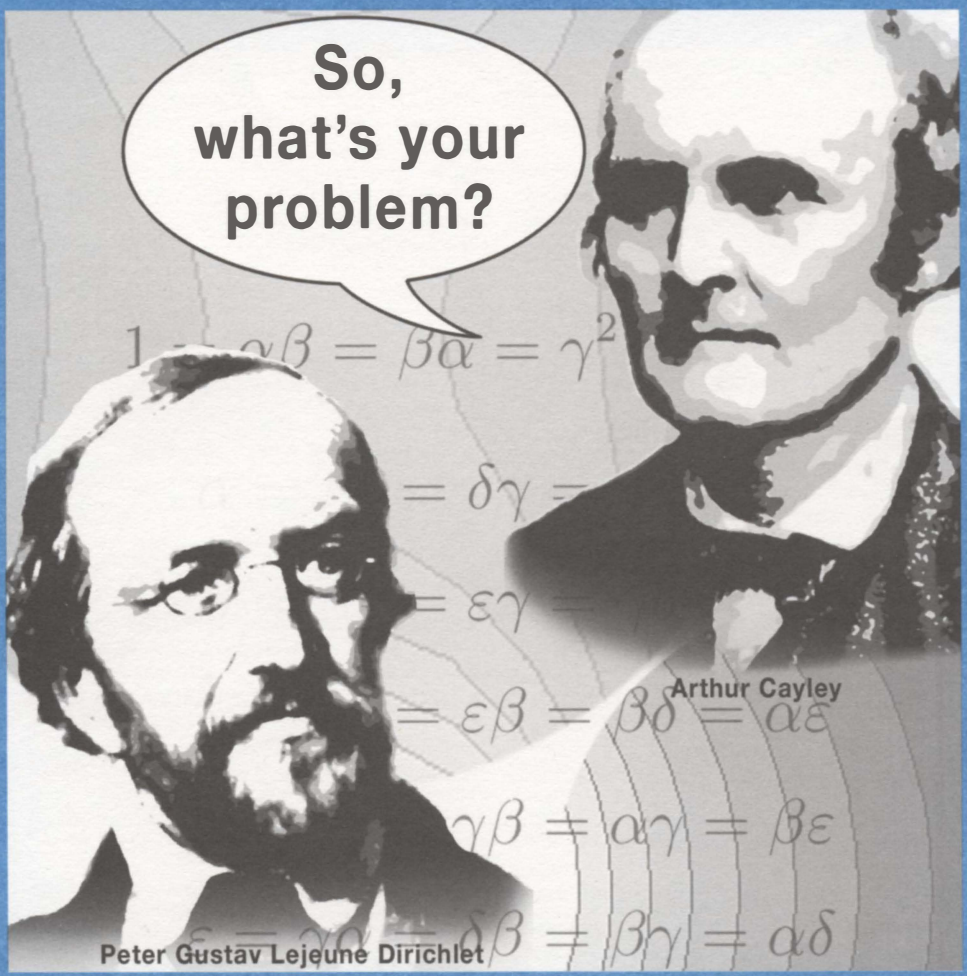
Vol. 78, No. 4, October 2005

MATHEMATICS MAGAZINE



- Stopping Strategies and Gambler's Ruin
- Arthur Cayley and the Abstract Group Concept
- Dirichlet: His Life, His Principle, and His Problem

An Official Publication of The MATHEMATICAL ASSOCIATION OF AMERICA

EDITORIAL POLICY

Mathematics Magazine aims to provide lively and appealing mathematical exposition. The *Magazine* is not a research journal, so the terse style appropriate for such a journal (lemma-theorem-proof-corollary) is not appropriate for the *Magazine*. Articles should include examples, applications, historical background, and illustrations, where appropriate. They should be attractive and accessible to undergraduates and would, ideally, be helpful in supplementing undergraduate courses or in stimulating student investigations. Manuscripts on history are especially welcome, as are those showing relationships among various branches of mathematics and between mathematics and other disciplines.

A more detailed statement of author guidelines appears in this *Magazine*, Vol. 74, pp. 75–76, and is available from the Editor or at www.maa.org/pubs/mathmag.html. Manuscripts to be submitted should not be concurrently submitted to, accepted for publication by, or published by another journal or publisher.

Submit new manuscripts to Allen Schwenk, Editor-Elect, Mathematics Magazine, Department of Mathematics, Western Michigan University, Kalamazoo, MI, 49008. Manuscripts should be laser printed, with wide line spacing, and prepared in a style consistent with the format of *Mathematics Magazine*. Authors should mail three copies and keep one copy. In addition, authors should supply the full five-symbol 2000 Mathematics Subject Classification number, as described in *Mathematical Reviews*.

Cover image, *What's Dirichlet's Problem?*, by Jason Challas. Inquiring Arthur Cayley wants to know. You can find out more about Dirichlet's Problem by reading the article by Pamela Gorkin and Joshua H. Smith in this issue.

Jason Challas teaches at West Valley College in Saratoga, CA, where he helps students solve their own problems with computer graphics.

AUTHORS

James D. Harper has been teaching the full spectrum of undergraduate math courses at Central Washington University since 1988. Although he was trained as a harmonic analyst, these days he is more of a mathematical hobbyist dabbling in number theory and infinite series. Jim got the idea for this article when he generalized the gambler's ruin example in Susanna Epp's discrete math book. Since probability is not his strong suit, he asked Ken for help on getting all his *p*s and *q*s to sum to one. His nonmathematical interests include hiking, running, and losing his voice at Hayward Field track meets in Eugene, Oregon.

Kenneth A. Ross's first real job was at the University of Rochester, where the chairman was his mathematical godfather, Leonard Gillman. Ken taught at the University of Oregon from 1965 to 2000. He was Secretary and Associate Secretary of the MAA from 1984 to 1993, and he served as MAA President, 1995–1996. For relaxation, he prefers passive activities such as attending concerts, plays, movies and baseball games, though he has been known to raise his voice at baseball games. His latest book is *A Mathematician at the Ballpark: Odds and Probabilities for Baseball Fans*, published in 2004.

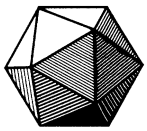
Pamela Gorkin is Professor of Mathematics at Bucknell University, where she was named Presidential Professor during the years 2000–2003. She teaches a wide range of classes, and her research interests include function theory and operator theory. Professor Gorkin is a frequent visitor to Bern, Switzerland, the University of Metz in France, and she has had the pleasure of taking part in the RIP program in Oberwolfach on several occasions. According to the Mathematics Genealogy Web site, Professor Gorkin is a descendant of Dirichlet.

Joshua H. Smith is a Ph.D. student in the Department of Mechanical and Aerospace Engineering at the University of Virginia. His research interests include the transport of chemical solutes in porous media, with application to perfusion in biological tissue. He completed his Bachelor's degree in mathematics at Bucknell University, including an honors thesis under the guidance of Pamela Gorkin.

Sujoy Chakraborty was born in 1972 in Comilla, Bangladesh. He entered the University of Dhaka in 1989 to read mathematics. He earned the M.Sc. degree in Pure Mathematics and continued with the M.Phil. program. He was awarded the M.Phil. degree in 2002 for a dissertation on "The theory of groups from Cayley to Frobenius," written under the supervision of Professor M. R. Chowdhury. He has been teaching at Shah Jalal University of Science and Technology since 1999. His interests include algebra, number theory, and history of mathematics.

Munibur Rahman Chowdhury was born in 1941 in Faridpur in what was then British India, now in Bangladesh. He entered the University of Dhaka in 1958 to read physics, but went to Germany to read mathematics. Entering the University of Hamburg in fall 1960, he attended the last cycle of lectures on algebra by the legendary Emil Artin (1898–1962). After Artin's sudden demise, he moved to the University of Göttingen, where he received the degree of Dr. rer. nat. in 1967 for a dissertation on "Unitary groups over algebraic number fields," written under the supervision of Martin Kneser (1928–2004). He has taught at several universities at home and abroad, and has been a professor at the University of Dhaka since 1984. His interests include algebra, number theory, history of mathematics and mathematics education. He is a past president of Bangladesh Mathematical Society.

Vol. 78, No. 4, October 2005



MATHEMATICS MAGAZINE

EDITOR
Frank A. Farris
Santa Clara University

ASSOCIATE EDITORS
Glenn D. Appleby
Santa Clara University
Arthur T. Benjamin
Harvey Mudd College
Paul J. Campbell
Beloit College
Annalisa Crannell
Franklin & Marshall College
David M. James
Howard University
Elgin H. Johnston
Iowa State University
Victor J. Katz
University of District of Columbia
Jennifer J. Quinn
Occidental College
David R. Scott
University of Puget Sound
Sanford L. Segal
University of Rochester
Harry Waldman
MAA, Washington, DC

EDITORIAL ASSISTANT
Martha L. Giannini

MATHEMATICS MAGAZINE (ISSN 0025-570X) is published by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, D.C. 20036 and Montpelier, VT, bimonthly except July/August.
The annual subscription price for *MATHEMATICS MAGAZINE* to an individual member of the Association is $131. Student and unemployed members receive a 66% dues discount; emeritus members receive a 50% discount; and new members receive a 20% dues discount for the first two years of membership.)

Subscription correspondence and notice of change of address should be sent to the Membership/ Subscriptions Department, Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036. Microfilmed issues may be obtained from University Microfilms International, Serials Bid Coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

Advertising correspondence should be addressed to Frank Peterson (*FPetersonj@aol.com*), Advertising Manager, the Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036.

Copyright © by the Mathematical Association of America (Incorporated), 2005, including rights to this journal issue as a whole and, except where otherwise noted, rights to each individual contribution. Permission to make copies of individual articles, in paper or electronic form, including posting on personal and class web pages, for educational and scientific use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear the following copyright notice:

Copyright the Mathematical Association of America 2005. All rights reserved.

Abstracting with credit is permitted. To copy otherwise, or to republish, requires specific permission of the MAA's Director of Publication and possibly a fee.

Periodicals postage paid at Washington, D.C. and additional mailing offices.

Postmaster: Send address changes to Membership/ Subscriptions Department, Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036-1385.

Printed in the United States of America

ARTICLES

Stopping Strategies and Gambler's Ruin

JAMES D. HARPER
Central Washington University
Ellensburg, WA 98926
harperj@cwu.edu

KENNETH A. ROSS
University of Oregon
Eugene, OR 97403
ross@math.uoregon.edu

Let's play a game. Roll a die and you win \$2 if the die shows 1 or 2. Otherwise you lose \$1. Thus about one-third of the time you win \$2 and about two-thirds of the time you lose \$1. Suppose you have a definite idea in mind about how much you would like to win. To be concrete, suppose you start with \$5 and decide to play until you double your fortune or lose it all (that is, are ruined). In other words, you will stop playing when you have \$0, \$10, or \$11.

This game with a die is fair because, on average, for each 3 games, you win \$2 once and lose \$1 twice. However, it is not the same fair game as in the classical coin-flipping game where you win or lose \$1, each with probability 1/2. One difference is the experience of a player facing ruin at the gambling table. The classical theory of what is called "gambler's ruin" tells us that the probability of ruin in the coin-flipping game is 1/2, that is, a player who starts with \$5 and swears to stop at \$10—a *double-or-nothing strategy*—faces even chances of being ruined or winning double.

Knowing this about the coin-flipping game calls some parallel questions to mind. In our die-rolling game, is it still true that probabilities for success or ruin are 1/2, that the double-or-nothing strategy is fair? What is the expected time for the duration of this strategy? In other words, how many games will you play on average?

We ask similar questions for unfair games. For example, we consider the game where you win \$2 with probability 4/40, you win \$1 with probability 11/40, and you lose \$1 with probability 25/40. This game is not fair; the average loss per game is 15 cents.

We refer to gambling strategies such as the double-or-nothing strategies above as *stopping strategies*. We refer to the possible values of your fortune (\$0, \$10, and \$11 in our first example) as "stopping values."

In this paper we show how to answer the first questions (probabilities of success and ruin) using recurrence relations. Then we introduce the language and methods of random variables, showing how these probabilities can be used to solve the duration question. A key will be two identities due to Wald, for which we give elementary proofs at the end of the paper.

This paper should be accessible to any reader with a working background with recurrence relations and knowledge of sophomore level probability, in particular, an acquaintance with discrete random variables and expectation, and a willingness to work with infinite sums and matrices. All random variables in this paper will be discrete ones

(that is, have countable range—integers in our case); the concepts of independence and expectation are easier in this setting and we need nothing more.

A classical ruin problem Our investigation was inspired by the classical ruin problem based on flipping a fair coin. We imagine a person repeatedly betting \$1 on heads who is willing to risk his or her fortune, \$$a$, to win \$$b$. It turns out that

$$\text{probability of ruin} = \frac{b}{a+b} \text{ and probability of success} = \frac{a}{a+b}.$$

These answers are reasonable because we would expect the strategy to be fair, and with these probabilities the expected gain is

$$b \times \frac{a}{a+b} - a \times \frac{b}{a+b} = 0.$$

It turns out that the expected duration of this strategy is ab. That is, if this strategy were repeated over and over, then the average duration would involve ab flips of the coin. We will verify this in passing after we introduce Wald's second identity.

Much more information about the classical ruin problem, both when the coin is fair and when the coin is not fair, can be found in Takács [**11**], Jewett and Ross [**7**], Ross [**9**, chapter 7], and Feller [**6**, chapters III and XIV]. Reference [**11**] is an excellent source for history on the subject. Bak [**1**] also starts with a classical ruin problem, but rather than consistently betting the same amount, his gambler varies his bet as his anxiety level increases. This is an interesting story, which is very different from ours.

Solution to the 1/3 versus 2/3 game

Recall our game where, for each \$1 bet, one-third of the time you win \$2 and two-thirds of the time you lose your \$1. Suppose that you have \$5 to wager and you wish to (at least) double your fortune, that is, you would like to end up with \$10 or \$11. Let $P_N^{(10)}$ denote the probability that you will *eventually* end up with \$10 given that you have \$$N$, where $0 \le N \le 11$. The other probability functions, $P_N^{(11)}$ and $P_N^{(0)}$, are defined similarly. Note that $P_N^{(10)}$ and $P_N^{(11)}$ are the success probability functions and $P_N^{(0)}$ is the ruin probability function. The stopping values $k = 0, 10, 11$ provide us with the following initial values: $P_N^{(k)}$ is 1 when $N = k$ and is 0 when $N \neq k$ for $N = 0, 10, 11$.

We use the tools of recurrence relations to find the probabilities of success and ruin or, to be more precise, the probability of each of the stopping values. Our primary and most complete reference for recurrence relations is Rosen [**8**, pp. 413–418]. Actually, many other discrete math texts have the pieces necessary to solve the recurrence relations we will encounter (for instance, Epp [**5**, Chapter 8] and Ross and Wright [**10**, section 4.5]). We need to know how single roots and double roots of the characteristic equation contribute to the general solution of a recurrence relation.

Here is the crucial observation: Each of these probability functions satisfies the following recursion relation:

$$P_N^{(k)} = (1/3)P_{N+2}^{(k)} + (2/3)P_{N-1}^{(k)} \quad \text{for } 1 \le N \le 9.$$

The subscripts of the right-hand side probability functions correspond to winning \$2 (with probability 1/3) and losing \$1 (with probability 2/3). Now suppose this relation has a solution of the form $P_N^{(k)} = x^N$ for some real number x. When we plug

this solution into our recursion we have $x^N = (1/3)x^{N+2} + (2/3)x^{N-1}$. Dividing both sides by x^{N-1} gives us $x = (1/3)x^3 + (2/3)$, which is the *characteristic equation* for this recursion relation. From the characteristic equation, we have the *characteristic polynomial*

$$f(x) = (1/3)x^3 - x + (2/3) = (1/3)(x-1)^2(x+2).$$

It can be shown that, when the characteristic polynomial has a double root at $x = r$, then $P_N^{(k)} = N \cdot r^N$ is another solution. The general solutions in our case are linear combinations of $1^N = 1$, $N \cdot 1^N = N$, and $(-2)^N$. A different linear combination will produce the correct solution for each value of k, that is,

$$\begin{aligned} P_N^{(0)} &= x_{11} + x_{12} \cdot N + x_{13} \cdot (-2)^N, \\ P_N^{(10)} &= x_{21} + x_{22} \cdot N + x_{23} \cdot (-2)^N, \\ P_N^{(11)} &= x_{31} + x_{32} \cdot N + x_{33} \cdot (-2)^N. \end{aligned}$$

Plugging in the initial values for $N = 0, 10, 11$ leads to the following matrix equation:

$$\begin{bmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 & 1 \\ 0 & 10 & 11 \\ 1 & 1024 & -2048 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Solving this equation is equivalent to finding the following inverse:

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 10 & 11 \\ 1 & 1024 & -2048 \end{bmatrix}^{-1} = \frac{1}{31743} \begin{bmatrix} 31744 & -3072 & -1 \\ -11 & 2049 & 11 \\ 10 & 1023 & -10 \end{bmatrix}.$$

The first row of the inverse provides us with the coefficients of the ruin probability function $P_N^{(0)}$, and the second and third rows provide us with the coefficients of the success probability functions $P_N^{(10)}$ and $P_N^{(11)}$, respectively. We can now give explicit formulas for these functions:

$$\begin{aligned} P_N^{(0)} &= \left[31744 - 3072N - (-2)^N\right]/31743, \\ P_N^{(10)} &= \left[-11 + 2049N + 11 \cdot (-2)^N\right]/31743, \\ P_N^{(11)} &= \left[10 + 1023N - 10 \cdot (-2)^N\right]/31743. \end{aligned}$$

In the scenario we described earlier, where you begin with \$5 we have:

$$P_5^{(0)} = \frac{1824}{3527} \approx .517153, \quad P_5^{(10)} = \frac{1098}{3527} \approx .311313, \quad P_5^{(11)} = \frac{605}{3527} \approx .171534.$$

Does this ruin probability, $P_5^{(0)}$, seem reasonable to you? Since you would like to win, on the average, a little more than your initial fortune, the probability of ruin ought to be a little more than $1/2$, and it is.

Suppose you would be satisfied to win a little less than half your initial fortune by stopping at 0, 9, or 10. Then the probability of ruin should be a little less than $1/2$, and it is. In fact, the probabilities are

$$P_5^{(0)} = \frac{736}{1593} \approx .462021, \quad P_5^{(9)} = \frac{605}{1593} \approx .379787, \quad P_5^{(10)} = \frac{252}{1593} \approx .158192.$$

Without any of these calculations, the strategy where you win \$4 or \$5 seems similar to the fictitious coin-flipping strategy where you have $a = \$5$ and you wish to win $b = \$4.50$. The probability of ruin for this strategy would be $\frac{b}{a+b} = 4.5/9.5 \approx .473684$, which is pretty close to the actual ruin probability .462021.

General set-up

It is not hard to generalize the 1/3 versus 2/3 game: Each time you play, you win \$1 with probability p_1, win \$2 with probability $p_2, \ldots$, and win \$$u$ with probability p_u, and you lose \$1 with probability q_1, lose \$2 with probability $q_2, \ldots$, and lose \$$v$ with probability q_v. It should be noted that in this general situation you are essentially betting \$$v$ each time you play. You could lose some of your bet or all of your bet or, in happier circumstances, you could win up to \$$u$. Here, of course, we are assuming that the probabilities for the greatest win (\$$u$) and the most feared loss (\$$v$), p_u and q_v, are positive. The expected value, each time you bet, of this game is

$$1 \cdot p_1 + 2 \cdot p_2 + \cdots + u \cdot p_u - 1 \cdot q_1 - 2 \cdot q_2 - \cdots - v \cdot q_v.$$

Our stopping strategy is as follows: Consider $0 < v \leq N < M$. You begin with N, you are successful if you reach M or more, and you are ruined if your fortune goes below v. Usually, v will be 1; in this case, we write q for q_1. Also, we use $u > 1$ in this paper, though the classical ruin problem corresponds to the case $u = v = 1$.

The games we mentioned in the introduction all involve $u = 2$ and $v = 1$. In the first example, $p_1 = 0$, $p_2 = 1/3$, $q_1 = q = 2/3$, $N = 5$, and $M = 10$. In the unfair game, $p_1 = 11/40$, $p_2 = 4/40$, $q = 25/40$, and we did not specify N or M. The expected value for this unfair game is $1 \cdot (11/40) + 2 \cdot (4/40) - 1 \cdot (25/40) = -.15$ dollars. A gambler playing this game would lose, on the average, 15 cents per game.

As we did in the 1/3 versus 2/3 game, let $P_N^{(k)}$ be the probability that you will eventually end up with \$$k$ when you have \$$N$, $0 \leq N < M + u$. Here k is one of the desired stopping values $M, M+1, \ldots, M+u-1$, if you are successful, and one of the undesirable stopping values $0, 1, \ldots, v-1$, if you lose. This leads to the following recursive relations:

$$P_N^{(k)} = \sum_{j=1}^{u} p_j \cdot P_{N+j}^{(k)} + \sum_{j=1}^{v} q_j \cdot P_{N-j}^{(k)}, \qquad v \leq N < M.$$

Moreover, for each possible stopping value k, we have $u + v$ initial conditions because $P_N^{(k)}$ is 1 for $N = k$ and is 0 for other integers N among $M, M+1, \ldots, M+u-1, 0, 1, \ldots, v-1$. Since we have $u + v$ possible stopping values k, we have $(u+v)(u+v)$ initial conditions in all.

The characteristic equation for *each* of these recursion relations is

$$x^v = \sum_{j=1}^{u} p_j \cdot x^{v+j} + \sum_{j=1}^{v} q_j \cdot x^{v-j}.$$

Hence the characteristic polynomial for our game is

$$f(x) = \sum_{j=1}^{u} p_j \cdot x^{v+j} - x^v + \sum_{j=1}^{v} q_j \cdot x^{v-j}.$$

Note that this is a polynomial of degree $u + v$ and that q_v is the constant term. Since each of the probability functions has the same recursion relation, $f(x)$ is the charac-

teristic polynomial for each $P_N^{(k)}$. Also, $f(1) = 0$ because the sum of the probabilities of winning and losing, the p_js and q_js, is 1.

Recall that 1 was a double root of the characteristic polynomial in the 1/3 versus 2/3 game. This is a feature of all fair games. Indeed, we can say a little more. Observe that

$$\begin{aligned} f'(1) &= \sum_{j=1}^{u} p_j \cdot (v + j) - v + \sum_{j=1}^{v} q_j \cdot (v - j) \\ &= v \cdot \left[\sum_{j=1}^{u} p_j - 1 + \sum_{j=1}^{v} q_j \right] + \sum_{j=1}^{u} j \cdot p_j - \sum_{j=1}^{v} j \cdot q_j \\ &= v \cdot f(1) + \sum_{j=1}^{u} j \cdot p_j - \sum_{j=1}^{v} j \cdot q_j = \sum_{j=1}^{u} j \cdot p_j - \sum_{j=1}^{v} j \cdot q_j, \end{aligned}$$

which is exactly the expected value of this game. Isn't that interesting? In particular, 1 is a double root of f if and only if the game is fair.

If you look at the form of the characteristic polynomial, you will see that $f(x)$ has exactly one negative interior term and therefore there are two sign changes in the coefficients. Hence, by Descartes' Rule of Signs, this polynomial has either two (counting multiplicities) or zero positive roots. Since 1 is a root free of charge, $f(x)$ has two positive roots. When the game is unfavorable, $f'(1) < 0$ and therefore the other positive root is larger than 1. When the game is favorable, $f'(1) > 0$ and this implies that the other positive root is between 0 and 1. For unfair games we will call these non-unity roots the *ruin root* and the *fortune root*, respectively. (Feller [**6**] gives a geometric argument for these observations.)

The method for finding closed forms for the probability functions $P_N^{(k)}$ parallels the method we used in the 1/3 versus 2/3 game. The first step is to factor the characteristic polynomial. Then the set of stopping values $M, M + 1, \ldots, M + u - 1$ and $v - 1, \ldots, 0$ will lead us to solving $u + v$ systems of linear equations each of which has $u + v$ unknowns. Solving these systems is equivalent to finding the inverse of the corresponding coefficient matrix. All of this is nice and tidy in theory, but in practice we still need to find the roots and the inverse of a (possibly large) matrix. This being done, the rows of the inverse matrix will provide us with the corresponding coefficients for the probability functions $P_N^{(k)}$. It is interesting to note that our original questions were posed with fixed N and M, but this process will give us, for a *fixed* M, solutions for all N.

Cubic characteristic polynomials

Here we analyze the case $u = 2$ and $v = 1$, where you gain \$1 or \$2 or lose \$1. In this case, the characteristic polynomial, f, is a cubic. Since f has two positive roots and f is real-valued, its third root, which we call s, is negative. We now fix M, that is, our gambler wishes to finish the game with either $\$M$ or $\$(M + 1)$. We deal with the fair case first.

In the fair case, 1 is a double root of the characteristic polynomial. It is not hard to show that the other root is $s = -q/p_2$, where p_2 is the probability of winning \$2 and q is the probability of losing \$1. (For example, in the 1/3 versus 2/3 game, $p_2 = 1/3$ and $q = 2/3$, so $s = -2$.) Our probability functions $P_N^{(0)}$, $P_N^{(M)}$, $P_N^{(M+1)}$ for this fair

game have the form

$$P_N^{(0)} = x_{11} + x_{12} \cdot N + x_{13} \cdot s^N,$$
$$P_N^{(M)} = x_{21} + x_{22} \cdot N + x_{23} \cdot s^N,$$
$$P_N^{(M+1)} = x_{31} + x_{32} \cdot N + x_{33} \cdot s^N.$$

When we substitute the stopping values $N = 0$, M, $M + 1$, the inverse of our corresponding matrix is

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & M & M+1 \\ 1 & s^M & s^{M+1} \end{bmatrix}^{-1} = \frac{1}{d} \begin{bmatrix} s^M(Ms - M - 1) & s^M(1-s) & 1 \\ M+1 & s^{M+1} - 1 & -(M+1) \\ -M & 1 - s^M & M \end{bmatrix},$$

where $d = (Ms - M - 1)s^M + 1$. From here we can give an explicit description of our probability functions. Indeed,

$$P_N^{(0)} = \left[s^M(Ms - M - 1) + s^M(1-s) \cdot N + s^N\right]/d,$$
$$P_N^{(M)} = \left[(M+1) + (s^{M+1} - 1) \cdot N - (M+1) \cdot s^N\right]/d,$$
$$P_N^{(M+1)} = \left[-M + (1 - s^M) \cdot N + M \cdot s^N\right]/d.$$

These formulas not only give us the general solution for the 1/3 versus 2/3 game, they can be used in any fair game with $u = 2$ and $v = 1$. For example, consider the fair game where $p_1 = p_2 = 1/5$ and $q = 3/5$. Then the negative root is $s = -q/p_2 = -3$. This game is a little closer to the coin-flipping game than the 1/3 versus 2/3 game, since the probability of success in this game is 40%. Intuitively, the probability of ruin should be a little closer to one-half than in our first game. Let's see: When we plug in the values $N = 5$, $M = 10$, and $s = -3$, we get

$$P_5^{(0)} = \frac{77517}{151313} \approx .512296,$$
$$P_5^{(10)} = \frac{55191}{151313} \approx .364747,$$
$$P_5^{(11)} = \frac{18605}{151313} \approx .122957.$$

Well, the ruin probability is not much closer to 1/2, but it is nevertheless closer. Now let us plug in $N = 5$, $M = 9$, and $s = -3$:

$$P_5^{(0)} = \frac{20898}{45517} \approx .459125, \quad P_5^{(9)} = \frac{18605}{45517} \approx .408748, \quad P_5^{(10)} = \frac{6014}{45517} \approx .132126.$$

Not quite what we expected, because $P_5^{(0)}$ is further from 1/2 than in the 1/3 versus 2/3 case. Perhaps the negative roots for these games cause this oscillatory behavior. We leave the reader to experiment with other double-or-nothing strategies to see if this phenomenon persists.

We now turn our attention to the unfair case. Once again $u = 2$ and $v = 1$. In this case, 1 is a single root of the characteristic polynomial. As we mentioned earlier, the characteristic polynomial will have another positive root r (the ruin root) and the third root s will be negative. Since the roots are single roots, the probability functions have

the form

$$P_N^{(0)} = x_{11} + x_{12} \cdot r^N + x_{13} \cdot s^N,$$
$$P_N^{(M)} = x_{21} + x_{22} \cdot r^N + x_{23} \cdot s^N,$$
$$P_N^{(M+1)} = x_{31} + x_{32} \cdot r^N + x_{33} \cdot s^N.$$

As we did in the fair case, we substitute the stopping values $N = 0, M, M+1$ and compute the inverse of the coefficient matrix:

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & r^M & r^{M+1} \\ 1 & s^M & s^{M+1} \end{bmatrix}^{-1} = \frac{1}{d} \begin{bmatrix} (s-r) \cdot (sr)^M & (1-s) \cdot s^M & (r-1) \cdot r^M \\ r^{M+1} - s^{M+1} & s^{M+1} - 1 & 1 - r^{M+1} \\ s^M - r^M & 1 - s^M & r^M - 1 \end{bmatrix},$$

where $d = (s^{M+1} - 1)(r^M - 1) - (r^{M+1} - 1)(s^M - 1)$. You really didn't expect the inverse to be as nice as in the fair case did you? Again the rows of this inverse provide the coefficients for the probability functions $P_N^{(k)}$, where $k = 0, M, M+1$. Thus the formulas for these probability functions are

$$P_N^{(0)} = \left[(s-r) \cdot (sr)^M + (1-s) \cdot s^M \cdot r^N + (r-1) \cdot r^M \cdot s^N\right]/d,$$
$$P_N^{(M)} = \left[r^{M+1} - s^{M+1} + (s^{M+1} - 1) \cdot r^N + (1 - r^{M+1}) \cdot s^N\right]/d,$$
$$P_N^{(M+1)} = \left[s^M - r^M + (1 - s^M) \cdot r^N + (r^M - 1) \cdot s^N\right]/d.$$

We can now use these formulas to find the probabilities of stopping values for the unfair game mentioned in the introduction. You win \$2 with probability 4/40, win \$1 with probability 11/40 and lose \$1 with probability 25/40. Recall that the average loss per game is 15 cents. In keeping with our stopping strategies in our fair game examples, we will use the double-or-nothing strategy with $N = 5$ and $M = 10$. The characteristic polynomial for this game is

$$f(x) = (10/40) \cdot x^3 + (11/40) \cdot x^2 - x + (25/40) = (x-1)(x - 5/4)(x+5)/40.$$

Hence our ruin root is $r = 5/4$ and the negative root is $s = -5$. When we use the double-or-nothing strategy with an initial fortune of \$5 we find

The probability of being ruined is	$P_5^{(0)} \approx .764215,$
The probability of ending up with \$10 is	$P_5^{(10)} \approx .196434,$
The probability of ending up with \$11 is	$P_5^{(11)} \approx .039351.$

The expected value using this strategy is

$$0 \cdot .764215 + 10 \cdot .196434 + 11 \cdot .039351 \approx 2.3972.$$

That is, on the average, you would lose \$2.60 using this stopping strategy. (Wow! You would lose 52% of your initial fortune.) How much better would we do if we would settle for the "at most double-or-nothing strategy" with $M = 9$? Here are the probabilities:

The probability of being ruined is	$P_5^{(0)} \approx .696458,$
The probability of ending up with \$9 is	$P_5^{(9)} \approx .253218,$
The probability of ending up with \$10 is	$P_5^{(10)} \approx .050324.$

This time the expected value is

$$0 \cdot .696458 + 9 \cdot .253218 + 10 \cdot .050324 \approx 2.7822,$$

which amounts to an average loss of \$2.22.

Expectations

Now we rephrase our questions in terms of discrete random variables. For a sequence ω of possible outcomes, we let $X_i(\omega)$ be the random variable that records the gain or loss in the ith game. Then the sum $X_1 + \cdots + X_n = S_n$ represents the change in the initial capital after n games. Thus S_n represents the amount gained or lost, depending on whether it is positive or negative.

For any random variable Y, we write $\mathbf{Pr}(Y = k)$ for the probability that Y is equal to k. The *expectation* $\mathbf{E}[Y]$ of Y is the probabilistic average of Y; if Y takes only integer values, we have

$$\mathbf{E}[Y] = \sum_k k \cdot \mathbf{Pr}(Y = k).$$

The gambling strategies in this paper are all based on *stopping times* and are hence called *stopping strategies*. Consider our earlier examples where, for each sequence ω of outcomes, $X_i(\omega)$ is either 2, 1, or -1. For each k, $S_k(\omega)$ represents the gain or loss after k games. For any sequence ω of outcomes, we write $T(\omega)$ for the first subscript for which $S_{T(\omega)}(\omega)$ is one of the values -5, 5, or 6. Clearly this value depends only on the values $X_1(\omega), X_2(\omega), \ldots, X_{T(\omega)}(\omega)$. In other words, whether $T(\omega) = n$ depends only on the values $X_1(\omega), \ldots, X_n(\omega)$. This is the essential property of a stopping time. In our example, if the first few values of $S_n(\omega)$ happened to be

$$1, 0, -1, -2, 0, -1, -2, -1, 1, 2, 3, 4, 6,$$

then the process stops when $n = 14$, so that $T(\omega) = 14$ and $S_{T(\omega)}(\omega) = S_{14}(\omega) = 6$. Note that S_T is a new and interesting random variable, and in our example it takes on only the values -5, 5 and 6. This is the random variable we have been interested in all along, because its value at each ω is the amount gained or lost when the strategy ends. The probabilities obtained so far have had the form $\mathbf{Pr}(S_T = k)$ for suitable stopping values k.

Given the probabilities $\mathbf{Pr}(S_T = k)$ obtained earlier, we want (a) the expected values $\mathbf{E}[S_T]$ of these stopping strategies, and (b) the expected duration times $\mathbf{E}[T]$ that the strategies will last. The answers depend on whether the original games are fair or not. In either case, we need

WALD'S IDENTITY I. $\mathbf{E}[S_T] = \mathbf{E}[X_1] \cdot \mathbf{E}[T]$.

This is reasonable: If on average you expect to gain $\mathbf{E}[X_1]$ at each game and on average you expect to play $\mathbf{E}[T]$ games, then you would expect on average to gain $\mathbf{E}[X_1] \cdot \mathbf{E}[T]$ using your strategy. This is all that Wald's first identity is saying, but this is surprisingly delicate to prove, as we see at the end of this article.

