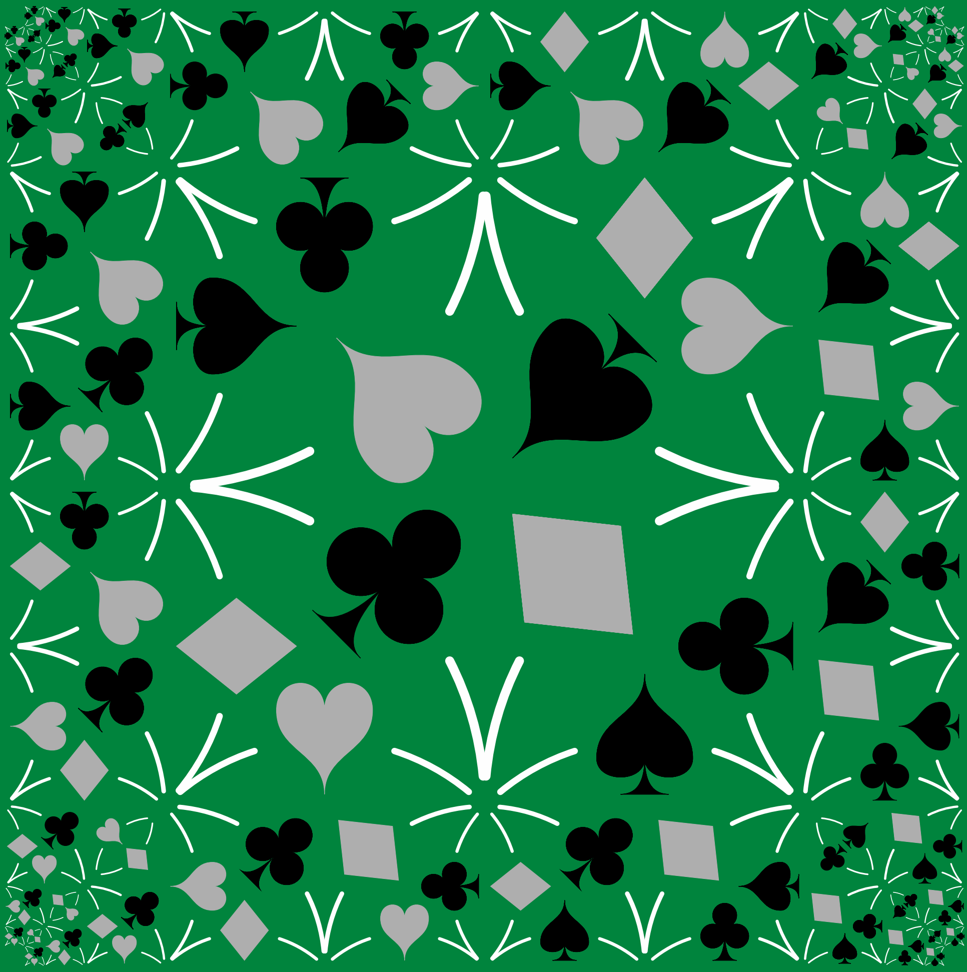
Vol. 88, No. 2, April 2015

MAA

MATHEMATICS MAGAZINE



- Permutations and a trick with playing cards
- Julia sets of 4-dimensional graphs
- Return of the ubiquitous (7,3,1) design
- Algorithms for rationalizing denominators

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.

Submissions of articles are required via the *Mathematics Magazine*'s Editorial Manager System. The name(s) of the author(s) should not appear in the file. Initial submissions in pdf or LaTeX form can be sent to the editor at www.editorialmanager.com/mathmag/.

The Editorial Manager System will cue the author for all required information concerning the paper. Questions concerning submission of papers can be addressed to the editor at mathmag@maa.org. Authors who use LaTeX are urged to use the Magazine article template. However, a LaTeX file that uses a generic article class with no custom formatting is acceptable. The template and the Guidelines for Authors can be downloaded from www.maa.org/pubs/mathmag.

MATHEMATICS MAGAZINE (ISSN 0025-570X) is published by the Mathematical Association of America at 1529 Eighteenth Street, NW, Washington, DC 20036 and Lancaster, PA, in the months of February, April, June, October, and December.

Microfilmed issues may be obtained from
University Microfilms International, Serials Bid Coordinator, 300 North Zeeb Road, Ann Arbor, MI 48106.

Address advertising correspondence to

MAA Advertising
1529 Eighteenth St. NW
Washington, DC 20036
Phone: (202) 319-8461
E-mail: advertising@maa.org

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

Change of address, missing issue inquiries, and other subscription correspondence can be sent to:

The MAA Customer Service Center
P.O. Box 91112
Washington, DC 20090-1112
(800) 331-1622
(301) 617-7800
maaservice@maa.org

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, NW, Washington, DC 20036-1385.

Printed in the United States of America.

COVER IMAGE

Suit Soirée © 2015 David A. Reimann (*Albion College*). Used by permission.

This artwork is a four-fold arrangement of the conventional playing card suits after a self-similar division of the square used by M.C. Escher in his 1956 work *Smaller and Smaller*.

Vol. 88, No. 2, April 2015

MATHEMATICS MAGAZINE

LETTER FROM THE EDITOR

How do you visualize the graph of a function from the complex plane to itself? In the lead article of this issue, Julia A. Barnes, Clinton P. Curry, Elizabeth D. Russell, Lisbeth E. Schaubroeck do so by considering the graphs of the real and imaginary parts of complex functions, viewing them as "shadows" of the four-dimensional graph. They use these shadows to consider the filled Julia sets that emerge when complex functions are iterated.

Ezra Brown provided many names for the (7, 3, 1) combinatorial design in his 2002 article for THIS MAGAZINE. In this issue, Brown offers more names for the design through its connections to error-correcting codes, finite projective geometries, difference sets, and real normed algebras.

