THE ART OF
COMPUTER PROGRAMMING
VOLUME 4 PRE-FASCICLE 5A

MATHEMATICAL
PRELIMINARIES
REDUX

DONALD E. KNUTH Stanford University

ADDISON–WESLEY
May 20, 2015

Note to readers:
Please ignore these
sidemarks; they’re just
hints to myself for
preparing the index,
and they’re often flaky!

KNUTH
**PREFACE**

*We— or the Black Chamber— have a little agreement with [Knuth]: he doesn’t publish the real Volume 4 of The Art of Computer Programming, and they don’t render him metabolically challenged.*


This booklet contains draft material that I’m circulating to experts in the field, in hopes that they can help remove its most egregious errors before too many other people see it. I am also, however, posting it on the Internet for courageous and/or random readers who don’t mind the risk of reading a few pages that have not yet reached a very mature state. *Beware:* This material has not yet been proofread as thoroughly as the manuscripts of Volumes 1, 2, 3, and 4A were at the time of their first printings. And those carefully-checked volumes, alas, were subsequently found to contain thousands of mistakes.

Given this caveat, I hope that my errors this time will not be so numerous and/or obtrusive that you will be discouraged from reading the material carefully. I did try to make the text both interesting and authoritative, as far as it goes. But the field is vast; I cannot hope to have surrounded it enough to corral it completely. So I beg you to let me know about any deficiencies that you discover.

To put the material in context, this pre-fascicle contains an exposition of mathematical material (mostly about probability theory) that I plan to include at the beginning of Volume 4B. Its *mison d’être* is explained below, in an excerpt from the preface to that volume.

* * *

Probability theory has made huge strides since I “completed” my college education in 1963; hence I’m basically self-taught with respect to these new-fangled ideas, and I fear that in many respects my knowledge lags behind that of today’s students. I’ve tried my best to get the story right, yet I fear that in many respects I’m woefully ignorant.

For example, I urgently need your help with respect to some exercises that I made up as I was preparing this material. I certainly don’t like to receive credit for things that have already been published by others, and most of these results are quite natural “fruits” that were just waiting to be “plucked.” Therefore please tell me if you know who deserves to be credited, with respect to the ideas found in exercises 6, 8, 9, 19, 32, 33, 38, 73, 88, or 96.

May 20, 2015
Special thanks are due to Persi Diaconis, Omid Etesami, Svante Janson, Sheldon Ross, Ernst Schulte-Geers, and ... for their detailed comments on my early attempts at exposition, as well as to numerous other correspondents who have contributed crucial corrections.

I happily offer a “finder’s fee” of $2.56 for each error in this draft when it is first reported to me, whether that error be typographical, technical, or historical. The same reward holds for items that I forgot to put in the index. And valuable suggestions for improvements to the text are worth 32¢ each. (Furthermore, if you find a better solution to an exercise, I’ll actually do my best to give you immortal glory, by publishing your name in the eventual book: —)

Cross references to yet-unwritten material sometimes appear as ‘00’; this impossible value is a placeholder for the actual numbers to be supplied later.

Happy reading!

Stanford, California
21 October 2012

D. E. K.
Part of the Preface to Volume 4B

During the years that I've been preparing Volume 4, I've often run across basic techniques of probability theory that I would have put into Section 1.2 of Volume 1 if I'd been clairvoyant enough to anticipate them in the 1960s. Finally I realized that I ought to collect most of them together in one place, near the beginning of Volume 4B, because the story of these developments is too interesting to be broken up into little pieces scattered here and there.

Therefore this volume begins with a special section entitled “Mathematical Preliminaries Redux,” and future sections use the abbreviation ‘MPR’ to refer to its equations and its exercises.
In books of this nature I can only suggest you keep it as simple as the subject will allow.

— KODE VICIOUS (2012)
MATHEMATICAL PRELIMINARIES REDUX

Many parts of this book deal with discrete probabilities, namely with a finite or countably infinite set \( \Omega \) of atomic events \( \omega \), each of which has a given probability \( \Pr(\omega) \), where

\[
0 \leq \Pr(\omega) \leq 1 \quad \text{and} \quad \sum_{\omega \in \Omega} \Pr(\omega) = 1. \tag{1}
\]

This set \( \Omega \), together with the function \( \Pr \), is called a “probability space.” For example, \( \Omega \) might be the set of all ways to shuffle a pack of 52 playing cards, with \( \Pr(\omega) = 1/52! \) for every such arrangement.

An event is, intuitively, a proposition that can be either true or false with certain probability. It might, for instance, be the statement “the top card is an ace,” with probability 1/13. Formally, an event \( A \) is a subset of \( \Omega \), namely the set of all atomic events for which the corresponding proposition \( A \) is true; and

\[
\Pr(A) = \sum_{\omega \in A} \Pr(\omega) = \sum_{\omega \in \Omega} \Pr(\omega) \mid \omega \in A. \tag{2}
\]

A random variable is a function that assigns a value to every atomic event. We typically use uppercase letters for random variables, and lowercase letters for the values that they might assume; thus, we might say that the probability of the event \( X = x \) is \( \Pr(X = x) = \sum_{\omega \in \Omega} \Pr(\omega) \mid X(\omega) = x \). In our playing card example, the top card \( T \) is a random variable, and we have \( \Pr(T = \heartsuit) = 1/52 \). (Sometimes, as here, the lowercase-letter convention is ignored.)

The random variables \( X_1, \ldots, X_k \) are said to be independent if

\[
\Pr(X_1 = x_1 \text{ and } \cdots \text{ and } X_k = x_k) = \Pr(X_1 = x_1) \cdots \Pr(X_k = x_k) \tag{3}
\]

for all \((x_1, \ldots, x_k)\). For example, if \( F \) and \( S \) denote the face value and suit of the top card \( T \), clearly \( F \) and \( S \) are independent. Hence in particular we have \( \Pr(T = \heartsuit) = \Pr(F = \heartsuit) \Pr(S = \heartsuit) \). But \( T \) is not independent of the bottom card, \( B \); indeed, we have \( \Pr(T = t \text{ and } B = b) \neq 1/52^2 \) for any cards \( t \) and \( b \).

A system of \( n \) random variables is called \( k \)-wise independent if no \( k \) of its variables are dependent. With pairwise (2-wise) independence, for example, we could have variable \( X \) independent of \( Y \), variable \( Y \) independent of \( Z \), and variable \( Z \) independent of \( X \); yet all three variables needn’t be independent (see exercise 6). Similarly, \( k \)-wise independence does not imply \((k + 1)\)-wise independence. But \((k + 1)\)-wise independence does imply \( k \)-wise independence.

The conditional probability of an event \( A \), given an event \( B \), is

\[
\Pr(A \mid B) = \frac{\Pr(A \cap B)}{\Pr(B)} = \frac{\Pr(A \text{ and } B)}{\Pr(B)}, \tag{4}
\]
when \( \Pr(B) > 0 \), otherwise it’s \( \Pr(A) \). Imagine breaking the whole probability space \( \Omega \) into two parts, \( \Omega' = B \) and \( \Omega'' = \Omega \setminus B \), with \( \Pr(\Omega') = \Pr(B) \) and \( \Pr(\Omega'') = 1 - \Pr(B) \). If we assign new probabilities to atomic events by the rules

\[
\Pr'(\omega) = \frac{\Pr(\omega | \Omega')}{\Pr(\Omega')}, \quad \Pr''(\omega) = \frac{\Pr(\omega | \Omega'')}{\Pr(\Omega'')},
\]

we obtain new probability spaces \( \Omega' \) and \( \Omega'' \), allowing us to contemplate a world where \( B \) is always true and another world where \( B \) is always false. It’s like taking two branches in a tree, each of which has its own logic. Conditional probability is important for the analysis of algorithms because algorithms often get into different states where different probabilities are relevant. Notice that we always have

\[
\Pr(A) = \Pr(A | B) \cdot \Pr(B) + \Pr(A | \overline{B}) \cdot \Pr(\overline{B}). \quad (5)
\]

The events \( A_1, \ldots, A_k \) are said to be independent if the random variables \( [A_1], \ldots, [A_k] \) are independent. (Bracket notation applies in the usual way to events-as-statements, not just to events-as-subsets; \( [A] = 1 \) if \( A \) is true, otherwise \( [A] = 0 \).) Exercise 20 proves that this happens if and only if

\[
\Pr\left(\bigcap_{j \in J} A_j\right) = \prod_{j \in J} \Pr(A_j), \quad \text{for all } J \subseteq \{1, \ldots, k\}. \quad (6)
\]

In particular, events \( A \) and \( B \) are independent if and only if \( \Pr(A | B) = \Pr(A) \).

When the values of a random variable \( X \) are real numbers or complex numbers, we’ve defined its expected value \( E(X) \) in Section 1.2.10: We said that

\[
E(X) = \sum_{\omega \in \Omega} X(\omega) \Pr(\omega) = \sum_x x \Pr(X = x), \quad (7)
\]

provided that this definition makes sense when the sums are taken over infinitely many nonzero values. (The sum should be absolutely convergent.) A simple but extremely important case arises when \( A \) is any event, and when \( X = [A] \) is a binary random variable representing the truth of that event; then

\[
E[A] = \sum_{\omega \in \Omega} [A](\omega) \Pr(\omega) = \sum_{\omega \in \Omega} [\omega \in A] \Pr(\omega) = \sum_{\omega \in A} \Pr(\omega) = \Pr(A). \quad (8)
\]

We’ve also noted that the expectation of a sum, \( E(X_1 + \cdots + X_k) \), always equals the sum of the expectations, \( (E(X_1) + \cdots + E(X_k)) \), whether or not the random variables \( X_j \) are independent. Furthermore the expectation of a product, \( E X_1 \ldots X_k \), is the product of the expectations, \( (E X_1) \ldots (E X_k) \), if these variables do happen to be independent. In Section 3.3.2 we defined the covariance,

\[
\text{covar}(X, Y) = E((X - E(X))(Y - E(Y))) = (E X Y) - (E X)(E Y), \quad (9)
\]

which tends to measure the way \( X \) and \( Y \) depend on each other. The variance, \( \text{var}(X) \), is \( \text{covar}(X, X) \); the middle formula in (9) shows why it is nonnegative whenever the random variable \( X \) takes on only real values.

All of these notions of expected value carry over to conditional expectation,

\[
E(X | A) = \sum_{\omega \in A} X(\omega) \frac{\Pr(\omega)}{\Pr(A)} = \sum_x x \frac{\Pr(X = x \text{ and } A)}{\Pr(A)}, \quad (10)
\]
conditioned on any event \( A \), when we want to work in the probability space for
which \( A \) is true. One of the most important formulas, analogous to (5), is

\[
E X = \sum_y E(X | Y = y) \Pr(Y = y)
\]

\[
= \sum_y \sum_x x \Pr(X = x | Y = y) \Pr(Y = y).
\]  

(11)

Furthermore there’s also another important kind of conditional expectation:
When \( X \) and \( Y \) are random variables, it’s often helpful to write \( E(X | Y) \) for
“the expectation of \( X \) given \( Y \)” Using that notation, Eq. (11) becomes simply

\[
E X = E(E(X | Y)).
\]  

(12)

This is a truly marvelous identity, great for hand-waving and for impressing outsiders—except that it can be confusing until you understand what it means.

In the first place, if \( Y \) is a Boolean variable, \( E(X | Y) \) might look as if it
means \( E(X | Y = 1) \); thus asserting that \( Y \) is true, just as \( E(X | A) \) asserts the
truth of \( A \) in (10). No; that interpretation is wrong, quite wrong. Be warned.

In the second place, you might think of \( E(X | Y) \) as a function of \( Y \). Well,
yes; but the best way to understand \( E(X | Y) \) is to regard it as a random variable.
That’s why we’re allowed to compute its expected value in (12).

All random variables are functions of the atomic events \( \omega \). The value of
\( E(X | Y) \) at \( \omega \) is the average of \( X(\omega') \) over all events \( \omega' \) such that \( Y(\omega') = Y(\omega) \):

\[
E(X | Y)(\omega) = \sum_{\omega' \in Y^{-1}(\omega)} X(\omega') \Pr(\omega')/\Pr(Y = Y(\omega)).
\]  

(13)

Similarly, \( E(X | Y_1, \ldots, Y_r) \) averages over events with \( Y_j(\omega') = Y_j(\omega) \) for \( 1 \leq j \leq r \).

For example, suppose \( X_1 \) through \( X_n \) are binary random variables con-
strained by the condition that \( \nu(X_1 \ldots X_n) = X_1 + \cdots + X_n = m \), where \( m \) and \( n \)
are constants with \( 0 \leq m \leq n \); all \( \binom{n}{m} \) such bit vectors \( X_1 \ldots X_n \) are assumed to
be equally likely. Clearly \( E X_1 = m/n \). But what is \( E(X_2 | X_1) \)? If \( X_1 = 0 \),
the expectation of \( X_2 \) is \( m/(n - 1) \); otherwise that expectation is \((m - 1)/(n - 1)\):
consequently \( E(X_2 | X_1) = (m - X_1)/(n - 1) \). And what is \( E(X_k | X_1, \ldots, X_{k-1}) \)?
The answer is easy, once you get used to the notation: If \( \nu(X_1 \ldots X_{k-1}) = r \),
then \( X_1 \ldots X_n \) is a random bit vector with \( \nu(X_1 \ldots X_n) = m - r \); hence the
average value of \( X_k \) will be \((m - r)/(n + 1 - k) \) in that case. We conclude that

\[
E(X_k | X_1, \ldots, X_{k-1}) = \frac{m - \nu(X_1 \ldots X_{k-1})}{n + 1 - k}, \text{ for } 1 \leq k \leq n.
\]  

(14)

The random variables on both sides of these equations are the same.

Inequalities. In practice we often want to prove that certain events are rare,
in the sense that they occur with very small probability. Conversely, our goal
is sometimes to show that an event is not rare. And we’re in luck, because
mathematicians have devised several fairly easy ways to derive upper bounds or
lower bounds on probabilities, even when the exact values are unknown.

May 20, 2015
We’ve already discussed the most important technique of this kind in Section 1.2.10. Stated in highly general terms, the basic idea can be formulated as follows: Let \( f \) be any nonnegative function such that \( f(x) \geq s > 0 \) when \( x \in S \). Then

\[
\Pr(X \in S) \leq E[f(X)] / s,
\]

provided that \( \Pr(X \in S) \) and \( E[f(X)] \) both exist. For example, \( f(x) = |x| \) yields

\[
\Pr(|X| \geq m) \leq E[|X|] / m
\]

whenever \( m > 0 \). The proof is amazingly simple, because we obviously have

\[
E[f(X)] \geq \Pr(X \in S) \cdot s + \Pr(X \notin S) \cdot 0.
\]

Formula (15) is often called Markov’s inequality, because A. A. Markov discussed the special case \( f(x) = |x|^a \) in Izv. v. d. Akad. Nauk (6) 1 (1907), 707–716. If we set \( f(x) = (x - E[X])^2 \), we get the famous 19th-century inequality of Bienaymé and Chebyshev:

\[
\Pr(|X - E[X]| \geq r) \leq \text{var}(X) / r^2.
\]

The case \( f(x) = e^{ax} \) is also extremely useful.

Another fundamental estimate, known as Jensen’s inequality [Acta Mathematica 30 (1906), 175–193], applies to convex functions \( f \); we’ve seen it so far only by a “hint” to exercise 6.2.2–36(!). The real-valued function \( f \) is said to be convex in an interval \( I \) of the real line, and \(-f\) is said to be concave in \( I \), if

\[
f(px + qy) \leq pf(x) + qf(y) \quad \text{for all } x, y \in I,
\]

whenever \( p \geq 0, q \geq 0 \), and \( p+q = 1 \). This condition turns out to be equivalent to saying that \( f''(x) \geq 0 \) for all \( x \in I \), if \( f \) has a second derivative \( f'' \). For example, the functions \( e^{ax} \) and \( x^{2n} \) are convex for all constants \( a \) and all nonnegative integers \( n \); and if we restrict consideration to positive values of \( x \), then \( f(x) = x^n \) is convex for all integers \( n \) (notably \( f(x) = 1/x \) when \( n = -1 \)). The functions \( \ln(1/x) \) and \( x \ln x \) are also convex for \( x > 0 \). Jensen’s inequality states that

\[
f(E[X]) \leq E[f(X)]
\]

when \( f \) is convex in the interval \( I \) and the random variable \( X \) takes values only in \( I \). (See exercise 42 for a proof.) For example, we have \( 1/E[X] \leq E(1/X) \) and \( \ln E[X] \geq E(\ln X) \) and \( (E[X]) \ln E[X] \leq E(X \ln X) \), when \( X \) is positive. Notice that (20) actually reduces to the very definition of convexity, (19), in the special case when \( X = x \) with probability \( p \) and \( X = y \) with probability \( q \).

Third and fourth on our list of remarkably useful inequalities are two classical results that apply to any random variable \( X \) whose values are nonnegative integers:

\[
\Pr(X > 0) \leq E[X]; \quad \text{("the first moment principle")}
\]

\[
\Pr(X > 0) \geq (E[X])^2 / (E[X^2]). \quad \text{("the second moment principle")}
\]

Formula (21) is obvious, because the left side is \( p_1 + p_2 + p_3 + \cdots \) when \( p_k \) is the probability that \( X = k \), while the right side is \( p_1 + 2p_2 + 3p_3 + \cdots \).
Formula (22) isn’t quite so obvious; it is \( p_1 + p_2 + p_3 + \cdots \) on the left and \( (p_1 + 2p_2 + 3p_3 + \cdots)^2/(1 + 4p_2 + 9p_3 + \cdots) \) on the right. However, as we saw with Markov’s inequality, there is a remarkably simple proof, once we happen to discover it:

\[
E X^2 = E(X^2 | X > 0) \Pr(X > 0) + E(X^2 | X = 0) \Pr(X = 0)
\]

\[
= E(X^2 | X > 0) \Pr(X > 0)
\]

\[
\geq (E(X | X > 0))^2 \Pr(X > 0) = (E X)^2 / \Pr(X > 0). \tag{23}
\]

In fact this proof shows that the second moment principle is valid even when \( X \) is not restricted to integer values (see exercise 46). Furthermore the argument can be strengthened to show that (22) holds even when \( X \) can take arbitrary negative values, provided only that \( E X \geq 0 \) (see exercise 47). See also exercise 118.

Exercise 54 applies (21) and (22) to the study of random graphs.

Another important inequality, which applies in the special case where \( X = X_1 + \cdots + X_m \) is the sum of binary random variables \( X_j \), was introduced more recently by S. M. Ross [Probability, Statistics, and Optimization (New York: Wiley, 1994), 185–190], who calls it the “conditional expectation inequality”:

\[
\Pr(X > 0) \geq \sum_{j=1}^{m} \frac{E X_j}{E(X | X_j = 1)}. \tag{24}
\]

Ross showed that the right-hand side of this inequality is always at least as big as the bound \( (E X)^2 / (E X^2) \) that we get from the second moment principle (see exercise 50). Furthermore, (24) is often easier to compute, even though it may look more complicated at first glance.

For example, his method applies nicely to the problem of estimating a reliability polynomial, \( f(p_1, \ldots, p_n) \), where \( f \) is a monotone Boolean function; here \( p_j \) represents the probability that component \( j \) of a system is “up.” We observed in Section 7.1.4 that reliability polynomials can be evaluated exactly, using BDD methods, when \( n \) is reasonably small; but approximations are necessary when \( f \) gets complicated. The simple example \( f(x_1, \ldots, x_5) = x_1 x_2 x_3 \lor x_2 x_3 x_4 \lor x_4 x_5 \) illustrates Ross’s general method: Let \((Y_1, \ldots, Y_5)\) be independent binary random variables, with \( E Y_j = p_j \), and let \( X = X_1 + X_2 + X_3 \), where \( X_1 = Y_1 Y_2 Y_3 \), \( X_2 = Y_2 Y_3 Y_4 \), and \( X_3 = Y_4 Y_5 \) correspond to the prime implicants of \( f \). Then \( \Pr(X > 0) = \Pr(f(Y_1, \ldots, Y_5) = 1) = E f(Y_1, \ldots, Y_5) = f(p_1, \ldots, p_5) \), because the \( Y \)’s are independent. And we can evaluate the bound in (24) easily:

\[
\Pr(X > 0) \geq \frac{p_1 p_2 p_3}{1 + p_1 + p_4} + \frac{p_2 p_3 p_4}{p_1 + 1 + p_5} + \frac{p_4 p_5}{p_1 p_2 p_3 + p_2 p_3 + 1}. \tag{25}
\]

If, for example, each \( p_j = 0.9 \), this formula gives \( \approx 0.848 \), while \( (E X)^2 / (E X^2) \approx 0.847 \); the true value, \( p_1 p_2 p_3 + p_2 p_3 p_4 + p_4 p_5 - p_1 p_2 p_3 p_4 - p_2 p_3 p_4 p_5 \), is 0.9558.

Many other important inequalities relating to expected values have been discovered, of which the most significant for our purposes in this book is the \textit{FKG inequality} discussed in exercise 61. It yields easy proofs that certain events are correlated, as illustrated in exercise 62.

May 20, 2015
Martingales. A sequence of dependent random variables can be difficult to analyze, but if those variables obey invariant constraints we can often exploit their structure. In particular, the “martingale” property, named after a classic betting strategy (see exercise 67), proves to be amazingly useful when it applies. Joseph L. Doob featured martingales in his pioneering book *Stochastic Processes* (New York: Wiley, 1953), and developed their extensive theory.

The sequence $\langle Z_n \rangle = Z_0, Z_1, Z_2, \ldots$ of real-valued random variables is called a martingale if it satisfies the condition

$$E(Z_{n+1} | Z_0, \ldots, Z_n) = Z_n \quad \text{for all } n \geq 0. \quad (26)$$

(We also implicitly assume, as usual, that the expectations $E Z_n$ are well defined.) For example, when $n = 0$, the random variable $E(Z_1 | Z_0)$ must be the same as the random variable $Z_0$ (see exercise 63).

Figure 1 illustrates George Pólya’s famous “urn model” [F. Eggenberger and G. Pólya, *Zeitschrift für angewandte Math. und Mech.* 3 (1923), 279–289], which is associated with a particularly interesting martingale. Imagine an urn that initially contains two balls, one red and one black. Repeatedly remove a randomly chosen ball from the urn, then replace it and contribute a new ball of the same color. The numbers $(r, b)$ of red and black balls will follow a path in the diagram, with the respective local probabilities indicated on each branch.

One can show without difficulty that all $n+1$ nodes on level $n$ of Fig. 1 will be reached with the same probability, $1/(n+1)$. Furthermore, the probability that a red ball is chosen when going from any level to the next is always $1/2$. Thus the urn scheme might seem at first glance to be rather tame and uniform. But in fact the process turns out to be full of surprises, because any inequity between red and black tends to perpetuate itself. For example, if the first ball chosen is black, so that we go from $(1, 1)$ to $(1, 2)$, the probability is only $2 \ln 2 - 1 \approx .386$ that the red balls will ever overtake the black ones in the future (see exercise 88).

One good way to analyze Pólya’s process is to use the fact that the ratios $r/(r+b)$ form a martingale. Each visit to the urn changes this ratio either to $(r+1)/(r+b+1)$ (with probability $r/(r+b)$) or to $r/(r+b+1)$ (with probability $b/(r+b)$); so the expected new ratio is $(r^2 + r + r)/(r+b) (r+b+1) = r/(r+b)$, no different from what it was before. More formally, let $X_0 = 1$, and for $n > 0$ let $X_n$ be the random variable ‘[the $n$th ball chosen is red]’. Then there are $X_0 + \cdots + X_n$ red balls and $\overline{X_0} + \cdots + \overline{X_n} + 1$ black balls at level $n$ of Fig. 1, and the sequence $\langle Z_n \rangle$ is a martingale if we define

$$Z_n = (X_0 + \cdots + X_n)/(n+2). \quad (27)$$

In practice it’s usually most convenient to define martingales $Z_0, Z_1, \ldots$ in terms of auxiliary random variables $X_0, X_1, \ldots$, as we’ve just done. The sequence $\langle Z_n \rangle$ is said to be a martingale with respect to the sequence $\langle X_n \rangle$ if $Z_n$ is a function of $(X_0, \ldots, X_n)$ that satisfies

$$E(Z_{n+1} | X_0, \ldots, X_n) = Z_n \quad \text{for all } n \geq 0. \quad (28)$$
Furthermore we say that a sequence $\{Y_n\}$ is fair with respect to the sequence $\{X_n\}$ if

$$E(Y_{n+1} \mid X_0, \ldots, X_n) = 0 \quad \text{for all } n \geq 0; \quad (29)$$

and we call $\{Y_n\}$ fair whenever

$$E(Y_{n+1} \mid Y_0, \ldots, Y_n) = 0 \quad \text{for all } n \geq 0. \quad (30)$$

Exercise 77 proves that (28) implies (26) and that (29) implies (30); thus an auxiliary sequence $\{X_n\}$ is sufficient but not necessary for defining martingales and fair sequences.

Whenever $\{Z_n\}$ is a martingale, we obtain a fair sequence $\{Y_n\}$ by letting $Y_0 = Z_0$ and $Y_n = Z_n - Z_{n-1}$ for $n > 0$, because the identity $E(Y_{n+1} \mid Z_0, \ldots, Z_n) = E(Z_{n+1} - Z_n \mid Z_0, \ldots, Z_n) = Z_n - Z_n$ shows that $\{Y_n\}$ is fair with respect to $\{Z_n\}$. Conversely, whenever $\{Y_n\}$ is fair, we obtain a martingale $\{Z_n\}$ by letting $Z_0 = Y_0 + \cdots + Y_n$, because the identity $E(Z_{n+1} \mid Y_0, \ldots, Y_n) = E(Z_n + Y_{n+1} \mid Y_0, \ldots, Y_n) = Z_n$ shows that $\{Z_n\}$ is a martingale with respect to $\{Y_n\}$. In other words, fairness and martingaleness are essentially equivalent. The $Y$'s represent unbiased “tweaks” that change one $Z$ to its successor.

It’s easy to construct fair sequences. For example, every sequence of independent random variables with mean 0 is fair. And if $\{Y_n\}$ is fair with respect to $\{X_n\}$, so is the sequence $\{Y'_n\}$ defined by $Y'_n = f_n(X_0, \ldots, X_{n-1})Y_n$ when $f_n(X_0, \ldots, X_{n-1})$ is almost any function whatsoever! (We need only keep $f_n$ small enough that $EY'_n$ is well defined.) In particular, we can let $f_n(X_0, \ldots, X_{n-1}) = 0$ for all large $n$, thereby making $\{Z_n\}$ eventually fixed.

A sequence of functions $N_n(x_0, \ldots, x_{n-1})$ is called a stopping rule if each value is either 0 or 1 and if $N_n(x_0, \ldots, x_{n-1}) = 0$ implies $N_{n+1}(x_0, \ldots, x_n) = 0$. We can assume that $N_0 = 1$. The number of steps before stopping, with respect to a sequence of random variables $\{X_n\}$, is then the random variable

$$N = N_1(X_0) + N_2(X_0, X_1) + N_3(X_0, X_1, X_2) + \cdots \quad (31)$$

(Intuitively, $N_n(x_0, \ldots, x_{n-1})$ means [the values $X_0 = x_0, \ldots, X_{n-1} = x_{n-1}$ do not stop the process]; hence it’s really more about “going” than “stopping.”)

Any martingale $Z_n = Y_0 + \cdots + Y_n$ with respect to $\{X_n\}$ can be adapted to fair with respect to the sequence martingale differences, see fair sequences fair independent stopping rule.
stop with this strategy if we change it to \( Z'_n = Y'_0 + \cdots + Y'_n \), where \( Y'_0 = N_n(X_0, \ldots, X_{n-1})Y_n \). Gamblers who wish to "quit when ahead" are using the stopping rule \( N_{n+1}(X_0, \ldots, X_n) = [Z'_n \leq 0] \), when \( Z'_n \) is their current balance.

