n \in \mathbb{Z}$. In (4.3) we can let n be a negative integer on the right-hand side. It is easy to see that these two extensions of f to $\mathbb{Z}$ agree.

4.2.3 Proposition. *Let $d \in \mathbb{N}$ and $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ with $\alpha_d \neq 0$. Suppose that $f : \mathbb{Z} \to \mathbb{C}$ satisfies*

$$f(n + d) + \alpha_1 f(n + d - 1) + \cdots + \alpha_d f(n) = 0 \text{ for all } n \in \mathbb{Z}.$$

Thus, $\sum_{n \geq 0} f(n) = F(x)$ is a rational function, as is $\sum_{n \geq 1} f(-n)x^n = \overline{F}(x)$. We then have

$$\overline{F}(x) = -F(1/x),$$

as rational functions.

NOTE. It is important to realize that Proposition 4.2.3 is a statement about the equality of *rational functions*, not power series. For instance, suppose that $f(n) = 1$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

for all $n \in \mathbb{Z}$. Then $F(x) = \sum_{n\geq 0} x^n = 1/(1-x)$ and $\overline{F}(x) = \sum_{n\geq 1} x^n = x/(1-x)$. Then as rational functions we have

$$-F(1/x) = -\frac{1}{1-1/x} = -\frac{x}{x-1} = \frac{x}{1-x} = \overline{F}(x).$$

Proof. Let $F(x) = P(x)/Q(x)$, where $Q(x) = 1+\alpha_1 x+\cdots+\alpha_d x^d$. Let $\mathcal{L}$ denote the complex vector space of all formal Laurent series $\sum_{n\in\mathbb{Z}} a_n x^n$, $a_n \in \mathbb{C}$. Although two such Laurent series cannot be formally multiplied in a meaningful way, we *can* multiply such a Laurent series by the polynomial $Q(x)$. The map $\mathcal{L} \xrightarrow{Q} \mathcal{L}$ given by multiplication by $Q(x)$ is a linear transformation. The hypothesis on f implies that

$$Q(x)\sum_{n\in\mathbb{Z}} f(n)x^n = 0.$$

Since multiplication by $Q(x)$ is linear, we have

$$Q(x)\sum_{n\geq 1} f(-n)x^{-n} = -Q(x)\sum_{n\geq 0} f(n)x^n = -P(x).$$

Substituting $1/x$ for x yields

$$\sum_{n\geq 1} f(-n)x^n = -\frac{P(1/x)}{Q(1/x)} = -F(1/x),$$

as desired. (The reader suspicious of this argument should check carefully that all steps are formally justified. Note in particular that the vector space $\mathcal{L}$ contains the two rings $\mathbb{C}[[x]]$ and $\left\{\sum_{n\leq n_0} a_n x^n\right\}$, whose intersection is $\mathbb{C}[x]$.) □

Proposition 4.2.3 allows us to explain the significance of certain properties of the rational function $P(x)/Q(x)$.

4.2.4 Corollary. *Let $d \in \mathbb{P}$ and $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ with $\alpha_d \neq 0$. Suppose that $f : \mathbb{Z} \to \mathbb{C}$ satisfies*

$$f(n+d)+\alpha_1 f(n+d-1)+\cdots+\alpha_d f(n) = 0$$

for all $n \in \mathbb{Z}$. Thus, $\sum_{n\geq 0} f(n)x^n = P(x)/Q(x)$ where $Q(x) = 1+\alpha_1 x+\cdots+\alpha_d x^d$ and $\deg P < \deg Q$. Say $P(x) = \beta_0+\beta_1 x+\cdots+\beta_{d-1}x^{d-1}$.

i. $\min\{n \in \mathbb{N} : f(n) \neq 0\} = \min\{j \in \mathbb{N} : \beta_j \neq 0\}$.
Moreover, if r denotes the value of the above minimum, then $f(r) = \beta_r$.

ii. $\min\{n \in \mathbb{P} : f(-n) \neq 0\} = \min\{j \in \mathbb{P} : \beta_{d-j} \neq 0\} = \deg Q - \deg P$.
Moreover, if s denotes the value of the above minimum, then $f(-s) = -\alpha_d^{-1}\beta_s$.

iii. Let $F(x) = P(x)/Q(x)$, and let r and s be as above. Then $F(x) = \pm x^{r-s}F(1/x)$ if and only if $f(n) = \mp f(-n+r-s)$ for all $n \in \mathbb{Z}$.

Proof. If

$$P(x) = \beta^r x^r + \beta_{r+1}x^{r+1}+\cdots+\beta_{d-1}x^{d-1},$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

then $P(x)/Q(x) = \beta_r x^r + \cdots$, so (i) is clear. If

$$P(x) = \beta_{d-s}x^{d-s} + \beta_{d-s-1}x^{d-s-1} + \cdots + \beta_0,$$

then by Proposition 4.2.3 we have

$$\sum_{n\geq 1} f(-n)x^n = -\frac{P(1/x)}{Q(1/x)} = -\frac{\beta_{d-s}x^{-(d-s)} + \cdots + \beta_0}{1 + \alpha_1 x^{-1} + \cdots + \alpha_d x^{-d}}$$

$$= \frac{-\alpha_d^{-1}(\beta_{d-s}x^s + \cdots + \beta_0 x^d)}{1 + \alpha_{d-1}\alpha_d^{-1}x + \cdots + \alpha_d^{-1}x^d} = -\alpha_d^{-1}\beta_{d-s}x^s + \cdots,$$

from which (ii) follows. Finally, (iii) is immediate from Proposition 4.2.3. □

Corollary 4.2.4(ii) answers the question raised earlier regarding the significance of $\deg Q - \deg P$ when $\deg Q > \deg P$. A situation to which this result applies is Corollary 3.15.13.

It is clear that if $F(x)$ and $G(x)$ are rational power series belonging to $\mathbb{C}[[x]]$, then $\alpha F(x) + \beta G(x)$ $(\alpha, \beta, \in \mathbb{C})$ and $F(x)G(x)$ are also rational. Moreover, if $F(x)/G(x) \in \mathbb{C}[[x]]$, then $F(x)/G(x)$ is rational. Perhaps somewhat less obvious is the closure of rational power series under the operation of *Hadamard product*. The Hadamard product $F * G$ of the power series $F(x) = \sum_{n\geq 0} f(n)x^n$ and $G(x) = \sum_{n\geq 0} g(n)x^n$ is defined by

$$F(x) * G(x) = \sum_{n\geq 0} f(n)g(n)x^n.$$

4.2.5 Proposition. *If $F(x)$ and $G(x)$ are rational power series, then so is the Hadamard product $F * G$.*

Proof. By Theorem 4.1.1 and Proposition 4.2.2, the power series $H(x) = \sum_{n\geq 0} h(n)x^n$ is rational if and only if $h(n) = \sum_{i=1}^m R_i(n)\zeta_i^n$, where $\zeta_1, \ldots, \zeta_m$ are fixed nonzero complex numbers, and $R_1, \ldots, R_m$ are fixed polynomials in n. Thus, if $F(x) = \sum_{n\geq 0} f(n)x^n$ and $G(x) = \sum_{n\geq 0} g(n)x^n$, then $f(n) = \sum_{i=1}^k P_i(n)\gamma_i^n$ and $g(n) = \sum_{j=1}^l Q_i(n)\delta_j^n$ for n large. Then

$$f(n)g(n) = \sum_{i,j} P_i(n)Q_j(n)(\gamma_i\delta_j)^n$$

for n large, so $F * G$ is rational. □

4.3 Polynomials

An important special class of functions $f: \mathbb{N} \to \mathbb{C}$ whose generating function $\sum_{n\geq 0} f(n)x^n$ is rational are the *polynomials*. Indeed, the following result is an immediate corollary of Theorem 4.1.1.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

4.3.1 Corollary. *Let $f : \mathbb{N} \to \mathbb{C}$, and let $d \in \mathbb{N}$. The following three conditions are equivalent:*

i. $\displaystyle\sum_{n\geq 0} f(n)x^n = \frac{P(x)}{(1-x)^{d+1}}$, *where* $P(x) \in \mathbb{C}[x]$ *and* $\deg P \leq d$.

ii. For all $n \geq 0$,

$$\sum_{i=0}^{d+1} (-1)^{d+1-i} \binom{d+1}{i} f(n+i) = 0.$$

In other words, $\Delta^{d+1} f(n) = 0$.

iii. $f(n)$ *is a polynomial function of* n *of degree at most* d. *(Moreover,* $f(n)$ *has degree exactly* d *if and only if* $P(1) \neq 0$.*)*

Note that the equivalence of (ii) and (iii) is just Proposition 1.9.2(a). Also note that when $P(1) \neq 0$, so that $\deg f = d$, then the leading coefficient of $f(n)$ is $P(1)/d!$. This may be seen, for example, by considering the coefficient of $(1-x)^{d+1}$ is the Laurent expansion of $\sum_{n\geq 0} f(n)x^n$ about $x = 1$.

The set of all polyonomials $f : \mathbb{N} \to \mathbb{C}$ (or $f : \mathbb{Z} \to \mathbb{C}$) of degree at most d is a vector space P_d of dimension $d+1$ over $\mathbb{C}$. This vector space has many natural choices of a basis. A description of these bases and the transition matrices among them would occupy a book in itself. Here we list what are perhaps the four most important bases, with a brief discussion of their significance. Note that any set of polynomials $p_0(n), p_1(n), \ldots, p_d(n)$ with $\deg p_i = i$ is a basis for P_d [why?].

a. n^i, $0 \leq i \leq d$. When a polynomial $f(n)$ is expanded in terms of this basis, then we of course obtain the usual coefficients of $f(n)$.

b. $\binom{n}{i}$, $0 \leq i \leq d$. (Alternatively, we could use $(n)_i = i!\binom{n}{i}$.) By Proposition 1.9.2(b) we have the expansion $f(n) = \sum_{i=0}^{d} (\Delta^i f(0)) \binom{n}{i}$, the discrete analogue of the Taylor series (still assuming that $f(n) \in P_d$) $f(x) = \sum_{i=0}^{d} D^i f(0) \frac{x^i}{i!}$, where $Df(t) = \frac{d}{dt} f(t)$. By Proposition 1.9.2(c), the transition matrices between the bases n^i and $\binom{n}{i}$ are essentially the Stirling numbers of the first and second kind, that is

$$n^j = \sum_{i=0}^{j} i! S(j,i) \binom{n}{i} = \sum_{i=0}^{j} S(j,i)(n)_i,$$

$$\binom{n}{j} = \frac{1}{j!} \sum_{i=0}^{j} s(j,i) n^i, \text{ or } (n)_j = \sum_{i=0}^{j} s(j,i) n^i.$$

c. $\left(\binom{n}{i}\right) = (-1)^i \binom{-n}{i}$, $0 \leq i \leq d$. (Alternatively, we could use the rising factorial $n(n+1)\cdots(n+i-1) = i!\left(\binom{n}{i}\right)$.) We thus have

$$f(n) = \sum_{i=0}^{d} (-1)^i (\Delta^i f(-n))_{n=0} \left(\binom{n}{i}\right).$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Equivalently, if one forms the difference table of $f(n)$ then the coefficients of $\left(\binom{n}{i}\right)$ in the expansion $f(n) = \sum c_i \left(\binom{n}{i}\right)$ are the elements of the diagonal beginning with $f(0)$ and moving southwest. For instance, if $f(n) = n^3 + n + 1$ then we get the difference table

$$\begin{array}{ccccccc} & & -29 & & -9 & & -1 \qquad 1 = f(0) \\ & 20 & & 8 & & 2 & \\ -12 & & -6 & & & & \\ & 6, & & & & & \end{array}$$

so $n^3 + n + 1 = 1 + 2\left(\binom{n}{1}\right) - 6\left(\binom{n}{2}\right) + 6\left(\binom{n}{3}\right)$. The transition matrices with n^i and with $\binom{n}{i}$ are given by

$$n^j = \sum_{i=0}^{j} (-1)^{j-i} i! S(j,i) \left(\binom{n}{i}\right),$$

$$\left(\binom{n}{j}\right) = \frac{1}{j!} \sum_{i=0}^{j} c(j,i) n^i, \text{ where } c(j,i) = (-1)^{j-i} s(j,i),$$

$$\binom{n}{j} = \sum_{i=1}^{j} (-1)^{j-i} \binom{j-1}{i-1} \left(\binom{n}{i}\right),$$

$$\left(\binom{n}{j}\right) = \sum_{i=1}^{j} \binom{j-1}{i-1} \binom{n}{i}.$$

d. $\binom{n+d-i}{d}$, $0 \le i \le d$. There are (at least) two quick ways to see that this is a basis for P_d. Given that $f(n) = \sum_{i=0}^{d} c_i \binom{n+d-i}{d}$, set $n = 0$ to obtain c_0 uniquely. Then set $n = 1$ to obtain c_1 uniquely, and so on. Thus, the $d+1$ polynomials $\binom{n+d-i}{d}$ are linearly independent and therefore form a basis for P_d. Alternatively, observe that

$$\sum_{n \ge 0} \binom{n+d-i}{d} x^n = \frac{x^i}{(1-x)^{d+1}}.$$

Hence, the statement that the polynomials $\binom{n+d-i}{d}$ form a basis for P_d is equivalent (in view of Corollary 4.3.1) to the obvious fact that the rational functions $x^i/(1-x)^{d+1}$, $0 \le i \le d$, form a basis for all rational functions $P(x)/(1-x)^{d+1}$, where $P(x)$ is a polynomial of degree at most d. If

$$\sum_{n \ge 0} f(n) x^n = \frac{w_0 + w_1 x + \cdots + w_d x^d}{(1-x)^{d+1}},$$

then the numbers $w_0, w_1, \ldots, w_d$ are called the *f-Eulerian numbers*, and the polynomial $P(x) = w_0 + w_1 x + \cdots + w_d x^d$ is called the *f-Eulerian polynomial*. If in particular $f(n) = n^d$, then it follows from Proposition 1.4.4 that the f-Eulerian numbers are simply the *Eulerian numbers* $A(d,i)$, whereas the

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

f-Eulerian polynomial is the *Eulerian polynomial* $A_d(x)$. Just as for ordinary Eulerian numbers, the f-Eulerian numbers frequently have combinatorial significance. A salient example are order polynomials $\Omega_{P,\omega}(m)$ of labeled posets (Theorem 3.15.8). We could discuss the transition matrices between the basis $\binom{n+d-i}{d}$ and the other three bases considered earlier, but this is not a particularly fruitful endeavor and will be omitted.

4.4 Quasipolynomials

A *quasipolynomial* (known by many other names, such as *pseudopolynomial* and *polynomial on residue classes* (PORC)) of *degree* d is a function $f : \mathbb{N} \to \mathbb{C}$ (or $f : \mathbb{Z} \to \mathbb{C}$) of the form

$$f(n) = c_d(n)n^d + c_{d-1}(n)n^{d-1} + \cdots + c_0(n),$$

where each $c_i(n)$ is a *periodic function* (with integer period), and where $c_d(n)$ is not identically zero. Equivalently, f is a quasipolynomial if there exists an integer $N > 0$ (namely, a common period of $c_0, c_1, \ldots, c_d$) and polynomials $f_0, f_1, \ldots, f_{N-1}$ such that

$$f(n) = f_i(n) \text{ if } n \equiv i \pmod{N}.$$

The integer N (which is not unique) will be called a *quasiperiod* of f.

4.4.1 Proposition. *The following conditions on a function $f : \mathbb{N} \to \mathbb{C}$ and integer $N > 0$ are equivalent.*

i. f *is a quasipolynomial of quasiperiod* N.

ii. $\displaystyle\sum_{n\geq 0} f(n)x^n = \frac{P(x)}{Q(x)}$, *where* $P(x), Q(x) \in \mathbb{C}[x]$, *every zero* α *of* $Q(x)$ *satisfies* $\alpha^N = 1$ *(provided* $P(x)/Q(x)$ *has been reduced to lowest terms), and* $\deg P < \deg Q$.

iii. For all $n \geq 0$,

$$f(n) = \sum_{i=1}^{k} P_i(n)\gamma_i^n, \tag{4.9}$$

where each P_i *is a polynomial function of* n *and each* γ_i *satisfies* $\gamma_i^N = 1$.

Moreover, the degree of $P_i(n)$ *in equation (4.9) is equal to one less than the multiplicity of the root* γ_i^{-1} *in* $Q(x)$, *provided* $P(x)/Q(x)$ *has been reduced to lowest terms.*

Proof. The proof is a simple consequence of Theorem 4.1.1; the details are omitted. □

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

4.4.2 Example. Let $\overline{p}_k(n)$ denote the number of partitions of n into at most k parts. Thus from equation (1.76), we have

$$\sum_{n\geq 0} \overline{p}_k(n)x^n = \frac{1}{(1-x)(1-x^2)\cdots(1-x^k)}.$$

Hence $\overline{p}_k(n)$ is a quasipolynomial. Its minimum quasiperiod in equal to the least common multiple of $1,2,\ldots,k$, and its degree is $k-1$. Much more precise statements are possible; consider for instance the case $k=6$. Then

$$\overline{p}_6(n) = c_5 n^5 + c_4 n^4 + c_3 n^3 + c_2(n)n^2 + c_1(n)n + c_0(n),$$

where $c_3, c_4, c_5 \in \mathbb{Q}$ (and in fact $c_5 = 1/5!6!$, as may be seen by considering the coefficient of $(1-x)^{-6}$ in the Laurent expansion of $1/(1-x)(1-x^2)\cdots(1-x^6)$ about $x=1$), $c_2(n)$ has period 2, $c_1(n)$ has period 6, and $c_0(n)$ has period 60. (These need not be the minimum periods.) Moreover, $c_1(n)$ is in fact the sum of periodic functions of periods 2 and 3. The reader should be able to read these facts off from the generating function $1/(1-x)(1-x^2)\cdots(1-x^6)$.

The case $k=3$ is particularly elegant. Let us write $[a_0,a_1,\ldots,a_{p-1}]_p$ for the periodic function $c(n)$ of period p satisfying $c(n)=a_i$ if $n \equiv i \pmod{p}$. A rather tedious computation yields

$$\overline{p}_3(n) = \frac{1}{12}n^2 + \frac{1}{2}n + \left[1, \frac{5}{12}, \frac{2}{3}, \frac{3}{4}, \frac{2}{3}, \frac{5}{12}\right]_6.$$

It is essentially an "accident" that this expression for $\overline{p}_3(n)$ can be written in the concise form $\| \frac{1}{12}(n+3)^2 \|$, where $\| t \|$ denotes the nearest integer to the real number t, that is, $\| t \| = \lfloor t + \frac{1}{2} \rfloor$.

4.5 Linear Homogeneous Diophantine Equations

The remainder of this chapter will be devoted to two general areas in which rational generating functions play a prominent role. Another such area is the theory of (P,ω)-partitions developed in Section 3.15.

Let Φ be an $r \times m$ matrix with integer entries (or $\mathbb{Z}$-*matrix*). Many combinatorial problems turn out to be equivalent to finding all (column) vectors $\boldsymbol{\alpha} \in \mathbb{N}^m$ satisfying

$$\Phi\boldsymbol{\alpha} = \mathbf{0}, \tag{4.10}$$

where $\mathbf{0} = (0,0,\ldots,0) \in \mathbb{N}^r$. (For convenience of notation we will write column vectors as row vectors.) Equation (4.10) is equivalent to a system of r homogeneous linear equations with integer coefficients in the m unknowns $\boldsymbol{\alpha} = (\alpha_1,\ldots,\alpha_m)$. Note that if we were searching for solutions $\boldsymbol{\alpha} \in \mathbb{Z}^m$ (rather than $\boldsymbol{\alpha} \in \mathbb{N}^m$), then there would be little problem. The solutions in $\mathbb{Z}^m$ (or $\mathbb{Z}$-*solutions*) form a subgroup G of $\mathbb{Z}^m$ and hence by the theory of finitely generated abelian groups, G is a finitely generated free abelian group. The minimal number of generators (or *rank*)

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

of G is equal to the nullity of the matrix Φ, and there are well-known algorithms for finding the generators of G explicitly. The situation for solutions in $\mathbb{N}^m$ (or $\mathbb{N}$-*solutions*) is not so clear. The set of solutions forms not a group but rather a (commutative) *monoid* (semigroup with identity) $E = E_\Phi$. It certainly is not the case that E is a free commutative monoid; that is, there exist $\boldsymbol{\alpha_1}, \ldots, \boldsymbol{\alpha_s} \in E$ such that every $\boldsymbol{\alpha} \in E$ can be written uniquely as $\sum_{i=1}^{s} a_i \boldsymbol{\alpha_i}$, where $a_i \in \mathbb{N}$. For instance, take $\Phi = [1, 1, -1, -1]$. Then in E there is the nontrivial relation $(1,0,1,0) + (0,1,0,1) = (1,0,0,1) + (0,1,1,0)$.

Without loss of generality, we may assume that the rows of Φ are linearly independent; that is, $\operatorname{rank} \Phi = r$. If now $E \cap \mathbb{P}^m = \emptyset$ (i.e., equation (4.10) has no $\mathbb{P}$-solution), then for some $i \in [m]$, every $(\alpha_1, \ldots, \alpha_m) \in E$ satisfies $\alpha_i = 0$. It costs nothing to ignore this entry α_i. Hence, we may assume from now on that $E \cap \mathbb{P}^m \neq \emptyset$. We then call E a *positive* monoid.

We will analyze the structure of the monoid E to the extent of being able to write down a formula for the generating function

$$E(\boldsymbol{x}) = E(x_1, \ldots, x_m) = \sum_{\boldsymbol{\alpha} \in E} \boldsymbol{x}^{\boldsymbol{\alpha}}, \tag{4.11}$$

where if $\boldsymbol{\alpha} = \{\alpha_1, \ldots, \alpha_m\}$ then $\boldsymbol{x}^{\boldsymbol{\alpha}} = x_1^{\alpha_1} \cdots x_m^{\alpha_m}$. We will also consider the closely related generating function

$$\overline{E}(\boldsymbol{x}) = \sum_{\boldsymbol{\alpha} \in \overline{E}} \boldsymbol{x}^{\boldsymbol{\alpha}}, \tag{4.12}$$

where $\overline{E} = E \cap \mathbb{P}^m$. Since we are assuming that $\overline{E} \neq \emptyset$, it follows that $\overline{E}(\boldsymbol{x}) \neq 0$. In general throughout this section, if G is any subset of $\mathbb{N}^m$, then we write

$$G(\boldsymbol{x}) = \sum_{\boldsymbol{\alpha} \in G} \boldsymbol{x}^{\boldsymbol{\alpha}}.$$

First, let us note that there is no real gain in generality by also allowing *inequalities* of the form $\Psi \boldsymbol{\alpha} \geq \mathbf{0}$ for some $s \times m$ $\mathbb{Z}$-matrix Ψ. This is because we can introduce slack variables $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_s)$ and replace the inequality $\Psi \boldsymbol{\alpha} \geq \mathbf{0}$ by the equality $\Psi \boldsymbol{\alpha} - \boldsymbol{\gamma} = \mathbf{0}$. An $\mathbb{N}$-solution to the latter equality is equivalent to an $\mathbb{N}$-solution to the original inequality. In particular, the theory of P-partitions (where the labeling ω is natural) of Section 3.15 can be subsumed by the general theory of $\mathbb{N}$-solutions to equation (4.10), though P-partitions have many additional special features. Specifically, introduce variables α_t for all $t \in P$ and α_{st} for all pairs $s < t$ (or in fact just for $s \lessdot t$). Then an $\mathbb{N}$-solution α to the system

$$\alpha_s - \alpha_t - \alpha_{st} = 0, \text{ for all } s < t \text{ in } P \text{ (or just for all } s \lessdot t) \tag{4.13}$$

is equivalent to the P-partition $\sigma\colon P \to \mathbb{N}$ given by $\sigma(t) = \alpha_t$. Moreover, a $\mathbb{P}$-solution to equation (4.13) is equivalent to a strict P-partition τ with positive parts. If we merely subtract one from each part, then we obtain an arbitrary strict P-partition. Hence by Theorem 3.15.10, the generating functions $E(\boldsymbol{x})$ and

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

$\overline{E}(\boldsymbol{x})$ of (4.11) and (4.12), for the system (4.13), are related by

$$\overline{E}(\boldsymbol{x}) = (-1)^p E(1/\boldsymbol{x}), \tag{4.14}$$

where $1/\boldsymbol{x}$ denotes the substitution of $1/x_i$ for x_i in the rational function $E(\boldsymbol{x})$. This suggests a reciprocity theorem for the general case (4.10), and one of our goals will be to prove such a theorem. (We do not even know yet whether $E(\boldsymbol{x})$ and $\overline{E}(\boldsymbol{x})$ are rational functions; otherwise, equation (4.14) makes no sense.) The theory of P-partitions provides clues about obtaining a formula for $E(\boldsymbol{x})$. Ideally, we would like to partition in an explicit and canonical way the monoid E into finitely many easily understood parts. Unfortunately, we will have to settle for somewhat less. We will express E as a union of nicely behaved parts (called "simplicial monoids"), but these parts will not be disjoint, and it will be necessary to analyze how they intersect. Moreover, the simplicial monoids themselves will be obtained by a rather arbitrary construction (not nearly as elegant as associating a P-partition to a unique $w \in \mathcal{L}(P)$), and it will require some work to analyze the simplicial monoids themselves. But the reward for all this effort will be an extremely general theory with a host of interesting and significant applications.

Although the theory we are about to derive can be developed purely algebraically, it is more convenient and intuitive to proceed geometrically. To this end we will briefly review some of the basic theory of convex polyhedral cones. A *linear half-space* $\mathcal{H}$ of $\mathbb{R}^m$ is a subset of $\mathbb{R}^m$ of the form $\mathcal{H} = \{\boldsymbol{v} : \boldsymbol{v} \cdot \boldsymbol{w} \geq 0\}$ for some fixed nonzero vector $\boldsymbol{w} \in \mathbb{R}^m$. A *convex polyhedral cone* $\mathcal{C}$ in $\mathbb{R}^m$ is defined to be the intersection of finitely many half-spaces. (Some authorities would require that $\mathcal{C}$ contain a vector $\boldsymbol{v} \neq 0$.) We say that $\mathcal{C}$ is *pointed* if it doesn't contain a line; or equivalently, whenever $\mathbf{0} \neq \boldsymbol{v} \in \mathcal{C}$ then $-\boldsymbol{v} \notin \mathcal{C}$. A *supporting hyperplane* $\mathcal{H}$ of $\mathcal{C}$ is a linear hyperplane of which $\mathcal{C}$ lies entirely on one side. In other words, $\mathcal{H}$ divides $\mathbb{R}^m$ into two closed half-spaces $\mathcal{H}^+$ and $\mathcal{H}^-$ (whose intersection is $\mathcal{H}$), such that either $\mathcal{C} \subseteq \mathcal{H}^+$ or $\mathcal{C} \subseteq \mathcal{H}^-$. A *face* of $\mathcal{C}$ is a subset $\mathcal{C} \cap \mathcal{H}$ of $\mathcal{C}$, where $\mathcal{H}$ is a supporting hyperplane. Every face $\mathcal{F}$ of $\mathcal{C}$ is itself a convex polyhedral cone, including the degenerate face $\{\mathbf{0}\}$. The *dimension* of $\mathcal{F}$, denoted $\dim \mathcal{F}$, is the dimension of the subspace of $\mathbb{R}^m$ spanned by $\mathcal{F}$. If $\dim \mathcal{F} = i$, then $\mathcal{F}$ is called an *i-face*. In particular, $\{\mathbf{0}\}$ and $\mathcal{C}$ are faces of $\mathcal{C}$, called *improper*, and $\dim\{\mathbf{0}\} = 0$. A 1-face is called an *extreme ray*, and if $\dim \mathcal{C} = d$ then a $(d-1)$-face is called a *facet*. We will assume the standard result that a pointed polyhedral cone $\mathcal{C}$ has only finitely many extreme rays, and that $\mathcal{C}$ is the convex hull of its extreme rays. A *simplicial cone* σ is an e-dimensional pointed convex polyhedral cone with e extreme rays (the minimum possible). Equivalently, σ is simplicial if there exist *linearly independent* vectors $\boldsymbol{\beta_1}, \ldots, \boldsymbol{\beta_e}$ for which $\sigma = \{a_1\boldsymbol{\beta_1} + \cdots + a_e\boldsymbol{\beta_e} : a_i \in \mathbb{R}_+\}$. A *triangulation* of $\mathcal{C}$ consists of a finite collection $\Gamma = \{\sigma_1, \ldots, \sigma_t\}$ of simplicial cones satisfying: (i) $\cup\sigma_i = \mathcal{C}$, (ii) if $\sigma \in \Gamma$, then every face of σ is in Γ, and (iii) $\sigma_i \cap \sigma_j$ is a common face of σ_i and σ_j. An element of Γ is called a *face* of Γ.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

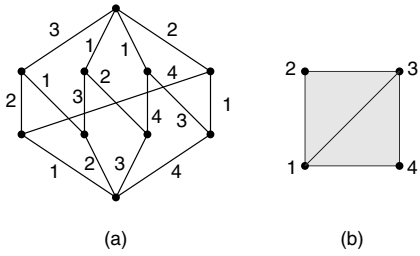

Figure 4.2 An edge-labeled face lattice and corresponding triangulation.

4.5.1 Lemma. *A pointed polyhedral cone $\mathcal{C}$ possesses a triangulation Γ whose 1-faces (= 1-dimensional faces of Γ) are the extreme rays of $\mathcal{C}$.*

Proof. Let L denote the lattice of faces of $\mathcal{C}$, so the face $\{0\}$ is the unique minimal element of L. The extreme rays of $\mathcal{C}$ are the atoms of L. Choose an ordering $\mathcal{R}_1,\ldots,\mathcal{R}_m$ of the extreme rays. Given an edge $e = uv$ of the Hasse diagram of L (so $u \lessdot v$ in L), define $\lambda(e)$ to be the least integer i for which $v = u \vee \mathcal{R}_i$ in L. Let $\mathfrak{m}$ be a maximal chain of L, say $\hat{0} = t_0 \lessdot t_1 \lessdot \cdots \lessdot t_d = \mathcal{C}$, for which $\lambda(t_0,t_1) > \lambda(t_1,t_2) > \cdots > \lambda(t_{d-1},t_d)$. Suppose that $\lambda(t_{i-1},t_i) = j_i$. Let $\Delta_{\mathfrak{m}}$ be the convex hull of the extreme rays $\mathcal{R}_{j_1},\ldots,\mathcal{R}_{j_d}$. We leave it to the reader to check that the $\Delta_{\mathfrak{m}}$'s are the facets of a triangulation Γ whose 1-faces are the extreme rays of $\mathcal{C}$. (Is the similarity to Example 3.14.5 just a coincidence?) □

As an illustration of the preceding proof, consider a 3-dimensional cone $\mathcal{C}$ whose cross-section is a quadrilateral Q. Let $\mathcal{R}_1,\ldots,\mathcal{R}_4$ be the extreme rays of $\mathcal{C}$ in cyclic order. Figure 4.2(a) shows the edge-labeled face lattice of $\mathcal{C}$ (or the face lattice of Q). There are two decreasing chains, labeled 321 and 431. The corresponding triangulation of Q (a cross-section of the triangulation Γ of $\mathcal{C}$) is shown in Figure 4.2(b).

The *boundary* of $\mathcal{C}$, denoted $\partial\mathcal{C}$, is the union of all facets of $\mathcal{C}$. (This definition coincides with the usual topological notion of boundary.) If Γ is a triangulation of $\mathcal{C}$, define the *boundary* $\partial\Gamma = \{\sigma \in \Gamma : \sigma \subseteq \partial\mathcal{C}\}$, and define the *interior* $\Gamma^\circ = \Gamma - \partial\Gamma$.

4.5.2 Lemma. *Let Γ be any triangulation of $\mathcal{C}$. Let $\widehat{\Gamma}$ denote the poset (actually a lattice) of elements of Γ, ordered by inclusion, with a $\hat{1}$ adjoined. Let μ denote the Möbius function of $\widehat{\Gamma}$. Then $\widehat{\Gamma}$ is graded of rank $d+1$, where $d = \dim\mathcal{C}$, and*

$$\mu(\sigma,\tau) = \begin{cases} (-1)^{\dim\tau - \dim\sigma}, & \text{if } \sigma \le \tau < \hat{1}, \\ (-1)^{d-\dim\sigma+1}, & \text{if } \sigma \in \Gamma^\circ \text{ and } \tau = \hat{1}, \\ 0, & \text{if } \sigma \in \partial\Gamma \text{ and } \tau = \hat{1}. \end{cases}$$

Proof. This result is a special case of Proposition 3.8.9. □

Let us now return to the system of equations (4.10). Let $\mathcal{C}$ denote the set of solutions $\boldsymbol{\alpha}$ in nonnegative *real* numbers. Then $\mathcal{C}$ is a pointed convex polyhedral cone. We will always denote $\dim\mathcal{C}$ by the letter d. Since we are assuming that $\operatorname{rank}\Phi = r$ and that E is positive, it follows that $d = m - r$ [why?]. Although we

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

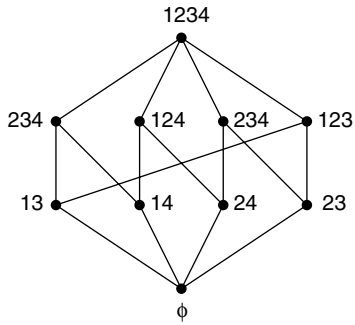

Figure 4.3 A support lattice $L(E)$.

don't require it here, it is natural to describe the faces of $\mathcal{C}$ directly in terms of E. We will simply state the relevant facts without proof. If $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{R}^m$, then define the *support* of $\boldsymbol{\alpha}$, denoted $\operatorname{supp}\boldsymbol{\alpha}$, by $\operatorname{supp}\boldsymbol{\alpha} = \{i : \alpha_i \neq 0\}$. If X is any subset of $\mathbb{R}^m$, then define

$$\operatorname{supp} X = \bigcup_{\boldsymbol{\alpha} \in X} (\operatorname{supp}\boldsymbol{\alpha}).$$

Let $L(\mathcal{C})$ be the lattice of faces of $\mathcal{C}$, and let $L(E) = \{\operatorname{supp}\boldsymbol{\alpha} : \boldsymbol{\alpha} \in E\}$, ordered by inclusion. Define a map $f : L(\mathcal{C}) \to B_m$ (the boolean algebra on $[m]$) by $f(\mathcal{F}) = \operatorname{supp}\mathcal{F}$. Then f is an isomorphism of $L(\mathcal{C})$ onto $L(E)$.

4.5.3 Example. Let $\Phi = [1, 1, -1, -1]$. The poset $L(E)$ is given by Figure 4.3. Thus, $\mathcal{C}$ has four extreme rays and four 2-faces. The four extreme rays are the rays from $(0,0,0,0)$ passing through $(1,0,1,0)$, $(1,0,0,1)$, $(0,1,1,0)$, and $(0,1,0,1)$.

Now let Γ be a triangulation of $\mathcal{C}$ whose extreme rays are the extreme rays of $\mathcal{C}$. Such a triangulation exists by Lemma 4.5.1. If $\sigma \in \Gamma$, then let

$$E_\sigma = \sigma \cap \mathbb{N}^m. \tag{4.15}$$

Then each E_σ is a submonoid of E, and $E = \bigcup_{\sigma \in \Gamma} E_\sigma$. Moreover, if we set

$$\overline{E}_\sigma = \{\boldsymbol{u} \in E_\sigma : \boldsymbol{u} \notin E_\tau \text{ for any } \tau \subset \sigma\}, \tag{4.16}$$

then $\overline{E} = \biguplus_{\sigma \in \Gamma} \overline{E}_\sigma$ (disjoint union). This provides the basic decomposition of E and $\overline{E}$ into "nice" subsets, just as Lemma 3.15.3 did for (P, ω)-partitions.

The "triangulation" $\{E_\sigma : \sigma \in \Gamma\}$ of E and $\{\overline{E}_\sigma : \sigma \in \Gamma^\circ\}$ of $\overline{E}$ yield the following result about generating functions.

4.5.4 Lemma. *The generating functions $E(\boldsymbol{x})$, $\overline{E}(\boldsymbol{x})$ and $E_\sigma(\boldsymbol{x})$, $\overline{E}_\sigma(\boldsymbol{x})$ are related by*

$$E(\boldsymbol{x}) = -\sum_{\sigma \in \Gamma} \mu(\sigma, \hat{1}) E_\sigma(\boldsymbol{x}), \tag{4.17}$$

$$\overline{E}(\boldsymbol{x}) = \sum_{\sigma \in \Gamma^\circ} \overline{E}_\sigma(\boldsymbol{x}). \tag{4.18}$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Proof. Equation (4.17) follows immediately from Möbius inversion. More specifically, set $\overline{E}_{\hat{1}}(\boldsymbol{x}) = 0$ and define

$$H_\sigma(\boldsymbol{x}) = \sum_{\tau \le \sigma} \overline{E}_\tau(\boldsymbol{x}), \quad \sigma \in \widehat{\Gamma}.$$

Clearly,

$$\begin{aligned} H_\sigma(\boldsymbol{x}) &= E_\sigma(\boldsymbol{x}), \quad \sigma \in \Gamma, \\ H_{\hat{1}}(\boldsymbol{x}) &= E(\boldsymbol{x}). \end{aligned} \tag{4.19}$$

By Möbius inversion,

$$0 = \overline{E}_{\hat{1}}(\boldsymbol{x}) = \sum_{\sigma \le \hat{1}} H_\sigma(\boldsymbol{x}) \mu(\sigma, \hat{1}),$$

so equation (4.17) follows from (4.19).

Equation (4.18) follows immediately from the fact that the union $\overline{E} = \bigcup_{\sigma \in \Gamma^\circ} \overline{E}_\sigma$ is disjoint. □

4.5.5 Example. Let E be the monoid of Example 4.5.3. Triangulate $\mathcal{C}$ as shown in Figure 4.4, where $\operatorname{supp}\boldsymbol{a} = \{1,3\}$, $\operatorname{supp}\boldsymbol{b} = \{1,4\}$, $\operatorname{supp}\boldsymbol{c} = \{2,4\}$, $\operatorname{supp}\boldsymbol{d} = \{2,3\}$. Then the poset $\widehat{\Gamma}$ is given by Figure 4.5. Note also that $\Gamma^\circ = \{bd, abd, bcd\}$. Lemma 4.5.4 states that

$$\begin{aligned} E(\boldsymbol{x}) &= E_{abd}(\boldsymbol{x}) + E_{bcd}(\boldsymbol{x}) - E_{bd}\boldsymbol{x} \\ \overline{E}(\boldsymbol{x}) &= \overline{E}_{abd}(\boldsymbol{x}) + \overline{E}_{bcd}(\boldsymbol{x}) + \overline{E}_{bd}(\boldsymbol{x}). \end{aligned} \tag{4.20}$$

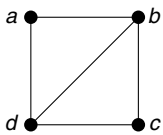

Figure 4.4 Triangulation of a cross-section of a cone $\mathcal{C}$.

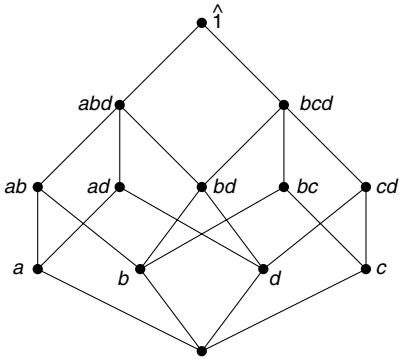

Figure 4.5 Face poset of the triangulation of Figure 4.4.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Our next step is the evaluation of the generating functions $E_\sigma(\boldsymbol{x})$ and $\overline{E}_\sigma(\boldsymbol{x})$ appearing in equations (4.17) and (4.18). Let us call a submonoid F of $\mathbb{N}^m$ (or even $\mathbb{Z}^m$) *simplicial* if there exist linearly independent vectors $\boldsymbol{\alpha_1},\ldots,\boldsymbol{\alpha_t} \in F$ (called *quasigenerators* of F) such that

$$F = \{\boldsymbol{\gamma} \in \mathbb{N}^m : n\boldsymbol{\gamma} = a_1\boldsymbol{\alpha_1} + \cdots + a_t\boldsymbol{\alpha_t} \text{ for some } n \in \mathbb{P} \text{ and } a_i \in \mathbb{N}\}.$$

The quasigenerators $\boldsymbol{\alpha_1},\ldots,\boldsymbol{\alpha_t}$ are not quite unique. If $\boldsymbol{\alpha'_1},\ldots,\boldsymbol{\alpha'_s}$ is another set of quasigenerators, then $s = t$ and with suitable choice of subscripts $\boldsymbol{\alpha'_1} = q_i\boldsymbol{\alpha'_i}$ where $q_i \in \mathbb{Q}$, $q_i > 0$. Define the *interior* $\overline{F}$ of F by

$$\overline{F} = \{\boldsymbol{\alpha} \in \mathbb{N}^m : n\boldsymbol{\alpha} = a_1\boldsymbol{\alpha_1} + \cdots + a_t\boldsymbol{\alpha_t} \text{ for some } n \in \mathbb{P} \text{ and } a_i \in \mathbb{P}\}. \tag{4.21}$$

Note that $\overline{F}$ depends only on F, not on $\boldsymbol{\alpha_1},\ldots,\boldsymbol{\alpha_t}$.

4.5.6 Lemma. *The submonoids E_σ of E defined by equation (4.15) are simplicial. If $\mathcal{R}_1,\ldots,\mathcal{R}_t$ are the extreme rays of σ, then we can pick as quasigenerators of E_σ any nonzero integer vectors in $\mathcal{R}_1,\ldots,\mathcal{R}_t$ (one vector from each $\mathcal{R}_i$). Moreover, the interior of E_σ, as defined by equation (4.21), coincides with the definition* (4.16) *of $\overline{E}_\sigma$.*

Proof. This is an easy consequence of the fact that σ is a simplicial cone. The details are left to the reader. □

If $F \subseteq \mathbb{N}^m$ is a simplicial monoid with quasigenerators $Q = \{\boldsymbol{\alpha_1},\ldots,\boldsymbol{\alpha_t}\}$, then define two subsets D_F and $\overline{D}_F$ (which depend on the choice of Q) as follows:

$$D_F = \{\boldsymbol{\gamma} \in F : \boldsymbol{\gamma} = a_1\boldsymbol{\alpha_1} + \cdots + a_t\boldsymbol{\alpha_t},\ 0 \le a_i < 1\}, \tag{4.22}$$

$$\overline{D}_F = \{\boldsymbol{\gamma} \in F : \boldsymbol{\gamma} = a_1\boldsymbol{\alpha_1} + \cdots + a_t\boldsymbol{\alpha_t},\ 0 < a_i \le 1\}. \tag{4.23}$$

Note that D_F and $\overline{D}_F$ are finite sets, since they are contained in the intersection of the discrete set F (or $\mathbb{N}^m$) with the bounded set of all vectors $a_1\boldsymbol{\alpha_1} + \cdots + a_t\boldsymbol{\alpha_t} \in \mathbb{R}^m$ with $0 \le a_i \le 1$.

4.5.7 Lemma. *Let $F \subseteq \mathbb{N}^m$ be a simplicial monoid with quasigenerators $\boldsymbol{\alpha_1},\ldots,\boldsymbol{\alpha_t}$.*

i. Every element $\boldsymbol{\gamma} \in F$ can be written uniquely in the form

$$\boldsymbol{\gamma} = \boldsymbol{\beta} + a_1\boldsymbol{\alpha_1} + \cdots + a_t\boldsymbol{\alpha_t},$$

where $\boldsymbol{\beta} \in D_F$ and $a_i \in \mathbb{N}$. Conversely, any such vector belongs to F.

ii. Every element $\boldsymbol{\gamma} \in \overline{F}$ can be written uniquely in the form

$$\boldsymbol{\gamma} = \bar{\boldsymbol{\beta}} + a_1\boldsymbol{\alpha_1} + \cdots + a_t\boldsymbol{\alpha_t},$$

where $\bar{\boldsymbol{\beta}} \in \overline{D}_F$ and $a_i \in \mathbb{N}$. Conversely, any such vector belongs to $\overline{F}$.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Proof. i. Let $\boldsymbol{\gamma} \in F$, and write (uniquely) $\boldsymbol{\gamma} = b_1\boldsymbol{\alpha_1} + \cdots + b_t\boldsymbol{\alpha_t}$, $b_i \in \mathbb{Q}$. Let $a_i = \lfloor b_i \rfloor$, and let $\boldsymbol{\beta} = \boldsymbol{\gamma} - a_1\boldsymbol{\alpha_1} - \cdots - a_t\boldsymbol{\alpha_t}$. Then $\boldsymbol{\beta} \in F$, and since $0 \le b_i - a_i < 1$, in fact $\boldsymbol{\beta} \in D_F$. If $\boldsymbol{\gamma} = \boldsymbol{\beta}' + a_1'\boldsymbol{\alpha_1} + \cdots + a_t'\boldsymbol{\alpha_t}$ were another such representation, then $\mathbf{0} = \boldsymbol{\beta} - \boldsymbol{\beta}' = (a_1 - a_1')\boldsymbol{\alpha_1} + \cdots + (a_t - a_t')\boldsymbol{\alpha_t}$. Each $a_i - a_i' \in \mathbb{Z}$, whereas if $\boldsymbol{\beta} - \boldsymbol{\beta}' = c_1\boldsymbol{\alpha_1} + \cdots + c_t\boldsymbol{\alpha_t}$, then $-1 < c_i < 1$. Hence $c_i = 0$ and the two representations agree. The converse statement is clear.

ii. The proof is analogous to (i). Instead of $a_i = \lfloor b_i \rfloor$ we take $a_i = \lceil b_i - 1 \rceil$, and so on.

□

4.5.8 Corollary. *The generating functions*

$$F(\boldsymbol{x}) = \sum_{\boldsymbol{\alpha} \in F} \boldsymbol{x}^{\boldsymbol{\alpha}}, \quad \overline{F}(\boldsymbol{x}) = \sum_{\boldsymbol{\alpha} \in \overline{F}} \boldsymbol{x}^{\boldsymbol{\alpha}}$$

are given by

$$F(\boldsymbol{x}) = \left(\sum_{\boldsymbol{\beta} \in D_F} \boldsymbol{x}^{\boldsymbol{\beta}} \right) \prod_{i=1}^{t} \left(1 - \boldsymbol{x}^{\boldsymbol{\alpha_i}}\right)^{-1}, \tag{4.24}$$

$$\overline{F}(\boldsymbol{x}) = \left(\sum_{\boldsymbol{\beta} \in \overline{D}_F} \boldsymbol{x}^{\boldsymbol{\beta}} \right) \prod_{i=1}^{t} \left(1 - \boldsymbol{x}^{\boldsymbol{\alpha_i}}\right)^{-1}. \tag{4.25}$$

Proof. Immediate from Lemma 4.5.7. □

NOTE. For the algebraic-minded, we mention the algebraic significance of the sets D_F and $\overline{D}_F$. Let G be the subgroup of $\mathbb{Z}^m$ generated by F, and let H be the subgroup of G generated by the quasigenerators $\boldsymbol{\alpha_1}, \ldots, \boldsymbol{\alpha_t}$. Then each of D_F and $\overline{D}_F$ is a set of coset representatives for H in G. Moreover, D_F (respectively, $\overline{D}_F$) consists of those coset representatives that belong to F (respectively, $\overline{F}$) and are closest to the origin. It follows from general facts about finitely generated abelian groups that the index $[G : H]$ (i.e., the cardinalities of D_F and $\overline{D}_F$) is equal to the greatest common divisor of the determinants of the $t \times t$ submatrices of the matrix whose rows are $\boldsymbol{\alpha_1}, \ldots, \boldsymbol{\alpha_t}$.