Allan Berele and Stefan Catoiu use rationalizing denominators of fractions as a springboard to explain ideas from linear algebra, symmetric function theory, field theory, and algebraic number theory. Their article shows how systematic thinking of even elementary topics may lead to higher mathematics. This contrasts well with the piece by Breeanne Baker Swart and Brittany Shelton. They demonstrate that mathematical thinking may also arise in unusual places by describing and generalizing a card trick they first saw on *The Ellen DeGeneres Show*.

This issue marks the first in which anecdotes from past MAGAZINE editors appear to celebrate the 100th anniversary of the MAA. Look for the anecdote that describes how Roger B. Nelsen suggested that proofs without words be used to fill white space at the end of articles. Nelsen and co-drawer Claudi Alsina provide a proof without words of the Cauchy-Schwarz inequality. Nelsen also offers a picture to prove a trigonometric identity.

In between the two proofs without words is Owen D. Byer and Deirdre L. Smeltzer's extension to higher dimensions of a geometric result about three mutually tangent circles in the plane. They use the method of inversions to prove their result, relating it to an observation by H.S.M. Coxeter. Massimo Galuzzi generalizes two unusual proofs of Fermat's Little Theorem from THIS MAGAZINE by considering families of functions with certain properties. The Chebyshev polynomials also satisfy the properties.

The issue rounds out with a crossword puzzle by Brendan W. Sullivan as well as the Reviews and Problems sections. You may have noticed that the Magazine is behind in its production schedule. This is due in part to a number of changes in how the MAA journals are produced. In an effort to return to the schedule, in this issue, the Problems section is abbreviated, only containing proposals, quickies, and the answers to the quickies. Solutions will return in the June issue.

Michael A. Jones, Editor

Emerging Julia Sets

JULIA A. BARNES
Western Carolina University
Cullowhee, NC 28723
jbarnes@email.wcu.edu

CLINTON P. CURRY
Huntingdon College
Montgomery, AL 36106
clintonc@clintoncurry.net

ELIZABETH D. RUSSELL
Western New England University
Springfield, MA 01119
elizabeth.d.russell@gmail.com

LISBETH E. SCHAUBROECK
United States Air Force Academy
USAF Academy, CO 80840
beth.schaubroeck@usafa.edu

In single-variable calculus, if we want to see the graph of a function, we simply push a few buttons on a calculator. In multivariable calculus, we can use a computer algebra system. However, it gets much more complicated to visualize graphs of functions from the complex plane to itself. Why? The complex plane is two dimensional, so the graph of any function from $\mathbb{C} \to \mathbb{C}$ is four dimensional. We live in a three-dimensional world, so it is a bit complicated to imagine a four-dimensional graph, much less find appropriate technology to generate one.

What would happen if we instead look at the real and imaginary parts of these functions? Then we are dealing with graphs that lie in $\mathbb{C} \times \mathbb{R}$, which is three dimensional. The resulting surfaces are much like those we study in a standard multivariable calculus class and can be analyzed by generating contour plots. However, these images are only "shadows" of graphs in four dimensions. We would expect to lose a lot of information. Yet, the images of these functions display some familiar patterns. When we generate contour plots for both the real and imaginary parts of the iterates of some standard complex functions, the filled Julia sets for the original functions start to appear in the center, as we will see soon in FIGURE 2. Even more surprising is the fact that, even though the contour plots look very similar, there is something different about the real and imaginary parts.

In this paper, we explore the connections between the graphs of the real and imaginary parts of various complex functions and their corresponding filled Julia sets. We will initially focus on results for the well-known family of complex quadratic polynomials of the form $q_c(z) = z^2 + c$, where $c \in \mathbb{C}$, and end with a more general class of complex rational maps.

Math. Mag. **88** (2015) 91–102. doi:10.4169/math.mag.88.2.91. © Mathematical Association of America
MSC: Primary 37F10, Secondary 30D05.

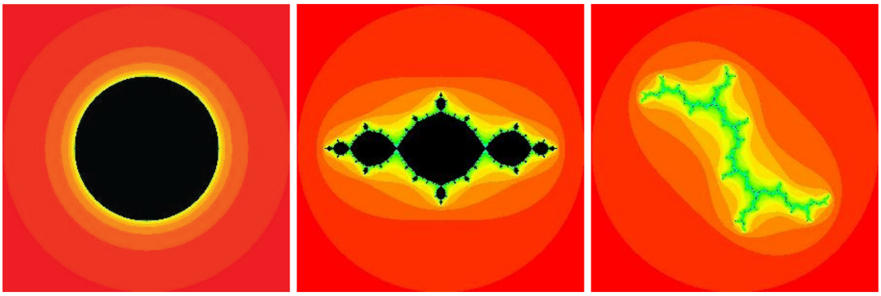


Figure 1 The filled Julia sets for $q_0(z) = z^2$, $q_{-1}(z) = z^2 - 1$, and $q_i(z) = z^2 + i$

Basic Definitions

In this section, we provide a brief review of some basic complex dynamics definitions. More background information is in Devaney's books [**5**], [**6**].

Let $f : \mathbb{C} \to \mathbb{C}$ be a function. To *iterate* f is to apply f repeatedly to an input; each result is called an *iterate*. For example, the first iterate of a complex number z_0 is $f(z_0)$, and the second iterate is $f(f(z_0))$, which we write as $f^2(z_0)$. In general, we denote the kth iterate as

$$f^k(z_0) = \underbrace{(f \circ f \circ \cdots \circ f)}_{k \text{ times}}(z_0)$$

for any natural number k. The sequence $\{z_0, f(z_0), f^2(z_0), f^3(z_0), \ldots, f^n(z_0), \ldots\}$ is called the *orbit* of z_0 under the function f. We define