If the games are fair, then $\mathbf{E}[X_1] = 0$, so $\mathbf{E}[S_T] = 0$ by Wald's first identity. In fact, very general results assert that fair games stay fair no matter what sort of stopping strategy is used. Similarly, unfair games stay unfair when a stopping strategy is used.

However, $\mathbf{E}[S_T]$ will not usually be the same as $\mathbf{E}[X_1]$. But with the probabilities $\mathbf{Pr}(S_T = k)$ at hand, it is easy to calculate

$$\mathbf{E}[S_T] = \sum_k k \cdot \mathbf{Pr}(S_T = k),$$

and then $\mathbf{E}[T] = \mathbf{E}[S_T]/\mathbf{E}[X_1]$ by Wald's first identity.

If the games are fair, both sides of Wald's identity are 0, so it is of no use in calculating $\mathbf{E}[T]$. We need

WALD'S IDENTITY II. If $\mathbf{E}[X_1] = 0$, then $\mathbf{E}[S_T^2] = \mathbf{E}[X_1^2] \cdot \mathbf{E}[T]$.

To compute $\mathbf{E}[T]$ from this, we need $\mathbf{E}[X_1^2]$, which is easy, and

$$\mathbf{E}[S_T^2] = \sum_k k^2 \cdot \mathbf{Pr}(S_T = k).$$

Wald's identities hold under certain conditions, which are satisfied in our case; we give more details at the end of the article.

Let us return to the classical ruin problem involving a fair coin, where success means winning b and ruin means losing a (a and b are positive integers). Now $X_i = \pm 1$ with probability $1/2$ each, so $\mathbf{E}[X_1^2] = 1$ and $\mathbf{E}[T] = \mathbf{E}[S_T^2]$ by Wald's identity II. As noted earlier, though without our new notation, $S_T = b$ with probability $a/(a+b)$, and $S_T = -a$ with probability $b/(a+b)$. So the expected duration is

$$\mathbf{E}[T] = \mathbf{E}[S_T^2] = b^2 \times \frac{a}{a+b} + (-a)^2 \times \frac{b}{a+b} = ab,$$

that is, the hoped-for gain times the feared loss.

Return to the game in which one-third of the time you win \$2, and two-thirds of the time you lose \$1, using starting and ending values $N = 5$ and $M = 10$. Then

$$\mathbf{E}[X_i^2] = 2^2 \times \frac{1}{3} + (-1)^2 \times \frac{2}{3} = 2.$$

Since $S_T = -5$ with probability .517153, $S_T = 5$ with probability .311313, and $S_T = 6$ with probability .171534, Wald's second identity gives

$$\mathbf{E}[T] = \frac{1}{2}\left[(-5)^2 \times .517153 + 5^2 \times .311313 + 6^2 \times .171534\right] \approx 13.44.$$

Is the last answer $\mathbf{E}[T] \approx 13.44$ reasonable? Well, in our hearts we feel this game is similar to the imaginary fair game where $b = 5.5/2$ (because your steps go up 2 at a time) and $a = 5$. In that imaginary strategy (because b is not an integer), the expectation is $\mathbf{E}[T] = ab = 13.75$.

If you play the $1/3$ versus $2/3$ game and $N = 5$ but $M = 9$, then a similar computation yields

$$\mathbf{E}[T] = \frac{1}{2}\left[(-5)^2 \times .462021 + 4^2 \times .379787 + 5^2 \times .158192\right] \approx 10.79.$$

For unfair games, finding $\mathbf{E}[T]$ is easy once we have $\mathbf{E}[S_T]$ and $\mathbf{E}[X_1]$. For the unfair example in the introduction we already calculated $\mathbf{E}[X_1] = -.15$. For the double-or-nothing strategy with $N = 5$ and $M = 10$, we found that the expected value of the strategy was about 2.3792, so that $\mathbf{E}[S_T] \approx 2.40 - 5 \approx -2.60$. Since, on average, you

lose 15 cents per game and \$2.60 using this stopping strategy, it seems intuitive that, on average, playing this stopping strategy will take $260/15 = 17.33$ games. This intuition is correct, but not obvious. It is exactly what Wald's first identity gives us.

Feller's fourth degree example

We now illustrate with a fair game analyzed by Feller [**6**, section XIV.8], where $u = v = 2$ and $p_1 = p_2 = q_1 = q_2 = 1/4$. As Feller notes, the monic characteristic polynomial is

$$f(x) = (x-1)^2(x-\sigma_3)(x-\sigma_4),$$

where

$$\sigma_3 = \frac{-3+\sqrt{5}}{2} \quad \text{and} \quad \sigma_4 = \sigma_3^{-1} = \frac{-3-\sqrt{5}}{2}.$$

Consider the case where we have \$2 and wish to gain \$4, that is, $N = 2$ and $M = 4$. Using our methods, $\mathbf{Pr}(S_T = -2) = 4/15$, $\mathbf{Pr}(S_T = -1) = \mathbf{Pr}(S_T = 2) = 1/3$, and $\mathbf{Pr}(S_T = 3) = 1/15$. Note that

$$\mathbf{Pr}(\text{ruin}) = \mathbf{Pr}(S_T = -2 \text{ or } S_T = -1) = 3/5.$$

Of course, $\mathbf{E}(S_T) = 0$, because the game is fair. Also

$$\mathbf{E}(S_T^2) = 4 \times \frac{4}{15} + 1 \times \frac{1}{3} + 4 \times \frac{1}{3} + 9 \times \frac{1}{15} = \frac{10}{3}.$$

Since $\mathbf{E}(X_1^2) = 1^2 \times .5 + 2^2 \times .5 = 2.5$, Wald's second identity gives

$$\mathbf{E}(T) = \frac{10/3}{2.5} = \frac{4}{3}.$$

This strategy has a very short duration, on average.

Now consider $M = 5$, $N = 2$. Then $\mathbf{Pr}(S_T = -2) = .300$, $\mathbf{Pr}(S_T = -1) = .400$, $\mathbf{Pr}(S_T = 3) = .200$, and $\mathbf{Pr}(S_T = 4) = .100$. Note that $\mathbf{Pr}(\text{ruin}) = .700$. Now

$$\mathbf{E}(S_T^2) = 4 \times .30 + 1 \times .40 + 9 \times .20 + 16 \times .10 = 5,$$

so $\mathbf{E}(T) = \mathbf{E}(S_T^2)/\mathbf{E}(X_1^2) = 2$.

Feller focuses only on the probability of ruin, so he does not calculate the expected duration $\mathbf{E}(T)$. However, he works with general M and N. His model is shifted by 1, because he views 0 and -1 as ruin. We prefer our set up because in gambling casinos they frown on you if you lose more than you have. Feller's notation is quite different and his formula (8.10) for ruin is wrong. In his notation, it should read

$$u_z = 1 - \frac{z}{a} + \frac{(2z-a)(1-\sigma_4^a) - a(\sigma_3^{z-a} - \sigma_4^z)}{a\{(a+2)(1-\sigma_4^a) - a(\sigma_3 - \sigma_4^{a+1})\}}.$$

In our notation, the probability of ruin is

$$1 - \frac{N-1}{M-1} + \frac{(2N-M-1)(1-\sigma_4^{M-1}) - (M-1)(\sigma_3^{N-M} - \sigma_4^{N-1})}{(M-1)\{(M+1)(1-\sigma_4^{M-1}) - (M-1)(\sigma_3 - \sigma_4^M)\}}.$$

With this formula, our work agrees with Feller's, that is, the formula gives .600 when $M = 4$ and $N = 2$, and it gives .700 when $M = 5$ and $N = 2$.

By symmetry, we've covered the interesting cases for $M = 4$ and $M = 5$ except to find the duration of the strategy when $M = 5$ and $N = 3$. Here N is midway between ruin (0 or 1) and success (5 or 6), so the expectation of ruin is .500. But we need more to get $\mathbf{E}(T)$. In this case, $\mathbf{Pr}(S_T = -3) = \mathbf{Pr}(S_T = 3) = .100$ and $\mathbf{Pr}(S_T = -2) = \mathbf{Pr}(S_T = 2) = .400$. Then $E(S_T^2) = 9 \times .200 + 4 \times .800 = 5$, so $\mathbf{E}(T) = 2$ again. That's interesting.

Other questions

One may wonder whether the expectation, $\mathbf{E}[T]$, which is the average time of *all* outcomes of stopping strategies, is also the average time of all winning outcomes of stopping strategies (equivalently, of all losing outcomes). Consider the simple example of the fair coin-flipping ruin problem where we have \$1 and hope to gain \$2, so that $b = 2$ and $a = 1$. In this example, S_n must oscillate between 1 and 0 until just before the strategy ends at -1 or 2. So we can calculate directly the conditional expectation of T, *given the outcome is a success*, and the conditional expectation of T, *given ruin*. First note that strategies that end at 2 end with T even, while strategies that end at -1 end with T odd. Since $\mathbf{Pr}(\text{strategy ends at } 2) = 1/3$ and $\mathbf{Pr}(\text{strategy ends at } -1) = \mathbf{Pr}(\text{ruin}) = 2/3$, the first conditional expectation is

$$\frac{1}{\mathbf{Pr}(\text{strategy ends at 2})} \sum_{k=1}^{\infty} 2k\, \mathbf{Pr}(T = 2k) = 6 \sum_{k=1}^{\infty} k \left(\frac{1}{2}\right)^{2k} = \frac{8}{3}$$

and the second conditional expectation is

$$\frac{1}{\mathbf{Pr}(\text{ruin})} \sum_{k=1}^{\infty} (2k-1)\, \mathbf{Pr}(T = 2k-1) = \frac{3}{2} \sum_{k=1}^{\infty} (2k-1) \left(\frac{1}{2}\right)^{2k-1} = \frac{5}{3}.$$

Then $\mathbf{E}[T]$ would have to be $\frac{1}{3} \times \frac{8}{3} + \frac{2}{3} \times \frac{5}{3} = 2$. This agrees with $\mathbf{E}[T] = ab = 2$.

In a fair game, all stopping strategies are also fair. And, as we have already seen, with a negative expectation for each game, a stopping strategy will also have a negative expectation. But the expected losses for various stopping strategies are different from the expected loss per game and different from each other. Is there anything we can say?

Suppose, for example, that we have two games, one where the winning value is always \$1 and one where the winning value is \$$w$ where $w > 1$. Suppose also that the expected loss per game is the same in these two games and that our stopping strategies are the same, that is, we begin with \$$N$ and hope to reach \$$M$ before going broke. Which game is better from the point of view of the stopping strategy? We suspect that the expectation of a strategy does not depend on the loss per game, but rather on its ruin root. This is a question that deserves further study. We now give an example to show that there can be a big difference between the expectations.

In roulette, there are 38 equally likely outcomes, 18 of which are black, 18 of which are red and 2 of which are green. The probability of winning on red is $9/19$, and the probability of winning on green is $1/19$. A winning \$1 bet on red will pay \$1, and a winning bet on green will pay \$17. Both games (betting on red or green) have the same expectation per game: $-\$1/19$, that is, on average the loss will be about 5.26 cents per game. As gambling at casinos goes, this is not a bad expectation. Suppose that Mrs. Rose bets on red and Mr. Green bets on green, and that they use the same stopping strategy by starting with \$12 and hoping to reach \$18, or more, before going

broke. Since Mr. Green will stop immediately if he ever wins a game, we can calculate both of their expectations using this strategy. Mrs. Rose's expected loss is about \$3.94 whereas Mr. Green's is only about 48 cents, as follows:

The only way Mr. Green can be ruined is if he loses the first 12 times he plays. If he wins just once, he will go home with money in his pocket. The probability that he wins on the first spin of the wheel is $1/19$ and he would take home \$29. The probability that he loses on the first spin and then wins on the second spin is $(18/19) \cdot (1/19)$ and he would take home \$28. In general, the probability that he loses on the first $k-1$ spins and then wins on the kth spin ($1 \le k \le 12$) is $(18/19)^{k-1} \cdot (1/19)$ in which case he'd take home $\$(30-k)$. Hence his take-home expectation is

$$\sum_{k=1}^{12} (18/19)^{k-1} \cdot (1/19) \cdot (30-k) \approx \$11.52.$$

Mrs. Rose's stopping strategy is the classical gambler's ruin strategy where $p = 9/19$ is the probability of winning \$1 and $q = 10/19$ is the probability of losing \$1. Formula (2.4) in section XIV.2 of Feller **[6]** shows that the probability that Mrs. Rose will succeed and reach \$18, rather than lose \$12 is

$$\frac{(p/q)^6 - (p/q)^{18}}{1-(p/q)^{18}} = \frac{(9/10)^6 - (9/10)^{18}}{1-(9/10)^{18}} \approx .448;$$

Therefore Mrs. Rose's take-home expectation is $\$18 \cdot .448 \approx \$8.06$. Since both Mr. Green and Mrs. Rose started with \$12, their expected losses are 48 cents and \$3.94 per stopping strategy, respectively.

Even if they change the rules and both start with \$1, or both start with \$17, Mr. Green has the better expectation. In the first case, his expected loss is about 10.5 cents while Mrs. Rose's is over 66 cents. In the second case, Mr. Green's expected loss is about \$1.24 while Mrs. Rose's is about \$2.00.

Proving Wald's identities

In keeping with the spirit of this article, we will avoid complications involving σ-fields and other advanced notions by assuming that the random variables X_i are discrete random variables taking integer values. We further assume that they are *i.i.d.*, that is, independent and identically distributed. *Identically distributed* means that they take the same values with the same probabilities, that is, for each k,

$$\mathbf{Pr}(X_i = k) = \mathbf{Pr}(X_j = k) \quad \text{for all } i \text{ and } j.$$

This implies that all $\mathbf{E}[X_i]$ are equal and that all $\mathbf{E}[X_i^2]$ are equal.

Independence means that knowing the values of some of the random variables does not affect the probabilities of the values of the other random variables. This can be stated in terms of conditional probabilities, for instance, $\mathbf{Pr}(X_2 = 5 | X_1 = -1) = \mathbf{Pr}(X_2 = 5)$. Our needs are rather special, and we won't need such detailed information. What we need is that if Y and Z are independent random variables, then $\mathbf{E}[YZ] = \mathbf{E}[Y] \cdot \mathbf{E}[Z]$. In probability, the characteristic function of an event A is called an *indicator function* and written I_A. Two events A and B are independent if and only if their indicator functions I_A and I_B are independent random variables.

To help understand the proofs of Wald's identities, first imagine for a moment that the stopping time T is independent of *all* of the outcomes $X_1, X_2, \ldots$, so that whether $T(\omega) = n$ does *not* depend on the values $X_1(\omega), X_2(\omega), \ldots, X_n(\omega)$. For example, suppose Jim and Ken played independent sequences of games, that Jim used a double-

or-nothing stopping time T, and that Ken used the same stopping time, so that they would quit at the same time. Then T would be independent of Ken's sequence of outcomes, and there would be no limit on how much Ken might lose (or win).

In this case, where T is independent of all outcomes, the proof of Wald's first identity is easy and natural by considering T on each of the sets where it is constant and summing:

$$\mathbf{E}(S_T) = \sum_{n=1}^{\infty} \mathbf{E}(S_T \cdot I_{\{T=n\}}) = \sum_{n=1}^{\infty} \mathbf{E}(S_n \cdot I_{\{T=n\}}).$$

Since S_n and $I_{\{T=n\}}$ are independent, we get

$$\mathbf{E}(S_T) = \sum_{n=1}^{\infty} \mathbf{E}(S_n) \cdot \mathbf{E}(I_{\{T=n\}}) = \sum_{n=1}^{\infty} n \cdot \mathbf{E}(X_1) \cdot \mathbf{E}(I_{\{T=n\}}),$$

so that

$$\mathbf{E}(S_T) = \mathbf{E}(X_1) \cdot \sum_{n=1}^{\infty} n \cdot \mathbf{Pr}(\{T = n\}) = \mathbf{E}(X_1) \cdot \mathbf{E}(T).$$

However, in each of our examples, the stopping time T is not independent of the variables S_n. This is what makes them interesting. For instance, if we knew that $T(\omega) = 17$ in one of our first examples, then we would know that $S_{17}(\omega)$ must be -5, 5 or 6. What is true in all of our examples is that X_n is independent of $\{T = n - 1\}$ and, in fact, X_n is independent of $\{T \leq n - 1\}$—knowing that the process stops before n steps gives no information about the nth outcome. Then X_n also is independent of the complement $\{T \geq n\}$. In terms of functions,

$$\text{for each } n, \text{ the random variables } X_n \text{ and } I_{\{T \geq n\}} \text{ are independent.}$$

To prove Wald's identities, all we need is this observation and the following key formulas, which hold for any sequence $\{X_i\}$ of random variables and any random variable T with range $\{1, 2, 3, \ldots\}$:

$$S_T = \sum_{n=1}^{\infty} X_n \cdot I_{\{T \geq n\}} \quad \text{and} \quad \mathbf{E}[T] = \sum_{n=1}^{\infty} \mathbf{Pr}\{T \geq n\}.$$

The first equality is easily checked at each sequence ω of outcomes. For instance, if $T(\omega) = 17$ then $I_{\{T \geq n\}}(\omega) = 1$ if and only if $n \leq 17$, so the sum equals $\sum_{n=1}^{17} X_n(\omega) = S_{17}(\omega) = S_T(\omega)$.

We derive the second equality from the first equality by letting each X_n be the identically 1 function, a random variable that isn't very random. This gives $T = \sum_{n=1}^{\infty} I_{\{T \geq n\}}$. Taking the expectation $\mathbf{E}$ of both sides yields the second equality.

These computations work so long as $\mathbf{E}[|X_1|]$ and $\mathbf{E}[T]$ are finite.

WALD'S IDENTITY I. With the hypotheses above, $\mathbf{E}[|X_1|]$ finite and $\mathbf{E}[T]$ finite,

$$\mathbf{E}[S_T] = \mathbf{E}[X_1] \cdot \mathbf{E}[T].$$

Proof. Since X_n and $I_{\{T \geq n\}}$ are independent, we have

$$\mathbf{E}[S_T] = \sum_{n=1}^{\infty} \mathbf{E}[X_n \cdot I_{\{T \geq n\}}] = \sum_{n=1}^{\infty} \mathbf{E}[X_n] \cdot \mathbf{E}[I_{\{T \geq n\}}] = \sum_{n=1}^{\infty} \mathbf{E}[X_1] \cdot \mathbf{Pr}[T \geq n]$$

and this equals $\mathbf{E}[X_1] \cdot \mathbf{E}[T]$.

Actually, to interchange sum and expectation, we need dominated convergence. First put $|X_n|$ into the equations above to get the dominating function (a sum), and proceed. ■

WALD'S IDENTITY II. With the same hypotheses, if $\mathbf{E}[X_1] = 0$, and if $\mathbf{E}[X_1^2]$ is finite, then we have

$$\mathbf{E}[S_T^2] = \mathbf{E}[X_1^2] \cdot \mathbf{E}[T].$$

Proof. Again, convergence must be dealt with in general, but here is the basic idea. Since $S_T = \sum_{n=1}^{\infty} X_n \cdot I_{\{T \geq n\}}$, we have

$$S_T^2 = \sum_{n=1}^{\infty} \sum_{m=1}^{\infty} X_n X_m \cdot I_{\{T \geq n\}} \cdot I_{\{T \geq m\}} = \sum_{n=1}^{\infty} X_n^2 \cdot I_{\{T \geq n\}} + 2 \sum_{n=1}^{\infty} \sum_{m=n+1}^{\infty} X_n X_m \cdot I_{\{T \geq m\}}.$$

For $m > n$, X_m and X_n are independent, and so are X_m and $I_{\{T \geq m\}}$. So X_m is independent of the product $X_n \cdot I_{\{T \geq m\}}$. Therefore

$$\mathbf{E}[X_m \cdot X_n \cdot I_{\{T \geq m\}}] = \mathbf{E}[X_m] \cdot \mathbf{E}[X_n \cdot I_{\{T \geq m\}}] = 0 \cdot \mathbf{E}[X_n \cdot I_{\{T \geq m\}}] = 0.$$

Thus $\mathbf{E}[S_T^2] = \sum_{n=1}^{\infty} \mathbf{E}[X_n^2 \cdot I_{\{T \geq n\}}]$. Since each X_n is independent of $I_{\{T \geq n\}}$, it follows that each X_n^2 is independent of $I_{\{T \geq n\}}$. Hence

$$\mathbf{E}[S_T^2] = \sum_{n=1}^{\infty} \mathbf{E}[X_n^2] \cdot \mathbf{Pr}[T \geq n] = \mathbf{E}[X_1^2] \cdot \mathbf{E}[T].$$ ■

Our treatment of Wald's identities is based on the proof in Chow and Teicher [**2**, section 5.3] and other places, including Chung [**3**, section 5.5] and Durrett [**4**, section 3.1]; in the latter two books, Wald II is an exercise. All three books are graduate-level measure-theory-based texts.

Acknowledgment. We thank the anonymous referees for their many improvements to the exposition and for an additional reference.

REFERENCES

→ Joseph Bak, The anxious gambler's ruin, this MAGAZINE **74** (2001), 182–193.

2. Yuan Shih Chow and Henry Teicher, *Probability Theory: Independence, Interchangeability, Martingales*, 1978, Springer-Verlag, New York.
3. Kai Lai Chung, *A Course in Probability Theory*, 2nd ed., 1974, Academic Press, New York.
4. Richard Durrett, *Probability: Theory and Examples*, Wadsworth & Brooks/Cole, 1991. Third edition published in 2004.
5. Susanna S. Epp, *Discrete Mathematics with Applications*, 3rd ed., 2004, Thomson/Brooks-Cole.
6. William Feller, *An Introduction to Probability Theory and its Applications*, Volume 1, 3rd ed., 1968, John Wiley & Sons, Inc., New York.

→ Robert I. Jewett and Kenneth A. Ross, Random walks on $\mathbb{Z}$, *Coll. Math. J.* **19** (1988), 330–342.

8. Kenneth H. Rosen, *Discrete Mathematics and its Applications*, 4th ed., 1999, WCB McGraw-Hill, Boston.
9. Ken Ross, *A Mathematician at the Ballpark: Odds and Probabilities for Baseball Fans*, 2004, Pi Press, Inc.
10. Kenneth A. Ross and Charles R. B. Wright, *Discrete Mathematics*, 5th ed., 2003, Prentice-Hall, Upper Saddle River, NJ.
11. Lajos Takács, On classical ruin problems, *J. Amer. Statist. Assoc.* **64** (1969), 889–906.

Arthur Cayley and the Abstract Group Concept

SUJOY CHAKRABORTY
Shah Jalal University of Science and Technology
Sylhet-3114, Bangladesh
sujoy_chbty@yahoo.com

MUNIBUR RAHMAN CHOWDHURY
University of Dhaka
Dhaka-1000, Bangladesh

In this article, we examine in considerable detail Cayley's first three papers on abstract group theory (1854–59), with special reference to Cayley's formulation of the abstract group concept. We show convincingly that—as far as finite groups are concerned—Cayley's definition was complete and unequivocal, in contrast to opinion expressed by some other writers. These early papers on abstract group theory [**4, 5, 6**] seem to have been completely neglected and swept away by the burgeoning subject of permutation groups. The abstract group concept resurfaced in the work of Kronecker in 1870.

Arthur Cayley (1821–1895) graduated from Cambridge in 1842 as Senior Wrangler and was awarded the prestigious First Smith's Prize. He then served as Fellow and Tutor of Trinity College (Cambridge) for three years. Since there was no prospect of a permanent academic position, he left for London and entered Lincoln's Inn to qualify for the legal profession. He was called to the Bar in 1849 and he practiced in London as a barrister for the next fourteen years until his appointment as the first incumbent of the Sadleirian Professorship of Pure Mathematics at the University of Cambridge. Even during the years of his legal practice, Cayley published a very large number of research papers in diverse areas of mathematics.

Cayley's work spreads over a very wide range of topics, predominantly in the broad fields of algebra and geometry. He was one of the creators of the theory of algebraic invariants. This elaborate edifice, now almost completely forgotten, reigned supreme during the last quarter of the 19th century, and was the "modern higher algebra" of the day. His *Collected Mathematical Papers* were published by Cambridge University Press in thirteen volumes from 1889 to 1897 and contain 966 items ranging from very short notes to lengthy memoirs.

Prelude: Cayley on November 2, 1853

On November 2, 1853 Cayley dashed off two manuscripts to the *Philosophical Magazine*; one was published before the year was out, while the other appeared in the first issue of the *Magazine* in 1854. The first of these is called, "On a property of the caustic by refraction of the circle" [**3**]. We contend that the work on this paper served Cayley as the inspiration to generalize the group concept. Therefore we discuss its content in some detail.

A thorough exposition of caustics would lead us far beyond our scope. We provide only a general description, referring the reader to papers by Bruce, Giblin, and Gibson [**1**] or Loe and Beagley [**13**]. A *caustic* is a curve that is always tangent to rays of light that proceed from a point to be reflected (or refracted) at a given surface. Readers familiar with envelopes will recognize this description of a caustic as the envelope of the reflected (or refracted) rays. One common way to compute caustics was to use an intermediate curve, the *secondary caustic* or *orthotomic* curve, which consists of the

reflections of the source point across all lines tangent to the reflecting surface. The caustic is the evolute of the secondary caustic.

The paper under discussion was not the first time that Cayley was writing on caustics. Six years earlier, Cayley had published an alternative derivation of the equation of the caustic resulting from reflection at a circle (meaning: across a circular surface) [**2**], a result first given by St. Laurent in 1826. The paper [**3**] also draws on a subsequent paper of St. Laurent, who showed that "in certain cases the caustic by refraction of a circle is identical with the caustic of reflexion of a circle (the reflecting circle and radiant point being, of course, properly chosen)." Cayley proposes

> to demonstrate the more general theorem, that the same caustic by refraction of a circle may be considered as arising from *six* different systems of a radiant point, circle, and index of refraction. The demonstration is obtained by means of the secondary caustic, which is (as is well known) an oval of Descartes. Such oval has three foci, any one of which may be taken for the radiant point: whichever be selected, there can always be found two corresponding circles and indices of refraction. [**3**]

Cayley derives the equation of the secondary caustic, which contains three parameters: the abscissa ξ of the radiant point, the radius c of the refracting circle, and the index μ of refraction, and puts it in several equivalent forms of which one is as follows:

$$c\left(\mu-\frac{1}{\mu}\right)\sqrt{\left(x-\frac{c^2}{\xi}\right)^2+y^2}+\left(-\xi+\frac{c^2}{\xi}\right)\sqrt{\left(x-\frac{\xi}{\mu^2}\right)^2+y^2}$$
$$+\left(\frac{\xi}{\mu}-\frac{c^2\mu}{\xi}\right)\sqrt{(x-\xi)^2+y^2}=0. \quad [\mathbf{3}, \text{p. } 120]$$

FIGURE 1 shows this locus, using particular values of the parameters.

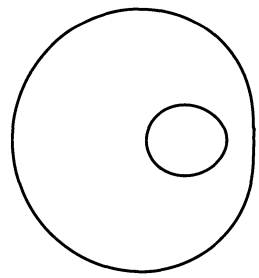


Figure 1 Cayley's secondary caustic, with $\xi = 1/3$, $c = 1/2$, $\mu = 2$

Cayley observes that if

> we write successively,

$$\xi'=\xi, \qquad c'=c, \qquad \mu'=\mu, \tag{1}$$
$$\xi'=\frac{c^2}{\xi}, \qquad c'=\frac{c}{\mu}, \qquad \mu'=\frac{c}{\xi}, \tag{α}$$
$$\xi'=\frac{\xi}{\mu^2}, \qquad c'=\frac{c}{\mu}, \qquad \mu'=\frac{1}{\mu}, \tag{β}$$
$$\xi'=\xi, \qquad c'=\frac{\xi}{\mu}, \qquad \mu'=\frac{\xi}{c}, \tag{γ}$$

$$\xi'=\frac{c^2}{\xi}, \qquad c'=c, \qquad \mu'=\frac{c\mu}{\xi}, \tag{δ}$$

$$\xi'=\frac{\xi}{\mu^2}, \qquad c'=\frac{\xi}{\mu}, \qquad \mu'=\frac{\xi}{c\mu}, \tag{ε}$$

... then, whichever system of values of ξ', c', μ' be substituted for ξ, c, μ, we have in each case identically the same secondary caustic, the effect of the substitution being simply to interchange the different forms of the equation; and we have therefore identically the same caustic. By writing

$$(\xi', c', \mu') = \alpha(\xi, c, \mu), \&c,$$

$\alpha, \beta, \gamma, \delta, \varepsilon$ will be functional symbols, such as are treated of in my paper "On the Theory of Groups as depending on the symbolic equation $\theta^n = 1$," and it is easy to verify the equations

$$1 = \alpha\beta = \beta\alpha = \gamma^2 = \delta^2 = \varepsilon^2,$$

$$\alpha = \beta^2 = \delta\gamma = \varepsilon\delta = \gamma\varepsilon,$$

$$\beta = \alpha^2 = \varepsilon\gamma = \gamma\delta = \delta\varepsilon,$$

$$\gamma = \delta\alpha = \varepsilon\beta = \beta\delta = \alpha\varepsilon,$$

$$\delta = \varepsilon\alpha = \gamma\beta = \alpha\gamma = \beta\varepsilon,$$

$$\varepsilon = \gamma\alpha = \delta\beta = \beta\gamma = \alpha\delta. \quad [\mathbf{3}, \text{pp. } 120\text{–}121]$$

There is a difficulty here; these equations do not hold if the substitutions are named as above (for example, $\alpha^2 = \varepsilon$). But they do hold if we interchange β and ε, and γ and δ.

The paper referred to here is the second one that Cayley completed on November 2, 1853 [**4**] and the first of the three that we will analyze. In this paper, Cayley wrote on groups for the first time. (In 1849 Cayley had published in the *Philosophical Magazine* a "Note on the theory of permutations," which had, however, no connection with permutation groups or the group concept. In the 19th century, it was customary to make a distinction between substitution and permutation; the former referred to the process or operation, and the latter referred to the result or image.) Groups of substitutions had been around for some time, at least since Cauchy's numerous papers on the subject from the years 1844–46.

As composition of substitutions is associative, the above six substitutions (as renamed) form a nonabelian group of order 6. Pleasantly surprised and enormously encouraged by the unexpected appearance of a nonabelian group of order 6 in a physical context, Cayley reflected upon the group concept and realized that it was capable of far-reaching generalization. This is what Cayley set out to do in the paper [**4**]; but he went much further. To be specific, we contend that in this paper Cayley put forward the abstract group concept (albeit limited to the finite case) and consciously and purposely developed abstract group theory to a considerable extent.

Detailed analysis of Cayley's first paper

Preparation for the abstract group concept Writers on group theory, before Cayley, dealt with groups of concrete objects (mostly of permutations or, more generally, of operations). Cayley laid the groundwork for the abstract group concept by suggesting that the operations are assumed to obey the associative law, though in general, not the commutative law. Indeed, Cayley devoted considerable effort to prepare the reader for the abstract group concept by alluding to operations, in general, starting thus:

> Let θ be a symbol of operation, which may, if we please, have for its operand, not a single quantity x, but a system $(x, y, \ldots)$, so that $\theta(x, y, \ldots) = (x', y', \ldots)$, where $x', y', \ldots$ are any functions whatever of $x, y, \ldots$, it is not even necessary that $x', y', \ldots$ should be the same in number with $x, y, \ldots$. In particular x', y', &c. may represent a permutation of x, y, &c, θ is in this case what is termed a substitution. [**4**, p. 123]

He continues:

> ... the symbol 1 will naturally denote an operation which (either generally or in regard to the particular operand) leaves the operand unaltered, ... A symbol $\theta\phi$ denotes the compound operation, the performance of which is equivalent to the performance, first of the operation ϕ, and then of the operation θ; $\theta\phi$ is of course in general different from $\phi\theta$. But the symbols $\theta, \phi, \ldots$ are in general such that $\theta \,.\, \phi\chi = \theta\phi \,.\, \chi$, &c, so that $\theta\phi\chi$, $\theta\phi\chi\omega$, &c. have a definite signification independent of the particular mode of compounding the symbols; this will be the case even if the functional operations involved in the symbols θ, ϕ, &c. contain parameters such as the quaternion imaginaries i, j, k; but not if these functional operations contain parameters such as the imaginaries which enter into the theory of octaves, &c, and for which, *e.g.* $\alpha \,.\, \beta\gamma$ is something different from $\alpha\beta \,.\, \gamma$, a supposition which is altogether excluded from the present paper. [**4**, pp. 123–124]

Concerning the last sentence of this quote, it is pertinent to recall that the division ring of quaternions was discovered by Sir William Rowan Hamilton (1805–1865) in 1843, while the nonassociative division algebra of octaves (also known as Cayley numbers) was discovered by Cayley in 1845.

Cautioning the reader, "The order of the factors of a product $\theta\phi\chi \ldots$ must of course be attended to, since even in the case of a product of two factors the order is material," Cayley sums up his preparatory remarks as follows:

> ... the distributive law has no application to the symbols $\theta\phi \ldots$; and that these symbols are not in general convertible, but are associative. It is easy to see that $\theta^\circ = 1$, and that the index law $\theta^m \,.\, \theta^n = \theta^{m+n}$, holds for all positive or negative integer values, not excluding 0. It should be noticed also, that if $\theta = \phi$, then, whatever the symbols α, β may be, $\alpha\theta\beta = \alpha\phi\beta$, and conversely. [**4**, p. 124]

In olden days, $\theta^\circ = 1$ was treated as a deduction from the index law by setting m or n equal to 0. Nowadays, it is treated as an extra convention, needed to ensure validity of the index law when m or n is equal to 0. The implication $\theta = \phi \Rightarrow \alpha\theta\beta = \alpha\phi\beta$ is the requirement that the operation is well-defined. The reverse implication $\alpha\theta\beta = \alpha\phi\beta \Rightarrow \theta = \phi$ is called the (left and right) cancellation law, and is a uniquely special feature of groups.

The group concept and the group table After these preparatory remarks, Cayley immediately introduces the abstract group concept by saying:

> A set of symbols $1, \alpha, \beta, \ldots$ all of them different, and such that the product of any two of them (no matter in what order), or the product of any of them onto itself, belongs to the set, is said to be a *group*[1]. [**4**, p. 124]

(As we will explain later, the footnote explains Cayley's motivation for using the word *group*.) It is important to note that the "symbols" (elements) may be any kind of mathematical objects, not necessarily "symbols of operation" (that is, functions or mappings); Cayley is thus quite clearly speaking of a "group" in the abstract sense, a point which becomes abundantly clear when we study his classification of groups of orders 4 and 6.

