Random Orders and Gambler's Ruin

Andreas Blass*
Mathematics Department
University of Michigan
Ann Arbor, MI 48109–1109
U.S.A.
ablass@umich.edu

Gábor Braun †
Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences
Budapest
Reáltanoda 13–15
1053
Hungary
braung@renyi.hu

Submitted: Aug 23, 2004; Accepted: Apr 20, 2005; Published: May 13, 2005
2000 Mathematics Subject Classifications: Primary: 05A15, Secondary: 05A19, 60C05

Abstract

We prove a conjecture of Droste and Kuske about the probability that 1 is minimal in a certain random linear ordering of the set of natural numbers. We also prove generalizations, in two directions, of this conjecture: when we use a biased coin in the random process and when we begin the random process with a specified ordering of a finite initial segment of the natural numbers. Our proofs use a connection between the conjecture and a question about the game of gambler's ruin. We exhibit several different approaches (combinatorial, probabilistic, generating function) to the problem, of course ultimately producing equivalent results.

1 Introduction

Droste and Kuske [4] have studied several random processes for producing a linear ordering $\prec$ on the set $\mathbb{N}$ of positive integers. In contrast to random graphs [2] and similar structures, random orders cannot be produced by deciding independently about each of the relations $a \prec b$, for all pairs a, b, because the transitivity of the ordering imposes dependencies between these relations. Droste and Kuske consider processes that make decisions about the relations $a \prec b$ one after another, the decision about any particular pair a, b being made at random *provided* it is not already determined by previous decisions about other pairs. To specify such a process, one must specify the order in which the various pairs a, b are to be considered; several such specifications are considered in [4].

*Partially supported by NSF grant DMS–0070723. Part of this paper was written during a visit of the first author to the Centre de Recerca Matemàtica in Barcelona.
†Partially supported by grant T043034 of Hungarian Scientific Research Fund.

This paper arose from a conjecture of Droste and Kuske concerning a particular specification of the random process described above, namely the specification that considers pairs a, b in order of increasing $\max\{a, b\}$ and, when pairs have the same $\max\{a, b\}$, in order of decreasing $\min\{a, b\}$. Here is a less formal description of the process, which will be convenient for our purposes. We regard the process as proceeding in a sequence of steps. Initially, we have the set $\{1\}$ (with its unique ordering). The first $n-1$ steps determine the linear ordering relation $\prec$ on the set $\{1, 2, \ldots, n\}$. Step n does not change the relative ordering of $1, 2, \ldots, n$ but inserts $n+1$ into it at a location determined as follows. First, a fair coin is flipped to decide the position of $n+1$ relative to n, i.e., whether $n+1 \prec n$ or $n \prec n+1$. This decision may determine, via transitivity, the position of $n+1$ relative to $n-1$ (namely if either $n-1 \prec n \prec n+1$ or $n+1 \prec n \prec n-1$). If it does not, then another (independent) fair coin is flipped to decide the position of $n+1$ relative to $n-1$. Similarly, for each $j = n-2, n-3, \ldots, 2, 1$ in turn, in this order, if the position of $n+1$ relative to j is not already determined by decisions for previous (larger) values of j, then this decision is made by flipping a fair coin (independent of all the other coin flips).

Droste and Kuske conjectured, on the basis of calculations for small n, that the probability $P(n)$ that 1 is the first element in the ordering $\prec$ of $\{1, 2, \ldots, n\}$ is given by

$$P(n) = \prod_{i=1}^{n-1} \frac{2i-1}{2i}.$$

We shall prove this conjecture, and we shall also establish several related results. Specifically, we obtain a formula for $P(n)$ when the coins are not fair but have a constant bias. Our results also cover the situation where, for some positive integer w, the process is started with the ordering $1 \prec 2 \prec \cdots \prec w$ and only the integers greater than w are inserted by the random process described above.

The history of this work is as follows. After learning of the conjecture of Droste and Kuske, we independently proved it, by quite different methods. One of the proofs (by Braun) included the generalization to biased coins. The other (by Blass) included the generalization to an initial ordering $1 \prec 2 \prec \cdots \prec w$. After we learned, via Droste, of each other's work, we jointly extended the proofs to handle both generalizations simultaneously. But the proofs gave rather different-looking formulas.

We therefore present, in this paper, the arguments leading to both formulas. In a final section, we directly verify that the formulas are, despite their different appearances, equivalent — a result which also follows, of course, from the fact that they both solve the same problem.

In fact, as our work progressed, we found additional approaches to the problem, all leading to the same two formulas. We therefore take this opportunity to show, in a particular case, a number of techniques for attacking problems of this sort. A reader who wants just one complete proof, not a multiplicity of techniques, could read Section 2 and then either Subsection 3.6 or Subsection 4.2.

The paper is organized as follows. In Section 2, we reduce the problem to a question about the random process or game called "gambler's ruin." In Section 3, we deduce a recurrence relation for the probabilities we seek, and we solve the recurrence relation by reducing it to a variant of the familiar "Pascal triangle" recurrence for binomial coefficients. We also give a second way to see the correctness of the resulting formula. In Section 4, we give an alternative approach, using a well-known generalization of the Catalan numbers. The formula obtained by this approach looks different from the one in the previous section, though of course they are equivalent. In Section 5, we present a second derivation of this formula, using generating functions. Finally, in Section 6, we present some additional observations, including, as mentioned above, a direct verification that the two formulas obtained in the preceding sections are equal.

Convention 1.1 Throughout this paper, all coin flips are understood to be (probabilistically) independent.

Convention 1.2 Because we shall need to refer to both the standard ordering $\leq$ and the randomly constructed ordering $\prec$ of $\mathbb{N}$, we adopt the following terminology. We use "time" words like "earlier, later, before, after" to refer to $\prec$, and we use "size" words like "larger, smaller" to refer to $\leq$. Thus, for example, when we insert $n+1$ into the ordering, we decide whether $n+1$ comes before or after each j smaller than $n+1$ by going through the j's in order from largest to smallest and flipping coins to make all decisions not already forced.

Convention 1.3 When a coin flip is used to decide whether $n+1$ comes before or after some smaller number j, we refer to the decision $j \prec n+1$ as "heads" and to $n+1 \prec j$ as "tails". When we consider biased coins, we let p be the probability of heads and $q = 1-p$ the probability of tails.

2 Gambler's Ruin

The key to our analysis of the problem is the critical sequence associated to any ordering $\prec$ of $\{1, 2, \ldots, n\}$ as follows.

Definition 2.1 Let $\prec$ linearly order $\{1, 2, \ldots, n\}$. The *critical sequence* of $\prec$ begins with the largest element n of its field. Thereafter, each term is the largest number that is earlier (in $\prec$) than the preceding term.

For example, if $n = 7$ and the ordering is given by

$$2 \prec 5 \prec 3 \prec 1 \prec 7 \prec 6 \prec 4,$$

then the critical sequence is $\langle 7, 5, 2 \rangle$. Notice that the critical sequence is always decreasing with respect to both $\leq$ and $\prec$ and that it ends with the earliest element. In particular, $P(n)$ can be described as the probability that 1 is in the critical sequence (equivalently, that the critical sequence ends with 1) for an ordering $\prec$ obtained by the random process described above.

What makes critical sequences useful is that the critical sequence at any stage n of the random process suffices to determine the probabilities of all the possible critical sequences at the next stage. In other words, the process can be regarded as randomly generating critical sequences, and we can forget the rest of the information in $\prec$.

To see this, consider the step where $\prec$ is already defined on $\{1, 2, \ldots, n\}$ and we are inserting $n+1$ into this ordering. Suppose the critical sequence before the insertion was $\langle c_1, c_2, \ldots, c_k \rangle$, so $c_1 = n$. What can we say about the new critical sequence? Of course, it begins with $n+1$. What happens next depends on the first coin flip, the one that determines the location of $n+1$ relative to n. If $n \prec n+1$ (i.e., the first coin flip was heads), then the next term of the new critical sequence is $n = c_1$, and in fact from this point on the new critical sequence is identical with the old. The reason is that $n+1$, being inserted after n in the ordering, will have nothing to do with any of the comparisons defining the rest of the critical sequence. Thus, if $n \prec n+1$, then the new sequence is just the old one with $n+1$ added at the beginning.