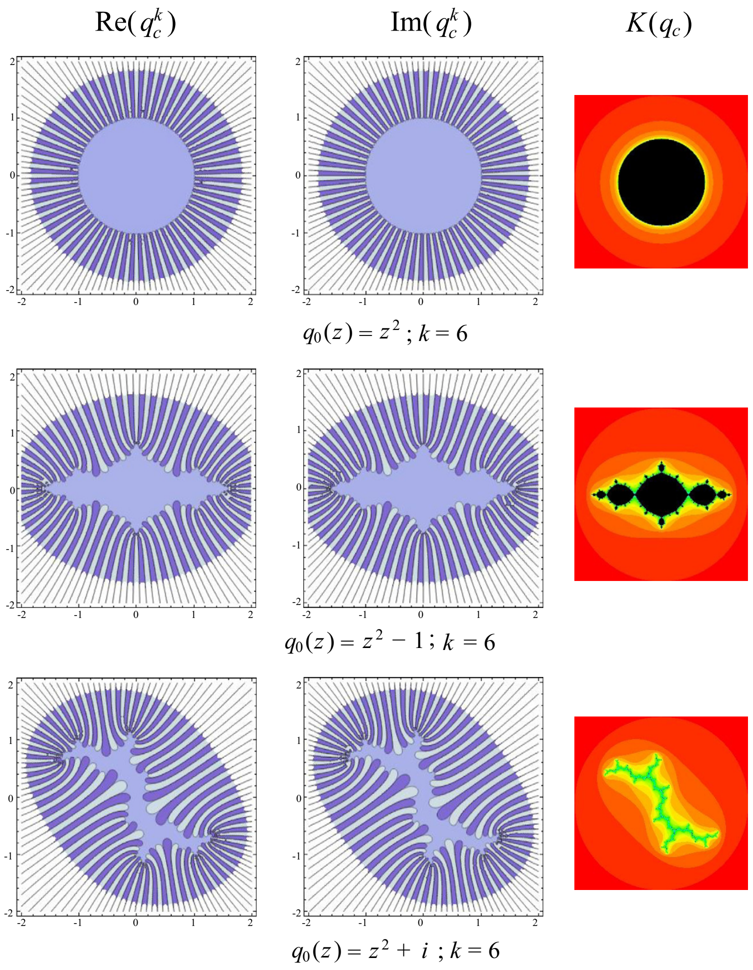
$$K(f) = \{z : \{f^k(z)\}_{k=0}^{\infty} \text{ is bounded}\}.$$

That is, $K(f)$ is the collection of points $z \in \mathbb{C}$ whose orbits under iteration by f are bounded. In the case of polynomials, $K(f)$ is called the *filled Julia set*. Also, for the classes of functions described in this paper, the boundary of $K(f)$ is defined to be the *Julia set*.

The filled Julia set, $K(q_0)$, for $q_0(z) = z^2$ can be easily computed. Consider z in polar form, so $z = re^{i\theta}$ with $r = |z|$, and θ being the angle between the positive x-axis and the ray from 0 to z. When we evaluate $q_0(z)$, we see that $q_0(z) = z^2 = (re^{i\theta})^2 = r^2e^{i2\theta}$. If we continue in this fashion, we find that $q_0^k(z) = r^{2^k}e^{i2^k\theta}$ and $|q_0^k(z)| = |r^{2^k}||e^{i2^k\theta}| = r^{2^k}$. If $r < 1$, then the iterates of z converge to 0. For $r > 1$, the iterates of z approach infinity. When $r = 1$, the iterates of z remain on the unit circle. Therefore, $\{q_0^k(z) : k \text{ is a natural number}\}$ is bounded if and only if $r \leq 1$, which can also be written as $|z| \leq 1$. Hence, the filled Julia set, $K(q_0)$, is the closed unit disk. It follows that the Julia set is simply the unit circle.

For most functions, it is not possible to determine the filled Julia set by hand, but it is not difficult to have a computer generate approximate images. See FIGURE 1 for filled Julia sets for $q_0(z) = z^2$, $q_{-1}(z) = z^2 - 1$, and $q_i(z) = z^2 + i$. The filled Julia sets, $K(q_c)$, are the black regions. These images show the basic three types of filled Julia sets for functions of the form q_c: one has a single piece, one has an infinite number of smaller and smaller distinct pieces, and the third has no area. Just from this small sample, we see that filled Julia sets can be extremely intricate.

A complex function $f : \mathbb{C} \to \mathbb{C}$ can be written as $f(z) = u(z) + iv(z)$, where $u(z) = \text{Re}(f(z))$, the *real part* of f, and $v(z) = \text{Im}(f(z))$, the *imaginary part* of f. For example, if $q_{-1}(z) = z^2 - 1$ where $z = x + iy$, then $q_{-1}(x + iy) = (x^2 - y^2 - 1) + i(2xy)$. Then, $u(x, y) = \text{Re}(q_{-1}(z)) = x^2 - y^2 - 1$ and $v(x, y) = \text{Im}(q_{-1}(z))$



$q_0(z) = z^2$; $k = 6$

$q_0(z) = z^2 - 1$; $k = 6$

$q_0(z) = z^2 + i$; $k = 6$

Figure 2 *Mathematica* images of contour plots for $\mathrm{Re}(q_c^k)$, $\mathrm{Im}(q_c^k)$; *FracTool* images of filled Julia sets for the corresponding functions

$= 2xy$. The second iterate is $q_{-1}^2(z) = (z^2 - 1)^2 - 1 = z^4 - 2z^2$. Its real and imaginary parts are $\mathrm{Re}(q_{-1}^2(z)) = x^4 - 6x^2y^2 + y^4 - 2x^2 + 2y^2$ and $\mathrm{Im}(q_{-1}^2(z)) = 4x^3y - 4xy^3 - 4xy$, respectively.