The use of the term *set* here, in its precise technical sense, long before Georg Cantor (1845–1918), is noteworthy. The pivotal role of the symbol 1 as the identity element is tacitly implied, and the requirement of the associativity is not repeated as being superfluous after the introductory remarks. The very next sentence is the following:

> It follows that if the entire group is multiplied by any one of the symbols, either as further or nearer factor, the effect is simply to reproduce the group; or what is the same thing, that if the symbols of the group are multiplied together so as to form a table, thus:

		Further factors: 1	α	β	...
Nearer factors	1	1	α	β	...
	α	α	α^2	$\beta\alpha$	...
	β	β	$\alpha\beta$	β^2	...
	⋮	⋮	⋮	⋮	⋮

> that as well each line as each column of the square will contain all the symbols $1, \alpha, \beta, \ldots$. [**4**, p. 124]

The statement is insightful and informative. In modern language, each of the maps $x \to xa$ (right multiplication by a) and $x \to ax$ (left multiplication by a) is bijective. In other words, each of these maps effects a permutation of the elements of the group. We have to consider this as the earliest occurrence of what later came to be known as Cayley's Theorem: *Every group of order n is isomorphic to a group of permutations on n letters.* This is the real significance of the sentence quoted above; the introduction of the group table is merely an adjunct. Observe that nowadays the group table is usually the transpose of Cayley's group table.

The reason that the maps $x \to xa$ and $x \to ax$ are injective is the validity of the right and left cancellation law in a group. The proof of the cancellation law requires the use of the existence of inverse elements. It may seem that Cayley is not explicit about the existence of inverse elements in connection with his introduction of the abstract group concept. One might, therefore, think that Cayley's definition of a group is incomplete; someone has gone so far as to say that it is "muddled" [**11**]. The objection is not valid, because for a finite set closed under a binary operation, the existence of inverse elements follows from the associative property and the cancellation law: *Every finite cancellative semigroup is a group.*

For easy reference we include a proof of this result. Here we need not assume the existence of an identity element. It is enough to show that such a semigroup S has a left identity element e, and each $a \in S$ has a left inverse $a' \in S$ with respect to e. Choose $c \in S$ (arbitrary but fixed), the map $x \to xc$ is injective (by the right cancellation law); hence also surjective (because S is finite). So, there exists an element $e \in S$ such that $ec = c$. This e, we claim, is a left identity for S. Given any $a \in S$, the map $x \to cx$ is surjective (for similar reasons). So, there exists an element $b \in S$ such that $cb = a$. Then $ea = e(cb) = (ec)b = cb = a$. The existence of a left inverse of a with respect to e results from the surjectivity of the mapping $x \to xa$.

Further, Cayley's allusion to the index law $\theta^m \,.\, \theta^n = \theta^{m+n}$, "for all positive or negative integer values," in the preparatory remarks shows that he was fully aware that in a group, every element θ must have an inverse element θ^{-1}, because he refers expressly to negative values of m or n, and because negative integral powers of θ are defined as positive integral powers of θ^{-1}. Moreover, in a finite group, θ^{-1} is expressible as a positive integral power of θ, a fact implied by the very title of the paper ($\theta^n = 1 \Rightarrow \theta^{-1} = \theta^{n-1}$).

From Cayley's writing we cannot really be sure whether Cayley implicitly assumed the left and right cancellation laws as constituting a defining property of a (finite) group or whether he considered these laws as consequences of the (somewhat implicit but essentially complete) group axioms. In the former event, Cayley's definition of a finite group (as a cancellative semigroup) would be complete and unequivocal. In the latter event, this would still be true if our interpretation about Cayley's implicit reference to inverse elements is accepted.

The order of an element and groups of order 4 Observing that "the product of any number of the symbols, with or without repetitions, and in any order whatever, is a symbol of the group," Cayley continues:

> Suppose that the group $1, \alpha, \beta, \ldots$ contains n symbols, it may be shown that each of these symbols satisfies the equation $\theta^n = 1$; so that a group may be considered as representing a system of roots of this symbolic binomial equation. It is, moreover, easy to show that if any symbol α of the group satisfies the equation $\theta^r = 1$, where r is less than n, then that r must be a submultiple of n; it follows that when n is a prime number, the group is of necessity of the form $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, $(\alpha^n = 1)$; and the same may be (but is not necessarily) the case, when n is a composite number. [**4**, pp. 124–125]

Again, these lines are insightful and informative. First, every element of a finite group of order n satisfies the equation $a^n = e$ (to use present-day notation) and the *order* (*index* in Cayley's terminology) of every element is a divisor of n. The existence of a least positive integer r with this property follows from considering the sequence of positive integral powers of θ; r is clearly $\leq n$. That r must be a submultiple of n (meaning that n is divisible by r), when $r < n$, is a claim Cayley passes over without proof as being "easy to show"; whereas just in the preceding sentence Cayley says: "it may be shown that each of these symbols satisfies the equation $\theta^n = 1$," likewise without proof. For a nonabelian group the relation $\theta^n = 1$ is not at all obvious. One is at a loss to understand why Cayley chose to suppress the proofs.

Second, when n is prime, the only abstract group of order n is the cyclic group of that order, but this may be the case also for certain composite values of n. It is known that every group of order n is cyclic if and only if n is coprime to $\varphi(n)$, the number of natural numbers not exceeding n that are coprime to n. An inductive proof of the sufficiency part of the Theorem appeared in our paper, "When is every group of order n cyclic?" [**8**].

An abstract group of order n may, therefore, be regarded as a system of roots of the symbolic equation $\theta^n = 1$. The analogy to the system of the n (complex) roots of the equation $x^n = 1$ is immediate. Indeed, these roots constitute a cyclic group of order n, whether n is prime or composite. The analogy is, however, tenuous for it breaks down in the very simplest and first possible, case $n = 4$. Indeed, Cayley himself says, "The distinction of the theory of the symbolic equation $\theta^n = 1$, and that of the ordinary equation $x^n - 1 = 0$, presents itself in the very simplest case, $n = 4$" [**4**, p. 125]. In addition to the cyclic group of order 4, there exists a noncyclic group $1, \alpha, \beta, \gamma$ of order 4. Cayley's proof of the classification of groups of order 4 is as elegant as any to be found in present-day textbooks. For the latter group he proves

$$\alpha^2 = \beta^2 = \gamma^2 = 1, \qquad \alpha = \beta\gamma = \gamma\beta, \qquad \beta = \gamma\alpha = \alpha\gamma, \qquad \gamma = \alpha\beta = \beta\alpha;$$

"and we have thus a group essentially distinct from that of the system of roots of the ordinary equation $x^4 - 1 = 0$" [**4**, p. 126].

Cayley then mentions three concrete realizations of this abstract group. The first two are groups of transformations of elliptic functions and binary quadratic forms,

respectively, while the third example is from the then emerging theory of matrices ("a theory which indeed might have preceded the theory of determinants"). This example is especially interesting, because here the group is generated by the two operations of *inversion* and *transposition* of (invertible) matrices (of a fixed order greater than 1), whose commutativity Cayley expressly points out.

Without pausing to explain the terminology or the notation, we mention Cayley's first two examples [**4**, p. 126]: In the theory of elliptic functions, let

$$\alpha(n) = \frac{c^2}{n}, \quad \beta(n) = -\frac{c^2+n}{1+n}, \quad \text{and} \quad \gamma(n) = -\frac{c^2(1+n)}{c^2+n},$$

where n is the parameter. In the theory of the quadratic form $Q(x, y) = ax^2 + 2bxy + cy^2$, let

$$\alpha(a, b, c) = (c, b, a), \quad \beta(a, b, c) = (a, -b, c), \quad \text{and} \quad \gamma(a, b, c) = (c, -b, a).$$

Then in each case, $1, \alpha, \beta, \gamma$ form a noncyclic group of order 4. Two further examples that may be more accessible are

(i) the residue classes $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ modulo 8, under multiplication modulo 8 and

(ii) the matrices

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

under multiplication of matrices.

Groups of order 6 and the group algebra Next, Cayley embarks upon a detailed and careful analysis of all possible abstract groups of order 6, and proves—much as present-day textbooks do—that there exist two, and only two, nonisomorphic abstract groups of order 6: one is the cyclic group of order 6 and the other group may be presented in the form $1, \alpha, \alpha^2, \gamma, \alpha\gamma, \alpha^2\gamma$, where $\alpha^3 = 1$, $\gamma^2 = 1$, and $\gamma\alpha = \alpha^2\gamma$.

Cayley begins his analysis of a group of six symbols $1, \alpha, \beta, \gamma, \delta, \varepsilon$, by showing that

> ... it is impossible that *all* the roots [except 1, of the symbolic equation $\theta^6 = 1$] should have the index 2. This may be done by means of a theorem which I shall for the present assume, viz. that if among the roots of the symbolic equation $\theta^n = 1$, there are contained a system of roots of the symbolic equation $\theta^p = 1$ (or, in other words, *if among the symbols forming a group of the order n there are contained symbols forming a group of the order p), then p is a submultiple of n* [our italics]. In the particular case in question, a group of the order 4 cannot form part of the group of the order 6. [**4**, p. 127]

A group of order 6 cannot have a *cyclic* subgroup of order 4 because, as Cayley stated earlier (without proof), the order of every element divides the order of the group. Cayley proved: if every nonidentity element had order 2, then any two of them would generate the noncyclic group of order 4. This would violate the general theorem that Cayley states so clearly. Thus, Cayley has stated here, without proof, Lagrange's Theorem for abstract groups and applied it in a specific situation. Why Cayley simply assumed the theorem and omitted the proof is somewhat of a mystery.

Having proved the existence of a root (element) of index (order) 3, Cayley denotes this element by α. Then the group must have the form $1, \alpha, \alpha^2, \gamma, \alpha\gamma, \alpha^2\gamma$ (with $\alpha^3 = 1$), where γ^2 must be $1, \alpha$, or α^2. The suppositions $\gamma^2 = \alpha$ and $\gamma^2 = \alpha^2$ give a cyclic group.

It only remains, therefore, to assume $\gamma^2 = 1$; then we must have either $\gamma\alpha = \alpha\gamma$ or else $\gamma\alpha = \alpha^2\gamma$. The former assumption leads to the group $1, \alpha, \alpha^2, \gamma, \alpha\gamma, \alpha^2\gamma, (\alpha^3 = 1, \gamma^2 = 1, \gamma\alpha = \alpha\gamma)$, which is, in fact, analogous to the system of roots of the ordinary equation $x^6 - 1 = 0$; and by putting $\alpha\gamma = \lambda$, might be exhibited in the form

$$1, \lambda, \lambda^2, \lambda^3, \lambda^4, \lambda^5, \quad (\lambda^6 = 1),$$

under which this system has previously been considered. The latter assumption leads to the group $1, \alpha, \alpha^2, \gamma, \alpha\gamma, \alpha^2\gamma, (\alpha^3 = 1, \gamma^2 = 1, \gamma\alpha = \alpha^2\gamma)$, and we have thus two, and only two, essentially distinct forms of a group of six. [**4**, p. 127]

Denoting the elements by $1, \alpha, \beta, \gamma, \delta, \varepsilon$, Cayley presents the multiplication table of each group.

An instance of a group of this kind [the nonabelian group of order 6] is given by the permutations of three letters; the group $1, \alpha, \beta, \gamma, \delta, \varepsilon$ may represent a group of substitutions as follows:

$$\begin{array}{cccccc} a\,b\,c, & c\,a\,b, & b\,c\,a, & a\,c\,b, & c\,b\,a, & b\,a\,c \\ a\,b\,c & a\,b\,c & a\,b\,c & a\,b\,c & a\,b\,c & a\,b\,c. \end{array}$$

Another singular instance is given by the optical theorem proved in my paper 'On a property of the Caustic by refraction of a Circle'. [**4**, p. 129]

In our opinion, it is the discovery of this group that prompted Cayley to introduce the abstract group concept.

Cayley then hints at the construction of the group algebra of a group in these words:

... if instead of considering α, β, &c. as symbols of operation, we consider them as quantities (or, to use a more abstract term, 'cogitables') such as the quaternion imaginaries; [then] the equations expressing the existence of the group are, in fact the equations defining the meaning of the product of two complex quantities of the form $w + a\alpha + b\beta + \cdots$; [**4**, p. 129]

Thus in the case of the noncyclic group of order 6,

$$\begin{aligned} &(w + a\alpha + b\beta + c\gamma + d\delta + e\varepsilon)(w' + a'\alpha + b'\beta + c'\gamma + d'\delta + e'\varepsilon) \\ &\quad = (W + A\alpha + B\beta + C\gamma + D\delta + E\varepsilon), \end{aligned}$$

where

$$\begin{aligned} W &= ww' + ab' + a'b + cc' + dd' + ee', \\ A &= wa' + w'a + bb' + dc' + ed' + ce', \quad \text{etc.} \end{aligned}$$

"It is notable that Bartel van der Waerden (1903–1996) saw this as a significant remark and an early introduction of a 'group algebra'," says Crilly [**10**, p. 4] and refers to B. L. van der Waerden: *A History of Algebra: From Al-Khwarizmi to Emmy Noether* [**16**]. Many years were to elapse before this clear hint was taken up and group algebras were accorded the attention they deserved.

It is worth noting that neither Cayley nor any of the other 19th century writers use the word *abstract* in connection with the group concept. The appellation *abstract group* is a later development; it is used profusely in Miller's 1916 text [**14**].

The end of Cayley's first paper Cayley ends this paper by expressing the hope "shortly to resume the subject of the present paper" and concludes with two examples

of nonabelian groups of higher orders. It is impossible to determine whether these examples were constructed in an *ad hoc* manner, or whether Cayley had in his possession general examples of nonabelian groups of orders $2p^2$ and p^3 (where p is prime).

> The first of these is a group of [order] eighteen, viz.
>
> $$1, \alpha, \beta, \gamma, \alpha\beta, \beta\alpha, \alpha\gamma, \gamma\alpha, \beta\gamma, \gamma\beta, \alpha\beta\gamma, \beta\gamma\alpha, \gamma\alpha\beta, \alpha\beta\alpha, \beta\gamma\beta, \gamma\alpha\gamma, \alpha\beta\gamma\beta, \beta\gamma\beta\alpha,$$
>
> where
>
> $$\alpha^2 = 1, \quad \beta^2 = 1, \quad \gamma^2 = 1, \quad (\beta\gamma)^3 = 1, \quad (\gamma\alpha)^3 = 1, \quad (\alpha\beta)^3 = 1,$$
> $$(\alpha\beta\gamma)^2 = 1, \quad (\beta\gamma\alpha)^2 = 1, \quad (\gamma\alpha\beta)^2 = 1;$$
>
> and the other a group of [order] twenty-seven, viz.
>
> $$1, \alpha, \alpha^2, \gamma, \gamma^2, \gamma\alpha, \alpha\gamma, \gamma\alpha^2, \alpha^2\gamma, \gamma^2\alpha, \alpha\gamma^2, \gamma^2\alpha^2, \alpha^2\gamma^2, \alpha\gamma\alpha, \alpha\gamma^2\alpha, \alpha^2\gamma\alpha, \alpha^2\gamma^2\alpha,$$
> $$\alpha\gamma\alpha^2, \alpha\gamma^2\alpha^2, \alpha^2\gamma\alpha^2, \alpha^2\gamma^2\alpha^2, \gamma\alpha\gamma^2, \gamma\alpha^2\gamma^2, \gamma^2\alpha\gamma, \gamma^2\alpha^2\gamma, \gamma^2\alpha\gamma\alpha^2, \gamma\alpha\gamma^2\alpha^2,$$
>
> where
>
> $$\alpha^3 = 1, \quad \gamma^3 = 1, \quad (\gamma\alpha)^3 = 1, \quad (\gamma^2\alpha)^3 = 1, \quad (\gamma\alpha^2)^3 = 1, \quad (\gamma^2\alpha^2)^3 = 1.$$
>
> It is hardly necessary to remark, that each of these groups is in reality perfectly symmetric, the omitted terms being, in virtue of the equations defining the nature of the symbols, identical with some of the terms of the group. Thus, in the group of [order] 18, the equations $\alpha^2 = 1$, $\beta^2 = 1$, $\gamma^2 = 1$, $(\alpha\beta\gamma)^2 = 1$ give $\alpha\beta\gamma = \gamma\beta\alpha$, and similarly for all the other omitted terms. It is easy to see that in the group of [order] 18 the index of each term is 2 or 3, while in the group of [order] 27 the index of each term is 3. [**4**, p. 130]

Cayley's motivation for the abstract group concept It is our contention that Cayley's unexpected discovery of a nonabelian group of order 6 in the practical context of geometrical optics, served as the trigger for generalizing the group concept. The crucial point was Cayley's discovery of the six transformations that leave the equation of the secondary caustic unchanged, and his realization that these transformations form a group under the composition of mappings. One may wonder how Cayley noticed that. For one who had discovered the nonassociative algebra of octaves (Cayley numbers) very soon after the discovery (1843) of the division ring of quaternions by Sir William Rowan Hamilton and had worked on invariants, it would have been natural for Cayley to ask himself the question: What, if any, transformation of variables leaves the equation unchanged?

As we mentioned, Cayley's first paper on group theory has a single footnote, marked "1," next to his first usage of the term *group*:

> The idea of a group as applied to permutations or substitutions is due to Galois, and the introduction of it may be considered as marking an epoch in the progress of the theory of algebraic equations. [**4**, p. 124]

There is no other footnote or any reference to any other writer in the entire series of papers [**4, 5, 6**]. So, clearly permutation groups served Cayley as a prime motivating example. After classifying the groups of order 4 and before moving on to three concrete examples of the noncyclic group of order 4, Cayley makes the following observation:

> Systems of this form are of frequent occurrence in analysis, and it is only on account of their extreme simplicity that they have not been expressly remarked. [**4**, p. 126]

After classifying the groups of order 6, Cayley gives two examples of the nonabelian groups of order 6.

Noting that all five of these examples are groups of transformations (including one where the transformations are mappings defined on the set of all invertible matrices of a given order), there is no question that finite transformation groups were for Cayley an equally important motivation for the abstract group concept. Indeed, we are inclined to believe that as far as Cayley was concerned, permutation groups played only a reinforcing role as one instance of the diverse types of concrete examples that are subsumed under a common umbrella by the new concept.

Cayley felt so enthusiastic about the abstract group concept that, as early as 1860, he included it among "Recent Terminology in Mathematics, *The English Encyclopedia*" [**7**], a collection of terms mostly from the then-emerging theory of invariants. The entry *Group* covers almost an entire page and is a brief summary of the first several sections of Cayley's paper [**4**]. Thus there is clear, though indirect, evidence that the theory of invariants—largely a creation of Cayley's—played an important role in shaping the abstract group concept.

Cayley's second paper on group theory

In Cayley's second paper on group theory [**5**], published soon after the first (but in contrast bearing no date), Cayley introduces the concept of normal subgroup of a group (due to Galois) in a somewhat curious manner by calling a normal subgroup of a group a *submultiple* of the group, whereas its cosets are called (by him) *symmetrical holders.*

Through his study of *symmetrical holders*, Cayley arrives at some important results that, possibly because they were couched in somewhat obscure terms, have so far escaped attention. For one, Cayley shows that the nonabelian group of order 6 has a unique nontrivial normal subgroup (of order 3). For another, he shows (without using the terminology) that the only other abstract group (the cyclic group) of order 6 is the (internal) direct product of two subgroups of orders 3 and 2. To substantiate our interpretation we quote Cayley in full:

> the group of six $1, \alpha, \alpha^2, \gamma, \gamma\alpha, \gamma\alpha^2$, $(\alpha^3 = 1, \gamma^2 = 1, \alpha\gamma = \gamma\alpha)$, is a multiple of the group of three, $1, \alpha, \alpha^2$ (in fact, $1, \alpha, \alpha^2$ and $\gamma, \gamma\alpha, \gamma\alpha^2$ are each of them a symmetrical holder of the group $1, \alpha, \alpha^2$); and so in like manner the group of six is a multiple of the group of two, $1, \gamma$ (in fact, $1, \gamma$ and $\alpha, \alpha\gamma$ and $\alpha^2, \alpha^2\gamma$ are each a symmetrical holder of the group $1, \gamma$). There would not, in a case such as the one in question, be any harm in speaking of the group of six as the product of the two groups $1, \alpha, \alpha^2$ and $1, \gamma$, but upon the whole it is, I think, better to dispense with the expression.
>
> Considering, secondly, the other form of a group of six, viz. $1, \alpha, \alpha^2, \gamma, \gamma\alpha, \gamma\alpha^2$, $(\alpha^3 = 1, \gamma^2 = 1, \alpha\gamma = \gamma\alpha^2)$; here the group of six is a multiple of the group of three, $1, \alpha, \alpha^2$ (in fact, as before, $1, \alpha, \alpha^2$ and $\gamma, \gamma\alpha, \gamma\alpha^2$, are each a symmetrical holder of the group $1, \alpha, \alpha^2$, since, as regards $\gamma, \gamma\alpha, \gamma\alpha^2$, we have $(\gamma, \gamma\alpha, \gamma\alpha^2) = \gamma(1, \alpha, \alpha^2) = (1, \alpha^2, \alpha)\gamma$). But the group of six is not a multiple of any group of two whatever; in fact, besides the group $1, \gamma$ itself, there is not any symmetrical holder of this group $1, \gamma$; and so in like manner, with respect to the other groups of two, $1, \gamma\alpha$, and $1, \gamma\alpha^2$. The group of three, $1, \alpha, \alpha^2$, is therefore, in the present case, the only submultiple of the group of six. [**5**, p. 132]

It is a pity that having arrived at an example of the (internal) direct product of two subgroups, Cayley seems to have preferred not to follow up the idea behind it.

Cayley's third paper on group theory

Cayley's third paper on group theory [**6**] is clearly the sequel to the first. Without preamble Cayley begins:

> The following is, I believe, a complete enumeration of the groups of [order] 8:
>
> **I.** $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7$ $(\alpha^8 = 1)$.
>
> **II.** $1, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3$ $(\alpha^4 = 1, \beta^2 = 1, \alpha\beta = \beta\alpha)$.
>
> **III.** $1, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3$ $(\alpha^4 = 1, \beta^2 = 1, \alpha\beta = \beta\alpha^3)$.
>
> **IV.** $1, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3$ $(\alpha^4 = 1, \beta^2 = \alpha^2, \alpha\beta = \beta\alpha^3)$.
>
> **V.** $1, \alpha, \beta, \beta\alpha, \gamma, \gamma\alpha, \gamma\beta, \gamma\beta\alpha$ $(\alpha^2 = 1, \beta^2 = 1, \gamma^2 = 1, \alpha\beta = \beta\alpha, \alpha\gamma = \gamma\alpha, \beta\gamma = \gamma\beta)$.
>
> That the groups are really distinct is perhaps most readily seen by writing down the indices [orders] of the different terms of each group; these are
>
> **I.** 1, 8, 4, 8, 2, 8, 4, 8.
> **II.** 1, 4, 2, 4, 2, 4, 2, 4.
> **III.** 1, 4, 2, 4, 2, 2, 2, 2.
> **IV.** 1, 4, 2, 4, 4, 4, 4, 4.
> **V.** 1, 2, 2, 2, 2, 2, 2, 2. [**6**, p. 88]

This enumeration is, as we know, correct and complete. However, Cayley does not embark upon a proof of his claim. One point is implicit here: two groups of the same order whose numbers of elements of each (possible) order do not all coincide, must be "really distinct" (in modern terms, nonisomorphic).

Cayley next considers the question, "Why there is no group where the symbols α, β are such that $\alpha^4 = 1$, $\beta^2 = \alpha^2$, $\alpha\beta = \beta\alpha$."

> A group which presents itself for consideration is $1, \alpha, \alpha^2, \alpha^3, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3$ $(\alpha^4 = 1, \beta^2 = \alpha^2, \alpha\beta = \beta\alpha)$ but the indices of the different terms of this group are 1, 4, 2, 4, 4, 2, 4, 2, and if we write $\beta\alpha^2 = \gamma$, then we find $\gamma^2 = \beta\alpha\beta\alpha = \beta\beta\alpha\alpha = \alpha^4 = 1$, $\alpha\gamma = \alpha\beta\alpha = \beta\alpha\alpha = \gamma\alpha$; and the group is $1, \alpha, \alpha^2, \alpha^3, \gamma, \gamma\alpha, \gamma\alpha^2, \gamma\alpha^3$ $(\alpha^4 = 1, \gamma^2 = 1, \alpha\gamma = \gamma\alpha)$, which is the group II. [**6**, pp. 88–89]

This is a further confirmation that Cayley was aware of the idea of isomorphism of groups.

The group IV (in Cayley's enumeration) is the *Quaternion group* and Cayley discusses it in detail. "The group IV is a remarkable one; ... the nature of the group in question will be better understood by presenting it under a different form," says Cayley, and continues:

> In fact, if we write $\beta\alpha^3 = \gamma$, $\alpha^2 = \beta^2 = \theta$, then we find $\alpha^3 = \theta\alpha$, $\beta\alpha^2 = \theta\beta$ and $\beta\alpha = \theta\gamma$, and the group will be $1, \alpha, \beta, \gamma, \theta, \theta\alpha, \theta\beta, \theta\gamma$, where the laws of combination are
>
> $$\theta^2 = 1, \quad \alpha^2 = \beta^2 = \gamma^2 = \theta, \quad \beta\gamma = \alpha, \quad \gamma\alpha = \beta, \quad \alpha\beta = \gamma,$$
>
> $$\gamma\beta = \alpha\theta = \theta\alpha, \quad \alpha\gamma = \beta\theta = \theta\beta, \quad \beta\alpha = \gamma\theta = \theta\gamma.$$
>
> Observe that θ is a symbol of operation such that $\theta^2 = 1$, and that θ is convertible with each of the other symbols α, β, γ. It will be not so much a restrictive assumption in regard to θ, as a definition of -1 considered as a symbol of operation if we write $\theta = -1$; the group thus becomes
>
> $$1, \alpha, \beta, \gamma, -1, -\alpha, -\beta, -\gamma,$$

where

$$\alpha^2 = \beta^2 = \gamma^2 = -1, \quad \alpha = \beta\gamma = -\gamma\beta, \quad \beta = \gamma\alpha = -\alpha\gamma, \quad \gamma = \alpha\beta = -\beta\alpha.$$

Hence α, β, γ combine according to the laws of quaternion symbols i, j, k; and it is the only point of view from which the question is here considered which obliges us to consider the symbols as belonging to a group of 8, instead of (as in the theory of quaternions) a group of 4. [**6**, p. 89]

By presenting the group IV in the alternative form, Cayley makes it clear that the *quaternion group* $\{\pm 1, \pm i, \pm j, \pm k\}$ is a concrete realization of this group. As Crilly [**10**] says, "This is Cayley's really strong point: his ability to see connections." The last part of the quote points to the fact that the group of four quaternion units $\{1, i, j, k\}$ is not a group in the technical sense.

Cayley then investigates the conditions under which the mn symbols $\alpha^p \beta^q$ (where p has the values $0, 1, 2, \ldots, m-1$ and q has the values $0, 1, 2, \ldots, n-1$) may form a group for which $\alpha^m = 1$, $\beta^n = 1$, $\alpha\beta = \beta\alpha^s$, where s is a positive integer to be determined.

...then we find $\alpha^u \beta^v = \beta^v \alpha^{us^v}$; and therefore if $v = n$, $\alpha^u = \alpha^{us^n}$ or $\alpha^{u(s^n-1)} = 1$, whence $u(s^n - 1) \equiv 0 \pmod{m}$; or since u is arbitrary, $s^n - 1 \equiv 0 \pmod{m}$, an equation which, if m, n are given, determines the admissible values of s; thus, for example, if $n = 2$, and m is a prime number, then $s = 1$ or $s = m - 1$. The equation $\alpha^u \beta^v = \beta^v \alpha^{us^v}$ shows that any combination whatever of the symbols α, β can be expressed in the form $\beta^q \alpha^p$ (or, if we please, in the form $\alpha^p \beta^q$). [**6**, pp. 89–90]

Cayley then carefully shows "that the assumed law is consistent with the associative law, viz. that the expression $\beta^b \alpha^a \cdot \beta^d \alpha^c \cdot \beta^f \alpha^e$ can be transformed in one way only into the form $\beta^q \alpha^p$" [**6**, p. 90]. Indeed, either manner of forming the above product leads to the result $\beta^{b+d+f} \alpha^{as^{d+f}+cs^f+e}$; so that the associative law is satisfied.

Thus, $s^n \equiv 1 \pmod{m}$ is a necessary condition for the mn symbols $\alpha^p \beta^q$ (or $\beta^q \alpha^p$), where p has the values $0, 1, 2, \ldots, m-1$ and q has the values $0, 1, 2, \ldots, n-1$, to form a group.

In particular, as already noticed, if $n = 2$, and m is [an odd] prime, then either $s = 1$ or $s = m - 1$; the two groups so obtained are essentially distinct from each other. If $n = 2$, but m is not prime, then s has in general more than two values: thus for $m = 12$, $s^2 \equiv 1 \pmod{12}$, which is satisfied by $s = 1, 5, 7$ and 11; the group corresponding to $s = 1$ is distinct from that for any other value of s, but I have not ascertained whether the values other than unity do, or do not, give groups distinct from each other. [**6**, p. 90]

Cayley has thus constructed here the abstract dihedral group of order $2m$. As an example, he writes down the elements of the dihedral group of order 10 as follows:

$$1, \alpha, \alpha^2, \alpha^3, \alpha^4, \beta, \beta\alpha, \beta\alpha^2, \beta\alpha^3, \beta\alpha^4, \quad \text{where} \quad \alpha^5 = 1, \quad \beta^2 = 1, \quad \alpha\beta = \beta\alpha^4;$$

and observes that the indices (orders) of these elements are, respectively, 1, 5, 5, 5, 5, 2, 2, 2, 2, 2; and says:

The group is here expressed by means of the symbols α, β, having the indices 5 and 2 respectively, but it may be expressed by means of two symbols having each of them the index 2. Thus putting $\beta\alpha = \gamma$, we find $\beta^2 = 1$, $\gamma^2 = 1$, $(\beta\gamma)^5 = 1$, which is equivalent to $(\gamma\beta)^5 = 1$, and the group may be represented in the form

$$1, \beta, \gamma, \beta\gamma, \gamma\beta, \beta\gamma\beta, \gamma\beta\gamma, \beta\gamma\beta\gamma, \gamma\beta\gamma\beta, \beta\gamma\beta\gamma = \gamma\beta\gamma\beta\gamma,$$

the equality of the last two symbols being an obvious consequence of the equation $(\beta\gamma)^5 = 1$. It is clear that for any even number $2p$ whatever, there is always a group which can be expressed in this form. [**6**, p. 91]

Concluding remarks

Cayley's early papers on group theory apparently had very little influence on his contemporaries. Even modern writers seem reluctant to give Cayley his due in the creation of the abstract group theory. Thus J. Nicholson [**15**] states that the process of abstraction of group theory "took place mainly during the period 1870–1890 and was carried out almost exclusively by German mathematicians," and is completely silent on Cayley's seminal contribution. On the other hand, Crilly [**10**, p. 3] says: "he [Cayley] was far from the modern abstract definition of a group in which symbols are defined by their obedience to stated axioms." We trust that we have been able to dispel such a misconception. Cayley had indeed defined a group as "a set of symbols" (of any nature, an epithet which he did not feel necessary to add) obeying certain axioms, stated or implied. His classification of groups of small orders leaves no doubt that he was fully aware of the abstract group concept.

Both Wussing and Kleiner clearly recognize Cayley's contribution in this respect.

> Cayley published *two* [our italics] papers [140, 141] [[**4**] and [**5**] in our list], "On the Theory of Groups as depending on the Symbolic Equation $\theta^n = 1$," in which he presented a remarkable conception of groups. At a time when the Galois theory of equations had just began to be known, and when the only explicit groups under study were permutation groups, Cayley recognized the generalizability of the group concept as well as the implicitly group-theoretic nature of many contemporary ideas. [**17**, p. 230]
>
> Cayley's orientation towards an abstract view of groups—a remarkable accomplishment at this time of the evolution of group theory—was due, at least in part, to his contact with the abstract work of G. Boole. The concern with the abstract foundations of mathematics was characteristic of the circles around Boole, Cayley, and Sylvester already in 1840s. Cayley's achievement was, however, only a personal triumph. His abstract definition of a group attracted no attention at the time, even though Cayley was already well known. The mathematical community was apparently not ready for such abstraction: permutation groups were the only groups under serious investigation, and more generally, the formal approach to mathematics was still in its infancy. [**12**, p. 209]

Textbooks also for the most part ignore Cayley's contributions to group theory, except for mentioning "Cayley's Theorem." The fact that Cayley had, in his first paper (1854) on group theory, completely classified abstract groups of orders up to 6, and extended this classification (correctly) to groups of order 8 (by 1859), is never even mentioned in connection with groups of small orders. F. Chowdhury [**9**] rightly observes:

> While the fact that every abstract group is realizable as a group of permutations (something which Cayley mentioned in passing) has been codified into (and glorified as) Cayley's theorem, the fact that (at the same time, 1854) Cayley had classified all abstract groups of orders up to 6, seems to have fallen into complete oblivion. [p. 21]

Even more curious is the fact that the (abstract) noncyclic group of order 4 is named after Felix Klein (Klein's *Vierergruppe*). Klein was a boy of five when Cayley's first paper appeared. G. A. Miller [**14**, p. 65, Footnote] mentions as many as eight names—with precise references for their occurrence—for this group, but none of them is associated with Cayley. These observations further substantiate our contention that Cayley's

early papers on group theory were ignored by his contemporaries and were all but forgotten when abstract group theory came to be studied by other mathematicians.

The fact that the *Philosophical Magazine* was primarily a journal of science was no doubt partially responsible for Cayley's papers on group theory going unnoticed by mathematicians. Perhaps, Cayley's choice of the title of the first paper we discussed did little to attract attention to it. "The General Theory of Groups" would have been a more appropriate and attractive title. Or perhaps, the whole topic "may have been *too* new" [T. Crilly, personal communication]. At any rate, Cayley's early work in abstract group theory was a remarkable accomplishment for its time.

