12

Additional Topics

This chapter covers a variety of topics illustrating different aspects of enumerative combinatorics and probability. The treatment of each topic is essentially self-contained.

12.1 Cyclic Shifting of Paths

This section illustrates another technique for enumerating certain collections of lattice paths. The basic idea is to introduce an equivalence relation on paths by cyclically shifting the steps of a path. A similar idea was used in §3.14 to enumerate lists of terms.

12.1. Theorem: Enumeration of Rational-Slope Dyck Paths. Let r and s be positive integers such that $\gcd(r,s)=1$. The number of lattice paths from $(0,0)$ to (r,s) that never go below the diagonal line $sx=ry$ is

$$\frac{1}{r+s}\binom{r+s}{r,s}.$$

(Such paths are called *r/s-Dyck paths.*)

Proof. Step 1. Let $X=\mathcal{R}(\mathrm{E}^r\mathrm{N}^s)$, which is the set of all rearrangements of r copies of E and s copies of N. Thinking of E as an east step and N as a north step, we see that X can be identified with the set of all lattice paths from $(0,0)$ to (r,s). Given $v=v_1v_2\cdots v_{r+s}\in X$, we define an associated *label vector* $L(v)=(m_0,m_1,\ldots,m_{r+s})$ as follows. We set $m_0=0$. Then we recursively calculate $m_i=m_{i-1}+r$ if $v_i=N$, $m_i=m_{i-1}-s$ if $v_i=E$. For example, if $r=5$, $s=3$, and $v=\text{NEEENENE}$, then $L(v)=(0,5,2,-1,-4,1,-2,3,0)$. We can also describe this construction in terms of the lattice path encoded by v. If we label each lattice point (x,y) on this path by the integer $ry-sx$, then $L(v)$ is the sequence of labels encountered as we traverse the path from $(0,0)$ to (r,s). This construction is illustrated by the lattice paths in Figure 12.1. Note that v is recoverable from $L(v)$, since $v_i=\mathrm{N}$ iff $m_i-m_{i-1}=r$ and $v_i=\mathrm{E}$ iff $m_i-m_{i-1}=-s$.

Step 2. We prove that for all $v\in X$, if $L(v)=(m_0,m_1,\ldots,m_{r+s})$ then m_0, m_1, …, m_{r+s-1} are *distinct*, whereas $m_{r+s}=0=m_0$. To see this, suppose there exist x,y,a,b with $0<a\leq r$ and $0<b\leq s$, such that (x,y) and $(x+a,y+b)$ are two points on the lattice path for v that have the same label. This means that $ry-sx=r(y+b)-s(x+a)$, which simplifies to $rb=sa$. Thus the number $rb=sa$ is a common multiple of r and s. Since $\gcd(r,s)=1$, we have $\operatorname{lcm}(r,s)=rs$, so that $rb\geq rs$ and $sa\geq rs$. Thus $b\geq s$ and $a\geq r$, forcing $b=s$ and $a=r$. But then (x,y) must be $(0,0)$ and $(x+a,y+b)$ must be (r,s). So the only two points on the path with equal labels are $(0,0)$ and (r,s), which correspond to m_0 and m_{r+s}.

Step 3. Introduce an equivalence relation $\sim$ on X by setting $v\sim w$ iff v is a cyclic shift of w. More precisely, defining $C(w_1w_2\cdots w_{r+s})=w_2w_3\cdots w_{r+s}w_1$, we have $v\sim w$ iff

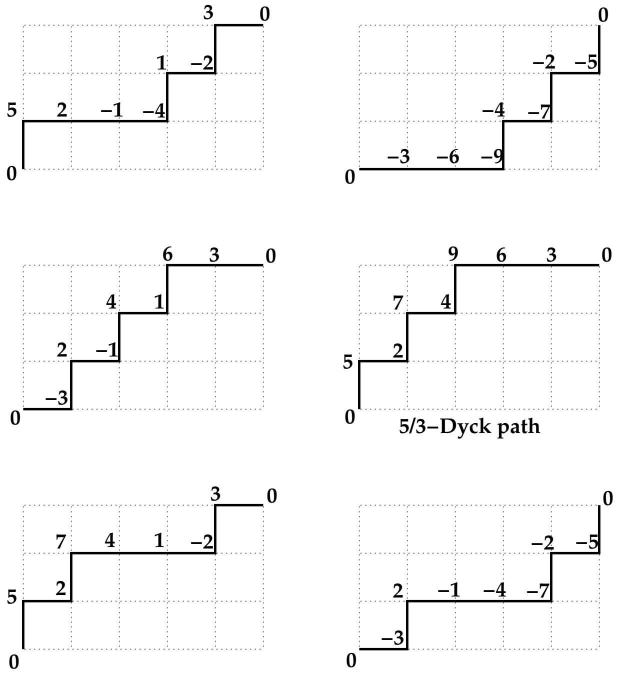


FIGURE 12.1
Cyclic shifts of a lattice path.

$v = C^i(w)$ for some integer i (which can be chosen in the range $0 \le i < r+s$). For each $v \in X$, let $[v] = \{w \in X : w \sim v\}$ be the equivalence class of v relative to this equivalence relation. Figure 12.1 shows the paths in the class [NEEENENE].

Step 4. We show that $|[v]| = r+s$ for all $v \in X$, which means that all $r+s$ cyclic shifts of v are *distinct*. Suppose $v = v_1v_2\cdots v_{r+s}$ has $L(v) = (m_0, m_1, \ldots, m_{r+s})$. By definition of L, for each i with $0 \le i < r+s$, the label vector of the cyclic shift $C^i(v) = v_{i+1}\cdots v_{r+s}v_1\cdots v_i$ is

$$L(C^i(v)) = (0, m_{i+1} - m_i, m_{i+2} - m_i, \ldots, m_{r+s} - m_i, m_1 - m_i, \ldots, m_i - m_i)$$

(cf. Figure 12.1). The set of integers appearing in the label vector $L(C^i(v))$ is therefore obtained from the set of integers in $L(v)$ by subtracting m_i from each integer in the latter set. In particular, if μ is the smallest integer in $L(v)$, then the smallest integer in $L(C^i(v))$ is $\mu - m_i$. Since the numbers $m_0, m_1, \ldots, m_{r+s-1}$ are distinct (by step 2), we see that the minimum elements in the sequences $L(C^i(v))$ are distinct, as i ranges from 0 to $r+s-1$. This implies that the sequences $L(C^i(v))$, and hence the words $C^i(v)$, are pairwise distinct.

Step 5. We show that, for all $v \in X$, there exists a unique word $w \in [v]$ such that w encodes a rational-slope Dyck path. By the way we defined the labels, w is an r/s-Dyck path iff $L(w)$ has no negative entries. Recall from step 4 that the set of labels in $L(C^i(v))$ is obtained from the set of labels in $L(v)$ by subtracting m_i from each label in the latter set. By step 2, there is a unique i in the range $0 \le i < r+s$ such that $m_i = \mu$, the minimum value in $L(v)$. For this choice of i, we have $m_j \ge \mu = m_i$ for every j, so that $m_j - m_i \ge 0$ and $L(C^i(v))$ has no negative labels. For any other choice of i, $m_i > \mu$ by step 4, so that $L(C^i(v))$ contains the negative label $\mu - m_i$.

Step 6. Suppose $\sim$ has n equivalence classes in X. By step 5, n is also the number of rational-slope Dyck paths. By step 4, each equivalence class has size $r+s$. Since X is the

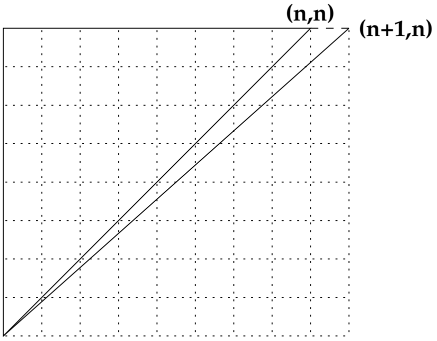


FIGURE 12.2
Comparing Dyck paths to $(n+1)/n$-Dyck paths.

disjoint union of its equivalence classes, the sum rule and 1.46 give

$$\binom{r+s}{r,s} = |X| = n(r+s).$$

Dividing by $r+s$ gives the formula stated in the theorem. □

12.2. Corollary: Enumeration of Dyck Paths and m-Dyck Paths. For $n \geq 1$, the number of Dyck paths ending at (n,n) is

$$\frac{1}{2n+1}\binom{2n+1}{n+1,n}.$$

For $m,n \geq 1$, the number of m-Dyck paths ending at (mn,n) is

$$\frac{1}{(m+1)n+1}\binom{(m+1)n+1}{mn+1,n}.$$

Proof. Let X be the set of Dyck paths ending at (n,n), and let X' be the set of $(n+1)/n$-Dyck paths ending at $(n+1,n)$. Since $\gcd(n+1,n)=1$, we know that $|X'| = \frac{1}{2n+1}\binom{2n+1}{n+1,n}$. On the other hand, passing from the diagonal $y=x$ to the line $(n+1)y-nx=0$ does not introduce any new lattice points in the region of interest, except for $(n+1,n)$. See Figure 12.2. It follows that appending a final east step gives a bijection from X onto X', so the first result holds. The second result is proved in the same way: appending a final east step gives a bijection from the set of m-Dyck paths ending at (mn,n) to the set of $(mn+1)/n$-Dyck paths ending at $(mn+1,n)$. □

12.2 Chung-Feller Theorem

In §1.10, we defined Dyck paths and proved that the number of Dyck paths of order n is the Catalan number $C_n = \frac{1}{n+1}\binom{2n}{n,n}$. This section discusses a remarkable generalization of this result called the *Chung-Feller Theorem*.

12.3. Definition: Flawed Paths. Suppose $\pi = ((x_0, y_0), \ldots, (x_{2n}, y_{2n}))$ is a lattice path from $(0, 0)$ to (n, n). For $1 \leq j \leq n$, we say that π has a *flaw in row* j iff there exists a point (x_i, y_i) visited by π such that $y_i = j - 1$, $y_i < x_i$, and $(x_{i+1}, y_{i+1}) = (x_i, y_i + 1)$. This means that the jth north step of π occurs in the region southeast of the diagonal line $y = x$. For $1 \leq j \leq n$, define

$$X_j(\pi) = \chi(\pi \text{ has a flaw in row } j).$$

Also define the *number of flaws of* π by setting $\text{flaw}(\pi) = X_1(\pi) + X_2(\pi) + \cdots + X_n(\pi)$.

For example, the paths shown in Figure 12.3 have zero and six flaws, respectively. The paths shown in Figure 12.4 have five and zero flaws, respectively. Observe that π is a *Dyck* path iff $\text{flaw}(\pi) = 0$.

12.4. Chung-Feller Theorem. Fix $n \geq 0$, and let A be the set of lattice paths from $(0, 0)$ to (n, n). For $0 \leq k \leq n$, let

$$A_k = \{\pi \in A : \text{flaw}(\pi) = k\}.$$

Then $|A_k| = |A_0|$ for all k. In particular, for $0 \leq k \leq n$,

$$|A_k| = \frac{1}{n+1}|A| = \frac{1}{n+1}\binom{2n}{n, n} = C_n.$$

Proof. Fix $k > 0$. To prove that $|A_0| = |A_k|$, we define a bijection $\phi_k : A_0 \to A_k$. See Figure 12.3 for an example where $n = 10$ and $k = 6$. Given a Dyck path $\pi \in A_0$, we begin by drawing the line $y = k$ superimposed on the Dyck path. There is a unique point (x_i, y_i) on π such that $y_i = k$ and π arrives at (x_i, y_i) by taking a vertical step. Call this step the *special vertical step.* Let $(a_1, a_2, \ldots) \in \{H, V\}^{2n - x_i - y_i}$ be the ordered sequence of steps of π reading northeast from (x_i, y_i), where H means "horizontal step" and V means "vertical step." Let $(b_0 = V, b_1, b_2, \ldots) \in \{H, V\}^{x_i + y_i}$ be the ordered sequence of steps of π reading southwest from (x_i, y_i). For the Dyck path shown on the left in Figure 12.3, we have

$$a_1 a_2 \cdots = \text{VHVHHHVHVHH}, \quad b_0 b_1 b_2 \cdots = \text{VVHVHVVHV}.$$

We compute $\phi_k(\pi) = c_1 c_2 \cdots c_{2n} \in \{V, H\}^{2n}$ as follows. Let $c_1 = a_1$, $c_2 = a_2$, etc., until we obtain a horizontal step $c_k (= a_k)$ that ends strictly below the diagonal $y = x$. Then set $c_{k+1} = b_1$, $c_{k+2} = b_2$, etc., until we obtain a vertical step $c_{k+m} (= b_m)$ that ends on the line $y = x$. Then set $c_{k+m+1} = a_{k+1}$, $c_{k+m+2} = a_{k+2}$, etc., until we take a horizontal step that ends strictly below $y = x$. Then switch back to using the steps $b_{m+1}, \ldots$ until we return to $y = x$. Continue in this way until all steps are used. By convention, the special vertical step $b_0 = V$ is the last "b-step" to be consumed.

For example, for the path π in Figure 12.3, we have labeled the steps of π as A through T for ease of reference. The special vertical step is step I. We begin by transferring steps J,K,L,M,N to the image path (starting at the origin). Step N goes below the diagonal, so we jump to the section of π prior to the special vertical step and work southwest. After taking only one step (step H), we have returned to the diagonal. Now we jump back to our previous location in the top part of π and take step O. This again takes us below the diagonal, so we jump back to the bottom part of π and transfer steps G,F,E,D,C. Now we return to the top part and transfer steps P,Q,R,S,T. Finally, we return to the bottom part of π and transfer steps B, A, and finally the special vertical step I.

This construction has the following crucial property. Vertical steps above the line $y = k$ in π get transferred to vertical steps above the line $y = x$ in $\phi_k(\pi)$, while vertical steps below the line $y = k$ in π get transferred to vertical steps below the line $y = x$ in $\phi_k(\pi)$. Thus, $\phi_k(\pi)$ has exactly k flaws, and is therefore an element of A_k.

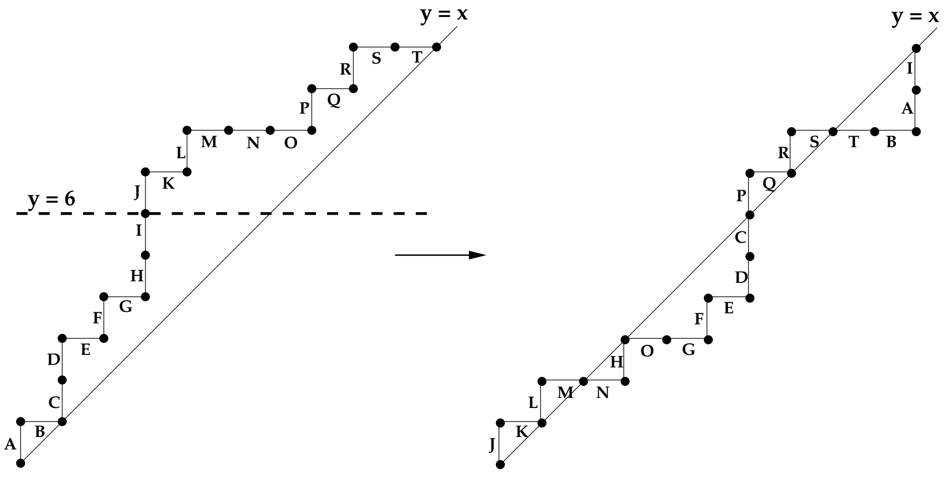


FIGURE 12.3
Mapping Dyck paths to flawed paths.

Moreover, consider the coordinates of the special point (x_i, y_i). By definition, $y_i = k = \text{flaw}(\phi_k(\pi))$. On the other hand, we claim that $y_i - x_i$ equals the number of horizontal steps in $\phi_k(\pi)$ that start on $y = x$ and end to the right of $y = x$. Each such horizontal step corresponds to a step after (x_i, y_i) in π that brings the path closer to the main diagonal $y = x$. For instance, these steps are N, O, and T in Figure 12.3. The definition of ϕ_k shows that the steps in question (in π) are the earliest east steps after (x_i, y_i) that arrive on the lines $y = x + d$ for $d = y_i - x_i - 1, \ldots, 2, 1, 0$. The number of such steps is therefore $y_i - x_i$ as claimed.

The observations in the last paragraph allow us to compute the inverse map $\phi'_k : A_k \to A_0$. For, suppose $\pi \in A_k$ is a path with k flaws. We can recover (x_i, y_i) since $y_i = k$ and $y_i - x_i$ is the number of east steps of π departing from $y = x$. Next, we transfer the steps of π to the top and bottom portions of $\phi'_k(\pi)$ by reversing the process described earlier. Figure 12.4 gives an example where $n = 10$ and $k = 5$. First we find the special point $(x_i, y_i) = (2, 5)$. We start by transferring the initial steps A,B,C of π to the part of the image path starting at $(2, 5)$ and moving northeast. Since C goes below the diagonal in π, we now switch to the bottom part of the image path. The special vertical step must be skipped, so we work southwest from $(2, 4)$. We transfer steps D,E,F,G,H. Since H returns to $y = x$ in π, we then switch back to the top part of the image path. We only get to transfer one step (step I) before returning to the bottom part of the image path. We transfer step J, then move back to the top part and transfer steps K through S. Finally, step T is transferred to become the special vertical step from $(2, 4)$ to $(2, 5)$. One checks that ϕ'_k is the two-sided inverse of ϕ_k, so $\phi_k : A_0 \to A_k$ is a bijection.

Now that we know $|A_k| = |A_0|$ for all k, the final statement of the theorem follows. For A is the disjoint union of the $n + 1$ sets $A_0, A_1, \ldots, A_n$, all of which have cardinality $|A_0|$. By the sum rule,

$$|A| = |A_0| + |A_1| + \cdots + |A_n| = (n + 1)|A_0|,$$

and therefore

$$|A_k| = |A_0| = \frac{|A|}{n + 1} = \frac{1}{n + 1}\binom{2n}{n, n} = C_n$$

for $0 \leq k \leq n$. □

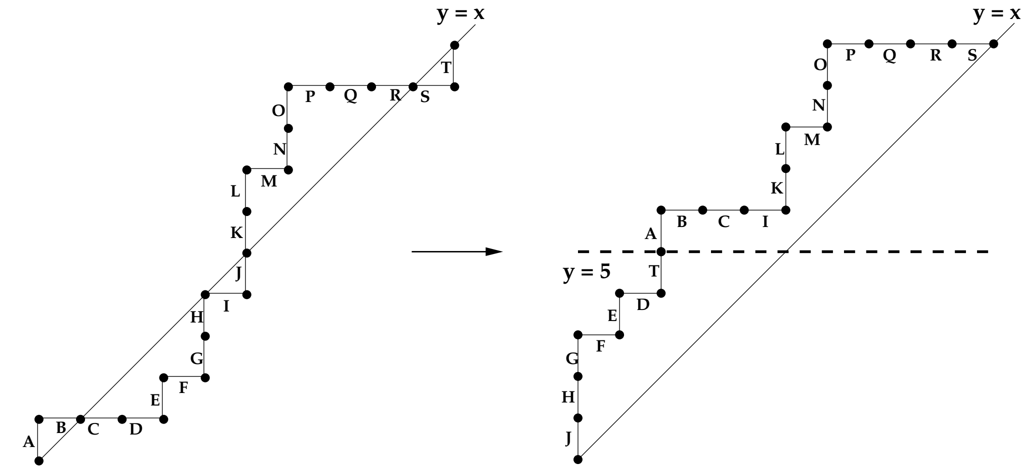


FIGURE 12.4
Mapping flawed paths to Dyck paths.

In probabilistic language, the Chung-Feller Theorem can be stated as follows.

12.5. Corollary. Suppose we pick a random lattice path π from the origin to (n,n). The number of flaws in this path is uniformly distributed on $\{0,1,2,\dots,n\}$. In other words,

$$P(\text{flaw}(\pi)=k)=\frac{1}{n+1}\qquad\text{for } k=0,1,\dots,n.$$

Proof. We compute

$$P(\text{flaw}(\pi)=k)=\frac{|A_k|}{|A|}=\frac{\frac{1}{n+1}\binom{2n}{n,n}}{\binom{2n}{n,n}}=\frac{1}{n+1}.\qquad\square$$

12.6. Remark. The Chung-Feller Theorem is significant in probability theory for the following reason. One of the most celebrated theorems of probability is the *central limit theorem.* Roughly speaking, this theorem says that the sum of a large number of independent, identically distributed random variables (suitably normalized) will converge to a *normal distribution.* The normal distribution is described by the "bell curve" that appears ubiquitously in probability and statistics. One often deals with situations involving random variables that are *not* identically distributed and are *not* independent of one another. One might hope that a generalization of the central limit theorem would still hold in such situations.

Chung and Feller used the example of flawed lattice paths to show that such a generalization is not always possible. Fix $n>0$, and let the sample space S consist of all lattice paths from the origin to (n,n). Given a lattice path $\pi\in S$, recall that

$$\text{flaw}(\pi)=X_1(\pi)+X_2(\pi)+\cdots+X_n(\pi),$$

where $X_j(\pi)=\chi(\pi \text{ has a flaw in row } j)$. The random variables $X_1,X_2,\dots,X_n$ are identically distributed; in fact, one can show that $P(X_j=0)=1/2=P(X_j=1)$ for all j (see 12.96). But we have seen that the sum of these random variables, namely $X_1+X_2+\cdots+X_n=\text{flaw}$, is uniformly distributed on $\{0,1,2,\dots,n\}$ for every n. A uniform distribution is about as far as one can get from a normal distribution! The trouble is that the random variables $X_1,\dots,X_n$ are not independent.

12.3 Rook-Equivalence of Ferrers Boards

This section continues the investigation of rook theory begun in §2.11. We define the notion of a rook polynomial for a Ferrers board and derive a characterization of when two Ferrers boards have the same rook polynomial.

12.7. Definition: Ferrers Boards and Rook Polynomials. Let $\mu = (\mu_1 \geq \mu_2 \geq \cdots \geq \mu_s > 0)$ be an integer partition of n. The *Ferrers board* F_μ is a diagram consisting of s left-justified rows of squares with μ_i squares in row i. A *non-attacking placement of k rooks* on F_μ is a subset of k squares in F_μ such that no two squares lie in the same row or column. Let $r_k(\mu)$ be the number of non-attacking placements of k rooks on F_μ. The *rook polynomial* of μ is

$$R_\mu(x) = \sum_{k\geq 0} r_k(\mu)x^k.$$

12.8. Example. If $\mu = (4,1,1,1)$, then $R_\mu(x) = 9x^2 + 7x + 1$. To see this, note that there is one empty subset of F_μ (which is a non-attacking placement of zero rooks). We can place one rook on any of the 7 squares in F_μ, so the coefficient of x^1 in R_μ is 7. To place two non-attacking rooks, we place one rook in the first column but not in the first row (3 ways), and we place the second rook in the first row but not in the first column (3 ways). The product rule gives 9 as the coefficient of x^2 in R_μ. It is impossible to place three or more non-attacking rooks on F_μ, so all higher coefficients in R_μ are zero.

As seen in the previous example, the constant term in any rook polynomial is 1, whereas the linear coefficient of a rook polynomial is the number $|\mu|$ of squares on the board F_μ. Furthermore, $R_\mu(x)$ has degree at most $\min(\mu_1, \ell(\mu))$, since all rooks must be placed in distinct rows and columns of the board.

It is possible for two different partitions to have the same rook polynomial. For example, one may check that

$$R_{(2,2)}(x) = 2x^2 + 4x + 1 = R_{(3,1)}(x) = R_{(2,1,1)}(x).$$

More generally, $R_\mu(x) = R_{\mu'}(x)$ for any partition μ.

12.9. Definition: Rook-Equivalence. We say that two integer partitions μ and ν are *rook-equivalent* iff they have the same rook polynomial, which means $r_k(\mu) = r_k(\nu)$ for all $k \geq 0$.

A necessary condition for μ and ν to be rook equivalent is that $|\mu| = |\nu|$. The next theorem gives an easily tested necessary and sufficient criterion for deciding whether two partitions are rook-equivalent.

12.10. Theorem: Rook-Equivalence of Ferrers Boards. Suppose μ and ν are partitions of n. Write $\mu = (\mu_1 \geq \cdots \geq \mu_n)$ and $\nu = (\nu_1 \geq \ldots \geq \nu_n)$ by adding zero parts if necessary. The rook polynomials $R_\mu(x)$ and $R_\nu(x)$ are equal iff the multisets

$$[\mu_1 + 1, \mu_2 + 2, \ldots, \mu_n + n] \text{ and } [\nu_1 + 1, \nu_2 + 2, \ldots, \nu_n + n]$$

are equal.

Proof. The idea of the proof is to use the falling factorial basis $\{(x)\!\downarrow_n : n \geq 0\}$ for the vector space of polynomials in x instead of the monomial basis $\{x^n : n \geq 0\}$ (see 2.76). For any partition λ, define

$$R'_\lambda(x) = \sum_{k=0}^{n} r_{n-k}(\lambda)(x)\downarrow_k = \sum_{k=0}^{n} r_{n-k}(\lambda)x(x-1)\cdots(x-k+1).$$

Note that $R_\mu(x) = R_\nu(x)$ iff $r_k(\mu) = r_k(\nu)$ for $0 \leq k \leq n$ (by linear independence of the monomial basis) iff $R'_\mu(x) = R'_\nu(x)$ in $\mathbb{R}[x]$ (by linear independence of the falling factorial basis). We will prove that this last condition holds iff the multisets mentioned in the theorem are equal.