In FIGURE 2, we use contour diagrams to visualize what happens with the graphs of some of the iterates of the functions in FIGURE 1. The contour plots show the contour lines for function values of -2 and 2. Note that because some values of these functions vary drastically in magnitude between nearby points in the domain, the contour lines for -2 and 2 are so close to each other that they almost appear on top of each other in these plots. Obviously, contour lines cannot cross, but they can be so close to each other that we cannot distinguish between them. The alternating very dark to very light shading as we look around the edges of the images indicates that the functions are oscillating between heights well above 2 and well below -2. The center portion of these contour plots is shaded with a color that is between the very dark and very light we see around the edges; it represents places where the values of the function remain between -2 and 2. In FIGURE 2, we include images of the filled Julia sets of the original functions next to these contour diagrams. Notice that the center regions, where $|q_c^k(z)| \leq 2$, resemble the corresponding filled Julia sets in shape, even after this small number of iterations. But, how are they related mathematically? To analyze this more precisely, we define two new sets that correspond to points where the iterates of the function are bounded in the real and imaginary directions.

Definition 1. *For any complex function $f : \mathbb{C} \to \mathbb{C}$, we define the sets for which the real or imaginary parts of the iterates are bounded. Let*

$$U(f) = \{z : \{\mathrm{Re}(f^k(z))\}_{k=0}^{\infty} \textit{ is bounded}\}$$

and

$$V(f) = \{z : \{\mathrm{Im}(f^k(z))\}_{k=0}^{\infty} \textit{ is bounded}\}.$$

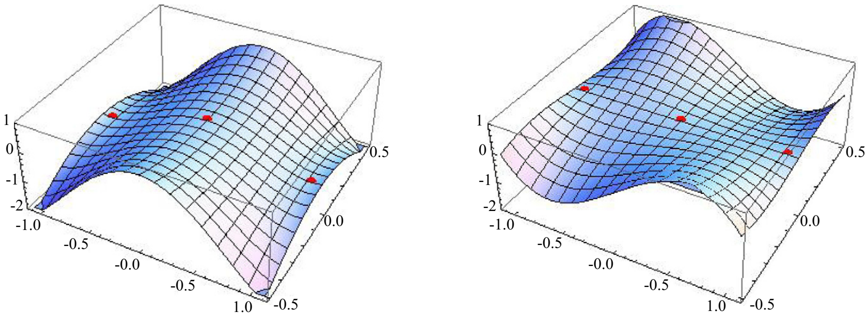
Note that we are not iterating $\mathrm{Re}(f)$ and $\mathrm{Im}(f)$. Instead, we are looking at the real and imaginary parts of the iterates of f. As we will see soon, $U(f)$ and $V(f)$ are related to $K(f)$ by $K(f) = U(f) \cap V(f)$.

Critical Points

The term *critical point* is used somewhat differently in single-variable calculus and multivariable calculus, which, at first glance, could result in confusion for complex functions. We can view a function $f : \mathbb{C} \to \mathbb{C}$ either as a function of one complex variable or as two functions of two real variables, but we will see that the two different perspectives produce the same critical points, as we describe now.

The "one-dimensional" viewpoint is that the critical points of $f(z)$ are the solutions to the equation $f'(z) = 0$. For q_{-1} as described earlier in the Basic Definitions portion of this paper, $q'_{-1}(z) = 2z$, and therefore, the only critical point is the complex number $0 = 0 + 0i$ (which we identify with $(0, 0)$). However, in thinking of $q_{-1}(z)$ as $(u(x, y), v(x, y))$, the critical points in multivariable calculus are the simultaneous solutions to $u_x = 0$, $u_y = 0$, $v_x = 0$, and $v_y = 0$. Again, since $u_x = 2x$, $u_y = -2y$, $v_x = 2y$, and $v_y = 2x$, the unique critical point of $(u(x, y), v(x, y))$ is $(0, 0)$. It is no accident that the critical points from both points of view coincide; both concepts of critical point capture the notion that a small change in z (in any given direction) results in a much smaller change in $f(z)$.

The critical points of q_{-1}^2 (in both senses) are 0, 1, and -1 (identified with $(0, 0)$, $(1, 0)$, and $(-1, 0)$, respectively). In FIGURE 3, we display the graphs of $\mathrm{Re}(q_{-1}^2)$ and $\mathrm{Im}(q_{-1}^2)$, with the positions of the critical points of q_{-1}^2 marked. Notice that the surfaces appear to have saddle points at the critical points; we will show that this is also not a



Re (q_{-1})

Im (q_{-1})

Figure 3 The real and imaginary parts of $q_{-1}^2(z) = z^2 - 1$ with critical points marked

coincidence. We state this theorem for the family $q_c(z)$, although it is true for any nonconstant, complex analytic function.

Theorem 2. *Let $q_c : \mathbb{C} \to \mathbb{C}$ be the complex analytic function $q_c(z) = z^2 + c$ that can also be written in the form $q_c(z) = u(z) + iv(z)$ for some real valued functions $u(z)$ and $v(z)$. Then the following are true.*

a) *p is a solution of $q_c'(z) = 0$ if and only if p is a solution to all four equations*

$$u_x = 0 \quad u_y = 0$$
$$v_x = 0 \quad v_y = 0.$$

Hence, the phrase "critical point" used above is unambiguous.

b) *The discriminants $D_u = u_{xx}u_{yy} - (u_{xy})^2$ and $D_v = v_{xx}v_{yy} - (v_{xy})^2$ are equal.*

c) *For all x and y, $D_u \leq 0$ and $D_v \leq 0$.*

d) *Every critical point of q_c must be a saddle point for both u and v.*

Proof. Let $q_c = u + iv$ as described in the theorem. Since q_c is analytic, the Cauchy–Riemann equations hold (see, for example, [**4**, Chapter 2]). That is, $q_c'(z) = u_x(z) + iv_x(z) = v_y(z) - iu_y(z)$. Hence, $q_c'(z) = 0$ if and only if all of the first partial derivatives of u and v at z are zero. This proves part (a) of the theorem.

