Vol. 85, No. 2, April 2012

MAA

MATHEMATICS MAGAZINE

Still Life with Magic Square

- Game, Set, Math
- Mathematics and Magz (and Pascal's tetrahedron)
- Irrationality, inequality, periodicity, probability, and more

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. 83, at pages 73–74, and is available at the *Magazine*'s website 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.

Please submit new manuscripts by email directly to the editor at mathmag@maa.org. A brief message containing contact information and with an attached PDF file is preferred. Word-processor and DVI files can also be considered. Alternatively, manuscripts may be mailed to Mathematics Magazine, 132 Bodine Rd., Berwyn, PA 19312-1027. If possible, please include an email address for further correspondence.

Cover image: "Still Life with Magic Square," oil paint on canvas, 2011, by Sylvie Donmoyer (`http://www.illustration-scientifique.fr/index-A.html`).

MATHEMATICS MAGAZINE (ISSN 0025-570X) is published by the Mathematical Association of America at 1529 Eighteenth Street, N.W., Washington, D.C. 20036 and Lancaster, PA, 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

MAA Advertising
1529 Eighteenth St. NW
Washington DC 20036

Phone: (877) 622-2373
E-mail: tmarmor@maa.org

Further advertising information can be found online at www.maa.org

Change of address, missing issue inquiries, and other subscription correspondence:

MAA Service Center, *maahq@maa.org*

All at the address:

The Mathematical Association of America
1529 Eighteenth Street, N.W.
Washington, DC 20036

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

Vol. 85, No. 2, April 2012

MATHEMATICS MAGAZINE

LETTER FROM THE EDITOR

The cover image is of Sylvie Donmoyer's painting, "Still Life with Magic Square," which won first place in the Joint Mathematics Meetings art exhibition in Boston. You can also see it in the MAA's Found Math Gallery (link from www.maa.org; Jan. 9) and at the artist's own site (www.illustration-scientifique.fr/index-A.html; expect to spend some time there). Or, perhaps you can see the original painting by visiting the Math for America offices at 160 Fifth Ave. in New York, www.mathforamerica.org.

Our first two articles mention George Pólya, and the benefits of playing with with toys and games.

Ben Coleman and Kevin Hartshorn describe the mathematics of the game of SET. (You can find the game anywhere, or start at www.setgame.com.) The game begins with twelve cards on the table. How many essentially different deals of twelve cards are there? The answer is on page 84, if you know where to look for it. The method is Pólya's counting theorem, an instrument of great power.

Peter Hilton and Jean Pedersen use Magz (and Sylvie Donmoyer's illustrations) to visualize a theorem about trinomial coefficients. They combine familiar algebra with surprisingly rich geometry, and with Pólya's notion of "homologues." When you read the article you'll find the key role played by one particular set of homologues, which are three interpenetrating squares. Then you can look back at the cover image, and find—a particular set of homologues, which are three interpenetrating squares! (The Magz very much deserve a link, too: www.magz.com.)

We are honored to have this paper co-authored by Peter Hilton, who died in November, 2010. He contributed more than most, to the mathematical community and to the world. He is missed.

Are your Pythagorean friends still in denial about irrational numbers? In this issue Grant Cairns proves irrationality for the square root of 2, Steve Miller and David Montague for other square roots, and David Gilat for roots of polynomials—all without using prime factors. Elsewhere in the Notes Section we have a wider-than-usual range of topics: The AM-GM inequality, sums of cosines, determinants (not worthless ones, but ones with zero value), Fibonacci-like sequences, and integration by parts.

This is our third consecutive April issue with color. Could we have predicted that? Perhaps so, based on Mark Schilling's note on long runs of identical events.

Harry Waldman has now completed his nearly thirty years with the MAA as writer, editor, and manager, with special responsibility for the three print journals. His name first appeared on the Magazine's title page in February, 1985, and has appeared with the names of seven editors. Everything you see here reflects his influence, and like my predecessors I have appreciated his guidance and good will. Now we welcome Beverly Ruedi to the role of Managing Editor; also a pillar of the MAA, she has worked on the production of the Magazine before, and has most recently helped to manage the MAA's books program.

Walter Stromquist, Editor

ARTICLES

Game, Set, Math

BEN COLEMAN
Moravian College
Bethlehem, PA 18018
coleman@cs.moravian.edu

KEVIN HARTSHORN
Moravian College
Bethlehem, PA 18018
hartshorn@math.moravian.edu

One of the joys of mathematics is the serendipitous meeting of seemingly different ideas—in this case a popular card game, genetics research on dogs, and a polynomial of degree 81. In 1974, geneticist Marsha Falco [**4**] was observing German shepherds in order to understand the genetics of epilepsy, and she developed a simple labeling system for the characteristics of interest. At home, she and her husband organized these symbols into four attributes of three possible values and created a game using the 81 cards shown in FIGURE 1. After years of playing the game with their family, they marketed the game SET in 1991. As the game became popular, mathematicians at all levels explored patterns in it that the Falco family had never anticipated [**14**].

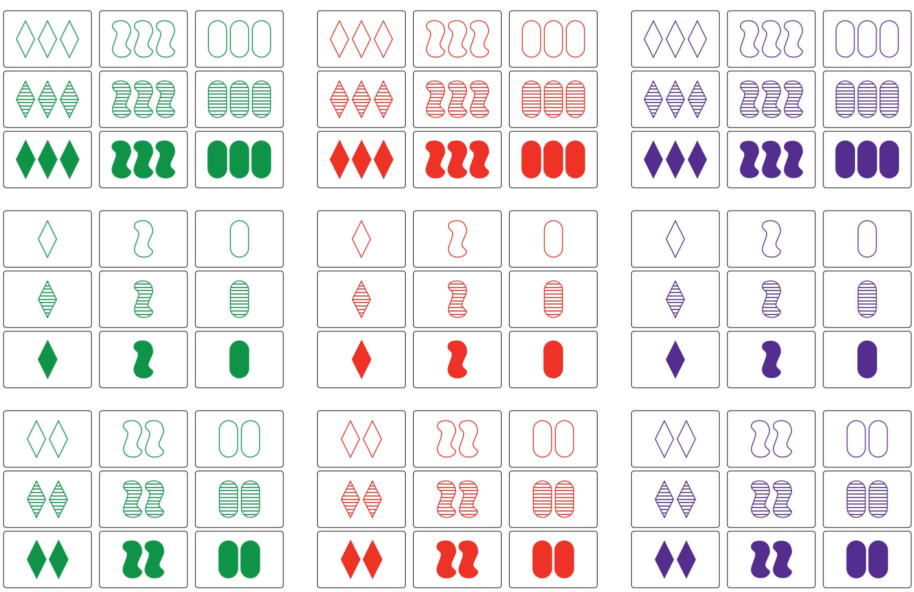


Figure 1 The 81 SET cards organized in a nine-by-nine grid

Math. Mag. **85** (2012) 83–96. doi:10.4169/math.mag.85.2.083. © Mathematical Association of America

Questions such as “how many structurally different ways are there for the game to begin?” led to our work using Pólya’s theorem to reach the beautiful spindle-shaped polynomial in FIGURE 2. The coefficient of t^n in that polynomial tells us how many inequivalent ways there are to deal n cards in the game.

In this paper, we define *inequivalent* more precisely, provide an overview of the rich activity that has followed this game, and share our own contribution—counting unique patterns of collections of cards.

$$
\begin{gathered}
t^{81} + \\
t^{80} + t^{79} + \\
2t^{78} + 3t^{77} + 6t^{76} + \\
15t^{75} + 34t^{74} + 105t^{73} + \\
384t^{72} + 1658t^{71} + 8135t^{70} + \\
41407t^{69} + 205211t^{68} + 963708t^{67} + \\
4231059t^{66} + 17295730t^{65} + 65807588t^{64} + \\
233346408t^{63} + 772518828t^{62} + 2392611091t^{61} + \\
6946116261t^{60} + 18937468347t^{59} + 48568206996t^{58} + \\
117356752981t^{57} + 267548687984t^{56} + 576222904363t^{55} + \\
1173737365919t^{54} + 2263568972663t^{53} + 4136780036942t^{52} + \\
7170309576688t^{51} + 11796184561289t^{50} + 18431386920534t^{49} + \\
27367649303603t^{48} + 38636503940897t^{47} + 51883126670392t^{46} + \\
66294936428615t^{45} + 80628826002618t^{44} + 93359571424793t^{43} + \\
102934827016066t^{42} + 108081525023972t^{41} + 108081525023972t^{40} + \\
102934827016066t^{39} + 93359571424793t^{38} + 80628826002618t^{37} + \\
66294936428615t^{36} + 51883126670392t^{35} + 38636503940897t^{34} + \\
27367649303603t^{33} + 18431386920534t^{32} + 11796184561289t^{31} + \\
7170309576688t^{30} + 4136780036942t^{29} + 2263568972663t^{28} + \\
1173737365919t^{27} + 576222904363t^{26} + 267548687984t^{25} + \\
117356752981t^{24} + 48568206996t^{23} + 18937468347t^{22} + \\
6946116261t^{21} + 2392611091t^{20} + 772518828t^{19} + \\
233346408t^{18} + 65807588t^{17} + 17295730t^{16} + \\
4231059t^{15} + 963708t^{14} + 205211t^{13} + \\
41407t^{12} + 8135t^{11} + 1658t^{10} + \\
384t^{9} + 105t^{8} + 34t^{7} + \\
15t^{6} + 6t^{5} + 3t^{4} + \\
2t^{3} + t^{2} + \\
t + 1
\end{gathered}
$$

Figure 2 The polynomial representing the pattern inventory for separating SET cards into two piles. The coefficient of t^n is the number of inequivalent ways to select n cards.

The game

We begin with a description of the game. On the SET cards, the symbols have the following attributes:

1. *Quantity*: 1, 2, or 3 copies of the symbol occur on each card.
2. *Color*: the symbols are red, green, or purple.
3. *Shading*: the interior of each symbol is solid, striped, or open (i.e., only the outline of the shape appears).
4. *Shape*: the symbols on the cards are diamonds, squiggles, or ovals.

A *set* is a collection of three cards such that for each of the four attributes above, the three cards are all matching or all distinct. For example, in FIGURE 3, the three cards form a *set*, as they have different quantities, same colors, different shadings, and same shapes. On the other hand, the cards in FIGURE 4 do *not* form a *set* since two of the cards are striped while the third is solid, although the other three attributes for the cards do obey the rules.

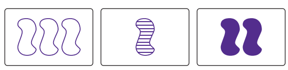


Figure 3 Example of a *set*

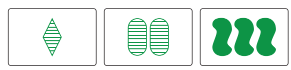


Figure 4 Example of a non-*set*

When playing the game, players compete to find *sets* among twelve cards placed face-up on the table. The player who first identifies a *set* takes the three cards and scores one point. Three cards from the deck are added to the table, and the players resume their search for *sets*. If no player can locate a *set*, then three additional cards are added to the table. This race to find a *set* repeats until there are no additional cards in the deck and no *sets* on the table, at which point the winner is the player who found the most *sets*. A complete description of the rules, as well as the history of the game's development are available through the official web site [**14**].

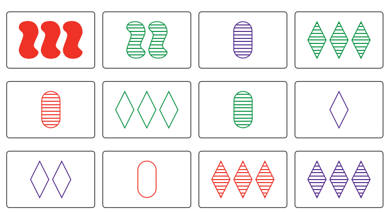


Figure 5 Twelve cards containing six *sets*

The game has won wide acclaim including the MENSA Select Award and the Parents' Choice Award. The "puzzle master" Wil Shortz took the game to the first World Puzzle Championship in 1992. Perhaps as a result of this endorsement, the New York Times hosts a daily SET solitaire puzzle like the one in FIGURE 5, where players must find six *sets* in a collection of twelve cards. More academically, the game has sparked interest in the fields of artificial intelligence [**16**], theoretical computer science [**2**], and programming pedagogy [**5**].

Many mathematics departments, from elementary school through college, use the game of SET for classroom engagement. The SET web site [**14**] shares lesson plans developed by Anthony Macula and Michael J. Doughty [**10**] that introduce traditional set theory using SET cards while Holdener [**7**] uses SET for an undergraduate abstract algebra project. In her honors work, Maureen Jackson [**8**] describes a litany of applications of the game SET in many mathematical fields, including their connection to magic squares.

In the context of SET, a *magic square* is a three-by-three array of distinct cards where every row, column and each of the six diagonals forms a *set*, resulting in twelve *sets* among nine cards. A "diagonal" is a generalized diagonal; that is, any arrangement of three cards with one in each row and one in each column. We can construct a magic square by starting with three cards that do not form a *set*. By placing them as shown in FIGURE 6, the upper-right and lower-left cards are specified. In turn, the middle card is specified, and in this way, we can complete the square. Jackson proves that this process always produces a magic square. Note that each of the nine sections of FIGURE 1 is also a magic square.

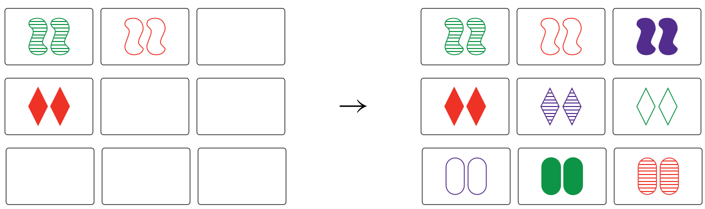


Figure 6 Constructing a magic square

The SET deck is a vector space

To go further we need some notation. By $\mathbb{F}_3$ we mean the unique field of order 3, which is just the set of integers $\{0, 1, 2\}$ with addition modulo 3. The SET deck can be identified with the 4-dimensional vector space $\mathbb{F}_3^4$. To see this, we map the attributes of each card to the integers 0, 1, and 2, as in FIGURE 7. Using these mappings, the three cards on the left in FIGURE 6 correspond to the vectors $[2, 0, 1, 1]$, $[2, 1, 0, 1]$, and $[2, 1, 2, 0]$.

	0	1	2
Quantity	3	1	2
Color	green	red	purple
Shading	open	striped	solid
Shape	diamond	squiggle	oval

Figure 7 Mapping attribute values to 0, 1, and 2

The mapping provides two equivalent ways to mathematically define a *set*:

1. A *set* consists of three vectors that sum to $[0, 0, 0, 0]$ modulo 3. Note that this occurs only if for each attribute the cards are all the same or all different.
2. A *set* consists of three vectors that lie on a line in this vector space. The equation of a line through two points $\mathbf{a}$ and $\mathbf{b}$ is given by $\mathbf{a} + t(\mathbf{b} - \mathbf{a})$ and in $\mathbb{F}_3$ we have $t = 0, 1, 2$, providing exactly 3 points on any line. It is a good exercise to show that three vectors form a line if and only if they sum to $[0, 0, 0, 0]$ modulo 3 and thus correspond to a *set*.

The three cards defining a magic square also determine an affine plane in the vector space $\mathbb{F}_3^4$. In general, there is a unique plane through any three non-collinear points **a**, **b**, **c**, given by the equation $\mathbf{a} + t(\mathbf{b} - \mathbf{a}) + s(\mathbf{c} - \mathbf{a})$. Since we are working over the field $\mathbb{F}_3$, the parameters s and t take the values 0, 1, or 2, and the reader can check that the nine possible choices for these parameters result in the magic square on the right in FIGURE 6 if we let **a**, **b**, **c** be the vectors [2, 0, 1, 1], [2, 1, 0, 1], and [2, 1, 2, 0].

The vector-space model provides a way to understand an interesting fact about the end of a game. If the last card of the deck is placed face down, it is possible to determine that last card from the other cards that remain on the table. The sum of all 81 cards is [0, 0, 0, 0] modulo 3. When a *set* is removed that sum does not change. Thus at the end of the game, the sum of the cards on the table must still be [0, 0, 0, 0] modulo 3. To predict the last card, determine the vector that preserves this property. For example, in FIGURE 8 the first coordinate of the missing vector is 1 because the sum of other first coordinates is $0 + 2 + 0 + 1 + 2 = 2 \mod 3$. Doing the same for the other attributes, we find that the missing vector is [1, 2, 1, 1] or one-purple-striped-squiggle. As a corollary, note that a properly played game can never end with three cards—the last three cards always form a *set*.

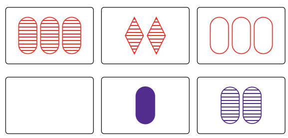


Figure 8 A six-card endgame

Liz McMahon and Gary Gordon of Lafayette College discovered another property of a game that ends with exactly six cards. Group the cards into three pairs, and for each pair, determine the card that turns it into a *set*. No matter how the cards are grouped, the three cards that complete the *sets* will themselves form a *set*. For example, in FIGURE 8, if we group the cards in columns, then the three cards that complete the *sets* are two-green-striped-diamonds, three-green-open-squiggles, and one-green-solid-oval. The proof of this fascinating property is left as a challenge for the reader.

There has also been interest in how many cards you can place on the table without any *set* occurring. This maximal number, sometimes referred to as a *maximal cap*, was first proven to be 20 by G. Pellegrino [**11**] who wasn't actually considering the game (it hadn't been created yet). Benjamin Lent Davis and Diane Maclagan [**3**] put Pellegrino's work into the context of SET and also extended his results to consider maximal caps when playing the game with different numbers of attributes. Robert Bosch [**1**] proved that the maximal cap is 20 using a branch-and-bound technique to solve an integer program, and Holdener [**7**] used this question to motivate independent research in an undergraduate abstract algebra course.

Knowing this maximal cap, Zabrocki [**17**] asked about the number of ways to make a 20-card collection with no *sets*, and Donald Knuth wrote computer programs to generate all the non-isomorphic collections of 20 cards with no *sets* [**9**]. More generally, Zabrocki asked how many n-card collections could contain a given number of *sets*. Questions of this form led us to the result in this paper: for fixed n, how many non-isomorphic collections of n cards are there?

Linear transformations

As we move toward answering this question, we note that our particular arrangement of cards in FIGURE 1 was chosen deliberately. If we select any collection of five cards that contains no *sets*, then we can use these cards as a basis to define an equivalent nine-by-nine array. Choosing as an example two-green-striped-squiggles, two-red-open-squiggles, and two-red-solid-diamonds (as we did in FIGURE 6) allows us to complete the plane or magic square seen in the top-left section in FIGURE 9. By picking the card two-red-solid-squiggles, and placing it in the top-left corner of the top-center block in FIGURE 9, there is a unique completion of the top row of cards. Finally, the rest of the 9×9 arrangement is determined by the choice of three-purple-solid-ovals in the top-left corner of the leftmost block of the second row. In essence, we are choosing a new basis for the 4-dimensional affine space. This particular choice can be represented by the transformation

$$T(\mathbf{x}) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 1 & 1 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 2 & 0 \end{bmatrix} \mathbf{x} + \begin{bmatrix} 2 \\ 0 \\ 1 \\ 1 \end{bmatrix}. \tag{1}$$

To illustrate this correspondence, consider the card three-red-solid-squiggles in FIGURE 1, which has coordinates $[0, 1, 2, 1]$. Under the transformation, this card is mapped to

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 1 & 1 \\ 1 & 0 & 0 & 2 \\ 1 & 0 & 2 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 2 \\ 1 \end{bmatrix} + \begin{bmatrix} 2 \\ 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 1 \\ 0 \\ 2 \end{bmatrix},$$

which is the vector for two-red-open-ovals, seen in the same location in FIGURE 9.

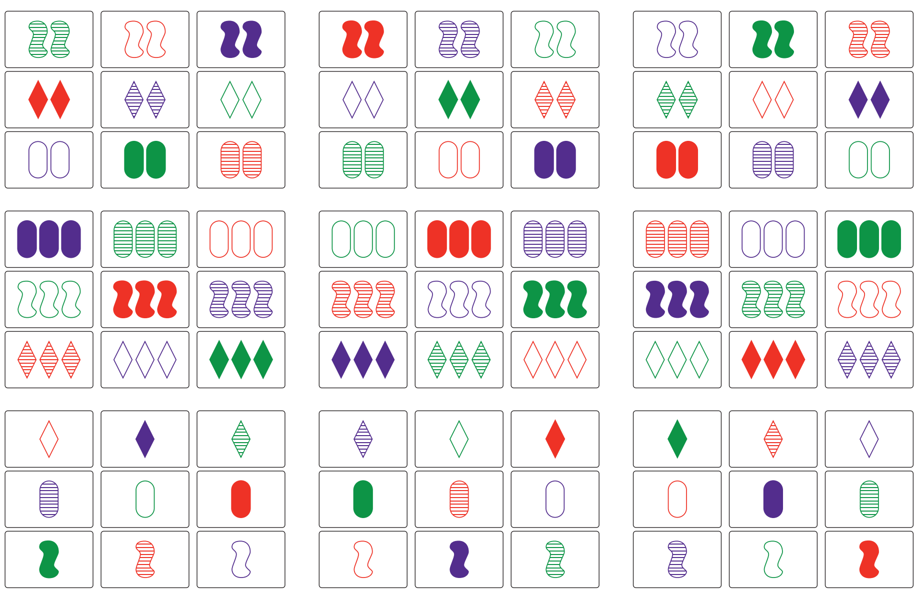


Figure 9 Transformed nine-by-nine grid

For our purposes, then, isomorphisms of the SET deck are affine transformations from one such basis to the another. The order of this group is $81 \cdot 80 \cdot 78 \cdot 72 \cdot 54 = 1,965,150,720$, and the isomorphisms are of the form

$$T(\mathbf{x}) = L\mathbf{x} + \mathbf{v},$$

where L is an element of $\mathrm{GL}(\mathbb{F}_3^4)$, the group of invertible 4×4 matrices over the field $\mathbb{F}_3$, and $\mathbf{v} \in V$ is a 4-vector. Such a transformation always preserves the game structure in the sense that *sets* are mapped to *sets*. We consider two collections of cards to be equivalent if they are related by such an affine transformation. As an illustration of this equivalence, in FIGURE 10, we see the cards from FIGURE 5 transformed by the map T of Equation 1. Note that we see the exact same arrangement of *sets* both before and after the transformation.

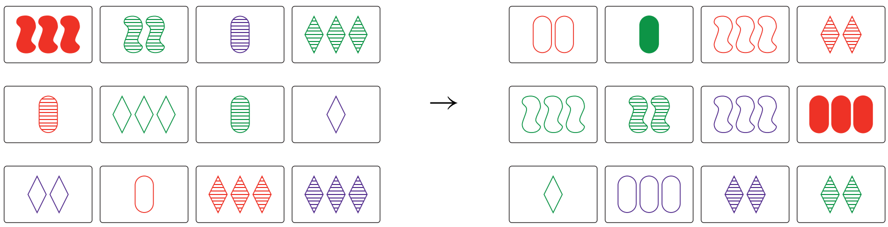


Figure 10 The cards from FIGURE 5, transformed by T in Equation 1

Counting inequivalent layouts

If two layouts are equivalent under a transformation of the deck, then we say that they are in the same orbit, and we consider those layouts effectively equivalent, since each has the same number of *sets* exhibiting the same intersection properties within the geometric structure. Counting distinct collections of n cards thus amounts to counting the number of orbits of the action of the transformation group of the SET deck on the space of $\binom{81}{n}$ n-card layouts.

For example, there are only two distinct ways to draw three cards: either they form a *set* or they do not. Any two *sets* are equivalent under the group of transformations of the SET deck, and any collection of three cards that do not form a *set* can be mapped by an affine transformation to the triple one-green-open-diamond, one-green-striped-diamond, one-green-open-squiggle from FIGURE 1. There are three distinct ways to draw four cards. If the four cards contain a *set* (that is, a line), then the *set* and the fourth card determine a plane, and any two such structures are equivalent (first way). Otherwise, three of the four cards determine a plane and the fourth card is (second way) or is not (third way) contained in that plane.

Applying Pólya's theorem

As the number of cards on the table increases, so does the difficulty in enumerating the possible arrangements of those cards. Ultimately, the challenge is to find the *pattern inventory* shown in FIGURE 2, a polynomial of the form

$$p(t) = \sum_{i=0}^{81} c_i t^i,$$

where c_i is the number distinct layouts of size i. We computed the pattern inventory using Pólya's theorem.

The central idea in Pólya's theorem is the *cyclic index* of the transformations. For example, FIGURE 11 shows graphically how the diamond cards map to one another when the transformation

$$R(\mathbf{x}) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \mathbf{x} + \begin{bmatrix} 2 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \tag{2}$$

is iterated (the oval and squiggle cards demonstrate an identical structure). The cycle structure encodes this cyclic behavior as $x_3^9 x_6^9$, since there are nine cycles of length three as well as nine cycles of length six.

Formally, the cycle structure of a transformation is a recording of the iterates of actions of that mapping on a set. Given a transformation, define b_i to be the number of cycles of length i (up to a maximum cycle-length of k). Then the *cycle structure* for the transformation is the monomial $x_1^{b_1} x_2^{b_2} \cdots x_k^{b_k}$, and the *cycle index* for a group is the average of the cycle structures of all the group elements:

$$P_G(x_1, x_2, \ldots, x_k) = \frac{1}{|G|} \sum_{T \in G} x_1^{b_1} x_2^{b_2} \cdots x_k^{b_k}$$

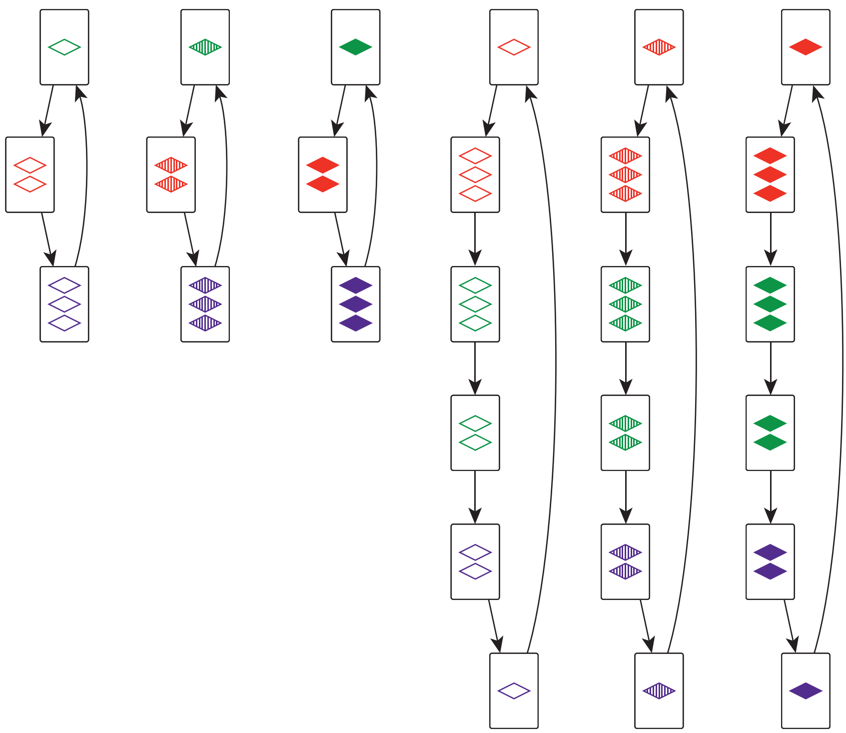


Figure 11 Cycles of diamond cards when Equation (2) is applied to the deck

Pólya's theorem tells us that the pattern inventory for the SET deck, $p(t)$, is computed using the cycle index. Specifically,

$$p(t) = P_G(1 + t, 1 + t^2, \ldots, 1 + t^k).$$

which is shown in FIGURE 2.

In its most general form, Pólya's theorem allows us to consider an arbitrary number of colors and ask questions about colorings using any subset of those colors. For example, we could ask questions about the number of ways to have cards in the deck (d), on the table (t), and in the discard (x). In this case, Pólya's theorem tells us the pattern inventory is

$$p(t, d, x) = P_G(t + d + x, t^2 + d^2 + x^2, \ldots, t^k + d^k + x^k).$$

Observe that an alternative way to compute the pattern inventory in FIGURE 2 is to compute $p(t, 1, 0)$. See the textbooks by Fred S. Roberts [**13**] and Alan Slomson [**15**] for a more detailed introduction to this powerful theorem, and the paper by R. C. Read [**12**] for more advanced applications.

In order to compute the coloring polynomial we must first compute the cycle structure for each element of the group of transformations of the SET deck. The affine group for SET contains over 1.9 billion elements, and computation of the cyclic structure for each element individually would be time consuming and ultimately contain redundant information. Instead, we take advantage of the fact that conjugate elements have the same cyclic structure. Two transformations T_1 and T_2 are *conjugate* to one another if there is some third transformation P such that $PT_1P^{-1} = T_2$. For example, you can check that the transformation T used to generate FIGURE 9 is similar to R by letting

$$P(\mathbf{x}) = \begin{bmatrix} 1 & 1 & 2 & 2 \\ 2 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 2 & 1 \end{bmatrix} \mathbf{x} + \begin{bmatrix} 1 \\ 1 \\ 2 \\ 0 \end{bmatrix}$$

and verifying that $T = PRP^{-1}$. You can read more about conjugacy classes in most basic modern algebra texts (Hoffman [**6**] provides a particularly thorough background). Conjugation allows us to discuss a class of transformations that all behave "the same way" on the SET deck. Decomposing this group of transformations into conjugacy classes will greatly simplify our application of Pólya's theorem.

Because the decomposition of the full group of transformations is a tedious process, we shall illustrate the computation of the coloring polynomial in the 2-dimensional case, where we are looking at the transformations of 9 cards (for example, the solid green cards). This will show the essence of the ideas behind our main result and provide some motivation to study linear algebra over finite fields.