We now use rook combinatorics to derive a formula for $R'_\mu(x)$. Fix a positive integer x. Consider the extended board $F_\mu(x)$, which has $\mu_i + x$ squares in row i, for $1 \leq i \leq n$. We obtain $F_\mu(x)$ from the board F_μ by adding x new squares on the left end of each of the n rows. Let us count the number of placements of n non-attacking rooks on $F_\mu(x)$. On one hand, we can build such a placement by working up the rows from bottom to top, placing a rook in a valid column of each successive row. By the product rule, the number of valid placements is

$$(x+\mu_n)(x+\mu_{n-1}-1)\cdots(x+\mu_1-(n-1)) = \prod_{i=1}^{n}(x+[\mu_i-(n-i)]).$$

On the other hand, let us count the number of placements of n non-attacking rooks on $F_\mu(x)$ that have exactly k rooks on the original board F_μ. We can place these rooks first in $r_k(\mu)$ ways. The remaining $n-k$ rooks must go in the remaining $n-k$ unused rows in one of the leftmost x squares. Placing these rooks one at a time, we obtain $r_k(\mu)x(x-1)(x-2)\cdots(x-(n-k-1))$ valid placements. Adding over k gives the identity

$$\sum_{k=0}^{n} r_k(\mu)(x)\downarrow_{n-k} = \prod_{i=1}^{n}(x+[\mu_i-(n-i)]).$$

Replacing k by $n-k$ in the summation, we find that

$$R'_\mu(x) = \prod_{i=1}^{n}(x+[\mu_i-(n-i)]).$$

This polynomial identity holds for infinitely many values of x (namely, for each positive integer x), so the identity must hold in the polynomial ring $\mathbb{R}[x]$. Similarly,

$$R'_\nu(x) = \prod_{i=1}^{n}(x+[\nu_i-(n-i)]).$$

The proof is now completed by invoking the uniqueness of prime factorizations for one-variable polynomials with real coefficients. More precisely, note that we have exhibited factorizations of $R'_\mu(x)$ and $R'_\nu(x)$ into products of linear factors. These two monic polynomials are equal iff their linear factors (counting multiplicities) are the same, which holds iff the multisets

$$[\mu_i-(n-i) : 1 \leq i \leq n] \text{ and } [\nu_i-(n-i) : 1 \leq i \leq n]$$

are the same. Adding n to everything, this is equivalent to the multiset equality in the theorem statement. □

12.11. Example. The partitions $(2,2,0,0)$ and $(3,1,0,0)$ are rook-equivalent, because $[3,4,3,4] = [4,3,3,4]$. The partitions $(4,2,1)$ and $(5,2)$ are not rook-equivalent, since $[5,4,4,4,5,6,7] \neq [6,4,3,4,5,6,7]$.

12.4 Parking Functions

This section illustrates the use of a probabilistic argument to enumerate a collection of combinatorial objects, namely the parking functions defined next.

12.12. Definition: Parking Functions. A *parking function of order n* is a function $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ such that

$$|\{x : f(x) \leq i\}| \geq i \qquad \text{for } 1 \leq i \leq n.$$

12.13. Example. For $n = 8$, the function f defined in Figure 12.5 is a parking function, but the function g is not.

x	1	2	3	4	5	6	7	8
$f(x)$	2	6	3	2	6	2	2	1
$g(x)$	5	6	1	5	6	1	7	1

FIGURE 12.5
A parking function and a non-parking function.

The name "parking function" arises as follows. Consider a one-way street with n parking spaces numbered $1, 2, \ldots, n$. Cars numbered $1, 2, \ldots, n$ arrive at the beginning of this street in numerical order. Each car wants to park in its own preferred spot on the street. We encode these parking preferences by a function $h : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, by letting $h(x)$ be the parking spot preferred by car x. Given h, the cars park in the following way. For $x = 1, 2, \ldots, n$, car x arrives and drives forward along the street to the spot $h(x)$. If that spot is empty, car x parks there. Otherwise, the car continues to drive forward on the one-way street and parks in the first available spot after $h(x)$, if any. The cars cannot return to the beginning of the street, so it is possible that not every car will be able to park.

For example, suppose the parking preferences are given by the parking function f defined in Figure 12.5. Car 1 arrives first and parks in spot 2. The next two cars arrive and park in spots 6 and 3, respectively. When car 4 arrives, spots 2 and 3 are full, so car 4 parks in spot 4. This process continues. At the end, every car has parked successfully, and the parking order is $8, 1, 3, 4, 6, 2, 5, 7$. Now suppose the parking preferences are given by the non-parking function g defined in Figure 12.5. After the first six cars have arrived, the parking spots on the street are filled as follows:

$$3, 6, -, -, 1, 2, 4, 5.$$

Car 7 arrives and drives to spot $g(7) = 7$. Since spots 7 and 8 are both full at this point, car 7 cannot park.

12.14. Theorem. A function $h : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is a parking function iff every car is able to park using the parking preferences determined by h.

Proof. We prove the contrapositive in each direction. Suppose first that h is not a parking function. Then there exists $i \leq n$ such that $|\{x : h(x) \leq i\}| < i$. This means that fewer than i cars prefer to park in the first i spots. But then the first i spots cannot all be used, since a car never parks in a spot prior to the spot it prefers. Since there are n cars and n spots, the existence of an unused spot implies that not every car was able to park.

Conversely, assume not every car can park. Let i be the earliest spot that is not taken

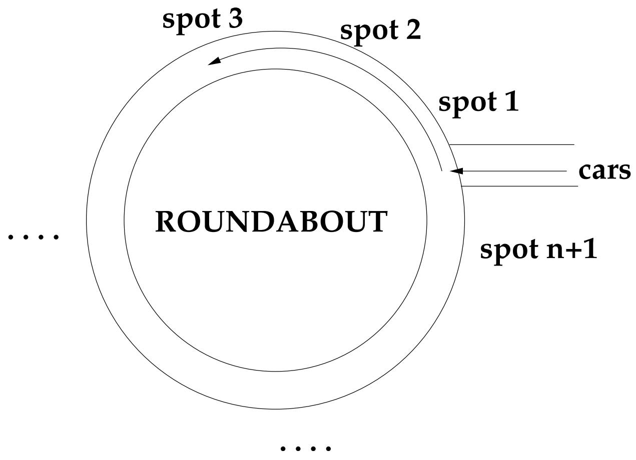


FIGURE 12.6
Parking on a roundabout.

after every car has attempted to park. Then no car preferred spot i. Suppose i or more cars preferred the first $i-1$ spots. Not all of these cars can park in the first $i-1$ spots. But then one of these cars would have parked in spot i, a contradiction. We conclude that $|\{x : h(x) \leq i\}| < i$, so that h is not a parking function. □

12.15. Theorem: Enumeration of Parking Functions. There are $(n+1)^{n-1}$ parking functions of order n.

Proof. Fix $n > 0$. Define a *circular parking function* of order n to be any function $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n+1\}$. Let Z be the set of all such functions; we know that $|Z| = (n+1)^n$. We interpret circular parking functions as follows. Imagine a roundabout (circular street) with $n+1$ parking spots numbered $1, 2, \ldots, n+1$. See Figure 12.6. As before, f encodes the parking preferences of n cars that wish to park on the roundabout. Thus, for $1 \leq x \leq n$ and $1 \leq y \leq n+1$, $y = f(x)$ iff car x prefers to park in spot y. Cars $1, 2, \ldots, n$ arrive at the roundabout in increasing order. Each car x enters just before spot 1, then drives around to spot $f(x)$ and parks there if possible. If spot $f(x)$ is full, car x keeps driving around the roundabout and parks in the first empty spot that it encounters.

No matter what f is, every car will succeed in parking in the circular situation. Moreover, since there are now $n+1$ spots and only n cars, there will always be one empty spot at the end. Suppose we randomly select a circular parking function. Because of the symmetry of the roundabout, each of the $n+1$ parking spaces is equally likely to be the empty one. (The fact that the entrance to the roundabout is at spot 1 is irrelevant here, since for parking purposes we may as well assume that car x enters the roundabout at its preferred spot $f(x)$.) Thus, the probability that spot k is empty is $\frac{1}{n+1}$, for $1 \leq k \leq n+1$. On the other hand, spot $n+1$ will be the empty spot iff f is a parking function of order n. For, if spot $n+1$ is empty, then no car preferred spot $n+1$, and no car passed spot $n+1$ during the parking process. Thus, the circular parking process on the roundabout coincides with the original parking process on the one-way street (and conversely). Since spot $n+1$ is empty with probability $1/(n+1)$ and the sample space Z has size $(n+1)^n$, we conclude that the number of ordinary parking functions must be $|Z|/(n+1) = (n+1)^{n-1}$. □

12.16. Remark. Let $A_{n,k}$ be the set of circular parking functions of order n with empty spot k. The preceding proof shows that $|A_{n,k}| = (n+1)^{n-1}$ for $1 \leq k \leq n+1$. We established this counting result by a probabilistic argument, using symmetry to deduce that $P(A_{n,k}) = 1/(n+1)$ for all k. This symmetry property is intuitively evident, but it can also be proved rigorously as follows. Suppose $f \in A_{n,k_1}$ and k_2 are given. Let $\phi(f)$ be the function $i \mapsto f(i) + k_2 - k_1 \bmod (n+1)$ for $1 \leq i \leq n$, taking the remainder to lie in $\{1, 2, \ldots, n+1\}$. One may check that ϕ defines a bijection from A_{n,k_1} onto A_{n,k_2}. These bijections prove that all the sets $A_{n,k}$ (for $1 \leq k \leq n+1$) have the same cardinality.

12.17. Remark. One of the early motivations for studying parking functions was their connection to hashing protocols. In computing applications, one often stores information in a data structure called a *hash table.* We consider a simplified model where n items are to be stored in a linear array of n cells. A *hash function* $h : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is used to determine where each item will be stored. We store item i in position $h(i)$, *unless* that position has already been taken by a previous item — this circumstance is called a *collision.* We handle collisions via the following *collision resolution policy*: if $h(i)$ is full, we store item i in the earliest position after position i that is not yet full (if any). If there is no such position, the collision resolution fails (we do not allow "wraparound"). This scenario is exactly like that of the cars parking on a one-way street according to the preferences encoded by h. Thus, we will be able to store all n items in the hash table iff h is a parking function.

12.5 Parking Functions and Trees

We can use parking functions (§12.4) to give a bijective proof of Cayley's formula 3.72 for the number of n-vertex trees. The proof involves labeled lattice paths, which we now define.

12.18. Definition: Labeled Lattice Paths. A *labeled lattice path* consists of a lattice path π from $(0,0)$ to (a,b), together with a labeling of the b north steps of π with labels $1, 2, \ldots, b$ (each used exactly once) such that the labels for the north steps in a given column increase from bottom to top.

We can illustrate a labeled lattice path by drawing π inside an $(a+1) \times b$ grid of unit squares and placing the label of each north step in the unit square to the right of that north step. For example, Figure 12.7 displays a labeled lattice path ending at $(5,7)$.

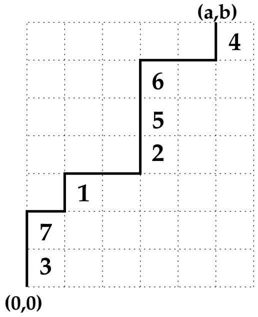


FIGURE 12.7
A labeled lattice path.

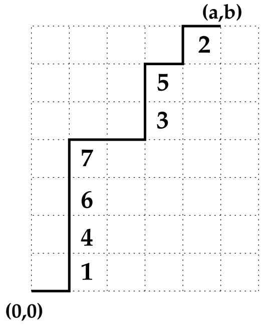


FIGURE 12.8
Converting a function to a labeled path.

12.19. Theorem: Enumeration of Labeled Paths. There are $(a+1)^b$ labeled lattice paths from $(0,0)$ to (a,b).

Proof. It suffices to construct a bijection between the set of labeled lattice paths ending at (a,b) and the set of all functions $f:\{1,2,\ldots,b\}\to\{1,2,\ldots,a+1\}$. Given a labeled lattice path P, define the associated function by setting $f(i)=j$ for all labels i in column j of P.

The inverse map acts as follows. Given a function $f:\{1,2,\ldots,b\}\to\{1,2,\ldots,a+1\}$, let $S_i=\{x:f(x)=i\}$ and $s_i=|S_i|$ for $1\leq i\leq a+1$. The labeled path associated to f is the lattice path $N^{s_1}EN^{s_2}E\cdots N^{s_{a+1}}$ where the ith string of consecutive north steps is labeled by the elements of S_i in increasing order. □

12.20. Example. The function associated to the labeled path P in Figure 12.7 is given by

$$1\mapsto 2,\ 2\mapsto 4,\ 3\mapsto 1,\ 4\mapsto 6,\ 5\mapsto 4,\ 6\mapsto 4,\ 7\mapsto 1.$$

Going the other way, the function $f:\{1,2,\ldots,7\}\to\{1,2,\ldots,6\}$ defined by

$$f(1)=2,\ f(2)=5,\ f(3)=4,\ f(4)=2,\ f(5)=4,\ f(6)=2,\ f(7)=2,$$

is mapped to the labeled lattice path shown in Figure 12.8.

A *labeled Dyck path of order* n is a Dyck path ending at (n,n) that is labeled according to the rules in 12.18. For example, Figure 12.9 displays the sixteen labeled Dyck paths of order 3.

12.21. Theorem: Enumeration of Labeled Dyck Paths. There are $(n+1)^{n-1}$ labeled Dyck paths of order n.

Proof. Using the bijection in 12.19, we can regard labeled lattice paths from $(0,0)$ to (n,n) as functions $f:\{1,2,\ldots,n\}\to\{1,2,\ldots,n+1\}$. We first show that non-Dyck labeled paths correspond to non-parking functions under this bijection. A labeled path P is *not* a Dyck path iff some east step of P goes from $(i-1,j)$ to (i,j) for some $i>j$. This condition holds for P iff the function f associated to P satisfies $|\{x:f(x)\leq i\}|=j$ for some $i>j$. In turn, this condition on f is equivalent to the existence of i such that $|\{x:f(x)\leq i\}|<i$. But this means that f is *not* a parking function (see 12.12). It now follows that labeled Dyck paths are in bijective correspondence with parking functions. So the result follows from 12.15. □

12.22. Cayley's Theorem via Parking Functions. There are $(n+1)^{n-1}$ trees with vertex set $\{0,1,2,\ldots,n\}$.

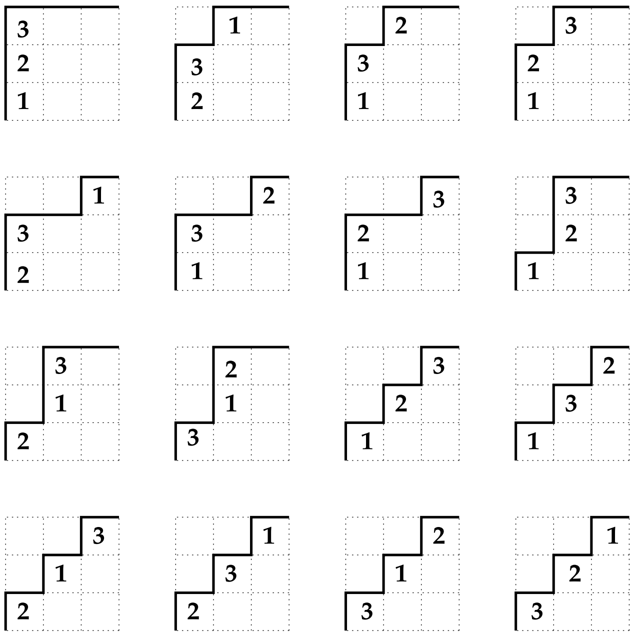


FIGURE 12.9
Labeled Dyck paths.

Proof. In light of the previous result, it suffices to define bijections between the set B of labeled Dyck paths of order n and the set C of all trees with vertex set $\{0, 1, 2, \ldots, n\}$. To define $f : B \to C$, let π be a labeled Dyck path of order n. Let $(a_1, a_2, \ldots, a_n)$ be the sequence of labels in the diagram of π, reading from the bottom row to the top row, and set $a_0 = 0$. Define a graph $T = f(\pi)$ as follows. For $0 \leq j \leq n$, there is an edge in T from vertex a_j to each vertex whose label appears in column $j+1$ of the diagram of π. These are all the edges of T. Using the fact that π is a labeled *Dyck* path, one proves by induction on j that every a_j is either 0 or appears to the left of column $j+1$ in the diagram, so that every vertex in column $j+1$ of π is reachable from vertex 0 in T. Thus, $T = f(\pi)$ is a connected graph with n edges and $n+1$ vertices, so T is a tree by 3.71.

12.23. Example. Figure 12.10 shows a parking function f, the labeled Dyck path π corresponding to f, and the tree $T = f(\pi)$. We can use the figure to compute the edges of T by writing a_j underneath column $j+1$, for $0 \leq j \leq n$. If we regard zero as the ancestor of all other vertices, then the labels in column $j+1$ are the children of vertex a_j.

Continuing the proof, we define the inverse map $f' : C \to B$. Let $T \in C$ be a tree with vertex set $\{0, 1, 2, \ldots, n\}$. We generate the diagram for $f'(T)$ by inserting labels into an $n \times n$ grid from bottom to top. Denote these labels by $(a_1, \ldots, a_n)$, and set $a_0 = 0$. The labels $a_1, a_2, \ldots$ in column 1 are the vertices of T adjacent to vertex $a_0 = 0$ (written in increasing order from bottom to top). The labels in the second column are the neighbors of a_1 other than vertex 0. The labels in the third column are the neighbors of a_2 not in the set $\{a_0, a_1\}$. In general, the labels in column $j+1$ are the neighbors of a_j not in the set $\{a_0, a_1, \ldots, a_{j-1}\}$. Observe that we do not know the full sequence $(a_1, \ldots, a_n)$ in advance, but we reconstruct this sequence as we go along. We will show momentarily that a_j is always known by the time we reach column $j+1$.

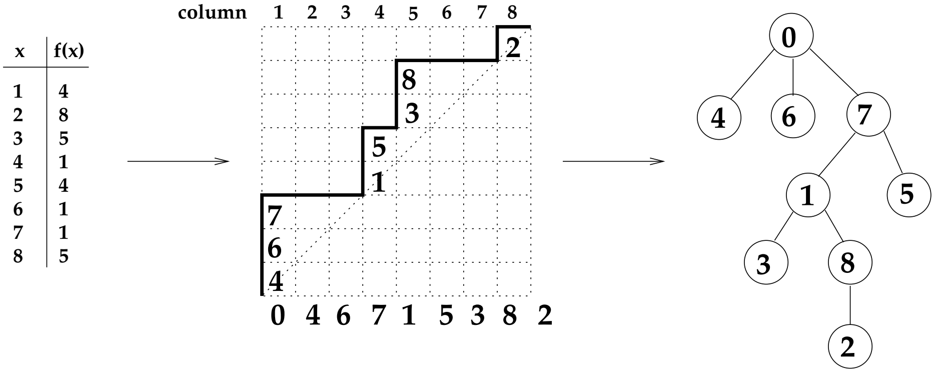


FIGURE 12.10
Mapping parking functions to labeled Dyck paths to trees.

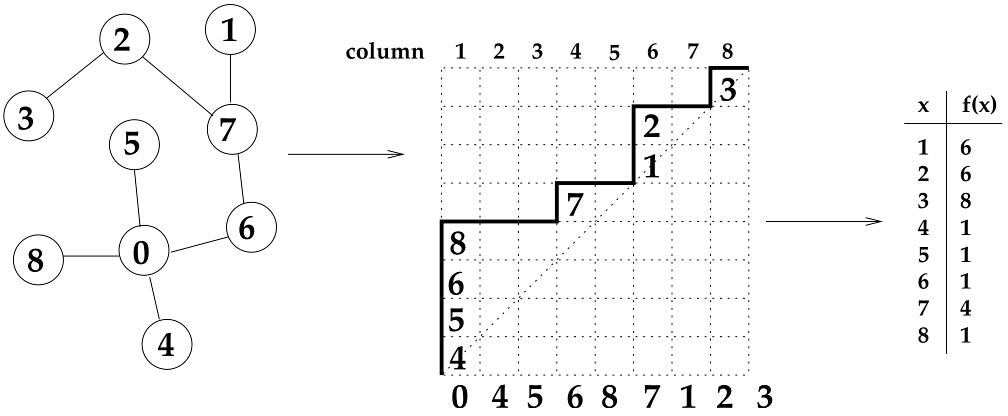


FIGURE 12.11
Mapping trees to labeled Dyck paths to parking functions.

12.24. Example. Figure 12.11 shows a tree T, the labeled Dyck path $\pi = f'(T)$, and the parking function associated to π.

Let us check that f' is well defined. We break up the computation of $f'(T)$ into stages, where stage j consists of choosing the increasing sequence of labels $a_i < \cdots < a_k$ that occur in column j. We claim that at each stage j with $1 \leq j \leq n+1$, a_{j-1} has already been computed, so that the labels entered in column j occur in rows j or higher. This will show that the algorithm for computing f' is well defined and produces a labeled *Dyck* path. We proceed by induction on j. The claim holds for $j = 1$, since $a_0 = 0$ by definition. Assume that $1 < j \leq n+1$ and that the claim holds for all $j' < j$. To get a contradiction, assume that a_{j-1} is not known when we reach column j. Since the claim holds for $j - 1$, we must have already recovered the labels in the set $W = \{a_0 = 0, a_1, \ldots, a_{j-2}\}$, which are precisely the labels that occur in the first $j - 1$ columns. Let z be a vertex of T not in W. Since T is a tree, there is a path from 0 to z in T. Let y be the earliest vertex on this path not in W, and let x be the vertex just before y on the path. By choice of y, we have $x \in W$, so that $x = 0$ or $x = a_k$ for some $k \leq j - 2$. But if $x = 0$, then y occurs in column 1 and hence $y \in W$. And if $x = a_k$, then the algorithm for f' would have placed y in column $k + 1 \leq j - 1$, and again $y \in W$. These contradictions show that the claim holds for j. It is now routine to check that f' is the two-sided inverse of f. □

12.6 Möbius Inversion and Field Theory

This section gives two applications of the material in §4.7 to field theory. We show that every finite subgroup of the multiplicative group of any field must be cyclic; and we count the number of irreducible polynomials of a given degree with coefficients in a given finite field. The starting point for proving the first result is the relation $n = \sum_{d|n} \phi(d)$, proved in 4.34. We begin by giving a combinatorial interpretation of this identity in terms of the orders of elements in a cyclic group of size n.

12.25. Theorem: Order of Elements in a Cyclic Group. Suppose G is a cyclic group of size $d < \infty$, written multiplicatively. If $x \in G$ generates G and $c \geq 1$, then x^c generates a cyclic subgroup of G of order $d/\gcd(c,d) = \operatorname{lcm}(c,d)/c$.

Proof. Since $\langle x^c \rangle \subseteq G$, the order of x^c must be finite. Let k be the order of x^c. We have seen in 9.79 that k is the smallest positive integer such that $x^{ck} = 1_G$, and that the k elements x^c, x^{2c}, …, x^{kc} are distinct and constitute the cyclic subgroup of G generated by x^c. Since x has order d, we know from 9.79 that $x^m = 1$ iff $d|m$. It follows from this and the definition of k that kc is the least positive multiple of c that is also a multiple of d. In other words, $kc = \operatorname{lcm}(c,d)$. It follows that the order of x^c is $k = \operatorname{lcm}(c,d)/c$. Since $cd = \operatorname{lcm}(c,d)\gcd(c,d)$, we also have $k = d/\gcd(c,d)$. □

12.26. Theorem: Counting Generators in a Cyclic Group. If G is a cyclic group of size $d < \infty$, then there are exactly $\phi(d)$ elements in G that generate G.

Proof. Let x be a fixed generator of G. By 9.79, the d distinct elements of G are $x^1, x^2, \ldots, x^d = 1_G$. By 12.25, the element x^c generates all of G iff $\gcd(c,d) = 1$. By the definition of ϕ (see 4.19), the number of such integers c between 1 and d is precisely $\phi(d)$. □

12.27. Theorem: Subgroup Structure of Cyclic Groups. Let G be a cyclic group of size $n < \infty$. For each d dividing n, there exists exactly one subgroup of G of size d, and this subgroup is cyclic.

Proof. We only sketch the proof, which uses some results about group homomorphisms that were stated as exercises in Chapter 9. We know from 9.59 that every subgroup of the cyclic group $\mathbb{Z}$ has the form $k\mathbb{Z}$ for some unique $k \geq 0$, and is therefore cyclic. Next, any finite cyclic group G can be viewed as the quotient group $\mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$. This follows by applying the fundamental homomorphism theorem 9.207 to the map from $\mathbb{Z}$ to G sending 1 to a generator of G. By the correspondence theorem 9.211, each subgroup H of G has the form $H = m\mathbb{Z}/n\mathbb{Z}$ for some subgroup $m\mathbb{Z}$ of $\mathbb{Z}$ containing $n\mathbb{Z}$. Now, $m\mathbb{Z}$ contains $n\mathbb{Z}$ iff $m|n$, and in this case $|m\mathbb{Z}/n\mathbb{Z}| = n/m$. It follows that there is a bijection between the positive divisors of n and the subgroups of G. Each such subgroup is the homomorphic image of a cyclic group $m\mathbb{Z}$, so each subgroup of G is cyclic. □

Suppose G is cyclic of size n. For each $d|n$, let G_d be the unique (cyclic) subgroup of G of size d. On one hand, each element y of G generates exactly one of the subgroups G_d (namely, y generates the group G_d such that d is the order of y). On the other hand, we have shown that G_d has exactly $\phi(d)$ generators. Invoking the sum rule, we obtain a new proof of the fact that

$$n = \sum_{d|n} \phi(d).$$

12.28. Theorem: Detecting Cyclic Groups. If G is a group of size n such that for each d dividing n, G has at most one subgroup of size d, then G is cyclic.