The Cauchy–Riemann equations also tell us that

$$u_x = v_y \quad u_y = -v_x.$$

Since q_c is analytic, all partial derivatives of u and v exist and are continuous (see [**4**, Chapter 2]). Taking the partial derivatives of both equations with respect to x and y results in

$$\begin{aligned} u_{xx} &= v_{yx} \quad u_{yx} = -v_{xx} \\ u_{xy} &= v_{yy} \quad u_{yy} = -v_{xy}. \end{aligned} \tag{1}$$

By Clairaut's theorem [**10**, Chapter 14], we have that $u_{xy} = u_{yx}$ and $v_{xy} = v_{yx}$. It follows that

$$D_u = -v_{xy}^2 - u_{xy}^2 \leq 0$$

and

$$D_v = -u_{xy}^2 - v_{xy}^2 = D_u.$$

We therefore conclude that, for all x and y, D_u and D_v are either equal and negative or zero. This proves parts (b) and (c).

Since q_c is complex analytic, the functions u and v are infinitely differentiable and indeed harmonic, that is, $u_{xx} + u_{yy} = 0$ and $v_{xx} + v_{yy} = 0$. As such, u and v satisfy a maximum modulus property: if u (respectively v) has a maximum value on an open disk Ω, then u (respectively v) is constant on Ω. Since q_c is nonconstant, u and v cannot be constant on any disk. Hence, any critical point of u or v cannot be the location of a local extremum and is therefore a saddle point, proving part (d). ■

Theorem 2 gives interesting information about the real and imaginary parts of analytic functions—for example, any graph for a nonconstant analytic function cannot have any maximum or minimum values. Therefore, the surface would be both unbounded above and unbounded below on the complex plane. Also, since all critical points are saddle points, the surface consists of "waves" between the critical points. When we iterate the original function, the degrees of the iterates increase and we pick up more saddle points; this increases the number of undulations on the graphs.

Relationship Between $U(q_c)$, $V(q_c)$ and $K(q_c)$

By looking at the images in FIGURE 2, it appears that $\mathrm{Re}(q_c^k)$, $\mathrm{Im}(q_c^k)$, and $K(q_c)$ are closely related, and consequently, $U(q_c)$, $V(q_c)$, and $K(q_c)$ should be related. It is especially striking that the contour plots appear to be approximating the filled Julia set in the center. Therefore, it is not surprising that $K(q_c)$ is always contained in both $U(q_c)$ and $V(q_c)$, as seen in the next theorem. Furthermore, the proof of Theorem 3 does not use anything unique to the family $q_c(z)$. Therefore, the result is actually true for any complex function.

Theorem 3. (see [1, Theorem 9]) *For the family of functions $q_c(z) = z^2 + c$, $K(q_c) = U(q_c) \cap V(q_c)$.*

Proof. By the triangle inequality,

$$|q_c^k(z)| \le |\mathrm{Re}(q_c^k(z))| + |\mathrm{Im}(q_c^k(z))| \le 2|q_c^k(z)|$$

so $(q_c^k(z))_{k=1}^{\infty}$ is bounded if and only if both $(\mathrm{Re}(q_c^k(z)))_{k=1}^{\infty}$ and $(\mathrm{Im}(q_c^k(z)))_{k=1}^{\infty}$ are bounded. ■

The next natural question is whether either $U(q_c)$ or $V(q_c)$ is equal to $K(q_c)$. For this family of functions, $q_c(z)$, it can be shown that $U(q_c) = K(q_c)$.

Theorem 4. *Let $q_c(z) = z^2 + c$. For any $c \in \mathbb{C}$, $U(q_c) = K(q_c)$.*

Proof. From Theorem 3, we know that $K(q_c) = U(q_c) \cap V(q_c)$. Here, we show that $U(q_c) \subset K(q_c)$, which implies that $K(q_c) = U(q_c)$.

Suppose z is in $U(q_c)$ but not in $K(q_c)$. Then, there exists an $M > |\mathrm{Re}(c)|$ such that $|\mathrm{Re}(q_c^n(z))| < M$ for all natural numbers n. That is, if $S = \{z : |\mathrm{Re}(z)| < M\}$, then $q_c^n(z) \in S$ for all natural numbers n. Since z is not in $K(q_c)$ and $\mathrm{Re}(q_c^n(z))$ is bounded, it follows that $\mathrm{Im}(q_c^n(z))$ is unbounded by Theorem 3. Therefore, there is a k such that $|\mathrm{Im}(q_c^k(z))| > \sqrt{M^2 + M + \mathrm{Re}(c)}$. The image of the line segment L from $-M + i\sqrt{M^2 + M + \mathrm{Re}(c)}$ to $M + i\sqrt{M^2 + M + \mathrm{Re}(c)}$ is a segment of a parabola opening to the right. Therefore, any points z with $|\mathrm{Im}(z)| > \sqrt{M^2 + M + \mathrm{Re}(c)}$ will be sent to the left of the image of the endpoints of L. That is,

$$\begin{aligned}
\mathrm{Re}(q_c^{k+1}(z)) &= \mathrm{Re}(q_c(q_c^k(z))) \\
&< \mathrm{Re}(q_c(M + i\sqrt{M^2 + M + \mathrm{Re}(c)})) \\
&= \mathrm{Re}(M^2 + i2M\sqrt{M^2 + M + \mathrm{Re}(c)} \\
&\quad -(M^2 + M + \mathrm{Re}(c)) + \mathrm{Re}(c) + i\,\mathrm{Im}(c)) \\
&= M^2 - M^2 - M - \mathrm{Re}(c) + \mathrm{Re}(c) \\
&= -M.
\end{aligned}$$

Therefore, $q_c^{k+1}(z) \not\in S$, which is a contradiction. Hence, $U(q_c) \subset K(q_c)$, which implies that $U(q_c) = K(q_c)$. ■