Given an affine transformation $T(\mathbf{x}) = L\mathbf{x} + \mathbf{v}$, we want to characterize the affine transformations conjugate to T. Let $P(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$, so that $P^{-1}(\mathbf{x}) = A^{-1}\mathbf{x} - A^{-1}\mathbf{b}$. Then

$$PTP^{-1}(\mathbf{x}) = A\left(L\left(A^{-1}\mathbf{x} - A^{-1}\mathbf{b}\right) + \mathbf{v}\right) + \mathbf{b} \tag{3}$$

$$= ALA^{-1}\mathbf{x} + \left(A\mathbf{v} + \left(I - ALA^{-1}\right)\mathbf{b}\right). \tag{4}$$

Thus we see that $L\mathbf{x} + \mathbf{v}$ is conjugate to $M\mathbf{x} + \mathbf{w}$ for some vector $\mathbf{w}$ if and only if M and L are conjugate matrices in the linear group $\mathrm{GL}\left(\mathbb{F}_3^2\right)$. So we will need to decompose the linear group into conjugacy classes. Once we do that, however, we need to know when $L\mathbf{x} + \mathbf{v}$ and $L\mathbf{x} + \mathbf{w}$ are conjugate. Again, we conjugate $T(\mathbf{x}) = L\mathbf{x} + \mathbf{v}$ by $P(\mathbf{x}) = A\mathbf{x} + \mathbf{b}$, this time assuming that $ALA^{-1} = L$. This reduces equation (4) to

$$PTP^{-1}(\mathbf{x}) = L\mathbf{x} + (A\mathbf{v} + (I - L)\mathbf{b}). \tag{5}$$

Notice that if $\mathbf{v}$ is in the range of $(I - L)$, say $\mathbf{v} = (I - L)\mathbf{u}$, then we see that $PTP^{-1}(\mathbf{x}) = L\mathbf{x} + (I - L)(A\mathbf{u} + \mathbf{b})$, which implies that $\mathbf{w}$ must also be in the range of $(I - L)$. Further, if we let $\mathbf{b} = -A\mathbf{u}$, then we find that the transformation $T(\mathbf{x}) = L\mathbf{x} + \mathbf{v}$ is in the same conjugacy class as the linear transformation $L(\mathbf{x}) = L\mathbf{x}$ if and only if $\mathbf{v}$ is in the range of $(I - L)$.

With this in mind, let us consider the possibilities for choosing a transformation $T(\mathbf{x}) = L\mathbf{x} + \mathbf{v}$ depending on the dimension of the range of $(I - L)$.

1. Suppose $(I - L)$ has a 2-dimensional range.
   In this case, $T(\mathbf{x}) = L\mathbf{x} + \mathbf{v}$ and $L(\mathbf{x}) = L\mathbf{x}$ are always in the same conjugacy class, since all vectors $\mathbf{v}$ are in the range of $(I - L)$.
2. Suppose $(I - L)$ has a 1-dimensional range.
   Let $T(\mathbf{x}) = L\mathbf{x} + \mathbf{v}$ where $\mathbf{v}$ is not in the range of $(I - L)$. Since our vector space is 2-dimensional, any vector $\mathbf{w}$ can be expressed as $\mathbf{w} = c\mathbf{v} + \mathbf{u}$ for some unique scalar c and some unique $\mathbf{u}$ in the range of $(I - L)$. Conjugating T by the transformation $P_1(\mathbf{x}) = \mathbf{x} + \mathbf{b}$ gives
   $$P_1 T P_1^{-1}(\mathbf{x}) = L\mathbf{x} + (\mathbf{v} + (I - L)\mathbf{b}) .$$
   This implies that $L\mathbf{x} + \mathbf{w}$ is conjugate to $T(\mathbf{x})$ for any $\mathbf{w}$ of the form $\mathbf{w} = \mathbf{v} + \mathbf{u}$. On the other hand we can let $P_2(\mathbf{x}) = 2\mathbf{x} + \mathbf{b}$ and conjugate T to get
   $$P_2 T P_2^{-1}(\mathbf{x}) = L\mathbf{x} + (2\mathbf{v} + (I - L)\mathbf{b}) ,$$
   showing that $L\mathbf{x} + \mathbf{w}$ is also conjugate to T when $\mathbf{w} = 2\mathbf{v} + \mathbf{u}$. Thus when $(I - L)$ is 1-dimensional, we have two conjugacy classes. One consists of the three transformations $L\mathbf{x} + \mathbf{u}$ where $\mathbf{u}$ is in the range of $(I - L)$ while the other consists of the six transformations $L\mathbf{x} + \mathbf{v}$, where $\mathbf{v}$ is not in the range of $(I - L)$.
3. Suppose $(I - L)$ has a 0-dimensional range.
   In this case, $L = I$, and $T(\mathbf{x}) = \mathbf{x} + \mathbf{v}$ is a translation. The identity transformation forms a conjugacy class by itself, while the non-trivial translations form a second conjugacy class (another nice exercise for the reader is to show that any two non-trivial translations are conjugate).

To decompose the linear group $\mathrm{GL}(\mathbb{F}_3^2)$ itself into conjugacy classes we use the *characteristic polynomial* (the polynomial $c(\lambda) = \det(\lambda I - L)$) and the *minimal polynomial* (the polynomial $m(\lambda)$ of least degree such that $m(L) = 0$). Some standard results from linear algebra will be needed:

- Conjugate matrices have the same characteristic polynomial and the same minimal polynomial.
- For any matrix, the characteristic and minimal polynomials have the same irreducible factors.
- The minimal polynomial divides the characteristic polynomial.

In the two-dimensional case, we can say even more: if two 2×2 matrices have the same minimal polynomial and the same characteristic polynomial, then they are conjugate (this is a good exercise for an undergraduate linear algebra course).

Because our matrices are invertible (and thus $\lambda = 0$ cannot be an eigenvalue), there are only six possibilities for the characteristic polynomial. FIGURE 12 provides the six characteristic polynomials with their factorization, the possible corresponding minimal polynomials, and a representative matrix for those polynomials.

There are $8 \times 6 = 48$ invertible matrices to check. However, since there are only $3^4 = 81$ square 2×2 matrices, we can use a simple loop to check all the 2×2 matrices with either *Maple* or *Mathematica* to find the characteristic and minimal polynomial for each matrix to sort the 48 matrices into the six conjugacy classes, omitting any matrix that has determinant zero. Note that even in the four-dimensional case, this inefficiency is only the difference between checking the $(81 - 1) \cdot (81 - 3) \cdot$

Characteristic polynomial	Minimal polynomial	Representative matrix	Class size	Dimension of $(I-L)$
λ^2+1 (irreducible)	λ^2+1	$\begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$	6	2
$\lambda^2+2=(\lambda+2)(\lambda+1)$	λ^2+2	$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$	12	1
$\lambda^2+\lambda+1=(\lambda+2)^2$	$\lambda+2$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	1	0
	$(\lambda+2)^2$	$\begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}$	8	2
$\lambda^2+\lambda+2$ (irreducible)	$\lambda^2+\lambda+2$	$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$	6	2
$\lambda^2+2\lambda+1=(\lambda+1)^2$	$\lambda+1$	$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$	1	2
	$(\lambda+1)^2$	$\begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}$	8	1
$\lambda^2+2\lambda+2$ (irreducible)	$\lambda^2+2\lambda+2$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	6	2

Figure 12 List of conjugacy classes for $\mathrm{GL}(\mathbb{F}_3^2)$

$(81-9)\cdot(81-27)=24{,}261{,}120$ invertible matrices or the complete collection of $3^{16}=43{,}046{,}721$ matrices (a difference of only a few moments of computer time). This provides the size of each conjugacy class in $\mathrm{GL}(\mathbb{F}_3^2)$.

To finish our analysis, we find the conjugacy classes for which the eigenvalue $\lambda=1$ has a 1-dimensional eigenspace. Per the affine group breakdown above, we need to find a vector that is not in the range of $(I-L)$ for the representative matrix L. In FIGURE 12, there are only two matrices that have a 1-dimensional eigenspace for $\lambda=1$: the matrix

$$L=\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$$

for which $(I-L)$ has range $\left[\begin{smallmatrix} a \\ 2a \end{smallmatrix}\right]$, and the matrix

$$L=\begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}$$

for which $(I-L)$ has range $\left[\begin{smallmatrix} 0 \\ a \end{smallmatrix}\right]$. In both cases, we pick the vector $\left[\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right]$ as the designated vector $\mathbf{v}$ not in the range of $(I-L)$.

Thus we find that there are 13 conjugacy classes of transformation in $\mathrm{GA}(\mathbb{F}_3^2)$. For the given representative of each of these classes, we compute the cyclic structure of the class, as was shown in FIGURE 11 for the matrix R from equation 2. A summary of the conjugacy classes, including a chosen representative, the number of elements

Representative $T(\mathbf{x})$	Number of elements	Cyclic structure
$\begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}\mathbf{x}$	$9 \cdot 6$	$x_1x_4^2$
$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\mathbf{x}$	$3 \cdot 12$	$x_1^3x_2^3$
$\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}\mathbf{x}+\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$6 \cdot 12$	x_3x_6
$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\mathbf{x}$	$1 \cdot 1$	x_1^9
$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\mathbf{x}+\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$8 \cdot 1$	x_3^3
$\begin{bmatrix} 0 & 2 \\ 1 & 1 \end{bmatrix}\mathbf{x}$	$9 \cdot 8$	$x_1x_2x_6$
$\begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}\mathbf{x}$	$9 \cdot 6$	x_1x_8
$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}\mathbf{x}$	$9 \cdot 1$	$x_1x_2^4$
$\begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}\mathbf{x}$	$3 \cdot 8$	$x_1^3x_2^3$
$\begin{bmatrix} 0 & 2 \\ 1 & 2 \end{bmatrix}\mathbf{x}+\begin{bmatrix} 1 \\ 0 \end{bmatrix}$	$6 \cdot 8$	x_3^3
$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}\mathbf{x}$	$9 \cdot 6$	x_1x_8

Figure 13 Summary of group structure for $\mathrm{GA}(\mathbb{F}_3^2)$

in the class, and the cyclic structure, is shown in FIGURE 13. Note in the table that the number of elements is listed as $a \cdot \ell$, where ℓ is the number of elements in the conjugacy class of the matrix in $\mathrm{GL}(\mathbb{F}_3^2)$, and a is the multiplicative factor derived from the discussion of the range of $(I - L)$.

From this data, we compute the cyclic structure of $\mathrm{GL}(\mathbb{F}_3^2)$ to be

$$\begin{aligned} P &= \frac{1}{432}\big(54x_1x_4^2 + 36x_1^3x_2^3 + 72x_3x_6 + x_1^9 + 8x_3^3 + 72x_1x_2x_6 + 54x_1x_8 \\ &\quad + 9x_1x_2^4 + 24x_1^3x_2^3 + 48x_3^3 + 54x_1x_8\big) \\ &= \frac{x_1^9}{432} + \frac{7x_3^3}{54} + \frac{x_1x_2^4}{48} + \frac{x_1^3x_3^2}{18} + \frac{x_1^3x_2^3}{12} + \frac{x_3x_6}{6} + \frac{x_1x_4^2}{8} + \frac{x_1x_8}{4} + \frac{x_1x_2x_6}{6}. \end{aligned}$$

We substitute $x_i = (1+t)^i$ into P to yield the coloring polynomial. The coefficient of t^k indicates how many different ways we can draw k cards from the 9-card table:

$$t^9 + t^8 + t^7 + 2t^6 + 2t^5 + 2t^4 + 2t^3 + t^2 + t + 1.$$

For the higher dimensions, complications arise in two key points. First, the characteristic and minimal polynomials will no longer be sufficient for characterizing conjugate matrices. Instead, we have to use the *rational canonical form*, a generalization of the notion of diagonalizing a matrix. Second, the analysis of the affine transformations becomes more complicated when the difference between the dimension of the range of $(I - L)$ and the dimension of the vector space is greater than 1. Nonetheless, with persistence we find the coloring polynomial for the 3-dimensional case in FIGURE 14, and the coloring polynomial for the 4-dimensional case is provided in FIGURE 2 at the beginning of the article. Details on how we worked through these cases are left to a future publication.

$$
\begin{gathered}
t^{27} + \\
t^{26} + t^{25} + 2t^{24} + \\
3t^{23} + 5t^{22} + 10t^{21} + 16t^{20} + 28t^{19} + \\
47t^{18} + 68t^{17} + 91t^{16} + 114t^{15} + 127t^{14} + \\
127t^{13} + 114t^{12} + 91t^{11} + 68t^{10} + 47t^{9} + \\
28t^{8} + 16t^{7} + 10t^{6} + 5t^{5} + 3t^{4} + \\
2t^{3} + t^{2} + t + \\
1
\end{gathered}
$$

Figure 14 The coloring polynomial for 3-dimensional SET

Thus, in terms of the structure of *sets* that can be found, there are 114 essentially distinct ways to draw 12 cards from a 3-dimensional SET deck (say, if you only used diamonds), while there are 41,407 essentially distinct ways to draw those 12 cards from a full 4-dimensional SET deck. The later number represents the number of ways to *start* the game—but what about other stages of the game?

In order to model this temporal relationship, we use Pólya's Theorem with three labels: deck, table, and discard. The resulting polynomial is drastically larger than the one in FIGURE 2, but many of the terms are meaningless to the actual game play. For example, there can never be 13 cards in the deck, 51 on the table and 17 cards in the discard. Unfortunately, even after removing these meaningless cases this grouping still lacks the constraint that the "discard" group is formed by a sequences of *sets*. Thus, Pólya's Theorem alone is not enough to answer such a question. We are currently working on ways to incorporate this constraint into the computation.

Another way to view our result is as a window into the complex structure of the game. With 41,407 different positions using the complete deck, there is a certain kind of depth and variety to the game play. Our experiments with different versions of the game show that there is a fragile balance between the mathematical structure of the game and its playability. For example, consider a deck made of cards with six attributes, each with two possibilities. In this case there are $2^6 = 64$ cards, and a *set* is three cards such that the sum of their six-dimensional vectors is the zero vector, modulus 2. Keeping track of six attributes requires super-human cognitive skills to play. Alternatively, if we take three decks of SET cards and give them each a distinct background, we have a game with $3^5 = 243$ cards, which is both unwieldy to shuffle and cognitively difficult to play.

Ultimately, our study of SET provides a detailed mathematical picture of the elegance of the game. Interestingly, recognition and understanding of the underlying structure does not appear to improve our skill at the game or affect our enjoyment of playing.

REFERENCES

1. Robert A. Bosch, 'Set'less collections of SET cards, *Optima: Mathematical Programming Society Newsletter*, No. 63, January 2000.
2. Kamalika Chaudhuri, Brighten Godfrey, David Ratajczak, and Hoeteck Wee, On the complexity of the game of set, manuscript, 2003.
3. Benjamin Lent Davis and Diane Maclagan, The card game Set. *Mathematical Intelligencer*, **25**(3) (2003) 33–40; http://dx.doi.org/10.1007/BF02984846.
4. M. J. Falco, J. Barker, and M. E. Wallace, The genetics of epilepsy in the British Alsatian, *Journal of Small Animal Practice*, **15**(11) (1974) 685–692; http://dx.doi.org/10.1111/j.1748-5827.1974.tb05651.x.
5. Stuart A. Hansen, The game of Set: an ideal example for introducing polymorphism and design patterns. In Dan Joyce, Deborah Knox, in *Proceedings of the Thirty-Fifth SIGCSE Technical Symposium on Computer Science Education: SIGCSE 2004: Norfolk, Virginia, USA, March 3-7, 2004*, ACM, 2004, 110–114.
6. Kenneth Hoffman and Ray Kunze, *Linear algebra, Second edition*, Prentice-Hall, Englewood Cliffs, N.J., 1971.
7. Judy A. Holdener, Product-free sets in the card game Set, *PRIMUS* **15**(4) (December, 2005) 289–297; http://dx.doi.org/10.1080/10511970508984123.
8. Maureen Jackson, The mathematics behind the game of Set, Master's thesis, Lafayette College, 2006.
9. Donald Knuth, Programs setset, setset-all, and setset-random. http://sunburn.stanford.edu/~knuth/programs.html, accessed July 1, 2011.
10. Anthony Macula and Michael J. Doughty, Set theory using the game Set. http://www.setgame.com/set/set_theory.htm, accessed July 1, 2011.
11. G. Pellegrino, The maximal order of the spherical cap in s4,3, *Matematiche*, 1971.
12. R. C. Read, Pólya's theorem and its progeny, *Math. Mag.*, **60**(5) (1987) 275–282; http://dx.doi.org/10.2307/2690407.
13. Fred S. Roberts, *Applied Combinatorics*, Prentice-Hall Inc., Englewood Cliffs, New Jersey, 1984.
14. Set Enterprises Inc., Set, the family game of visual perception (homepage). http://www.setgame.com/set/index.html, accessed July 1, 2011.
15. Alan Slomson, *An Introduction to Combinatorics*. Chapman and Hall Mathematics, London, England, 1991.
16. N. A. Taatgen, M. van Oploo, J. Braaksma, and J. Niemantsverdriet, How to construct a believable opponent using cognitive modeling in the game of set. In *Proceedings of the fifth international conference on cognitive modeling* (2003) 201–206.
17. Mike Zabrocki, The joy of Set. http://www.math.yorku.ca/~zabrocki/set/joyofset.pdf, accessed July 1, 2011.

Summary We describe the card game SET, and discuss interesting mathematical properties of the game that illustrate ideas from group theory, linear algebra, discrete geometry, and computational complexity. We then suggest a criteria to identify when two card collections are similar to one another and appeal to Pólya's Theorem to determine the number of structurally distinct collections. For example, we find there are 41,407 collections of 12 cards, the layout most commonly seen in gameplay.

BEN COLEMAN earned a B.S. in computer science from Ithaca College in 1997, and M.S. and Ph.D. degrees in computer science from The College of William and Mary in 1999 and 2004. Since then he has been a member of the Mathematics and Computer Science department at Moravian College. He is active in the computer science education community and he regularly engages students to design and implement software that enhances education.

KEVIN HARTSHORN earned a Ph.D. in mathematics at U.C. Berkeley before working his way east to Pennsylvania with visiting positions at U.C. Davis and Oberlin College. He has been teaching mathematics at Moravian College since 2004, where he is currently an associate professor. His focus for both research and teaching is geometry and connections of mathematics to art and design. He has a special interest in raising student enthusiasm in mathematics, whether through the college mathematical society, the local chapter of Pi Mu Epsilon, or helping organize the annual student mathematics conference at Moravian. His interest in SET grew out of his work with the local mathematics club.

Mathematics, Models, and Magz, Part I: Patterns in Pascal's Triangle and Tetrahedron

PETER HILTON
JEAN PEDERSEN
Santa Clara University
Santa Clara, CA 95053-0290
jpedersen@scu.edu

Illustrations by Sylvie Donmoyer
Photographs by Chris Pedersen

This article began with a set of Magz. The authors had just completed an article on binomial coefficients [**4**] and were thinking about possible analogs of their results for trinomial coefficients. The Magz, which are magnetic construction toys, allowed us to build a three-dimensional analog of Pascal's Triangle which we call Pascal's Tetrahedron, and to examine some of its surprising properties. In this article we would like to describe some of our discoveries, and leave you with some questions to ponder.

If you share our interest in these questions, then you, too, may want to acquire a set of Magz or similar magnetic toys. Certainly they were, for us, a remarkable source of intriguing conjectures—some false, some true, and some leading to great generalizations.

In describing our results we will use a very special case of a concept due to George Pólya (1887–1985), which he called *homologues*. As we will see, homologues are special sets of addresses in Pascal's Triangle or in Pascal's Tetrahedron. We will use them to explain and explore the Star of David Theorem for binomial coefficients, and to generalize that theorem. Then we will look at analogues of the Star of David theorem, and its generalizations, involving trinomial coefficients. Because we have the Magz, we can present photographs of the homologues.

First definitions

Binomial coefficients. The symbol $\binom{n}{r\ s}$, where n, r, s are nonnegative integers and $r + s = n$, is the number defined by

$$\binom{n}{n\ \ 0} = \binom{n}{0\ \ n} = 1 \quad \text{for each } n \geq 0, \text{ and}$$

$$\binom{n}{r\ \ s} = \binom{n-1}{r-1\ \ s} + \binom{n-1}{r\ \ s-1} \quad \text{when } n \geq 1.$$

The last line is called *Pascal's identity.* The value of $\binom{n}{r\ s}$ is the coefficient of $a^r b^s$ in the expansion of $(a + b)^n$, and is given by

$$\binom{n}{r\ \ s} = \frac{n!}{r!\,s!}.$$

Math. Mag. **85** (2012) 97–109. doi:10.4169/math.mag.85.2.097.

Trinomial coefficients. The symbol $\binom{n}{r\ s\ t}$, where n, r, s, t are nonnegative integers and $r + s + t = n$, is the number defined by

$$\binom{n}{n\ 0\ 0} = \binom{n}{0\ n\ 0} = \binom{n}{0\ 0\ n} = 1 \quad \text{for each } n \geq 0, \text{ and}$$

$$\binom{n}{r\ s\ t} = \binom{n-1}{r-1\ s\ t} + \binom{n-1}{r\ s-1\ t} + \binom{n-1}{r\ s\ t-1} \quad \text{when } n \geq 1.$$

The last line is again called Pascal's identity. The value of $\binom{n}{r\ s\ t}$ is the coefficient of $a^r b^s c^t$ in the expansion of $(a + b + c)^n$, and is given by

$$\binom{n}{r\ s\ t} = \frac{n!}{r!s!t!}.$$

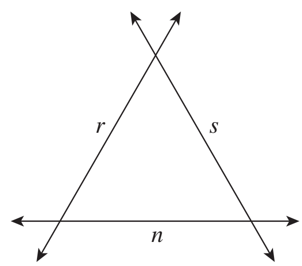
The binomial coefficient $\binom{n}{r\ s}$ is usually written as $\binom{n}{r}$ or $\binom{n}{s}$. We use the expanded notation to emphasize the analogy to trinomial coefficients, and also to highlight the role of the "addresses"; that is, the triples n, r, s that define the coefficients. The binomial addresses naturally arrange themselves into the triangular array known as Pascal's Triangle, shown in FIGURE 1a. The corresponding values are shown in FIGURE 1b. FIGURE 1c illustrates the fact that, when we view the triangle as a geometric object, the coordinate r is constant along upward-sloping diagonals, s is constant along downward-sloping diagonals, and n is constant along horizontal lines.

$$\begin{array}{c} \binom{0}{0\ 0} \\ \binom{1}{0\ 1}\ \binom{1}{1\ 0} \\ \binom{2}{0\ 2}\ \binom{2}{1\ 1}\ \binom{2}{2\ 0} \\ \binom{3}{0\ 3}\ \binom{3}{1\ 2}\ \binom{3}{2\ 1}\ \binom{3}{3\ 0} \\ \binom{4}{0\ 4}\ \binom{4}{1\ 3}\ \binom{4}{2\ 2}\ \binom{4}{3\ 1}\ \binom{4}{4\ 0} \end{array}$$

(a) Addresses

$$\begin{array}{c} 1 \\ 1 \quad 1 \\ 1 \quad 2 \quad 1 \\ 1 \quad 3 \quad 3 \quad 1 \\ 1 \quad 4 \quad 6 \quad 4 \quad 1 \end{array}$$

(b) Values of the coefficients



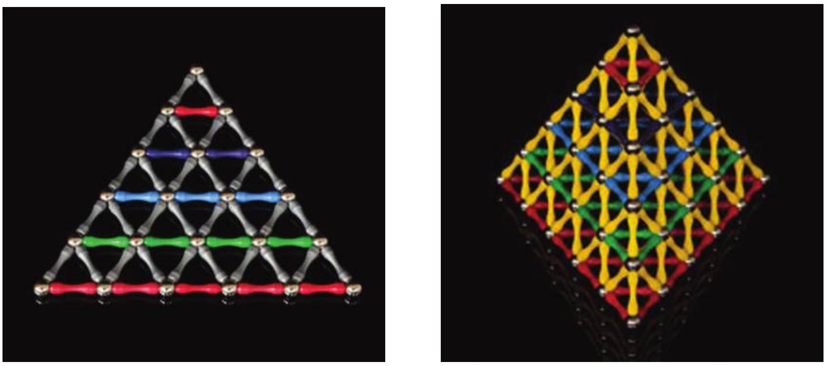
(c) Lines of constant n, r, s

Figure 1 Addresses, values, and lines of constant n, r, s in Pascal's Triangle

The photographs in FIGURE 2 show the locations of the binomial coefficients in a plane and of the trinomial coefficients in space.

One way to think of the tetrahedron is in terms of its *layers*. The layers are planes with constant n, and in FIGURE 2b they are represented by planes of constant color. In FIGURE 3a we display the addresses of the trinomial coefficients, and the corresponding numerical values appear in FIGURE 3b. Think of these as the layers stacked up from the top down as in FIGURE 2b. FIGURE 3c shows the constant planes and FIGURE 3d shows the constant directions, at layer n, for Pascal's Tetrahedron.

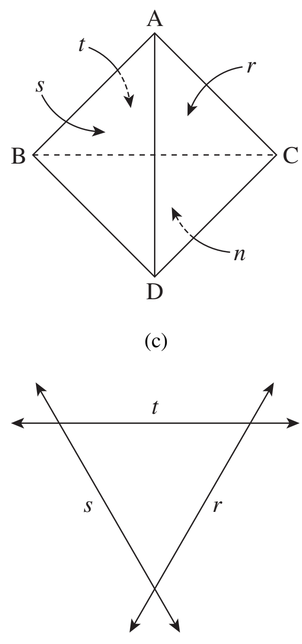
Homologues. We need also the concept of *homolgues*, which, as we have said, is due to the mathematician and expositor George Pólya. Pólya often spoke of homologues but never wrote about them explicitly. However, we were fortunate to enjoy a relaxed, friendly relationship with Pólya in his later years, and he asked us to write about this idea on his behalf—which we have now done [**3**, pp. 172–193]. Here we introduce a simplified definition, suitable for our setting.



(a) (b)

Figure 2 (a) Triangle in a plane; (b) Tetrahedron in space

$$
\begin{array}{lc}
n=0: & \binom{0}{0\ 0\ 0} \\[1em]
n=1: & \binom{1}{1\ 0\ 0}\binom{1}{0\ 1\ 0} \\
 & \binom{1}{0\ 0\ 1} \\[1em]
n=2: & \binom{2}{2\ 0\ 0}\binom{2}{1\ 1\ 0}\binom{2}{0\ 2\ 0} \\
 & \binom{2}{1\ 0\ 1}\binom{2}{0\ 1\ 1} \\
 & \binom{2}{0\ 0\ 2} \\[1em]
n=3: & \binom{3}{3\ 0\ 0}\binom{3}{2\ 1\ 0}\binom{3}{1\ 2\ 0}\binom{3}{0\ 3\ 0} \\
 & \binom{3}{2\ 0\ 1}\binom{3}{1\ 1\ 1}\binom{3}{0\ 2\ 1} \\
 & \binom{3}{1\ 0\ 2}\binom{3}{0\ 1\ 2} \\
 & \binom{3}{0\ 0\ 3}
\end{array}
\qquad
\begin{array}{c}
1 \\[1em]
1 \quad 1 \\
1 \\[1em]
1 \quad 2 \quad 1 \\
2 \quad 2 \\
1 \\[1em]
1 \quad 3 \quad 3 \quad 1 \\
3 \quad 6 \quad 3 \\
3 \quad 3 \\
1
\end{array}
$$



(a) (b)

Figure 3 (a) Addresses in Pascal's Tetrahedron; (b) Values of the coefficients; (c) Planes of constant n, r, s, t; (d) At level n, lines of constant r, s, t

Start with n pairwise-disjoint sets of addresses in Pascal's Triangle (or Pascal's Tetrahedron), with each set consisting of q addresses. Furthermore, the sets of addresses must be congruent, when seen as geometric figures. Then these sets of addresses are called *homologues* (of each other), or *a set of homologues*, if each is the image of any of the others under a proper rotation in 2 or 3 dimensions.

FIGURE 5 serves as an example with $n = 2$ and $q = 3$. The figure highlights the 6 addresses surrounding a particular address in Pascal's Triangle. We take the central point to be $\binom{n}{r\ s}$. The 6 addresses define a regular hexagon. In the figure, they are partitioned into 2 sets marked ♣ and ◇, each consisting of 3 addresses forming an equilateral triangle. A rotation of $\pm 60°$ maps either set onto the other, so they are homologues of each other.

Known results

In the last half century, patterns have been identified in Pascal's Triangle that can be moved to any location in the triangle and preserve certain numerical relationships among the coefficients in the patterns. Often these turn out to involve homologues. One of the beautiful patterns involves the homologues of FIGURE 5. Wherever the pattern is centered, these 6 coefficients have the interesting property that the products of the coefficients in each of the two homologues are the same, say N. Consequently, the product of all six vertices of the hexagon forms a perfect square N^2. This result (from [**6**, p. 120]) is also shown in FIGURE 4 where the symbol $\bigstar = \binom{n}{r\ s}$ marks the center of the array. With the homologues labeled $\clubsuit$ and $\diamondsuit$ we may state this briefly as:

$$\prod \clubsuit = \prod \diamondsuit.$$

This result is known as the *Star of David Theorem*.

$$\begin{array}{ccccc} & \clubsuit & & \diamondsuit & \\ \diamondsuit & & \bigstar & & \clubsuit \\ & \clubsuit & & \diamondsuit & \end{array}$$

Figure 4 The Star of David Theorem: $\prod \clubsuit = \prod \diamondsuit$

$$\begin{array}{ccccc} & \binom{n-1}{r-1\ \ s}_{\clubsuit} & & \binom{n-1}{r\ \ s-1}_{\diamondsuit} & \\ \binom{n}{r-1\ \ s+1}_{\diamondsuit} & & \bigstar & & \binom{n}{r+1\ \ s-1}_{\clubsuit} \\ & \binom{n+1}{r\ \ s+1}_{\clubsuit} & & \binom{n+1}{r+1\ \ s}_{\diamondsuit} & \end{array}$$

Figure 5 The addresses for the lattice points in FIGURE 4, with subscripts to show the $\clubsuit$ and $\diamondsuit$ homologues

A straightforward algebraic proof involves writing out each of the binomial coefficients of FIGURE 5 and computing the products directly. One then finds that

$$\prod \clubsuit = \prod \diamondsuit = \frac{(n-1)!\, n!\, (n+1)!}{(r-1)!\, r!\, (r+1)!\, (s-1)!\, s!\, (s+1)!}.$$

It is possible, however, using what we have observed about the geometry of Pascal's Triangle, to give a much easier proof that works not only for this theorem but for others like it.