Suppose, on the other hand, that the first coin flip was tails, resulting in $n+1 \prec n$. Then of course $n = c_1$ will not be in the new critical sequence (since the sequence is decreasing with respect to $\prec$). For any j in the range $c_2 < j < n$, we have $n \prec j$ by definition of c_2 and so the first coin flip has already forced $n+1 \prec j$. But $c_2 \prec n$, so the next coin flip will serve to decide the location of $n+1$ relative to c_2. (If there is no c_2, i.e., if the length k of the old critical sequence was 1, then there are no more coin flips and the new critical sequence is $\langle n+1 \rangle$.) If this second coin flip is heads, making $c_2 \prec n+1$, then c_2 is the next term in the new critical sequence (after $n+1$), and the remainder of the critical sequence, after c_2, is as before, since $n+1$, inserted into the order after c_2, will have no effect on this part of the construction of the critical sequence.

Suppose, on the other hand, that the second coin flip is tails, resulting in $n+1 \prec c_2$. Then c_2 is not in the new critical sequence, nor is any j from the range $c_3 < j < c_2$ as these satisfy $c_2 \prec j$ by definition of c_3 and therefore $n+1 \prec j$. The next coin flip will serve to determine the location of $n+1$ relative to c_3. Continuing in this fashion, we find that the new critical sequence can be obtained from the old by the following simple procedure.

Start with $n+1$. Then go through the old critical sequence, flipping a coin for each term until a coin flip comes up heads (or you reach the end of the old sequence). All the terms, if any, for which the flips came up tails (before any flip came up heads) are deleted. The term for which the flip came up heads is kept, as are all subsequent terms of the old sequence, and they, together with the initial $n+1$, constitute the new critical sequence. If no coin comes up heads, then the new critical sequence is just $\langle n+1 \rangle$.

In particular, if the old critical sequence had length k then the new critical sequence has length

- $k+1$ with probability p,
- k with probability qp,
- $k-1$ with probability q^2p,

- $\dots$,
- 3 with probability $q^{k-2}p$,
- 2 with probability $q^{k-1}p$, and
- 1 with probability q^k.

(Recall that p and q are the probabilities of heads and tails, respectively.) Notice also that 1 ceases to be the earliest element (in $\prec$) at some stage of the process if and only if at that stage a new element is inserted at the beginning of the $\prec$-order, i.e., if and only if at that stage the length of the critical sequence drops down to 1. Thus, the probability $P(n)$ that 1 is $\prec$-minimal in $\{1, 2, \dots, n\}$ can be described as the probability that, during the first $n-1$ steps of the process, the length of the critical sequence, which was initially 1 (when $\prec$ ordered only the set $\{1\}$), never returns to 1.

From here on, we shall be concerned only with the length of the critical sequence, which we call the *critical length*; we shall not need to consider the critical sequence itself (much less the order $\prec$ from which it came). The critical length begins (when $n = 1$) with the value 1 and changes from one step to the next according to the probabilities listed above. As long as it has not returned to 1, we can describe these probabilities in the following equivalent way. When the critical length is k, the step to the next critical length can be split into small micro-steps, one for each coin flip. Decrease the critical length by 1 for each coin flip as long as they all come up tails, and then increase it by 1 the first time the coin comes up heads. This produces the same next critical length as the probability list above, as long as we don't have so many consecutive tails as to drive the critical length down to 0 (from which a head at the next micro-step would bring it to 1).

But now the process admits the following simpler description, essentially ignoring the original steps and concentrating on the micro-steps. The critical length is initially 1. We repeatedly flip coins (independent, with bias given by p and q). Every time a coin comes up heads, the critical length increases by 1, and every time a coin comes up tails, the critical length decreases by one. We stop when the critical length reaches 0 (for then at the end of the current step of the original process the critical length will be 1). If we substitute the words "our wealth" for "the critical length," we find that this description exactly matches the game of gambler's ruin. We begin with 1 euro, and we repeatedly flip coins winning (or losing) 1 euro whenever the coin comes up heads (or tails, respectively), until we run out of money.

$P(n)$ is the probability that we have not run out of money after $n-1$ steps of the original process (which may be a much larger number of micro-steps). Thus, $\lim_{n\to\infty} P(n)$ is the probability that we never run out of money. It is well-known (see for example [6, Section 12.2]) that this limit, the probability of never running out of money when playing gambler's ruin, starting with one euro against an infinitely wealthy opponent, is

$$\lim_{n\to\infty} P(n) = \begin{cases} 1 - \frac{q}{p} = 2 - \frac{1}{p}, & \text{if } p \geq \frac{1}{2} \\ 0, & \text{if } p \leq \frac{1}{2}. \end{cases}$$

In particular, in the case of a fair coin, the case considered by Droste and Kuske, the limiting probability is 0. That is, with probability 1, the number 1 will not be the earliest element of $\mathbb{N}$ after all of $\mathbb{N}$ has been ordered by $\prec$. This fact, a consequence of the conjecture of Droste and Kuske, is what was actually needed for their analysis in [4] of the ordering $\prec$.

To establish the conjecture of Droste and Kuske (rather than only its limit as $n \to \infty$), it is convenient to prove a stronger result in order to facilitate an induction. Instead of starting with just 1 euro, let us begin with an arbitrary, non-negative (whole) number w of euros. As before, we win or lose one euro at each coin flip, according to whether the flip was heads or tails, and if we run out of money the game ends. In terms of the ordering $\prec$, this generalization means that we start with a critical sequence of length w rather than 1, for example with the ordering $1 \prec 2 \prec \cdots \prec w$ of the first w integers. From this starting point, we proceed as before to insert larger integers into the ordering.

Definition 2.2 Let $P(w, m)$ be the probability that, in the gambler's ruin game described above, with initial wealth w, at least m coin flips are heads before we run out of money.

Thus, the $P(n)$ that we set out to compute is, in this new notation, $P(1, n-1)$. The remainder of this paper is devoted to several methods for evaluating $P(w, m)$ for all w and m.

Remark 2.3 The probability $P(w, m)$ obviously depends on the probabilities p and $q = 1-p$ describing the bias of the coin that we flip. We do not include them in the notation $P(w, m)$ because they will always be clear from the context.

Remark 2.4 The definition of $P(w, m)$ is unclear if $w = m = 0$, since we have, at the start of the game, already achieved the required number 0 of heads but we have also already run out of money. We therefore take $P(0, 0)$ to be undefined. In particular, Theorems 3.1 and 4.1 tacitly assume that at least one of w and m is positive.

3 The Pascal Recurrence

3.1 The first formula

In this section, we shall prove (twice) the following formula for the probability $P(w, m)$ defined above.

Theorem 3.1

$$P(w, m) = \sum_{j \geq 0} p^{m+j} q^{w+m-j-1} \left[\binom{w+2m-1}{m+j} - \binom{w+2m-1}{w+m+j} \right].$$

Convention 3.2 Here and throughout this paper, we adopt the convention that binomial coefficients $\binom{n}{k}$ are 0 whenever either (1) $k < 0$ or (2) n is a non-negative integer and $k > n$.

Thus the sum in the theorem is really a finite sum, because large values of j make both of the binomial coefficients vanish.

Remark 3.3 In most of the paper, we follow the fairly standard convention that, for non-negative integers k and arbitrary x (possibly negative, possibly not an integer), the binomial coefficients are given by a polynomial in x,

$$\binom{x}{k} = \frac{x(x-1)\cdots(x-k+1)}{k!}.$$

The only exception is this section. Here it is convenient to adopt instead the alternative convention that $\binom{n}{k} = 0$ for negative integer n and arbitrary integer k. We emphasize that, although these two conventions contradict each other (for negative integer n and non-negative integer k), they are both consistent with Convention 3.2 above. Also note that the formula in Theorem 3.1 means the same with both conventions because negative "numerators" would arise only if $m = w = 0$, and, as indicated in Remark 2.4, $P(w,m)$ is not defined in that situation.

Before proving the theorem, we record some special cases. First, we specialize to $w = 1$.

Corollary 3.4

$$P(1,m) = \sum_{j\geq 0} p^{m+j} q^{m-j} \left[\binom{2m}{m+j} - \binom{2m}{m+j+1} \right].$$

Returning to general w, we specialize instead to fair coins.

Corollary 3.5 *For* $p = q = \frac{1}{2}$,

$$P(w,m) = \left(\frac{1}{2}\right)^{w+2m-1} \sum_{r=m}^{w+m-1} \binom{w+2m-1}{r}.$$

Proof When $p = q = \frac{1}{2}$, the factors $p^{m+j}q^{w+m-j-1}$ in the theorem become $(1/2)^{w+2m-1}$, which is independent of j and so factors out of the sum. The positive terms remaining in the sum are binomial coefficients with "denominators" ranging from m upward. The negative terms have denominators ranging from $w+m$ upward. The negative ones exactly cancel the positive ones except for the first w of the latter. Those w surviving terms are the sum in the corollary. □

Notice that the cancellation in the proof of the corollary would not occur if $p \neq q$, for then the binomial coefficients that should cancel are multiplied by different powers of p and q.