Since $U(q_c) = K(q_c)$ and the contour lines for $\mathrm{Re}(q_c)$ look very much like the contour lines for $\mathrm{Im}(q_c)$, it is natural to suspect that $V(q_c) = K(q_c)$. However, this is not the case. Consider $q_0(z) = z^2$, and let $z = 2$. Then $q_0(2)$ is real, and furthermore, $q_0^k(2) = 2^{2^k}$ is real for all values of k. Thus, the imaginary part of $q_0^k(2)$ is 0 for all k, so $2 \in V(q_0)$. In addition, $\lim_{k\to\infty} q_0^k(2) = \infty$, so $2 \not\in K(q_0)$. Thus, $V(q_0) \neq K(q_0)$. Then $K(q_0)$ is a proper subset of $V(q_0)$. Furthermore, suppose that z lies along a ray beginning at the origin with an angle of $m\pi/(2^N)$ for natural numbers N, m. Then, $q_0^k(z)$ is real for all $k \geq N$. Therefore, $\{\text{Im}(q_0^j(z))\}_{j=0}^{\infty}$ is bounded, and all these rays are contained in $V(q_0)$. Thus, $V(q_0)$ not only contains points that are not in $K(q_0)$, but $V(q_0)$ is also dense in the complex plane. Later on, we will see that actually $V(q_c) \neq K(q_c)$ for all $c \in \mathbb{C}$, even though $U(q_c) = K(q_c)$.

We can summarize this result in Theorem 5. Note that this is a special case of Theorem 11 found in [**1**] concerning complex polynomials, although that proof uses more difficult techniques than the above discussion.

Theorem 5. *Let $q_c(z) = z^2 + c$ where $c \in \mathbb{C}$. Then*

a) *$U(q_c) = K(q_c)$, and*

b) *$V(q_c) \neq K(q_c)$.*

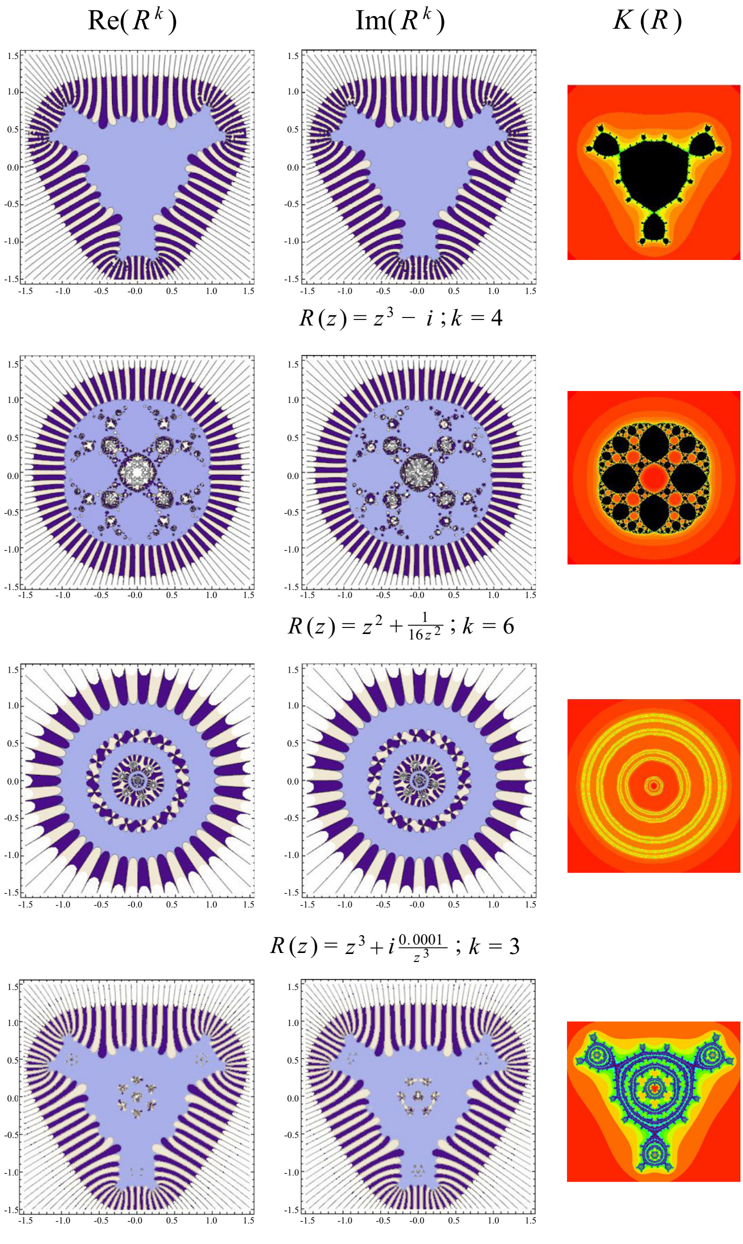
Why is $V(q_c)$ larger than $U(q_c)$ when the contour lines for $\text{Re}(q_c)$ and $\text{Im}(q_c)$ are so similar? Consider the function $q_0(z) = z^2$ where it is easy to compute iterates by hand. The difference between $V(q_0)$ and $U(q_0)$ lies in the rays mentioned above that are all eventually mapped onto the real axis under iteration by z^2. Once those rays land on the real axis, they remain there under iteration because the real line is *closed under iteration* by $q_0(z)$. That is $q_0(\mathbb{R}) \subseteq \mathbb{R}$. Therefore, the imaginary parts of the iterates of any points on those rays will eventually be 0, causing the rays to all be in $V(q_0)$. For the same thing to occur with $U(q_0)$, we would have to have rays that land on the imaginary axis under iteration and stay there. However, squaring any complex number on the imaginary axis sends it to the real axis, where it remains real under iteration. Therefore, the imaginary axis is not closed under iteration by $q_0(z)$ and the behavior is different. The reason this is not visible on the contour diagrams is because a single contour plot shows only a particular iteration and does not indicate where any ray is located under the next iteration.

Extending to Graphs of Rational Maps

The results stated in Theorem 5 actually extend beyond complex quadratic functions and beyond the polynomial case in [**1**]. Consider the family of rational functions $R(z) = z^n + P(z)/Q(z)$, where $P(z)$ and $Q(z)$ are polynomials and $n \geq 2$. Some examples are displayed in FIGURE 4. Like before, the contour lines for function values of -2 and 2 are shown. Also, we define $K(R)$ as before as the set of points whose iterates under R are bounded. In the case of polynomials, this is the same definition of the filled Julia set described at the beginning of this paper. The Julia set is then the boundary of $K(R)$.