REFERENCES

1. J. W. Bruce, P. J. Giblin, and C. G. Gibson, On caustics of plane curves, *Amer. Math. Monthly* **88**:9 (Nov. 1981), 651–667.
2. Arthur Cayley, On the caustic by reflection at a circle, *Camb. Dubl. Math. J.* **2** (1847), 128–130, reprinted in Collected Papers 42, vol. 1, 273–275.
3. ———, On a property of the caustic by refraction of the circle, *Phil. Mag.* **6** (1853), 427–431, reprinted in Collected Papers 124, vol. 2, 118–122. Dated: Nov. 2, 1853.
4. ———, On the theory of groups, as depending on the symbolic equation $\theta^n = 1$, *Phil. Mag.* **7** (1854), 40–47, reprinted in Collected Papers 125, vol. 2, 123–130. Dated: Nov. 2, 1853.
5. ———, On the theory of groups, as depending on the symbolic equation $\theta^n = 1$.—Second Part, *Phil. Mag.* **7** (1854), 408–409, reprinted in Collected Papers 126, vol. 2, 131–132.
6. ———, On the theory of groups, as depending on the symbolic equation $\theta^n = 1$.—Third Part, *Phil. Mag.* **18** (1859), 34–37, reprinted in Collected Papers 243, vol. 3, 88–91. Dated: June 9, 1859.
7. ———, Recent terminology in mathematics, *The English Encyclopedia* **5** (1860), 534–542, reprinted in Collected Papers 299, vol. 3, 594–602.
8. S. Chakraborty and M. R. Chowdhury, When is every group of order n cyclic?, *GANIT J. Bangladesh Math. Soc.* **20** (2000), 97–106.
9. F. Chowdhury, Arthur Cayley and the theory of groups, *J. Math. & Math. Sci.* **10** (1995), 21–31.
10. T. Crilly, The appearance of set operators in Cayley's group theory, *Newsl. S. Afr. Math. Soc.* **31**:2 (2000), 9–22 (Our page references are to the electronic copy of the manuscript received from the author).
11. J. J. Gray, Arthur Cayley (1821–1895), *Math. Intelligencer* **17**:4 (1995), 62–63.
12. Israel Kleiner, The evolution of group theory: a brief survey, this MAGAZINE **59** (1986), 195–215.
13. Brian J. Loe and Nathaniel Beagley, The coffee cup caustic for calculus students, *Coll. Math. J.* **28**:4 (1997), 277–284.
14. G. A. Miller, Substitution and abstract groups, in *G. A. Miller, H. F. Blichfeldt and L. E. Dickson, Theory and Applications of Finite Groups*, J. Wiley, 1916, pp. 1–192.
15. J. Nicholson, The development and understanding of the concept of the quotient group, *Historia Math.* **20** (1993), 68–88.
16. B. L. van der Waerden, *A History of Algebra: From Al-Kwarizmi to Emmy Noether*, Springer-Verlag, 1985.
17. H. Wussing (trans. A. Shenitzer), *The Genesis of the Abstract Group Concept*, MIT Press, Cambridge, Mass, 1984, p. 331.

Continued from Page 333

Response from Maureen T. Carroll and Steven T. Dougherty We are thrilled to receive the Merten M. Hasse Prize. It is a great honor to be recognized by the MAA for our exposition. As professors, we have dedicated ourselves to guiding students in the path of mathematical discovery. In the paper, out hope was to make interesting results from finite geometry, combinatorics, and game theory accessible to students through the use of our game. We are especially proud to be honored by an organization that dedicates itself to beautiful mathematics, excellence in teaching, and student involvement. In addition to thanking the University of Scranton for its support, we must also thank our students. Not only did they help inspire the idea of the game, they also keep the spirit alive by competing in our annual tic-tac-toe contest.

Dirichlet: His Life, His Principle, and His Problem

PAMELA GORKIN
Bucknell University
Lewisburg, PA 17837
pgorkin@bucknell.edu

JOSHUA H. SMITH
Department of Mechanical and Aerospace Engineering
University of Virginia
Charlottesville, VA 22904-4746
josh@virginia.edu

In Joseph Fourier's book, *Théorie analytique de la chaleur* (Analytic Theory of Heat), published in 1822, Fourier studies heat conduction. In his model, temperature is a function of time t and position on a bounded domain, so at a point (x, y, z) of the domain, the function u may be written $u(t, x, y, z)$. This function satisfies the heat equation:

$$\frac{1}{c^2}\frac{\partial u}{\partial t} = \frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2},$$

where c is a positive constant. As time passes things might stabilize, entering a state of equilibrium. This means that the function u would be independent of t, implying that $\partial u/\partial t = 0$ and therefore the object on the right (which is called the Laplacian of u and denoted Δu) must vanish. We might wish to find the equilibrium temperature in the domain when the temperature on the boundary is independent of time. In this context, we are asking for a solution to something now known as the Dirichlet problem, which is also connected to problems in electrostatics and elasticity theory. (Gårding [**17**] provides a more detailed explanation of this connection.)

Informally, the Dirichlet problem asks whether, given a bounded domain and a continuous function f on the boundary of that domain, we can find a function u, continuous on the domain together with its boundary, for which $\Delta u = 0$ throughout the domain and $u = f$ on the boundary of the domain.

As we shall see, Dirichlet used a technique that came to be known as the "Dirichlet principle" to solve this problem. This principle, which was justified by physical arguments, asserts that among all functions (satisfying certain smoothness conditions) with the correct boundary values, there is one particular solution for which the integral of the square of the norm of the gradient is minimal. Other mathematicians used this principle as well. Though the principle was useful and influential, there was a difficulty with it—an objection raised by Karl Weierstrass (1815–1897), who pointed out that no one had proved this useful principle. Following Weierstrass's criticism, some mathematicians tried to solve Dirichlet's problem without the principle and others tried to save the (quite useful) principle. In Kline's words [**24**, p. 704],

> The history of the Dirichlet principle is remarkable. Green, Dirichlet, Thomson, and others of their time regarded it as a completely sound method and used it freely. Then Riemann in his complex function theory showed it to be extraordinarily instrumental in leading to major results. All of these men were aware that the fundamental existence question was not settled, even before Weierstrass an-

> nounced his critique in 1870, which discredited the method for several decades. The principle was then rescued by Hilbert and was used and extended in this [the 20th] century. Had the progress made with the use of the principle awaited Hilbert's work, a large segment of nineteenth-century work on potential theory and function theory would have been lost.

In this paper, we look at Dirichlet's problem and principle. We shall explain Dirichlet's solution as well as Weierstrass's criticism. Having done so, we then turn to our own solution of a very special Dirichlet problem: the case in which the domain is the open unit disk, the boundary is the unit circle, and the continuous function on the boundary is a rational function. Finally, we exhibit an algorithm that produces exact solutions to this famous problem for the special case of rational functions on the unit disk. This solution is surprisingly easy to understand and implement. It was part of the second author's undergraduate honors thesis at Bucknell University [**40**].

The Dirichlet problem is ideal for early study, not only because of its widespread interest and applicability in many areas of mathematics, physics, and engineering, but also because of its rich history. Yet students rarely see it early in their studies. More often, they first solve the Dirichlet problem in an advanced course that requires a strong background in analysis (such solutions on the ball or disk can be found in several texts, [**4**, p. 12] or [**32**, p. 227], though it should be mentioned that Palka's book [**32**] contains an elementary solution when the data is a polynomial). Some students might not even see it until they take a course in functional analysis [**44**, p. 199 or p. 254]. It is our hope that our simple solution will be accessible to students at a much earlier stage.

Dirichlet

We briefly describe Dirichlet and many of the people who were to play a key role in developing the solution of the problem. In order to gain a more complete picture of Dirichlet's life than what we provide, the reader may consult various sources [**9, 18, 27, 25, 34, 36, 37, 39**]. Much of the material in Koch's work [**26**, p. 174] has been translated into English [**8**]. In addition, the web site http://www-gap.dcs.st-and.ac.uk/~history/ is easily accessible and quite informative. Each of these articles provides a different point of view, and all are well worth reading. We turn now to Dirichlet's life.

Peter Gustav Lejeune Dirichlet was born on February 13, 1805 in Düren, between Aachen and Cologne. His father was a postmaster and his grandfather hailed from the Belgian town of Richelet (hence the name "Le jeune de Richelet"). In 1817, he went to gymnasium in Bonn and two years later in Cologne, where he was taught by the not-yet-famous Georg Simon Ohm.

At this time, Paris was a hub of mathematical activity; Fourier and Poisson were just two of the many brilliant mathematicians living there. Fourier (1768–1830), motivated by physical concerns, was interested in the flow of heat. In 1822, Fourier published what was to become a mathematical classic on the subject of heat, *Théorie analytique de la chaleur*. Following Fourier, from about 1815 on, Poisson (1781–1840) also worked on heat conduction problems. This active mathematical environment was what attracted Dirichlet when he went to study in Paris in 1822. Fourier's ideas would strongly influence Dirichlet's later work in mathematical physics and trigonometric series.

Dirichlet attended lectures at the *Collège de France* and the *Faculté des Sciences*. Most sources refer to his study of Gauss's *Disquisitiones arithmeticae*, which he not only read carefully and understood, but also simplified. As Kline points out [**24**, p. 829], "Dirichlet's great work, *Vorlesungen über Zahlentheorie*, expounded Gauss's

Disquisitiones and gave his own contributions." Dirichlet's simplification and clarity of thought, which was to characterize his work, also served the purpose of making Gauss's work accessible to others.

In 1823, the well-educated General Foy, leader of the opposition in the Chamber of Deputies, began looking for someone to teach his children, primarily German language and literature. Dirichlet was recommended and, making a fine impression on the General, he was hired. Dirichlet was pleased with the position for it enabled him to earn money while leaving him enough time for mathematics [**27**].

Dirichlet's first paper, *Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré*, won recognition from Fourier and Alexander von Humboldt. In 1827, through von Humboldt, Dirichlet secured a position at the University of Breslau, after being awarded his doctorate (*honoris causa*, or honorary doctorate) from the University of Bonn. This degree, which would enable Dirichlet to advance through the system, was awarded on January 18, 1827. (Though some literature [**1**] cites Cologne as the institution awarding Dirichlet this degree, the University of Cologne, founded in 1388, was closed down by the French occupation troops in 1798, and did not reopen until after the First World War [**3**].) Dirichlet's salary at this time was 400 thalers, which was about half of the amount sought by von Humboldt.

At the University of Breslau, to obtain the title of *Privatdozent* (which would enable him to lecture at the university) Dirichlet was required to give a *Probevorlesung* or lecture, write his *Habilitation* (a post Ph.D. thesis), and present it in Latin. He did give his lecture (on the irrationality of the number π) and, because the university needed him to teach, they allowed Dirichlet to complete his *Habilitation* later. Dirichlet was not terribly successful teaching in Breslau and, though he was thought of as a well-educated and pleasant young man, students found his teaching style unusual [**27**]. Since Dirichlet never talked about himself or his accomplishments and since this was just the beginning of his career, his reputation was not widely known among the students. Dirichlet published two works while in Breslau, the second of which was written in Latin. In 1828, Dirichlet was promoted to *ausserordentlicher Professor*, or senior lecturer (much like our associate professor) in Breslau, but his salary remained at 400 thalers.

In 1828, he took a position at the *Allgemeine Kriegsschule* (General Military School) in Berlin. According to Kummer [**27**], Dirichlet felt comfortable teaching in this environment, due in part to the years he had spent with General Foy. While he continued teaching at the *Kriegsschule*, he also taught at the University of Berlin. In 1829 he became a *Privatdozent* at the University of Berlin, in 1831 he was promoted to *ausserordentlicher Professor*, and in 1839 he became *ordentlicher Professor*, or full professor.

In 1832, Dirichlet married Rebekka Mendelssohn. They had three sons and a daughter. Rebekka's brother was the composer Felix Mendelssohn-Bartholdy, her sister was the composer Fanny Mendelssohn, and her father was a banker. Her grandfather was the philosopher Moses Mendelssohn. (Much more information on the Mendelssohn family is available in Sebastian Hensel's book [**19**].) Dirichlet remained in Berlin, except for a period from the fall of 1843 through the spring of 1845, which he spent in Italy together with Carl Jacobi (1804–1851) and the Swiss geometer Jakob Steiner (1796–1863). The Swiss teacher, Ludwig Schläfli (1814–1895), who was later to become a well-known mathematician, accompanied Jakob Steiner. According to Koch [**26**], Dirichlet presented lectures to Schläfli on a daily basis during this time. (Curiously, while trying to show that the circle is the curve with the largest area among all plane closed curves with a given length, Steiner assumed without proof that a particular maximum value could be attained—the same type of unjustified assumption present in Dirichlet's work. Surprisingly, Steiner's proof was criticized by none other

than Dirichlet, and existence of a solution was first proven by Weierstrass. Blåsjö's article [**11**] and Monna's text [**30**, p. 38] contain more information about this.)

In 1855, Dirichlet was asked to come to Göttingen to succeed Gauss. Though Dirichlet had at first enjoyed teaching at the *Kriegsschule*, his dual obligations at the *Kriegsschule* and the University of Berlin began to overwhelm him. At the university, Dirichlet had a large group of followers, whom he found intellectually stimulating. So, Dirichlet asked the Prussian Ministry of Culture to excuse him from teaching at the *Kriegsschule*, and he said that he would accept the position in Göttingen if he were not excused from his teaching duties at the *Kriegsschule* by a certain date. The Prussian Minister waited too long, and Dirichlet moved to Göttingen in 1855. In 1858, Dirichlet traveled to Switzerland to give a memorial speech about Gauss, and it was there that Dirichlet had a heart attack. In December of 1858, after his return to Göttingen and during his illness, his wife died. Dirichlet died the following spring at the age of 54.

Dirichlet was not only an excellent mathematician, he also attracted a large audience. According to Kummer [**27**] (who was, incidentally, Dirichlet's successor in Berlin), "Particularly in the later years of his academic endeavors, the success of his teaching, measured externally by the number of listeners, was so significant that, in this respect, surely no other instructor at a German university can match him in the subject of higher mathematics. It was in no way his didactic art to which he owed this success, nor the gift of a brilliant lecture, but rather solely the inner clarity of his mind, which made it possible for him to grasp and present the simple truth of even the most difficult things."

Dirichlet's publications, students, and lectures were to be a strong influence on the development of mathematics. Students in Dirichlet's lecture included Eisenstein (1823–1852), Kronecker (1823–1891), Riemann (1826–1866), and Dedekind (1831–1916). Lipschitz (1832–1903) also studied under Dirichlet, completing his doctorate in 1853. (In some literature, Dirichlet is cited as Lipschitz's advisor; in others, as a second reader on his thesis.)

In 1856–1857, Dirichlet lectured on potential theory in Göttingen, and notes of those lectures were published by F. Grube in 1876. The subject treated in these notes is mathematical, but the influence of physics is apparent. Both Gauss and Dirichlet were influenced by Newton's law of gravitation, which the reader will recall states that any two objects exert a gravitational force of attraction on each other; the direction of the force is along the line joining the centers of mass of the objects and the magnitude of the force is proportional to the product of the masses of the objects, and inversely proportional to the square of the distance between the centers of mass. In electricity and magnetism this law takes the form of Coulomb's law.

Newton studied the problem of attraction between a point mass and solid sphere, but the earth was known not to be spherical, and thus Dirichlet's lectures include the attraction on an object by an ellipsoid. Other applications in the lectures include the theory of electricity and of magnetism.

In this set of lecture notes, the Dirichlet problem and Dirichlet's method of treating it (which came to be called Dirichlet's principle) both appear. We mention briefly that this is not the first occurrence of the use of the principle. (The first use of the principle, which is another story in and of itself, seems to be by George Green (1793–1841) whose work was published privately by Green, neglected, and then rediscovered by Sir William Thomson (1824–1907), also known as Lord Kelvin.) We return to the story of the Dirichlet principle later.

Dirichlet's influence was not limited to potential theory. Indeed, Dirichlet is perhaps best known for his influence on the field of number theory (and this is the focus of the articles by Shields [**39**] and Rowe [**34**]). Another very nice article on Dirichlet's mathematics is in the *Dictionary of Scientific Biography* [**1**].

Keith Devlin mentions Dirichlet's influence in his article, *The Forgotten Revolution* (http://www.maa.org/devlin/devlin_03_03.html):

> In the middle of the nineteenth century, however, a revolution took place. One of its epicenters was the small university town of Göttingen in Germany, where the local revolutionary leaders were the mathematicians Lejeune Dirichlet, Richard Dedekind, and Bernhard Riemann. In their new conception of the subject, the primary focus was not performing a calculation or computing an answer, but formulating and understanding abstract concepts and relationships—a shift in emphasis from doing to understanding. Within a generation, this revolution would completely change the way pure mathematicians thought of their subject. Nevertheless, it was an extremely quiet revolution that was recognized only when it was all over. It is not even clear that the leaders knew they were spearheading a major change.

As an example, Devlin cites Dirichlet's definition of function. In fact, "Dirichlet abandoned the then universally accepted idea of a function as an expression formulated in terms of special mathematical symbols or operations." [**1**] Indeed, Dirichlet introduced the modern idea of thinking of a function as a correspondence that associates to each x a unique value denoted $f(x)$. (Much more information on this can be found in other articles, such as Kleiner's article on the *Evolution of the Function Concept* [**23**] or Rüthing's list of the ever-changing definition of function [**35**]). Dirichlet's influence is also made clear by Riemann who, in his *Habilitation* on Fourier series, wrote the following in the introduction [**8**, p. 37]: "In composing this thesis, I had the privilege of using some tips of the famous mathematician, to whom we are indebted for the first fundamental work in this subject."

Dirichlet published relatively little, but what he published was of very high quality. Perhaps this is best summed up by the following well-known quote of Gauss: "Gustav Lejeune Dirichlet's works are jewels, and jewels are not weighed with a grocer's scale." [**33**]

The Dirichlet principle

We now turn to the Dirichlet problem and the principle that was first used to find a solution to it.

A real-valued function u on an open subset Ω of $\mathbb{R}^n$ is called harmonic if it is twice continuously differentiable and the Laplacian of u, defined by $\Delta u = \partial^2 u/\partial x_1^2 + \cdots + \partial^2 u/\partial x_n^2$, satisfies $\Delta u = 0$ throughout Ω.

The problem that motivated Dirichlet appears below. The conditions are vague, just as they were in the original motivating problem. When we work on our Dirichlet problem, we promise to state the conditions more precisely [**10**, p. 385; **14**].

THE DIRICHLET PROBLEM IN $\mathbb{R}^3$. *Given a bounded region Ω, does there exist a unique function u of variables x, y and z which, together with its first derivatives, is continuous within the domain, satisfies*

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{\partial^2 u}{\partial z^2} = 0$$

and assumes a given value at each point of the boundary?

The idea was, then, to start with a function f continuous on the boundary of the domain, and to find a harmonic function u continuous on the domain together with its

boundary, and equal to f on the boundary. As we have already indicated, the problem was solved using something called the Dirichlet principle:

THE DIRICHLET PRINCIPLE IN $\mathbb{R}^3$. *On the boundary of a bounded connected set, continuous boundary values are prescribed. Among all functions that are continuous on the set together with its boundary, have continuous partials, and have the given boundary values, there is a function u for which*

$$\int_\Omega \left[\left(\frac{\partial u}{\partial x}\right)^2 + \left(\frac{\partial u}{\partial y}\right)^2 + \left(\frac{\partial u}{\partial z}\right)^2 \right] dV$$

takes its minimum value.

Let us clarify what the principle has to do with the problem. According to Grube's notes [**10**], Dirichlet sets up this integral of the square magnitude of the gradient, uses the Dirichlet principle to find the minimizing function, and then shows three things: first, that any harmonic function (with the prescribed boundary values) minimizes the integral; second, that any function (with the prescribed boundary values) minimizing the integral must be harmonic; finally, that only one function yields the minimum value of the integral.

We present the argument for the first assertion in $\mathbb{R}^2$ here. The second argument is similar and can be found in Dirichlet's lectures, or rather the translation of Grube's version of Dirichlet's lectures [**10**, p. 385]. Note that once Dirichlet has this result, his notes indicate that this proves that there always exists a function with the desired properties. Why? He believed that it was clear that the integral had a function minimizing it, and now he shows that any minimizing function is harmonic. So if we put these two things together, the minimizing function solves the problem. Uniqueness follows from the maximum principle for harmonic functions, and will not be proved here.

Taking a harmonic function u that solves the Dirichlet problem for the function f, let us show why u minimizes the given integral. Suppose $w = u$ on the boundary of Ω and that w is such that we can take first partial derivatives. Consider the function $v = u - w$ and note that since u and w agree on the boundary of Ω, we have $v = 0$ on the boundary of Ω. Now

$$\begin{aligned}\int_\Omega \left(\frac{\partial w}{\partial x}\right)^2 + \left(\frac{\partial w}{\partial y}\right)^2 dA &= \int_\Omega \left(\frac{\partial (u-v)}{\partial x}\right)^2 + \left(\frac{\partial (u-v)}{\partial y}\right)^2 dA \\ &= \int_\Omega \left(\frac{\partial u}{\partial x}\right)^2 + \left(\frac{\partial u}{\partial y}\right)^2 dA + \int_\Omega \left(\frac{\partial v}{\partial x}\right)^2 + \left(\frac{\partial v}{\partial y}\right)^2 dA \\ &\quad - 2\int_\Omega \left(\frac{\partial u}{\partial x}\frac{\partial v}{\partial x} + \frac{\partial u}{\partial y}\frac{\partial v}{\partial y}\right) dA.\end{aligned}$$

Using Green's theorem, recalling that $v = 0$ on the boundary of Ω, and omitting the details, we get

$$\int_\Omega \left(\frac{\partial u}{\partial x}\frac{\partial v}{\partial x} + \frac{\partial u}{\partial y}\frac{\partial v}{\partial y}\right) dA = -\int_\Omega v \Delta u \, dA.$$

Since u is harmonic, this last integral must be zero. Therefore, if u solves the Dirichlet problem and w is any other smooth function with the same boundary values,

$$\int_\Omega \left(\frac{\partial w}{\partial x}\right)^2 + \left(\frac{\partial w}{\partial y}\right)^2 dA \geq \int_\Omega \left(\frac{\partial u}{\partial x}\right)^2 + \left(\frac{\partial u}{\partial y}\right)^2 dA.$$

Thus, u minimizes the integral, as claimed.

Weierstrass weighs in

The Dirichlet principle was used by many mathematicians, including Gauss, Green, Riemann, Thomson, and others. The principle and the existence of a solution to the Dirichlet problem were justified on physical grounds. For example, when Weierstrass wrote his article he used Dedekind's notes of Dirichlet's lectures; in reference to the Dirichlet problem, the notes say [**43**]

> In fact this theorem is identical with one from the theory of heat that is evident to everyone in that field, namely the theorem that says that when an arbitrarily prescribed temperature remains constant on the boundary of the region, there is one and only one temperature distribution in the interior such that equilibrium takes place. In other words, if the temperature in the interior were arbitrary, then it would approach a final state in which equilibrium would occur.

But as the demand for rigor in mathematics increased, so did the realization that knowing that a set was bounded below was not enough to assure the existence of a function achieving the infimum; in other words, an infimum is not the same as a minimum.

It was Weierstrass who indicated that the Dirichlet principle required a proof. His paper is remarkably easy to read, and his example—showing explicitly how the argument can fail—is easy as well. In fact, the example is so simple that it is somewhat surprising that it is not included in introductory analysis texts. (It can be found in texts on variational methods, such as Mikhlin's book [**28**, p. xvi], and as it makes good reading on the difference between the minimum and infimum, a brief history of the problem is included in the text [**13**].) We summarize Weierstrass's paper below, just to make our point self-evident.

Weierstrass [**43**] begins his paper, "On the so-called Dirichlet Principle," by reconstructing Dirichlet's argument as it appeared in Dedekind's notes. He then proceeds to the following example in $\mathbb{R}$. His example is sometimes referred to as a "modified Dirichlet integral" because it seems to be very similar to the one appearing in the Dirichlet principle.

We consider a family of integrals

$$\int_{-1}^{1} \left(x \frac{df_\epsilon(x)}{dx} \right)^2 dx,$$

where each integral is similar to the one Dirichlet considered. This family has an infimum (it is obviously bounded below by zero), but no minimum. To define the functions, let a and b be real numbers with $a \neq b$. Define f_ϵ, for each $\epsilon > 0$, on the interval $[-1, 1]$ by

$$f_\epsilon(x) = \frac{a+b}{2} + \frac{b-a}{2} \cdot \frac{\arctan(x/\epsilon)}{\arctan(1/\epsilon)}.$$

The graphs of some members of this family, with $a = -1, b = 1$, appear in FIGURE 1.

We first note, as Weierstrass did, that this function satisfies $f_\epsilon(1) = b$ while $f_\epsilon(-1) = a$.

Let's compute the infimum over ϵ of the integrals

$$\int_{-1}^{1} \left(x \frac{df_\epsilon(x)}{dx} \right)^2 dx,$$

and then see what happens if we assume, as many mathematicians of the 19th century did, that there is a function that minimizes the integral. An easy computation of the

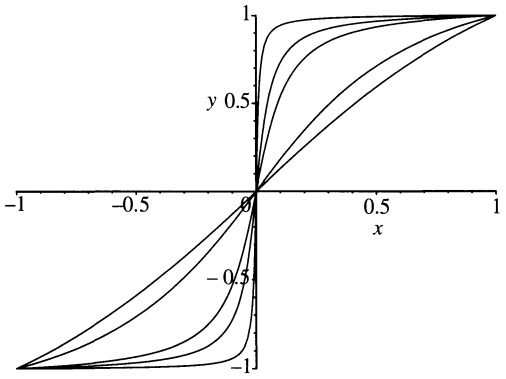


Figure 1 A typical family of f_ϵ for $\epsilon = 1, 0.5, 0.1, 0.05, 0.01$

derivative shows that

$$\frac{df_\epsilon(x)}{dx} = \frac{b-a}{2\arctan(1/\epsilon)} \cdot \frac{\epsilon}{x^2+\epsilon^2}.$$

Thus, we see that

$$\begin{aligned}\int_{-1}^{1} \left(x\frac{df_\epsilon(x)}{dx}\right)^2 dx &= \epsilon^2 \frac{(b-a)^2}{(2\arctan(1/\epsilon))^2} \int_{-1}^{1} \frac{x^2}{(x^2+\epsilon^2)^2}\, dx \\ &\le \epsilon^2 \frac{(b-a)^2}{(2\arctan(1/\epsilon))^2} \int_{-1}^{1} \frac{x^2+\epsilon^2}{(x^2+\epsilon^2)^2}\, dx \\ &= \epsilon \frac{(b-a)^2}{(2\arctan(1/\epsilon))^2} \int_{-1}^{1} \frac{\epsilon}{x^2+\epsilon^2}\, dx = \epsilon \frac{(b-a)^2}{2\arctan(1/\epsilon)}.\end{aligned}$$

We already know that the infimum must be greater than or equal to zero. Letting $\epsilon \to 0^+$, we see that the infimum over all such f_ϵ must be zero.

Suppose there were a function, call it f, with continuous derivative, that yields the minimum value of the integral. Then this function would have to satisfy

$$\int_{-1}^{1} \left(x\frac{df(x)}{dx}\right)^2 dx = 0.$$

Since the integrand is squared, the only way this can happen is if $x^2(df/dx)^2 = 0$ on the interval $[-1, 1]$. Now, this can only happen if $df/dx = 0$ on the interval, and consequently f must be constant. But $f(1) = b$, while $f(-1) = a$ and Weierstrass had carefully chosen $a \neq b$.

The Weierstrass example is simple and clever. Remember, though, that we are after a solution to the Dirichlet problem—not a proof of the Dirichlet principle.

For example, in this case the Dirichlet problem asks for a function, harmonic on the interval $(-1, 1)$, continuous on the closed interval $[-1, 1]$, and equal to a given continuous function on the boundary of $[-1, 1]$, that is, at the points -1 and 1. Finding a solution to the Dirichlet problem in this case is easy (try it!), and certainly does not require the Dirichlet principle.

Towards the end of the 19th century, work in this area continued along two lines. First, some mathematicians tried to prove the principle. This lead to the need for a better understanding of maxima and minima. Following Weierstrass's criticism of the principle, many mathematicians also worked on finding alternate solutions to the

Dirichlet problem, that is, solutions independent of the Dirichlet principle. These mathematicians included a student of Weierstrass, Hermann Amandus Schwarz (1843–1921), who made significant progress on the two-dimensional problem, Carl Neumann (1832–1925), who was able to prove the existence of a function that solves the Dirichlet problem under fairly general conditions [**31**], and others [**41**]. Finally David Hilbert (1862–1943), in 1904 and 1905, presented his "resuscitation" of the Dirichlet principle by establishing it for sufficiently general domains. Hilbert presented his work [**20**] before the German mathematical congress. More information on this can be found in Monna's text [**30**, p. 55].

As Courant states in his text entitled *Dirichlet's Principle* [**12**, p. 2], "Since Hilbert's pioneering achievement, the theory has been both simplified and extended. Today Dirichlet's principle has become a tool as flexible and almost as simple as that already envisaged by Riemann. It has, moreover, been the starting point for the development of the so-called direct methods of the variational calculus, a development equally important to both pure and applied mathematics."

Rational boundary functions

In this section, we present our solution [**40**] of a special case of the Dirichlet problem. This solution was motivated by the solution to the Dirichlet problem on the ball in $\mathbb{R}^n$ discovered by Axler and Ramey [**6**]. Like their solution, our solution is integration-free, and consequently does not use the Dirichlet principle.

Other relatively simple (though not quite so simple) solutions for various cases have appeared [**7, 21, 29**]. An interesting use of the existence and uniqueness of the solution to the Dirichlet problem can be found in Edstrom's paper [**16**], where the author indicates how the solution can be used to sum certain series.

We will solve the Dirichlet problem on the open unit disk $\mathbf{D}$ in $\mathbb{R}^2$ with rational data on the boundary. In other words, our continuous boundary function has the form p/q, where p and q are polynomials in x and y, and q has no zeros on the unit circle. Theoretically, our solutions are exact. However, the method requires finding the partial fraction expansion of a rational function, which requires finding the roots of a complex polynomial. Once this has been done, we obtain exact solutions to the Dirichlet problem, which provide a useful way to test algorithms for computing solutions to the Dirichlet problem and are accessible to students at a very early stage in their mathematical career.

OUR DIRICHLET PROBLEM. *Given a rational function R of two variables that is continuous on the unit circle, find a function u, continuous on the closed unit disk, harmonic on the open unit disk* $\mathbf{D}$*, and equal to R on the unit circle.*

EXAMPLE 1. *Let $R_1(x, y) = x$. What is u?*

It is easy to see that $u_1(x, y) = x$ is harmonic on $\mathbf{D}$, continuous on the closed unit disk, and equal to R_1 on the unit circle.

EXAMPLE 2. *Let $R_2(x, y) = x^3 + xy^2$.*

This one is harder, but not really that much harder. Note that $R_2(x, y) = x(x^2 + y^2)$ and we want something that equals R_2 on the circle $x^2 + y^2 = 1$. As luck would have it, the function $u_2(x, y) = x$ is continuous on the closed unit disk, harmonic on the open disk, and equal to our function R_2 on the unit circle.

EXAMPLE 3. *Let* $R_3(x, y) = 1/(5 + 3x)$.

This one is more difficult and the solution will require our algorithm. After explaining the algorithm, we will show how to work through the details to obtain the desired function.

EXAMPLE 4. *Let* $R_4(x, y) = y^4/(1 + x^2)$.

You will not get this one without our help. (At least we don't think you will.) We will solve this at the end of the paper as well.

The solution to the Dirichlet problem on the disk is usually given by integration against the Poisson kernel [**4**, p. 12] and an exact computation of the solution is often quite difficult. When the function R is a polynomial defined on the open ball in $\mathbb{R}^n$, Axler and Ramey [**6**] developed a fast, exact algorithm to compute the solution to the Dirichlet problem using differentiation. In a private communication, Axler mentioned the question of creating an algorithm for rational functions. One such algorithm was developed by R. Walker [**42**], who created a function of one complex variable and then used the Schwarz integral [**2**, p. 168] to obtain an exact solution to the Dirichlet problem on the disk when the boundary data is a continuous rational function. As indicated in the introduction, our solution differs from Walker's in that the techniques are integration-free, and based primarily upon techniques available to a student after a second course in calculus.

To understand the solution, the reader will need to know that $z = x + iy$, that the conjugate of z ($\overline{z} = x - iy$) satisfies $\overline{z} = 1/z$ on the circle, how to compute the partial fraction expansion of a rational function over the complex numbers, what a complex analytic function is, and that the real part of an analytic function is harmonic. Since this follows readily from the Cauchy-Riemann equations, students should be able to understand this proof early in their studies in mathematics, physics, or engineering.

Our algorithm has been implemented in *Mathematica*. You can download the package from the MAGAZINE website. In addition to implementing the algorithm, our program also checks that the solution is harmonic on $\mathbf{D}$ and equal to the original function on the unit circle $\partial\mathbf{D}$.

The solution We seek to solve the Dirichlet problem for a rational function R of x and y that is continuous on the unit circle. Our solution will be the real part of a certain analytic function H, which we denote by $\mathrm{Re}(H)$. First, we create a rational function of one complex variable, which we will call h, that agrees with R on the boundary. Throughout, the substitutions we make depend heavily on the fact that we are working on the unit circle.

The new rational function arises from the well-known fact that $x = (z + \overline{z})/2$ and $y = (z - \overline{z})/2i$ and from noticing that $\overline{z} = 1/z$ on the unit circle. So if we define

$$h(z) = R\big((z + 1/z)/2, (z - 1/z)/2i\big),$$

then h is as desired: a rational function of one complex variable that is continuous on $\partial\mathbf{D}$ and equal to R on $\partial\mathbf{D}$.

Now we examine h. It is a rational function of one complex variable and long division decomposes h as $h = p + s$, where p is a polynomial in z and s is a rational function of z for which the degree of the numerator is less than the degree of the denominator. The Dirichlet problem is linear; that is, if we have the solution for each term in a sum, we can add them to get the solution to the Dirichlet problem for the entire sum. Since p is a polynomial and it is analytic, we know that once we solve the problem for s, we can use linearity to solve the problem for h. So, let's focus on s.