Notice that if the stopping rule always stops after at most \( m \) steps— in other words, if the function \( N_m(x_0, \ldots, x_{m-1}) \) is identically zero— then we have \( Z'_m = Z'_N \), because \( Z'_N \) doesn't change after the process has stopped. Therefore \( E Z'_N = E Z'_m = E Z'_0 = E Z_0 \). No stopping rule can change the expected outcome of a martingale when the number of steps is bounded.

An amusing game of chance called Ace Now illustrates this optional stopping principle. Take a deck of cards, shuffle it and place the cards face down; then turn them face up one at a time as follows. Just before seeing the \( n \)-th card, you are supposed to say either "Stop" or "Deal," based on the cards you've already observed. (If \( n = 52 \) you must say "Stop.") After you've decided to stop, you win \$12 if the next card is an ace; otherwise you lose \$1. What is the best strategy for playing this game? Should you hold back until you have a pretty good chance at the \$12? What is the worst strategy? Exercise 82 has the answer.

**Tail inequalities from martingales.** The essence of martingales is equality of expectations. Yet martingales turn out to be important in the analysis of algorithms because we can use them to derive inequalities, namely to show that certain events occur with very small probability.

To begin our study, let's introduce inequality into Eq. (26): A sequence \( \{Z_n\} \) is called a submartingale if it satisfies

\[
E(Z_{n+1} | Z_0, \ldots, Z_n) \geq Z_n \quad \text{for all } n \geq 0.
\]

Similarly, it's called a supermartingale if \( \geq \) is changed to \( \leq \) in the left-hand part of this definition. (Thus a martingale is both sub- and super-.) In a submartingale we have \( E Z_0 \leq E Z_1 \leq E Z_2 \leq \cdots \), by taking expectations in (32). A supermartingale, similarly, has ever smaller expectations as \( n \) grows. One way to remember the difference between submartingales and supermartingales is to observe that their names are the reverse of what you might expect.

Submartingales are significant largely because of the fact that they're quite common. Indeed, if \( \{Z_n\} \) is any martingale and if \( f \) is any convex function, then \( \{f(Z_n)\} \) is a submartingale (see exercise 84). For example, the sequences \( \{ |Z_n| \} \) and \( \{ \max(Z_n, 0) \} \) and \( \{ Z_n^+ \} \) and \( \{ e^{Z_n} \} \) all are submartingales whenever \( \{Z_n\} \) is known to be a martingale. If, furthermore, \( Z_n \) is always positive, then \( \{ Z_n^+ \} \) and \( \{ 1/Z_n \} \) and \( \{ \ln(1/Z_n) \} \) and \( \{ Z_n \ln Z_n \} \), etc., are submartingales.

If we modify a submartingale by applying a stopping rule, it's easy to see that we get another submartingale. Furthermore, if that stopping rule is guaranteed to quit within \( m \) steps, we'll have \( E Z_m \geq E Z_N = E Z'_N = E Z'_m \). Therefore no stopping rule can increase the expected outcome of a submartingale, when the number of steps is bounded.

That comparatively simple observation has many important consequences. For example, exercise 86 uses it to give a simple proof of the so-called "maximal
inequality". If \( \langle Z_n \rangle \) is a nonnegative submartingale then
\[
\Pr(\max(Z_0, Z_1, \ldots, Z_n) \geq x) \leq \left( \frac{\mathbb{E} Z_n}{x} \right), \quad \text{for all } x > 0. \tag{33}
\]
Special cases of this inequality are legion. For instance, martingales \( \langle Z_n \rangle \) satisfy
\[
\Pr(\max(|Z_0|, |Z_1|, \ldots, |Z_n|) \geq x) \leq \frac{\mathbb{E} (|Z_n|)}{x}, \quad \text{for all } x > 0; \tag{34}
\]
\[
\Pr(\max(Z_0^2, Z_1^2, \ldots, Z_n^2) \geq x) \leq \frac{\mathbb{E}(Z_n^2)}{x}, \quad \text{for all } x > 0. \tag{35}
\]
Relation (35) is known as Kolmogorov's inequality, because A. N. Kolmogorov proved it when \( Z_n = X_1 + \cdots + X_n \) is the sum of independent random variables with \( \mathbb{E} X_k = 0 \) and \( \text{var}(X_k) = \sigma_k^2 \) for \( 1 \leq k \leq n \) [Math. Annalen 99 (1928), 309–311]. In that case \( \text{var}(Z_n) = \sigma_1^2 + \cdots + \sigma_n^2 = \sigma^2 \), and the inequality can be written
\[
\Pr(|X_1| < \sigma, |X_1 + X_2| < 2\sigma, \ldots, |X_1 + \cdots + X_n| < n\sigma) \geq 1 - 1/t^2. \tag{36}
\]
Chebyshev's inequality gives only \( \Pr(|X_1 + \cdots + X_n| < t\sigma) \geq 1 - 1/t^2 \), which is a considerably weaker result.

Another important inequality applies in the common case where we have good bounds on the terms \( Y_1, \ldots, Y_n \) that enter into the standard representation \( Z_n = Y_0 + Y_1 + \cdots + Y_n \) of a martingale. This one is called the Hoeffding–Azuma inequality, after papers by W. Hoeffding [J. Amer. Statistical Association 58 (1963), 13–30] and K. Azuma [Tohoku Math. Journal 2 (1967), 357–367]. It reads as follows: If \( \langle Y_n \rangle \) is any fair sequence with \( a_n \leq Y_n \leq b_n \), then
\[
\Pr(Y_1 + \cdots + Y_n \geq x) \leq e^{-x^2/(2(b_n - a_n)^2)}. \tag{37}
\]
The same bound applies to \( \Pr(Y_1 + \cdots + Y_n \leq -x) \), since \( -b_n \leq -Y_n \leq -a_n \); so
\[
\Pr(|Y_1 + \cdots + Y_n| \geq x) \leq 2e^{-x^2/(2(b_n - a_n)^2)} + \text{two similar terms}. \tag{38}
\]
Exercise 90 breaks the proof of this result into small steps. In fact, the proof even shows that \( a_n \) and \( b_n \) may be functions of \( \{Y_0, \ldots, Y_{n-1}\} \).

Applications. The Hoeffding–Azuma inequality is useful in the analysis of many algorithms because it applies to "Doob martingales," a very general class of martingales that J. L. Doob featured as Example 1 in his Stochastic Processes (1953), page 92. (In fact, he had already considered them many years earlier, in Trans. Amer. Math. Soc. 47 (1940), 486.) Doob martingales arise from any sequence of random variables \( \{X_n\} \), independent or not, and from any other random variable \( Q \); we simply define
\[
Z_n = \mathbb{E}(Q | X_0, \ldots, X_n). \tag{39}
\]
Then, as Doob pointed out, the resulting sequence is a martingale (see exercise 91). In our applications, \( Q \) is an aspect of some algorithm that we wish to study, and the variables \( X_0, X_1, \ldots \) reflect the inputs to the algorithm. For example, in an algorithm that uses random bits, the \( X \)'s are those bits.

Consider a hashing algorithm in which \( t \) objects are placed into \( m \) random lists, where the \( n \)th object goes into list \( X_n \); thus \( 1 \leq X_n \leq m \) for \( 1 \leq n \leq t \), and we assume that each of the \( m^t \) possibilities is equally likely. Let \( Q(x_1, \ldots, x_t) \) be

May 20, 2015
the number of lists that remain empty after the objects have been placed into lists
$x_1, \ldots, x_t$, and let $Z_n = E(Q[X_1, \ldots, X_n]$ be the associated Doob martingale.
Then $Z_0 = E(Q)$ is the \textit{average} number of empty lists; and $Z_t = Q(X_1, \ldots, X_t)$
is the \textit{actual} number, in any particular run of the algorithm.

What fair sequence corresponds to this martingale? If $1 \leq n \leq t$, the random
variable $Y_n = Z_n - Z_{n-1}$ is $f_n(x_1, \ldots, X_n)$, where $f_n(x_1, \ldots, x_n)$ is the average of
\begin{equation}
\Delta(x_1, \ldots, x_t) = \sum_{x=1}^{m} \Pr(X_n = x) \left( Q(x_1, \ldots, x_{n-1}, x_n, x_{n+1}, \ldots, x_t) \\
- Q(x_1, \ldots, x_{n-1}, x, x_{n+1}, \ldots, x_t) \right)
\end{equation}
taken over all $m^{t-n}$ values of $(x_{n+1}, \ldots, x_t)$.

In our application the function $Q(x_1, \ldots, x_t)$ has the property that
\begin{equation}
\left| Q(x_1, \ldots, x_{n-1}, x', x_{n+1}, \ldots, x_t) - Q(x_1, \ldots, x_{n-1}, x, x_{n+1}, \ldots, x_t) \right| \leq 1
\end{equation}
for all $x$ and $x'$, because a change to any one hash address always changes the
number of empty lists by either 1, 0, or $-1$. Consequently, for any fixed setting of the variables $(x_1, \ldots, x_{n-1}, x_{n+1}, \ldots, x_t)$, we have
\begin{equation}
\max_{x_n} \Delta(x_1, \ldots, x_t) \leq \min_{x_n} \Delta(x_1, \ldots, x_t) + 1.
\end{equation}
The Höfbling–Azuma inequality (37) therefore allows us to conclude that
\begin{equation}
\Pr(Z_t \geq Z_0) = \Pr(Y_1 + \cdots + Y_t \geq x) \leq e^{-2x^2/3}.
\end{equation}
Furthermore, $Z_0$ in this example is $m(m - 1)^t/m^t$, because exactly $(m - 1)^t$ of
the $m^t$ possible hash sequences leave any particular list empty. And the random
variable $Z_t$ is the actual number of empty lists when the algorithm is run. Hence
we can, for example, set $x = \sqrt{\ln f(t)}$ in (43), thereby proving that
\begin{equation}
\Pr(Z_t \geq (m - 1)^t/m^{t-1} + \sqrt{\ln f(t)}) \leq 1/f(t)^2, \text{ whenever } f(t) > 1.
\end{equation}
The same upper bound applies to $\Pr(Z_t \leq (m - 1)^t/m^{t-1} - \sqrt{\ln f(t)})$.

Notice that the inequality (41) was crucial in this analysis. Therefore
the strategy we’ve used to prove (43) is often called the “method of bounded
differences.” In general, a function $Q(x_1, \ldots, x_t)$ is said to satisfy a \textit{Lipschitz condition}
in coordinate $n$ if we have
\begin{equation}
\left| Q(x_1, \ldots, x_{n-1}, x, x_{n+1}, \ldots, x_t) - Q(x_1, \ldots, x_{n-1}, x', x_{n+1}, \ldots, x_t) \right| \leq c_n
\end{equation}
for all $x$ and $x'$. (This terminology mimics a well-known but only slightly
similar constraint that was introduced long ago into functional analysis by Rudolf
Lipschitz [Crelle 63 (1864), 296–308].) Whenever condition (45) holds, for a
function $Q$ associated with a Doob martingale for \textit{independent} random variables
$X_1, \ldots, X_t$, we can prove that $\Pr(Y_1 + \cdots + Y_t \geq x) \leq \exp(-2x^2/(c_1^2 + \cdots + c_t^2))$.

Let’s work out one more example, due to Colin McDiarmid [London Math. Soc. Lecture Notes 141 (1989), 148–188, §8(a)]. A gain we consider independent
integer-valued random variables $X_1, \ldots, X_t$ with $1 \leq X_n \leq m$ for $1 \leq n \leq t$;

May 20, 2015
but this time we allow each $X_n$ to have a different probability distribution. Furthermore we define $Q(x_1, \ldots, x_t)$ to be the minimum number of bins into which objects of sizes $x_1, \ldots, x_t$ can be packed, where each bin has capacity $m$.

This bin-packing problem sounds a lot harder than the hashing problem that we just solved. Indeed, the task of evaluating $Q(x_1, \ldots, x_t)$ is well known to be NP-complete [see M. R. Garey and D. S. Johnson, *SICOMP* 4 (1975), 397–411]. Yet $Q$ obviously satisfies the condition $(45)$ with $c_n = 1$ for $1 \leq n \leq t$. Therefore the method of bounded differences tells us that inequality $(43)$ is true, in spite of the apparent difficulty of this problem!

The only difference between this bin-packing problem and the hashing problem is that we’re clueless about the value of $Z_0$. Nobody knows how to compute $\mathbb{E} Q(X_1, \ldots, X_t)$, except for very special distributions of the random variables. However—and this is the magic of martingales—we do know that, whatever the value is, the actual numbers $Z_t$ will be tightly concentrated around that average.

If all the $X$’s have the same distribution, the values $\beta_t = \mathbb{E} Q(X_1, \ldots, X_t)$ satisfy $\beta_{t+\epsilon} \leq \beta_t + \beta_{\epsilon}$, because we could always pack the $t$ and $t'$ items separately. Therefore, by the subadditive law (see the answer to exercise 2.5–39), $\beta_t/t$ approaches a limit $\beta$ as $t \to \infty$. Still, however, random trials won’t give us decent bounds on that limit, because we have no good way to compute the $Q$ function.

*If only he could have enjoyed Martingale for its beauty and its peace without being chained to it by this band of responsibility and guilt!*  
— P. D. JAMES, *Cover Her Face* (1962)

**Statements that are almost sure, or quite sure.** Probabilities that depend on an integer $n$ often have the property that they approach 0 or 1 as $n \to \infty$, and special terminology simplifies the discussion of such phenomena. If, say, $A_n$ is an event for which $\lim_{n \to \infty} \Pr(A_n) = 1$, it’s convenient to express this fact in words by saying, “$A_n$ occurs almost surely, when $n$ is large.” (Indeed, we usually don’t bother to state that $n$ is large, if we already understand that $n$ is approaching infinity in the context of the current discussion.)

For example, if we toss a fair coin $n$ times, we’ll find that the coin almost surely comes up heads more than $.49n$ times, but fewer than $.51n$ times.

Furthermore, we’ll occasionally want to express this concept tersely in formulas, by writing just ‘a.s.’ instead of spelling out the words “almost surely.” For instance, the statement just made about $n$ coin tosses can be formulated as

$$0.49n < X_1 + \cdots + X_n < 0.51n \text{ a.s.}, \quad (46)$$

if $X_1, \ldots, X_n$ are independent binary random variables, each with $\mathbb{E} X_j = 1/2$.

In general a statement such as “$A_n$ a.s.” means that $\lim_{n \to \infty} \Pr(A_n) = 1$; or, equivalently, that $\lim_{n \to \infty} \Pr(\neg A_n) = 0$.

If $A_n$ and $B_n$ are both a.s., then the combined event $C_n = A_n \cap B_n$ is also a.s., regardless of whether those events are independent. The reason is that

$$\Pr(C_n) = \Pr(A_n \cup B_n) \leq \Pr(A_n) + \Pr(B_n),$$

which approaches 0 as $n \to \infty$.

Thus, to prove (46) we need only show that $X_1 + \cdots + X_n > .49n$ a.s. and that $X_1 + \cdots + X_n < .51n$ a.s., or in other words that $\Pr(X_1 + \cdots + X_n > .49n)$

May 20, 2015
and \( \Pr(X_1 + \cdots + X_n \geq 0.51n) \) both approach 0. Those probabilities are actually equal, by symmetry between heads and tails; so we need only show that \( p_n = \Pr(X_1 + \cdots + X_n \leq 0.49n) \) approaches 0. And that’s no sweat, because we know from Exercise 1.2.10-21 that \( p_n \leq e^{-0.001n} \).

In fact, we’ve proved more: We’ve shown that \( p_n \) is *superpolynomially small*, namely that

\[
  p_n = O(n^{-K}) \quad \text{for all fixed numbers} \ K. \tag{47}
\]

When the probability of an event \( \mathcal{A}_n \) is superpolynomially small, we say that \( \mathcal{A}_n \) holds “quite surely,” and abbreviate that by “q.s.” In other words, we’ve proved

\[
  0.49n < X_1 + \cdots + X_n < 0.51n \quad \text{q.s.} \tag{48}
\]

We’ve seen that the combination of any two a.s. events is a.s.; hence the combination of any finite number of a.s. events is also a.s. That’s nice, but q.s. events are even nicer: The combination of any polynomial number of q.s. events is also q.s. For example, if \( n^4 \) different people each toss \( n \) coins, it is quite sure that every one of them, without exception, will obtain between \( 0.49n \) and \( 0.51n \) heads!

(When making such asymptotic statements we ignore the inconvenient truth that our bound on the failure of the assertion, \( 2n^4 e^{-0.001n} \) in this case, becomes negligible only when \( n \) is greater than 700,000 or so.)

**EXERCISES**

1. [M31] (Nontransitive dice.) Suppose three biased dice with the respective faces

   \[ A = \begin{array}{ccc}
   \begin{array}{ccc}
   \text{\ding{112}} & \text{\ding{113}} & \text{\ding{117}} \\
   \text{\ding{116}} & \text{\ding{114}} & \text{\ding{115}} \\
   \text{\ding{116}} & \text{\ding{114}} & \text{\ding{115}} \\
   \end{array}
   \end{array}, \quad \begin{array}{ccc}
   \begin{array}{ccc}
   \text{\ding{112}} & \text{\ding{113}} & \text{\ding{117}} \\
   \text{\ding{116}} & \text{\ding{114}} & \text{\ding{115}} \\
   \text{\ding{116}} & \text{\ding{114}} & \text{\ding{115}} \\
   \end{array}
   \end{array}, \quad \begin{array}{ccc}
   \begin{array}{ccc}
   \text{\ding{112}} & \text{\ding{113}} & \text{\ding{117}} \\
   \text{\ding{116}} & \text{\ding{114}} & \text{\ding{115}} \\
   \text{\ding{116}} & \text{\ding{114}} & \text{\ding{115}} \\
   \end{array}
   \end{array} \]

   are rolled independently at random.

   a) Show that \( \Pr(A > B) = \Pr(B > C) = \Pr(C > A) = 5/9 \).

   b) Find dice with \( \Pr(A > B), \Pr(B > C), \Pr(C > A) \) all greater than \( 5/9 \).

   c) If Fibonacci dice have \( F_m \) faces instead of just six, show that we could have

   \[
   \Pr(A > B) = \Pr(B > C) = F_{m-1}/F_m \quad \text{and} \quad \Pr(C > A) = F_{m-1}/F_m \pm 1/F_m. \]

2. [M32] Prove that the previous exercise is asymptotically optimum, in the sense that \( \min(\Pr(A > B), \Pr(B > C), \Pr(C > A)) < 1/6 \), regardless of the number of faces.

3. [22] (Lake Wobegon dice.) Continuing the previous exercises, find three dice such that \( \Pr(A > \frac{1}{3}(A + B + C)) \geq \Pr(B > \frac{1}{3}(A + B + C)) \geq \Pr(C > \frac{1}{3}(A + B + C)) \geq 16/27 \). Each face of each die should be \( \square \) or \( \blacksquare \) or \( \blacklozenge \) or \( \blackdiamond \) or \( \blacktriangle \).

4. [22] (Nontransitive Bingo.) Each player in the game of NanoBingo has a card containing four numbers from the set \( S = \{1, 2, 3, 4, 5, 6\} \), arranged in two rows. An announcer calls out the elements of \( S \), in random order; the first player whose card has a horizontal row with both numbers called shouts “Bingo!” and wins. (Or victory is

May 20, 2015
shared when there are multiple Binges.) For example, consider the four cards

\[
A = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}, \quad B = \begin{bmatrix} 2 & 3 \\ 4 & 6 \end{bmatrix}, \quad C = \begin{bmatrix} 3 & 4 \\ 1 & 5 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 4 \\ 2 & 6 \end{bmatrix}
\]

If the announcer calls “6, 2, 5, 1” when A plays against B, then A wins; but the sequence 
“1, 3, 2” would yield a tie. One can show that \( \Pr(A \text{ beats } B) = \frac{3}{10}, \) \( \Pr(B \text{ beats } A) = \frac{31}{125}, \) and \( \Pr(A \text{ and } B \text{ tie}) = \frac{12}{125}. \) Determine the probabilities of all possible outcomes when there are (a) two (b) three (c) four different players using those cards.

5. [HM22] (T. M. Cover, 1989.) Common wisdom asserts that longer games favor the stronger player, because they provide more evidence of the relative skills. However, consider an \( n \)-round game in which Alice scores \( A_1, \ldots, A_n \) points while Bob scores \( B_1, \ldots, B_n \) points, where each of \( A_1, \ldots, A_n \) are independent random variables representing Alice’s strength, and each of \( B_1, \ldots, B_n \) independently represent Bob’s (and are independent of the \( A_i \)’s). Suppose Alice wins with probability \( P_n \).

a) Show that it’s possible to have \( P_1 = 0.9 \) but \( P_{100} < 0.001 \).

b) Let \( m_k = 2^{-k}, n_k = 2^{3k+4}, \) and \( q_k = 2^{-3k}/D, \) where \( D = 2^{-1} + 2^{-4} + 2^{-9} + \cdots \approx 1.5647. \) Suppose \( A \) and \( B \) are zero except that \( A = m_k \) with probability \( q_k \) when \( k \geq 0 \) is even, \( B = n_k \) with probability \( q_k \) when \( k \geq 1 \) is odd. What are \( \Pr(A > B), \) \( \Pr(A < B), \) and \( \Pr(A = B) \)?

c) With the distributions in (b), prove that \( P_{2k} \to [k \text{ even}] \) as \( k \to \infty \).

6. [M22] Consider \( n \geq 2 \) random Boolean (or binary) variables \( x_1, \ldots, x_n \) with the following joint distribution: The vector \( x_1, \ldots, x_n \) occurs with probability \( 1/(n-1)^2 \) if \( x_1 + \cdots + x_n = 2, \) with probability \( (n-2)/(2n-2) \) if \( x_1 + \cdots + x_n = 0, \) and with probability 0 otherwise. Show that the variables are pairwise independent (that is, \( X_i \) is independent of \( X_j \) when \( i \neq j \)); but they are not \( k \)-wise independent for \( k > 2 \).

Also find a joint distribution, depending only on \( \nu x = x_1 + \cdots + x_n, \) that is \( k \)-wise independent for \( k = 2 \) and \( k = 3 \) but not \( k = 4 \).

7. [M20] (Ernst Schulte-Geers, 2012.) Generalizing exercise 6, construct a \( \nu x \)-based distribution that has \( k \)-wise but not \( (k+1) \)-wise independence, given \( k \geq 1 \).

8. [M20] Suppose the Boolean vector \( x_1, \ldots, x_n \) occurs with probability \( (2 + (-1)^{\nu x})/2^{n+1} \), where \( \nu x = x_1 + \cdots + x_n. \) For what \( k \) is this distribution \( k \)-wise independent?

9. [M20] Find a distribution of Boolean vectors \( x_1, \ldots, x_n \) such that any two variables are independent; yet if we know the value of any \( x_j, \) the remaining variables are \( (n-1) \)-wise independent. Hint: The answer is so simple, you might feel humiliated.

10. [M21] Let \( Y_1, \ldots, Y_m \) be independent and uniformly distributed elements of \( \{0, 1, \ldots, p-1\}, \) where \( p \) is prime. Also let \( X_j = (2^n + Y_j)^{-1} + \cdots + Y_m \) mod \( p \), for \( 1 \leq j \leq n. \) For what \( k \) are the \( X_j \)’s \( k \)-wise independent?

11. [M20] If \( X_1, \ldots, X_{2n} \) are independent random variables with the same discrete distribution, and if \( \alpha \) is any real number whatsoever, prove that

\[
\Pr\left( \frac{X_1 + \cdots + X_{2n}}{2n} - \alpha \leq \frac{X_1 + \cdots + X_n}{n} - \alpha \right) > \frac{1}{2}.
\]

12. [18] Which of the following four statements are equivalent to the statement that \( \Pr(A \mid B) > \Pr(A) \)? (i) \( \Pr(B \mid A) > \Pr(B); \) (ii) \( \Pr(A \mid B) > \Pr(A \mid \bar{B}); \) (iii) \( \Pr(B \mid A) > \Pr(B \mid \bar{A}); \) (iv) \( \Pr(A \mid \bar{B}) > \Pr(A \mid B). \)

13. [15] True or false: \( \Pr(A \mid C) > \Pr(A) \) if \( \Pr(A \mid B) > \Pr(A) \) and \( \Pr(B \mid C) > \Pr(B) \).
14. [10] (Thomas Bayes, 1763.) Prove the “chain rule” for conditional probability:
\[ \Pr(A_1 \cap \cdots \cap A_n) = \Pr(A_1) \Pr(A_2 | A_1) \cdots \Pr(A_n | A_1 \cap \cdots \cap A_{n-1}). \]

15. [12] True or false: \( \Pr(A \mid B \cap C) = \Pr(A \cap B \mid C) \).

16. [M15] Under what circumstances is \( \Pr(A \cup C \mid B) = \Pr(A \mid C \cup B) \)?

17. [15] Evaluate the conditional probability \( \Pr(T \text{ is an ace} \mid B = \emptyset) \) in the playing card example of the text, where \( T \) and \( B \) denote the top and bottom cards.

18. [20] Let \( M \) and \( m \) be the maximum and minimum values of the random variable \( X \). Prove that \( \var(X) \leq (M - E(X))(E(X) - m) \).

19. [HM28] Let \( X \) be a random nonnegative integer, with \( \Pr(X = x) = 1/2^{x+1} \), and suppose that \( X = (\ldots X_3 X_1 X_0)_2 \) and \( X + 1 = (\ldots Y_3 Y_1 Y_0)_2 \) in binary notation.
   a) What is \( E(X) \)? Hint: Express this number in the binary number system.
   b) Prove that the random variables \( \{X_0, X_1, \ldots, X_n\} \) are independent.
   c) Find the mean and variance of \( S = X_0 + X_1 + X_2 + \cdots \).
   d) Find the mean and variance of \( R = X_0 \oplus X_1 \oplus X_2 \oplus \cdots \).
   e) Let \( \pi = (1,1,0,0,1,2,3) \). What is the probability that \( X_n = p_n \) for all \( n \geq 0 \)?
   f) What is \( E(Y) \)? Show that \( Y_0 \) and \( Y_1 \) are not independent.
   g) Find the mean and variance of \( T = Y_0 + Y_1 + Y_2 + \cdots \).

20. [M18] Let \( X_1, \ldots, X_k \) be binary random variables for which we know that \( \Pr(\bigcap_{i \in J} X_i) = \prod_{i \in J} \Pr(X_i) \) for all \( J \subseteq \{1, \ldots, k\} \). Prove that the \( X_i \)'s are independent.

21. [M20] Find a small-as-possible example of random variables \( X \) and \( Y \) that satisfy \( \cov(X, Y) = 0 \), that is, \( E(XY) = (E(X))(E(Y)) \), although they aren’t independent.

22. [M20] Use Eq. (8) to prove the “union inequality”
\[ \Pr(A_1 \cup \cdots \cup A_n) \leq \Pr(A_1) + \cdots + \Pr(A_n). \]

23. [M21] If each \( X_i \) is an independent binary random variable with \( \Pr(X_i = 1) = p_i \), the cumulative binomial distribution \( B_{n,m}(p) \) is the probability that \( X_1 + \cdots + X_n \leq m \). Thus it’s easy to see that \( B_{n,m}(p) = \sum_{k=0}^{m} \binom{n}{k} p^k (1-p)^{n-k} \).

   Show that \( B_{n,m}(p) \) is also equal to \( \sum_{k=0}^{m} \binom{n-\lfloor k/p \rfloor}{k} \binom{k+1}{n-k} p^{k+1} (1-p)^{n-k-m} \), for \( 0 \leq m \leq n \).
   \text{Hint: Consider the random variables} \( J_1, J_2, \ldots, J_T \) defined by the rule that \( X_j = 0 \) if and only if \( j \) has one of the \( T \) values \( \{J_1, J_2, \ldots, J_T\} \), where \( 1 \leq J_1 < J_2 < \cdots < J_T \leq n \). What is \( \Pr(T \geq r \text{ and } J_r = s) \)?