Proof. For each d dividing n, let T_d be the set of elements in G of order d. G is the disjoint union of the sets T_d by 9.119. Consider a fixed choice of d such that T_d is nonempty. Then G has an element of order d, hence has a cyclic subgroup of size d. By assumption, this is the only subgroup of G of size d, and we know this subgroup has $\phi(d)$ generators. Therefore, $|T_d| = \phi(d)$ whenever $|T_d| \neq 0$. We conclude that

$$n = |G| = \sum_{d|n} |T_d| \leq \sum_{d|n} \phi(d) = n.$$

Since the extreme ends of this calculation both equal n, the middle inequality here must in fact be an equality. This is only possible if every T_d is nonempty. In particular, T_n is nonempty. Therefore, G is cyclic, since it is generated by each of the elements in T_n. □

12.29. Theorem: Multiplicative Subgroups of Fields. Let F be any field, possibly infinite. If G is a finite subgroup of the multiplicative group of F, then G is cyclic.

Proof. Suppose G is a subgroup of F^* (the multiplicative group of nonzero elements in F) such that $|G| = n < \infty$. By 12.28, it suffices to show that G has at most one subgroup of size d, for each $d|n$. If not, let H and K be two distinct subgroups of G of size d. Then $H \cup K$ is a set with at least $d+1$ elements; and for each $z \in H \cup K$, it follows from 9.119 that z is a root of the polynomial $x^d - 1$ in F. But any polynomial of degree d over F has at most d distinct roots in the field F (see 2.157). This contradiction completes the proof. □

Our next goal is to count irreducible polynomials of a given degree over a finite field. We shall assume a number of results from field theory, whose proofs may be found in Chapter V of the algebra text by Hungerford [70]. Let F be a finite field with q elements. It is known that q must be a prime power, say $q = p^e$, and F is uniquely determined (up to isomorphism) by its cardinality q. Every finite field F with $q = p^e$ elements is a splitting field for the polynomial $x^q - x$ over $\mathbb{Z}/p\mathbb{Z}$.

12.30. Theorem: Enumeration of Irreducible Polynomials. Let F be a field with $q = p^e$ elements. For each $n \geq 1$, let $I(n, q)$ be the number of monic irreducible polynomials of degree n in the polynomial ring $F[x]$. Then

$$q^n = \sum_{d|n} dI(d, q)$$

and hence

$$I(n, q) = \frac{1}{n} \sum_{d|n} q^d \mu(n/d).$$

Proof. The strategy of the proof is to classify the elements in a finite field K of size q^n based on their minimal polynomials. From field theory, we know that each element $u \in K$ is the root of a uniquely determined monic, irreducible polynomial in $F[x]$ (called the *minimal polynomial of* u *over* F). The degree d of this minimal polynomial is $d = [F(u) : F]$, where for any field extension $E \subseteq H$, $[H : E]$ denotes the dimension of H viewed as a vector space over E. It is known that $n = [K : F] = [K : F(u)] \cdot [F(u) : F]$, so that $d|n$. Conversely, given any divisor d of n, we claim that every irreducible polynomial of degree d in $F[x]$ has d distinct roots in K. Sketch of proof: Suppose g is such a polynomial and $z \neq 0$ is a root of g in a splitting field of g over K. Since z lies in $F(z)$, which is a field with q^d elements, it follows from 9.119 (applied to the multiplicative group $F(z)^*$) that $z^{q^d-1} = 1$. One checks that $q^d - 1$ divides $q^n - 1$ (since $d|n$), so that $z^{q^n-1} = 1$, and hence z is a root of $x^{q^n} - x$. It follows that every root z of g actually lies in K (which is a splitting field for $x^{q^n} - x$). Furthermore, since z is a root of $x^{q^n} - x$, it follows that the minimal polynomial for z over F (namely g) divides $x^{q^n} - x$ in $F[x]$. We conclude that g divides $x^{q^n} - x$ in $K[x]$ also. The polynomial $x^{q^n} - x$ is known to split into a product of q^n *distinct* linear factors over K; in fact, $x^{q^n} - x = \prod_{x_0 \in K}(x - x_0)$. By unique factorization in the polynomial ring $K[x]$, g must also be a product of d *distinct* linear factors. This completes the proof of the claim.

We can now write K as the disjoint union of sets R_g indexed by all irreducible polynomials in $F[x]$ whose degrees divide n, where R_g consists of the $\deg(g)$ distinct roots of g in K. Invoking the sum rule and grouping together terms indexed by polynomials of degree d dividing n, we obtain

$$q^n = |K| = \sum_{\substack{\text{irreducible } g \\ \deg(g)|n}} |R_g| = \sum_{\substack{\text{irreducible } g \\ \deg(g)|n}} \deg(g) = \sum_{d|n} dI(d, q).$$

We can now apply the Möbius inversion formula 4.30 to the functions $f(n) = q^n$ and $g(n) = nI(n, q)$ to obtain

$$nI(n, q) = \sum_{d|n} q^d \mu(n/d). \qquad \square$$

12.7 Quantum Binomial Coefficients and Subspaces

Recall (§6.7) that the *quantum binomial coefficients* are the polynomials in $\mathbb{N}[x]$ defined by the formula

$$\begin{bmatrix} n \\ k \end{bmatrix}_x = \frac{[n]!_x}{[k]!_x[n-k]!_x} = \frac{\prod_{i=1}^n (x^i - 1)}{\prod_{i=1}^k (x^i - 1) \prod_{i=1}^{n-k} (x^i - 1)}.$$

We gave a number of combinatorial interpretations of these polynomials in §6.7. In this section, we discuss a linear-algebraic interpretation of the integers $\begin{bmatrix} n \\ k \end{bmatrix}_q$, where q is a prime power. To read this section, the reader should have some previous experience with fields and vector spaces. We begin by using bases to determine the possible sizes of vector spaces over finite fields.

12.31. Theorem: Size of Vector Spaces over Finite Fields. Suppose V is a d-dimensional vector space over a finite field F with q elements. Then $|V| = q^d$.

Proof. Let $(v_1, \ldots, v_d)$ be an ordered basis for V. By definition of a basis, for each $v \in V$, there exists exactly one d-tuple of scalars $(c_1, \ldots, c_d) \in F^d$ such that $v = c_1v_1 + c_2v_2 + \cdots + c_dv_d$. In other words, there is a bijection $v \mapsto (c_1, \ldots, c_d)$ from V to F^d. Because $|F| = q$, the product rule gives $|V| = |F^d| = |F|^d = q^d$. □

12.32. Theorem: Size of Finite Fields. If K is a finite field, then $|K| = p^e$ for some prime p and some $e \geq 1$.

Proof. Given K, let F be the cyclic subgroup of the additive group $(K, +)$ generated by 1_K. The size of F is some finite number p (since K is finite), and $p > 1$ since $1_K \neq 0_K$. We know that p is the smallest positive integer such that $p1_K = 0_K$. One checks (using the distributive laws) that F is a subring of K, not just a subgroup. If p were not prime, say $p = ab$ with $1 < a, b < p$, then $(a1_K) \cdot (b1_K) = ab1_K = p1_K = 0_K$, and yet $a1_K, b1_K \neq 0$. This contradicts the fact that fields have no zero divisors. Thus, p must be prime. It now follows that F is a *field* isomorphic to the field of integers modulo p. K can be regarded as a vector space over its subfield F, by defining scalar multiplication $F \times K \to K$ to be the restriction of the multiplication $K \times K \to K$ in the field. Since K is finite, it must be a finite-dimensional vector space over F. Thus the desired result follows from 12.31. □

12.33. Remark. One can show that, for every prime power p^e, there exists a finite field of size p^e, which is unique up to isomorphism. The existence proof is sketched in 12.126.

We now give the promised linear-algebraic interpretation of quantum binomial coefficients.

12.34. Theorem. Let K be a finite field with q elements. For all integers $n \geq 0$ and $0 \leq k \leq n$, $\begin{bmatrix} n \\ k \end{bmatrix}_q$ is the number of k-dimensional subspaces of any n-dimensional vector space V over K.

Proof. Let $f(n, k, q)$ be the number of k-dimensional subspaces of V. (One can check that this number depends only on k, q, and $n = \dim(V)$.) Recall from 12.31 that $|V| = q^n$ and each d-dimensional subspace of V has size q^d. By rearranging factors in the defining formula for $\begin{bmatrix} n \\ k \end{bmatrix}_q$, we see that $\begin{bmatrix} n \\ k \end{bmatrix}_q = f(n, k, q)$ holds iff

$$f(n, k, q)(q^k - 1)(q^{k-1} - 1) \cdots (q^1 - 1) = (q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1).$$

We establish this equality by the following counting argument. Let S be the set of all ordered lists $(v_1, \ldots, v_k)$ of k linearly independent vectors in V. Here is one way to build such a list. First, choose a nonzero vector $v_1 \in V$ in any of $q^n - 1$ ways. This vector spans a one-dimensional subspace W_1 of V of size $q = q^1$. Second, choose a vector $v_2 \in V \sim W_1$ in any of $q^n - q$ ways. The list (v_1, v_2) must be linearly independent since v_2 is not in the space W_1 spanned by v_1. Vectors v_1 and v_2 span a two-dimensional subspace W_2 of V of size q^2. Third, choose $v_3 \in V \sim W_2$ in $q^n - q^2$ ways. Continue similarly. When choosing v_i, we have already found $i - 1$ linearly independent vectors $v_1, \ldots, v_{i-1}$ that span a subspace of V of size q^{i-1}. Consequently, $(v_1, \ldots, v_i)$ will be linearly independent iff we choose $v_i \in V \sim W_i$, which is a set of size $q^n - q^{i-1}$. By the product rule, we conclude that

$$|S| = \prod_{i=1}^{k}(q^n - q^{i-1}) = \prod_{i=1}^{k} q^{i-1}(q^{n+1-i} - 1) = q^{k(k-1)/2}(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1).$$

Now let us count S in a different way. Observe that the vectors in each list $(v_1, \ldots, v_k) \in S$ span some k-dimensional subspace of V. So we can begin by choosing such a subspace W in any of $f(n, k, q)$ ways. Next we choose $v_1, \ldots, v_k \in W$ one at a time, following the same process used in the first part of the proof. We can choose v_1 in $|W| - 1 = q^k - 1$ ways, then v_2 in $q^k - q$ ways, and so on. By the product rule,

$$|S| = f(n, k, q) \prod_{i=1}^{k} (q^k - q^{i-1}) = f(n, k, q) q^{k(k-1)/2} (q^k - 1)(q^{k-1} - 1) \cdots (q^1 - 1).$$

Equating the two formulas for $|S|$ and cancelling $q^{k(k-1)/2}$ gives the desired result. □

In 6.36, we saw that

$$\begin{bmatrix} n \\ k \end{bmatrix}_x = \sum_{\mu \in P(k, n-k)} x^{|\mu|}$$

where $P(k, n - k)$ is the set of all integer partitions μ that fit in a $k \times (n - k)$ rectangle. In the rest of this section, we shall give a second proof of 12.34 by showing that

$$f(n, k, q) = \sum_{\mu \in P(k, n-k)} q^{|\mu|}.$$

This proof is longer than the one just given, but it reveals a close connection between enumeration of subspaces on one hand, and enumeration of partitions in a box (or, equivalently, lattice paths) on the other hand.

For convenience, we shall work with the vector space $V = K^n$ whose elements are n-tuples of elements of K. We regard elements of V as row vectors of length n. The key linear-algebraic fact we need is that every k-dimensional subspace of $V = K^n$ has a unique "reduced row-echelon form basis."

12.35. Definition: Reduced Row-Echelon Form. Let A be a $k \times n$ matrix with entries in K. Let $A_1, \ldots, A_k \in K^n$ be the k rows of A. We say A is a *reduced row-echelon form* (RREF) matrix iff the following conditions hold: (i) $A_i \neq 0$ for all i, and the leftmost nonzero entry of A_i is 1_K (call these entries *leading ones*); (ii) if the leading one of A_i occurs in column $j(i)$, then $j(1) < j(2) < \cdots < j(k)$; (iii) every leading one is the only nonzero entry in its column. An ordered basis $B = (v_1, \ldots, v_k)$ for a k-dimensional subspace of K^n is called a *RREF basis* iff the matrix whose rows are $v_1, \ldots, v_k$ is a RREF matrix.

12.36. Theorem: RREF Bases. Let K be any field. Every k-dimensional subspace of K^n has a unique RREF basis. Conversely, the rows of every $k \times n$ RREF matrix comprise an ordered basis for a k-dimensional subspace of K^n. Consequently, there is a bijection between the set of such subspaces and the set of $k \times n$ RREF matrices with entries in K.

Proof. We sketch the proof, trusting the reader's ability to supply the remaining linear algebra details. *Step 1:* We use row-reduction to show that any given k-dimensional subspace W of K^n has *at least one* RREF basis. Start with any ordered basis $v_1, \ldots, v_k$ of W, and let A be the matrix with rows $v_1, \ldots, v_k$. There are three "elementary row operations" we can use to simplify A: interchange two rows; multiply one row by a nonzero scalar; add any scalar multiple of one row to a different row. A routine verification shows that performing any one of these operations has no effect on the subspace spanned by the rows of A. Therefore, we can create new ordered bases for W by performing sequences of row operations on A. Using the well-known Gaussian elimination algorithm ("row reduction"), we can bring the matrix A into reduced row-echelon form. The rows of the new matrix give the desired RREF basis of W.

Step 2: We show that a given subspace W has *at most one* RREF basis. Use induction on k, the base case $k = 0$ being immediate. For the induction step, assume $n \geq 1$ and $k \geq 1$ are fixed, and the uniqueness result is known for smaller values of k. Let A and B be two RREF matrices whose rows form bases of W; we must prove $A = B$. Let $j(1) < j(2) < \cdots < j(k)$ be the positions of the leading ones in A, and let $r(1) < \cdots < r(k)$ be the positions of the leading ones in B. If $j(1) < r(1)$, then the first row of A (which is a vector in W) has a 1 in position $j(1)$. This vector cannot possibly be a linear combination of the rows of B, all of whose nonzero entries occur in columns after $j(1)$. Thus, $j(1) < r(1)$ is impossible. A similar argument rules out $r(1) < j(1)$, so we must have $j(1) = r(1)$. Let W' be the subspace of W consisting of vectors with zeroes in positions $1, 2, \ldots, j(1)$. Consideration of leading ones shows that rows 2 through k of A must form a basis for W', and rows 2 through k of B also form a basis for W'. Since $\dim(W') = k - 1$, the induction hypothesis implies that rows 2 through k of A equal the corresponding rows of B. In particular, we now know that $r(i) = j(i)$ for $1 \leq i \leq k$. To finish, we must still check that row 1 of A equals row 1 of B. Let the rows of B be $w_1, \ldots, w_k$, and write v_1 for the first row of A. Since $v_1 \in W$, we have $v_1 = a_1 w_1 + \cdots + a_k w_k$ for suitable scalars a_k. Consideration of column $j(1)$ shows that $a_1 = 1$. On the other hand, if $a_i \neq 0$ for some $i > 1$, then $a_1 w_1 + \cdots + a_k w_k$ would have a nonzero entry in position $j(i)$, whereas v_1 has a zero entry in this position (since the leading ones occur in the same columns in A and B). This is a contradiction, so $a_2 = \cdots = a_k = 0$. Thus $v_1 = w_1$, as desired, and we have now proved that $A = B$.

Step 3: We show that the k rows $v_1, \ldots, v_k$ of a given RREF matrix form an ordered basis for some k-dimensional subspace of K^n. It suffices to show that the rows in question are linearly independent vectors. Suppose $c_1 v_1 + \cdots + c_k v_k = 0$, where $c_i \in K$. Recall that the leading one in position $(i, j(i))$ is the only nonzero entry in its column. Therefore, taking the $j(i)$th component of the preceding equation, we get $c_i = 0$ for $1 \leq i \leq k$.

□

Because of the preceding theorem, the problem of counting k-dimensional subspaces of K^n (where $|K| = q$) reduces to the problem of counting $k \times n$ RREF matrices with entries in K. Our second proof of 12.34 will therefore be complete once we prove the following result.

12.37. Theorem: Enumeration of RREF Matrices. Let K be a finite field with q elements. The number of $k \times n$ RREF matrices with entries in K is

$$\sum_{\mu \in P(k,n-k)} q^{|\mu|} = \begin{bmatrix} n \\ k \end{bmatrix}_q .$$

Proof. Let us classify the $k \times n$ RREF matrices based on the columns $j(1) < j(2) < \cdots < j(k)$ where the leading ones occur. To build a RREF matrix with the leading ones in these positions, we must put zeroes in all matrix positions (i, p) such that $p < j(i)$; we must also put zeroes in all matrix positions $(r, j(i))$ such that $r < i$. However, in all the other positions to the right of the leading ones, there is no restriction on the elements that occur except that they must come from the field K of size q. How many such "free positions" are there? The first row contains $n - j(1)$ entries after the leading one, but $k - 1$ of these entries are in columns above other leading ones. So there are $\mu_1 = n - j(1) - (k - 1)$ free positions in this row. The next row contains $n - j(2)$ entries after the leading one, but $k - 2$ of these occur in columns above other leading ones. So there are $\mu_2 = n - j(2) - (k - 2)$ free positions in row 2. Similarly, there are $\mu_i = n - j(i) - (k - i) = n - k + i - j(i)$ free positions in row i for $1 \leq i \leq k$. The condition $1 \leq j(1) < j(2) < \cdots < j(k) \leq n$ is logically equivalent to $0 \leq j(1) - 1 \leq j(2) - 2 \leq \cdots \leq j(k) - k \leq n - k$, which is in turn equivalent to $n - k \geq \mu_1 \geq \mu_2 \geq \cdots \geq \mu_k \geq 0$. *Thus there is a bijection between the set of valid* *positions* $j(1) < j(2) < \ldots < j(k)$ *for the leading ones, and the set of integer partitions* $\mu = (\mu_1, \ldots, \mu_k)$ *that fit in a* $k \times (n-k)$ *box, given by* $\mu_i = n - k + i - j(i)$*.* Furthermore, $|\mu| = \mu_1 + \cdots + \mu_k$ is the total number of free positions in each RREF matrix with leading ones in the positions $j(i)$. Using the product rule to fill these free positions one at a time with elements of K, we see that there are $q^{|\mu|}$ RREF matrices with leading ones in the given positions. The theorem now follows from the sum rule, keeping in mind the bijection just constructed between j-sequences and partitions. □

12.38. Example. To illustrate the preceding proof, take $n = 10$, $k = 4$, and consider RREF matrices of the form

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

Here $*$'s mark the free positions in the matrix, and $(j(1), j(2), j(3), j(4)) = (2, 5, 6, 9)$. The associated partition is $\mu = (5, 3, 3, 1)$, which does fit in a 4×6 box. We can see the (reflected) diagram of this partition in the matrix by erasing the columns without stars and right-justifying the remaining columns. Evidently there are $q^{12} = q^{|\mu|}$ ways of completing this template to get an RREF matrix with the leading ones in the indicated positions.

Going the other way, consider another partition $\mu = (6, 2, 2, 0)$ that fits in a 4×6 box. Using the formula $j(i) = n - k + i - \mu_i$, we recover $(j(1), j(2), j(3), j(4)) = (1, 6, 7, 10)$, which tells us the locations of the leading ones. So this particular partition corresponds to RREF matrices that match the following template:

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

12.8 Tangent and Secant Numbers

In calculus, one learns the following power series expansions for the trigonometric functions sine, cosine, and arctangent:

$$\sin x = x - x^3/3! + x^5/5! - x^7/7! + \cdots = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k+1}}{(2k+1)!};$$

$$\cos x = 1 - x^2/2! + x^4/4! - x^6/6! - \cdots = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k}}{(2k)!};$$

$$\arctan x = x - x^3/3 + x^5/5 - x^7/7 + \cdots = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k+1}}{2k+1}.$$

These expansions are all special cases of Taylor's formula $f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n$. Using Taylor's formula, one can also find power series expansions for the tangent and secant functions:

$$\tan x = x + \frac{1}{3}x^3 + \frac{2}{15}x^5 + \frac{17}{315}x^7 + \frac{62}{2835}x^9 + \frac{1382}{155925}x^{11} + \cdots;$$

$$\sec x = 1 + \frac{1}{2}x^2 + \frac{5}{24}x^4 + \frac{61}{720}x^6 + \frac{277}{8064}x^8 + \frac{50521}{3628800}x^{10} + \cdots.$$

The coefficients of these series seem quite irregular and unpredictable compared to the preceding three series. Remarkably, as we shall see in this section, these coefficients encode the solution to a counting problem involving permutations.

As in Chapter 7, we consider formal versions of the tangent and secant power series to avoid any questions of convergence. We define $\tan x = \sin x/\cos x$ and $\sec x = 1/\cos x$, where $\sin x$ and $\cos x$ are the formal series defined in 7.52. Now, for each $n \geq 0$, set $a_n = (\tan x)^{(n)}(0)$ and $b_n = (\sec x)^{(n)}(0)$. The formal Maclaurin formula 7.55 asserts that

$$\tan x = \sum_{n=0}^{\infty} \frac{a_n}{n!}x^n; \qquad \sec x = \sum_{n=0}^{\infty} \frac{b_n}{n!}x^n. \tag{12.1}$$

Since the ordinary Maclaurin series for the tangent and secant functions converge in a neighborhood of zero, the coefficients in the formal power series above match the coefficients in the ordinary power series representing the tangent and secant functions. The first several values of a_n and b_n are

$$\begin{aligned} (a_n : n \geq 0) &= (0,1,0,2,0,16,0,272,0,7936,0,353792,\ldots); \\ (b_n : n \geq 0) &= (1,0,1,0,5,0,61,0,1385,0,50521,\ldots). \end{aligned} \tag{12.2}$$

One can check that $a_n = 0$ for all even n and $b_n = 0$ for all odd n (cf. 7.161).

Next, for each integer $n \geq 0$, let c_n be the number of permutations $w = w_1w_2\cdots w_n$ of $\{1, 2, \ldots, n\}$ such that

$$w_1 < w_2 > w_3 < w_4 > \cdots < w_{n-1} > w_n; \tag{12.3}$$

note that $c_n = 0$ for all even n. For each integer $n \geq 0$, let d_n be the number of permutations w of $\{1, 2, \ldots, n\}$ (or any n-letter ordered alphabet) such that

$$w_1 < w_2 > w_3 < w_4 > \cdots > w_{n-1} < w_n; \tag{12.4}$$

note that $d_n = 0$ for all odd n. By reversing the ordering of the letters, one sees that d_n also counts the permutations w of n letters such that

$$w_1 > w_2 < w_3 > w_4 < \cdots < w_{n-1} > w_n. \tag{12.5}$$

Permutations of the form (12.3) or (12.4) are called *up-down permutations.* We aim to prove that $a_n = c_n$ and $b_n = d_n$ for all integers $n \geq 0$. The proof consists of five steps.

Step 1. Using the formal derivative rules, one may show that $(\tan x)' = \sec^2 x$ (see 7.159). Differentiating the first series in (12.1), squaring the second series using 7.6, and equating the coefficients of x^n, we obtain

$$\frac{a_{n+1}}{n!} = \sum_{k=0}^{n} \frac{b_k}{k!} \frac{b_{n-k}}{(n-k)!}$$

or equivalently,

$$a_{n+1} = \sum_{k=0}^{n} \binom{n}{k} b_k b_{n-k}. \tag{12.6}$$

Step 2. We also have $(\sec x)' = \tan x \sec x$ (see 7.159). Differentiating the second series

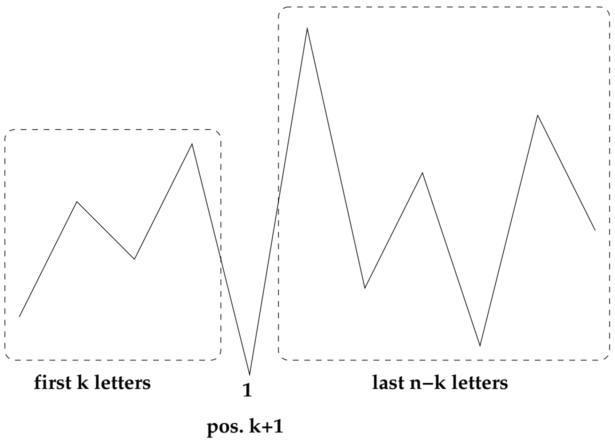


FIGURE 12.12
Counting up-down permutations of odd length.

in (12.1), multiplying the two series together using 7.6, and equating the coefficients of x^n, we obtain

$$\frac{b_{n+1}}{n!} = \sum_{k=0}^{n} \frac{a_k}{k!} \frac{b_{n-k}}{(n-k)!}$$

or equivalently,

$$b_{n+1} = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}. \tag{12.7}$$

Step 3. We give a counting argument to prove the relation

$$c_{n+1} = \sum_{k=0}^{n} \binom{n}{k} d_k d_{n-k}. \tag{12.8}$$

If n is odd, then both sides of this relation are zero, since at least one of k or $n-k$ is odd for each k. Now suppose n is even. How can we build a typical permutation

$$w = w_1 < w_2 > w_3 < \cdots > w_{n+1}$$

counted by c_{n+1}? Let us first choose the position of 1 in w; say $w_{k+1} = 1$ for some k between 0 and n. The required inequalities at position $k+1$ will be satisfied if and only if k is even. Observe that in the case where k is odd, $d_k d_{n-k} = 0$ so this term contributes nothing to the right side of (12.8). Given that k is even, choose a k-element subset A of the n remaining letters in $\binom{n}{k}$ ways. Use these letters to fill in the first k positions of w, subject to the required inequalities (12.4), in any of d_k ways. Use the remaining letters to fill in the last $(n+1)-(k+1) = n-k$ positions of w (subject to the inequalities (12.5), reindexed to begin at index $k+2$), in any of d_{n-k} ways. The desired relation now follows from the sum and product rules. See Figure 12.12, in which w is visualized as a sequence of line segments connecting the points (i, w_i) for $1 \leq i \leq n+1$.