4.5.9 Example. Let $\boldsymbol{\alpha_1} = (1,3,0)$ and $\boldsymbol{\alpha_2} = (1,0,3)$. The greatest common divisor of the determinants

$$\begin{vmatrix} 1 & 3 \\ 1 & 0 \end{vmatrix}, \begin{vmatrix} 1 & 0 \\ 1 & 3 \end{vmatrix}, \begin{vmatrix} 3 & 0 \\ 0 & 3 \end{vmatrix}$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

is $3 = \#D_F = \#\overline{D}_F$. Indeed, $D_F = \{(0,0,0),(1,1,2),\ (1,2,1)\}$ and $\overline{D}_F = \{(1,1,2),(1,2,1),\ (2,3,3)\}$. Hence,

$$F(\boldsymbol{x}) = \frac{1 + x_1x_2x_3^2 + x_1x_2^2x_3}{(1-x_1x_2^3)(1-x_1x_3^3)},$$

$$\overline{F}(\boldsymbol{x}) = \frac{x_1x_2x_3^2 + x_1x_2^2x_3 + x_1^2x_2^3x_3^3}{(1-x_1x_2^3)(1-x_1x_3^3)}.$$

We mentioned earlier that if the simplicial monoid $F \subseteq \mathbb{N}^m$ has quasigenerators $\boldsymbol{\alpha_1},\dots,\boldsymbol{\alpha_t}$, then any nonzero rational multiples of $\boldsymbol{\alpha_1},\dots,\boldsymbol{\alpha_t}$ (provided they lie in $\mathbb{N}^m$) can be taken as the quasigenerators. Thus there is a unique set $\boldsymbol{\beta_1},\dots,\boldsymbol{\beta_t}$ of quasigenerators such that any other set has the form $a_1\boldsymbol{\beta_1},\dots,a_t\boldsymbol{\beta_t}$, where $a_i \in \mathbb{P}$. We call $\boldsymbol{\beta_1},\dots,\boldsymbol{\beta_t}$ the *completely fundamental* elements of F and write $\mathrm{CF}(F) = \{\boldsymbol{\beta_1},\dots,\boldsymbol{\beta_t}\}$. Now suppose that E is the monoid of all $\mathbb{N}$-solutions to equation (4.10). Define $\boldsymbol{\beta} \in E$ to be *completely fundamental* if for all $n \in \mathbb{P}$ and $\boldsymbol{\alpha},\boldsymbol{\alpha}' \in E$ for which $n\boldsymbol{\beta} = \boldsymbol{\alpha} + \boldsymbol{\alpha}'$, we have $\boldsymbol{\alpha} = i\boldsymbol{\beta}$ and $\boldsymbol{\alpha}' = (n-i)\boldsymbol{\beta}$ for some $i \in \mathbb{P}$, $0 \le i \le n$. Denote the set of completely fundamental elements of E by $\mathrm{CF}(E)$.

4.5.10 Proposition. *Let Γ be a triangulation of $\mathcal{C}$ whose extreme rays coincide with those of $\mathcal{C}$, and let $E = \bigcup_{\sigma\in\Gamma} E_\sigma$ be the corresponding decomposition of E into simplicial monoids E_σ. Then the following sets are identical:*

i. $CF(E)$,
ii. $\bigcup_{\sigma\in\Gamma} \mathrm{CF}(E_\sigma)$,
iii. $\{\boldsymbol{\beta} \in E : \boldsymbol{\beta}$ lies on an extreme ray of $\mathcal{C}$, and $\boldsymbol{\beta} \neq n\boldsymbol{\beta}'$ for some $n \ge 1$, $\boldsymbol{\beta}' \in E\}$,
iv. The nonzero elements $\boldsymbol{\beta}$ of E of minimal support that are not of the form $n\boldsymbol{\beta}'$ for some $n > 1$, $\boldsymbol{\beta}' \in E$.

Proof. Suppose that $0 \neq \boldsymbol{\beta} \in E$ and $\operatorname{supp}\boldsymbol{\beta}$ is not minimal. Then some $\alpha \in E$ satisfies $\operatorname{supp}\boldsymbol{\alpha} \subset \operatorname{supp}\boldsymbol{\beta}$. Hence for $n \in \mathbb{P}$ sufficiently large, $n\boldsymbol{\beta} - \boldsymbol{\alpha} \ge \mathbf{0}$ and so $n\boldsymbol{\beta} - \boldsymbol{\alpha} \in E$. Setting $\boldsymbol{\alpha}' = n\boldsymbol{\beta} - \boldsymbol{\alpha}$, we have $n\boldsymbol{\beta} = \boldsymbol{\alpha} + \boldsymbol{\alpha}'$ but $\boldsymbol{\alpha} \neq i\boldsymbol{\beta}$ for any $i \in \mathbb{N}$. Thus, $\boldsymbol{\beta} \notin \mathrm{CF}(E)$.

Suppose that $\boldsymbol{\beta} \in E$ belongs to set (iv), and let $n\boldsymbol{\beta} = \boldsymbol{\alpha} + \boldsymbol{\alpha}'$, where $n \in \mathbb{P}$ and $\boldsymbol{\alpha},\boldsymbol{\alpha}' \in E$. Since $\operatorname{supp}\boldsymbol{\beta}$ is minimal, either $\boldsymbol{\alpha} = 0$ or $\operatorname{supp}\boldsymbol{\alpha} = \operatorname{supp}\boldsymbol{\beta}$. In the latter case, let p/q be the largest rational number where $q \in \mathbb{P}$, for which $\boldsymbol{\beta} - (p/q)\boldsymbol{\alpha} \ge \mathbf{0}$. Then $q\boldsymbol{\beta} - p\boldsymbol{\alpha} \in E$ and $\operatorname{supp}(q\boldsymbol{\beta} - p\boldsymbol{\alpha}) \subset \operatorname{supp}\boldsymbol{\beta}$. By the minimality of $\operatorname{supp}\boldsymbol{\beta}$, we conclude $q\boldsymbol{\beta} = p\boldsymbol{\alpha}$. Since $\boldsymbol{\beta} \neq \boldsymbol{\beta}'$ for $n > 1$ and $\boldsymbol{\beta}' \in E$, it follows that $p = 1$ and therefore $\boldsymbol{\beta} \in \mathrm{CF}(E)$. Thus, the sets (i) and (iv) coincide.

Now let $\mathcal{R}$ be an extreme ray of $\mathcal{C}$, and suppose that $\boldsymbol{\alpha} \in \mathcal{R}$, $\boldsymbol{\alpha} = \boldsymbol{\alpha}_1 + \boldsymbol{\alpha}_2$, $\boldsymbol{\alpha}_i \in \mathcal{C}$. By definition of extreme ray, it follows that $\boldsymbol{\alpha}_1 = a\boldsymbol{\alpha}_2$, $0 \le a \le 1$. (Otherwise, $\boldsymbol{\alpha}_1$ and $\boldsymbol{\alpha}_2$ lie on different sides of the hyperplane $\mathcal{H}$ supporting $\mathcal{R}$.) From this observation, it is easy to deduce that the sets (i) and (iii) coincide.

Since the extreme rays of Γ and $\mathcal{C}$ coincide, an element $\boldsymbol{\beta}$ of $\mathrm{CF}(E_\sigma)$ lies on some extreme ray $\mathcal{R}$ of $\mathcal{C}$ and hence in set (iii). Conversely, if $\sigma \in \Gamma$ contains the

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

extreme ray $\mathcal{R}$ of $\mathcal{C}$ and if $\mathcal{H}$ supports $\mathcal{R}$ in $\mathcal{C}$, then $\mathcal{H}$ supports $\mathcal{R}$ in σ. Thus, $\mathcal{R}$ is an extreme ray of σ. Since $E = \bigcup_{\sigma\in\Gamma} E_\sigma$, it follows that set (iii) is contained in set (ii). □

We finally come to the first of the two main theorems of this section.

4.5.11 Theorem. *The generating functions $E(\boldsymbol{x})$ and $\overline{E}(\boldsymbol{x})$ represent rational functions of $\boldsymbol{x} = (x_1,\ldots,x_m)$. When written in lowest terms, both these rational functions have denominator*

$$D(\boldsymbol{x}) = \prod_{\boldsymbol{\beta}\in \mathrm{CF}(E)} \left(1 - x^{\boldsymbol{\beta}}\right).$$

Proof. Let Γ be a triangulation of $\mathcal{C}$ whose extreme rays coincide with those of $\mathcal{C}$ (existence guaranteed by Lemma 4.5.1). Let $E = \bigcup_{\sigma\in\Gamma} E_\sigma$ be the corresponding decomposition of E. Since $\mathrm{CF}(E_\sigma)$ is a set of quasigenerators for the simplicial monoid E_σ, it follows from Corollary 4.5.8 that $E_\sigma(\boldsymbol{x})$ and $\overline{E}_\sigma(\boldsymbol{x})$ can be written as rational functions with denominator

$$D(\boldsymbol{x}) = \prod_{\boldsymbol{\beta}\in \mathrm{CF}(E)} \left(1 - \boldsymbol{x}^{\boldsymbol{\beta}}\right).$$

By Proposition 4.5.10, $\mathrm{CF}(E_\sigma) \subseteq \mathrm{CF}(E)$. Hence by Lemma 4.5.4, we can put the expressions (4.17) and (4.18) for $E(\boldsymbol{x})$ and $\overline{E}(\boldsymbol{x})$ over the common denominator $D(\boldsymbol{x})$.

It remains to prove that $D(\boldsymbol{x})$ is the *least* possible denominator. We will consider only $E(\boldsymbol{x})$, the proof being essentially the same (and also following from Theorem 4.5.14) for $\overline{E}(\boldsymbol{x})$. Write $E(\boldsymbol{x}) = N(\boldsymbol{x})/D(\boldsymbol{x})$. Suppose that this fraction is not in lowest terms. Then some factor $T(\boldsymbol{x})$ divides both $N(\boldsymbol{x})$ and $D(\boldsymbol{x})$. By the unique factorization theorem for the polynomial ring $\mathbb{C}[x_1,\ldots,x_m]$, we may assume that $T(\boldsymbol{x})$ divides $1 - \boldsymbol{x}^{\boldsymbol{\gamma}}$ for some $\boldsymbol{\gamma} \in \mathrm{CF}(E)$. Since $\boldsymbol{\gamma} \neq n\boldsymbol{\gamma}'$ for any integer $n > 1$ and any $\boldsymbol{\gamma}' \in \mathbb{N}^m$, the polynomial $1 - \boldsymbol{x}^{\boldsymbol{\gamma}}$ is irreducible. Hence, we may assume that $T(\boldsymbol{x}) = 1 - \boldsymbol{x}^{\boldsymbol{\gamma}}$. Thus, we can write

$$F(\boldsymbol{x}) = \frac{N'(\boldsymbol{x})}{\displaystyle\prod_{\substack{\boldsymbol{\beta}\in \mathrm{CF}(E)\\ \boldsymbol{\beta}\neq\boldsymbol{\gamma}}} \left(1 - \boldsymbol{x}^{\boldsymbol{\beta}}\right)}, \tag{4.26}$$

where $N'(\boldsymbol{x}) \in \mathbb{C}[x_1,\ldots,x_m]$. Since, for any $n \in \mathbb{P}$ and $a_{\boldsymbol{\beta}} \in \mathbb{N}$ $(\boldsymbol{\beta} \neq \boldsymbol{\gamma})$, we have

$$n\boldsymbol{\gamma} \neq \sum_{\substack{\boldsymbol{\beta}\in \mathrm{CF}(E)\\ \boldsymbol{\beta}\neq\boldsymbol{\gamma}}} a_{\boldsymbol{\beta}} \cdot \boldsymbol{\beta},$$

it follows that only finitely many terms of the form $\boldsymbol{x}^{n\boldsymbol{\gamma}}$ can appear in the expansion of the right-hand side of equation (4.26). This contradicts the fact that each $n\boldsymbol{\gamma} \in E$, and completes the proof. □

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Our next goal is the reciprocity theorem that connects $E(\boldsymbol{x})$ and $\overline{E}(\boldsymbol{x})$. As a preliminary lemma we need to prove a reciprocity theorem for simplicial monoids.

4.5.12 Lemma. *Let $F \subseteq \mathbb{N}^m$ be a simplicial monoid with quasigenerators $\boldsymbol{\alpha_1},\dots,\boldsymbol{\alpha_t}$, and suppose that $D_F = \{\boldsymbol{\beta_1},\dots,\boldsymbol{\beta_s}\}$. Then*

$$\overline{D}_F = \{\boldsymbol{\alpha}-\boldsymbol{\beta_1},\dots,\boldsymbol{\alpha}-\boldsymbol{\beta_s}\},$$

where $\boldsymbol{\alpha} = \boldsymbol{\alpha_1}+\cdots+\boldsymbol{\alpha_t}$.

Proof. Let $\boldsymbol{\gamma} = a_1\boldsymbol{\alpha_1}+\cdots+a_t\boldsymbol{\alpha_t} \in F$. Since $0 \le a_i < 1$ if and only if $0 < 1-a_i \le 1$, the proof follows from the definitions (4.22) and (4.23) of D_F and $\overline{D}_F$. □

Recall that if $R(\boldsymbol{x}) = R(x_1,\dots,x_m)$ is a rational function, then $R(1/\boldsymbol{x})$ denotes the rational function $R(1/x_1,\dots,1/x_m)$.

4.5.13 Lemma. *Let $F \subseteq \mathbb{N}^m$ be a simplicial monoid of dimension t. Then*

$$\overline{F}(\boldsymbol{x}) = (-1)^t F(1/\boldsymbol{x}).$$

Proof. By equation (4.24), we have

$$\begin{aligned} F(1/\boldsymbol{x}) &= \left(\sum_{\boldsymbol{\beta}\in D_S} \boldsymbol{x}^{-\boldsymbol{\beta}}\right)\prod_{i=1}^{t}\left(1-\boldsymbol{x}^{-\boldsymbol{\alpha_i}}\right)^{-1} \\ &= (-1)^t\left(\sum_{\boldsymbol{\beta}\in D_S} \boldsymbol{x}^{\boldsymbol{\alpha}-\boldsymbol{\beta}}\right)\prod_{i=1}^{t}\left(1-\boldsymbol{x}^{\boldsymbol{\alpha_i}}\right)^{-1}, \end{aligned}$$

where $\boldsymbol{\alpha}$ is as in Lemma 4.5.12. By Lemma 4.5.12,

$$\sum_{\boldsymbol{\beta}\in D_S} \boldsymbol{x}^{\boldsymbol{\alpha}-\boldsymbol{\beta}} = \sum_{\boldsymbol{\beta}\in \overline{D}_S} \boldsymbol{x}^{\boldsymbol{\beta}}.$$

The proof follows from equation (4.25). □

We now have all the necessary tools to deduce the second main theorem of this section.

4.5.14 Theorem (the reciprocity theorem for linear homogeneous diophantine equations). *Assume (as always) that the monoid E of $\mathbb{N}$-solutions to equation (4.10) is positive, and let $d = \dim \mathcal{C}$. Then*

$$\overline{E}(\boldsymbol{x}) = (-1)^d E(1/\boldsymbol{x}).$$

Proof. By Lemma 4.5.2 and equation (4.17), we have

$$E(1/\boldsymbol{x}) = -\sum_{\sigma\in\Gamma^\circ} (-1)^{d-\dim\sigma+1} E_\sigma(1/\boldsymbol{x}).$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Thus by Lemma 4.5.13,

$$E(1/\boldsymbol{x}) = (-1)^d \sum_{\sigma \in \Gamma^\circ} \overline{E}_\sigma(\boldsymbol{x}).$$

Comparing with equation (4.18) completes the proof. □

We now give some examples and applications of the preceding theory. First, we dispose of the equation $\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4 = 0$ discussed in Examples 4.5.3 and 4.5.5.

4.5.15 Example. Let $E \subset \mathbb{N}^4$ be the monoid of $\mathbb{N}$-solutions to $\alpha_1 + \alpha_2 - \alpha_3 - \alpha_4 = 0$. According to equation (4.20), we need to compute $E_{abd}(\boldsymbol{x})$, $E_{bcd}(\boldsymbol{x})$, and $E_{bd}(\boldsymbol{x})$. Now $\mathrm{CF}(E) = \{\boldsymbol{\beta_1}, \boldsymbol{\beta_2}, \boldsymbol{\beta_3}, \boldsymbol{\beta_4}\}$, where $\boldsymbol{\beta_1} = (1,0,1,0)$, $\boldsymbol{\beta_2} = (1,0,0,1)$, $\boldsymbol{\beta_3} = (0,1,0,1)$, $\boldsymbol{\beta_4} = (0,1,1,0)$. A simple computation reveals that $D_{abd} = D_{bcd} = D_{bd} = \{(0,0,0,0\}$ (the reason for this being that each of the sets $\{\boldsymbol{\beta_1}, \boldsymbol{\beta_2}, \boldsymbol{\beta_4}\}$, $\{\boldsymbol{\beta_2}, \boldsymbol{\beta_3}, \boldsymbol{\beta_4}\}$, and $\{\boldsymbol{\beta_2}, \boldsymbol{\beta_4}\}$ can be extended to a set of free generators of the group $\mathbb{Z}^4$). Hence by Lemma 4.5.12, we have $\overline{D}_{abd} = \{\boldsymbol{\beta_1} + \boldsymbol{\beta_2} + \boldsymbol{\beta_4}\} = \{(2,1,2,1\}$, $\overline{D}_{bcd} = \{\boldsymbol{\beta_2} + \boldsymbol{\beta_3} + \boldsymbol{\beta_4}\} = \{(1,2,1,2)\}$, $\overline{D}_{bd} = \{\boldsymbol{\beta_2} + \boldsymbol{\beta_4}\} = \{(1,1,1,1)\}$. There follows

$$\begin{aligned} E(\boldsymbol{x}) &= \frac{1}{(1-x_1x_3)(1-x_1x_4)(1-x_2x_3)} \\ &\quad + \frac{1}{(1-x_1x_4)(1-x_2x_4)(1-x_2x_3)} \\ &\quad - \frac{1}{(1-x_1x_4)(1-x_2x_3)} \\ &= \frac{1-x_1x_2x_3x_4}{(1-x_1x_3)(1-x_1x_4)(1-x_2x_3)(1-x_2x_4)}, \end{aligned}$$

$$\begin{aligned} \overline{E}(\boldsymbol{x}) &= \frac{x_1^2x_2x_3^2x_4}{(1-x_1x_3)(1-x_1x_4)(1-x_2x_3)} \\ &\quad + \frac{x_1x_2^2x_3x_4^2}{(1-x_1x_4)(1-x_2x_4)(1-x_2x_3)} \\ &\quad + \frac{x_1x_2x_3x_4}{(1-x_1x_4)(1-x_2x_3)} \\ &= \frac{x_1x_2x_3x_4(1-x_1x_2x_3x_4)}{(1-x_1x_3)(1-x_1x_4)(1-x_2x_3)(1-x_2x_4)}. \end{aligned}$$

Note that indeed $\overline{E}(\boldsymbol{x}) = -E(1/\boldsymbol{x})$. Note also that $\overline{E}(\boldsymbol{x}) = x_1x_2x_3x_4E(\boldsymbol{x})$. This is because $\boldsymbol{\alpha} \in E$ if and only if $\boldsymbol{\alpha} + (1,1,1,1) \in \overline{E}$. More generally, we have the following result.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

4.5.16 Corollary. *Let E be the monoid of $\mathbb{N}$-solutions to equation (4.10), and let $\boldsymbol{\gamma} \in \mathbb{Z}^m$. The following two conditions are equivalent.*

i. $E(1/\boldsymbol{x}) = (-1)^d \boldsymbol{x}^{\boldsymbol{\gamma}} E(\boldsymbol{x})$,
ii. $\overline{E} = \boldsymbol{\gamma} + E$ *(i.e.,* $\boldsymbol{\alpha} \in E$ *if and only if* $\boldsymbol{\alpha} + \boldsymbol{\gamma} \in \overline{E}$*).*

Proof. Condition (ii) is clearly equivalent to $\overline{E}(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{\gamma}} E(\boldsymbol{x})$. The proof follows from Theorem 4.5.14. □

NOTE. There is another approach toward computing the generating function $E(\boldsymbol{x})$ of Example 4.5.15. Namely, the monoid E is generated by the vectors $\boldsymbol{\beta_1}$, $\boldsymbol{\beta_2}$, $\boldsymbol{\beta_3}$, $\boldsymbol{\beta_4}$, subject to the single relation $\boldsymbol{\beta_1} + \boldsymbol{\beta_3} = \boldsymbol{\beta_2} + \boldsymbol{\beta_4}$. Hence, the number of representations of a vector δ in the form $\sum a_i \boldsymbol{\beta_i}$, $a_i \in \mathbb{N}$, is one more than the number of representations of $\delta - (1,1,1,1)$ in this form. It follows that

$$E(\boldsymbol{x}) = \frac{1 - x_1x_2x_3x_4}{(1-x_1x_3)(1-x_1x_4)(1-x_2x_3)(1-x_2x_4)}.$$

The relation $\boldsymbol{\beta_1} + \boldsymbol{\beta_3} = \boldsymbol{\beta_2} + \boldsymbol{\beta_4}$ is called a *syzygy of the first kind*. In general, there can be relations among the relations, called *syzygies of the second kind*, and so on. In order to develop a "syzygetic proof" of Theorem 4.5.11, techniques from commutative algebra are necessary but which will not be pursued here.

Only in the simplest cases is it practical to compute $E(\boldsymbol{x})$ by brute force, such as was done in Example 4.5.15. However, even if we can't compute $E(\boldsymbol{x})$ explicitly, we can still draw some interesting conclusions, as we now discuss. First, we need a preliminary result concerning specializations of the generating function $E(\boldsymbol{x})$.

4.5.17 Lemma. *Let E be the monoid of $\mathbb{N}$-solutions to equation (4.10). Let $a_1, \ldots, a_m \in \mathbb{Z}$ such that for each $r \in \mathbb{N}$, the number $g(r)$ of solutions $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in E$ satisfying $L(\boldsymbol{\alpha}) := a_1\alpha_1 + \cdots + a_m\alpha_m = r$ is finite. Assume that $g(r) > 0$ for at least one $r > 0$. Let $G(\lambda) = \sum_{r \geq 0} g(r)\lambda^r$. Then*

i. $G(\lambda) = E(\lambda^{a_1}, \ldots, \lambda^{a_m}) \in \mathbb{C}(\lambda)$*, where* $E(\boldsymbol{x}) = \sum_{\boldsymbol{\gamma} \in E} \boldsymbol{x}^{\boldsymbol{\gamma}}$ *as usual.*
ii. $\deg G(\lambda) < 0$.

Proof. i. We first claim that $g(s) = 0$ for all $s < 0$. Let $\boldsymbol{\alpha} \in E$ satisfy $L(\boldsymbol{\alpha}) = r > 0$, and suppose that there exists $\boldsymbol{\beta} \in E$ with $L(\boldsymbol{\beta}) = s < 0$. Then for all $t \in \mathbb{N}$, the vectors $-ts\boldsymbol{\alpha} + tr\boldsymbol{\beta}$ are distinct elements of E, contradicting $g(0) < \infty$. Hence, the claim is proved, from which it is immediate that $G(\lambda) = E(\lambda^{a_1}, \ldots, \lambda^{a_m})$. Since $E(\boldsymbol{x}) \in \mathbb{C}(\boldsymbol{x})$, we have $G(\lambda) \in \mathbb{C}(\lambda)$.

ii. By equation (4.17) and Lemma 4.5.2, it suffices to show that $\deg E_\sigma(\lambda^{a_1}, \ldots, \lambda^{a_m}) < 0$ for all $\sigma \in \Gamma^\circ$. Consider the expression (4.24) for $E_\sigma(\boldsymbol{x})$ (where $F = E_\sigma$), and let $\boldsymbol{\beta} \in D_S$. Thus by equation (4.22), $\boldsymbol{\beta} = b_1\boldsymbol{\alpha_1} + \cdots + b_t\boldsymbol{\alpha_t}$, $0 \leq b_i < 1$. Hence, $L(\boldsymbol{\beta}) \leq L(\boldsymbol{\alpha_1}) + \cdots + L(\boldsymbol{\alpha_t})$ with equality if and only if $t = 0$ (so $\sigma = \{\boldsymbol{0}\}$). But $\{\boldsymbol{0}\} \notin \Gamma^\circ$, so $L(\boldsymbol{\beta}) < L(\boldsymbol{\alpha_1}) + \cdots + L(\boldsymbol{\alpha_t})$. Since the

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

monomial $\boldsymbol{x}^{\boldsymbol{\beta}}$ evaluated at $\boldsymbol{x} = (x^{a_1}, \ldots, x^{a_m})$ has degree $L(\boldsymbol{\beta})$, it follows that each term of the numerator of $E_\sigma(\lambda^{a_1}, \ldots, \lambda^{a_m})$ has degree less than the degree $L(\boldsymbol{\alpha_1}) + \cdots + L(\boldsymbol{\alpha_t})$ of the denominator.

□

Note that in the preceding proof we did not need Lemma 4.5.2 to show that $G(\lambda) \leq 0$. We only required this result to show that the constant term $G(0)$ of $G(\lambda)$ was "correct" (in the sense of Proposition 4.2.2).

4.6 Applications

4.6.1 Magic Squares

We now come to our first real application of the preceding theory. Let $H_n(r)$ be the number of $n \times n$ $\mathbb{N}$-matrices such that every row and column sums to r. We call such matrices *magic squares*, though our definition is far less stringent than the classical one. For instance, $H_1(r) = 1$ (corresponding the the 1×1 matrix $[r]$), $H_2(r) = r + 1$ (corresponding to $\begin{bmatrix} i & r-i \\ r-i & i \end{bmatrix}$, $0 \leq i \leq r$), and $H_n(1) = n!$ (corresponding to all $n \times n$ permutation matrices). Introduce n^2 variables α_{ij} for $(i, j) \in [n] \times [n]$. Then an $n \times n$ $\mathbb{N}$-matrix with every row and column sum r corresponds to an $\mathbb{N}$-solution to the system of equations

$$\sum_{i=1}^{n} \alpha_{ij} = \sum_{i=1}^{n} \alpha_{ki}, \quad 1 \leq j \leq n, \quad 1 \leq k \leq n, \tag{4.27}$$

with $\alpha_{11} + \alpha_{12} + \cdots + \alpha_{1n} = r$. It follows from Lemma 4.5.17(i) that if E denotes the monoid of $\mathbb{N}$-solutions to equation (4.27), then

$$E(x_{ij})\Big|_{\substack{x_{1j}=\lambda \\ x_{ij}=1, i>1}} = \sum_{r \geq 0} H_n(r)\lambda^r. \tag{4.28}$$

In particular, $H_n(r)$ is a quasipolynomial in r. To proceed further, we must find the set $\mathrm{CF}(E)$.

4.6.1 Lemma. *The set* $\mathrm{CF}(E)$ *consists of the* $n!$ $n \times n$ *permutation matrices.*

Proof. Let $\boldsymbol{\pi}$ be a permutation matrix, and suppose that $k\boldsymbol{\pi} = \boldsymbol{\alpha_1} + \boldsymbol{\alpha_2}$, where $\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2} \in E$. Then $\boldsymbol{\alpha_1}$ and $\boldsymbol{\alpha_2}$ have at most one nonzero entry in every row and column (since $\operatorname{supp} \boldsymbol{\alpha_i} \subseteq \operatorname{supp} \boldsymbol{\pi}$) and hence are multiples of $\boldsymbol{\pi}$. Thus, $\boldsymbol{\pi} \in \mathrm{CF}(E)$.

Conversely, suppose that $\boldsymbol{\pi} = (\pi_{ij}) \in E$ is not a permutation matrix. If $\boldsymbol{\pi}$ is a proper multiple of a permutation matrix, then clearly $\boldsymbol{\pi} \notin \mathrm{CF}(E)$. Hence, we may assume that some row, say i_1, has at least two nonzero entries $\pi_{i_1 j_1}$ and $\pi_{i_1, j_1'}$. Since column j_1 has the same sum as row i_1, there is another nonzero entry in column j_1, say $\pi_{i_2 j_1}$. Since row i_2 has the same sum as column j_1, there is another nonzero entry in row i_2, say $\pi_{i_2 j_2}$. If we continue in this manner, we

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

eventually must reach some entry twice. Thus, we have a sequence of at least four nonzero entries indexed by (i_r, j_r), (i_{r+1}, j_r), $(i_{r+1}, j_{r+1}), \ldots, (i_s, j_{s-1})$, where $i_s = i_r$ (or possibly beginning (i_{r+1}, j_r)—this is irrelevant). Let $\boldsymbol{\alpha_1}$ (respectively, $\boldsymbol{\alpha_2}$) be the matrix obtained from $\boldsymbol{\pi}$ by adding 1 to (respectively, subtracting 1 from) the entries in positions $(i_r, j_r), (i_{r+1}, j_{r+1}), \ldots, (i_{s-1}, j_{s-1})$ and subtracting 1 from (respectively, adding 1 to) the entries in positions $(i_{r+1}, j_r), (i_{r+2}, j_{r+1}), \ldots, (i_s, j_{s-1})$. Then $\boldsymbol{\alpha_1}, \boldsymbol{\alpha_2} \in E$ and $2\pi = \boldsymbol{\alpha_1} + \boldsymbol{\alpha_2}$. But neither $\boldsymbol{\alpha_1}$ nor $\boldsymbol{\alpha_2}$ is a multiple of π, so $\pi \notin \mathrm{CF}(E)$. □

We now come to the main result concerning the function $H_n(r)$.

4.6.2 Proposition. *For fixed $n \in \mathbb{P}$ the function $H_n(r)$ is a polynomial in r of degree $(n-1)^2$. Since it is a polynomial, it can be evaluated at any $r \in \mathbb{Z}$, and we have*

$$H_n(-1) = H_n(-2) = \cdots = H_n(-n+1) = 0,$$
$$(-1)^{n-1} H_n(-n-r) = H_n(r). \tag{4.29}$$

Proof. By Lemma 4.6.1, any $\boldsymbol{\pi} = (\pi_{ij}) \in \mathrm{CF}(E)$ satisfies $\pi_{11} + \pi_{12} + \cdots + \pi_{1n} = 1$. Hence if we set $x_{ij} = \lambda$ and $x_{ij} = 1$ for $i \geq 2$ in $1 - \boldsymbol{x}^{\boldsymbol{\pi}}$ (where $\boldsymbol{x}^{\boldsymbol{\pi}} = \prod_{i,j} x_{ij}^{\pi_{ij}}$), then we obtain $1 - \lambda$. Let

$$F_n(\lambda) = \sum_{r \geq 0} H_n(r) \lambda^r.$$

Then by Theorem 4.5.11 and Lemma 4.5.17, $F_n(\lambda)$ is a rational function of degree less than 0 and with denominator $(1-\lambda)^{t+1}$ for some $t \in \mathbb{N}$. Thus by Corollary 4.3.1, $H_n(r)$ is a polynomial function of r.

Now $\boldsymbol{\alpha}$ is an $\mathbb{N}$-solution to equation (4.27) if and only if $\boldsymbol{\alpha} + \boldsymbol{\kappa}$ is a $\mathbb{P}$-solution, where $\boldsymbol{\kappa}$ is the $n \times n$ matrix of all 1's. Thus by Corollary 4.6.16,

$$E(1/\boldsymbol{x}) = \pm \left(\prod_{i,j} x_{ij} \right) E(\boldsymbol{x}).$$

Substituting $x_{1j} = \lambda$ and $x_{ij} = 1$ if $j > 1$, we obtain

$$F_n(1/\lambda) = \pm \lambda^n F_n(\lambda) = \pm \sum_{r \geq 0} \overline{H}_n(r) \lambda^r,$$

where $\overline{H}_n(r)$ is the number of $n \times n$ $\mathbb{P}$-matrices with every row and column sum equal to r. Hence by Proposition 4.2.3,

$$H_n(-n-r) = \pm H_n(r)$$

(the sign being $(-1)^{\deg H_n(r)}$). Since $\overline{H}_n(1) = \cdots = \overline{H}_n(n-1) = 0$, we also get $H_n(-1) = \cdots = H_n(n-1) = 0$.

There remains to show that $\deg H_n(r) = (n-1)^2$. We will give two proofs, one analytic and one algebraic. First, we give the analytic proof. If $\boldsymbol{\alpha} = (\alpha_{ij})$ is an

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

$\mathbb{N}$-matrix with every row and column sum equal to r, then (a) $0 \le \alpha_{ij} \le r$, and (b) if α_{ij} is given for $(i,j) \in [n-1] \times [n-1]$, then the remaining entries are uniquely determined. Hence,

$$H_n(r) \le (r+1)^{(n-1)^2}, \text{ so } \deg H_n(r) \le (n-1)^2.$$

On the other hand, if we arbitrarily choose

$$\frac{(n-2)r}{(n-1)^2} \le \alpha_{ij} \le \frac{r}{n-1}$$

for $(i,j) \in [n-1] \times [n-1]$, then when we fill in the rest of $\boldsymbol{\alpha}$ to have row and column sums equal to r, every entry will be in $\mathbb{N}$. Thus,

$$\begin{aligned} H_n(r) &\ge \left(\frac{r}{n-1} - \frac{(n-2)r}{(n-1)^2} \right)^{(n-1)^2} \\ &= \left(\frac{r}{(n-1)!^2} \right)^{(n-1)^2}, \end{aligned}$$

so $\deg H_n(r) \ge (n-1)^2$. Hence, $\deg H_n(r) = (n-1)^2$.

For the algebraic proof that $\deg H_n(r) = (n-1)^2$, we compute the dimension of the cone $\mathcal{C}$ of all solutions to equation (4.27) in nonnegative real numbers. The n^2 equations appearing in (4.27) are highly redundant; we need for instance only

$$\sum_{j=1}^{n} \alpha_{1j} = \sum_{j=1}^{n} \alpha_{ij}, \quad 2 \le i \le n,$$

and

$$\sum_{i=1}^{n} \alpha_{i1} = \sum_{i=1}^{n} \alpha_{ij}, \quad 2 \le j \le n.$$

Thus, $\mathcal{C}$ is defined by $2n-2$ linearly independent equations in $\mathbb{R}^{n^2}$, so $\dim \mathcal{C} = n^2 - 2n + 2$. Hence, the denominator of the rational generating function $\sum_{r \ge 0} H_n(r)\lambda^r$, when reduced to lowest terms, is $(1-\lambda)^{n^2-2n+2}$, so $\deg H_n(r) = n^2 - 2n + 1 = (n-1)^2$. □

One immediate use of Proposition 4.6.2 is for the actual computation of the values $H_n(r)$. Since $H_n(r)$ is a polynomial of degree $(n-1)^2$, we need to compute $(n-1)^2 + 1$ values to determine it completely. Since $H_n(-1) = \cdots = H_n(-n+1) = 0$ and $H_n(-n-r) = (-1)^{n-1} H_n(r)$, once we compute $H_n(0), H_n(1), \ldots, H_n(i)$ we know $2i + n + 1$ values. Hence it suffices to take $i = \binom{n-1}{2}$ in order to determine $H_n(r)$. For instance, to compute $H_3(r)$, we only need the trivially computed values $H_3(0) = 1$ and $H_3(1) = 3! = 6$. To compute $H_4(r)$, we need only $H_4(0) = 1$, $H_4(1) = 24$, $H_4(2) = 282$, $H_4(3) = 2008$. Some

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

small values of $F_n(\lambda)$ are given by

$$F_3(\lambda) = \frac{1+\lambda+\lambda^2}{(1-\lambda)^5},$$

$$F_4(\lambda) = \frac{1+14\lambda+87\lambda^2+148\lambda^3+87\lambda^4+14\lambda^5+\lambda^6}{(1-\lambda)^{10}},$$

$$F_5(\lambda) = \frac{P_5(\lambda)}{(1-\lambda)^{17}},$$

where

$$\begin{aligned} P_5(\lambda) = 1 &+ 103\lambda + 4306\lambda^2 + 63110\lambda^3 \\ &+ 388615\lambda^4 + 1115068\lambda^5 + 1575669\lambda^6 + 1115068\lambda^7 \\ &388615\lambda^8 + 63110\lambda^9 + 4306\lambda^{10} + 103\lambda^{11} + \lambda^{12}. \end{aligned}$$

NOTE. We can apply the method discussed in the Note following Corollary 4.5.16 to the computation of $H_n(r)$. When $n = 3$ the computation can easily be done without recourse to commutative algebra. This approach is the subject of Exercise 2.15, which we now further explicate. Let P_w be the permutation matrix corresponding to the permutation $w \in \mathfrak{S}_3$. Any five of these matrices are linearly independent, and all six of them satisfy the unique linear dependence (up to multiplication by a nonzero scalar)

$$P_{123} + P_{231} + P_{312} = P_{213} + P_{132} + P_{321}. \tag{4.30}$$

Let E be the monoid of all 3×3 $\mathbb{N}$-matrices with equal row and column sums. For $A = (a_{ij}) \in E$, write

$$x^A = \prod_{i,j=1}^{3} x_{ij}^{a_{ij}}.$$

In particular,

$$x^{P_w} = \prod_{i=1}^{3} x_{i,w(i)}.$$

It follows easily from equation (4.30) that

$$\sum_{A \in E} x^A = \frac{1 - x^{P_{123}} x^{P_{231}} x^{P_{312}}}{\prod_{w \in \mathfrak{S}_3} (1 - x^{P_w})}. \tag{4.31}$$

Hence,

$$\begin{aligned} \sum_{r \geq 0} H_3(r)\lambda^r &= \frac{1-\lambda^3}{(1-\lambda)^6} \\ &= \frac{1+\lambda+\lambda^2}{(1-\lambda)^5}. \end{aligned}$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Moreover, we can write the numerator of the right-hand side of equation (4.31) as

$$(1-x^{P_{123}})+x^{P_{123}}(1-x^{P_{231}})+x^{P_{123}}x^{P_{231}}(1-x^{P_{312}}).$$

Each expression in parentheses cancels a factor of the denominator. It follows that we can describe a *canonical form* for the elements of E. Namely, every element of E can be uniquely written in exactly one of the forms

$$aP_{132}+bP_{213}+cP_{231}+dP_{312}+eP_{321},$$

$$(a+1)P_{123}+bP_{132}+cP_{213}+dP_{312}+eP_{321},$$

$$(a+1)P_{123}+bP_{132}+cP_{213}+(d+1)P_{231}+eP_{321},$$

where $a,b,c,d,e \in \mathbb{N}$.

As a modification of Proposition 4.6.2, consider the problem of counting the number $S_n(r)$ of *symmetric* $\mathbb{N}$-matrices with every row (and hence every column) sum equal to r. Again the crucial result is the analogue of Lemma 4.6.1.

4.6.3 Lemma. *Let E be the monoid of symmetric $n \times n$ $\mathbb{N}$-matrices with all row (and column) sums equal. Then* $\mathrm{CF}(E)$ *is contained in the set of matrices of the form $\boldsymbol{\pi}$ or $\boldsymbol{\pi}+\boldsymbol{\pi}^t$, where $\boldsymbol{\pi}$ is a permutation matrix and $\boldsymbol{\pi}^t$ is its transpose (or inverse).*

Proof. Let $\boldsymbol{\alpha} \in E$. Forgetting for the moment that $\boldsymbol{\alpha}$ is symmetric, we have by Lemma 4.6.1 that $\operatorname{supp}\boldsymbol{\alpha}$ contains the support of some permutation matrix $\boldsymbol{\pi}$. Thus for some $k \in \mathbb{P}$ (actually, $k=1$ will do, but this is irrelevant), $k\boldsymbol{\alpha} = \boldsymbol{\pi}+\boldsymbol{\rho}$ where $\boldsymbol{\rho}$ is an $\mathbb{N}$-matrix with equal line sums. Therefore, $2k\boldsymbol{\alpha} = k(\boldsymbol{\alpha}+\boldsymbol{\alpha}^t) = (\boldsymbol{\pi}+\boldsymbol{\pi}^t)+(\boldsymbol{\rho}+\boldsymbol{\rho}^t)$. Hence, $\operatorname{supp}(\boldsymbol{\pi}+\boldsymbol{\pi}^t) \subseteq \operatorname{supp}(\boldsymbol{\alpha})$. It follows that any $\boldsymbol{\beta} \in \mathrm{CF}(E)$ satisfies $j\boldsymbol{\beta} = \boldsymbol{\pi}+\boldsymbol{\pi}^t$ for some $j \in \mathbb{P}$ and permutation matrix $\boldsymbol{\pi}$. If $\boldsymbol{\pi} = \boldsymbol{\pi}^t$, then we must have $j=2$; otherwise, $j=1$, and the proof follows. □

4.6.4 Proposition. *For fixed $n \in \mathbb{P}$, there exist polynomials $P_n(r)$ and $Q_n(r)$ such that* $\deg P_n(r) = \binom{n}{2}$ *and*

$$S_n(r) = P_n(r)+(-1)^r Q_n(r).$$

Moreover,

$$S_n(-1) = S_n(-2) = \cdots = S_n(-n+1) = 0,$$

$$S_n(-n-r) = (-1)^{\binom{n}{2}} S_n(r).$$

Proof. By Lemma 4.6.3, any $\boldsymbol{\beta} = (\beta_{ij}) \in \mathrm{CF}(E)$ satisfies $\beta_{11}+\beta_{12}+\cdots+\beta_{1n} = 1$ or 2. Hence, if we set $x_{ij} = \lambda$ and $x_{ij} = 1$ for $i \geq 2$ in $1-\boldsymbol{x}^{\boldsymbol{\beta}}$, then we obtain either $1-\lambda$ or $1-\lambda^2$. Set $G_n(\lambda) = \sum_{r\geq 0} S_n(r)\lambda^r$. Then by Theorem 4.5.11 and Lemma 4.5.17, $G_n(x)$ is a rational function of negative degree and with denominator $(1-\lambda)^s(1-\lambda^2)^t$ for some $s,t \in \mathbb{N}$. Hence by Proposition 4.4.1 (or the more general Theorem 4.1.1), $S_n(r) = P_n(r)+(-1)^r Q_n(r)$ for certain polynomials $P_n(r)$ and $Q_n(r)$. The remainder of the proof is analogous to that of Proposition 4.6.2. □

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

For the problem of computing $\deg Q_n(r)$, see equation (4.50) and the sentence following.

Some small values of $G_n(\lambda)$ are given by

$$G_1(\lambda) = \frac{1}{1-\lambda}, \quad G_2(\lambda) = \frac{1}{(1-\lambda)^2},$$
$$G_3(\lambda) = \frac{1+\lambda+\lambda^2}{(1-\lambda)^4(1+\lambda)},$$
$$G_4(\lambda) = \frac{1+4\lambda+10\lambda^2+4\lambda^3+\lambda^4}{(1-\lambda)^7(1+\lambda)},$$
$$G_5(\lambda) = \frac{V_5(\lambda)}{(1-\lambda)^{11}(1+\lambda)^6},$$

where

$$\begin{aligned} V_5(\lambda) = 1 &+ 21\lambda + 222\lambda^2 + 1082\lambda^3 + 3133\lambda^4 \\ &+ 5722\lambda^5 + 7013\lambda^6 + 5722\lambda^7 + 3133\lambda^8 \\ &+ 1082\lambda^9 + 222\lambda^{10} + 21\lambda^{11} + \lambda^{12}. \end{aligned}$$

4.6.2 The Ehrhart Quasipolynomial of a Rational Polytope

An elegant and useful application of the preceding theory concerns a certain function $i(\mathcal{P},n)$ associated with a convex polytope $\mathcal{P}$. By definition, a *convex polytope* $\mathcal{P}$ is the convex hull of a finite set of points in $\mathbb{R}^m$. Then $\mathcal{P}$ is homeomorphic to a ball $\mathbb{B}^d$. We write $d = \dim \mathcal{P}$ and call $\mathcal{P}$ a *d-polytope*. Equivalently, the affine span $\mathrm{aff}(\mathcal{P})$ of $\mathcal{P}$ is a d-dimensional affine subspace of $\mathbb{R}^m$. By $\partial\mathcal{P}$ and $\mathcal{P}^\circ$ we denote the boundary and interior of $\mathcal{P}$ in the usual topological sense (with respect to the embedding of $\mathcal{P}$ in its affine span). In particular $\partial\mathcal{P}$ is homeomorphic to the $(d-1)$-sphere $\mathbb{S}^{d-1}$.

A point $\boldsymbol{\alpha} \in \mathcal{P}$ is a *vertex* of $\mathcal{P}$ if there exists a closed affine half-space $\mathcal{H} \subset \mathbb{R}^m$ such that $\mathcal{P} \cap \mathcal{H} = \{\boldsymbol{\alpha}\}$. Equivalently, $\boldsymbol{\alpha} \in \mathcal{P}$ is a vertex if it does not lie in the interior of any line segment contained in $\mathcal{P}$. Let V be the set of vertices of $\mathcal{P}$. Then V is finite and $\mathcal{P} = \mathrm{conv}\, V$, the convex hull of V. Moreover, if $S \subset \mathbb{R}^m$ is any set for which $\mathcal{P} = \mathrm{conv}\, V$, then $V \subseteq S$. The (convex) polytope $\mathcal{P}$ is called *rational* if each vertex of $\mathcal{P}$ has rational coordinates.

If $\mathcal{P} \subset \mathbb{R}^m$ is a rational convex polytope and $n \in \mathbb{P}$, then define integers $i(\mathcal{P},n)$ and $\bar{i}(\mathcal{P},n)$ by

$$i(\mathcal{P},n) = \mathrm{card}(n\mathcal{P} \cap \mathbb{Z}^m),$$
$$\bar{i}(\mathcal{P},n) = \mathrm{card}(n\mathcal{P}^\circ \cap \mathbb{Z}^m),$$

where $n\mathcal{P} = \{n\boldsymbol{\alpha} : \boldsymbol{\alpha} \in \mathcal{P}\}$. Equivalently, $i(\mathcal{P},n)$ (respectively, $\bar{i}(\mathcal{P},n)$) is equal to the number of rational points in $\mathcal{P}$ (respectively, $\mathcal{P}^\circ$) all of whose coordinates have least denominator dividing n. We call $i(\mathcal{P},n)$ (respectively, $\bar{i}(\mathcal{P},n)$) the

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Ehrhart quasipolynomial of $\mathcal{P}$ (respectively, $\mathcal{P}^\circ$). Of course, we have to justify this terminology by showing that $i(\mathcal{P},n)$ and $\bar{i}(\mathcal{P},n)$ are indeed quasipolynomials.