24. [HM27] The cumulative binomial distribution also has many other properties.
   a) Prove that \( B_{n,m}(p) = \binom{n}{m} \int_{x=m}^{n-m} x^m (1-x)^{n-m} \, dx < m \).
   b) Use that formula to prove that \( B_{n,m}(m/n) > \frac{1}{2} \), for \( 0 \leq m < n/2 \). \text{Hint: Show that} \( \int_{x=m}^{n-m} x^m (1-x)^{n-m} \, dx < \frac{1}{2} \).
   c) Show furthermore that \( B_{n,m}(m/n) > \frac{1}{4} \) when \( n/2 \leq m \leq n \). [Thus \( m \) is the median value of \( X_1 + \cdots + X_n \), when \( p = m/n \) and \( m \) is an integer.]

25. [M25] Suppose \( X_1, X_2, \ldots \) are independent random binary variables, with means \( \mathbb{E}(X_i) = p_i \). Let \( \binom{\binom{n}{k}}{\binom{n-1}{k+1}} \) be the probability that \( X_1 + \cdots + X_n = k \); thus \( \binom{\binom{n}{k}}{\binom{n-1}{k+1}} = p_k (\binom{n}{k} - 1) \).

   a) Prove that \( \binom{\binom{n}{k}}{\binom{n-1}{k+1}} \geq \binom{\binom{n}{k+1}}{\binom{n}{k}} \), if \( p_j \leq (k+1)/(n+1) \) for \( 1 \leq j \leq n \).
   b) Furthermore \( \binom{\binom{n}{k}}{\binom{n}{k+1}} \leq \binom{\binom{n}{k}}{\binom{n}{k}} q^{n-k} \), if \( p_j \leq p \leq k/n \) for \( 1 \leq j \leq n \).

26. [M27] Continuing exercise 25, prove that \( \binom{\binom{n}{k+1}}{\binom{n}{k}} \geq \left( \frac{n}{k+1} \right) \left( 1 + \frac{1}{k+1} \right) \left( 1 + \frac{1}{k+2} \right) \) for \( 0 < k < n \). \text{Hint: Consider} \( r_{n,k} = \binom{\binom{n}{k+1}}{\binom{n}{k}} \).

May 20, 2015
27. \([M22]\) Find an expression for the generalized cumulative binomial distribution 
\(\sum_{i=0}^{n} g(k)(\binom{n}{k})\) that is analogous to the alternative formula in exercise 23.

28. \([HM29]\) (W. Hoeffding, 1956.) Let \(X = X_1 + \cdots + X_n\) and \(p_1 + \cdots + p_n = np\) in exercise 25, and suppose that \(E g(X) = \sum_{i=0}^{n} g(k)(\binom{n}{k})\) for some function \(g\).
   a) Prove that \(E g(X) \leq \sum_{k=0}^{n} g(k)(\binom{n}{k}) p^k (1-p)^{n-k}\) if \(g\) is convex in \([0, n]\).
   b) If \(g\) isn’t convex, show that the maximum of \(E g(X)\), over all choices of \(\{p_1, \ldots, p_n\}\) with \(p_1 + \cdots + p_n = np\) can always be attained by a set of probabilities for which at most three distinct values \(0, a, 1\) occur among the \(p_j\).
   c) Furthermore, \(\sum_{k=0}^{n} g(k)(\binom{n}{k}) \leq B_{m,n}(p)\), whenever \(p_1 + \cdots + p_n = np \geq m + 1\).

29. \([HM29]\) (S. M. Samuels, 1965.) Continuing exercise 28, prove that we have \(B_{m,n}(p) \geq ((1-p)/(1-p/m+1))^{n-m} \) whenever \(np \leq m + 1\).

30. \([HM34]\) Let \(X_1, \ldots, X_n\) be independent random variables whose values are non-negative integers, where \(E X_i = 1\) for all \(i\), and let \(p = Pr(X_1 + \cdots + X_n \leq n)\).
   a) What is \(p\) if each \(X_i\) takes only the values 0 and \(n + 1\)?
   b) Show that, in any set of distributions that minimize \(p\), each \(X_i\) assumes only two integer values, 0 and \(m_i\), where \(1 \leq m_i \leq n + 1\).
   c) Furthermore we have \(p > 1/e\) if each \(X_i\) has the same two-valued distribution.

31. \([M20]\) Assume that \(A_1, \ldots, A_n\) are random events such that, for every subset \(I \subseteq \{1, \ldots, n\}\), the probability \(Pr(\cap_{i \in I} A_i)\) that all \(A_i\) for \(i \in I\) occur simultaneously is \(\pi_I\); here \(\pi_I\) is a number with \(0 \leq \pi_I \leq 1\), and \(\pi_I = 1\). Show that the probability of any combination of the events, \(Pr(f([A_1], \ldots, [A_n]))\) for any Boolean function \(f\), can be found by expanding \(f\)’s multilinear reliability polynomial \(f([A_1], \ldots, [A_n])\) and replacing each term \(\prod_{i \in I} A_i\) by \(\pi_I\). For example, the reliability polynomial of \(X_1 \& X_2 \& X_3 = X_1 + X_2 + X_3 - X_1 X_2 - X_2 X_3 - X_1 X_3 + X_1 X_2 X_3\); hence \(Pr([A_1] \& [A_2] \& [A_3]) = \pi_1 + \pi_2 + \pi_3 - \pi_1 \pi_2 - \pi_1 \pi_3 - \pi_2 \pi_3 + \pi_1 \pi_2 \pi_3\). (Here \(\pi_{12}\) is short for \(\pi_{1,2}\), etc.)

32. \([M22]\) Not all sets of numbers \(\pi_I\) in the preceding exercise can arise in an actual probability distribution. For example, if \(I \subseteq J\) we must have \(\pi_I \geq \pi_J\). What is a necessary and sufficient condition for the \(2^n\) values of \(\pi_I\) to be legitimate?

33. \([M20]\) Suppose \(X, Y\) are binary random variables whose joint distribution is defined by the probability generating function \(G(w, z) = E(w^X z^Y) = pw + qz + rwz\), where \(p, q, r > 0\) and \(p + q + r = 1\). Use the definitions in the text to compute the probability generating function \(E(z^{M_{[XY]}})\) for the conditional expectation \(E(X \mid Y)\).

34. \([M17]\) Write out an algebraic proof of (12), using the definitions (7) and (13).

35. \([M22]\) True or false: (a) \(E(E(X) \mid Y) = E(X \mid Y)\); (b) \(E(E(X \mid Y) \mid Z) = E(X \mid Z)\).

36. \([M21]\) Simplify the following formulas (a) \(E(f(X)) \mid X\); (b) \(E(f(Y)) \mid g(Y)\).

37. \([M20]\) Suppose \(X_1, \ldots, X_n\) is a random permutation of \(\{1, \ldots, n\}\), with every permutation occurring with probability \(1/n!\). What is \(E(X_1, X_1, \ldots, X_{n-1})\)?

38. \([M26]\) Let \(X_1, \ldots, X_n\) be a random restricted growth string of length \(n\), each with probability \(1/n\). (See Section 7.2.1.5). What is \(E(X_1, X_1, \ldots, X_{n-1})\)?

39. \([HM29]\) A hen lays \(N\) eggs, where \(Pr(N = n) = e^{-n} n^n / n!\) obeys the Poisson distribution. Each egg hatches with probability \(p\), independent of all other eggs. Let \(K\) be the resulting number of chicks. Express (a) \(E(K \mid N)\), (b) \(E(K)\), and (c) \(E(N \mid K)\) in terms of \(N, K, p, \mu\).

40. \([M16]\) Suppose \(X\) is a random variable with \(X \leq M\), and let \(m\) be any value with \(m < M\). Show that \(Pr(X > m) \geq (E X - m) / (M - m)\).

May 20, 2015
41. [HM21] Which of the following functions are convex in the set of all real numbers $x^a$: (a) $|x|^a$, where $a$ is a constant; (b) $\sum_{k \geq n} x^k/k!$, where $n \geq 0$ is an integer; (c) $e^{ax^2}$; (d) $f(x) = \{x \in I \mid f(x) + \infty [x \notin I],$ where $f$ is convex in the interval $I$.

42. [HM21] Prove Jensen's inequality (20).

- 43. [M18] Use (22) and (20) to strengthen (20): If $f$ is convex in $I$ and if the random variable $X$ takes values in $I$, then $E(X) \leq E(f(E(X|I))) \leq E(f(X))$.

- 44. [M25] If $f$ is convex on the real line and if $E(X) = 0$, prove that $E(f(aX)) \leq E(f(bX))$ whenever $0 \leq a \leq b$.

45. [M18] Derive the first moment principle (21) from Markov's inequality (15).

46. [M15] Explain why $E(X^2 | X > 0) \geq (E(X | X > 0))^2$ in (23).

47. [M15] If $X$ is random and $Y = \max(0, X)$, show that $E Y \geq E X$ and $E Y^2 \leq E X^2$.

48. [M20] Suppose $X_i, \ldots, X_n$ are independent random variables with $E X_i = 0$ and $E X_i^2 = \sigma_i^2$ for $1 \leq i \leq n$. Chebyshev's inequality tells us that $Pr(|X_1 + \cdots + X_n| \geq a) \leq \frac{(\sigma_1^2 + \cdots + \sigma_n^2) a^2}{2}$. Show that the second moment principle gives a somewhat better one-sided estimate, $Pr(|X_1 + \cdots + X_n| \geq a) \leq \frac{(\sigma_1^2 + \cdots + \sigma_n^2)}{a^2}$, if $a \geq 0$.

49. [M20] If $X$ is random and $E X \geq 0$, prove that $Pr(X = 0) \leq \frac{(E X^2)^2}{(E X)^2} - 1$.

50. [M27] Let $X = X_1 + \cdots + X_n$ be the sum of binary random variables, with $E X_j = p_j$. Let $J$ be independent of the $X$’s, and uniformly distributed in $\{1, \ldots, m\}$.
   
   a) Prove that $Pr(X > 0) = \sum_{j=1}^m E(X_j \mid X_j > 0) \cdot Pr(X_j > 0)$.
   
   b) Therefore (24) holds. Hint: Use Jensen's inequality with $f(x) = 1/x$.
   
   c) What are $Pr(X_j = 1)$ and $Pr(J = j \mid X_j = 1)$?
   
   d) Let $t_j = E(1 \mid X_j = j)$ and $t_j = 1$. Prove that $E X^2 = \sum_{j=1}^m p_j t_j$.
   
   e) Jensen's inequality now implies that the right side of (24) is $\geq (E X^2)^2/(E X^2)$.

51. [M21] Show how to use the conditional expectation inequality (24) to obtain also an upper bound on the value of a reliability polynomial, and apply your method to the case illustrated in (25).

52. [M21] What lower bound does inequality (24) give for the reliability polynomial of the symmetric function $S_{2k}(x_1, \ldots, x_n)$, when $p_1 = \cdots = p_n = p$?

53. [M20] Use (24) to obtain a lower bound for the reliability polynomial of the non-monotonic Boolean function $f(x_1, \ldots, x_n) = x_1 x_2 x_3 + x_3 x_4 x_5 + \cdots \lor x_2 x_4 x_7 + x_6 x_1 x_2$.

54. [M22] Suppose each edge of a random graph on the vertices $\{1, \ldots, n\}$ is present with probability $p$, independent of every other edge. If $u, v, w$ are distinct vertices, let $X_{uvw}$ be the probability that $(u, v, w)$ is a 3-clique, namely the probability that $u \rightarrow v, u \rightarrow w, v \rightarrow u$. Also let $X = \sum_{1 \leq u < v < w \leq n} X_{uvw}$ be the total number of 3-cliques. Use the (a) first and (b) second moment principle to derive bounds on the probability that the graph contains at least one 3-clique.

55. [29] Evaluate the upper and lower bounds in the previous exercise numerically in the case $n = 10$, and compare them to the true probability, when (a) $p = 1/2$; (b) $p = 1/10$.

56. [HM20] Evaluate the upper and lower bounds of exercise 54 asymptotically when $p = 1/n$ and $n \to \infty$.

57. [M21] Obtain a lower bound for the probability in exercise 54(b) by using the conditional expectation inequality (24) instead of the second moment principle (22).
58. \[M22\] Generalizing exercise 54, find bounds on the probability that a random graph on \(n\) vertices has a \(k\)-clique, when each edge has probability \(p\).

59. \[HM25\] (The four functions theorem.) The purpose of this exercise is to prove an inequality that applies to four sequences \(\langle a_n \rangle, \langle b_n \rangle, \langle c_n \rangle, \langle d_n \rangle\) of nonnegative numbers:

\[
a_j b_k \leq c_{j+k} d_{j+k} \quad \text{for } 0 \leq j, k < \infty \quad \text{implies} \quad \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} a_j b_k \leq \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} c_{j+k} d_{j+k}.
\]

(The sums will be \(\infty\) if they don’t converge.) Although the inequality might appear at first to be merely a curiosity, of interest only to a few lovers of esoteric formulas, we shall see that it’s a fundamental result with many applications of great importance.

\[a\] Prove the special case where \(a_j = b_j = c_j = d_j = 0\) for \(j \geq 2\), namely that

\[
a_0 b_0 \leq c_0 d_0, \quad a_0 b_1 \leq c_1 d_0, \quad a_1 b_0 \leq c_1 d_1, \quad \text{and} \quad a_1 b_1 \leq c_1 d_1
\]

implies \(a_0 + a_1)(b_0 + b_1) \leq (c_0 + c_1)(d_0 + d_1)\).

Can equality hold in the first four relations but not in the last one? Can equality hold in the last relation but not in the first four?

\[b\] Use that result to prove \((a)\) when \(a_j = b_j = c_j = d_j = 0\) for all \(j \geq 2\), given \(n > 0\).

\[c\] Conclude that \((a)\) is true in general.

60. \[M21\] If \(\mathcal{F}\) is a family of sets, and if \(\alpha\) is a function that maps sets into real numbers, let \(\alpha(\mathcal{F}) = \sum_{S \in \mathcal{F}} \alpha(S)\). Suppose \(\mathcal{F}\) and \(\mathcal{G}\) are finite families of sets for which nonnegative set functions \(\alpha, \beta, \gamma, \text{ and } \delta\) have been defined with the property that

\[
\alpha(S) \beta(T) \leq \gamma(S \cup T) \delta(S \cap T) \quad \text{for all } S \in \mathcal{F} \text{ and } T \in \mathcal{G}.
\]

\[a\] Use exercise 50 to prove that \(\alpha(\mathcal{F}) \beta(\mathcal{G}) \leq \gamma(\mathcal{F} \cup \mathcal{G}) \delta(\mathcal{F} \cap \mathcal{G})\).

\[b\] In particular, \(|\mathcal{F}| |\mathcal{G}| \leq |\mathcal{F} \cup \mathcal{G}| |\mathcal{F} \cap \mathcal{G}|\) for all families \(\mathcal{F}\) and \(\mathcal{G}\).

61. \[M28\] Consider random sets in which \(S\) occurs with probability \(\mu(S)\), where

\[
\mu(S) \geq 0 \quad \text{and} \quad \mu(S) \mu(T) \leq \mu(S \cup T) \mu(S \cap T) \quad \text{for all sets } S \text{ and } T.
\]

Assume also that \(U = \bigcup_{\mu(S) > 0} S\) is a finite set.

\[a\] Prove the FKG inequality (which is named for C. M. Fortuin, P. W. Kasteleyn, and J. Ginibre): If \(f\) and \(g\) are real-valued set functions, then

\[
f(S) \leq f(T) \quad \text{and} \quad g(S) \leq g(T) \quad \text{for all } S \subseteq T \quad \text{implies} \quad E(fg) \geq E(f) E(g).
\]

Here, as usual, \(E(f)\) stands for \(\sum_{S} \mu(S) f(S)\). The conclusion can also be written \(\text{cov}(f, g) \geq 0\), using the notation of \((g)\); we say that \(f\) and \(g\) are “positively correlated” when this is true. (The awkward term “nonnegatively correlated” would be more accurate, because \(f\) and \(g\) might actually be independent.) \(\text{Hint:}\) Prove the result first in the special case that both \(f\) and \(g\) are nonnegative.

\[b\] Furthermore,

\[
f(S) \geq f(T) \quad \text{and} \quad g(S) \geq g(T) \quad \text{for all } S \subseteq T \quad \text{implies} \quad E(fg) \geq E(f) E(g);
\]

\[
f(S) \leq f(T) \quad \text{and} \quad g(S) \geq g(T) \quad \text{for all } S \subseteq T \quad \text{implies} \quad E(fg) \leq E(f) E(g).
\]

\[c\] It isn’t necessary to verify condition \((**\ast)\) for all sets, if \((**\ast)\) is known to hold for sufficiently many pairs of “neighboring” sets. Given \(\mu\), let’s say that set \(S\) is supported if \(\mu(S) \neq 0\). Prove that \((**\ast)\) holds for all \(S\) and \(T\) whenever the following three conditions are satisfied: (i) If \(S\) and \(T\) are supported, so are \(S \cup T\) and \(S \cap T\).
(ii) If $S$ and $T$ are supported and $S \subseteq T$, the elements of $T \setminus S$ can be labeled $t_1, \ldots, t_k$ such that each of the intermediate sets $S \cup \{t_1, \ldots, t_j\}$ is supported, for $1 \leq j \leq k$. (iii) Condition (**) holds whenever $S = R \cup s$ and $T = R \cup t$ and $s, t \notin R$.

d) The multivariate Bernoulli distribution $B(p_1, \ldots, p_m)$ on subsets of $\{1, \ldots, m\}$ is

\[ p(S) = \left( \prod_{j=1}^{m} p_j^{j \in S} \right) \left( \prod_{j=1}^{m} (1 - p_j)^{j \notin S} \right), \]

given $0 \leq p_1, \ldots, p_m \leq 1$. (Thus each element $j$ is included independently with probability $p_j$, as in exercise 25.) Show that this distribution satisfies (**).

e) Describe other simple distributions for which (**) holds.

62. [M20] Suppose the $m = \binom{n}{2}$ edges $E$ of a random graph $G$ on $n$ vertices are chosen with the Bernoulli distribution $B(p_1, \ldots, p_m)$. Let $f(E) = |G|$ [is connected] and $g(E) = [G]$ is 4-colorable]. Prove that $f$ is negatively correlated with $g$.

63. [M17] Suppose $Z_0$ and $Z_1$ are random ternary variables with $Pr(Z_0 = a 
\text{and } Z_1 = b) = p_{ab}$ for $0 \leq a, b \leq 2$, where $p_{00} + p_{01} + \ldots + p_{22} = 1$. What can you say about these probabilities $p_{ab}$ when $E(Z_1 | Z_0) = Z_0$?

64. [M22] (a) If $E(Z_{n+1} | Z_n) = Z_n$ for all $n \geq 0$, is $\langle Z_n \rangle$ a martingale? (b) If $\langle Z_n \rangle$ is a martingale, is $E(Z_{n+1} | Z_n) = Z_n$ for all $n \geq 0$?

65. [M21] If $\langle Z_n \rangle$ is any martingale, show that any subsequence $\langle Z_{m(n)} \rangle$ is also a martingale, where the nonnegative integers $\{m(n)\}$ satisfy $m(0) < m(1) < m(2) < \cdots$.

66. [M22] Find all martingales $Z_0, Z_1, \ldots$ such that each random variable $Z_n$ assumes only the values $\pm n$.

67. [M20] The Equitable Bank of El Dorado features a money machine such that, if you insert $k$ dollars, you receive $2k$ dollars back with probability exactly $1/2$; otherwise you get nothing. Thus you either gain $k$ or lose $k$, and your expected profit is $0$. (Of course these transactions are all done electronically.)

a) Consider, however, the following scheme: Insert $\$1$; if that loses, insert $\$2$; if that also loses, insert $\$4$; then $\$8$, etc. If you first succeed after inserting $2^k$ dollars, stop (and take the $2^{n+1}$ dollars). What’s your expected net profit at the end?

b) Continuing (a), what’s the expected total amount that you put into the machine?

c) If $Z_n$ is your net profit after $n$ trials, show that $\langle Z_n \rangle$ is a martingale.

68. [HM23] When J. H. Quick (a student) visited El Dorado, he decided to proceed by making repeated bets of $\$1$ each, and to stop when he first came out ahead. (He was in no hurry, and was well aware of the perils of the high-stakes strategy in exercise 67.)

a) What martingale $\langle Z_n \rangle$ corresponds to this more conservative strategy?

b) Let $N$ be the number of bets that Quick made before stopping. What is the probability that $N = n$?

c) What is the probability that $N \geq n$?

d) What is $E(N)$?

e) What is the probability that $\min(Z_0, Z_1, \ldots) = -m$? (Possible “gambler’s ruin.”)

f) What is the expected number of indices $n$ such that $Z_n = -m$, given $m \geq 0$?

69. [M20] Section 1.2.5 discusses two basic ways by which we can go from permutations of $\{1, \ldots, n-1\}$ to permutations of $\{1, \ldots, n\}$: “Method 1” inserts $n$ among the previous elements in all possible ways; “Method 2” puts a number $k$ from 1 to $n$ in the final position, and adds $k$ to each previous number that was $\geq k$.

May 20, 2015
Show that, using either method, every permutation can be associated with a node of Fig. 1, using a rule that obeys the probability assumptions of Pólya’s urn model.

70. [M85] If Pólya’s urn model is generalized so that we start with \( c \) balls of different colors, is there a martingale that generalizes Fig. 1?

71. [M81] (G. Pólya.) What is the probability of going from node \((r, b)\) to node \((r', b')\) in Fig. 1, given \( r', r, b, \) and \( b' \) with \( r' \geq r \) and \( b' \geq b \)?

72. [M81] Let \( X_n \) be the red-ball indicator for Pólya’s urn, as discussed in the text. What is \( E(X_1, X_2, \ldots, X_m) \) when \( 0 < n_1 < n_2 < \cdots < n_m \)?

73. [M84] The ratio \( Z_n = r/(n+2) \) at node \((r, n+2-r)\) of Fig. 1 is not the only martingale definable on Pólya’s urn. For example, \( r/[n=r-1] \) is another; so is \( r/(r+1)/2^n \).

Find the most general martingale \((Z_n)\) for this model: Given any sequence \( a_0, a_1, \ldots \), show that there’s exactly one suitable function \( Z_n = f(r, n) \) such that \( f(1, k) = a_k \).

74. [M80] (Bernard Friedman’s urn.) Instead of contributing a ball of the same color, as in Fig. 1, suppose we use the opposite color. Then the process changes to

and the probabilities of reaching each node become quite different. What are they?

75. [M85] Find an interesting martingale for Bernard Friedman’s urn.

76. [M80] If \( \langle Z_n \rangle \) and \( \langle Z'_n \rangle \) are martingales, is \( \langle Z_n + Z'_n \rangle \) a martingale?

77. [M81] Prove or disprove: If \( \langle Z_n \rangle \) is a martingale with respect to \( \langle X_n \rangle \), then \( \langle Z_n \rangle \) is a martingale with respect to itself (that is, a martingale).

78. [M80] A sequence of random variables \( \langle V_n \rangle \) for which \( E(V_{n+1} | V_0, \ldots, V_n) = 1 \) is called “multiplicatively fair.” Show that \( Z_n = V_0 V_1 \cdots V_n \) is a martingale in such a case. Conversely, does every martingale lead to a multiplicatively fair sequence?

79. [M80] (De Moivre’s martingale.) Let \( X_1, X_2, \ldots \) be a sequence of independent coin tosses, with \( P(\text{"heads" occurred on the nth toss}) = P(X_n = 1) = p \) for each \( n \). Show that \( Z_n = (q/p)^2(X_1 + \cdots + X_n)^{n} \) defines a martingale, where \( q = 1 - p \).

80. [M80] Are the following statements true or false for every fair sequence \( \langle Y_n \rangle \)?
   (a) \( E(Y_2^2 Y_3) = 0 \), (b) \( E(Y_3^2 Y_3^2) = 0 \), (c) \( E(Y_1^2 Y_3^2 \cdots Y_{n-1}^2) = 0 \) if \( n_1 < n_2 < \cdots < n_m \).

81. [M81] Suppose \( E(X_{n+1} | X_0, \ldots, X_n) = X_n + X_{n-1} \) for \( n \geq 0 \), where \( X_{n-1} = 0 \). Find sequences \( a_n \) and \( b_n \) of coefficients so that \( Z_n = a_n X_n + b_n X_{n-1} \) is a martingale, where \( Z_0 = X_0 \) and \( Z_1 = 2X_0 - X_1 \). (We might call this a “Fibonacci martingale.”)

82. [M80] In the game of Ace Now, let \( X_n = \) [the nth card is an ace], with \( X_0 = 0 \).
   a) Show that \( Z_n = (4 - X_1 - \cdots - X_n)/(52 - n) \) satisfies (28) for \( 0 \leq n < 52 \).
   b) Consequently \( E Z_X = 1/13 \), regardless of the stopping rule employed.
   c) Hence all strategies are equally good (or bad); you win $0 on average.
83. [HM22] Given a sequence \( \{X_n\} \) of independent and nonnegative random variables, let \( S_n = X_1 + \cdots + X_n \). If \( N_n(x_0, \ldots, x_{n-1}) \) is any stopping rule and if \( N \) is defined by (31), prove that \( E S_N = E \sum_{i=1}^N E X_i \). (In particular, if \( E X_n = E X_1 \) for all \( n > 0 \) we have “Wald’s equation,” which states that \( E S_N = \left( E N \right) \langle E X_1 \rangle \).)

84. [HM21] Let \( f(x) \) be a convex function for \( a \leq x \leq b \), and assume that \( \{Z_n\} \) is a martingale such that \( a \leq Z_n \leq b \) for all \( n \geq 0 \). (Possibly \( a = -\infty \) and/or \( b = +\infty \).)
   a) Prove that \( f(Z_n) \) is a submartingale.
   b) What can you say if the sequence \( \{Z_n\} \) is assumed only to be a submartingale?

85. [M20] Suppose there are \( R_n \) red balls and \( B_n \) black balls at level \( n \) of Pólya’s urn (Fig. 1). Prove that the sequence \( \{R_n/B_n\} \) is a submartingale.

86. [M22] Prove (33) by inventing a suitable stopping rule \( N_{n+1}(Z_0, \ldots, Z_n) \).

87. [M17] What does the maximal inequality (33) reveal about the chances that Pólya’s urn will hold thrice as many red balls as black balls at some point?

88. [HM30] Let \( S = \sup Z_n \) be the least upper bound of \( Z_n \) as \( n \to \infty \) in Fig. 1.
   a) Prove that \( S > 1/2 \) with probability \( \ln 2 \approx .693 \).
   b) Similarly, show that \( \Pr(S > 2/3) = \ln 3 - \pi/\sqrt{27} \approx .494 \). 
   c) Generalize to \( \Pr(S > (t-1)/t) \), for all \( t \geq 2 \). Hint: See exercise 7.2.1.6-36.

89. [M16] Let \( \{X_1, \ldots, X_n\} \) be random variables that have the Bernoulli distribution \( B(p, \ldots, p_n) \). Use (37) to show that \( \Pr(X_1 + \cdots + X_n \geq p_1 + \cdots + p_n + x) \leq e^{-2x^2/n} \).

90. [HM25] The Hoeffding–Azuma inequality (37) can be derived as follows:
   a) Show first that \( \Pr(Y_1 + \cdots + Y_n \geq x) \leq \frac{e^{t^2/2} - e^{-t^2/2}}{e^{t^2/2}} \) for all \( t > 0 \).
   b) If \( 0 \leq p \leq 1 \) and \( q = 1 - p \), show that \( e^{tq} \leq e^{t^2/2} + Y h(t) \), where \( h(t) = -tp + \ln(q + pe^t) \) and \( q(t) = -pt + \ln(e^t - 1) \).
   c) Prove that \( f(t) \leq t^2/8 \). Hint: Use Taylor’s formula, Eq. 1.2.11-3-(5).
   d) Consequently \( a \leq Y \leq b \) implies \( e^{ty} \leq e^{ty^2/8} + Y h(t) \), for some function \( h(t) \).
   e) Let \( c = \ell^2/8 \), where \( c_k = kb_k - n_k \). Prove that \( E(e^{c_1Y_1 + \cdots + c_nY_n}) \leq e^{ct^2/8} \).
   f) We obtain (37) by choosing the best value of \( t \).