Finally, we specialize to both $w = 1$ and $p = q = \frac{1}{2}$ simultaneously.

Corollary 3.6 *For $p = q = \frac{1}{2}$,*

$$P(1, m) = \left(\frac{1}{2}\right)^{2m} \binom{2m}{m} = \prod_{i=1}^{m} \frac{2i-1}{2i}.$$

Proof The first equality in this corollary comes directly from the preceding corollary; when $w = 1$, the sum there contains only a single term.

For the second equality, write out the binomial coefficient as $(2m)!/(m!)^2$; separate, in the numerator, the odd factors (from 1 to $2m - 1$) from the even factors (from 2 to $2m$); and observe that the product of the even factors is $2^m m!$. □

Recalling that the $P(n)$ of the Droste-Kuske conjecture is, in our present notation, $P(1, n - 1)$ for $p = q = \frac{1}{2}$, we see that the last corollary establishes the conjecture.

We now turn to the proof of the theorem.

3.2 A recurrence relation

When both w and m are positive, we can analyze $P(w, m)$ in terms of the outcome of the first coin flip.

With probability p, this flip is heads. In this case, our wealth increases to $w + 1$, and, in order to obtain a total of m heads before running out of money, we need $m - 1$ more heads in addition to the first one. The probability of getting those additional heads is $P(w + 1, m - 1)$.

On the other hand, with probability q, the first flip is tails, our wealth decreases to $w - 1$, and we still need m heads. The probability of getting those heads is $P(w - 1, m)$.

Therefore,

$$P(w, m) = p \cdot P(w + 1, m - 1) + q \cdot P(w - 1, m) \tag{3.1}$$

when $w, m > 0$. The initial conditions for this recurrence are $P(0, m) = 0$ for $m > 0$ (as we're already out of money at the start of the game) and $P(w, 0) = 1$ for $w > 0$ (as we've already flipped 0 heads at the start of the game). As indicated in Remark 2.4, $P(0, 0)$ is undefined, and it is not needed for the recursion.

We could now complete the proof of Theorem 3.1 by verifying that the formula given there satisfies the recurrence and initial conditions. This would give the theorem a rather ad hoc appearance — the formula just happens to work. So we shall show instead how to deduce the theorem from the recurrence relation.

3.3 Simplifying the recurrence

Plotting the points (w, m), $(w + 1, m - 1)$, and $(w - 1, m)$ at which P is evaluated in the recurrence formula, we see that the last two (coming from the right side of the recurrence) lie on a line of slope $-\frac{1}{2}$, while the first (coming from the left side) lies on the next higher line of that slope passing through integer points. This suggests introducing the variable

$n = w + 2m$ that is constant on lines of slope $-\frac{1}{2}$. We therefore express P in terms of the variables n and m; calling the resulting function F, we define

$$F(n, m) = P(n - 2m, m) \quad \text{or equivalently} \quad P(w, m) = F(w + 2m, m).$$

In terms of the new variables, our recursion simplifies to

$$F(n, m) = p \cdot F(n - 1, m - 1) + q \cdot F(n - 1, m)$$

for $m > 0$ and $n > 2m$. The initial conditions become $F(2m, m) = 0$ for $m > 0$ and $F(n, 0) = 1$ for $n > 0$.

Notice that, except for the factors p and q, the new form of the recurrence looks just like the "Pascal triangle" recurrence for the binomial coefficients. This observation suggests another simplification, designed to remove the factors p and q. Define

$$G(n, m) = \frac{F(n, m)}{p^m q^{n-m}} \quad \text{or equivalently} \quad F(n, m) = p^m q^{n-m} G(n, m).$$

Now the recurrence relation reads

$$G(n, m) = G(n - 1, m - 1) + G(n - 1, m)$$

for $m > 0$ and $n > 2m$, with initial conditions $G(2m, m) = 0$ for $m > 0$ and $G(n, 0) = 1/q^n$ for $n > 0$.

Thus, the function $G(n, m)$ satisfies the same recurrence relation as the binomial coefficients $\binom{n}{m}$ but with different initial conditions.

3.4 Binomial coefficients and their recursion formula

Before proceeding with the calculation, it will be useful to examine the recurrence relation for the binomial coefficients,

$$\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}$$

when n and m are integers, in the light of our convention that binomial coefficients $\binom{n}{m}$ are 0 whenever $m < 0$ or n is a non-negative integer and $m > n$. Recall that in this section we use the additional convention that $\binom{n}{m}$ is 0 when $n < 0$. One easily checks that this convention does no harm to the recurrence formula *except* at $n = m = 0$ where the left side is 1 while the right side is 0. The binomial coefficients $\binom{n}{m}$ can thus be described as the unique function $h(n, m)$ that

- vanishes identically for $n < 0$, and
- satisfies the Pascal recurrence at all $(n, m) \neq (0, 0)$, but
- has a "discrepancy" $h(n, m) - h(n - 1, m - 1) - h(n - 1, m)$ of 1 at $(0, 0)$.

Of course it follows that, for any fixed pair (n_0, m_0) of non-negative integers, the function $\binom{n-n_0}{m-m_0}$ has the same properties listed above but with the discrepancy 1 at (n_0, m_0). It further follows that we can manufacture a function $h(n, m)$ that

- vanishes identically for $n < 0$,
- satisfies the Pascal recurrence at all (n, m) except
- has prescribed discrepancies $h(n, m) - h(n-1, m-1) - h(n-1, m)$ of d_i at prescribed locations (n_i, m_i)

by setting

$$h(n, m) = \sum_i d_i \cdot \binom{n - n_i}{m - m_i}.$$

We shall take advantage of this to express our $G(n, m)$ in terms of binomial coefficients.

3.5 Extending G

Because $P(w, m)$ was defined for w and m non-negative and not both zero, $G(n, m)$ is defined for $n \geq 2m \geq 0$ and not $n = m = 0$. It satisfies the Pascal recurrence in the "interior" of this domain, $n > 2m > 0$. One could, in principle, imagine G as extended by 0's outside its domain of definition, thereby introducing discrepancies at the boundary of the (original) domain. Those discrepancies can be determined from the initial conditions for G, and one could then produce, using the general method outlined above, a formula for G in terms of these discrepancies and binomial coefficients. The resulting formula would be very messy. The extension of G can be chosen much more intelligently, to give nice formulas.

To visualize the following, it helps to think of the pairs (n, m) as arranged in the plane as follows. (This corresponds to one of the standard ways of drawing Pascal's triangle, a way that emphasizes its symmetry.) The pairs with a fixed value of n lie equally spaced in a row, larger values of n being in lower rows and larger values of m being to the right of smaller m. The rows are aligned vertically so that the points $(2m, m)$ lie on a vertical line. Thus, the lines "$m =$ constant" slope downward to the left. (The symmetry of Pascal's triangle is now given by reflection in the vertical center line, the line through the points $(2m, m)$.)

Our G is defined in the left half of the region occupied by (the non-zero part of) Pascal's triangle. Its values are $\frac{1}{q^n}$ along the left side of this region and 0 down the right side (the center line of the Pascal triangle region). The first few rows of G look like (starting with $n = 1$):

$$\begin{array}{ccccccc}
 & & & \frac{1}{q} & & & \\
 & & \frac{1}{q^2} & & 0 & & \\
 & \frac{1}{q^3} & & \frac{1}{q^2} & & & \\
\frac{1}{q^4} & & \frac{1}{q^3} + \frac{1}{q^2} & & 0 & & .
\end{array}$$

There is a very natural way to extend G to the region $0 \le m \le n$ (the same region occupied by Pascal's triangle) by reflecting it in the vertical center line and reversing the signs to the right of the center, thus:

$$\begin{array}{ccccccccc}
 & & & \frac{1}{q} & & -\frac{1}{q} & & & \\
 & & \frac{1}{q^2} & & 0 & & -\frac{1}{q^2} & & \\
 & \frac{1}{q^3} & & \frac{1}{q^2} & & -\frac{1}{q^2} & & -\frac{1}{q^3} & \\
\frac{1}{q^4} & & \frac{1}{q^3}+\frac{1}{q^2} & & 0 & & -\frac{1}{q^3}-\frac{1}{q^2} & & -\frac{1}{q^4}
\end{array} .$$

The point here is that the 0's down the center line now arise from the recurrence. Thus, the recurrence holds for all (n, m) in the region $0 < m < n$, with discrepancies only along the left and right diagonal sides of the triangle (if we extend by 0 outside the triangle). The discrepancies are of the form $\pm(1-q)/q^n$ except when $n = 1$ where they are just $\pm 1/q$. This results in a tolerable formula for G in terms of binomial coefficients, but we can do better by extending G some more.