4.6.5 Example. a. Let $\mathcal{P}_m$ be the convex hull of the set $\{(\varepsilon_1,\ldots,\varepsilon_m) \in \mathbb{R}^m : \varepsilon_i = 0 \text{ or } 1\}$. Thus, $\mathcal{P}_m$ is the *unit cube* in $\mathbb{R}^m$. It should be geometrically obvious that $i(\mathcal{P}_m,n) = (n+1)^m$ and $\bar{i}(\mathcal{P}_m,n) = (n-1)^m$.

b. Let $\mathcal{P}$ be the line segment joining 0 and $\alpha > 0$ in $\mathbb{R}$, where $\alpha \in \mathbb{Q}$. Clearly, $i(\mathcal{P},n) = \lfloor n\alpha \rfloor + 1$, which is a quasipolynomial of minimum quasiperiod equal to the denominator of α when written in lowest terms.

In order to prove the fundamental result concerning the Ehrhart quasipolynomials $i(\mathcal{P},n)$ and $\bar{i}(\mathcal{P},n)$, we will need the standard fact that a convex polytope $\mathcal{P}$ may also be defined as a bounded intersection of finitely many half-spaces. In other words, $\mathcal{P}$ is the set of all real solutions $\boldsymbol{\alpha} \in \mathbb{R}^m$ to a finite system of linear inequalities $\boldsymbol{\alpha} \cdot \boldsymbol{\delta} \le a$, provided that this solution set is bounded. (Note that the equality $\boldsymbol{\alpha} \cdot \boldsymbol{\delta} = a$ is equivalent to the two inequalities $\boldsymbol{\alpha} \cdot (-\boldsymbol{\delta}) \le -a$ and $\boldsymbol{\alpha} \cdot \boldsymbol{\delta} \le a$, so we are free to describe $\mathcal{P}$ using inequalities and equalities.) The polytope $\mathcal{P}$ is rational if and only if the inequalities can be chosen to have rational (or integral) coefficients.

Since $i(\mathcal{P},n)$ and $\bar{i}(\mathcal{P},n)$ are not affected by replacing $\mathcal{P}$ with $\mathcal{P}+\boldsymbol{\gamma}$ for $\boldsymbol{\gamma} \in \mathbb{Z}^m$, we may assume that all points in $\mathcal{P}$ have nonnegative coordinates, denoted $\mathcal{P} \ge 0$. We now associate with a rational convex polytope $\mathcal{P} \ge 0$ in $\mathbb{R}^m$ a monoid $E_{\mathcal{P}} \subseteq \mathbb{N}^{m+1}$ of $\mathbb{N}$-solutions to a system of homogeneous linear inequalities. (Recall that an inequality may be converted to an equality by introducting a slack variable.) Suppose that $\mathcal{P}$ is the set of solutions $\boldsymbol{\alpha}$ to the system

$$\boldsymbol{\alpha} \cdot \boldsymbol{\delta_i} \le a_i, \quad 1 \le i \le s,$$

where $\boldsymbol{\delta_i} \in \mathbb{Q}^m$, $a_i \in \mathbb{Q}$. Introduce new variables $\boldsymbol{\gamma} = (\gamma_1,\ldots,\gamma_m)$ and t, and define $E_{\mathcal{P}} \subseteq \mathbb{N}^{m+1}$ to be the set of all $\mathbb{N}$-solutions to the system

$$\boldsymbol{\gamma} \cdot \boldsymbol{\delta_i} \le a_i t, \quad 1 \le i \le s.$$

4.6.6 Lemma. *A nonzero vector $(\boldsymbol{\gamma},t) \in \mathbb{N}^{m+1}$ belongs to $E_{\mathcal{P}}$ if and only if $\boldsymbol{\gamma}/t$ is a rational point of $\mathcal{P}$.*

Proof. Since $\mathcal{P} \ge 0$, any rational point $\boldsymbol{\gamma}/t \in \mathcal{P}$ with $\boldsymbol{\gamma} \in \mathbb{Z}^m$ and $t \in \mathbb{P}$ satisfies $\boldsymbol{\gamma} \in \mathbb{N}^m$. Hence a nonzero vector $(\boldsymbol{\gamma},t) \in \mathbb{N}^{m+1}$ with $t > 0$ belongs to $E_{\mathcal{P}}$ if and only if $\boldsymbol{\gamma}/t$ is a rational point of $\mathcal{P}$.

It remains to show that if $(\boldsymbol{\gamma},t) \in E_{\mathcal{P}}$ and $t = 0$, then $\boldsymbol{\gamma} = \mathbf{0}$. Because $\mathcal{P}$ is bounded, it is easily seen that every vector $\boldsymbol{\beta} \ne \mathbf{0}$ in $\mathbb{R}^m$ satisfies $\boldsymbol{\beta} \cdot \boldsymbol{\delta_i} > 0$ for some $1 \le i \le s$. Hence, the only solution $\boldsymbol{\gamma}$ to $\boldsymbol{\gamma} \cdot \boldsymbol{\delta_i} \le 0$, $1 \le i \le s$, is $\boldsymbol{\gamma} = \mathbf{0}$, and the proof follows. □

Our next step is to determine $\mathrm{CF}(E_{\mathcal{P}})$, the completely fundamental elements of $E_{\mathcal{P}}$. If $\boldsymbol{\alpha} \in \mathbb{Q}^m$, then define $\operatorname{den}\boldsymbol{\alpha}$ (the *denominator* of $\boldsymbol{\alpha}$) as the least integer

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

$q \in \mathbb{P}$ such that $q\boldsymbol{\alpha} \in \mathbb{Z}^m$. In particular, if $\alpha \in \mathbb{Q}$, then $\operatorname{den}\boldsymbol{\alpha}$ is the denominator of α when written in lowest terms.

4.6.7 Lemma. *Let $\mathcal{P} \geq 0$ be a rational convex polytope in $\mathbb{R}^m$ with vertex set V. Then*

$$\mathrm{CF}(E_{\mathcal{P}}) = \{((\operatorname{den}\boldsymbol{\alpha})\boldsymbol{\alpha}, \operatorname{den}\boldsymbol{\alpha}) : \boldsymbol{\alpha} \in V\}.$$

Proof. Let $(\boldsymbol{\gamma}, t) \in E_{\mathcal{P}}$, and suppose that for some $k \in \mathbb{P}$ we have

$$k(\boldsymbol{\gamma}, t) = (\boldsymbol{\gamma_1}, t_1) + (\boldsymbol{\gamma_2}, t_2),$$

where $(\boldsymbol{\gamma_i}, t_i) \in E_{\mathcal{P}}$, $t_i \neq 0$. Then

$$\boldsymbol{\gamma}/t = (t_1/kt)(\boldsymbol{\gamma_1}/t_1) + (t_2/kt)(\boldsymbol{\gamma_2}/t_2),$$

where $(t_1/kt) + (t_2/kt) = 1$. Thus, $\boldsymbol{\gamma}/t$ lies on the line segment joining $\boldsymbol{\gamma_1}/t_1$ and $\boldsymbol{\gamma_2}/t_2$. It follows that $(\boldsymbol{\gamma}, t) \in \mathrm{CF}(E_{\mathcal{P}})$ if and only if $\boldsymbol{\gamma}/t \in V$ (so that $\boldsymbol{\gamma_1}/t_1 = \boldsymbol{\gamma_2}/t_2 = \boldsymbol{\gamma}/t$) and $(\boldsymbol{\gamma}, t) \neq j(\boldsymbol{\gamma}', t')$ for $(\boldsymbol{\gamma}', t') \in \mathbb{N}^{m+1}$ and an integer $j > 1$. Thus, we must have $t = \operatorname{den}(\boldsymbol{\gamma}/t)$, and the proof follows. □

It is now easy to establish the two basic facts concerning $i(\mathcal{P}, n)$ and $\bar{i}(\mathcal{P}, n)$.

4.6.8 Theorem. *Let $\mathcal{P}$ be a rational convex polytope of dimension d in $\mathbb{R}^m$ with vertex set V. Let $F(\mathcal{P}, \lambda) = 1 + \sum_{n \geq 1} i(\mathcal{P}, n)\lambda^n$. Then $F(\mathcal{P}, \lambda)$ is a rational function of λ of degree less than 0, which can be written with denominator $\prod_{\boldsymbol{\alpha} \in V}(1 - \lambda^{\operatorname{den}\boldsymbol{\alpha}})$. (Hence, in particular, $i(\mathcal{P}, n)$ is a quasipolynomial whose "correct" value at $n = 0$ is $i(\mathcal{P}, 0) = 1$.) The complex number $\lambda = 1$ is a pole of $F(\mathcal{P}, \lambda)$ of order $d + 1$, while no value of λ is a pole whose order exceeds $d + 1$.*

Proof. Let the variables x_i correspond to γ_i and y to t in the generating function $E_{\mathcal{P}}(\boldsymbol{x}, y)$; that is,

$$E_{\mathcal{P}}(\boldsymbol{x}, y) = \sum_{(\boldsymbol{\gamma}, t) \in E_{\mathcal{P}}} \boldsymbol{x}^{\boldsymbol{\gamma}} y^t.$$

Lemma 4.6.6, together with the observation $E_{\mathcal{P}}(\mathbf{0}, 0) = 1$, shows that

$$E_{\mathcal{P}}(1, \ldots, 1, \lambda) = F(P, \lambda). \tag{4.32}$$

Hence by Lemma 4.5.17, $F(\mathcal{P}, \lambda)$ is a rational function of degree less than 0. By Theorem 4.5.11 and Lemma 4.6.7, the denominator of $E_{\mathcal{P}}(\boldsymbol{x}, y)$ is equal to

$$\prod_{\boldsymbol{\alpha} \in V} \left(1 - \boldsymbol{x}^{(\operatorname{den}\boldsymbol{\alpha})\boldsymbol{\alpha}} y^{\operatorname{den}\boldsymbol{\alpha}}\right).$$

Thus by equation (4.32), the denominator of $F(\mathcal{P}, \lambda)$ can be taken as $\prod_{\boldsymbol{\alpha} \in V}\left(1 - \lambda^{\operatorname{den}\boldsymbol{\alpha}}\right)$.

Now $\dim E_{\mathcal{P}}$ is equal to the dimension of the vector space $\langle \mathrm{CF}(E_{\mathcal{P}}) \rangle$ spanned by $\mathrm{CF}(E_{\mathcal{P}}) = \{((\operatorname{den}\boldsymbol{\alpha})\boldsymbol{\alpha}, \operatorname{den}\boldsymbol{\alpha}) : \boldsymbol{\alpha} \in V\}$. Clearly then we also have $\langle \mathrm{CF}(E_{\mathcal{P}}) \rangle = \langle (\boldsymbol{\alpha}, 1) : \boldsymbol{\alpha} \in V \rangle$. The dimension of this latter space is just the maximum number of $\boldsymbol{\alpha} \in V$ that are affinely independent in $\mathbb{R}^m$ (i.e., such that no nontrivial linear

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

combination with zero coefficient sum is equal to 0). Since $\mathcal{P}$ spans a d-dimensional affine subspace of $\mathbb{R}^m$ there follows $\dim E_{\mathcal{P}} = d+1$. Now by Lemmas 4.5.2 and 4.5.4, we have

$$E_{\mathcal{P}}(\boldsymbol{x}, y) = \sum_{\sigma \in \overline{\Gamma}} (-1)^{d+1-\dim \sigma} E_{\sigma}(\boldsymbol{x}, y),$$

so

$$F(\mathcal{P}, \lambda) = \sum_{\sigma \in \overline{\Gamma}} (-1)^{d+1-\dim \sigma} E_{\sigma}(1, \ldots, 1, \lambda). \tag{4.33}$$

Looking at the expression (4.24) for $E_{\sigma}(\boldsymbol{x}, y)$, we see that those terms of equation (4.33) with $\dim \sigma = d+1$ have a positive coefficient of $(\lambda - 1)^{d+1}$ in the Laurent expansion about $\lambda = 1$, whereas all other terms have a pole of order at most d at $\lambda = 1$. Moreover, no term has a pole of order greater than $d+1$ at any $\lambda \in \mathbb{C}$. The proof follows. □

4.6.9 Theorem (the reciprocity theorem for Ehrhart quasipolynomials). *Since $i(\mathcal{P}, n)$ is a quasipolynomial, it can be defined for all $n \in \mathbb{Z}$. If $\dim \mathcal{P} = d$, then $\bar{i}(\mathcal{P}, n) = (-1)^d i(\mathcal{P}, -n)$.*

Proof. A vector $(\boldsymbol{\gamma}, t) \in \mathbb{N}^m$ lies in $\overline{E}_{\mathcal{P}}$ if and only if $\boldsymbol{\gamma}/t \in \mathcal{P}^{\circ}$. Thus,

$$\overline{E}_{\mathcal{P}}(1, \ldots, 1, \lambda) = \sum_{n \geq 1} \bar{i}(\mathcal{P}, n) \lambda^n.$$

The proof now follows from Theorem 4.5.14, Proposition 4.2.3, and the fact (shown in the proof of the previous theorem) that $\dim E_{\mathcal{P}} = d+1$. □

Unlike Theorem 4.5.11, the denominator $D(\lambda) = \prod_{\boldsymbol{\alpha} \in V} \left(1 - \lambda^{\operatorname{den} \boldsymbol{\alpha}}\right)$ of $F(\mathcal{P}, \lambda)$ is not in general the *least* denominator of $F(\mathcal{P}, \lambda)$. By Theorem 4.6.8, the least denominator has a factor $(1-\lambda)^{d+1}$ but not $(1-\lambda)^{d+2}$, while $D(\lambda)$ has a factor $(1-\lambda)^{\#V}$. We have $\#V = d+1$ if and only if $\mathcal{P}$ is a simplex. For roots of unity $\zeta \neq 1$, the problem of finding the highest power of $1 - \zeta\lambda$ dividing the least denominator of $F(\mathcal{P}, \lambda)$ is very delicate and subtle. A result in this direction is given by Exercise 4.66. Here we will content ourselves with one example showing that there is no obvious solution to this problem.

4.6.10 Example. Let $\mathcal{P}$ be the convex 3-polytope in $\mathbb{R}^3$ with vertices $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, $(1,1,0)$, and $(\frac{1}{2}, 0, \frac{1}{2})$. An examination of all the preceding theory will produce no theoretical reason why $F(\mathcal{P}, \lambda)$ does not have a factor $1+\lambda$ in its least denominator, but such is indeed the case. It is just an "accident" that the factor $1+\lambda$ appearing in $\prod_{\boldsymbol{\alpha} \in V} \left(1 - \lambda^{\operatorname{den} \boldsymbol{\alpha}}\right) = (1-\lambda)^5(1+\lambda)$ is eventually canceled, yielding $F(\mathcal{P}, \lambda) = (1-\lambda)^{-4}$.

One special case of Theorems 4.6.8 and 4.6.9 deserves special mention.

4.6.11 Corollary. *Let $\mathcal{P} \subset \mathbb{R}^m$ be an* integral *convex d-polytope (i.e., each vertex has integer coordinates). Then $i(\mathcal{P}, n)$ and $\bar{i}(\mathcal{P}, n)$ are polynomial functions of n*

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

of degree d, satisfying

$$i(\mathcal{P},0) = 1, \;\; i(\mathcal{P},n) = (-1)^d \bar{i}(\mathcal{P},n).$$

Proof. By Theorem 4.6.8, the least denominator of $F(\mathcal{P},\lambda)$ is $(1-\lambda)^{d+1}$. Now apply Corollary 4.3.1. □

If $\mathcal{P} \subset \mathbb{R}^m$ is an integral polytope, then of course we call $i(\mathcal{P},n)$ and $\bar{i}(\mathcal{P},n)$ the *Ehrhart polynomials* of $\mathcal{P}$ and $\mathcal{P}^\circ$. One interesting and unexpected application of Ehrhart polynomials is to the problem of finding the volume of $\mathcal{P}$. Somewhat more generally, we need the concept of the relative volume of an integral d-polytope. If $\mathcal{P} \subset \mathbb{R}^m$ is such a polytope, then the integral points of the affine space $\mathcal{A}$ spanned by $\mathcal{P}$ is a translate (coset) of some d-dimensional sublattice $L \cong \mathbb{Z}^d$ of $\mathbb{Z}^m$. Hence, there exists an invertible affine transformation $\phi\colon \mathcal{A} \to \mathbb{R}^d$ satisfying $\phi(\mathcal{A} \cap \mathbb{Z}^m) = \mathbb{Z}^d$. The image $\phi(\mathcal{P})$ of $\mathcal{P}$ under ϕ is an integral convex d-polytope in $\mathbb{R}^d$, so $\phi(\mathcal{P})$ has a positive volume (= Jordan content or Lebesgue measure) $v(\mathcal{P})$, called the *relative volume* of $\mathcal{P}$. It is easy to see that $v(\mathcal{P})$ is independent of the choice of ϕ and hence depends on $\mathcal{P}$ alone. If $d = m$ (i.e., $\mathcal{P}$ is an integral d-polytope in $\mathbb{R}^d$), then $v(\mathcal{P})$ is just the usual volume of $\mathcal{P}$ since we can take ϕ to be the identity map.

4.6.12 Example. Let $\mathcal{P} \subset \mathbb{R}^2$ be the line segment joining $(3,2)$ to $(5,6)$. The affine span $\mathcal{A}$ of $\mathcal{P}$ is the line $y = 2x-4$, and $\mathcal{A} \cap \mathbb{Z}^2 = \{(x,2x-4) : x \in \mathbb{Z}\}$. For the map $\phi\colon \mathcal{A} \to \mathbb{R}$, we can take $\phi(x,2x-4) = x$. The image $\phi(\mathcal{P})$ is the interval $[3,5]$, which has length 2. Hence, $v(\mathcal{P}) = 2$. To visualize this geometrically, draw a picture of $\mathcal{P}$ as in Figure 4.6(a). When "straightened out" $\mathcal{P}$ looks like Figure 4.6(b), which has length 2 when we think of the integer points $(3,2)$, $(4,4)$, $(5,6)$ as consecutive integers on the real line.

4.6.13 Proposition. *Let $\mathcal{P} \subset \mathbb{R}^m$ be an integral convex d-polytope. Then the leading coefficient of $i(\mathcal{P},n)$ is $v(\mathcal{P})$.*

Sketch of proof. The map $\phi\colon \mathcal{A} \to \mathbb{R}^d$ constructed earlier satisfies $i(\mathcal{P},n) = i(\phi(\mathcal{P}),n)$. Hence, we may assume $m = d$. Given $n \in \mathcal{P}$, for each point $\gamma \in \mathcal{P}$

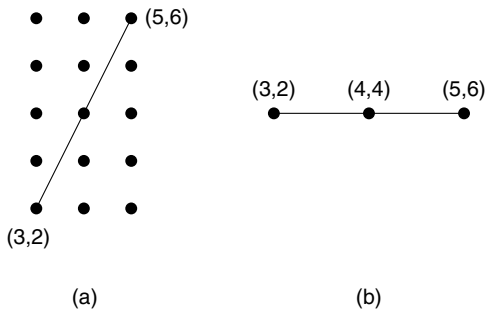

Figure 4.6 Computing relative volume.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

with $m\gamma \in \mathbb{Z}^d$ construct a d-dimensional hypercube H_γ with center γ and sides of length $1/n$ parallel to the coordinate axes. These hypercubes fit together to fill $\mathcal{P}$ without overlap, except for a small error on the boundary of $\mathcal{P}$. There are $i(\mathcal{P},n)$ hypercubes is all with a volume n^{-d} each, and hence a total volume of $n^{-d}i(\mathcal{P},n)$. As $n \to \infty$, it is geometrically obvious (and not hard to justify rigorously – this is virtually the definition of the Riemann integral) that the volume of these hypercubes will converge to the volume of $\mathcal{P}$. Hence, $\lim_{n\to\infty} n^{-d}i(\mathcal{P},n) = v(\mathcal{P})$, and the proof follows. □

4.6.14 Corollary. *Let $\mathcal{P} \subset \mathbb{R}^m$ be an integral convex d-polytope. If we know any d of the numbers $i(\mathcal{P},1)$, $\bar{i}(\mathcal{P},1)$, $i(\mathcal{P},2)$, $\bar{i}(\mathcal{P},2),\ldots$, then we can determine $v(\mathcal{P})$.*

Proof. Since $i(\mathcal{P},0) = 1$ and $i(\mathcal{P},-n) = (-1)^d\bar{i}(\mathcal{P},n)$, once we know d of the given numbers we know $d+1$ values of the polynomial $i(\mathcal{P},n)$ of degree d. Hence, we can find $i(\mathcal{P},n)$ and in particular its leading coefficient $v(\mathcal{P})$. □

4.6.15 Example. a. If $\mathcal{P} \subset \mathbb{R}^m$ is an integral convex 2-polytope, then

$$v(\mathcal{P}) = \frac{1}{2}(i(\mathcal{P},1) + \bar{i}(\mathcal{P},1) - 2).$$

This classical formula (for $m = 2$) is usually stated in the form

$$v(\mathcal{P}) = \frac{1}{2}(2A - B - 2),$$

where $A = \#(\mathbb{Z}^2 \cap \mathcal{P}) = i(\mathcal{P},1)$ and $B = \#(\mathbb{Z}^2 \cap \partial\mathcal{P}) = i(\mathcal{P},1) - \bar{i}(\mathcal{P},1)$.

b. If $\mathcal{P} \subset \mathbb{R}^m$ is an integral convex 3-polytope, then

$$v(\mathcal{P}) = \frac{1}{6}(i(\mathcal{P},2) - 3i(\mathcal{P},1) + \bar{i}(\mathcal{P},1) + 3).$$

c. If $\mathcal{P} \in \mathbb{R}^m$ is an integral convex d-polytope, then

$$v(\mathcal{P}) = \frac{1}{d!}\left((-1)^d + \sum_{k=1}^{d}\binom{d}{k}(-1)^{d-k}i(\mathcal{P},k)\right).$$

Let $\mathcal{P}$ be an integral convex d-polytope in $\mathbb{R}^m$. Because $i(\mathcal{P},n)$ is an integer-valued polynomial of degree d, we have from Corollary 4.3.1 that

$$\sum_{n\geq 0} i(\mathcal{P},n)x^n = \frac{A(\mathcal{P},x)}{(1-x)^{d+1}}$$

for some polynomial $A(\mathcal{P},x) \in \mathbb{Z}[x]$ of degree at most d. We call $A(\mathcal{P},x)$ the *$\mathcal{P}$-Eulerian polynomial*. For instance, if $\mathcal{P}$ is the unit d-dimensional cube then $i(\mathcal{P},n) = (n+1)^d$. It follows from Proposition 1.4.4 that $A(\mathcal{P},x) = A_d(x)/x$, where $A_d(x)$ is the ordinary Eulerian polynomial. Note that by Proposition 4.6.13 and the paragraph following Corollary 4.3.1, we have for a general integral convex d-polytope that $A_d(1) = d!v(\mathcal{P})$. Hence, $A(\mathcal{P},x)$ may be regarded as a

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

refinement of the relative volume $v(\mathcal{P})$. If $A(\mathcal{P},x) = \sum_{i=0}^{d} h_i^* x^i$, then the vector $h^*(\mathcal{P}) = (h_0^*, \ldots, h_d^*)$ is called the *h^*-vector* or *δ-vector* of $\mathcal{P}$. It can be shown that the h^*-vector is nonnegative (Exercise 4.48).

NOTE. Corollary 4.6.14 extends without difficulty to the case where $\mathcal{P}$ is not necessarily convex. We need only assume that $\mathcal{P} \subset \mathbb{R}^m$ is an integral polyhedral d-manifold with boundary; that is, a union of integral convex d-polytopes in $\mathbb{R}^m$ such that the intersection of any two is a common face of both and such that $\mathcal{P}$, regarded as a topological space, is a manifold with boundary. (In fact, we can replace this last condition with a weaker condition about the Euler characteristic of $\mathcal{P}$ and local Euler characteristic of $\mathcal{P}$ at any point $\alpha \in \mathcal{P}$, but we will not enter into the details here.) Assume for simplicity that $m = d$. Then the only change in the theory is that now $i(\mathcal{P},0) = \chi(\mathcal{P})$, the Euler characteristic of $\mathcal{P}$. Details are left to the reader.

We conclude with two more examples.

4.6.16 Example (Propositions 4.6.2 and 4.6.4 revisited). a. Let $\mathcal{P} = \Omega_n \subset \mathbb{R}^{n^2}$, the convex polytope of all $n \times n$ *doubly-stochastic matrices* (i.e., matrices of nonnegative real numbers with every row and column sum equal to one). Clearly, $M \in r\Omega_n \cap \mathbb{Z}^{n^2}$ if and only if M is an $\mathbb{N}$-matrix with every row and column sum equal to r. Hence, $i(\Omega_n, r)$ is just the function $H_n(r)$ of Proposition 4.6.2. Lemma 4.6.1 is equivalent to the statement that $V(\Omega_n)$ consists of the $n \times n$ permutation matrices. Thus, Ω_n is an integral polytope, and the conclusions of Proposition 4.6.2 follow also from Corollary 4.6.11.

b. Let $\mathcal{P} = \Sigma_n \in \mathbb{R}^{n^2}$, the convex polytope of all *symmetric* doubly stochastic matrices. As in (a), we have $i(\Sigma_n, r) = S_n(r)$, where $S_n(r)$ is the function of Proposition 4.6.4. Lemma 4.6.3 is equivalent to the statement that

$$V(\Sigma_n) \subseteq \left\{ \frac{1}{2}(P + P^t) \,:\, P \text{ is an } n \times n \text{ permutation matrix} \right\}.$$

Hence, $\operatorname{den} M = 1$ or 2 for all $M \in V(\Sigma_n)$, and the conclusions of Proposition 4.6.4 follow also from Theorem 4.6.8.

4.6.17 Example. Let $P = \{t_1, \ldots, t_p\}$ be a finite poset. Let $\mathcal{O} = \mathcal{O}(P)$ be the convex hull of incidence vectors of dual-order ideals K of P; that is, vectors of the form $(\varepsilon_1, \ldots, \varepsilon_p)$, where $\varepsilon_i = 1$ if $t_i \in K$ and $\varepsilon_i = 0$ otherwise. Then

$$\mathcal{O} = \{(a_1, \ldots, a_p) \in \mathbb{R}^p \,:\, 0 \le a_i \le 1 \text{ and } a_i \le a_j \text{ if } t_i \le t_j\}.$$

Thus, $(b_1, \ldots, b_p) \in n\mathcal{O} \cap \mathbb{Z}^p$ if and only if (i) $b_i \in \mathbb{Z}$, (ii) $0 \le b_i \le n$, and (iii) $b_i \le b_j$ if $t_i \le t_j$. Hence, $i(\mathcal{O}(P), n) = \Omega_P(n+1)$, where Ω_P is the order polynomial of P. The volume of $\mathcal{O}(P)$ is $e(P)/p!$, the leading coefficient of $\Omega_P(n+1)$ or $\Omega_P(n)$. (The volume is the same as the relative volume since $\dim \mathcal{O}(P) = p$.) The polytope $\mathcal{O}(P)$ is called the *order polytope* of P.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

4.7 The Transfer-Matrix Method

4.7.1 Basic Principles

The transfer-matrix method, like the Principle of Inclusion-Exclusion and the Möbius inversion formula, has simple theoretical underpinnings but a very wide range of applicability. The theoretical background can be divided into two parts – combinatorial and algebraic. First, we discuss the combinatorial part. A (finite) *directed graph* or *digraph* D is a triple (V, E, ϕ), where $V = \{v_1, \ldots, v_p\}$ is a set of *vertices*, E is a finite set of (directed) *edges* or *arcs*, and ϕ is a map from E to $V \times V$. If $\phi(e) = (u, v)$, then e is called an edge *from* u *to* v, with *initial vertex* u and *final vertex* v. This is denoted $u = \operatorname{init} e$ and $v = \operatorname{fin} e$. If $u = v$, then e is called a *loop*. A *walk* Γ in D of *length* n from u to v is a sequence $e_1 e_2 \cdots e_n$ of n edges such that $\operatorname{init} e_1 = u$, $\operatorname{fin} e_n = v$, and $\operatorname{fin} e_i = \operatorname{init} e_{i+1}$ for $1 \le i < n$. If also $u = v$, then Γ is called a *closed walk based at* u. (Note that if Γ is a closed walk, then $e_i e_{i+1} \cdots e_n e_1 \cdots e_{i-1}$ is in general a different closed walk. In some graph-theoretical contexts this distinction would not be made.)

Now let $w\colon E \to R$ be a *weight function* with values in some commutative ring R. (For our purposes here, we can take $R = \mathbb{C}$ or a polynomial ring over $\mathbb{C}$.) If $\Gamma = e_1 e_2 \cdots e_n$ is a walk, then the *weight* of Γ is defined by $w(\Gamma) = w(e_1) w(e_2) \cdots w(e_n)$. Let $i, j \in [p]$ and $n \in \mathbb{N}$. Since D is finite, we can define

$$A_{ij}(n) = \sum_{\Gamma} w(\Gamma),$$

where the sum is over all walks Γ in D of length n from v_i to v_j. In particular, $A_{ij}(0) = \delta_{ij}$. If all $w(e) = 1$, then we are just counting the *number* of walks of length n from u to v. The fundamental problem treated by the transfer matrix method is the evaluation of $A_{ij}(n)$. The first step is to interpret $A_{ij}(n)$ as an entry in a certain matrix. Define a $p \times p$ matrix $A = (A_{ij})$ by

$$A_{ij} = \sum_{e} w(e),$$

where the sum ranges over all edges e satisfying $\operatorname{init} e = v_i$ and $\operatorname{fin} e = v_j$. In other words, $A_{ij} = A_{ij}(1)$. The matrix A is called the *adjacency matrix* of D, with respect to the weight function w. The eigenvalues of the adjacency matrix A play a key role in the enumeration of walks. These eigenvalues are also called the *eigenvalues of* D (as a weighted digraph).

4.7.1 Theorem. *Let $n \in \mathbb{N}$. Then the (i, j)-entry of A^n is equal to $A_{ij}(n)$. (Here we define $A^0 = I$ even if A is not invertible.)*

Proof. The proof is immediate from the definition of matrix multiplication. Specifically, we have

$$(A^n)_{ij} = \sum A_{ii_1} A_{i_1 i_2} \cdots A_{i_{n-1} j},$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

where the sum is over all sequences $(i_1,\dots,i_{n-1}) \in [p]^{n-1}$. The summand is 0 unless there is a walk $e_1e_2\cdots e_n$ from v_i to v_j with $\operatorname{fin} e_k = v_{i_k}$ $(1 \le k < n)$ and $\operatorname{init} e_k = v_{i_{k-1}}$ $(1 < k \le n)$. If such a walk exists, then the summand is equal to the sum of the weights of all such walks, and the proof follows. □

The second step of the transfer-matrix method is the use of linear algebra to analyze the behavior of the function $A_{ij}(n)$. Define the generating function

$$F_{ij}(D,\lambda) = \sum_{n\ge 0} A_{ij}(n)\lambda^n.$$

4.7.2 Theorem. *The generating function $F_{ij}(D,\lambda)$ is given by*

$$F_{ij}(D,\lambda) = \frac{(-1)^{i+j}\det(I-\lambda A : j,i)}{\det(I-\lambda A)}, \tag{4.34}$$

where $(B : j,i)$ denotes the matrix obtained by removing the j-th row and i-th column of B. Thus in particular $F_{ij}(D,\lambda)$ is a rational function of λ whose degree is strictly less than the multiplicity n_0 of 0 as an eigenvalue of A.

Proof. $F_{ij}(D,\lambda)$ is the (i,j)-entry of the matrix $\sum_{n\ge 0}\lambda^n A^n = (I-\lambda A)^{-1}$. If B is any invertible matrix, then it is well known from linear algebra that $(B^{-1})_{ij} = (-1)^{i+j}\det(B : j,i)/\det(B)$, so equation (4.34) follows.

Suppose now that A is a $p \times p$ matrix. Then

$$\det(I-\lambda A) = 1 + \alpha_1\lambda + \cdots + \alpha_{p-n_0}\lambda^{p-n_0},$$

where

$$(-1)^p\left(\alpha_{p-n_0}\lambda^{n_0} + \cdots + \alpha_1\lambda^{p-1} + \lambda^p\right)$$

is the characteristic polynomial $\det(A-\lambda I)$ of A. Thus as polynomials in λ, we have $\deg\det(I-\lambda A) = p - n_0$ and $\deg\det(I-\lambda A : j,i) \le p-1$. Hence,

$$\deg F_{ij} \le p - 1 - (p-n_0) < n_0.$$ □

One special case of Theorem 4.7.2 is particularly elegant. Let

$$C_D(n) = \sum_{\Gamma} w(\Gamma),$$

where the sum is over all closed walks Γ in D of length n. For instance, $C_D(1) = \operatorname{tr} A$, where tr denotes trace.

4.7.3 Corollary. *Let $Q(\lambda) = \det(I-\lambda A)$. Then*

$$\sum_{n\ge 1} C_D(n)\lambda^n = -\frac{\lambda Q'(\lambda)}{Q(\lambda)}.$$

Proof. By Theorem 4.7.1, we have

$$C_D(n) = \sum_{i=1}^{p} A_{ii}(n) = \operatorname{tr} A^n.$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Let $\omega_1, \ldots, \omega_q$ be the nonzero eigenvalues of A. Then

$$\operatorname{tr} A^n = \omega_1^n + \cdots + \omega_q^n, \tag{4.35}$$

so

$$\sum_{n \geq 1} C_D(n)\lambda^n = \frac{\omega_1 \lambda}{1 - \omega_1 \lambda} + \cdots + \frac{\omega_q \lambda}{1 - \omega_q \lambda}.$$

When put over the denominator $(1 - \omega_1\lambda)\cdots(1 - \omega_q\lambda) = Q(\lambda)$, the numerator becomes $-\lambda Q'(\lambda)$. (Alternatively, this result may be deduced directly from Theorem 4.7.2.) □

4.7.2 Undirected Graphs

The preceding theory applies also to ordinary (undirected) graphs G. If we replace each edge e in G between vertices u and v with the two directed edges e' from u to v and e'' from v to u, then walks in the resulting digraph D_G of length n from u to v correspond exactly to walks in G of length n from u to v, as defined in the Appendix. The same remarks apply to weighted edges and walks. Hence, the counting of walks in undirected graphs G is just a special case of counting walks in digraphs. The undirected case corresponds to a *symmetric* adjacency matrix A. Symmetric matrices enjoy algebraic properties that lead to some additional formulas for the enumeration of walks.

Recall that a real symmetric $p \times p$ matrix A has p linearly independent real eigenvectors, which can in fact be chosen to be orthonormal (i.e., orthogonal and of unit length). Let $u_1^t, \ldots, u_p^t$ (where ^{t} denotes transpose, so u_i is a row vector) be real orthonormal eigenvectors for A, with corresponding eigenvalues $\lambda_1, \ldots, \lambda_p$. Each u_i is a row vector, so u_i^t is a column vector. Thus, the dot (or scalar or inner) product of the vectors u and v is given by uv^t (ordinary matrix multiplication). In particular, $u_i u_j^t = \delta_{ij}$. Let $U = (u_{ij})$ be the matrix whose columns are $u_1^t, \ldots, u_p^t$, denoted $U = [u_1^t, \ldots, u_p^t]$. Thus, U is an orthogonal matrix and

$$U^t = U^{-1} = \begin{bmatrix} u_1 \\ \vdots \\ u_p \end{bmatrix},$$

the matrix whose rows are $u_1, \ldots, u_p$. Recall from linear algebra that the matrix U *diagonalizes* A, that is,

$$U^{-1} A U = \operatorname{diag}(\lambda_1, \ldots, \lambda_p),$$

where $\operatorname{diag}(\lambda_1, \ldots, \lambda_p)$ denotes the diagonal matrix with diagonal entries $\lambda_1, \ldots, \lambda_p$.

4.7.4 Corollary. *Given the graph G as above, fix the two vertices v_i and v_j. Let $\lambda_1, \ldots, \lambda_p$ be the eigenvalues of G, that is, of the adjacency matrix $A = A(G)$.*

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Then there exist real numbers $c_1, \ldots, c_p$ such that for all $n \geq 1$, we have

$$(A^n)_{ij} = c_1\lambda_1^n + \cdots + c_p\lambda_n^n.$$

In fact, if $U = (u_{rs})$ is a real orthogonal matrix such that $U^{-1}AU = \operatorname{diag}(\lambda_1, \ldots, \lambda_p)$, then we have

$$c_k = u_{ik}u_{jk}.$$

Proof. We have [why?]

$$U^{-1}A^nU = \operatorname{diag}(\lambda_1^n, \ldots, \lambda_p^n).$$

Hence,

$$A^n = U \cdot \operatorname{diag}(\lambda_1^n, \ldots, \lambda_p^n)U^{-1}.$$

Taking the (i,j)-entry of both sides (and using $U^{-1} = U^t$) gives

$$(A^n)_{ij} = \sum_k u_{ik}\lambda_k^n u_{jk},$$

as desired. □

4.7.3 Simple Applications

With the basic theory out of the way, let us look at some applications.

4.7.5 Example. For $p, n \geq 1$, let $f_p(n)$ denote the number of sequences $a_1a_2\cdots a_n \in [p]^n$ such that $a_i \neq a_{i+1}$ for $1 \leq i \leq n$, and $a_n \neq a_1$. We are simply counting closed walks of length n in the complete graph K_p; we begin at vertex a_1, then walk to a_2, and so on. Let A be the adjacency matrix of K_p. Then $A + I$ is the all 1's matrix J and, hence, has rank 1. Thus, $p - 1$ eigenvalues of $A + I$ are equal to 0, so $p - 1$ eigenvalues of A are equal to -1. To obtain the remaining eigenvalue of A, note that $\operatorname{tr} A = 0$. Since the trace is the sum of the eigenvalues, the remaining eigenvalue of A is $p - 1$. This may also be seen by noting that the column vector $[1, 1, \ldots, 1]^t$ is an eigenvector for A with eigenvalue $p - 1$. We obtain from equation (4.35) that

$$f_p(n) = (p-1)^n + (p-1)(-1)^n. \tag{4.36}$$

By symmetry, the number of closed walks of length n in K_p that start at a particular vertex, say 1, is given by

$$(A^n)_{11} = \frac{1}{p}f_p(n) = \frac{1}{p}\left((p-1)^n + (p-1)(-1)^n\right).$$

The number of walks of length n between two *unequal* vertices, say 1 and 2, is given by

$$(A^n)_{12} = \frac{1}{p-1}\left((p-1)^n - (A^n)_{11}\right)$$

$$= \frac{1}{p}\left((p-1)^n - (-1)^n\right).$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

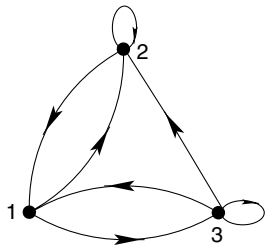

Figure 4.7 A digraph illustrating the transfer-matrix method.

Another way to obtain these results is to note that $J^k = p^{k-1}J$ for $k \geq 1$. Hence,

$$\begin{aligned} A^n &= (J-I)^n \\ &= (-1)^n I + \sum_{k=1}^{n} (-1)^{n-k} \binom{n}{k} J^k \\ &= (-1)^n I + \left(\sum_{k=1}^{n} (-1)^{n-k} \binom{n}{k} p^{k-1} \right) J \\ &= (-1)^n I + \frac{1}{p} \left((p-1)^n - (-1)^n \right) J. \end{aligned}$$

It is now easy to extract the $(1,1)$ and $(1,2)$ entries.

4.7.6 Example. Let $f(n)$ be the number of sequences $a_1 a_2 \cdots a_n \in [3]^n$ such that neither 11 nor 23 appear as two consecutive terms $a_i a_{i+1}$. Let D be the digraph on $V = [3]$ with an edge (i,j) if j is allowed to follow i in the sequence. Thus, D is given by Figure 4.7. If we set $w(e) = 1$ for every edge e, then clearly $f(n) = \sum_{i,j=1}^{3} A_{ij}(n-1)$. Setting $Q(\lambda) = \det(I - \lambda A)$ and $Q_{ij}(\lambda) = \det(I - \lambda A : j,i)$, there follows from Theorem 4.7.2 that

$$F(\lambda) := \sum_{n \geq 0} f(n+1)\lambda^n = \frac{\sum_{i,j=1}^{3} (-1)^{i+j} Q_{ij}(\lambda)}{Q(\lambda)}.$$

Now

$$A = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix},$$

so by direct calculation,

$$(1-\lambda A)^{-1} = \frac{1}{1-2\lambda-\lambda^2+\lambda^3} \begin{bmatrix} (1-\lambda)^2 & \lambda & \lambda(1-\lambda) \\ \lambda(1-\lambda) & 1-\lambda-\lambda^2 & \lambda^2 \\ \lambda & \lambda(1+\lambda) & 1-\lambda-\lambda^2 \end{bmatrix}.$$

It follows that

$$F(\lambda) = \frac{3+\lambda-\lambda^2}{1-2\lambda-\lambda^2+\lambda^3}, \tag{4.37}$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

or equivalently,

$$\sum_{n\geq 0} f(n)\lambda^n = \frac{1+\lambda}{1-2\lambda-\lambda^2+\lambda^3}.$$

In the present situation, we do not actually have to compute $(I-\lambda A)^{-1}$ in order to write down equation (4.37). First, compute $\det(I-\lambda A) = 1-2\lambda-\lambda^2+\lambda^3$. Since this polynomial has degree 3, it follows from Theorem 4.7.2 that $\deg F(\lambda) < 0$. Hence, the numerator of $F(\lambda)$ is determined by the initial values $f(1) = 3$, $f(2) = 7$, $f(3) = 16$. This approach involves a considerably easier computation than evaluating $(I-\lambda A)^{-1}$.

Now suppose that we impose the additional restriction on the sequence $a_1 a_2 \cdots a_n$ that $a_n a_1 \neq 11$ or 23. Let $g(n)$ be the number of such sequences. Then $g(n) = C_D(n)$, the number of closed walks in D of length n. Hence with no further computation, we obtain

$$\sum_{n\geq 1} g(n)\lambda^n = -\frac{\lambda Q'(\lambda)}{Q(\lambda)} = \frac{\lambda(2+2\lambda-3\lambda^2)}{1-2\lambda-\lambda^2+\lambda^3}. \tag{4.38}$$

It is somewhat magical that, unlike the case for $f(n)$, we did not need to consider any initial conditions. Note that equation (4.38) yields the value $g(1) = 2$. The method disallows the sequence 1, since $a_1 a_n = 11$. This illustrates a common phenomenon in applying Corollary 4.7.3 – for small values of n (never larger than $p-1$) the value of $C_D(n)$ may not conform to our combinatorial expectations.

4.7.7 Example. A *factor* of a word w is a subword of w consisting of consecutive letters. In other words, v is a factor of w if we can write $w = uvy$ for some words u and y. Let $f(n)$ be the number of words (i.e., sequences) $a_1 a_2 \cdots a_n \in [3]^n$ such that there are no factors of the form $a_i a_{i+1} = 12$ or $a_i a_{i+1} a_{i+2} = 213$, 222, 231, or 313. At first sight, it may seem as if the transfer-matrix method is inapplicable, since an allowed value of a_i depends on more than just the previous value a_{i-1}. A simple trick, however, circumvents this difficulty – make the digraph D big enough to incorporate the required past history. Here we take $V = [3]^2$, with edges (ab, bc) if abc is allowed as three consecutive terms of the word. Thus, D is given by Figure 4.8. If we now define all weights $w(e) = 1$, then

$$f(n) = \sum_{ab,cd\in V} A_{ab,cd}(n-2).$$

Thus, $\sum_{n\geq 0} f(n)\lambda^n$ is a rational function with denominator $Q(\lambda) = \det(I-\lambda A)$ for a certain 8×8 matrix A. (The vertex 12 is never used, so we can take A to be 8×8 rather than 9×9.)

It is clear that this technique applies equally well to prove the following result.

4.7.8 Proposition. *Let S be a finite set, and let $\mathcal{F}$ be a finite set of finite words with terms (letters) from S. Let $f(n)$ be the number of words $a_1 a_2 \cdots a_n \in S^n$ such that*

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

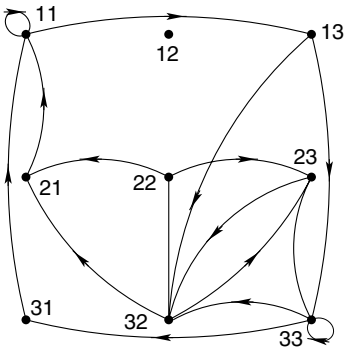

Figure 4.8 The digraph for Example 4.7.7.

no factor $a_i a_{i+1} \cdots a_{i+j}$ appears in $\mathcal{F}$. Then $\sum_{n \geq 0} f(n)\lambda^n \in \mathbb{Q}(\lambda)$. The same is true if we take the subscripts appearing in $a_i a_{i+1} \cdots a_{i+j}$ modulo n. In this case, if $g(n)$ is the number of such words, then $\sum_{n \geq 1} g(n)\lambda^n = -\lambda Q'(\lambda)/Q(\lambda)$ for some $Q(\lambda) \in \mathbb{Q}[\lambda]$, provided that $g(n)$ is suitably interpreted for small n.

Even though there turn out to be special methods for actually computing the generating functions appearing in Proposition 4.7.8 (see for example Exercise 4.40), at least the transfer-matrix method shows transparently that the generating functions are rational.