The rational function s will have finitely many poles, and we denote them by c_m. Since s is continuous on the unit circle, $|c_m| \neq 1$. The partial fraction expansion of s will look like

$$s = \sum_m k_m = \sum_{\{m:|c_m|<1\}} k_m + \sum_{\{m:|c_m|>1\}} k_m,$$

where $k_m(z) = a_m/(z - c_m)^{n_m}$, $a_m \in \mathbb{C}$, and $n_m \in \mathbb{Z}^+$. If $|c_m| > 1$, then k_m is analytic on an open set containing $\overline{\mathbf{D}}$. On the other hand, if $|c_m| < 1$, we have to replace k_m by an analytic function in $\mathbf{D}$ without changing the boundary values.

Here's what we have to do: Let $k(z) = a/(z - c)^n$, where a is a complex number, $c \in \mathbf{D}$, and n is a positive integer. We claim that the function K defined by

$$K(z) = \overline{k(1/\overline{z})}$$

is a rational function that is analytic on an open set containing $\overline{\mathbf{D}}$ and satisfies $\mathrm{Re}(K) = \mathrm{Re}(k)$ on $\partial\mathbf{D}$. To check this, simplify K to obtain

$$K(z) = \frac{\overline{a}z^n}{(1 - \overline{c}z)^n}.$$

Since $|c| < 1$, it is clear that K is analytic on an open set containing $\overline{\mathbf{D}}$. Furthermore, on $\partial\mathbf{D}$,

$$\mathrm{Re}(K(z)) = \mathrm{Re}\left(\frac{a}{(1/\overline{z} - c)^n}\right) = \mathrm{Re}\left(\frac{a}{(z - c)^n}\right) = \mathrm{Re}\left(k(z)\right),$$

which is what we needed to show.

Let's review: We start with a rational function R and replace it with a rational function of one variable, h, which has the same values as R on the circle. Using the linearity of the Dirichlet solution, long division, and a partial fraction decomposition, we reduce our problem to solving the Dirichlet problem for each term in the partial fraction decomposition of h. Now we return to the partial fraction decomposition and handle the poles that fall inside the circle.

If $|c_m| < 1$, trade the poles inside the disk for poles outside the disk by replacing k_m with the corresponding function K_m as described above. In every step, the real part of the boundary values remain the same.

Define a new function S by

$$S = \sum_{\{m:|c_m|<1\}} K_m + \sum_{\{m:|c_m|>1\}} k_m.$$

Then S is analytic on an open set containing $\overline{\mathbf{D}}$ and, since $\mathrm{Re}(K_m) = \mathrm{Re}(k_m)$, it is clear that $\mathrm{Re}(S) = \mathrm{Re}(s)$ on $\partial\mathbf{D}$.

Let $H = p + S$. Then H is analytic on an open set containing $\overline{\mathbf{D}}$ and $\mathrm{Re}(H) = \mathrm{Re}(p + S) = \mathrm{Re}(p + s) = \mathrm{Re}(h) = R$ on $\partial\mathbf{D}$. Since the real part of an analytic function is harmonic, we have proved the following theorem:

THEOREM. *Let R be a rational function of x and y continuous on $\partial\mathbf{D}$. Then there exists a rational function u, harmonic on $\mathbf{D}$, continuous on $\overline{\mathbf{D}}$, and such that $u = R$ on $\partial\mathbf{D}$.*

This theorem not only gives us an algorithm for finding the solution, it also shows that if the function we start out with is rational, then the solution will be as well. A well-known result [**6, 38**] says that if the data we begin with is a polynomial, and the

region is the ball in $\mathbb{R}^n$, then the solution is again a polynomial. A natural question to ask is whether or not this result generalizes to rational functions. After completing this paper, we learned from P. Ebenfelt, D. Khavinson, and H. Shapiro that, in fact, this is not the case. They give an example of a rational function in $\mathbb{R}^3$ for which the solution to the Dirichlet problem on the ball is a transcendental function [**15**]. Of course, because of our theorem above, this cannot happen in $\mathbb{R}^2$.

Examples As we shall show in this section, the solutions are generally quite complicated, even if the original function is simple.

EXAMPLE 3 REVISITED. *We return to our function* $R_3(x, y) = 1/(5 + 3x)$, *and we use it to show how our algorithm works.*

We first obtain a function of one variable by making the substitutions

$$x = (z + 1/z)/2 \quad \text{and} \quad y = (z - 1/z)/2i$$

to get

$$h(z) = R_3\big((z + 1/z)/2, (z - 1/z)/2i\big) = \frac{1}{5 + 3\frac{z+1/z}{2}} = \frac{2z}{3z^2 + 10z + 3}.$$

Since h is a rational function for which the degree of the numerator is less than the degree of the denominator, there is no need for long division.

There are two poles of this rational function: one outside the disk at $z = -3$ and one inside the disk at $z = -1/3$. Expanding h using partial fractions yields

$$h(z) = -\frac{1/4}{3z + 1} + \frac{3/4}{z + 3}.$$

The next step in our algorithm is to fix whatever problems the first rational function might have. Following our algorithm, we replace the first term by $-(1/4)/(1 + 3/z)$ to obtain

$$H(z) = -\frac{1/4}{3/z + 1} + \frac{3/4}{z + 3} = \frac{-(z - 3)}{4(z + 3)} = \frac{9 - x^2 - y^2 - 6iy}{36 + 24x + 4(x^2 + y^2)}.$$

Now our algorithm tells us that u_3 should be the real part of H, so

$$u_3(x, y) = \mathrm{Re}\big(H(z)\big) = \frac{9 - x^2 - y^2}{36 + 24x + 4(x^2 + y^2)}.$$

To verify that this solution is correct, we must check that $\Delta u_3 = 0$ and that $u_3 = R_3$ on the unit circle. The former is messy, but easy. For the latter, recall that on the unit circle $x^2 + y^2 = 1$ and so

$$u_3(x, y) = \frac{9 - 1}{36 + 24x + 4} = \frac{8}{40 + 24x} = \frac{1}{5 + 3x} = R_3(x, y).$$

A contour plot of u_3 appears in FIGURE 2 (where higher values are colored lighter). In general, the solution can be quite complicated, as the solution to Example 4 below shows. In this case, checking that it is correct involves replacing powers of $x^2 + y^2$ by 1, which can be difficult.

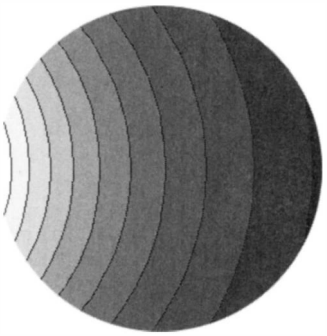


Figure 2 Contour plot of u_3

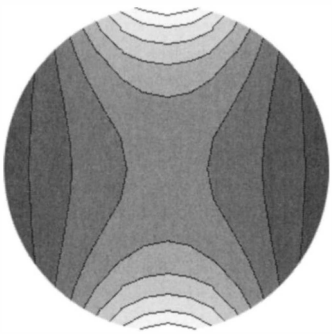


Figure 3 Contour plot of u_4

EXAMPLE 4 REVISITED. *We return to our function* $R_4(x, y) = y^4/(1 + x^2)$. *Our algorithm produces the following solution, depicted in* FIGURE 3*:*

$$\begin{aligned} u_4(x, y) = (&-5 + 4\sqrt{2} - 27x^2 + 24\sqrt{2}x^2 + 14x^4 + 10x^6 - 24\sqrt{2}x^6 + 7x^8 - 4\sqrt{2}x^8 + x^{10} \\ &+ 27y^2 - 24\sqrt{2}y^2 + 60x^2y^2 - 6x^4y^2 - 24\sqrt{2}x^4y^2 - 20x^6y^2 - 16\sqrt{2}x^6y^2 \\ &+ 3x^8y^2 + 14y^4 + 6x^2y^4 + 24\sqrt{2}x^2y^4 - 54x^4y^4 - 24\sqrt{2}x^4y^4 + 2x^6y^4 - 10y^6 \\ &+ 24\sqrt{2}y^6 - 20x^2y^6 - 16\sqrt{2}x^2y^6 - 2x^4y^6 + 7y^8 - 4\sqrt{2}y^8 - 3x^2y^8 - y^{10})/ \\ &(2 + 24x^2 + 76x^4 + 24x^6 + 2x^8 - 24y^2 + 120x^2y^2 + 24x^4y^2 + 8x^6y^2 + 76y^4 \\ &- 24x^2y^4 + 12x^4y^4 - 24y^6 + 8x^2y^6 + 2y^8). \end{aligned}$$

Last thoughts There is also another elementary solution to the special case of the Dirichlet problem for polynomials on the ball in $\mathbb{R}^n$ that makes a nice addition to an elementary course in linear algebra [**7, 21, 22**]. It is also possible to solve the Dirichlet problem for polynomial boundary data on an ellipsoid using partial derivatives and linearity [**5**].

We hope that the simple algorithm presented here will pique a student's interest in the Dirichlet problem—a problem with a fascinating history, as well as broad and appealing applications.

Acknowledgment. This work was part of the second author's honor thesis completed at Bucknell University under the direction of the first author. We thank Bucknell University for its support. We are grateful to Ulrich Daepp for his assistance with the translations as well as his careful reading of the manuscript. We are also grateful to Michael von Renteln, Karl Voss, and the anonymous referees of this paper for their very helpful comments.

REFERENCES

1. *Dictionary of Scientific Biography*, Charles Scribner's Sons, New York, 1971.
2. Lars V. Ahlfors, *Complex Analysis*, McGraw-Hill Book Co., New York, 1978.
3. University of Cologne Archives, *Private communication*, Letter, 2004.
4. Sheldon Axler, Paul Bourdon, and Wade Ramey, *Harmonic Function Theory*, Graduate Texts in Mathematics, vol. 137, Springer-Verlag, New York, 2001.
5. Sheldon Axler, Pamela Gorkin, and Karl Voss, The Dirichlet problem on quadratic surfaces, *Math. Comp.* (to appear), no. 9.
6. Sheldon Axler and Wade Ramey, Harmonic polynomials and Dirichlet-type problems, *Proc. Amer. Math. Soc.* **123**:12 (1995), 3765–3773.
7. John A. Baker, The Dirichlet problem for ellipsoids, *Amer. Math. Monthly* **106**:9 (1999), 829–834.
8. H. G. W. Begehr, H. Koch, J. Kramer, N. Schappacher, and E.-J. Thiele, *Mathematics in Berlin*, Birkhäuser Verlag, Berlin, 1998.
9. K.-R. Biermann, Johann Peter Gustav Lejeune Dirichlet, Dokumente für sein Leben und Wirken, Abh. der Deutschen Akademie der Wissenschaften zu Berlin, *Klasse für Mathematik, Physik und Technik* **2** (1959), 2–88.

10. Garrett Birkhoff, *A Source Book in Classical Analysis*, Harvard University Press, Cambridge, Mass., 1973.
11. Viktor Blåsjö, The evolution of... the isoperimetric problem, *Amer. Math. Monthly* **112**:6 (2005), 526–566.
12. Courant, R., *Dirichlet's Principle, Conformal Mapping, and Minimal Surfaces*, Interscience Publishers, Inc., New York, N.Y., 1950.
13. Ulrich Daepp and Pamela Gorkin, *Reading, Writing, and Proving: A Closer Look at Mathematics*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2003.
14. P. G. Le Jeune Dirichlet, *Vorlesungen über die im umgekehrten Verhältniss des Quadrats der Entfernung wirkenden Kräfte*, herausgegeben von Dr. F. Grube, Leipzig, 1876.
15. P. Ebenfelt, D. Khavinson, and H. Shapiro, Algebraic aspects of the Dirichlet problem with rational data, *Operator Theory Advances and Applications* **156** Birkhäuser, 2005, 151–172.
16. Clarence R. Edstrom, *A Dirichlet problem*, this MAGAZINE **45** (1972), 204–205.
17. Lars Gårding, The Dirichlet problem, *Math. Intelligencer* **2**:1 (1979/80), 43–53.
18. K. Gruhl, *Studienerinnerungen 1853–1856*, Mathematik aus Berlin, Auszüge von Gert Schubring (Berlin), Weidler, Berlin, 1997, pp. 55–57.
19. Sebastian Hensel, *Die Familie Mendelssohn, nach Briefen und Tagebüchern*, Insel Verlag, Frankfurt am Main und Leipzig, 1995.
20. David Hilbert, Über das Dirichletsche Prinzip, *Math. Ann.* **59** (1904), 161–186.
21. Dmitry Khavinson, Cauchy's problem for harmonic functions with entire data on a sphere, *Canad. Math. Bull.* **40**:1 (1997), 60–66.
22. Dmitry Khavinson and Harold S. Shapiro, Dirichlet's problem when the data is an entire function, *Bull. London Math. Soc.* **24**:5 (1992), 456–468.
23. Israel Kleiner, Evolution of the function concept: A brief survey, *College Math. J.* **20** (1989), 282–300.
24. Morris Kline, *Mathematical thought from ancient to modern times*, vol. 3, Oxford University Press, New York, 1972.
25. H. Koch, J. P. G. Lejeune Dirichlet zu seinem 175. Geburtstag, *Mitt. Math. Ges. DDR* (1981), no. 2-4, 153–164.
26. H. Koch, *P. J. Lejeune Dirichlet*, Mathematik in Berlin (Berlin), Birkhäuser Verlag, Berlin, 1998, p. 174.
27. E. E. Kummer, *Gedächtnisrede auf Gustav Peter Lejeune Dirichlet*, Abh. König. Akad. Wissen. zu Berlin; reprinted in G. Lejeune Dirichlet's *Werke*, ed. L. Kronecker and L. Fuchs (1981), no. 2, 309–344.
28. S. G. Mikhlin, *Variational Methods in Mathematical Physics*, trans. T. Boddington; editorial introduction by L. I. G. Chambers; The Macmillan Co., New York, 1964.
29. David Minda, The Dirichlet problem for a disk, *Amer. Math. Monthly* **97**:3 (1990), 220–223.
30. A. F. Monna, *Dirichlet's Principle: A Mathematical Comedy of Errors and Its Influence on the Development of Analysis*, Oosthoek, Scheltema, and Holkema, Utrecht, 1975.
31. C. Neumann, Untersuchungen über das Logarithmische und Newton'sche Potential, *Math. Ann.* **13** (1878), 255–300.
32. Bruce P. Palka, *An Introduction to Complex Function Theory*, Springer-Verlag, New York, 1991.
33. Michael von Renteln, *Geschichte der Analysis im 19. Jahrhundert, von Cauchy bis Cantor*, Skriptum zur Vorlesung, Universität Karlsruhe, 1989.
34. David E. Rowe, Gauss, Dirichlet, and the law of biquadratic reciprocity, *Math. Intelligencer* **10**:2 (1988), 13–25.
35. Dieter Rüthing, Some definitions of the concept of function from Joh. Bernoulli to N. Bourbaki, *Math. Intelligencer* **6**:4 (1984), 72–77.
36. Gert Schubring, The three parts of the Dirichlet *nachlass*, *Historia Math.* **13**:1 (1986), 52–56.
37. ———, Dirichlet. Comment on: "Gauss, Dirichlet, and the law of biquadratic reciprocity" [Math. Intelligencer 10 (1988), no. 2, 13–25; MR 89e:01031] by D. E. Rowe, *Math. Intelligencer* **12** (1990), no. 1, 5–6.
38. Harold S. Shapiro, An algebraic theorem of E. Fischer, and the holomorphic Goursat problem, *Bull. London Math. Soc.* **21**:6 (1989), 513–537.
39. Allen Shields, Lejeune Dirichlet and the birth of analytic number theory: 1837–1839, *Math. Intelligencer* **11**:4 (1989), 7–11.
40. Joshua H. Smith, *The Dirichlet Problem for Rational Functions*, Honors Thesis, Bucknell University, 1999.
41. Rossana Tazzioli, Green's function in some contributions of 19th century mathematicians, *Historia Math.* **28**:3 (2001), 232–252.
42. Ronald Walker, *Problems in Harmonic Function Theory*, Undergraduate Thesis, University of Richmond, 1998.
43. Karl Weierstrass, *Über das sogenannte Dirichlet'sche Princip, gelesen in der Königl. Akademie der Wissenschaften am 14. Juli 1870*, Karl Weierstrass, Mathematische Werke (Berlin), vol. 2, Mayer & Müller, Berlin, 1895, pp. 49–54.
44. Dirk Werner, *Funktionalanalysis*, Springer-Verlag, Berlin, 2000.

NOTES

Heads Up: No Teamwork Required

MARTIN J. ERICKSON
Division of Mathematics and Computer Science
Truman State University
Kirksville, MO 63501
erickson@truman.edu

Many team games require collaborative strategies. In this Note, I present a game that paradoxically requires cooperation, but at the same time forbids communication of any kind. A team skilled in probability can compete as if they could confer (almost).

In the "Hat Problem" [**1**], each contestant on a team tries to guess the color (blue or red) of a hat on his/her head while seeing only the hats of the other contestants. The guesses are made simultaneously, and "passing" is an option. The team wins if at least one person guesses and no one guesses incorrectly. Before the guessing round, the participants are allowed to discuss strategy. With best play, an n-person team (where n is one less than a power of 2) can win with the surprisingly high probability $n/(n+1)$. (The solution to the Hat Problem provides a novel perspective on Hamming codes, but you don't need to know anything about Hamming codes to understand this note.) I enjoyed the Hat Problem and was investigating variations of it when I thought of eliminating both the pregame strategy meeting and any information the teammates could gain from each other. The resulting game, recast in the context of coin-flipping, has some curious mathematical features.

> **Heads Up:** A team of $n \geq 2$ people is selected to participate in a game in which the team may win a prize. The players are not allowed to communicate with each other before or during the game. (Assume, for reasons that should become clear in a moment, that the players have never met before and know nothing about each other.) Each player is given a fair coin. At a signal, the players simultaneously open their hands to reveal either the coin or nothing. Those players showing coins then flip their coins. The team wins if at least one coin is flipped and all the flipped coins land heads. What strategy should each player follow in order to maximize the likelihood of the team winning, and what is the probability of winning?

The crucial factor in Heads Up is that the team members cannot communicate with each other so they cannot form a strategy together. (In the solution to the Hat Problem, the players determine an ordering of themselves so that they can convert the hat color distribution into a vector.) Ideally, the team would choose one member to flip the coin (and the team would win half of the time), but this is impossible because of the ban on communication. Are there, then, only two alternative strategies for each player: either flip the coin or don't flip it? If so, then not flipping the coin isn't good because if everyone does that, the team loses. But if everyone flips the coin, the team wins with very low probability ($(1/2)^n$). With $n = 2$, the probability of winning if both players flip the coin is $1/4$. However, with a superior strategy a two-person team can

do better than 1/4. In fact, the same is true for any number of players. With best play, an n-person team can do better than they could if they were able to choose two members to flip their coins!

Since the problem is about probabilities, we suppose that the players approach their strategies probabilistically. In addition, the players must assume that their teammates will also arrive at this conclusion. Each player should flip the coin with probability p, where the value of p is to be determined ($0 \le p \le 1$). We obtain the probability of the team winning, $w_n(p)$, via a binomial expansion:

$$w_n(p) = \sum_{k=1}^{n} \left(\frac{1}{2}\right)^k \binom{n}{k} p^k (1-p)^{n-k}$$

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

Using calculus, we find that w_n is maximized at

$$p_n \equiv p = \frac{2^{n/(n-1)} - 2}{2^{n/(n-1)} - 1}, \tag{2}$$

and the maximum winning probability is

$$w_n(p_n) = \left(2^{n/(n-1)} - 1\right)^{1-n}. \tag{3}$$

For example, with two players, $p_2 = 2/3$ and $w_2(p_2) = 1/3$. The coin can be used to generate an event with the required probability: express p_n in base 2 and flip the coin until the number generated (heads = 1, tails = 0) deviates from p_n. (This concept was the subject of a Putnam Competition problem [**2**, p. 137].) The case $n = 2$ can be handled in a particularly simple way: flip the coin twice; if it lands tails both times, do over; the probability of one heads and one tails is then 2/3.

Let's analyze our solution to Heads Up. Although we might conjecture that the maximum probability of winning in (3) tends to 0 as n tends to infinity, a calculation with l'Hôpital's rule reveals that

$$\lim_{n\to\infty} w_n(p_n) = \frac{1}{4}. \tag{4}$$

Actually, we might have guessed this result! Observing that in the formula in (1) the second quantity is almost the square of the first quantity, we could reason that the limit has the form $x - x^2$, and everyone who can complete a square knows that the maximum value of $x - x^2$ is 1/4.

It seems reasonable that the maximum probability of winning in (3) is a decreasing function of n. Numerical calculations indicate that this is true, and our intuition about the problem reinforces it (the chances of the team winning would appear to decrease as n increases). Let us define a real-variable version of the function:

$$f(x) = \left(2^{x/(x-1)} - 1\right)^{1-x}, \quad x > 1.$$

It is a tricky problem to prove that $f(x)$ is decreasing. Here is a calculus proof found by my undergraduate student Khang Tran. Take a logarithm:

$$g(x) = \ln f(x) = (1-x) \ln\left(2^{x/(x-1)} - 1\right).$$

Now

$$g'(x) = -\ln\left(2^{x/(x-1)} - 1\right) + \frac{2^{x/(x-1)} \ln 2}{(x-1)(2^{x/(x-1)} - 1)},$$

and we want to show that $g'(x)$ is negative for $x > 1$. Make a change of variables, $y = 1/(x-1)$:

$$h(y) = -\ln\left(2^{y+1}-1\right) + \frac{2^{y+1}y\ln 2}{2^{y+1}-1} = -\ln\left(2^{y+1}-1\right) + y\ln 2 + \frac{y\ln 2}{2^{y+1}-1}.$$

It suffices to show that $h(y)$ is negative for $y > 0$. Observe that $h(0) = 0$ and

$$h'(y) = -\frac{2^{y+1}\ln 2}{2^{y+1}-1} + \ln 2 + \frac{\ln 2}{2^{y+1}-1} + \frac{-2^{y+1}y(\ln 2)^2}{(2^{y+1}-1)^2}.$$

The first three terms sum to zero and the last term is negative.

Surprisingly, we can give a short proof that $w_n(p_n)$ is decreasing via the solution to Heads Up. Here it is:

$$w_n(p_n) \geq w_n(p_{n+1}) = w_{n+1}(p_{n+1}). \tag{5}$$

The inequality in (5) holds by virtue of the definition of p_n. The equality, which can be proved directly by combining (1) and (2), is an algebraic curiosity; it says that, for each n, the maximum value of w_{n+1} occurs on the graph of w_n. Put another way, this peculiar identity says that the success probabilities for n and $n+1$ are equal for the optimum probability p_{n+1}. This is like one team member "dropping out" (but, of course, no one member can drop out).

We see from (2) that the optimum probability p_n decreases to 0 as n tends to infinity. What can we say about $n\,p_n$, the expected number of coins flipped? From (2), using l'Hôpital's rule, we determine the limiting value:

$$\lim_{n\to\infty} n\,p_n = \ln 4. \tag{6}$$

(We could have guessed this result by invoking the fact that $\lim_{n\to\infty}(1-c/2n)^n = e^{-c/2}$ and recognizing that $x - x^2$ is maximized when $x = 1/2$.)

Furthermore, the expected number of coins flipped increases with n; that is,

$$n\,p_n < (n+1)p_{n+1}, \quad n \geq 2, \tag{7}$$

as we shall prove. Does intuition support this result? A calculus proof, with n replaced by a real variable x, is possible but tedious (make the change of variables $y = 2^{x/(x-1)}$ and differentiate). We prefer to stay with the discrete variable. The inequality (7) is equivalent to

$$n \cdot \frac{2^{n/(n-1)}-2}{2^{n/(n-1)}-1} < (n+1)\cdot\frac{2^{(n+1)/n}-2}{2^{(n+1)/n}-1},$$

which is equivalent to

$$\frac{1}{n+1}\cdot\frac{2^{(n+1)/n}-1}{2^{1/n}-1} < \frac{1}{n}\cdot\frac{2^{n/(n-1)}-1}{2^{1/(n-1)}-1},$$

and, by the formula for the sum of a geometric series, to

$$\frac{1+2^{1/n}+2^{2/n}+\cdots+2^{n/n}}{n+1} < \frac{1+2^{1/(n-1)}+2^{2/(n-1)}+\cdots+2^{(n-1)/(n-1)}}{n}. \tag{8}$$

This last inequality has a pleasing form. It's a consequence of a simple proposition on convex functions (applied to the function $f(x) = 2^x$).

PROPOSITION. *Let f be a convex function defined on the interval* $[0, 1]$. *Then, for* $n \geq 2$,

$$\frac{1}{n+1}\sum_{i=0}^{n} f\left(\frac{i}{n}\right) \leq \frac{1}{n}\sum_{i=0}^{n-1} f\left(\frac{i}{n-1}\right).$$

If f is strictly convex, then this inequality is strict.

This proposition is easy to prove using Jensen's inequality for convex functions: $f(\lambda a + (1-\lambda)b) \leq \lambda f(a) + (1-\lambda) f(b)$, for $0 \leq \lambda \leq 1$.

Returning to the Hat Problem, we ask the question, what happens if there is no pregame strategy meeting (and this is the only change we make)? In the case $n = 3$, no prearranged ordering of players is needed, and the team wins with probability $3/4$. (A player seeing two hats of the same color guesses the other color, and otherwise passes.) For $n > 3$, is the winning probability merely $w_n(p_n)$, or is there a way for the players to use the knowledge of each other's hat colors?

Acknowledgment. I am grateful to Suren Fernando, Upendra Kulkarni, Anthony Vazzana, and the referees for their suggestions concerning this note.

REFERENCES

1. M. Bernstein, The hat problem and hamming codes, *Focus* **21**:8 (2001), 4–6.
2. L. Larson, 50th annual William Lowell Putnam Mathematical Competition, winners and solutions, this MAGAZINE **63**:2 (1990), 136–139.

The Humble Sum of Remainders Function

MICHAEL Z. SPIVEY
University of Puget Sound
Tacoma, WA 98416
mspivey@ups.edu

The sum of divisors function is one of the fundamental functions in elementary number theory. In this note, we shine a little light on one of its lesser-known relatives, the sum of remainders function. We do this by illustrating how straightforward variations of the sum of remainders can 1) provide an alternative characterization for perfect numbers, and 2) help provide a formula for sums of powers of the first n positive integers. Finally, we give a brief discussion of perhaps why the sum of remainders function, despite its usefulness, is less well known than the sum of divisors function.

Some notation is in order. The standard notation [**3**] for the sum of divisors function is $\sigma(n)$:

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

We denote the sum of remainders function by $\rho(n)$, namely,

$$\rho(n) = \sum_{d=1}^{n} (n \bmod d).$$

Sums of remainders and perfect numbers A *perfect number* is a number equal to the sum of its positive divisors, excluding itself. Another way to express this is to say that perfect numbers are those for which $\sigma(n) = 2n$. The three smallest perfect numbers are 6, 28, and 496. Euclid proved that every number of the form $2^{p-1}(2^p - 1)$, where p and $2^p - 1$ are prime, is perfect. Euler proved the converse, that numbers of this form are the only even perfect numbers [**4**, p. 59]. One of the famous unsolved problems in number theory is whether or not there are any odd perfect numbers.

To see the connection between the sum of remainders and perfect numbers, let's take a look at what $\rho(n)$ is actually adding up. A table of remainders for $n = 15$ is as follows:

divisor: d	1	2	3	4	5	6	7	8	9	10	11	12	13	14
15 mod d	0	1	0	3	0	3	1	7	6	5	4	3	2	1

Two patterns are fairly immediate: There are zeroes in the entries for which d divides n, and once past half of 15, the remainders count down from 7 (just under half of 15) to 1. Other than that, there does not appear to be much of a pattern.

However, if we line up the remainders for several consecutive integers we start to see a pattern:

divisor: d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1 mod d	0														
2 mod d	0	0													
3 mod d	0	1	0												
4 mod d	0	0	1	0											
5 mod d	0	1	2	1	0										
6 mod d	0	0	0	2	1	0									
7 mod d	0	1	1	3	2	1	0								
8 mod d	0	0	2	0	3	2	1	0							
9 mod d	0	1	0	1	4	3	2	1	0						
10 mod d	0	0	1	2	0	4	3	2	1	0					
11 mod d	0	1	2	3	1	5	4	3	2	1	0				
12 mod d	0	0	0	0	2	0	5	4	3	2	1	0			
13 mod d	0	1	1	1	3	1	6	5	4	3	2	1	0		
14 mod d	0	0	2	2	4	2	0	6	5	4	3	2	1	0	
15 mod d	0	1	0	3	0	3	1	7	6	5	4	3	2	1	0
16 mod d	0	0	1	0	1	4	2	0	7	6	5	4	3	2	1
17 mod d	0	1	2	1	2	5	3	1	8	7	6	5	4	3	2
18 mod d	0	0	0	2	3	0	4	2	0	8	7	6	5	4	3

For fixed d and increasing n, $n \bmod d$ cycles from 0 to $d - 1$, hitting 0 at all the integers that d divides. This makes sense, of course, when you think about it.

In particular, if we compare $n \bmod d$ and $(n - 1) \bmod d$, we see that the difference between them is either 1, if d does not divide n, or $1 - d$, if d does divide n. In symbols, this becomes

$$(n \bmod d) - (n - 1 \bmod d) = \begin{cases} 1, & \text{if } d \nmid n, \\ 1 - d, & \text{if } d \mid n. \end{cases} \tag{1}$$

Now, define the *backward difference operator* ∇ by $\nabla f(n) = f(n) - f(n - 1)$. Then the connection between the sum of remainders and perfect numbers is the following:

THEOREM 1. *n is perfect if and only if $\nabla\rho(n) = -1$.*

Proof. Summing up the left-hand side of the equation in (1) over d from 1 to $n-1$ yields $\rho(n) - \rho(n-1)$. The sum of the right-hand side of the equation in (1) over d from 1 to $n-1$ can be split into the sum over those d that do not divide n and the sum over those that do. Setting the two expressions equal to each other yields

$$\rho(n) - \rho(n-1) = \sum_{d\nmid n} 1 + \sum_{d|n, d\neq n} (1-d) = \sum_{d=1}^{n-1} 1 - \sum_{d|n, d\neq n} d$$

$$= n - 1 - \sum_{d|n} d + n = 2n - 1 - \sigma(n).$$

Since a number is perfect if and only if $\sigma(n) = 2n$, the theorem follows. ∎

Theorem 1 is a surprisingly simple characterization of perfect numbers in terms of the sum of remainders. The theorem is proved by Cross [**1**] and by Lucas [**8**, p. 374]. (Cross's reference to p. 388 in Lucas is in error.)

The proof of Theorem 1 also implies simple characterizations of numbers that are close to being perfect. Define an *almost perfect* number to be a number n such that $\sigma(n) = 2n - 1$. Powers of 2 are almost perfect, but these are the only numbers known to be almost perfect. Define a *quasi-perfect* number to be a number n such that $\sigma(n) = 2n + 1$. It is not known if there are any quasi-perfect numbers, but it is known that they must be odd squares [**5**]. Slight modifications of the proof of Theorem 1 then yield

COROLLARY 1. *We have the following:*

- *n is almost perfect if and only if $\nabla\rho(n) = 0$.*
- *n is quasi-perfect if and only if $\nabla\rho(n) = -2$.*

This can go on, of course, for other numbers that are close to being perfect.

There is another interesting corollary to Theorem 1. Calculus, as any freshman math major knows, involves derivatives and integrals of functions defined over real numbers. Calculus can also be done with discrete functions, functions defined over, say, the integers, in which case it is known as *calculus of finite differences*. The discrete analog of the derivative is the *finite difference*:

$$\Delta f(n) = f(n+1) - f(n).$$

And the discrete analog of the antiderivative is the *antidifference*:

$$\Delta^{-1} f(n) \text{ is any function } F \text{ such that } \Delta F = f.$$

With finite calculus in mind, we see that the proof of Theorem 1 says that the finite difference of $\rho(n)$ is $2n + 1 - \sigma(n+1)$, or, alternatively, that an antidifference of $\sigma(n)$ is $(n-1)^2 - \rho(n-1)$. Thus the ρ and σ functions are related to each other in a simple way via finite calculus. We are not aware of any other basic number-theoretic functions for which this is the case.

Sums of remainders and power sums For various integers k, the sums of kth powers of the first n positive integers, $1^k + 2^k + \cdots + n^k$, are among the most popular sums in all of mathematics. Jakob Bernoulli developed a whole new class of numbers, later named in his honor, to represent these sums. In addition to formulas using Bernoulli numbers, there are formulas involving Eulerian numbers and binomial coefficients, as well as Stirling numbers and binomial coefficients [**10**]. Many other papers have appeared on the subject [**7, 9**].

The promised formula for the power sum using remainders involves variations of both ρ and σ. Recall that the value of $\sigma(n)$ is determined by summing the divisors of n. Besides summing the divisors, however, we can also sum up powers of the divisors; that is, squares, cubes, or even any real powers. The standard notation is

$$\sigma_k(n) = \sum_{d|n} d^k.$$

Results concerning this function are scattered throughout Chapter X of Dickson [**3**]; other problems, some solved and some unsolved, appear in books by Dudley [**4**, p. 56] and Guy [**5**, pp. 102–105].

We could also sum powers of the remainders. However, for our purposes we need remainders that are *weighted* by powers of integers; namely, multiply $n \bmod d$ by d^k and then add up. This leads to the following definition:

$$\rho(n, k) = \sum_{d=1}^{n} d^k (n \bmod d).$$

Then the formula for the power sum in terms of $\sigma_k(n)$ and $\rho(n, k)$ is

THEOREM 2. *For any real number k,*

$$1^k + 2^k + \cdots + n^k = \frac{1}{n}\left(\rho(n, k) + \sum_{i=1}^{n} \sigma_{k+1}(i)\right).$$

A nice property of Theorem 2 is that k can be any real number; most other formulas for the power sum restrict k to the nonnegative integers.

Two special cases of Theorem 2 are worth mentioning. If $k = 0$, we have the nice formula

$$n^2 = \rho(n) + \sum_{i=1}^{n} \sigma(i),$$

which appears in Lucas [**8**, p. 388]. This formula can also be derived easily from the proof of Theorem 1. In addition, the case $k = -1$ can be rewritten as

$$\sum_{i=1}^{n} \lfloor n/i \rfloor = \sum_{i=1}^{n} d(i),$$

where $d(i)$ gives the number of divisors of the integer i. This result is discussed in the proof of Theorem 320 in Hardy and Wright [**6**].