91. [M20] Prove that Doob’s general formula (39) always defines a martingale.

92. [M20] Let \( Q_n \) be the Doob martingale that corresponds to Pólya’s urn (27) when \( Q = X_n \), for some fixed \( m > 0 \). Calculate \( Q_0, Q_1, Q_2, \) etc.

93. [M20] Solve the text’s hashing problem under the more general model considered in the bin-packing problem: Each variable \( X_j \) has probability \( p_{x_j} \) of being equal to \( k \), for \( 1 \leq j \leq k \), and \( 1 \leq k \leq m \). What formula do you get instead of (44)?

94. [M22] Where is the fact that the variables \( \{X_1, \ldots, X_7\} \) are independent used in the previous exercise?

95. [M20] True or false: “Pólya’s urn q.s. accumulates more than 100 red balls.”

96. [HM22] Let \( X \) be the number of heads seen in \( n \) flips of an unbiased coin. Decide whether each of the following statements about \( X \) is a.s., q.s., or neither, as \( n \to \infty \):
   (i) \(|X - n/2| < \sqrt{n \ln n} \)
   (ii) \(|X - n/2| < \sqrt{n \ln n} \)
   (iii) \(|X - n/2| < \sqrt{n \ln n} \)
   (iv) \(|X - n/2| < \sqrt{n} \).

97. [HM21] Suppose \( \lfloor n^{1+\delta} \rfloor \) items are hashed into \( n \) bins, where \( \delta \) is a positive constant. Prove that every bin q.s. gets between \( \frac{1}{2}n^\delta \) and \( 2n^\delta \) of them.

May 20, 2015
98. [MB1] Many algorithms are governed by a loop of the form

\[ X \leftarrow n; \text{ while } X > 0, \text{ set } X \leftarrow X - F(X) \]

where \( F(X) \) is a random integer in the range \([1 \ldots X]\). We assume that each integer \( F(X) \) is completely independent of any previously generated values, subject only to the requirement that \( EF(j) \geq g_j \), where \( 0 < g_1 \leq g_2 \leq \cdots \leq g_n \).

Prove that the loop sets \( X \leftarrow X - F(X) \) at most \( 1/g_1 + 1/g_2 + \cdots + 1/g_n \) times, on the average. (If one step reduces by \( g_n \), then perhaps \([1/g_n] \) of a step reduces by \( 1 \).)

99. [HM30] Show that the result in the previous exercise holds even when the range of \( F(X) \) is \((-\infty \ldots X]\), given \( 0 < g_1 \leq \cdots \leq g_n \leq g_{n+1} \leq \cdots \). (Thus \( X \) might increase.)

100. [HM17] A certain randomized algorithm takes \( T \) steps, where \( \Pr (T = t) = p_t \) for \( 1 \leq t \leq \infty \). Prove that \( (a) \lim_{n \to \infty} E \min (m, T) = E T; \lim_{n \to \infty} p_n = 0 \).

101. [HM22] Suppose \( X = X_1 + \cdots + X_m \) is the sum of independent geometrically distributed random integers, with \( \Pr (X_i = n) = p_i (1 - p_i)^{n-1} \) for \( n \geq 1 \). Prove that \( \Pr (X \geq \mu r_i) \leq re^{-r} \) for all \( r \geq 1 \), where \( \mu = E X = \sum \mu_i p_i \).

102. [MB20] Cora collects coupons, using a random process. After already owning \( k - 1 \) of them, her chance of success when trying for the \( k \)th is at least one chance in \( s_k \), independent of any previous successes or failures. Prove that she will own \( m \) coupons before making \((s_1 + \cdots + s_m) \ln n \) trials. And she will own \( m \) coupons in \( (s_1 + \cdots + s_m) \ln n \) trials to obtain the \( k \)th coupon, for each \( k \leq m \), if \( m = O(n^{-1/2}) \).

103. [MB30] This exercise is based on two functions of the ternary digits \( \{0, 1, 2\} \):

\[ f_0(x) = \max (0, x - 1); \quad f_1(x) = \min (2, x + 1). \]

a) What is \( \Pr (f_X (f_{X_2} (\ldots (f_{X_i} (i)) \ldots )) = j) \), for each \( i \in \{0, 1, 2\} \), assuming that \( X_1, X_2, \ldots, X_m \) are independent, uniformly random bits?

b) Here's an algorithm that computes \( f_{X_1} (f_{X_2} (\ldots (f_{X_i} (i)) \ldots )) \) for \( i \in \{0, 1, 2\} \), and stops when all three values have coalesced to a common value:

Set \( a_{00}, a_{02} \leftarrow 012 \) and \( n \leftarrow 0 \). Then while \( a_0 \neq a_2 \), set \( n \leftarrow n + 1, \)

\[ t_{01} t_{21} \leftarrow \text{if } X_n \? \text{122: 001}, \text{and } a_{01} \leftarrow a_{02}, a_{12} \leftarrow a_{0a_2}. \]

Output \( a_0 \).

(Notice that \( a_0 \leq a_1 \leq a_2 \) always holds.) What is the probability that this algorithm outputs \( j \)? What are the mean and variance of \( N \), the final value of \( n \)?

c) A similar algorithm computes \( f_{X_1} (f_{X_2} (\ldots (f_{X_i} (i)) \ldots )) \), if we change \( 'a_{0a_1}, a_{02}' \) to \( 't_{0a} t_{1a} t_{2a}' \). What's the probability of output \( j \) in this algorithm?

d) Why on earth are the results of (b) and (c) so different?

e) The algorithm in (c) doesn't really use \( a_1 \). Therefore we might try to speed up process (b) by cleverly evaluating the functions in the opposite direction. Consider the following subroutine, called \( \text{sub} (T) \): Set \( a_{02} \leftarrow 002 \) and \( n \leftarrow 0 \). Then while \( n < T \) set \( n \leftarrow n + 1, X \leftarrow \text{random} \)

bit, and \( a_{02} \leftarrow \text{if } X_n \? f_1 (a_0 f_1 (a_2) : f_0 (a_0) f_0 (a_2)). \]

If \( a_0 = a_2 \) output \( a_0 \), otherwise output \( -1 \).

Then the algorithm of (b) would seem to be equivalent to

Set \( T \leftarrow 1, a \leftarrow -1 \); while \( a < 0 \) set \( T \leftarrow 2T \) and \( a \leftarrow \text{sub} (T) \); output \( a \).

Prove, however, that this fails. (Randomized algorithms can be quite delicate!)

f) Patch the algorithm of (e) and obtain a correct alternative to (b).

104. [MBI] Solve exercise 103(b) and 103(c) when each \( X_i \) is 1 with probability \( p \).
105. [M30] (Random walk on an n-cycle.) Given integers $a$ and $n$, with $0 \leq a \leq n$, let $N$ be minimum such that $(a + (-1)^k + \ldots + (-1)^{n-k}) \mod n = 0$, where $X_1, X_2, \ldots$ is a sequence of independent random bits. Find the generating function $g_k = \sum_{x=0}^N \Pr(X = k)x^{x}$. What are the mean and variance of $N$?

106. [M22] Consider the algorithm of exercise 103(b) when the digits are $\delta$-ary instead of ternary; thus $f_0(x) = \max(0, x - 1)$ and $f_1(x) = \min(d - 1, x + 1)$. Find the generating function, mean, and variance of the number of steps required before $a_0 = a_1 = \ldots = a_{d-1}$ is first reached in this more general situation.

107. [M22] (Coupling.) If $X$ is a random variable on the probability space $\Omega$ and $Y$ is another random variable on another probability space $\Omega'$, we can study them together by redefining them on a common probability space $\Omega$. All conclusions about $X$ or $Y$ are valid with respect to $\Omega$, provided that we have $\Pr(X = x) = \Pr'(X = x)$ and $\Pr(Y = y) = \Pr''(Y = y)$ for all $x$ and $y$.

Such “coupling” is obviously possible if we let $\Omega$ be the set $\Omega' \times \Omega''$ of pairs $\{\omega', \omega'' \mid \omega' \in \Omega', \omega'' \in \Omega''\}$, and if we define $\Pr(\omega, \omega') = \Pr'(\omega') \Pr''(\omega'')$ for each pair of events. But coupling can also be achieved in many other ways.

For example, suppose $\Omega'$ and $\Omega''$ each contain only two events, $\{a, b\}$ and $\{\mathbf{a}, \mathbf{b}\}$, with $\Pr(\mathbf{a}) = p$, $\Pr(\mathbf{b}) = 1 - p$, $\Pr'(\mathbf{a}) = q$, $\Pr'(\mathbf{b}) = 1 - q$. We could couple them with a four-event space $\Omega = \{\mathbf{a}, \mathbf{b}, a, b\}$, having $\Pr(\mathbf{a}) = pq$, $\Pr(\mathbf{b}) = p(1-q)$, $\Pr(a) = (1-p)q$, $\Pr(b) = (1-p)(1-q)$. But if $p < q$ we could also get by with just three events, letting $\Pr(\mathbf{a}) = p$, $\Pr(\mathbf{b}) = q - p$, $\Pr(a) = 1 - q$. A similar scheme works when $p > q$, omitting $\mathbf{b}$. And if $p = q$ we need only two events, $\mathbf{a}$ and $\mathbf{b}$.

a) Show that if $\Omega'$ and $\Omega''$ each have just three events, with respective probabilities $\{p_1, p_2, p_3\}$ and $\{q_1, q_2, q_3\}$, they can always be coupled in a five-event space $\Omega$.

b) Also, four events suffice if $\{p_1, p_2, p_3\} = \{1/3, 1/3, 1/3\}$, $\{q_1, q_2, q_3\} = \{1/3, 1/3, 1/3\}$.

c) But some three-event distributions cannot be coupled with fewer than five.

108. [HM91] If $X$ and $Y$ are integer-valued random variables such that $\Pr(X \geq n) \leq \Pr(Y \geq n)$ for all integers $n$, find a way to couple them so that $X \leq Y$ always holds.

109. [M22] Suppose $X$ and $Y$ have values in a finite partially ordered set $P$, and that

$$\Pr'(X \geq a \text{ for some } a \in A) \leq \Pr''(Y \geq a \text{ for some } a \in A),$$

for all $A \subseteq P$.

We will show that there's a coupling in which $X \leq Y$ always holds.

a) Write out exactly what needs to be proved, in the simple case where $P = \{1, 2, 3\}$ and the partial order has $1 \prec 2$, $2 \prec 3$. (Let $p_1 = \Pr'(X = k)$ and $q_1 = \Pr''(Y = k)$ for $k \in P$. When $P = \{1, \ldots, n\}$, a coupling is an $n \times n$ matrix $(p_{ij})$ of nonnegative probabilities whose row sums are $\sum_i p_{ij} = p_i$ and column sums are $\sum_j p_{ij} = q_j$.)

Compare this to the result proved in the preceding exercise.

b) Prove that $\Pr'(X \leq b \text{ for some } b \in B) \geq \Pr''(Y \leq b \text{ for some } b \in B)$, for all $B \subseteq P$.

c) A coupling between $n$ pairs of events can be viewed as a flow in a network that has $2n + 2$ vertices $\{x, y, 1, 2, \ldots, n, t\}$, where there are $p_{ij}$ units of flow from $x$ to $x_i$, $p_{ij}$ units of flow from $y_i$ to $y$, and $q_{ij}$ units of flow from $y_j$ to $t$. The “max-flow min-cut theorem” [see Section 7.5.3] states that such a flow is possible if and only if there are no subsets $I, J \subseteq \{1, \ldots, n\}$ such that (i) every path from $s$ to $t$ goes through some arc $s \to x_i$ for $i \in I$ or some arc $y_j \to t$ for $j \in J$, and (ii) $\sum_{ij} p_{ij} + \sum_{ij} q_{ij} < 1$. Use that theorem to prove the desired result.

110. [M22] If $X$ and $Y$ takes values in $\{1, \ldots, n\}$, let $p_k = \Pr'(X = k)$, $q_k = \Pr''(Y = k)$, and $r_k = \min(p_k, q_k)$ for $1 \leq k \leq n$. The probability that $X = Y$ in any coupling is obviously at most $r = \sum_{k=1}^n r_k$.

May 20, 2015
a) Show that there always is a coupling with $\Pr(X = Y) = r$.

b) Can the result of the previous exercise be extended, so that we have not only $\Pr(X \leq Y) = 1$ but also $\Pr(X = Y) = r$?

111. [M20] A family of $N$ permutations of the numbers $\{1, \ldots, n\}$ is called \textbf{minwise independent} if, whenever $1 \leq j \leq k \leq n$ and $\{a_1, \ldots, a_k\} \subseteq \{1, \ldots, n\}$, exactly $N/k$ of the permutations $\pi$ have $\min(a_1 \pi, \ldots, a_k \pi) = a_j$.

For example, the family $F$ of $N = 60$ permutations obtained by cyclic shifts of $123456, 123465, 152346, 152634, 164235, 154263, 165324, 165432, 165342$ can be shown to be minwise independent permutations of $\{1, 2, 3, 4, 5, 6\}$.

a) Verify the independence condition for $F$ in the case $k = 3$, $a_1 = 1$, $a_2 = 3$, $a_3 = 4$.

b) Suppose we choose a random $\pi$ from a minwise independent family, and assign the “sketch” $S_A = \min_{\pi \in A} a \pi$ to every $A \subseteq \{1, \ldots, n\}$. Prove that, if $A$ and $B$ are arbitrary subsets, $\Pr(S_A = S_B) = |A \cap B| / |A \cup B|$.

c) Given three subsets $A$, $B$, $C$, what is $\Pr(S_A = S_B = S_C)$?

112. [M22] The \textbf{size} of a family $F$ of minwise independent permutations must be a multiple of $k$ for each $k \leq n$, by definition. In this exercise we’ll see how to construct such a family with the minimum possible size, namely $N = \text{lcm}(1, 2, \ldots, n)$.

The basic idea is that, if all elements of the permutations in $F$ that exceed $m$ are replaced by $\infty$, the “truncated” family is still minwise independent in the sense that, if $\min_{\pi \in A} a \pi = \infty$, we can imagine that the minimum occurs at a random element of $A$. (This can happen only if $\pi$ takes all elements of $A$ to $\infty$.)

a) Conversely, show that an $m$-truncated family can be lifted to an $(m+1)$-truncated family if, for each subset $B$ of size $n - m$, we insert $m + 1$ equally often into each of $B$'s $n - m$ positions, within the permutations whose $\infty$'s are in $B$.

b) Use this principle to construct minimum-size families $F$.

113. [M23] Although minwise permutations are defined only in terms of the minimum operation, a minwise independent family actually turns out to be also \textbf{maxwise independent}—and even more is true!

a) Let $E$ be the event that $a \pi < k$, $b \pi = k$, and $c \pi > k$, for any disjoint sets $\{a_1, \ldots, a_t\}$, $\{b\}$, $\{c_1, \ldots, c_s\} \subseteq \{1, \ldots, n\}$. Prove that, if $\pi$ is chosen randomly from a minwise independent set, $\Pr(E)$ is the same as the probability that $E$ occurs when $\pi$ is chosen randomly from the set of all permutations. (For example, $\Pr(5\pi < 7, 2\pi = 7, 1\pi > 7, 8\pi > 7) = 6(n - 7)(n - 8)(n - 4)/n!$, whenever $n \geq 8$.)

b) Furthermore, if $\{a_1, \ldots, a_t\} \subseteq \{1, \ldots, n\}$, the probability that $a_j$ is the $r$th largest element of $\{a_1 \pi, \ldots, a_t \pi\}$ is $1/k$, whenever $1 \leq j, r \leq k$.

114. [M28] (The “\textit{combinatorial nullstelleinsatz}”) Let $f(x_1, \ldots, x_n)$ be a polynomial in which the coefficient of $x_1^{d_1} \ldots x_n^{d_n}$ is nonzero and each term has degree $d_1 + \cdots + d_n$. Given subsets $S_1, \ldots, S_n$ of the field of coefficients, with $|S_j| > d_j$ for $1 \leq j \leq n$, choose $X_1, \ldots, X_n$ independently and uniformly, with each $X_j \in S_j$. Prove that

$$
\Pr(f(X_1, \ldots, X_n) \neq 0) \geq \frac{|S_1| + \cdots + |S_n| - (d_1 + \cdots + d_n) + n}{|S_1| \cdots |S_n|}.
$$

\textbf{Hint:} See exercise 4.6.1–16.

115. [M21] Prove that an $m \times n$ grid cannot be covered by $p$ horizontal lines, $q$ vertical lines, $r$ diagonal lines of slope $1$, and $s$ diagonal lines of slope $-1$, if $m = p + 2[r/2] + 1$ and $n = q + 2[r/2] + 1$. \textbf{Hint:} Apply exercise 114 to a suitable polynomial $f(x, y)$.

\textit{May 20, 2015}
116. [HM25] Use exercise 114 to prove that, if \( p \) is prime, any multigraph \( G \) on \( n \) vertices with more than \( (p - 1)n \) edges contains a nonempty subgraph in which the degree of every vertex is a multiple of \( p \). (In particular, if each vertex of \( G \) has fewer than \( 2p \) neighbors, \( G \) contains a \( p \)-regular subgraph. A loop from \( v \) to itself adds two to \( v \)'s degree.) \( \text{Hint:} \) Let the polynomial contain a variable \( x_e \) for each edge \( e \) of \( G \).

117. [HM25] Let \( X \) have the binomial distribution \( B_n(p) \), so that \( \Pr(X = k) = \binom{n}{k} p^k (1 - p)^{n-k} \) for \( 0 \leq k \leq n \). Prove that \( X \) mod \( m \) is approximately uniform:

\[
\left| \Pr(X \mod m = r) - \frac{1}{m} \right| < \frac{2}{m} \sum_{j=1}^{\infty} e^{-8p (1-p)^2 n / m^2}, \quad \text{for } 0 \leq r < m.
\]

118. [M20] Prove that the second moment principle implies the Paley-Zygmund inequality

\[
\Pr(X \geq x) \geq \frac{(EX - x)^2}{EX^2}, \quad \text{if } 0 \leq x \leq EX.
\]

_Every man must judge for himself between conflicting vague probabilities._

— CHARLES DARWIN, letter to N. A. von Mengden (5 June 1879)
ANSWERS TO EXERCISES

It isn’t that they can’t see the solution.
It is that they can’t see the problem.

MATHMATICAL PRELIMINARIES REDUX

1. (a) A beats B in 5 + 0 + 5 + 5 + 0 + 5 cases out of 36; B beats C in 4 + 2 + 4 + 4 + 2 + 4; C beats A in 2 + 2 + 2 + 6 + 2 + 6.

(b) The unique solution, without going to more than six spots per face, is

\[ A = \begin{array}{|ccc|}
\hline
& & \\
& & \\
\hline
\end{array}, \quad B = \begin{array}{|ccc|}
\hline
& & \\
& & \\
\hline
\end{array}, \quad C = \begin{array}{|ccc|}
\hline
& & \\
& & \\
\hline
\end{array}. \]

(c) \( A = \{F_{m-2} \times 1, F_{m-1} \times 4\}, \quad B = \{F_m \times 3\}, \quad C = \{F_{m-1} \times 2, F_{m-2} \times 5\} \) makes \( \Pr(C > A) = F_{m-2} F_{m+1} / F_m^3 \); and we have \( F_{m-3} F_{m+1} = F_{m-1} F_m = (-1)^n \). [Similarly, with \( n \) faces and \( A = \{[n/\phi]^2 \times 1, [n/\phi] \times 4\} \), etc. the probabilities are \( 1/\phi - O(1/n) \).] See R. P. Savage, Jr., AMM 101 (1994), 429–436.

2. Let \( \Pr(A > B) = A, \quad \Pr(B > C) = B, \quad \Pr(C > A) = C \). We can assume that no \( x \) appears on more than one die; if it did, we could replace it by \( x + \epsilon \) in \( A \) and \( x - \epsilon \) in \( C \) (for small enough \( \epsilon \)) without decreasing \( A, B, \) or \( C \). So we can list the face elements in nondecreasing order and replace each one by the name of its die; for example, the previous answer (b) yields CBBBAAAACCCCBBA. Clearly \( AB, BC, \) and \( CA \) are never consecutive in an optimal arrangement of this kind: \( BA \) is always better than \( AB \).

Suppose the sequence is \( C^{a_1} B^{b_1} A^{a_2} \cdots C^{a_k} B^{b_k} A^{a_2} \) where \( c_i > 0 \) for \( 1 \leq i \leq k \) and \( b_i, a_i > 0 \) for \( 1 \leq i < k \). Let \( \alpha_i = a_i/(a_1 + \cdots + a_k), \quad \beta_i = b_i/(b_1 + \cdots + b_k), \quad \gamma_i = c_i/(c_1 + \cdots + c_k); \) then \( A = \alpha_1 \beta_1 + a_2 (\beta_1 + \beta_2) + \cdots, \quad B = \beta_1 \gamma_1 + b_2 (\gamma_1 + \gamma_2) + \cdots, \quad C = \gamma_2 a_1 + \gamma_3 (a_1 + a_2) + \cdots \). We will show that \( \min(A, B, C) \leq 1/\phi \) when the \( \alpha \)'s, \( \beta \)'s, and \( \gamma \)'s are nonnegative real numbers; then it is \( < 1/\phi \) when they are rational.

The key idea is that we can assume \( k \leq 2 \) and \( a_2 = 0 \). Otherwise the following transformation leads to a shorter array without decreasing \( A, B, \) or \( C \):

\[ \gamma_2' = \lambda \gamma_2, \quad \gamma_1' = \gamma_1 + \gamma_2 - \gamma_2', \quad \beta_2' = \lambda \beta_2, \quad \beta_1' = \beta_1 + \beta_2 - \beta_2', \quad \alpha_1' = \alpha_1/\lambda, \quad \alpha_2' = \alpha_1 + \alpha_2 - \alpha_1'. \]

Indeed, \( A' = A, \quad C' = C, \) and \( B' = B - (1 - \lambda)(\beta_1 - \lambda \beta_2) \gamma_2, \) and we can choose \( \lambda \) thus:

Case 1: \( \beta_1 \geq \beta_2 \). Choose \( \lambda = \alpha_1/(\alpha_1 + \alpha_2) \), making \( \alpha_2' = 0 \).

Case 2: \( \beta_1 < \beta_2 \) and \( \gamma_1/\gamma_2 \geq \beta_1/\beta_2 \). Choose \( \lambda = 1 + \gamma_1/\gamma_2 \), making \( \gamma_1' = 0 \).

Case 3: \( \beta_1 < \beta_2 \) and \( \gamma_1/\gamma_2 \leq \beta_1/\beta_2 \). Choose \( \lambda = 1 + \beta_1/\beta_2 \), making \( \beta_1' = 0 \).

Finally, then, \( A = \beta_1, \quad B = 1 - \beta_1 \gamma_2, \quad C = \gamma_2 \); they can’t all be greater than \( 1/\phi \).

Similarly, with \( n \) dice, the asymptotic optimum probability \( p_n \) satisfies \( p_n = \alpha_2^{(n)} = 1 - \alpha_1^{(n-1)} a_2^{(n)} = \cdots = 1 - \alpha_1^{(2)} \alpha_2^{(3)} = \alpha_1^{(2)}. \) One can show that \( f_n(1 - p_n) = 0, \)

May 20, 2015
where \( f_{n+1}(x) = f_n(x) - x f_{n-1}(x) \), \( f_0(x) = 1 \), \( f_1(x) = 1 - x \). Then \( f_n(x^2) \) is expressible as the Chebyshev polynomial \( x^{n+1} U_{n+1} \left( \frac{x}{2} \right) \); and we have \( p_n = 1 - 1/(4 \cos^2 \pi/(n + 2)) \).

3. Brute force (namely a program) finds eight solutions, of which the simplest is

\[
A = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}, \quad B = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix},
\]

all with respective probabilities \( \frac{1}{7}, \frac{6}{7}, \frac{16}{56} \). [If \( \mathbb{E} \) is also allowed, the unique solution]

\[
A = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}, \quad B = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}, \quad C = \begin{bmatrix}
1 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{bmatrix}
\]

has the property that every roll has exactly one die below the average and two above, with each of \( A, B, C \) equally likely to be below; hence all three probabilities are \( 2/3 \).


4. (a) The permutation \((1234)(56)\) takes \( A \to B \to C \to D \to A \). So \( B \) versus \( C \) is like \( A \) versus \( B \), etc. Also \( \Pr(A \text{ beats } C) = \Pr(C \text{ beats } A) = \Pr(B \text{ beats } D) = \Pr(D \text{ beats } B) = \frac{28}{49} \); \( \Pr(A \text{ and } C \text{ tie}) = \Pr(B \text{ and } D \text{ tie}) = \frac{14}{49} \).

(b) Assume by symmetry the players are \( A, B, C \). Then the bingoes are \( (A, B, C, AB, AC, BC, ABC) \) with respective probabilities \( 168, 216, 168, 48, 72, 36, 12 \)/720.

(c) It's \((A, AB, AC, ABC, ABCD)\) with probabilities \((120, 24, 48, 12, 0)\)/720.

5. (a) If \( A_4 = 1001 \) with probability \( .99 \), otherwise \( A_4 = 0 \), but \( B_4 = 1000 \) always, then \( P_{1000} = .99^{1000} \approx .000043 \). This example gives the smallest possible \( P_{1000} \), because \( \Pr(\{A_4 = B_1 \} + \cdots + \{A_4 > B_n \} > 0) = \Pr([\{A_4 > B_1 \} \cdots \{A_4 > B_n \}]) = P_{1000}^n \).

(b) Let \( E = q_0 + q_1 + \cdots + (A_4 - B_n) > 0 \geq \Pr([A_4 > B_1 \cdots A_4 > B_n]) = P_{1000}^n \).

(c) During the first \( n_4 \) rounds, the probability that either Alice or Bob has scored more than \( m_4 \) is at most \( n_4 (q_{k+1} + q_{k+2} + \cdots) = O(2^{-n_4}) \); and the probability that neither has ever scored \( m_4 \) is \( (1 - q_{k+1})^{n_4} \leq \exp(-q_{k+1} n_4) = \exp(-2/n_4) \). Also \( m_k > n_k m_{k+1} \) when \( k > 1 \). Thus Alice "quite surely" wins when \( k \) is even, but loses when \( k \) is odd, as \( k \to \infty \). [The American Statistician 43 (1989), 277–278.]

6. The probability that \( X_j = 1 \) is clearly \( p_1 = 1/(n-1) \); hence \( X_j = 0 \) with probability \( p_0 = (n-2)/(n-1) \). And the probability that \( X_i = X_j = 1 \) when \( i < j < k \) is \( p_1^2 \). Thus (see exercise 2), \( (X_i, X_j) \) will equal \((0, 1), (1, 0), \) or \((0, 0)\) with the correct probabilities \( p_0 p_1, p_1 p_0, p_0 p_0 \). But \( X_j = X_k = 1 \) with probability \( 0 \) when \( i < j < k \).

For 3-wise independence let \( \Pr(X_1 \cdots X_n = x_1 \cdots x_n) = a_{x_1 \cdots x_n} / (n-3)^3 \), where \( a_0 = 2 \binom{n-3}{2} , a_1 = \binom{n-3}{3} , a_2 = 1 \), and \( a_3 = 0 \).