4.7.9 Example. Let $f(n)$ be the number of permutations $a_1 a_2 \cdots a_n \in \mathfrak{S}_n$ such that $|a_i - i| = 0$ or 1. Again it may first seem that the transfer-matrix method is inapplicable, since the allowed values of a_i depend on *all* the previous values $a_1, \ldots, a_{i-1}$. Observe, however, that there are really only three possible choices for a_i – namely, $i-1$, i, or $i+1$. Moreover, none of these values could be used prior to a_{i-2}, so the choices available for a_i depend only on the choices already made for a_{i-2} and a_{i-1}. Thus, the transfer-matrix method is applicable. The vertex set V of the digraph D consists of those pairs $(\alpha, \beta) \in \{-1, 0, 1\}^2$ for which it is possible to have $a_i - i = \alpha$ and $a_{i+1} - i - 1 = \beta$. An edge connects (α, β) to (β, γ) if it is possible to have $a_i - i = \alpha$, $a_{i+1} - i - 1 = \beta$, $a_{i+2} - i - 2 = \gamma$. Thus, $V = \{v_1, \ldots, v_7\}$, where $v_1 = (-1,-1)$, $v_2 = (-1,0)$, $v_3 = (-1,1)$, $v_4 = (0,0)$, $v_5 = (0,1)$, $v_6 = (1,-1)$, $v_7 = (1,1)$. (Note, for instance, that $(1,0)$ cannot be a vertex, since if $a_i - i = 1$ and $a_{i+1} - i - 1 = 0$, then $a_i = a_{i+1}$.) Writing $\alpha_1\alpha_2$ for the vertex (α_1, α_2), and so on, it follows that a walk $(\alpha_1\alpha_2, \alpha_2\alpha_3)$, $(\alpha_2\alpha_3, \alpha_3\alpha_4)$, $\ldots, (\alpha_n, \alpha_{n+1}, \alpha_{n+1}\alpha_{n+2})$ of length n in D corresponds to the permutation $1+\alpha_1$, $2+\alpha_2, \ldots, n+2+\alpha_{n+2}$ of $[n+2]$ of the desired type, provided that $\alpha_1 \neq -1$ and $\alpha_{n+2} \neq 1$. Hence, $f(n+2)$ is equal to the number of walks of length n in D from one of the vertices v_4, v_5, v_6, v_7 to one of the vertices v_1, v_2, v_4, v_6. Thus, if we set $w(e) = 1$ for all edges e in D, then

$$f(n+2) = \sum_{i=4,5,6,7} \sum_{j=1,2,4,6} (A^n)_{ij}.$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

The adjacency matrix is given by

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

and $Q(\lambda) = \det(I - \lambda A) = (1-\lambda)^2(1-\lambda-\lambda^2)$. As in Example 4.7.6, we can compute the numerator of $\sum_{n\geq 0} f(n+2)\lambda^n$ using initial values, rather than finding $(I-\lambda A)^{-1}$. According to Theorem 4.7.2, the polynomial $(1-\lambda^2)(1-\lambda-\lambda^2)\sum_{n\geq 0} f(n+2)\lambda^n$ may have degree as large as 6, so in order to compute $\sum_{n\geq 0} f(n)\lambda^n$ we need the initial values $f(0), f(1), \ldots, f(6)$. If this work is actually carried out, then we obtain

$$\sum_{n\geq 0} f(n)\lambda^n = \frac{1}{1-\lambda-\lambda^2}, \tag{4.39}$$

so that $f(n)$ is just the Fibonacci number F_{n+1} (!).

Similarly we may ask for the number $g(n)$ of permutations $a_1a_2\cdots a_n \in \mathfrak{S}_n$ such that $a_i - i \equiv 0, \pm 1 \pmod n$. This condition has the effect of allowing $a_1 = n$ and $a_n = 1$, so that $g(n)$ is just the number of closed walks $(\alpha_1\alpha_2, \alpha_2\alpha_3)$, $(\alpha_2\alpha_3, \alpha_3\alpha_4), \ldots, (\alpha_{n-1}\alpha_n, \alpha_n\alpha_1)$, $(\alpha_n\alpha_1, \alpha_1\alpha_2)$ in D of length n. Hence,

$$\sum_{n\geq 1} g(n)\lambda^n = -\frac{\lambda Q'(\lambda)}{Q(\lambda)} = \frac{2\lambda}{1-\lambda} + \frac{\lambda(1+2\lambda)}{1-\lambda-\lambda^2}. \tag{4.40}$$

Hence, $g(n) = 2 + L_n$, where L_n is the nth Lucas number. Note the "spurious" values $g(1) = 3$, $g(2) = 5$.

It is clear that the preceding arguments generalize to the following result.

4.7.10 Proposition. *a. Let S be a finite subset of $\mathbb{Z}$. Let $f_S(n)$ be the number of permutations $a_1a_2\cdots a_n \in \mathfrak{S}_n$ such that $a_i - i \in S$ for $i \in [n]$. Then $\sum_{n\geq 0} f_S(n)\lambda^n \in \mathbb{Q}(\lambda)$.*

b. Let $g_S(n)$ be the number of permutations $a_1a_2\cdots a_n \in \mathfrak{S}_n$ such that for all $i \in [n]$ there is a $j \in S$ for which $a_i - i \equiv j \pmod n$. If we suitably interpret $g_S(n)$ for small n, then there is a polynomial $Q(\lambda) \in \mathbb{Q}[\lambda]$ for which $\sum_{n\geq 1} g(n)\lambda^n = -\lambda Q'(\lambda)/Q(\lambda)$.

4.7.4 Factorization in Free Monoids

The reader is undoubtedly wondering, in view of the simplicity of the generating functions (4.39) and (4.40), whether there is a simpler way of obtaining them. Surely it seems unnecessary to find the characteristic polynomial of a 7×7 matrix

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

A when the final answer is $1/(1-\lambda-\lambda^2)$. The five eigenvalues 0,0,0,1,1 do not seem relevant to the problem. Actually, the vertices v_5 and v_7 are not needed for computing $f(n)$, but we are still left with a 5×5 matrix. This brings us to an important digresson – the method of factoring words in a free monoid. While this method has limited application, when it does work it is extremely elegant and simple.

Let $\mathcal{A}$ be a finite set, called the *alphabet*. A *word* is a finite sequence $a_1 a_2 \cdots a_n$ of elements of $\mathcal{A}$, including the empty word 1. The set of all words in the alphabet $\mathcal{A}$ is denoted $\mathcal{A}^*$. Define the *product* of two words $u = a_1 \cdots a_n$ and $v = b_1 \cdots b_m$ to be their juxtaposition,

$$uv = a_1 \cdots a_n b_1 \cdots b_m.$$

In particular, $1u = u1 = u$ for all $u \in \mathcal{A}^*$. The set $\mathcal{A}^*$, together with the product just defined, is called the *free monoid* on the set $\mathcal{A}$. (A *monoid* is a set with an associative binary operation and an identity element.) If $u = a_1 \cdots a_n \in \mathcal{A}^*$ with $a_i \in \mathcal{A}$, then define the *length* of u to be $\ell(u) = n$. In particular, $\ell(1) = 0$. If $\mathcal{C}$ is any subset of $\mathcal{A}^*$, then define

$$\mathcal{C}_n = \{u \in \mathcal{C} : \ell(u) = n\}.$$

Let $\mathcal{B}$ be a subset of $\mathcal{A}^*$ (possibly infinite), and let $\mathcal{B}^*$ be the submonoid of $\mathcal{A}^*$ generated by $\mathcal{B}$; that is, $\mathcal{B}^*$ consists of all words $u_1 u_2 \cdots u_n$ where $u_i \in \mathcal{B}$. We say that $\mathcal{B}^*$ is *freely generated* by $\mathcal{B}$ if every word $u \in \mathcal{B}^*$ can be written *uniquely* as $u_1 u_2 \cdots u_n$ where $u_i \in \mathcal{B}$. For instance, if $\mathcal{A} = \{a, b\}$ and $\mathcal{B} = \{a, ab, aab\}$, then $\mathcal{B}^*$ is not freely generated by $\mathcal{B}$ (since $a \cdot ab = aab$), but is freely generated by $\{a, ab\}$. On the other hand, if $\mathcal{B} = \{a, ab, ba\}$, then $\mathcal{B}^*$ is not freely generated by any subset of $\mathcal{A}^*$ (since $ab \cdot a = a \cdot ba$).

Now suppose that we have a *weight function* $w : \mathcal{A} \to R$ (where R is a commutative ring), and define $w(u) = w(a_1) \cdots w(a_n)$ if $u = a_1 \cdots a_n, a_i \in \mathcal{A}$. In particular, $w(1) = 1$. For any subset $\mathcal{C}$ of $\mathcal{A}^*$, define the generating function

$$\mathcal{C}(\lambda) = \sum_{u \in \mathcal{C}} w(u) \lambda^{\ell(u)} \in R[[\lambda]].$$

Thus, the coefficient $f(n)$ of λ^n in $\mathcal{C}(\lambda)$ is $\sum_{u \in \mathcal{C}_n} w(u)$. The following proposition is almost self-evident.

4.7.11 Proposition. *Let $\mathcal{B}$ be a subset of $\mathcal{A}^*$ that freely generates $\mathcal{B}^*$. Then*

$$\mathcal{B}^*(\lambda) = (1 - \mathcal{B}(\lambda))^{-1}.$$

Proof. We have

$$f(n) = \sum_{i_1 + \cdots + i_k = n} \prod_{j=1}^{k} \left(\sum_{u \in \mathcal{B}_{i_j}} w(u) \right).$$

Multiplying by λ^n and summing over all $n \in \mathbb{N}$ yields the result. □

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

As we shall soon see, even the very straightforward Proposition 4.7.11 has interesting applications. But first we seek a result, in the context of the preceding proposition, analogous to Corollary 4.7.3. It turns out that we need the monoid $\mathcal{B}^*$ to satisfy a property stronger than being freely generated by $\mathcal{B}$. This property depends on the way in which $\mathcal{B}^*$ is embedded in $\mathcal{A}^*$, and not just on the abstract structure of $\mathcal{B}^*$. If $\mathcal{B}^*$ is freely generated by $\mathcal{B}$, then we say that $\mathcal{B}^*$ is *very pure* if the following condition, called *unique circular factorization* (UCF), holds:

(UCF) Let $u = a_1 a_2 \cdots a_n \in \mathcal{B}^*$, where $\mathcal{B}^*$ is freely generated by $\mathcal{B}$, with $a_i \in \mathcal{A}$. Thus for unique integers $0 < n_1 < n_2 < \cdots < n_k < n$, we have

$$a_1 a_2 \cdots a_{n_1} \in \mathcal{B}, \;\; a_{n_1+1} a_{n_1+2} \cdots a_{n_2} \in \mathcal{B},$$

$$a_{n_2+1} a_{n_2+2} \cdots a_{n_3} \in \mathcal{B}, \ldots, a_{n_k+1} a_{n_k+2} \cdots a_n \in \mathcal{B}.$$

Suppose that for some $i \in [n]$ we have $a_i a_{i+1} \cdots a_n a_1 \cdots a_{i-1} \in \mathcal{B}^*$. Then $i = n_j + 1$ for some $0 \le j \le k$, where we set $n_0 = 0$.

In other words, if the letters of u are written in clockwise order around a circle, as in Figure 4.9(a), with the initial letter u_1 *not* specified, then there is a unique way of inserting bars between pairs of consecutive letters such that the letter between any two consecutive bars, read clockwise, form a word in $\mathcal{B}$. See Figure 4.9(b).

For example, if $\mathcal{A} = \{a\}$ and $\mathcal{B} = \{aa\}$, then $\mathcal{B}^*$ fails to have UCF since the word $u = aa$ can be "circularly factored" in the two ways shown in Figure 4.10. Similarly, if $\mathcal{A} = \{a, b, c\}$ and $\mathcal{B} = \{abc, ca, b\}$ then $\mathcal{B}^*$ again fails to have UCF since the word $u = abc$ can be circularly factored as shown in Figure 4.11.

Though not necessary for what follows, for the sake of completeness we state the following characterization of very pure monoids. The proof is left to the reader.

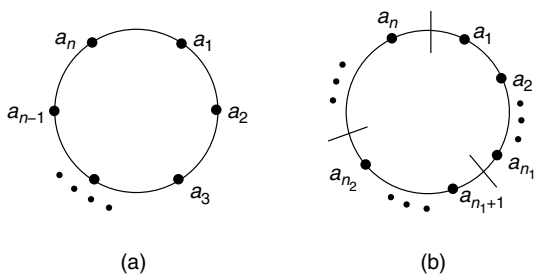

Figure 4.9 Unique circular factorization.

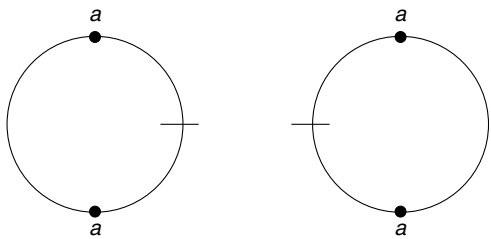

Figure 4.10 Failure of unique circular factorization.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

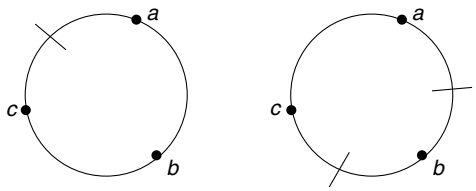

Figure 4.11 Another failure of unique circular factorization.

4.7.12 Proposition. *Suppose that $\mathcal{B}^*$ is freely generated by $\mathcal{B} \subset \mathcal{A}^*$. The following two conditions are equivalent:*

i. $\mathcal{B}^*$ *is very pure.*
ii. If $u \in \mathcal{A}^*$, $v \in \mathcal{A}^*$, $uv \in \mathcal{B}^*$ *and* $vu \in \mathcal{B}^*$, *then* $u \in \mathcal{B}^*$ *and* $v \in \mathcal{B}^*$.

Suppose now that $\mathcal{B}^*$ has UCF. We always compute the length of a word with respect to the alphabet $\mathcal{A}$, so $\mathcal{B}_n^* = \mathcal{B}^* \cap \mathcal{A}_n^*$. If $a_j \in \mathcal{A}$ and $u = a_1 a_2 \cdots a_n \in \mathcal{B}_n^*$, then an $\mathcal{A}^*$-*conjugate* (or *cyclic shift*) of u is a word $a_i a_{i+1} \cdots a_n a_1 \cdots a_{i-1} \in \mathcal{A}_n^*$. Define $g(n) = \sum w(u)$, where the sum is over all *distinct* $\mathcal{A}^*$-conjugates u of words in $\mathcal{B}_n^*$. For instance, if $\mathcal{A} = \{a, b\}$ and $\mathcal{B} = \{a, ab\}$, then

$$\begin{aligned} g(4) &= w(aaaa) + w(aaab) + w(aaba) + w(abaa) + w(baaa) \\ &\quad + w(abab) + w(baba) = w(a)^4 + 4w(a)^3 w(b) + 2w(1)^2 w(b)^2. \end{aligned}$$

Define the generating function

$$\widetilde{\mathcal{B}}(\lambda) = \sum_{n \geq 1} g(n) \lambda^n.$$

4.7.13 Proposition. *Assume $\mathcal{B}^*$ is very pure. Then*

$$\widetilde{\mathcal{B}}(\lambda) = \frac{\lambda \frac{d}{d\lambda} \mathcal{B}(\lambda)}{1 - \mathcal{B}(\lambda)} = \lambda \mathcal{B}^*(\lambda) \frac{d}{d\lambda} \mathcal{B}(\lambda) = \frac{\lambda \frac{d}{d\lambda} \mathcal{B}^*(\lambda)}{\mathcal{B}^*(\lambda)}.$$

Equivalently,

$$\mathcal{B}^*(\lambda) = \exp \sum_{n \geq 1} g(n) \frac{\lambda^n}{n}. \tag{4.41}$$

First Proof. Fix a word $v \in \mathcal{B}$. Let $g_v(n)$ be the sum of the weights of distinct $\mathcal{A}^*$-conjugates $a_i a_{i+1} \cdots a_{i-1}$ of words in $\mathcal{B}_n^*$ such that for some $j \leq i$ and $k \geq i$, we have $a_j a_{j+1} \cdots a_k = v$. Note that j and k are unique by UCF. If $\ell(v) = m$, then clearly $g_v(n) = m w(v) f(n-m)$, where $\mathcal{B}^*(\lambda) = \sum_{n \geq 0} f(n) \lambda^n$. Hence,

$$g(n) = \sum_{v \in \mathcal{B}} g_v(n) = \sum_{m=0}^{n} m b(m) f(n-m),$$

where $b(n) = \sum_{v \in \mathcal{B}_n} w(v)$. We therefore get

$$\widetilde{\mathcal{B}}(\lambda) = \left(\sum_{m \geq 0} m b(m) \lambda^m \right) \mathcal{B}^*(\lambda) = \lambda \mathcal{B}^*(\lambda) \frac{d}{d\lambda} \mathcal{B}(\lambda). \qquad \square$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Our second proof of Proposition 4.7.13 is based on a purely combinatorial lemma involving the relationship between "ordinary" words in $\mathcal{B}^*$ and their $\mathcal{A}^*$-conjugates. This is the general result mentioned after the first proof of Lemma 2.3.4.

4.7.14 Lemma. *Assume that $\mathcal{B}^*$ is very pure. Let $f_k(n) = \sum_u w(u)$, where u ranges over all words in $\mathcal{B}_n^*$ that are a product of k words in $\mathcal{B}$. Let $g_k(n) = \sum_v w(v)$, where v ranges over all distinct $\mathcal{A}^*$-conjugates of the above words u. Then $nf_k(n) = kg_k(n)$.*

Proof. Let A be the set of ordered pairs (u,i), where $u \in \mathcal{B}_n^*$ and u is the product of k words in $\mathcal{B}$, and where $i \in [n]$. Let B be the set of ordered pairs (v,j), where v has the preceding meaning, and where $j \in [k]$. Clearly, $\#A = nf_k(n)$ and $\#B = kg_k(n)$. Define a map $\psi : A \to B$ as follows: Suppose that $u = a_1a_2\cdots a_n = b_1b_2\cdots b_k \in \mathcal{B}_n^*$, where $a_i \in \mathcal{A}$, $b_i \in \mathcal{B}$. Then let

$$\psi(u,i) = (a_ia_{i+1}\cdots a_{i-1}, j),$$

where a_i is one of the letters of b_j. It is easily seen that ψ is a bijection that preserves the weight of the first component, and the proof follows. □

Second Proof of Proposition 4.7.13. By Lemma 4.7.14,

$$nf(n) = \sum_k nf_k(n) = \sum_k kg_k(n). \tag{4.42}$$

The right-hand side of equation (4.42) counts all pairs (v,b_i), where v is an $\mathcal{A}^*$-conjugate of some word $b_1b_2\cdots b_k \in \mathcal{B}_n^*$, with $b_j \in \mathcal{B}$. Thus, v may be written uniquely in the form $b_j'b_{j+1}\cdots b_kb_1b_2\cdots b_{j-1}b_j''$. where $b_j''b_j' = b_j$. Associate with v the ordered pair $(b_ib_{i+1}\cdots b_{i-1}, b_j'b_{j+1}\cdots b_{i-1}b_j'')$. This sets up a bijection between the pairs (v,b_i) above and pairs (y_1,y_2), where $y_1 \in \mathcal{B}^*$, y_2 is an $\mathcal{A}^*$-conjugate of an element of $\mathcal{B}^*$, and $\ell(y_1) + \ell(y_2) = n$. Hence,

$$\sum_k kg_k(n) = \sum_{i=0}^{n} f(i)g(n-i).$$

By equation (4.42), this says $\lambda \frac{d}{d\lambda}\mathcal{B}^*(\lambda) = \mathcal{B}^*(\lambda)\widetilde{\mathcal{B}}(\lambda)$. □

Note that when $\mathcal{B}$ is finite, $\widetilde{\mathcal{B}}(\lambda)$ and $\mathcal{B}^*(\lambda)$ are rational. See Exercise 4.8 for further information on this situation.

4.7.15 Example. Let us take another look at Lemma 2.3.4 from the viewpoint of Lemma 4.7.14. Let $\mathcal{A} = \{0,1\}$ and $\mathcal{B} = \{0,10\}$. An $\mathcal{A}^*$-conjugate of an element of $\mathcal{B}_m^*$ that is also the product of $m-k$ words in $\mathcal{B}$ corresponds to choosing k points, no two consecutive, from a collection of m points arranged in a circle. (The position of the 1's corresponds to the selected points.) Since there are $\binom{m-k}{k}$ permutations of $m-2k$ 0's and k 10's, we have $f_{m-k}(m) = \binom{m-k}{k}$. By Lemma 4.7.14, $g_{m-k}(m) = \frac{m}{m-k}\binom{m-k}{k}$, which is Lemma 2.3.4. Note that $f_1(1) = 0$, not 1, since a single point on a circle is regarded as being adjacent to itself.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

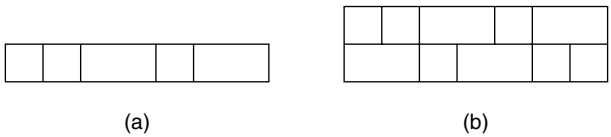

Figure 4.12 A representation of the composition 11212 and the pair (11212, 21211).

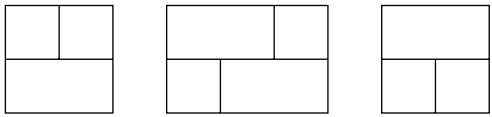

Figure 4.13 The prime blocks corresponding to Figure 4.12(b).

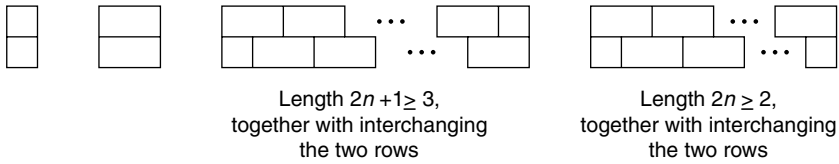

Figure 4.14 The prime blocks.

4.7.16 Example. Recall from Exercise 1.35(c) that the Fibonacci number F_{n+1} counts the number of compositions of n into parts equal to 1 or 2. We may represent such a composition as a row of "bricks" of length 1 or 2; for example, the composition $1+1+2+1+2$ is represented by Figure 4.12(a). An ordered pair (α,β) of such compositions of n is therefore represented by two rows of bricks, as in Figure 4.12(b). The vertical line segments passing from top to bottom serve to "factor" these bricks into blocks of smaller length. For example, Figure 4.13 shows the factorization of Figure 4.12(b). The prime blocks (i.e., those that cannot be factored any further) are given by Figure 4.14. Since there are F_{n+1}^2 pairs (α,β), we conclude that

$$\begin{aligned}\sum_{n\geq 0} F_{n+1}^2\lambda^n &= \left(1-\lambda-\lambda^2-\frac{2\lambda^2}{1-\lambda}\right)^{-1}\\ &= \frac{1-\lambda}{(1+\lambda)(1-3\lambda+\lambda^2)}.\end{aligned}$$

In principle, the same type of reasoning would yield combinatorial evaluations of the generating functions $\sum_{n\geq 0} F_{n+1}^k\lambda^n$, where $k\in\mathbb{P}$. However, it is no longer easy to enumerate the prime blocks when $k\geq 3$. On the contrary, we can reverse the above reasoning to enumerate the prime blocks. For instance, it can be deduced from the explicit formula (4.5) for F_n (or otherwise) that

$$y := \sum_{n\geq 0} F_{n+1}^3\lambda^n = \frac{1-2\lambda-\lambda^2}{1-3\lambda-6\lambda^2+3\lambda^3+\lambda^4}.$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Let $g_3(n)$ be the number of prime blocks of length n and height 3, and set $z = \sum_{n\geq 1} g_3(n)\lambda^n$. Since $y = 1/(1-z)$, we get

$$\begin{aligned} z &= 1 - \frac{1}{y} \\ &= \frac{\lambda + 5\lambda^2 - 3\lambda^3 - \lambda^4}{1 - 2\lambda - \lambda^2} \\ &= \lambda + 7\lambda^2 + 12\lambda^3 + 30\lambda^4 + 72\lambda^5 + 174\lambda^6 + \cdots. \end{aligned}$$

Can the recurrence $g_3(n+2) = 2g_3(n+1) + g_3(n)$ for $n \geq 3$ be proved combinatorially?

As a variant of the preceding one-row case, where the generating function is $F(\lambda) = 1/(1-\lambda-\lambda^2)$, suppose that we have n points on a circle that we cover by bricks of length 1 or 2, where a brick of length i covers i consecutive points. Let $g(n)$ be the number of such coverings. If we choose the second point in clockwise order of each brick of length two, then we obtain a bijection with subsets of the n points, no two consecutive. Hence by Exercise 1.40, we have $g(n) = L_n$. On the other hand, by Proposition 4.7.13 we have

$$\sum_{n\geq 0} g(n)\lambda^n = \frac{\lambda \frac{d}{d\lambda}(\lambda + \lambda^2)}{1 - \lambda - \lambda^2} = \frac{\lambda + 2\lambda^2}{1 - \lambda - \lambda^2}.$$

Moreover, we can build a circular covering by bricks one unit at a time (say in clockwise order) by adding at each step either a brick of length one, the first half of a brick of length two, or the second half of a brick of length two. The rules for specifying what steps can follow what other steps are encoded by the transfer matrix

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

The eigenvalues of A are 0 and $(1 \pm \sqrt{5})/2$, so by equation (4.35) we get

$$g(n) = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

We therefore have a theoretical explanation of why L_n has the simple form $\alpha^n + \beta^n$.

We now derive equations (4.39) and (4.40) using Propositions 4.7.11 and 4.7.13.

4.7.17 Example. Represent a permutation $a_1 a_2 \cdots a_n \in \mathfrak{S}_n$ by drawing n vertices $v_1, \ldots, v_n$ in a line and connecting v_i to v_{a_i} by a directed edge. For instance, the permutation 31542 is represented by Figure 4.15. A permutation $a_1 a_2 \cdots a_n \in \mathfrak{S}_n$ for which $|a_i - i| = 0$ or 1 is then represented as a sequence of the "prime" graphs G and H of Figure 4.16. In other words, if we set $\mathcal{A} = \{a, b, c\}$ amd $G = a$, $H = bc$, then the function $f(n)$ of Example 4.7.9 is just the number of words in

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

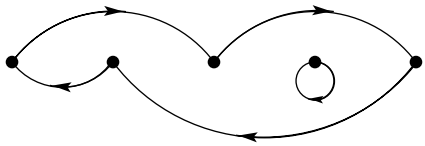

Figure 4.15 A representation of the permutation 31542.

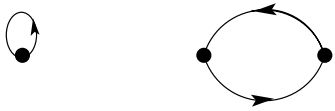

Figure 4.16 The prime graphs for permutations satisfying $|a_i - i| = 0, 1$.

and

Figure 4.17 Graphs of two exceptional permutations.

$\mathcal{B}_n^*$, where $\mathcal{B} = \{a, bc\}$. Setting $w(a) = w(b) = w(c) = 1$, we therefore have by Proposition 4.7.11 that

$$\sum_{n \geq 0} f(n)\lambda^n = \mathcal{B}^*(\lambda) = (1 - \mathcal{B}(\lambda))^{-1},$$

where $\mathcal{B}(\lambda) = w(a)\lambda^{\ell(a)} + w(bc)\lambda^{\ell(bc)} = \lambda + \lambda^2$. Consider now the number $g(n)$ of permutations $a_1 a_2 \cdots a_n \in \mathfrak{S}_n$ such that $a_i = 0, \pm 1 \pmod{n}$. Every cyclic shift of a word in $\mathcal{B}^*$ gives rise to one such permutation. There are exactly two other such permutations ($n \geq 3$), namely, $234 \cdots n1$ and $n123 \cdots (n-1)$, as shown in Figure 4.17. Hence,

$$\begin{aligned} \sum_{n \geq 1} g(n)\lambda^n &= \frac{\lambda \frac{d}{d\lambda}\mathcal{B}(\lambda)}{1 - \mathcal{B}(\lambda)} + \sum_{n \geq 1} 2\lambda^n \\ &= \frac{\lambda(1 + 2\lambda)}{1 - \lambda - \lambda^2} + \frac{2\lambda}{1 - \lambda}, \end{aligned}$$

provided of course we suitably interpret $g(1)$ and $g(2)$.

4.7.18 Example. Let $f(n)$ be the number of permutations $a_1 a_2 \cdots a_n \in \mathfrak{S}_n$ with $a_i - i = \pm 1$ or ± 2. To use the transfer-matrix method would be quite unwieldy, but the factorization method is very elegant. A permutation enumerated by $f(n)$ is represented by a sequence of graphs of the types shown in Figure 4.18. Hence,

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

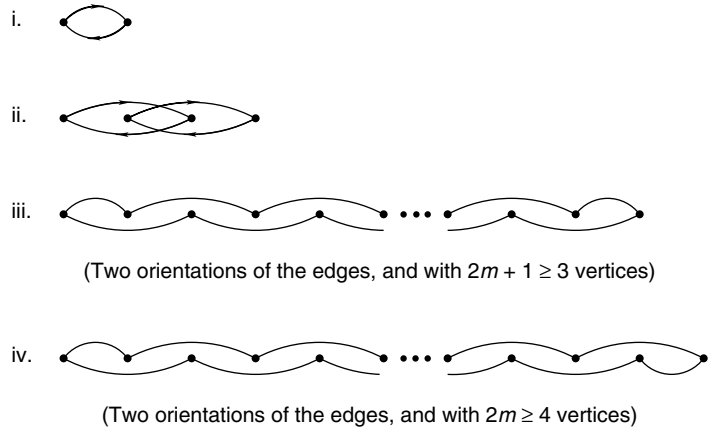

Figure 4.18 The prime graphs for permutations satisfying $a_i - i = \pm 1$ or ± 2.

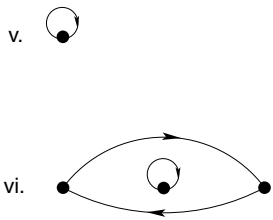

Figure 4.19 Two additional prime graphs.

$\mathcal{B}(\lambda) = \lambda^2 + \lambda^4 + 2\sum_{m\geq 3} \lambda^m$, and

$$\sum_{n\geq 0} f(n)\lambda^n = \mathcal{B}^*(\lambda) = \left(1 - \lambda^2 - \lambda^4 - \frac{2\lambda^3}{1-\lambda}\right)^{-1}$$
$$= \frac{1-\lambda}{1-\lambda-\lambda^2-\lambda^3-\lambda^4+\lambda^5}.$$

Suppose now that we also allow $a_i - i = 0$. Thus, let $f^*(n)$ be the number of permutations $a_1 a_2 \cdots a_n \in \mathfrak{S}_n$ with $a_i - i = \pm 1, \pm 2$, or 0. There are exactly two new elements of $\mathcal{B}$ introduced by this change, shown in Figure 4.19. Hence,

$$\sum_{n\geq 0} f^*(n)\lambda^n = \left(1 - \lambda - \lambda^2 - \lambda^3 - \lambda^4 - \frac{2\lambda^3}{1-\lambda}\right)^{-1}$$
$$= \frac{1-\lambda}{1-2\lambda-3\lambda^3+\lambda^5}.$$

4.7.19 Example (k-discordant permutations). In Section 2.3, we discussed the problem of counting the number $f_k(n)$ of *k-discordant permutations* $a_1 a_2 \cdots a_n \in$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

$\mathfrak{S}_n$, that is, $a_i - i \not\equiv 0, 1, \ldots, k-1 \pmod{n}$. We saw that

$$f_k(n) = \sum_{i=0}^{n} (-1)^i r_i(n)(n-i)!,$$

where $r_i(n)$ is the number of ways of placing i nonattacking rooks on the board

$$B_n = \{(r,s) \in [n] \times [n] : s - r \equiv 0, 1, \ldots, k-1 \pmod{n}\}.$$

The evaluation of $r_i(n)$, or equivalently the rook polynomial $R_n(x) = \sum_i r_i(n) x^i$, can be accomplished by methods analogous to those used to determine $g_S(n)$ in Proposition 4.7.10. The transfer-matrix method will tell us the general form of the generating function $F_k(x,y) = \sum_{n \geq 1} R_n(x) y^n$ (suitably interpreting $R_n(x)$ for $n < k$), whereas the factorization method will enable us to compute $F_k(x,y)$ easily when k is small.

First, we consider the transfer-matrix approach. We begin with the first row of B_n and either place a rook in a square of this row or leave the row empty. We then proceed to the second row, either placing a rook that doesn't attack a previously placed rook or leaving the row empty. If we continue in this manner, then the options available to us at the ith row depend on the configuration of the rooks on the previous $k-1$ rows. Hence, for the vertices of our digraph D_k, we take all possible placements of nonattacking rooks on the first $k-1$ rows of B_n (where $n \geq 2k-1$ to allow all possibilities). An edge connects two placements P_1 and P_2 if the last $k-2$ rows are identical to the first $k-2$ rows of P_2, and if we overlap P_1 and P_2 in this way (yielding a configuration with k rows), then the rooks remain nonattacking. For instance, D_2 is given by Figure 4.20. There is no arrow from v_2 to v_3 since their overlap would be shown in Figure 4.21(a), which is not allowed. Similarly D_3 has 14 vertices, a typical edge being shown in Figure 4.21(b). If we overlap these two vertices, then we obtain the legal configuration shown in Figure 4.21(c). Define the weight $w(P_1, P_2)$ of an edge (P_1, P_2) to be $x^{\nu(P_2)}$, where $\nu(P_2)$ is the number of rooks in the last row of P_2. It is then clear that a closed walk Γ of length n and weight $x^{\nu(\Gamma)}$ in D_k corresponds to a placement of $\nu(\Gamma)$ nonattacking rooks on B_n (provided $n \geq k$). Hence, if A_k is the adjacency matrix of D_k with respect to the weight function w, then

$$R_n(x) = \operatorname{tr} A_k^n, \quad n \geq k.$$

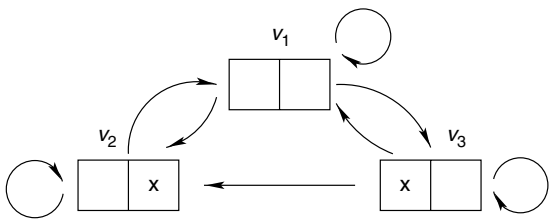

Figure 4.20 The nonattacking rook digraph D_2.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

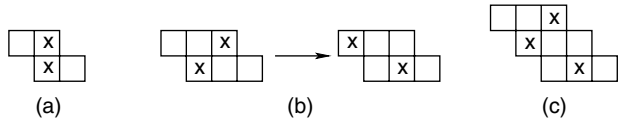

Figure 4.21 Nonedges and edges in the digraphs D_2 and D_3.

Thus, if we set $Q_k(\lambda) = \det(I - \lambda A_k) \in \mathbb{C}[x,\lambda]$, then by Corollary 4.7.3 we conclude

$$\sum_{n\geq 1} R_n(x)\lambda^n = -\frac{\lambda Q_k'(\lambda)}{Q_k(\lambda)}. \tag{4.43}$$

For instance, when $k = 2$ (the "problème des ménages") then with the vertex labeling given by Figure 4.20, we read off from Figure 4.20 that

$$A_k = \begin{bmatrix} 1 & x & x \\ 1 & x & 0 \\ 1 & x & x \end{bmatrix},$$

so that

$$Q_2(\lambda) = \det \begin{bmatrix} 1-\lambda & -\lambda x & -\lambda x \\ -\lambda & 1-\lambda x & 0 \\ -\lambda & -\lambda x & 1-\lambda x \end{bmatrix}$$

$$= 1 - \lambda(1+2x) + \lambda^2 x^2.$$

Therefore,

$$\sum_{n\geq 1} R_n(x)\lambda^n = \frac{\lambda(1+2x) - 2\lambda^2 x^2}{1-\lambda(1+2x)+\lambda^2 x^2} \quad (k=2).$$

The preceding technique, applied to the case $k = 3$, would involve the determinant of a 14×14 matrix. The factorization method yields a much easier derivation. Regard a placement P of nonattacking rooks on B_n (or on any subset of $[n] \times [n]$) as a digraph with vertices $1, 2, \ldots, n$, and with a directed edge from i to j if a rook is placed in row i and column j. For instance, the placement shown in Figure 4.22(a) corresponds to the digraph shown in Figure 4.22(b). In the case $k = 2$, every such digraph is a sequence of the primes shown in Figure 4.23(a), together with the additional digraph shown in Figure 4.23(b). If we weight such a digraph with q edges by x^q, then by Proposition 4.7.13 there follows

$$\sum_{n\geq 1} R_n(x)\lambda^n = \frac{\lambda \frac{d}{d\lambda}\mathcal{B}(\lambda)}{1-\mathcal{B}(\lambda)} + \sum_{n\geq 2} x^n \lambda^n, \tag{4.44}$$

where

$$\mathcal{B}(\lambda) = x\lambda + \sum_{i\geq 1} x^{i-1}\lambda^i$$

$$= x\lambda + \frac{\lambda}{1-x\lambda}.$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

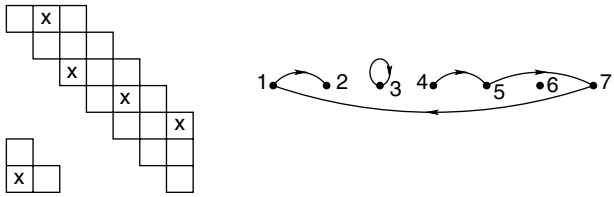

Figure 4.22 A rook placement and its corresponding digraph.

Figure 4.23 Prime digraphs and an exception for $k = 2$.

Figure 4.24 A complicated prime digraph.

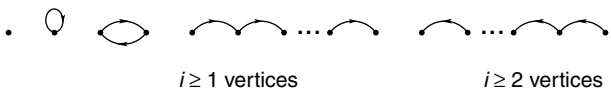

Figure 4.25 The prime digraphs for B'_n.

Figure 4.26 The two exceptions for B'_n.

This yields the same answer as before, except that we get the correct value $R_1(x) = 1 + x$ rather than the spurious value $R_1(x) = 1 + 2x$. To obtain $R_1(x) = 1 + 2x$, we would have to replace $\sum_{n\geq 2} x^n\lambda^n$ in equation (4.44) by $\sum_{n\geq 1} x^n\lambda^n$. Thus in effect, we are counting the first digraph of Figure 4.23(a) twice, once as a prime and once as an exception.

When the foregoing method is applied to the case $k = 3$, it first appears extremely difficult because of the complicated set of prime digraphs that can arise, as in Figure 4.24. A simple trick eliminates this problem; namely, instead of using the board $B_n = \{(j, j), (j, j + 1), (j, j + 2) \,(\mathrm{mod}\, n)\}$, use instead $B'_n = \{(j, j-1), (j, j), (j, j+1) \,(\mathrm{mod}\, n)\}$. Clearly, B_n and B'_n are isomorphic and therefore have the same rook polynomials, but surprisingly B'_n has a much simpler set of prime placements than B_n. The primes for B'_n are given by Figure 4.25. In addition, there are exactly two exceptional placements, shown in Figure 4.26. Hence,

$$\sum_{n\geq 1} R_n(x)\lambda^n = \frac{\lambda \frac{d}{d\lambda}\mathcal{B}(\lambda)}{1 - \mathcal{B}(\lambda)} + 2\sum_{n\geq 3} x^n\lambda^n, \tag{4.45}$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

where

$$\mathcal{B}(\lambda) = \lambda + x\lambda + x^2\lambda^2 + 2\sum_{i\geq 2} x^{i-1}\lambda^i$$
$$= \lambda + x\lambda + x^2\lambda^2 + \frac{2x\lambda^2}{1-x\lambda}.$$

If we replace $\sum_{n\geq 3} x^n\lambda^n$ in equation (4.45) by $\sum_{n\geq 1} x^n\lambda^n$ (causing $R_1(x)$ and $R_2(x)$ to be spurious), then after simplification there results

$$\sum_{n\geq 1} R_n(x)\lambda^n = \frac{\lambda(1+2x+2x\lambda-3x^3\lambda^2)}{1-(1+2x)\lambda-x\lambda^2+x^3\lambda^3} + \frac{x\lambda}{1-x\lambda}.$$

4.7.5 Some Sums Over Compositions

Here we will give a more complex use of the transfer-matrix than treated previously.

A *polyomino* is a finite union P of unit squares in the plane such that the vertices of the squares have integer coordinates, and P is connected and has no finite cut set. Two polynominoes will be considered *equivalent* if there is a translation that transforms one into the other (reflections and rotations not allowed). A polynomino P is *horizontally convex* (or HC) if each "row" of P is an unbroken line of squares, that is, if L is any line segment parallel to the x-axis with its two endpoints in P, then $L \subset P$. Let $f(n)$ be the number of HC-polyominoes with n squares. Thus $f(1) = 1$, $f(2) = 2$, $f(3) = 6$, as shown by Figure 4.27. Suppose that we build up an HC-polyomino one row at a time, starting at the bottom. If the ith row has r squares, then we can add an $(i+1)$-st row of s squares in $r+s-1$ ways. It follows that

$$f(n) = \sum (n_1+n_2-1)(n_2+n_3-1)\cdots(n_s+n_{s+1}-1), \tag{4.46}$$

where the sum is over all 2^{n-1} compositions $n_1+n_2+\cdots+n_{s+1}$ of n (where the composition with $s=0$ contributes 1 to the sum). This formula suggests studying the more general sum, over all compositions $n_1+n_2+\cdots+n_{s+k-1}=n$ with $s\geq 0$, given by

$$f(n) = \sum (f_1(n_1)+f_2(n_2)+\cdots+f_k(n_k))(f_1(n_2)+f_2(n_3)+\cdots+f_k(n_{k+1}))$$
$$\cdots(f_1(n_s)+f_2(n_{s+1})+\cdots+f_k(n_{s+k-1})), \tag{4.47}$$

where $f_1,\ldots,f_k$ are arbitrary functions from $\mathbb{P}\to\mathbb{C}$ (or to any commutative ring R). We make the convention that the term in equation (4.47) with $s=0$ is 1. The

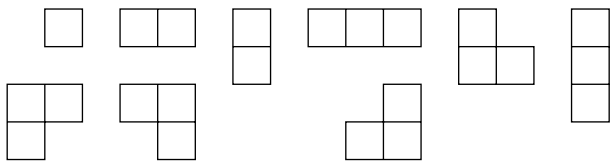

Figure 4.27 Horizontally convex polyominoes with at most three squares.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

situation (4.46) corresponds to $f_1(m) = m + \alpha$ and $f_2(m) = m - \alpha - 1$ for any fixed $\alpha \in \mathbb{C}$.

It is surprising that the transfer-matrix method can be used to write down an explicit expression for the generating function $F(x) = \sum_{n \geq 1} f(n)x^n$ in terms of the generating functions $F_i(x) = \sum_{n \geq 1} f_i(n)x^n$. We may compute a typical term of the product appearing in equation (4.47) by first choosing a term $f_{i_1}(n_{i_1})$ from the first factor $\phi_1 = f_1(n_1) + f_2(n_2) + \cdots + f_k(n_k)$, then a term $f_{i_2}(n_{i_2+1})$ from the second factor $\phi_2 = f_1(n_2) + f_2(n_3) + \cdots + f_k(n_{k+1})$, and so on, and finally multiplying these terms together.

Alternatively we could have obtained this term by first deciding from which factors we choose a term of the form $f_{i_1}(n_1)$, then deciding from which factors we choose a term of the form $f_{i_2}(n_2)$, and so on. Once we've chosen the terms $f_{i_j}(n_{i_j})$, the possible choices for $f_{i_{j+1}}(n_{i_{j+1}})$ are determined by which of the $k-1$ factors $\phi_{j-k+2}, \phi_{j-k+3}, \ldots, \phi_j$ we have already chosen a term from. Hence, define a digraph D_k with vertex set $V = \{(\varepsilon_1, \ldots, \varepsilon_{k-1}) : \varepsilon_i = 0 \text{ or } 1\}$. The vertex $(\varepsilon_1, \ldots, \varepsilon_{k-1})$ indicates that we have already chosen a term from ϕ_{j-k+l} if and only if $\varepsilon_{l-1} = 1$. Draw an edge from $(\varepsilon_1, \ldots, \varepsilon_{k-1})$ to $(\varepsilon'_1, \ldots, \varepsilon'_{k-1})$ if it is possible to choose terms of the form $f_{i_j}(n_{j+1})$ consistent with $(\varepsilon_1, \ldots, \varepsilon_{k-1})$, and then of the form $f_{i_{j+1}}(n_{j+1})$ consistent with $(\varepsilon'_1, \ldots, \varepsilon'_{k-1})$ and our choice of $f_{i_j}(n_j)$'s. Specifically, this means that $(\varepsilon'_1, \ldots, \varepsilon'_{k-1})$ can be obtained from $(\varepsilon_2, \ldots, \varepsilon_{k-1}, 0)$ by changing some 0's to 1's. It now follows that a path in D_k of length $s+k-1$ that starts at $(1, 1, \ldots, 1)$ (corresponding to the fact that when we first pick out terms of the form $f_{i_1}(n_{i_1})$, we cannot choose from nonexistent factors prior to ϕ_1) and ends at $(0, 0, \ldots, 0)$ (since we cannot have chosen from nonexistent factors following ϕ_s) corresponds to a term in the expansion of $\phi_1\phi_2\cdots\phi_s$. For instance, if $k = 3$, then the term $f_3(n_3)f_1(n_2)f_1(n_3)f_2(n_5)f_3(n_7)$ in the expansion of $\phi_1\phi_2\cdots\phi_5$ corresponds to the path shown in Figure 4.28. The first edge in the path corresponds to choosing no term $f_{i_1}(n_1)$, the second edge to choosing $f_1(n_2)$, the third to $f_1(n_3)f_3(n_3)$, the fourth to no term $f_{i_4}(n_4)$, the fifth to $f_2(n_5)$, the sixth to no term $f_{i_6}(n_6)$, and the seventh to $f_3(n_7)$.

We now have to consider the problem of weighting the edges of D_k. For definiteness, consider for example the edge e from $v = (0,0,1,0,0,1)$ to $v' = (1,1,0,1,1,0)$. This means that we have chosen a factor $f_3(m)f_6(m)f_7(m)$, as illustrated schematically by

	7	**6**	**5**	**4**	**3**	**2**	**1**
$\boldsymbol{v}$	0	0	1	0	0	1	
$\boldsymbol{v'}$		1	1	0	1	1	0

If $2 \leq i \leq k-1$, then we include $f_i(m)$ when column i is given by $\binom{0}{1}$. We include $f_k(m)$ if the first entry of v is 0, and we include $f_1(m)$ if the last entry of v' is 1.

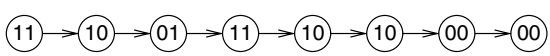

Figure 4.28 A path in the digraph D_3.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

We are free to choose m to be any positive integer. Thus, if we weight edge e with the generating function

$$\sum_{m\geq 1} f_3(m) f_6(m) f_7(m) x^m = F_3 * F_6 * F_7,$$

where $*$ denotes the Hadamard product, then the total weight of a path from $(1,1,\ldots,1)$ to $(0,0,\ldots,0)$ is precisely the contribution of this path to the generating function $F(x)$. Note that in the case of an edge e where we pick *no* terms of the $f_i(m)$ for fixed m, then we are contributing a factor of 1, so that the edge must be weighted by $\sum_{m\geq 1} x^m = x/(1-x)$, which we will denote as $J(x)$. Since there is no need to keep track of the length of the path, it follows from Theorem 4.7.2 that $F(x) = F_{ij}(D_k, 1)$, where i is the index of $(1,1,\ldots,1)$ and j of $(0,0,\ldots,0)$. (In general, it is meaningless to set $\lambda = 1$ in $F_{ij}(D,\lambda)$, but here the weight function has been chosen so that $F_{ij}(D_k,1)$ is a well-defined formal power series. Of course, if we wanted to do so, we could consider the more refined generating function $F_{ij}(D_k,\lambda)$, which keeps track of the number of parts of each composition.)