Step 4. We give a counting argument to prove the relation

$$d_{n+1} = \sum_{k=0}^{n} \binom{n}{k} c_k d_{n-k}. \tag{12.9}$$

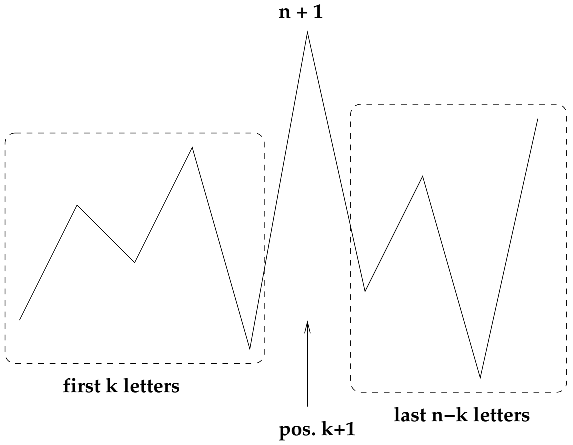


FIGURE 12.13
Counting up-down permutations of even length.

Both sides are zero if n is even. If n is odd, we must build a permutation

$$w = w_1 < w_2 > w_3 < \cdots < w_{n+1}.$$

First choose an index k with $0 \leq k \leq n$, and define $w_{k+1} = n+1$. This time, to get a nonzero contribution from this value of k, we need k to be odd. Now pick a k-element subset A of the n remaining letters. Use the letters in A to fill in $w_1, w_2, \ldots, w_k$ (c_k ways), and use the remaining letters to fill in $w_{k+2}, \ldots, w_{n+1}$ (d_{n-k} ways). See Figure 12.13.

Step 5: A routine induction argument now shows that $a_n = c_n$ and $b_n = d_n$ for all $n \geq 0$, since the pair of sequences $(a_n), (b_n)$ satisfy the same system of recursions and initial conditions as the pair of sequences $(c_n), (d_n)$. This completes the proof.

12.9 Tournaments and the Vandermonde Determinant

This section uses the combinatorics of tournaments to prove a famous determinant formula.

12.39. Definition: Tournaments. An *n-player tournament* is a digraph t with vertex set $[n] = \{1, 2, \ldots, n\}$ such that, for $1 \leq i < j \leq n$, exactly one of the directed edges (i, j) or (j, i) is an edge of t. Let T_n be the set of all such tournaments.

Intuitively, the n vertices represent n players who compete in a series of one-on-one matches. Each player plays every other player exactly once, and there are no ties. If player i beats player j, the edge (i, j) is part of the tournament; otherwise, the edge (j, i) is included.

12.40. Definition: Weights, Inversions, and Sign for Tournaments. Suppose $t \in T_n$ is a tournament. The *weight* of t is $\mathrm{wt}(t) = \prod_{i=1}^{n} x_i^{\mathrm{outdeg}_t(i)}$. The *inversion number* of t is $\mathrm{inv}(t) = \sum_{1 \leq i < j \leq n} \chi((j, i) \in t)$. The *sign* of t is $\mathrm{sgn}(t) = (-1)^{\mathrm{inv}(t)}$.

Informally, $\mathrm{wt}(t) = x_1^{e_1} \cdots x_n^{e_n}$ iff player i beats e_i other players for all i. If we think of the numbers $1, 2, \ldots, n$ as giving the initial rankings of the players, $\mathrm{inv}(t)$ counts the number of times a lower-ranked player beats a higher-ranked one (with 1 being the highest rank).

12.41. Example. Consider the tournament $t \in T_5$ with edge set

$$\{(1,3),(1,4),(1,5),(2,1),(2,4),(3,2),(3,4),(3,5),(5,2),(5,4)\}.$$

We have $\mathrm{wt}(t) = x_1^3x_2^2x_3^3x_5^2$, $\mathrm{inv}(t) = 4$, and $\mathrm{sgn}(t) = +1$.

12.42. Theorem: Tournament Generating Function. For all $n \geq 1$,

$$\sum_{t \in T_n} \mathrm{sgn}(t)\,\mathrm{wt}(t) = \prod_{1 \leq i < j \leq n} (x_i - x_j).$$

Proof. We can build a tournament $t \in T_n$ by making a sequence of binary choices, indexed by the pairs $i < j$ with $i, j \in [n]$: for each $i < j$, pick either (i,j) or (j,i) and add this edge to t. Let us examine the effect of this choice on $\mathrm{wt}(t)$, $\mathrm{inv}(t)$, and $\mathrm{sgn}(t)$. If we add (i,j) to t (so i beats j), the exponent of x_i goes up by 1, inversions go up by zero, and the sign is unchanged. If we add (j,i) to t instead, the exponent of x_j goes up by 1, inversions go up by one, and the sign is multiplied by -1. The generating function $(+x_i - x_j)$ records the effect of this choice. The proof is completed by invoking the product rule for generating functions. □

Given a tournament t, there may exist three players u, v, w where u beats v, v beats w, and w beats u. This situation occurs whenever the digraph t contains a directed 3-cycle. Let us give a name to tournaments where this circularity condition does *not* occur.

12.43. Definition: Transitive Tournaments. A tournament $t \in T_n$ is *transitive* iff for all $u, v, w \in [n]$, $(u,v) \in t$ and $(v,w) \in t$ imply $(u,w) \in t$.

Note that $(u,v) \in t$ and $(v,w) \in t$ force $u \neq w$, and then $(u,w) \notin t$ is equivalent to $(w,u) \in t$. It follows that a tournament is not transitive iff there exist $u, v, w \in [n]$ with $(u,v) \in t$ and $(v,w) \in t$ and $(w,u) \in t$.

12.44. Theorem: Generating Function for Transitive Tournaments. Let T_n' be the set of transitive tournaments in T_n. Then

$$\sum_{t \in T_n'} \mathrm{sgn}(t)\,\mathrm{wt}(t) = \sum_{w \in S_n} \mathrm{sgn}(w) \prod_{k=1}^{n} x_{w(k)}^{n-k}.$$

Proof. We define a bijection $f : T_n' \to S_n$ that will be used to transfer signs and weights from T_n' to S_n. Given $t \in T_n'$, define an associated relation $\preceq$ on $[n]$ by setting $u \preceq v$ iff $u = v$ or $(u,v) \in t$. This relation is evidently reflexive, antisymmetric (since t is a tournament), and transitive (since t is transitive). Furthermore, $u \preceq v$ or $v \preceq u$ for all $u, v \in [n]$ since t is a tournament. So $\preceq$ is a total ordering of $[n]$. This ordering determines a unique permutation of the players, namely

$$f(t) = w = w_1 \prec w_2 \prec \cdots \prec w_n.$$

For all k, player w_k beats all players w_m for $m > k$ and loses to all players w_m for $m < k$. This remark shows that t is uniquely determined by w, so the map f is a bijection.

Let us compare $\mathrm{inv}(t)$ to $\mathrm{inv}(w)$, where $w = f(t)$. Consider two players $i = w_k$ and $j = w_m$ with $i < j$ (so $w_m > w_k$). This pair contributes to $\mathrm{inv}(t)$ iff $(j,i) \in t$ iff j beats i in t iff j appears before i in w iff $m < k$ iff the letters in positions m, k of w contribute to $\mathrm{inv}(w)$. So $\mathrm{inv}(t) = \mathrm{inv}(w)$ and $\mathrm{sgn}(t) = \mathrm{sgn}(w)$. Next, let us express $\mathrm{wt}(t)$ in terms of w. Since player w_k beats all players in the range $k < m \leq n$, we see that

$$\mathrm{wt}(t) = \prod_{k=1}^{n} x_{w_k}^{n-k}.$$

Define $\text{wt}(w)$ by the right side of this formula. The theorem now follows because f is a weight-preserving, sign-preserving bijection. □

We can use the bijection f to characterize transitive tournaments.

12.45. Theorem: Criterion for Transitive Tournaments. A tournament $t \in T_n$ is transitive iff no two vertices in $[n]$ have the same outdegree.

Proof. If t is transitive, consider $w = f(t) = w_1 \prec w_2 \prec \cdots \prec w_n$. As shown above, $\text{wt}(t) = \prod_{k=1}^{n} x_{w_k}^{n-k}$. The exponents $n-k$ are all distinct, so every vertex has a different outdegree. Conversely, suppose $t \in T_n$ is such that every vertex has a different outdegree. There are n vertices and n possible outdegrees (namely $0, 1, \ldots, n-1$), so each possible outdegree occurs at exactly one vertex. Let w_1 be the unique vertex with outdegree $n-1$. Then w_1 beats all other players. Next, let w_2 be the unique vertex with outdegree $n-2$. Then w_2 must beat all players except w_1. Continuing similarly, we obtain a permutation $w = w_1, w_2, \ldots, w_n$ of $[n]$ such that w_j beats w_k iff $j < k$. To confirm that t is transitive, consider three players w_i, w_j, w_k with $(w_i, w_j) \in t$ and $(w_j, w_k) \in t$. Then $i < j$ and $j < k$, so $i < k$, so $(w_i, w_k) \in t$. □

12.46. Theorem: Vandermonde Determinant Formula. Let $x_1, \ldots, x_n$ be fixed elements in a commutative ring R. Define an $n \times n$ matrix V by setting $V(i,j) = x_j^{n-i}$ for $1 \le i, j \le n$. Then

$$\det(V) = \prod_{1 \le i < j \le n} (x_i - x_j).$$

Proof. According to the definition of determinants in 9.37,

$$\det(V) = \sum_{w \in S_n} \text{sgn}(w) \prod_{k=1}^{n} V(k, w(k)) = \sum_{w \in S_n} \text{sgn}(w) \prod_{k=1}^{n} x_{w(k)}^{n-k}. \tag{12.10}$$

This is the generating function for transitive tournaments, whereas $\prod_{i<j}(x_i - x_j)$ is the generating function for all tournaments with n players. So, it suffices to define a sign-reversing, weight-preserving involution $I : T_n \to T_n$ with fixed point set T'_n. Define $I(t) = t$ for $t \in T'_n$. Now consider a non-transitive tournament $t \in T_n \sim T'_n$. By 12.45, there exist two vertices $i < j \in [n]$ with the same outdegree in t. If there are several pairs of vertices with the same outdegree, choose the pair such that i and then j is minimized. Define $I(t)$ by switching the roles of i and j in t; more precisely, replace every directed edge (u, v) in t by $(s_{i,j}(u), s_{i,j}(v))$, where $s_{i,j}$ is the transposition $(i, j) \in S_n$. The resulting tournament is non-transitive (since i and j still have the same outdegree in $I(t)$) and has the same weight as t. Furthermore, $I(I(t)) = t$.

Finally, we show that $\text{sgn}(I(t)) = -\text{sgn}(t)$. Consider the factorization of $(i, j) \in S_n$ into $2(j-i)-1$ basic transpositions:

$$(i,j) = (j-1,j)(j-2,j-1)\cdots(i+1,i+2)(i,i+1)(i+1,i+2)\cdots(j-2,j-1)(j-1,j).$$

We can pass from t to $I(t)$ in stages, by applying these basic transpositions one at a time to the endpoints of the directed edges in t. We claim that each such step changes the sign of the tournament. For, consider what happens to the inversion count when we pass from a tournament z to z' by switching labels k and $k+1$. The inversion $(k+1, k)$ is present in exactly one of the tournaments z and z', and the other inversions are unaffected by the label switch. So $\text{inv}(z')$ differs from $\text{inv}(z)$ by ± 1, and hence $\text{sgn}(z') = -\text{sgn}(z)$. Since we pass from t to $I(t)$ by an odd number of moves of this type (namely $2(j-i)-1$), we see that $\text{sgn}(I(t)) = -\text{sgn}(t)$, as desired. □

12.10 Hook-Length Formula

This section presents a probabilistic proof of the hook-length formula for the number of standard tableaux of a given shape. This formula was first stated in the Introduction. For the reader's convenience, we begin by recalling the relevant definitions.

12.47. Definitions. An *integer partition of* n is a weakly decreasing sequence $\lambda = (\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_l)$ of positive integers with $\lambda_1 + \cdots + \lambda_l = n$. The *diagram* of λ is

$$\mathrm{dg}(\lambda) = \{(i,j) \in \mathbb{N} \times \mathbb{N} : 1 \leq i \leq l, 1 \leq j \leq \lambda_i\}.$$

Each $(i,j) \in \mathrm{dg}(\lambda)$ is called a *box* or a *cell.* We take i as the row index and j as the column index, where the topmost row is row 1. Given any cell $c = (i,j) \in \mathrm{dg}(\lambda)$, the *hook* of c in λ is

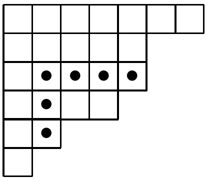
$$H(c) = \{(i,k) \in \mathrm{dg}(\lambda) : k \geq j\} \cup \{(k,j) \in \mathrm{dg}(\lambda) : k \geq i\}.$$

The *hook-length* of c in λ is $h(c) = |H(c)|$. A *corner box* of λ is a cell $c \in \mathrm{dg}(\lambda)$ with $h(c) = 1$. A *standard tableau of shape* λ is a bijection $S : \mathrm{dg}(\lambda) \to \{1, 2, \ldots, n\}$ such that $S(i,j) < S(i,j+1)$ for all i,j such that $(i,j),(i,j+1) \in \mathrm{dg}(\lambda)$, and $S(i,j) < S(i+1,j)$ for all i,j such that $(i,j),(i+1,j) \in \mathrm{dg}(\lambda)$. Let $\mathrm{SYT}(\lambda)$ be the set of standard tableaux of shape λ, and let $f^\lambda = |\,\mathrm{SYT}(\lambda)|$.

12.48. Example. If $\lambda = (7,5,5,4,2,1)$ and $c = (3,2)$, then

$$H(c) = \{(3,2),(3,3),(3,4),(3,5),(4,2),(5,2)\}$$

and $h(c) = 6$. We can visualize $\mathrm{dg}(\lambda)$ and $H(c)$ using the following picture.



Let λ'_j be the number of boxes in column j of $\mathrm{dg}(\lambda)$. Then $h(i,j) = (\lambda_i - j) + (\lambda'_j - i) + 1$. We use this formula to establish the following lemma.

12.49. Lemma. Suppose λ is a partition of n, (r,s) is a corner box of λ, and $(i,j) \in \mathrm{dg}(\lambda)$ satisfies $i < r$ and $j < s$. Then $h(i,j) = h(r,j) + h(i,s) - 1$.

Proof. Since (r,s) is a corner box, $\lambda_r = s$ and $\lambda'_s = r$. So

$$\begin{aligned} h(r,j) + h(i,s) - 1 &= [(\lambda_r - j) + (\lambda'_j - r) + 1] + [(\lambda_i - s) + (\lambda'_s - i) + 1] - 1 \\ &= s - j + \lambda'_j - r + \lambda_i - s + r - i + 1 \\ &= (\lambda_i - j) + (\lambda'_j - i) + 1 = h(i,j). \quad \square \end{aligned}$$

12.50. Theorem: Hook-Length Formula. For any partition λ of n,

$$f^\lambda = \frac{n!}{\prod_{c \in \mathrm{dg}(\lambda)} h(c)}.$$

The idea of the proof is to define a *random algorithm* that takes a partition λ of n as input and produces a standard tableau $S \in \mathrm{SYT}(\lambda)$ as output. We will prove in 12.55 that this algorithm outputs any given standard tableau S with probability

$$p = \frac{\prod_{c \in \mathrm{dg}(\lambda)} h(c)}{n!}.$$

This probability depends only on λ, not on S, so we obtain a uniform probability distribution on the sample space $\mathrm{SYT}(\lambda)$. So, on one hand, each standard tableau is produced with probability p; and on the other hand, each standard tableau is produced with probability $1/|\mathrm{SYT}(\lambda)| = 1/f^\lambda$. Thus $f^\lambda = 1/p$, and we obtain the hook-length formula.

Here is an informal description of the algorithm for generating a random standard tableau of shape λ. Start at a random cell in the shape λ. As long as we are not at a corner box, we jump from our current box c to some other cell in $H(c)$; each cell in the hook is chosen with equal probability. This jumping process eventually takes us to a corner cell. We place the entry n in this box, and then pretend this cell is no longer there. We are left with a partition μ of size $n-1$. Proceed recursively to select a random standard tableau of shape μ. Adding back the corner cell containing n gives the desired tableau of shape λ.

Now we give a formal description of the algorithm. Every random choice below is to be independent of all other choices.

12.51. Tableau Generation Algorithm. The input to the algorithm is a partition λ of n. The output is a tableau $S \in \mathrm{SYT}(\lambda)$, constructed according to the following random procedure. As a base case, if $n = 0$, return the empty tableau of shape 0.

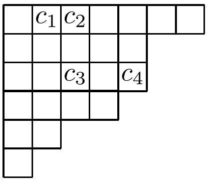
1. Choose a random cell $c \in \mathrm{dg}(\lambda)$. Each cell in $\mathrm{dg}(\lambda)$ is chosen with probability $1/n$.
2. While $h(c) > 1$, do the following.

   2a. Choose a random cell $c' \in H(c) \sim \{c\}$. Each cell in $H(c) \sim \{c\}$ is chosen with probability $1/(h(c)-1)$.

   2b. Replace c by c' and go back to step 2.
3. Now c is a corner box of $\mathrm{dg}(\lambda)$, so $\mathrm{dg}(\lambda) \sim \{c\}$ is the diagram of some partition μ of $n-1$. Recursively use the same algorithm to generate a random standard tableau $S' \in \mathrm{SYT}(\mu)$. Extend this to a standard tableau $S \in \mathrm{SYT}(\lambda)$ by setting $S(c) = n$, and output S as the answer.

Let $(c_1, c_2, c_3, \ldots, c_k)$ be the sequence of cells chosen in steps 1 and 2. Call this sequence the *hook walk for n*. Note that the hook walk must be finite, since $h(c_1) > h(c_2) > h(c_3) > \cdots$. Writing $c_s = (i_s, j_s)$ for each s, define $I = \{i_1, \ldots, i_{k-1}\} \sim \{i_k\}$ and $J = \{j_1, \ldots, j_{k-1}\} \sim \{j_k\}$. We call I and J the *row set* and *column set* for this hook walk.

12.52. Example. Given $n = 24$ and $\lambda = (7,5,5,4,2,1)$, the first iteration of the algorithm might proceed as follows.



Here we will place $n = 24$ in corner box c_4 and proceed recursively to fill in the rest of the tableau. The probability that the algorithm will choose this particular hook walk for n is

$$\frac{1}{n} \cdot \frac{1}{h(c_1)-1} \cdot \frac{1}{h(c_2)-1} \cdot \frac{1}{h(c_3)-1} = \frac{1}{24} \cdot \frac{1}{9} \cdot \frac{1}{7} \cdot \frac{1}{3}.$$

The row set and column set for this hook walk are $I = \{1\}$ and $J = \{2, 3\}$.

The next lemma is the key technical fact needed to analyze the behaviour of the tableau generation algorithm.

12.53. Lemma. Given a partition λ of n, a corner box $c = (r, s)$, and sets $I \subseteq \{1, 2, \dots, r-1\}$ and $J \subseteq \{1, 2, \dots, s-1\}$, the probability that the hook walk for n ends at c with row set I and column set J is

$$p(\lambda, c, I, J) = \frac{1}{n} \prod_{i \in I} \frac{1}{h(i,s) - 1} \prod_{j \in J} \frac{1}{h(r,j) - 1}.$$

Proof. Write $I = \{i_1 < i_2 < \cdots < i_\ell\}$ and $J = \{j_1 < j_2 < \cdots < j_m\}$, where $\ell, m \geq 0$. First we consider some degenerate cases. Say $I = J = \emptyset$. Then the hook walk for n consists of the single cell c. This happens with probability $1/n$, in agreement with the formula in the lemma (interpreting the empty products as 1). Next, suppose I is empty but J is not. The hook walk for n in this case must be $c_1 = (r, j_1)$, $c_2 = (r, j_2)$, …, $c_m = (r, j_m)$, $c_{m+1} = (r, s)$. The probability of this hook walk is

$$\frac{1}{n} \cdot \frac{1}{h(c_1) - 1} \cdot \frac{1}{h(c_2) - 1} \cdot \cdots \cdot \frac{1}{h(c_m) - 1} = \frac{1}{n} \prod_{j \in J} \frac{1}{h(r,j) - 1}.$$

Similarly, the result holds when J is empty and I is nonempty.

Now consider the case where both I and J are nonempty. We will argue by induction on $|I| + |J|$. A hook walk with row set I and column set J ending at c must begin with the cell $c_1 = (i_1, j_1)$; this cell is chosen in step 1 of the algorithm with probability $1/n$. Now, there are two possibilities for cell c_2: either $c_2 = (i_1, j_2)$ or $c_2 = (i_2, j_1)$. Each possibility for c_2 is chosen with probability $1/(h(c) - 1) = 1/(h(i_1, j_1) - 1)$. When $c_2 = (i_1, j_2)$, the sequence $(c_2, \dots, c_k)$ is a hook walk ending at c with row set I and column set $J' = J \sim \{j_1\}$. By induction, such a hook walk occurs with probability

$$\frac{1}{n} \prod_{i \in I} \frac{1}{h(i,s) - 1} \prod_{j \in J'} \frac{1}{h(r,j) - 1}.$$

However, since the walk really started at c_1 and proceeded to c_2, we replace the first factor $1/n$ by $\frac{1}{n} \cdot \frac{1}{h(c_1)-1}$. Similarly, when $c_2 = (i_2, j_1)$, the sequence $(c_2, \dots, c_k)$ is a hook walk ending at c with row set $I' = I \sim \{i_1\}$ and column set J. So the probability that the hook walk starts at c_1 and proceeds through $c_2 = (i_2, j_1)$ is

$$\frac{1}{n} \cdot \frac{1}{h(c_1) - 1} \prod_{i \in I'} \frac{1}{h(i,s) - 1} \prod_{j \in J} \frac{1}{h(r,j) - 1}.$$

Adding these two terms, we see that

$$p(\lambda, c, I, J) = \frac{1}{n} \cdot \frac{1}{h(c_1) - 1} \prod_{i \in I'} \frac{1}{h(i,s) - 1} \prod_{j \in J'} \frac{1}{h(r,j) - 1} \cdot \left(\frac{1}{h(i_1, s) - 1} + \frac{1}{h(r, j_1) - 1} \right).$$

The factor in parentheses is

$$\frac{h(r, j_1) + h(i_1, s) - 2}{(h(i_1, s) - 1)(h(r, j_1) - 1)}.$$

Using 12.49, the numerator simplifies to $h(i_1, j_1) - 1 = h(c_1) - 1$. This factor cancels and leaves us with

$$p(\lambda, c, I, J) = \frac{1}{n} \prod_{i \in I} \frac{1}{h(i,s) - 1} \prod_{j \in J} \frac{1}{h(r,j) - 1}.$$

This completes the induction proof. □

12.54. Theorem: Probability that a Hook Walk ends at c. Given a partition λ of n and a corner box $c=(r,s)$ of $\mathrm{dg}(\lambda)$, the probability that the hook walk for n ends at c is

$$p(\lambda,c)=\frac{1}{n}\prod_{i=1}^{r-1}\frac{h(i,s)}{h(i,s)-1}\prod_{j=1}^{s-1}\frac{h(r,j)}{h(r,j)-1}.$$

Proof. Write $[r-1]=\{1,2,\ldots,r-1\}$ and $[s-1]=\{1,2,\ldots,s-1\}$. By the sum rule for probabilities,

$$\begin{aligned}p(\lambda,c) &= \sum_{I\subseteq[r-1]}\sum_{J\subseteq[s-1]}p(\lambda,c,I,J)\\ &= \frac{1}{n}\sum_{I\subseteq[r-1]}\sum_{J\subseteq[s-1]}\prod_{i\in I}\frac{1}{h(i,s)-1}\prod_{j\in J}\frac{1}{h(r,j)-1}\\ &= \frac{1}{n}\left(\sum_{I\subseteq[r-1]}\prod_{i\in I}\frac{1}{h(i,s)-1}\right)\cdot\left(\sum_{J\subseteq[s-1]}\prod_{j\in J}\frac{1}{h(r,j)-1}\right).\end{aligned}$$

By 2.7, we have

$$\sum_{I\subseteq[r-1]}\prod_{i\in I}\frac{1}{h(i,s)-1}=\prod_{i=1}^{r-1}\left(1+\frac{1}{h(i,s)-1}\right)=\prod_{i=1}^{r-1}\frac{h(i,s)}{h(i,s)-1}.$$

The sum over J can be simplified in a similar way, giving the formula in the theorem. □

The next theorem is the final step in the proof of the hook-length formula.

12.55. Theorem: Probability of Generating a Given Tableau. If λ is a partition of n and $S\in\mathrm{SYT}(\lambda)$, the tableau generation algorithm outputs S with probability

$$\frac{\prod_{c\in\mathrm{dg}(\lambda)}h(c)}{n!}.$$

Proof. We prove the theorem by induction on n. Note first that the result does hold for $n=0$ and $n=1$. For the induction step, assume the result is known for partitions and tableaux with fewer than n boxes. Let $c^*=(r,s)$ be the cell such that $S(c^*)=n$, let μ be the partition obtained by removing c^* from $\mathrm{dg}(\lambda)$, and let $S'\in\mathrm{SYT}(\mu)$ be the tableau obtained by erasing n from S. First, the probability that the hook walk for n (in steps 1 and 2 of the algorithm) ends at c^* is $p(\lambda,c^*)$. Given that this has occurred, induction tells us that the probability of generating S' in step 3 is

$$\frac{\prod_{c\in\mathrm{dg}(\mu)}h_\mu(c)}{(n-1)!},$$

where $h_\mu(c)$ refers to the hook length of c relative to $\mathrm{dg}(\mu)$. Multiplying these probabilities, the probability of generating S is therefore

$$\frac{1}{n!}\prod_{c\in\mathrm{dg}(\mu)}h_\mu(c)\prod_{i=1}^{r-1}\frac{h_\lambda(i,s)}{h_\lambda(i,s)-1}\prod_{j=1}^{s-1}\frac{h_\lambda(r,j)}{h_\lambda(r,j)-1}.$$

Now, consider what happens to the hook lengths of cells when we pass from μ to λ by restoring the box $c^*=(r,s)$. For every cell $c=(i,j)\in\mathrm{dg}(\mu)$ with $i\neq r$ and $j\neq s$, we have $h_\mu(c) = h_\lambda(c)$. If $c = (i, s) \in \mathrm{dg}(\mu)$ with $i < r$, then $h_\mu(c) = h_\lambda(c) - 1 = h_\lambda(i, s) - 1$. Thus, the fractions in the second product convert $h_\mu(c)$ to $h_\lambda(c)$ for each such c. Similarly, if $c = (r, j) \in \mathrm{dg}(\mu)$ with $j < s$, then $h_\mu(c) = h_\lambda(c) - 1 = h_\lambda(r, j) - 1$. So the fractions in the third product convert $h_\mu(c)$ to $h_\lambda(c)$ for each such c. So we are left with

$$\frac{1}{n!} \prod_{c \in \mathrm{dg}(\mu)} h_\lambda(c) = \frac{\prod_{c \in \mathrm{dg}(\lambda)} h_\lambda(c)}{n!},$$

where the last equality follows since $h_\lambda(c^*) = 1$. This completes the induction. □

12.11 Knuth Equivalence

Let X be a totally ordered set, and let $X^* = \bigcup_{n \geq 0} X^n$ be the set of all words over the alphabet X. Given a word $w \in X^*$, we can use the RSK algorithm to construct the insertion tableau $P(w)$, which is a semistandard tableau using the same multiset of letters as w (§10.23). This section studies some of the relationships between w and $P(w)$. In particular, we show that the shape of $P(w)$ contains information about increasing and decreasing subsequences of w. First we show how to encode semistandard tableaux using words.