Before we prove Theorem 2, though, we need to define the *indicator function* $I_{\{p\}}$ for a statement p. This is given by the following:

$$I_{\{p\}} = \begin{cases} 1, & \text{if } p \text{ is true,} \\ 0, & \text{if } p \text{ is false.} \end{cases}$$

Let us proceed to prove Theorem 2.

Proof. The division algorithm tells us that, for any integers n and d, $n = dq_d + r_d$, where q_d is the quotient and r_d is the remainder when n is divided by d. Multiplying both sides of this equation by d^k and summing over d from 1 to n yields the following:

$$n \sum_{d=1}^{n} d^k = \sum_{d=1}^{n} \left(d^{k+1} q_d + d^k r_d\right) = \sum_{d=1}^{n} d^{k+1} q_d + \rho(n, k). \tag{2}$$

At this point we can start to see the formula becoming clear. All that remains is to show that $\sum_{d=1}^{n} d^{k+1} q_d = \sum_{i=1}^{n} \sigma_{k+1}(i)$. To see this, we need the fact that q_d counts the number of integers between 1 and n that d divides evenly. For example, 37 divided by 7 leaves a quotient of 5; this is because 7 divides exactly five integers between 1 and 37: 7, 14, 21, 28, and 35. Therefore,

$$\sum_{d=1}^{n} d^{k+1} q_d = \sum_{d=1}^{n} d^{k+1} \sum_{i=1}^{n} I_{\{d|i\}} = \sum_{i=1}^{n} \sum_{d=1}^{n} d^{k+1} I_{\{d|i\}}$$

$$= \sum_{i=1}^{n} \sum_{d|i} d^{k+1} = \sum_{i=1}^{n} \sigma_{k+1}(i).$$

Substituting this expression into (2) and dividing both sides of the equation by n yields the formula. ■

Some limitations of the sum of remainders function With so many uses of the sum of remainders function, why is it so little known relative to the sum of divisors function? While some of the answer may be historical, much of it also lies in the fact that ρ does not have some of the nice properties that σ has, properties that σ shares with other well-known arithmetical functions.

For example, ρ is not multiplicative, whereas σ is. Multiplicative arithmetical functions f are those that are not identically zero and have the property that $f(mn) = f(m)f(n)$ whenever m and n are relatively prime. This property means that the values of multiplicative functions are completely determined by their behavior on powers of primes. It is easy to see that ρ is not multiplicative; for example, $\rho(2) = 0$, but no other even number n has $\rho(n) = 0$. Dudley [**4**, p. 54] gives a proof that σ is multiplicative.

Another nice property that σ has but ρ does not is that σ is a unit in the standard ring of arithmetical functions. (Recall that the units in a ring are the elements that have multiplicative inverses.) In a recent article in this MAGAZINE, Delaney [**2**] characterizes the units in this ring. He also gives a formula for σ as the Dirichlet product of two simple functions, and one can use his subsequent discussion to construct the inverse of σ. Again, it is easy to see that ρ has no inverse. The multiplicative identity in the ring is the indicator function $1(n) = I_{\{n=1\}}$, and since $\rho(1) = 0$, ρ can have no inverse. (Further details on the ring of arithmetical functions can be found in Delaney's paper [**2**].)

Final remarks We have seen that the sum of remainders function ρ can provide a simple alternative characterization for perfect numbers, and, in conjunction with a variation of the sum of divisors function, give a new formula for sums of powers. We have also seen that the sum of remainders function does not have two nice properties that many more well-known arithmetical functions do have, namely, ρ is not multiplicative, and ρ is not a unit in the standard ring of arithmetical functions.

In the absence of much literature on the subject, interested readers may enjoy framing their own questions concerning the sum of remainders function.

REFERENCES

1. James T. Cross, A note on almost perfect numbers, this MAGAZINE **47** (1974), 230–231.
2. James E. Delaney, Groups of arithmetical functions, this MAGAZINE **78** (2005), 83–95.
3. Leonard E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York, 1952.
4. Underwood Dudley, *Elementary Number Theory*, W. H. Freeman, New York, 2nd ed., 1978.

5. Richard K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 3rd ed., 2004.
6. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, 5th ed., 1979.
7. Donald E. Knuth, Johann Faulhaber and sums of powers, *Mathematics of Computation* **61** (1993), 277–294.
8. Édouard Lucas, *Théorie des Nombres*, Gauthier-Villars, Paris, 1891.
9. Robert W. Owens, Sums of powers of integers, this MAGAZINE **65** (1992), 38–40.
10. Kenneth H. Rosen, ed., *Handbook of Discrete and Combinatorial Mathematics*, CRC Press, Boca Raton, FL, 2000.

On Tiling the n-Dimensional Cube

WILLIAM STATON
BENTON TYLER
University of Mississippi
University, MS 38677
mmstaton@olemiss.edu

Take a square and cut it into smaller pieces, each of which is a square. Now count the number of pieces. It is easy to show that the answer is not 2, 3, or 5, but it might be anything else. Asking the question a different way: for what values of k can one tile a square with k squares? Here *tiling* means covering with pieces that overlap only on edges. FIGURE 1 shows tilings of a square with $k = 4$, 6, 7, and 8.

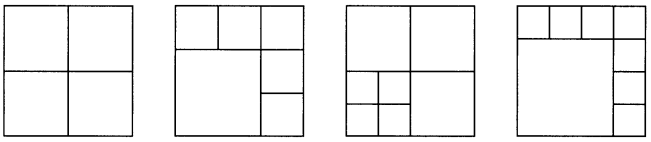


Figure 1 Some tilings of a square

It is an easy observation that if a tiling with k squares exists, then a tiling with $k + 3$ squares also exists. For in a tiling, a single square may be replaced by the first tiling in FIGURE 1. So, the existence of tilings for $k = 6$, 7, and 8, along with the easy passage from k to $k + 3$, provide an inductive proof of the existence of tilings for all $k \geq 6$. We leave as an exercise the impossibility of $k = 2$, 3, and 5. Hint: count corners.

Now we ask similar questions in higher dimensions. Can an n-dimensional cube (n-*cube* for short) be tiled with k smaller n-cubes?

FACT 1. The standard tiling of a unit n-dimensional cube with r^n cubes each of edge length $1/r$ shows that the answer is yes in dimension n for $k = 2^n, 3^n, 4^n, \ldots$.

Here is another key to solving the higher dimensional problem: Note that in a given k-tiling, a single tile may be replaced by a cube tiled with l tiles. This observation gives us Fact 2.

FACT 2. If the n-cube can be tiled with k cubes and can be tiled with l cubes, then it can be tiled with $k + l - 1$ cubes.

Now let $k = 1$ and $l = (2^n - 1)^n$ and apply Fact 2 j times to learn that the n-cube may be tiled with $1 + j[(2^n - 1)^n - 1] = j(2^n - 1)^n - j + 1$ cubes. As j varies from 0 to $2^n - 2$, the resulting numbers of tiles hit every congruence class modulo $2^n - 1$. For example, in dimension three, the situation is as in TABLE 1.

Now, by Fact 2, if a tiling exists with k tiles, then one exists for $k + 2^n - 1$ tiles, so if a tiling exists with k_1 tiles then a tiling exists with any larger $k_2 \equiv k_1 \bmod (2^n - 1)$. We conclude that tilings exist in dimension n for all k greater than or equal to

$$(2^n - 2)(2^n - 1)^n - (2^n - 2) + 1.$$

TABLE 1: Some possible tilings of the 3-cube

j	$j(2^3 - 1)^3 - j + 1 = 343j - j + 1$	mod 7
0	1	1
1	343	0
2	685	6
3	1027	5
4	1369	4
5	1711	3
6	2053	2

Now it is perhaps interesting to ask for the smallest number $f(n)$ so that an n-dimensional cube can be tiled with k n-dimensional cubes for all $k \geq f(n)$. We have shown $f(2) = 6$.

Examine TABLE 1. The values of k in the interval [2047, 2053] are covered in the 7 congruence classes, but $k = 2046$ is not, since 2053 is the smallest number covered that is congruent to 2 mod 7. These 7 numbers, along with the k to $k + 7$ induction show that in fact $f(3) \leq 2047$.

Similarly, in n dimensions, the threshold is actually no larger than

$$(2^n - 2)(2^n - 1)^n - 2^n + 3 - (2^n - 2) = (2^n - 2)(2^n - 1)^n - 2^{n+1} + 5.$$

Our general upper bound for $f(n)$ is probably very bad. We will show that in fact $f(3) \leq 48$.

We must cover every congruence class modulo $7 = 2^3 - 1$. We accomplish this with the following values of k:

TABLE 2: Better ways to tile the 3-cube

k mod 7	0	1	2	3	4	5	6
k	49	1	51	38	39	54	20

Beginning with the simplest, we note that tiling with 1 cube is trivial. Tiling with 20 cubes can be done by taking a standard tiling of 27 congruent cubes and replacing the 8 cubes of a $2 \times 2 \times 2$ subcube with a single cube, as in FIGURE 2.

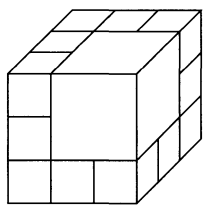


Figure 2 Using 20 cubes

Now we invoke Fact 2 with $k = l = 20$ to obtain a tiling with 39 cubes. This is shown in FIGURE 3. To construct a tiling with 38 cubes, begin with a standard tiling of 64 cubes and replace the 27 cubes of a $3 \times 3 \times 3$ subcube with a single cube.

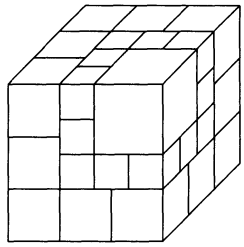


Figure 3 Tiling with 39 cubes

To construct a tiling with 49 cubes, imagine a unit cube sliced into three horizontal slabs of thickness $1/2$, $1/3$, and $1/6$. Tile the first slab with 4 cubes of side length $1/2$, the second with 9 cubes of side length $1/3$, and the third slab with 36 cubes of side length $1/6$. This is shown in FIGURE 4.

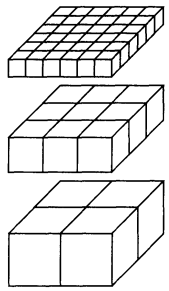


Figure 4 A 49er

Now tiling with 51 cubes is a bit trickier. Begin with a tiling of 20 cubes as above, recalling that 19 of the 20 are the same size. Look at the 6 faces of the cube and note that three are like the right-hand image in FIGURE 5 and three are like the left-hand one.

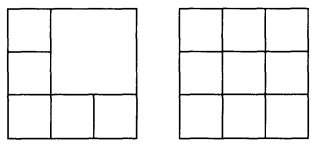


Figure 5 Faces of the 20 cube tiling

Pick two small cubes of the 20 cube tiling that share a face. Replace each of the two with a cube tiled with 20 in such a way that the shared face of each of the two looks like the right-hand picture in FIGURE 5. Now observe that 8 of the smallest cubes form a $2 \times 2 \times 2$ subcube, which can be replaced with a single cube. The result is a tiling with $20 + (20 - 1) + (20 - 1) - 8 + 1 = 51$ cubes.

The construction of a tiling with 54 cubes is similar. Recall our construction of a tiling with 38 cubes. Begin with a standard tiling using 8 cubes. Replace 2 cubes that share a common face with 38 cubes apiece so that the shared faces of the two are as

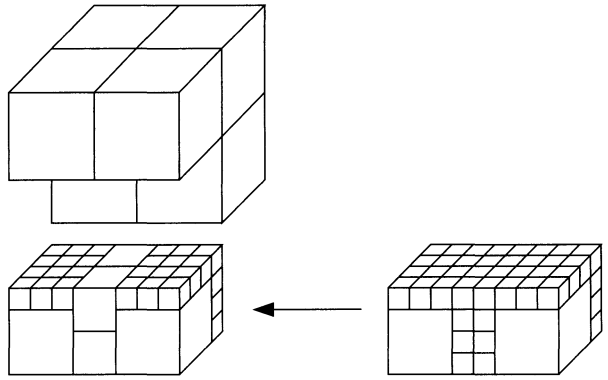


Figure 6 Tiling with 54 subcubes

in FIGURE 6. There are now four subcubes each consisting of 8 cubes. Each of these can be replaced by a single cube. This yields a tiling with $8 + (38 - 1) + (38 - 1) - 4(8 - 1) = 54$ cubes. We note that our constructions yield no tiling with 47 cubes, but that along with Fact 2, they yield tilings for all larger values of k.

Many interesting questions remain. What is the exact value of $f(n)$? Even $f(3)$ may be difficult. For $n = 2$ we know all values of k for which no tiling exists. For larger n one can easily see by counting corners that no tiling exists for $2 \leq k \leq 2^n - 1$. We conjecture that for $n \geq 3$ no tiling exists in dimension n for $2^n + 1 \leq k \leq 2^{n+1} - 2$. For $n = 3$, this conjecture can be proved with a lengthy examination of cases.

Acknowledgment. The referee has drawn our attention to an article by Hudelson [**1**], where most of our results have been anticipated, indeed with better bounds in four dimensions and higher.

REFERENCE

1. Matthew Hudelson, Dissecting d-cubes into smaller d-cubes, *Journal of Combinatorial Theory, Series A* **81** (1998), 190–200.

The Magic Mirror Property of the Cube Corner

JUAN A. ACEBRÓN
Departamento de Automática
Escuela Politécnica
Universidad de Alcalá de Henares
28871 Alcalá de Henares, Madrid, Spain
juan.acebron@uah.es

RENATO SPIGLER
Università di "Roma Tre"
00146 Roma, Italy
spigler@mat.uniroma3.it

We show that a ray of light, successively reflected from three mutually perpendicular planes in ordinary three-space, comes back in the same direction it came from. This

fact has applications in laser resonators, space measurements, and communications, but also in such simple devices as the retro-reflectors on bicycles and cars.

The so-called "cube corner," or also "corner cube," consists of three reflecting surfaces that are portions of concurrent faces of a cube. It can be realized in silica or other vitreous material, possibly coated with a mirror surface. If a ray hits any of the three surfaces, assuming that it does not hit an edge (in particular, the corner point), it turns out that, after three reflections (in general), it is reflected back in exactly the same direction of the original ray.

This result is well known within the community of optical physicists, since it has been applied in a number of laboratory laser devices [**5**]. A more dramatic application is to reflect laser rays from the Moon, where many such devices have been in place since the 1969 Apollo mission, which sent men to the Moon for the first time [**2, 4**]; among other things, the Earth-Moon distance can be measured by firing a laser beam from the Earth to the Moon, and measuring the travel time it takes for the beam to reflect back. This has allowed an estimate of the distance to within an accuracy of 3 cm.

Two other applications are worth mentioning. All retro-reflectors used in bicycles and cars are actually arrays of hundreds of cube corners. (The curious reader may find an interesting and exhaustive discussion of bicycle safety on the web [**1**], in particular, the use of cube-corner retro-reflectors.) A more hi-tech application of these devices is in an invention called "Smart Dust" [**3, 6**].

Smart Dust refers to an ensemble of very tiny devices—one millimeter or less—meant to be used in large numbers (so to represent a dust of particles), acting like "intelligent" dust motes. Each mote would contain very small sensors and possibly other little devices. Tiny micromachined cube-corner retro-reflectors located inside such motes are considered good candidates for passive transmitters in free-space optical communication systems, since they do not need to emit energy, but only reflect it. Smart Dust has potential applications in disparate areas from meteorology to medicine. A handful of such particles thrown on the back of a subject could be used to collect medical data; disseminating them in the air or sea would allow one to monitor the state of the environment as it evolves in time.

We establish the main useful property of the cube corner: It reflects any incoming ray back in the same direction it came from, usually after three successive reflections. We confine ourselves to geometric optics, ignoring, for instance, changes in the polarization of light. In fact, a number of issues may arise depending on the exact material and coating. These remain the subject of active investigation.

The reflective property of the cube corner Since our claim is about the directions of rays, it suffices to consider the direction cosines of the vectors that represent such rays; see FIGURE 1.

Let us assume, once and for all, that the incoming ray hits exactly one of the three faces of the cube corner, ruling out the pathological cases that it might hit one edge or the origin. In the real-world applications, almost none of the rays will be pathological.

Without loss of generality, we assume that the incoming ray, characterized by the direction cosines (λ, μ, ν), hits the face represented by the (x, y) plane. As with all other triples of direction cosines, we have $\lambda^2 + \mu^2 + \nu^2 = 1$. Let us also assume that the incoming ray is not perpendicular to this plane. After all, the property is observed quite simply in this case; hence $\nu^2 \neq 1$.

By the laws of optics, the reflected ray, whose direction cosines are $(\lambda_1, \mu_1, \nu_1)$, must be coplanar with both the previous ray and the normal to the plane (x, y). Therefore,

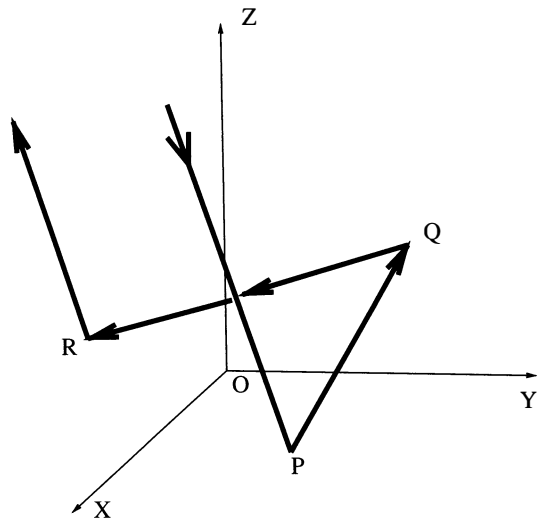


Figure 1 Three reflections of a light ray by a cube corner

$$\begin{vmatrix} \lambda & \mu & \nu \\ \lambda_1 & \mu_1 & \nu_1 \\ 0 & 0 & 1 \end{vmatrix} = 0,$$

from which we obtain that $\lambda\mu_1 = \lambda_1\mu$ and hence $\lambda_1 = r\lambda$ and $\mu_1 = r\mu$ for some number r. Moreover, $\lambda_1^2 + \mu_1^2 + \nu_1^2 = 1$.

On the other hand, the laws of optics also imply that incoming and reflected rays form the same angle with the normal to the $x - y$ plane, whose direction cosines are $(0, 0, 1)$, so that $(\lambda_1, \mu_1, \nu_1) \cdot (0, 0, 1) = (\lambda, \mu, \nu) \cdot (0, 0, 1)$, which means $\nu_1 = \nu$. The latter, along with the previous result, yields $(\lambda_1, \mu_1, \nu_1) = (r\lambda, r\mu, \nu)$, and then $r^2(\lambda^2 + \mu^2) + \nu^2 = 1$. But since $\lambda^2 + \mu^2 + \nu^2 = 1$, we conclude that $r^2 = 1$, and $r = 1$ or $r = -1$. The solution $r = 1$, however, is ruled out by the fact that the reflected ray cannot be parallel to the incoming ray, unless the latter is perpendicular to the plane (x, y), a case that we can exclude. Therefore, $r = -1$ and

$$(\lambda_1, \mu_1, \nu_1) = (-\lambda, -\mu, \nu).$$

We proceed similarly with the other reflections. After a ray reflects off a given coordinate plane, the cosine of the angle with the normal to that plane will be unchanged, while the other two direction cosines will change sign. For instance, if the ray with direction cosines $(\lambda_1, \mu_1, \nu_1)$ next hits the $x - z$ plane and then the $y - z$ plane, the successively reflected rays will have direction cosines

$$(\lambda_2, \mu_2, \nu_2) = (-\lambda_1, \mu_1, -\nu_1) = (\lambda, -\mu, -\nu),$$

and

$$(\lambda_3, \mu_3, \nu_3) = (\lambda_2, -\mu_2, -\nu_2) = (\lambda, \mu, \nu),$$

respectively. In the case of a ray hitting first the $y - z$ plane and then the $x - z$ plane, we have

$$(\lambda_2, \mu_2, \nu_2) = (\lambda_1, -\mu_1, -\nu_1) = (-\lambda, \mu, -\nu),$$

and then

$$(\lambda_3, \mu_3, \nu_3) = (-\lambda_2, \mu_2, -\nu_2) = (\lambda, \mu, \nu).$$

The final result will be the same. This shows that the ray emerging after three reflections is parallel to the original ray.

Finally, we consider the special occurrence of a ray entering the cube corner parallel to one of its faces. This case can be viewed as if the reflections take place on a billiard table, with a ball hitting successively two concurrent sides of the table; the answer is the same.

Conclusion We have shown that (almost) every ray emerging from a cube corner system after reflecting off its three plane walls has the same direction as the incoming ray that produced it. Thanks to clever applications of this magic mirror property, our travel is safer and we can measure the distance all the way to the Moon. If you ever encounter Smart Dust, remember the reflective property behind its design.

REFERENCES

1. J. S. Allen, About bicycle reflectors contents, <http://www.bikexprt.com/bicycle/reflectors/>, last revised March 14, 2003, and all links, last revised April 27, 2002.
2. J. E. Faller and E. J. Wampler, The lunar laser reflector, *Scientific American*, **38**, March 1970, 38–50.
3. J. M. Kahn, R. H. Katz, and K. S. J. Pister, Emerging challenges: mobile networking for "Smart Dust," *J. Comm. and Networks* **2**:3 (2000), 188–196.
4. M. S. Scholl, Ray trace through a corner-cube retroflector with complex reflection coefficients, *J. Opt. Soc. Amer.* A **12** (1995), 1589–1592.
5. Chun-Ching Shih, Depolarization effect in a resonator with corner-cube reflectors, *J. Opt. Soc. Amer.* A **13** (1996), 1378–1384.
6. L. Zhou, J. M. Kahn, and K. S. J. Pister, Corner-cube retro-reflectors based on structure-assisted assembly for free-space optical communication, *IEEE J. Microelectromech. Syst.* **12**:3 (2003), 233–242.

Spherical Triangles of Area π and Isosceles Tetrahedra

JEFF BROOKS
JOHN STRANTZEN
La Trobe University
Victoria 3086, Australia
J.Brooks@latrobe.edu.au
J.Strantzen@latrobe.edu.au

There is a beautiful theorem in spherical geometry that is not well known, and that doesn't appear in most texts on the subject.

The theorem says that for any spherical triangle of area π on the unit sphere, four congruent copies of it tile the sphere; that is, the copies can be positioned so that any two triangles meet at an edge, with vertices meeting vertices, and the union of these four triangles is the sphere [**1**; **3**, p. 44; **6**, p. 94]. The configuration is shown in FIGURE 1, which may aid readers in guessing the proof.

What appears to be less known (in fact, the authors can find no reference to it) is that the four vertices on the sphere determined by this tiling form the vertices of an

isosceles tetrahedron (opposite edges of the tetrahedron are equal) [**2**]. Hence, every such tiling of the sphere is obtained as the projection from the center of an inscribed isosceles tetrahedron.

Background We introduce some preliminary definitions and results that the reader may already know, in which case it is possible to skip ahead. Given a point P on the unit sphere, the intersection of the line joining the center of the sphere to P meets the sphere at a diametrically opposite point P'. The pair P and P' are called *antipodal points*. We define a *line* on the sphere to be a great circle, that is, the intersection of the sphere with a plane containing the center of the sphere. The complement of a line is two disjoint open hemispheres.

Given two distinct nonantipodal points, P and Q, there is a unique line containing them. This line is the intersection of the sphere with the plane containing P and Q and the center of the sphere. We denote it by lPQ. We let $\overline{PQ}$ denote the smaller of the arcs on the line that connects P to Q. It follows that length of $\overline{PQ}$ is less than π. We denote the fact that two arcs $\overline{PQ}$ and $\overline{RS}$ have equal length by $\overline{PQ} = \overline{RS}$, blurring the distinction between a segment and its measurement.

Given three distinct noncollinear points A, B, C, no two of which are antipodal, we define the *spherical triangle* $\triangle ABC$ to be the union of the arcs $\overline{AB}$, $\overline{BC}$, and $\overline{CA}$. We call $\overline{AB}$ the *edge* of the triangle joining vertex A to vertex B, similarly for $\overline{BC}$ and $\overline{CA}$. Such a triangle necessarily lies in an open hemisphere. Clearly each edge of $\triangle ABC$ determines an open hemisphere containing the remaining vertex. The intersection of these three open hemispheres is the interior of $\triangle ABC$. The area of $\triangle ABC$ is defined to be the area of its interior. It should be intuitive as to what is meant by the three angles of $\triangle ABC$, and we denote by $\angle CAB$, $\angle ABC$, and $\angle BCA$ the measure in radians of these three angles. The main result that we use to prove our theorem is a remarkable theorem attributed to Girard. Girard's theorem says that

$$\angle CAB + \angle ABC + \angle BCA - \pi = \text{Area}(\triangle ABC)$$

Weeks [**8**] gives an elegant proof of this result.

Finally, we need to say what we mean by two triangles being congruent. We adopt the Euclidean notion, which says that two triangles are congruent if there is an isometry between the triangles. The isometries of the sphere are of three types, a reflection in a line, a product of two reflections (this is equivalent to a rotation about an axis through the antipodal points where the lines meet), and a reflection followed by a rotation perpendicular to the line of reflection (a glide reflection) [**5**].

Reflections and glide reflections do not preserve orientation, which we wish to do in this discussion. Hence, for us two triangles are congruent if one can be rotated onto the other, see [**7**]. The usual theorems for congruence of spherical triangles—SSS, SAS, ASA, and AAA—will determine uniqueness up to isometry, so we must show that the copies of our triangle are all rotations of it.

Proving the theorem To demonstrate our result, let $\triangle ABC$ be a spherical triangle of area π. Choose an edge (say $\overline{AB}$), let M be the midpoint of that edge, as in FIGURE 1.

From our definition of a triangle it follows that $\overline{MC}\backslash\{M, C\}$ lies in the interior of $\triangle ABC$. Rotate $\triangle ABC$ by π about the axis through M and its antipodal point M'. Under this rotation A and B interchange and C maps to a fourth distinct point D. It is clear that C and D are distinct, since the length of $\overline{MC}$ is less than π. Also C, M, and D lie on the line determined by M, M', and C.

It is not difficult to see that $\overline{MC}$ has a length greater than $\pi/2$ otherwise $\triangle ABC$ would fit inside a quadrant (as the length of $\overline{AB}$ is less than π) and hence have area

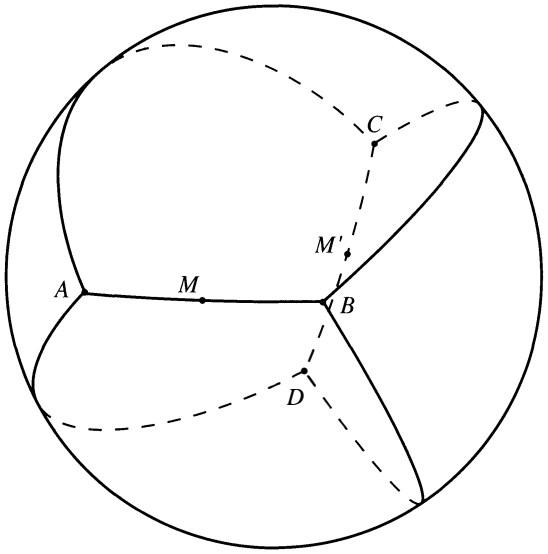


Figure 1

strictly less than π. Hence, M' is the midpoint of $\overline{CD}$. The points C, M, and D lie on the line determined by M, M', and C and $\overline{M'D} = \overline{M'C}$. Also M, M', and A lie on line lAB, with A and B lying in distinct open hemispheres determined by line lCD.

Consider the four triangles $\triangle ABC$, $\triangle BAD$, $\triangle CDA$, and $\triangle DCB$. Clearly any two meet at a common edge with vertices meeting vertices. If we partition $\triangle CDA$ into $\triangle CM'A$ and $\triangle AM'D$, and $\triangle DCB$ into $\triangle DM'B$ and $\triangle BM'C$, we see that the three triangles $\triangle CM'A$, $\triangle ABC$, and $\triangle BM'C$ tile the closed hemisphere determined by line AB and C. Similarly $\triangle AM'D$, $\triangle BAD$, and $\triangle DM'B$ tile the closed hemisphere determined by line lAB and D. It follows that $\triangle ABC$, $\triangle BAD$, $\triangle CDA$, and $\triangle DCB$ tile the sphere.

We have $\triangle ABC$ congruent to $\triangle BAD$, as they are rotations of each other by π about the axis through M, M'. Also $\triangle CDA$ is congruent to $\triangle DCB$ for the same reason. By Girard's theorem, we have $\angle CAB + \angle ABC + \angle BCA = 2\pi$ (since Area $\triangle ABC = \pi$). Also, $\angle CAB + \angle DAC + \angle BAD = 2\pi$ (sum of angles around vertex A). But $\angle BAD = \angle ABC$ ($\triangle ABC$ is congruent to $\triangle BAD$) hence $\angle DAC = \angle BCA$.

It now follows that if we rotate $\triangle ABC$ by π about the midpoint N of $\overline{AC}$, then A and C change places and B maps to D ($\overline{DA} = \overline{CB}$ as $\triangle CDA$ is congruent to $\triangle DCB$). Thus $\triangle ABC$ is congruent to $\triangle CDA$ and so the four triangles are congruent. In particular $\overline{AB} = \overline{CD}$, $\overline{BC} = \overline{AD}$ and $\overline{AC} = \overline{BD}$, which means that the tetrahedron formed by the vertices $ABCD$ is isosceles.

Now the great circle through M, M', and the midpoint N of AC has $\overline{MN} = \overline{M'N}$ ($\triangle ABC$ is congruent to $\triangle CDA$), and as $\overline{MN} + \overline{M'N} = \pi$, it follows that $\overline{MN} = \pi/2$. We therefore deduce that the medial triangle of $\triangle ABC$ is an octant [**1, 4**].

Constructions This proof gives a method for drawing such triangles on a sphere: Mark two antipodal points on the sphere. Center congruent arcs of length less than π on these points in such a way that the arcs do not lie on the same great circle. Connect the end points of the arcs in the appropriate way to obtain the tiling. Varying the length of the arcs and the angle they make with each other gives all possible tilings.

To construct an isosceles tetrahedron, note that its faces must be four congruent acute angled triangles. Take any acute angled triangle ABC and rotate it by π about an axis through the midpoint of $\overline{AB}$ perpendicular to the plane of the triangle. Let D be

the image of C. Then $\overline{AB} < \overline{CD}$. Now rotate $\triangle ABD$ about $\overline{AB}$ so that the image of D is D' and $\overline{AB} = \overline{CD'}$. It follows that tetrahedron $ABCD'$ is isosceles.

Acknowledgment. The authors would like to thank Paul Pontikis for the typing, Jeanette Varrenti and Marcel Jackson for the electronic picture.

REFERENCES

1. Grant Cairns, Margaret McIntyre, and John Strantzen, Geometric proofs of some recent results of Yang Lu, this MAGAZINE **66**:4 (October 1993), 263–265.
2. N. A. Court, *Modern Pure Solid Geometry*, Chelsea Publishing Co., New York, 1964.
3. H. L. Davies, Packings of spherical triangles, *Proceedings of The Colloquium on Convexity*, Copenhagen, August 1965, pp. 42–51.
4. W. J. M'Clelland and T. Preston, *A Treatise on Spherical Trigonometry with Applications to Spherical Geometry Part I*, Macmillan Publishing Co., New York, 1907, *and Part II*, 1909.
5. Patrick J. Ryan, *Euclidean and Non-Euclidean Geometry, An Analytic Approach*, Cambridge University Press, Cambridge, London, New York, New Rochelle, Melbourne, Sydney, 1986.
6. D. M. Y. Sommerville, Division of space by congruent triangles and tetrahedra, *Proceedings of The Royal Society of Edinburgh*, **43** (1923) pp. 85–116.
7. I. Todhunter and J. G Leatham, *Spherical Trigonometry*, Macmillan and Co. Limited, St. Martin's Street, London, 1943.
8. Jeffrey R. Weeks, *The Shape of Space*, 2nd ed., Marcel Decker, Inc., New York, Basel, 2002.

A Butterfly Theorem for Quadrilaterals

SIDNEY KUNG
University of North Florida
Jacksonville, FL 32224
sidneykung@yahoo.com

One of the more appealing theorems in plane geometry is the butterfly theorem:

BUTTERFLY THEOREM. *Through the midpoint I of a chord AC of a circle, two other chords EF and HG are drawn. If EG and HF intersect AC at M and N, respectively, then $IM = IN$.*

Since 1815, when this theorem appeared as a proposed problem in the *Gentleman's Diary* (1815, pp. 39–40; see also [**1**, p. 195]) it has attracted many lovers of mathematics, some of whom have produced simple and elegant proofs, while others devised various generalizations. In a delightful and well-documented article, Bankoff [**1**] discusses the butterfly theorem for circles and some variants. In particular, on p. 207 one finds an "area method" applied to prove that if I is a point anywhere on the chord AC (as in FIGURE 1), $IA = a$, $IC = c$, $IM = m$, $IN = n$, then:

$$\frac{1}{m} - \frac{1}{n} = \frac{1}{a} - \frac{1}{c} \tag{1}$$

In this note, we give a similar proof of a butterfly theorem for quadrilaterals. Our proof depends primarily upon the following properties for areas of triangles:

P1 If K is the intersection of the lines XY and UV, $V \neq K$ (FIGURE 2a), then

$$\frac{\mathcal{A}(UXY)}{\mathcal{A}(VXY)} = \frac{UK}{VK}, \quad \text{where } \mathcal{A}(UXY) \text{ denotes the area of triangle } UXY.$$

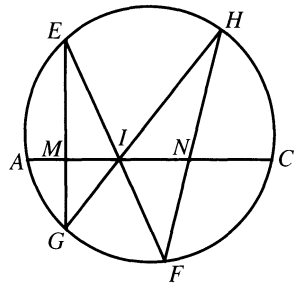
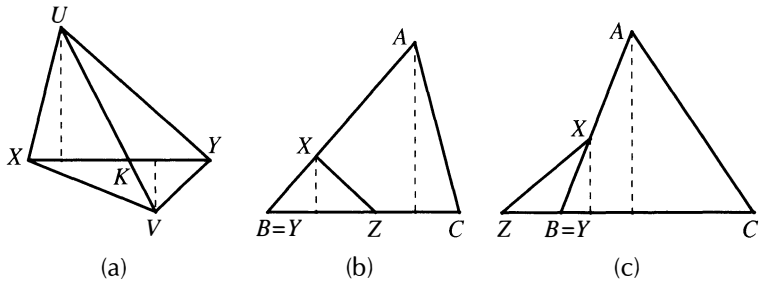


Figure 1 A variant of the butterfly theorem for circles

P2 Given triangles ABC and XYZ, suppose that, as in FIGURE 2b, 2c, we have

$$\angle ABC = \angle XYZ \quad \text{or} \quad \angle ABC + \angle XYZ = 180^\circ, \quad \text{then} \quad \frac{\mathcal{A}(ABC)}{\mathcal{A}(XYZ)} = \frac{AB \cdot BC}{XY \cdot YZ}.$$

For a proof of P1, consider FIGURE 2a. We see that the two triangles $\triangle UXY$ and $\triangle VXY$ share base XY. Furthermore, their altitudes are in the same proportion as UK/VK. Hence, so are their areas. In a similar manner we can easily establish P2.