Each of the functions depicted in FIGURE 4 is either of the form $z^n + c$ where n is an integer and c is a complex number or it is the result of perturbing a polynomial function of this form by placing a pole at the critical point, $z = 0$. A *pole* is simply a place where we divide by zero causing a singularity, much like when we have a vertical asymptote in the one-variable case. When a pole is present, there are more critical points. Since the orbits of the critical points determine both the dynamics of the function and the structure of $K(R)$, having more critical points leads to more intricate graphs.

In FIGURE 4, notice that the images for $z^3 - i$ are very similar to what we saw for the family q_c depicted in FIGURE 2. The filled Julia set is the solid black region, and the contour diagrams have a center that looks like the filled Julia set with curved rays that extend away from the center and shading that alternates between very dark and very light around the edges. This is what we expect to see for polynomial functions, even when the degree is greater than two.



$R(z) = z^3 - i\,; k = 4$

$R(z) = z^2 + \frac{1}{16z^2}\,; k = 6$

$R(z) = z^3 + i\frac{0.0001}{z^3}\,; k = 3$

$R(z) = z^3 - i - \frac{0.0001}{z^3}\,; k = 4$

Figure 4 *Mathematica* images of contour plots for Re(R^k), Im(R^k), and $K(z^3 - i - \frac{0.0001}{z^3})$; *FracTool* images of $K(R)$ for the other three functions. Note that $K(z^3 + i\frac{0.0001}{z^3})$ and $K(z^3 - i - \frac{0.0001}{z^3})$ are actually the Julia sets.

The rest of the images of $K(R)$ found in FIGURE 4 are a bit more intricate and described in more detail below. These functions are all of the form

$$z^n + \frac{\lambda}{z^n} + c$$

where the value of λ is chosen to be very small so that the perturbation is concentrated at $z = 0$. Therefore, far from zero, the functions $z^n + \lambda/z^n$ in FIGURE 4 behave like z^n (z^2 in the second example and z^3 in the rest). The last example has both a small perturbation and a nonzero c value. In all of these, $K(f)$ still seems to appear in the center of the contour diagrams of $\mathrm{Re}(f^n)$ and $\mathrm{Im}(f^n)$. This time, however, there is even more structure emerging in the contour lines.

The Julia set for $z^2 + \frac{1}{16z^2}$ in FIGURE 4 is known as a checkerboard Julia set [**2**]. The unbounded outside region is often referred to as the domain of infinity. On the boundary of that domain, the function behaves exactly like z^2. The point $z = 0$ maps to infinity, and the large disk centered at $z = 0$ maps to the domain of infinity. All of the other disks that are not black eventually map to the disk centered at $z = 0$ (this is why the central disk is sometimes called the "trap door") and then to the domain of infinity. The orbits of all of the black points are bounded and make up the set $K(z^2 + \frac{1}{16z^2})$ described earlier. The Julia set is the union of the boundaries of all of the regions that are black and the regions that are not black, together with an uncountable "dusting" of what we call buried points—points that are in the Julia set but which are not on the boundary of any particular complementary component of the Julia set. Every region that is not black touches only black regions at a single point, and every black region touches only regions that are not black at a single point.

The Julia set for $z^3 + i\frac{0.0001}{z^3}$ in FIGURE 4 is a collection of closed curves whose union is equal to our set $K(z^3 + i\frac{0.0001}{z^3})$. This type of Julia set can occur in families of functions of the form $z^n + \lambda/z^n$ when n is an integer larger than two [**9**]. If λ is chosen small enough so that each of the new critical points maps inside the trap door after exactly one iterate, the Julia set will have this structure. To describe how intricate the set $K(z^3 + i\frac{0.0001}{z^3})$ is, imagine constructing circles by the following process. Begin with the unit interval and remove the open middle third. Then, remove the open middle thirds of the two remaining intervals. The scatter of points that remains after repeating the process of removing the open middle third of each remaining interval produces the *Cantor middle thirds set*. Finally, connect every point on the right-hand side with its mirror image on the left-hand side with a circle centered at $1/2$. This set of uncountably many concentric circles is known as a *Cantor set of circles*. The Julia set pictured in FIGURE 4 is not the result of exactly a middle thirds removal from an interval and rotated around $1/2$, although the idea is similar. In addition, the curves that make up the set are not true circles, but instead are infinitely wiggly circles called *quasicircles*. For the purposes of this paper, you can think of these curves as approximately circles. Except for these two differences, the structure of the Julia set pictured is identical to the description above.

The bottom Julia set in FIGURE 4 is known as the perturbed rat [**3**], i.e., a perturbation of the Julia set for $z^3 - i$; compare the right bottom image in FIGURE 4 to the right top image. The type of Julia set found on the bottom of the table results from functions of the form

$$z^n + c + \frac{\lambda}{z^n}$$

where n is an integer larger than two, c is chosen so that 0 is a point of period k for $p(z) = z^n + c$ (in other words, $p^k(0) = 0$), and λ is small enough so that the kth iterate of each of the new critical points is inside the trap door. This Julia set, which is equal to $K(p)$, is made up of *Cantor sets of decorated circles*. If you focus on the center region and imagine slicing off all of the decorations, what you would end up with is a single Cantor set of circles.

Relationship Between $U(R)$, $V(R)$, and $K(R)$ for Rational Maps

If we compare the contours of the real and imaginary parts of the iterates of the new functions from the Rational Maps section with their Julia sets, we see a similar kind of relationship between the corresponding sets $U(R)$ and $V(R)$ and the set $K(R)$ that we saw for the family q_c earlier in this paper.