We can sum up our conclusions in the following result.

4.7.20 Proposition. *Let A_k be the following $2^{k-1}\times 2^{k-1}$ matrix whose rows and columns are indexed by $V = \{0,1\}^{k-1}$. If $v = (\varepsilon_1,\ldots,\varepsilon_{k-1})$, $v' = (\varepsilon'_1,\ldots,\varepsilon'_{k-1}) \in V$, then define the (v,v')-entry of A_k as follows:*

$$(A_k)_{vv'} = \begin{cases} 0, & \text{if for some } 1\leq i\leq k-2, \text{ we have } \varepsilon_{i+1}=1, \\ & \text{and } \varepsilon'_i = 0, \\ F_{i_1} * \cdots * F_{i_r}, & \text{otherwise, where } \{i_1,\ldots,i_r\} = \{i : \varepsilon_{k-i+1} = 0 \text{ and} \\ & \varepsilon'_{k-i} = 1\}, \text{ and where we set } \varepsilon_k = 0,\ \varepsilon'_0 = 1, \text{ and an} \\ & \text{empty Hadamard product equal to } J = x/(1-x). \end{cases}$$

Let B_k be the matrix obtained by deleting row $(0,0,\ldots,0)$ and column $(1,1,\ldots,1)$ from $I - A_k$ (where I is the identity matrix) and multiplying by the appropriate sign. Then the generating function $F(x) = \sum_{n\geq 1} f(n)x^n$, as defined by equation (4.47), is given by

$$F(x) = \frac{\det B_k}{\det(I - A_k)}.$$

In particular, if each $F_i(x)$ is rational, then $F(x)$ is rational, by Proposition 4.2.5.

Here are some small examples. When $k = 2$, we have D_2 given by Figure 4.29, while

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

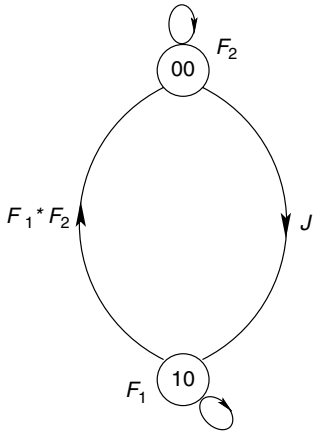

Figure 4.29 The digraph D_2.

$$A_2 = \begin{bmatrix} F_2 & F_1 * F_2 \\ J & F_1 \end{bmatrix}, \quad B_2 = [J],$$

$$F(x) = \frac{J}{(1-F_1)(1-F_2) - J \cdot (F_1 * F_2)}. \tag{4.48}$$

In the original problem of enumerating HC-polyominoes,

$$F_1(x) = \sum_{n \geq 1} n x^n = x/(1-x)^2,$$

$$F_2(x) = \sum_{n \geq 1} (n-1) x^n = x^2/(1-x)^2,$$

$$(F_1 * F_2)(x) = \sum_{n \geq 1} n(n-1) x^n = 2x^2/(1-x)^3,$$

yielding

$$F(x) = \frac{x/(1-x)}{\left(1 - \dfrac{x}{(1-x)^2}\right)\left(1 - \dfrac{x^2}{(1-x)^2}\right) - \dfrac{x}{1-x} \cdot \dfrac{2x^2}{(1-x)^3}}$$

$$= \frac{x(1-x)^3}{1 - 5x + 7x^2 - 4x^3}.$$

It is by no means obvious that $f(n)$ satisfies the recurrence

$$f(n+3) = 5f(n+2) - 7f(n+1) + 4f(n), \quad n \geq 2, \tag{4.49}$$

and it is difficult to give a combinatorial proof.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

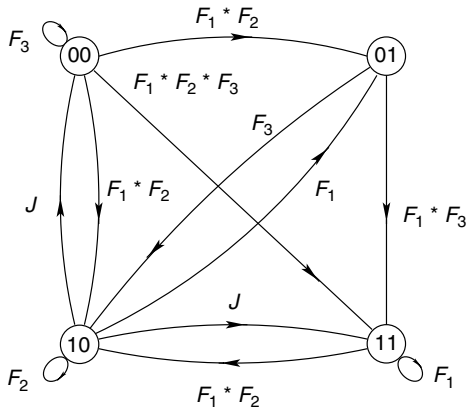

Figure 4.30 The digraph D_3.

Finally, let us consider the case $k = 3$. Figure 4.30 shows D_3, while

$$A_3 = \begin{bmatrix} F_3 & F_1 * F_3 & F_2 * F_3 & F_1 * F_2 * F_3 \\ 0 & 0 & F_3 & F_1 * F_3 \\ J & F_1 & F_2 & F_1 * F_2 \\ 0 & 0 & J & F_1 \end{bmatrix},$$

$$B_3 = \begin{bmatrix} 0 & 1 & -F_3 \\ -J & -F_1 & 1 - F_2 \\ 0 & 0 & J \end{bmatrix},$$

$$F(x) = \frac{J^2}{\det(I - A_3)},$$

where

$$\begin{aligned} \det(I - A_3) = {} & (1 - F_1)(1 - F_3)(1 - F_2 - F_1 F_3) \\ & - J(1 - F_1)(F_2 * F_3 + F_3(F_1 * F_3)) \\ & - J(1 - F_3)(F_1 * F_2 + F_1(F_1 * F_3)) \\ & - J^2((F_1 * F_3)^2 + F_1 * F_2 * F_3). \end{aligned}$$

Notes

The basic theory of rational generating functions in one variable belongs to the calculus of finite differences. Charles Jordan [4.25] ascribes the origin of this calculus to Brook Taylor in 1717 but states that the real founder was James Stirling in 1730. The first treatise on the subject was written by Euler in 1755, where the notation Δ for the difference operator was introduced. It would probably be an arduous task to ascertain the precise origin of the various parts of Theorem 4.1.1, Corollary 4.2.1,

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Proposition 4.2.2, Proposition 4.2.5, Corollary 4.3.1, and Proposition 4.4.1. The reader interested in this question may wish to consult the extensive bibliography in Nörlund [4.39].

The reciprocity result Proposition 4.2.3 seems to be of more recent vintage. It is attributed by E. Ehrhart [4.12, p. 21] to T. Popoviciu [4.44, p. 8]. However, Proposition 4.2.3 is actually a special case of a result of G. Pólya [4.42, §44, p. 609]. It is also a special case of the less general (than Pólya) result of R. M. Robinson [4.47, §3].

The operation of Hadamard product was introduced by J. Hadamard [4.16], who proved Proposition 4.2.5. This result fails for power series in more than one variable, as observed by A. Hurwitz [4.20].

Methods for dealing with quasipolynomials such as $\overline{p}_k(n)$ in Example 4.4.2 were developed by Herschel, Cayley, Sylvester, Glaisher, Bell, and others. For references, see [2.3, §2.6]. Some interesting properties of quasipolynomials are given by I. G. Macdonald as an appendix to the monograph [4.14, pp. 145–155] of Ehrhart and by N. Li and S. Chen [4.30, §3].

The theory of linear homogeneous diophantine equations developed in Section 4.5 was investigated in the weaker context of Ehrhart quasipolynomials by E. Ehrhart beginning around 1955. (It is remarkable that Ehrhart did most of his work as a teacher in a *lycée* and did not receive his Ph.D. until 1966 at the age of 59 or 60.) Ehrhart's work is collected together in his monograph [4.14], which contains detailed references. Some aspects of Ehrhart's work were corrected, streamlined, and expanded by I. G. Macdonald [4.34][4.35].

The extension of Ehrhart's work to linear homogeneous diophantine equations appeared in Stanley [4.52] and is further developed in [4.54][4.57]. In these references, commutative algebra is used as a fundamental tool. The approach given here in Section 4.5 is more in line with Ehrhart's original work. Reference [4.57] is primarily concerned with *inhomogeneous* equations and the extension of Theorem 4.5.14 (reciprocity) to this case. A more elementary but less comprehensive approach to inhomogeneous equations and reciprocity is given in [4.53, §§8–11]; see also Exercises 4.34 and 4.35. For further background information on convex polytopes, see Ziegler [3.97].

Other approaches toward "Ehrhart theory" appear in M. Beck and F. Sottile [4.5], P. McMullen [4.37], S. V. Sam [4.48], S. V. Sam and K. M. Woods [4.49], and R. Stanley [4.56]. A nice exposition of Ehrhart theory and related topics at the undergraduate level is given by M. Beck and S. Robins [4.4].

The triangulation defined in the proof of Lemma 4.5.1 is called the *pulling triangulation* and has several other descriptions. See for instance Beck–Robins [4.4, Appendix] and De Loera–Rambau–Santos Leal [4.11, §4.3.2]. Our description of the pulling triangulation follows Stanley [4.56, Lemma 1.1].

The study of "magic squares" (as defined in Section 4.6) was initiated by MacMahon [4.36][1.55, §404–419]. In the first of these two references MacMahon writes down in Art. 129 a multivariate generating function for all 3×3 magic squares, though he doesn't explictly write down a formula for $H_3(r)$. In the second

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

reference he does give the formula in §407. For MacMahon's proof, see Exercise 2.15. Proposition 4.6.2 was conjectured by H. Anand, V. C. Dumir, and H. Gupta [4.1] and was first proved by Stanley [4.52]. Ehrhart [4.13] also gave a proof of Proposition 4.6.2 using his methods. An elementary proof (essentially an application of the transfer-matrix method) of part of Proposition 4.6.2 was given by J. H. Spencer [4.51]. The fundamental Lemma 4.6.1 on which Proposition 4.6.2 rests is due to Garrett Birkhoff [4.6]. It was rediscovered by J. von Neumann [4.61] and is sometimes called the "Birkhoff–von Neumann theorem." The proof given here is that of von Neumann. There are several papers earlier than that of Birkhoff that are equivalent to or easily imply the Birkhoff–von Neumann theorem. Perhaps the first such results are two nearly identical papers, one in German and one in Hungarian, by D. König [4.27][4.28].

L. Carlitz [4.8, p. 782] conjectured that Proposition 4.6.4 is valid for some *constant* $Q_n(r)$ and proved this fact for $n \leq 4$. The value of $G_5(r)$ given after Proposition 4.6.4 shows that Carlitz's conjecture is false for $n = 5$. Proposition 4.6.4 itself was first proved by Stanley [4.52], and a refinement appears in [4.54, Thm. 5.5]. In particular, it was shown that

$$\deg Q_n(r) \leq \begin{cases} \binom{n-1}{2} - 1, & n \text{ odd}, \\ \binom{n-2}{2} - 1, & n \text{ even}, \end{cases} \tag{4.50}$$

and it was conjectured that equality holds for all n. This conjecture was proved by R.-Q. Jia, [4.23][4.24]. The values of $F_n(\lambda)$ (given for $n \leq 5$ preceding Lemma 4.6.3) were computed for $n \leq 6$ by D. M. Jackson and G. H. J. van Rees [4.21]. They were extended to $n \leq 9$ by M. Beck and D. Pixton [4.3]. The values for $G_n(\lambda)$ for $n \leq 5$ appearing after Proposition 4.6.4 were first given in [4.54].

Example 4.6.15(a) is a classical result of G. A. Pick [4.41]. The extension (b) to three dimensions is due to J. E. Reeve [4.45], while the general case (c) (or even more general Corollary 4.6.14) is due to Macdonald [4.34].

The connection between the powers A^n of the adjacency matrix A of a digraph D and the counting of walks in D (Theorem 4.7.1) is part of the folklore of graph theory. An extensive account of the adjacency matrix A is given by D. M. Cvetković, M. Doob, and H. Sachs [4.10]; see §1.8 and §7.5 in particular for its use in counting walks. We should also mention that the transfer-matrix method is essentially the same as the theory of finite Markov chains in probability theory. For a noncommutative version of the transfer-matrix method, see §6.5 of volume 2 of the present text.

The transfer-matrix method has been used with great success by physicists in the study of phase transitions in statistical mechanics. See for instance Baxter [4.2] and Percus [4.40] for further information.

For more information on Example 4.7.7, see Exercise 4.40 and the references given there. For work related to Examples 4.7.9, 4.7.17, and 4.7.18, see Lagrange [4.29] and Metropolis, Stein, and Stein [4.38], and the references given there. These approaches are less combinatorial than ours.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Our discussion of factorization in free monoids merely scratched the surface of an extensive subject. An excellent overall reference is Lothaire [4.31], from which we have taken most of our terminology and notation. Sequels appear in [4.32][4.33]. Other interesting references include Cohn [4.9] and Fliess [4.15]. The application to summing $\sum F_{n+1}^2 \lambda^n$ (Example 4.7.16) appears in Shapiro [4.50]. For more information on powers of Fibonacci numbers, see Jarden and Motzkin [4.22], Hathaway and Brown [4.17], Riordan [4.46], Carlitz [4.7], and Horadam [4.19].

Two topics with close connections to factorization in monoids are the combinatorial theory of orthogonal polynomials and the theory of heaps. Basic references are two papers [4.59][4.60] of X. G. Viennot.

The first published statement for the generating function $F(x)$ for HC-polyominoes appearing before equation (4.49) seems to be due to H. N. V. Temperley [4.58]. Earlier the recurrence (4.49) was found by Pólya in 1938 but was unpublished by him until 1969 [4.43]. A proof of the more general equation (4.48) is given by Klarner [4.26], while an algebraic version of this proof appears in Stanley [4.55, Ex. 4.2]. The elegant transfer-matrix approach given here was suggested by I. M. Gessel. The combinatorial proof of equation (4.49) alluded to after (4.49) is due to D. R. Hickerson [4.18].

Bibliography

[1] H. Anand, V. C. Dumir, and H. Gupta, A combinatorial distribution problem, *Duke Math. J.* **33** (1966), 757–770.

[2] R. J. Baxter, *Exactly Solved Models in Statistical Mechanics*, Academic Press, London/New York, 1982.

[3] M. Beck and D. Pixton, The Ehrhart polynomial of the Birkhoff polytope, *Discrete Comput. Geom.* **30** (2003), 623–637.

[4] M. Beck and S. Robins, *Computing the Continuous Discretely: Integer-Point Enumeration in Polyhedra*, Springer-Verlag, New York, 2007.

[5] M. Beck and F. Sottile, Irrational proofs for three theorems of Stanley, *European J. Combinatorics* **28** (2007), 403–409.

[6] G. Birkhoff, Tres observaciones sobre el algebra lineal, *Univ. Nac. Tucamán Rev. Ser. (A)* **5** (1946), 147–150.

[7] L. Carlitz, Generating functions for powers of a certain sequence of numbers, *Duke Math. J.* **29** (1962), 521–537.

[8] L. Carlitz, Enumeration of symmetric arrays, *Duke Math. J.* **33** (1966), 771–782.

[9] P. M. Cohn, Algebra and language theory, *Bull. London Math. Soc.* **7** (1975), 1–29.

[10] D. M. Cvetković, M. Doob, and H. Sachs, *Spectra of Graphs*, 3rd ed., Johann Ambrosius Barth, Heidelberg, 1995.

[11] J. A. De Loera, J. Rambau, and F. Santos Leal, *Triangulations*, Springer-Verlag, Berlin, 2010.

[12] E. Ehrhart, Sur les problème de géométrie diophantienne linéaire I, II, *J. Reine Angew. Math.* **226** (1967), 1–29, and **227** (1967), 25–49. Correction, **231** (1968), 220.

[13] E. Ehrhart, Sur les carrés magiques, *C. R. Acad. Sci. Paris* **227 A** (1973), 575–577.

[14] E. Ehrhart, *Polynômes arithmétiques et Méthode des Polyèdres en Combinatoire*, International Series of Numerical Mathematics, vol. 35, Birkhäuser, Basel/Stuttgart, 1977.

[15] M. Fliess, Sur divers produits de séries formelles, *Bull. Soc. Math. France* **102** (1974), 181–191.
[16] J. S. Hadamard, Théorèm sur les séries entières, *Acta Math.* **22** (1899), 55–63.
[17] D. K. Hathaway and S. L. Brown, Fibonacci powers and a fascinating triangle, *College Math. J.* **28** (1997), 124–128.
[18] D. R. Hickerson, Counting horizontally convex polyominoes, *J. Integer Sequences* **2** (1999), article 99.1.8.
[19] A. F. Horadam, Generating functions for powers of a certain generalized sequence of numbers, *Duke Math. J.* **32** (1965), 437–446.
[20] A. Hurwitz, Sur une théorème de M. Hadamard, *C. R. Acad. Sci. Paris* **128** (1899), 350–353.
[21] D. M. Jackson and G. H. J. van Rees, The enumeration of generalized double stochastic nonnegative integer square matrices, *SIAM J. Comput.* **4** (1975), 474–477.
[22] D. Jarden and T. Motzkin, The product of sequences with a common linear recursion formula of order 2 (Hebrew with English summary), *Riveon Lematematika* **3** (1949), 25–27, 38.
[23] R.-Q. Jia, Symmetric magic squares and multivariate splines, *Linear Algebra Appl.* **250** (1997), 69–103.
[24] R.-Q. Jia, Multivariate discrete splines and linear Diophantine equations, *Trans. Amer. Math. Soc.* **340** (1993), 179–198.
[25] C. Jordan, *Calculus of Finite Differences*, 3rd ed., Chelsea, New York, 1965.
[26] D. A. Klarner, A combinatorial formula involving the Fredholm integral equation, *J. Combinatorial Theory* **5** (1968), 59–74.
[27] D. König, Grafok és alkalmaszásuk és a halmazok elméletére, *Mat. Természz. Ért.* **34** (1916), 104–119.
[28] D. König, Über Graphen und ihre Anwendung auf Determinantentheorie and Mengenlehre, *Math. Ann.* **77** (1916), 453–465.
[29] M. R. Lagrange, Quelques résultats dans la métrique des permutations, *Ann. scient. Éc. Norm. Sup.* **79** (1962), 199–241.
[30] N. Li and S. Chen, On Popoviciu type formulas for generalized restricted partition function, `arXiv:0709.3571`.
[31] M. Lothaire, *Combinatorics on Words*, Addison-Wesley, Reading, Mass., 1983; reprinted by Cambridge University Press, Cambridge, 1997.
[32] M. Lothaire, *Algebraic Combinatorics on Words*, Encyclopedia of Mathematics and Its Applications **90**, Cambridge University Press, Cambridge, 2002.
[33] M. Lothaire, *Applied Combinatorics on Words*, Encyclopedia of Mathematics and Its Applications **105**, Cambridge University Press, Cambridge, 2005.
[34] I. G. Macdonald, The volume of a lattice polyhedron, *Proc. Camb. Phil. Soc.* **59** (1963), 719–726.
[35] I. G. Macdonald, Polynomials associated with finite cell complexes, *J. London Math. Soc. (2)* **4** (1971), 181–192.
[36] P. A. MacMahon, Memoir on the theory of partitions of numbers—Part III, *Phil. Trans.* **205** (1906), 37–58.
[37] P. McMullen, Lattice invariant valuations on rational polytopes, *Arch. Math. (Basel)* **31** (1978/79), 509–516.
[38] N. C. Metropolis, M. L. Stein, and P. R. Stein, Permanents of cyclic (0,1)-matrices, *J. Combinatorial Theory* **7** (1969), 291–321.
[39] N. E. Nörlund, *Vorlesungen über Differenzenrechnung*, Springer-Verlag, Berlin, 1924.
[40] J. K. Percus, *Combinatorial Methods*, Springer-Verlag, Berlin/Heidelberg/New York, 1971.
[41] G. A. Pick, Geometrisches zur Zahlenlehre, *Sitzungsber. Lotos (Prague)* **19** (1899), 311–319.
[42] G. Pólya, Untersuchungen über Lücken and Singularitäten von Potenzreihen, *Math. Zeit.* **29** (1928–1929), 549–640.

[43] G. Pólya, On the number of certain lattice polygons, *J. Combinatorial Theory* **6** (1969), 102–105.
[44] T. Popoviciu, Asupra unei probleme de partitie a numerelor, *Acad. R. P. R., Filiala Cluj*, Studie şi certetari şiintifice, 1–2, anul. IV (1953), 7–58.
[45] J. E. Reeve, On the volume of lattice polyhedra, *Proc. London Math. Soc.* **7** (1957), 378–395.
[46] J. Riordan, Generating functions for powers of Fibonacci numbers, *Duke Math. J.* **29** (1962), 5–12.
[47] R. M. Robinson, Integer-valued entire functions, *Trans. Amer. Math. Soc.* **153** (1971), 451–468.
[48] S. V. Sam, A bijective proof for a theorem of Ehrhart, *Amer. Math. Monthly* **116** (2009), 688–701.
[49] S. V. Sam and K. M. Woods, A finite calculus approach to Ehrhart polynomials, *Electronic J. Combin.* **17** (2010), R68.
[50] L. W. Shapiro, A combinatorial proof of a Chebyshev polynomial identity, *Discrete Math.* **34** (1981), 203–206.
[51] J. H. Spencer, Counting magic squares, *Amer. Math. Monthly* **87** (1980), 397–399.
[52] R. Stanley, Linear homogeneous diophantine equations and magic labelings of graphs, *Duke Math. J.* **40** (1973), 607–632.
[53] R. Stanley, Combinatorial reciprocity theorems, *Advances in Math.* **14** (1974), 194–253.
[54] R. Stanley, Magic labelings of graphs, symmetric magic squares, systems of parameters, and Cohen-Macaulay rings, *Duke Math. J.* **43** (1976), 511–531.
[55] R. Stanley, Generating functions, in *Studies in Combinatorics* (G.-C. Rota, ed.), Mathematical Association of America, Washington, DC, 1978, pp. 100–141.
[56] R. Stanley, Decompositions of rational convex polytopes, *Ann. Discrete Math.* **6** (1980), 333–342.
[57] R. Stanley, Linear diophantine equations and local cohomology, *Inventiones Math.* **68** (1982), 175–193.
[58] H. N. V. Temperley, Combinatorial problems suggested by the statistical mechanics of domains and of rubber-like molecules, *Phys. Rev. (2)* **103** (1956), 1–16.
[59] X. G. Viennot, A combinatorial theory for general orthogonal polynomials with extensions and applications, in *Orthogonal polynomials and applications (Bar-le-Duc, 1984)*, Lecture Notes in Math., no. 1171, Springer, Berlin, 1985, pp. 139–157.
[60] X. G. Viennot, Heaps of pieces. I. Basic definitions and combinatorial lemmas, *Graph Theory and Its Applications: East and West (Jinan, 1986)*, Ann. New York Acad. Sci. **576** (1989), 542–570.
[61] J. von Neumann, A certain zero-sum two person game equivalent to the optimal assignment problem, in *Contributions to the Theory of Games*, vol. 2 (H. W. Kuhn and A. W. Tucker, eds.), Annals of Mathematical Studies, no. 28, Princeton University Press, Princeton, 1950, pp. 5–12.

Exercises for Chapter 4

1. [2+] Let $F(x)$ and $G(x)$ be rational functions. Is it true that $F(x)+G(x)$ is also rational?

2. **a.** [3–] Suppose that $f(x)=\sum_{n\geq 0}a_n x^n$ is a rational function with integer coefficients a_n. Show that we can write $f(x)=P(x)/Q(x)$, where P and Q are relatively prime (over $\mathbb{Q}[x]$) polynomials with integer coefficients such that $Q(0)=1$.

b. [3–] Suppose that $f(x_1,\ldots,x_n)$ is a formal power series (over $\mathbb{C}$, say) that represents a rational function $P(x_1,\ldots,x_n)/Q(x_1,\ldots,x_n)$, where P and Q are relatively prime polynomials. Show that $Q(0,0,\ldots,0)\neq 0$.

3. [3–] Suppose that $f(x) \in \mathbb{Z}[[x]]$, $f(0) \neq 0$, and $f'(x)/f(x) \in \mathbb{Z}[[x]]$. Prove or disprove that $f(x)/f(0) \in \mathbb{Z}[[x]]$. (While this problem has nothing to do with rational functions, it is similar in flavor to Exercise 4.2(a).)

4. **a.** [3+] Suppose that $\sum_{n\geq 0} a_n x^n \in \mathbb{C}[[x]]$ is rational. Define $\chi : \mathbb{C} \to \mathbb{Z}$ by

$$\chi(a) = \begin{cases} 1, & a \neq 0, \\ 0, & a = 0. \end{cases}$$

Show that $\sum_{n\geq 0} \chi(a_n) x^n$ is also rational (and hence its coefficients are eventually periodic, by Exercise 4.46(b)).

b. [2+] Show that the corresponding result is false for $\mathbb{C}[[x, y]]$; that is, we can have $\sum a_{mn} x^m y^n$ rational but $\sum \chi(a_{mn}) x^m y^n$ nonrational.

c. [3+] Let $\sum_{n\geq 0} a_n x^n$ and $\sum_{n\geq 0} b_n x^n$ be rational functions with integer coefficients a_n and b_n. Suppose that $c_n := a_n/b_n$ is an integer for all n (so in particular $b_n \neq 0$). Show that $\sum_{n\geq 0} c_n x^n$ is also rational.

5. [5] Given polynomials $P(x), Q(x) \in \mathbb{Q}[x]$ for which $P(x)/Q(x) = \sum_{n\geq 0} a_n x^n$, is it decidable whether there is some n for which $a_n = 0$?

6. [3–] Given a sequence $\boldsymbol{a} = (a_0, a_1, \ldots)$ with entries in a field, the *Hankel determinant* $H_n(\boldsymbol{a})$ is defined by

$$H_n(\boldsymbol{a}) = \det(a_{i+j})_{0\leq i,j\leq n}.$$

Show that the power series $\sum_{n\geq 0} a_n x^n$ is ratonal if and only if $H_n(\boldsymbol{a}) = 0$ for all sufficiently large n. Equivalently, the infinite matrix (a_{i+j}) has finite rank.

7. **a.** [2+] Let $b_i \in \mathbb{P}$ for $i \geq 1$. Use Exercise 4.4 to show that the formal power series

$$F(x) = \sum_{i\geq 1} (1 - x^{2i-1})^{-b_i}$$

is not a rational function of x.

b. [2+] Find $a_i \in \mathbb{P}$ ($i \geq 1$) for which the formal power series

$$F(x) = \sum_{i\geq 1} (1 - x^i)^{-a_i}$$

is a rational function of x.

8. [2] Let $F(x) = \sum_{n\geq 0} a_{n+1} x^n \in \mathbb{C}[[x]]$. Show that the following conditions are equivalent.

i. There exists a rational power series $G(x)$ for which $F(x) = G'(x)/G(x)$.

ii. The series $\exp \sum_{n\geq 1} a_n \dfrac{x^n}{n}$ is rational.

iii. There exist nonzero complex numbers (not necessarily distinct) $\alpha_1, \ldots, \alpha_j, \beta_1, \ldots, \beta_k$ such that for all $n \geq 1$,

$$a_n = \sum \alpha_i^n - \sum \beta_i^n.$$

9. [2+] If $F(x)$ is a rational function over $\mathbb{Q}$ such that $F(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$, does it follow that $F(x)$ is a polynomial?

10. [3] Let $f(z)$ be an analytic function in an open set containing the disk $|z| \leq 1$. Suppose that the only singularities of $f(z)$ inside or on the boundary of this disk are poles, and that the Taylor series $\sum a_n z^n$ of $f(z)$ at $z = 0$ has integer coefficients a_n. Show that $f(z)$ is a rational function.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

11. Solve the following recurrences.
- **a.** [2–] $a_0 = 2$, $a_1 = 3$, $a_n = 3a_{n-1} - 2a_{n-2}$ for $n \geq 2$.
- **b.** [2–] $a_0 = 0$, $a_1 = 2$, $a_n = 4a_{n-1} - 4a_{n-2}$ for $n \geq 2$.
- **c.** [2] $a_0 = 5$, $a_1 = 12$, $a_n = 4a_{n-1} - 3a_{n-2} - 2^{n-2}$ for $n \geq 2$.
- **d.** [2+] $a_i = i$ for $0 \leq i \leq 7$, and

$$a_n = a_{n-1} - a_{n-3} + a_{n-4} - a_{n-5} + a_{n-7} - a_{n-8}, \ \ n \geq 8.$$

Rather than an explicit formula for a_n, give a simple description. For instance, compute a_{105} without using the recurrence.

12. [2] Consider the decimal expansion

$$\frac{1}{9899} = 0.000102030508132134 55 \cdots .$$

Why do the Fibonacci numbers 1, 2, 3, 5, 8, 13, 21, 34, 55, ... appear?

13. [2+] Is it true that for every $n \in \mathbb{P}$ there is a Fibonacci number F_k, $k \geq 1$, divisible by n?

14. [3] Let $a, b \in \mathbb{P}$, and define $f(0) = a$, $f(1) = b$, and $f(n+1) = f(n) + f(n-1)$ for $n \geq 1$. Show that we can choose a, b so that $f(n)$ is composite for all $n \in \mathbb{N}$.

15. [2+] Let I be an order ideal of the poset $\mathbb{N}^m$, and define $f(n) = \#\{(a_1, \ldots, a_m)\} \in I : a_1 + \cdots + a_m = n\}$. In other words, $f(n)$ is the number of $t \in I$ whose rank in $\mathbb{N}^m$ in n. Show that there is a polynomial $P(n)$ such that $f(n) = P(n)$ for n sufficiently large. For instance, if I is finite then $P(n) = 0$.

16. [2+] How many partitions $\lambda = (\lambda_1, \lambda_2, \ldots)$ of n satisfy $\lambda_3 = 2$? Give an exact formula.

17. **a.** [2+]* Let A_k be the set of all permutations $w = a_1 a_2 \cdots a_{2n}$ of the multiset $M_n = \{1^2, 2^2, \ldots, n^2\}$ with the following property: If $r < s < t$ and $a_r = a_t$, then $a_s > a_r$. For instance, $A_2 = \{1122, 1221, 2211\}$. Let B_n be the set of all permutations $w = a_1 a_2 \cdots a_{2n}$ of M_n with the following property: if $r < s$ and $a_r = a_s < a_t$, then $r < t$. For instance, $B_2 = \{1122, 1212, 1221\}$. Let

$$F_n(x) = \sum_{w \in A_n} x^{\mathrm{des}(w)},$$

$$G_n(x) = \sum_{w \in B_n} x^{\mathrm{des}(w)},$$

where $\mathrm{des}(w)$ denotes the number of descents of w. Show that $F_n(x) = G_n(x)$.

- **b.** [2+] Show that

$$\sum_{k \geq 0} S(n+k, k) x^k = \frac{x F_n(x)}{(1-x)^{2n+1}},$$

where $S(n+k, k)$ denotes a Stirling number of the second kind.

18. [2+]* Define polynomials $p_n(u)$ by

$$\sum_{n \geq 0} p_n(u) x^n = \frac{1}{1 - ux - x^2}.$$

Use combinatorial reasoning to find $\sum_{n \geq 0} p_n(u) p_n(v) x^n$.

19. [2]* Let $a, b \in \mathbb{R}$. Define a function $f : \mathbb{N} \to \mathbb{R}$ by $f(0) = a$, $f(1) = b$, and

$$f(n+2) = |f(n+1)| - f(n), \ \ n \geq 0.$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

Find $F(x) = \sum_{n\geq 0} f(n)x^n$. (If you prefer not to look at a large number of cases, then assume that $0 \leq a \leq b$.)

20. [2+]* Show that the function $f(n)$ of Example 4.1.3 (i.e., the number of words w of length n in the alphabet $\{N, E, W\}$ such that EW and WE are not factors of w) is equal to the number of nonzero coefficients of the polynomial

$$P_n(x) = \prod_{j=1}^{n}(1 + x_j - x_{j+1}).$$

Show moreover that all these coefficients are equal to ± 1. (For a related result, see Exercise 1.35(k).)

21. [3] A *tournament* T on $[n]$ is a directed graph on the vertex set $[n]$ with no loops and with exactly one edge between any two distinct vertices. The *outdegree* of a vertex i is the number of edges $i \to j$. The *degree sequence* of T is the set of outdegrees of its vertices, arranged in decreasing order. (Hence the degree sequence is a partition of $\binom{n}{2}$.) A degree sequence is *unique* if all tournaments with that degree sequence are isomorphic. Let $f(n)$ be the number of unique degree sequences of tournaments on $[n]$. Set $f(0) = 1$. Show that

$$\sum_{n\geq 0} f(n)x^n = \frac{1}{1 - x - x^3 - x^4 - x^5}$$
$$= 1 + x + x^2 + 2x^3 + 4x^4 + 7x^5 + 11x^6 + 18x^7 + 31x^8 + \cdots.$$

22. [2+]* Let $\alpha \in \mathbb{C}$, and define for $n \in \mathbb{N}$,

$$f_\alpha(n) = \sum_{k=0}^{n} \binom{n-k}{k} \alpha^k.$$

Show that $F_\alpha(x) := \sum_{n\geq 0} f_\alpha(n)x^n$ is a rational function, and compute it explicitly. Find an explicit formula for $f_\alpha(n)$. What value of α requires special treatment?

23. **a.** [2+]* Let S be a finite sequence of positive integers, say 2224211. We can describe this sequence as "three two's, one four, one two, two one's," yielding the *derived sequence* $32141221 = \delta(S)$. Suppose we start with $S = 1$ and form successive derived sequences $\delta(S) = 11$, $\delta^2(S) = 21$, $\delta^3(S) = 1211$, $\delta^4(S) = 111221$, $\delta^5(S) = 312211$, and so on. Show that for all $n \geq 0$, no term of $\delta^n(S)$ exceeds 3.

b. [3] Beginning with $S = 1$ as in (a), let $f(n)$ be the length (number of terms) of $\delta^n(S)$, and set

$$F(x) = \sum_{n\geq 0} f(n)x^n = 1 + 2x + 2x^2 + 4x^3 + 6x^4 + 6x^5 + \cdots.$$

Show that $F(x)$ is a rational function, which, when reduced to lowest terms, has denominator $D(x)$ of degree 92. Moreover, the largest reciprocal zero $\lambda = 1.30357726903\cdots$ (which controls the rate of growth of $f(n)$) of $D(x)$ is an algebraic integer of degree 71.

c. [3] Compute the (integer) polynomial $x^{71} - x^{69} - 2x^{68} - \cdots$ of degree 71 for which λ is a zero.

d. [3+] What if we start with a sequence other than $S = 1$?

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

24. **a.** [3] Let $f(x) = f(x_1, \ldots, x_k) \in \mathbb{F}_q[x_1, \ldots, x_k]$. Show that for each $\alpha \in \mathbb{F}_q - \{0\}$ there exist $\mathbb{Z}$-matrices $A_0, A_1, \ldots, A_{q-1}$ of some square size, and there exist a row vector u and a column vector v with the following property. For any integer $n \geq 1$ let $a_0 + a_1 q + \cdots + a_r q^r$ be its base q expansion, so $0 \leq a_i \leq q-1$. Let $N_\alpha(n)$ be the number of coefficients of $f(x)^n$ equal to α. Then

$$N_\alpha(n) = u A_{a_0} A_{a_1} \cdots A_{a_r} v.$$

b. [2–]* Deduce that the generating function

$$\sum_{n \geq 1} N_\alpha(1 + q + q^2 + \cdots + q^{n-1}) x^n$$

is rational.

25. Let $k = 1$ in Exercise 4.24. Without loss of generality we may assume $f(0) \neq 0$.

a. [3–] Show that there exist periodic functions $u(m)$ and $v(m)$ depending on $f(x)$ and α, such that

$$N_\alpha(q^m - 1) = u(m) q^m + v(m) \tag{4.51}$$

for all m sufficiently large.

b. [3–] Let d be the least positive integer for which $f(x)$ divides $x^{q^m(q^d-1)} - 1$ for some $m \geq 0$. In other words, d is the degree of the extension field of $\mathbb{F}_q$ obtained by adjoining all zeros of $f(x)$. Then the functions $u(m)$ and $v(m)$ have period d (and possibly smaller periods, necessarily dividing d).

c. [2+] Let μ be the largest multiplicity of any irreducible factor (or any zero) of $f(x)$. Then equation (4.51) holds for all $m \geq \lceil \log_q \mu \rceil$. In particular, if $f(x)$ is squarefree, then (4.51) holds for all $m \geq 0$.

d. If $f(x)$ is primitive over $\mathbb{F}_q$ (i.e., $f(x)$ is irreducible, and any zero ζ of $f(x)$ is a generator of the multiplicative group of the field $\mathbb{F}_q(\zeta)$), then $d = \deg f$ and $u(m) = dq^{d-1}/(q^d - 1)$ (a constant).

e. [3–] Write $[a_0, a_1, \ldots, a_{k-1}]$ for the periodic function $p(m)$ on $\mathbb{Z}$ satisfying $p(m) = a_i$ for $m \equiv i \pmod{k}$. Verify the following examples:

- If $f(x) = 1 + x \in \mathbb{F}_q^n$ where $q = 2^k$, then $N_1(m) = 2^m$.
- If $f(x) = 1 + x \in \mathbb{F}_q^n$ where q is odd, then

$$N_1(m) = \frac{1}{2}(q^m + 1), \quad N_{-1}(m) = \frac{1}{2}(q^m - 1).$$

- If $f(x) = 1 + x + x^2 + x^3 + x^4 \in \mathbb{F}_2[x]$, then $f(x)$ is irreducible but not primitive, and

$$N_1(m) = \frac{1}{5}[8, 12] 2^m + \frac{1}{5}[-3, 1, 3, -1].$$

- If $g(x) = 1 + x^2 + x^5 \in \mathbb{F}_2[x]$, then $g(x)$ is primitive and

$$N_1(m) = \frac{80}{31} 2^m + \frac{1}{31}[-49, -67, -41, 11, -9].$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

- If $g(x) = 1 + x + x^3 + x^4 + x^5 \in \mathbb{F}_2[x]$, then $g(x)$ is primitive and

$$N_1(m) = \frac{80}{31}2^m + \frac{1}{31}[-49, -5, -41, 11, -9].$$

  Note the closeness to the previous item.
- Let $g(x) = (1 + x^2 + x^5)^3 \in \mathbb{F}_2[x]$. Then

$$N_1(m) = \begin{cases} 1, & m = 0, \\ 9, & m = 1, \\ \frac{168}{31}2^m + \frac{1}{31}[297, -243, -393, -507, -177], & m \geq 2. \end{cases}$$

- Let $g(x) = 2 + x + x^2 \in \mathbb{F}_3[x]$. Then $g(x)$ is primitive and

$$N_1(m) = \frac{3}{4}3^m + \frac{1}{2} - \frac{1}{4}(-1)^m,$$
$$N_2(m) = \frac{3}{4}3^m - \frac{1}{2} - \frac{1}{4}(-1)^m.$$

- Let $g(x) = 2 + x^2 + x^3 \in \mathbb{F}_3[x]$. Then $g(x)$ is irreducible but not primitive, and

$$N_1(m) = \frac{18}{13}3^m + \frac{1}{13}[-5, 11, 7],$$
$$N_2(m) = \frac{9}{13}3^m - \frac{1}{13}[9, 14, 3].$$

26. a. [3+] Let p be a prime, and let $g_n(p)$ denote the number of nonisomorphic groups of order p^n. Write (i, j) for the greatest common divisor of i and j. Show that

$$g_1(p) = 1$$
$$g_2(p) = 2$$
$$g_3(p) = 5$$
$$g_4(p) = 15, \quad p \geq 3$$
$$g_5(p) = 2p + 61 + 2(p-1,3) + (p-1,4), \quad p \geq 5$$
$$g_6(p) = 3p^2 + 39p + 344 + 24(p-1,3) + 11(p-1,4) + 2(p-1,5), \quad p \geq 5$$
$$g_7(p) = 3p^5 + 12p^4 + 44p^3 + 170p^2 + 707p + 2455$$
$$(4p^2 + 44p + 291)(p-1,3) + (p^2 + 19p + 135)(p-1,4)$$
$$+(3p + 31)(p-1,5) + 4(p-1,7) + 5(p-1,8) + (p-1,9), \quad p \geq 7.$$

b. [3+] Show that for fixed p,

$$g_n(p) = p^{\frac{2}{27}n^3 + O(n^{5/2})}.$$

c. [5] Show that for fixed n, $g_n(p)$ is a quasipolynomial in p for p sufficiently large.

27. Let X be a finite alphabet, and let X^* denote the free monoid generated by X. Let M be the quotient monoid of X^* corresponding to relations $w_1 = w_1', \ldots, w_k = w_k'$,

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

where w_i and w_i' have the same length, $1 \le i \le k$. Thus, if $w \in M$, then we can speak unambiguously of the *length* of w as the length of any word in X^* representing w. Let $f(n)$ be the number of distinct words in M of length n, and let $F(x) = \sum_{n \ge 0} f(n)x^n$.

a. [3–] If $k = 1$, then show that $F(x)$ is rational.

b. [3] Show that in general $F(x)$ need not be rational.

c. [3–] Linearly order the q letters in X, and let M be defined by the relations $acb = cab$ and $bac = bca$ for $a < b < c$, and $aba = baa$ and $bab = bba$ for $a < b$. Compute $F(x)$.

d. [3–] Show that if M is commutative, then $F(x)$ is rational.

28. a. [2+] Let A and B be $n \times n$ matrices (over $\mathbb{C}$, say). Given $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_r), \boldsymbol{\beta} = (\beta_1, \ldots, \beta_r) \in \mathbb{N}^r$, define

$$t(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \operatorname{tr} A^{\alpha_1} B^{\beta_1} A^{\alpha_2} B^{\beta_2} \cdots A^{\alpha_r} B^{\beta_r}.$$

Show that $T_r(\boldsymbol{x}, \boldsymbol{y}) := \sum_{\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^r} t(\boldsymbol{\alpha}, \boldsymbol{\beta}) \boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{y}^{\boldsymbol{\beta}}$ is rational. What is the denominator of $T_r(\boldsymbol{x}, \boldsymbol{y})$?

b. Compute $T_1(x, y)$ for $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$.

29. [2+] Let A, B, C be square matrices of the same size over some field K. *True or false*: for fixed i, j, the generating function

$$\sum_{n \ge 1} (A^n B^n C^n)_{ij} x^n$$

is rational.

30. [2+] Let E be the monoid of $\mathbb{N}$-solutions to the equation $x + y - 2z - w = 0$. Write the generating function

$$E(\boldsymbol{x}) = E(x, y, z, w) = \sum_{\boldsymbol{\alpha} \in E} \boldsymbol{x}^{\boldsymbol{\alpha}}$$

explicitly in the form

$$E(\boldsymbol{x}) = \frac{P(\boldsymbol{x})}{\prod_{\boldsymbol{\beta} \in \mathrm{CF}(E)} (1 - \boldsymbol{x}^{\boldsymbol{\beta}})}.$$

That is, determine explicitly the elements of $\mathrm{CF}(E)$ and the polynomial $P(\boldsymbol{x})$.

31. [3–] Let $f(n)$ denote the number of distinct $\mathbb{Z}/n\mathbb{Z}$-solutions $\boldsymbol{\alpha}$ to equation (4.10) modulo n. For example, if $\Phi = [1 \ -1]$ then $f(n) = n$, the number of solutions $(\alpha, \beta) \in (\mathbb{Z}/n\mathbb{Z})^2$ to $\alpha - \beta = 0 \pmod{n}$. Show that $f(n)$ is a quasipolynomial for n sufficiently large (so in particular $\sum_{n \ge 1} f(n)x^n$ is rational).

32. [2+] Let E^* be the set of all $\mathbb{N}$-solutions to equation (4.10) in *distinct* integers $\alpha_1, \ldots, \alpha_m$. Show that the generating function $E^*(\boldsymbol{x}) := \sum_{\boldsymbol{\alpha} \in E^*} \boldsymbol{x}^{\boldsymbol{\alpha}}$ is rational.

33. a. [2]* Let $\Phi = \Phi_n$ be the $1 \times (n+1)$ matrix

$$\Phi = [1, 2, 3, \ldots, n, -n].$$

Show that the number of generators of the monoid E_Φ, as a function of n, is superpolynomial (i.e., grows faster than any polynomial in n).

b. [2]* Compute the generating function

$$E_{\Phi_3}(\boldsymbol{x}) = \sum_{\alpha \in E_{\Phi_3}} \boldsymbol{x}^{\boldsymbol{\alpha}}.$$

Express your answer as a rational function reduced to lowest terms.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

34. [3] Let $\Phi\boldsymbol{\alpha} = \mathbf{0}$ be a system of r linear equations in m unknowns $x_1, \ldots, x_m$ over $\mathbb{Z}$, as in equation (4.10). Let S be a subset of $[m]$. Suppose that $\Phi\boldsymbol{\alpha} = \mathbf{0}$ has a solution $(\gamma_1, \ldots, \gamma_m) \in \mathbb{Z}^m$ satisfying $\gamma_i > 0$ if $i \in S$ and $\gamma_i < 0$ if $i \notin S$. Let

$$F_S(\boldsymbol{x}) = \sum_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}},$$

$$\overline{F}_S(\boldsymbol{x}) = \sum_{\boldsymbol{\beta}} \boldsymbol{x}^{\boldsymbol{\beta}},$$

where $\boldsymbol{\alpha}$ runs over all $\mathbb{N}$-solutions to $\Phi\boldsymbol{\alpha} = \mathbf{0}$ satisfying $\alpha_i > 0$ if $i \in S$, while $\boldsymbol{\beta}$ runs over all $\mathbb{N}$-solutions to $\Phi\boldsymbol{\beta} = \mathbf{0}$ satisfying $\beta_i > 0$ if $i \notin S$. Show that

$$\overline{F}_S(\boldsymbol{x}) = (-1)^{\operatorname{corank}(\Phi)} F_S(1/\boldsymbol{x}).$$

35. **a.** [2+] Let Φ be an $r \times m$ $\mathbb{Z}$-matrix, and fix $\boldsymbol{\beta} \in \mathbb{Z}^r$. Let $E_{\boldsymbol{\beta}}$ be the set of all $\mathbb{N}$-solutions $\boldsymbol{\alpha}$ to $\Phi\boldsymbol{\alpha} = \boldsymbol{\beta}$. Show that the generating function $E_{\boldsymbol{\beta}}(\boldsymbol{x})$ represents a rational function of $\boldsymbol{x} = (x_1, \ldots, x_m)$. Show also that either $E_{\boldsymbol{\beta}}(\boldsymbol{x}) = 0$ (i.e., $E_{\boldsymbol{\beta}} = \emptyset$) or else $E_{\boldsymbol{\beta}}(\boldsymbol{x})$ has the same least denominator $D(\boldsymbol{x})$ as $E(\boldsymbol{x})$ (as given in Theorem 4.5.11).

b. [2+] Assume for the remainder of this exercise that the monoid E is positive and that $E_{\boldsymbol{\beta}} \neq \emptyset$. We say that the pair $(\Phi, \boldsymbol{\beta})$ has the *R-property* if $\overline{E}_{\boldsymbol{\beta}}(\boldsymbol{x}) = (-1)^d E_{\boldsymbol{\beta}}(1/\boldsymbol{x})$, where $\overline{E}_{\boldsymbol{\beta}}$ is the set of $\mathbb{P}$-solutions to $\Phi\boldsymbol{\alpha} = -\boldsymbol{\beta}$, and where d is as in Theorem 4.5.14. (Thus, Theorem 4.5.14 asserts that $(\Phi, \mathbf{0})$ has the R-property.) For what integers β does the pair $([1\ 1\ -1\ -1], \beta)$ have the R-property?

c. [3] Suppose that there exists a vector $\boldsymbol{\alpha} \in \mathbb{Q}^m$ satisfying $-1 < \alpha_i \leq 0$ $(1 \leq i \leq m)$ and $\Phi\boldsymbol{\alpha} = \boldsymbol{\beta}$. Show that $(\Phi, \boldsymbol{\beta})$ has the R-property.

d. [3+] Find a "reasonable" necessary and sufficient condition for $(\Phi, \boldsymbol{\beta})$ to have the R-property.