12.56. Definition: Reading Word of a Tableau. Let $T \in \mathrm{SSYT}_X(\lambda)$, with $\lambda = (\lambda_1, \ldots, \lambda_k)$. The *reading word of* T is

$$\begin{aligned} \mathrm{rw}(T) \;=\; & T(k,1), T(k,2), \ldots, T(k,\lambda_k), T(k-1,1), T(k-1,2), \ldots, T(k-1,\lambda_{k-1}), \ldots, \\ & T(1,1), T(1,2), \ldots, T(1,\lambda_1). \end{aligned}$$

Thus, $\mathrm{rw}(T)$ is the concatenation of the weakly increasing words appearing in each row of T, reading the rows from bottom to top. Note that $T(j, \lambda_j) \geq T(j, 1) > T(j-1, 1)$ for all $j > 1$. This implies that we can recover the shape of T from $\mathrm{rw}(T)$ by starting a new row whenever we see a strict descent in $\mathrm{rw}(T)$.

12.57. Example. Given the tableau

$$T = \begin{array}{ccccccc} 1 & 1 & 2 & 3 & 4 & 4 & 6 \\ 2 & 4 & 5 & 6 & 6 & & \\ 3 & 5 & 7 & 8 & & & \\ 4 & 6 & & & & & \end{array},$$

the reading word of T is

$$\mathrm{rw}(T) = 463578245661123446.$$

Given that the word $w = 7866453446223511224$ is the reading word of some tableau S, we deduce that S must be

$$S = \begin{array}{ccccc} 1 & 1 & 2 & 2 & 4 \\ 2 & 2 & 3 & 5 & \\ 3 & 4 & 4 & 6 & \\ 4 & 5 & & & \\ 6 & 6 & & & \\ 7 & 8 & & & \end{array}$$

by looking at the descents in w.

Next we introduce two equivalence relations on X^* that are related to the map $w \mapsto P(w)$.

12.58. Definition: P-Equivalence. Two words $v, w \in X^*$ are called *P-equivalent*, denoted $v \equiv_P w$, iff $P(v) = P(w)$.

12.59. Definition: Knuth Equivalence. The set of *elementary Knuth relations of the first kind on X* is

$$K_1 = \{(\mathbf{u}yxz\mathbf{v}, \mathbf{u}yzx\mathbf{v}) : \mathbf{u}, \mathbf{v} \in X^*, x, y, z \in X \text{ and } x < y \leq z\}.$$

The set of *elementary Knuth relations of the second kind on X* is

$$K_2 = \{(\mathbf{u}xzy\mathbf{v}, \mathbf{u}zxy\mathbf{v}) : \mathbf{u}, \mathbf{v} \in X^*, x, y, z \in X \text{ and } x \leq y < z\}.$$

Two words $v, w \in X^*$ are *Knuth equivalent*, denoted $v \equiv_K w$, iff there is a finite sequence of words $v = v^0, v^1, v^2, \ldots, v^k = w$ such that, for $1 \leq i \leq k$, either $(v^{i-1}, v^i) \in K_1 \cup K_2$ or $(v^i, v^{i-1}) \in K_1 \cup K_2$.

12.60. Remark. Informally, Knuth equivalence allows us to modify words by repeatedly changing subsequences of three consecutive letters according to certain rules. Specifically, if the middle *value* among the three letters does not occupy the middle *position*, then the other two values can switch positions. To determine which value is the "middle value" in the case of repeated letters, use the rule that the letter to the right is larger. These comments should aid the reader in remembering the inequalities in the definitions of K_1 and K_2.

It is routine to check that $\equiv_P$ and $\equiv_K$ are equivalence relations on X^*. Our current goal is to prove that these equivalence relations are actually the *same*. First we show that we can simulate each step in the tableau insertion algorithm 10.52 using the elementary Knuth relations.

12.61. Theorem: Reading Words and Knuth Equivalence. For all $v \in X^*$, $v \equiv_K \mathrm{rw}(P(v))$.

Proof. First note that, for any words $u, z, w, w' \in X^*$, if $w \equiv_K w'$ then $uwz \equiv_K uw'z$. Now, write $v = v_1 v_2 \cdots v_k$ and argue by induction on k. The theorem holds if $k \leq 1$, since $\mathrm{rw}(P(v)) = v$ in this case. For the induction step, assume $k > 1$ and write $T' = P(v_1 v_2 \cdots v_{k-1})$, $T = P(v)$. By the induction hypothesis, $v_1 \cdots v_{k-1} \equiv_K \mathrm{rw}(T')$, so $v = (v_1 \cdots v_{k-1})v_k \equiv_K \mathrm{rw}(T')v_k$. It will therefore suffice to prove that $\mathrm{rw}(T')v_k$ is Knuth equivalent to $\mathrm{rw}(T) = \mathrm{rw}(T' \leftarrow v_k)$. This will be proved by induction on ℓ, the number of rows in the tableau T'.

For the base case, let $\ell = 1$. Then $\mathrm{rw}(T')$ is a weakly increasing sequence $u_1 u_2 \cdots u_{k-1}$. If $u_{k-1} \leq v_k$, then T is obtained from T' by appending v_k at the end of the first row. In this situation, $\mathrm{rw}(T')v_k = u_1 \cdots u_{k-1} v_k = \mathrm{rw}(T)$, so the desired result holds. On the other hand, if $v_k < u_{k-1}$, let j be the least index with $v_k < u_j$. When inserting v_k into T', v_k will bump u_j into the second row, so that

$$\mathrm{rw}(T) = u_j u_1 u_2 \cdots u_{j-1} v_k u_{j+1} \cdots u_{k-1}.$$

Let us show that this word can be obtained from $u_1 \cdots u_{k-1} v_k$ by a sequence of elementary Knuth equivalences. If $j \leq k-2$, then $v_k < u_{k-2} \leq u_{k-1}$ implies

$$(u_1 \cdots u_{k-3} u_{k-2} v_k u_{k-1}, u_1 \cdots u_{k-3} u_{k-2} u_{k-1} v_k) \in K_1.$$

So $\mathrm{rw}(T')v_k$ is Knuth-equivalent to the word obtained by interchanging v_k with the letter u_{k-1} to its immediate left. Similarly, if $j \leq k-3$, the inequality $v_k < u_{k-3} \leq u_{k-2}$ lets us interchange v_k with u_{k-2}. We can continue in this way, using elementary Knuth relations of the first kind, to see that

$$\mathrm{rw}(T')v_k \equiv_K u_1 \cdots u_{j-1}u_jv_ku_{j+1}\cdots u_{k-1}.$$

Now, we have $u_{j-1} \leq v_k < u_j$, so an elementary Knuth relation of the second kind transforms this word into

$$u_1 \cdots u_{j-2}u_ju_{j-1}v_ku_{j+1}\cdots u_{k-1}.$$

If $j > 2$, we now have $u_{j-2} \leq u_{j-1} < u_j$, so we can interchange u_j with u_{j-2}. We can continue in this way until u_j reaches the left end of the word. We have now transformed $\mathrm{rw}(T')v_k$ into $\mathrm{rw}(T)$ by elementary Knuth equivalences, so $\mathrm{rw}(T')v_k \equiv_K \mathrm{rw}(T)$.

For the induction step, assume $\ell > 1$. Let T'' be the tableau T' with its first (longest) row erased. Then $\mathrm{rw}(T') = \mathrm{rw}(T'')u_1\cdots u_p$ where $u_1 \leq \cdots \leq u_p$ is the weakly increasing sequence in the first row of T'. If $u_p \leq v_k$, then $\mathrm{rw}(T')v_k = \mathrm{rw}(T)$. Otherwise, assume v_k bumps u_j in the insertion $T' \leftarrow v_k$. By the result in the last paragraph,

$$\mathrm{rw}(T')v_k \equiv_K \mathrm{rw}(T'')u_ju_1\cdots u_{j-1}v_ku_{j+1}\cdots u_p.$$

Now, by the induction hypothesis, $\mathrm{rw}(T'')u_j \equiv_K \mathrm{rw}(T'' \leftarrow u_j)$. Thus,

$$\mathrm{rw}(T')v_k \equiv_K \mathrm{rw}(T'' \leftarrow u_j)u'$$

where u' is $u_1\cdots u_p$ with u_j replaced by v_k. But, by definition of tableau insertion, $\mathrm{rw}(T'' \leftarrow u_j)u'$ is precisely $\mathrm{rw}(T)$. This completes the induction step. □

12.62. Example. Let us illustrate how elementary Knuth equivalences implement the steps in the insertion $T \leftarrow 3$, where

$$T = \begin{array}{|c|c|c|c|c|c|}\hline 1&1&3&4&4&6\\ \hline 2&2&4&5\\ \cline{1-4} 3&4\\ \cline{1-2}\end{array}$$

Appending a 3 at the right end of $\mathrm{rw}(T)$, we first compute

$$34\ 2245\ 113446\ 3 \equiv_K 34\ 2245\ 1134436 \equiv_K 34\ 2245\ 1134346 \equiv_K$$

$$34\ 2245\ 1143346 \equiv_K 34\ 2245\ 1413346 \equiv_K 34\ 2245\ 4\ 113346.$$

The steps so far correspond to the insertion of 3 into the first row of T, which bumps the leftmost 4 into the second row. Continuing,

$$34\ 22454\ 113346 \equiv_K 34\ 22544\ 113346 \equiv_K 34\ 25244\ 113346 \equiv_K 34\ 5\ 2244\ 113346,$$

and now the incoming 4 has bumped the 5 into the third row. The process stops here with the word

$$3452244113346 = \mathrm{rw}\left(\begin{array}{|c|c|c|c|c|c|}\hline 1&1&3&3&4&6\\ \hline 2&2&4&4\\ \cline{1-4} 3&4&5\\ \cline{1-3}\end{array}\right) = \mathrm{rw}(T \leftarrow 3).$$

This illustrates that $\mathrm{rw}(T)3 \equiv_K \mathrm{rw}(T \leftarrow 3)$.

12.63. Definition: Increasing and Decreasing Subsequences. Let $w = w_1w_2\cdots w_n \in X^*$. An *increasing subsequence of w of length ℓ* is a subset $I = \{i_1 < i_2 < \cdots < i_\ell\}$ of $\{1, 2, \ldots, n\}$ such that $w_{i_1} \leq w_{i_2} \leq \cdots \leq w_{i_\ell}$. A *decreasing subsequence of w of length ℓ* is a subset $I = \{i_1 < i_2 < \cdots < i_\ell\}$ such that $w_{i_1} > w_{i_2} > \cdots > w_{i_\ell}$. A *set of k disjoint increasing subsequences of w* is a set $\{I_1, \ldots, I_k\}$ of pairwise disjoint increasing subsequences of w. For each $k \geq 1$, let $\mathrm{inc}_k(w)$ be the maximum value of $|I_1| + \cdots + |I_k|$ over all such sets. Similarly, let $\mathrm{dec}_k(w)$ be the maximum total length of a set of k disjoint decreasing subsequences of w.

12.64. Theorem: Knuth Equivalence and Monotone Subsequences. For all $v, w \in X^*$ and all $k \geq 1$, $v \equiv_K w$ implies $\operatorname{inc}_k(v) = \operatorname{inc}_k(w)$ and $\operatorname{dec}_k(v) = \operatorname{dec}_k(w)$.

Proof. It suffices to consider the case where v and w differ by a single elementary Knuth relation. First suppose

$$v = \mathbf{a}yxz\mathbf{b}, \quad w = \mathbf{a}yzx\mathbf{b}, \quad (x < y \leq z)$$

where the y occurs at position i. If I is an increasing subsequence of w, then $i+1$ and $i+2$ do not both belong to I (since $z > x$). Therefore, if $\{I_1, \ldots, I_k\}$ is any set of k disjoint increasing subsequences of w, we can obtain a set $\{I_1', \ldots, I_k'\}$ of disjoint increasing subsequences of v by replacing $i+1$ by $i+2$ and $i+2$ by $i+1$ in any I_j in which one of these indices appears. This implies that $\operatorname{inc}_k(w) \leq \operatorname{inc}_k(v)$.

To establish the opposite inequality, let $\mathbf{I} = \{I_1, I_2, \ldots, I_k\}$ be any set of k disjoint increasing subsequences of v. We will construct a set of k disjoint increasing subsequences of w having the same total size as $\mathbf{I}$. The device used in the previous paragraph works here, unless some member of $\mathbf{I}$ (say I_1) contains both $i+1$ and $i+2$. In this case, we cannot have $i \in I_1$, since $y > x$. If no other member of $\mathbf{I}$ contains i, we replace I_1 by $(I_1 \sim \{i+2\}) \cup \{i\}$, which is an increasing subsequence of w. On the other hand, suppose $i+1, i+2 \in I_1$, and some other member of $\mathbf{I}$ (say I_2) contains i. Write

$$\begin{aligned} I_1 &= \{j_1 < j_2 < \cdots < j_r < i+1 < i+2 < j_{r+1} < \cdots < j_p\}, \\ I_2 &= \{k_1 < k_2 < \cdots < k_s < i < k_{s+1} < \cdots < k_q\}, \end{aligned}$$

and note that $v_{j_r} \leq x < z \leq v_{j_{r+1}}$ and $v_{k_s} \leq y \leq v_{k_{s+1}}$. Replace these two disjoint increasing subsequences of v by

$$\begin{aligned} I_1' &= \{j_1 < j_2 < \cdots < j_r < i+2 < k_{s+1} < \cdots < k_q\}, \\ I_2' &= \{k_1 < k_2 < \cdots < k_s < i < i+1 < j_{r+1} < \cdots < j_p\}. \end{aligned}$$

Since $w_{j_r} \leq x \leq w_{k_{s+1}}$ and $w_{k_s} \leq y \leq z \leq w_{j_{r+1}}$, I_1' and I_2' are two disjoint increasing subsequences of w having the same total length as I_1 and I_2. This completes the proof that $\operatorname{inc}_k(w) \geq \operatorname{inc}_k(v)$.

Similar reasoning (left as an exercise for the reader) proves the result in the case where

$$v = \mathbf{a}xzy\mathbf{b}, \quad w = \mathbf{a}zxy\mathbf{b}, \quad (x \leq y < z).$$

We also let the reader prove the statement about decreasing subsequences. □

12.65. Theorem: Subsequences and the Shape of Insertion Tableaux. Let $w \in X^*$ and suppose $P(w)$ has shape λ. For all $k \geq 1$,

$$\operatorname{inc}_k(w) = \lambda_1 + \cdots + \lambda_k, \qquad \operatorname{dec}_k(w) = \lambda_1' + \cdots + \lambda_k'.$$

In particular, λ_1 is the length of the longest increasing subsequence of w, whereas $\ell(\lambda)$ is the length of the longest decreasing subsequence of w.

Proof. Let $w' = \operatorname{rw}(P(w))$. We know $w \equiv_K w'$ by 12.61, so $\operatorname{inc}_k(w) = \operatorname{inc}_k(w')$ and $\operatorname{dec}_k(w) = \operatorname{dec}_k(w')$ by 12.64. So we need only prove

$$\operatorname{inc}_k(w') = \lambda_1 + \cdots + \lambda_k, \qquad \operatorname{dec}_k(w') = \lambda_1' + \cdots + \lambda_k'.$$

Now, w' consists of increasing sequences of letters of successive lengths $\lambda_l, \ldots, \lambda_2, \lambda_1$ (where $l = \ell(\lambda)$). By taking $I_1, I_2, \ldots, I_k$ to be the set of positions of the last k of these sequences, we obtain k disjoint increasing subsequences of w' of length $\lambda_1+\cdots+\lambda_k$. Therefore, $\mathrm{inc}_k(w') \geq \lambda_1+\cdots+\lambda_k$.

On the other hand, let $\{I_1,\ldots,I_k\}$ be any k disjoint increasing subsequences of w'. Each position i in w' is associated to a particular box in the diagram of λ, via 12.56. For example, position 1 corresponds to the first box in the last row, while the last position corresponds to the last box in the first row. For each position i that belongs to some I_j, place an X in the corresponding box in the diagram of λ. Since entries in a given column of $P(w)$ strictly decrease reading from bottom to top, the X's coming from a given increasing subsequence I_j must all lie in different columns of the diagram. It follows that every column of the diagram contains k or fewer X's. Suppose we push all these X's up their columns as far as possible. Then all the X's in the resulting figure must lie in the top k rows of λ. It follows that the number of X's, which is $|I_1|+\cdots+|I_k|$, cannot exceed $\lambda_1+\cdots+\lambda_k$. This gives $\mathrm{inc}_k(w') \leq \lambda_1+\cdots+\lambda_k$. The proof for $\mathrm{dec}_k(w)$ is similar, and is left as an exercise. □

12.66. Theorem: Knuth Equivalence vs. Tableau Shape. For all $v,w\in X^*$, $v\equiv_K w$ implies that $P(v)$ and $P(w)$ have the same shape.

Proof. Let λ and μ be the shapes of $P(v)$ and $P(w)$, respectively. Using 12.64 and 12.65, we see that $v\equiv_K w$ implies

$$\lambda_k=\mathrm{inc}_k(v)-\mathrm{inc}_{k-1}(v)=\mathrm{inc}_k(w)-\mathrm{inc}_{k-1}(w)=\mu_k \quad (k\geq 1). \qquad \square$$

12.67. Example. Consider the word $w=35164872$. As shown in Figure 10.1, we have

$$P(w)=\begin{array}{|c|c|c|c|}\hline 1&2&6&7\\ \hline 3&4&8\\ \cline{1-3} 5\\ \cline{1-1}\end{array}$$

Since the shape is $\lambda=(4,3,1)$, the longest increasing subsequence of w has length 4. Two such subsequences are $I_1=\{1,2,4,7\}$ (corresponding to the subword 3567) and $I_2=\{1,2,4,6\}$. Note that the first row of $P(w)$, namely 1267, does *not* appear as a subword of w. Since the column lengths of λ are $(3,2,2,1)$, the longest length of two disjoint decreasing subsequences of w is $3+2=5$. For example, we could take $I_1=\{6,7,8\}$ and $I_2=\{4,5\}$ to achieve this. Note that $w'=\mathrm{rw}(P(w))=5\ 348\ 1267$. To illustrate the end of the previous proof, consider the two disjoint increasing subsequences $I_1=\{1,4\}$ and $I_2=\{2,3,7,8\}$ of w' (this pair does not achieve the maximum length for such subsequences). Drawing X's in the boxes of the diagram associated to the positions in I_1 (resp. I_2) produces

$$\begin{array}{|c|c|c|c|}\hline &&&\\ \hline &&X\\ \cline{1-3} X\\ \cline{1-1}\end{array} \qquad \left(\text{resp. } \begin{array}{|c|c|c|c|}\hline &&X&X\\ \hline X&X&\\ \cline{1-3} \\ \cline{1-1}\end{array}\right).$$

Combining these diagrams and pushing the X's up as far as they will go, we get

$$\begin{array}{|c|c|c|c|}\hline X&X&X&X\\ \hline X&&X\\ \cline{1-3} \\ \cline{1-1}\end{array}$$

So, indeed, the combined length of I_1 and I_2 does not exceed $\lambda_1+\lambda_2$.

The next lemma provides the remaining ingredients needed to establish that P-equivalence and Knuth equivalence are the same.

12.68. Lemma. Suppose $v,w\in X^*$ and z is the largest letter appearing in both v and w. Let v' (resp. w') be the word obtained by erasing the rightmost z from v (resp. w). If $v\equiv_K w$, then $v'\equiv_K w'$. Furthermore, if $T=P(v)$ and $T'=P(v')$, then T' can be obtained from T by erasing the rightmost box containing z.

Proof. Write $v = azb$ and $w = czd$ where $a, b, c, d \in X^*$ and z does not appear in b or d. First assume that v and w differ by a single elementary Knuth relation. If the triple of letters affected by this relation are part of the subword a, then $a \equiv_K c$ and $b = d$, so $v' = ab \equiv_K cd = w'$. Similarly, the result holds if the triple of letters is part of the subword b. The next possibility is that

$$v = a'yxzb, \quad w = a'yzxb \qquad (x < y \leq z)$$

(or vice versa). Then $v' = a'yxb = w'$, so certainly $v' \equiv_K w'$. Another possibility is that

$$v = a'xzyb', \quad w = a'zxyb' \qquad (x \leq y < z)$$

(or vice versa), and again $v' = a'xyb' = w'$. Since the z under consideration is the rightmost occurrence of the largest letter in both v and w, the possibilities already considered are the only elementary Knuth relations that involve this symbol. So the result holds when v and w differ by one elementary Knuth relation. Now, if $v = v^0, v^1, v^2, \ldots, v^k = w$ is a sequence of words as in 12.59, we can write each $v^i = a^i z b^i$ where z does not appear in b^i. Letting $(v^i)' = a^i b^i$ for each i, the chain $v' = (v^0)', (v^1)', \ldots, (v^k)' = w'$ proves that $v' \equiv_K w'$.

Now consider the actions of the tableau insertion algorithm applied to $v = azb$ and to $v' = ab$. We prove the statement about T and T' by induction on the length of b. The statement holds if b is empty. Assume b has length $k > 0$ and the statement is known for smaller values of k. Write $b = b'x$ where $x \in X$. Then $T_1' = P(ab')$ is the tableau $T_1 = P(azb')$ with the rightmost z erased. By definition, $T' = T_1' \leftarrow x$ and $T = T_1 \leftarrow x$. When we insert the x into these two tableaux, the bumping paths will be the same (and hence the desired result holds), unless x bumps the rightmost z in T_1. If this happens, the rightmost z (which must have been the only z in its row) will get bumped into the next lower row. It will come to rest there without bumping anything else, and it will still be the rightmost z in the tableau. Thus it is still true that erasing this z in T produces T'. The induction is therefore complete. □

12.69. Theorem: P-Equivalence vs. Knuth Equivalence. For all $v, w \in X^*$, $v \equiv_P w$ iff $v \equiv_K w$.

Proof. First, if $v \equiv_P w$, then 12.61 shows that $v \equiv_K \mathrm{rw}(P(v)) = \mathrm{rw}(P(w)) \equiv_K w$, so $v \equiv_K w$ by transitivity of $\equiv_K$. Conversely, assume $v \equiv_K w$. We prove $v \equiv_P w$ by induction on the length k of v. For $k \leq 1$, we have $v = w$ and so $v \equiv_K w$. Now assume $k > 1$ and the result is known for words of length $k - 1$. Write $v = azb$ and $w = czd$ where z is the largest symbol in v and w and z does not occur in b or d. Write $v' = ab$ and $w' = cd$. By 12.68, $v' \equiv_K w'$, $P(v')$ is $P(v)$ with the rightmost z erased, and $P(w')$ is $P(w)$ with the rightmost z erased. By induction, $P(v') = P(w')$. If we knew that $P(v)$ and $P(w)$ had the same shape, it would follow that $P(v) = P(w)$. But $P(v)$ and $P(w)$ do have the same shape, thanks to 12.66. So $v \equiv_P w$. □

We conclude with an application of 12.65.

12.70. Erdös-Szekeres Subsequence Theorem. Every word of length exceeding mn either has an increasing subsequence of length $m + 1$ or a decreasing subsequence of length $n + 1$.

Proof. Suppose w is a word with no increasing subsequence of length $m+1$ and no decreasing subsequence of length $n+1$. Let λ be the shape of $P(w)$. Then 12.65 implies that $\lambda_1 \leq m$ and $\ell(\lambda) \leq n$. Therefore the length of w, which is $|\lambda|$, can be no greater than $\lambda_1 \ell(\lambda) \leq mn$. □

12.12 Pfaffians and Perfect Matchings

Given a *square* matrix A with N rows and N columns, we have defined the *determinant* of A by the formula

$$\det(A) = \sum_{w \in S_N} \operatorname{sgn}(w) \prod_{i=1}^{N} A(i, w(i)).$$

This section studies *Pfaffians*, which are numbers associated to a *triangular* array of numbers $(a_{i,j} : 1 \leq i < j \leq N)$ where N is even. Pfaffians arise in the theory of skew-symmetric matrices.

12.71. Definition: Skew-Symmetric Matrices. An $N \times N$ matrix A is called *skew-symmetric* iff $A^t = -A$ iff $A(i,j) = -A(j,i)$ for $1 \leq i, j \leq N$.

If A is a real or complex skew-symmetric matrix, then $A(i,i) = 0$ for all i. Moreover, A is completely determined by the triangular array of numbers $(A(i,j) : 1 \leq i < j \leq N)$ lying strictly above the main diagonal. The starting point for the theory of Pfaffians is the observation that, for N even and A skew-symmetric, $\det(A)$ is always a perfect square. (For N odd, the condition $A^t = -A$ can be used to show that $\det(A) = 0$.)