(a) (b) (c)

Figure 2 Proportional areas in triangles

BUTTERFLY THEOREM FOR QUADRILATERALS. *Through the intersection I of the diagonals AC, BD of a convex quadrilateral $ABCD$, draw two lines EF and HG that meet the sides of $ABCD$ at E, F, G, H. If $M = EG \cap AC$, $N = HF \cap AC$, then*

$$\frac{AM}{IM} \cdot \frac{IN}{CN} = \frac{IA}{IC}$$

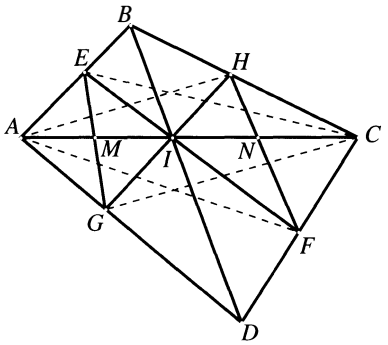


Figure 3 A butterfly theorem for quadrilaterals

Proof. Refer to FIGURE 3. We find that there are twelve pairs of triangles, each pair of which has a common side or a common angle (or two congruent angles one from each triangle of the pair). Applying P1 and P2 on these triangles we have

$$\frac{AM}{IM}\cdot\frac{IN}{CN}=\frac{\mathcal{A}(AEG)}{\mathcal{A}(IEG)}\cdot\frac{\mathcal{A}(IFH)}{\mathcal{A}(CHF)} \qquad \text{(P1)}$$

$$=\frac{\mathcal{A}(IFH)}{\mathcal{A}(IEG)}\cdot\frac{\mathcal{A}(CBD)}{\mathcal{A}(CHF)}\cdot\frac{\mathcal{A}(ABD)}{\mathcal{A}(CBD)}\cdot\frac{\mathcal{A}(AEG)}{\mathcal{A}(ABD)}$$

$$=\frac{IF\cdot IH}{IE\cdot IG}\cdot\frac{CD\cdot CB}{CF\cdot CH}\cdot\frac{IA}{IC}\cdot\frac{AE\cdot AG}{AB\cdot AD} \qquad \text{(P1, P2)}$$

$$=\frac{\mathcal{A}(FAC)}{\mathcal{A}(EAC)}\cdot\frac{\mathcal{A}(HAC)}{\mathcal{A}(GAC)}\cdot\frac{\mathcal{A}(DAC)}{\mathcal{A}(FAC)}\cdot\frac{\mathcal{A}(BAC)}{\mathcal{A}(HAC)}\cdot\frac{IA}{IC}\cdot\frac{\mathcal{A}(EAC)}{\mathcal{A}(BAC)}\cdot\frac{\mathcal{A}(GAC)}{\mathcal{A}(DAC)}$$

$$=\frac{IA}{IC}. \qquad \text{(P1)}\ \blacksquare$$

Thus, if we let $IA=a$, $IC=c$, $IM=m$, $IN=n$, we get

$$\frac{a-m}{m}\cdot\frac{n}{c-n}=\frac{a}{c},$$

which simplifies to

$$\frac{1}{m}-\frac{1}{n}=\frac{1}{a}-\frac{1}{c}.$$

Hence a butterfly inscribed in a quadrilateral satisfies the same relation (1) as a butterfly inscribed in a circle. Equivalently, the conclusion of the theorem indicates that the ratio of the ratios, $(AM/IM)/(CN/IN)$, is the same as the ratio IA/IC, or that the harmonic mean of IC and IM equals the harmonic mean of IA and IN. In either case, if $IC=IA$, we have $IM=IN$ thereby the analog of the usual butterfly theorem for quadrilaterals.

Acknowledgment. The author would like to thank the referees for their helpful suggestions, and Joseph Kung for preparation of the article.

REFERENCE

1. Leon Bankoff, The metamorphosis of the butterfly problem, this MAGAZINE **60** (1987), 195–210.

Row Rank Equals Column Rank

WILLIAM P. WARDLAW
U. S. Naval Academy
Annapolis, MD 21402-5000
wpw@usna.edu

Dedicated to George Mackiw, a good friend and an excellent mathematical expositor.

The purpose of this note is to present a short (perhaps shortest?) proof that the row rank of a matrix is equal to its column rank. The proof is elementary and accessible to students in a beginning linear algebra course. It requires only the definition of

matrix multiplication and the fact that a minimal spanning set is a basis. It differs in approach from proofs given in textbooks as well as from some interesting proofs in MAA journals [**1, 2**]. And, unlike the latter, this proof is valid over any field of scalars.

But first, recall that if the $m \times n$ matrix $A = BC$ is a product of the $m \times r$ matrix B and the $r \times n$ matrix C, then it follows from the definition of matrix multiplication that the ith row of A is a linear combination of the r rows of C with coefficients from the ith row of B, and the jth column of A is a linear combination of the r columns of B with coefficients from the jth column of C. (If you have trouble understanding this or the next paragraph, you should construct several examples of small matrix products, say, a 3×2 times a 2×3 matrix, etc., with small integer as well as symbolic entries.)

On the other hand, if any collection of r row vectors $\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_r$, spans the row space of A, an $r \times n$ matrix C can be formed by taking these vectors as its rows. Then the ith row of A is a linear combination of the rows of C, say $\overline{a}_i = b_{i1}\overline{c}_1 + b_{i2}\overline{c}_2 + \cdots + b_{ir}\overline{c}_r$. This means $A = BC$, where $B = (b_{ij})$ is the $m \times r$ matrix whose ith row, $\overline{b} = (b_{i1}, b_{i2}, \ldots, b_{ir})$, is formed from the coefficients giving the ith row of A as a linear combination of the r rows of C.

Similarly, if any r column vectors span the column space of A, and B is the $m \times r$ matrix formed by these columns, then the $r \times n$ matrix C formed from the appropriate coefficients satisfies $A = BC$. Now the four sentence proof.

THEOREM. *If A is an $m \times n$ matrix, then the row rank of A is equal to the column rank of A.*

Proof. If $A = 0$, then the row and column rank of A are both 0; otherwise, let r be the smallest positive integer such that there is an $m \times r$ matrix B and an $r \times n$ matrix C satisfying $A = BC$. Thus the r rows of C form a minimal spanning set of the row space of A and the r columns of B form a minimal spanning set of the column space of A. Hence, row and column ranks are both r. ∎

Several other properties of the rank of a matrix over a field are also very easy to obtain. The factorizations $A = I_m A = AI_n$ show that $r \leq m$ and $r \leq n$, which proves that the rank of A is less than or equal to the number of rows and the number of columns of A. Since $A = BC$ implies $A^T = C^T B^T$, the transpose clearly has the same rank as the original matrix. Since $A = BC$ and $D = EF$ implies $AD = B(CD) = (AE)F$, the rank of AD must be less than or equal to the rank of A and to the rank of D.

These concepts suggest the following definition [**5**, p. 123]:

DEFINITION. Let R be a commutative ring with identity and let A be an $m \times n$ matrix over R. Then the *spanning rank of* A is 0 if $A = 0$ and otherwise is the smallest positive integer r such that there is an $m \times r$ matrix B and an $r \times n$ matrix C satisfying $A = BC$.

This definition is one way of extending the notion of rank to matrices over commutative rings. Even if the ring has no identity, it can be embedded in a ring with identity so that the definition can be used. Care must be taken in considering rank over commutative rings, because several different extensions of the definitions over a field can give different results over rings, even though they all give the standard concept of rank over a field. Nonetheless, if the above definition is used, matrices over rings *automatically* have row rank equal to column rank, have rank less than or equal to the number of rows and the number of columns, the rank of the transpose is equal to the rank of the matrix, and the rank of a product is less than or equal to the rank of either factor.

Another application of the spanning rank, first used by the author in a problem [**3**] and later a Note [**5**] in the MAGAZINE, is the proof that a matrix over a commutative

ring with spanning rank r satisfies a polynomial equation of degree at most $r + 1$. For if $A = BC$ is an $n \times n$ matrix of spanning rank r, then $D = CB$ is an $r \times r$ matrix with characteristic polynomial $f_D(x) = \det(xI - D)$ of degree r and $f_D(D) = 0$ follows from the Cayley-Hamilton Theorem. (The author has shown [**4**] that the Cayley-Hamilton Theorem holds for matrices over commutative rings.) Thus there is a polynomial $m(x)$ of smallest positive degree such that $m(D) = 0$. Then $p(x) = xm(x)$ is a polynomial of degree $\leq r + 1$ such that $p(A) = Am(A) = BCm(BC) = Bm(CB)C = Bm(D)C = 0$.

REFERENCES

1. H. Liebeck, A proof of the equality of column and row rank of a matrix, *Amer. Math. Monthly* **73** (1966), 1114.
2. G. Mackiw, A note on the equality of column and row rank of a matrix, this MAGAZINE **68** (1995), 285–286.
3. W. Wardlaw, problem **1179**, this MAGAZINE **56** (1983), 326, and solution **1179**, this MAGAZINE **57** (1984), 303.
4. ———, A transfer device for matrix theorems, this MAGAZINE **59** (1986), 30–33.
5. ———, Minimum and characteristic polynomials of low-rank matrices, this MAGAZINE **68** (1995), 122–127.

A Modern Approach to a Medieval Problem

AWANI KUMAR, Director
Lucknow Zoological Garden
Lucknow 226001 INDIA
awanieva@eth.net

The following problem from *Lilavati* [**1**], a mathematical treatise written by Bhaskaracharya, a 12th-century Indian mathematician and astronomer, deserves a modern approach:

> A snake's hole is at the foot of pillar, nine cubits high, and a peacock is perched on its summit. Seeing a snake at the distance of thrice the pillar gliding towards his hole, he pounces obliquely upon him. Say quickly at how many cubits from the snake's hole they meet, both proceeding an equal distance.

Since both proceed an equal distance, it is reasonable to assume that their speeds are equal. Readers are invited to solve this problem before proceeding.

Assuming that the peacock flies along the hypotenuse of a right-angled triangle and knows the Pythagorean Theorem, it will grab the snake at a distance of 12 cubits from the pillar. Practically, however, such a thing does not happen. Why should a peacock know—*a priori*—to fly along the hypotenuse of a right-angled triangle having a base of 12 cubits? A more peacock-like behavior would be to keep an eagle eye on the snake and change its direction at every instant, always aiming toward the snake.

This type of pursuit problem has a history of over five hundred years. However, this particular problem is a bit different from most. Instead of the prey running away from the predator, here prey and the predator are moving toward each other. Even so, the results are startling.

Although the reader may have seen similar problems, I offer a general analysis. We assume that the snake and the peacock move at different, but constant, speeds: the snake in a straight line toward its hole and the peacock along a curve, changing its direction at every instant so as to be flying directly toward the snake.

Let v be the speed of the peacock, and u be the speed of the snake. The snake is at the origin $(0, 0)$ and the peacock is perched on the pillar at (x_0, y_0). They start moving at time $t = 0$ and are at $S(ut, 0)$ and $P(x, y)$ respectively after time t (as in FIGURE 1). Let θ be the angle between the x-axis and the line connecting peacock and snake. Readers may wish to solve the problem themselves, using this notation, before continuing.

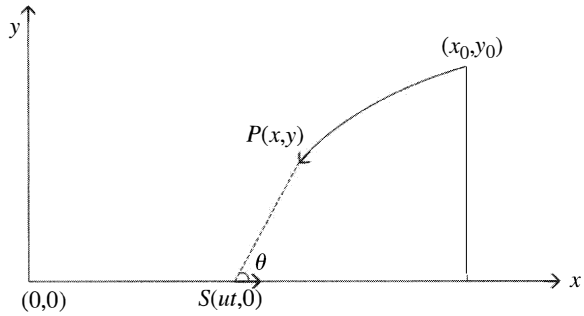


Figure 1 Notation for the pursuit problem: θ is the angle between the x-axis and the line joining the snake and the peacock

Differential equations for the peacock's path Since the horizontal component of the peacock's velocity is $v\cos\theta$ towards the snake, the rate of change of the horizontal distance between them is $-(u + v\cos\theta)$. Similarly, the component of snake's velocity towards the peacock is $u\cos\theta$ and so the rate of change of the distance between them is $-(v + u\cos\theta)$. The negative signs indicate that the distances are decreasing.

Initially, the horizontal distance between them is x_0 and the distance between them is $\sqrt{x_0^2 + y_0^2}$. They will meet after time T if the following conditions are satisfied.

$$\sqrt{x_0^2 + y_0^2} = \int_0^T (v + u\cos\theta)\,dt \quad \text{and} \quad x_0 = \int_0^T (u + v\cos\theta)\,dt \tag{1}$$

We find the meeting time by eliminating $\int_0^T \cos\theta\,dt$ from (1) to get

$$T = \frac{\sqrt{x_0^2 + y_0^2} - kx_0}{v(1 - k^2)}, \quad \text{where} \quad k = u/v. \tag{2}$$

Equation (2) implies that if $k \to 1$ then $T \to \infty$. The startling result is that, however small the pillar may be, if the speeds of the peacock and snake are equal, the animals will never meet! We rarely find such a counter-intuitive result in mathematics. Let us look into it in more detail. The key is to turn our assumptions into differential equations. The tangent line to the curve of pursuit at $P(x, y)$ must pass through the point $S(ut, 0)$. Looking at its slope, we have

$$dy/dx = y/(x - ut) \quad \text{or} \quad x - ut = y\,dx/dy. \tag{3}$$

We will eliminate t to find an ordinary differential equation in x and y. As a first step, let s be the distance covered by the peacock in time t, so that $s = vt$. Substitution into (3) gives

$$y\frac{dx}{dy} = x - ks. \tag{4}$$

For the next step, it is fruitful to treat y as the independent variable, a trick common in solving ordinary differential equations. The distance s is also the length of the pursuit curve from (x_0, y_0) to (x, y). Therefore, using the arc-length formula, we get

$$s = \int_y^{y_0} \sqrt{1 + (dx/dy)^2}\, dy \quad \text{or} \quad ds/dy = -\sqrt{1 + (dx/dy)^2}. \tag{5}$$

Differentiating (4) with respect to y gives,

$$y\frac{d^2x}{dy^2} = -k\frac{ds}{dy}, \quad \text{and thus} \quad y\frac{d^2x}{dy^2} = k\sqrt{1 + (dx/dy)^2}.$$

This second order differential equation can be reduced to first order by another standard trick, namely, putting p for dx/dy. Therefore, $y\, dp/dy = k\sqrt{1 + p^2}$ or, separating variables,

$$\frac{dp}{\sqrt{1 + p^2}} = k\frac{dy}{y}. \tag{6}$$

At $t = 0$, $x = x_0$, $y = y_0$ and $p = x_0/y_0$. Substituting $p = \tan\alpha$ (where $\alpha = \pi/2 - \theta$), we get $dp = \sec^2\alpha\, d\alpha$ and $dp/\sqrt{1 + p^2} = \sec\alpha\, d\alpha$. Therefore, integrating (6) and applying the initial condition gives

$$p + \sqrt{1 + p^2} = c_1(y/y_0)^k, \tag{7}$$

where $c_1 = x_0/y_0 + \sqrt{1 + (x_0/y_0)^2}$. Using lots of algebra, (7) simplifies to

$$p = \frac{dx}{dy} = \frac{1}{2}\left[c_1(y/y_0)^k - \frac{1}{c_1}(y_0/y)^k\right] \tag{8}$$

Let us investigate the position of the peacock when $p = 0$, which means that the peacock is exactly above the snake. This situation distinguishes the cases where the peacock catches the snake while always flying away from the pillar from those where it reverses direction. Putting $p = 0$ in (7) gives $c_1(y/y_0)^k = 1$ or,

$$y = y_0(1/c_1)^{1/k}. \tag{9}$$

This gives the relationship between the position of the peacock, its initial positions and k. In the given problem, $k = 1$ and $c_1 = 3 + \sqrt{10} \approx 6.16$ cubits. So, from (9), the peacock is exactly above the snake at $y = 1.46$ cubits. Before this position, the peacock was moving away from the pillar and after this, it will be moving toward the pillar, while always heading for the snake. Whatever the value of k, (9) shows that the peacock always reverses its direction before catching the snake.

This is a surprise: However fast the peacock may fly and however small the pillar may be, the peacock can never catch the snake before reversing its direction! Mathematics, like nature, is full of surprises.

At what angle does the peacock catch the snake? Readers are challenged to find it from the given analysis.

Catching the snake We have seen earlier that the peacock and snake do not meet when $k = 1$. Let us confirm this using our solution. We can also determine the critical value of k that allows the peacock to catch the snake. When $k = 1$, integrating (8) gives

$$x = x_0 + A_1 \ln\left(\frac{y_0}{y}\right) - \frac{y_0^2 - y^2}{8A_1}, \tag{10}$$

where $A_1 = y_0/(2c_1)$. Let r be the separation between the peacock and the snake. According to our analysis,

$$r = \sqrt{(x - ut)^2 + y^2} = \sqrt{y^2(1 + (dx/dy)^2)}$$
$$= y\sqrt{1 + \frac{1}{4}\left(c_1\frac{y}{y_0} - \frac{1}{c_1}\frac{y_0}{y}\right)^2} = A_1 + \frac{y^2}{4A_1}. \tag{11}$$

Since $y^2/4A_1 > 0$, this distance is greater than A_1 cubits. In the given problem with a pillar nine cubits high, the peacock cannot get closer than 0.73 cubits. What a narrow escape for the snake!

When $k \neq 1$, integrating (8) gives

$$x = x_0 - \frac{y_0}{2}\left[\frac{1}{c_1(1-k)}\left\{\left(\frac{y}{y_0}\right)^{1-k} - 1\right\} - \frac{c_1}{1+k}\left\{\left(\frac{y}{y_0}\right)^{1+k} - 1\right\}\right]. \tag{12}$$

FIGURE 2 shows the path of the peacock for various values of k. If the peacock does not wish to go hungry, then it will have to maintain a greater speed than the snake. To investigate the critical situation where the snake is caught just as it enters its lair, we substitute $x = x_0$ and $y = 0$ into (12) and find

$$k_{\text{critical}} = \frac{c_1^2 - 1}{c_1^2 + 1}.$$

If $k > k_{\text{critical}}$ (here $k_{\text{critical}} \approx 0.95$), then the snake will safely reach its hole; otherwise, the peacock will have a nice dinner!

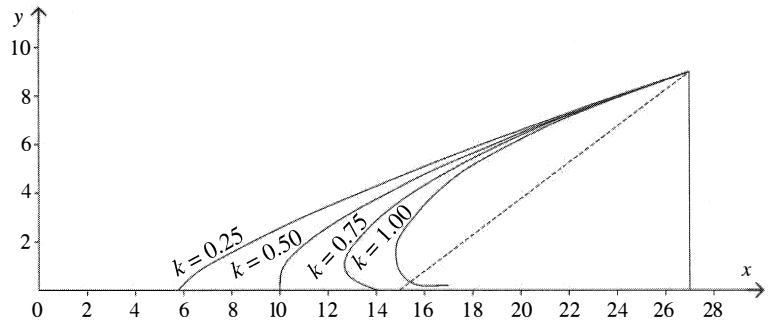
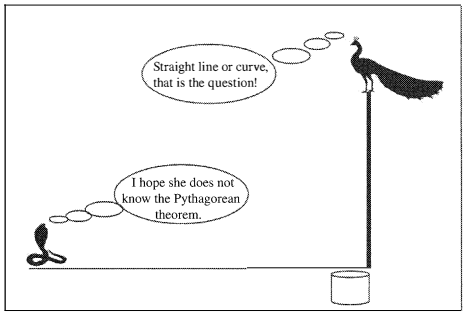


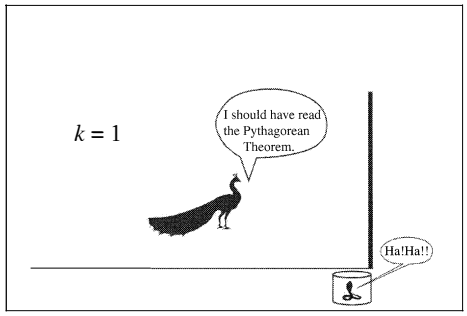
Figure 2 The flight of the peacock

This particular story about peacocks pursuing snakes may be new, but the mathematics behind it is not. Knaust [**2**] credits Leonardo da Vinci (1452–1519) with first studying pursuit curves. Pluckette [**3**] and Neville [**4**] have also pondered them. Many textbooks on differential equations, such as those by Simmons [**5**] cover pursuit problems. Crough [**6**] gives some information about their history. None of these authors solve the exact same problem of the peacock and the snake.

However, I found that my efforts were not completely original. In the Advanced Problems section of the August–September 1941 issue of the *American Mathematical Monthly*, the problem is given for $k = 2$ and is solved by H. A. Luther. It is noted there that the problem appears on p. 295 of Fine's *Calculus*, and on p. 332 of Osgood's *Advanced Calculus*. It also appears as Example 3 on p. 138 of *Elements of Ordinary*

Differential Equations by Golomb and Shanks and probably in many other similar textbooks. But what must be the earliest published solution is noted by Arthur Bernhart in *Scripta Mathematica*, **20**, p. 127 : Pierre Bourguer (1698–1758) in a 1732 memoir *Upon New Curves Which May be Called Lines of Pursuit* [*Lignes de poursuite, Memoires de L'Academie Royale des Sciences* (1732), pp. 1–14] derives the very same equation I have. My work has been anticipated by 238 years! Even after 500 years, pursuit problems have not lost their charm and deserve to be pursued!





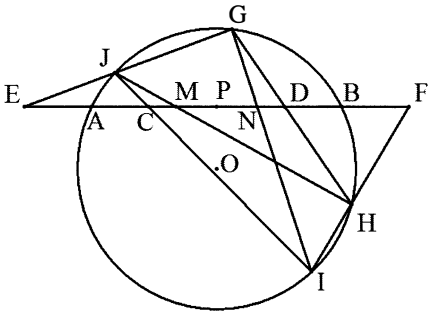
REFERENCES

1. Bhaskaracharya, *Lilavati*, The Book Company Ltd., Calcutta, India, 1927.
2. Helmut Knaust, Lab on pursuit curves, www.math.utep.edu/classes/3226/lab2b/lab2b.html
3. C. C. Pluckette, The curve of pursuit, *Math. Gaz.* **37** (1953), 256–260.
4. E. H. Neville, The curve of pursuit, *Math. Gaz.* **15** (1930), 436.
5. Simmons, *Differential Equations: Applications and Historical Notes*, McGraw Hill Education, Europe, 2nd ed., 1961, pp. 68–70.
6. Gerald Crough, A pursuit problem, this MAGAZINE **24** (Mar–Apr. 1971), 94–97.

40 Years Ago in the MAGAZINE

Readers who enjoyed Kung's note,"A Butterfly Theorem for Quadrilaterals," might enjoy recalling Klamkin's "An Extension of the Butterfly Problem," **38** (1965), 206–208. His main result can be summarized as follows:

Let AB be an arbitrary chord of a circle with midpoint P, and let chords JH and GI intersect AB at M and N respectively. If $MP = PN$, then if AB intersects JI at C and GH at D we have $CP = PD$. Furthermore, if line segments AB, GJ, and IH are extended so that AB intersects GJ and IH at E and F respectively, then $EP = PF$.



PROBLEMS

ELGIN H. JOHNSTON, *Editor*
Iowa State University

Assistant Editors: RĂZVAN GELCA, Texas Tech University; ROBERT GREGORAC, Iowa State University; GERALD HEUER, Concordia College; VANIA MASCIONI, Ball State University; BYRON WALDEN, Santa Clara University; PAUL ZEITZ, The University of San Francisco

Proposals

To be considered for publication, solutions should be received by March 1, 2006.

1726. *Proposed by Jerry Metzger, University of North Dakota, Grand Forks, ND.*

Let a and j be positive integers with $a \geq 2$. Show that there is a positive integer n such that $a^n \equiv -j \pmod{a^j + 1}$ if and only if $j = a^k$ for some $k \geq 0$.

1727. *Proposed by Jody M. Lockhart and William P. Wardlaw, U. S. Naval Academy, Annapolis, MD.*

Chain addition is a technique used in cryptography to extend a short sequence of digits, called the seed, to a longer sequence of pseudorandom digits. If the seed sequence of digits is $a_1, a_2, \ldots, a_n$, then for positive integer k, $a_{n+k} = a_k + a_{k+1} \pmod{10}$, that is, a_{n+k} is the units digit in the sum $a_k + a_{k+1}$. Suppose that the seed sequence is 3, 9, 6, 4. Prove that the sequence is periodic and find, without the use of calculator or computer, the number of digits in the sequence before the first repetition of 3, 9, 6, 4.

1728. *Proposed by José Luis Díaz-Barrero, Universitat Politènica de Catalunya, Barcelona, Spain.*

Let $A_1A_2 \ldots A_{3n}$ be a regular polygon with $3n$ sides, and let P be a point on the shorter arc A_1A_{3n} of its circumcircle. Prove that

$$\left(\sum_{k=1}^{n} PA_{n+k}\right) \sum_{k=1}^{n} \left(\frac{1}{PA_k} + \frac{1}{PA_{2n+k}}\right) \geq 4n^2.$$

We invite readers to submit problems believed to be new and appealing to students and teachers of advanced undergraduate mathematics. Proposals must, in general, be accompanied by solutions and by any bibliographical information that will assist the editors and referees. A problem submitted as a Quickie should have an unexpected, succinct solution.

Solutions should be written in a style appropriate for this MAGAZINE. Each solution should begin on a separate sheet.

Solutions and new proposals should be mailed to Elgin Johnston, Problems Editor, Department of Mathematics, Iowa State University, Ames IA 50011, or mailed electronically (ideally as a LaTeX file) to ehjohnst@iastate.edu. All communications should include the readers name, full address, and an e-mail address and/or FAX number.

1729. *Proposed by Brian T. Gill, Seattle Pacific University, Seattle, WA*

For positive integer k, let c_k denote the product of the first k odd positive integers, and let $c_0 = 1$. Prove that for each nonnegative integer n,

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k}\frac{n!}{k!}2^{n-k}c_k = c_n.$$

1730. *Proposed by Steven Butler, University of California San Diego, La Jolla, CA.*

Let A and B be symmetric, positive semi-definite matrices such that $A + B$ is positive definite, and let $\|\mathbf{y}\|$ denote the usual 2-norm of the vector $\mathbf{y}$. Prove that for all $\mathbf{x} \neq \mathbf{0}$,

$$\left\|(I - A)(I + A)^{-1}(I - B)(I + B)^{-1}\mathbf{x}\right\| < \|\mathbf{x}\|.$$

1718. *Proposed by David Callan, Madison, WI.*

Let k, n be integers with $1 \leq k \leq n$. Prove the identity

$$\sum_{i=0}^{k-1}\binom{k-1}{i}\binom{n-(k-1)}{k-i}2^{k-i-1} = \sum_{i=0}^{k-1}\binom{k-1}{i}\binom{n-i}{k}.$$

Note. This corrects a typo in the April 2005 appearance of the problem.

Quickies

Answers to the Quickies are on page 328.

Q953. *Proposed by Michael W. Botsko, Saint Vincent College, Latrobe, PA.*

Let f be a derivative and g an increasing differentiable function on $[a, b]$. Prove that fg is also a derivative on $[a, b]$.

Q954. *Proposed by Arthur Benjamin, Harvey Mudd College, Claremont, CA, and Michel Bataille, Rouen, France.*

Show that for positive integer n,

$$\sum_{k=0}^{n}\binom{n}{k}\binom{n+k}{k} = \sum_{k=0}^{n}2^k\binom{n}{k}^2.$$

Solutions

A real inequality **October 2004**

1701. *Proposed by Murray S. Klamkin, University of Alberta, Edmunton, AB.*

Prove that for all positive real numbers a, b, c, d,

$$a^4b + b^4c + c^4d + d^4a \geq abcd(a + b + c + d).$$

I. *Solution by Zuming Feng, Philips Exeter Academy, Exeter, NH.*

By the arithmetic-geometric mean inequality,

$$a^4b + abc^2d + abcd^2 \geq 3a^2bcd.$$

Similarly,

$$b^4c + abcd^2 + a^2bcd \geq 3ab^2cd$$
$$c^4d + a^2bcd + ab^2cd \geq 3abc^2d$$
$$d^4a + ab^2cd + abc^2d \geq 3abcd^2.$$

Adding these four inequalities leads to the desired result.

II. *Solution by Chip Curtis, Missouri Southern State University, Joplin MO.*

Note that

$$\left(a^4b\right)^{23/51}\left(b^4c\right)^{7/51}\left(c^4d\right)^{1/51}\left(d^4a\right)^{10/51} = a^2bcd,$$

so by the weighted arithmetic-geometric mean inequality,

$$\frac{23}{51}a^4b + \frac{7}{51}b^4c + \frac{11}{51}c^4d + \frac{10}{51}d^4a \geq a^2bcd.$$

Adding this to the analogous results for b^2cda, c^2dab, d^2abc gives the desired inequality.

Note. A few readers proved that if $a_1, a_2, \ldots, a_n$ are nonnegative real numbers, then

$$a_1^n a_2 + a_2^n a_3 + \cdots + a_n^n a_1 \geq a_1a_2\cdots a_n(a_1 + a_2 + \cdots + a_n).$$

Also solved by Arkady Alt, George Baloglou, Roy Barbara (Lebanon), Rafael Benguria (Chile), Paul Bracken, Daniele Donini (Italy), David Farnsworth, Fejéntaláltuka Szeged Problem Group (Hungary), Michael Goldenberg and Mark Kaplan, G.R.A.20 Math Problems Group (Italy), John Kieffer and Ana Mantilla, Elias Lampakis (Greece), Kee-Wai Lau (China), T. L. McCoy (Taiwan), Microsoft Research Problems Group, David A. Morales (Venezuela), Michael G. Neubauer, Michael Reid, Heinz-Jürgen Seiffert, Achilleas Sinefakopoulos, Nicholas C. Singer, Paul Weisenhorn (Germany), Li Zhou, and the proposer. There was one incorrect submission.

Bounds on a sum of distances **October 2004**

1702. *Proposed by Roy Barbara, American University of Beirut, Beirut, Lebanon.*

Let R be the circumradius of nondegenerate triangle ABC. For point P on or inside of triangle ABC, let $S(P) = |PA| + |PB| + |PC|$. Find the maximum value of k and the minimum value of K such that $kR \leq S(P) \leq KR$ for all acute triangles ABC.

Solution by Microsoft Research Problems Group, Redmond, WA.

The maximum value for k is 2, and the minimum value for K is 4. We first show that $2R < S(P)$. Using the triangle inequality, the Law of Sines, and the fact that $\sin\theta > \frac{2}{\pi}\theta$ for $0 < \theta < \frac{\pi}{2}$ we have

$$\begin{aligned} 2S(P) &= \big(|PB| + |PC|\big) + \big(|PC| + |PA|\big) + \big(|PA| + |PB|\big) \\ &\geq |BC| + |CA| + |AB| \\ &= 2R\sin\angle A + 2R\sin\angle B + 2R\sin\angle C \\ &> 2R \cdot \frac{2}{\pi}(\angle A + \angle B + \angle C) = 4R. \end{aligned}$$

To prove that $S(P) \leq 4R$, place the triangle in the complex plane with the circumcenter at the origin, and let A, B, C also represent the complex coordinates of the vertices. Because P is on or inside of the triangle, there are nonnegative real numbers a, b, c with $P = aA + bB + cC$ and $a + b + c = 1$. Then

$$|P - A| = |aA + bB + cC - A| \le |(a-1)A| + |bB| + |cC| = (1 - a + b + c)R,$$

with similar inequalities for $|P - B|$ and $|P - C|$. We then have

$$\begin{aligned} S(P) &= |P - A| + |P - B| + |P - C| \\ &\le (1 - a + b + c)R + (1 + a - b + c)R + (1 + a + b - c)R \\ &= (3 + a + b + c)R = 4R. \end{aligned}$$

To show that $k = 2$ and $K = 4$ are best possible, consider the triangle with vertices $A = -1$, $B = e^{2i\theta}$, and $C = e^{-2i\theta}$, where θ is small and positive. This triangle has circumradius $R = 1$ and sides $|AB| = |AC| = 2\cos\theta$ and $BC = 2\sin 2\theta$. Observe that $S(A)/R = 4\cos\theta$ can be made arbitrarily close to 4, and that $S(B)/R = 2\cos\theta + 2\sin 2\theta$ can be made arbitrarily close to 2.

Also solved by Michel Bataille (France), Allen Broughton and Herb Bailey, Daniele Donini (Italy), Elias Lampakis (Greece), Raúl Simón (Chile), Michael Vowe (Switzerland), Paul Weisenhorn (Germany), Li Zhou, and the proposer.

Polynomial multiples of 3^n **October 2004**

1703. *Proposed by Shahin Amrahov, ARI College, Ankara, Turkey.*

Let $p(x) = ax^3 + bx^2 + cx + d$ where a, b, c, d are integers with $a \equiv c \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$. Prove that for any positive integer n there is an integer k such that $p(k)$ is a multiple of 3^n.

Solution by Nicholas C. Singer, Annandale, VA.