36. **a.** [2] Let σ be a d-dimensional simplex in $\mathbb{R}^m$ with integer vertices $v_0, \ldots, v_d$. We say that σ is *primitive* (or *unimodular*) if $v_1 - v_0, v_2 - v_0, \ldots, v_d - v_0$ form part of a $\mathbb{Z}$-basis for $\mathbb{Z}^m$. This condition is equivalent to the statement that the relative volume of σ is equal to $1/d!$, the smallest possible relative volume of an integer d-simplex. Now let $\mathcal{P}$ be an integer polytope in $\mathbb{R}^m$. We say that a triangulation Γ of $\mathcal{P}$ is *primitive* (or *unimodular*) if every simplex $\sigma \in \Gamma$ is primitive. (We are allowed to have vertices of Γ that are not vertices of $\mathcal{P}$. For instance, the line segment $[0, 2]$ has a primitive triangulation whose facets are $[0, 1]$ and $[1, 2]$.) Does every integral polytope have a primitive triangulation?

b. [2+] Let Γ be a primitive triangulation of the integer polytope $\mathcal{P}$. Suppose that Γ has f_i i-dimensional faces. Express the Ehrhart polynomial $i(\mathcal{P}, n)$ in terms of the f_i's.

37. **a.** [2+]* Let $\mathcal{P}$ be an integer polytope in $\mathbb{R}^d$ with vertex set V. Suppose that $\mathcal{P}$ is defined by inequalities $\alpha_i \cdot x \leq \beta_i$. Given $v \in V$, let the *support cone* at v be the cone $\mathcal{C}_v$ defined by $\alpha_i \cdot x \leq \beta_i$ whenever $\alpha_i \cdot v = \beta_i$. Let

$$F_v(x) = \sum_{\gamma \in \mathcal{C}_v \cap \mathbb{Z}^d} x^{\gamma}.$$

Show that each $F_v(x)$ is a rational Laurent series.

b. [3] Show that

$$\sum_{v \in V} F_v(x) = \sum_{\gamma \in \mathcal{P} \cap \mathbb{Z}^d} x^{\gamma},$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

where the sum on the left is interpreted as a sum of *rational functions* (not formal Laurent series).

Example. Let $\mathcal{P}$ be the interval $[2,5] \subset \mathbb{R}$. Then

$$F_2(x) = \sum_{n \geq 2} x^n = \frac{x^2}{1-x},$$

$$F_5(x) = \sum_{n \leq 5} x^n = \frac{x^5}{1-x^{-1}},$$

and

$$\begin{aligned} \frac{x^2}{1-x} + \frac{x^5}{1-x^{-1}} &= x^2 + x^3 + x^4 + x^5 \\ &= \sum_{n \in [2,5]} x^n. \end{aligned}$$

As another example, let $\mathcal{P}$ have vertices $(0,0)$, $(0,2)$, $(2,0)$, and $(4,2)$. Then $\mathcal{C}_{(2,0)}$ is defined by $y \geq 0$ and $x - y \leq 2$, and

$$\begin{aligned} F_{(2,0)}(x,y) &= \sum_{n \geq 0} \sum_{m \leq n+2} x^m y^n \\ &= \sum_{n \geq 0} y^n \cdot \frac{x^{n+2}}{1-x^{-1}} \\ &= \frac{x^2}{1-x^{-1}} \cdot \frac{1}{1-xy} \\ &= -\frac{x^3}{(1-x)(1-xy)}. \end{aligned}$$

38. [3] Let Φ be an $r \times m$ matrix whose entries are polynomials in n with integer coefficients. Let $\boldsymbol{\beta}$ be a column vector of length m whose entries are also polynomials in n with integer coefficients. Suppose that for each fixed $n \in \mathbb{P}$ the number $f(n)$ of solutions $\boldsymbol{\alpha} \in \mathbb{N}^m$ to $\Phi\boldsymbol{\alpha} = \boldsymbol{\beta}$ is finite. Show that $f(n)$ is a quasipolynomial for n sufficiently large.

39. a. [4–] Let $P_1, \ldots, P_k \in \mathbb{F}_q[x_1, \ldots, x_m]$. Let $f(n)$ be the number of solutions $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_{q^n}^m$ to the equations $P_1(\boldsymbol{\alpha}) = \cdots = P_k(\boldsymbol{\alpha}) = 0$. Show that $F(x) := \exp \sum_{n \geq 1} f(n)x^n/n$ is rational. (See Exercise 4.8 for equivalent forms of this condition.)

b. [4–] Let $P_1, \ldots, P_k \in \mathbb{Z}[x_1, \ldots, x_m]$, and let p be a prime. Let $f(n)$ be the number of solutions $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_m) \in (\mathbb{Z}/p^n\mathbb{Z})^m$ to the congruences

$$P_1(\boldsymbol{\alpha}) \equiv \cdots \equiv P_k(\boldsymbol{\alpha}) \equiv 0 \pmod{p^n}.$$

Show that $F(x) := \sum_{n \geq 1} f(n)x^n$ is rational.

40. a. [2+] Let $X = \{x_1, \ldots, x_n\}$ be an alphabet with n letters, and let $\mathbb{C}\langle\langle X \rangle\rangle$ be the *noncommutative* power series ring (over $\mathbb{C}$) in the variables X; that is, $\mathbb{C}\langle\langle X \rangle\rangle$ consists of all formal expressions $\sum_{w \in X^*} \alpha_w w$, where $\alpha_w \in \mathbb{C}$ and X^* is the free monoid

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

generated by X. Multiplication in $\mathbb{C}\langle\langle X\rangle\rangle$ is defined in the obvious way, namely,

$$\left(\sum_u \alpha_u u\right)\left(\sum_v \beta_v v\right) = \sum_{u,v} \alpha_u \beta_v uv$$
$$= \sum_w \gamma_w w,$$

where $\gamma_w = \sum_{uv=w} \alpha_u \beta_v$ (a finite sum).

Let L be a set of words such that no proper factor of a word in L belongs to L. (A word $v \in X^*$ is a *factor* of $w \in X^*$ if $w = uvy$ for some $u, y \in X^*$.) Define an *L-cluster* to be a triple $(w, (v_1, \ldots, v_k), (\ell_1, \ldots, \ell_k)) \in X^* \times L^k \times [r]^k$, where r is the length of $w = \sigma_1\sigma_2\cdots\sigma_r$ and k is some positive integer, satisfying:

- **i.** For $1 \le j \le k$ we have $w = uv_j y$ for some $u \in X^*_{\ell_j - 1}$ and $y \in X^*$ (i.e., w contains v_j as a factor beginning in position ℓ_j). Henceforth we identify v_j with this factor of w.
- **ii.** For $1 \le j \le k-1$, we have that v_j and v_{j+1} overlap in w, and that v_{j+1} begins to the right of the beginning of v_j (so $0 < \ell_1 < \ell_2 < \cdots < \ell_k < r$).
- **iii.** v_1 contains σ_1, and v_k contains σ_r.

Note that two different L-clusters can have the same first component w. For instance, if $X = \{a\}$ and $L = \{aaa\}$, then $(aaaaa, (aaa, aaa, aaa), (1,2,3))$ and $(aaaaa, (aaa, aaa), (1,3))$ are both L-clusters.

Let $D(L)$ denote the set of L-clusters. For each word $v \in L$ introduce a new variable t_v commuting with the x_i's and with each other. Define the *cluster-generating function*

$$C(\boldsymbol{x}, \boldsymbol{t}) = \sum_{(w,\mu,\nu)\in D(L)} \left(\prod_{v\in L} t_v^{m_v(\mu)}\right) w \in \mathbb{C}[[t_v : v \in L]]\langle\langle X\rangle\rangle,$$

where $m_v(\mu)$ denotes the number of components v_i of $\mu \in L^k$ that are equal to v. Show that in the ring $\mathbb{C}[[t_v : v \in L]]\langle\langle X\rangle\rangle$ we have

$$\sum_{w\in X^*} \left(\prod_{v\in L} t_v^{m_v(w)}\right) w = (1 - x_1 - \cdots - x_n - C(\boldsymbol{x}, \boldsymbol{t-1}))^{-1}, \tag{4.52}$$

where $m_v(w)$ denotes the number of factors of w equal to v, and where $\boldsymbol{t-1}$ denotes the substitution of $t_v - 1$ for each t_v.

b. [1+]* Note the following specializations of equation (4.52):

- **i.** If we let the variables x_i in (4.52) commute and set each $t_v = t$, then the coefficient of $t^k x_1^{m_1} \cdots x_n^{m_n}$ is the number of words $w \in X^*$ with m_i x_i's for $1 \le i \le n$, and with exactly k factors belonging to L.
- **ii.** If we set each $x_i = x$ and $t_i = t$ in (4.52), then the coefficient of $t^k x^m$ is the number of words $x \in X^*$ of length m, with exactly k factors belonging to L.
- **iii.** If we set each $x_i = x$ and each $t_v = 0$ in (4.52), then the coefficient of x^m is the number of words $w \in X^*$ with no factors belonging to L.

c. [2] Show that if L is finite and the x_i's commute in (4.52), then (4.52) represents a rational function of $x_1, \ldots, x_n$ and the t_v's.

d. [2] If $w = a_1 a_2 \cdots a_l \in X^*$, then define the *autocorrelation polynomial* $A_w(x) = c_1 + c_2 x + \cdots + c_l x^{l-1}$, where

$$c_i = \begin{cases} 1, & \text{if } a_1 a_2 \cdots a_{l-i+1} = a_i a_{i+1} \cdots a_l, \\ 0, & \text{otherwise.} \end{cases}$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

For instance, if $w = abacaba$, then $A_w(x) = 1 + x^4 + x^6$. Let $f(m)$ be the number of words $w \in X^*$ of length m that don't contain w as a factor. Show that

$$\sum_{m \geq 0} f(m)x^m = \frac{A_w(x)}{(1-nx)A_w(x) + x^l}. \tag{4.53}$$

41. a. [1+]* Let $B_k(n)$ be the number of ways to place k nonattacking queens on an $n \times n$ chessboard. Show that $B_1(n) = n^2$.

b. [2+] Show that

$$B_2(n) = \frac{1}{6}n(n-1)(n-2)(3n-1).$$

c. [3–] Show that

$$B_3(n) = \begin{cases} \frac{1}{12}n(n-2)^2(2n^3 - 12n^2 + 23n - 10), & n \text{ even}, \\ \frac{1}{12}(n-1)(n-3)(2n^4 - 12n^3 + 25n^2 - 14n + 1), & n \text{ odd}. \end{cases}$$

d. [2+] Show that for fixed $k \geq 1$,

$$B_k(n) = \frac{1}{k!}n^{2k} - \frac{5}{3 \cdot (k-2)!}n^{2k-1} + O(n^{2k-2}).$$

e. [3–] Show that $\sum_{n \geq 0} B_k(n)x^n$ is a rational power series. In fact, $B_k(n)$ is a quasipolynomial.

42. a. [2+]* Show that the number of ways to place k nonattacking bishops on the white squares of an $(n-1) \times n$ chessboard is the Stirling number $S(n, n-k)$.

b. [3–] Let $A_k(n)$ be the number of ways to place k nonattacking bishops on an $n \times n$ chessboard. Show that $A_k(n)$ is a quasipolynomial with quasiperiod two.

c. [3] Find an explicit formula for $A_k(n)$ in the form of a triple sum.

43. [2+] Let $t(n)$ be the number of noncongruent triangles whose sides have integer length and whose perimeter in n. For instance $t(9) = 3$, corresponding to $3+3+3$, $2+3+4$, $1+4+4$. Find $\sum_{n \geq 3} t(n)x^n$.

44. [2+] Let $k, r, n \in \mathbb{P}$. Let $N_{kr}(n)$ be the number of n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n) \in [k]^n$ such that no r consecutive elements of α are equal (e.g., $N_{kr}(r) = k^r - k$.) Let $F_{kr}(x) = \sum_{n \geq 0} N_{kr}(n)x^n$. Find $F_{kr}(x)$ explicitly. (Set $N_{kr}(0) = 1$.)

45. a. [3] Let $m \in \mathbb{P}$ and $k \in \mathbb{Z}$. Define a function $f : \{m, m+1, m+2, \ldots\} \to \mathbb{Z}$ by

$$\begin{aligned} f(m) &= k, \\ f(n+1) &= \left\lfloor \frac{n+2}{n} f(n) \right\rfloor, \quad n \geq m. \end{aligned} \tag{4.54}$$

Show that f is a quasipolynomial on its domain.

b. [5–] What happens when $(n+2)/n$ is replaced by some other rational function $R(n)$?

46. a. [2+] Define $f : \mathbb{N} \to \mathbb{Q}$ by

$$f(n+2) = \frac{6}{5}f(n+1) - f(n), \quad f(0) = 0, \quad f(1) = 1. \tag{4.55}$$

Show that $|f(n)| < \frac{5}{4}$.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

b. [2] Suppose that $f : \mathbb{N} \to \mathbb{Z}$ satisfies a linear recurrence (4.2) where each $\alpha_i \in \mathbb{Z}$, and that $f(n)$ is bounded as $n \to \infty$. Show that $f(n)$ is periodic.

c. [3+] Suppose that y is a power series with integer coefficients and radius of convergence one. Show that y is either rational or has the unit circle as a natural boundary.

47. [3] If $\alpha \in \mathbb{N}^m$ and $k > 0$, then let $f_k(\alpha)$ denote the number of partitions of α into k parts belonging to $\mathbb{N}^m$. For example, $f_2(2,2) = 5$, since $(2,2) = (2,2) + (0,0) = (1,0) + (1,2) = (0,1) + (2,1) = (2,0) + (0,2) = (1,1) + (1,1)$. If $\alpha = (\alpha_1, \ldots, \alpha_m)$, then write as usual $x^\alpha = x_1^{\alpha_1} \cdots x_m^{\alpha_m}$. Clearly,

$$\sum_{\alpha \in \mathbb{N}^m} \sum_{k \geq 0} f_k(\alpha) t^k x^\alpha = \prod_{\alpha \in \mathbb{N}^m} \left(1 - t x^\alpha\right)^{-1},$$

the m-dimensional generalization of equation (1.77). Show that

$$\sum_{\alpha \in \mathbb{N}^m} f_k(\alpha) x^\alpha = \left[\sum x_1^{\mathrm{maj}(w_1)} \cdots x_m^{\mathrm{maj}(w_m)}\right] \left[\prod_{i=1}^{m} (1 - x_i)(1 - x_i^2) \cdots (1 - x_i^k)\right]^{-1},$$

where the second sum is over all m-tuples $(w_1, \ldots, w_m) \in \mathfrak{S}_k^m$ satisfying $w_1 w_2 \cdots w_m = 1$. Note that Proposition 1.1.8.6(a) is equivalent to the case $m = 1$.

48. **a.** [3] Let $\mathcal{P}$ be an integral convex d-polytope with $\mathcal{P}$-Eulerian polynomial $A(\mathcal{P}, x)$. Show that the coefficients of $A(\mathcal{P}, x)$ are nonnegative.

b. [3+] Let $\mathcal{Q} \subset \mathbb{R}^m$ be a finite union of integral convex d-polytopes, such that the intersection of any two of these polytopes is a common face (possibly empty) of both. Suppose that $\mathcal{Q}$, regarded as a topological space, satisfies

$$H_i(\mathcal{Q}, \mathcal{Q} - p; \mathbb{Q}) = 0 \text{ if } i < d, \text{ for all } p \in \mathcal{Q},$$
$$\widetilde{H}_i(\mathcal{Q}; \mathbb{Q}) = 0 \text{ if } i < d.$$

Here H_i and $\widetilde{H}_i$ denote relative singular homology and reduced singular homology, respectively. We may define the Ehrhart function $i(\mathcal{Q}, n)$ for $n \geq 1$ exactly as for polytopes $\mathcal{P}$, and one easily sees that $i(\mathcal{Q}, n)$ is a polynomial of degree d for $n \geq 1$. Define $i(\mathcal{Q}, 0) = 1$, despite the fact that the value of the polynomial $i(\mathcal{Q}, n)$ at $n = 0$ is $\chi(\mathcal{Q})$, the Euler characteristic of $\mathcal{Q}$. Set

$$\sum_{n \geq 0} i(\mathcal{Q}, n) x^n = \frac{A(\mathcal{Q}, x)}{(1 - x)^{d+1}}.$$

Show that the coefficients of the polynomial $A(\mathcal{Q}, x)$ are nonnegative.

c. [3] Suppose that $\mathcal{P}$ and $\mathcal{Q}$ are integral convex polytopes (not necessarily of the same dimension) in $\mathbb{R}^m$ with $\mathcal{Q} \subseteq \mathcal{P}$. Show that the polynomial $A(\mathcal{P}, x) - A(\mathcal{Q}, x)$ has nonnegative coefficients. Note that (a) follows from taking $\mathcal{Q} = \emptyset$.

49. Let $\mathcal{P}$ be an integral convex d-polytope in $\mathbb{R}^m$, and let $A(\mathcal{P}, x) = 1 + h_1 x + \cdots + h_d x^d$.

a. [3] Show that

$$h_d + h_{d-1} + \cdots + h_{d-i} \leq h_0 + h_1 + \cdots + h_{i+1}, \tag{4.56}$$

for $1 \leq i \leq \lfloor d/2 \rfloor - 1$.

b. [3] Let $s = \max\{i : h_i \neq 0\}$. Show that

$$h_0 + h_1 + \cdots + h_i \leq h_s + h_{s-1} + \cdots + h_{s-i}, \tag{4.57}$$

for $0 \leq i \leq \lfloor s/2 \rfloor$.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

50. [2] Let $\partial\mathcal{P}$ denote the boundary of the d-dimensional integral convex polytope $\mathcal{P}$ in $\mathbb{R}^m$. For $n \in \mathbb{P}$, we can define

$$i(\partial\mathcal{P}, n) = \#(n \cdot \partial\mathcal{P} \cap \mathbb{Z}^m),$$

exactly as was done for $\mathcal{P}$. Set $i(\partial\mathcal{P}, 0) = 1$. Show that

$$\sum_{n \geq 0} i(\partial\mathcal{P}, n)x^n = \frac{h_0 + h_1 x + \cdots + h_d x^d}{(1-x)^d},$$

where $h_i \in \mathbb{Z}$ and $h_i = h_{d-i}$ for $0 \leq i \leq d$.

51. **a.** [2] Fix $r, s \in \mathbb{P}$. Let $\mathcal{P}$ be the convex polytope in $\mathbb{R}^{r+s}$ defined by

$$x_1 + x_2 + \cdots + x_r \leq 1, \;\; y_1 + y_2 + \cdots + y_s \leq 1, \;\; x_i \geq 0, \;\; y_i \geq 0.$$

Let $i(n) = i(\mathcal{P}, n)$ be the Ehrhart (quasi)polynomial of $\mathcal{P}$. Use Exercise 3.169 to find $F(x) = \sum_{n \geq 0} i(n)x^n$ explicitly; that is, find the denominator of $F(x)$ and the coefficients of the numerator. What is the volume of $\mathcal{P}$? What are the vertices of $\mathcal{P}$?

b. [2] Find a partially ordered set P_{rs} for which $i(\mathcal{P}, n-1) = \Omega_{P_{rs}}(n)$, the order polynomial of P_{rs}.

52. [3–]* Let σ_d be the d-dimensional simplex in $\mathbb{R}^d$ with vertices $(0,0,0,\ldots,0)$, $(1,0,0,\ldots,0)$, $(1,2,0,\ldots,0)$, $\ldots$, $(1,2,3,\ldots,d)$. Show that $i(\sigma_d, n) = (n+1)^d$.

53. An *antimagic square* of index n is a $d \times d$ $\mathbb{N}$-matrix $M = (m_{ij})$ such that for every permutation $w \in \mathfrak{S}_d$ we have $\sum_{i=1}^d m_{i,w(i)} = n$. In other words, any set of d entries, no two in the same row or column, sum to n.

a. [2] For what positive integers d do there exist $d \times d$ antimagic squares whose entries are the distinct integers $1, 2, \ldots, d^2$?

b. [2+] Let R_i (respectively, C_i) be the $d \times d$ matrix with 1's in the ith row (respectively, ith column) and 0's elsewhere. Show that a $d \times d$ antimagic square has the form

$$M = \sum_{i=1}^n a_i R_i + \sum_{j=1}^n b_j C_j,$$

where $a_i, b_j \in \mathbb{N}$.

c. [2+] Use (b) to find a simple explicit formula for the number of $d \times d$ antimagic squares of index n.

d. [2] Let $\mathcal{P}_d$ be the convex polytope in $\mathbb{R}^{d^2}$ of all $d \times d$ matrices $X = (x_{ij})$ satisfying

$$x_{ij} \geq 0, \;\; \sum_{i=1}^d x_{i,w(i)} = 1 \;\text{ for all } w \in \mathfrak{S}_d.$$

What are the vertices of $\mathcal{P}_d$? Find the Ehrhart polynomial $i(\mathcal{P}_d, n)$.

e. [2] Find the $\mathcal{P}_d$-Eulerian polynomial $A(\mathcal{P}_d, x)$ and the relative volume $v(\mathcal{P}_d)$.

54. **a.** [2+] Let

$$H_n(r) = \sum_{i=0}^{(n-1)^2} c(n,i) r^{(n-1)^2 - i},$$

where $H_n(r)$ denotes the number of $n \times n$ $\mathbb{N}$-matrices with line sum r, as in Section 4.6.1. Show that $c(n,1)/c(n,0) = \frac{1}{2}n(n-1)^2$.

b. [5–] (rather speculative) Fix $k \geq 0$. Then as $n \to \infty$ we have the asymptotic formula

$$\frac{c(n,k)}{c(n,0)} \sim \frac{n^{3k}}{2^k k!}.$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

55. [2+]* Let $f(n)$ denote the number of 2×3 $\mathbb{N}$-matrices such that every row sums to $3n$ and every column to $2n$. Find an explicit formula for $f(n)$ and compute (as a rational function reduced to lowest terms) the generating function $\sum_{n \geq 0} f(n)x^n$.

56. **a.** [2+] Let $P = \{t_1, \ldots, t_p\}$ be a finite poset. Let $\mathcal{C}(P)$ denote the convex polytope in $\mathbb{R}^p$ defined by

$$\mathcal{C}(P) = \{(\varepsilon_1, \ldots, \varepsilon_p) \in \mathbb{R}^p : 0 \leq \varepsilon_{i_1} + \cdots + \varepsilon_{i_k} \leq 1 \text{ whenever } t_{i_1} < \cdots < t_{i_k}\}.$$

Find the vertices of $\mathcal{C}(P)$.

b. [2+] Show that the Ehrhart (quasi)polynomial of $\mathcal{C}(P)$ is given by $i(\mathcal{C}(P), n-1) = \Omega_P(n)$, the order polynomial of P. Thus, we have *two* polytopes associated with P whose Ehrhart polynomial is $\Omega_P(n+1)$, the second given by Example 4.6.17.

c. [2] Given $n, k \geq 1$, let $\mathcal{C}_{n,k}$ be the convex polytope in $\mathbb{R}^n$ defined by $x_i \geq 0$ for $1 \leq i \leq n$ and

$$x_{i+1} + x_{i+2} + \cdots + x_{i+k} \leq 1, \quad 0 \leq i \leq n-k.$$

Find the volume $v(\mathcal{C}_{n,2})$. (Note that the volume of $\mathcal{C}_{n,k}$ is the same as the relative volume since $\dim \mathcal{C}_{n,k} = n$.)

d. [5] Find the volume V_n of $\mathcal{C}_{n,3}$. For instance,

$$(1!\,V_1, 2!\,V_2, \ldots, 10!\,V_{12}) = (1, 1, 1, 2, 5, 14, 47, 182, 786, 3774, 19974, 115236).$$

e. [2+] Let $k \leq n \leq 2k$. Show that the volume of $\mathcal{C}_{n,k}$ is $C_{n-k+1}/n!$, where C_{n-k+1} is a Catalan number.

57. [2+] Let P and Q be partial orderings of the same p-element set. Suppose that the incomparability graph $\mathrm{inc}(P)$ of P is a proper (spanning) subgraph of $\mathrm{inc}(Q)$. Use Exercise 4.56 to show that $e(P) < e(Q)$.

58. **a.** [3–] Let P be a finite poset and let $\mathcal{V}(P)$ denote the set of all maps $f : P \to \mathbb{R}$ such that for every order ideal I of P we have

$$0 \leq \sum_{t \in I} f(t) \leq 1.$$

Clearly, $\mathcal{V}(P)$ is a convex polytope in the vector space $\mathbb{R}^P$, called the *valuation polytope* of P. It is linearly equivalent to the polytope of all valuations on $J(P)$ (as defined in Exercise 3.94) with values in the interval $[0,1]$. Show that the vertices of $\mathcal{V}(P)$ consist of all functions f_C, where C is a chain $t_1 < t_2 < \cdots < t_k$ in P, defined by

$$f(t) = \begin{cases} (-1)^{i-1}, & t = t_i \\ 0, & \text{otherwise.} \end{cases}$$

Thus, $\mathcal{V}(P)$ is an integer polytope.

b. [2–]* Show that $\dim \mathcal{V}(P) = \#P$.

c. [2] Compute the Ehrhart polynomial $i(\mathcal{V}(P), n)$ of the valuation polytope of a p-element chain.

d. [2+] Show that

$$A(\mathcal{V}(P+Q), x) = A(\mathcal{V}(P), x) A(\mathcal{V}(Q), x),$$

where $A(\mathcal{P}, x)$ denotes the $\mathcal{P}$-Eulerian polynomial.

e. [2] Show that $i(\mathcal{V}(P), 1)$ is the total number of chains of P (including the empty chain).

f. [2+] Let $p = \#P$, and let m denote the number of minimal elements of P. Show that $\deg A(\mathcal{V}(P), x) = p - m$.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

g. [2+] Show that $x^{p-m}A(\mathcal{V}(P),1/x) = A(\mathcal{V}(P),x)$ if and only if every connected component of P has a unique minimal element.

h. [2+]* Let U_k denote the ordinal sum of k 2-element antichains, as in Exercise 3.139. Let $A(n)$ denote the $n \times n$ real matrix, with rows and columns indexed by $[n+1]$, defined by

$$A(n)_{ij} = \begin{cases} i+j-1, & \text{if } i+j \le n+2, \\ 2n-i-j+3, & \text{if } i+j \ge n+2. \end{cases}$$

Show that $i(\mathcal{V}(U_k),n)$ is the sum of the entries of the first row of $A(n)^k$. Is there a more explicit formula for $i(\mathcal{V}(U_k),n)$? Is there a nice formula for the volume of $\mathcal{V}(U_k)$? If we write $\mathrm{vol}(\mathcal{V}(U_k)) = u_k/(2k)!$, then

$$(u_1,\ldots,u_6)) = (2,8,162,6128,372560,33220512).$$

i. [5–] What more can be said about $\mathcal{V}(P)$ in general? Is there a nice combinatorial interpretation of its volume? Are the coefficients of $i(\mathcal{V}(P),n)$ nonnegative?

59. [3] Let $t \in \mathbb{R}$, and define $v_d(t) = (t,t^2,\ldots,t^d) \in \mathbb{R}^d$. The set of all points $v_d(t)$, $t \in \mathbb{R}$, is called the *moment curve*. Let $n > d$ and $T = \{t_1,\ldots,t_n\}$, where the t_i's are real numbers satisfying $t_1 < \cdots < t_n$. Define the *cyclic polytope* $C_d(T)$ to be the convex hull of the points $v_d(t_1),\ldots,v_d(t_n)$. Suppose that each t_i is an integer, so $C_d(T)$ is an integral polytope. Show that

$$i(C_d(T),m) = \mathrm{vol}(C_d(T))m^d + i(C_{d-1}(T),m),$$

where we set $i(C_0(T),m) = 1$. In particular, the polynomial $i(C_d(T),m)$ has positive coefficients.

60. [2+] Give an example of a 3-dimensional simplex (tetrahedron) $\mathcal{P}$ with integer vertices such that the Ehrhart polynomial $i(\mathcal{P},n)$ has a negative coefficient.

61. **a.** [2+] Let e_j be the jth unit coordinate vector in $\mathbb{R}^d$, and let $\mathcal{P}_d$ be the convex hull of the $2d$ vectors $\pm e_j$. (This polytope is the d-dimensional *cross-polytope*. When $d = 3$ it is an octahedron.) Let $i(\mathcal{P}_d,n)$ denote the Ehrhart polynomial of $\mathcal{P}_d$. Find explicitly the polynomial $P_d(x)$ for which

$$\sum_{n \ge 0} i(\mathcal{P}_d,n)x^n = \frac{P_d(x)}{(1-x)^{d+1}}.$$

b. [3–] Show that every (complex) zero of $i(\mathcal{P}_d,n)$ has real part $-1/2$.

62. Let $1 \le k \le n-1$. The *hypersimplex* $\Delta_{k,d}$ is the convex hull of all $(0,1)$-vectors in $\mathbb{R}^d$ with exactly k 1's.

a. [2–]* Show that $\dim \Delta_{k,d} = d-1$.

b. [2+] Show that the relative volume of $\Delta_{k,d}$ is $A(d-1,k)/(d-1)!$, where $A(d-1,k)$ is an Eulerian number (the number of permutations $w \in \mathfrak{S}_{d-1}$ with $k-1$ descents).

c. [2+] Show that

$$i(\Delta_{k,d},n) = [x^{kn}]\left(\frac{1-x^{n+1}}{1-x}\right)^d.$$

d. [2]* Deduce from (c) that

$$i(\Delta_{k,d},n) = \sum_{j=0}^{\lfloor kn/(n+1) \rfloor} (-1)^j \binom{d}{j} \binom{(k-j)n-j+d-1}{d-1}.$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

e. [5–] Are the coefficients of $i(\Delta_{k,d},n)$ nonnegative?
f. [2]* Let $A(\Delta_{k,d},x)$ be the $\Delta_{k,d}$-Eulerian polynomial. Show that $A(\Delta_{1,d},x)=1$.
g. [2+] Show that

$$A(\Delta_{2,d},x)=\begin{cases}1+\frac{1}{2}d(d-3)x+\binom{d}{4}x^2+\binom{d}{6}x^3+\cdots+\binom{d}{d}x^{d/2}, & d \text{ even},\\ 1+\frac{1}{2}d(d-3)x+\binom{d}{4}x^2+\binom{d}{6}x^3+\cdots+\binom{d}{d-1}x^{(d-1)/2}, & d \text{ odd}.\end{cases}$$

h. [5–] Find a combinatorial interpretation of the coefficients of $A(\Delta_{k,d},x)$.
i. [3] Define the "half-open" hypersimplex $\Delta'_{k,d}$ to be the set of all vectors $(x_1,\ldots,x_d)\in\mathbb{R}^d$ satisfying $0\le x_i\le 1$ and

$$\begin{array}{rcccl} 0 & \le & x_1+\cdots+x_d & \le & 1,\ k=1,\\ k-1 & < & x_1+\cdots+x_d & \le & k,\ 2\le k\le d.\end{array}$$

Thus, the unit cube $[0,1]^d$ is a disjoint union of the $\Delta'_{k,d}$'s. Show that

$$A(\Delta'_{k,d},x)=\sum_w x^{\mathrm{des}(w)},$$

where w ranges over all permutations in $\mathfrak{S}_d$ with $k-1$ excedances. For instance, $A(\Delta'_{3,4},x)=4x+6x^2+x^3$, corresponding to the permutations 2314, 2413, 3412, 1342 (one descent), 2431, 3421, 2143, 3142, 3241, 4312 (two descents), and 4321 (three descents).

63. [3] Let $v_1,\ldots,v_k\in\mathbb{Z}^m$. Let

$$\mathcal{Z}=\{a_1v_1+\cdots+a_kv_k : 0\le a_i\le 1\}.$$

Thus, $\mathcal{Z}$ is a convex polytope with integer vertices. Show that the Ehrhart polynomial of $\mathcal{Z}$ is given by $i(\mathcal{Z},n)=c_mn^m+\cdots+c_0$, where $c_i=\sum_X f(X)$, the sum being over all linearly independent i-element subsets X of $\{v_1,\ldots,v_k\}$, and where $f(X)$ is the greatest common divisor (always taken to be positive) of the determinants of the $i\times i$ submatrices of the matrix whose rows are the elements of X.

64. **a.** [3] Let $\mathcal{P}_d$ denote the convex hull in $\mathbb{R}^d$ of the $d!$ points $(w(1),w(2),\ldots,w(d))$, $w\in\mathfrak{S}_d$. The polytope $\mathcal{P}_d$ is called the *permutohedron*. Show that the Ehrhart polynomial of $\mathcal{P}_d$ is given by

$$i(\mathcal{P}_d,n)=\sum_{i=0}^{d-1}f_in^i,$$

where f_i is the number of forests with i edges on a set of d vertices. For example, $f_0=1$, $f_1=\binom{d}{2}$, $f_{d-1}=d^{d-2}$. In particular, the relative volume of $\mathcal{P}_d$ is d^{d-2}.
b. [3] Generalize (a) as follows. Let G be a finite graph (loops and multiple edges permitted) with vertices $v_1,\ldots,v_d$. An *orientation* $\mathfrak{o}$ of the edges may be regarded as an assignment of a direction $u\to v$ to every edge e of G, where e is incident to vertices u and v. If in the orientation $\mathfrak{o}$ there are δ_i edges pointing out of v_i, then call $\delta(\mathfrak{o})=(\delta_1,\ldots,\delta_d)$ the *outdegree sequence* of $\mathfrak{o}$. Define $\mathfrak{o}$ to be *acyclic* if there are no directed cycles $u_1\to u_2\to\cdots\to u_k\to u_1$, as in Exercise 3.60. Let $\mathcal{P}_G$ denote

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

the convex hull in $\mathbb{R}^d$ of all outdegree sequences $\delta(\mathfrak{o})$ of acyclic orientations of G. Show that

$$i(\mathcal{P}_G, n) = \sum_{i=0}^{d-1} f_i(G) n^i,$$

where $f_i(G)$ is the number of spanning forests of G with i edges. Show also that

$$\mathcal{P}_G \cap \mathbb{Z}^d = \{\delta(\mathfrak{o}) : \mathfrak{o} \text{ is an orientation of } G\},$$

and deduce that the number of distinct $\delta(\mathfrak{o})$ is equal to the number of spanning forests of G. (Note that (a) corresponds to the case $G = K_d$.)

65. [3] An *FHM-graph* is a graph G (allowing multiple edges, but not loops) such that every induced subgraph has at most one connected component that is not bipartite. A *spanning quasiforest* of a graph G is a spanning subgraph H of G for which every connected component is either a tree or has exactly one cycle C, such that C has odd length. Let $c(H)$ denote the number of (odd) cycles of the quasiforest H. If H is a graph with vertices $v_1, \ldots, v_p$ and q edges, then the *extended degree sequence* of H is the sequence $\tilde{d}(H) = (d_1, \ldots, d_p, q) \in \mathbb{R}^{p+1}$, where v_i has degree (number of incident edges) d_i. Let $\widetilde{\mathcal{D}}(G)$ denote the convex hull in $\mathbb{R}^p$ of the extended degree sequence $\tilde{d}(H)$ of all spanning subgraphs H of G. Show that if G is an FHM-graph, then

$$i(\widetilde{\mathcal{D}}(G), n) = a_p n^p + a_{p-1} n^{p-1} + \cdots + a_0, \tag{4.58}$$

where

$$a_i = \sum_H \max\{1, 2^{c(H)-1}\},$$

the sum being over all spanning quasiforests H of G with i edges.

66. **a.** [3] Let $\mathcal{P}$ be a d-dimensional rational convex polytope in $\mathbb{R}^m$, and let the Ehrhart quasipolynomial of $\mathcal{P}$ be

$$i(\mathcal{P}, n) = c_d(n) n^d + c_{d-1}(n) n^{d-1} + \cdots + c_0(n),$$

where $c_0, \ldots, c_d$ are periodic functions of n. Suppose that for some $j \in [0, d]$, the affine span of every j-dimensional face of $\mathcal{P}$ contains a point with integer coordinates. Show that if $k \geq j$, then $c_k(n)$ is constant (i.e., period one).

b. [3] Generalize (a) as follows: the (not necessarily least) period of $c_i(n)$ is the least positive integer p such that each i-face of $p\mathcal{P}$ contains an integer vector.

67. [2]* Let M be a diagonalizable $p \times p$ matrix over a field K. Let $\lambda_1, \ldots, \lambda_r$ be the distinct nonzero eigenvalues of M. Fix $(i, j) \in [p] \times [p]$. Show that there exist constants $a_1, \ldots, a_r \in K$ such that for all $n \in \mathbb{P}$,

$$(M^n)_{ij} = a_1 \lambda_1^n + \cdots + a_r \lambda_r^n.$$

68. **a.** [2]* By combinatorial reasoning, find the number $f(r, n)$ of sequences $\emptyset = S_0, S_1, \ldots, S_{2n} = \emptyset$ of subsets of $[r]$ such that for each $1 \leq i \leq 2n$, either $S_{i-1} \subset S_i$ and $|S_i - S_{i-1}| = 1$, or $S_i \subset S_{i-1}$ and $|S_{i-1} - S_i| = 1$.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

b. [2]* Let $A(r)$ be the adjacency matrix of the Hasse diagram of the boolean algebra B_r. Thus, the rows and columns of $A(r)$ are indexed by $S \in B_r$, with

$$A(r)_{S,T} = \begin{cases} 1, & \text{if } S \text{ covers } T \text{ or } T \text{ covers } S \text{ in } B_r, \\ 0, & \text{otherwise.} \end{cases}$$

Use (a) to find the eigenvalues of $A(r)$. (It is more customary to use (b) to solve (a).)

69. [2]* Use reasoning similar to the previous exercise to find the eigenvalues of the adjacency matrix of the complete bipartite graph K_{rs}. Thus, first compute the number of closed walks of length ℓ in K_{rs}.

70. a. [2+] Let G be a finite graph (allowing loops and multiple edges). Suppose that there is some integer $\ell > 0$ such that the number of walks of length ℓ from any fixed vertex u to any fixed vertex v is independent of u and v. Show that G has the same number k of edges between any two vertices (including k loops at each vertex).

b. [3–] Again let G be a finite graph (allowing loops and multiple edges). For any vertex v, let d_v be its degree (number of incident edges). Start at any vertex of G and do a random walk as follows: If we are at a vertex v, then walk along an edge incident to v with probability $1/d_v$. Suppose that there is some integer $\ell \geq 1$ such that for any intial vertex u, after we take ℓ steps we are equally likely to be at any vertex. Show that we have the same conclusion as (a) (i.e., G has the same number k of edges between any two vertices).

71. [2+] Let K_p^o denote the complete graph with p vertices, with one loop at each vertex. Let $K_p^o - K_r^o$ denote K_p^o with the edges of K_r^o removed, i.e., choose r vertices of K_p^o, and remove all edges between these vertices (including loops). Thus, $K_p^o - K_r^o$ has $\binom{p+1}{2} - \binom{r+1}{2}$ edges. Find the number $C_G(\ell)$ of closed walks in $G = K_{21}^o - K_{18}^o$ of length $\ell \geq 1$.

72. [3–] Let G be a finite graph on p vertices. Let G' be the graph obtained from G by placing a new edge e_v incident to each vertex v, with the other vertex of e_v being a new vertex v'. Thus, G' has p new edges and p new vertices. The new vertices all have degree one. By combinatorial reasoning, express the eigenvalues of the adjacency matrix $A(G')$ in terms of the eigenvalues of $A(G)$.

73. a. [2]* Let $F(n)$ be the number of ways a $2 \times n$ chessboard can be partitioned into copies of the two pieces  and  . (Any rotation or reflection of the pieces is allowed.) For instance, $f(0) = 1$, $f(1) = 1$, $f(2) = 2$, $f(3) = 5$. Find $F(x) = \sum_{n \geq 0} f(n)x^n$.

b. [2]* Let $g(n)$ be the number of ways if we also allow the piece  . Thus, $g(0) = 1$, $g(1) = 2$, $g(2) = 11$. Find $G(x) = \sum_{n \geq 0} g(n)x^n$.

74. [2+] Suppose that the graph G has 16 vertices and that the number of closed walks of length ℓ in G is $8^\ell + 2 \cdot 3^\ell + 3 \cdot (-1)^\ell + (-6)^\ell + 5$ for all $\ell \geq 1$. Let G' be the graph obtained from G by adding a loop at each vertex (in addition to whatever loops are already there). How many closed walks of length ℓ are there in G'? Give a linear algebraic solution and (more difficult) a combinatorial solution.

75. a. [2+] Let $M = (m_{ij})$ be an $n \times n$ circulant matrix with first row $(a_0, \ldots, a_{n-1}) \in \mathbb{C}^n$, that is, $m_{ij} = a_{j-i}$, the subscript $j - i$ being taken modulo n. Let $\zeta = e^{2\pi i/n}$. Show that the eigenvalues of M are given by

$$\omega_r = \sum_{j=0}^{n-1} a_j \zeta^{jr}, \quad 0 \leq r \leq n-1.$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

b. [1] Let $f_k(n)$ be the number of sequences of integers $t_1, t_2, \ldots, t_n$ modulo k (i.e., $t_j \in \mathbb{Z}/k\mathbb{Z}$) such that $t_{j+1} \equiv t_j - 1, t_j$, or $t_j + 1 \pmod{k}$, $1 \le j \le n-1$. Find $f_k(n)$ explicitly.

c. [2] Let $g_k(n)$ be the same as $f_k(n)$, except that in addition we require $t_1 \equiv t_n - 1$, t_n, or $t_n + 1 \pmod{k}$. Use the transfer-matrix method to show that

$$g_k(n) = \sum_{r=0}^{k-1} \left(1 + 2\cos\frac{2\pi r}{k}\right)^n.$$

d. [5–] From (c) we get $g_4(n) = 3^n + 2 + (-1)^n$ and $g_6(n) = 3^n + 2^{n+1} + (-1)^n$. Is there a combinatorial proof?

76. a. [2+] Let $A = A(n)$ be the $n \times n$ real matrix given by

$$A_{ij} = \begin{cases} 1, & j = i+1 \ (1 \le i \le n-1), \\ 1, & j = i-1 \ (2 \le i \le n), \\ 0, & \text{otherwise.} \end{cases}$$

Thus, A is the adjacency matrix of an n-vertex path. Let $V_n(x) = \det(xI - A)$, so $V_0(x) = 1$, $V_1(x) = x$, $V_2(x) = x^2 - 1$, $V_3(x) = x^3 - 2x$. Show that $V_{n+1}(x) = xV_n(x) - V_{n-1}(x)$, $n \ge 1$.

b. [2+]* Show that

$$V_n(2\cos\theta) = \frac{\sin((n+1)\theta)}{\sin(\theta)}.$$

Deduce that the eigenvalues of $A(n)$ are $2\cos(j\pi/(n+1))$, $1 \le j \le n$.

c. [2–] Let $u_n(k)$ be the number of sequences of integers $t_1, t_2, \ldots, t_k$, $1 \le t_i \le n$, such that $t_{j+1} = t_j - 1$ or $t_j + 1$ for $1 \le j \le n-1$, and $t_k = t_1 - 1$ or $t_1 + 1$ (if defined, i.e., 1 can be followed only by 2, and n by $n-1$). Find $u_n(k)$ explicitly.

d. [2+] Find a simple formula for $u_{2n}(2n)$.

77. [2]* Let $f_p(n)$ be as in Example 4.7.5. Give a simple combinatorial proof that $f_p(n-1) + f_p(n) = p(p-1)^{n-1}$, and deduce from this the formula $f_p(n) = (p-1)^n + (p-1)(-1)^n$ (equation (4.36)).

78. a. [2] Let $g_k(n)$ denote the number of $k \times n$ matrices $(a_{ij})_{1 \le i \le k,\ 1 \le j \le n}$ of integers such that $a_{11} = 1$, the rows and columns are weakly increasing, and adjacent entries differ by at most 1. Thus, $a_{i,j+1} - a_{ij} = 0$ or 1, and $a_{i+1,j} - a_{ij} = 0$ or 1. Show that $g_2(n) = 2 \cdot 3^{n-1}$, $n \ge 1$.

b. [2+] Show that $G_k(x) = \sum_{n \ge 1} g_k(n) x^n$ is a rational function. In particular,

$$G_3(x) = \frac{2x(2-x)}{1 - 5x + 2x^2}.$$

79. a. [2+] Let $G_1, \ldots, G_k$ be finite graphs on the vertex sets $V_1, \ldots, V_k$. Given any graph H, write $m(u,v)$ for the number of edges between vertices u and v. Let $u = (u_1, \ldots, u_k) \in V_1 \times \cdots \times V_k$ and $v = (v_1, \ldots, v_k) \in V_1 \times \cdots \times V_k$. Define the *star product* $G_1 * \cdots * G_k$ of $G_1, \ldots, G_k$ to be the graph on the vertex set $V_1 \times \cdots \times V_k$ with edges defined by

$$m(u,v) = \begin{cases} 0, & \text{if } u, v \text{ differ in at least two coordinates,} \\ \sum_i m(u_i, u_i), & \text{if } u = v, \\ m(u_i, v_i), & \text{if } u, v \text{ differ only in coordinate } i. \end{cases}$$

Find the eigenvalues of the adjacency matrix $A(G_1 * \cdots * G_k)$ in terms of the eigenvalues of $A(G_1), \ldots, A(G_k)$.

b. [2+] Let $V_i = [m_i]$, and regard $B = V_1 \times \cdots \times V_k$ as a k-dimensional chessboard. A rook moves from a vertex u of B to any other vertex v that differs from u in

exactly one coordinate. Suppose without loss of generality that $u = (1, 1, \ldots, 1)$ and $v = (1^{k-r}, 2^r)$ (i.e., a vector of $k-r$ 1's followed by r 2's). Find an explicit formula for the number N of ways a rook can move from u to v in exactly n moves.