We extend G to the whole half-plane $n > 0$, including all values for m, even negative ones, in such a way that the Pascal recurrence is satisfied whenever $n > 1$ (for all m), and there are discrepancies only along the line $n = 1$.

There is no choice about how to do such an extension; the values we already have plus the Pascal recurrence force everything. Specifically, we already have the values $1/q^n$ along the left edge of the triangle ($m = 0$). For these to agree with Pascal's recurrence (except at $n = 1$ where a discrepancy is allowed), we must set $G(n-1, -1) = (1/q^n) - (1/q^{n-1}) = (1-q)/q^n$ for $n \ge 2$. And for these values to agree with the Pascal recurrence, we must set $G(n-2, -2) = (1-q)^2/q^n$ for $n \ge 3$. Continuing in this manner, we find that we need

$$G(n-j, -j) = \frac{(1-q)^j}{q^n} \quad \text{for } j \ge 0 \text{ and } n \ge j+1.$$

In particular, taking $n = j + 1$, we have $G(1, -j) = (1-q)^j/q^{j+1}$ for all $j \ge 0$. Symmetrically (with signs reversed) on the right side of the triangle, we want $G(1, j+1) = -(1-q)^j/q^{j+1}$.

Making this extension of G, and finally setting $G(n, m) = 0$ outside the half-plane, i.e., for $n \le 0$, we find that G is a solution of the Pascal recurrence except for discrepancies at the points $(1, m)$; the discrepancy at each such point is the value of G, since Pascal's recurrence would give 0 there (because of the 0's on the line $n = 0$ immediately above).

Plugging these discrepancies and their locations into the general formula above, we get

$$G(n, m) = \sum_{j \ge 0} \frac{(1-q)^j}{q^{j+1}} \left[\binom{n-1}{m+j} - \binom{n-1}{m-j-1} \right].$$

By the symmetry of the binomial coefficients we can replace $\binom{n-1}{m-j-1}$ with $\binom{n-1}{n-m+j}$. Finally, we use the formulas $F(n, m) = p^m q^{n-m} G(n, m)$ and $P(w, m) = F(w + 2m, m)$ (which served to define G and F) to convert our formula for G into one for P. The result is as asserted in the theorem, so the proof is complete.

3.6 Another view of Theorem 3.1

There is another way to understand the formula for $P(w,m)$ given by Theorem 3.1. Let us consider the positive and negative parts of the sum separately.

The positive terms are

$$\sum_{j\geq 0} p^{m+j} q^{w+m-j-1} \binom{w+2m-1}{m+j},$$

and this sum has a simple probabilistic interpretation. Term number j is the probability of getting exactly $m+j$ heads in $w+2m-1$ flips of our coin (whose probabilities of heads and tails are p and q respectively). So the sum is the probability of getting at least m heads in those $w+2m-1$ coin flips. Let us abbreviate this as $\mathrm{Prob}(\geq m \text{ in } w+2m-1)$.

The sum of the negative terms,

$$\sum_{j\geq 0} p^{m+j} q^{w+m-j-1} \binom{w+2m-1}{w+m+j},$$

is a bit more complicated but only by a factor $(q/p)^w$; it is $(q/p)^w$ times the probability $\mathrm{Prob}(\geq w+m \text{ in } w+2m-1)$. So if we multiply the formula for $P(w,m)$ in the theorem by p^w it becomes

$$p^w P(w,m) = p^w \,\mathrm{Prob}(\geq m \text{ in } w+2m-1) - q^w \,\mathrm{Prob}(\geq w+m \text{ in } w+2m-1).$$

Every term here has a probabilistic interpretation, as follows.

By definition, $P(w,m)$ is the probability that, if we play gambler's ruin starting with wealth w, we have at least m successes (heads) before running out of money. Equivalently, it is the probability that in this game we can play for $w+2m-1$ coin flips without (yet) running out of money. So when this is multiplied by p^w, it becomes the probability that, in a sequence of $2w+2m-1$ coin flips, the first w are all heads, and in any nonempty initial segment (including the whole sequence) the number of heads strictly exceeds the number of tails. In gambling terminology, the idea is that we start with 0 money but win the first w flips, building up wealth w, and thereafter play gambler's ruin as before. So the left hand side of the last equation is the total probability of all strings of heads and tails of length $2w+2m-1$ in which the first w items are heads and thereafter the wealth (number of heads minus number of tails, since the beginning of the sequence) remains strictly positive. Call this probability A.

The first term on the right side is the probability that, in a string of length $2w+2m-1$, the first w items are heads and the total number of heads is at least $w+m$. (In this $w+m$, the w comes from the initial factor p^w and the m comes from the Prob factor.) Call this probability B. To say that the total number of heads is at least $w+m$, i.e., a majority of the total number of flips, is just to say that the wealth at the end of the string is positive, but it may have dropped to zero or less at earlier points in the string.

The second term on the right is, similarly, the probability that, in $2w+2m-1$ flips, the first w are tails but at least $w+m$ (again a majority) are heads. Call this probability C.

Our formula, which with all these abbreviations reads simply $A = B - C$, admits the following easy proof, using a version of the reflection principle (attributed to André [1] in [3, page 22]; see also [8, Section 2] for historical information).

Notice that A and B are probabilities of rather similar events, referring to a sequence of $2w + 2m - 1$ flips of the biased coin. In both events, the first w flips are heads and the final wealth is positive. The difference between them is that in A the wealth must remain positive at all times, whereas this is not required in B. So $B - A$ is the probability of the following event: The first w flips are heads, the total wealth is positive at the end, but it was zero (and possibly negative) at least once during the game.

Consider the strings s that constitute this event. In each such string, there is a first point where the wealth was 0, i.e., a shortest nonempty initial segment that contains equally many heads and tails. Let s^* be the string obtained by changing all heads to tails and all tails to heads in this initial segment of s, leaving the remainder of s unchanged. Notice that s^* is a string of the sort that contributes to the probability C; that is, it begins with w tails and ends with positive wealth (the same final wealth that s had).

Furthermore, every string that contributes to C is s^* for a unique s as above. The point here is that the strings involved in C have negative wealth after the first w items but positive wealth at the end, so they have 0 wealth somewhere in between. Take the first such moment and interchange heads with tails at all earlier flips, to get the required s.

Finally, notice that s and s^* have the same probability, because the initial segment where heads and tails were reversed contains equally many of both.

Thus, the strings that contribute to C are in one-to-one correspondence with the strings that contribute to $B - A$, and corresponding strings have the same probability. Therefore $C = B - A$, as the theorem asserts.

4 Catalan Numbers

4.1 The second formula

In this section, we shall prove a rather different-looking formula for $P(w, m)$.

Theorem 4.1

$$P(w, m) = 1 - \sum_{s=0}^{m-1} \frac{w}{w+s} \binom{w+2s-1}{s} p^s q^{w+s}$$

Remark 4.2 When $w = 0$ the term for $s = 0$ in the sum is undefined because it involves $w/(w+s) = 0/0$; we interpret this undefined fraction as 1. This gives $P(0, m)$ the correct value, 0, and it agrees with the arguments to be given in the proof.

As with Theorem 3.1, we give some specializations of this formula before proving it. Recall, from Remark 3.3, that here (and everywhere outside Section 3) we use the convention whereby $\binom{x}{k}$ is a polynomial function of x for every fixed integer k.

Corollary 4.3

$$P(1,m) = 1 - \sum_{s=0}^{m-1} \frac{1}{s+1}\binom{2s}{s} p^s q^{s+1} = 1 - \frac{1}{2p} + \frac{1}{2p}\sum_{t=0}^{m}\binom{\frac{1}{2}}{t}(-4pq)^t.$$

Proof The first equation is just the result of setting $w = 1$ in the theorem. Note that the coefficients occurring here are the Catalan numbers. The second equation results from a well-known identity for the Catalan numbers; for the sake of completeness, we give the proof.

$$\begin{aligned}
\frac{1}{s+1}\binom{2s}{s} &= \frac{(2s)!}{(s+1)!s!} \\
&= \frac{2^{2s} \cdot \frac{1}{2} \cdot 1 \cdot \frac{3}{2} \cdot 2 \cdot \frac{5}{2} \cdots \frac{2s-1}{2} \cdot s}{(s+1)!s!} \\
&= \frac{2^{2s} \cdot \frac{1}{2} \cdot \frac{3}{2} \cdot \frac{5}{2} \cdots \frac{2s-1}{2}}{(s+1)!} \\
&= \frac{2^{2s+1}(-1)^s \frac{1}{2} \cdot \frac{-1}{2} \cdot \frac{-3}{2} \cdot \frac{-5}{2} \cdots \frac{-(2s-1)}{2}}{(s+1)!} \\
&= 2^{2s+1}(-1)^s \binom{\frac{1}{2}}{s+1}.
\end{aligned}$$

Inserting this formula into the expression for $P(w,m)$, changing the summation variable from s to $t = s+1$ (which ranges from 1 to m), and adding and subtracting $1/(2p)$, which corresponds to $t = 0$, we get the second equation in the corollary. □

Returning to general w but specializing to fair coins, we get the following formula by substituting in the theorem.