7. Let \( f_m(n) = \sum_{i=0}^m \binom{m}{i} (-1)^i (n + 1 - m)^{-i} \), and define probabilities via \( a_j = f_k-j(n-j) \) as in answer 6. (In particular, we have \( f_0(n) = 1, f_1(n) = 0, f_2(n) = \binom{n-2}{2} \), \( f_3(n) = \binom{n-3}{3} + \binom{n-3}{2} \).) This definition is valid if we can prove that \( f_m(n) \geq 0 \) for \( n \geq m \), because of the identity \( \sum_{i=0}^m \binom{m}{i} f_{m-i}(n-j) = (n + 1 - m)^m \).

To prove that inequality, Schulte-Geers notes (see CMath (5.19)) that \( f_m(n) = \sum_{k=0}^m \binom{m}{k} (n-k)^{m-k} \leq \sum_{k=0}^m \binom{m}{k} (n-m)^m \leq n^m \), these terms pair up nicely to yield \( \sum_{k=0}^m k (n-m)^{m-k}_{[k \text{ even}]} + (n-m)^m_{[m \text{ even}]} \).

May 20, 2015

Chebyshev polynomial
Usiskin
Trybula
Moraleda
Stork
quite surely
8. If $0 < k < n$, the probability that $k$ of the variables have any particular setting is $1/2^k$, because the remaining variables have even parity as often as odd parity. So there's $(n - 1)$-wise independence, but not $n$-wise.

9. Give probability $1/2$ to $0 \ldots 0$ and $1 \ldots 1$; all other vectors have probability 0.

10. If $n > p$ we have $X_{p+1} = X_1$, so there's no independence. Otherwise, if $m < n \leq p$, there's $m$-wise independence because any $m$ vectors $(1, j, \ldots, j^{m-1})$ are linearly independent modulo $p$ (they're columns of Vandermonde's matrix; exercise 1.23–37); but the $X$'s are dependent $(m+1)$-wise, because a polynomial of degree $m$ cannot have $m+1$ different roots. If $m \geq n$ and $n \leq p$ there is complete independence.

Instead of working mod $p$, we could use any finite field in this construction.

11. We can assume that $n = 1$, because $(X_1 + \cdots + X_n)/n$ and $(X_{n+1} + \cdots + X_{2n})/n$ are independent random variables with the same discrete distribution. Then $\Pr|X_1 + X_2 - 2\alpha| \leq 2|X_1 - \alpha| \geq \Pr|X_1 - \alpha| = \Pr|X_2 - \alpha| \leq |X_1 - \alpha| = (1 + \Pr(X_1 = X_2))/2 > 1/2$. [This exercise was suggested by T. M. Cover.]

12. Let $w = \Pr(A$ and $B)$, $x = \Pr(A$ and $\bar{B})$, $y = \Pr(\bar{A}$ and $B)$, $z = \Pr(\bar{A}$ and $\bar{B})$. All five statements are equivalent to $w \geq xy$, or to $\sum |a_i| > 0$, or to $A$ and $B$ are strictly positively correlated (see exercise 6). [This exercise was suggested by E. Georgiadis.]

13. False in many cases. For example, take $\Pr(\bar{A}$ and $B$ and $\bar{C}) = \Pr(\bar{A}$ and $B$ and $\bar{C}) = 0$, $\Pr(A$ and $B$ and $C) = 2/7$, and all other probabilities 1/7.

14. Induction on $n$. [Philosophical Transactions 53 (1763), 370–418, proof of Prop. 6.]

15. If $\Pr(C) > 0$, this is the chain rule, conditional on C. But if $\Pr(C) = 0$, it’s false by our conventions, unless $A$ and $B$ are independent.

16. If and only if $\Pr(A \cap B \cap C) = 0 \neq \Pr(B)$ or $\Pr(\bar{A} \cap C) = 0$.

17. 4/51, because four of the cards other than the aces are aces.

18. Since $(M - X)(X - m) \geq 0$, we have $(M \cdot X) = (E \cdot X^2) + (m \cdot E) - m \cdot M \geq 0$. [See C. Davis and R. Bhatia, AMM 107 (2000), 353–356, for generalizations.]

19. (a) The binary values of $\Pr(X_n = 1)$ are $E(X_n)$ for $n = 0, 1, 2, \ldots$, are respectively $(0(10001001010101 \ldots), 0(01001001001110 \ldots), \ldots$; thus they’re the complemented reflections of the “magic masks” 7.1.3–47). The answer is therefore $(2n - 1)/(2^{n+1} - 1) = 1/(2^n + 1)$.

(b) $\Pr(X_0X_1 \ldots X_{n-1} = x_0x_1 \ldots x_{n-1}) = 2^n - 1$ and $\Pr(X_n = 1)$ can be read off from the magic masks by ANDing and complementing. [See E. Lulacs, Characteristic functions (1960), 119, for related theory].

(c) The infinite sum $S$ is well defined because $\Pr(S = \infty) = 0$. Its expectation $E \cdot S = \sum_{n \to 0} 1/(2^{n+1}) \approx 0.9999$ corresponds to the case $z = 1/2$ in answer 7.13–41(c). By independence, var $S = \sum_{n \to 0} \text{var } X_n = \sum_{n \to 0} 2^n/(2^{n+1}) \approx 0.44148$.

(d) The parity number $E \cdot R = (01010010100101 \ldots)$ has the decimal value

0.41234 40336 40107 59778 33633 68238 45528 30895

and can be shown to equal $\frac{1}{2} - \frac{1}{4}P$ where $P = \prod_{n \to 0} (1 - 1/2^{n})$ [R. W. Gosper and R. Schroeppel, MIT AI Laboratory Memo 239 (29 February 1972), Hack 122], which is transcendental. [K. Mahler, Mathematische Annalen 101 (1929), 342–366; 103 (1930), 532]. (Furthermore it turns out that $1/P - 1/2 = \sum_{n \to 0} 1/\prod_{n \to 0} (2^n - 1)$.) Since $R$ is binary, $\text{var } R = (E \cdot R)(1 - E \cdot R) \approx 0.241233$.

May 20, 2015

Vandermonde’s matrix
Cover
positively correlated
Georgiadis
chain rule
Davis
Bhatia
magic masks
Lulacs
parity number
Gosper
Schroeppel
HARMEM
Mahler
Thas-Morse constant
(e) Zero (because π is irrational, hence \( p_0 + p_1 + \cdots = \infty \)). However, if we ask the analogous question for Euler’s constant γ instead of π, nobody knows the answer.

(f) \( \text{E} Y_n = 2 \text{E} X_n \); in fact, \( \text{Pr}(Y_0 Y_1 Y_2 \cdots = x_0 x_1 x_2 \cdots) = 2^n x_0 x_1 x_2 \cdots \mod 1 \), because we shift the binary representation one place to the left (and drop any carry). Thus in particular, \( Y_n Y_n = 2 \text{E} X_n X_n = \frac{2}{\text{E}} Y_n \text{E} Y_n \) when \( m \neq n \); \( Y_n \) and \( Y_n \) are negatively correlated because \( \text{cov}(Y_n, Y_n) = -\frac{1}{\text{E}} Y_n Y_n \).

(g) Clearly \( \text{E} T = 2 \text{E} S \). Also \( \text{E} T^2 = 2 \text{E} S^2 \), because \( \text{E} Y_n Y_n = 2 \text{E} X_n X_n \) for all \( m \) and \( n \). So \( \text{var}(T) = 2(\text{var}(S) + (\text{E} S)^2) = 2(\text{var}(S) + 2(\text{E} S)^2) \approx 0.17237 \).

20. Let \( p_1 = \text{E} X_j \). We must prove, for example, that \( E(X_1(1 - X_2)(1 - X_3)X_4) = p_1(1 - p_2)(1 - p_3)p_4 \) when \( k \geq 4 \). But this is \( E(X_1 X_4 - X_1 X_3 X_4 - X_3 X_4 + X_1 X_2 X_3 X_4) = p_1 p_4 - p_1 p_3 p_4 - p_1 p_2 p_4 + p_1 p_2 p_3 p_4 \).

21. From the previous exercise we know that they can’t both be binary. Let \( X \) be binary and \( Y \) ternary, taking the values \( (0,0) \), \( (0,1) \), \( (0,2) \), \( (1,0) \), \( (1,1) \), \( (1,2) \) with probabilities respectively proportional to \( (a,b,3a-b+3d,d,1,1) \). Then \( \text{E} X Y = 3/2D \), \( \text{E} X = 2/D \), and \( \text{E} Y = 3/2 \), where \( D = 4a + 2b + 4d + 2 \).

22. By (8) we have \( \text{Pr}(A_1 \cup \cdots \cup A_n) = E[A_1 \cup \cdots \cup A_n] = E \text{max}(A_1, \ldots, A_n) \leq E[A_1] + \cdots + E[A_n] = \text{Pr}(A_1) + \cdots + \text{Pr}(A_n). \)

23. The hinted probability is \( \text{Pr}(X_1 = 0 \text{ and } X_1 + \cdots + X_{n-1} = s) \). So it equals \( (\binom{n-1}{s})p^{n-s}(1-p)^s \). To get \( B_{m,n}(p) \), sum it for \( r = n - m \) and \( n - m \leq s \leq n \). For an algebraic rather than probabilistic/combinatorial proof, see CMath, exercise 8.17.

24. (a) The derivative of \( B_{m,n}(x) = \sum_{i=0}^{n-m} \binom{n}{k} x^k (1-x)^{n-k} \) is

\[
B'_{m,n}(x) = \sum_{k=0}^{n-m} \binom{n}{k} kx^{k-1} (1-x)^{n-k} - (n-k)x^k (1-x)^{n-1-k}
\]

\[
= n \sum_{k=0}^{n-m} \binom{n-1}{k} x^{k} (1-x)^{n-k} - \sum_{k=0}^{m} \binom{n-1}{k} x^k (1-x)^{n-1-k}
\]

\[
= n \binom{n-1}{n-m} x^m (1-x)^{n-m}.
\]

[See Karl Pearson, Biometrika 16 (1924), 202–203.]

(b) The hint says that \( \int_0^{a+b} x^m (1-x)^n dx \leq \int_0^{a/\alpha} x^m (1-x)^n dx \leq \int_0^{(a+b)/\alpha} x^m (1-x)^n dx \), where \( a \) and \( b \) are positive.

(c) Let \( t_k = \binom{n}{k} m^k (n-m)^{n-k} \). When \( m \geq n/2 \) we can show that \( 1 - B_{m,n}(m/n) = \sum_{k=0}^{n-m} t_k / m^n < B_{m,n}(m/n) = \sum_{k=0}^{n-m} t_k / m^n \), because \( t_{m+d} < t_{m+1+d} \) for \( 1 \leq d \leq n-m \). For if \( r_d = t_{m+d} / t_{m+1+d} \), we have \( r_1 = m/(m+1) < 1 \); also

\[
\frac{r_{d+1}}{r_d} = \frac{(n - m + d)(m - n - d)m^2}{(m + 1 + d)(m + 1 - d)(n - m)^2} < 1,
\]

May 20, 2015
because \((m+1)^2-d^2-((n-m)^2-d^2)=\left((m+1)(n-m)^2+(2m-n)d^2\right)\).

[Peter Neumann proved in *Wissenschaftliche Zeitschrift der Technischen Universität Dresden* 15 (1966), 223–226, that \(m\) is the median. The argument in part (c) is due to Nick Lord, in *The Mathematical Gazette* 94 (2010), 331–332.]

25. (a) \((\binom{n}{k}) - (\binom{n}{k+1})\) is \(\sum_{p_{ij}q_{ij}f_{ij}(n-k) - p_{ij}/(k+1)}\), summed over all partitions of \(\{1, \ldots, n\}\) into disjoint sets \(I \cup J \cup \{k\}\), where \(|I|=k, |J|=n-k-1, p_I=\prod_{i \in I} q_i, q_J=\prod_{i \in J} q_i\). And \(q_I(n-k) - p_I/(k+1) \geq 0 \iff p_I \leq (k+1)/(n+1)\).

(b) Given \(p_1, \ldots, p_{n-1}\), the quantity \((\binom{n}{k})\) is maximized when \(p_n = p\), by (a). The same argument applies symmetrically to all indices \(j\).

26. The inequality is equivalent to \(r_{n-k}^2 \geq r_{n-k+1}^2\), which was stated without proof on pages 242–245 of Newton’s *Arithmetica Universalis* (1707), then finally proved by Sylvester many years later [Proc. London Math. Soc. 1 (1865), 1–16]. We have \(nr_{n-k} = kpr_{n-k-1} + (n-k)(q_{n-k}r_{n-k-1})\); hence \(n^2(r_{n-k}^2 - r_{n-k-1}^2) = (pr_{n-k-1} - q_{n-k}r_{n-k-1})^2 + (k^2 - 1)p^2 + (n-k)^2(q_{n-k}^2 - 1)q_{n-k}B + ((n-k)^2 - 1)q_{n-k}C\), where \(A = r_{n-k-1}r_{n-k}, B = r_{n-k-1} + r_{n-k}, C = r_{n-k-1}^2 + r_{n-k-1}\), and \(r_{n-k-1}^2 - r_{n-k-1}\) are nonnegative, by induction on \(n\).

27. \(\sum_{k=0}^{m} \binom{n}{k} = \sum_{k=0}^{n} \binom{n-1}{k} (1 - p\binom{n-1}{k})\), by the same argument as before.

28. (a) \((\binom{n}{k}) = \binom{n-1}{k} + \binom{n-1}{k+1}\) and \(E\left|g(X) = \sum_{k=0}^{n} \binom{n}{k} / 2^n\right| h_k\), where \(A = 1 - p_{n-1}, p_{n-1} = B - nA, C = p_{n-1}A, h_k = \lambda g(k) + Bg(k+1) + Cg(k+2)\). If the \(p_i\)'s aren't all equal, we may assume that \(p_{n-1} < p < p_n\). Setting \(p_{n-1} = p_{n-1} + \epsilon\) and \(p_n = p_n - \epsilon\), changes \(A, B, C\) to \(A' = A + \delta, B' = B - \delta, C' = C + \delta\), where \(\delta = (p_n - p)(p - p_{n-1})\); hence \(h_k\) changes to \(h_k' = h_k + \delta g(k) - 2g(k+1) + g(k+2)\). Convex functions satisfy \(g(k) - 2g(k+1) + g(k+2) \geq 0\), by (c) with \(x = k\) and \(y = k+2\); hence we can permute the \(p_i\) and repeat this transformation until \(p_j = p\) for \(1 \leq j \leq n\).

(b) Suppose \(E\left|g(X) = \sum_{k=0}^{n} \binom{n}{k}\right| h_k\), and that \(r\) of the \(p_i\) are 0 and \(s\) of them are 1. Let \(a\) satisfy \((n-r-s)a + s = np\) and assume that \(0 < p_{n-1} < a < p_n\). As in part (a) we can write \(E\left|g(X) = \alpha A\right| + \beta B + \gamma C\) for some coefficients \(\alpha, \beta, \gamma\).

If \(\alpha - 2\beta + \gamma > 0\), the transformation in (a) (but with \(a\) in place of \(p\)) will increase \(E\left|g(X)\right|\). And if \(\alpha - 2\beta + \gamma < 0\), we could increase it with a similar transformation, using \(\delta = -\min(p_{n-1}, 1 - p_n)\). Therefore \(\alpha - 2\beta + \gamma = 0\); and we can repeat the transformation of (a) until every \(p_j = 0, 1, \text{ or } a\).

(c) Since \(\sum_{k=0}^{m} \binom{n}{k} = 0\) when \(s > m\), we may assume that \(s \leq m\), hence \(r + s < n\). For this function \(g(k) = 0 \leq k \leq m\) we have \(\alpha - 2\beta + \gamma = \binom{n-m}{m}\). This difference cannot be positive if the choice of \(\{p_1, \ldots, p_n\}\) is optimum; in particular we cannot have \(s = m\). If \(r > 0\) we can make \(p_{n-k} = 0\) and \(p_{n-k-1} = a\), so that \(\binom{n-m}{m} = \binom{n-m-1}{m} / (1 - a)^{n-m-1} / a^{n-m} \) and \(\binom{n-m}{m} = \binom{n-m-1}{m} / (1 - a)^{n-m} - 1\). But then the ratio \(\binom{n-m}{m} / \binom{n-m}{m} = (n - m - a)/(1 - a)\) exceeds 1; hence \(r = 0\).

Similarly if \(s > 0\) we can set \(p_{n-1} = p_{n-1} = a\), getting the ratio \(\binom{n-m}{m} / \binom{n-m}{m} = (n - m - a)/(1 - a)\) exceeds 1. In this case \(\binom{n-m}{m} = \binom{n-m}{m}\) if and only if \(np = m + 1\); we can transform without changing \(E\left|g(X)\right|\), until \(s = 0\) and each \(p_j = p\).

[Reference: *Annals of Mathematical Statistics* 27 (1956), 713–721. The coefficients \(\binom{n}{k}\) also have many other important properties; see exercise 7.2.15–63, and the survey by J. Pitman in *J. Combinatorial Theory* A77 (1997), 279–303.]
30. ANSWERS TO EXERCISES

If \( p = (m + 1)/n \) we have \( R_{m,n}(p) = \left( (1 - p)(m + 1)/(1 - p)(m + 1) \right)^{n-m} \). So if \( m > 0 \) and \( \hat{p} = m/(n-1) \), we can apply exercise 28(c) with \( p_1 = \cdots = p_{n-1} = \hat{p} \) and \( p_n = 1 \):

\[
B_{m,n}(p) \geq \sum_{k=0}^{n-1} \binom{n}{k} (\hat{p})^k (1 - \hat{p})^{n-k} = B_{m-1,n-1}(\hat{p}).
\]

When \( 1 \leq m < n-1 \), let \( Q_{m,n}(p) = B_{m,n}(p) - R_{m,n}(p) \). The derivative

\[
Q'_{m,n}(p) = (n - m)\binom{n}{m}(1 - p)^{n-m-1}(A - F(p)) / ((1 - p)(m + 1))^{n-m+1},
\]

where \( A = (m + 1)^{n-m} / \binom{n}{m} > 1 \) and \( F(p) = p^n ((1 - p)(m + 1))^{n-m+1} \), begins positive at \( p = 0 \), eventually becomes negative but then is positive again at \( p = 1 \). (Notice that \( F(0) = 0 \), and \( F(p) \) increases dramatically until \( p = (m + 1)/(n + 1) \); then it decreases to \( F(1) = 1 \). The facts that \( Q_{m,n}(\frac{m+1}{n}) \geq 0 = Q_{m,n}(0) = Q_{m,n}(1) \) now complete the proof, because \( Q'_{m,n}(p) \) changes sign only once in \([0, \frac{m+1}{n}] \). \[Annals of Mathematical Statistics 36 (1965), 1272–1278.\]

30. (a) \( \Pr(X_k = 0) = n/(n + 1) \); hence \( p = n/(n + 1) \) is \( \geq 0.368 \).

(b) (Solution by J. H. Elton.) Let \( p_{x_m} = \Pr(X_k = m) \). Assume that these probabilities are fixed for \( 1 \leq k \leq n \), and let \( x_m = p_{x_m} \). Then \( x_0 = x_1 + 2x_2 + 3x_3 + \cdots \); we want to minimize \( p = \sum_{m=1}^{n-1} (A_m + (m - 1)A_0)x_m \) in nonnegative variables \( x_1, x_2, \ldots \), where \( A_m = \Pr(X_1 = \cdots = X_{n-1} \leq n-m) \), subject to the condition \( \sum_{m=1}^{n} mx_m = 1 \). Since all coefficients of \( p \) are nonnegative, the minimum is achieved when all \( x_m \) for \( m \geq 1 \) are zero except for one value \( m = m_n \), which minimizes \( (A_m + (m - 1)A_0)/m \). And \( m_n \leq n - 1 \), because \( A_m = 0 \) whenever \( m > n \). Similarly \( m_1, \ldots, m_n \) also exist.

(c) (Solution by E. Schulze-Geersen.) Letting \( m_1 = \cdots = m_n = m \leq n - 1 \), we want to minimize \( B_{[\frac{m}{n}],\frac{1}{n}}^{m,n}(1/t) \). The inequality of Samuels in exercise 29 implies that

\[
B_{m,n}(p) \geq \left( 1 - \frac{1}{f(m,n,p)} \right)^n \text{ for } p \leq \frac{m + 1}{n}, \text{ where } f(m,n,p) = \frac{(m + 1)(1 - p)n}{(n - m)p},
\]

because we can set \( x = (1 - p)(m + 1)/(1 - p)(m + 1) \) in the arithmetic-geometric mean inequality \( x^n / (\binom{n}{m} \binom{x}{m})^{n/m} \). Now \( 1/t \leq \frac{[n/t] + 1}{(n + 1)} \) and \( f([n/t], n, 1/t) \geq n! \); hence \( B_{[\frac{m}{n}],\frac{1}{n}}^{m,n}(1/t) \geq n!/(n + 1)^n \).

31. This result is immediate because \( \Pr(f([A_1], \ldots, [A_n]) = E f([A_1], \ldots, [A_n]) \). But a more detailed, lower-level proof will be helpful with respect to exercise 32.

Suppose, for example, that \( n = 4 \). The reliability polynomial is the sum of the reliability polynomials for the minterms of \( f \); so it suffices to show that the result is true for functions like \( x_1 \wedge x_2 \wedge x_3 \wedge x_4 = x_1(1 - x_2)(1 - x_3) x_4 \). And it’s clear that \( \Pr(A_1 \wedge A_2 \wedge A_3) = \Pr(A_1 \wedge A_2 \wedge A_4) - \Pr(A_1 \wedge A_2 \wedge A_3 \wedge A_4) = \pi_{14} - \pi_{124} - \pi_{134} + \pi_{1234} \). (See exercise 7.1.1.12; also recall the inclusion-exclusion principle.)

32. The 2nd minterm probabilities in the previous answer must all be nonnegative, and they must sum to 1. We’ve already stipulated that \( \pi_{14} = 1 \), so the sum-to-1 condition is automatically satisfied. (The condition stated in the exercise when \( I \subseteq J \) is necessary but not sufficient; for example, \( \pi_{12} \) must be \( \geq \pi_1 + \pi_2 - 1 \).

May 20, 2015
33. The three events \((X, Y) = (1, 0), (0, 1), (1, 1)\) occur with probabilities \(p, q, r\), respectively. The value of \(E(X | Y = 1)\) is \(r/(q + r)\), \(r/(q + r)\) in those cases. Hence the answer is \(pz + (q + r)y^*/(q + r)\). This example demonstrates why univariate generating functions are not used in the study of conditional random variables such as \(E(X | Y)\). But we do have the simple formula \(E(X | Y = k) = \left(\left[\frac{z^k}{G(1, z)}\right] \frac{1}{G(1, z)}\right)\).

34. The right-hand side is

\[
\sum_\omega E(X | Y) \Pr(\omega) = \sum_\omega \sum_{\omega'} \Pr(\omega) \Pr(\omega') \Pr(Y(\omega') = Y(\omega)) / \Pr(Y = Y(\omega))
\]

\[
= \sum_\omega \Pr(\omega) \sum_{\omega'} \Pr(\omega') \Pr(Y(\omega') = Y(\omega)) / \Pr(Y = Y(\omega))
\]

\[
= \sum_\omega \Pr(\omega) \sum_{\omega'} \Pr(\omega') \Pr(Y(\omega') = Y(\omega')) / \Pr(Y = Y(\omega'))
\]

35. Part (b) is false. If, for instance, \(X, Z\) are independent random bits and \(Z = X\), we have \(E(X | Y) = \frac{1}{2}\) and \(E(\frac{1}{2} | Z) = \frac{1}{2} \neq X = E(X | Z)\). The correct formula instead of (b) is

\[
E(E(X | Z) | Z) = E(X | Z).
\]

This is (12) in the probability spaces conditioned by \(Z\), and it is the crucial identity that underlies exercise 91. Part (a) is true because it is the case \(Y = Z\) (of (s)).

36. (a) \(E(f(X))\); (b) \(E(f(Y)g(X))\), generalizing (12). Proof: \(E(f(Y)g(X) | Y) = \sum_y f(y) g(x) \Pr(x, y) = \sum_{x, y} f(y) g(x) \Pr(X = x, Y = y) = E(f(Y)g(X))\).

37. If we’re given the values of \(X_1, \ldots, X_{n-1}\), the value of \(X_n\) is equally likely to be any of the \(n + 1 - k\) values in \(\{1, \ldots, n\} \setminus \{X_1, \ldots, X_{n-1}\}\). Hence its average value is \((1 + \cdots + n - X_1 - \cdots - X_{n-1})/(n + 1 - k)\). We conclude that \(E(X_n | X_1, \ldots, X_{n-1}) = \frac{n(n + 1)/2 - (n - X_1 - \cdots - X_{n-1})}{n + 1 - k}\). (Incidentally, the sequence \(Z_0, Z_1, \ldots\), defined by \(Z_n = (n + j) X_1 + (n + j - 2) X_2 + \cdots + (n - j) X_{j+1} + (j + 1)n(n + 1)/2\) for \(0 \leq j < n\) and \(Z_n = Z_{n-1}\) for \(j \geq n\), is therefore a martingale.)

38. Let \(t_{m,n}\) be the number of restricted growth strings of length \(m + n\) that begin with \((01 \ldots m-1)\). (This is the number of set partitions of \(\{1, \ldots, m + n\}\) in which each of \(\{1, \ldots, m\}\) appears in a different block.) The generating function \(\sum_{n \geq 0} t_{m,n} z^n/n!\) turns out to be \(\exp(e^z - 1 + mz)\); hence \(t_{m,n} = \sum_i \binom{n}{i} m^i\).

39. (a) Since \(E(K | N = n) = np\), we have \(E(K | [N]) = np\).

(b) Hence \(E(K) = E(E(K | N)) = E(np) = np\).

(c) Let \(p_{m,n} = \Pr(N = n, K = k) = (e^{-n} n^k/k! \cdots (1 - p)^n (1 - p))\times(n - k)^{n - k} = (e^{-n} p^k/k! \cdots (1 - p)^n (1 - p))\times f(n - k),\) where \(f(n) = (1 - p)^n p^n/n!\). Then \(E(K | N = k) = \frac{n!}{\sum_{n_k} n_{n_k}}\). Since \(n f(n - k) = k f(n - k) + (n - k) f(n - k)\) and \(n f(n) = (1 - p)^n f(n - 1)\), the answer is \(k + (1 - p)\mu\). Hence \(E(N | K) = K + (1 - p)\mu\). [G. Grimmett and D. Stirzaker, Probability and Random Processes (Oxford: 1982), §3.7.]

40. If \(p = \Pr(X > m)\), clearly \(E(X) \leq (1 - p)m + p M\). [We also get this result from (15), by taking \(S = \{x \mid x \leq m\}, f(x) = M - x, s = M - m\].

41. (a) Convex when \(a \geq 1\) or \(a = 0\); otherwise neither convex nor concave. (However, \(x^a\) is concave when \(0 < a < 1\) and convex when \(a < 0\), if we consider only positive values of \(x\).) (b) Convex when \(n\) is even or \(n = 1\); otherwise neither convex nor concave.
(This function is \( \int_0^1 e^{-t} \frac{1}{t} \, dt/(n-1)! \), according to 1.2.11.3-(5); so \( f''(x)/x > 0 \) when \( n \geq 3 \) is odd.) (c) Convex. (In fact \( f'(x) \) is convex whenever \( f(z) \) has a power series with nonnegative coefficients, convergent for all \( z \).) (d) Convex, provided of course that we allow \( f \) to be infinite in the definition \((19)\).

42. We can show by induction on \( n \) that 
\[
 f(p_1 x_1 + \cdots + p_n x_n) \leq p_1 f(x_1) + \cdots + p_n f(x_n),
\]
when \( p_1, \ldots, p_n \geq 0 \) and \( p_1 + \cdots + p_n = 1 \), as in exercise 6.2.2-36. The general result follows by taking limits as \( n \to \infty \). [The quantity \( p_1 x_1 + \cdots + p_n x_n \) is called a “convex combination” of \( \{x_1, \ldots, x_n\} \); similarly, \( EX \) is a convex combination of \( X \) values. Jensen actually began his study by assuming only the case \( p = q = \frac{1}{n} \) of \((19)\).]