A geometric proof of the Star of David Theorem

First, in FIGURE 5, observe that along any horizontal line (where n is fixed) through any $\clubsuit$ or $\diamondsuit$, there are the same number of $\clubsuit$ and $\diamondsuit$ (exactly one of each in this case). This ensures the *same* entry in the n position for that pair of coefficients. Next, observe that along any upward sloping line (where r is fixed) through any $\clubsuit$ or $\diamondsuit$, there are the same number of $\clubsuit$ and $\diamondsuit$ (again, one of each in this case), which ensures the *same* entry in the r position for that pair of lattice points. The same thing happens on the downward-sloping lines, where s is fixed. We have guaranteed that every $\clubsuit$ and every $\diamondsuit$ in the array has horizontal, upward-sloping, and downward-sloping lines passing through it that pair it with lattice-point "partners" of a different suit. Since each side of the equation has the same contributions from n, the same contributions from r, and the same contributions from s, we conclude that $\prod \clubsuit = \prod \diamondsuit$.

In FIGURE 6 we have eliminated $\bigstar$ and drawn the lines slightly offset so that they don't obscure the symbols. A small triangle is thereby created about each $\clubsuit$ and each $\diamondsuit$. Looking ahead, it turns out that the analogue of this proof for trinomial coefficients (where lines are replaced with planes) will create a small tetrahedron about each suit symbol.

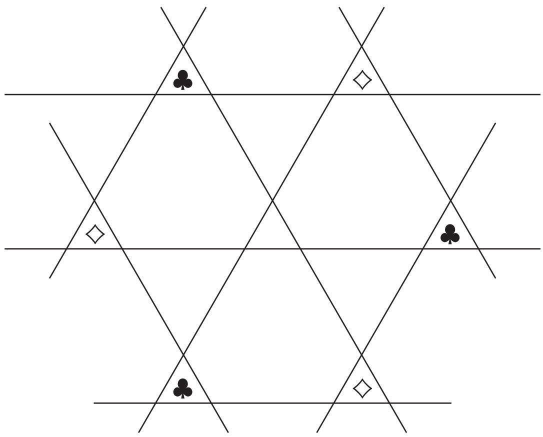


Figure 6 Geometric proof of the Star of David Theorem: $\prod \clubsuit = \prod \diamondsuit$

A generalization. In [**2**, pp. 211–216] and [**3**, pp. 172–192] we discovered, using sliding parallelograms, a generalization of the Star of David Theorem. The most useful way to describe that result is as follows.

In Pascal's Triangle, take an equilateral triangle of lattice points with edge-length k that points *up*. Truncate from each corner an equilateral triangle of edge-length ℓ, with $0 < \ell < k/2$, to obtain a semi-regular hexagon whose vertices are all lattice points. This is shown in a typical case in FIGURE 7, where $\bigstar = \binom{n}{r\;s}$, $k = 8$, $\ell = 2$. It is then the case that $\prod \heartsuit = \prod \spadesuit$ and, once again, the homologues are two equilateral triangles (this time within a semi-regular hexagon). The geometric proof provides a very quick way to see that this assertion is true.

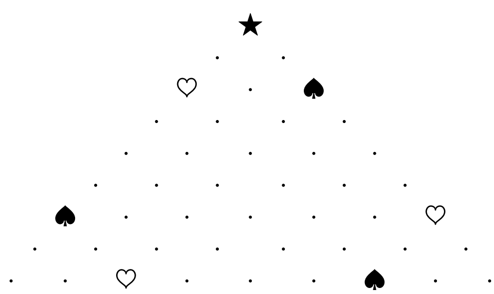


Figure 7 A more general Star of David theorem: $\prod \heartsuit = \prod \spadesuit$

In the papers [**1**, pp. 337–346], [**5**, pp. 351–356, 420], [**6**, p. 120], [**7**, pp. 252–255] the authors always placed reference points $\bigstar = \binom{n}{r\ s}$ at the center of each pattern, thus restricting their results to patterns with centers at a lattice point. But since the reference point plays no role in the proof, no such restriction is required. Here we place a reference point $\bigstar$ *outside* the pattern, at the apex of the original triangle. This suffices to define the addresses in the configuration.

To prove that $\prod \heartsuit = \prod \spadesuit$ we may either work out the addresses and check the arithmetic, or draw the 9 lines, three parallel lines in each of the n, r, and s directions, to verify the geometric proof.

If an equilateral triangle of edge-length ℓ is truncated from each vertex of a triangle of edge-length $k = 3\ell$, the result is a regular hexagon (of edge-length ℓ), rather than a semi-regular hexagon, and so produces a symmetrical Star of David of arbitrary size.

Moving to the tetrahedron

Hoggatt and Alexanderson [**5**] begin with the following abstract:

> The multinomial coefficients "surrounding" a given multinomial coefficient in a generalized Pascal pyramid are partitioned into subsets such that the product of the coefficients in each subset is a constant N and such that the product of the coefficients "surrounding" a given m-nomial coefficient is N^m....

In this article we are only concerned with the trinomial case $m = 3$:

HOGGATT-ALEXANDERSON THEOREM (from [**5**], with $m = 3$). *The* 12 *trinomial coefficients surrounding a given trinomial coefficient,* $\binom{n}{r\ s\ t}$, *may be partitioned into* 3 *subsets such that the product of the coefficients in each subset is a constant N and such that the product of all the coefficients "surrounding" a given trinomial coefficient is* N^3.

The right-hand part of FIGURE 8 shows the Magz model of these 12 coefficients. On the surface of this figure one can see the vertices (balls) and edges (rods) of a cuboctahedron.* The left-hand part of FIGURE 8 shows how the magnetic model is embedded within the Pascal Tetrahedron.

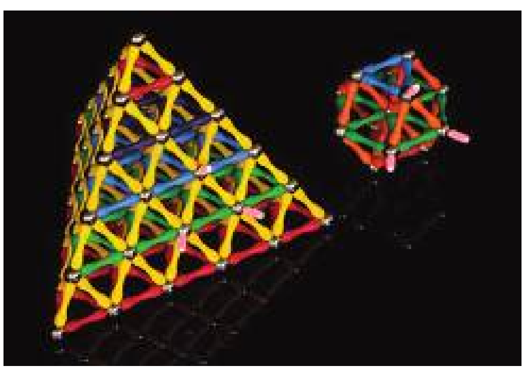


Figure 8 On the right the 12 neighbors to $\binom{n}{r\ s\ t}$ are at the vertices of a cuboctahedron. The rods extending from the vertices of the front triangle on the cuboctahedron correspond with the extended rods of the same triangular face embedded within a Pascal Tetrahedron on the left.

*The cuboctahedron has 6 square and 8 regular triangular faces, with every vertex surrounded by the same arrangement of faces. It is one of the 13 semi-regular polyhedra known as the Archimedean solids.

Level $n-1$:	$\binom{n-1}{r-1\ s\ t}_{\diamondsuit}$ $\binom{n-1}{r\ s-1\ t}_{\clubsuit}$ $\binom{n-1}{r\ s\ t-1}_{\heartsuit}$
Level n:	$\binom{n}{r-1\ s\ t+1}_{\clubsuit}$ $\binom{n}{r\ s-1\ t+1}_{\diamondsuit}$ $\binom{n}{r-1\ s+1\ t}_{\heartsuit}$ $\bigstar$ $\binom{n}{r+1\ s-1\ t}_{\heartsuit}$ $\binom{n}{r\ s+1\ t-1}_{\diamondsuit}$ $\binom{n}{r+1\ s\ t-1}_{\clubsuit}$
Level $n+1$:	$\binom{n+1}{r\ s\ t+1}_{\heartsuit}$ $\binom{n+1}{r\ s+1\ t}_{\clubsuit}$ $\binom{n+1}{r+1\ s\ t}_{\diamondsuit}$

Figure 9 The trinomial coefficients at levels $n-1$, n, and $n+1$ for the cuboctahedron of FIGURE 8. We find that $\prod\clubsuit = \prod\diamondsuit = \prod\heartsuit$.

To prove that the product of all the vertices on the boundary of the cuboctahedron is a perfect cube, say N^3, simply multiply together all of the trinomial coefficients whose addresses are explicitly given in FIGURE 9, surrounding $\bigstar = \binom{n}{r\ s\ t}$. Remembering that $\binom{n}{r\ s\ t} = \frac{n!}{r!s!t!}$, we readily see that the product of these 12 coefficients is

$$\left\{\frac{(n-1)!\,[n!]^2(n+1)!}{(r-1)!\,(s-1)!\,(t-1)!\,[r!]^2\,[s!]^2\,[t!]^2\,(r+1)!\,(s+1)!\,(t+1)!}\right\}^3 = N^3.$$

The subscripts in FIGURE 9 indicate the $\clubsuit$, $\diamondsuit$, and $\heartsuit$ homologues, each consisting of 4 lattice points in the Pascal Tetrahedron.* Now, since the Star of David Theorem for binomial coefficients has two homologues, each of which is an equilateral triangle, we guess that the 3 homologues here will be the vertices of a tetrahedron, but we need to check this out. In FIGURE 10 we show a topographical illustration of the vertices of the cuboctahedron as seen when looking straight down towards the center of the model through the triangular face lying in the plane where $n-1$ is constant; that is, the top triangular face in the cuboctahedron of FIGURE 8. Similar topographical illustrations could be drawn looking straight towards the center of the model through a triangular face lying in the plane where $r-1$, $s-1$, or $t-1$ are fixed.

It is then a straightforward computation to show that

$$\prod\clubsuit = \prod\diamondsuit = \prod\heartsuit$$
$$= \frac{(n-1)!\,[n!]^2\,(n+1)!}{(r-1)!\,(s-1)!\,(t-1)!\,[r!]^2\,[s!]^2\,[t!]^2\,(r+1)!\,(s+1)!\,(t+1)!} = N.$$

With the magnetic model in hand it is, in fact, very easy to give a geometric proof completely analogous to that given for the Star of David Theorems in the plane. One need only verify that each of the 4 planes passing through the boundary points of the cuboctahedron, in each of the 4 four directions n, r, s, and t, contains the same number of $\clubsuit$, $\diamondsuit$, and $\heartsuit$, so that each $\clubsuit$, $\diamondsuit$, and $\heartsuit$ lies in a plane with matching symbols of the

*This partition of the 12 points is not unique. There are other partitions that satisfy the product property, but we have not found any other partitions that produce homologues.

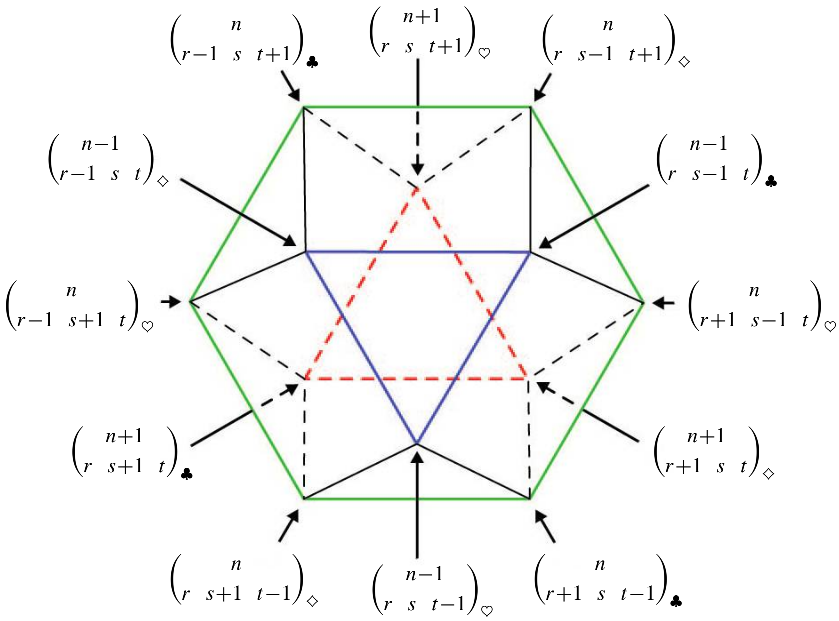


Figure 10 A topographical diagram of the cuboctahedron in FIGURE 8

other two types. If these planes were offset slightly, each symbol would be surrounded by a small tetrahedron (which is analogous to the small triangles surrounding each suit in FIGURE 6).

Now we check to see if the three homologues are, in fact, in the shape of tetrahedra. Surprisingly, they are not! Our guess was wrong! With the model in hand, or with FIGURE 10, one quickly sees that the 4 vertices connecting either the ♣, ◇, and ♡ form, in fact, a square! The squares are, of course, still homologues, but they don't have the shape we expected.

Understanding the 3-dimensional analogues

It was this unexpected discovery that led us to get out the Magz and try to understand the situation better. We first conjectured that the way to generalize the more general Star of David Theorem to trinomial coefficients was to begin with a regular tetrahedron within the Pascal Tetrahedron and then truncate a smaller tetrahedron from each vertex, obtaining a truncated tetrahedron, as shown in FIGURE 11.

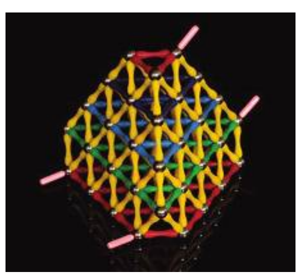


Figure 11 The result of truncating a unit tetrahedron from each vertex of a tetrahedron of edge-length 5. The rods protruding from the vertices correspond with the vertices labeled ♡ in FIGURE 12.

The addresses for the vertices of the models of the form shown in FIGURE 11 are expressed in terms of the address of the top lattice point, $\binom{n}{r\ s\ t}$, of the original tetrahedron (before truncation). (The centers of regular tetrahedra within Pascal's Tetrahedron are not necessarily lattice points, so we can't reliably choose the center as a reference point.) Thus, when a regular tetrahedron of integer edge-length k has cut off from each vertex a tetrahedron of integer edge-length ℓ, where $0 < \ell < k/2$, the addresses, at levels $n + \ell$, $n + k - \ell$, and $n + k$ may be expressed according to level as shown by the topographical diagram in FIGURE 12.

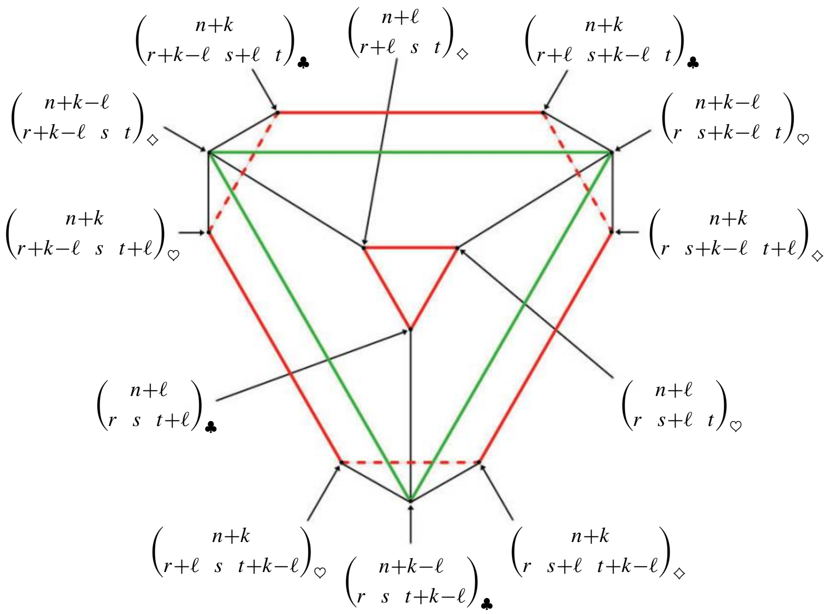


Figure 12 A topographical diagram generalizing the polyhedron of FIGURE 11, where a tetrahedron with integer edge-length k, with top vertex at $\binom{n}{r\ s\ t}$, has cut off from each vertex a tetrahedron of integer edge-length ℓ, where $0 < \ell < k/2$.

In FIGURE 12,

$$\prod \clubsuit = \prod \diamondsuit = \prod \heartsuit$$

$$= \frac{(n+k-\ell)!\,(n+\ell)!\,[(n+k)!]^2}{(r!)^2\,(s!)^2\,(t!)^2\,(r+\ell)!\,(s+\ell)!\,(t+\ell)!\,(r+k-\ell)!\,(s+k-\ell)!\,(t+k-\ell)!}.$$

Once again each of the three homologues has 4 vertices, but this time each homologue is a special *semi-regular tetrahedron* whose faces are isosceles triangles with the 2 shortest edges being perpendicular to each other in space as can be seen by studying FIGURE 11.

This generalization still didn't explain the Hoggatt-Alexanderson result. So we considered what happens when you begin with a regular tetrahedron and truncated each edge. We will explain this with a particular, but not special, case to illustrate what happens.

Beginning with a 5-unit tetrahedron whose top vertex is located at $\binom{n}{r\ s\ t}$ we truncate each edge by 1 unit to obtain the polyhedron shown in FIGURE 13.

If the top of the original 5-unit tetrahedron is located at $\binom{n}{r\ s\ t}$ then the addresses for the trinomial coefficients at the three levels are as shown in FIGURE 14, with suit subscripts indicating the partitioning of the 12 vertices into 3 sets, each of which is a

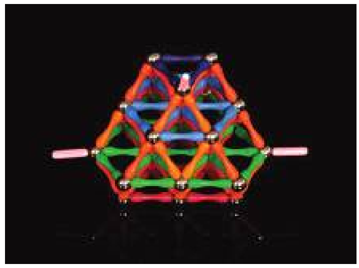


Figure 13 A 5-unit tetrahedron with 1 unit truncated from each edge. The protruding rods correspond with the vertices labeled ◇ in FIGURE 14. The ◇ vertex at the top in FIGURE 14 is not visible in this photograph.

semi-regular tetrahedral homologue, and for each of which the product of the trinomial coefficients at their vertices is the same number, N (and, consequently, the product of all 12 vertices is N^3).

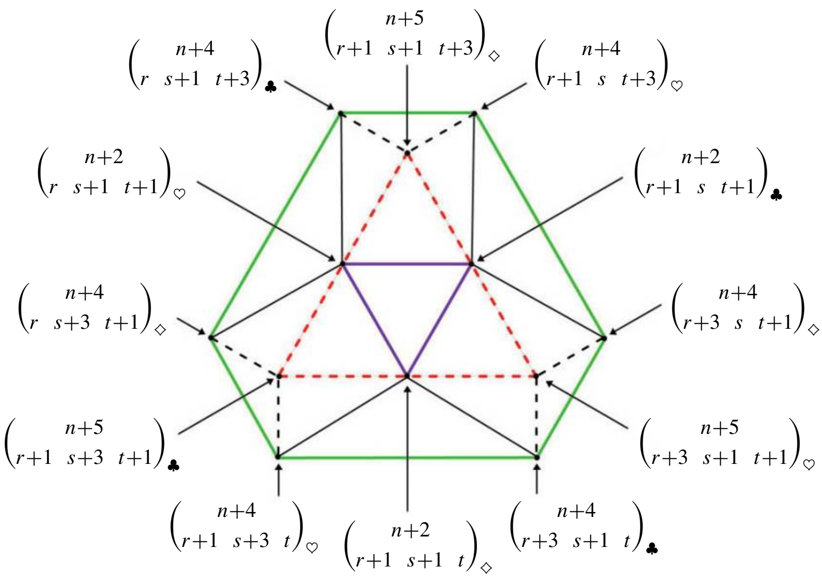


Figure 14 A topographical diagram of the polyhedron of FIGURE 13

Thus, in each of the homologues for the truncated tetrahedron shown in FIGURES 13 and 14,

$$\prod \clubsuit = \prod \diamondsuit = \prod \heartsuit$$
$$= \frac{(n+5)!\,[(n+4)!]^2\,(n+2)!}{(r!\,s!\,t!)\,[(r+1)!]^2\,[(s+1)!]^2\,[(t+1)!]^2\,(r+3)!\,(s+3)!\,(t+3)!} = N.$$

When the truncation results in genuine rectangles, the partition results in homologues that form interpenetrating *tetrahedra*. (The vertices of one such tetrahedron are shown by the short rods sticking out from its vertices in FIGURE 13.) However, when the dimensions of the truncation with relation to the original tetrahedron are such that the quadrilaterals become squares, then the partitioned sets become the vertices of *squares* on a cuboctahedron (see FIGURE 8). And now we can see that the Hoggatt-Alexanderson theorem may be regarded as the degenerate case of the edge truncation of a regular tetrahedron.

But that isn't the end of the story, for if in FIGURE 12 the value of k is an even number, then the choice of $\ell = k/2$ produces an octahedron where the two distinct vertices along the edge of the original large tetrahedron coalesce, producing a regular octahedron having only 6 vertices. So let us look more carefully (see FIGURE 15) at a typical (or perhaps special) case; namely when $k = 4$ and $\ell = 2$.

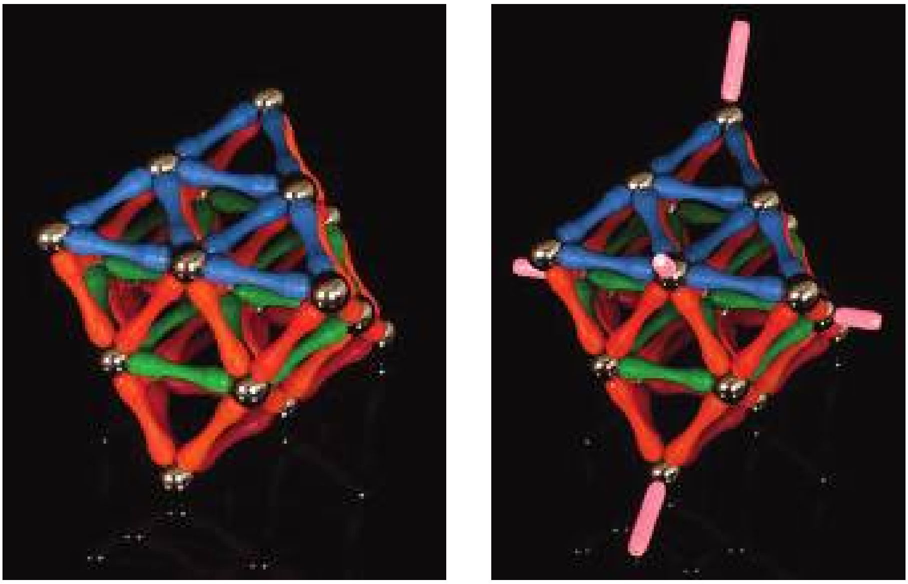


Figure 15 (a) The octahedron resulting from truncating a 2-unit tetrahedron from each vertex of a 4-unit tetrahedron. (b) The octahedron in Figure (a), where short protruding rods identify the "equator" and long protruding rods identify the north and south poles of one of the 3 octahedral homologues. The 5 visible rods that you can see correspond to 5 of the ♣ symbols in FIGURE 16 (the ♣ at "1 o'clock" in FIGURE 16 is not visible in this photograph)

Now we see that, for this special octahedron of edge-length 2, the product of its 6 vertices is

$$\left(\frac{(n+2)!\,(n+4)!}{r!\,(r+2)!\,s!\,(s+2)!\,t!\,(t+2)!}\right)^3,$$

and the 3 homologues are the line segments joining opposite vertices. (These are the vertices of the biggest hexagon in the FIGURE 16.) However, if you were to truncate at each of this octahedron's vertices a 1-unit square pyramid, this figure would be the Hoggatt-Alexanderson polyhedron, and we already know that for that polyhedron we have 3 homologues that are squares. If we put these two facts together we get another surprising result; namely, the product of the 18 lattice points on the boundary of the octahedron in FIGURE 15 (whose addresses are displayed in FIGURE 16) is

$$\left[\left(\frac{(n+2)!\,(n+3)!\,(n+4)!}{r!\,(r+1)!\,(r+2)!\,s!\,(s+1)!\,(s+2)!\,t!\,(t+1)!\,(t+2)!}\right)^2\right]^3,$$

and each of the 3 homologues is an *octahedron*(!) (where the side length of the polygon about the octahedron's "equator" is shorter than the side lengths that go from the equator to the north and south "poles"). The rods sticking out from the edges in FIGURE 15b show one such homologue. Another feature of these homologues that is *different* from our preceding examples is that the product of the 6 trinomial coefficients of each individual homologue is a perfect square. This may be seen from the fact that two elements from each homologue lie in each of the n, r, s, and t planes. This naturally raises the question as to whether we can find other analogous sets of homologues for binomial coefficients—and whether we can find a set of homologues, in either the binomial or trinomial coefficients, where each individual homologue is a perfect cube, fourth power, or something else.

In FIGURE 16 the six points that are the vertices of the big outer hexagon are, in the Pascal Tetrahedron, the vertices on an octahedron, so products of pairs of the corresponding trinomial coefficients are equal. The remaining 12 points (the points of bisection of the edges of the octahedron) are, of course, the vertices of a cuboctahedron.

FIGURE 10 is also a cuboctahedron, and the two may be made compatible by the substitutions of $r-1$ for r, $s-1$ for s, $t-1$ for t, and $n-3$ for n in the 12 points of FIGURE 16.

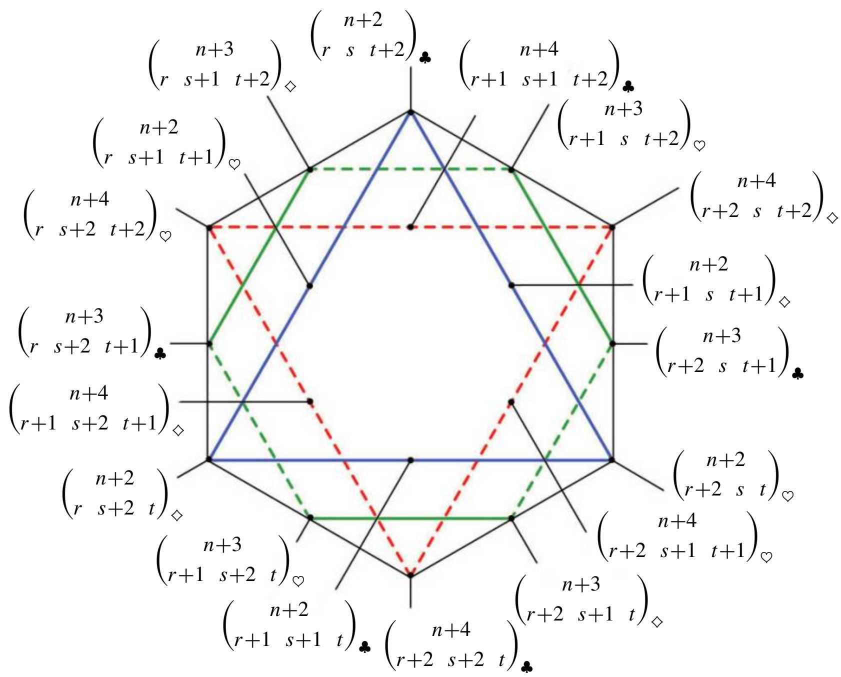


Figure 16 A topographical view of the model shown in FIGURE 15, assuming that the top of the original tetrahedron, before truncation, was $\binom{n}{r\ s\ t}$

Now we have yet another way to view the Hoggatt-Alexanderson result. But we also have many more questions. For example, if we consider all of the boundary points on our previous constructions can we obtain suitable homologues for those lattice points? The number of vertices involved along all the edges is a multiple of 3, so it looks plausible.

Thus, although we have come some way in understanding the analogue of the Star of David Theorem for trinomial coefficients, we are convinced that we are a long way from understanding the general situation for multinomial coefficients—and there may even be much more to explore for the trinomial coefficients. However, we are content, for the moment, to stop here and let interested readers pursue these matters on their own.

We hope you will want to find some magnetic toys and begin your own explorations!

In Part II, by one of the authors (JP) and her student, Victor Garcia, a generalization of the edge-truncated tetrahedron is discussed and analogues of both the vertex-truncated and edge-truncated tetrahedron are carried out in Pascal simplex. In this investigation the authors use the restriction that $\ell < k/3$ in the edge-truncated case so that they avoid the complexities of the degenerate cases above (and leave them for others to study).

Acknowledgment The authors would like to thank Gerald Alexanderson, Victor Garcia, Peter Ross, Geoffrey Shephard, and the referees for their helpful comments, and contributions to, various versions of this manuscript.

REFERENCES

1. H. W. Gould, Equal products of generalized binomial coefficients, *Fibonacci Quarterly* **9** (1971) 337–346.
2. Peter Hilton, Derek Holton, and Jean Pedersen, *Mathematical Reflections—In a Room with Many Mirrors*, 2nd printing, Springer Verlag, N. Y. (1998).
3. Peter Hilton, Derek Holton, and Jean Pedersen, *Mathematical Vistas—From a Room with Many Windows*, Springer Verlag, N. Y. (2002).
4. Peter Hilton and Jean Pedersen, Stop-sign theorems and binomial coefficients, *Mathematical Gazette* **94** (2010) 247–261.
5. V. E. Hoggatt, Jr., and G. L. Alexanderson, A property of multinomial coefficients, *Fibonacci Quarterly* **9** (1971), 351–356, 420.
6. V. E. Hoggatt and W. Hansell, The hidden hexagon squares, *Fibonacci Quarterly* **9** (1971), 120.
7. Calvin T. Long, Arrays of binomial coefficients whose products are squares, *Fibonacci Quarterly* **11** (1973), 449–456.
8. Calvin T. Long and Verner E. Hoggatt, Jr., Sets of binomial coefficients with equal products, *Fibonacci Quarterly* **12** (1974), 71–79.
9. Calvin T. Long and Shiro Ando, Another generalization of Gould's Star of David Theorem, *Fibonacci Quarterly* **30** (1992), 251–255.
10. Zalman Usiskin, Perfect square patterns in the Pascal triangle, *Math. Mag.* **46** (1973), 203–208; http://dx.doi.org/10.2307/2688302.