Corollary 4.4 *For* $p = q = \frac{1}{2}$,

$$P(w,m) = 1 - \sum_{s=0}^{m-1} \frac{w}{w+s}\binom{w+2s-1}{s}\left(\frac{1}{2}\right)^{w+2s}.$$

Finally, doing both specializations together, we obtain the following formula by substituting in Corollary 4.3.

Corollary 4.5 *For* $p = q = \frac{1}{2}$,

$$P(1,m) = 1 - \sum_{s=0}^{m-1} \frac{1}{s+1}\binom{2s}{s}\left(\frac{1}{2}\right)^{2s+1} = \sum_{t=0}^{m}(-1)^t\binom{\frac{1}{2}}{t}.$$

To obtain the conjecture of Droste and Kuske from this result, we need the following well-known formula.

Lemma 4.6 *For any x and any positive integer m,*

$$\sum_{t=0}^{m}(-1)^t\binom{x}{t} = (-1)^m\binom{x-1}{m}.$$

Proof Since both sides of the formula to be proved are polynomials in x, it suffices to verify the formula when x is an integer larger than m. In this case, the left side of the equation counts the number of even-sized subsets minus the number of odd-sized subsets, all of size $\leq m$, in the set $\{1, 2, \ldots x\}$. There is almost a one-to-one correspondence between the even and odd sets, namely, delete the element 1 from any set that contains it and insert it into any set that doesn't contain it. This would be a bijection, were it not for the bound of m on the size of the sets. When a set has size m and doesn't contain 1, then inserting 1 would make it too big. Thus, all the sets are paired off, making a net contribution of zero, except for the sets of size m that don't contain 1. There are $\binom{x-1}{m}$ of these sets, and each contributes $(-1)^m$. □

According to the lemma, the formula in the last corollary simplifies as follows.

Corollary 4.7 *For $p = q = \frac{1}{2}$,*

$$P(1, m) = (-1)^m\binom{-\frac{1}{2}}{m} = \prod_{i=1}^{m}\frac{2i-1}{2i}.$$

Proof The first equation comes from the preceding corollary and lemma. The second comes from writing out the definition of the binomial coefficient and simplifying. □

4.2 Strings of parentheses

We now turn to the proof of Theorem 4.1. As the form "$1 - \ldots$" of the formula in the theorem suggests, we are interested here in the probability complementary to $P(w, m)$, i.e., the probability that, playing gambler's ruin with initial wealth w, we run out of money *before* obtaining m heads.

Consider therefore a play of the game in which we finish with no money. The record of such a play can be conveniently represented by a string of parentheses as follows.

- Start with w left parentheses, representing the w euros we have at the beginning of the game.
- At each successful flip (heads), append a left parenthesis to the string, representing the euro we won.
- At each unsuccessful flip(tails), append a right parenthesis to the string, representing the loss of a euro.

Since we continued playing until we ran out of money (and no longer), there are equally many left and right parentheses in the string, but there are strictly more left than right parentheses in each nonempty, proper, initial segment. This means that the parentheses can be paired off in the usual way — each right parenthesis matches with an earlier left one, and all parentheses between a matched pair are matched with each other, not with parentheses outside the pair — and the first parenthesis is matched with the last.

The formula for the number of such parenthesis strings of any given length is well known (see [8, Section 2] for its history), but for the sake of completeness we indicate a proof. For the sake of variety, we give a proof that does not use the reflection principle; the method is related to the proof of the Lagrange inversion formula in [5]. (A proof using the reflection principle is given in [7, Solution to Exercise 6.20].)

Lemma 4.8 *For integers $l \geq w \geq 0$, let X be the number of strings consisting of l left and l right parentheses, starting with w consecutive left parentheses, and having the property that every nonempty, proper, initial segment has strictly more left than right parentheses. Then*

$$X = \frac{w}{2l-w}\binom{2l-w}{l}.$$

When $w = l = 0$, the undefined fraction $w/(2l-w)$ is to be interpreted as 1, since this gives the correct value $X = 1$, corresponding to the empty string of parentheses.

Proof of Lemma Consider first the set S consisting of strings of $l-w$ left and l right parentheses such that, when an additional w left parentheses are added at the beginning, the resulting string is as described in the statement of the lemma. Let S' be the set of "marked strings" from S, meaning a string from S supplemented with a mark, either between two of its parentheses or at the very end. Since $|S| = X$ and since each string, having length $2l-w$, can be marked in any of $2l-w$ places, we have $|S'| = (2l-w)X$.

Now consider the set T of arbitrary strings of $l-w$ left and l right parentheses, and the set T' of well-marked strings from T. Here "well-marked" means marked (as above) in such a way that, if we insert w left parentheses at the mark and then cyclically permute the resulting string so that these parentheses are at the beginning, the resulting string is as described in the lemma. (Formally, with $\frown$ denoting concatenation of strings and $(^w$ denoting a string of w left parentheses, if a marked string is $u\frown v$ with the mark between u and v, then it is well-marked if $(^w\frown v\frown u$ is as described in the lemma.)

Notice that there is a simple one-to-one correspondence between S' and T'. Given any marked string in either set, cyclically permute it so that its mark is moved to the end, and move the mark to where the string originally ended. Thus, $|T'| = (2l-w)X$.

But $|T'|$ can also be evaluated another way. Obviously, $|T| = \binom{2l-w}{l}$. It remains to compute how many well-markings a string from T has, i.e., how many elements it contributes to T'.

So consider an arbitrary string $s \in T$, and imagine writing, after each initial segment, the number of left minus right parentheses in that segment. So this count starts at 0 (for the empty segment) increases (or decreases) by 1 at each left (or right, respectively) parenthesis, and ends at $-w$ because s has l right and only $l-w$ left parentheses. (In gambling terminology, this count is just our wealth after the coin flips corresponding to the initial segment, assuming that we start with no money. In contrast to the gambler's ruin game, here our wealth can become negative.)

Let $-z$ be the smallest (the most negative) value attained by the count at any point in the string s. Note that $-z \le -w$ because the count is $-w$ at the end. Let $-y$ be any integer in the range from $-z$ to $-z+w-1$, i.e., one of the w smallest counts. (Since counts change by only ± 1 at each step, all counts between 0 and $-z$ must occur.) Consider putting a mark at the first place where $-y$ occurs, say between substrings u and v in $s = u^\frown v$. We claim that this is a well-marking, i.e., that in $(^{w\frown} v^\frown u$ every nonempty, proper, initial segment has more left than right parentheses. For initial segments that end before the start of v this is obvious, as there are only left parentheses there. For those that end in v or at the end of v, the count in $(^{w\frown} v^\frown u$ is $y+w$ plus the count at the corresponding place in $s = u^\frown v$. This follows from the fact that the count at the beginning of v is w in $(^{w\frown} v^\frown u$ and $-y$ in s. Since the count in s never drops below $-z$, we find that the count in the v part of $(^{w\frown} v^\frown u$ never drops below $y+w-z$. And this is positive because we chose y with $-y \le -z+w-1$, i.e., $1 \le y+w-z$.

Before looking at the counts occurring in the u part of $(^{w\frown} v^\frown u$, observe that, in s, the count was $-y$ at the beginning of v and $-w$ at the end, so v contributed $-w+y$ to the count. Thus, in $(^{w\frown} v^\frown u$, the part preceding u contributes y, and therefore the count at any point in u is y plus the count at the corresponding place in the u part of s. Those counts in s never get as low as $-y$ until we reach the end of u. This is because we placed the mark in s at the *first* place where the count reached $-y$. Therefore, the counts in the u part of $(^{w\frown} v^\frown u$ never get as low as 0 until we reach the end.

This completes the proof that, for any $-y$ in the specified range, we get a well-marking of s. Furthermore, these are the only well-markings of s. Indeed, if we put the mark at the second or later place where the count reaches a certain $-y$, then, arguing as above, we would find that the count in $(^{w\frown} v^\frown u$ reaches 0 somewhere in u, not only at the end; in fact, it would reach 0 at the places where $-y$ previously occurred in s. Also, if we put the mark at the first place in s where the count is $-y$ but $-y$ is not in the specified range, i.e., $-y \ge -z+w$, then the v part of the argument above would fail, and the count in $(^{w\frown} v^\frown u$ would drop to 0 somewhere in v, namely at the place where the count in s reached $-z$. (This place is in v, not in u, because we marked the first occurrence of $-y$, and the count must reach $-y$ before it can descend further to $-z$.)