43. \( f(E(X,Y)) \leq E(f(E(X,Y))) \leq E(E(f(X,Y))) = E(f(X)) \). [S. M. Ross, Probability Models for Computer Science (2002), Lemma 3.2.1.]

44. The function \( f(xy) \) is convex in \( y \) for any fixed \( x \). Therefore \( g(y) = E(f(xy)) \) is convex in \( y \); it's a convex combination of convex functions. Also \( g(y) \geq f(E(XY)) = f(0) = g(0) \) by \((22)\). Hence \( 0 \leq a \leq b \) implies \( g(0) \leq g(a) \leq g(b) \) by convexity of \( g \).


45. \( Pr(X > 0) = Pr(E(X) \geq 1) \); set \( m = 1 \) in \((36)\).

46. \( EX^2 \geq (EX)^2 \) in any probability distribution, by Jensen’s inequality, because squaring is convex. We can also prove it directly, since \( EX^2 - (EX)^2 = E(X - EX)^2 \).

47. We always have \( Y \geq X \) and \( Y^2 \leq X^2 \). (Consequently \((22)\) yields \( Pr(X > 0) = Pr(Y > 0) \geq (EY)^2/(EY^2) \geq (EX)^2/(EX^2) \) when \( EX \geq 0 \).

48. \( Pr(aX - bX_1 - \cdots - bX_n > 0) \geq a^2/(a+b)^2 + \cdots + b^2 \), by exercise 47. [This inequality was also known to Chebyshev; see J. Math. Pures et Appl. (19) (1874), 157–160. In the special case \( n = 1 \) it is equivalent to “Cantelli’s inequality.”]

\[
 Pr(X \geq EX + a) \leq \frac{var(X)}{(var(X) + a^2)} \quad \text{for} \quad a \geq 0; \tag{c}
\]

see Atti del Congresso Internazionale dei Mathematici 6 (Bologna: 1928), 47–59, §6–§7.]

49. \( Pr(X = 0) = 1 - Pr(X > 0) \leq (EX^2 - (EX)^2) / EX^2 \leq (EX^2 - (EX)^2) / (EX^2) = (EX^2) / (EX^2) = 1. [Some authors call this inequality the “second moment principle.”]

but it is strictly weaker than \((22)\).]

50. (a) Let \( Y_j = X_j / X \) if \( X_j > 0 \), otherwise \( Y_j = 0 \). Then \( Y_1 + \cdots + Y_n = [X > 0] \).

Hence \( Pr(X > 0) = \sum_{i=1}^n EY_j \); and \( EY_j = E(X_j / X) \cdot Pr(X_j > 0) \). [This identity, which requires only that \( X_j \geq 0 \), is elementary yet nonlinear, so it apparently lay undiscovered for many years. See D. Aldous, Discrete Math. 76 (1989), 168.]

(b) Since \( X_j \in \{0, 1\} \), we have \( Pr(X_j > 0) = E X_j = p_j \); and \( E(X_j / X) \cdot Pr(X_j > 0) = E(X_j / X | X_j = 1) = E(1/X | X_j = 1) = 1/E(X | X_j = 1). \)

(c) \( Pr(X_j = 1) = \sum_{i=1}^m Pr(J = j \text{ and } X_j = 1) = \sum_{i=1}^m p_j / m = E X / m \). Hence \( Pr(J = j | X_j = 1) = Pr(J = j \text{ and } X_j = 1) / Pr(X_j = 1) = (p_j / m) / (E(X) / m) = p_j / E X. \)

(d) Since \( J \) is independent we have \( t_j = E(X | J = j) = E(X | X_j = 1) = E(X) | X_j = 1). \)

(e) The right side is \( (EX) \sum_{j=1}^m p_j / E X \cdot t_j \geq (EX) / \sum_{j=1}^m p_j / E X \cdot t_j. \)

51. If \( g(q_1, \ldots, q_m) = 1 - f(p_1, \ldots, p_m) \) is the dual of \( f \), where \( q_i = 1 - p_i \), a lower bound on \( g \) gives an upper bound on \( f \). For example, when \( f \) is \( x_1 x_2 x_3 \vee x_1 x_2 x_4 \vee x_2 x_5, \)
\( \bar{f} \) is \( \bar{x}_1 \bar{x}_4 + \bar{x}_2 \bar{x}_4 + \bar{x}_1 \bar{x}_5 + \bar{x}_2 \bar{x}_5 + \bar{x}_3 \bar{x}_5 \). So the inequality \((24)\) gives \( g(q_1, \ldots, q_m) \geq \max(q_1 + q_2 + q_3 + q_4 + q_5, q_1 q_2 + q_3 q_4 + q_5, q_1 q_2 q_3 q_4 q_5, q_1 q_2 q_3 q_4, q_2 q_3 q_4, q_1 q_2, q_1 q_3, q_1 q_4, q_2 q_3, q_4 q_5, q_1 q_2 q_3 q_4 q_5, q_1 q_2 q_3 q_4 q_5 q_6 q_7). \)

In particular, \( \sum_{i=0}^{m-1} \binom{m}{i} p^i q^{m-i} \geq \sum_{i=0}^{m-1} \binom{m}{i} (1-p)^i p^i. \)

May 20, 2015
53. \( f(p_1, \ldots, p_k) \geq p_1 p_2 (1 - p_3) / (1 + p_2 p_3 (1 - p_4)) + \cdots + p_2 p_4 (1 - p_5) / (1 + p_4 p_5 (1 - p_3)) \). Monotonicity is not required when applying this method, nor need the implicants be prime. The result is exact when the implicants are disjoint.

54. (a) \( \Pr(X > 0) \leq E_X = \left( \frac{1}{3} \right)^3 \), because \( E_{X_{w_w}} = p^3 \) for all \( u < v < w \).

(b) \( \Pr(X > 0) \geq (E_X)^2 / (E_X^2) \), where the numerator is the square of \( \Pr(X > 0) \) and the denominator can be shown to be \( \left( \frac{1}{2} \right)^3 + 12 \left( \frac{1}{3} \right)^2 + 30 \left( \frac{1}{3} \right) p^0 + 20 \left( \frac{1}{3} \right)^3 \). For example, the expansion of \( X^2 \) contains 12 terms of the form \( X_{w_w} X_{w'_w} \) with \( u < v < w < w' \), and each of these terms has expected value \( p^3 \).

55. A BDD for the corresponding Boolean function of \( \binom{10}{3} = 45 \) variables has about 1.4 million nodes, and allows us to evaluate the true probability \( \left( 1 - \frac{1}{6} \right)^{15} G(p(1 - \frac{1}{6})) \) exactly, where \( G(z) \) is the corresponding generating function (see exercise 7.1.4.25). The results are: (a) \( 30/37 \approx .814 \), (b) \( 351/366 \approx .964 \). See P. Erdős and A. Rényi, Magyar Tudományos Akadémia Mat. Kut. Int. Közl. 5 (1960), 17–61, [3, 3].

56. The upper bound is \( \mu = \lambda^3/6 \); the lower bound divides by \( 1 + \mu \). The exact asymptotic value can be obtained using the principle of inclusion and exclusion and its “bracketing” property, as in Eq. 7.2.1.4.48; the result is \( 1 - e^{-\mu} \). See P. Erdős and A. Rényi, Magyar Tudományos Akadémia Mat. Kut. Int. Közl. 5 (1960), 17–61, [3, 3].

57. To compute \( E_X (X_{w_w} = 1) \) we sum \( \Pr(X_{w'_w} | X_{w_w} = 1) \) over all \( \binom{3}{2} \) choices of \( u' < v < w' \). If \( \{u', v', w'\} \cap \{u, v, w\} \) has \( t \) elements, this probability is \( p^{3-t}(1-t)/2 \); and there are \( \binom{3}{2} \binom{t}{2} \) such cases. Consequently we get

\[
\Pr(X > 0) \geq \binom{3}{2} p^3 / \binom{3}{2} + 3 \binom{3}{2} p^3 + 3 \binom{3}{2} p^2 + \binom{3}{2} p^0.
\]

[In this problem the lower bound turns out to be the same using either inequality; but the derivation here was easier.]

58. \( \Pr(X > 0) \leq \left( \frac{1}{3} \right)^{10} \). The lower bound, using the conditional expectation inequality as in the previous answer, divides this by \( \sum_{i=t}^{n} \binom{n}{i} \left( \frac{1}{3} \right)^{10} \left( \frac{1}{2} \right)^{t-i} \left( \frac{1}{2} \right)^{n-i} \).

59. (a) The hypotheses imply that \( a_0 a_1 b_0 b_1 \leq a_0 c_1 d_0 d_1 \). The key observation is that

\[
c_1 d_1 ((c_1 + a_1) (d_1 + a_1) - (a_0 + a_1) (b_0 + b_1)) = c_1 d_1 (a_0 a_1 b_0 b_1) + c_1 d_1 (a_0 c_1 d_0 d_1) - (a_0 a_1 b_0 b_1) = a_0 c_1 d_0 d_1 - a_0 a_1 b_0 b_1.
\]

Thus the result holds when \( c_1 d_1 \neq 0 \). If \( c_1 = 0 \) we have \( a_0 a_1 b_0 b_1 = a_0 c_1 d_0 d_1 \). And a similar argument applies to the case \( a_1 d_1 = 0 \).

(b) Let \( A_1 = \sum_{i=1}^{\infty} a_{2i+1} \) for \( 0 

## Exercises

### 59. (a) The hypotheses imply that \( a_0 a_1 b_0 b_1 \leq a_0 c_1 d_0 d_1 \). The key observation is that

\[
c_1 d_1 ((c_1 + a_1) (d_1 + a_1) - (a_0 + a_1) (b_0 + b_1)) = c_1 d_1 (a_0 a_1 b_0 b_1) + c_1 d_1 (a_0 c_1 d_0 d_1) - (a_0 a_1 b_0 b_1) = a_0 c_1 d_0 d_1 - a_0 a_1 b_0 b_1.
\]

Thus the result holds when \( c_1 d_1 \neq 0 \). If \( c_1 = 0 \) we have \( a_0 a_1 b_0 b_1 = a_0 c_1 d_0 d_1 \). And a similar argument applies to the case \( a_1 d_1 = 0 \).

(b) Let \( A_1 = \sum_{i=1}^{\infty} a_{2i+1} \) for \( 0 \leq j < 2(n-1) \) define \( B_i, C_i, D_i \), similarly from \( b_{2i+1} \). The hypotheses for \( j \) mod 2 = 1 and \( k \) mod 2 = \( m \) prove that \( A_{2n} = C_{2n}, D_{2n} \). For induction on \( n \), hence by part (a), we have the desired inequality \( A_0 + A_1, B_0 + B_1 \leq C_0 + C_1, D_0 + D_1 \). This result is due to R. Ash ken and D. E. Daykin, Zeitschrift für Wahrscheinlichkeitstheorie und verwandte Gebiete 43 (1978), 183–185, who stated it in the language of the next exercise.

(c) Now let \( A_n = a_0 + \cdots + a_{2n-1} \), and define \( B_n, C_n, D_n \). Similarly if \( A_n B_n > C_n D_n \) we have \( A_{2n} B_{2n} = C_{2n} D_{2n} \) for some \( n \). But \( C_{2n} D_{2n} \geq C_n D_n \), contra (b).

### 60. (a) We can consider each set to be a subset of the nonnegative integers. Let \( \overline{\alpha}(S) = \alpha(S) [S \in \mathcal{F}] \), \( \overline{\beta}(S) = \beta(S) [S \in \mathcal{G}] \), \( \overline{\gamma}(S) = \gamma(S) [S \in \mathcal{F} \cup \mathcal{G}] \), \( \overline{\delta}(S) = \delta(S) [S \in \mathcal{F} \cap \mathcal{G}] \); then \( \overline{\alpha}(\phi) = \alpha(\phi), \overline{\beta}(\phi) = \beta(\phi), \overline{\gamma}(\phi) = \gamma(\phi \mathcal{F} \cup \mathcal{G}), \) and \( \overline{\delta}(\phi) = \delta(\phi \mathcal{F} \cap \mathcal{G}) \), where \( \phi \) is the prime implicants.

BDD

Boolean function

generating function

inclusion and exclusion

bracketing

enveloping series

Erdős

Reényi

conditional expectation inequality

Ahlsweide

Daykin

\( p^3 \)
family of all possible subsets. Since any set \( S \) of nonnegative integers can be encoded in the usual way as the binary number \( s = \sum_j s_j 2^j \), the desired result follows from the four functions theorem if we let \( a_s = \text{wt}(S) \), \( b_s = \beta(S) \), \( c_s = \mu(S) \), \( d_s = \delta(S) \).

(b) Let \( \alpha(S) = \beta(S) = \gamma(S) = \delta(S) = 1 \) for all sets \( S \).

61. (a) In the hinted case we can let \( \alpha(S) = f(S)\mu(S) \), \( \beta(S) = g(S)\mu(S) \), \( \gamma(S) = f(S)g(S)\mu(S) \), \( \delta(S) = \mu(S) \); the four functions theorem yields the result. The general case follows because we have \( E(fg) - E(f)E(g) = E(fg) - E(f)E(g) \), where \( f(S) = f(S - f(\emptyset)) \) and \( g(S) = g(S - g(\emptyset)) \). [See Commun. Math. Phys. 22 (1971), 89–103.]

(b) Changing \( f(S) \) to \( \theta f(S) \) and \( g(S) \) to \( \phi g(S) \) changes \( E(fg) - E(f)E(g) \) to \( \theta\phi E(fg) - \theta E(f)\phi E(g) \), for all real numbers \( \theta \) and \( \phi \).

(c) If \( S \) and \( T \) are supported, then \( R = S \cap T \) and \( U = S \cup T \) are supported. Furthermore we can write \( S = R \cup \{s_1, \ldots, s_k\} \) and \( T = R \cup \{t_1, \ldots, t_l\} \) as their unions \( U_{i,j} = S_i \cup T_j \), for \( 0 \leq i \leq k \) and \( 0 \leq j \leq l \). By (iii) we know that \( \mu(U_{i,j})/\mu(U_{i,j}) \leq \mu(U_{i,j+1})/\mu(U_{i,j+1}) \) when \( 0 \leq i \leq k \) and \( 0 \leq j < l \). Multiplying these inequalities for \( 0 \leq i \leq k \), we obtain \( \mu(U_{i,j})/\mu(U_{0,j}) \leq \mu(U_{i,j+1})/\mu(U_{0,j+1}) \). Hence \( \mu(S)/\mu(R) \leq \mu(U_{i,j})/\mu(U_{0,j}) \) for all \( i \) and \( j \).

[Note: Random variables with this distribution are often confusingly called “Poisson trials,” a term that conflicts with the (quite different) Poisson distribution of exercise 39.]

(e) Choose \( c \) in the following examples so that \( \sum \mu(S) = 1 \). In each case the supported sets are subsets of \( U = \{1, \ldots, m\} \). (i) Let \( \mu(S) = cr_{1,2} \ldots r_{1,\ell} \), where \( 0 < r_1 \leq \cdots \leq r_m \). (ii) Let \( \mu(S) = c_{i,j} \) when \( S = \{1, \ldots, j\} \) and \( 1 \leq j \leq m \), otherwise \( \mu(S) = 0 \). (If \( p_1 = \cdots = p_m \), in this case, the FKG inequality reduces to Chentsov’s monotonicity inequality of exercise 1.23–31.) (iii) Let

\[
\mu(S) = c p_1(S \cap U_1) p_2(S \cap U_2) \cdots p_k(S \cap U_k),
\]

where each \( p_j \) is a distribution on the subsets of \( U_j \subseteq U \) that satisfies (**) . The subuniverses \( U_1, \ldots, U_k \) needn’t be disjoint. (iv) Let \( \mu(S) = ce^{-f(S)} \), where \( f \) is a submodular set function on the supported subsets of \( U \): \( f(S \cup T) + f(S \cap T) \leq f(S) + f(T) \) whenever \( f(S) \) and \( f(T) \) are defined. (See Section 7.6.)

62. A Boolean function is essentially a set function whose values are 0 or 1. In general, under the Bernoulli distribution or any other distribution that satisfies the condition of exercise 61, the FKG inequality implies that any monotone increasing Boolean function is positively correlated with any other monotone increasing Boolean function, but negatively correlated with any monotone decreasing Boolean function. In this case, \( f \) is monotone increasing but \( g \) is monotone decreasing: Adding an edge doesn’t disconnect a graph; deleting an edge doesn’t invalidate a 4-coloring.

(Notice that when \( f \) is a Boolean function, \( E(f) \) is the probability that \( f \) is true under the given distribution. The fact that \( \text{covar}(f, g) \leq 0 \) in such a case is equivalent to saying that the conditional probability \( \text{Pr}(f \mid g) \) is \( \leq \text{Pr}(f) \).)

63. If \( \omega \) is the event \( (Z_0 = a, Z_1 = b) \), we have \( Z_0(\omega) = a \) and \( E(Z_1 \mid Z_0(\omega)) = (p_{a+1} + 2p_{a+2})/(p_{a+1} + p_{a+2}) \). Hence \( p_{a+1} = p_{a+2} = p_{a+1} = p_{a+2} = 0 \), and \( p_{a+1} = p_{a+2} \); these conditions are necessary and sufficient for \( E(Z_1 \mid Z_0) = Z_0 \).

64. (a) No. Consider the probability space consisting of just three events \( (Z_0, Z_1, Z_2) = (0, 0, -2), (1, 0, 2), (1, 2, 2) \), each with probability 1/3. Call these events \( a, b, c \). Then \( E(Z_1 \mid Z_0)(a) = 0 = Z_0(a) \); \( E(Z_1 \mid Z_0(b,c) = \frac{1}{2}(0 + 2) = Z_0(b,c) \); \( E(Z_2 \mid Z_1)(a,b) = \frac{1}{2}(-2 + 2) = Z_1(a,b) \); \( E(Z_2 \mid Z_1)(c) = 2 = Z_1(c) \). But \( E(Z_2 \mid Z_0, Z_1)(a) = -2 \neq Z_1(a) \).
(b) Yes. We have \(\sum_{n=0}^{\infty} (z_{n+1} - z_n) \Pr(Z_0 = z_0, \ldots, Z_n = z_n) = 0\) for all fixed \((z_0, \ldots, z_n)\). Sum these to get \(\sum_{n=0}^{\infty} (z_{n+1} - z_n) \Pr(Z_0 = z_n, Z_{n+1} = z_n + 1) = 0\).

65. Observe first that \(E(Z_{n+1} | Z_0, \ldots, Z_k) = E(E(Z_{n+1} | Z_0, \ldots, Z_n) | Z_0, \ldots, Z_k) = E(Z_n | Z_0, \ldots, Z_k)\) whenever \(k < n\). Thus \(E(Z_{n+1} | Z_0, \ldots, Z_{m(n)}) = E(Z_m | Z_0, \ldots, Z_{m(n)})\) for all \(n \geq 0\). Hence \(E(Z_{m(n+1)} | Z_{m(n)}, \ldots, Z_{m(n+1)}) = Z_{m(n+1)}\), as in the previous exercise.

66. We need to specify the joint distribution of \(\{Z_0, \ldots, Z_n\}\), and it’s not difficult to see that there is only one solution. Let \(p(\sigma_1, \ldots, \sigma_n) = \Pr(Z_1 = \sigma_1, \ldots, Z_n = \sigma_n)\) when \(\sigma_1, \ldots, \sigma_n\) are each \(\pm 1\). The martingale law \(p(\sigma_1, \ldots, \sigma_n, 1) = p(\sigma_1, \ldots, \sigma_n, 0) + p(\sigma_1, \ldots, \sigma_n, 1)\) gives \(p(\sigma_1, \ldots, \sigma_n, 1)/p(\sigma_1, \ldots, \sigma_n) = (1 + 2n[\sigma_1, \ldots, \sigma_n, 1 > 0])/(2n + 2)\). Hence we find that \(\Pr(Z_1 = z_1, \ldots, Z_n = z_n) = (\prod_{i=1}^{n-1} (1 + 2k[2z_i z_{i+1} > 0]))/(2^n n!)\). When \(n = 3\), for example, the eight possible cases \(z_1 z_2 z_3 = 123, 132, \ldots, 321\) occur with probabilities \((5, 3, 15, 3, 5, 1, 3, 15)/48\).

67. (a) You “always” (with probability 1) make \(2^{n+1} - (1 + 2 + \cdots + 2^n) = 1\) dollar.

(b) Your total payments are \(X = X_0 + X_1 + \cdots\) dollars, where \(X_n = 2^n\) with probability \(2^{-n}\), otherwise \(X_n = 0\). So \(E(X_n) = 1\) and \(E(X) = E(X_0) + E(X_1) + \cdots = \infty\).

(c) Let \(\{T_n\}\) be a sequence of uniformly random bits; and define the fair sequence \(Y_n = (-1)^{T_n} T_0 \cdots T_{n-1}\), or \(Y_n = 0\) if there is no \(n\)th bit. Then \(Z_n = Y_0 + \cdots + Y_n\).

The famous adventurer Casanova lost a fortune in 1754 using this strategy, which he called “the martingale” in his autobiography Histoire de ma vie. A similar betting scheme had been proposed by Nicolas Bernoulli (see P. R. de Montmort, Essay d’Analyse sur les Jeux de Hazard, second edition (1713), page 102); and the perplexities of (a) and (b) were studied by his cousin Daniel Bernoulli, whose important paper in Commentarii Academiae Scientiarum Imperialis Petropolitanae 5 (1731), 175–192, has caused this scenario to become known as the St. Petersburg paradox.

68. (a) Now \(Z_n = Y_1 + \cdots + Y_n\), where \(Y_n = (-1)^n [N \geq n]\). Again \(\Pr(Z_N = 1) = 1\).

(b) The generating function \(g(z)\) equals \(z(1 + g(z)^2)/2\), since he must win \$2 if the first bit loses. Hence \(g(z) = (1 - \sqrt{1 - z^2})/z\); and the desired probability is \([z^n] g(z) = C_{n+1} \binom{n+1}{n} [n \text{ odd}]/2^n\), where \(C_k\) is the Catalan number \(\binom{2k}{k}/(k+1)\).

(c) \(\Pr(N \geq n) = \left[z^n\right] (1 - g(z)) / (1 - z) = \left[z^n\right] (1 + z) / \sqrt{1 - z^2} = \left[z^n\right] \binom{[n+1] / 2}{n+1}\).

(d) \(E N = g'(1) = \infty\). (It’s also \(\sum_{n=0}^{\infty} \Pr(N \geq n)\), where \(\Pr(N \geq n) \sim 1/\sqrt{\pi n}\) )

(e) Let \(p_m = \Pr(Z_m \geq -m)\) for all \(n \geq 0\). Clearly \(p_0 = 1/2\) and \(p_{m+1} = (1 + p_{m-1} p_m^2) / 2\) for \(m > 0\); this recurrence has the solution \(p_m = (m+1)/(m+2)\). So the answer is \(1/(m+1)(m+2)\); it’s another probability distribution with infinite mean.

(f) The generating function \(g_m(z)\) for the number of times \(-m\) is hit satisfies \(g_0(z) = z/(2-z), g_m(z) = (1 + g_{m-1}(z) g_m(z))/2m + 1\) for \(m > 0\). So \(g_m(z) = h_m(z) / h_{m+1}(z)\) for \(m \geq 0\), where \(h_m(z) = 2m - (2m - 1)z\), and \(g_0(1) = 2\). [A distribution with finite mean! See W. Feller, An Introduction to Probability Theory 2, second edition (1971), XII.2]

69. Each permutation of \(n\) elements corresponds to a configuration of \(n+1\) balls in the urn. For Method 1, the number of corresponding “red balls” is the position of element 1; for Method 2, it is the value in position 1. For example, we’d put 3 1 2 4 into node (2,3) with respect to Method 1 but into (3,2) with respect to Method 2. (In fact, Methods 1 and 2 construct permutations that are inverses of each other.)

70. Start with the permutation \(12 \cdots (c-1)\) at the root, and use Method 1 of the previous exercise to generate all \(n!/(c-1)!\) permutations in which these elements retain that order. A permutation with \(j\) in position \(l_j\) for \(1 \leq j < c\) stands for \(P_j = P_{j+1}\) balls of color \(j\), where \(P_0 = 0\) and \(P_c = n + 1\); for example, if \(c = 3\), the permutation...

May 20, 2015
3.142 would correspond to node (2, 2, 1). The resulting tuples \((A_1, \ldots, A_n)/(n + 1)\) then form a martingale for \(n = c, c + 1, \ldots\), uniformly distributed (for each \(n\)) among all \(\binom{n + 1}{c}\) compositions of \(n + 1\) into \(c\) positive parts.

We can also use this setup to deal with Pólya’s two-color model when there are \(r\) red balls and \(b\) black balls at the beginning: Imagine \(r + b\) colors, then identify the first \(r\) of them with red. This model was first studied by D. Blackwell and D. Kendall, *J. Applied Probability* 1 (1964), 284–296.

71. If \(m = r' - r\) and \(n = b' - b\) we must move \(m\) times to the right and \(n\) times to the left; there are \(\binom{m + n}{m}\) such paths. Every path occurs with the same probability, because the numerators of the fractions are \(r' - r - 1\ldots(r - 1)\cdot(b + 1)\ldots(b' - 1) = \binom{m}{r}b^{n-r}\) in some order, and the denominators are \((r + b) (r + b + 1) \ldots (r' + b' - 1) = (r + b)^{m+n}\).

The answer, \(\binom{m + n}{r} \binom{m + n}{n} (r + b)^{m+n-2}\), reduces to \(1/(r' + b' - 1)\) when \(r = b = 1\).

72. Since all paths have the same probability, the expected value is the same as \(E(X_1X_2 \ldots X_n)\), which is obviously \(1/(m+1)\). (Thus the \(X\)'s are very highly correlated: This expected value would be \(1/2^m\) if they were independent. Notice that the probability of an event such as \((X_1 = 1, X_5 = 0, X_6 = 1)\) is \(E(X_2(1 - X_2)X_6) = 1/3 - 1/4.\)

The far-reaching ramifications of such exchangeable random variables are surveyed in O. Kallenberg’s book *Probabilistic Symmetries and Invariance Principles* (2005.).

73. \(f(r, n) = r^{r+1} \sum_{k=0}^{n} \binom{n}{k} (-1)^k q_{n+1-r+k},\) where \(q_k = a_k/(k+1),\) by induction on \(r\).

74. Note \((r, n + 2 - r)\) on level \(n\) is reached with probability \(\binom{n+1}{n}/n!,\) proportional to an Eulerian number (see Section 5.1.3). (Indeed, we can associate the permutations of \(\{1, \ldots, n+1\}\) that have exactly \(r\) runs with this node, using Method 1 as in exercise 69.)

Reference: *Communications on Pure and Applied Mathematics* 2 (1949), 59–70.

75. As before, let \(R_n = X_0 + \cdots + X_n\) be the number of red balls at level \(n\). Now we have \(E(X_{n+1} | X_0, \ldots, X_n) = 1 - R_n/(n + 2)\). Hence \(E(R_{n+1} | R_n) = (n + 1)R_n/(n + 2) + 1,\) and the definition \(Z_n = (n + 1)R_n - (n + 2)(n + 1)/2\) is a natural choice.

76. No. For example, let \(Z_0 = X, Z_1 = Y,\) and \(Z_1 = Z_2 = X + Y,\) where \(X\) and \(Y\) are independent with \(E X = E Y = 0.\) Then \(E(Z_1 | Z_0) = Z_0\) and \(E(Z_2 | Z_0) = Z_0\), but \(E(Z_1 + Z_2 | Z_0 + Z_0) = 2(2Z_0 + 2Z_0).\) (On the other hand, if \(Z_1\) and \(Z_2\) are both martingales with respect to some common sequence \(\langle X_n \rangle\), then \(\langle Z_n + Z_n \rangle\) is also.)