Summary This paper describes how the authors used a set of magnetic toys to discover analogues in 3 dimensions of well known theorems about binomial coefficients. In particular, they looked at the Star of David theorem involving the six nearest neighbors to a binomial coefficient $\binom{n}{r}$. If one labels the vertices of the bounding hexagon with the numbers 1, 2, 3, 4, 5, 6, consecutively (in either direction), then the product of the coefficients with even labels is the same as the product as the coefficients with odd labels. Furthermore the two figures formed by connecting the odd and even vertices are both equilateral triangles arranged so that a rotation of $\pm 60°$ exchanges the triangles. There is a generalized Star of David theorem concerning a semi-regular hexagon with similar results. The paper describes analogous results for trinomial coefficients involving, sometimes but not always, tetrahedra instead of triangles.

PETER HILTON (1923–2010) began his mathematical career at the age of 18. He was "drafted" during his freshman year at Oxford, in January of 1942, and sent to work decoding German codes at Bletchley Park during WWII. After the war he was awarded an M.A. at Oxford in 1948, a D.Phil. from Oxford in 1950, and a Ph.D. from Cambridge in 1952. Subsequently he became a world-renowned algebraic topologist. However, he had an interest in all things mathematical. He worked on any mathematical problem that piqued his interest and maintained, until the time of his death, an enthusiasm for mathematical problems and their solutions. This is the last paper on which he worked.

JEAN PEDERSEN began her mathematical career many years later than Peter Hilton. She has mathematical interests in polyhedral geometry, combinatorics and number theory. Jean and Peter co-authored 144 papers and 6 books. Their most recent book, *A Mathematical Tapestry: Demonstrating the Beautiful Unity of Mathematics* (Cambridge University Press, 2010) chronicles many of their discoveries over the past 30 years. The current paper is a result of questions that arose when she taught Combinatorics at Santa Clara University. A sequel to this paper, written with her student, Victor Garcia, will appear soon in this MAGAZINE.

NOTES

Picturing Irrationality

STEVEN J. MILLER
Williams College
Williamstown, MA 01267
Steven.J.Miller@williams.edu

DAVID MONTAGUE
University of Michigan
Ann Arbor, MI 48109
davmont@umich.edu

Proving the irrationality of $\sqrt{2}$ is a rite of passage for mathematicians. The purpose of this note is to spread the word of a remarkable geometric proof, and to generalize it. The proof was discovered by Stanley Tennenbaum [**9**] in the 1950's, and first appeared in print in an article by John H. Conway [**3**]. Details omitted here can be found in our arXiv post [**8**].

Tennenbaum's proof

We now describe Tennenbaum's wonderful geometric proof of the irrationality of $\sqrt{2}$. Suppose that $\sqrt{2} = a/b$ for some positive integers a and b; then $a^2 = 2b^2$. We may assume that a is the smallest positive integer for which this is possible. We interpret this geometrically by constructing a square of side a and, within it, two squares of side b (see FIGURE 1). Since the combined areas of the squares of side b equals the area of the square of side a, the shaded, doubly-counted square must have the same area as the two white squares. We have therefore found a smaller pair of integers u and v with $u^2 = 2v^2$, which is a contradiction. Thus $\sqrt{2}$ is irrational.

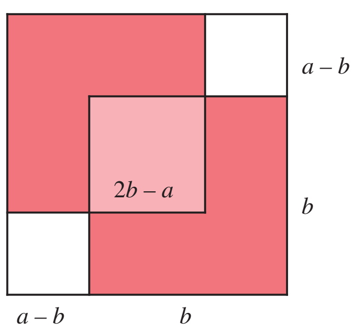


Figure 1 Geometric proof of the irrationality of $\sqrt{2}$

Math. Mag. **85** (2012) 110–114. doi:10.4169/math.mag.85.2.110. © Mathematical Association of America

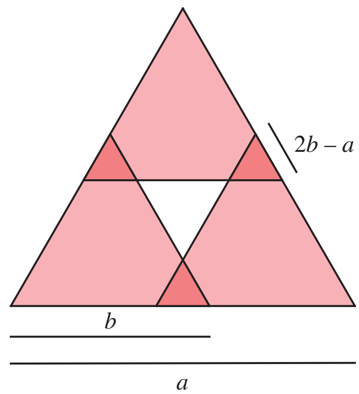


Figure 2 Geometric proof of the irrationality of $\sqrt{3}$. The white equilateral triangle in the middle has sides of length $2a - 3b$.

The square root of 3 is irrational

We generalize Tennenbaum's geometric proof to show $\sqrt{3}$ is irrational. Suppose not; then $\sqrt{3} = a/b$, and again we may assume that a and b are the smallest positive integers satisfying $a^2 = 3b^2$. As the area of an equilateral triangle is proportional to the square of its side s (the area is $s^2 \cdot \sqrt{3}/4$), we may interpret $a^2 = 3b^2$ as the area of one equilateral triangle of side length a being equal to the area of three equilateral triangles of side length b. We represent this in FIGURE 2, which consists of three equilateral triangles of side length b placed at the corners of an equilateral triangle of side length a. Note that the area of the three doubly covered, shaded triangles (which have side length $2b - a$) is therefore equal to that of the uncovered, equilateral triangle in the middle (which has integral sides of length $2a - 3b$). This is clearly a smaller solution, and a contradiction!

The square root of 5 is irrational

For the irrationality of $\sqrt{5}$ we have to modify our approach, as the overlapping regions are not so nicely shaped (see FIGURE 3).

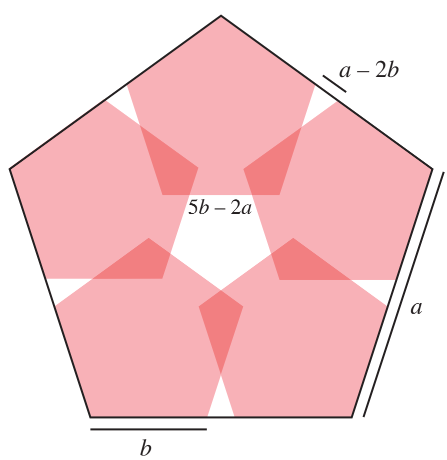


Figure 3 Geometric proof of the irrationality of $\sqrt{5}$

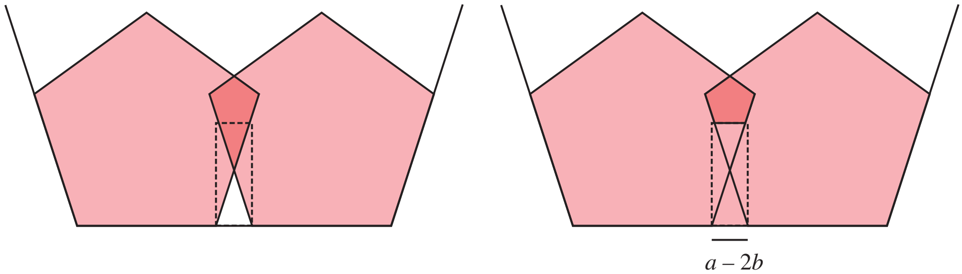


Figure 4 Geometric proof of the irrationality of $\sqrt{5}$: the kites, triangles and the small pentagons. The small pentagon has sides of length $a - 2b$.

Suppose $a^2 = 5b^2$ with, as always, a and b minimal. We place five regular pentagons of side length b at the corners of a regular pentagon of side length a.

Note that this gives five small triangles on the edge of the larger pentagon which are uncovered, one uncovered regular pentagon in the middle of the larger pentagon, and five kite-shaped doubly covered regions. As before, the doubly covered regions must have the same combined area as the uncovered regions.

We now take the uncovered triangles from the edge and match them with the doubly covered parts at the bottoms of the kites (see FIGURE 4). This leaves five doubly covered pentagons, and one larger uncovered pentagon.

A straightforward analysis shows that the five doubly covered pentagons are all regular, with side length $a - 2b$, and the middle pentagon is also regular, with side length $b - 2(a - 2b) = 5b - 2a$ (see [**8**] for the full calculations). We now have a smaller solution, with the five doubly counted regular pentagons having the same area as the omitted pentagon in the middle. Specifically, we have $5(a - 2b)^2 = (5b - 2a)^2$; as $a = b\sqrt{5}$ and $2 < \sqrt{5} < 3$, note that $a - 2b < b$ and thus we have our contradiction.

How far can we generalize: To $\sqrt{6}$ and beyond

We conclude with a discussion of one generalization of our method that allows us to consider certain triangular numbers, though other generalizations are possible and yield similar results. We hope the reader will explore these constructions further.

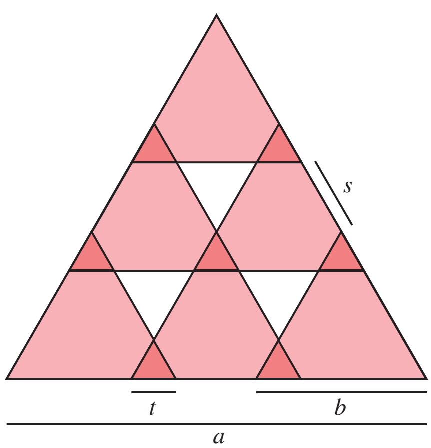


Figure 5 Geometric proof of the irrationality of $\sqrt{6}$

FIGURE 5 shows the construction for the irrationality of $\sqrt{6}$. Assume $\sqrt{6} = a/b$ so $a^2 = 6b^2$; as always, we assume a and b are the smallest positive integers satisfying this relation. The large equilateral triangle has side length a and the six medium equilateral triangles have side length b. The 7 smallest equilateral triangles (6 double counted, one in the center triple counted) have side length $t = (3b - a)/2$. It's a little work, but not too hard, to show that the triple-counted triangle is the same size. For the three omitted triangles, they are all equilateral (angles equal) and of side length $s = b - 2(3b - a)/2 = a - 2b$. As the area of the smaller equilateral triangles is proportional to t^2 and for the larger it is proportional to s^2, we find $8t^2 = 3s^2$ or $16t^2 = 6s^2$ so $(4t/s)^2 = 6$. Note that although t itself may not be an integer, $4t = 2(3b - a)$ is an integer, and we obtain our contradiction as we have found a smaller solution.

Can we continue this argument? We may interpret the argument here as adding three more triangles to the argument for the irrationality of $\sqrt{3}$; thus the next step would be adding four more triangles to this to prove the irrationality of $\sqrt{10}$. Proceeding along these lines leads us to study the square roots of triangular numbers. Triangular numbers are of the form $n(n + 1)/2$ for some positive integer n, and thus the first few are $1, 3, 6, 10, 15, \dots$. We continue more generally by producing images like FIGURE 5 with n equally spaced rows of side length b triangles. This causes us to start with $a^2 = \frac{n(n+1)}{2} b^2$, so we can attempt to show that $\sqrt{n(n + 1)/2}$ is irrational.

By similar reasoning to the above, we see that the smaller multiply covered triangles all have the same side length t, and that the uncovered triangles also all have the same side length s. Further, t equals $(nb - a)/(n - 1)$, and we have that $s = b - 2t$, so $s = b - 2(nb - a)/(n - 1) = (2a - (n + 1)b)/(n - 1)$. To count the number of side length t triangles, we note that there are $(n - 2)(n - 1)/2$ triply covered triangles (as there is a triangle-shaped configuration of them with $n - 2$ rows), and that there are $3(n - 1)$ doubly covered triangles around the edge of the figure, for a grand total of $2(n - 2)(n - 1)/2 + 3(n - 1) = (n - 1)(n + 1)$ coverings of the smaller triangle. Further, note that in general there are $(n - 1)n/2$ smaller, uncovered triangles, so we have that $(n - 1)(n + 1)t^2 = ((n - 1)n/2)s^2$. Writing out the formula for s, t (to verify that our final smaller solution is integral), we have $(n - 1)(n + 1)((nb - a)/(n - 1))^2 = ((n - 1)n/2)((2a - (n + 1)b)/(n - 1))^2$. We now multiply both sides of the equation by $n - 1$ to ensure integrality, giving $(n + 1)(nb - a)^2 = (n/2)(2a - (n + 1)b)^2$. We multiply both sides by $n/2$ to achieve a smaller solution to $a^2 = (n(n + 1)/2)b^2$, giving us $(n(n + 1)/2)(nb - a)^2 = (n(2a - (n + 1)b)/2)^2$. Note that this solution is integral, as n odd implies that $2a - (n + 1)b$ is even. Finally, to show that this solution is smaller, we just need that $nb - a < b$. This is equivalent to $n - \sqrt{n(n + 1)/2} < 1$.

We see that this inequality holds for $n \leq 4$, but not for $n > 4$. So, we have shown that the method used above to prove that $\sqrt{6}$ is irrational can also be used to show that $\sqrt{10}$ (the square root of the fourth triangular number) is irrational, but that this method will not work for any further triangular numbers. It is good (perhaps it is better to say, "it is not unexpected") to have such a problem, as some triangular numbers are perfect squares. For example, when $n = 8$ then we have $8 \cdot 9/2 = 2^2 \cdot 3^2$, and thus we should not be able to prove that this has an irrational square root!

Final remarks

There are many proofs of the irrationality of $\sqrt{2}$; see for example [**1, 2, 7**]. One particularly nice one can be interpreted as an origami construction (see proof 7 of [**2**] and the references there, and [**4**, pp. 183–185] for the origami interpretation). Cwikel [**5**] has generalized these origami arguments to yield the irrationality of other numbers as well.

The purpose of this note is to describe a geometric method which can be pushed further than one might initially expect. The examples studied are not meant to be exhaustive, but rather should be viewed as a representative sample of what can be done. Our hope is that the reader will find and communicate many more.

Acknowledgments This paper was inspired by Margaret Tucker's senior colloquium talk at Williams College (February 9, 2009, advisor Ed Burger), where she introduced the first named author to Tennenbaum's wonderful proof of the irrationality of $\sqrt{2}$, and a comment during the talk by Frank Morgan, who wondered if the method could be generalized to other numbers. We thank Peter Sarnak for pointing out the reference [**5**]. Some of the work was done at the 2009 SMALL Undergraduate Research Program at Williams College and the 2009 Young Mathematicians Conference at The Ohio State University; it is a pleasure to thank the NSF (Grant DMS0850577), Ohio State and Williams College for their support; the first named author was also supported by NSF Grants DMS0600848 and DMS0970067.

REFERENCES

1. T. M. Apostol, Irrationality of the square root of two—A geometric proof, *Amer. Math. Monthly* **107** (2000), no. 9, 841–842; http://dx.doi.org/10.2307/2695741.
2. A. Bogomolny, Square root of 2 is irrational, http://www.cut-the-knot.org/proofs/sq_root.shtml
3. J. H. Conway, "The power of mathematics," in *Power* (A. Blackwell and D. MacKay, eds.), Darwin College Lectures **16**, Cambridge University Press, 2006.
4. J. H. Conway and R. K. Guy, *The Book of Numbers*, Copernicus, 1996.
5. M. Cwikel, "Origami" proofs of irrationality of square roots, preprint, http://www.math.technion.ac.il/~mcwikel/paperfold.pdf
6. A. Hahn, *Basic Calculus: From Archimedes to Newton to its Role in Science*, Springer Verlag & Key College, 1998. Also available online at http://www.nd.edu/~hahn/
7. G. H. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Science Publications, Clarendon Press, Oxford, 1995.
8. S. J. Miller and D. Montague, *Irrationality from The Book*, http://arxiv.org/abs/0909.4913.
9. P. Tennenbaum, private communication, 2009.

Summary In the 1950's Tennenbaum gave a wonderful geometric proof of the irrationality of the square root of two. We show how to generalize his arguments to prove the irrationality of other numbers, and invite the reader to explore how far these arguments can go.

Gauss's Lemma and the Irrationality of Roots, Revisited

DAVID GILAT
Tel Aviv University, Israel
gilat@math.tau.ac.il

Browsing through the Biscuits [**1**], I came across an article by Harley Flanders that was originally published in this MAGAZINE [**3**, 1999]. In it, Flanders rephrases T. Estermann's [**2**, 1975] proof of the irrationality of $\sqrt{2}$ to show the irrationality of $\sqrt{k}$ for every non-square positive integer k. It turns out that Estermann's idea can be further extended to conclude that $\sqrt[n]{k}$ is either an integer or irrational, for every pair k, n of positive integers. Even more is true: Estermann's idea leads to a simple proof of Gauss's Lemma:

Math. Mag. **85** (2012) 114–116. doi:10.4169/math.mag.85.2.114.

GAUSS'S LEMMA. *Every real root of a monic polynomial with integer coefficients is either an integer or irrational.*

For the case of $\sqrt[n]{k}$, apply the theorem to the monic polynomial $P(x) = x^n - k$.

The standard proof

The standard proof of Gauss's lemma (e.g. [**4**, p. 41]) runs this way. Let r be a real root of the monic polynomial

$$P(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0, \tag{1}$$

where n is a positive integer and $c_0, \ldots, c_{n-1}$ are integers. If r is not irrational, then represent it as a fraction a/b with $(a, b) = 1$. Multiply the equality $P(a/b) = 0$ by b^n and isolate the leading term to obtain

$$a^n = -\left(c_{n-1}a^{n-1}b + \cdots + c_0 b^n\right).$$

The right side is a multiple of b, but if $b > 1$ then the left side is not. Therefore $b = 1$ and r is an integer. ■

Though quite simple and short, this proof hinges in an essential way on divisibility properties of the integers. One must know that if b has a prime factor p that does not divide a, then p does not divide any positive power of a. The use of this principle in some form seems unavoidable.

An alternative proof is offered below. It uses neither prime factorization nor divisibility; it does not even require one to know what it means for a number to be prime. It assumes only that the set of natural numbers is well ordered, i.e., that each of its nonempty subsets has a least element.

The alternative proof

Let r be a real root of the monic polynomial (1), and suppose that r is rational but not an integer. Then r is uniquely (and strictly) sandwiched between two consecutive integers, say $q < r < q + 1$.

Since r is rational, so are its first $(n - 1)$ powers, $r^1, r^2, \ldots, r^{n-1}$. Consequently, the set

$$M := \{m > 0 \mid m, mr, mr^2, \ldots, mr^{n-1} \text{ are integers}\}$$

is nonempty. Since r is a root of the polynomial, $r^n = -(c_{n-1}r^{n-1} + \cdots + c_0)$. For every $m \in M$, $m(c_{n-1}r^{n-1} + \cdots + c_1 r + c_0)$ is an integer, and thus mr^n is an integer as well.

We claim that, for every $m \in M$ there is an $m' \in M$ with $0 < m' < m$. Given $m \in M$, set $m' = (r - q)m$. Then for each $i = 0, \ldots, n - 1$ we have $m'r^i = mr^{i+1} - qmr^i$, which is an integer; so $m' \in M$; and $0 < m' < m$ because $0 < r - q < 1$.

Thus M cannot have a least element. It follows that r must be an integer or irrational. ■

Should one be interested in $\sqrt[n]{k}$ only, specializing the above argument to polynomials of form $x^n - k$ yields a direct proof. Further specialization to the single polynomial $x^2 - 2$ leads all the way back to Estermann's argument [**2**] for the irrationality of $\sqrt{2}$.

The simple alternative argument presented here deserves to be widely publicized and should become a standard textbook proof.

Acknowledgment I have known this proof in the case of $\sqrt[n]{k}$ for many years and have used it in teaching and informal chats with colleagues and students, but never considered writing it down for submission to a journal until being recently encouraged to do so by Arthur Benjamin. Subsequently, I was challenged by another colleague to extend the idea to prove the stronger result. I wish to thank them both, each for his respective contribution, without which this note would not materialize.

REFERENCES

1. A. T. Benjamin and E. Brown (eds.), *Biscuits of Number Theory*, Mathematical Association of America, Washington, DC, 2009.
2. T. Estermann, The irrationality of $\sqrt{2}$, *Math. Gazette* **59** (1975) p. 110; http://dx.doi.org/10.2307/3616647.
3. H. Flanders, Math. Bite: Irrationality of $\sqrt{k}$, *Math. Mag.* **72** (1999) p. 235; http://dx.doi.org/10.2307/2690889.
4. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford University Press, New York, 1959.

Summary An idea of T. Estermann (1975) for demonstrating the irrationality of $\sqrt{2}$ is extended to obtain a conceptually simple proof of Gauss's Lemma, according to which real roots of monic polynomials with integer coefficients are either integers or irrational. The standard proof of the lemma is also reviewed.

Minimizing Areas and Volumes and a Generalized AM–GM Inequality

WALDEN FREEDMAN
Humboldt State University
Arcata, CA 95521
Walden.Freedman@humboldt.edu

Most calculus teachers have, at some point, encountered optimization problems like these:

> **Problem A.** Find an equation of the line through the point (3, 5) that cuts off the least area from the first quadrant. (Exercise 4.7.50 of [**14**])
>
> **Problem B.** Find an equation of the plane that passes through the point (1, 2, 3) and cuts off the smallest volume in the first octant. (Exercise 14.7.56 of [**14**])

We will see that these problems and their solutions generalize in a natural way to an arbitrary number of dimensions, as well as to different classes of curves and surfaces. This leads us to a generalized Arithmetic-Mean–Geometric-Mean Inequality, and some related inequalities. We then suggest some related problems, suitable for student projects, with answers provided at the end. The bibliography provides readers with further avenues to explore both the AM-GM inequality and optimization.

Minimizing volume in $\mathbb{R}^3$

In Problem A, observe that the area of the triangle determined by the line becomes arbitrarily large as either the line's x-intercept approaches 3 or its y-intercept approaches 5.

Therefore, by continuity, there must be a line for which the area is minimized. A similar argument shows that in Problem B, there must be a plane for which the volume is minimized. Having determined that such a plane exists, we set about finding it, replacing the point $(1, 2, 3)$ with an arbitrary point, (r, s, t) in the first octant. So, we want the equation of the plane that contains the point (r, s, t), passes through the positive coordinate axes, and cuts off the least volume (in the first octant).

Suppose the plane has equation

$$\frac{x}{a} + \frac{y}{b} + \frac{z}{c} = 1,$$

where $a > r > 0$, $b > s > 0$, and $c > t > 0$. Then a, b, and c are the intercepts, and we are treating them as the variables that define the unknown plane.

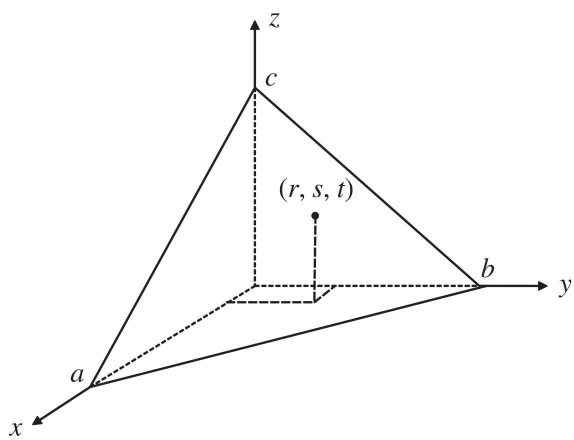


Figure 1 Volume formed in the first octant

Since the volume of the tetrahedron cut off by the plane is

$$V = \frac{abc}{3!},$$

we need to minimize the function $f(a, b, c) = abc$ on the region $a > r, b > s, c > t$ subject to the constraint

$$g(a, b, c) = \frac{r}{a} + \frac{s}{b} + \frac{t}{c} = 1.$$

The technique of Lagrange Multipliers (left to the reader) shows that the minimum volume occurs when $a = 3r$, $b = 3s$, and $c = 3t$, so that the desired equation of the plane is

$$\frac{x}{3r} + \frac{y}{3s} + \frac{z}{3t} = 1,$$

and the minimum volume equals $V = (3^3/3!)rst$. For example, in Problem B, the desired plane has equation

$$\frac{x}{3} + \frac{y}{6} + \frac{z}{9} = 1,$$

and the minimum volume is $V = 27$ cubic units.

The general case in $\mathbb{R}^n$

Here, we are given a point $r = (r_1, r_2, \ldots, r_n)$ in $\mathbb{R}^n$, with $r_i > 0$ for all i, and we wish to find the equation of the hyperplane that contains the point r such that the content (n-dimensional "volume") of the resulting region "cut off" by the hyperplane is minimized. If the hyperplane has equation

$$\frac{x_1}{a_1} + \frac{x_2}{a_2} + \cdots + \frac{x_n}{a_n} = 1,$$

where for each i, we have $a_i > r_i > 0$, then the content of the region is

$$C_n = \frac{a_1 a_2 \ldots a_n}{n!}.$$

(See [**13**]. Note that the case $n = 2$ is the familiar formula for the area of a right triangle.) Thus, the problem becomes that of finding the values of a_i minimizing the function $f(a_1, a_2, \ldots, a_n) = a_1 a_2 \cdots a_n$ subject to the constraint

$$g(a_1, a_2, \ldots, a_n) = \frac{r_1}{a_1} + \frac{r_2}{a_2} + \cdots + \frac{r_n}{a_n} = 1. \tag{1}$$

Again, the technique of Lagrange Multipliers leads us to conclude that the minimum content occurs precisely when $a_i = nr_i$, so the hyperplane has equation

$$\frac{x_1}{nr_1} + \frac{x_2}{nr_2} + \cdots + \frac{x_n}{nr_n} = 1,$$

and the minimum content is

$$C_n = \frac{n^n}{n!} r_1 r_2 \cdots r_n.$$

For example, in Problem A, the minimum area is $(2^2/2!) \cdot 3 \cdot 5 = 30$ square units.

We can state the result of this minimization in the form of an inequality. If $a_1, a_2, \ldots, a_n$ are any values satisfying the constraint (1), then

$$a_1 a_2 \cdots a_n \geq n^n r_1 r_2 \cdots r_n. \tag{2}$$

Since the minimum we found above is unique, equality occurs in (2) if and only if $a_i = nr_i$ for all i.

(An aside: If we consider an infinite sequence (r_n) of positive real numbers such that $r_n \to 1$, then curiously, we have

$$\lim_{n\to\infty} \frac{C_{n+1}}{C_n} = e.)$$

If we take $a_i = \sum_{j=1}^n r_j$ for all i, then (1) is satisfied, so, applying (2), we obtain

$$\left(\sum_{j=1}^n r_j\right)^n \geq n^n r_1 r_2 \cdots r_n, \tag{3}$$

with equality if and only if $\sum_{j=1}^n r_j = nr_i$ for all i, which is easily seen to be equivalent to $r_1 = r_2 = \cdots = r_n$. Dividing both sides of (3) by n^n and taking nth roots yields the Arithmetic-Mean–Geometric-Mean (AM-GM) Inequality:

$$\frac{1}{n}\sum_{j=1}^n r_j \geq \sqrt[n]{r_1 r_2 \cdots r_n}, \tag{4}$$

with equality if and only if $r_1 = r_2 = \cdots = r_n$.

A generalized AM-GM inequality

There is nothing special about planes in this construction. We might just as well consider an ellipsoid, with constraint equation

$$\left(\frac{r_1}{a_1}\right)^2 + \cdots + \left(\frac{r_n}{a_n}\right)^2 = 1.$$

Or, we might consider surfaces with other exponents in place of 2. We are thus led to the problem of minimizing $f(a_1, a_2, \ldots, a_n) = a_1 a_2 \cdots a_n$ subject to the constraint

$$g(a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} \left(\frac{r_i}{a_i}\right)^q = 1,$$

where q is a fixed positive exponent. In this case, we find that the minimum value of f is $n^{n/q} r_1 r_2 \cdots r_n$, which is attained when $a_i = n^{1/q} r_i$ for each i.

We can generalize further by allowing exponents in the objective function, and further still by allowing all of the exponents to be different in each dimension. This suggests we consider the general problem of minimizing the function

$$f(a_1, a_2, \ldots, a_n) = a_1^{p_1} a_2^{p_2} \cdots a_n^{p_n}$$

subject to the constraint

$$g(a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} \left(\frac{r_i}{a_i}\right)^{q_i} = 1 \tag{5}$$

where $p_i, q_i > 0$, and $a_i > r_i > 0$ for all i. The technique of Lagrange Multipliers then requires us to solve the system

$$\begin{aligned} &f(a_1, a_2, \ldots, a_n) \langle p_1/a_1, p_2/a_2, \ldots, p_n/a_n \rangle \\ &\qquad = \lambda \left\langle -q_1 r_1^{q_1}/a_1^{(q_1+1)}, -q_2 r_2^{q_2}/a_2^{(q_2+1)}, \ldots, -q_n r_n^{q_n}/a_n^{(q_n+1)} \right\rangle, \end{aligned}$$

together with the above constraint.

Leaving the details of solving the above system to the reader, and setting $k_i = p_i/q_i$, and $K = \sum_{i=1}^{n} k_i$, we find that the minimum value of f subject to the constraint (5) occurs when

$$a_i = \left(\frac{K}{k_i}\right)^{1/q_i} r_i.$$

Thus, if $a_i > r_i$ satisfy (5), then

$$\begin{aligned} f(a_1, a_2, \ldots, a_n) = a_1^{p_1} a_2^{p_2} \cdots a_n^{p_n} &\geq \left(\frac{K}{k_1}\right)^{k_1} r_1^{p_1} \left(\frac{K}{k_2}\right)^{k_2} r_2^{p_2} \cdots \left(\frac{K}{k_n}\right)^{k_n} r_n^{p_n} \\ &= \frac{K^K}{k_1^{k_1} k_2^{k_2} \cdots k_n^{k_n}} r_1^{p_1} r_2^{p_2} \cdots r_n^{p_n}. \end{aligned}$$

Dividing both sides by K^K, we have

$$\frac{a_1^{p_1} a_2^{p_2} \cdots a_n^{p_n}}{K^K} \geq \frac{r_1^{p_1} r_2^{p_2} \cdots r_n^{p_n}}{k_1^{k_1} k_2^{k_2} \cdots k_n^{k_n}}. \tag{6}$$

Now, if for each i we take $a_i = \left(\sum_{j=1}^n r_j^{q_j}\right)^{1/q_i}$, then (5) is satisfied, since for each i, we have

$$\left(\frac{r_i}{a_i}\right)^{q_i} = \frac{r_i^{q_i}}{a_i^{q_i}} = \frac{r_i^{q_i}}{\sum_{j=1}^n r_j^{q_j}}.$$

So, substituting $a_i = \left(\sum_{j=1}^n r_j^{q_j}\right)^{1/q_i}$ in (6), and taking Kth roots of both sides of the resulting inequality, we obtain the following generalization of the AM-GM Inequality.