12.72. Example. A general skew-symmetric 2×2 matrix has the form $A = \begin{bmatrix} 0 & a \\ -a & 0 \end{bmatrix}$. In this case, $\det(A) = a^2$ is a square. A skew-symmetric 4×4 matrix looks like

$$A = \begin{bmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{bmatrix}.$$

A somewhat tedious calculation reveals that

$$\begin{aligned} \det(A) &= a^2f^2 + b^2e^2 + c^2d^2 - 2abef + 2acdf - 2bcde \\ &= (af + cd - be)^2. \end{aligned}$$

The remainder of this section develops the theory needed to explain the phenomenon observed in the last example.

12.73. Definition: Pfaffians. Suppose N is even and A is a skew-symmetric $N \times N$ matrix. Let SPf_N be the set of all permutations $w \in S_N$ such that

$$w_1 < w_3 < w_5 < \cdots < w_{N-1}, \quad w_1 < w_2,\ w_3 < w_4,\ w_5 < w_6,\ \ldots,\ w_{N-1} < w_N.$$

The *Pfaffian* of A, denoted $\mathrm{Pf}(A)$, is the number

$$\mathrm{Pf}(A) = \sum_{w \in \mathrm{SPf}_N} \operatorname{sgn}(w) A(w_1, w_2) A(w_3, w_4) A(w_5, w_6) \cdots A(w_{N-1}, w_N).$$

12.74. Example. If $N = 2$, $\mathrm{SPf}_2 = \{12\}$ and $\mathrm{Pf}(A) = A(1,2)$ (we write permutations in one-line form here). If $N = 4$, $\mathrm{SPf}_4 = \{1234, 1423, 1324\}$ and

$$\mathrm{Pf}(A) = A(1,2)A(3,4) + A(1,4)A(2,3) - A(1,3)A(2,4).$$

For a general $N \times N$ matrix A, $\det(A)$ is a sum of $|S_N| = N!$ terms. Similarly, for a skew-symmetric matrix A, $\mathrm{Pf}(A)$ is a sum of $|\,\mathrm{SPf}_N\,|$ terms.

12.75. Theorem: Size of SPf_N. For each even N, $|\,\mathrm{SPf}_N\,| = 1 \times 3 \times 5 \times \cdots \times (N-1)$.

Proof. We can construct each permutation $w \in \mathrm{SPf}_N$ as follows. First, w_1 must be 1. There are $N-1$ choices for w_2, which can be anything other than 1. To finish building w, choose an arbitrary permutation $v = v_1 v_2 \cdots v_{N-2} \in \mathrm{SPf}_{N-2}$. For $1 \le i \le N-2$, set

$$w_{i+2} = \begin{cases} v_i + 1 & \text{if } v_i < w_2 - 1 \\ v_i + 2 & \text{otherwise.} \end{cases}$$

Informally, we are renumbering the v's to use symbols in $\{1,2,\ldots,N\} \sim \{w_1 = 1, w_2\}$ and then appending this word to $w_1 w_2$. By the product rule, $|\,\mathrm{SPf}_N\,| = (N-1) \times |\,\mathrm{SPf}_{N-2}\,|$. Since $|\,\mathrm{SPf}_2\,| = 1$, the formula in the theorem follows by induction. □

Recall that the Laplace expansions in 9.48 provide recursive formulas for evaluating determinants. Similar recursive formulas exist for evaluating Pfaffians. The key difference is that *two* rows and columns get erased at each stage, whereas in Laplace expansions only one row and column get erased at a time.

12.76. Theorem: Pfaffian Expansion along Row 1. Suppose N is even and A is an $N \times N$ skew-symmetric matrix. For each $i < j$, let $A[[i,j]]$ be the matrix obtained from A by deleting row i and row j and column i and column j; this is a skew-symmetric matrix of size $(N-2) \times (N-2)$. We have

$$\mathrm{Pf}(A) = \sum_{j=2}^{N} (-1)^j A(1,j)\,\mathrm{Pf}(A[[1,j]]).$$

Proof. By definition,

$$\mathrm{Pf}(A) = \sum_{w \in \mathrm{SPf}_N} \mathrm{sgn}(w) \prod_{\substack{i=1 \\ i \text{ odd}}}^{N} A(w_i, w_{i+1}).$$

By the proof of 12.75, there is a bijection $\mathrm{SPf}_N \to \{2,3,\ldots,N\} \times \mathrm{SPf}_{N-2}$ that maps $w \in \mathrm{SPf}_N$ to (j,v), where $j = w_2$ and v is obtained from $w_3 w_4 \cdots w_N$ by renumbering the symbols to be $1,2,\ldots,N-2$. We will use this bijection to change the indexing set for the summation from SPf_N to $\{2,\ldots,N\} \times \mathrm{SPf}_{N-2}$. Counting inversions, we see that $\mathrm{inv}(w) = \mathrm{inv}(v) + j - 2$ since $w_2 = j$ exceeds $j-2$ symbols to its right. So $\mathrm{sgn}(w) = (-1)^j \mathrm{sgn}(v)$. Next, $A(w_1, w_2) = A(1,j)$. For odd $i > 1$, it follows from the definitions that $A(w_i, w_{i+1}) = A[[1,j]](v_{i-2}, v_{i-1})$. Putting all this information into the formula, we see that

$$\mathrm{Pf}(A) = \sum_{j=2}^{N} (-1)^j A(1,j) \sum_{v \in \mathrm{SPf}_{N-2}} \mathrm{sgn}(v) \prod_{\substack{i=1 \\ i \text{ odd}}}^{N-2} A[[1,j]](v_i, v_{i+1}).$$

The inner sum is precisely $\mathrm{Pf}(A[[1,j]])$, so the proof is complete. □

12.77. Example. Let us compute the Pfaffian of the matrix

$$A = \begin{bmatrix} 0 & x & -y & 0 & 0 & 0 \\ -x & 0 & 0 & y & 0 & 0 \\ y & 0 & 0 & x & -y & 0 \\ 0 & -y & -x & 0 & 0 & y \\ 0 & 0 & y & 0 & 0 & x \\ 0 & 0 & 0 & -y & -x & 0 \end{bmatrix}.$$

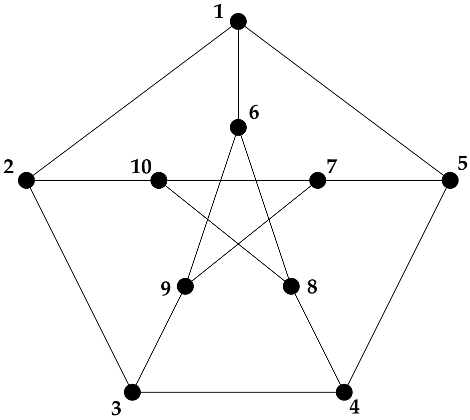


FIGURE 12.14
Graph used to illustrate perfect matchings.

Expanding along row 1 gives

$$\mathrm{Pf}(A) = x\,\mathrm{Pf}\begin{bmatrix} 0 & x & -y & 0 \\ -x & 0 & 0 & y \\ y & 0 & 0 & x \\ 0 & -y & -x & 0 \end{bmatrix} - (-y)\,\mathrm{Pf}\begin{bmatrix} 0 & y & 0 & 0 \\ -y & 0 & 0 & y \\ 0 & 0 & 0 & x \\ 0 & -y & -x & 0 \end{bmatrix}.$$

By expanding these 4 × 4 Pfaffians in the same way, or by using the formula in 12.74, we obtain

$$\mathrm{Pf}(A) = x(x^2 + y^2) + y(xy) = x^3 + 2xy^2.$$

The combinatorial significance of this Pfaffian evaluation will be revealed in §12.13.

Pfaffians are closely related to perfect matchings of graphs, which we now discuss.

12.78. Definition: Perfect Matchings. Let G be a simple graph with vertex set V and edge set E. A *perfect matching of* G is a subset M of E such that each $v \in V$ is the endpoint of exactly one edge in M. Let $\mathrm{PM}(G)$ be the set of perfect matchings of G.

12.79. Example. For the graph shown in Figure 12.14, one perfect matching is

$$M_1 = \{\{1,6\},\{2,10\},\{3,9\},\{4,8\},\{5,7\}\}.$$

Another perfect matching is

$$M_2 = \{\{1,2\},\{3,4\},\{5,7\},\{6,9\},\{8,10\}\}.$$

A perfect matching on a graph G is a set partition of the vertex set of G into blocks of size 2 where each such block is an edge of G. Therefore, if G has N vertices and a perfect matching exists for G, then N must be even. The next result shows that perfect matchings on a *complete* graph can be encoded by permutations in SPf_N.

12.80. Theorem: Perfect Matchings on a Complete Graph. Suppose N is even and K_N is the simple graph with vertex set $\{1, 2, \ldots, N\}$ and edge set $\{\{i, j\} : 1 \leq i < j \leq N\}$. The map $f : \mathrm{SPf}_N \to \mathrm{PM}(K_N)$ defined by

$$f(w_1 w_2 \cdots w_N) = \{\{w_1, w_2\}, \{w_3, w_4\}, \ldots, \{w_{N-1}, w_N\}\}$$

is a bijection. Consequently,

$$|\operatorname{PM}(K_N)| = 1 \times 3 \times 5 \times \cdots \times (N-1).$$

Proof. Note first that f does map into the set $\operatorname{PM}(K_N)$. Next, a matching $M \in \operatorname{PM}(K_N)$ is a set of $N/2$ edges $M = \{\{i_1, i_2\}, \{i_3, i_4\}, \ldots, \{i_{N-1}, i_N\}\}$. Since $\{i, j\} = \{j, i\}$, we can choose the notation so that $i_1 < i_2$, $i_3 < i_4$, …, and $i_{N-1} < i_N$. Similarly, since the $N/2$ edges of M can be presented in any order, we can change notation again (if needed) to arrange that $i_1 < i_3 < i_5 < \cdots < i_{N-1}$. Then the permutation $w = i_1 i_2 i_3 \cdots i_N \in \operatorname{SPf}_N$ satisfies $f(w) = M$. Thus f maps *onto* $\operatorname{PM}(K_N)$. To see that f is one-to-one, suppose $v = j_1 j_2 j_3 \cdots j_N$ is another element of SPf_N such that $f(v) = M = f(w)$. We must have $j_1 = 1 = i_1$. Since M has only one edge incident to vertex 1, and since $\{i_1, i_2\} \in M$ and $\{j_1, j_2\} \in M$ by definition of f, we conclude that $i_2 = j_2$. Now i_3 and j_3 must both be the smallest vertex in the set $\{1, 2, \ldots, N\} \sim \{i_1, i_2\}$, so $i_3 = j_3$. Then $i_4 = j_4$ follows, as above, since M is a perfect matching. Continuing similarly, we see that $i_k = j_k$ for all k, so $v = w$ and f is one-to-one. Since f is a bijection, the formula for $|\operatorname{PM}(K_N)|$ follows from 12.75. □

The preceding theorem leads to the following combinatorial interpretation for Pfaffians. Given a perfect matching $M \in \operatorname{PM}(K_N)$, use 12.80 to write $M = f(w)$ for some $w \in \operatorname{SPf}_N$. Define the *sign* of M to be $\operatorname{sgn}(w)$, and define the *weight* of M to be

$$\operatorname{wt}(M) = \prod_{\{i,j\} \in M} x_{i,j} = \prod_{\substack{i=1 \\ i \text{ odd}}}^{N} x_{w_i, w_{i+1}},$$

where the $x_{i,j}$ (for $1 \leq i < j \leq N$) are indeterminates. Let X be the skew-symmetric matrix with entries $x_{i,j}$ above the main diagonal. It follows from 12.80 and the definition of a Pfaffian that

$$\sum_{M \in \operatorname{PM}(K_N)} \operatorname{sgn}(M) \operatorname{wt}(M) = \operatorname{Pf}(X).$$

More generally, we have the following result.

12.81. Theorem: Pfaffians and Perfect Matchings. Let N be even, and let G be a simple graph with vertex set $V = \{1, 2, \ldots, N\}$ and edge set $E(G)$. Let $X = X(G)$ be the skew-symmetric matrix with entries

$$X(i,j) = \begin{cases} x_{i,j} & \text{if } i < j \text{ and } \{i,j\} \in E(G) \\ -x_{i,j} & \text{if } i > j \text{ and } \{i,j\} \in E(G) \\ 0 & \text{otherwise.} \end{cases}$$

Then $\sum_{M \in \operatorname{PM}(G)} \operatorname{sgn}(M) \operatorname{wt}(M) = \operatorname{Pf}(X(G))$.

Proof. We have already observed that

$$\sum_{M \in \operatorname{PM}(K_N)} \operatorname{sgn}(M) \operatorname{wt}(M) = \operatorname{Pf}(X(K_N)). \tag{12.11}$$

Given the graph G, let ϵ be the evaluation homomorphism (see 7.102) that sends $x_{i,j}$ to $x_{i,j}$ if $\{i, j\} \in E(G)$, and sends $x_{i,j}$ to 0 if $\{i, j\} \notin E(G)$. Applying ϵ to the left side of (12.11) produces

$$\sum_{M \in \operatorname{PM}(G)} \operatorname{sgn}(M) \operatorname{wt}(M),$$

since all matchings of K_N that use an edge not in $E(G)$ are mapped to zero. On the other hand, since ϵ is a ring homomorphism and the Pfaffian of a matrix is a polynomial in the entries of the matrix, we can compute $\epsilon(\mathrm{Pf}(X(K_N)))$ by applying ϵ to each entry of $X(K_N)$ and taking the Pfaffian of the resulting matrix. So, applying ϵ to the right side of (12.11) gives

$$\epsilon(\mathrm{Pf}(X(K_N))) = \mathrm{Pf}(\epsilon(X(K_N))) = \mathrm{Pf}(X(G)). \qquad \square$$

12.82. Remark. The last result shows that $\mathrm{Pf}(X(G))$ is a *signed* sum of distinct monomials, where there is one monomial for each perfect matching of G. Because of the signs, one cannot compute $|\mathrm{PM}(G)|$ by setting $x_{i,j} = 1$ for each $\{i,j\} \in E(G)$. However, for certain graphs G, one can introduce extra signs into the upper part of the matrix $X(G)$ to counteract the sign arising from $\mathrm{sgn}(M)$. This process is illustrated in the next section.

We can now give a combinatorial proof of the main result linking Pfaffians and determinants.

12.83. Theorem: Pfaffians vs. Determinants. For every even N and every $N \times N$ skew-symmetric matrix A, $\det(A) = \mathrm{Pf}(A)^2$.

Proof. First we use the skew-symmetry of A to cancel some terms in the sum

$$\det(A) = \sum_{w \in S_N} \mathrm{sgn}(w) \prod_{i=1}^{N} A(i, w(i)).$$

We will cancel every term indexed by a permutation w whose functional digraph contains at least one cycle of odd length (cf. §3.6). If w has a cycle of length 1, then $w(i) = i$ for some i. So $A(i, w(i)) = A(i,i) = 0$ by skew-symmetry, and the term indexed by this w is zero. On the other hand, suppose w has no fixed points, but w does have at least one cycle of odd length. Among all the odd-length cycles of w, choose the cycle $(i_1, i_2, \ldots, i_k)$ whose minimum element is as small as possible. Reverse the orientation of this cycle to get a permutation $w' \neq w$. For example, if $w = (3,8,4)(2,5,7)(1,6)(9,10)$, then $w' = (3,8,4)(7,5,2)(1,6)(9,10)$. In general, $\mathrm{sgn}(w') = \mathrm{sgn}(w)$ since w and w' have the same cycle structure (see 9.34). However, since k is odd and A is skew-symmetric,

$$A(i_1,i_2)A(i_2,i_3)\cdots A(i_{k-1},i_k)A(i_k,i_1) = -A(i_2,i_1)A(i_3,i_2)\cdots A(i_k,i_{k-1})A(i_1,i_k).$$

It follows that the term in $\det(A)$ indexed by w' is the negative of the term in $\det(A)$ indexed by w, so this pair of terms cancels. Since $w \mapsto w'$ is an involution, we conclude that

$$\det(A) = \sum_{w \in S_N^{ev}} \mathrm{sgn}(w) \prod_{i=1}^{N} A(i, w(i)),$$

where S_N^{ev} denotes the set of permutations of N objects with only even-length cycles.

The next step is to compare the terms in this sum to the terms in $\mathrm{Pf}(A)^2$. Using the distributive law to square the defining formula for $\mathrm{Pf}(A)$, we see that

$$\mathrm{Pf}(A)^2 = \sum_{u \in \mathrm{SPf}_N} \sum_{v \in \mathrm{SPf}_N} \mathrm{sgn}(u)\,\mathrm{sgn}(v) \prod_{i \text{ odd}} [A(u_i, u_{i+1})A(v_i, v_{i+1})].$$

Given $w \in S_N^{ev}$ indexing an uncanceled term in $\det(A)$, we associate a pair $(u,v) \in \mathrm{SPf}_N^2$ indexing a summand in $\mathrm{Pf}(A)^2$ as follows. Consider the functional digraph $G(w)$ with vertex set $\{1,2,\ldots,N\}$ and edge set $\{(i,w(i)) : 1 \leq i \leq N\}$, which is a disjoint union of cycles. Define a perfect matching M_1 on $G(w)$ (viewed as an undirected graph) by starting at the minimum element in each cycle and including every other edge as one travels around the cycle. Define another perfect matching M_2 on $G(w)$ by taking all the edges not used in M_1. Finally, let u and v be the permutations in SPf_N that encode M_1 and M_2 via the bijection in 12.80. For example, if $w = (1,5,2,8,6,3)(4,7)$, then $M_1 = \{\{1,5\},\{2,8\},\{6,3\},\{4,7\}\}$ and $M_2 = \{\{5,2\},\{8,6\},\{3,1\},\{7,4\}\}$, so $u = 15283647$ and $v = 13254768$. The association $w \mapsto (u,v)$ is a bijection from S_N^{ev} to SPf_N^2. To compute the inverse map, one need only take the union of the perfect matchings encoded by u and v. This produces a graph that is a disjoint union of cycles of even length, as is readily checked. One can restore the directions on each cycle by recalling that the outgoing edge from the minimum element in each cycle belongs to the matching encoded by u. For example, the pair $(u',v') = (15234867, 12374856)$ maps to $w' = (1,5,6,7,3,2)(4,8)$ under the inverse bijection.

Throughout the following discussion, assume $w \in S_N^{ev}$ corresponds to $(u,v) \in \mathrm{SPf}_N^2$. To complete the proof, it suffices to show that the term in $\det(A)$ indexed by w equals the term in $\mathrm{Pf}(A)^2$ indexed by (u,v). Write w in cycle form as

$$w = (m_1, n_1, \ldots, z_1)(m_2, n_2, \ldots, z_2) \cdots (m_k, n_k, \ldots, z_k)$$

where $m_1 < m_2 < \cdots < m_k$ are the minimum elements in their cycles. Define two words (permutations in one-line form)

$$\begin{aligned} u^* &= m_1 n_1 \cdots z_1 \; m_2 n_2 \cdots z_2 \; \cdots \; m_k n_k \cdots z_k; \\ v^* &= n_1 \cdots z_1 m_1 \; n_2 \cdots z_2 m_2 \; \cdots \; n_k \cdots z_k m_k. \end{aligned}$$

Thus u^* is obtained by erasing the parentheses in the particular cycle notation for w just mentioned, and v^* is obtained similarly after first cycling the values in each cycle one step to the left. Since each m_i is the smallest value in its cycle, it follows that

$$\mathrm{inv}(v^*) = N - k + \mathrm{inv}(u^*) \qquad (k = \mathrm{cyc}(w)).$$

Therefore $\mathrm{sgn}(u^*)\,\mathrm{sgn}(v^*) = (-1)^{N-\mathrm{cyc}(w)} = \mathrm{sgn}(w)$. Since all the edges $(i, w(i))$ in $G(w)$ arise by pairing off consecutive letters in u^* and v^*, we have

$$\mathrm{sgn}(w) \prod_{i=1}^{N} A(i, w(i)) = \mathrm{sgn}(u^*)\,\mathrm{sgn}(v^*) \prod_{i \text{ odd}} [A(u_i^*, u_{i+1}^*) A(v_i^*, v_{i+1}^*)].$$

We now transform the right side to the term indexed by (u,v) in $\mathrm{Pf}(A)^2$, as follows. Note that the words u^* and v^* provide *non-standard* encodings of the perfect matchings M_1 and M_2 encoded by u and v (the edges of the matchings are found by grouping pairs of consecutive symbols in u^* and v^*). To get to the standard encodings, first reverse each pair of consecutive letters u_i^*, u_{i+1}^* in u^* such that $u_i^* > u_{i+1}^*$ and i is odd. Each such reversal causes $\mathrm{sgn}(u^*)$ to change, but this change is balanced by the fact that $A(u_{i+1}^*, u_i^*) = -A(u_i^*, u_{i+1}^*)$. Similarly, we can reverse pairs of consecutive letters in v^* that are out of order. The next step is to sort the pairs in u^* to force $u_1 < u_3 < u_5 < \cdots < u_{N-1}$. This sorting can be achieved by repeatedly swapping adjacent pairs $a < b; c < d$ in the word, where $a > c$. The swap $abcd \mapsto cdab$ can be achieved by applying the two transpositions (a,c) and (b,d) on the left. So this modification of u^* does not change $\mathrm{sgn}(u^*)$, nor does it affect the product of the factors $A(u_i^*, u_{i+1}^*)$ (since multiplication is commutative). Similarly, we can sort the pairs in v^* to obtain v without changing the formula. We conclude finally that

$$\begin{aligned} \mathrm{sgn}(w) \prod_{i=1}^{N} A(i, w(i)) &= \mathrm{sgn}(u^*)\,\mathrm{sgn}(v^*) \prod_{i \text{ odd}} [A(u_i^*, u_{i+1}^*) A(v_i^*, v_{i+1}^*)] \\ &= \mathrm{sgn}(u)\,\mathrm{sgn}(v) \prod_{i \text{ odd}} [A(u_i, u_{i+1}) A(v_i, v_{i+1})]. \quad \square \end{aligned}$$

The following example illustrates the calculations at the end of the preceding proof.

12.84. Example. Suppose $w = (3, 8)(11, 4, 2, 9)(1, 10, 6, 7, 5, 12) \in S_{12}^{ev}$, so $k = \mathrm{cyc}(w) = 3$. We begin by writing the standard cycle notation for w:

$$w = (1, 10, 6, 7, 5, 12)(2, 9, 11, 4)(3, 8).$$

Next we set

$$u^* = 1, 10; 6, 7; 5, 12; 2, 9; 11, 4; 3, 8; \qquad v^* = 10, 6; 7, 5; 12, 1; 9, 11; 4, 2; 8, 3.$$

Observe that $\mathrm{inv}(v^*) = \mathrm{inv}(u^*) + (12 - 3)$ due to the cyclic shifting of $1, 2, 3$, so that $\mathrm{sgn}(u^*)\,\mathrm{sgn}(v^*) = (-1)^{12-3} = \mathrm{sgn}(w)$. Now we modify u^* and v^* so that the elements in each pair increase:

$$u' = 1, 10; 6, 7; 5, 12; 2, 9; 4, 11; 3, 8; \qquad v' = 6, 10; 5, 7; 1, 12; 9, 11; 2, 4; 3, 8.$$

Note that $\mathrm{sgn}(u') = -\,\mathrm{sgn}(u^*)$ since we switched 11 and 4, but this is offset by the fact that $A(11, 4) = -A(4, 11)$. So $\mathrm{sgn}(u^*) \prod_i A(u_i^*, u_{i+1}^*) = \mathrm{sgn}(u') \prod_i A(u_i', u_{i+1}')$, and similarly for v^* and v'. Finally, we sort the pairs so that the minimum elements increase, obtaining

$$u = 1, 10; 2, 9; 3, 8; 4, 11; 5, 12; 6, 7; \qquad v = 1, 12; 2, 4; 3, 8; 5, 7; 6, 10; 9, 11.$$

This sorting does not introduce any further sign changes, so we have successfully transformed the term indexed by w in $\det(A)$ to the term indexed by (u, v) in $\mathrm{Pf}(A)^2$.

12.13 Domino Tilings of Rectangles

This section presents P. W. Kasteleyn's proof of a formula for the number of ways to tile a rectangle with dominos. Let $\mathrm{Dom}(m, n)$ be the set of domino tilings of a rectangle of width m and height n. This set is empty if m and n are both odd, so we will assume throughout that m is even. Given a tiling $T \in \mathrm{Dom}(m, n)$, let $N_h(T)$ and $N_v(T)$ be the number of horizontal and vertical dominos (respectively) appearing in T. Define the *weight* of the tiling T to be $\mathrm{wt}(T) = x^{N_h(T)} y^{N_v(T)}$.

12.85. Theorem: Domino Tiling Formula. For all even $m \geq 1$ and all $n \geq 1$,

$$\sum_{T \in \mathrm{Dom}(m,n)} \mathrm{wt}(T) = 2^{mn/2} \prod_{j=1}^{m/2} \prod_{k=1}^{n} \sqrt{x^2 \cos^2\left(\frac{j\pi}{m+1}\right) + y^2 \cos^2\left(\frac{k\pi}{n+1}\right)}. \qquad (12.12)$$

By setting $x = y = 1$, we obtain the expression for $|\mathrm{Dom}(m, n)|$ stated in the Introduction.