77. \(E(Z_n + 1 | Z_0, \ldots, Z_n) = E(E(Z_{n+1} | Z_0, \ldots, Z_n, X_0, \ldots, X_n) | Z_0, \ldots, Z_n),\) which equals \(E(E(Z_{n+1} | X_0, \ldots, X_n) | Z_0, \ldots, Z_n)\) because \(Z_n\) is a function of \(X_0, \ldots, X_n;\) and that equals \(E(Z_n | Z_0, \ldots, Z_n) = Z_n.\) (Furthermore \(Z_n\) is a martingale with respect to, say, a constant sequence. But not with respect to every sequence.)

A similar proof shows that any sequence \(\langle Y_n \rangle\) that is fair with respect to \(\langle X_n \rangle\) is also fair with respect to itself.

78. \(E(Z_n+1 | \tilde{V}_0, \ldots, \tilde{V}_n) = E(Z_n \tilde{V}_{n+1} \tilde{V}_0, \ldots, \tilde{V}_n) = Z_n.\)

The converse holds with \(\tilde{V}_0 = Z_0\) and \(\tilde{V}_n = Z_n/Z_{n-1}\) for \(n > 0,\) provided that \(Z_{n-1} = 0\) implies \(Z_n = 0,\) and that we define \(V_n = 1\) when that happens.

79. \(Z_n = \tilde{V}_0 \tilde{V}_1 \cdots \tilde{V}_n,\) where \(\tilde{V}_0 = 1\) and each \(\tilde{V}_n\) for \(n > 0\) is independently equal to \(q/p\) (with probability \(p\)) or to \(p/q\) (with probability \(q\)). Since \(E(V_n) = q + p = 1, \langle V_n \rangle\) is multiplicatively fair. [See A. de Moivre, *The Doctrine of Chances* (1718), 102–154.]

80. (a) True: in fact \(E(f_n(V_0 \ldots V_{n-1}) V_n) = 0\) for any function \(f_n.\)

(b) False: For example, let \(Y_3 = \pm 1\) if \(Y_3 > 0,\) otherwise \(Y_3 = 0.\) (Hence permutations of a fair sequence needn’t be fair. The statement is, however, true if the \(Y\)'s are independent with mean zero.)

May 20, 2015
(c) False if $n_1 = 0$ and $m = 1$ (or if $m = 0$); otherwise true. (Sequences that satisfy $E(Y_{n_1} - E Y_{n_1}) \cdots (Y_{n_m} - E Y_{n_m}) = E(Y_{n_1} - E Y_{n_1}) \cdots E(Y_{n_m} - E Y_{n_m})$ are called totally uncorrelated. Such sequences, with $E Y_n = 0$ for all $n$, are not always fair; but fair sequences are always totally uncorrelated.)

81. Assuming that $X_0, \ldots, X_n$ can be deduced from $Z_0, \ldots, Z_n$, we have $a_n X_n + b_n X_{n-1} = Z_n = E(Z_{n+1} 
 Z_0, \ldots, Z_n) = E(a_{n+1} X_{n+1} + b_{n+1} X_n \mid X_0, \ldots, X_n) = a_{n+1} (X_n + X_{n-1}) + b_{n+1} X_n$ for $n \geq 1$. Hence $a_{n+1} = b_n, b_{n+1} = a_{n+1} = b_n - b_0$; and we have $a_n = F_{-n-1}, b_n = F_{-n-2}$ by induction, verifying the assumption.


82. (a) $Z_n = A_n/C_n$, where $A_n = 4 - X_1 \cdots - X_n$ is the number of arms and $C_n$ is the number of cards remaining after you’ve seen $n$ cards. Hence $E Z_{n+1} = (A_{n+1}/C_n)\{A_n - 1\}/C_n + (1 - A_n/C_n)A_n/\{C_n - 1\} = A_n/C_n$. (In every generalization of Pólya’s urn for which the $n$th step adds $k_n$ balls of the chosen color, the ratio red/ red + black) is always a martingale, even when $k_n$ is negative, as long as enough balls of the chosen color remain. This exercise represents the case $k_n = -1$.)

(b) This is the optional stopping principle in a bounded-time martingale.

(c) $Z_n = A_n/C_n$ is the probability that an ace will be next. [“Ace Now” is a variant of R. Connelly’s game “Say Red”; see Pullman Review 9 (1974), 702.]

83. $Z_n = \sum_{i=1}^{n} X_n - E X_n$ is a martingale, for which we can study the bounded stopping rules $\min(m, N)$ for any $m$. But Svante Janson suggests a direct computation, beginning with the formula $S_n = \sum_{i=1}^{n} X_n[N \geq n]$ where $N$ might be $\infty$. We have $E(X_n[N \geq n]) = (E(X_n)\{E[N \geq n]\})$, because $[N \geq n]$ is a function of $\{X_0, \ldots, X_{n-1}\}$, hence independent of $X_n$. And since $X_n \geq 0$, we have $E S_N = \sum_{i=1}^{n} E(X_n[N \geq n]) = \sum_{i=1}^{n} (E(X_n)\{E[N \geq n]\}) = E \sum_{i=1}^{n} E(X_n)[N \geq n]$, which is $E \sum_{i=1}^{n} E(X_n)$. (The equation might be $= \infty$.)

[Wald’s original results, in Annals of Mathematical Statistics 15 (1944), 283–296, 16 (1945), 287–293, solved a somewhat different problem and proved more.]

84. (a) We have $f(Z_n) = f(E(Z_{n+1} \mid Z_0, \ldots, Z_n)) \leq E(f(Z_{n+1}) \mid Z_0, \ldots, Z_n)$ by Jensen’s inequality. And the latter is $E(f(Z_{n+1}) | f(Z_n), \ldots, f(Z_1))$ as in answer 77. [Incidentally, D. Gatz has shown that every nonnegative submartingale is $\{Z_n\}$ for some martingale $\{Z_n\}$; see Annals of Probability 5 (1977), 475–481.]

(b) Again we get a submartingale, provided that we also have $f(x) \leq f(y)$ for $a \leq x \leq y \leq b$. (J. L. Doob, Stochastic Processes (1953), 295–296.)

85. Since $(B_n/(R_n + B_n)) = (1 - R_n/(R_n + B_n))$ is a martingale by (27), and since $f(x) = 1/x$ is convex for positive $x$, $(B_n/(R_n + B_n)) = (R_n/(B_n + 1))$ is a submartingale by exercise 84. (A direct proof could also be given.)

86. The rule $N_{n+1}(Z_0, \ldots, Z_{n+1}) = \max(Z_0, \ldots, Z_n) < x$ and $n + 1 < m$ is bounded. If $\max(Z_0, \ldots, Z_{n-1}) < x$ then we have $Z_{n+1} < x$, where $N$ is defined by (31); similarly, if $\max(Z_0, \ldots, Z_{n-1}) \geq x$ then $Z_n \geq x$. Hence $Pr[\max(Z_0, \ldots, Z_n) \geq x] = (E X_n)/x$ by Markov’s inequality; and $E(Z_n) \leq E X_n$ in a submartingale.

87. This is the probability that $Z_n$ becomes 3/4, which also is $Pr(\max(Z_0, \ldots, Z_n) \geq 3/4)$. But $E Z_n = 1/2$ for all $n$, hence (33) tells us that it is at most $(1/2)/(3/4) = 2/3$.

(The exact value can be calculated as in the following exercise. It turns out to be $\sum_{x=0}^\infty \frac{x}{3x+2(3x+3)} = \frac{1}{2}H_1/4 - \frac{1}{2}H_1/2 = \frac{1}{2} - \frac{1}{2} \ln 2 \simeq .439$.)

88. (a) We have $S > 1/2$ if and only if there comes a time when there are more red balls than black balls. Since that happens if and only if the process passes through one
of the nodes \((2, 1), (3, 2), (4, 3), \ldots\), the desired probability is \(p_1 + p_2 + \cdots\), where \(p_k\)
is the probability that node \((k+1, k)\) is hit before any of \((j+1, j)\) for \(j < k\).

All paths from the root to \((k + 1, k)\) are equally likely, and the paths that meet our restrictions are equivalent to the paths in 7.2.1.6-(28). Thus we can use Eq. 7.2.1.6-(23) to show that \(p_k = 1/(2k - 1) - 1/(2k);\) and \(1 - 1/2 + 1/3 - 1/4 + \cdots = \ln 2\).

(b,c) If \(p_k\) is the probability of hitting node \((t - 1)k + 1, k)\) before any previous \(((t - 1)j + 1, j)\), a similar calculation using the \(t\)-ary ballot numbers \(C_{n,t}\) yields \(p_k = (t - 1)/(tk - 1) - 1/(tk);\) Then \(\sum_{t=1}^{\infty} p_k = 1 - (1 - 1/t)H_{t-1,t}\) (see Appendix A).

Notes: We have \(\Pr(S = 1/2) = 1 - \ln 2,\) since \(S\) is always \(\geq 1/2\). But we cannot claim that \(\Pr(S \geq 2/3)\) is the sum of cases that pass through \((2, 1), (4, 2), (6, 3), \ldots,\) because the supremum might be \(2/3\) even though the value \(2/3\) is never reached. Those cases occur with probability \(\pi/\sqrt{27};\) hence \(\Pr(S = 2/3) \geq 2\pi/\sqrt{27} - \ln 3 \approx 1.11.\) A determination of the exact value of \(\Pr(S = 2/3)\) is beyond the scope of this book, because we’ve avoided the complications of measure theory by defining probability only in discrete spaces; we can’t consider a limiting quantity such as \(S\) to be a random variable, by our definitions! But we can assign a probability to the event that \(\max(Z_n, Z_1, \ldots, Z_n) > x,\) for any given \(n\) and \(x,\) and we can reason about the limits of such probabilities.

With the help of deeper methods, E. Schulte-Geers and W. Stadje have proved that the supremum is reached within \(n\) steps, a.s. Hence \(\Pr(S = 2/3) \geq 2\pi/\sqrt{27} - \ln 3;\) indeed, \(\Pr(S) = \text{rational}\) = 1, since only rationals are reached; and \(\Pr(S = (t - 1)/t) = (2 - 3/t)H_{t-1,t} - (1 - 2/t)H_{t-1,t} - (t-2)/(t-1),\) [J. Applied Prob. 52 (2015), 180-190.]

89. Set \(Y_n = X_n - p_n, a_n = -p_n, b_n = 1 - p_n,\) (Incidentally, exercise 1.2.10-22 gives an upper bound for this quantity that has quite a different form.)

90. (a) Apply Markov’s inequality to \(\Pr(e^{(Y_1 + \cdots + Y_n)t} \geq e^{ct}).\)

(b) \(e^{at} \leq e^{-ax} (a - y) + e^a (y - p) = e^{at} + ye^{(1/t)} \) because the function \(e^{at}\) is convex.

(c) We have \(f(t) = -p + p e^t / (q + p e^t)\) and \(f''(t) = p q e^t / (q + p e^t)^2;\) hence \(f(0) = f'(0) = 0.\) And \(f''(t) \leq 1/2,\) because the geometric mean of \(q\) and \(pe^t,\) \((pe^t)^{1/2},\) is less than or equal to the arithmetic mean, \((q + pe^t)/2.\)

(d) Set \(c = b - a, p = -a/c, q = b/c, Y = Y/c, t = ct, h(t) = e^{(ct)} / c.\)

(e) In \(E(e^{(e^{ct})^2/4} + Y_1 h_1(t) + \cdots + e^{(e^{ct})^2/4} + Y_n h_n(t))\) the terms involving \(h_i(t)\) all drop out, because \(Y_n)\) is fair. So we’re left with the constant term, \(e^{ct^2/4}.\)

(f) Let \(t = 2x/c,\) to make \(ct^2/4 - xt = -x^2/c.\)

91. \(E(Z_{n+1} | X_0, \ldots, X_n) = E(E(Q | X_0, \ldots, X_n, X_{n+1}) | X_0, \ldots, X_n),\) and this is equal to \(E(Q | X_0, \ldots, X_n)\) by formula (o) in answer 35. Apply exercise 77.

92. \(Q_0 = E(X_n) = 1/2.\) If \(n < m\) we have \(Q_n = E(X_n | X_0, \ldots, X_n),\) which is the same as \(E(X_{n+1} | X_0, \ldots, X_n)\) (see exercise 72); and this is \((1 + X + \cdots + X_n) / (n + 2),\) which is the same as \(Z_n\) in (27). If \(n \geq m,\) however, we have \(Q_n = X_m.\)

93. Everything goes through exactly as before, except that we must replace the quantity \((m - 1)/m^{1/2}\) by the generalized expected value, which is \(\sum_{s=1}^m (1 - p_n).\)

94. If the \(X\)'s are dependent, the Doob martingale still is well defined; but when we write its fair sequence as an average of \(\Delta(x_1, \ldots, x_t)\) there is no longer a nice formula such as \(\langle q \rangle.\) In any formula for \(\Delta\) that has the form \(\sum_p \sum_p (Q(x_{n+1} - Q(x_{n+1} - x_{n+1} \ldots \ldots) / (\Pr(X_n = x_n) \Pr(X_{n+1} = x_{n+1})), \ldots)\) must equal \(\sum_p p_n,\) so it must be independent of \(x_n.\) Thus \(\langle q \rangle\) can’t be used.

95. False, the probability of only one red ball at level \(n\) is \(1/(n+1) = \Omega(n^{-1}).\) But there are \(a.s.\) more than 100 red balls, because that happens with probability \((n-99)/(n+1).

May 20, 2015
96. Exercise 1.2.10-21, with $\epsilon n$ equal to the bound on $|X - n/2|$, tells us that (i) is q.s. and that (i), (ii), (iii) are a.s. To prove that (iv) isn’t a.s., we can use Stirling’s approximation to show that $(\frac{an}{k+1})^n/2^n = \Theta(n^{-1/2})$ when $k = \sqrt{n}$; consequently

$$\Pr(|X| < \sqrt{n}) = \Theta(1).$$

A similar calculation shows that (ii) isn’t q.s.

97. We need to show only that a single bin q.s. receives that many. The probability generating function for the number of items $H$ that appear in any particular bin is $G(z) = \{(n - 1 + z)/n\}^N$, where $N = \lfloor n^{1/2} \epsilon \rfloor$. If $r = \frac{\epsilon n}{\sqrt{n}}$, we have

$$\Pr(H \leq r) \leq \left(\frac{1}{2} \right)^r \cdot G\left(\frac{1}{2}\right) \left(1 - \frac{1}{2n}\right)^{2nr} \leq 2^r\left(1 - \frac{1}{2n}\right)^{2nr - 1} \leq 2^r \epsilon^{-r},$$

by 1.2.10–(24). And if $r = 2n^\epsilon$ we have

$$\Pr(H \geq r) \leq 2^{-r} G(2) = 2^{-r} \left(1 + \frac{1}{n}\right)^{\epsilon r/2} \leq 2^{-r} \left(1 + \frac{1}{n}\right)^{\epsilon r/2} \leq 2^{-r} \epsilon^{r/2},$$

by 1.2.10–(25). Both are exponentially small. [See Knuth, Motwani, and Pittel, Random Structures & Algorithms 1 (1990), 1–14, Lemma 1.1]

98. Let $E_n = E R$, where $R$ is the number of reduction steps; and suppose $F(n) = k$ with probability $p_k$, where $\sum_{k=1}^n p_k = 1$ and $\sum_{k=1}^n k p_k = g_n$. (The values of $p_1, \ldots, p_n$, and $g$ may be different, in general, every time we compute $F(n)$.) Let $\Sigma_n = \sum_{i=1}^n 1/g_i$. Clearly $E_0 = 0$. And if $n > 0$, we have by induction

$$E_n = 1 + \sum_{i=1}^n p_i E_{n-i} \leq 1 + \sum_{i=1}^n p_i \Sigma_{n-i}^n = 1 + \sum_{i=1}^n p_i (\Sigma_{n}^n - \Sigma_{n-i}^n)$$

$$= \Sigma_n + 1 - \sum_{i=1}^n p_i \Sigma_{n-i}^n + 1 - \sum_{i=1}^n p_i g_n \leq \Sigma_n.$$ [See R. M. Karp, E. Upfal, and A. Wigderson, J. Comp. and Syst. Sci. 36 (1988), 252]

99. The same proof would work, provided that induction could be justified, if we were to do the sums from $K = -\infty$ to $n$ and define $\Sigma_n = -\sum_{i=-\infty}^{n-1} 1/g_i$ when $a > b$. (For example, that definition gives $\Sigma_{n+1} = 1/g_{n+1} + 1/g_{n+2} \leq 2/g_{n+1}$.)

And in fact it does become a proof, by induction on $m$, that we have $E_{m,n} \leq \Sigma_n$ for all $m, n \geq 0$, where $E_{m,n} = E \min(m, R)$. Indeed, we have $E_{0,n} = E_{m+1,0} = 0$; and $E_{m+1,n} = 1 + \sum_{i=n}^{m-n+1} p_i E_{m,n-i}$ when $n > 0$. (This problem is exercise 1.6 in Randomized Algorithms by Motwani and Raghavan (1995). Svante Janson observes that the random variable $Z_n = \sum_{i=1}^{X_n} \min(m, R)$ is a supermartingale, where $X_n$ is the value of $X$ after $m$ iterations, as a consequence of this proof.)

100. (a) $\sum_{i=1}^m k p_i \leq E \min(m, T) = p_1 + 2p_2 + \cdots + mp_m + mp_{m+1} + \cdots + mp_{\infty} \leq ET$.

(b) $\min(m, T) \geq mp_{\infty}$ for all $m$. (We assume that $\epsilon n \geq \epsilon n > 0$.

101. (Solution by Svante Janson.) If $0 < \theta < \min(p_1, \ldots, p_m) = p$, we have $E e^{tX} = \sum_{k=0}^m E e^{tX} = \sum_{k=0}^m \sum_{i=1}^k \sum_{j=1}^i (e^{tX} - 1 + p_i) \leq \sum_{i=1}^m p_i (e^t - 1)$, because $e^t - 1 > t^t/t!$. By 1.2.10–(25), therefore, and setting $t = \theta/p$, $\Pr(X \geq r/p) \leq e^{-r/p} \sum_{k=0}^m p_k (e^{r/p} - 1) = \exp(-r - \sum_{i=1}^m p_i (e^{r/p} - 1)) \leq \exp(-r - \sum_{i=1}^m p_i (e^{r/p} - 1)) = \exp(-r - \sum_{i=1}^m p_i (1 - e^{r/p}) \ln(1 - e^{r/p}) = \exp(-r - \ln(1 - e^t))$. Choose $\theta = r (1-p)/p$ to get the desired bound $re^{-r}$. (The bound is nearly sharp when $m = 1$ and $p$ is small, since $\Pr(X > r/p) = (1-p) [r/(r/p)]^{-1} \approx e^{-r}$.)

102. Applying exercise 101 with $\mu \leq s_1 + \cdots + s_n$, and $r = \ln n$ gives probability $O(n^{-1} \ln n)$ that $s_1 + \cdots + s_n \geq r$ trials aren’t enough. And if $r = f(n) \ln n$, where $f(n)$ is any increasing function that is not bounded as $n \to \infty$, the probability that $s \geq r$ trials don’t obtain coupon $k$ is superpolynomially small. So is the probability that any one of a polynomial number of such failures will occur.
103. (a) The recurrence $p_{0ij} = [i = j]$, $p_{(i+1)ij} = \sum_{k=0}^{i} p_{nk} i ([f_0(k) = j] + [f_1(k) = j])/2$ leads to generating functions $g_{ij} = \sum_{n=0}^{\infty} p_{nk} z^n$ that satisfy $g_{0i}^n = [i = 0] + (g_{01} + g_{11}) z/2$, $g_{1i} = [i = 1] + (g_{01} + g_{11}) z/2$, $g_{0i} = [i = 2] + (g_{01} + g_{11}) z/2$. From the solution $g_{00} = A + B + C$, $g_{11} = A - 2B$, $g_{22} = A + B - C$, $A = (1-3[i = 1] + [i + 1] + 2)/(1 + z) / 2)$, and $C = \frac{3}{2}[(i = 0) - [i = 1] + (1 - z)/2]$, we conclude that the probability is $\frac{3}{2} + O(2^n)$; in fact it is always either $\frac{2^n}{3}/2^2$ or $\frac{2^n}{3}/2^2$. The former occurs if and only if $i \neq n$ and $i + j = n$ is odd.

(b) Letting $\alpha_{00} = (1 - \frac{1}{2})^{-2} (g_{01} + g_{11})$, $\alpha_0 1 = (1 - \frac{1}{2})^{-2} (j = 0) + g_{11}$, etc., yields the generating function $\alpha_{111} = ((j \neq 1) + [j = 1]) z^2/(4 - z^2)$. Hence each $j$ occurs with probability $1/3$, and the generating function for $N$ is $z^2/(2 - z^2)$; mean $3$, variance $2$.

(c) Now $\alpha_{001} = (1 - \frac{1}{2})^{-2} (j = 0) + g_{11}$, etc.; the output is never 1, 0 and 2 are equally likely; and $N$ has the same distribution as before.

(d) Functional composition isn’t commutative, so the stopping criterion is different: In the second case, 111 cannot occur unless the previous step had 000 or 222. The crucial difference is that, without stopping, process (b) becomes fixed at coalescence; process (c) continues to change a00, a22 as $n$ increases (although all three remain equal).

(e) If $T$ is even, $\text{sub}(T)$ returns $(-1, 0, 1, 2)$ with probability $(2, 2^2 - 1)/3, (2^2 - 1)/3)$, (2$^2 - 1)/3$). Thus the supposed alternative to (b) will output 0 with probability $\frac{1}{2} + \frac{3}{2} + \frac{3}{2} = \frac{1}{2} \sum_{n=1}^{\infty} 2^{n+1} (2^{2n+1} - 1) = 2/3 \approx 0.427$, not 1/3.

(f) Change sub(T) to use consistent bits $X_T, X_{T-1}, \ldots, X_1$ instead of generating new random bits $X$ each time; then the method of (b) is faithfully simulated. (The necessary consistency can be achieved by carefully resetting the seed of a suitable random number generator at appropriate times.)

The technique of (f) is called “coupling from the past” in a monotone Monte Carlo simulation. It can be used to generate uniformly random objects of many important kinds, and it runs substantially faster than method (b) when there are thousands or millions of possible states instead of just three. See J. A. Propp and D. B. Wilson, *Random Structures & Algorithms* 9 (1996), 223–252.

104. Let $q = 1 - p$. The probability of output 0, 1, 2 in (b) is $(q^2, 2pq, p^2)$; in (c) it is $(p^2 + pq, q^2, pq^2)$. In both cases $N$ has generating function $(1 - pq(2 - z))/z^3/(1 - pqz^2)$, mean $3/(1 - pq - 1)$, variance $(5 - 2pq)/pq/(1 - pq)^2$.

105. Suppose $n = 2m$ is even. Experiments for small $m$ suggest that there are polynomials $t_k$ such that $g_n = z^{m-1} t_k / t_m$ for $0 \leq a \leq m$ and indeed, the polynomials defined by $t_0 = 1$, $t_{k+1} = 2t_k - z^2 t_{k-1}$ fill the bill, because they make $g_m = z g_{m-1}$. The generating function $T(w) = \sum_{m=0}^{\infty} t_m z^m = (1 - w)/(1 - 2w + w^2 z^2)$ now shows, after differentiation by $z$, that we have $e_m(1) = -m(m - 1)$ and $e_m(1) = (m^2 - 3m + 3)(m - 1)/3$, hence $e_m(1) - e_m(1) = \frac{2}{3} (m^2 - m^2)$. The mean and variance, given $a$, are therefore $e_m(1) = (m - a)(m - a - 1)$ and $e_m(1) = a(a - n) + 2a(a - 1) - 2a(a - n)$, respectively.

When $n = 2m$ we can write $g_n = z^m t_{2m} / t_m$ for $0 \leq a = m$. With $u_{m+1} = 2u_m - z^2 u_{m-1}$. In this case we want $u_0 = 1$ and $u_1 = z$, so that $g_m = z g_{m-1}$. From $U(w) = \sum_{m=0}^{\infty} u_m z^m = (1 + (z - 2)w)/(1 - 2w + w^2 z^2)$ we deduce $u_m(1) = -m(m - 2)$ and $u_m(1) = m(m - 1)(m^2 - m^2 + 7m + 3) / 3$. It follows that, also in this case, the mean number of steps in the walk is $a(a - n)$ and the variance is $\frac{2}{3} (n^2 - 2a(a - n) - 2a(a - n))$.

The polynomials $t_k$ and $u_k$ in this analysis are disguised relatives of the classical Chebyshev polynomials defined by $T_n(\cos \theta) = \cos n \theta, U_n(\cos \theta) = \sin (m + 1) \theta / \sin \theta$. Let us also write $V_n(\cos \theta) = \cos (m - 1/2) \theta / \sqrt{\theta}$. Then $V_n(x) = (2 - 1/x) T_n(x) + (1/2 - 1/x) U_n(x)$; and we have $t_m = z^m T_m(1/z)$, $u_m = z^m V_m(1/z)$.
106. Before coalescing, the array $a_0a_1 \ldots a_{d-1}$ always has the form $a^{(a+1)}(b-1)b'$ for some $0 \leq a < b < d$, $r > 0$, and $s > 0$, where $r + s + b - a = d + 1$. Initially $a = 0$, $b = d - 1$, $r = s = 1$. The behavior of the algorithm while $r + s = t$ is like a random walk on the $t$-cycle, as in the previous exercise, starting at $a = 1$. Let $G_t$ be the generating function for that problem, which has mean $t - 1$ and variance $2t^3$. Then this problem has the generating function $G_tG_{t-1}\ldots G_1$; so its mean is $\sum_{i=1}^{c} (k-1) = \binom{d}{2}$, and the variance is $\sum_{i=1}^{c} 2\binom{d}{3} = 2\binom{d+1}{4}$.

107. (a) If the probabilities can be renumbered so that $p_1 \leq p_2 \leq \ldots \leq p_q$, the five events of $\Omega$ can have probabilities $p_1, p_2, p_3 - p_1, p_4 - p_2, q_1$ because $p_3 = (q_1 - p_1) + (q_2 - p_2) + q_3$. But if that doesn’t work, we can suppose that $p_1 < q_2 \leq q_3 < p_2 \leq p_3$. Then $p_1, p_1 - p_1, p_2 - q_1, p_3 - q_1, q_2$ are nonnegative.

(b) Give $\Omega$’s events the probabilities $\frac{1}{p_1}, \frac{1}{p_2}, \frac{1}{p_3}, \frac{1}{q_1}, \frac{1}{q_2}$.

(c) For example, let $p_1 = \frac{1}{y}$, $p_2 = p_3 = \frac{1}{x}$, $q_1 = q_2 = \frac{1}{x}$. We get a different formula for $Y(\omega)$ for each $\omega$.

108. Let $p = \Pr(X = k)$ and $q = \Pr(Y = k)$. The set $\bigcup_{i = 1}^{q} \{\sum_{k > i} p_k, \sum_{i < k} q_k\}$ defines the unit interval $[0, 1]$ into countably many subintervals, which we take as the set of atomic events $\omega$. Let $X(\omega) = n$ if and only if $\omega \subseteq \{\sum_{k = n} p_k \ldots \sum_{i < n} p_k\}$; a similar definition works for $Y(\omega)$. And $X(\omega) \leq Y(\omega)$ for all $\omega$.

109. (a) We’re given that $p_1 + p_3 \leq q_1 + q_2$, $p_2 + p_3 \leq q_2 + q_3$, and $p_3 \leq q_3$. (Also that $0 \leq 0$ and $p_1 + p_3 \leq q_1 + q_2 + q_3$; but those inequalities always hold.) We must find a coupling with $p_{12} = p_{21} = p_{31} = p_{32} = 0$, because $1 \not\leq 2, 2 \not\leq 1, 3 \not\leq 1$, and $3 \not\leq 2$. In the previous problem we were given that $p_2 + p_3 \leq q_2 + q_3$ and $p_3 \leq q_3$, and we had to find a coupling with $p_{12} = p_{21} = p_{31} = p_{32} = 0$.