THEOREM. *Let $r_j, p_j, q_j > 0$ be given for $1 \le j \le n$; for each j let $k_j = \frac{p_j}{q_j}$, and let $K = \sum_{j=1}^n k_j$. Then*

$$\frac{1}{K}\sum_{j=1}^n r_j^{q_j} \ge \left(\frac{r_1^{p_1} r_2^{p_2} \cdots r_n^{p_n}}{k_1^{k_1} k_2^{k_2} \cdots k_n^{k_n}}\right)^{1/K}, \tag{7}$$

with equality if and only if

$$\frac{r_1^{q_1}}{k_1} = \frac{r_2^{q_2}}{k_2} = \cdots = \frac{r_n^{q_n}}{k_n}.$$

The AM-GM Inequality (4) is obtained upon taking $p_j = q_j = 1$ for all j in (7).

By making particular choices of the constants p_j, q_j, r_j, we obtain some interesting special cases, which we give as corollaries. After the statement of each corollary we indicate briefly how to verify the result. The first corollary, below, was previously given in [**9**]. It has been referred to as the general AM-GM inequality in [**12**], and can itself be used to derive (7).

COROLLARY 1. *Let $r_j, p_j > 0$ be given for $1 \le j \le n$, and suppose $\sum_{j=1}^n p_j = 1$. Then*

$$\sum_{j=1}^n p_j r_j \ge r_1^{p_1} r_2^{p_2} \cdots r_n^{p_n}.$$

To verify, in (7) take $q_j = 1$ for all j, replace r_j with $p_j r_j$, and use the assumption that $\sum_{j=1}^n p_j = 1$. As noted in [**9**], this result yields Young's Inequality:

$$\sum_{j=1}^n \frac{1}{p_j} a_j^{p_j} \ge a_1 a_2 \cdots a_n,$$

where $a_j, p_j > 0$ for all j and $\sum_{j=1}^n \dfrac{1}{p_j} = 1$.

COROLLARY 2. *Let $p_j > 0$ for $1 \le j \le n$, and let $p = \sum_{j=1}^n p_j$. Then*

$$p^p \le (np_1)^{p_1}(np_2)^{p_2} \cdots (np_n)^{p_n}.$$

To verify, in (7) take $r_j = q_j = 1$ for all j. Then, take reciprocals of both sides of (7) to obtain

$$\frac{p}{n} \le \left(p_1^{p_1} p_2^{p_2} \cdots p_n^{p_n}\right)^{1/p}.$$

Raise both sides to the power p and simplify.

For example, for each n, let

$$s_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{n}.$$

Then

$$\left(\frac{s_n}{n}\right)^{s_n} \leq 2^{-1/2} 3^{-1/3} \cdots n^{-1/n}.$$

COROLLARY 3. *Let* $r > 0$ *and let* $q_j > 0$ *for* $1 \leq j \leq n$. *Let*

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

Then

$$Q \sum_{j=1}^{n} r^{q_j} \geq \left((r q_1^{1/q_1})(r q_2^{1/q_2}) \cdots (r q_n^{1/q_n})\right)^{Q}.$$

To verify, in (7) take $p_j = 1$ and $r_j = r$ for all j, and let Q be as defined, so that $Q = 1/K$.

COROLLARY 4. *Suppose* $q_j > 1$ *for all* j, *and* $\sum_{j=1}^{n} \frac{1}{q_j} = 1$. *Then for all* $x > 0$, *we have*

$$\sum_{j=1}^{n} x^{q_j - n} \geq q_1^{1/q_1} q_2^{1/q_2} \cdots q_n^{1/q_n}.$$

This is easily verified by substituting x for r in Corollary 3, and simplifying.

EXAMPLE. *Taking*

$$q_1 = 2, q_2 = 3, \text{ and } q_3 = 6,$$

we have

$$f(x) = \frac{1}{x} + 1 + x^3 \geq \sqrt{2}\sqrt[3]{3}\sqrt[6]{6},$$

for all $x > 0$.

In fact, this last inequality is not the best possible. The minimum value of f on $(0, \infty)$ is $1 + 4/3^{3/4} \approx 2.75477$, while $\sqrt{2}\sqrt[3]{3}\sqrt[6]{6} \approx 2.74946$.

Problems

These vary in difficulty, and may admit interesting generalizations, suitable for student projects. Throughout, we assume $r, s, t > 0$ are given. Answers are given in the last section.

1. Find the equation of the parabola in $\mathbb{R}^2$ that opens downward, with nonnegative y-intercept, that passes through the point (r, s), and that cuts off the smallest area in the first quadrant. (This problem was also discussed in [**5**].)

2. Find the cosine function of the form
$$y = b\cos\left(\frac{\pi x}{2a}\right)$$
whose graph passes through the point (r, s) and cuts off the smallest area in the first quadrant. Repeat for sine functions of the form $y = b\sin\left(\frac{\pi x}{a}\right)$. (Note: In both cases, a, b can only be determined numerically.)
3. Find the equation of the elliptic cone about the z-axis of the form
$$z = c\left(1 - \sqrt{x^2/a^2 + y^2/b^2}\right),$$
that passes through the point (r, s, t) such that the volume of the solid region bounded by the cone and the xy-plane is minimal.
4. Find the equation of the elliptic paraboloid, centered at the origin, of the form
$$z = c\left(1 - x^2/a^2 - y^2/b^2\right)$$
that passes through the point (r, s, t) such that the volume of the solid region bounded by the paraboloid and the xy-plane is minimal.
5. Find the function $f(x, y) = Ce^{-kx-my}$, where $C, k, m > 0$ whose graph passes through the point (r, s, t) and such that the volume under the surface $z = f(x, y)$, given by $\int_0^\infty \int_0^\infty f(x, y)\, dA$, is minimized. Similarly, find $C, a, b > 0$ for the surface $f(x, y) = C \cdot \exp\left(-\frac{x^2}{a^2} - \frac{y^2}{b^2}\right)$ over all of $\mathbb{R}^2$.

Answers to the problems

1. The equation is $y = -\frac{s}{r^2}x(2x - 3r)$, giving minimum area $\frac{9}{8}rs$.
2. Let α be the unique angle in the interval $(0, \pi/2)$ such that $\alpha\tan(\alpha) = 1$. (Note that $\alpha \approx 0.860334$.) The cosine function is $y = s\sec(\alpha)\cos(\alpha x/r)$, giving minimum area $A = (\sec(\alpha)/\alpha)rs \approx 1.78223rs$. Let β be the unique angle in the interval $(\pi/2, \pi)$ such that $\tan(\beta) = -\beta$. (Note that $\beta \approx 2.02876$.) The sine function is $y = s\csc(\beta)\sin(\beta x/r)$, giving minimum area $A = 2(\csc(\beta)/\beta)rs \approx 1.09908rs$.
3. The cone has equation $z = 3t - t\sqrt{\frac{2x^2}{r^2} + \frac{2y^2}{s^2}}$, giving minimal volume $V = \frac{9\pi}{2}rst$.
4. The paraboloid has equation $z = 2t\left(1 - \frac{x^2}{4r^2} - \frac{y^2}{4s^2}\right)$, giving minimal volume $V = 4\pi rst$.
5. The first surface has equation $z = t\exp(2 - x/r - y/s)$, giving minimal volume $V = e^2 rst$. The second surface has equation $z = t\exp(1 - x^2/2r^2 - y^2/2s^2)$, giving minimal volume $V = (2\pi e)rst$.

Resources

Here is a basic guide to the topics discussed in the references.

The AM-GM inequality: [**3, 4, 8**]

Optimization: [**1, 5, 9, 11**]; in particular [**5**] discusses an interesting property of the solutions to optimization problems like those above.

Both optimization and the AM-GM inequality: [**2, 6, 7, 12**].

REFERENCES

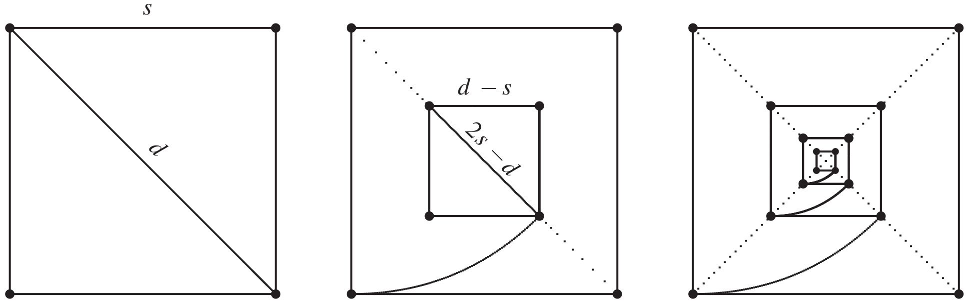
1. H. Bailey, A surprising Max-Min result, *College Math. J.*, **18**, no. 3, (1987), 225–229; http://dx.doi.org/10.2307/2686384.
2. W. Barnier and D. Martin, Unifying a family of extrema problems, *College Math. J.*, **28**, no. 5, (1997), 388–391; http://dx.doi.org/10.2307/2687071.
3. K-M. Chong, The arithmetic mean-geometric mean inequality: A New Proof, *Math. Mag.*, **49**, no. 2, (1976), 87–88; http://dx.doi.org/10.2307/2689438.
4. D. E. Daykin and C. J. Eliezer, Generalizations of the A.M. and G.M. inequality, *Math. Mag.*, **40**, no. 5, (1967), 247–250; http://dx.doi.org/10.2307/2688278.
5. R. A. Gordon, A generalization of a minimum area problem, *College Math. J.*, **34**, no. 1, (2003), 21–23; http://dx.doi.org/10.2307/3595838.
6. P. W. Gwanyama, The HM-GM-AM-QM inequalities, *College Math. J.*, **35**, no. 1, (2004), 47–50; http://dx.doi.org/10.2307/4146884.
7. M. S. Klamkin, On two classes of extremum problems without calculus, *Math. Mag.*, **65**, no. 2, (1992), 113–117; http://dx.doi.org/10.2307/2690491.
8. N. Schaumberger, A coordinate approach to the AM-GM inequality, *Math. Mag.*, **64**, no. 4, (1991), 273; http://dx.doi.org/10.2307/2690837.
9. ———, A general form of the arithmetic-geometric mean inequality via the mean value theorem, *College Math. J.*, **19**, no. 2, (1988), 172–173; http://dx.doi.org/10.2307/2686183.
10. D. M. Y. Sommerville, *An Introduction to the Geometry of N Dimensions*, Dover Publications, New York, 1958.
11. D. Spring, Solution of a calculus problem on minimal volume, *Amer. Math. Monthly*, **108**, no. 3, (2001), 217–221; http://dx.doi.org/10.2307/2695382.
12. J. M. Steele, *The Cauchy-Schwarz Master Class: An introduction to the Art of Mathematical Inequalities*, Cambridge University Press, New York, 2004.
13. P. Stein, A note on the volume of a simplex, *Amer. Math. Monthly*, **73**, no. 3, (1966), 299–301; http://dx.doi.org/10.2307/2315353.
14. J. Stewart, *Calculus, ET*, Brooks/Cole, Belmont, CA, 2008.

Summary Solving optimization problems via Lagrange Multipliers leads us to a generalized AM-GM inequality. We give several related optimization problems, suitable as projects for calculus students, with answers provided at the end.

Proof Without Words: $\sqrt{2}$ Is Irrational

GRANT CAIRNS
La Trobe University
Melbourne, Australia 3086
G.Cairns@latrobe.edu.au

The side length and diagonal are incommensurable.



Math. Mag. **85** (2012) 123. doi:10.4169/math.mag.85.2.123. © Mathematical Association of America

A Generalization of the Identity $\cos\frac{\pi}{3} = \frac{1}{2}$

ERIK PACKARD
Colorado Mesa University
Grand Junction, CO 81501
epackard@coloradomesa.edu

MARKUS REITENBACH
Colorado Mesa University
Grand Junction, CO 81501
mreitenb@coloradomesa.edu

Recently, while computing Riemann sums for the integral $\int_0^{\pi/2} \cos x\, dx$ in a calculus class, the first author noticed that

$$\cos\tfrac{\pi}{5} = 0.809016994\ldots \quad \text{and} \quad \cos\tfrac{2\pi}{5} = 0.309016994\ldots$$

appear to share all but their first digit. Is this a coincidence? No, since it turns out that

$$\cos\tfrac{\pi}{5} - \cos\tfrac{2\pi}{5} = \tfrac{1}{2}.$$

It is also true that

$$\begin{aligned} \cos\tfrac{\pi}{7} - \cos\tfrac{2\pi}{7} + \cos\tfrac{3\pi}{7} &= \tfrac{1}{2}, \\ \cos\tfrac{\pi}{9} - \cos\tfrac{2\pi}{9} + \cos\tfrac{3\pi}{9} - \cos\tfrac{4\pi}{9} &= \tfrac{1}{2}, \\ \cos\tfrac{\pi}{11} - \cos\tfrac{2\pi}{11} + \cos\tfrac{3\pi}{11} - \cos\tfrac{4\pi}{11} + \cos\tfrac{5\pi}{11} &= \tfrac{1}{2}, \end{aligned}$$

and so on. In general, we will prove the following

THEOREM. *Let n be any natural number. Then*

$$\sum_{k=1}^{n} (-1)^{k+1} \cos\left(\frac{k\pi}{2n+1}\right) = \frac{1}{2}.$$

Proof. Our proof uses complex numbers, the formula for the geometric sum and the following two simple facts.

1. If $x + y = 2\pi$ then $\cos x = \cos y$.
2. If $x + y = \pi$ then $\cos x = -\cos y$.

First, observe that $\sum_{k=1}^{2n+1} \cos\left(\frac{2k\pi}{2n+1}\right)$ is the real part of $\sum_{k=1}^{2n+1} e^{i\frac{2k\pi}{2n+1}}$ and the latter is a geometric sum whose value is 0. Hence

$$\sum_{k=1}^{2n+1} \cos\left(\frac{2k\pi}{2n+1}\right) = 0,$$

a fact that has been explained in this and other ways in this MAGAZINE [**1, 2**]. Separating the last term gives

$$\sum_{k=1}^{2n} \cos\left(\frac{2k\pi}{2n+1}\right) = -1.$$

Math. Mag. **85** (2012) 124–125. doi:10.4169/math.mag.85.2.124. © Mathematical Association of America

Splitting the sum and letting the summation of the terms for $k \geq n+1$ run backwards, we obtain

$$\sum_{k=1}^{n} \cos\left(\frac{2k\pi}{2n+1}\right) + \sum_{k=1}^{n} \cos\left(\frac{2(2n+1-k)\pi}{2n+1}\right) = -1.$$

By Fact 1, $\cos\left(\frac{2(2n+1-k)\pi}{2n+1}\right) = \cos\left(\frac{2k\pi}{2n+1}\right)$, so division by 2 gives

$$\sum_{k=1}^{n} \cos\left(\frac{2k\pi}{2n+1}\right) = -\frac{1}{2}.$$

Choose ℓ such that $n = 2\ell$ or $n = 2\ell + 1$. Splitting the sum again and letting the summation of the terms for $k \geq \ell + 1$ run backwards, we obtain

$$\sum_{k=1}^{\ell} \cos\left(\frac{2k\pi}{2n+1}\right) + \sum_{k=1}^{n-\ell} \cos\left(\frac{2(n+1-k)\pi}{2n+1}\right) = -\frac{1}{2}.$$

By Fact 2, $\cos\left(\frac{2(n+1-k)\pi}{2n+1}\right) = -\cos\left(\frac{(2k-1)\pi}{2n+1}\right)$, so the equation becomes

$$\sum_{k=1}^{\ell} \cos\left(\frac{2k\pi}{2n+1}\right) - \sum_{k=1}^{n-\ell} \cos\left(\frac{(2k-1)\pi}{2n+1}\right) = -\frac{1}{2}.$$

Combining terms gives

$$\sum_{k=1}^{n} (-1)^k \cos\left(\frac{k\pi}{2n+1}\right) = -\frac{1}{2}$$

and multiplying by -1 yields the claim. ∎

One can use the theorem just proved and the identity $\sin x = \cos(\frac{\pi}{2} - x)$ to obtain a similar result for sums of alternating sines, namely

$$\sum_{k=1}^{n} (-1)^{k+1} \sin\left(\frac{(2k-1)\pi}{4n+2}\right) = \frac{(-1)^{n+1}}{2},$$

which generalizes the identity $\sin \frac{\pi}{6} = \frac{1}{2}$.

REFERENCES

1. J. A. Holdener, Math Bite: Sums of sines and cosines, *Math. Mag.* **82** (April, 2009) 126; http://dx.doi.org/10.4169/193009809X468940.
2. M. P. Knapp, Sines and cosines of angles in arithmetic progression, *Math. Mag.* **82** (December, 2009) 371–372; http://dx.doi.org/10.4169/002557009X478436.

Summary Using Euler's Theorem and the Geometric Sum Formula, we prove trigonometric identities for alternating sums of sines and cosines.

A Class of Matrices with Zero Determinant

ANDRÉ L. YANDL
Seattle University
Seattle, WA 98122
alyandl@seattleu.edu

CARL SWENSON
Seattle University
Seattle, WA 98122
swenson@seattleu.edu

A linear algebra student noticed that

$$\det\begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix} = 0$$

and asked whether this result could be generalized. A fruitful discussion followed and eventually led to a matrix whose determinant involved the product of two Vandermonde determinants.

The first observation was that an $n \times n$ matrix, $[a_{ij}]$, $n \geq 3$, with integer entries $a_{ij} = i + (j-1)n$ has determinant 0. This is seen by subtracting the first column from both the second and third columns, and then subtracting the second from the third column of the resulting matrix. We get two identical columns, so the determinant is zero.

This was a quick result that used elementary row and column operations and answered our question. However, we were not satisfied, so we looked for another direction to generalize and tried investigating determinants with entries raised to a power. We found:

$$\det\begin{pmatrix} 1^2 & 4^2 & 7^2 \\ 2^2 & 5^2 & 8^2 \\ 3^2 & 6^2 & 9^2 \end{pmatrix} = -216.$$

However, this direction became fruitful when we found that

$$\det\begin{pmatrix} 1^2 & 5^2 & 9^2 & 13^2 \\ 2^2 & 6^2 & 10^2 & 14^2 \\ 3^2 & 7^2 & 11^2 & 15^2 \\ 4^2 & 8^2 & 12^2 & 16^2 \end{pmatrix} = 0.$$

This result led us to consider the following.

EXAMPLE. For real numbers $a_1, a_2, a_3, a_4, b_2, b_3, b_4$:

$$\det\begin{pmatrix} a_1^2 & (a_1+b_2)^2 & (a_1+b_3)^2 & (a_1+b_4)^2 \\ a_2^2 & (a_2+b_2)^2 & (a_2+b_3)^2 & (a_2+b_4)^2 \\ a_3^2 & (a_3+b_2)^2 & (a_3+b_3)^2 & (a_3+b_4)^2 \\ a_4^2 & (a_4+b_2)^2 & (a_4+b_3)^2 & (a_4+b_4)^2 \end{pmatrix} = 0.$$

Math. Mag. **85** (2012) 126–130. doi:10.4169/math.mag.85.2.126. © Mathematical Association of America

Solution. Subtract column 1 from columns 2, 3, and 4. In the resulting matrix factor b_2, b_3, and b_4 out of columns 2, 3, and 4, respectively. In the new matrix subtract column 2 from columns 3 and 4. By factoring $b_3 - b_2$ and $b_4 - b_2$ out of columns 3 and 4, we obtain a new matrix with two identical columns. The new matrix must have determinant zero, so the original matrix must have a zero determinant as well.

Using a computer, we confirmed that the determinant is zero for cases such as the 6×6 matrix $[a_{ij}]$ with integer entries $a_{ij} = (i + 6(j - 1))^4$. This led to a general proposition, for which the proof followed steps similar to the previous proof but was extremely cumbersome. However, as is often the case, a second proof, given below, turned out to be surprisingly simple.

PROPOSITION 1. *Let k and n be positive integers with $n \geq k + 2$. For real numbers $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ define*

$$C = \begin{pmatrix} (a_1 + b_1)^k & (a_1 + b_2)^k & (a_1 + b_3)^k & \cdots & (a_1 + b_n)^k \\ (a_2 + b_1)^k & (a_2 + b_2)^k & (a_2 + b_3)^k & \cdots & (a_2 + b_n)^k \\ (a_3 + b_1)^k & (a_3 + b_2)^k & (a_3 + b_3)^k & \cdots & (a_3 + b_n)^k \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ (a_n + b_1)^k & (a_n + b_2)^k & (a_n + b_3)^k & \cdots & (a_n + b_n)^k \end{pmatrix}.$$

Then, $\det(C) = 0$.

In the example, b_1 was forced to be 0. Allowing b_1 to be nonzero adds symmetry to the proposition, but does not enlarge the class of matrices covered by it.

Proof. We note matrix C has entries

$$c_{ij} = (a_i + b_j)^k = a_i^k + \binom{k}{1} a_i^{k-1} b_j + \cdots + \binom{k}{k-1} a_i b_j^{k-1} + b_j^k,$$

where $1 \leq i \leq n$ and $1 \leq j \leq n$.

Write matrix C as a product of two $n \times n$ matrices with entries:

$$d_{ij} = \begin{cases} \binom{k}{j-1} a_i^{k+1-j} & \text{for } 1 \leq i \leq n \text{ and } 1 \leq j \leq k+1, \\ 0 & \text{for } 1 \leq i \leq n \text{ and } k+2 \leq j \leq n. \end{cases}$$

and

$$e_{ij} = \begin{cases} 1 & \text{for } i = 1 \text{ and } 1 \leq j \leq n, \\ b_j^{i-1} & \text{for } 2 \leq i \leq k+1 \text{ and } 1 \leq j \leq n, \\ \text{arbitrary} & \text{for } k+2 \leq i \leq n \text{ and } 1 \leq j \leq n. \end{cases}$$

$$C = \begin{pmatrix} a_1^k & \binom{k}{1}a_1^{k-1} & \binom{k}{2}a_1^{k-2} & \cdots & 1 & 0 & \cdots & 0 \\ a_2^k & \binom{k}{1}a_2^{k-1} & \binom{k}{2}a_2^{k-2} & \cdots & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ a_n^k & \binom{k}{1}a_n^{k-1} & \binom{k}{2}a_n^{k-2} & \cdots & 1 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ b_1 & b_2 & b_3 & \cdots & b_n \\ b_1^2 & b_2^2 & b_3^2 & \cdots & b_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_1^k & b_2^k & b_3^k & \cdots & b_n^k \\ \# & \# & \# & \# & \# \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \# & \# & \# & \# & \# \end{pmatrix}.$$

Since $C = [d_{ij}] \cdot [e_{ij}]$ and $\det([d_{ij}]) = 0$, we have $\det(C) = 0$. ∎

An $m \times n$ matrix in which each row is a geometric progression starting with 1 is called a *Vandermonde* matrix.

$$V = \begin{pmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & a_m & a_m^2 & \cdots & a_m^{n-1} \end{pmatrix}$$

and if the matrix is square ($m = n$), then

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

The factorization of the matrix C in the proof of Proposition 1 leads to the next result, where $n = k + 1$.

PROPOSITION 2. *Let k be a positive integer with $n = k + 1$. For the matrix C as defined in Proposition 1,*

$$\det(C) = \left((-1)^{[n/2]} \prod_{j=1}^{k} \binom{k}{j} \right) \left(\prod_{1 \le i < j \le n} (a_i - a_j) \right) \left(\prod_{1 \le i < j \le n} (b_i - b_j) \right)$$

Proof. Write

$$C = \begin{pmatrix} a_1^k & \binom{k}{1}a_1^{k-1} & \binom{k}{2}a_1^{k-2} & \cdots & 1 \\ a_2^k & \binom{k}{1}a_2^{k-1} & \binom{k}{2}a_2^{k-2} & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{k+1}^k & \binom{k}{1}a_{k+1}^{k-1} & \binom{k}{2}a_{k+1}^{k-2} & \cdots & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ b_1 & b_2 & b_3 & \cdots & b_n \\ b_1^2 & b_2^2 & b_3^2 & \cdots & b_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_1^k & b_2^k & b_3^k & \cdots & b_n^k \end{pmatrix}.$$

Taking the determinant of C and factoring out the binomial coefficients we obtain

$$\det(C) = \prod_{j=0}^{k} \binom{k}{j} \det \begin{pmatrix} a_1^k & a_1^{k-1} & a_1^{k-2} & \cdots & 1 \\ a_2^k & a_2^{k-1} & a_2^{k-2} & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{k+1}^k & a_{k+1}^{k-1} & a_{k+1}^{k-2} & \cdots & 1 \end{pmatrix} \det \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ b_1 & b_2 & b_3 & \cdots & b_n \\ b_1^2 & b_2^2 & b_3^2 & \cdots & b_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ b_1^k & b_2^k & b_3^k & \cdots & b_n^k \end{pmatrix}.$$

Interchanging the order of the columns in the first determinant, we obtain a Vandermonde determinant. We account for the column change by using the greatest integer function in the factor $(-1)^{[n/2]}$. Transposing the second determinant gives another Vandermonde determinant:

$$\det(C) = \left((-1)^{[n/2]} \prod_{j=1}^{k} \binom{k}{j} \right) \left(\prod_{1 \le i < j \le n} (a_i - a_j) \right) \left(\prod_{1 \le i < j \le n} (b_i - b_j) \right) \qquad \blacksquare$$

We note that matrix C is zero if, and only if, two rows, or columns, of the matrix are identical.

It is common to use matrices to solve a system of m linear equations in n unknowns. If the coefficient matrix is A, and if $m = n$, then the matrix equation

$$AX = B$$

can be solved if A is invertible, that is, if $\det(A) \neq 0$.

APPLICATION 1. Find the equation of a polynomial of degree $n - 1$ whose graph passes through n given points. This leads to a system of n linear equations in n unknowns whose coefficient matrix is a Vandermonde matrix.

APPLICATION 2. If the columns of an $n \times n$ matrix A are n-dimensional vectors, then the linear dependency of these vectors is determined by considering the equation

$$A \begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

If $\det(A) \neq 0$, then the vectors are linearly independent; otherwise they are dependent.

The matrix C defined in propositions 1 and 2 occurs in problems of interpolation by translates of a single function. Our results imply that for a positive integer k, $k + 1$ distinct shifts $(x + a_i)^k$ of the polynomial x^k are linearly independent, while $k + 1$ shifts of x^n, $n < k$ are linearly dependent. Details of this application are found in [**1**, Ch. 11].

Although most recent Linear Algebra texts omit Vandermonde determinants, their usefulness is illustrated in a number of publications, which include [**2, 3, 4, 5, 6**]. We found the generalization obtained above was well suited for class discussion and later independent study.

REFERENCES

1. Ward Cheney and Will Light, *A Course in Approximation Theory*, American Mathematical Society, Providence, RI, 2009
2. Dan Kalman, The Generalized Vandermonde Matrix, *Math. Mag.* **28** (1984) 15–21; http://dx.doi.org/10.2307/2690290.
3. Allan Klinger, The Vandermonde Matrix, *Amer. Math. Monthly* **74** (1967) 571–574; http://dx.doi.org/10.2307/2314898.
4. David C. Lay, *Linear Algebra and its Applications*, Addison-Wesley, 1994.
5. Joseph J. Rushanan, On the Vandermonde Matrix, *Amer. Math. Monthly* **96** (1989) 921–924; http://dx.doi.org/10.2307/2324589.
6. Mariam Schapiro Grosof and Geraldine Taiani, Vandermonde Strikes Again, *Amer. Math. Monthly* **100** (1993) 575–577; http://dx.doi.org/10.2307/2324617.

Summary Let $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ be real numbers and the $n \times n$ matrix C be defined with entries $c_{ij} = (a_i + b_j)^k$, where k is a positive integer. If $n > k + 1$, then $\det(C) = 0$, and if $n = k + 1$, then $\det(C)$ is a product involving two Vandermonde determinants.

Splitting Fields and Periods of Fibonacci Sequences Modulo Primes

SANJAI GUPTA
Irvine Valley College
Irvine, CA 92618
sgupta@ivc.edu

PAROUSIA ROCKSTROH
Simon Fraser University
Burnaby, British Columbia V5A 1S6, Canada
parousia_rockstroh@sfu.ca

FRANCIS EDWARD SU
Harvey Mudd College
Claremont, CA 91711
su@math.hmc.edu

The Fibonacci sequence defined by $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$ is clearly periodic when reduced modulo an integer m, since there are only finitely many possible pairs of consecutive elements chosen from $\mathbb{Z}/m\mathbb{Z}$ (in fact, m^2 such pairs) and any such pair determines the rest of the sequence, both forwards and backwards. What is the period of this sequence?

An upper bound is $m^2 - 1$ (since the sequence does not have a consecutive pair of 0's), but the period is often much smaller. As examples, the Fibonacci sequence mod 11 is:

$$0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, 1, \ldots$$

and has period 10; the Fibonacci sequence mod 7 is:

$$0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, \ldots$$

and has period 16.

Math. Mag. **85** (2012) 130–135. doi:10.4169/math.mag.85.2.130.

This problem was first considered by Wall [**8**] and shortly thereafter by Robinson [**5**]. Among other cases, they studied the Fibonacci sequence for prime moduli, and showed that for primes p that are congruent to 1 or 4 (mod 5) the period length of the Fibonacci sequence mod p divides $p-1$, while for primes p that are congruent to 2 or 3 (mod 5) the period length divides $2(p+1)$. The examples above illustrate these facts. As we will see, the prime $p=5$ is a special case with period 20; the prime $p=2$ is also special in some ways with period 3.

Wall's proofs use different combinatorial techniques for each of these classes of primes. Robinson proves these results by appealing to a directed graph of points formed by multiplication by a *Fibonacci matrix*. In this paper, we give alternative proofs of these results that also use the Fibonacci matrix, but unlike Robinson, we place the roots of its characteristic polynomial in an appropriate splitting field. This allows us to obtain bounds for the periods of the more general recurrence

$$E_{n+1} = AE_n + BE_{n-1}$$

modulo a prime, which neither Wall nor Robinson consider.