80. [2+] As in Exercise 4.40, let $X = \{x_1, \ldots, x_n\}$ be an alphabet with n letters. Let N be a finite set of words. Define $f_N(m)$ to be the number of words $w \in X_m^*$ (i.e., of length m) such that w contains no subwords (as defined in Exercise 3.134) belonging to N. Use the transfer-matrix method to show that $F_N(x) := \sum_{m \geq 0} f_N(m) x^m$ is rational.

81. **a.** [2] Fix $k \in \mathbb{P}$, and for $n \in \mathbb{N}$ define $f_k(n)$ to be the number of ways to cover a $k \times n$ chessboard with $\frac{1}{2}kn$ nonoverlapping dominoes (or *dimers*). Thus, $f_k(n) = 0$ if kn is odd, $f_1(2n) = 1$, and $f_2(2) = 2$. Set $F_k(x) = \sum_{n \geq 0} f_k(n) x^n$. Use the transfer-matrix method to show that $F_k(x)$ is rational. Compute $F_k(x)$ for $k = 2, 3, 4$.

b. [3] Use the transfer-matrix method to show that

$$f_k(n) = \prod_{j=1}^{\lfloor k/2 \rfloor} \frac{c_j^{n+1} - \bar{c}_j^{n+1}}{2b_j}, \quad nk \text{ even}, \tag{4.59}$$

where

$$\begin{aligned} c_j &= a_j + \sqrt{1 + a_j^2}, \\ \bar{c}_j &= a_j - \sqrt{1 + a_j^2}, \\ b_j &= \sqrt{1 + a_j^2}, \\ a_j &= \cos \frac{j\pi}{k+1}. \end{aligned}$$

c. [3–] Use (b) to deduce that we can write $F_k(x) = P_k(x)/Q_k(x)$, where P_k and Q_k are polynomials with the following properties:

i. Set $\ell = \lfloor k/2 \rfloor$. Let $S \subseteq [\ell]$ and set $\overline{S} = [\ell] - S$. Define

$$c_S = \left(\prod_{j \in S} c_j \right) \left(\prod_{j \in \overline{S}} \bar{c}_j \right).$$

Then

$$Q_k(x) = \begin{cases} \displaystyle\prod_S (1 - c_S x), & k \text{ even}, \\ \displaystyle\prod_S (1 - c_S^2 x^2), & k \text{ odd}, \end{cases}$$

where S ranges over all subsets of $[\ell]$.

ii. $Q_k(x)$ has degree $q_k = 2^{\lfloor (k+1)/2 \rfloor}$.

iii. $P_k(x)$ has degree $p_k = q_k - 2$.

iv. If $k > 1$, then $P_k(x) = -x^{p_k} P_k(1/x)$. If k is odd or divisible by 4, then $Q_k(x) = x^{q_k} Q_k(1/x)$. If $k \equiv 2 \pmod 4$ then $Q_k(x) = -x^{q_k} Q_k(1/x)$. If k is odd, then $P_k(x) = P_k(-x)$ and $Q_k(x) = Q_k(-x)$.

82. For $n \geq 2$, let T_n be the $n \times n$ toroidal graph, that is, the vertex set is $(\mathbb{Z}/n\mathbb{Z})^2$, and (i, j) is connected to its four neighbors $(i-1, j)$, $(i+1, j)$, $(i, j-1)$, $(i, j+1)$ with entries modulo n. (Thus, T_n has n^2 vertices and $2n^2$ edges.) Let $\chi_n(\lambda)$ denote the chromatic polynomial of T_n, and set $N = n^2$.

a. [1+] Find $\chi_n(2)$.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

b. [3+] Use the transfer-matrix method to show that

$$\log \chi_n(3) = \frac{3N}{2} \log(4/3) + o(N).$$

c. [5] Show that

$$\log \chi_n(3) = \frac{3N}{2} \log(4/3) - \frac{\pi}{6} + o(1).$$

d. [5] Find $\lim_{N\to\infty} N^{-1} \log \chi_n(4)$.

e. [3–] Let $\chi_n(\lambda) = \lambda^N - q_1(N)\lambda^{N-1} + q_2(N)\lambda^{N-2} - \cdots$. Show that there are polynomials $Q_i(N)$ such that $q_i(N) = Q_i(N)$ for all N sufficiently large (depending on i). For instance, $Q_1(N) = 2N$, $Q_2(N) = N(2N-1)$, and $Q_3(N) = \frac{1}{3}N(4N^2 - 6N - 1)$.

f. [3] Let $\alpha_i = Q_i(1)$. Show that

$$\begin{aligned} 1 + \sum_{i\geq 1} Q_i(N)x^i &= (1 + \alpha_1 x + \alpha_2 x^2 + \cdots)^N \\ &= (1 + 2x + x^2 - x^3 + x^4 - x^5 + x^6 - 2x^7 + 9x^8 - 38x^9 \\ &\quad + 130x^{10} - 378x^{11} + 987x^{12} - 2436x^{13} + 5927x^{14} \\ &\quad - 14438x^{15} + 34359x^{16} - 75058x^{17} \\ &\quad + 134146x^{18} + \cdots)^N. \end{aligned} \tag{4.60}$$

Equivalently, in the terminology of Exercise 5.37, the sequence $1, 1! \cdot Q_1(N), 2! \cdot Q_2(N), \ldots$ is a sequence of polynomials of binomial type.

g. [5–] Let $L(\lambda) = \lim_{N\to\infty} \chi_n(\lambda)^{1/N}$. Show that for $\lambda \geq 2$, $L(\lambda)$ has the asymptotic expansion

$$L(\lambda) \sim \lambda(1 - \alpha_1\lambda^{-1} + \alpha_2\lambda^{-2} + \cdots).$$

Does this infinite series converge?

Solutions to Exercises

1. No. Suppose that $F(x) \in K(x)$ and $G(x) \in L(x)$, where K and L are fields of different characteristics (or even isomorphic fields but with no explicit isomorphism given, such as $\mathbb{C}$ and the algebraic closure of the p-adic field $\mathbb{Q}_p$). Then $F(x) + G(x)$ is undefined.

2. **a.** Define a formal power series $\sum_{n\geq 0} a_n x^n$ with integer coefficients to be *primitive* if no integer $d > 1$ divides *all* the a_i. One easily shows that the product of primitive series is primitive (a result essentially due to Gauss but first stated explicitly by Hurwitz; this result is equivalent to the statement that $\mathbb{F}_p[[x]]$ is an integral domain, where $\mathbb{F}_p$ is the field of prime order p).

Clearly, we can write $f(x) = P(x)/Q(x)$ for some relatively prime integer polynomials P and Q. Assume that no integer $d > 1$ divides every coefficient of P and Q. Then Q is primitive, for otherwise if $Q/d \in \mathbb{Z}[x]$ for $d > 1$, then

$$\frac{P}{d} = f\frac{Q}{d} \in \mathbb{Z}[x],$$

a contradiction. Since $(P, Q) = 1$ in $\mathbb{Q}[x]$, there is an integer $m > 0$ and polynomials $A, B \in \mathbb{Z}[x]$ such that $AP + BQ = m$. Then $m = Q(Af + B)$. Since Q is primitive, the coefficients of $Af + B$ are divisible by m. (Otherwise, if $d < m$ is the largest

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

integer dividing $Af + B$, then the product of the primitive series Q and $(Af + B)/d$ would be the imprimitive polynomial $m/d > 1$.) Let c be the constant term of $Af + B$. Then $m = Q(0)c$. Since m divides c, we have $Q(0) = \pm 1$.

This result is known as *Fatou's lemma* and was first proved in P. Fatou, *Acta Math.* **30** (1906), 369. The proof given here is due to A. Hurwitz; see G. Pólya, *Math. Ann.* **77** (1916), 510–512.

b. This result, while part of the "folklore" of algebraic geometry and an application of standard techniques of commutative algebra, seems first to be explicitly stated and proved (in an elementary way) by I. M. Gessel, *Utilitas Math.* **19** (1981), 247–251 (Thm. 1).

3. The assertion is true. Without loss of generality we may assume that $f(x)$ is primitive, as defined in the solution to Exercise 4.2. Let $f'(x) = f(x)g(x)$, where $g(x) \in \mathbb{Z}[[x]]$. By Leibniz's rule for differentiating a product, we obtain by induction on n that $f(x)|f^{(n)}(x)$ in $\mathbb{Z}[[x]]$. But also $n!|f^{(n)}(x)$, since if $f(x) = \sum a_i x^i$ then $\frac{1}{n!} f^{(n)}(x) = \sum \binom{i}{n} a_i x^{i-n}$. Write $f(x)h(x) = n!(f^{(n)}(x)/n!)$, where $h(x) \in \mathbb{Z}[[x]]$. Since the product of primitive polynomials is primitive, we obtain just as in the solution to Exercise 4.2 that $n!|h(x)$ in $\mathbb{Z}[[x]]$, so $f(x)|(f^{(n)}(x)/n!)$. In particular, $f(0)|(f^{(n)}(0)/n!)$ in $\mathbb{Z}$, which is the desired conclusion.

NOTE. An alternative proof uses the known fact that $\mathbb{Z}[[x]]$ is a unique factorization domain. Since $f(x)|f^{(n)}(x)$, and since $f(x)$ and $n!$ are relatively prime in $\mathbb{Z}[[x]]$, we get $n!f(x)|f^{(n)}(x)$.

This exercise is due to David Harbater.

4. **a.** This result was first proved by T. A. Skolem, *Oslo Vid. Akad. Skrifter I*, no. 6 (1933), for rational coefficients, then by K. Mahler, *Proc. Akad. Wetensch. Amsterdam* **38** (1935), 50–60, for algebraic coefficients, and finally independently by Mahler, *Proc. Camb. Phil. Soc.* **52** (1956), 39–48, and C. Lech, *Ark. Math.* **2** (1953), 417–421, for complex coefficients (or over any field of characteristic 0) and is known as the *Skolem-Mahler-Lech theorem*. All the proofs use p-adic methods. As pointed out by Lech, the result is false over characteristic p, an example being the series

$$F(x) = \frac{1}{1-(t+1)x} - \frac{1}{1-x} - \frac{1}{1-tx}$$

over the field $\mathbb{F}_p(t)$. See also J.-P. Serre, *Proc. Konin. Neder. Akad. Weten. (A)* **82** (1979), 469–471.

For an interesting article on the Skolem–Mahler–Lech theorem, see G. Myerson and A. J. van der Poorten, *Amer. Math. Monthly* **102** (1995), 698–705. For a proof, see J. W. S. Cassels, *Local Fields*, Cambridge University Press, Cambridge, 1986. For further information on coefficients of rational generating functions, see A. J. van der Poorten, in Coll. Math. Sci. János Bolyai **34**, *Topics in Classical Number Theory* (G. Hal'asz, ed.), vol. 2, North-Holland, New York, 1984, pp. 1265–1294. (This paper, however, contains many inaccuracies, beginning on page 1276.)

b. Let

$$\begin{aligned} F(x,y) &= \sum_{m,n\geq 0} (m-n^2)x^m y^n \\ &= \frac{1}{(1-x)^2(1-y)} - \frac{y+y^2}{(1-x)(1-y)^3}. \end{aligned}$$

Then

$$\sum_{m,n\geq 0} \chi(m-n^2)x^m y^n = \sum x^{m^2} y^n,$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

which is seen to be nonrational, for example, by setting $y = 1$ and using (a). This problem was suggested by D. A. Klarner.

c. A proof based on the same p-adic methods used to prove (a) is sketched by A. J. van der Poorten, *Bull. Austral. Math. Soc.* **29** (1984), 109–117.

5. This problem was raised by T. Skolem, *Skand. Mat. Kongr. Stockholm, 1934* (1934), 163–188. For the current status of this problem, see V. Halava, T. Harju, M. Hirvensalo, and J. Karhumäki, Skolem's problem—On the border between decidability and undecidability, preprint.

6. This fundamental result is due to L. Kronecker, *Monatsber. K. Preuss. Akad. Wiss. Berlin* (1881), 535–600. For an exposition, see F. R. Gantmacher, *Matrix Theory*, vol. 2, Chelsea, New York, 1989 (§XV.10).

7. **a.** Write

$$\frac{xF'(x)}{F(x)} = \frac{b_1 x}{1-x} + G(x). \tag{4.61}$$

where $G(x) = \sum_{n\geq 1} c_n x^n$. By arguing as in Example 1.1.14, we have

$$c_n = \sum_{\substack{(2i-1)|n \\ i\neq 1}} (2i-1)b_i.$$

If n is a power of 2 then this sum is empty and $c_n = 0$; otherwise, $c_n \neq 0$. By Exercise 4.4, $G(x)$ is not rational. Hence by equation (4.61), $F(x)$ is not rational.

This result is essentially due to J.-P. Serre, *Proc. Konin. Neder. Akad. Weten. (A)* **82** (1979), 469–471.

b. Let $F(x) = 1/(1-\alpha x)$, where $\alpha \geq 2$. Then by the same reasoning as Example 1.1.14, we have that $a_i \in \mathbb{Z}$ and

$$\begin{aligned} a_i &= \frac{1}{i}\sum_{d|i} \mu(i/d)\alpha^d \\ &\geq \frac{1}{i}\left(\alpha^i - \sum_{j=1}^{i-1} \alpha^j\right) > 0. \end{aligned}$$

It is also possible to interpret a_i combinatorially when $\alpha \geq 2$ is an integer (or a prime power) and thereby see combinatorially that $a_i > 0$. See Exercise 2.7 for the case when α is a prime power.

8. (i)⇒(iii) If $F(x) \in \mathbb{C}[[x]]$ and $F(x) = G'(x)/G(x)$ with $G(x) \in \mathbb{C}((x))$, then $G(0) \neq 0, \infty$. Hence, if $G(x)$ is rational, then we can write

$$G(x) = \frac{c\prod(1-\beta_i x)}{\prod(1-\alpha_i x)}$$

for certain nonzero $\alpha_i, \beta_i \in \mathbb{C}$. Direct computation yields

$$\frac{G'(x)}{G(x)} = \sum \frac{\alpha_i}{1-\alpha_i x} - \sum \frac{\beta_i}{1-\beta_i x},$$

so $a_n = \sum \alpha_i^n - \sum \beta_i^n$.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

(iii)⇒(ii) If $a_n = \sum \alpha_i^n - \sum \beta_i^n$. then

$$\exp \sum_{n \geq 1} a_n \frac{x^n}{n} = \frac{\prod (1 - \beta_i x)}{\prod (1 - \alpha_i x)}$$

by direct computation.
(ii)⇒(i) Set $G(x) = \exp \sum_{n \geq 1} a_n \frac{x^n}{n}$ and compute that

$$F(x) = \frac{d}{dx} \log G(x) = \frac{G'(x)}{G(x)}.$$

9. Yes. Suppose that $F(x) = P(x)/Q(x)$, where $P, Q \in \mathbb{Q}[x]$. By the division algorithm for polynomials we have

$$F(x) = G(x) + \frac{R(x)}{Q(x)},$$

where $\deg R < \deg Q$ (with $\deg 0 = -\infty$, say). If $R(x) \neq 0$, then we can find positive integer p, n for which $pG(n) \in \mathbb{Z}$ and $0 < |R(n)/Q(n)| < 1/p$, a contradiction.

10. This result is due to E. Borel, *Bull. Sci. Math.* **18** (1894), 22–25. It is a useful tool for proving that generating functions are not meromorphic. For instance, let p_n be the nth prime and $f(z) = \sum_{n \geq 1} p_n z^n = 2z + 3z^2 + 5z^3 + \cdots$. It is easy to see that $f(z)$ has radius of convergence 1 and is not rational [why?]. Hence by Borel's theorem, $f(z)$ is not meromorphic.

11. **a.** *Answer.* $a_n = 2^n + 1$. A standard way to solve this recurrence that does not involve guessing the answer in advance is to observe that the denominator of the rational function $\sum_{n \geq 0} a_n x^n$ is $1 - 3x + 2x^2 = (1 - x)(1 - 2x)$. Hence, $a_n = \alpha 2^n + \beta 1^n = \alpha 2^n + \beta$. The initial conditions give $\alpha + \beta = 2$, $2\alpha + \beta = 3$, whence $\alpha = \beta = 1$.

b. *Answer.* $a_n = n2^n$.

c. *Answer.* $a_n = 3^{n+1} + 2^n + 1$.

d. The polynomial $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ is just the 15th cyclotomic polynomial (i.e., its zeros are the primitive 15th roots of unity). It follows that the sequence $a_0, a_1, \ldots$ is periodic with period 15. Thus, we need only compute $a_8 = 4$, $a_9 = 0$, $a_{10} = -5, a_{11} = -7, a_{12} = -9, a_{13} = -7, a_{14} = -4$ to determine the entire sequence. In particular, since $105 \equiv 0 \pmod{15}$, we have $a_{105} = a_0 = 0$. To solve this problem without recognizing that $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$ is a cyclotomic polynomial, simply compute a_n for $8 \leq n \leq 22$. Since $a_n = a_{n+15}$ for $0 \leq n \leq 7$, it follows that $a_n = a_{n+15}$ for all $n \geq 0$.

12. Note that

$$\frac{10000}{9899} = \frac{1}{1 - \frac{1}{100} - \frac{1}{100^2}}$$

and

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

13. Because the Fibonacci recurrence can be run in reverse to compute F_i from F_{i+1} and F_{i+2}, and because there are only finitely many pairs $(a, b) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, it follows that the sequence $(F_i)_{i \in \mathbb{Z}}$ is periodic modulo n for all $n \in \mathbb{Z}$. Since $F_0 = 0$, it follows that some F_k for $k \geq 1$ must be divisible by n. Although there is an extensive literature on Fibonacci numbers modulo n (e.g., D. D. Wall, *Amer. Math. Monthly* **67** (1960), 525–532, and S. Gupta, P. Rockstroh, and F. E. Su, Splitting fields and periods of Fibonacci

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

sequences modulo primes, `arXiv:0909.0362`), it is not clear who first came up with the preceding elegant argument. Problem A3 from the 67th Putnam Mathematical Competition (2006) involves a similar idea. Note that the result of the present exercise fails for the Lucas numbers when $n = 5$. The foregoing proof breaks down because $L_i \neq 0$ for all $i \in \mathbb{Z}$.

14. The first such sequence was obtained by R. L. Graham, *Math. Mag.* **37** (1964), 322–324. At present the smallest pair (a,b) is due to J. W. Nicol, *Electronic J. Combinatorics* **6** (1999), #R44, namely,

$$a = 62638280004239857 = 127 \cdot 2521 \cdot 195642524071,$$
$$b = 49463435743205655 = 3 \cdot 5 \cdot 83 \cdot 89 \cdot 239 \cdot 1867785589.$$

15. Two solutions appear in R. Stanley, *Amer. Math. Monthly* **83** (1976), 813–814. The crucial lemma in the elementary solution given in this reference is that every antichain of $\mathbb{N}^m$ is finite.

16. Denote the answer by $f(n)$. The Young diagram of λ contains a 2×3 rectangle in the upper-left-hand corner. To the right of this rectangle is the diagram of a partition with at most two parts. Below the rectangle is the diagram of a partition with parts 1 and 2. Hence,

$$\begin{aligned}\sum_{n\geq 0} f(n)x^n &= \frac{x^6}{(1-x)^2(1-x^2)^2} \\ &= 1 + \frac{1}{4(1-x)^4} - \frac{5}{4(1-x)^3} + \frac{39}{16(1-x)^2} - \frac{9}{4(1-x)} \\ &\quad + \frac{1}{16(1+x)^2} - \frac{1}{4(1+x)}.\end{aligned}$$

It follows that for $n \geq 1$,

$$\begin{aligned}f(n) &= \frac{1}{4}\binom{n+3}{3} - \frac{5}{4}\binom{n+2}{2} + \frac{39}{16}(n+1) - \frac{9}{4} + \frac{1}{16}(-1)^n(n+1) - \frac{1}{4}(-1)^n \\ &= \frac{1}{48}\left(2n^3 - 18n^2 + 49n - 39\right) + \frac{1}{16}(-1)^n(n-3).\end{aligned}$$

This problem was suggested by A. Postnikov, private communication, 2007.

17. **b.** See Exercise 3.62 and I. M. Gessel and R. Stanley, *J. Combinatorial Theory, Ser. A* **24** (1978), 24–33. The polynomial $F_n(x)$ is called a *Stirling polynomial*.

21. See P. Tetali, *J. Combinatorial Theory Ser. B* **72** (1998), 157–159. For a connection with radar tracking, see T. Khovanova, Unique tournaments and radar tracking, `arXiv:0712.1621`.

23. **b.** This remarkable result is due to J. H. Conway, *Eureka* **46** (1986), 5–18, and §5.11 in *Open Problems in Communication and Computation* (T. M. Cover and B. Gopinath, eds.), Springer-Verlag, New York, 1987 (pp. 173–188). For additional references, see item A005150 of *The On-Line Encyclopedia of Integer Sequences*.

c. $F(x) = x^{71} - x^{69} - 2x^{68} - x^{67} + 2x^{66} + x^{64} - x^{63} - x^{62} - x^{61} - x^{60} - x^{59} + 2x^{58} + 5x^{57} + 3x^{56} - 2x^{55} - 10x^{54} - 3x^{53} - 2x^{52} + 6x^{51} + 6x^{50} + x^{49} + 9x^{48} - 3x^{47} - 7x^{46} - 8x^{45} - 8x^{44} + 10x^{43} + 6x^{42} + 8x^{41} - 5x^{40} - 12x^{39} + 7x^{38} - 7x^{37} + 7x^{36} + x^{35} - 3x^{34} + 10x^{33} + x^{32} - 6x^{31} - 2x^{30} - 10x^{29} - 3x^{28} + 2x^{27} + 9x^{26} - 3x^{25} +$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

$14x^{24} - 8x^{23} - 7x^{21} + x^{20} - 3x^{19} - 4x^{18} - 10x^{17} - 7x^{16} + 12x^{15} + 7x^{14} + 2x^{13} - 12x^{12} - 4x^{11} - 2x^{10} - 5x^9 + x^7 - 7x^6 + 7x^5 - 4x^4 + 12x^3 - 6x^2 + 3x - 6.$

d. For any initial sequence the generating function $F(x)$ is still rational, though now the behavior is more complicated and more difficult to analyze. See the references in (b).

24. a. Suppose that $a_0, a_1, \ldots$ is an infinite sequence of integers satisfying $0 \le a_i \le q-1$. Let $\mathcal{P}'$ be the Newton polytope of f, i.e., the convex hull in $\mathbb{R}^k$ of the exponent vectors of monomials appearing in f, and let $\mathcal{P}$ be the convex hull of $\mathcal{P}'$ and the origin. If $c > 0$, then write $c\mathcal{P} = \{cv : v \in \mathcal{P}\}$. Set $S = (q-1)\mathcal{P} \cap \mathbb{N}^k$ and $r_m = \sum_{i=0}^{m} a_i q^i$.

Suppose that $f(\boldsymbol{x})^{r_m} = \sum_\gamma c_{m,\gamma} \boldsymbol{x}^\gamma$. We set $f(\boldsymbol{x})^{r-1} = 1$. Let $\mathbb{F}_q^S$ be the set of all functions $F\colon S \to \mathbb{F}_q$. We will index our matrices and vectors by elements of $\mathbb{F}_q^S$ (in some order). Set

$$R_m = \{0, 1, \ldots, q^{m+1} - 1\}^k.$$

For $m \ge -1$, define a column vector ψ_m by letting $\psi_m(F)$ (the coordinate of ψ_m indexed by $F \in \mathbb{F}_q^S$) be the number of vectors $\gamma \in R_m$ such that for all $\delta \in S$ we have $c_{m,\gamma+q^{m+1}\delta} = F(\delta)$. Note that by the definition of S we have $c_{m,\gamma+q^{m+1}\delta} = 0$ if $\delta \notin S$. (This is the crucial finiteness condition that allows our matrices and vectors to have a fixed finite size.) Note also that given m, every point η in $\mathbb{N}^k$ can be written uniquely as $\eta = \gamma + q^{m+1}\delta$ for $\gamma \in R_{m+1}$ and δ in $\mathbb{N}^k$.

For $0 \le i \le q-1$ define a matrix Φ_i with rows and columns indexed by $\mathbb{F}_q^S$ as follows. Let $F, G \in \mathbb{F}_q^S$. Set

$$\begin{aligned} g(\boldsymbol{x}) &= f(\boldsymbol{x})^i \sum_{\beta \in S} G(\beta) \boldsymbol{x}^\beta \\ &= \sum_\gamma d_\gamma \boldsymbol{x}^\gamma \in \mathbb{F}_q[\boldsymbol{x}]. \end{aligned}$$

Define the (F,G)-entry $(\Phi_i)_{FG}$ of Φ_i to be the number of vectors $\gamma \in R_0 = \{0, 1, \ldots, q-1\}^k$ such that for all $\delta \in S$ we have $d_{\gamma+q\delta} = F(\delta)$. A straightforward computation shows that

$$\Phi_{a_m} \psi_{m-1} = \psi_m, \quad m \ge 0. \tag{4.62}$$

Let $u = u_\alpha$ be the row vector for which $u(F)$ is the number of values of F equal to α, and let $n = a_0 + a_1 q + \cdots + a_r q^r$ as in the statement of the theorem. Then it follows from equation (4.62) that

$$N_\alpha(n) = u \Phi_{a_r} \Phi_{a_{r-1}} \cdots \Phi_{a_0} \psi_{-1},$$

completing the proof.

This proof is an adaptation of an argument of Y. Moshe, *Discrete Math.* **297** (2005), 91–103 (Theorem 1) and appears in T. Amdeberhan and R. Stanley, Polynomial coefficient enumeration, preprint, dated 3 February 2008;

⟨`http://math.mit.edu/~rstan/papers/coef.pdf`⟩ (Theorem 2.1).

25. See T. Amdeberhan and R. Stanley, ibid. (Theorem 2.8), where the result is given in the slightly more general context of the polynomial $f(x)^{q^n - c}$ for $c \in \mathbb{P}$.

26. a. The case $n = 5$ was obtained by G. Bagnera, *Ann. di Mat. pura e applicata* (3) **1** (1898), 137–228. The case $n = 6$ is due to M. F. Newman, E. A. O'Brien, and M. R. Vaughan-Lee, *J. Algebra* **278** (2004), 283–401. The case $n = 7$ is due to E. A. O'Brien and M. R. Vaughan-Lee, *J. Algebra* **292** (2005), 243–258. An interesting book on enumerating groups of order n is S. R. Blackburn, P. M. Neumann,

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

and G. Venkataraman, *Enumeration of Finite Groups*, Cambridge University Press, Cambridge, 2007.

b. The lower bound $g_n(p) \geq p^{\frac{2}{27}n^2(n-6)}$ is due to G. Higman, *Proc. London Math. Soc.* (3) **10** (1960), 24–30. The upper bound with the error term $O(n^{8/3})$ in the exponent is due to C. C. Sims, *Proc. London Math. Soc. (3)* **15** (1965), 151–166. The improved error term $O(n^{5/2})$ is due to M. F. Newman and C. Seeley, appearing in Blackburn, et al., ibid. (Chapter 5).

c. This is a conjecture of G. Higman, ibid. (page 24). See also Higman, *Proc. London Math. Soc.* **10** (1960), 566–582.

27. a. Follows from J. Backelin, *C. R. Acad. Sc. Paris* **287(A)** (1978), 843–846.

b. The first example was given by J. B. Shearer, *J. Algebra* **62** (1980), 228–231. A nice survey of this subject is given by J.-E. Roos, in *18th Scandanavian Congress of Mathematicians* (E. Balslev, ed.), *Progress in Math.*, vol. 11, Birkhäuser, Boston, 1981, pp. 441–468.

c. Using Theorems 4 and 6 of D. E. Knuth, *Pacific J. Math.* **34** (1970), 709–727, one can give a bijection between words in M of length n and symmetric $q \times q$ $\mathbb{N}$-matrices whose entries sum to n. It follows that

$$F(x) = \frac{1}{(1-x)^q (1-x^2)^{\binom{q}{2}}}.$$

See Corollary 7.13.6 and Section A1.1 (Appendix 1) of Chapter 7.

d. This result is a direct consequence of a result of Hilbert-Serre on the rationality of the Hilbert series of commutative finitely generated graded algebras. See, for example, M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, Mass., 1969 (Theorem 11.1); W. Bruns and J. Herzog, *Cohen–Macaulay Rings*, Cambridge University Press, Cambridge, 1993 (Chapter 4); and D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York, 1995 (Exercise 10.12).

28. a. We have

$$\begin{aligned} T_r(\boldsymbol{x},\boldsymbol{y}) &= \operatorname{tr} \sum A^{\alpha_1} B^{\beta_1} \cdots A^{\alpha_r} B^{\beta_r} \boldsymbol{x}^{\boldsymbol{\alpha}} \boldsymbol{y}^{\boldsymbol{\beta}} \\ &= \operatorname{tr} \left(\sum A^{\alpha_1} x_1^{\alpha_1} \right) \left(\sum B^{\beta_1} y_1^{\beta_1} \right) \cdots \left(\sum A^{\alpha_r} x_r^{\alpha_r} \right) \left(\sum B^{\beta_r} y_r^{\beta_r} \right) \\ &= \operatorname{tr} (1 - Ax_1)^{-1} (1 - By_1)^{-1} \cdots (1 - Ax_r)^{-1} (1 - By_r)^{-1}. \end{aligned}$$

Now for any invertible matrix M, the entries of M^{-1} are rational functions (with denominator $\det M$) of the entries of M. Hence, the entries of $(1 - Ax_1)^{-1} \cdots (1 - By_r)^{-1}$ are rational functions of $\boldsymbol{x}$ and $\boldsymbol{y}$ with coefficients in $\mathbb{C}$, so the trace has the same property. The denominator of $T_r(\boldsymbol{x},\boldsymbol{y})$ can be taken to be

$$\begin{aligned} &\det(1 - Ax_1)(1 - By_1) \cdots (1 - Ax_r)(1 - By_r) \\ &\quad = \prod_{i=1}^{r} \det(1 - Ax_i) \cdot \prod_{j=1}^{r} \det(1 - By_j). \end{aligned}$$

b.

$$\begin{aligned} (1 - Ax)(1 - By) &= \begin{bmatrix} 1 - y + xy & x - y \\ -x + y + xy & 1 + xy \end{bmatrix} \\ \Rightarrow T_1(x,y) &= \frac{2 - y + xy}{(1 + x^2)(1 - y + y^2)}. \end{aligned}$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

29. True. The generating function $\sum_{n\geq 0}(A^n)_{rs}\lambda^n$ is rational by Theorem 4.7.2. Hence, $(A^n)_{rs}$ has the form of Theorem 4.1.1(iii), namely,

$$(A^n)_{rs} = \sum_{m=1}^{k} P_m(n)\gamma_m^n, \quad n \gg 0.$$

The same is true of B and C and hence of $(A^nB^nC^n)_{ij}$ by the definition of matrix multiplication, so the proof follows.

30. *Answer.*

$$\frac{1+xyz-x^2yzw-xy^2zw}{(1-x^2z)(1-xw)(1-y^2z)(1-yw)}.$$

31. Let $S = \{\boldsymbol{\beta} \in \mathbb{Z}^m : \text{ there exist } \boldsymbol{\alpha} \in \mathbb{N}^m \text{ and } n \in \mathbb{P} \text{ such that } \Phi\boldsymbol{\alpha} = n\boldsymbol{\beta} \text{ and } 0 \leq \alpha_i < n\}$. Clearly, S is finite. For each $\boldsymbol{\beta} \in S$, define $F_{\boldsymbol{\beta}} = \sum y^{\boldsymbol{\alpha}}x^n$, summed over all solutions $\boldsymbol{\alpha} \in \mathbb{N}^m$ and $n \in \mathbb{P}$ to $\Phi\boldsymbol{\alpha} = n\boldsymbol{\beta}$ and $\alpha_i < n$. Now $\sum_{n\geq 0} f(n)x^n = \sum_{\boldsymbol{\beta}\in S} F_{\boldsymbol{\beta}}(\mathbf{1},x)$ (where $\mathbf{1} = (1,\dots,1) \in \mathbb{N}^m$), and the proof follows from Theorem 4.5.11.

32. For $S \subseteq \binom{[m]}{2}$, let E_S denote the set of $\mathbb{N}$-solutions $\boldsymbol{\alpha}$ to equation (4.10) that also satisfy $\alpha_i = \alpha_j$ if $\{i,j\} \in S$. By Theorem 4.5.11, the generating function $E_S(\boldsymbol{x})$ is rational, whereas by the Principle of Inclusion-Exclusion

$$E^*(\boldsymbol{x}) = \sum_S (-1)^{\#S} E_S(\boldsymbol{x}), \tag{4.63}$$

and the proof follows.

NOTE. For practical computation, one should replace $S \subseteq \binom{[m]}{2}$ by $\pi \in \Pi_m$ and should replace equation (4.63) by Möbius inversion on Π_m.

34. See Proposition 8.3 of Stanley [4.53].

35. **a.** Given $\boldsymbol{\beta} \in \mathbb{Z}^r$, let $S = \{i : \beta_i < 0\}$. Now if $\boldsymbol{\gamma} = (\gamma_1,\dots,\gamma_r)$, then define $\boldsymbol{\gamma}^S = (\gamma_1',\dots,\gamma_r')$ where $\gamma_i' = \gamma_i$ if $i \notin S$ and $\gamma_i' = -\gamma_i$ if $i \in S$. Let F^S be the monoid of all $\mathbb{N}$-solutions $(\boldsymbol{\alpha},\boldsymbol{\gamma})$ to $\Phi\boldsymbol{\alpha} = \boldsymbol{\gamma}^S$. By Theorem 4.5.11, the generating function

$$F^S(\boldsymbol{x},\boldsymbol{y}) = \sum_{(\boldsymbol{\alpha},\boldsymbol{\gamma})\in F^S} \boldsymbol{x}^{\boldsymbol{\alpha}}\boldsymbol{y}^{\boldsymbol{\gamma}}$$

is rational. Let $\boldsymbol{\beta}^S = (\beta_1',\dots,\beta_r')$. Then

$$E_{\boldsymbol{\beta}}(\boldsymbol{x}) = \frac{1}{\beta_1'!\cdots\beta_r'!}\frac{\partial^{\beta_1'}}{\partial y_1^{\beta_1'}}\cdots\frac{\partial^{\beta_r'}}{\partial y_r^{\beta_r'}}F^S(\boldsymbol{x},\boldsymbol{y})\Bigg|_{\boldsymbol{y}=\mathbf{0}}, \tag{4.64}$$

so $E_{\boldsymbol{\beta}}(\boldsymbol{x})$ is rational. Moreover, if $\boldsymbol{\alpha} \in \mathrm{CF}(E)$ then $(\boldsymbol{\alpha},\mathbf{0}) \in \mathrm{CF}(F^S)$. The factors $1-\boldsymbol{x}^{\boldsymbol{\alpha}}$ in the denominator of $F^S(\boldsymbol{x},\boldsymbol{y})$ are unaffected by the partial differentiation in equation (4.64), whereas all other factor disappear upon setting $\boldsymbol{y} = \mathbf{0}$. Hence, $D(\boldsymbol{x})$ is a denominator of $E_{\boldsymbol{\beta}}(\boldsymbol{x})$. To see that it is the *least* denominator (provided $E_{\boldsymbol{\beta}} \neq \emptyset$), argue as in the proof of Theorem 4.5.11.

b. *Answer.* $\beta = 0, \pm 1$.

c. Let $\alpha_i = p_i/q_i$ for integers $p_i \geq 0$ and $q_i > 0$. Let ℓ be the least common multiple of $q_1,q_2,\dots,q_m$. Let $\Phi = [\boldsymbol{\gamma_1},\dots,\boldsymbol{\gamma_m}]$ where $\boldsymbol{\gamma_i}$ is a column vector of length r, and define $\boldsymbol{\gamma_i'} = (\ell/q_i)\boldsymbol{\gamma_i}$. Let $\Phi' = [\boldsymbol{\gamma_1'},\dots,\boldsymbol{\gamma_m'}]$. For any vector $\boldsymbol{\nu} = (\nu_1,\dots,\nu_m) \in \mathbb{Z}^m$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

satisfying $0 \le \nu_i < q_i$, let $E'_{(\boldsymbol{\nu})}$ be the set of all $\mathbb{N}$-solutions $\boldsymbol{\delta}$ to $\Phi'(\boldsymbol{\delta}) = \mathbf{0}$ such that $\delta_i \equiv \nu_i \pmod{q_i}$. If E' denotes the set of *all* $\mathbb{N}$-solutions $\boldsymbol{\delta}$ to $\Phi'(\boldsymbol{\delta}) = \mathbf{0}$, then it follows that $E' = \bigcup_{\boldsymbol{\nu}} E'_{(\boldsymbol{\nu})}$ (disjoint union). Hence by Theorem 4.5.14,

$$\overline{E}'(\boldsymbol{x}) = \pm E'(1/\boldsymbol{x}) = \pm \sum_{\boldsymbol{\nu}} E'_{(\boldsymbol{\nu})}(1/\boldsymbol{x}). \tag{4.65}$$

Now any monomial $\boldsymbol{x}^{\boldsymbol{\varepsilon}}$ appearing in the expansion of $E'_{(\boldsymbol{\nu})}(1/\boldsymbol{x})$ about the origin satisfies $\varepsilon_i \equiv -\nu_i \pmod{q'_i}$. It follows from equation (4.65) that $E'_{(\boldsymbol{\nu})}(1/\boldsymbol{x}) = \pm E'_{(\bar{\boldsymbol{\nu}})}(\boldsymbol{x})$, where $\bar{\nu}_i = q_i - \nu_i$ for $\nu_i \ne 0$ and $\bar{\nu}_i = \nu_i$ for $\nu_i = 0$, and where $\overline{E}'_{(\boldsymbol{\mu})} = E'_{(\boldsymbol{\mu})} \cap \overline{E}'$. Now let σ_i be the least nonnegative residue of p_i modulo q_i, and let $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_m)$. Define an affine transformation $\phi\colon \mathbb{R}^m \to \mathbb{R}^m$ by the condition

$$\phi(\boldsymbol{\delta}) = (\delta_1/q_1, \dots, \delta_m/q_m) + \boldsymbol{\alpha}.$$

One can check that ϕ defines a bijection between $E'_{(\boldsymbol{\sigma})}$ and $E_{\boldsymbol{\beta}}$ and between $\overline{E}'_{(\boldsymbol{\sigma})}$ and $\overline{E}_{\boldsymbol{\beta}}$, from which the proof follows.

This proof is patterned after Theorem 3.5 of R. Stanley, in *Proc. Symp. Pure Math.* (D. K. Ray-Chaudhuri, ed.), vol. 34, American Math. Society, Providence, RI, 1979, pp. 345–355. This result can also be deduced from Theorem 10.2 of [4.53], as can many other results concerning inhomogeneoous linear equations. A further proof is implicit in [4.57] (see Theorem 3.2 and Corollary 4.3).

d. See Corollary 4.3 of [4.57].

36. a. No. The simplest example is the simplex σ in $\mathbb{R}^3$ with vertices $(0,0,0)$, $(1,1,0)$, $(1,0,1)$, and $(0,1,1)$. Note that σ has no additional integer points, so σ itself is the only integer triangulation of σ. But σ is not primitive, for example, since

$$\det \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} = 2 > 1.$$

b. If σ is a primitive d-simplex, then it is not hard to see that $i(\sigma, n) = \binom{n+d}{d}$, so $\bar{i}(\sigma, n) = (-1)^d \binom{-n+d}{d} = \binom{n-1}{d}$. Since $\mathcal{P}$ is the disjoint union of the interior of the faces of Γ, we get

$$i(\mathcal{P}, n) = \sum_{j \ge 0} f_j \binom{n-1}{j}.$$

An elegant way to state this formula is $\Delta^j i(\mathcal{P}, 1) = f_j$, where Δ denotes the first difference operator.

37. b. This remarkable result is due to M. Brion, *Ann. Sci. École Norm. Sup. (4)* **21** (1988), 653–663. Many subsequent proofs and expositions have been given, such as M. Beck, C. Haase, and F. Sottile, *Math. Intell.* **31** (2009), 9–17.

38. This result is due to S. Chen, N. Li, and S. V. Sam, Generalized Ehrhart polynomials, `arXiv:1002.3658`. Their result generalizes the conjecture of Exercise 4.12 of the first edition of this book. A conjectured multivariate generalization is due to Ehrhart [4.14, p. 139].

39. a. This result was conjectured by A. Weil as part of his famous "Weil conjectures." It was first proved by B. M. Dwork, *Amer. J. Math.* **82** (1960), 631–648, and a highly

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

readable exposition appears in Chapter V of N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, 2nd ed., Springer-Verlag, New York, 1984. The entire Weil conjectures were subsequently proved by P. R. Deligne (in two different ways) and later by G. Laumon and K. S. Kedlaya (independently).

b. This exercise is a result of J.-I. Igusa, *J. Reine Angew. Math.* **278/279** (1975), 307–321, for the case $k = 1$. A simpler proof was later given by Igusa in *Amer. J. Math.* **99** (1977), 393–417 (appendix). A proof for general k was given by D. Meuser, *Math. Ann.* **256** (1981), 303–310, by adapting Igusa's methods. For another proof, see J. Denef, *Lectures on Forms of Higher Degree*, Springer-Verlag, Berlin/Heidelberg/New York, 1978.

40. a. Let D_w denote the set of all factors of w belonging to L. (We consider two factors u and v different if they start or end at different positions in w, even if $u = v$ as elements of X^*.) Clearly for fixed w,

$$\sum_{T \subseteq D_w} \left(\prod_{v \in T} s_v \right) = \prod_{v \in L} (1 + s_v)^{m_v(w)}.$$

Hence, if we set each $s_v = t_v - 1$ in equation (4.52), we obtain the equivalent formula

$$\sum_{u \in X^*} \sum_{T \subseteq D_w} \left(\prod_{v \in T} s_v \right) = (1 - x_1 - \cdots - x_n - C(\boldsymbol{x}, \boldsymbol{s}))^{-1}. \tag{4.66}$$

Now given $w \in X^*$ and $T \subseteq D_w$, there is a *unique* factorization $w = v_1 \cdots v_k$ such that either

i. $v_i \in X$ and v_i does not belong to one of the factors in T, or

ii. v_i is the first component of some L-cluster (v_i, μ, ν) where the components of μ consist of all factors of v_i contained in D_w.

Moreover,

$$\prod_{v \in T} s_v = \prod_i \prod_{v \in L} s_v^{m_v(\mu)},$$

where i ranges over all v_i satisfying (ii), and where μ is then given by (ii). It follows that when the right-hand side of equation (4.66) is expanded as an element of $\mathbb{C}[[t_v : v \in L]]\langle\langle X \rangle\rangle$, it coincides with the left-hand side of (4.66).

This result is due to I. P. Goulden and D. M. Jackson, *J. London Math. Soc. (2)* **20** (1979), 567–576, and also appears in [3.32, Ch. 2.8]. A special case was proved by D. Zeilberger, *Discrete Math.* **34** (1981), 89–91. (The precise hypotheses used in this paper are not clearly stated.)

c. Let $C_v(\boldsymbol{x}, \boldsymbol{t})$ consist of those terms of $C(\boldsymbol{x}, \boldsymbol{t})$ corresponding to a cluster (w, μ, ν) such that the last component of μ is v. Hence, $C(\boldsymbol{x}, \boldsymbol{t}) = \sum_{v \in L} C_v(\boldsymbol{x}, \boldsymbol{t})$. By equation (4.52) or (4.66), it suffices to show that each C_v is rational. An easy combinatorial argument expresses C_v as a linear combination of the C_u's and 1 with coefficients equal to polynomials in the x_i's and t_v's. Solving this system of linear equations by Cramer's rule (it being easily seen on combinatorial grounds that a unique solution exists) expresses C_v as a rational function. (Another solution can be given using the transfer-matrix method.) An explicit expression for $C(\boldsymbol{x}, \boldsymbol{t})$ obtained in this way appears in Goulden and Jackson, ibid., Prop. 3.2, and in [3.32, Lem. 2.8.10]. See also L. J. Guibas and A. M. Odlyzko, *J. Combinatorial Theory Ser. A* **30** (1981), 193–208.

d. The right-hand side of equation (4.53) is equal to $(1 - nx + x^\ell A_w(x)^{-1})^{-1}$. The proof follows from analyzing the precise linear equation obtained in the proof of (c). This result appears in L. J. Guibas and A. M. Odlyzko, ibid.

41. b. E. Lucas, *Théorie des nombres*, Gauthier-Villars, Paris, 1891.

c. E. Landau, *Naturwissenschaftliche Wochenschrift*, **11** (1896), 367–371.

d. This result and many more on this topic, such as the determination of $B_4(n)$ and similar results for other chess pieces, can be found in V. Kotěšovec, Non-attacking chess pieces, 2nd ed., 2010,

⟨http://web.telecom.cz/vaclav.kotesovec/math.htm⟩.

e. Identify an $n \times n$ chessboard with the set $[0,n-1]^2$. Then $k!B_k(n)$ is equal to the number of vectors $v = (\alpha_1,\dots,\alpha_k,\beta_1,\dots,\beta_k,\gamma) \in \mathbb{Z}^{2k+1}$ satisfying

$$\gamma = n-1, \tag{4.67}$$

$$0 \le \alpha_i \le \gamma, \;\; 0 \le \beta_i \le \gamma, \tag{4.68}$$

$$i \ne j \Rightarrow [(\alpha_i \ne \alpha_j)\,\&\,(\beta_i \ne \beta_j)\,\&\,(\alpha_i - \beta_i \ne \alpha_j - \beta_j)\,\&\,$$
$$\alpha_i + \beta_i \ne \alpha_j + \beta_j)]. \tag{4.69}$$

Label the $r = 4\binom{k}{2}$ inequalities of (4.69), say $I_1,\dots,I_r$. Let $\bar{I}_i$ denote the negation of I_i, that is, the equality obtained from I_i by changing $\ne$ to $=$. Given $S \subseteq [r]$, let $f_S(n)$ denote the number of vectors v satisfying (4.67), (4.68), and I_i for $i \in S$. By the Principle of Inclusion-Exclusion,

$$k!B_k(n) = \sum_S (-1)^{\#S} f_S(n). \tag{4.70}$$

Now by Theorem 4.5.11 the generating functions $F_S = \sum x_1^{\alpha_1}\cdots x_k^{\alpha_k} y_1^{\beta_1}\cdots y_k^{\beta_k} x^\gamma$ are rational, where the sum is over all vectors v satisfying (4.68) and $\bar{I}_i$ for $i \in S$. But $\sum f_S(n)x^{n-1}$ is obtained from F_S by setting each $x_i = y_j = 1$, so $\sum f_S(n)x^n$ is rational. It then follows from (4.70) that $\sum B_k(n)x^n$ is rational.