(b) Let $A^* = \{x \mid x \geq a \text{ for some } a \in A\}$ and $B^* = \{x \mid x \leq b \text{ for some } b \in B\}$.

We’re given that $A(\in A^*) \subseteq \Pr^*(Y \in A^*)$ for all $A$. Let $A = \{1, \ldots, n\} \setminus B^*$, so that $\Pr^*(X \in B^*) = 1 - \Pr^*(X \in A)$. The result follows because $A = A^*$.

(c) Remove all arcs $x_i \rightarrow x_j$ from the network when $i \neq j$. Then a blocking pair $(I, J)$ has the property that if $i < j$ implies $i \in I$ or $j \in J$. Let $A = \{x \mid x \geq a \text{ for some } a \in A\}$ and $B = \{1, \ldots, n\} \setminus A$. Then $A \subseteq I, B \subseteq J$, and $B = B^*$. Hence $\sum_{a \in I} p_a + \sum_{b \in J} q_b \geq \sum_{a \in A} p_a + \sum_{b \in J} q_b = 1$.

110. (a) (Solution by E. Schulte-Geers.) The result is trivial if $r = 1$. Otherwise consider the probability distributions $p_k = (p_k - r_k)/(1 - r)$ and $q_k = (q_k - r_k)/(1 - r)$; use the coupling $p_1 = (1 - r)p_1 + r_1[i = j]$.


(b) Yes, because the $(p’, q’)$ distribution satisfies the hypotheses of that exercise.

111. (a) Here are the 60 triples $t \in 3 \pi 4 \pi$, with the minima in **bold** type:

<table>
<thead>
<tr>
<th>134</th>
<th>131</th>
<th>126</th>
<th>142</th>
<th>124</th>
<th>153</th>
<th>145</th>
<th>163</th>
<th>154</th>
<th>215</th>
<th>234</th>
<th>354</th>
<th>563</th>
<th>623</th>
<th>562</th>
<th>632</th>
<th>652</th>
<th>534</th>
<th>643</th>
</tr>
</thead>
<tbody>
<tr>
<td>356</td>
<td>645</td>
<td>236</td>
<td>234</td>
<td>435</td>
<td>463</td>
<td>524</td>
<td>423</td>
<td>642</td>
<td>532</td>
<td>461</td>
<td>351</td>
<td>361</td>
<td>641</td>
<td>251</td>
<td>231</td>
<td>341</td>
<td>531</td>
<td>321</td>
</tr>
<tr>
<td>421</td>
<td>412</td>
<td>345</td>
<td>315</td>
<td>316</td>
<td>615</td>
<td>316</td>
<td>315</td>
<td>623</td>
<td>526</td>
<td>652</td>
<td>452</td>
<td>564</td>
<td>354</td>
<td>465</td>
<td>364</td>
<td>256</td>
<td>265</td>
<td></td>
</tr>
</tbody>
</table>


(b) Both $S_A$ and $S_B$ lie in $A \cup B$. Each element of $A \cup B$ is equally likely to have the minimum value $a \in A$; exactly $|A \cap B|$ of those elements have that value as their sketch.

(c) $|A \cap B \cap C| / |A \cup B \cup C|$.

Notes: The ratio $|A \cap B| / |A \cup B|$ is a useful measure of similarity called the Jaccard index, because Paul Jaccard used it to compare different Swiss sites according to the sets of plant species seen at each place [Bulletin de la Société Vaudoise des Sciences]
Naturelles 37 (1901), 249]. It is commonly used today to rank the similarity between web pages, based on a certain set of words in each page.

Minwise independence was introduced by Andrei Broder for that application in 1997, using n = 2^k and a method of identifying roughly 1000 words A on a typical web page. By calculating, say, independent sketches $S_1(A), \ldots, S_{100}(A)$ for each page, the number of j such that $S_j(A) = S_j(B)$ gives a highly reliable and quickly computable estimate of the Jaccard index. A perfectly minwise independent family is impossible in practice when n is huge, but the associated theory has suggested approximate "minhash" algorithms that work well. See A. Z. Broder, M. Charikar, A. M. Frieze, and M. Mitzenmacher, J. Computer and System Sciences 60 (2000), 630-659.

112. (a) Such a rule breaks ties properly, provided that the number of π with ∞’s in B is a multiple of n − m. Each B can have its own rule.

(b) In fact we can produce families whose permutations are all obtained from $N/n = d$ "seeds" by cyclic shifts, as in exercise 111. Begin with m = 1 and a table of $N = \text{lcm}(1, 2, \ldots, n)$ partial permutations whose entries $π_{ij}$ for $1 \leq i \leq N$ and $1 \leq j \leq n$ are entirely blank, except that $π_{ij} = 1$ for each pair $i j$ with $(j-1)d < i \leq jd$ and $1 \leq j \leq n$. When $n = 4$, for instance, the initial tableau

```
1234 1234 1234 1234 1
```

represents $N = 12$ truncated permutations with $m = 1$. We’ll insert some 2s next.

Let A be a subset of size $n - m$ that is all blank, in some π. Each A occurs equally often (as in uniform probing, Section 6.4); so the number of such π is $N/(n-m\binom{n}{m})$. Fortunately this is a multiple of $n - m$, because exercise 1.2-6-48 tells us that $N/(n-m\binom{n}{m}) = N\sum_{k=0}^{m}(-1)^k \binom{m}{k} (n - m + k)$.

Take $n - m$ such π and insert $m+1$ into different positions within them. Then find another such A, if possible, and repeat the process until no blank subsets of size $n - m$ remain. Then set $m \leftarrow m + 1$, and continue in the same way until $m = n$.

It’s not hard to see that the insertions can be done so that $π_i, π_{i+j}, \ldots, π_{(n-1)j+i}$ are maintained as cyclic shifts of each other. When $n = 4$ the 2s are essentially forced:

```
1234 1234 1234 1234 1
```

But then there are two ways to fill the two cases with $A = \{3, 4\}$:

```
1234 1234 1234 1234 1
```

Adapting the first of these leads to two ways to fill $A = \{2, 4\}$:

```
1234 1234 1234 1234 1
```

Here A is a cyclic shift of itself, but consistent placement is always possible.


113. (a) The probability is zero if $l \geq k$ or $r > n - k$. Otherwise the result follows if we can prove it in the "complete" case when $l = k - 1$ and $r = n - k$, because we can sum the probabilities of complete cases over all ways to specify which of the unconstrained elements are $< k$ and which are $> k$.

To prove the complete case, we may assume that $a_1 = i$, $b = k$, and $c_j = k + j$ for $1 \leq i \leq l = k - 1$ and $1 \leq j \leq r = n - k$. The probability can be computed

May 20, 2015
via the principle of inclusion and exclusion, because we know \( \Pr(\min_{k \in A} a \pi = k \pi) = 1/(n - k + t) = P_0 \) whenever \( A = \{k, \ldots, n\} \cup B \) and \( B \) consists of \( t \) elements less than \( k \). For example, if \( k = 4 \) the probability that \( 4\pi = 4 \) and \( \{1\pi, 2\pi, 3\pi\} = \{1, 2, 3\} \) is \( P_0 - P_{(1)} - P_{(2)} - P_{(3)} + P_{(1, 2)} + P_{(1, 3)} + P_{(2, 3)} - P_{(1, 2, 3)} \); each of those probabilities is correct for truly random \( \pi \).

(b) This event is the disjoint union of complete events of type (a). [See A. Z. Broder and M. Mitzenmacher, Random Structures & Algorithms 18 (2001), 18–30.]

Notes: The function \( \psi(n) = \ln(\operatorname{lcm}(1, 2, \ldots, n)) = \sum_{p \leq n} \left\lfloor \ln p \right\rfloor \) was introduced by P. L. Chebyshev [see J. de mathématiques purus et appliquées 17 (1852), 360–390], who proved that it is \( \Theta(n) \). Refinements by C. J. de la Vallée Poussin [Annales de la Société Scientifique de Bruxelles 20 (1896), 183–236] showed that in fact \( \psi(n) = n + O(ne^{-C\log n}) \) for some positive constant \( C \). Thus \( \psi(1, 2, \ldots, n) \) grows roughly as \( e^n \), and we cannot hope to generate a list of minwise independent permutations when \( n \) is large; the length of such a list is 232,792,560 already for \( 19 \leq n \leq 22 \).

114. First assume that \( |S_j| = d_j + 1 \) for all \( j \). Let \( x_j \) be an element of \( S_j \) with \( x_j \notin x_j \). We can replace \( x_j^{d_j+1} \) by \( x_j^{d_j+1} \), without changing the value of \( f(x_1, \ldots, x_n) \), when \( x_j \in S_j \). Doing this repeatedly until every term of \( f \) has degree \( \leq d_j \) in each variable \( x_j \), we can produce a polynomial that has at least one nonroot in \( S_1 \times \cdots \times S_n \), according to exercise 4.6.1–6. [See N. Alon, Combinatorics, Probab. and Comput. 8 (1999), 7–29.]

Now in general, if there were at most \( |S_1| + \cdots + |S_n| = (d_1 + 1 + \cdots + d_n + n) \) nonroots, we could find subsets \( S_j \subseteq S_j \) with \( |S_j| = d_j + 1 \) such that \( S_j \) differs from \( x_j \) in \( S_j \setminus d_j - 1 \) of the nonroots and \( S_j \times \cdots \times S_n \) avoids them all—a contradiction.

(1) Inequality above also implies stronger lower bounds when the sets \( S_j \) are large. If, for example, \( d_1 = \cdots = d_n = d \) and if each \( |S_j| \geq s \), where \( s = d + 1 + \lceil d/(n - 1) \rceil \), we can decrease each \( |S_j| \) to \( s \) and increase the right-hand side. For further asymptotic improvements see B. Bollobás, Extremal Graph Theory (1978), §6.2 and §6.3.

115. Representing the vertex in row \( x \) and column \( y \) by \( (x, y) \), if all points could be covered we’d have \( f(x, y) = \prod_{j=1}^{m} (x - a_j) \prod_{j=1}^{n} (y - b_j) \prod_{j=1}^{n} (x + y + c_j) (x - y + d_j) = 0 \), for all \( 1 \leq x \leq m \) and \( 1 \leq y \leq n \) and for some choices of \( a_j, b_j, c_j, d_j \). But \( f \) has degree \( p + q + 2r = m + n + 2 \), and the coefficient of \( x^{m-1} y^{n-1} \) is \( \binom{m+n-2}{m-1} \neq 0 \).

116. Let \( g_v = \sum \{x_v \mid v \in e \} \) for each vertex \( v \), including \( x_v \) twice if \( e \) is a loop from \( v \) to itself. Apply the multistellensatz with \( f = \prod_{j=1}^{m} (1 - y_v^{e_j}) - \prod_{j=1}^{n} (1 - x_j) \) and with each \( S_j = \{0, 1\} \), using \( p \) arithmetic. This polynomial has degree \( m \), the number of edges and variables, because the first product has degree \( (p - 1)n < m \); and the coefficient of \( \prod_{j=1}^{m} x_v \) is \(-1)^m \neq 0 \). Hence there is a solution \( x \) that makes \( f(x) \) nonzero. The subgraph consisting of all edges with \( x_v = 1 \) in this solution is nonempty and satisfies the desired condition, because \( g_v(x) \mod p = 0 \) for all \( v \).

(2) This proof works also if we consider that a loop contributes just 1 to the degree.

117. If \( \omega = e^{2\pi i/m} \), we have \( E^\omega X = \sum_{k=0}^{m} \begin{pmatrix} n \end{pmatrix} p^k (1 - p)^{n-k} \omega^k = (\omega p + 1 - p)^n \). Also \( |\omega| p + 1 - p |^2 = p^2 + (1 - p)^2 + p (1 - p)(\omega^2 + \omega^{-2}) = 1 - 4p(1 - p) \), thus \( \sin \pi t \geq 2t \) for \( 0 \leq t \leq 1/2 \). Hence, if \( 0 \leq j \leq m/2 \) we have \( |\omega^j p + 1 - p |^2 \leq 1 - 16(p - 1)p^{j/2} \). If \( m/2 \leq j \leq m \) we have \( \sin \pi j/m = \sin \pi (m - j/m) \). Thus \( \sum_{j=0}^{m-1} |E^\omega X |^2 \leq \sum_{j=0}^{m-1} \exp(-8p(1 - p)j^2/n/m^2) \).

The result follows, since \( \Pr(X \mod m = r) = 1/m \sum_{j=0}^{m-1} \omega^{-jr} E^\omega X \). [S. Janson and D. E. Knuth, Random Structures & Algorithms 10 (1997), 130–131.]

May 20, 2015
118. Indeed, (22) with $Y = X - x$ yields more (when we also apply exercise 47):

$$
\Pr(X \geq x) \geq \Pr(X > x) \geq \frac{(E X - x)^2}{E(X - x)^2} = \frac{(E X - x)^2}{E X^2 - x(2E X - x)}
$$

$$
\geq \frac{(E X - x)^2}{E X^2 - x E X} \geq \frac{(E X - x)^2}{E X^2 - x^2}.
$$

(The attribution of this result to Paley and Zygmund is somewhat dubious. They did, however, write an important series of papers [Proc. Cambridge Philos. Soc. 26 (1930), 337–357, 458–474; 28 (1932), 190–205] in which a related inequality appeared in the proof of Lemma 19.)
INDEX AND GLOSSARY

He writes indexes to perfection.
— OLIVER GOLDSMITH, Citizen of the World (1762)

When an index entry refers to a page containing a relevant exercise, see also the answer to that exercise for further information. An answer page is not indexed here unless it refers to a topic not included in the statement of the exercise.

\( \gamma \) (Euler's constant), 28.
\( \nu(x) \) (sideways sum), 13.
\( \pi \) (circle ratio), 14.
\( \phi \) (golden ratio), 12, 25.
a.s.: Almost surely, 11-12, 20, 21, 38, 39.
Aae Now, 8, 19.
Ahmed, Rudolph, 33.
Aldous, David John, 32.
Almost sure events, 11.
Alexander, Noga (BNF), 43.
Analysis of algorithms, 9, 21, 22.
Arithmetic-geometric mean inequality, 30, 38.
Asymptotic methods, 11, 12, 16.
Atomic events, 1.
Auman, Kazuo (吾妻一興), 9, 20.

\( B(p_1, \ldots, p_m) \), see Multivariate Bernoulli distribution.
\( B_n(p) \), see Binomial distribution.
\( B_{n\times m}(p) \), see Cumulative binomial distribution.
Backward versus forward, 21.
Ballot numbers, 38.
Bayes, Thomas, 14.
BDD (binary decision diagram), 5, 33.
Bell, Eric Temple, number, 15.
Bernoulli, Daniel, 35.
Bernoulli, Jacques (= Jakob = James), distribution, multivariate, 14, 18, 20.
Bernoulli, Nicolas (= Nikolaus), 35.
Beta distribution, 14.
Bhatia, Rajendra (भटिया राजेंद्र), 27.
Berzins, Irène Jules, inequality, 4.
Binary notation, 14.
Binggour, 12-13.
Binomial distribution, 14, 24, 31.
cumulative, 14-15, 30.
Bit vectors, 3, 9, 13-14.
Blackwell, David Harold, 36.
Bollobás, Béla, 43.
Boolean functions, 5, 15, 32, 34.
dual of, 32.
monotone, 5, 34.
symmetric, 16.

Boolean random variables, see Binary random variables.
Boolean vectors, see Bit vectors.
Boyd, Stephen Poyness, 32.
Bracket notation, 2.
Bracketing property, 33.
Broder, Andrej Zoro, 42, 43.
Brown, John O'Connor, 25.

Cutelli, Francesco Paolo, inequality, 32.
Casorati de Seinigul, Giacono Girolamo, 35.
Catalan, Eugène Charles, numbers, 35.
Chain rule for conditional probability, 14, 27.
Clarikčar, Miren Samson (चल्रिकचा), 42.
Chebyshev (= Tchebycheff), Paul Léonitchi (Чебышев, Пауль Льонич), 32, 43.
incompleteness, 12, 19.
monotone inequality, 21, 38.
nonmonotone inequality, 34.
polynomial, 26, 40.
Chesterfield, Gilbert Keith, 25.
Chickas, 15.
Circle ratio \( (\pi) \), 14.
Cliffords, 16-17.

Counting random walks, 21.
Coin tosses, 11-12, 19, 30.
Column sums, 22.
Combinatorial nullstellensatz, 23.
Commutative law, 30.
Compositions, 36.
Concave functions, 4, 31.
incompleteness, 5, 16, 33.
Conditional probability, 1, 13-14, 31.
Connell, Robert, Jr., 37.
Convex combinations, 32.
Convex functions, 4, 8, 16, 20, 32, 37, 38.
Correlated random variables, 17-18, 27, 36.
Correlation inequalities, 17.
Coupling, 22.
Covariance, 2, 14, 17, 27, 34.

May 20, 2015

GOLDSMITH
INDEX AND GLOSSARY

Coxer, Thomas Merrill, 13, 27.
Covering all points, 23.
Cumulative binomial distribution, 14–15, 30.
Cycle graph (Cn), 22, 40.

Davis, Chandler, 27.
Daykin, David Edward, 33.
de La Vallée Poussin, Charles Jean
Gustave Nicolas, 43.
de Moivre, Abraham, 36.

Decomposition, Pierre Rémond, 35.
Degree of a multivariate polynomial, 23.
Diagonals, Persi Warren, iv.
Diagonal lines, 23.
Discrete probabilities, 1.
Dobrushin, Roland L’vovich (Добрушин, Роланд Л’вович), 41.
Doob, Joseph Leo, 6, 9, 37.
martingales, 9–10, 20, 36, 38.
Dual of a Boolean function, 32.

Eggenberger, Florian, 6.
Elton, John Hancock, 30.
 enveloping series, 33.
Endre, Pál (= Paul), 33.
Etesami, Omid (آميد اتاصمي), iv.
Euler, Leonhard (Эйлер, Леонард = Эйлер, Леонар), constant γ, 28.
Eulerian numbers, 36.
Events, 1–3.
exchangeable random variables, 36.
Expected value, 2–5, 14–16, see also Conditional expectation.

Fair sequences, 7, 10, 19, 37.
with respect to a sequence, 7, 36.
Families of nets, 17.
Feige, Uriel (ויריע פייג’), iv, 30.
Feller, William (Вильям Феллер), 35.
Fibonacci, Leonardo, of Pisa (= Leonardo
filo Bonacci Pisano), 12, 19.
martingale, 19.
numbers, 12, 37.
First moment principle, 4, 16.
FKG inequality, 5, 17, 34.
Flow in a network, 22.
Fortuin, Cornelis Maria, 17.
Forward versus backward, 21.
Four functions theorem, 17, 33.
Friedland, Shmuel (שמעון וירידל), 43.
Friedmann, Bernard, iv, 19.
Frisch, Allan Michael, 42.

Games, 4, 8, 13.
Garey, Michael Randolph, 11.
Generating functions, 15, 22, 31, 32,
35, 39, 40.
Generation of random objects, 40.
Geometric distribution, 21.
Geometric mean and arithmetic mean,
30, 38.
Georgiadis, Evangelos (Γεωργιάδης,
Ευάγγελος), 27.
Gilat, David, 37.
Gnifbre, Jean, 17.
Golden ratio (ϕ), 12, 25.
Goldsmith, Oliver, 45.
Goldstein, Sheldon, 41.
Cooper, Ralph William, Jr., 27.
Graham, Ronald Lewis (葛蘭姆), 45.
Grid, 23.
Gumball machine problem, 30.
HAKMEM, 27.
Harmonic numbers, fractional, 37.
Hashing, 9–10, 20.
Hoeffding, Wassily, 9, 15.
inequality, 9–10, 20.

Inclusion and exclusion, 30, 33, 43.
Incomplete beta function, 14.
Independent events, 2.
Independent random variables, 1, 7, 9,
10, 13–15, 20, 36.
K-wise, 1, 13.
Infinite mean, 35, 37.
Integral multilinear representation, see Reliability polynomials.
Internet, ii, iii.
Inverses, 35.
Itoh, Toshiya (伊東利哉), 42.

Jaccard, Paul, 41.
index, 41–42.
James White, Phyllis Dorothy, 11.
Janssen, Carl Swante, iv, 37, 43.
Jensen, Johan Ludvig William Valdemar, 32.
inequality, 4, 16, 32, 37.
Johnson, David Stiller, 11.
Joint distribution, 13, 34.
K-cliques, 17.
K-wise independence, 1, 13.
Káli, Gil (גיל קַלְּי), 43.
Kallenberg, Olav Herbert, 36.
Karp, Richard Manning, 39.
Kasteleyn, Pietert Willem, 17.
Kendall, David George, 36.
Knuth, Donald Ervin (高德納), i, iii,
iv, 36, 39, 43, 45.
Kolmogorov, Andrei Nikolaevich
(Колмогоров, Андрей Николаевич), 9.
inequality, 9.

May 20, 2015
INDEX AND GLOSSARY 47

La Vallée Poussin, Charles Jean Gustave Nicolas de, 43.
Lake Wobegon dice, 12.
Large deviations, see Tail inequalities.
Larrue, Cora Maui, 21.
Least common multiple, 23.
Lipschitz, Rudolph Otto Sigismund, condition, 10.
Loops, running time of, 21.
Loops from a vertex to itself, 24.
Lord, Nicholas John, 29.
Lukács, Eugene (= Jenő), 27.
MacQueen, James Buhford, 37.
Magic masks, 27.
Mahler, Kurt, 27.
Markov (= Markoff), Andrei Andreevich
(Maposcope, Андрей Андреевич),
the elder, 4.
Markov inequality, 4, 5, 16, 37, 38.
Martingale differences, see Fair sequences.
Martingales, 6–11, 18–20, 31.
with respect to a sequence, 7, 19, 36.
Max-flow min-cut theorem, 22, 41.
Maximal inequality, 8, 9, 20.
McDiarmid, Colin John Hunter, 10.
Median value of a random variable, 14.
Mengden, Nikolaï Alexandrovitch von
Менден, Николай Александрович,
= Jaro, 24.
Method of bounded differences, 10.
Minhash algorithms, 42.
Mintes, 30.
Minwise independent permutations, 23.
Mitrashvili, Michael David, 42, 43.
Möbius, Abraham de, 19, 36.
Monotone Boolean functions, 5, 34.
Monotone Monte Carlo method, 40.
Monte Carlo, Pierre Rémond de, 35.
Monas operation, 21–22.
Monte Carlo, Oliva, Jorge Alfonso, 26.
Moore, Harold Calvin Martin, constant, 27.
Motwani, Rajeev (राजीव मोटवानी), 39.
MPR: Mathematical Preliminary Redux, v.
Multigraphs, 24.
Multiplicatively fair sequences, 19.
Multivariate Bernoulli distribution,
14, 18, 20.
Multivariate total positivity, see FKG inequality.
Nandi, 12–13.
Nawrotzki, Kurt, 41.
Negative binomial distribution, cumulative, 14.
Negatively correlated random variables, 18, 28.
Neumann, Peter, 29.
Neville-Neil, George Vernon, III, 48.
Newton, Isaac, 29.
Nonnegative submartingales, 9, 37.
Nonnegatively correlated random
variables, 17.
Nontransitive dice, 12.
NP-complete problems, 11.
Nullstellensatz, combinatorial, 23.
One-sided estimates, 16.
Optimal stopping principle, 8, 37.
Order ideals, 41.
$p$ (power set, the family of all subsets), 33.
Pairwise independent random variables, 1, 13.
Palay, Raymond Edward Alan Christopher, 24, 44.
Paradoxes, 12, 13, 35.
Parity number, 27.
Parity of a binary integer, 13.
Partial ordering, 22.
Patashnik, Owen, 45.
Pearson, Karl (= Carl), 28.
π (pi), 14.
Pitman, James William, 29.
Pittel, Boris Gershon (Herrera, Boris Геппел), 39.
Playing cards, 1, 8, 14, 19.
Pólya, Simon Denis, distribution, 15, 34.
trials, 34.
Pólya, György (= George), 6, 19.
urn model, iv, 6–7, 19–20, 37.
Polynomials, 23; see also Chebyshev polynomials, Reliability polynomials.
Positively correlated random variables, 17, 27.
Power series, 32.
Prime implicants of a Boolean function,
5, 33.
Probabilistic estimates, 3–5, 8–9, 16.
Probability generating functions, 15, 39.
Probability spaces, 1–2.
Prapp, James Gary, 40.
q.s.: Quite surely, 12, 20, 21.
Quick, Jonathan Horatio, 18.
Quite sure events, 12, 26.
Raghavan, Prabhakar (पर्यावरण
प्रभाकर), 39.
Random bits, 2, 3, 5, 9, 13–15, 35.
Random graphs, 16, 18.
Random number generators, 40.
Random permutations, 15.
Random variables, 1–21.
Random walk, 18.
converting, 21.
on-cycle, 22, 41.
Randomized algorithms, 21.
Recurrence relations, 35, 40.

Regular graphs and multigraphs, 24.

Reliability polynomials, 5, 15, 16.

Rémond de Montmort, Pierre, 35.

Rényi, Alfréd, 33.

Restricted growth strings, 15.

Ross, Sheldon Mark, iv, 5, 32.

Roe sums, 22.

Runs of a permutation, 36.

$S_n$ (a symmetric threshold function), 16.

Sáenz, Stephen Mitchell, 15, 30.

Saturating addition and subtraction, 21–22.

Savage, Richard Preston, Jr., 25.

Say Red, 37.

Schroeppe, Richard Crabtree, 27.

Schütte-Geers, Ernst Franz Fred, iv, 13, 30, 28, 41.

Second moment principle, 4, 16, 24, 32.

Set partitions, 29, 31.

Sets, represented as integers, 34.

Shinoda, Takahiro (篠田高朗), 42.

Shuffles, 1.

Sideways sum (aor), 13.

Sketches, 23.

St. Petersburg paradox, 35.

Stadje, Gerl Wolfgang, 38.

Stirnaker, David Robert, 31.


Stock, David Geoffrey, 26.

Strassen, Volker, 41.

Street, Charles David George, iii.

Subadditive law, 11.

Submartingales, 5–9, 20.

Submodular set functions, 34.

Subsequence of a martingale, 18.

Summation by parts, 37.

Supermartingales, 8, 30.

Superpolynomially small, 12, 39.

Supported sets, 17.

Sylvester, James Joseph, 29.

Symmetric Boolean functions, 16.

$t$-ary ballot numbers, 38.

Tails inequalities, 4, 8–11, 15, 20, 21.

Takai, Yoshinori (武田芳憲), 42.

Taylor, Brook, formula, 20.

Thue, Axel, constant, 27.

Totally uncorrelated sequences, 37.

Transcendental numbers, 27.

Triangles (biclique), 16.

Trybuła, Stanisław, 20.

Uncorrelated sequences, 37.

Uniform distribution, 1, 13, 16, 22,

23, 35, 36, 40.

Uniform random, 42.

Union inequality, 14.

Upfal, Eli (?229 [Y]), 39.

Urn models, 6–7, 18–20, 37.

Usiskin, Zalman Philip, 26.

Vallée Poussin, Charles Jean Gustave

Nicolas de la, 43.

Vandenberghe, Lieven Lodewijk André, 32.

Vandermónde, Alexandre Théophile,

matrix, 27.

Variance, 2, 4, 9, 14, 34.

Vicious, Rode (pen name of George Vernon

Neville-Neil III), vi.

von Mises, Richard Alexanderovich

(фом Мизес, Николай Александрович), 24.

Wald, Abraham (= Abrahám), 37.

equation, 20.

Web pages, 42.

Wchp (with high probability), see a.s.

Wigderson, Avi (?വിഗ്ഡെർസൺ, ആവി), 39.

Wilson, David Bruce, 40.

Winkler, Peter Mann, 30.

Zygmund, Antoni, 24, 44.