Vella and Vella [**7**] consider general recurrences, but only in the special case where the roots of the characteristic polynomial are integers. Using sophisticated methods, Pinch [**3**] proves general results about multiple-term recurrences with prime power moduli, but does not produce specific bounds of the kind that we consider here. Li [**4**] reviews prior work on period lengths of general recurrences in the context of a different problem: determining which residue classes appear in recurrence sequences.

The purpose of our brief paper is to illustrate an accessible, motivated treatment of this classical topic using only ideas from linear and abstract algebra (rather than the case-by-case analysis found in many papers on the subject, or techniques from graduate number theory). Our methods extend to general recurrences with prime moduli and provide some new insights, e.g., Theorem 8, below. And our treatment highlights a nice application of the use of splitting fields (explained below) that might be suitable to present in an undergraduate course in abstract algebra or Galois theory.

Eigenvalues of the Fibonacci matrix

Let p be an odd prime.

In accordance with previous literature [**5, 8**] we define $k(p)$, the *period* of the Fibonacci sequence mod p, to be the smallest positive index i such that $F_i \equiv 0 \bmod p$ and $F_{i+1} \equiv 1 \bmod p$. In our examples above, $k(11) = 10$, while $k(7) = 16$. Following Robinson [**5**], we consider the Fibonacci matrix:

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

This is a matrix over some field $\mathbb{F}$ that we should be careful to specify. If we choose $\mathbb{F} = \mathbb{R}$, then

$$U^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}.$$

And if we choose $\mathbb{F} = \mathbb{F}_p$, the finite field of order p (also known as $\mathbb{Z}/p\mathbb{Z}$, the integers mod p) then the entries of U^n are elements of the Fibonacci sequence mod p, the desired objects of study.

It is natural to consider the eigenvalues of the matrix U, which are roots of its characteristic polynomial $x^2 - x - 1$. If eigenvalues $\lambda, \bar{\lambda}$ exist in $\mathbb{F}_p$ and are distinct, then $U = CDC^{-1}$ where D is the diagonal matrix

$$D = \begin{bmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{bmatrix} \tag{1}$$

and C is a matrix with the corresponding eigenvectors as columns. Then $U^k = CD^kC^{-1}$. We see that for $k = k(p)$, we have $U^k = I$, the identity matrix. Therefore $D^k = C^{-1}U^kC$ is also I. We observe that the exponent $k = k(p)$ is the smallest non-zero exponent n such that $D^n = I$. Thus:

LEMMA 1. *The period $k(p)$ must divide any n that satisfies $D^n = I$.*

When do the eigenvalues $\lambda, \bar{\lambda}$ exist in $\mathbb{F}_p$? The quadratic formula shows that $ax^2 + bx + c$ has roots in the field $\mathbb{F}_p$ as long as the discriminant $\Delta = b^2 - 4ac$ is a square in $\mathbb{F}_p$; hence the characteristic polynomial $x^2 - x - 1$ has roots in $\mathbb{F}_p$ if and only if $\Delta = 5$ is a square. Quadratic reciprocity [**6**] shows that if p is an odd prime, then 5 is a square in $\mathbb{F}_p$ if and only if $p \equiv 0, 1, 4 \bmod 5$. And as long as $p \neq 5$, the eigenvalues are distinct. Hence:

THEOREM 2. *If p is an odd prime and p is congruent to* 1 *or* 4 *(*mod 5*), then $k(p)$ divides $p - 1$. In particular, $k(p) \leq p - 1$.*

Proof. The eigenvalues $\lambda, \bar{\lambda}$ of U are non-zero (since U is invertible) and distinct (since $p \neq 5$). Since p is prime, Fermat's (little) theorem implies both $\lambda^{p-1} = 1$ and $\bar{\lambda}^{p-1} = 1$. Hence $D^{p-1} = I$ and Lemma 1 gives the desired conclusion. ∎

When $p = 5$, the eigenvalues are not distinct (they are both 3) and D is not diagonal, so $D^4 \neq I$ even though $\lambda^4 = \bar{\lambda}^4 = 1$. One finds that $D^{20} = I$ and $k(5) = 20$.

A splitting field for the eigenvalues

The case of remaining classes of odd primes, $p \equiv 2, 3 \bmod 5$, requires more work, because for these primes, the characteristic polynomial $x^2 - x - 1$ is *irreducible.* It does not have roots in $\mathbb{F}_p$ unless we enlarge the field.

We can do this by a standard construction: to the field $\mathbb{F}_p$, we "adjoin" an element γ that has the property that $\gamma^2 = \gamma + 1$, and consider the set of linear combinations of 1 and γ over $\mathbb{F}_p$ with the natural arithmetic.

Let's make this construction more precise. As a set, the enlarged field has p^2 elements:

$$\mathbb{F}_{p^2} = \{a + b\gamma : a, b \in \mathbb{F}_p\}$$

We may regard these as formal expressions or as a particular way to write ordered pairs (a, b). They are added and multiplied as if γ were a number satisfying $\gamma^2 - \gamma - 1 = 0$. Here's a sample calculation: $(1 - \gamma)(\gamma) = \gamma - \gamma^2 = \gamma - (\gamma + 1) = -1$. With these operations, $\mathbb{F}_{p^2}$ is a field. In fact it is the unique finite field of size p^2 and some may recognize it also as the quotient field $\mathbb{F}_p[x]/(x^2 - x - 1)$, though this insight is not needed in what follows.

Note that the expressions of the form $a + 0\gamma$ (with $b = 0$) form a subfield identical to $\mathbb{F}_p$ itself. In this way we regard $\mathbb{F}_p$ as a subfield of $\mathbb{F}_{p^2}$. We note that this subfield obeys Fermat's theorem, so

$$a^p = a$$

holds for all $a \in \mathbb{F}_p$.

By construction, γ is automatically a root of $x^2 - x - 1$ in $\mathbb{F}_{p^2}$. One may check that

$$\bar{\gamma} = 1 - \gamma$$

is another root, distinct from γ. We will need the fact that $\gamma\bar{\gamma} = -1$, which follows from the sample calculation above.

Also by construction, $\mathbb{F}_{p^2}$ has *characteristic* p: any element $a + b\gamma$ multiplied by p (e.g., added to itself p times) is 0, since the coefficients a, b come from $\mathbb{F}_p$. So the following nifty fact holds, sometimes facetiously called "freshman exponentiation" [**1**, p. 422]: if $\mu, \nu \in \mathbb{F}_{p^2}$, then

$$(\mu + \nu)^p = \mu^p + \nu^p. \tag{2}$$

This follows from the binomial theorem. When p is prime and k is not equal to 0 or p, the binomial coefficient $\binom{p}{n}$ is divisible by p. Therefore all of the intermediate terms of the binomial expansion of $(\mu + \nu)^p$ vanish, and (2) holds.

This is the basis of an important lemma. We briefly consider an arbitrary polynomial in $\mathbb{F}_p$:

LEMMA 3. *If $P(x)$ is an irreducible polynomial in $\mathbb{F}_p$ that has a root γ in $\mathbb{F}_{p^2}$, then γ^p must be a different root of $P(x)$.*

(This is a standard fact in Galois theory: the *Frobenius map* $x \to x^p$ transitively permutes the roots of irreducible polynomials, though we have avoided that language here to keep this treatment friendly.)

Proof. Let $P(x) = a_n x^n + \cdots + a_0$ where $a_i \in \mathbb{F}_p$, and suppose γ is a root. Then

$$\begin{aligned} P(\gamma^p) &= a_n \gamma^{pn} + \cdots + a_0 \\ &= a_n^p \gamma^{np} + \cdots + a_0^p \\ &= (a_n \gamma^n + \cdots + a_0)^p \\ &= 0^p = 0. \end{aligned}$$

The second line follows because Fermat's theorem ($a = a^p$) holds for elements of $\mathbb{F}_p$, and the third line follows from freshman exponentiation.

So γ^p is a root of $P(x)$. Further, $\gamma^p \neq \gamma$, because there are at most p solutions to the equation $x^p = x$, and Fermat's theorem shows they are all the elements of the subfield $\mathbb{F}_p$. Therefore γ is not a solution, and γ^p must be a different root of $P(x)$. ∎

Returning to the case of $P(x) = x^2 - x - 1$, we immediately obtain:

LEMMA 4. *If $p \equiv 2, 3 \bmod 5$, then*

$$\gamma^p = \bar{\gamma} \quad \textit{and} \quad \bar{\gamma}^p = \gamma.$$

Proof. These statements follow from the fact that $x^2 - x - 1$ is irreducible in $\mathbb{F}_p$ when $p \equiv 2, 3 \bmod 5$, but has exactly two roots γ and $\bar{\gamma}$ in $\mathbb{F}_{p^2}$. ∎

Now we may determine the desired bound:

THEOREM 5. *Let p be an odd prime that is congruent to 2 or 3 (mod 5) then $k(p)$ divides $2(p + 1)$. In particular, $k(p) \leq 2(p + 1)$.*

Proof. We appeal to Lemma 1, now viewing the matrices U and D in the prior discussion with elements from the enlarged field $\mathbb{F}_{p^2}$. Note that the diagonal entries $\lambda, \bar{\lambda}$ of D in (1) are then the roots $\gamma, \bar{\gamma}$ of $x^2 - x - 1$.

Applying Lemma 4 ($\gamma^p = \bar{\gamma}$) and the fact that $\gamma\bar{\gamma} = -1$, we see that

$$\gamma^{2(p+1)} = (\gamma^p)^2\gamma^2 = \bar{\gamma}^2\gamma^2 = (-1)^2 = 1. \tag{3}$$

By reversing roles of $\gamma, \bar{\gamma}$ we see that $\bar{\gamma}^{2(p+1)} = 1$ as well. These conclusions show that $D^{2(p+1)} = I$, as desired in Lemma 1. ■

As Wall [**8**] notes, the upper bounds of Theorems 2 and 5 are tight for many small odd primes $p \neq 5$ (for $p < 100$, the only exceptions are 29, 47, and 89). The bounds appear to be less tight for larger p. Wall also shows for prime powers, $k(p^t) \leq p^{t-1}k(p)$ with equality if $k(p^2) \neq k(p)$. It is believed the latter condition always holds; see [**2**] for partial results. Combining knowledge of $k(p^t)$ with the fact that $\text{lcm}[k(m), k(n)] = k(\text{lcm}[m, n])$, one can obtain a bound on $k(m)$ for each positive integer m.

The general recurrence

Our methods can be adapted to obtain bounds for the period of the general recurrence

$$E_{n+1} = AE_n + BE_{n-1}$$

modulo a prime p, with $E_0 = 0$ and $E_1 = 1$. Let $k_{A,B}(p)$ be the period of E_n mod p. The analog of the Fibonacci matrix becomes

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

and the eigenvalues $\lambda, \bar{\lambda}$ are roots of the characteristic polynomial $x^2 - Ax - B$. This has roots in $\mathbb{F}_p$ as long as the discriminant

$$\Delta = A^2 + 4B$$

is a square in $\mathbb{F}_p$ (a *quadratic residue* mod p), and they are distinct if $\Delta \not\equiv 0$ mod p. The same arguments as in Theorem 2 will yield:

THEOREM 6. *If p is an odd prime and Δ is a non-zero quadratic residue mod p, then $k_{A,B}(p)$ divides $p - 1$. In particular $k_{A,B}(p) \leq p - 1$.*

For example, consider $E_{n+1} = 3E_n + 2E_{n-1}$ mod 13. Then $A = 3$, $B = 2$, and $\Delta = 17$. Since $\Delta \equiv 2^2$ mod 13, Δ is a non-zero quadratic residue mod 13. Our theorem shows that $k_{3,2}(13) \leq 12$ (and, in fact, it is 12).

A curious consequence of our theorem is that the sequence $E_{n+1} = E_n + 2E_{n-1}$ mod p has small period (that divides $p - 1$) for *every* odd prime p except 3 (since $\Delta = 3^2$ is always a square and the only prime p that divides Δ is 3).

If the discriminant Δ is not a square in $\mathbb{F}_p$, we consider U as a matrix with entries from $\mathbb{F}_{p^2}$, the splitting field of $x^2 - Ax - B$ obtained by adjoining an element γ that satisfies $\gamma^2 = A\gamma + B$. The roots of the characteristic polynomial $x^2 - Ax - B$ in $\mathbb{F}_{p^2}$ are then γ and $\bar{\gamma} = A - \gamma$. The irreducibility of $x^2 - Ax - B$ over $\mathbb{F}_p$ and Lemma 3 show that

LEMMA 7. *If Δ is a quadratic nonresidue mod p, then*

$$\gamma^p = \bar{\gamma} \quad \textit{and} \quad \bar{\gamma}^p = \gamma.$$

We can now obtain the following result. Let $\text{ord}(n)$ denote the *multiplicative order* of n: the smallest positive integer t such that $n^t \equiv 1$ mod p.

THEOREM 8. *If Δ is a quadratic nonresidue mod p, then $k_{A,B}(p)$ is a divisor of* $2(p+1)\cdot \operatorname{ord}(B^2)$. *In particular,*

$$k_{A,B}(p) \le 2(p+1)\cdot \operatorname{ord}(B^2).$$

Proof. We mimic the proof of Theorem 5. In light of Lemma 1, our goal is to show that

$$\gamma^{2(p+1)} = \bar{\gamma}^{2(p+1)} = B^2.$$

But these follow easily by noting $\gamma\bar{\gamma} = -B$, using Lemma 7, and repeating a similar calculation as (3). ∎

Note that if $B = 1$, then the original bound $2(p+1)$ still holds. For example, consider $E_{n+1} = 3E_n + E_{n-1}$ mod 19. Then $A = 3$, $B = 1$, and $\Delta = 13$. Since 13 is a nonresidue mod 19, our theorem shows $k_{3,1}(19)$ divides 40 (and, in fact, it is 40). For the same sequence mod 11, we find that 13 is a nonresidue mod 11, so $k_{3,1}(11)$ divides $2(11+1) = 24$ (and, in fact, it is 8).

For a general example where $B \ne 1$, consider $E_{n+1} = 3E_n + 2E_{n-1} \mod 7$. Then $A = 3$, $B = 2$, and $\Delta = 17$. Since 17 is a nonresidue mod 7, and $B^2 = 4$ satisfies $4^3 \equiv 1 \mod 7$, our theorem shows that the period $k_{3,2}$ divides $2(7+1)\cdot 3 = 48$ (and, in fact, is 48).

In general, we note that $\operatorname{ord}(B^2)$ is at most $(p-1)/2$ by Fermat's theorem, so the bound in Theorem 8 could be as high as $2(p+1)(p-1)/2 = p^2 - 1$, the bound at the beginning of this paper. This bound is actually achieved by $E_{n+1} = 3E_n + 2E_{n-1}$ mod 37, the sequence

$$0, 1, 3, 11, 2, 28, 14, 24, 26, 15, 23, 25, 10, 6, 1, 15, 10, 23, 15, 17, \ldots$$

which has period $1368 = (37+1)(37-1)$, and indicates that all possible consecutive pairs other than 0, 0 appear in this sequence mod 37.

Acknowledgment Francis Edward Su was supported in part by NSF DMS-0701308 and NSF DMS-1002938.

REFERENCES

1. J. B. Fraleigh, *A First Course in Abstract Algebra*, 7th ed., Addison Wesley, Boston, 2003.
2. S. E. Mamangakis, Remarks on the Fibonacci series modulo m, *Amer. Math. Monthly* **68** (1961) 648–649; http://dx.doi.org/10.2307/2311514.
3. R. G. E. Pinch, Recurrent sequences modulo prime powers, in *Cryptography and coding, III* (*Cirencester, 1991*), 297–310, *Inst. Math. Appl. Conf. Ser. New Ser.*, **45**, Oxford University Press, New York, 1993.
4. H. C. Li, Complete and reduced residue systems of second-order recurrences modulo p, *Fib. Quart.* **38** (2000) 272–281.
5. D. W. Robinson, The Fibonacci matrix modulo m, *Fib. Quart.* **1** (1963) 29–36.
6. W. Stein, *Elementary Number Theory: Primes, Congruences, and Secrets*, Springer, New York, 2008.
7. D. Vella and A. Vella, Cycles in the generalized Fibonacci sequence modulo a prime, *Math. Mag.* **75** (2002) 294–299; http://dx.doi.org/10.2307/3219168.
8. D. D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960) 525–532; http://dx.doi.org/10.2307/2309169.

Summary We consider the period of a Fibonacci sequence modulo a prime and provide an accessible, motivated treatment of this classical topic using only ideas from linear and abstract algebra. Our methods extend to general recurrences with prime moduli and provide some new insights. And our treatment highlights a nice application of the use of splitting fields that might be suitable to present in an undergraduate course in abstract algebra or Galois theory.

A Short Proof of the Chain Rule for Differentiable Mappings in $\mathbb{R}^n$

RAYMOND MORTINI
Université de Lorraine
F-57045 Metz, France
mortini@univ-metz.fr

I always found the proof of the differentiability of the composition of multivariable maps quite cumbersome. So I developed in my 2009 course an easier approach based on the notion I called M-differentiability. It turns out that M-differentiability is not entirely new (see below) and it coincides with the usual notion of differentiability. So here is my approach.

Let $M^{q,n}$ be the set of matrices over $\mathbb{R}$ with q rows and n columns. The product of a matrix $A \in M^{q,n}$ with a column vector $x \in \mathbb{R}^n$ is denoted by $A \cdot x$ or Ax. Let $U \subseteq \mathbb{R}^n$ be an open set, and let $a \in U$.

A map $f : U \to \mathbb{R}^q$ is said to be *M-differentiable at a* if there exists a matrix-valued function $A_{f,a} : U \to M^{q,n}$ that is continuous at a and such that

$$f(x) = f(a) + A_{f,a}(x)(x - a) \tag{1}$$

for all $x \in U$. The *derivative of f at a,* denoted by $f'(a)$, is the matrix $A_{f,a}(a)$.

Let us point out that if f is M-differentiable at a, then f is continuous at a.

We postpone for a moment the proof that $f'(a)$ is well defined. The usefulness of this definition lies in the absence of an error term in (1). The job of the error term is done by letting $A_{f,a}(x)$ vary with $x \in U$. Because there is no error term, the following theorem is just an exercise in matrix multiplication.

THEOREM 1. *Let $U \subseteq \mathbb{R}^n$ and $V \subseteq \mathbb{R}^p$ be open sets and $a \in U$. Let $f : U \to V$ and $g : V \to \mathbb{R}^q$, and let h be their composition, $h = g \circ f : U \to \mathbb{R}^q$. If f is M-differentiable at a and g is M-differentiable at $f(a)$, then h is M-differentiable at a and $h'(a) = g'(f(a)) \cdot f'(a)$.*

Proof. Here $f'(a) \in M^{p,n}$, $g'(f(a)) \in M^{q,p}$ and $h'(a) \in M^{q,n}$. By our hypotheses,

$$f(x) = f(a) + A_{f,a}(x)(x - a)$$

where $A_{f,a}$ is continuous at a and $f'(a) = A_{f,a}(a)$. Also,

$$g(y) = g(f(a)) + A_{g,f(a)}(y)(y - f(a))$$

where $A_{g,f(a)}$ is continuous at $f(a)$ and $g'(f(a)) = A_{g,f(a)}(f(a))$. Therefore,

$$\begin{aligned} h(x) = g(f(x)) &= g(f(a)) + A_{g,f(a)}(f(x)) \cdot (f(x) - f(a)) \\ &= g(f(a)) + A_{g,f(a)}(f(x)) \cdot \big(A_{f,a}(x)(x - a)\big) \\ &= g(f(a)) + \big(A_{g,f(a)}(f(x)) \cdot A_{f,a}(x)\big) \cdot (x - a). \end{aligned}$$

Math. Mag. **85** (2012) 136–141. doi:10.4169/math.mag.85.2.136. © Mathematical Association of America

Since $A_{g,f(a)}$ is continuous at $f(a)$ and $A_{f,a}$ and f are continuous at a, we get that $B(x) := A_{g,f(a)}(f(x)) \cdot A_{f,a}(x)$ is continuous at a. Thus h is M-differentiable at a and

$$h'(a) = B(a) = A_{g,f(a)}(f(a)) \cdot A_{f,a}(a) = g'(f(a)) \cdot f'(a). \qquad \blacksquare$$

The derivative is well defined

For $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, let $||x|| = (\sum_{j=1}^n |x_j|^2)^{1/2}$ be the Euclidean norm of x. Write 0_n and 0_q for the origins in $\mathbb{R}^n$ and $\mathbb{R}^q$, respectively, and $\mathcal{O}_{q,n}$ for the zero matrix in $M^{q,n}$.

Note that in general there are many matrix-valued functions B, continuous at a, such that $B(x)(x - a) = f(x) - f(a)$.

For example if $q = 1$, $n = 2$, and $f(u, v) = F(u, v)u + G(u, v)v$, then for any function $h(u, v)$ we also have

$$(F(u, v) + h(u, v)v)\, u + (G(u, v) - h(u, v)u)\, v = f(u, v). \tag{2}$$

Hence, if we put $B = (F, G)$ and $B_h(u, v) = B(u, v) + h(u, v)(v, -u)$, then

$$f(u, v) - f(0, 0) = B(u, v) \cdot \begin{pmatrix} u \\ v \end{pmatrix} = B_h(u, v) \cdot \begin{pmatrix} u \\ v \end{pmatrix}.$$

We now show that our derivative $f'(a)$ is well defined.

Let f be M-differentiable at $a \in U$, and let $A = A_{f,a}$ satisfy the requirements of the definition; that is, $A : U \to M^{q,n}$ is continuous at a and, rewriting (1), $A(x)(x - a) = f(x) - f(a)$ for all $x \in U$. Let B be any other matrix-valued function with the same properties; that is, $B : U \to M^{q,n}$ is also continuous at a and $B(x)(x - a) = f(x) - f(a)$ for $x \in U$. We must show that $B(a) = A(a)$.

We do this by showing that $(B(a) - A(a)) \cdot \xi = 0$ for every vector $\xi \in \mathbb{R}^n$.

First, if $\xi \in \mathbb{R}^n$, then $a + t\xi \in U$ for all sufficiently small t. For any such t, we have $B(a + t\xi) \cdot (t\xi) = f(a + t\xi) - f(a) = A(a + t\xi) \cdot (t\xi)$, so that

$$(B(a + t\xi) - A(a + t\xi)) \cdot (t\xi) = 0_q.$$

Hence, if $t \neq 0$,

$$(B(a + t\xi) - A(a + t\xi)) \cdot \xi = 0_q.$$

Now because both A and B are continuous at a, we have

$$\lim_{t\to 0} (B(a + t\xi) - A(a + t\xi)) = B(a) - A(a).$$

Therefore,

$$\begin{aligned}(B(a) - A(a)) \cdot \xi &= \Big(\lim_{t\to 0} \big(B(a + t\xi) - A(a + t\xi)\big)\Big) \cdot \xi \\ &= \lim_{t\to 0} \Big(\big(B(a + t\xi) - A(a + t\xi)\big) \cdot \xi\Big) \\ &= \lim_{t\to 0} 0_q \\ &= 0_q.\end{aligned}$$

Since this is true for every $\xi \in \mathbb{R}^n$, it follows that $B(a) - A(a) = \mathcal{O}_{q,n}$. Hence $f'(a)$ is well defined.

The equivalence of M-differentiability with differentiability

At first glance it appeared that M-differentiability is weaker than the usual notion of differentiability. This is not the case though.

Let us recall the usual definition of differentiability: Let $U \subseteq \mathbb{R}^n$ be open, $a \in U$, and $f : U \to \mathbb{R}^q$. Then f is *differentiable at a* if there is a linear map $\phi : \mathbb{R}^n \to \mathbb{R}^q$ and a map $R : U \to \mathbb{R}^q$ such that

$$f(x) = f(a) + \phi(x-a) + R(x) \text{ and } \frac{||R(x)||}{||x-a||} \to 0 \text{ as } x \to a.$$

In this case the *differential of f at a* is ϕ.

THEOREM 2. *Let $U \subseteq \mathbb{R}^n$ be open, $a \in U$, and $f : U \to \mathbb{R}^q$. Then f is differentiable at a if and only if f is M-differentiable at a.*

If, additionally, f is continuous in U, then $A_{f,a}$ can be chosen to be continuous in U, too, whenever f is M-differentiable at a. If f is continuously differentiable in U, then $A_{f,a}$ can be chosen so that the map $(x, a) \mapsto A_{f,a}(x)$ is continuous in $U \times U$.

Proof. We first consider the case where $q = 1$, that is where f is a scalar-valued function.

Differentiable implies M-differentiable. Suppose that f is differentiable at a. Then all the partial derivatives $\frac{\partial f}{\partial x_j}(a)$ exist at a and we may consider the gradient

$$\nabla f(a) = \left(\frac{\partial f}{\partial x_1}(a), \ldots, \frac{\partial f}{\partial x_n}(a)\right).$$

Then $\phi(x-a) = \nabla f(a) \cdot (x-a)$. Now let

$$\nu(x) = \begin{cases} \nabla f(a) & \text{if } x = a \\ \nabla f(a) + \frac{R(x)}{||x-a||^2}(x-a)^{\perp} & \text{if } x \neq a. \end{cases}$$

(Here $(x-a)^{\perp}$ denotes the transpose of the column-vector $x-a$; thus, $(x-a)^{\perp}$ is a row vector.)

Then for $x \neq a$ we have $\nu(x) \cdot (x-a) = f(x) - f(a)$ as desired. Moreover,

$$||\nu(x) - \nabla f(a)|| = \tfrac{|R(x)|}{||x-a||} \to 0 \text{ as } x \to a.$$

Thus ν is continuous at a. Hence the one-row matrix $A_{f,a} := \nu$ satisfies the conditions needed for M-differentiability,

$$f(x) = f(a) + A_{f,a}(x) \cdot (x-a).$$

We also see from the definition of ν that $A_{f,a} = \nu$ is continuous at each point $x \in U$, whenever f is. Also, if ∇f is continuous, then the function

$$H(x,a) = \frac{R_a(x)}{||x-a||} := \frac{f(x) - f(a) - \nabla f(a) \cdot (x-a)}{||x-a||}$$

if $x \neq a$ and $H(a,a) = 0$ is seen to be continuous at (a_0, a_0), since

$$|H(x,a)| = \frac{\left|\int_{[a,x]} [\nabla f(\xi) - \nabla f(a)] \cdot d\xi\right|}{||x-a||}$$

is small whenever $||x - a_0||$ and $||a - a_0||$ are small. Thus

$$(x, a) \mapsto \begin{cases} \nabla f(a) & \text{if } x = a \\ \nabla f(a) + \frac{R_a(x)}{||x-a||^2}(x-a)^{\perp} & \text{if } x \neq a \end{cases}$$

is continuous.

***M*-differentiable implies differentiable.** Let $f(x) = f(a) + A_{f,a}(x) \cdot (x - a)$ and $f'(a) = A_{f,a}(a)$. Consider the linear map $\phi : \mathbb{R}^n \to \mathbb{R}^q$ given by $\phi(x) = f'(a) \cdot x$. We are going to show that $R(x) := f(x) - f(a) - \phi(x - a)$ satisfies $\lim_{x \to a} R(x)/||x - a|| = 0$. In fact, by the Cauchy-Schwarz inequality,

$$\begin{aligned} &\frac{|f(x) - f(a) - \phi(x-a)|}{||x-a||} \\ &\quad = \frac{\big|\big(f(x) - f(a) - A_{f,a}(x)\cdot(x-a)\big) + \big(A_{f,a}(x)\cdot(x-a) - f'(a)\cdot(x-a)\big)\big|}{||x-a||} \\ &\quad = \frac{\big|\big(A_{f,a}(x) - f'(a)\big)\cdot(x-a)\big|}{||x-a||} \\ &\quad \leq \frac{||A_{f,a}(x) - A_{f,a}(a)||\ ||x-a||}{||x-a||} \\ &\quad = ||A_{f,a}(x) - A_{f,a}(a)|| \underset{x\to a}{\longrightarrow} 0. \end{aligned}$$

Hence f is differentiable at a.

The general case, where q is arbitrary, follows at once since $f = (f_1, \ldots, f_q)$ is M-differentiable if and only if each of the coordinate functions is M-differentiable. ■

Using *M*-differentiability

To sum up, we have two representations for differentiable mappings $f : U \subseteq \mathbb{R}^n \to \mathbb{R}^q$:

$$f(x) = f(a) + A_{f,a}(a) \cdot (x - a) + R(x)$$
$$f(x) = f(a) + A_{f,a}(x) \cdot (x - a)$$

where $\lim_{x \to a} ||R(x)||/||x - a|| = 0$ and $A_{f,a}(x)$ is continuous at a. The $q \times n$-matrix $A_{f,a}(a)$ is the Jacobian, $J_f(a)$, associated with f at a.

As a concrete application, we conclude from the second representation that a function f of two variables u and v with $f(0, 0) = 0$ is differentiable at the origin if and only if there exist two functions F and G that are continuous at the origin such that

$$f(u, v) = F(u, v)u + G(u, v)v.$$

In that case $\nabla f(0, 0) = (F(0, 0), G(0, 0))$. Note, however, that a function $f(u, v) = p(u, v)u + q(u, v)v$ may very well be differentiable at the origin if neither p nor q are continuous (or even bounded). This follows from formula (2) which tells us that the representation of f as a dot-product of some vector field $\langle p, q\rangle$ with the radial vector field $\langle u, v\rangle$ is not unique. Just consider the function

$$f(u, v) = \frac{v}{u^2 + v^2}u + \frac{-u}{u^2 + v^2}v \equiv 0,$$

where $p(u, v) = \frac{v}{u^2+v^2}$ and $q(u, v) = \frac{-u}{u^2+v^2}$ are discontinuous at $(0, 0)$.

Next we give an example of a function that is not M-differentiable at (0, 0). Let

$$g(u, v) = \begin{cases} \frac{u^3+v^3}{u^2+v^2} & \text{if } (u, v) \neq (0, 0) \\ 0 & \text{if } (u, v) \neq (0, 0). \end{cases}$$

Then we may write

$$g(u, v) = \underbrace{\frac{u^2}{u^2 + v^2}}_{=A(u,v)} u + \underbrace{\frac{v^2}{u^2 + v^2}}_{=B(u,v)} v,$$

$(u, v) \neq (0, 0)$. Since the factors A and B are discontinuous at (0, 0) we cannot draw a conclusion when applying directly the notion of M-differentiability. One may proceed in the following way, as was suggested to me by Michael Range.