First observe that

$$\begin{aligned} p(t) - p(u) &= (t - u)\left(a(t^2 + tu + u^2) + b(t + u) + c\right) \\ &\equiv (t - u)\left(2(t^2 + tu + u^2 + 1)\right) \pmod 3. \end{aligned}$$

Because $t^2 + tu + u^2 + 1$ is not a multiple of 3 for any integers t, u, it follows that $3^n \mid (p(t) - p(u))$ if and only if $3^n \mid (t - u)$. Thus, as k takes on integer values $1, 2, \ldots, 3^n$, $p(k)$ takes on 3^n distinct values modulo 3^n. One of these values must be a multiple of 3^n.

Also solved by Roy Barbara (Lebanon), Michel Bataille (France), John Christopher, Chip Curtis, Knut Dale (Norway), Richard Daquila, Fejéntaláltuka Szeged Problem Group (Hungary), Dmitry Fleishman, Michael Goldenberg and Mark Kaplan, Elana C. Greenspan, Russell Jay Hendel, Keun-Ae Jung and Hannah Harding, Victor Y. Kutsenok, Elias Lampakis (Greece), Microsoft Research Problems Group, Northwestern University Math Problem Solving Group, Manual Reyes, Rolf Richberg (Germany), Paul Weisenhorn (Germany), Hongbiao Zeng, Li Zhou, and the proposer.

Fermat-Torricelli cevians **October 2004**

1704. *Proposed by Mowaffaq Hajja, Yarmouk University, Irbid, Jordan.*

Let F be the Fermat-Torricelli point for triangle ABC. Let the cevian from B through F meet $\overline{AC}$ in B^* and the cevian from C through F meet $\overline{AB}$ in C^*. Prove that if $BB^* = CC^*$, then triangle ABC is isosceles. (The Fermat-Torricelli point F of triangle ABC is the point for which the sum of the distances from the vertices is minimum.)

Solution by David Finn and Herb Bailey, Rose Hulman Institute of Technology, Terre Haute, IN.

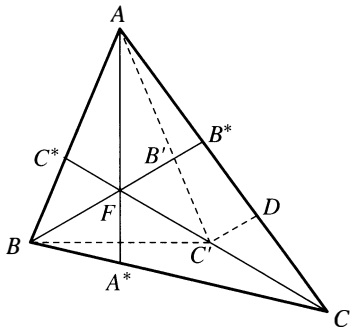
If each angle of the triangle has measure less than 120°, then F is in the interior of the triangle. In this case it is well known that $\angle AFB = \angle BFC = \angle CFA = 120°$.

If $\angle A \geq 120°$, then $F = A$ and the result is immediate. If either $\angle B \geq 120°$ or $\angle C \geq 120°$, then either B^* or C^* is undefined. Thus we assume that all angles have measure less than 120°.

If AF is extended to meet BC at A^*, then the six nonoverlapping angles with common vertex F each have measure 60°. We now establish two lemmas to prove and generalize the desired result.

LEMMA 1. If $FB = FC$, then $AB = AC$ and $BB^* = CC^*$.

Proof. Because $\triangle BFA \cong \triangle CFA$, it follows that $AB = AC$. To prove the other equality, note that $\angle FBC = \angle FCB$ and that $\angle C^*BC = \angle B^*CB$. Thus $\triangle BCC^* \cong \triangle CBB^*$, so $BB^* = CC^*$.



LEMMA 2. If $BB^* = CC^*$, then $FB = FC$.

Proof. Assume that $FB \neq FC$. Then without loss of generality we may assume that $FC > FB$. Construct C' on $\overline{FC}$ so that $FC' = FB$. Let B' be the intersection point of $\overline{AC'}$ and $\overline{BB^*}$, and let D be the point on $\overline{AC}$ such that $\overline{C'D}$ is parallel to $\overline{BB^*}$. Because F is also the Fermat-Torricelli point for $\triangle BC'A$, it follow from Lemma 1 that $BB' = C'C^*$. Since $\triangle CFB^* \sim \triangle CC'D$, we have $\angle CC'D = 60°$. Now in $\triangle AFC$, $\angle AFC = 120°$, and thus $\angle FCA < 60°$. Hence $\angle C'DC > 60°$ and $C'C > C'D$. Because $\triangle AC'D \sim \triangle AB'B^*$ and $AC' > AB'$, we have $C'D > B'B^*$. Combining inequalities we have $C'C > B'B^*$, and hence, $CC^* > BB^*$. This completes the proof of Lemma 2.

Combining Lemmas 1 and 2 shows that $BB^* = CC^*$ implies $AB = AC$, establishing the desired result. On the other hand, if we are given that $AB = AC$, then $\triangle AFB \cong \triangle AFC$ (by SSA with angle F obtuse) and $FB = FC$. Combining this with Lemmas 1 and 2 we see that each of the following three statements implies the other two: (i) $FB = FC$, (ii) $BB^* = CC^*$, (iii) $AB = AC$. Furthermore, these conditions occur if and only if $\angle CBB^* = 30°$.

Also solved by Herb Bailey, Roy Barbara (Lebanon), Daniele Donini (Italy), Ovidiu Furdui, Marty Getz and Dixon Jones, Michael Goldenberg and Mark Kaplan, Elana C. Greenspan, Geoffrey A. Kandall, Victor Y. Kutsenok, Microsoft Research Problems Group, Peter E. Nüesch (Switzerland), Raúl A. Simón (Chile), John W. Spellman and Ricardo Torrejón, Ricardo M. Torrejón, Michael Vowe (Switzerland), Paul Weisenhorn (Germany), Li Zhou, and the proposer.

A symmetric minimum **October 2004**

1705. *Proposed by Michel Bataille, Rouen, France.*

Let n be a positive integer. Find the minimum value of

$$\frac{(a-b)^{2n+1} + (b-c)^{2n+1} + (c-a)^{2n+1}}{(a-b)(b-c)(c-a)},$$

for distinct real numbers a, b, c with $bc + ca \geq 1 + ab + c^2$.

Solution by Northwestern Math Problem Solving Group, Northwestern University, Evanston, IL.

With the change of variables $u = b - c$, $v = c - a$, the problem becomes that of finding the minimum of

$$f(u, v) = \frac{(u+v)^{2n+1} - u^{2n+1} - v^{2n+1}}{(u+v)uv},$$

subject to $uv \geq 1$. Note that u and v must have the same sign and that $f(-u, -v) = f(u, v)$, so we may assume that u and v are positive. Applying the binomial theorem and grouping terms, we have

$$f(u, v) = \sum_{k=1}^{n} \binom{2n+1}{k} \frac{u^{2n+1-2k} + v^{2n+1-2k}}{u+v} u^{k-1} v^{k-1}.$$

By the power means inequality,

$$\frac{u^{2n+1-2k} + v^{2n+1-2k}}{2} \geq \left(\frac{u+v}{2}\right)^{2n+1-2k}.$$

Hence, by the arithmetic-geometric mean inequality,

$$\frac{u^{2n+1-2k} + v^{2n+1-2k}}{u+v} \geq \left(\frac{u+v}{2}\right)^{2n-2k} \geq (uv)^{n-k}.$$

Because $uv \geq 1$, we have

$$f(u, v) \geq \sum_{k=1}^{n} \binom{2n+1}{k} = 4^n - 1.$$

Thus, the minimum value for the given expression is $4^n - 1$. Equality is attained for $u = v = 1$, that is, for $b = c + 1 = a + 2$.

Also solved by Mohammed Aassila (France), Arkady Alt, Roy Barbara (Lebanon), Minh Can, Chip Curtis, Elnur Emrah (Turkey), Fejéntaláltuka Szeged Problem Group (Hungary), Marty Getz and Dixon Jones, Michael Goldenberg and Mark Kaplan, G.R.A.20 Math Problems Group (Italy), Elias Lampakis (Greece), T. L. McCoy (Taiwan), Microsoft Research Problems Group, Rolf Richberg (Germany), Heinz-Jürgen Seiffert, Nora Thornber, Paul Weisenhorn (Germany), Li Zhou, and the proposer. There were two incorrect submissions.

Answers

Solutions to the Quickies from page 324.

A953. Let F be an antiderivative for f and let

$$T(x) = F(x)g(x) - \int_a^x F(t)dg(t).$$

Note that the Riemann-Stieltjes integral exists because F is continuous and g is increasing. Because g is differentiable, we have

$$T'(x) = F(x)g'(x) + g(x)F'(x) - F(x)g'(x) = f(x)g(x),$$

showing that fg is the derivative of T.

A954. Let $[n]$ denote the set $\{1, 2, \ldots, n\}$ and S denote the set of ordered pairs (A, B) where A is a subset of $[n]$ and B is an n-subset of $[2n]$ that is disjoint from A. We can select elements for S in two ways:

(1) For $0 \le k \le n$, let Z be a k-subset of $[n]$. The let $A = Z^c$, the complement of Z, which is an $(n-k)$-subset of $[n]$, and let B be an n-subset of $\{n+1, \ldots, 2n\} \cup Z$. This yields

$$|S| = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k}.$$

(2) For $0 \le k \le n$, choose a k-subset B_1 from $\{n+1, \ldots, 2n\}$ and a k-subset B_2 of $[n]$. Then form $B = B_1 \cup B_2^c$, and choose A from among the 2^k subsets of B_2. This leads to

$$|S| = \sum_{k=0}^{n} 2^k \binom{n}{k}^2.$$

This completes the proof.

Note. Another proof, using lattice paths, can be found in Robert A. Sulanke's article, Objects Counted by the Central Delannoy Numbers, *The Journal of Integer Sequences*, Vol 6, 2003. A proof by polynomials is in Michel Bataille's paper Some Identities about an Old Combinatorial Sum, *The Mathematical Gazette*, March 2003, pp. 144–8.

A slight change in the above proof leads to

$$\sum_{k=0}^{n} \binom{n}{k}\binom{m+k}{n} = \sum_{k=0}^{n} 2^k \binom{n}{k}\binom{m}{k},$$

for $m \ge n$, a generalization proved by Li Zhou using lattice paths in *The Mathematical Gazette*, July 2004, p. 316.

To appear in The College Mathematics Journal, November 2005

Articles:

When the Pope was a Mathematician, *by Leigh Atkinson*
Ramanujan's Continued Fraction for a Puzzle, *by Poo-Sung Park*
Centers of the United States, *by David Richeson*
A Paper-and-Pencil gcd Algorithm for Gaussian Integers, *by Sandor Szabo*
How to Avoid the Inverse Secant (and Even the Secant Itself), *by S. A. Fulling*
Differentiability of Exponential Functions, *by Philip M. Anselone and John W. Lee*

Classroom Capsules:

A Non-Visual Counterexample in Elementary Geometry, *by Marita Barabash*
Can You Paint a Can of Paint?, *Robert M. Gethner*
A Paradoxical Paint Pail?, *by Mark Lynch*
Differentiate Early, Differentiate Often!, *by Robert Dawson*
A Two-Parameter Trigonometry Series, *by Xiang-Qian Chang*

REVIEWS

PAUL J. CAMPBELL, *Editor*
Beloit College

Assistant Editor: Eric S. Rosenthal, West Orange, NJ. Articles and books are selected for this section to call attention to interesting mathematical exposition that occurs outside the mainstream of mathematics literature. Readers are invited to suggest items for review to the editors.

Gardner, Martin, *Martin Gardner's Mathematical Games: The Entire Collection of His* Scientific American *Columns*, CD-ROM for Windows and Macintosh, MAA, $55.95 ($44.95 to MAA members). ISBN 0–88385–545–3. Albers, Don, On the way to "Mathematical Games": Part I of an interview with Martin Gardner, *College Mathematics Journal* 36 (3) (May 2005) 178–190; "Mathematical Games" and beyond: Part II of an interview with Martin Gardner, 36 (4) (September 2005) 301–314. Jackson, Allyn, Interview with Martin Gardner, *Notices of the American Mathematical Society* 52 (6) (June/July 2005) 602–611.

From 1956 to 1986, Martin Gardner wrote a "Mathematical Games" column in *Scientific American*, which delighted readers, fostered mathematicians (for example, me), and introduced to the public such discoveries as public-key cryptography, fractals, the game of Life, and Penrose tilings. Those columns were collected into 15 books and are now available on this searchable CD of PDF files, mostly from MAA editions of the books. The package also includes a printed booklet with a biographical sketch by Peter Renz and an interview by Donald J. Albers, and accompanying photos. The interviews were conducted in 2000–2001 and in in November 2004, just after Gardner turned 90.

Bewersdorff, Jörg, *Luck, Language, and White Lies: The Mathematics of Games*, A K Peters, 2005; xvii + 486 pp, $49. ISBN 1–56881–210–8.

Translated (by David Kramer) from German, this book continues Martin Gardner's tradition of explaining how to play and to win at various mathematical games. Bewersdorff classifies the uncertainty in games into chance ("luck"), logic, and bluff ("white lies"), corresponding to games of chance, combinatorial games, and strategic games—and, of course, games offering varying combinations of these elements. Bewersdorff describes and analyzes games of all these kinds, from dice games, lotteries, Monopoly, and blackjack; to Nim, Dominos, Go, Hex, backgammon, and Mastermind; and rock-paper-scissors, poker, and baccarat. He introduces probability distributions (binomial, Poisson, normal), Markov chains, minimax theory, Grundy values, complexity theory, game theory, and linear programming. The book gives up-to-date results about the games, as well as relevant citations to the literature and history.

Why computers are like the weather, *New Scientist* (9 July 2005) 17, `http://www.newscientist.com/article.ns?id=mg18725074.600` . Berry, Hugues, Daniel Gracia Pérez, and Olivier Teman, Chaos in computer performance, `http://www.arxiv.org/nlin.AO/0506030` .

"... microchips... Their behaviour is inherently unpredictable and chaotic." This somewhat misleading lead from *New Scientist* reports on a study whose authors analyzed the performance of microprocessors. During execution of certain programs, the microprocessors displayed "complex non-repetitive variations that challenge traditional analysis." The sources of the variations include randomness but also, as the authors demonstrate, deterministic chaos. However, what is under discussion here as "performance" is the rate of execution, not the results.

Peterson, Ivars, Closing the gap on twin primes, *Science News* (16 July 2005), http://www.sciencenews.org/articles/20050716/mathtrek.asp .

The average spacing between primes near p is $\log p$, but it is known that infinitely many pairs of primes have gaps between them smaller than $\log p/4$. Daniel A. Goldston (San Jose State University) and Cem Y. Yildirim (Bogaziçi University, Istanbul) presented a flawed proof last year that 4 can be replaced by an arbitrarily large integer. Now, with help from Janos Pintz (Hungarian Academy of Sciences), the proof has been fixed. This result offers hope that the twin prime conjecture—that there are infinitely many prime pairs of the form p, $p + 2$—may be proved soon.

Knight, Will, Computer generates verifiable mathematics proof, *New Scientist* (19 April 2005), http://www.newscientist.com/article.ns?id=dn7286 . Sherriff, Lucy, Proof by self-checking software: the four colour problem, *The Register* (18 April 2005), http://www.theregister.co.uk/2005/04/18/four_colour_self_checking/ .

George Gonthier (Microsoft Research Cambridge, UK) and Benjamin Werner (INRIA, France) have translated the thousands of maps in Appel and Haken's 1976 proof of the Four Color Theorem into logical statements and used "logic-checking software" to check them. But will the skeptics who objected to the use in the original proof of computers to check the maps be any more satisfied with a program that checks the map-checking software?

Wainer, Howard, *Graphic Discovery: A Trout in the Milk and Other Visual Adventures*, Princeton University Press, 2005; xvi + 192 pp, $29.95. ISBN 0–692–10301–1.

In this book, Wainer expands on the theme of his "Visual Revelations" column in *Chance* magazine to give a 'visual pudding": an account of "historical and future graphical practice." He cites predecessors to John Playfair, whom he dubs the inventor of statistical graphics, then goes on to note contributions from Francis Galton and others. A second section uses graphics to probe events in modern times (such as test scores during the Vietnam War, voting records of Supreme Court justices, and industrial malfeasance), and a third section summarizes discussions with John W. Tukey about "graphical tools for the twenty-first century" of computer screens. In keeping with the book's sense of history, brief biographical sketches are included of about 100 of the individuals mentioned.

Gould, Wayne. Sudoku: the program. http://www.sudoku.com. $14.95 (28-day free trial). Peterson, Ivars, Sudoku math, *Science News* (18 June 2005), http://www.sciencenews.org/articles/20050618/mathtrek.asp .

Last fall in Germany, a visiting professor of American literature showed me a book of number puzzles that he enjoyed and asked me if there was any mathematical theory behind them. They involved filling in the numbers 1 to n in a partitioned $n \times n$ grid, with numbers in some positions already specified ("clues"), so that each row, each column, and each partition contains just one of each number between 1 and n. Since then, a variation of such a puzzle has gradually taken the world by storm: sudoku, where a $n = 9$ and a 9×9 grid is partitioned into 3×3 boxes, each of which is a magic square. In effect, the solver constructs a particular kind of 9×9 Latin square. In mid-August, even the Milwaukee *Sentinel-Journal* began offering a daily sudoku puzzle (but newspapers in Germany were still holding out). Wayne Gould, a retired judge, discovered the puzzle in a Tokyo bookstore in 1997 (it had been invented by Howard Garnes in 1979 and originally named Number Place). Gould devised a computer program to generate puzzles and sold the London *Times* on the idea of printing a daily puzzle. Sudoku is a kind of language-independent numerical crossword puzzle, and solving a puzzle involves only logic (not mathematics); like all puzzles, it dangles a feeling of accomplishment. In the words of various newspaper writers, it is the "crack cocaine" of puzzles, "more a craze than a trend," and "makes train-spotting seem positively life-enhancing." Solving an $n \times n$ sudoku puzzle is an NP-complete problem; it is hard to solve one but easy to check the correctness of a solution. (Beware: Another reviewer reports that various sudoku solvers available on the Web also install spyware on Windows computers.) (Thanks to Robert Boyd, St. Louis Community College).

NEWS AND LETTERS

Carl B. Allendoerfer Award—2005

The Carl B. Allendoerfer Awards, established in 1976, are made to authors of expository articles published in Mathematics Magazine. The Awards are named for Carl B. Allendoerfer, a distinguished mathematician at the University of Washington and President of the Mathematical Association of America, 1959–60.

Roger B. Eggleton and William P. Galvin, Upper Bounds on the Sum of Principal Divisors of an Integer, MATHEMATICS MAGAZINE **77**:3 (June 2004), 190–200.

Citation If the prime p divides the positive integer n then the highest power of p dividing n is called a *principal divisor* of n. Consider an odd integer greater than 15 that is not a prime power. This integer—like all other integers—is equal to the *product* of its distinct principal divisors. But can you prove that such an integer is also greater than twice the *sum* of its principal divisors?

Motivated by this problem, the authors masterfully tell a wonderful story of mathematics that is both old and new. They give elegant solutions to the original problem, they develop new mathematics to put the introductory problem in a bigger context, and they do much more. A seamless historical connection to Greek mathematics and to classic questions in number theory (perfect numbers, the aliquot sequence, the series of the reciprocals of primes) is combined with a nice balance of rigorous proofs and intuitive arguments. They always have the reader in mind as they discuss ways to generalize the original concrete problem and, in the process, they give the novice reader a good idea of how mathematical research progresses. The exposition is first rate and keeps the reader engaged to the end. An ambitious undergraduate student would gain much from tackling this paper.

Biographical notes Roger Benjamin Eggleton is an Australian-born mathematician whose main fields of interest are combinatorics, graph theory, and number theory. His research and teaching career encompasses universities in five countries—Australia (1963–70), Canada (1970–73), Israel (1973–74) USA (1974–76), Australia (1976–88), Brunei (1989–92), and USA (1993–present). He obtained his Ph.D. in Calgary (1973), under Richard Guy. He has published over 60 research papers, and regards his collborations with many joint authors, including several papers with Paul Erdős, as one of the main pleasures of his career. He published four joint papers with William Galvin (2000–04).

William P. Galvin was born in Sydney, Australia on February 5, 1938. His professional career began as a high school mathematics and science teacher, transforming by 1970 into teacher training. Always a dedicated student, he completed four degrees while working full-time: B.A. (Sydney, 1962), M. Ed. (Newcastle, 1974), M. Math. (Newcastle, 1977), M. Eng. Sc. (Newcastle, 1982), all three masters degrees being research degrees. By 1989, Bill has head of the department responsible for teaching mathematics, computing, and mathematics education at the Hunter Institute of Higher Education —subsequently amalgamated with University of Newcastle, where Bill continued training mathematics teachers until he retired in 1997. After retirement, his research and other mathematical involvements continued unabated, despite growing ill health. Soon after completing a three-year term as coeditor of the Australian Mathematical Society's *Gazette* (2001–03), he died of cancer on December 12, 2003. The next issue fittingly published his obituary (*Austral. Math. Soc. Gaz.*, **31** (2004), 4–5.).

Response from Roger Eggleton (and on behalf of William Galvin) On behalf of my coauthor Bill Galvin and myself, it is with pleasure and humility that I accept the 2005 Allendoerfer Award for our paper on principal divisors of integers. After a long and strong-spirited battle with cancer, Bill passed away a few days after we received the welcome news that our paper was to be published in MATHEMATICS MAGAZINE. This was the last of four joint papers we wrote during 2000–03. Each of them gave us the pleasures of shared mathematical adventure—exploration, discovery, and wonder at the unfolding beauty of mathematics. When much else had begun to recede in relevance for Bill, he continued to find great satisfaction in the pursuit of the timeless beauty of mathematics. He would have been delighted with this recognition of our work. For myself, joining the distinguished list of recipients of the Allendoerfer Award is a wonderful endorsement of the conviction that we should continually strive to communicate the beauty of mathematics as transparently and seamlessly as possible.

Merten M. Hasse Prize—2005

In 1986, an anonymous donor gave the MAA funds sufficient to support a prize honoring inspiring and dedicated teachers. The prize was to be named after Merten M. Hasse, who was a former teacher of the donor, and who exemplified these qualities of a fine teacher. the prize is designed to be an encouragement to younger mathematicians to take up the challenge of exposition and communication. The Merten M. Hasse Prize is for a noteworthy expository paper appearing in an Association publication, at least one of whose authors is a younger mathematician.

This year the Merten M. Hasse Prize was awarded to an article appearing in the MAGAZINE.

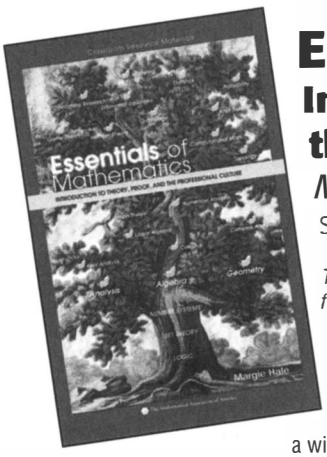
Maureen T. Carroll and Steven T. Dougherty, Tic-Tac-Toe on a Finite Plane, MATHEMATICS MAGAZINE, **77**:4 (October 2004), 260–274.

Citation In this entertaining article, the authors tweak the familiar game of tic-tac-toe by placing it in a new context: the finite affine or projective plane, noting that "with this new twist, the game that grew tiresome for us as children is transformed into an interesting, geometrically motivated game." And indeed it is! Not only does mathematics motivate the game, but the game motivates mathematics—we are treated to a tour of topics such as Latin squares, axioms for affine planes, and strategy-stealing and weight functions in game theory. These ideas help the authors classify those affine or projective planes on which there is a winning strategy. Throughout the article, the authors invite us to participate in the discoveries, just as they have involved their students. Their choice of topic, friendly exploration, tidy conclusion, and smooth exposition make this article fun and engaging reading.

Biographical notes Maureen T. Carroll is an Associate Professor at the University of Scranton. She and her coauthor first started their collaborations when they were both graduate students at Lehigh University. Although her dissertation field was functional analysis, she has also published papers in voting theory and game theory. She was a Project NExT fellow (green dot) and participated in the Institute in the History of Mathematics. Steven Dougherty received his doctorate from Lehigh University and is now a Professor of Mathematics at the University of Scranton. He has written over 40 papers in coding theory, number theory, and combinatorics with 19 coauthors from nine different countries. He has lectured at numerous universities and conferences spanning six countries.

(The response from Carroll and Doughetry appears on p. 282.)

From the **Mathematical Association of America**



Essentials of Mathematics

Introduction to Theory, Proof, & the Professional Culture

Margie Hale

Series: Classsroom Resource Materials

This book is well written, and will, I'm sure be useful. I would love to teach a course from it. —Marion Cohen, MAA Online

Every mathematician must make the transition from the calculations of high school to the structural and theoretical approaches of graduate school. That journey incorporates many aspects: more and deeper content, new methods, a widening of perspective experience with the various subfields of mathematics, and the influence of teachers, to name a few. **Essentials of Mathematics** provides the knowledge needed to move onto advanced mathematical work, and a glimpse of what being a mathematician might be like. No other book takes this particular approach to the task.

The content is of two types. There is material for a "Transitions" course at the sophomore level; introductions to logic and set theory, discussions of proof writing and proof discovery, and introductions to the number systems (natural, rational, real, and complex). The material is presented in a fashion suitable for a Moore Method course, although such an approach is not necessary. In addition to presenting the important results for student proof, each area provides warm-up and follow-up exercises to help students internalize the material.

The second type of content is an introduction to the professional culture of mathematics. There are many things that mathematicians know but weren't exactly taught. To give college students a sense of the mathematical universe, the book includes narratives on this kind of information. There are sections on pure and applied mathematics, the philosophy of mathematics, ethics in mathematical work, professional (including student) organizations, famous theorems, famous unsolved problems, famous mathematicians, a discussions of the nature of mathematics research and more.

The prerequisites for a course based on this book include the content of high school mathematics and a certain level of mathematical maturity. The student must be willing to think on an abstract level. Two semesters of calculus indicates a readiness for this material.

An Instructor's Manual is available to teachers who adopt this book for a course.

Catalog Code: ELM/JR • 186 pp., Hardbound, 2003
ISBN 0-88385-729-4 • List Price: $49.95 • Member Price: $39.95

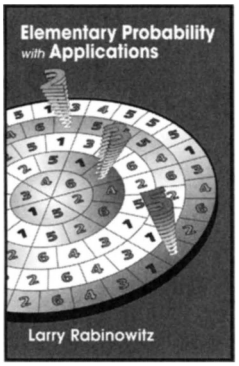
Order your copy today!
1-800-331-1622 or www.maa.org

The Mathematical Association of America

Elementary Probability with Applications

Larry Rabinowitz

2004; ISBN 1-56881-222-1
Hardcover; 208 pp.; $35.00



Elementary Probability presents real world applications of discrete probability with a large number of interesting exercises that test the understanding of these applications. *The only prerequisite is one year of high school algebra.*

Professor Rabinowitz, based on many years of teaching, has created an innovative, practical, and entertaining textbook.

Examples and related exercises in the areas of

sports • airline overbookings • population growth • elections • sensitive question surveys • jury models • legal cases • medical studies • drug testing • the military • cryptology, and more.

An instructor's manual with solutions and teaching aids is available.

Available from **A K Peters, Ltd.** www.akpeters.com 781-416-2888

Martin Gardner's Mathematical Games

The Entire Collection of His Scientific American Columns

Martin Gardner's "Mathematical Games" column ran in *Scientific American* from 1956 to 1986. In these columns, Gardner introduced hundreds of thousands of readers to the delights of mathematics and of puzzles and problem solving.

Now, this material has been brought together on one, searchable CD.

Martin Gardner is the author of more than 65 books and countless articles, ranging over science, mathematics, philosophy, literature, and conjuring. He has inspired and enlightened generations with the delights of mathematical recreations, the amazing phenomena of numbers, magic, puzzles, and the play of ideas. He is our premier writer on recreational mathematics, a great popularizer of science and a debunker of pseudoscience.

Spectrum
Catalog Code: TDG
On CD-ROM, 2005
ISBN: 0-88385-545-3
List Price: $55.95
Member Price: $44.95

To make sure the CD is compatible with your computer, system requirements are available online or by calling our service center

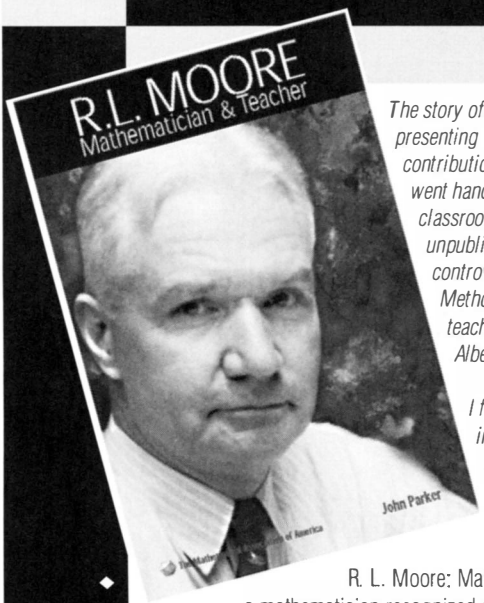
Order your copy today!
1.800.331.1622 • www.maa.org

The Mathematical Association of America

From the MAA...

R.L. Moore
Mathematician & Teacher

John Parker



The story of the mathematician R.L. Moore and his students is worth presenting to a wide audience not only because of their scientific contributions but especially because their creativeness in mathematics went hand in glove with their inspiration of creativeness in the classroom. The author has drawn on a large array of published and unpublished sources and does not overlook the criticisms and controversies that have been associated with Moore and the Moore Method. This personal history thus becomes a study in the art of teaching and in the discovery and nurture of talent.
Albert C. Lewis, C. S. Peirce Edition Project

I first studied under Moore in 1941. I found him to be an inspirational kind of teacher, and a man totally dedicated to his students, more so than any other teacher I've known. —Richard D. Anderson, Boyd Professor Emeritus, Louisiana State University, Past President MAA & Past Vice-President, AMS.

R. L. Moore: Mathematician & Teacher presents a full and frank biography of a mathematician recognized as one of the principal figures in the twentieth century American school of point set topology. He was equally well known as creator of the Moore Method (no textbooks, no lectures, no conferring) in which there is a current and growing revival of interest in both the United States and the United Kingdom.

Parker draws on Oral History, with first-person recollections from many leading figures in the American mathematics community of the last half-century. The story embraces some of the most famous and influential mathematical names in America and Europe from the late 1900s in what is undoubtedly a lively account of this controversial figure, once described as Mr. Chips with Attitude. He was the first American to become a Visiting Lecturer for the American Mathematical Society, was a member of the National Academy of Sciences, published 68 papers and a book which is still referred to seventy years later and which has been the subject of literally hundreds of papers by other mathematicians from around the globe.

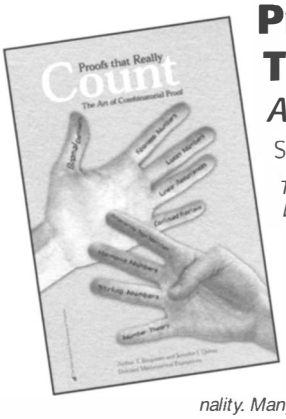
A professional genealogy forms a fascinating sub-text to the book. It describes three of Moore's students who followed him as president of the American Mathematical Society, three others who became vice-presidents, and another who served as secretary of the AMS for many years. Five served as president of the Mathematical Association of America, and three -- like Moore himself -- became members of the National Academy of Sciences while most of the rest became highly respected and well published mathematicians and teachers in top flight American universities. Given that the presidencies run for two years, his former students were at the helm of one or other of the two major mathematical organizations in the US for a third of the second half of the 20th Century.

Series: Spectrum • Catalog Code: MBIO • 380 pp., Harbdound • ISBN: 0-88385-550-X
List Price: $45.95 • Sale Price: $36.95

Available online at: www.maa.org

or call: 1.800.331.1622

From the **Mathematical Association of America**



Proofs That Really Count: The Art of Combinatorial Proof

Arthur T. Benjamin & Jennifer J. Quinn

Series: Dolciani Mathematical Expositions

This is a delightful book. In this wonderful volume, the authors have put together their combinatorial insights in a fascinating package that is appealing and accessible to a very broad audience stretching from clever high school students to university faculty. Benjamin and Quinn begin with the combinatorics of Fibonacci numbers and move on to a variety of interesting related problems. Their book will attract and inspire students young and old.

—George E. Andrews, Penn State University

This is a magical introduction to the simplicity, power, and beauty of bijective proofs, proofs that accomplish their task by counting the same set of objects in two different ways. The examples range widely, and the proofs are presented with clarity and originality. Many undergraduates—and not a few more senior mathematicians—will be seduced by this book into searching for their own proofs that count.

—David M Bressoud, Macalester College

This book blends the talents of Martin Gardner and Houdini; it gives magical 'aha' proofs that are real mathematics but accessible to everyone. It's as good a way as I've seen to show why we love mathematics.

—Persi Diaconis, Stanford University

It is a masterpiece. What a great way to introduce students to proofs! Combinatorics is a perfect medium to introduce that forbidding concept of 'formal proof,' and Benjamin and Quinn did a masterful job of making proofs both accessible, and so much fun.

—Doron Zeilberger, Rutgers University

Mathematics is the science of patterns, and mathematicians attempt to understand these patterns and discover new ones using a variety of tools. In **Proofs That Really Count**, award-winning math professors Arthur Benjamin and Jennifer Quinn demonstrate that many number patterns, even very complex ones, can be understood by simple counting arguments.

The arguments primarily take one of two forms: a counting question is posed and answered in two different ways. Since both answers solve the same question they must be equal; and, two different sets are described, counted, and a correspondence found between them. One-to-one correspondences guarantee sets of the same size. Almost one-to-one correspondences take error terms into account. Even many-to-one correspondences are utilized.

The book explores more than 200 identities throughout the text and exercises, frequently emphasizing numbers not often thought of as numbers that count: Fibonacci Numbers, Lucas Numbers, Continued Fractions, and Harmonic Numbers, to name a few. Numerous hints and references are given for all chapter exercises and many chapters end with a list of identities in need of combinatorial proof. The extensive appendix of identities will be a valuable resource. This book should appeal to readers of all levels, from high school math students to professional mathematicians.

Catalog Code: DOL-27/JR • 208 pp., Hardbound, 2003
ISBN 0-88385-333-7 • List Price: $43.95 • Member Price: $34.95

Order your copy today!
1-800-331-1622 or www.maa.org

The Mathematical Association of America

CONTENTS

ARTICLES

NOTES

PROBLEMS

REVIEWS

NEWS AND LETTERS

THE MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth Street, NW
Washington, DC 20036