Step 1: Conversion to a Perfect Matching Problem. Introduce a simple graph $G(m, n)$ with vertex set $V = \{1, 2, \ldots, mn\}$ and edge set $E = E_x \cup E_y$, where

$$E_x = \{\{k, k + 1\} : k \not\equiv 0 \pmod{m}\}, \quad E_y = \{\{k, k + m\} : 1 \leq k \leq m(n - 1)\}.$$

This graph models an $m \times n$ rectangle R, as follows. The unit square in the ith row from the bottom and the jth column from the left in R corresponds to the vertex $(i-1)m+j$, for $1 \leq i \leq n$ and $1 \leq j \leq m$. There is an edge in E_x for each pair of two horizontally adjacent

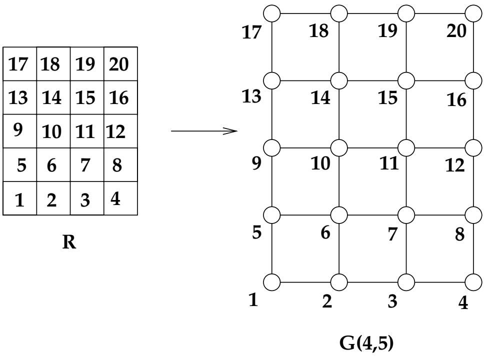


FIGURE 12.15
Graph used to model domino tilings.

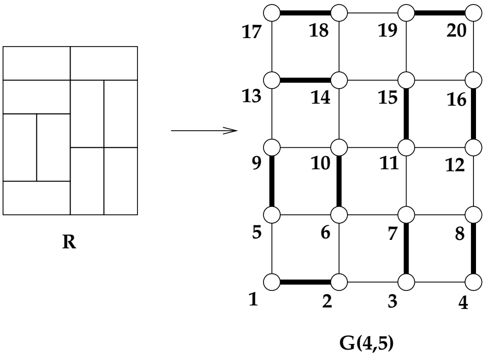


FIGURE 12.16
A domino tiling and a perfect matching.

squares in R, and there is an edge in E_y for each pair of two vertically adjacent squares in R. There is a bijection between the set $\mathrm{Dom}(m,n)$ of domino tilings of R and the set $\mathrm{PM}(G(m,n))$ of perfect matchings of $G(m,n)$. Given a domino tiling, one need only replace each domino covering two adjacent squares by the edge associated to these two squares. This does give a perfect matching, since each square is covered by exactly one domino. If a tiling T corresponds to a matching M under this bijection, we have $N_h(T) = |M \cap E_x|$ and $N_v(T) = |M \cap E_y|$. So, defining $\mathrm{wt}(M) = x^{|M\cap E_x|}y^{|M\cap E_y|}$, we have

$$\sum_{T\in\mathrm{Dom}(m,n)} \mathrm{wt}(T) = \sum_{M\in\mathrm{PM}(G(m,n))} \mathrm{wt}(M).$$

12.86. Example. Figure 12.15 shows the rectangle R and associated graph $G(m,n)$ when $m = 4$ and $n = 5$. Figure 12.16 shows a domino tiling of R and the associated perfect matching. The tiling and matching shown both have weight x^4y^6.

Step 2: Enumeration via Pfaffians. Let X_1 be the skew-symmetric matrix defined in 12.81, taking G there to be $G(m,n)$. We know that

$$\sum_{M\in\mathrm{PM}(G(m,n))} \mathrm{sgn}(M) \prod_{\{i<j\}\in M} x_{i,j} = \mathrm{Pf}(X_1). \tag{12.13}$$

$$\begin{bmatrix}
0 & x & 0 & 0 & -y & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-x & 0 & x & 0 & 0 & y & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -x & 0 & x & 0 & 0 & -y & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & -x & 0 & 0 & 0 & 0 & y & 0 & 0 & 0 & 0 \\
y & 0 & 0 & 0 & 0 & x & 0 & 0 & -y & 0 & 0 & 0 \\
0 & -y & 0 & 0 & -x & 0 & x & 0 & 0 & y & 0 & 0 \\
0 & 0 & y & 0 & 0 & -x & 0 & x & 0 & 0 & -y & 0 \\
0 & 0 & 0 & -y & 0 & 0 & -x & 0 & 0 & 0 & 0 & y \\
0 & 0 & 0 & 0 & y & 0 & 0 & 0 & 0 & x & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -y & 0 & 0 & -x & 0 & x & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & y & 0 & 0 & -x & 0 & x \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -y & 0 & 0 & -x & 0
\end{bmatrix}$$

FIGURE 12.17
Matrix used to enumerate domino tilings ($m = 4, n = 3$).

We introduce the terms *horizontal edge*, *odd vertical edge*, and *even vertical edge* to refer (respectively) to edges in E_x, edges $\{k, k+m\}$ in E_y with k odd, and edges $\{k, k+m\}$ in E_y with k even. Consider the evaluation homomorphism (see 7.102) that sends $x_{i,j}$ to x if $\{i,j\}$ is a horizontal edge, sends $x_{i,j}$ to y if $\{i,j\}$ is an even vertical edge, and sends $x_{i,j}$ to $-y$ if $\{i,j\}$ is an odd vertical edge. Let X be the matrix obtained by applying this homomorphism to each entry of the matrix X_1. Explicitly, X is the $mn \times mn$ matrix with entries

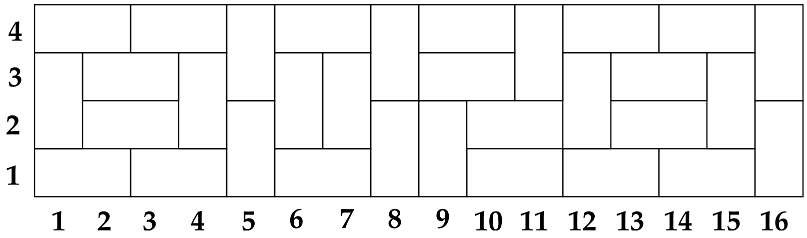
$$X(i,j) = \begin{cases} x & \text{if } j = i+1 \text{ and } i \not\equiv 0 \pmod{m} \\ y & \text{if } j = i+m \text{ and } i \equiv 0 \pmod{2} \\ -y & \text{if } j = i+m \text{ and } i \equiv 1 \pmod{2} \\ -x & \text{if } i = j+1 \text{ and } j \not\equiv 0 \pmod{m} \\ -y & \text{if } i = j+m \text{ and } j \equiv 0 \pmod{2} \\ y & \text{if } i = j+m \text{ and } j \equiv 1 \pmod{2} \\ 0 & \text{otherwise.} \end{cases} \tag{12.14}$$

For example, the matrix X when $m = 4$ and $n = 3$ appears in Figure 12.17. Let $\text{sgn}^*(M) = \text{sgn}(M)(-1)^t$, where t is the number of odd vertical edges in M. Applying the evaluation homomorphism to each side of (12.13) gives

$$\sum_{M \in \text{PM}(G(m,n))} \text{sgn}^*(M)\,\text{wt}(M) = \text{Pf}(X).$$

Step 3: Sign Analysis. The crucial fact to be verified is that $\text{sgn}^*(M) = +1$ *for every* M. Before proving this fact, we consider an example.

12.87. Example. Consider the following domino tiling of a 16×4 rectangle:



This tiling corresponds to a perfect matching M of $G(16,4)$, which is encoded (via 12.80) by a word $w \in \mathrm{SPf}_{64}$. By definition, $\mathrm{sgn}(M) = (-1)^{\mathrm{inv}(w)}$. In our example, the word of M is

$$\begin{aligned} w \quad = \quad & 1,2;3,4;5,21;6,7;8,24;9,25;10,11;12,13;14,15;16,32; \\ & 17,33;18,19;20,36;22,38;23,39;26,27;28,44;29,30;31,47;\ldots;60,61;62,63. \end{aligned}$$

Note that w consists of pairs of letters indicating the two squares occupied by each domino in the tiling. We imagine placing dominos on the board one at a time, in the order specified by w, and updating $\mathrm{sgn}(M)$ and $\mathrm{sgn}^*(M)$ as we go along. When computing $\mathrm{inv}(w)$, the second symbol in each pair sometimes causes inversions with symbols following it in w. Pairs corresponding to horizontal dominos never cause any inversions. Consider the inversions caused by a vertical domino (i.e., a vertical edge in M). The first vertical edge appearing in w is $\{5,21\}$. The 21 is greater than the fifteen symbols $6,7,\ldots,20$ corresponding to squares to the right of column 5 in row 1 and squares to the left of column 5 in row 2, which have not been covered by a domino yet. So this edge increases $\mathrm{inv}(w)$ by $15 = m-1$, which causes a sign change in $\mathrm{sgn}(M)$. However, since this edge is an odd vertical edge, that sign change is counteracted in $\mathrm{sgn}^*(M)$.

The next vertical edge in w is $\{8,24\}$. The symbol 24 causes $14 = m-2$ new inversions, corresponding to squares to the right of column 8 in row 1 and squares to the left of column 8 in row 2, excluding column 5. These inversions do not change $\mathrm{sgn}(M)$, and $\mathrm{sgn}^*(M)$ is also unchanged since $\{8,24\}$ is an even vertical edge.

Continuing similarly, we eventually come to the odd vertical edge $\{23,39\}$ in w. Recalling the order of domino placement, we see that the 39 causes inversions with the following nine symbols to its right in w: 37, 35, 34, 31, 30, 29, 28, 27, 26. Since nine is odd, we get a sign change in $\mathrm{sgn}(M)$, but this is counteracted in $\mathrm{sgn}^*(M)$ since we have just added an odd vertical edge. After accounting for all the dominos, we find that indeed $\mathrm{sgn}^*(M) = +1$, since the insertion of each vertical domino never leads to a net sign change (see 12.170).

Now we are ready to prove that $\mathrm{sgn}^*(M) = +1$ for a general $M \in G(m,n)$. Let $w \in \mathrm{SPf}_{mn}$ be the word encoding M. As in the example, we calculate $\mathrm{sgn}^*(M) = (-1)^{\mathrm{inv}(w)}(-1)^t$ incrementally by scanning the edges in w from left to right. Initially, before scanning any edges, this quantity is $+1$. Suppose the next edge in the scan is the horizontal edge $\{k, k+1\}$. By definition of w (see 12.80), k is the smallest symbol that has not appeared previously in w. So k and $k+1$ cannot cause any new inversions with symbols following them. Similarly, t (the number of odd vertical edges) does not increase when we scan this edge. So $\mathrm{sgn}^*(M)$ is still $+1$ after scanning this edge.

Before continuing, we need the following observation: for every row $i \geq 1$, the number of vertical dominos that start in row i and end in row $i+1$ is even (possibly zero). This is proved by induction on i. To prove the case $i = 1$, suppose there are a horizontal dominos in row 1. Then there must be $m-2a$ vertical dominos starting in row 1. This number is even, since m is even. Now assume the result holds in row $i-1$. In row i, suppose there are a horizontal dominos, b vertical dominos coming up from row $i-1$, and c vertical dominos leading up into row $i+1$. Then $c = m - 2a - b$. Since m is even and (by hypothesis) b is even, c must also be even.

Now suppose the next edge in the scan is a vertical edge $\{k, k+m\}$ in column j that covers rows i and $i+1$ (so $k = (i-1)m + j$). As before, the symbol k causes no new inversions. Let us count the inversions in w between $k+m$ and symbols to its right. There are $m-1$ symbols that might cause inversions with $k+m$, namely $k+1, k+2, \ldots, k+(m-1)$, but some of these symbols may have already appeared in w. Specifically, if there are a vertical dominos covering rows i and $i+1$ to the left of column j, and b vertical dominos covering rows $i-1$ and i to the right of column j, then $a+b$ of the symbols just mentioned will have already appeared in w. So, the inclusion of the new edge increases $\text{inv}(w)$ by $(m-1)-(a+b)$. Now, let there be b' vertical dominos covering rows $i-1$ and i to the left of column j, and c horizontal dominos in row i to the left of column j. Since $m-1 \equiv 1 \pmod 2$, $-a \equiv a \pmod 2$, $-b \equiv b' \pmod 2$ (by the observation in the last paragraph), and $2c \equiv 0 \pmod 2$, we see that

$$(m-1)-a-b \equiv 1+a+b'+2c \pmod 2.$$

But $1+a+b'+2c = j$ since $a+b'+2c$ counts all the columns left of column j in row i. We conclude, finally, that the increase in $\text{inv}(w)$ caused by the insertion of the edge $\{k, k+m\}$ has the same parity as the column index j. Since j and k have the same parity, the number of new inversions is odd iff the new vertical edge is an odd vertical edge. So there is no net change in $\text{sgn}(M^*) = (-1)^{\text{inv}(w)}(-1)^t$ when we add this edge. This completes the proof that $\text{sgn}(M^*) = +1$.

Step 4: Evaluation of the Pfaffian. Combining steps 1 through 3 and 12.83, we have

$$\sum_{T \in \text{Dom}(m,n)} \text{wt}(T) = \sum_{M \in \text{PM}(G(m,n))} \text{wt}(M) = \text{Pf}(X) = \sqrt{\det(X)},$$

where X is the $mn \times mn$ matrix defined by (12.14). So we are reduced to evaluating the determinant of X. The idea is to replace X by a similar matrix $U^{-1}XU$ whose determinant is easier to evaluate. For this purpose, it is convenient to introduce tensor products of matrices.

12.88. Definition: Tensor Product of Matrices. If A is any $n \times n$ matrix and B is any $m \times m$ matrix, let $A \otimes B$ be the $mn \times mn$ matrix given in block form by

$$A \otimes B = \begin{bmatrix} a_{1,1}B & a_{1,2}B & \cdots & a_{1,n}B \\ a_{2,1}B & a_{2,2}B & \cdots & a_{2,n}B \\ \cdots & \cdots & \cdots & \cdots \\ a_{n,1}B & a_{n,2}B & \cdots & a_{n,n}B \end{bmatrix}.$$

Formally, $(A \otimes B)(m(i_1-1)+i_2, m(j_1-1)+j_2) = A(i_1,j_1)B(i_2,j_2)$ for all $1 \le i_1, j_1 \le n$ and all $1 \le i_2, j_2 \le m$.

The following properties of tensor products may be routinely verified:
(a) $(A_1 + A_2) \otimes B = (A_1 \otimes B) + (A_2 \otimes B)$ and $A \otimes (B_1 + B_2) = (A \otimes B_1) + (A \otimes B_2)$.
(b) For any scalar c, $(cA) \otimes B = c(A \otimes B) = A \otimes (cB)$.
(c) $(A_1 \otimes B_1)(A_2 \otimes B_2) = (A_1A_2) \otimes (B_1B_2)$.
(d) If A and B are invertible, then $(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$.

For every $k \ge 1$, let I_k denote the $k \times k$ identity matrix, let F_k denote the $k \times k$ diagonal matrix with diagonal entries $-1, 1, -1, 1, \ldots, (-1)^k$, let I'_k denote the $k \times k$ matrix with 1's on the antidiagonal, and let Q_k denote the $k \times k$ matrix with ones on the diagonal above the main diagonal, -1's on the diagonal below the main diagonal, and zeroes elsewhere. For example,

$$I_5 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \quad F_5 = \begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & -1 \end{bmatrix},$$

$$I'_5 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix}, \quad Q_5 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 \\ 0 & 0 & -1 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{bmatrix}.$$

$$2i\begin{bmatrix}
xr_1 & 0 & 0 & -ys_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & xr_2 & -ys_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -ys_1 & xr_3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-ys_1 & 0 & 0 & xr_4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & xr_1 & 0 & 0 & -ys_2 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & xr_2 & -ys_2 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & -ys_2 & xr_3 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -ys_2 & 0 & 0 & xr_4 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & xr_1 & 0 & 0 & -ys_3 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & xr_2 & -ys_3 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -ys_3 & xr_3 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -ys_3 & 0 & 0 & xr_4
\end{bmatrix}$$

FIGURE 12.18
Transformed matrix $U^{-1}XU$ for $m = 4$, $n = 3$. (Here $r_a = 2i\cos(\pi a/5)$ and $s_b = 2i\cos(\pi b/4)$.)

The definition of X in (12.14) can now be written

$$X = x(I_n \otimes Q_m) + y(Q_n \otimes F_m).$$

(Compare to Figure 12.17.) The following lemma can be established by routine calculations, which we leave to the reader.

12.89. Lemma: Eigenvectors of Q_k. For $0 \le a \le k+1$ and $1 \le b \le k$, define complex numbers

$$U_k(a,b) = i^a \sin\left(\frac{\pi ab}{k+1}\right), \quad \lambda_k(b) = 2i\cos\left(\frac{b\pi}{k+1}\right).$$

For $1 \le a, b \le k$, we have

$$U_k(a+1,b) - U_k(a-1,b) = \lambda_k(b)U_k(a,b).$$

Therefore, the column vector $(U_k(1,b), U_k(2,b), \ldots, U_k(a,b))^t$ is an eigenvector of Q_k associated to the eigenvalue $\lambda_k(b)$. Letting $U_k = (U_k(a,b))_{1\le a,b\le k}$ and D_k be the $k \times k$ diagonal matrix with diagonal entries $\lambda_k(b)$, we have $Q_kU_k = U_kD_k$. Furthermore, $(-1)^aU_k(a,b) = -U_k(a,k+1-b)$ for $1 \le a,b \le k$, and therefore $F_kU_k = -U_kI'_k$.

The columns of U_k are linearly independent, because they are eigenvectors of Q_k associated to *distinct* eigenvalues. Therefore, U_k is invertible, so the lemma gives $U_k^{-1}Q_kU_k = D_k$ and $U_k^{-1}F_kU_k = -I'_k$. Let $U = U_n \otimes U_m$, so $U^{-1} = U_n^{-1} \otimes U_m^{-1}$. Using properties of tensor products, we calculate

$$\begin{aligned}
U^{-1}XU &= x(U_n^{-1} \otimes U_m^{-1})(I_n \otimes Q_m)(U_n \otimes U_m) + y(U_n^{-1} \otimes U_m^{-1})(Q_n \otimes F_m)(U_n \otimes U_m) \\
&= x(U_n^{-1}I_nU_n) \otimes (U_m^{-1}Q_mU_m) + y(U_n^{-1}Q_nU_n) \otimes (U_m^{-1}F_mU_m) \\
&= x(I_n \otimes D_m) - y(D_n \otimes I'_m).
\end{aligned}$$

For example, if X is the matrix shown in Figure 12.17, then $U^{-1}XU$ is the matrix shown in Figure 12.18. In general, $U^{-1}XU$ is a block-diagonal matrix consisting of n $m \times m$ blocks. The bth block has entries $-y\lambda_n(b)$ on the anti-diagonal and entries $x\lambda_m(a)$ (for $1 \le a \le m$) on the diagonal. Now, since m is even, we can reorder the rows and columns of each block into this order: $1, m, 2, m-1, 3, m-2, \ldots, m/2, m/2+1$. This reordering can be accomplished by performing an even number of row and column switches on $U^{-1}XU$, so the determinant does not change. The new matrix is also block-diagonal, consisting of $(mn/2)$ 2×2 blocks that look like

$$\begin{bmatrix} x\lambda_m(a) & -y\lambda_n(b) \\ -y\lambda_n(b) & x\lambda_m(m+1-a) \end{bmatrix} \qquad (1 \leq a \leq m/2, 1 \leq b \leq n).$$

Now, $\lambda_m(m+1-a) = 2i\cos(\pi(m+1-a)/(m+1)) = -2i\cos(\pi a/(m+1)) = -\lambda_m(a)$. It follows that the determinant of the 2×2 block just mentioned is

$$-x^2\lambda_m(a)^2 - y^2\lambda_n(b)^2 = 4\left[x^2\cos^2\left(\frac{\pi a}{m+1}\right) + y^2\cos^2\left(\frac{\pi b}{n+1}\right)\right].$$

Finally, $\det(X) = \det(U^{-1}XU)$ is the product of these determinants as a ranges from 1 to $m/2$ and b ranges from 1 to n. Taking the square root of $\det(X)$ and factoring out powers of 2 produces formula (12.12).

Summary

- *Rational-Slope Dyck Paths.* If $\gcd(r,s) = 1$, then the number of lattice paths from $(0,0)$ to (r,s) that never go below the line $sx = ry$ is $\frac{1}{r+s}\binom{r+s}{r,s}$. For any lattice path ending at (r,s), the $r+s$ cyclic shifts of this path are all distinct, and exactly one of them is an r/s-Dyck path.

- *Chung-Feller Theorem.* A path from $(0,0)$ to (n,n) has k flaws iff the path has k north steps starting below $y = x$. For $0 \leq k \leq n$, there are $C_n = \frac{1}{n+1}\binom{2n}{n,n}$ paths ending at (n,n) with k flaws. Thus the number of flaws in a random path is uniformly distributed on $\{0, 1, 2, \ldots, n\}$.

- *Rook-Equivalence of Ferrers Boards.* For each integer partition μ, $r_k(\mu)$ is the number of ways to place k non-attacking rooks on $F_\mu = \mathrm{dg}(\mu)$, and $R_\mu(x) = \sum_{k\geq 0} r_k(\mu)x^k$. For all partitions $\mu = (\mu_1 \geq \mu_2 \geq \cdots \geq \mu_n \geq 0)$ and $\nu = (\nu_1 \geq \nu_2 \geq \cdots \geq \nu_n \geq 0)$ with $|\mu| = n = |\nu|$, we have $R_\mu(x) = R_\nu(x)$ iff the multisets $[\mu_i + i : 1 \leq i \leq n]$ and $[\nu_i + i : 1 \leq i \leq n]$ are equal.

- *Parking Functions.* A function $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ is a *parking function* iff $|\{x : f(x) \leq i\}| \geq i$ for all $i \leq n$. There are $(n+1)^{n-1}$ parking functions of order n. A bijection from parking functions to labeled Dyck paths is given by putting the labels $\{x : f(x) = i\}$ in increasing order in column i for each i. A bijection from labeled Dyck paths to trees is given by letting the children of a_i be the labels in column $i+1$, for all $i \geq 0$ (where $a_0 = 0$ and $a_1, \ldots, a_n$ are the labels from bottom to top).

- *Facts about Cyclic Groups.* If G is a cyclic group of size $n < \infty$, then G has a unique cyclic subgroup of size d for each divisor d of n, and these are all the subgroups of G. Any cyclic group of size d has $\phi(d)$ generators, and hence $n = \sum_{d|n} \phi(d)$. If G is a group of size n with at most one subgroup of size d for each divisor d of n, then G must be cyclic. Hence, any finite subgroup of the multiplicative group of a field is cyclic.

- *Counting Irreducible Polynomials.* The size of a finite field must be a prime power. For each prime power q, there exists a field F with q elements, which is unique up to isomorphism. For such a field F, let $I(n,q)$ be the number of monic irreducible polynomials of degree n in $F[x]$. Classifying elements in the field of size q^n by their minimal polynomials in $F[x]$ gives $q^n = \sum_{d|n} dI(d,q)$. Hence, by Möbius inversion, $I(n,q) = \frac{1}{n}\sum_{d|n} q^d\mu(n/d)$ where μ is the Möbius function defined in 4.28.

- *Subspaces of Vector Spaces over Finite Fields.* A d-dimensional vector space over a q-element field has size q^d. The number of k-dimensional subspaces of an n-dimensional vector space over a q-element field is $\begin{bmatrix} n \\ k \end{bmatrix}_q$. Each such subspace has a unique basis in reduced row-echelon form (RREF). The number of $k \times n$ RREF matrices with entries in a q-element field is thus $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

- *Combinatorial Meaning of Tangent and Secant Power Series.* $\tan x = \sum_{n\geq 0}(a_n/n!)x^n$, where a_n counts permutations w satisfying $w_1 < w_2 > w_3 < w_4 > \cdots > w_n$; and $\sec x = \sum_{n\geq 0}(b_n/n!)x^n$, where b_n counts permutations w satisfying $w_1 < w_2 > w_3 < \cdots < w_n$.

- *Tournaments.* A tournament is a digraph with exactly one directed edge between each pair of distinct vertices. A tournament t is transitive iff $(u,v) \in t$ and $(v,w) \in t$ always imply $(u,w) \in t$ iff t contains no directed 3-cycle iff the outdegrees of the vertices of t are pairwise distinct. A sign-reversing involution exists that cancels all non-transitive tournaments, leading to this formula for the Vandermonde determinant:

$$\det ||x_j^{n-i}||_{1\leq i,j\leq n} = \sum_{w\in S_n} \operatorname{sgn}(w) \prod_{k=1}^{n} x_{w(k)}^{n-k} = \prod_{1\leq i<j\leq n} (x_i - x_j).$$

- *Hook-Length Formula.* For a partition λ with n boxes, the number of standard tableaux of shape λ is $n!/\prod_{c\in \mathrm{dg}(\lambda)} h(c)$, where $h(c)$ is the hook-length of cell c. This can be proved probabilistically by defining a random algorithm that generates each $S \in \mathrm{SYT}(\lambda)$ with probability $\prod_{c\in\mathrm{dg}(\lambda)} h(c)/n!$. To build S, start at a random cell in $\mathrm{dg}(\lambda)$, then repeatedly jump to a random cell in the hook of the current cell until reaching a corner. Place n in this corner and proceed recursively to fill the other cells in $\mathrm{dg}(\lambda)$.

- *Knuth Equivalence and Monotone Subsequences of Words.* Two words v and w are Knuth equivalent iff v can be changed into w by a sequence of moves of the form $\cdots yxz \cdots \leftrightarrow \cdots yzx \cdots$ (where $x < y \leq z$) or $\cdots xzy \cdots \leftrightarrow \cdots zxy \cdots$ (where $x \leq y < z$). These moves simulate tableau insertion (when applied to reading words), so every w is Knuth equivalent to the reading word of its insertion tableau $P(w)$. Words v and w are Knuth equivalent iff $P(v) = P(w)$. If $P(w)$ has shape λ, then $\lambda_1 + \cdots + \lambda_k$ is the maximum total length of a set of k disjoint weakly increasing subsequences of w, and $\lambda_1' + \cdots + \lambda_k'$ is the maximum total length of a set of k disjoint strictly decreasing subsequences of w.