Suppose that g is M-differentiable at (0, 0); that is

$$g(u, v) = F(u, v)u + G(u, v)v$$

with F, G continuous at (0, 0). Then, for $v \neq 0$, $v = g(0, v) = G(0, v)v$; hence $G(0, v) \equiv 1$ and so $G(0, 0) = 1$. Similarly, $F(0, 0) = 1$. But, on the other hand, for $u \neq 0$, $u = g(u, u) = F(u, u)u + G(u, u)u$, and so $F(u, u) + G(u, u) = 1$. If $u \to 0$, then we get the contradiction $2 = 1$.

One may of course use the usual method to prove that g is not differentiable at the origin.

The local inverse theorem revisited. Let us also mention that when using the concept of M-differentiability, one can give a very easy proof of the fact that if $T : \mathbb{R}^n \to \mathbb{R}^n$ is a continuously differentiable map for which the Jacobian $J_T(a)$ is an invertible matrix at some point $a \in \mathbb{R}^n$, then a (local) inverse T^{-1} of T exists on $T(U)$ for some open set U with $a \in U$ and T^{-1} is differentiable there.

In fact, for $s, t \in \mathbb{R}^n$ let $d(s, t) = \det A_{T,s}(t)$. Since by Theorem 2, $d(s, t)$ is continuous and $|d(a, a)| > 0$, we have that $|d(s, t)| \geq |d(a, a)|/2 > 0$ whenever s and t are close to a, say $s, t \in U$. In particular, the matrix $A_{T,s}(t)$ is invertible. Moreover, using the Cramer representation $M^{-1} = \frac{M^{adj}}{\det M}$, where M^{adj} is the adjungate (adjunct) of the invertible matrix M, we see that $[A_{T,s}(t)]^{-1}$ is continuous on $U \times U$, too.

Now supposing that $T(s) = T(t)$ for $s, t \in U$, we obtain

$$0_n = T(t) - T(s) = A_{T,s}(t) \cdot (t - s).$$

Hence $t = s$. We conclude that T is injective in a neighborhood of a and so the inverse T^{-1} of T is well defined on $T(U)$. It also follows from

$$[A_{T,u}(v)]^{-1} \cdot (T(v) - T(u)) = v - u$$

that T^{-1} is continuous on $T(U)$.

Now, for $y = Tx$ with $x \in U$, let $B(y) := [A_{T,a}(x)]^{-1}$ and $b = T(a)$. Then B is continuous at b. Moreover,

$$B(y) \cdot (y - b) = [A_{T,a}(x)]^{-1} \cdot (T(x) - T(a)) = x - a = T^{-1}(y) - T^{-1}(b).$$

Hence T^{-1} is M-differentiable at b.

The essence of our note is that in various situations it is preferable to use our concept of M-differentiability instead of the original (equivalent) definition of differentiability to prove some standard results. The advantage of the "M-method" is to avoid having to estimate the remainder term. Both approaches, though, should be presented in a course.

Addendum. After a first revised version of this note had been submitted, I learned from Professor Ingo Lieb that the notion that I call M-differentiability is not new; and is, in fact, contained in several German textbooks (see [**1, 2, 3, 4**]). It was mainly popularized by Professor Hans Grauert and its school. Some historical aspects on this approach appear also in [**5**] and [**6**].

Acknowledgment I warmly thank Professor Ingo Lieb and Professor Michael Range for their remarks and for forwarding to me the references below.

REFERENCES

1. W. Fischer and I. Lieb, *Einführung in die Komplexe Analysis*, Vieweg + Teubner, Wiesbaden, 2010.
2. H. Grauert and W. Fischer, *Differential-und Integralrechnung II*, Springer, Berlin, 1978.
3. H. Grauert, W. Fischer, and I. Lieb, Differential and integral calculus, *Izdat. "Mir,"* Moscow, 1971 (in Russian).
4. H. Grauert and I. Lieb, *Differential-und Integralrechnung I*, Springer, Berlin, 1973.
5. E. Hairer and G. Wanner, *Analysis in historischer Entwicklung*, Springer, Berlin, 2010.
6. M. Range, Where are limits needed in calculus? *Amer. Math. Monthly* **118** (2011) 404–417; http://dx.doi.org/10.4169/amer.math.monthly.118.05.404.

Summary Based on the notion of M-differentiability, we present a short proof of the differentiability of composite functions in the finite dimensional setting.

The Surprising Predictability of Long Runs

MARK F. SCHILLING
California State University, Northridge
Northridge, CA 91330
mark.schilling@csun.edu

On August 18, 1913, a growing crowd gathered around a roulette table in Monte Carlo as the wheel stopped at black numbers on 26 consecutive spins. On May 15, 1941, baseball player Joe DiMaggio began a hitting streak that lasted for 56 games. And the state of Missouri voted for the winning candidate in every presidential election from 1904 to 1952, then did it again from 1960 to 2004. Long runs of identical outcomes often attract considerable attention, and seem to call for explanation. While any of these events is remarkable in isolation, it turns out that their existence, and especially their lengths, are surprisingly predictable.

When a situation can be modeled as a sequence of independent Bernoulli trials, a simple rule of thumb predicts the length L of the longest run of successes, often with remarkable accuracy. Sometimes we can practically guarantee the exact value of L. The key result is the approximation of the distribution of L by an extreme value distribution. We provide applications to several situations, including the California State Lottery and the digits of π.

Math. Mag. **85** (2012) 141–149. doi:10.4169/math.mag.85.2.141.

The approximate length of the longest success run

Suppose we have a sequence of n independent Bernoulli trials, each with success probability p. (The classic example is a fair coin tossed n times, with success being the outcome "heads" and $p = 1/2$.) By a "success run" we mean a sequence of one or more consecutive successes at the start of the sequence or after any failure. We define the random variable $L = L_n$ to be the length of the longest success run. If N_F is the random variable representing the number of failures, then $E(N_F) = nq$, where $q = 1 - p$, and so we should expect about nq opportunities for success runs. (We assume that $nq \gg 1$, and take that as license to disregard any special considerations involving the first or last runs.) A fraction p of the failures, approximately, should be followed by at least one success, a fraction p^2 should be followed by two or more successes, and so on. In general, therefore, there should be on average about nqp^ℓ success runs of length at least ℓ.

To gauge the likely length of the longest success run, it is reasonable to find the largest value of ℓ for which at least one run of that length would be expected to occur. We thus set $nqp^\ell = 1$ and solve for ℓ to obtain

$$\ell = \log_{1/p}(nq). \tag{1}$$

Using the closest integer to ℓ provides a simple rule of thumb for predicting the length of the longest success run in situations where the Bernoulli trials model can be applied. This formula provides a reasonable approximation as long as $nq \gg 1$.

The run lengths given by this rule of thumb are often longer than what people expect. For example, formula (1) predicts that the longest run of heads in 200 tosses of a fair coin would have length about seven. Yet few individuals, when asked to write down a simulated sequence of 200 coin tosses, include a run as long as seven consecutive heads or tails ([**5**], [**6**]; see also [**7**]). This may go a long way toward explaining the so called "hot hand" phenomenon [**2**], in which a casual observer of a sporting contest or similar situation ascribes a long run to psychological "momentum" when it is entirely compatible with natural variation.

TABLE 1 shows what formula (1) predicts for various n in coin tossing ($p = 1/2$), in ESP card matching (five symbols, so $p = 1/5$), and for the longest run of a given face in tosses of a fair die ($p = 1/6$). Values of ℓ are rounded to the nearest integer.

TABLE 1: Predicted lengths of the longest run for coin tossing, ESP card matching and die tossing

No. of trials (n)	Head runs ($p = 1/2$)	Card Matching ($p = 1/5$)	Die tossing ($p = 1/6$)
100	6	3	2
1000	9	4	4
10,000	12	6	5
1,000,000	19	8	8

The longest runs of identical outcomes

Our model so far has involved consecutive successes in a sequence of Bernoulli trials. But in many situations, we are actually dealing with multinomial trials—that is, each trial has several equally likely outcomes, and we are interested in the longest run of identical outcomes, regardless of which outcome is being repeated.

For example, when rolling a die we might be concerned with the longest sequence in which each roll shows the same face. In the digits of π, any sequence where the same digit or the same pattern of digits repeats many times would draw our attention. Even when there are just two outcomes, it might be that the longest run of either outcome is of interest: a tail run is as notable as a head run, and a losing streak is as newsworthy as a winning streak.

Fortunately, we can adapt our model to this situation. In the case of multinomial trials, we call an outcome a "success" if it repeats the previous outcome. Now a sequence of ℓ "successes" is the same as a sequence of $\ell + 1$ consecutive identical values.

Consider a card-drawing experiment, where we treat the possible outcomes as $2, 3, 4, \ldots, 9, 10, J, Q, K, A$. An experiment might proceed as follows:

Card drawn:	J	J	8	A	K	4	2	9	8	7	7	7	3	A	4
Repeat?	-	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N

Note that the string of two repeats corresponds to a run of three 7's. Since the sequences of Y's and N's represent realizations of the Bernoulli trials model with the successes represented by the Y's, we can still apply formula (1), but need to add 1 to predict the length of the longest run of outcomes in the original sequence.

For the rest of the paper we will return to the success-run model, but now we know that we can translate when needed.

Predictability of the length of the longest run

A prediction such as those in TABLE 1 is just a "best guess" as to the likely length L_n of the longest success run in n trials. But how accurate is it likely to be?

To answer this question it is necessary to know something about the probability distribution of L_n. Here's an outline of how the approximate distribution of L_n can be found. The number of successes at the beginning of the sequence (if any) and the numbers of successes between any failure and the next one are independent, identically distributed random variables. Each of these variables has a *geometric* distribution, which means that the probability that the run has length k is given by

$$p(k) = p^k q$$

for $k = 0, 1, 2, 3, \ldots$. So the distribution of L_n is approximately that of the maximum of $\lfloor nq \rfloor$ independent geometric random variables, where $\lfloor \quad \rfloor$ represents the floor, or greatest integer function.

Due to their discreteness, the limiting distribution of the maximum of $\lfloor nq \rfloor$ independent geometric random variables with parameter p does not exist (see [**3**] and [**6**]). We can obtain an approximate limiting distribution, however, by studying the limiting distribution of the maximum of $\lfloor nq \rfloor$ independent exponential random variables, as exponential random variables are the continuous analog of geometric random variables.

To make the connection explicit, let X be an exponential random variable with parameter $\lambda = -\ln p$. The density and cumulative distribution function (cdf) for an exponential random variable are given by

$$f(x) = \lambda e^{-\lambda x} = \lambda p^x$$

and

$$F(x) = \Pr(X \le x) = 1 - e^{-\lambda x} = 1 - p^x$$

for $x \ge 0$. Now let $Y = \lfloor X \rfloor$; then

$$P(Y = k) = \int_k^{k+1} \lambda e^{-\lambda x}\, dx = e^{-\lambda k}(1 - e^{-\lambda}) = p^k q$$

for $k = 0, 1, 2, \ldots$, which is precisely the geometric probability mass function given above. Thus the distribution of the length of the longest success run can be approximated by the maximum of $\lfloor nq \rfloor$ independent exponential random variables.

Now let $X_1, X_2, X_3 \ldots$ be independent exponential random variables each having parameter $\lambda = -\ln p$, and let $M_n = \max(X_1, X_2, \ldots, X_{\lfloor nq \rfloor})$. We would like to understand the distribution of M_n. Since the value of M_n tends to increase as n increases, it will be more productive to focus on the difference between M_n and our rule-of-thumb estimate (1),

$$E_n = M_n - \log_{1/p}(nq).$$

Write F_E for the limiting cumulative distribution function of the variables E_n. We have

$$\begin{aligned} F_E(x) &= \lim_{n\to\infty} P\left(E_n \le x\right) \\ &= \lim_{n\to\infty} P\left(M_n - \log_p(1/nq) \le x\right) \\ &= \lim_{n\to\infty} \left[P\left(X_1 \le \log_p(1/nq) + x\right)\right]^{\lfloor nq \rfloor} \\ &= \lim_{n\to\infty} \left[1 - p^{\log_p(1/nq)+x}\right]^{\lfloor nq \rfloor} \\ &= \lim_{n\to\infty} \left[1 - \frac{1}{nq} p^x\right]^{\lfloor nq \rfloor} \\ &= e^{-p^x}. \end{aligned} \tag{2}$$

Thus E_n, which approximates the estimation error of our rule-of-thumb estimate, has the limiting distribution given by (2). A random variable whose cumulative distribution has this form is said to have an *extreme value distribution.* Such distributions have been well studied, as they arise in the investigation of the distribution of the maximum of a sequence of independent, identically distributed random variables. The particular type of the extreme value distribution that applies here is also known as the *Gumbel distribution.* Its general form is given below.

Cumulative distribution function:

$$F(x) = P(X \le x) = e^{-e^{-(x-\mu)/\sigma}} \qquad \text{for } -\infty < x < \infty;$$

Density function:

$$\frac{1}{\sigma} e^{(x-\mu)/\sigma} e^{-e^{-(x-\mu)/\sigma}} \qquad \text{for } -\infty < x < \infty;$$

where $-\infty < \mu < \infty$ is a location parameter and $\sigma > 0$ is a scale parameter. See [**1**] for further information regarding extreme value distributions.

For the distribution that approximates the normalized maximum of $\lfloor nq \rfloor$ independent geometric random variables with parameter p, the parameters of the limiting distribution are $\mu = 0$ and $\sigma = 1/\ln(1/p)$ respectively, and the associated density is

$$f(x) = \frac{d}{dx}\left(e^{-p^x}\right) = \ln(1/p)p^x e^{-p^x} \text{ for } -\infty < x < \infty.$$

The mean and standard deviation of the distribution are

Mean: $\gamma \ln(1/p)$, where γ is the Euler-Mascheroni constant $0.577215\ldots$;

Standard deviation: $\dfrac{\pi}{\sqrt{6}\ln(1/p)}$; (3)

and the mode is zero. The density for the case $p = 0.5$ is shown in FIGURE 1 below.

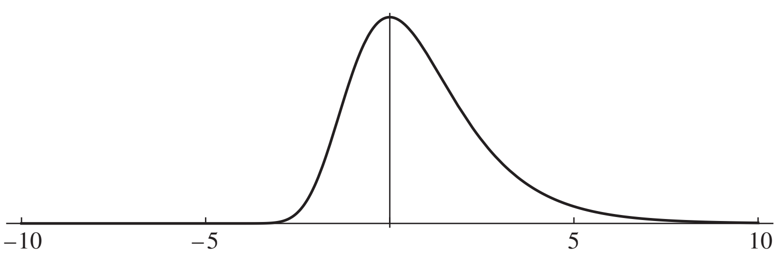


Figure 1 Exteme value (Gumbel) distribution for the case $p = 0.5$ ($\mu = 0$, $\sigma = 1/\ln(2)$)

We have established that the distribution of $L_n - \log_{1/p}(nq)$, the length of the longest success run in n independent Bernoulli trials minus its predicted value given by (1), is well approximated by $\lfloor X \rfloor$, where X is a random variable having the extreme value distribution given in (2). Therefore

$$P(L_n = \ell) \approx P(\ell - \log_{1/p}(nq) \le X < \ell + 1 - \log_{1/p}(nq)).$$

There are some important and interesting consequences of this result. First, notice that—remarkably—the approximate distribution of the prediction error, $L_n - \log_{1/p}(nq)$, does not depend on n. That means that one can predict the length of the longest success run found in, say, a million trials as well as in a hundred! Second, the standard deviation formula (3) shows that the spread of the distribution is generally quite small. This implies great predictability in the length of the longest success run.

For the case of coin tossing, for example, the length of the longest head run will very likely fall within about three of the predicted value $\ell = \log_2(n/2)$—no matter how many tosses are made. For $n = 100$, $\ell = \log_2 50 = 5.64$, so the longest run of heads (or tails) in one hundred tosses is very likely to be in the range 6 ± 3. See FIGURE 2. TABLE 2 illustrates this phenomenon for three values of n that are close to powers of 2.

In each instance there is approximately a 95% probability that the listed interval will capture the actual value of L_n. Again, what is most striking is that the prediction intervals do not get wider as n increases.

Using our theoretical results to check whether famous events such as Joe DiMaggio's hitting streak and the run of 26 spins landing on the black at Monte Carlo are beyond what should be expected presents some challenges. First of all, it is not possible to ascertain with much accuracy the value of n that should apply. Fortunately, since the predicted length of the longest run grows only logarithmically, predictions

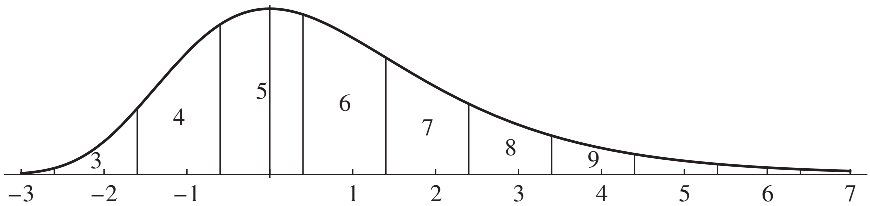


Figure 2 Approximating extreme value distribution for the longest success run in $n = 100$ tosses of a fair coin. The approximate probabilities $P(L = \ell)$ are shown graphically as areas under the curve for $\ell = 3, \ldots, 9$. Adding any positive integer i to each of these values of ℓ gives the graph for the case $n = 2^i \times 100$.

TABLE 2: Prediction intervals for the length of the longest run for coin tossing

No. of trials (n)	$\ell = \log_{1/p}(nq)$	Approximate 95% Prediction Interval
$1000 \approx 2^{10}$	8.97	9 ± 3
$1{,}000{,}000 \approx 2^{20}$	18.93	19 ± 3
$1{,}000{,}000{,}000 \approx 2^{30}$	28.90	29 ± 3

do not change greatly even when n changes by a lot. The Bernoulli trials model is not particularly suitable for baseball, given the great variation in the abilities of hitters and pitchers. Therefore predicting the likely length of the longest hitting streak goes beyond the scope of this paper. We can make a stab at investigating runs of one color in roulette, however.

A minor complication is that $p = P(\text{black})$ is different in American roulette and in the European version, being $18/38$ in the former and $18/37$ in the latter. TABLE 3 below shows the predictions formula (1) gives for both values of p and for various n, along with prediction intervals that take into account the spread of the approximating extreme value distributions around the value given by (1). These distributions have very similar spread to that shown in FIGURE 2 since both values of p are close to 0.5, therefore adding and subtracting three from the value given by (1) again gives a high probability (approximately 95%) of capturing the actual longest run length. The predictions (rounded to the nearest integer) shown in TABLE 3 are for the longest run of either black or red, which as shown earlier are obtained by simply adding 1 to the prediction for black alone.

TABLE 3: Predicted lengths and prediction intervals for the longest run of black or red in roulette

No. of spins (n)	American Roulette ($p = 18/38$)	European Roulette ($p = 18/37$)
100,000,000	25 (22, 28)	26 (23, 29)
500,000,000	27 (24, 30)	28 (25, 31)
1,000,000,000	28 (25, 31)	29 (26, 32)

The results are quite compatible with the actual run of 26; certainly that run was not suspiciously long when seen in the context of a century of experience. It seems reasonable that the actual number of plays of casino roulette that have ever been made is likely to be between 10^8 and 10^9, but even for n well above or below this range an observed longest run of 26 would not be very surprising.

Extremely predictable cases

The smaller the value of p, the more concentrated the approximating extreme value density becomes, and thus the length of the longest success run becomes even more predictable. For example in dice tossing, the probability that the length of the longest run of any particular face ($p = 1/6$) will be one of only three consecutive values oscillates between 92.5% and 97% as n varies (except for very small n, where the chance is even higher). See FIGURES 3 and 4.

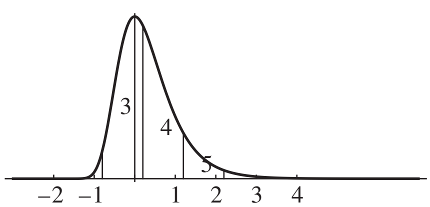


Figure 3 Approximating extreme value distribution for the longest success run in $n = 1000$ tosses of a fair die. There is approximately a 96% chance that the length of the longest run will be one of the three values 3, 4 and 5.

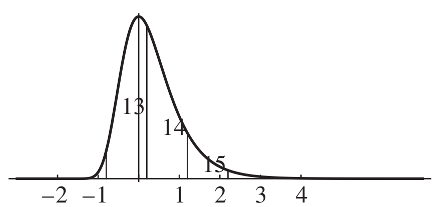


Figure 4 Approximating Extreme Value Distribution for the Longest Success Run in $n = 6^{10} \times 1000$ Tosses of a Fair Die. There is approximately a 96% chance that the length of the longest run will be one of the three values 13, 14 and 15.

In other situations where p is even smaller, we can often almost guarantee the exact length of the longest run. To see this, consider the following argument: The probability of a success run of length at least l immediately following a particular failure is p^ℓ. Let N_ℓ be the number of success runs of length ℓ or longer in n Bernoulli trials. If we condition on the number of failures n_F in the sequence (treat it as given), we obtain

$$\begin{aligned} P(L_n = \ell) &= P(N_\ell > 0, N_{\ell+1} = 0 | n_F) \\ &= P(N_{\ell+1} = 0|n_F) - P(N_\ell = 0|n_F) \\ &= (1 - p^{\ell+1})^{n_F} - (1 - p^\ell)^{n_F} \approx e^{-n_F p^{\ell+1}} - e^{-n_F p^\ell}. \end{aligned}$$

Writing $x = e^{-n_F p^\ell}$, we have $P(L_n = \ell) \approx g(x) = x^p - x$. Simple calculus shows that $g(x)$ is maximized at $x = p^{1/q}$. By the Law of Large Numbers, if n is large we cannot go far wrong by treating n_F as equal to its expected value, nq. Solving $e^{-nqp^\ell} = p^{1/q}$ for n yields

$$n = \frac{\ln(1/p)}{q^2 p^\ell}; \tag{4}$$

which gives

$$P(L_n = \ell) \approx p^{p/q} - p^{1/q}. \tag{5}$$

Formula (4) tells us the "special" values of n (when rounded to the nearest integer) that maximize $P(L_n = \ell)$ for a given success probability p and run length ℓ. The limit of the expression in (5) as p approaches zero (a good calculus exercise!) is 1. Thus if p is small enough and the number of trials is somewhere near the value of n given by (4), then $P(L_n = \ell)$ is close to one. In other words, the longest success run is very likely to have exactly length ℓ.

Here is an application: Twice a day the California Lottery Commission runs a game called the "Daily 3", in which a player chooses any three digit combination. When the drawing is held, the player wins if his or her three numbers match those drawn. The player may buy a ticket that requires that the numbers be matched in order (a "straight"), or one that allows the matches in any order (a "box"). Many other states also offer this game; it has also been run illegally in many big cities for decades.

Suppose we look at the sequence of all drawings over a certain period of time for cases in which the same three number combination appears in a consecutive run of games. As shown earlier, we can compare each drawing to the previous one and define success as the case when the numbers drawn in two successive games are the same. Thus a run of length ℓ successes represents $\ell + 1$ consecutive games with the same set of numbers.

For the case of "straights", $p = (1/10)^3 = .001$. Straightforward calculations from the formulas above show that within any string of around $n = 7000$ games, the longest run of repeats will almost certainly be $\ell = 1$; that is, there will be two games in a row with the same three number sequence, but never three. The chance of this outcome (from (5)) is approximately 99.2%. This is such a high probability that if there were three or more consecutive games with the same number sequence, or no consecutive games with the same number sequence, we might have reason to suspect fraud!

The California Daily 3 has been in operation since April 1992. Checking the first 7000 plays, which cover a span of approximately fifteen years, we find that indeed as predicted, the same straight has occurred in two consecutive drawings (on six occasions), but never has the same straight occurred three times in a row.

As a second illustration, consider the longstanding question of whether the digits of π are a pseudorandom sequence, that is, can be satisfactorily modeled as a string of independent digits in which each digit is equally likely be one of the values 0 through 9. Several studies of this question have been performed over the past half-century; none have found significant evidence against the pseudorandomness hypothesis (see [**4**]). The predictability of long run lengths provides an additional and very simple test of the pseudorandomness of the digits of π.

Clever algorithms along with recent advances in high speed computing have allowed the determination of more than ten trillion digits of π, providing a very large potential database for analysis. We will consider here a much smaller number, however: the first 5,000,000 digits. This n is nearly an optimal value (found from (4) above) for predicting the run length of any two-digit pair with a high degree of certainty. Note that $p = (1/10)^2 = .01$ here if π is pseudorandom. Formula (5) indicates that if the digits of π behave as a random sequence of digits, then with approximately 94.5% probability, the longest run length of any specified two-digit pair will be three. Thus, for example, the string ... 383838 ... will almost certainly be found somewhere within the first 4,700,000 digits of π, but the string ... 38383838 ... will quite likely not be found.

Searching all two-digit pairs (facilitated by the Pi-Search Page at `http://www.angio.net/pi/piquery`) reveals outstanding agreement with the prediction above. For 94 of these 100 pairs the longest run is indeed three. (The other six pairs each have longest runs that are four long—the most curious being 42424242, which begins at digit 242422!) Searches of the digits of π for longest runs of patterns with other than two digits also give excellent support for the hypothesis of pseudorandomness, corroborating what other tests of π have indicated.

Values of n satisfying (4) at least approximately are special values that place nearly all of the mass of the probability distribution of the longest success run on a single value. Even for arbitrary values of n, however, this distribution lives almost entirely on at most two values when p is small. For example, similar calculations to those above show, assuming the digits of π are a pseudorandom sequence, that the chance that the number of consecutive repeats of any particular three-digit pattern within the entire currently known ten trillion digits of π is either four or five is approximately 99.994%.

Acknowledgment Thanks to Andrea Nemeth for preparation of the figures.

REFERENCES

1. Stuart Coles, *An Introduction to Statistical Modeling of Extreme Values*, Springer-Verlag, New York, (2001).
2. T. Gilovich, R. Vallone, and A. Tversky, "The hot hand in basketball: On the misperception of random sequences," *Cognitive Psychology* **17**(3) (1985) 295–314; http://dx.doi.org/10.1016/0010-0285(85)90010-6.
3. L. Gordon, M. F. Schilling, and M. S. Waterman, "An extreme value theory for longest head runs," *Zeitschrift fur Wahrscheinlichkeitstheories verwandt Gebeite* (*Probability Theory and Related Fields*) **72** (1986) 279–287; http://dx.doi.org/10.1007/BF00699107.
4. T. Jaditz, Are the digits of π an independent and identically distributed sequence? *The American Statistician* **54**(1) (2000) 12–16; http://dx.doi.org/10.2307/2685604.
5. P. Révész, Strong Theorems on Coin Tossing, *Proceedings of the International Congress of Mathematicians*, Helsinki, 1978, pp. 749–754.
6. M. F. Schilling, The longest run of heads, *The College Mathematics Journal* **21**(3) (1990) 196–207; http://dx.doi.org/10.2307/2686886.
7. W. Wagenaar, Generation of random sequences by human subjects: A critical survey of the literature, *Psychological Bulletin* **77**(1) (1972) 65–72; http://dx.doi.org/10.1037/h0032060.

Summary When data arise from a situation that can be modeled as a collection of n independent Bernoulli trials with success probability p, a simple rule of thumb predicts the approximate length that the longest run of successes will have, often with remarkable accuracy. The distribution of this longest run is well approximated by an extreme value distribution. In some cases we can practically guarantee the length that the longest run will have. Applications to coin and die tossing, roulette, state lotteries and the digits of π are given.

PROBLEMS

BERNARDO M. ÁBREGO, *Editor*
California State University, Northridge

Assistant Editors: SILVIA FERNÁNDEZ-MERCHANT, California State University, Northridge; JOSÉ A. GÓMEZ, Facultad de Ciencias, UNAM, México; EUGEN J. IONASCU, Columbus State University; ROGELIO VALDEZ, Facultad de Ciencias, UAEM, México; WILLIAM WATKINS, California State University, Northridge

PROPOSALS

To be considered for publication, solutions should be received by September 1, 2012.

1891. *Proposed by Raúl A. Simón, Santiago, Chile.*

Let $ABCD$ be a quadrilateral in the plane. Let A', B', C', and D' be the centroids of the triangles BCD, ACD, ABD, and ABC, respectively. Prove that quadrilaterals $ABCD$ and $A'B'C'D'$ are similar with corresponding sides in the ratio 3 : 1.

1892. *Proposed by José Luis Díaz-Barrero, Applied Mathematics III, Polytechnical University of Catalonia, Barcelona, Spain.*

Compute the limit

$$\lim_{n\to\infty} \frac{1}{n^n} \prod_{k=1}^{n} \left(\frac{n\sqrt{n} + (n+1)\sqrt{k}}{\sqrt{n} + \sqrt{k}} \right).$$

1893. *Proposed by Jerrold W. Grossman and László Lipták, Oakland University, Rochester, MI, and Mike Shaughnessy, Portland State University, Portland, OR.*

Let n be an integer greater than 1, and let

$$f(a_1, a_2, \ldots, a_n) = \prod_{1\le i<j\le n} (a_i - a_j).$$

What is the greatest common divisor of $f(a_1, a_2, \ldots, a_n)$ over all choices of distinct integers $a_1, a_2, \ldots, a_n$?

Math. Mag. **85** (2012) 150–157. `doi:10.4169/math.mag.85.2.150`.

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. Submitted problems should not be under consideration for publication elsewhere.

Solutions should be written in a style appropriate for this MAGAZINE.

Solutions and new proposals should be mailed to Bernardo M. Ábrego, Problems Editor, Department of Mathematics, California State University, Northridge, 18111 Nordhoff St, Northridge, CA 91330-8313, or mailed electronically (ideally as a LaTeX or pdf file) to `mathmagproblems@csun.edu`. All communications, written or electronic, should include **on each page** the reader's name, full address, and an e-mail address and/or FAX number.