Thus, there is exactly one well-marking of s for each y in the specified range. Since that range has size w, each element of T gives rise to w elements of T'. Therefore

$$|T'| = w\binom{2l-w}{l}.$$

Comparing with the previous observation that $|T'| = (2l-w)X$, we obtain the lemma. $\square$

We are interested in the probability that the game of gambler's ruin has fewer than m successful flips (heads), which means that the corresponding string of parentheses has fewer than $w+m$ left parentheses (and, of course, equally many right parentheses). Writing s for the number of successful flips, we want the probability that $s < m$.

For any fixed s, the number of parenthesis strings of the relevant sort is, by the lemma with $l = w + s$, and by a trivial manipulation of binomial coefficients,

$$\frac{w}{w+2s}\binom{w+2s}{w+s} = \frac{w}{w+s}\binom{w+2s-1}{s}.$$

(As in the lemma, this is to be interpreted as 1 when $w = s = 0$.) The probability of any particular one of these strings arising in the game is $p^s q^{w+s}$, because, apart from the initial w left parentheses representing the initial wealth, there are s left and $w + s$ right parentheses arising from the coin flips during the game.

Thus, the probability that we have exactly s successful coin flips before we run out of money is

$$\frac{w}{w+s}\binom{w+2s-1}{s}p^s q^{w+s}.$$

Summing over all $s < m$, we obtain the sum in the theorem representing the probability of getting fewer than m successful flips before running out of money.

5 Generating Functions

The power series known as generating functions provide an efficient tool for solving recursions. In this section, we demonstrate their use by applying them to the recursion (3.1) for the probabilities $P(w, m)$. We thereby obtain another proof of the formula in Theorem 4.1.

5.1 Review of power series

The idea behind generating functions is as follows. To compute some numbers for which we have recursion equations, we introduce a power series having those numbers as its coefficients. The recursion equations give us equations (perhaps algebraic equations, perhaps differential equations) satisfied by this power series. We solve those equations by algebraic or analytic methods, and then, knowing the power series, determine the coefficients, the numbers we wanted in the first place. See [3, Sections 1.12 and 1.13], [7, Chapters 4 and 6], or [9, Chapter 2] for a very thorough treatment of this topic.

In general, the power series that occur as generating functions are *formal* power series. That is, they need not converge for any non-zero values of the variables, and even if they do, it may not be easy to prove it since the coefficients are unknown quantities. Nevertheless, checking the convergence is not required in most cases, because, as explained carefully in [3], [7], or [9, page 30], one can apply the usual methods of algebra and analysis to them. These are usually enough to solve the algebraic or differential equations that arise from the recursion conditions.

In our application, however, we can easily see that all the power series that we encounter are convergent before starting calculations with the series. Thus, we do not need any of the theory of formal power series; our series can be treated as ordinary, convergent power series of certain analytic functions defined near the origin. Nevertheless, we present our arguments in a form that can be read with either formal or convergent power series in mind.

In particular, our series can be evaluated at small values of the variables. This also enables us to substitute series with zero constant terms for the variables. The reader who prefers the formal power series approach should note that our substitutions are legitimate in this context as well.

We shall need the power series of two particular analytic functions:

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n,$$

$$\left(\frac{2}{1+\sqrt{1-4x}}\right)^k = \left(\frac{1-\sqrt{1-4x}}{2x}\right)^k = \sum_{n=0}^{\infty} \frac{k}{n+k}\binom{2n+k-1}{n} x^n, \quad k > 0. \tag{5.1}$$

The first of these is, of course, well known. The second is also well known; it appears in [9, Section 2.5, proof on page 170] or [5, p. 1034].

5.2 From recursion to power series

We apply the method of generating functions to compute $P(w,m)$ by solving the recursion equation (3.1), which, for convenience, we repeat here along with its initial conditions.

$$\begin{aligned} P(0,m) &= 0, & m &> 0, \\ P(w,0) &= 1, & w &> 0, \\ P(w,m) &= p \cdot P(w+1, m-1) + q \cdot P(w-1, m), & m, w &> 0. \end{aligned} \tag{5.2}$$

The first step is to combine the infinitely many unknowns, $P(w,m)$ for all w and m into one power series f, having these unknowns as its coefficients.

$$f = f(x,y) := \sum_{m=0,w=1}^{\infty} P(w,m) x^m y^{w-1}.$$

That the summation begins at $w = 1$ rather than $w = 0$ makes no difference because of the initial condition $P(0,m) = 0$. That the exponent of y is $w-1$ rather than w is just a technical convenience.

We observe that, as promised earlier, the power series $f(x,y)$ converges whenever $|x| < 1$ and $|y| < 1$. This is because probabilities are never larger than 1, so our power series is majorized, term for term, by the convergent series $\sum |x|^m |y|^{w-1}$. As remarked earlier, this convergence check is not needed in the formal approach.

The recursion conditions can be converted into an equation about the power series. Just multiply both sides of (5.2) by $x^m y^{w-1}$ and sum over all positive values of m and w.

The result is

$$\underbrace{\sum_{m,w>0} P(w,m)x^m y^{w-1}}_{A} = p \underbrace{\sum_{m,w>0} P(w+1,m-1)x^m y^{w-1}}_{B} + q \underbrace{\sum_{m,w>0} P(w-1,m)x^m y^{w-1}}_{C}. \tag{5.3}$$

At first sight this might look horrible, but we can express all three sums in terms of f:

$$A = f - \sum_{w=1}^{\infty} P(w,0)y^{w-1} = f - \frac{1}{1-y}, \tag{5.4}$$

$$B = \frac{x}{y}\left(f - \underbrace{\sum_{m=0}^{\infty} P(1,m)x^m}_{g} \right), \tag{5.5}$$

$$C = y\left(f - \sum_{w=1}^{\infty} P(w,0)y^{w-1} \right) + \underbrace{\sum_{m=1}^{\infty} P(0,m)x^m}_{0} = y\left(f - \frac{1}{1-y} \right). \tag{5.6}$$

Hence equation (5.3) for f becomes a simple one:

$$f - \frac{1}{1-y} = p\frac{x}{y}(f-g) + qy\left(f - \frac{1}{1-y} \right). \tag{5.7}$$

Here $g = g(x)$ is the power series introduced in (5.5).

It remains to solve equation (5.7) for f and g and then to extract the coefficients $P(w,m)$. Notice, by the way, that although the general problem of computing $P(w,m)$ amounts to computing f, the special case relevant to the conjecture of Droste and Kuske, where $w = 1$, amounts to computing g.

5.3 Solving the power series equation

We can rearrange our equation into a more convenient form by multiplying by y, transposing some terms, and subtracting $px/(1-y)$ from both sides to obtain

$$(qy^2 - y + px)\left(f - \frac{1}{1-y} \right) = px\left(g - \frac{1}{1-y} \right). \tag{5.8}$$

Unfortunately, we have two unknown quantities in this equation, g and f. We know, however, that the variable y does not occur in g. Therefore we can compute g by substituting into our equation a suitable value of y which makes the coefficient of f zero.

The coefficient of f is a quadratic polynomial of y, which we factor as

$$qy^2 - y + px = q(y - \alpha_+)(y - \alpha_-) \tag{5.9}$$

where

$$\alpha_+ = \alpha_+(x) := \frac{1 + \sqrt{1 - 4pqx}}{2q}, \tag{5.10}$$

$$\alpha_- = \alpha_-(x) := \frac{1 - \sqrt{1 - 4pqx}}{2q}. \tag{5.11}$$

Note that the constant term of α_- is zero. This means (from the viewpoint of both formal and convergent series) that we can substitute $\alpha_-(x)$ for y in (5.8) to obtain

$$g = \frac{1}{1 - \alpha_-}. \tag{5.12}$$

Let us plug (5.9) and (5.12) into (5.8). The result is

$$\begin{aligned} q(y - \alpha_+)(y - \alpha_-)\left(f - \frac{1}{1-y}\right) &= px\left(\frac{1}{1-\alpha_-} - \frac{1}{1-y}\right) \\ &= -px\frac{y - \alpha_-}{(1-\alpha_-)(1-y)}. \end{aligned}$$

We can solve this for f.

$$\begin{aligned} f - \frac{1}{1-y} &= \frac{px}{q(1-\alpha_-)} \cdot \frac{1}{1-y} \cdot \frac{1}{\alpha_+ - y} \\ &= \frac{px}{q(1-\alpha_-)(1-\alpha_+)} \cdot \left(\frac{1}{\alpha_+ - y} - \frac{1}{1-y}\right) \\ &= \frac{px}{p(x-1)} \sum_{w=0}^{\infty} \left(1/\alpha_+^{w+1} - 1\right) y^w, \end{aligned} \tag{5.13}$$

where in the last equation we used

$$q(1-\alpha_-)(1-\alpha_+) = q - 1 + px = p(x-1), \tag{5.14}$$

which follows from (5.9) by substituting $y = 1$.