Note that the basic idea of the proof is same as in Exercise 4.32; namely, replace non equalities by equalities and use Inclusion-Exclusion. For many more results of this nature, see S. Chaiken, C. R. H. Hanusa, and T. Zaslavsky, Mathematical analysis of a q-queens problem, preprint, dated 19 May 2011.

42. The explicit formula is due to C. E. Arshon, Reshenie odnoĭ kombinatorornoĭ zadachi, *Math. Proveschchenie* **8** (1936), 24–29, from which it is clear that $A_k(n)$ has the properties stated in (b). A polytopal approach to nonattacking bishops was developed by S. Chaiken, C. R. H. Hanusa, and T. Zaslavsky, op cit. Proofs can also be given using the theory of Ferrers boards of Section 2.4.

43. We want to count triples $(a,b,c) \in \mathbb{P}^3$ satisfying $a \le b \le c$, $a+b > c$, and $a+b+c = n$. Every such triple can be written uniquely in the form

$$(a,b,c) = \alpha(0,1,1) + \beta(1,1,1) + \gamma(1,1,2) + (1,1,1),$$

where $\alpha,\beta,\gamma \in \mathbb{N}$; namely,

$$\alpha = b-a, \quad \beta = a+b-c-1, \quad \gamma = c-b.$$

Moreover, $n-3 = 2\alpha+3\beta+4\gamma$. Conversely, any triple $(\alpha,\beta,\gamma) \in \mathbb{N}^3$ yields a valid triple (a,b,c). Hence, $t(n)$ is equal to the number of triples $(\alpha,\beta,\gamma) \in \mathbb{N}^3$ satisfying $2\alpha+3\beta+4\gamma = n-3$, so

$$\sum_{n\ge 3} t(n)x^n = \frac{x^3}{(1-x^2)(1-x^3)(1-x^4)}.$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

From the viewpoint of Section 4.5, we obtained such a simple answer because the monoid E of $\mathbb{N}$-solutions (a,b,c) to $a \le b \le c$ and $a+b \ge c$ is a *free* (commutative) monoid (with generators $(0,1,1)$, $(1,1,1)$, and $(1,1,2)$).

Equivalent results (with more complicated proofs) are given by J. H. Jordan, R. Walch, and R. J. Wisner, *Notices Amer. Math. Soc.* **24** (1977), A-450, and G. E. Andrews, *Amer. Math. Monthly* **86** (1979), 477–478. For some generalizations, see G. E. Andrews, *Ann. Combinatorics* **4** (2000), 327–338, and M. Beck, I. M. Gessel, S. Lee, and C. D. Savage, *Ramanujan J.* **23** (2010), 355–369.

44. A simple combinatorial argument shows that

$$N_{kr}(n+1) = kN_{kr}(n) - (k-1)N_{kr}(n-r+1), \quad n \ge r. \tag{4.71}$$

It follows from Theorem 4.1.1 and Proposition 4.2.2(ii) that $F_{kr}(x) = P_{kr}(x)/(1 - kx + (k-1)x^r)$, where $P_{kr}(x)$ is a polynomial of degree r (since the recurrence (4.71) fails for $n = r-1$). In order to satisfy the initial conditions $N_{kr}(0) = 1$, $N_{kr}(n) = k^r$ if $1 \le n \le r-1$, $N_{kr}(r) = k^r - k$, we must have $P_{kr}(x) = 1 - x^r$. Hence,

$$F_{kr}(x) = \frac{1-x^r}{1-kx+(k-1)x^r}.$$

If we reduce $F_{kr}(x)$ to lowest terms, then we obtain

$$F_{kr}(x) = \frac{1+x+\cdots+x^{r-1}}{1-(k-1)x-(k-1)x^2-\cdots-(k-1)x^{r-1}}.$$

This formula can be obtained by proving directly that

$$N_{kr}(n+1) = (k-1)[N_{kr}(n) + N_{kr}(n-1) + \cdots + N_{kr}(n-r+2)],$$

but then it is somewhat more difficult to obtain the correct numerator.

45. **a.** (I. M. Gessel and R. A. Indik, A recurrence associated with extremal problems, preprint, 1989) Let $q \in \mathbb{P}$, $p \in \mathbb{Z}$ with $(p,q) = 1$, and $i \in \mathbb{N}$. First one shows that the two classes of functions

$$f(n) = i + \sum_{j=1}^{n} \left\lceil \frac{pj}{q} \right\rceil, \quad \text{where } n \ge 2iq + q,$$

$$f(n) = -i + 1 + \sum_{j=1}^{n} \left\lceil \frac{pj+1}{q} \right\rceil, \quad \text{where } n \ge 2iq + 2q,$$

satisfy the recurrence (4.54). Then one shows that for any $m \in \mathbb{P}$ and $k \in \mathbb{Z}$, one of the preceding functions satisfies $f(m) = k$.

b. The most interesting case is when $R(n) = P(n)/Q(n)$, where

$$P(n) = x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_0$$
$$Q(n) = x^d + b_{d-2}x^{d-2} + \cdots + b_0,$$

where the coefficients are integers and $a_{d-1} > 0$. (Of course, we should assume that $Q(n) \ne 0$ for any integer $n \ge m$.) In this case, $f(n) = O(n^a)$, where $a = a_{d-1}$, and we can ask whether $f(n)$ is a quasipolynomial. Experimental evidence suggests that the answer is negative in general, although in many particular instances the answer is afirmative. Gessel has shown that in all cases the function $\Delta^a f(n)$ is bounded. A further reference is Z. Füredi and A. Kündgen, *J. Graph Theory* **40** (2002), 195–225 (Theorem 7).

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

46. **a.** A simple computation shows that

$$f(n) = \frac{5i}{8}(\alpha^n - \beta^n),$$

where $\alpha = \frac{1}{5}(3-4i)$ and $\beta = \frac{1}{5}(3+4i)$. Since $|\alpha| = |\beta| = 1$, we have

$$|f(n)| \le \frac{5}{8}(|\alpha|^n + |\beta|^n) = \frac{5}{4}.$$

The easiest way to show $f(n) \ne \pm 5/4$ is to observe that the recurrence (4.55) implies that the denominator of $f(n)$ is a power of 5.

b. Since f is integer-valued and bounded, there are only many finitely many different sequences $f(n+1), f(n+2), \ldots, f(n+d)$. Thus for some $r < s$, we have $f(r+i) = f(s+i)$ for $1 \le i \le d$; and it follows that f has period $s-r$.

c. This result was conjectured by G. Pólya in 1916 and proved by F. Carlson in 1921. Subsequent proofs and generalizations were given by Pólya and are surveyed in *Jahrber. Deutsch. Math. Verein.* **31** (1922), 107–115; reprinted in *George Pólya: Collected Papers*, vol. 1 (G. Pólya and R. P. Boas, eds.), M.I.T. Press, Cambridge, Mass., 1974, pp. 192–198. For more recent work in this area, see the commentary on pp. 779–780 of the *Collected Papers*.

47. See A. M. Garsia and I. M. Gessel, *Advances in Math.* **31** (1979), 288–305 (Remark 22). There is now a large literature on the subject of *vector partitions*. See for example B. Sturmfels, *J. Combin. Theory Ser. A* **72** (1995), 302–309; M. Brion and M. Vergne, *J. Amer. Math. Soc.* **1** (1997), 797–833; A. Szenes and M. Vergne, *Advances in Appl. Math.* **3)** (2003), 295–342; W. Baldoni and M. Vergne, *Transformation Groups* **13** (2009), 447–469.

48. **a.** Several proofs of this result are known. One [4.56, Thm. 2.1] uses the result (H. Bruggesser and P. Mani, *Math. Scand.* **29** (1971), 197–205) that the boundary complex of a convex polytope is shellable. The second proof (an immediate generalization of [4.54, Prop. 4.2]) shows that a certain commutative ring $R_{\mathcal{P}}$ associated with $\mathcal{P}$ is Cohen–Macaulay. A geometric proof was given by U. Betke and P. McMullen, *Monatshefte für Math.* **99** (1985), 253–265 (a consequence of Theorem 1, Theorem 2, and the remark at the bottom of page 257 that $h(K,t)$ has nonnegative coefficients). Further references include M. Beck and F. Sottile, *Europ. J. Combinatorics* **28** (2007), 403–409 (reproduced in M. Beck and S. Robins [4.4, Thm. 3.12]), and A. Stapledon, Ph.D. thesis, University of Michigan, 2009.

b. See R. Stanley, in *Commutative Algebra and Combinatorics* (M. Nagata and H. Matsumura, eds.), Advanced Studies in Pure Mathematics **11**, Kinokuniya, Tokyo, and North-Holland, Amsterdam/New York, 1987, pp. 187–213 (Theorem 4.4). The methods discussed in U. Betke, *Ann. Discrete Math.* **20** (1984), 61–64, are also applicable.

c. This result was originally proved using commutative algebra by R. Stanley, *Europ. J. Combinatorics* **14** (1993), 251–258. A geometric proof was given by A. Stapledon, Ph.D. thesis, University of Michigan, 2009, and `arXiv:0807.3542`.

49. Equation (4.56) is due to T. Hibi, *Discrete Math.* **83** (1990), 119–121, while (4.57) is a result of R. Stanley, *Europ. J. Combinatorics* **14** (1993), 251–258. Both proofs were based on commutative algebra. Subsequently geometric proofs were given by A. Stapledon, *Trans. Amer. Math. Soc.* **361** (2009), 5615–5626. Stapledon gives a small improvement of Hibi's inequality and some additional inequalities.

50. Let

$$F(x) = \sum_{n \ge 0} i(\mathcal{P}, n)x^n = \frac{\sum_{j=0}^{d} a_i x^i}{(1-x)^{d+1}}.$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

By the reciprocity theorem for Ehrhart polynomials (Theorem 4.6.9), we have

$$\sum_{n\geq 0} i(\partial\mathcal{P},n)x^n = F(x) - (-1)^{d+1}F(1/x)$$
$$= \frac{\sum_{j=0}^{d+1} a_j(x^j - x^{d+1-j})}{(1-x)^{d+1}},$$

from which the proof follows easily. For further information, including a reference to a proof that $h_i \geq 0$, see Exercise 4.48(b).

51. **a.** We have that $i(n)$ is equal to the number of $\mathbb{N}$-solutions to $x_1 + \cdots + x_r \leq n$, $y_1 + \cdots + y_s \leq n$. There are $\binom{n+r}{r}$ ways to choose the x_i's and $\binom{n+s}{s}$ ways to choose the y_i's, so $i(n) = \binom{n+r}{r}\binom{n+s}{s} = \left(\!\binom{n+1}{r}\!\right)\left(\!\binom{n+1}{s}\!\right)$. Hence by Exercise 3.169(b) we get

$$F(x) = \sum_{n\geq 1} \left(\!\binom{n}{r}\!\right)\left(\!\binom{n}{s}\!\right) x^{n-1}$$
$$= \frac{\sum_{k=0}^{r} \binom{r}{k}\binom{s}{k} x^k}{(1-x)^{r+s+1}}.$$

The volume of $\mathcal{P}$ is by Proposition 4.6.13

$$V(\mathcal{P}) = \frac{1}{(r+s)!}\sum_{k=0}^{r+s}\binom{r}{k}\binom{s}{k} = \frac{1}{r!s!}.$$

There are $(r+1)(s+1)$ vertices—all vectors $(x_1,\ldots,x_r,y_1,\ldots,y_s) \in \mathbb{N}^{r+s}$ such that $x_1 + \cdots + x_r \leq 1$ and $y_1 + \cdots + y_s \leq 1$.

b. $P_{rs} = \boldsymbol{r+s}$. See Exercise 4.56 for a generalization to any finite poset P.

53. **a.** For any d, the matrix

$$\begin{bmatrix} 1 & 2 & \cdots & d \\ d+1 & d+2 & \cdots & 2d \\ & & \vdots & \\ d^2-d+1 & d^2-d+2 & \cdots & d^2 \end{bmatrix}$$

is an antimagic square.

b. Let $M = (m_{ij})$ be antimagic. Row and column permutations do not affect the antimagic property, so assume that m_{11} is the minimal entry of M. Define $a_i = m_{i1} - m_{11} \in \mathbb{N}$ and $b_j = m_{1j} \in \mathbb{N}$. The antimagic properties implies $m_{ij} = m_{i1} + m_{1j} - m_{11} = a_i + b_j$.

c. To get an antimagic square M of index n, choose a_i and b_j in (b) so that $\sum a_i + \sum b_j = n$. This can be done in $\left(\!\binom{2d+n-1}{2d-1}\!\right)$ ways. Since the only linear relations holding among the R_i's and C_j's are scalar multiples of $\sum R_i = \sum C_j$, it follows that we get each M exactly once if we subtract from $\left(\!\binom{2d+n-1}{2d-1}\!\right)$ the number of solutions to $\sum a_i + \sum b_j = n$ with $a_i \in \mathbb{P}$ and $b_j \in \mathbb{N}$. It follows that the desired answer is $\left(\!\binom{2d+n-1}{2d-1}\!\right) - \left(\!\binom{d+n-1}{2d-1}\!\right)$. (Note the similarity to Exercise 2.15(b).)

d. The vertices are the $2d$ matrices R_i and C_j; this result is essentially a restatement of (b). An integer point in $n\mathcal{P}_d$ is just a $d \times d$ antimagic square of index n. Hence

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

by (c),

$$i(\mathcal{P}_d,n) = \binom{2d+n-1}{2d-1} - \binom{d+n-1}{2d-1}.$$

e. By (d) we have

$$\sum_{n\geq 0} i(\mathcal{P}_d,n)x^n = \frac{1}{(1-x)^{2d}} - \frac{x^d}{(1-x)^{2d}}$$
$$= \frac{1+x+\cdots+x^{d-1}}{(1-x)^{2d-1}},$$

whence $A(\mathcal{P}_d,x) = 1+x+\cdots+x^{d-1}$ and $\nu(\mathcal{P}_d) = d/(2d-2)!$.

54. a. It follows from equation (4.29) that the average of the zeros of $H_n(r)$ is $-n/2$. Since $\deg H_n(r) = (n-1)^2$, we get that the sum of the zeros is $-\frac{1}{2}n(n-1)^2/2$, and the proof follows. This result was observed empirically by R. Stanley and proved by B. Osserman and F. Liu (private communication, dated 16 November 2010).

56. a. The vertices are the characteristic vectors χ_A of antichains A of P; that is, $\chi_A = (\varepsilon_1,\ldots,\varepsilon_p)$, where

$$\varepsilon_i = \begin{cases} 1, & \text{if } x_i \in A, \\ 0, & \text{if } x_i \notin A. \end{cases}$$

b. Let $\mathcal{O}(P)$ be the order polytope of Example 4.6.17. Define a map $f : \mathcal{O}(P) \to \mathcal{C}(P)$ by $f(\varepsilon_1,\ldots,\varepsilon_p) = (\delta_1,\ldots,\delta_p)$, where

$$\delta_i = \min\{\varepsilon_i - \varepsilon_j : x_i \text{ covers } x_j \text{ in } P\}.$$

Then f is a bijection (and is continuous and piecewise-linear) with inverse

$$\varepsilon_i = \max\{\delta_{j_1} + \cdots + \delta_{j_k} : t_{j_1} < \cdots < t_{j_k} = t_i\}.$$

Moreover, the image of $\mathcal{O}(P) \cap (\frac{1}{n}\mathbb{Z})^p$ under f is $\mathcal{C}(P) \cap (\frac{1}{n}\mathbb{Z})^p$, and the proof follows from Example 4.6.17.

NOTE. Essentially the same bijection f is given in the solution to Exercise 3.143(a). Indeed, it is clear that $\mathcal{C}(P)$ depends only on $\mathrm{Com}(P)$, so any property of $\mathcal{C}(P)$ (such as its Ehrhart polynomial) depends only on $\mathrm{Com}(P)$.
The polytope $\mathcal{C}(P)$ is called the *chain polytope* of P. For more information on chain polytopes, order polytopes, and their connections, see R. Stanley, *Discrete Comput. Geom.* **1** (1986), 9–23. For a generalization, see F. Ardila, T. Bliem, and D. Salazar, Gelfand-Tsetlin polytopes and Feigin-Fourier-Littelmann polytopes as marked poset polytopes, `arXiv:1008.2365`.

c. Choose P to be the zigzag poset Z_n of Exercise 3.66. Then $\mathcal{C}(Z_n) = \mathcal{C}_{n,2}$. Hence by (b) and Proposition 4.6.13, $\nu(\mathcal{C}_n)$ is the leading coefficient of $\Omega_{Z_n}(m)$. Then by Section 3.12 we have $\nu(\mathcal{C}_{n,2}) = e(Z_n)/n!$. But $e(Z_n)$ is the number E_n of alternating permutations in $\mathfrak{S}_n$ (see Exercise 3.66(c)), so

$$\sum_{n\geq 0} e(Z_n)\frac{x^n}{n!} = \tan x + \sec x.$$

A more *ad hoc* determination of $\nu(\mathcal{C}_{n,2})$ is given by I. G. Macdonald and R. B. Nelsen (independently), *Amer. Math. Monthly* **86** (1979), 396 (problem proposed by R. Stanley), and R. Stanley, *SIAM Review* **27** (1985), 579–580 (problem proposed

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

by E. E. Doberkat). For an application to tridiagonal matrices, see P. Diaconis and P. M. Wood, Random doubly stochastic tridiagonal matrices, preprint.

d. Using the integration method of Macdonald and Nelsen, ibid., the following result can be proved. Define polynomials $f_n(a,b)$ by

$$f_0(a,b) = 1, \quad f_n(0,b) = 0 \text{ for } n > 0,$$

$$\frac{\partial}{\partial a} f_n(a,b) = f_{n-1}(b-a, 1-a).$$

For instance,

$$f_1(a,b) = a,$$
$$f_2(a,b) = \frac{1}{2}(2ab - a^2),$$
$$f_3(a,b) = \frac{1}{6}(a^3 - 3a^2 - 3ab^2 + 6ab).$$

Then $v(\mathcal{C}_{n,3}) = f_n(1,1)$. A "nice" formula or generating function is not known for $f_n(a,b)$ or V_n. Similar results hold for $v(\mathcal{C}_{n,k})$ for $k > 3$.

e. Let P be the poset with elements $t_1, \ldots, t_n$ satisfying $t_1 < t_2 < \cdots < t_k$, $t_{k+1} < t_{k+2} < \cdots < t_n$, and $t_{k+i} < t_{i+1}$ for $1 \le i \le n-k$, except that when $n = 2k$ we omit the relation $t_{2k} < t_{k+1}$. The equations defining $\mathcal{C}(P)$ are exactly the same as those defining $\mathcal{C}_{n,k}$, so $v(\mathcal{C}_{n,k}) = e(P)/n!$. If we add a $\hat{0}$ to P and remove successively $2k-n-1$ $\hat{1}$'s (where when $n = 2k$ we add a $\hat{1}$), we don't affect $e(P)$ and we convert P to $\mathbf{2} \times (\boldsymbol{n-k+1})$. It is easy to see that $e(\mathbf{2} \times (\boldsymbol{n-k+1})) = C_{n-k+1}$ (see Exercise 6.19(aaa), Vol. II), and the proof follows.

57. By Exercise 4.56(a), the set of vertices of the polytope $\mathcal{C}(P)$ is a proper subset of the set of vertices of $\mathcal{C}(Q)$, so $\mathrm{vol}(\mathcal{C}(P)) < \mathrm{vol}(\mathcal{C}(Q))$. By Exercise 4.56(b) we have $\mathrm{vol}(\mathcal{C}(P)) = e(P)/p!$ and similarly for $\mathrm{vol}(\mathcal{C}(Q))$, so the proof follows. No other proof of this "obvious" inequality (communicated by P. Winkler) is known.

58. **a.** This result was conjectured by L. D. Geissinger, in *Proc. Third Caribbean Conference on Combinatorics and Computing*, University of the West Indies, Cave Hill, Barbados, pp. 125–133, and proved by H. Dobbertin, *Order* **2** (1985), 193–198.

c. To compute $i(\mathcal{V}(\boldsymbol{p}),n)$ choose $f(1)$, $f(2)$, $\ldots$, $f(p)$ in turn so that $0 \le f(1) + f(2) + \cdots + f(j) \le n$. There are exactly $n+1$ choices for each $f(j)$, so $i(\mathcal{V}(P),n) = (n+1)^p$.

d. Let $0 \le k \le n$. There are $i(\mathcal{V}(P),k) - i(\mathcal{V}(P),k-1)$ maps $f\colon P \to \mathbb{Z}$ for which every order ideal sum is nonnegative and the maximum such sum is exactly k. Given such an f, there are then $i(\mathcal{V}(Q),n-k)$ choices for $g\colon Q \to \mathbb{Z}$ for which every order ideal sum is nonnegative and at most $n-k$. It follows that

$$i(\mathcal{V}(P+Q),n) = \sum_{k=0}^{n} (i(\mathcal{V}(P),k) - i(\mathcal{V}(P),k-1)) i(\mathcal{V}(Q),n-k).$$

Hence,

$$\left((1-x)\sum_{n\ge 0} i(\mathcal{V}(P),n)x^n\right)\left(\sum_{n\ge 0} i(\mathcal{V}(Q),n)x^n\right) = \sum_{n\ge 0} i(\mathcal{V}(P+Q),n)x^n$$
$$= \frac{A(\mathcal{V}(P+Q),x)}{(1-x)^{p+q+1}},$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

where $p = \#P$ and $q = \#Q$. The result now follows from $\sum_{n\geq 0} i(\mathcal{V}(P),n)x^n = A(\mathcal{V}(P),x)/(1-x)^{p+1}$ and $\sum_{n\geq 0} i(\mathcal{V}(Q),n)x^n = A(\mathcal{V}(Q),x)/(1-x)^{q+1}$.

e. In view of (a), we need to show that the only integer points of $\mathcal{V}(P)$ are the vertices. This is a straightforward argument.

f. It follows from Corollary 4.2.4(ii) and the reciprocity theorem for order polynomials (Theorem 4.6.9) that the quantity $p+1-\deg A(\mathcal{V}(P),x)$ is equal to the least $d>0$ for which there is a map $f: P \to \mathbb{Q}$ such that every order ideal sum lies in the open interval $(0,1)$ and $df(t) \in \mathbb{Z}$ for all $t \in P$. Since every subset of the set of m minimal elements $t_1,\ldots,t_m$ is an order ideal, we have $f(t_i) > 0$ and $f(t_1)+\cdots+f(t_m) < 1$. Hence the minimal d for which $df(t_i) \in \mathbb{Z}$ is $d = m+1$, obtained by taking each $f(t_i) = 1/(m+1)$. We can extend f to all of P by defining $f(t) = 0$ if t is not minimal, so the proof follows.

g. Let $f(t) = 1/(m+1)$ for each minimal $t \in P$. By the proof of (f) and by Corollary 4.2.4(iii), we have that $x^{p-m}A(\mathcal{V}(P),1/x) = A(\mathcal{V}(P),x)$ if and only if there is a unique extension of f to P for which each order ideal sum lies in $(0,1)$ and for which $(m+1)f(t) \in \mathbb{Z}$ for all $t \in P$. It is not difficult to show that this condition holds if and only if every connected component of P has a unique minimal element (in which case $f(t) = 0$ for all nonminimal $t \in P$).

59. This result was conjectured by M. Beck, J. A. De Loera, M. Develin, J. Pfeifle, and R. Stanley, *Contemp. Math.* **374** (2005), 15–36 (Conjecture 1.5) and proved by F. Liu, *J. Combinatorial Theory Ser. A* **111** (2005), 111–127. Liu subsequently greatly generalized this result, culminating in the paper Higher integrality conditions, volumes and Ehrhart polynomials, *Advances in Math.* **226** (2011), 3467–3494.

60. The tetrahedron with vertices $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, $(1,1,r)$, $r \geq 1$, has four integer points and volume going to ∞, so for sufficiently large r the Ehrhart polynomial must have a negative coefficient. In fact, $r = 13$ yields $\frac{13}{6}n^3 + n^2 - \frac{1}{6}n + 1$.

61. a. The facets of $\mathcal{P}_d$ are given by the 2^d inequalities

$$\pm x_1 \pm x_2 \pm \cdots \pm x_d \leq 1.$$

Hence, $i(\mathcal{P}_d,n)$ is the number of integer solutions to

$$|x_1| + |x_2| + \cdots + |x_d| \leq n,$$

or, after introducing a slack variable y,

$$|x_1| + |x_2| + \cdots |x_d| + y = n.$$

Equivalently,

$$i(\mathcal{P},n) = \sum f(a_1)f(a_2)\cdots f(a_d),$$

summed over all weak compositions $a_1 + \cdots + a_d + b = n$ of n into d parts, where

$$f(a) = \begin{cases} 1, & a = 0, \\ 2, & a > 0. \end{cases}$$

Now $\sum_{a\geq 0} f(a)x^a = (1+x)/(1-x)$, so

$$\sum_{n\geq 0} i(\mathcal{P},n)x^n = \left(\frac{1+x}{1-x}\right)^d \cdot \frac{1}{1-x} = \frac{(1+x)^d}{(1-x)^{d+1}}.$$

Hence, $P_d(x) = (1+x)^d$.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

b. Follows from F. R. Rodriguez-Villegas, *Proc. Amer. Math. Soc.* **130** (2002), 2251–2254. It is also a consequence of Theorem 3.2 of R. Stanley, *Europ. J. Combinatorics* **32** (2011), 937–943. For some related results, see T. Hibi, A. Higashitani, and H. Ohsugi, *Proc. Amer. Math. Soc.* **139** (2011), 3707–3717.

62. b. The projection of $\Delta_{k,d}$ to the first $d-1$ coordinates gives a linear bijection φ with the polytope $\mathcal{R}_{d-1,k}$ of Exercise 1.51. Moreover, φ takes $\operatorname{aff}(\Delta_{k,d}) \cap \mathbb{Z}^d$ to $\mathcal{R}_{d-1,k} \cap \mathbb{Z}^{d-1}$, where aff denotes affine span. Since $\Delta_{k,d}$ and $\mathcal{R}_{d-1,k}$ are both integer polytopes, it follows that they have the same Ehrhart polynomial and therefore the same relative volume.

c. The polytope $\Delta_{k,d}$ is defined by

$$0 \le x_i \le 1, \;\; x_1 + \cdots + x_d = k.$$

Hence, $i(\Delta_{k,d}, n)$ is equal to the number of integer solutions to the equation $x_1 + \cdots + x_d = kn$ such that $0 \le x_i \le n$, so

$$\begin{aligned} i(\Delta_{k,d}, n) &= [x^{kn}](1 + x + \cdots + x^n)^d \\ &= [x^{kn}] \left(\frac{1 - x^{n+1}}{1 - x} \right)^d. \end{aligned}$$

g. This result is equivalent to Theorem 13.2 of T. Lam and A. E. Postnikov, *Discrete & Comput. Geom.* **38** (2007), 453–478, after verifying that the triangulation of $\Delta_{2,d}$ appearing there is primitive and appealing to Exercise 4.36(b). It can also be proved directly from part (c) or (d) of the present exercise.

(i) This result was conjectured by R. Stanley and proved by N. Li (December, 2010).

63. This result follows from the techniques in §5 of G. C. Shephard, *Canad. J. Math.* **26** (1974), 302–321, and was first stated by R. Stanley [4.56, Ex. 3.1], with a proof due to G. M. Ziegler appearing in *Applied Geometry and Discrete Combinatorics*, DIMACS Series in Discrete Mathematics, vol. 4, American Mathematical Society, Providence, RI, 1991, pp. 555–570 (Theorem 2.2). The polytope $\mathcal{Z}$ is by definition a *zonotope*, and the basic idea of the proof is to decompose $\mathcal{Z}$ into simpler zonotopes (namely, parallelopipeds, the zonotopal analogue of simplices), each of which can be handled individually. There is also a proof based on the theory of mixed volumes.

64. b. The crucial fact is that the polytope $\mathcal{P}_G$ is a zonotope and so can be handled by the techniques of Exercise 4.63. See [4.56, Ex. 3.1]. A purely combinatorial proof that the number of $\delta(\mathfrak{o})$'s equals the number of spanning forests of G is given by D. J. Kleitman and K. J. Winston, *Combinatorica* **1** (1981), 49–54. The polytope $\mathcal{P}_G$ was introduced by T. K. Zaslavsky (unpublished) and called by him an *acyclotope*. For a vast generalization of the permutohedron, see A. Postnikov, *Int. Math. Res. Notices* **2009** (2009), 1026–1106.

65. The crucial fact is that for a loopless graph G, the integer points in the polytope $\widetilde{\mathcal{D}}(G)$ are the extended degree sequences of spanning subgraphs of G if and only if G is an FHM-graph. This result is due to D. R. Fulkerson, A. J. Hoffman, and M. H. McAndrew, *Canad. J. Math.* **17** (1965), 166–177, whence the term "FHM-graph." Equation (4.58) is due to R. Stanley, in *Applied Geometry and Discrete Combinatorics*, DIMACS Series in Discrete Mathematics, vol. 4, American Mathematical Society, Providence, RI, 1991, pp. 555–570 (§5). For the case $G = K_k$, see Exercise 5.16.

66. a. This result was conjectured by Ehrhart [4.14, p. 53] and solved independently by R. Stanley [4.56, Thm. 2.8] and P. McMullen, *Arch. Math. (Basel)* **31** (1978/79), 509–516. A polytope $\mathcal{Q}$ whose affine span contains an integer point is called *reticular*

by Ehrhart [4.14, p. 47], and the least j for which every j-face of $\mathcal{P}$ is reticular is called the *grade* of $\mathcal{P}$ [4.14, p. 12].

b. See McMullen, ibid., §4.

70. **a.** Let A denote the adjacency matrix of G. We have $A^\ell = pJ$ for some $p \geq 0$, where J is the all 1's matrix. The matrix pJ has one nonzero eigenvalue, so the same is true for A. Since A is symmetric, it therefore has rank one. Since $[1,1,\ldots,1]$ is a left eigenvector and $[1,1,\ldots,1]^t$ is a right eigenvector for pJ, the same is true for A. These conditions suffice to show that all entries of A are equal.

The analogous problem for directed graphs is much more complicated; see Exercise 5.74(f).

b. Let V be the vertex set of G, with $p = \#V$. Note that G must be connected so $d_v > 0$ for all $v \in V$. Let D be the diagonal matrix with rows and columns indexed by V, such that $D_{vv} = 1/d_v$. Let $M = DA$. Note that M_{uv} is the probability of stepping to v from u. The hypothesis on G is therefore equivalent to $M^\ell = \frac{1}{p}J$. Let E be the diagonal matrix with $E_{vv} = 1/\sqrt{d_v}$. Then $E^{-1}ME = EAE$, a symmetric matrix. Thus, M is conjugate to a symmetric matrix and hence diagonalizable. The proof is now parallel to that of (a).

71. The adjacency matrix A of G has only two distinct rows, so $\operatorname{rank} A = 2$. Thus, there are two nonzero eigenvalues (since A is symmetric), say x and y. We have

$$\operatorname{tr}(A) = x + y = \text{number of loops} = 3.$$

Furthermore, $\operatorname{tr}(A^2) = C_G(2)$, which is twice the number of nonloop edges plus the number of loops [why?]. Thus,

$$\operatorname{tr}(A^2) = x^2 + y^2 = 2\left(\binom{21}{2} - \binom{18}{2}\right) + 3 = 117.$$

(There are other ways to compute $\operatorname{tr}(A^2)$.) The solutions to the equations $x + y = 3$ and $x^2 + y^2 = 117$ are $(x,y) = (9,-6)$ and $(-6,9)$. Hence, $C_G(\ell) = 9^\ell + (-6)^\ell$.

72. Let us count the number $c_{G'}(n)$ of closed walks of length n in G'. We can do a closed walk W in G of length $n-2k$, and then between any two steps of the walk (including before the first step and after the last) insert "detours" of length two along an edge e_v and back. There are $\binom{n-k}{k}$ ways to insert the detours [why?]. Thus, the number of closed walks of G' that start at a vertex of G is

$$c_G(n) + \binom{n-1}{1} c_G(n-2) + \binom{n-2}{2} c_G(n-4) + \binom{n-3}{3} c_G(n-6) + \cdots.$$

On the other hand, we can start at a vertex v'. In this case, after one step we are at v and can take $n-2$ steps as in the previous case, ending at v, and then step to v'. Thus, the number of closed walks of G' that start at a vertex v' is

$$c_G(n-2) + \binom{n-3}{1} c_G(n-4) + \binom{n-4}{2} c_G(n-6) + \binom{n-5}{3} c_G(n-8) + \cdots.$$

Therefore

$$\begin{aligned} c_{G'}(n) = c_G(n) &+ \left(\binom{n-1}{1} + 1\right) c_G(n-2) \\ &+ \left(\binom{n-2}{2} + \binom{n-3}{1}\right) c_G(n-4) \\ &+ \left(\binom{n-3}{3} + \binom{n-4}{2}\right) c_G(n-6) + \cdots. \end{aligned}$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

The following formula can be proved in various ways and is closely related to Exercise 4.22: If $\lambda^2 \neq -4$, then

$$\lambda^n + \left(\binom{n-1}{1} + 1\right)\lambda^{n-2} + \left(\binom{n-2}{2} + \binom{n-3}{1}\right)\lambda^{n-4}$$
$$+ \left(\binom{n-3}{3} + \binom{n-4}{2}\right)\lambda^{n-6} + \cdots = \alpha^n + \overline{\alpha}^n,$$

where

$$\alpha = \frac{\lambda + \sqrt{\lambda^2+4}}{2}, \quad \overline{\alpha} = \frac{\lambda - \sqrt{\lambda^2+4}}{2}.$$

Since $c_G(n) = \sum \lambda_i^n$, where the λ_i's are the eigenvalues of $A(G)$, and similarly for $c_{G'}(n)$, we get that the eigenvalues of $A(G')$ are $(\lambda_i \pm \sqrt{\lambda_i^2+4})/2$. (We don't have to worry about the special situation $\lambda_i^2 = -4$ since the λ_i's are real.)

For a slight generalization and a proof using linear algebra, see Theorem 2.13 on page 60 of D. M. Cvetković, M. Doob, and H. Sachs [4.10].

74. *Answer.* $9^\ell + 2\cdot 4^\ell + (-5)^\ell + 5\cdot 2^\ell + 4$. Why is there a term $+4$?

75. **a.** The column vector $(1, \zeta^r, \zeta^{2r}, \ldots, \zeta^{(n-1)r})^t$ (^{t} denotes transpose) is an eigenvector for M with eigenvalue ω_r. The attempt to generalize this result from cyclic groups and other finite abelian groups to arbitrary finite groups led Frobenius to the discovery of group representation theory; see T. Hawkins, *Arch. History Exact Sci.* **7** (1970/71), 142–170; **8** (1971/72), 243–287; **12** (1974), 217–243.

b. $f_k(n) = k\cdot 3^{n-1}$

c. Let $\Gamma = \Gamma_k$ be the directed graph on the vertex set $\mathbb{Z}/k\mathbb{Z}$ such that there is an edge from i to $i+1 \pmod k$. Then $g_k(n)$ is the number of closed walks in Γ of length n. If for $(i,j) \in (\mathbb{Z}/k\mathbb{Z})^2$, we define

$$M_{ij} = \begin{cases} 1, & \text{if } j \equiv i-1, i, i+1 \pmod k, \\ 0, & \text{otherwise,} \end{cases}$$

then the transfer-matrix method shows that $g_k(n) = \operatorname{tr} M^n$, where $M = (M_{ij})$. By (a), the eigenvalues of M are $1 + \zeta^r + \zeta^{-r} = 1 + 2\cos(2\pi r/k)$, where $\zeta = e^{2\pi i/k}$, and the proof follows.

76. **a.** Expand $\det(xI - A)$ by the first row. We get $V_n(x) = xV_{n-1}(x) + \det(xI - A : 1,2)$. Subtract the first column of the matrix $(xI - A : 1,2)$ from the second. The determinant is then clearly $-V_{n-2}(x)$, and the result follows. NOTE. If $U_n(x)$ is the *Chebyshev polynomial of the first kind*, then $V_n(2x) = U_n(x)$.

c. *Answer.* $\sum_{j=1}^n \left(2\cos\frac{j\pi}{n+1}\right)^k$.

d. *Answer.* $(2n+1)\binom{2n}{n} - 4^n$.

78. **a.** There are two choices for the first column. Once a column has been chosen, there are always exactly three choices for the next column (to the right).

b. Let Γ_n be the graph whose vertex set is $\{0,1\}^{n-1}$, with m edges from $(a_1,\ldots,a_{n-1})$ to $(b_1,\ldots,b_{n-1})$ if there are m ways to choose the next column to be of the form $[d, d+b_1, d+b_1+b_2, \ldots, d+b_1+\cdots+b_{n-1}]^t$ when the current column has the form $[c, c+a_1, c+a_1+a_2, \ldots, c+a_1+\cdots+a_{n-1}]^t$. In particular, there are two loops at each vertex; otherwise, $m = 0$ or 1. Then $g_k(n)$ is the total number of walks of length $n-1$ in Γ_n, so by the transfer-matrix method (Theorem 4.7.2) $G_k(x)$ is rational.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

For the case $k = 3$, we get a 4×4 matrix A with $\det(I - xA) = (1-x)(2-x)(1-5x+2x^2)$, but the factor $(1-x)(2-x)$ is cancelled by the numerator. Thus, we are led to the question: What is the degree of the denominator of $G_k(x)$ when this rational function is reduced to lowest terms?

This exercise is due to L. Levine (private communication, 2009).

79. **a.** Write $c_i(n)$ for the number of closed walks of length n in G_i, and similarly $c(n)$ for the number of closed walks of length n in $G = G_1 * \cdots * G_k$. Then

$$c(n) = \sum_{\substack{i_1+\cdots+i_k=n \\ i_j \geq 0}} \binom{n}{i_1, \ldots, i_k} c_1(i_1) \cdots c_k(i_k).$$

It follows that if $F_i(x) = \sum_{n \geq 0} c_i(n) \frac{x^n}{n!}$ and $F(x) = \sum_{n \geq 0} c(n) \frac{x^n}{n!}$, then $F(x) = F_1(x) \cdots F_k(x)$. If the eigenvalues of a graph G are $\lambda_1, \ldots, \lambda_p$, then

$$\sum_{n \geq 0} (\lambda_1^n + \cdots + \lambda_p^n) \frac{x^n}{n!} = e^{\lambda_1 x} + \cdots + e^{\lambda_p x}.$$

It now follows from equation (4.35) that the eigenvalues of G are the numbers $\mu_1 + \cdots + \mu_k$, where μ_i is an eigenvalue of G_i.

The star product is usually called the *sum* and is denoted $G_1 + \cdots + G_k$, but this notation conflicts with our notation for disjoint union. The result of this exercise is a special case of a more general result of D. M. Cvetković, Grafovi i njihovi spektri (thesis), *Univ. Beograd Publ. Elektrotehn. Fak.*, Ser. Mat. Fiz., no. 354–356 (1971), 1–50, and also appears in [4.10, Thm. 2.23].

b. We are asking for the number of walks of length n in the star product $K_{m_1} * \cdots * K_{m_k}$, from $(1, 1, \ldots, 1)$ to $(1^{n-r}, 2^r)$. Write $f_m(n)$ for the number of closed walks of length n in K_m from some specified vertex i. Write $g_m(n)$ for the number of walks of length n in K_m from some specified vertex i to a specified different vertex j. Then the number N we seek is given by

$$N = \sum_{\substack{i_1+\cdots+i_k=n \\ i_j \geq 0}} \binom{n}{i_1, \ldots, i_k} f_{m_1}(i_1) \cdots f_{m_{k-r}}(i_{k-r}) g_{m_{k-r+1}}(i_{k-r+1}) \cdots g_{m_k}(i_k). \tag{4.72}$$

By Example 4.7.5 we have

$$f_m(n) = \frac{1}{m}\left((m-1)^n + (m-1)(-1)^n\right),$$
$$g_m(n) = \frac{1}{m}\left((m-1)^n - (-1)^n\right).$$

Substituting into equation (4.72), expanding the product, and arguing as in (a) gives

$$N = \frac{1}{m_1 \cdots m_k} \sum_{S \subseteq [k]} (-1)^{\#([r+1,k]-S)} \left(\prod_{i \in [r+1,k] \cap S} (m_i - 1) \right) \left(\sum_{j \in S} m_j - k \right)^n.$$

For instance, if $B = [a] \times [b]$, then the number of walks from $(1,1)$ to $(1,1)$ in n steps is

$$N = \frac{1}{ab}\left((a+b-2)^n + (b-1)(a-2)^n + (a-1)(b-2)^n + (a-1)(b-1)(-2)^n\right).$$

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

The number of walks from $(1,1)$ to $(1,2)$ in n steps is

$$N = \frac{1}{ab}\left((a+b-2)^n - (a-2)^n + (a-1)(b-2)^n - (a-1)(-2)^n\right).$$

The number of walks from $(1,1)$ to $(2,2)$ in n steps is

$$N = \frac{1}{ab}\left((a+b-2)^n - (a-2)^n - (b-2)^n + (-2)^n\right).$$

This problem can also be solved by explicitly diagonalizing the adjacency matrix of G and using Corollary 4.7.4.

80. Let $N = \{w_1, w_2, \ldots, w_r\}$. Define a digraph $D = (V, E)$ as follows: V consists of all $(r+1)$-tuples $(v_1, v_2, \ldots, v_r, y)$ where each v_i is a left factor of w_i and $v_i \neq w_i$ (so $w_i = v_i u_i$ where $\ell(u_i) \geq 1$) and where $y \in X$. Draw a directed edge from $(v_1, v_2, \ldots, v_r, y)$ to $(v_1', v_2', \ldots, v_r', y')$ if $v_i y' \notin N$ for $1 \leq i \leq r$, and if

$$v_i' = \begin{cases} v_i y', & \text{if } v_i' y \text{ is a left factor of } w_i \\ v_i, & \text{otherwise.} \end{cases}$$

A walk beginning with some $(1, 1, \ldots, 1, y_1)$ (where 1 denotes the empty word) and whose vertices have last coordinates $y_1, y_2, \ldots, y_m$ corresponds precisely to the word $w = y_1 y_2 \cdots y_m$ having no subword in N. Hence by the transfer-matrix method, $F_N(x)$ is rational.

81. a. Let D be the digraph with vertex set $V = \{0,1\}^n$. Think of $(\varepsilon_1, \ldots, \varepsilon_k) \in V$ as corresponding to a column of a $k \times n$ chessboard covered with dimers, where $\varepsilon_i = 1$ if and only if the dimer in row i extends into the next column to the right. There is a directed edge $u \to v$ if it is possible for column u to be immediately followed by column v. For instance, there is an edge $01000 \to 10100$, corresponding to Figure 4.31. Then $f_k(n)$ is equal to the number of walks in D of length $n-1$ with certain allowed initial and final vertices, so by Theorem 4.7.2 $F_k(x)$ is rational. (There are several tricks to reduce the number of vertices which will not be pursued here.)

Example. Let $k = 2$. The digraph D is shown if Figure 4.32. The paths must start at 00 or 11 and end at 00. Hence, if

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix},$$

then

$$F_2(x) = \frac{-\det(I - xA\colon 1,2) + \det(I - xA\colon 2,2)}{\det(I - xA)}$$
$$= \frac{x + (1-x)}{1 - x - x^2} = \frac{1}{1 - x - x^2},$$

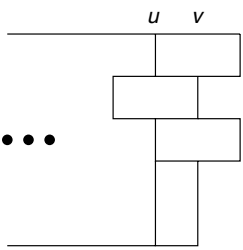

Figure 4.31 Dimers in columns u and v.

https://doi.org/10.1017/CBO9781139058520.005 Published online by Cambridge University Press

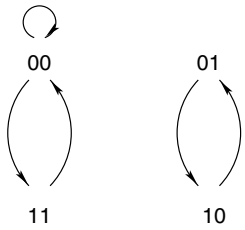

Figure 4.32 The digraph for dimer coverings of a $2 \times n$ board.

the generating function for Fibonacci numbers.

This result can also be easily be obtained by direct reasoning. We also have (see J. L. Hock and R. B. McQuistan, *Discrete Applied Math.* **8** (1984), 101–104; D. A. Klarner and J. Pollack, *Discrete Math.* **32** (1980), 45–52; R. C. Read, *Aequationes Math.* **24** (1982), 47–65):

$$F_3(x) = \frac{1-x^2}{1-4x^2+x^4},$$

$$F_4(x) = \frac{1-x^2}{1-x-5x^2-x^3+x^4},$$

$$F_5(x) = \frac{1-7x^2+7x^4-x^6}{1-15x^2+32x^4-15x^6+x^8},$$

$$F_6(x) = \frac{1-8x^2-2x^3+8x^4-x^6}{1-x-20x^2-10x^3+38x^4+10x^5-20x^6+x^7+x^8}.$$

b. Equation (4.59) was first obtained by P. W. Kastelyn, *Physica* **27** (1961), 1209–1225. It was proved *via* the transfer-matrix method by E. H. Lieb, *J. Math. Phys.* **8** (1967), 2339–2341. Further references to this and related results appear in the solution to Exercise 3.82(b). See also Section 8.3 of Cvetković, Doob, and Sachs [4.10].

c. See R. Stanley, *Discrete Applied Math.* **12** (1985), 81–87.

82. a. $\chi_n(2) = \begin{cases} 2, & n \text{ even}, \\ 0, & n \text{ odd}. \end{cases}$

b. This is equivalent to a result of E. H. Lieb, *Phys. Rev.* **162** (1967), 162–172. More detailed proofs appear in Percus [4.40, pp. 143–159] (this exposition has many minor inaccuracies), E. H. Lieb and F. Y. Wu, in *Phase Transitions and Critical Phenomena* (C. Domb and M. S. Green, eds.), vol. 1, Academic Press, London/New York, 1972, pp. 331–490, and Baxter [4.2] (see eq. (8.8.20) and p. 178).

c. The constant $-\pi/6$ has been empirically verified to eight decimal places.

e,f. See N. L. Biggs, *Interaction Models*, Cambridge University Press, Cambridge, 1977; Biggs, *Bull. London Math. Soc.* **9** (1977), 54–56; D. Kim and I. G. Enting, *J. Combinatorial Theory Ser. B* **26** (1979), 327–336. In particular, the expansion (4.60) is equivalent to equation (16) of the last reference. Part (f) is due to J. Schneider, 2011.