1894. *Proposed by Michael W. Botsko, Saint Vincent College, Latrobe, PA.*

Let $(X, \mathfrak{T})$ be a topological space, let S be any subset of X, and let iso(S) be the set of isolated points of S. (A point $x \in S$ is an isolated point of S if there exists an open set O such that $O \cap S = \{x\}$.)

(a) If $(X, \mathfrak{T})$ is second countable, prove that iso(S) is countable. (A topological space $(X, \mathfrak{T})$ is second countable if it has a countable open base.)

(b) If S is a closed set, prove that $S \setminus \text{iso}(S)$ is a closed set.

(c) Prove that the conclusion in (a) does not hold if $(X, \mathfrak{T})$ is only assumed to be separable. (A topological space $(X, \mathfrak{T})$ is separable if it has a countable dense subset.)

(d) Prove that the conclusion in (b) does not hold if S is not assumed to be closed.

1895. *Proposed by Steven Finch, Harvard University, Cambridge, MA*

Let ℓ denote a planar line with slope $\tan(\theta)$ and x-intercept ξ, where θ and ξ are independent random variables with uniform distributions over the intervals $[\pi/4, 3\pi/4]$ and $[-1, 1]$, respectively. Let ℓ_1, ℓ_2, and ℓ_3 be independent copies of ℓ. These three lines determine a compact triangle Δ almost surely. Find the probability density function for the maximum angle α in Δ. Find the first and second moments of α as well.

Quickies

Answers to the Quickies are on page 157.

Q1019. *Proposed by Michael W. Botsko, Saint Vincent College, Latrobe, PA.*

Let $f : [a, b] \to \mathbb{R}$ be a real valued function and $\Gamma = \{(x, f(x)) : x \in [a, b]\}$ the graph of f. Suppose that Γ is a closed and bounded subset of $\mathbb{R}^2$. Prove or disprove that f is continuous on $[a, b]$.

Q1020. *Proposed by Michael W. Ecker, Mathematics Department, Pennsylvania State University, Lehman, PA.*

Find all values of n for which the sum $1 + 2 + \cdots + n$ is an integer power of 10.

Solutions

Variations on the Steiner–Lehmus Theorem **April 2011**

1866. *Proposed by Sadi Abu-Saymeh and Mowaffaq Hajja, Mathematics Department, Yarmouk University, Irbid, Jordan.*

Let ABC be a triangle, and L and M interior points on $\overline{AB}$ and $\overline{AC}$, respectively, such that $AL = AM$. Let P be the intersection of $\overline{BM}$ and $\overline{CL}$. Prove that $PB = PC$ if and only if $AB = AC$.

Solution by I. E. Leonard, J. E. Lewis, A. C. F. Liu, and G. Tokarsky, University of Alberta, Edmonton, Alberta, Canada.
Suppose that $AB = AC$. (See FIGURE (a).) Hence triangle ABC is isosceles. It follows that $BL = AB - AL = AC - AM = CM$, and so by the SAS Congruency Theorem, $\triangle LBC \cong \triangle MCB$. Therefore, $\angle PCB = \angle PBC$ which means that $\triangle BPC$ is isosceles, and thus $BP = PC$.

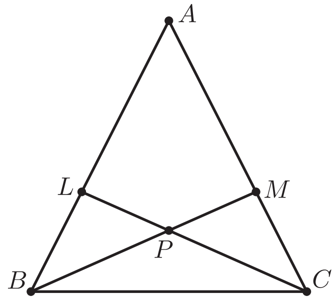


Figure (a)

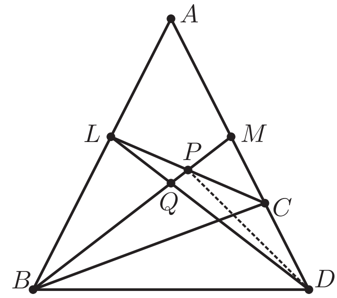


Figure (b)

Conversely, suppose that $AL = AM$, $PB = PC$ but, without loss of generality, $AB > AC$. (See FIGURE (b).) Let D be the point in the ray AC such that $AB = AD$. Let Q be the intersection of $\overline{BM}$ and $\overline{DL}$. By the sufficiency part $BQ = DQ$. Because C is between M and D, it follows that P is between Q and M. Hence, by the triangle inequality,

$$PB = PQ + QB = PQ + QD > PD.$$

An exterior angle of a triangle is greater than either of the opposite interior angles, and triangles ALM and ABD are similar isosceles triangles. Thus

$$\angle DCP > \angle ALC > \angle ALM = \angle ADB > \angle CDP.$$

In a triangle, the larger angle is opposite to the longer side, thus $\angle DCP > \angle CDP$ implies that $PD > PC$, and therefore $PB > PC$.

Editor's Note. As pointed out by Eugene A. Herman the statement of the problem needs to assume that $L \neq B$ or $M \neq C$, otherwise P is not uniquely defined. We modified the statement to avoid this ambiguity. We received many solutions which used a similar argument or end with an application of Ceva's Theorem instead. Many solutions were based on relatively hard calculations. This problem is closely related to the classical problem (Steiner–Lehmus Theorem) of showing that two angle bisectors in a triangle are equal if and only if the triangle is isosceles.

Also solved by Dionne Bailey, Michel Battaille (France), Elton Bojaxhiu (Germany) and Enkel Hysnelaj (Australia), Bruce S. Burdick, Robert Calcaterra, CMC 328, Tim Cross (United Kingdom), David Doster, Robert L. Doucette, Thomas Gettys, Ahmad Habil (Syria), Eugene A. Herman, Jeong Hwan Kim (Korea), L. R. King, Omran Kouba (Syria), Victor Y. Kutsenok, Elias Lampakis (Greece), Kee-Wai Lau (China), Longxiang Li and Luyuan Yu (China), Graham Lord, Masao Mabuchi (Japan), Kathleen Marsh, Joel Schlosberg, Vasile G. Teodorovici (Canada), Stuart V. Witt, Michael Woltermann, and the proposers. There were eight incomplete or incorrect submissions.

A Mean Value Theorem for *n* values **April 2011**

1867. *Proposed by Ángel Plaza and César Rodríguez, Department of Mathematics, Universidad de Las Palmas de Gran Canaria, Las Palmas, Spain.*

Let $f : [0, 1] \to \mathbb{R}$ be a continuous function such that $\int_0^1 f(t)\, dt = 1$ and n a positive integer. Show that

1. there are distinct $c_1, c_2, \ldots, c_n$ in $(0, 1)$ such that

$$f(c_1) + f(c_2) + \cdots + f(c_n) = n,$$

2. there are distinct $c_1, c_2, \ldots, c_n$ in $(0, 1)$ such that

$$\frac{1}{f(c_1)} + \frac{1}{f(c_2)} + \cdots + \frac{1}{f(c_n)} = n.$$

I. *Solution by Tania Moreno García, University of Holguín, Cuba, and Pablo Suárez, University of Las Palmas de Gran Canaria, Spain.*
By the Mean Value Theorem, for each $1 \le k \le n$, there exists $c_k \in ((k-1)/n, k/n)$ such that

$$n\int_{(k-1)/n}^{k/n} f(t)\,dt = \frac{1}{k/n-(k-1)/n}\int_{(k-1)/n}^{k/n} f(t)\,dt = f(c_k).$$

Adding these identities gives

$$n = n\int_0^1 f(t)\,dt = n\sum_{k=1}^{n}\int_{(k-1)/n}^{k/n} f(t)\,dt = \sum_{k=1}^{n} f(c_k).$$

This proves the first part.

For the second part, note that there are numbers $0 = a_0 < a_1 < \ldots < a_{n-1} < a_n = 1$ such that $\int_0^{a_k} f(t)dt = k/n$ for $1 \le k \le n$. Thus $\int_{a_{k-1}}^{a_k} f(t)dt = 1/n$ for $1 \le k \le n$. Applying the Mean Value Theorem to each of these integrals shows that there are $c_k \in (a_{k-1}, a_k)$ such that

$$\frac{1}{n(a_k - a_{k-1})} = \frac{1}{a_k - a_{k-1}}\int_{a_{k-1}}^{a_k} f(t)\,dt = f(c_k);$$

that is $1/f(c_k) = n(a_k - a_{k-1})$. Adding these identities gives

$$\sum_{k=1}^{n}\frac{1}{f(c_k)} = n\sum_{k=1}^{n}(a_k - a_{k-1}) = n.$$

II. *Solution by Arnold Adelberg and Eugene A. Herman, Department of Mathematics, Grinnell College, Grinnell, IA.*
We prove a more general result: Suppose g is a continuous, real-valued function on an open interval I, y is in $g(I)$, and n is a positive integer. If either g is constant on I or y is not an extreme value of g, then there are distinct $c_1, c_2, \ldots, c_n$ in I such that

$$g(c_1) + g(c_2) + \cdots + g(c_n) = ny. \tag{1}$$

In other words, any non-extremal value of a continuous non-constant function is the average of n nearby values, for any n.

If g is constant, then equation (1) holds for any $c_1, c_2, \ldots, c_n$ in I. Otherwise, since $g(I)$ is an interval and y is not an endpoint, there exists $\delta > 0$ such that $(y-\delta, y+\delta) \subseteq g(I)$. Thus, if $a_1, a_2, \ldots, a_n$ are distinct real numbers with $\sum_{k=1}^{n} a_k = 0$ and $|a_k| < \delta$ for $1 \le k \le n$, then $\sum_{k=1}^{n}(y + a_k) = ny$ and $y + a_k \in g(I)$ for $1 \le k \le n$. Since $y + a_k = g(c_k)$ for distinct $c_k \in I$, the result follows.

This result implies the statement in the problem as follows. By the Mean Value Theorem, there exists a $c \in (0, 1)$ such that $1 = \int_0^1 f(x)\,dx = f(c)$. By continuity, if f is not constant, then there are $a, b \in (0, 1)$ such that $f(a) < 1 < f(b)$. Also by continuity we may assume that $f > 0$ on (a, b). For the first part in the problem, let $g = f$, $I = (0, 1)$, and $y = 1$; for the second part, let $g = 1/f$, $I = (a, b)$, and $y = 1$.

Also solved by Michael Andreoli; Dionne Bailey, Elsie Campbell, and Charles Diminnie; Michel Bataille (part 1 only, France); Elton Bojaxhiu (Germany) and Enkel Hysnelaj (Australia); Michael W. Botsko and Larry J. Mismas; Paul Budney; Bruce S. Burdick; Charles Burnette; Robert Calcaterra; John Christopher; Con Amore Problem Group (Denmark); Charles Degenkolb; Patrick Devlin; Robert L. Doucette; Dmitry Fleischman; William R. Green; Lee O. Hagglund; Mowaffaq Hajja and Mostafa Hayajneh (Jordan); Robert Jones;

John C. Kieffer; Michael Knapp; Omran Kouba (Syria); Elias Lampakis (Greece); Longxiang Li and Luyuan Yu (China); Jody M. Lockhart; Raymond Maruca; Cristinel Mortici (Romania); Raymond Mortini (France); Edwin Gonzalo and Murcia Rodríguez (Colombia); Northwestern University Math Problem Solving Group; Joel Schlosberg; Allen Stenger; Philip Straffin; Haryono Tandra; Marian Tetiva (Romania); Texas State University Problem Solvers Group; Dave Trautman; Alfred Witkowski (Poland); Stuart V. Witt; and the proposers.

Tiling a square ring with dominoes **April 2011**

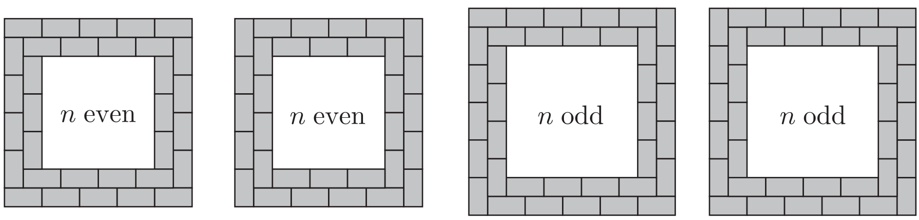
1868. *Proposed by Donald E. Knuth, Stanford University, Stanford, CA.*

Let $n \geq 2$ be an integer. Remove the central $(n-2)^2$ squares from an $(n+2) \times (n+2)$ array of squares. In how many ways can the remaining squares be covered with $4n$ dominoes?

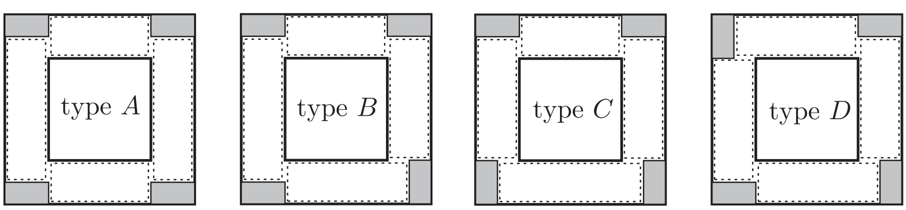
Solution by John Bonomo and David Offner, Department of Mathematics and Computer Science, Westminster College, New Wilmington, PA.

The total number of coverings is $16F_n^4 + 16(-1)^n F_n^2 + 4 = 4(2F_n^2 + (-1)^n)^2$, where F_n is the n^{th} Fibonacci number, defined recursively as $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$.

For every n, there are exactly two ways to cover the array so that no pair of dominoes covers a 2×2 sub-array.



The remaining cases can be divided according to the orientation of the dominoes covering the four corner squares of the array. Since each corner square of the array may be covered by a domino oriented horizontally or vertically, there are 16 possible configurations. These configurations can be partitioned into four symmetry classes: Two of type A, eight of type B, four of type C, and two of type D according to the figure below. To count the number of coverings for each configuration, it remains to count the number of ways to cover the rectangular arrays outlined by dashes in the figure.



It is well known that the number of ways to cover a $2 \times m$ array of squares with m dominoes is F_{m+1}. So, for configurations of type A, there are two $2 \times n$ rectangles, and two $2 \times (n-2)$ rectangles, and the total number of coverings of this type is $2F_{n+1}^2 F_{n-1}^2$. Similarly, there are $8F_{n+1}F_n^2 F_{n-1}$ coverings of type B, $4F_{n+1}F_n^2 F_{n-1}$ coverings of type C, and $2F_n^4$ coverings of type D, for a total number of coverings of

$$2F_{n+1}^2 F_{n-1}^2 + 12F_{n+1}F_n^2 F_{n-1} + 2F_n^4 + 2.$$

This total is equivalent to the answer given above, as is shown by using Cassini's Identity $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$.

Editor's Note. Some solvers pointed out that this problem was solved in Roberto Tauraso, A New Domino Tiling Sequence, *Journal of Integer Sequences* **7** (2004), Article 04.2.3. The sequence of solutions also appears as sequence A061646 in the *Sloane's On-Line Encyclopedia of Integer Sequences*.

Also solved by Elton Bojaxhiu (Germany) and Enkel Hysnelaj (Australia), Bruce S. Burdick, Con Amore Problem Group (Denmark), Marty Getz and Dixon Jones, Amanda Goodrick, G.R.A.20 Problem Solving Group (Italy), Harris Kwong, David Nacin, Joel Schlosberg, John H. Smith, Philip Straffin, and the proposer. There was one incorrect submission.

A triangle inequality for triangle side-lengths **April 2011**

1869. *Proposed by Marian Dincă, Bucharest, Romania.*

Let $f : \mathbb{R} \to \mathbb{R}$ be an increasing and concave-down function such that $f(0) = 0$. Prove that if x, y, and z are real numbers, and a, b, and c are the lengths of the sides of a triangle, then

$$(x-y)(x-z)f(a) + (y-x)(y-z)f(b) + (z-x)(z-y)f(c) \geq 0.$$

Solution by Charles Burnette, Philadelphia, PA.

Recall that if a function $f : \mathbb{R} \to \mathbb{R}$ is concave-down, and $f(0) \geq 0$, then f is sub-additive. Combining this with the fact that f is increasing and that a, b, and c are side lengths of a triangle, we have that $f(a) < f(b+c) \leq f(b) + f(c)$. Similarly $f(b) < f(a) + f(c)$ and $f(c) < f(a) + f(b)$. Hence $f(b) + f(c) - f(a) > 0$, $f(c) + f(a) - f(b) > 0$, and $f(a) + f(b) - f(c) > 0$.

We now employ the following notation:

$$\begin{aligned}\sum_{\text{cyc}} &(x-y)(x-z)f(a) \\ &= (x-y)(x-z)f(a) + (y-x)(y-z)f(b) + (z-x)(z-y)f(c),\end{aligned}$$

where the sum is taken over all cyclic permutations of (a, b, c) and (x, y, z) where (a, b, c) corresponds to (x, y, z). Thus $\sum_{\text{cyc}}(x-y)(x-z)f(a)$ equals

$$\begin{aligned}\sum_{\text{cyc}} \frac{1}{2}&(x-y)(x-z)\left[(f(c)+f(a)-f(b)) + (f(a)+f(b)-f(c))\right] \\ &= \frac{1}{2}\sum_{\text{cyc}}(x-y)(x-z)\left(f(c)+f(a)-f(b)\right) \\ &\qquad + \frac{1}{2}\sum_{\text{cyc}}(x-y)(x-z)\left(f(a)+f(b)-f(c)\right) \\ &= \frac{1}{2}\sum_{\text{cyc}}(z-x)(z-y)\left(f(b)+f(c)-f(a)\right) \\ &\qquad + \frac{1}{2}\sum_{\text{cyc}}(y-z)(y-x)\left(f(b)+f(c)-f(a)\right) \\ &= \frac{1}{2}\sum_{\text{cyc}}\left[(z-x)(z-y)+(y-z)(y-x)\right]\left(f(b)+f(c)-f(a)\right) \\ &= \frac{1}{2}\sum_{\text{cyc}}(y-z)^2((f(b)+f(c)-f(a)) \;\geq\; 0,\end{aligned}$$

as desired.

Also solved by Dionne Bailey, Elsie Campbell, and Charles Diminnie; Michel Bataille (France); Bruce S. Burdick; Robert Calcaterra; Con Amore Problem Group (Denmark); Dmitry Fleischman; Paul Loomis; Scott Pauley, Natalya Weir, and Andrew Welter; Paolo Perfetti (Italy); Joel Schlosberg; Haohao Wang and Jerzy Wojdyło; Stuart V. Witt; and the proposer. There were two incorrect submissions.

A double zeta sum **April 2011**

1870. *Proposed by Ovidiu Furdui, Campia Turzii, Cluj, Romania.*

Calculate

$$\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{m(\zeta(n+m)-1)}{(n+m)^2},$$

where ζ denotes the Riemann Zeta function.

Solution by Joel Schlosberg, Bayside, NY.
For $x \in (0,1)$, the power series for $x/(1-x)$ and $\ln(1-x)$ converge absolutely, so

$$\frac{x}{1-x}+\ln(1-x)=\sum_{k=1}^{\infty}x^k-\sum_{k=1}^{\infty}\frac{x^k}{k}=\sum_{k=1}^{\infty}\frac{k-1}{k}x^k=\sum_{k=2}^{\infty}\frac{k-1}{k}x^k.$$

The terms of the double series are all positive. So we may rearrange the order of summation. Then

$$\begin{aligned}
\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{m(\zeta(n+m)-1)}{(n+m)^2} &= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{m}{(n+m)^2}\sum_{j=2}^{\infty}\frac{1}{j^{n+m}} \\
&= \sum_{j=2}^{\infty}\sum_{m=1}^{\infty}\sum_{n=1}^{\infty}\frac{m}{(n+m)^2 j^{n+m}} = \sum_{j=2}^{\infty}\sum_{m=1}^{\infty}\sum_{k=m+1}^{\infty}\frac{m}{k^2 j^k} \\
&= \sum_{j=2}^{\infty}\sum_{k=2}^{\infty}\sum_{m=1}^{k-1}\frac{m}{k^2 j^k} = \sum_{j=2}^{\infty}\sum_{k=2}^{\infty}\frac{\frac{1}{2}(k-1)k}{k^2 j^k} = \frac{1}{2}\sum_{j=2}^{\infty}\sum_{k=2}^{\infty}\frac{k-1}{k}(j^{-1})^k \\
&= \frac{1}{2}\sum_{j=2}^{\infty}\left(\frac{j^{-1}}{1-j^{-1}}+\ln(1-j^{-1})\right) = \frac{1}{2}\sum_{j=2}^{\infty}\left(\frac{1}{j-1}+\ln(j-1)-\ln j\right) \\
&= \frac{1}{2}\lim_{N\to\infty}\sum_{j=2}^{N}\left(\frac{1}{j-1}+\ln(j-1)-\ln j\right) \\
&= \frac{1}{2}\lim_{N\to\infty}\left(\left(\sum_{j=1}^{N}\frac{1}{j}-\ln N\right)-\frac{1}{N}\right)=\frac{\gamma}{2},
\end{aligned}$$

where $\gamma=\lim_{N\to\infty}(\sum_{n=1}^{N}1/n-\ln N)$ is the Euler-Mascheroni constant.

Also solved by Michel Bataille (France), Bruce S. Burdick, Charles Burnette, Dmitry Fleischman, Michael Goldenberg and Mark Kaplan, G.R.A.20 Problem Solving Group (Italy), Eugene A. Herman, Enkel Hysnelaj (Australia) and Elton Bojaxhiu (Germany), Omran Kouba (Syria), Peter W. Lindstrom, Rituraj Nandan, Paolo Perfetti (Italy), Nicholas C. Singer, Satyanand Singh, Michael Vowe (Switzerland), and the proposer.

Answers

Solutions to the Quickies from page 151.

A1019. We prove that f is continuous on $[a, b]$. Define the function $g : \Gamma \to [a, b]$ such that $g((x, f(x))) = x$. Clearly g is both one-to-one and onto and thus the inverse function $g^{-1} : [a, b] \to \Gamma$ exists. Using the sequential definition of continuity, it follows that g is continuous on Γ. Thus g is a homeomorphism because it is a one-to-one continuous mapping of a compact space onto a Hausdorff space. Since g is a homeomorphism, g^{-1} is continuous on $[a, b]$. However, since $g^{-1}(y) = (y, f(y))$, it follows that f is continuous on $[a, b]$.

A1020. The only solutions are $n = 1$ and $n = 4$. Indeed $1 = 10^0$ and $1 + 2 + 3 + 4 = 10^1$. To prove no others exist, suppose $T_n := 1 + 2 + \cdots + n = \frac{1}{2}n(n + 1) = 10^k$ for some nonnegative integer k. If $n \geq 2$, then $T_n > 1$ and thus we may assume that $k \geq 1$. Then $n(n + 1) = 2 \cdot 10^k = 2^{k+1} \cdot 5^k$. Since n and $n + 1$ relatively prime, we must have $n = 2^{k+1}$ and $n + 1 = 5^k$, as $5^k > 2^{k+1}$ precludes the case of $n + 1 = 2^{k+1}$ and $n = 5^k$. Thus, $5^k - 2^{k+1} = 1$. However, $5^k = (2^2 + 1)^k \geq 2^{2k} + 1 \geq 2^{k+1} + 1$ where the equalities hold if and only if $k = 1$.

REVIEWS

PAUL J. CAMPBELL, *Editor*
Beloit College

Assistant Editor: Eric S. Rosenthal, West Orange, NJ. Articles, books, and other materials 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.

Aron, Jacob, Key mathematical tool sees first advance in 24 years, *New Scientist* (9 December 2011) http://www.newscientist.com/article/dn21255-key-mathematical-tool-sees-first-advance-in-24-years.html.

Lipton, R.J., A breakthrough on matrix product, http://rjlipton.wordpress.com/2011/11/29/a-breakthrough-on-matrix-product/. A brief history of matrix product, http://rjlipton.wordpress.com/2012/02/01/a-brief-history-of-matrix-product/.

Williams, Virginia Vassilevska, Breaking the Coppersmith-Winograd barrier, http://www.cs.berkeley.edu/~virgi/matrixmult.pdf.

Naïve multiplication of $n \times n$ matrices requires n^3 multiplications. In 1969, Volker Strassen, building on an algorithm to multiply 2×2 matrices with 7 multiplications instead of 8, devised an algorithm for $n \times n$ matrices with $n^{\lg 27} \approx n^{2.807}$ multiplications (at the expense of more additions). In 1990, Coppersmith and Winograd reduced the exponent to 2.376, with no further improvement until now, when Virginia Vassilevska Williams (UC Berkeley and Stanford University) has edged it down to 2.373 by applying the Coppersmith-Winograd method eight times. Lipton says the new algorithm is *galactic*: "wonderful in its asymptotic behavior, but is never used to actually compute anything."

Gonick, Larry, *The Cartoon Guide to Calculus*, HarperCollins, 2012; x + 240 pp, $18.99 (P). ISBN 978-0-06-168909-3.

Larry, what took you so long? Author Gonick has a master's in mathematics from Harvard, used to teach calculus there, and had an earlier success with his *The Cartoon Guide to Statistics*. No doubt doing 19 volumes of *The Cartoon History of the Universe* and a dozen other books delayed this inevitable contribution to student culture. The book is imaginative, fun, and thorough; there are proofs of almost everything, and there are even exercises (sorry, no answers to odd ones). This book is already outselling his *The Cartoon Guide to Sex*—which is to be anticipated, since fewer people can be expected to be self-educated in calculus.

Ash, Avner, and Robert Gross, *Elliptic Tales: Curves, Counting, and Number Theory*, Princeton University Press, 2012; xix + 250 pp, $29.95. ISBN 978-0-691-15119-9.

One of the Clay Institute's seven million-dollar Millennium Problems is the Birch–Swinnerton-Dyer (BSD) conjecture: An elliptic curve over the rationals has algebraic rank equal to its analytic rank. This book explains the conjecture. The reader needs to know some calculus, have a tolerance for mathematical symbolism, and be willing to learn concepts along the way (such as analytic continuation of L-functions, and the rank of a torsion subgroup of an infinite but finitely generated abelian group). Such minimal prerequisites and its clear writing make this book (which even has a few exercises) a great choice for a seminar for mathematics majors, who at some point should have such an excursion to one of the frontiers of mathematics.

Math. Mag. **85** (2012) 158–159. doi:10.4169/math.mag.85.2.158.

Stutzer, Michael, A simple Parrondo paradox, *Mathematical Scientist* 35 (1) (2010) 23–28, http://leeds.colorado.edu/asset/burridge/simpleparrondoparadox.pdf.

———, The paradox of diversification, *Journal of Investing* 19 (1) (Spring 2010) 32–35.http://leeds.colorado.edu/asset/burridge/paradoxofdiversification.pdf.

Abbott, Derek, Welcome to the Adelaide Parrondo's Paradox Group, http://www.eleceng.adelaide.edu.au/Groups/parrondo/index.html.

The Parrondo paradox: In terms of expected value, losing games can sometimes be combined to result in a winning game. The "official Parrondo's paradox website" at the University of Adelaide provides an introduction, an informative FAQ, and links to research papers and popular expositions. Author Stutzer pursues a variation, illustrating the same kind of paradox but in terms of median outcome. What should intensify the reader's interest in such paradoxes is his analogy to the stock market, for which he provides a "spectacular demonstration" of the value of the buy-and-hold strategy and of the even better strategy of continuously rebalancing.

Mackenzie, Dana, *What's Happening in the Mathematical Sciences*, vol. 8, American Mathematical Society, 2011; vi + 129 pp, $23 (P). ISBN 978-0-821-84999-6.

With a beautiful color illustration on almost every page, this volume in the series of popularizations of research mathematics is as attractive as it is informative. The nine essays by science writer Mackenzie reflect on the Netflix million-dollar algorithm contest, periodic orbits for dynamical systems, models behind the financial crisis, "the ultimate billiard shot," health models vs. clinical trials, the phase change between order and randomness, quantum chaos, geometric packings, and the instability of the Kervaire invariant involved in classifying exotic spheres.

Wainer, Howard, *Picturing the Uncertain World: How to Understand, Communicate, and Control Uncertainty through Graphical Display*, Princeton University Press, 2009; xviii + 244 pp, $29.95, $19.95 (P). ISBN 978-0-691-13759-9, 978-0-691-15267-7.

This volume collects 19 of Wainer's columns from *Chance* magazine plus two other previously published essays. He treats statistical analysis and data presentation for political issues and for educational testing, examines statistical methodology, and delves into the history of data presentation. There are friendly few equations (fewer than a handful), numerous and informative graphs, and 16 pages of delightful color plates. Even an experienced statistician will find valuable insights in this book of careful thought, clear exposition, and fine visualization.

Cambridge University Mathematical Society, *Eureka: A Journal of The Archimedeans* 61 (October 2011), 96 pp, £5. Subscription details from archim-subscriptions-manager@srcf.ucan.org.

Shepherd, Sarah, *iSquared Mathematics Magazine: Mathematics Beyond the Imaginary*, http://www.isquaredmagazine.co.uk/.

For decades, I have subscribed to *Eureka*, an annual publication by a society of undergraduate mathematics students at Cambridge University. Although most authors are undergraduates, there have also been contributions from "luminaries": Hardy, Dirac, Gowers, Erdős, Conway, Gardner, Penrose, Hawking. This latest issue, however, is not your doctoral grandfather's *Eureka* but a shockingly good "reinvention" directed at an audience beyond Cambridge: full color (including a striking cover), imaginative design, superb illustrations, a "number dictionary" accompanying the page numbers, and several advertisements (I hope those or a rich new patron are paying for the renovation!). *Eureka*'s articles are short; this year they include a Bayesian analysis of the Monty Hall problem, mathematical origami, how to teach physics to mathematicians (preview: physics courses are unsuitable), a showroom of images, using the finite simple groups, and much more. In addition, there are book reviews, movie reviews, and a problems section. The redesign reminds me of Sarah Shepherd's extraordinary but short-lived (2007–2010) magazine *iSquared: Mathematics Beyond the Imaginary*, which I wish I had discovered (and communicated to you) before she closed it to concentrate on finishing her mathematics Ph.D.

Sarah Shepherd died in late 2011. Purchase of back copies of *iSquared* contributes to Rethink Mental Illness, a registered U.K. charity.

MAA
MATHEMATICAL ASSOCIATION OF AMERICA 1529 Eighteenth St., NW • Washington, DC 20036

CONTENTS

ARTICLES

NOTES

PROBLEMS

REVIEWS