We express both ends of (5.13) as a power series in y.

$$\sum_{m=0,w=1}^{\infty} P(w,m)x^m y^{w-1} - \sum_{w=0}^{\infty} y^w = \frac{x}{1-x} \sum_{w=0}^{\infty} \left(1 - \frac{1}{\alpha_+^{w+1}}\right) y^w. \tag{5.15}$$

Comparing the coefficients of y^{w-1} gives

$$\sum_{m=0}^{\infty} P(w,m)x^m - 1 = \frac{x}{1-x}\left(1 - \frac{1}{\alpha_+^w}\right), \quad w > 0. \tag{5.16}$$

To go further, we evaluate the power series of $1/\alpha_+^w$ using (5.10) and (5.1).

$$\frac{1}{\alpha_+^w} = q^w \sum_{n=0}^{\infty} \frac{w}{n+w} \binom{2n+w-1}{n} (pqx)^n. \tag{5.17}$$

We plug this into (5.16); the result is

$$\begin{aligned}\sum_{m=0}^{\infty} P(w,m)x^m - 1 &= \left(\sum_{m=1}^{\infty} x^m\right)\left(1 - q^w \sum_{n=0}^{\infty} \frac{w}{n+w}\binom{2n+w-1}{n}(pqx)^n\right) \\ &= \sum_{m=1}^{\infty}\left(1 - \sum_{n=0}^{m-1} \frac{w}{n+w}\binom{2n+w-1}{n} p^n q^{n+w}\right) x^m.\end{aligned}$$

Comparing coefficients gives the formula for $P(w,m)$ in Theorem 4.1. Thus, generating functions have provided another proof of this theorem.

6 Additional Remarks

6.1 The formulas as polynomials

In the preceding sections, the probabilities p and q of heads and tails have been fixed, except for occasional specializations to $\frac{1}{2}$. We now look at our formulas for $P(w,m)$ as functions of p and q, or as functions of just one of these, since we can eliminate either variable using $p+q=1$. Either of our formulas, Theorem 3.1 or Theorem 4.1, shows that $P(w,m)$ is a polynomial function, but the nature of these polynomials looks rather different in the two formulas.

Consider the formulas first as polynomials in p, by replacing every q with $1-p$. In Theorem 3.1, the lowest power of p that occurs is p^m, occurring in the $j=0$ term when we take the term in $q^{w+m-1} = (1-p)^{w+m-1}$ that doesn't involve p. In contrast, the sum in Theorem 4.1 involves powers of p all the way down to a constant term. The constant term is 1 and cancels the 1 that is written explicitly in the formula. But the terms of degrees 1 through $m-1$ must cancel in order that the two formulas agree.

Similarly, the highest power of p that occurs in Theorem 3.1 is p^{w+2m-1}; it occurs in every term of the sum, as $q^{w+m-j-1}$ contains, when q is replaced by $1-p$, a term $p^{w+m-j-1}$. In contrast, the highest power of p that occurs in Theorem 4.1 is p^{w+2m-2}, occurring in the term of the sum with $s=m-1$. So the highest degree terms (with respect to p) in Theorem 3.1 must cancel.

Next, consider the same two formulas as polynomials in q, replacing every p with $1-q$. Now the formula in Theorem 3.1 involves powers of q from q^{w+2m-1} all the way down to a constant term. (To see the latter, notice that j can be as large as $w+m-1$ before both the binomial coefficients in the formula vanish.) In the formula from Theorem 4.1, there is a constant term, the 1 that was written separately from the sum over s, but apart from this term, all the others have q with an exponent of at least w. Furthermore, the highest power of q that occurs in the sum is q^{w+2m-2}, occurring when $s = m-1$. We conclude that, in the formula of Theorem 3.1, written in terms of q, the term of degree $w+2m-1$ and all the terms of degrees from 1 to $w-1$ must vanish.

It is interesting that $P(w,m)/p^m$ as a polynomial in q has only positive coefficients; we shall prove this in Subsection 6.3.

All the cancellations just described follow from the fact that Theorems 3.1 and 4.1 describe the same $P(w,m)$, so the two formulas must agree. In addition, we shall show directly, in Subsection 6.2, that the formulas are equal. We therefore omit here any direct verifications for most of the asserted cancellations.

One of the cancellations, however, is useful in motivating part of the calculation in Subsection 6.2, so we verify it directly here. This is the cancellation of the top degree terms in Theorem 3.1 when expressed in terms of p. Since terms of the top degree, $w+2m-1$, arise from taking the highest power of p in each of the factors $(1-p)^{w+m-j-1}$ that arise when q is replaced with $1-p$, we see that the coefficient of p^{w+2m-1} in Theorem 3.1 is

$$\sum_{j\geq 0}(-1)^{w+m-j-1}\left[\binom{w+2m-1}{m+j}-\binom{w+2m-1}{m-j-1}\right],$$

where in the second binomial coefficient we have used the symmetry property of binomial coefficients to replace $\binom{w+2m-1}{w+m+j}$. The positive terms here include all binomial coefficients $\binom{w+2m-1}{r}$ with $r \geq m$ (because $j \geq 0$) multiplied by $(-1)^{w+r-2j-1} = (-1)^{w+r-1}$ since $r = m+j$. The negative terms include all binomial coefficients $\binom{w+2m-1}{r}$ with $r < m$ (because $j \geq 0$) multiplied by $(-1)^{w+r}$ since $r = m-j-1$. Subtracting the negative terms from the positive terms, we get the sum over all r

$$\sum_{r}(-1)^{w+r-1}\binom{w+2m-1}{r} = 0,$$

since the alternating sum of all binomial coefficients with a fixed numerator vanishes.

We mention two consequences of the observations above about the degrees of terms in our formulas for $P(w,m)$. First, when $P(w,m)$ is expressed in terms of q, it is divisible by $(1-q)^m$. This is because, as we saw from Theorem 3.1, as a polynomial in p, its lowest degree is m and so it is divisible by p^m. Second, using the fact that the lowest degree in Theorem 4.1 with respect to q, except for the constant term, is w, we find that $1-P(w,m)$ is, when expressed in terms of p, divisible by $(1-p)^w$.

We do not have an interpretation of the factors that remain when $P(w,m)$ is divided by $(1-q)^m$ as a polynomial in q or when $1-P(w,m)$ is divided by $(1-p)^w$ as a polynomial in p.

6.2 The formulas agree

This subsection is devoted to a direct computation showing that the formulas in Theorems 3.1 and 4.1 agree. For convenience, we repeat the formulas here and give them different names so that we can refer to them without confusion:

$$Q(w,m) := \sum_{j\ge 0} p^{m+j} q^{w+m-j-1} \left[\binom{w+2m-1}{m+j} - \binom{w+2m-1}{w+m+j} \right], \tag{6.1}$$

$$R(w,m) := 1 - \sum_{s=0}^{m-1} \frac{w}{w+s} \binom{w+2s-1}{s} p^s q^{w+s}. \tag{6.2}$$

To prove that $Q(w,m) = R(w,m)$ for all w and m, we shall first check that this equation holds when $m = 0$ and then show that $Q(w,m) - Q(w,m+1) = R(w,m) - R(w,m+1)$ for all w and m. The desired conclusion will obviously follow by induction.

To prove $Q(w,0) = R(w,0)$, notice that, since $\binom{w-1}{w+j} = 0$ by Convention 3.2, we have

$$Q(w,0) = \sum_{j\ge 0} p^j q^{w-1-j} \binom{w-1}{j} = (p+q)^{w-1} = 1.$$

We obviously have $R(w,0) = 1$ because the sum is empty.

Turning to the proof of $Q(w,m) - Q(w,m+1) = R(w,m) - R(w,m+1)$, we first observe that the right side is very easy to evaluate, since the only effect m has on formula (6.2) is the upper limit of the sum. So the difference is

$$R(w,m) - R(w,m+1) = \frac{w}{w+m} \binom{w+2m-1}{m} p^m q^{w+m}. \tag{6.3}$$

It remains to treat the left side of the desired equation.