- *Pfaffians.* Let N be even. Given an $N \times N$ matrix A that is skew-symmetric ($A^t = -A$), the Pfaffian of A is

$$\mathrm{Pf}(A) = \sum_{w\in \mathrm{SPf}_N} \operatorname{sgn}(w) \prod_{i \text{ odd}} A(w_i, w_{i+1}),$$

where $w \in \mathrm{SPf}_N$ iff $w \in S_N$, $w_i < w_{i+1}$, and $w_i < w_{i+2}$ for all odd i. We have $\det(A) = \mathrm{Pf}(A)^2$. Each term of $\mathrm{Pf}(A)$ counts a signed, weighted perfect matching of a graph with vertex set $\{1,2,\ldots,N\}$, where an edge from i to j (for $i < j$) is weighted by $A(i,j)$. There is a recursion $\mathrm{Pf}(A) = \sum_{j=2}^{N}(-1)^j A(1,j)\,\mathrm{Pf}(A[[1,j]])$, where $A[[1,j]]$ is the matrix obtained by deleting rows 1 and j and columns 1 and j from A.

- *Domino Tilings.* For all $m, n \in \mathbb{N}^+$ with m even, the coefficient of $x^a y^b$ in
$$2^{mn/2} \prod_{j=1}^{m/2} \prod_{k=1}^{n} \sqrt{x^2 \cos^2\left(\frac{j\pi}{m+1}\right) + y^2 \cos^2\left(\frac{k\pi}{n+1}\right)}$$
is the number of ways to tile an $m \times n$ board with a horizontal dominos and b vertical dominos. The steps in the proof are: (a) model domino tilings by perfect matchings of a grid-shaped graph; (b) use a Pfaffian to enumerate these signed perfect matchings; (c) adjust signs in the matrix so every perfect matching has sign $+1$; (d) rewrite the Pfaffian as the square root of the determinant of the matrix; (e) evaluate the determinant by performing a similarity transformation that nearly diagonalizes the matrix, creating 2×2 blocks running down the diagonal. Each 2×2 block contributes one of the factors in the product formula above.

Exercises

12.90. Let $\sim$ be the cyclic shift relation from §12.1. Find all the equivalence classes of $\sim$ for: (a) the set of lattice paths ending at $(3,4)$; (b) the set of lattice paths ending at $(3,3)$.

12.91. For $v, w \in \mathcal{R}(N^s E^r)$, write $v \sim w$ iff w can be obtained from v by a cyclic shift. Which of the following statements is always true for all $r, s \geq 1$? (a) Every equivalence class of $\sim$ has size $r+s$. (b) Every equivalence class of $\sim$ contains at least one r/s-Dyck path. (c) Every equivalence class of $\sim$ contains at most one r/s-Dyck path.

12.92. Let $k \geq 0$ and $m \geq 1$ be integers. Show that the number of lattice paths from $(0,0)$ to $(k+mh, h)$ that never go below the line $x = k+my$ is
$$\binom{k+(m+1)h}{k+mh, h} - m\binom{k+(m+1)h}{k+mh+1, h-1}.$$
Give a bijective proof analogous to the proof of 1.56 in §1.10.

12.93. Verify the Chung-Feller theorem directly for $n=3$ by drawing all lattice paths from $(0,0)$ to $(3,3)$ with: (a) 0 flaws; (b) 1 flaw; (c) 2 flaws; (d) 3 flaws.

12.94. Let π be the Dyck path NNENEENNNENNENNEENEENENEEE. Use the bijections from 12.4 to compute the associated lattice path with: (a) 5 flaws; (b) 8 flaws; (c) 10 flaws.

12.95. For each flawed path π, find the Dyck path associated to π via the bijections in 12.4: (a) NENNEEEENENNNEENEENENNNE; (b) NEEENNENEEENNNNNEENE.

12.96. Let π be a random lattice path from $(0,0)$ to (n,n), and for $1 \leq j \leq n$, let
$$X_j(\pi) = \chi(\pi \text{ has a flaw in row } j).$$
Prove bijectively that $P(X_j = 0) = 1/2 = P(X_j = 1)$.

12.97. Let $X_1, X_2, \ldots, X_n$ be *independent* random variables such that $P(X_i = 1) = 1/2 = P(X_i = 0)$ for all i. (This means that, for all $v_1, \ldots, v_n \in \{0,1\}$, the events $X_1 = v_1, X_2 = v_2, \ldots, X_n = v_n$ are independent in the sense of 1.84.) Compute $P(X_1 + X_2 + \cdots + X_n = k)$ for $0 \leq k \leq n$. Contrast your answer with the Chung-Feller theorem.

12.98. Find a formula for the number of lattice paths from $(0,0)$ to (n,n) with k flaws and j east steps departing from the line $y = x$.

12.99. Compute the rook polynomial for each of the following partitions:
(a) $(3,2,1)$; (b) $(8,8,8,8,8,8,8,8)$; (c) (n); (d) $(n,n,1^k)$.

12.100. Draw the diagrams of all integer partitions of 8 and determine which pairs of partitions are rook-equivalent.

12.101. Prove: for any integer partition μ, $R_\mu(x) = R_{\mu'}(x)$.

12.102. (a) For any $n \geq 1$, prove that the partition μ consisting of n copies of n is rook-equivalent to the partition $\nu = (2n-1, 2n-3, \ldots, 5, 3, 1)$. (b) Define a bijection between the set of non-attacking placements of k rooks on μ and the set of non-attacking placements of k rooks on ν.

12.103. Let μ be an integer partition such that $\mathrm{dg}(\mu) \subseteq \mathrm{dg}(\Delta_N)$, where $\Delta_N = (N-1, N-2, \ldots, 3, 2, 1, 0)$. Suppose the sequence $(N-1-\mu_1, N-2-\mu_2, \ldots, 0-\mu_N)$ has a_k copies of k for $k \geq 0$. (Note that this sequence gives the row lengths of the skew shape Δ_N/μ.) Prove that the number of partitions that are rook-equivalent to μ is

$$\prod_{k\geq 1} \binom{a_{k-1} + a_k - 1}{a_{k-1} - 1, a_k}.$$

12.104. Show that for each integer partition μ, there is a unique integer partition ν with distinct parts that is rook-equivalent to μ.

12.105. Suppose μ is an integer partition with $\mathrm{dg}(\mu) \subseteq \mathrm{dg}(\Delta_N)$, where $\Delta_N = (N-1, N-2, \ldots, 2, 1, 0)$. (a) Using a suitable involution, prove that

$$r_k(\mu) = \sum_{i=0}^{k} S(N-i, N-k)(-1)^i e_i(N-1-\mu_1, N-2-\mu_2, \ldots, N-N-\mu_N),$$

where $S(u,v)$ is a Stirling number of the second kind and e_i is an elementary symmetric polynomial. (b) Deduce from (a) a combinatorial proof of part (d) of 2.77. (c) Deduce from (a) that the multiset condition in 12.10 is sufficient for $R_\mu(x) = R_\nu(x)$. (d) Assume μ and ν are rook-equivalent partitions. Use (a) and the Garsia-Milne involution principle 4.126 to construct a bijection from the set of non-attacking placements of k rooks on F_μ to the set of non-attacking placements of k rooks on F_ν.

12.106. For each labeled Dyck path in Figure 12.9, compute the associated parking function and tree (see 12.21 and 12.22).

12.107. (a) Convert the parking function f in Figure 12.5 to a labeled Dyck path and a tree. (b) Convert the labeled Dyck path NNENNEENEENENNEE with labels $5,8,2,4,1,6,3,7$ (from bottom to top) to a parking function and a tree. (c) Convert the tree

$$T = (\{0,1,\ldots 10\}, \{\{0,9\},\{5,7\},\{5,8\},\{9,4\},\{7,6\},\{6,9\},\{7,10\},\{10,1\},\{3,9\},\{2,9\}\})$$

to a labeled Dyck path and a parking function.

12.108. Suppose we represent a function $f : \{1,2,\ldots,b\} \to \{1,2,\ldots,a+1\}$ as a labeled lattice path ending at (a,b). Find conditions on the labeled path that are equivalent to f being (a) surjective; (b) injective.

12.109. (a) Given nonnegative integers $c_1, \ldots, c_{a+1}$ adding to b, how many labeled lattice paths from $(0,0)$ to (a,b) have c_i labels in column i for all i? (b) Use the bijections in §12.5 to translate (a) into enumeration results for parking functions and trees.

12.110. (a) Let p_n be the number of parking functions of order n. Give a combinatorial proof of the recursion

$$p_n = \sum_{m=1}^{n} m \binom{n-1}{m-1} p_{m-1} p_{n-m}.$$

(b) Use (a) and 3.186 to define a bijection between parking functions and trees.

12.111. For a parking function $f \in \mathcal{P}_n$, let $\mathrm{wt}(f) = n(n+1)/2 - \sum_{i=1}^{n} f(i)$. Let $P_n(x) = \sum_{f \in \mathcal{P}_n} x^{\mathrm{wt}(f)}$. Prove the recursion

$$P_n(x) = \sum_{m=1}^{n} [m]_x \binom{n-1}{m-1} P_{m-1}(x) P_{n-m}(x).$$

12.112. Let S be a k-element subset of $\{1, 2, \ldots, n\}$. Prove that there are kn^{n-k-1} parking functions f such that $S = \{x : f(x) = 1\}$.

12.113. For each $n, k, m \in \mathbb{N}$, let $\mathcal{P}_{n,k,m}$ be the set of labeled lattice paths ending at $(k + mn, n)$ that never go below the line $x = k + my$. Find a recursion satisfied by the quantities $|\mathcal{P}_{n,k,m}|$.

12.114. Find a bijection between the set of parking functions of order n and the quotient group $\mathbb{Z}_{n+1}^n / H$, where H is the subgroup generated by $(1, 1, \ldots, 1)$.

12.115. How many generators does an infinite cyclic group have?

12.116. Prove or disprove: if every proper subgroup of a finite group G is cyclic, then G itself must be cyclic.

12.117. Suppose G is a group such that, for all $d \geq 1$, G has at most d elements x such that $x^d = 1$. Prove that every finite subgroup of G is cyclic.

12.118. Describe all the finite subgroups of the field $\mathbb{C}$.

12.119. Quaternions. Let H be a four-dimensional real vector space with basis $1, i, j, k$. Define multiplication on H by letting 1 act as the identity, setting $i^2 = j^2 = k^2 = -1$, $ij = k = -ji$, $jk = i = -kj$, $ki = j = -ik$, and extending by linearity. (a) Show that H with this multiplication is a division ring (i.e., H satisfies all the axioms in the definition of a field except commutativity of multiplication). (b) Find a non-cyclic finite subgroup of H^* (cf. 12.29). (c) Show that the equation $x^2 = -1$ has infinitely many solutions in H^*.

12.120. Prove that the product of all the nonzero elements in a finite field F is -1_F. Deduce Wilson's theorem: for p prime, $(p-1)! \equiv -1 \pmod{p}$.

12.121. Compute the number of monic irreducible polynomials of degree 12 over a 9-element field.

12.122. (a) Enumerate all the irreducible polynomials in $\mathbb{Z}_2[x]$ of degree at most 5. (b) Use the formula in 12.30 to compute $I(n, 2)$ for $1 \leq n \leq 8$ (compare with the results in (a) for $n \leq 5$).

12.123. Construction of Finite Fields. Let F be a field with q elements, let $h \in F[x]$ be a fixed monic irreducible polynomial of degree n, and let

$$K = \{f \in F[x] : f = 0 \text{ or } \deg(f) < n\}.$$

For $f, g \in K$, define $f + g$ to be the usual sum of polynomials in $F[x]$, and define $f \times g$ to be the remainder when fg is divided by h. Show that K, with these operations, is a field of size q^n. The field K is denoted $F[x]/(h)$.

12.124. Let $K = \mathbb{Z}_2[x]/(x^3 + x + 1)$ (see 12.123). Construct addition and multiplication tables for K. Explicitly confirm that K^* is generated by x by computing x^i for $1 \leq i \leq 7$.

12.125. Let $h = x^4 + x + 1 \in \mathbb{Z}_2[x]$, and let $K = \mathbb{Z}_2[x]/(h)$, which is a 16-element field (see 12.123). (a) Explain why every element $y \in K$ satisfies $y^{16} = y$. (b) List all the elements of K and their minimal polynomials over $\mathbb{Z}_2$. (c) Factor the polynomial $x^{16} - x \in \mathbb{Z}_2[x]$ into a product of irreducible polynomials. (d) Explain the relation between part (b), part (c), and the formulas in 12.30. (e) Find all generators of the cyclic group K^*.

12.126. (a) Use 12.30 to show that $I(n, q) > 0$ for all prime powers q and all $n \geq 1$. (b) Prove that for every prime power p^n, there exists a field of size p^n.

12.127. Let F be a finite field of size q. A polynomial $h \in F[x]$ is called *primitive* iff h is a monic irreducible polynomial such that x is a generator of the multiplicative group of the field $K = F[x]/(h)$ (see 12.123). (a) Count the primitive polynomials of degree n in $F[x]$. (b) Give an example of an irreducible polynomial in $\mathbb{Z}_2[x]$ that is not primitive.

12.128. Let K be a q-element field. How many $n \times n$ matrices with entries in K are: (a) upper-triangular; (b) strictly upper-triangular (zeroes on the main diagonal); (c) unitriangular (ones on the main diagonal); (d) upper-triangular and invertible?

12.129. How many 2×2 matrices with entries in a q-element field have determinant 1?

12.130. Count the number of invertible $n \times n$ matrices with entries in a q-element field F. How is the answer related to $[n]!_q$?

12.131. How many 3-dimensional subspaces does the vector space $\mathbb{Z}_7^5$ have?

12.132. For each integer partition μ that fits in a box with 2 rows and 3 columns, draw a picture of the RREF matrix associated to μ in the proof of 12.37.

12.133. Find the RREF basis for the subspace of $\mathbb{Z}_5^5$ spanned by $v_1 = (1, 4, 2, 3, 4)$, $v_2 = (2, 3, 1, 0, 0)$, and $v_3 = (0, 0, 3, 1, 1)$.

12.134. Find the RREF basis for the subspace of $\mathbb{Z}_2^6$ spanned by $v_1 = (0, 1, 1, 1, 1, 0)$, $v_2 = (1, 1, 1, 0, 1, 1)$, and $v_3 = (1, 0, 1, 0, 0, 0)$.

12.135. Let V be an n-dimensional vector space over a field K. A *flag of subspaces of* V is a chain of subspaces $V = V_0 \supseteq V_1 \supseteq V_2 \supseteq \cdots \supseteq V_s = \{0\}$. Suppose $|K| = q$. Given $n_1, \ldots, n_s$ and $n = n_1 + \cdots + n_s$, count the number of such flags in V such that $\dim_K(V_{i-1}) - \dim_K(V_i) = n_i$ for $1 \leq i \leq s$.

12.136. (a) Give a linear-algebraic proof of the symmetry property $\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$ when q is a prime power. (b) Explain how the equality of formal polynomials $\begin{bmatrix} n \\ k \end{bmatrix}_x = \begin{bmatrix} n \\ n-k \end{bmatrix}_x$ can be deduced from (a).

12.137. Let V be an n-dimensional vector space over a q-element field, and let X be the poset of all subspaces of V, ordered by inclusion. Show that the Möbius function of X is given by $\mu_X(W,Y) = (-1)^d q^{d(d-1)/2}\chi(W \subseteq Y)$, where $d = \dim(Y) - \dim(W)$. (Use 6.61.)

12.138. Use the recursions for a_n and b_n in §12.8 to verify the values in (12.2).

12.139. Give probabilistic interpretations for the rational numbers appearing as coefficients in the Maclaurin series for $\tan x$ and $\sec x$.

12.140. Fill in the details of Step 5 of the proof in §12.8.

12.141. (a) List the permutations satisfying (12.3) for $n = 1, 3, 5$. (b) List the permutations satisfying (12.4) for $n = 0, 2, 4$.

12.142. (a) Develop ranking and unranking algorithms for up-down permutations. (b) Unrank 147 to get an up-down permutation in S_7. (c) Find the rank of $2, 5, 3, 6, 4, 8, 1, 7$ among up-down permutations of length 8.

12.143. Let $(q;q)_0 = 1$ and $(q;q)_n = (1-q)(1-q^2)\cdots(1-q^n)$ for $n \geq 1$. Consider the following q-analogues of formal trigonometric functions:

$$\sin_q = \sum_{k\geq 0} (-1)^k \frac{x^{2k+1}}{(q;q)_{2k+1}}; \quad \cos_q = \sum_{k\geq 0} (-1)^k \frac{x^{2k}}{(q;q)_{2k}} \in \mathbb{Q}(q)[[x]];$$

$$\tan_q = \sin_q / \cos_q; \quad \sec_q = 1/\cos_q .$$

Define *q-tangent numbers* and *q-secant numbers* by $t_n = (q;q)_n \tan_q(n) \in \mathbb{Q}(q)$ and $s_n = (q;q)_n \sec_q(n) \in \mathbb{Q}(q)$. (a) Show that for each $n \geq 0$,

$$t_n = \sum_{w \text{ satisfying } (12.3)} q^{\mathrm{inv}(w)}; \quad s_n = \sum_{w \text{ satisfying } (12.4)} q^{\mathrm{inv}(w)}.$$

(b) Use (a) to conclude that $t_n, s_n \in \mathbb{N}[q]$. Compute t_n for $n = 1, 3, 5$ and s_n for $n = 0, 2, 4$.

12.144. Let t be the tournament with edge set

$$\{(2,1),(1,3),(4,1),(1,5),(6,1),(2,3),(4,2),(5,2),(2,6),$$
$$(3,4),(3,5),(6,3),(4,5),(6,4),(6,5)\}.$$

Compute $\mathrm{wt}(t)$, $\mathrm{inv}(t)$, and $\mathrm{sgn}(t)$. Is t transitive?

12.145. Let t be the tournament in 12.41 and I the involution used to prove 12.46. Compute $t' = I(t)$, and verify directly that $\mathrm{wt}(t') = \mathrm{wt}(t)$, $\mathrm{sgn}(t') = -\mathrm{sgn}(t)$, and $I(t') = t$.

12.146. Use induction and 9.47 to give an algebraic proof of 12.46.

12.147. Suppose $x_0, x_1, \ldots, x_N$ are *distinct* elements of a field F. State why the Vandermonde matrix $[x_j^{N-i}]_{0\leq i,j\leq N}$ is invertible. Use this to prove the fact (asserted in 2.79) that if $p \in F[x]$ has degree at most N and satisfies $p(x_i) = 0$ for $0 \leq i \leq N$, then p must be the zero polynomial.

12.148. A *king* in a tournament t is a vertex v from which every other vertex can be reached by following at most 2 directed edges. Show that every vertex of maximum outdegree in a tournament is a king; in particular, every tournament has a king.

12.149. Use the hook-length formula to compute f^λ for the following shapes λ: (a) $(3,2,1)$; (b) $(4,4,4)$; (c) $(6,3,2,2,1,1,1)$; (d) $(n, n-1)$; (e) $(a, 1^b)$.

12.150. Show that $f^{(0)} = 1$ and, for all nonzero partitions λ, $f^\lambda = \sum_\mu f^\mu$ where we sum over all μ that can be obtained from λ by removing some corner square. Use this recursion to calculate f^λ for all λ with $|\lambda| \leq 6$.

12.151. (a) Develop ranking and unranking algorithms for standard tableaux of shape λ based on the recursion in 12.150. (b) Unrank 46 to get a standard tableau of shape $(4, 3, 1)$. (c) Rank the standard tableau $\begin{array}{|c|c|c|}\hline 1&3&4\\ \hline 2&5&8\\ \hline 6&7\\ \cline{1-2}\end{array}$.

12.152. Enumerate all the hook walks for the shape $\lambda = (4, 3, 2, 1)$ that end in the corner cell $(2, 3)$, and compute the probability of each walk. Use this computation to verify 12.54 in this case.

12.153. Suppose $\lambda \in \text{Par}(p)$ where p is prime. (a) Show that p divides f^λ if λ is not a hook (see 10.3). (b) Compute $f^\lambda \bmod p$ if λ is a hook.

12.154. Does the hook-length formula extend to enumerate standard tableaux of skew shape? Either adapt the probabilistic proof to this situation, or find the steps in the proof that cannot be generalized.

12.155. Confirm that $\equiv_P$ and $\equiv_K$ are equivalence relations on X^*, as asserted in §12.11.

12.156. Let T be the tableau in 12.62. Find an explicit chain of elementary Knuth equivalences demonstrating that $\text{rw}(T)1 \equiv_K \text{rw}(T \leftarrow 1)$.

12.157. Find the length of the longest increasing and decreasing subsequences of the word

$$w = 4135321462731132423142.$$

12.158. Complete the proofs of 12.64 and 12.65.

12.159. For any semistandard tableau T, prove that $P(\text{rw}(T)) = T$. Show that the set of reading words of semistandard tableaux intersects every Knuth equivalence class in exactly one point.

12.160. Prove 12.70 without using the RSK algorithm.

12.161. Show that if A is an $N \times N$ skew-symmetric matrix with N odd, then $\det(A) = 0$.

12.162. Verify by direct calculation that $\det(A) = (af + cd - be)^2$ for the 4×4 matrix A in 12.72.

12.163. Find the Pfaffian of a general 6×6 skew-symmetric matrix.

12.164. Count the number of perfect matchings for the graph shown in Figure 12.14.

12.165. Let G be the simple graph with $V(G) = \{1, 2, 3, 4, 5, 6\}$ and

$$E(G) = \{\{2, 3\}, \{3, 4\}, \{4, 5\}, \{2, 5\}, \{1, 2\}, \{1, 5\}, \{3, 6\}, \{4, 6\}, \{2, 4\}\}.$$

Find all perfect matchings of G. Use this to compute $\sum_{M \in \text{PM}(G)} \text{sgn}(M) \,\text{wt}(M)$, and verify your answer by evaluating a suitable Pfaffian.

12.166. Compute the images of the following permutations $w \in S_N^{ev}$ under the bijection $S_N^{ev} \to \text{SPf}_N^2$ used in the proof of 12.83: (a) $w = (3, 1, 5, 7)(2, 4, 8, 6)$; (b) $w = (1, 4)(2, 3)(5, 7)(6, 8)$; (c) $w = (2, 5, 1, 6, 8, 4, 7, 3)$; (d) $w = (3, 2, 1, 5, 6, 7)(4, 8)$.

12.167. Compute the images w of the following pairs $(u,v) \in \mathrm{SPf}_N^2$ under the bijection $\mathrm{SPf}_N^2 \to S_N^{ev}$ used in the proof of 12.83: (a) $u = 13254768$, $v = 15283647$; (b) $u = 13254768$, $v = 12374856$; (c) $u = 15243867 = v$. In each case, confirm that the term indexed by w in $\det(A)$ equals the term indexed by (u,v) in $\mathrm{Pf}(A)^2$.

12.168. Compute the exact number of domino tilings of a 10 × 10 board and a 6 × 9 board.

12.169. How many domino tilings of an 8 × 8 board use: (a) 24 horizontal dominos and 8 vertical dominos; (b) 4 horizontal dominos and 28 vertical dominos?

12.170. Complete 12.87 by writing out w in full and showing that the placement of every new domino never causes $\mathrm{sgn}^*(M)$ to become negative.

12.171. Verify the four properties of tensor products of matrices stated just below 12.88.

12.172. Prove 12.89.

12.173. Let U_k be the matrix defined in 12.89. Show that $\sqrt{2/(k+1)}U_k$ is a unitary matrix (i.e., $U^{-1} = U^*$, where U^* is the conjugate-transpose of U).

12.174. (a) Prove that, for even m,

$$\prod_{j=1}^{m/2} 4(u^2 + \cos^2(j\pi/(m+1))) = \frac{[u+\sqrt{1+u^2}]^{m+1} - [u-\sqrt{1+u^2}]^{m+1}}{2\sqrt{1+u^2}}.$$

(b) Deduce that

$$\prod_{j=1}^{m/2} 2\cos(j\pi/(m+1)) = 1.$$

12.175. Show that formula (12.12) simplifies to

$$\begin{cases} 2^{mn/2} \displaystyle\prod_{j=1}^{m/2}\prod_{k=1}^{n/2} \left[x^2\cos^2\left(\frac{j\pi}{m+1}\right) + y^2\cos^2\left(\frac{k\pi}{n+1}\right)\right] & (n \text{ even}) \\ 2^{m(n-1)/2}x^{m/2} \displaystyle\prod_{j=1}^{m/2}\prod_{k=1}^{(n-1)/2} \left[x^2\cos^2\left(\frac{j\pi}{m+1}\right) + y^2\cos^2\left(\frac{k\pi}{n+1}\right)\right] & (n \text{ odd}). \end{cases}$$

Notes

§12.1. Detailed treatments of the theory of lattice paths may be found in Mohanty and Narayana [94, 98]. **§12.2.** The Chung-Feller theorem was originally proved in Chung and Feller [25]; the bijective proof given here is due to Eu, Fu, and Yeh [35]. **§12.3.** There is a growing literature on rook theory; some of the early papers in this subject are [41, 55, 56, 74]. **§12.4.** More information about parking functions may be found in [39, 43, 81, 123]. **§12.6.** Expositions of field theory may be found in Hungerford [70] or Chapter 5 of Bourbaki [19]. An encyclopedic reference for the subject of finite fields is Lidl and Niederreiter [83]. **§12.7.** For more on Gaussian elimination and RREF matrices, see linear algebra texts such as Hoffman and Kunze [69]. **§12.8.** The combinatorial interpretation of the coefficients of the tangent and secant power series is due to André [2, 4]. For more information on q-analogues of the tangent and secant series, see [6, 7, 37]. **§12.9.** Moon [97] gives a thorough account of tournaments. The combinatorial derivation of the Vandermonde determinant is due to Gessel [52]. **§12.10.** The probabilistic proof of the hook-length formula is due to Greene, Nijenhuis, and Wilf [62]. **§12.11.** A discussion of Knuth equivalence and its connection to the RSK correspondence appears in Knuth [77]. The theorem 12.65 on disjoint monotone subsequences was proved by Greene [61]; this generalizes Schensted's original result [122] on the size of the longest increasing subsequence of a word. **§12.13.** Our treatment of the domino tiling formula closely follows the presentation in Kasteleyn's original paper [75].