We want the equation to hold when the variables p and q are related, as usual, by $p + q = 1$. Equivalently, we can regard p and q as independent variables and show that the difference $Q(w,m) - Q(w,m+1) - (R(w,m) - R(w,m+1))$ is divisible by $p + q - 1$. If this difference were homogeneous, then our task would be equivalent to showing that the difference vanishes identically (with p and q independent). But in fact, the difference is not quite homogeneous. The first term, $Q(w,m)$, has total degree $w + 2m - 1$; the second term, $Q(w,m+1)$, has total degree $w + 2m + 1$; and the last part has, according to (6.3), total degree $w + 2m$, midway between the others.

A way to simplify this situation is suggested by our calculation in Subsection 6.1, where we showed that the terms of highest degree in Theorem 3.1 vanish when the formula is expressed as a polynomial in p. Recall that in this calculation, we first replaced q by $1-p$ and then kept, in each expression of the form $q^k = (1-p)^k$, only the p^k term, because this is the only contribution to the highest power of p in the formula. To keep only the p^k term means that we effectively replaced q not by $1-p$ but by $-p$. The calculation showed that the result of this replacement vanishes identically. That means that the formula in Theorem 3.1, which we are currently calling $Q(w,m)$, is, when regarded as a polynomial in independent variables p and q, divisible by $p + q$, for it vanishes when $p + q = 0$. Of course, since m is arbitrary, $Q(w,m+1)$ is also divisible by $p+q$. Dividing it by $p+q$, we bring its total degree down to $w+2m$, which matches the degree of $R(w,m)-R(w,m+1)$.

Explicitly, we have

$$Q(w,m+1) = (p+q)\sum_{j\ge 0}\left[\binom{w+2m}{m+j+1} - \binom{w+2m}{m-j-1}\right]p^{m+j+1}q^{w+m-j-1}. \qquad (6.4)$$

To check this, simply multiply the sum by p and by q, and combine the $j-1$ term of the first product with the j term of the second. The Pascal recurrence for the binomial coefficients then immediately gives formula (6.1).

As long as we are interested in what happens for $p+q=1$, we may as well divide $Q(w,m+1)$ by $p+q$, bringing our desired equation a little closer to being homogeneous.

We can finish homogenizing our equation by multiplying the low-degree term, $Q(w,m)$, by $p+q$. First we multiply $Q(w,m)$ from (6.1) with p and q separately:

$$pQ(w,m) = \sum_{j\ge 1} p^{m+j}q^{w+m-j}\left[\binom{w+2m-1}{m+j-1} - \binom{w+2m-1}{m-j}\right],$$

where we have changed the summation variable, the new j being the old $j+1$;

$$qQ(w,m) = \sum_{j\ge 0} p^{m+j}q^{w+m-j}\left[\binom{w+2m-1}{m+j} - \binom{w+2m-1}{m-j-1}\right].$$

Adding the two results and using the Pascal recurrence for the binomial coefficients when $j\ge 1$, we get

$$\begin{aligned}(p+q)Q(w,m) = \sum_{j\ge 1} p^{m+j}q^{w+m-j}\left[\binom{w+2m}{m+j} - \binom{w+2m}{m-j}\right] + \\ + p^m q^{w+m}\left[\binom{w+2m-1}{m} - \binom{w+2m-1}{m-1}\right], \qquad (6.5)\end{aligned}$$

where the last term comes from the $j=0$ term in the sum expressing $qQ(w,m)$, a term unmatched in the other sum.

Comparing the last formula with (6.4), we find that the big sums in the two formulas differ by only a change in the summation variable, and hence

$$(p+q)Q(w,m) - \frac{Q(w,m+1)}{p+q} = p^m q^{w+m}\left[\binom{w+2m-1}{m} - \binom{w+2m-1}{m-1}\right].$$

We can simplify this by using the fact, immediate when one writes out the binomial coefficients in terms of factorials, that

$$\binom{w+2m-1}{m-1} = \frac{m}{w+m}\binom{w+2m-1}{m}.$$

Thus

$$\binom{w+2m-1}{m} - \binom{w+2m-1}{m-1} = \frac{w}{w+m}\binom{w+2m-1}{m},$$

and therefore

$$(p+q)Q(w,m) - \frac{Q(w,m+1)}{p+q} = p^m q^{w+m} \frac{w}{w+m} \binom{w+2m-1}{m}.$$

Since this agrees with $R(w,m) - R(w,m+1)$ by (6.3), the proof of the equivalence of the two formulas is complete.

6.3 Positive coefficients

In this subsection we prove that the coefficients of $P(w,m)/p^m$ as a polynomial in q are positive. We already know that the polynomial $P(w,m)$ is divisible by p^m and hence $P(w,m)/p^m$ is a polynomial. We also know that its degree is at most $w+m-2$. We show that the coefficient of q^i is a positive integer for $i \le w+m-2$. This will also illustrate the usefulness of power series in the style of Section 5.

To consider $P(w,m)/p^m$, it is convenient to introduce a new variable $z := px$ instead of x since this makes the coefficients of $z^m y^{w-1}$ in the power series f of Section 5 to be $P(w,m)/p^m$. We are aiming for an expression of f in which p does not appear, only q, z and y, and where the coefficients are obviously positive. A good starting point is the first line of (5.13), which we can write in the form:

$$\begin{aligned}\sum_{m=0,w=1}^{\infty} \frac{P(w,m)}{p^m} z^m y^{w-1} - \frac{1}{1-y} &= \frac{z}{q(1-\alpha_-)} \cdot \frac{1}{1-y} \cdot \frac{1}{\alpha_+ - y} = \\ &= z \left(\sum_{i=0}^{\infty} \alpha_-^i \right) \left(\sum_{i=0}^{\infty} y^i \right) \left(\sum_{j=0}^{\infty} \frac{y^j}{q\alpha_+^{j+1}} \right). \qquad (6.6)\end{aligned}$$

Let us carefully examine the right-hand side to see that there are no occurrences of p and no negative coefficients. Note that p does not appear, not even hidden in α_+ or α_-, because

$$\alpha_\pm = \frac{1 \pm \sqrt{1-4pqx}}{2q} = \frac{1 \pm \sqrt{1-4qz}}{2q}.$$

Now we can easily express the powers of α_+ and α_- similarly to (5.17):

$$\frac{\alpha_-^w}{z^w} = \frac{1}{(q\alpha_+)^w} = \sum_{n=0}^{\infty} \frac{w}{n+w} \binom{2n+w-1}{n} (qz)^n \quad w > 0. \qquad (6.7)$$

The right-hand side of (6.6) is a product of three sums. Every summand of the sums is a sum of monomials $q^i z^m y^w$ with positive integer coefficients. Hence if we multiply out the product and collect like terms then the coefficient of each $q^i z^m y^{w-1}$ will be a sum of products of positive integers. If $m > 0$ then the sum will be non-void (and hence a positive integer) if and only if $i \le m+w-2$. Thus comparing both sides of (6.6) gives that $P(w,m)/p^m$ is a polynomial in q with degree $m+w-2$ and all powers of q have positive integer coefficients.

References

[1] Désiré André, "Solution directe du problème résolu par M. Bertrand," *C. R. Acad. Sci. Paris* 105 (1887) 436–437.

[2] Béla Bollobás, *Random Graphs*, Cambridge Studies in Advanced Mathematics, 73. Cambridge University Press (2001).

[3] Louis Comtet, *Advanced Combinatorics*, Reidel (1974).

[4] Manfred Droste and Dietrich Kuske, "On random relational structures," *J. Combin. Theory Ser. A* 102 (2003) 241–254.

[5] Ira M. Gessel and Richard P. Stanley, "Algebraic Enumeration," Chapter 21 in *Handbook of Combinatorics*, Vol. 2, R. L. Graham, M. Grötschel, and L. Lovász (eds.), Elsevier (1995), pages 1021–1061.

[6] Charles M. Grinstead and J. Laurie Snell, *Introduction to Probability*, American Mathematical Society (1997). http://www.dartmouth.edu/~chance/teaching_aids/books_articles/probability_book/book.html

[7] Richard Stanley, *Enumerative Combinatorics*, Vol. 1, Wadsworth & Brooks/Cole Mathematics Series (1986), reprinted in Cambridge Studies in Advanced Mathematics 49 (1997), and Vol. 2, Cambridge Studies in Advanced Mathematics 62 (1999).

[8] Lajos Takács, *Combinatorial Methods in the Theory of Stochastic Processes*, Wiley (1967).

[9] Herbert S. Wilf, *generatingfunctionology*, second ed., Academic Press Inc., Boston, MA, (1994). http://www.math.upenn.edu/~wilf/DownldGF.html