The theorem below is for rational functions that, near infinity, behave like a polynomial of degree at least two. The proof that appears in [**1**] need not be modified since it relies on a change of coordinates valid on the connected component of $\mathbb{C} \setminus K$ containing infinity for the maps under consideration. We only sketch the proof here because the details, as seen in [**1**], are beyond the scope of this paper.

Theorem 6. *Let $R(z) = z^n + P(z)/Q(z)$ where $n \geq 2$, $P(z)$, and $Q(z)$ are polynomials, and the degree of $P(z)$ is less than that of $Q(z)$. Then*

a) *$U(R) = K(R)$ if n is even,*
b) *$U(R) \neq K(R)$ if n is odd, and*
c) *$V(R) \neq K(R)$.*

Sketch of proof. As mentioned in the descriptions of the Julia sets found in FIGURE 4, the rational function $R(z)$ behaves similarly to the function $z \mapsto z^n$ for large values of z. It is easy to verify that the claims stated in this theorem are true for $z \mapsto z^n$. Let's revisit what occurs in this case.

a) Let n be even. Can $U(z^n) \neq K(z^n)$? In light of Theorem 3, $K(z^n) \subseteq U(z^n)$ for the same reason that $K(q_c) \subseteq U(q_c)$. Suppose by way of contradiction that there is some $z_0 \in U(z^n) \setminus K(z^n)$. It is easy to show that $K(z^n)$ is the unit disk. Therefore, $|z_0| > 1$, and $\lim_{k\to\infty} |(z_0^n)^k| = \infty$. Therefore, the orbit of z_0 under $z \mapsto z^n$ spirals out away from the origin. However, since $z_0 \in U(z^n)$, there must be a bound $M > 0$ such that $|\operatorname{Re}(z_0^n)^k| \leq M$ for all $k > 0$. The only way the orbit of z_0 can remain in $\{z : -M \leq \operatorname{Re}(z) \leq M\}$ is if some iterate $(z_0^n)^k$ of z_0 lands on the imaginary axis. Then, since n is even, $(z_0^n)^{k+1}$ is real, and the rest of the orbit is unbounded on the real axis. This contradicts $z_0 \in U(z^n)$.
b) Let n be odd. Then the orbit of any purely imaginary number under z^n is purely imaginary and, therefore, in $U(z^n)$. Also, for any purely imaginary number z_0 with $|z_0| > 1$, $\lim_{k\to\infty} |(z_0^n)^k| = \infty$. Therefore, $z_0 \notin K(z^n)$. Hence, $U(z^n) \neq K(z^n)$.
c) Since all iterates of a real number are real, all real numbers belong to $V(z^n)$. Also, for any real number z_0 with $|z_0| > 1$, $\lim_{k\to\infty} |(z_0^n)^k| = \infty$. Therefore, $z_0 \notin K(z^n)$. Hence $V(z^n) \neq K(z^n)$. ■

What makes the proof work for functions other than $z \mapsto z^n$ is that, for sufficiently large z, $R(z)$ behaves like $z \mapsto z^n$; the precise formulation uses Böttcher's coordinates [**8**, Chapter 9]. Böttcher's coordinates provide a "straightened out" view of space and time for a filled Julia set. In FIGURE 5, we see two filled Julia sets from the $z \mapsto z^2 + c$ family resting upon a color-coded background as though surrounded by a patterned rubber tablecloth. As far as the topology of the situation goes, the two patterned regions are the same; however, the tablecloth rests straight on the table around the disk and must stretch and contort to fit the jagged contours of the rabbit (the common name for the filled Julia set on the right of FIGURE 5). Contortion is not necessary farther from the rabbit, where the tablecloth lays nearly the same as it does about the disk. This situation illustrates the content of the famous Riemann mapping theorem: the unbounded region surrounding a closed, bounded, connected set is conformally isomorphic to the exterior of the unit disk, and the isomorphism can be chosen to be asymptotic to the identity at infinity. Thus, Riemann maps provide a spatial straightening of the domain of infinity, an amazing feat!

Now we consider the temporal picture, i.e., how a point moves by a polynomial. The action of the polynomial for the picture on the left in FIGURE 5 is very "straight" in polar coordinates: square the distance from the origin, and double the angle from

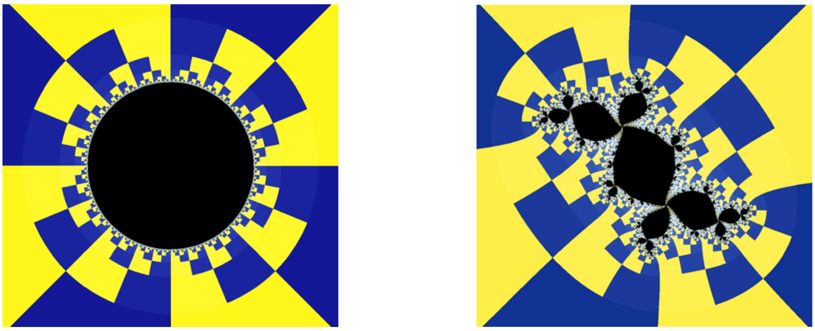


Figure 5 *FractalStream* representations of Böttcher's coordinates for $q_0(z) = z^2$ on the left and $q_{-0.123+0.745i}(z) = z^2 - 0.123 + 0.745i$ on the right. The image on the right is also known as the rabbit. Note that we usually draw a filled Julia set by iterating until a point escapes and color it by how many iterations that took. Here, we wait until a point escapes and then color it by whether it ended up in the upper half-plane or the lower half-plane at that point. This coloring indicates that for points far enough away from the origin, these two functions have similar behavior.

the real axis. For the polynomial chosen for the right picture, the action is necessarily more complicated due to the crinkly frontier of the domain of infinity. Farther from the filled Julia set, where the value of z^2 dwarfs the value of c, the map $z \mapsto z^2 + c$ behaves much more like $z \mapsto z^2$.

Thanks to this uniformization, many statements that are true about $z \mapsto z^2$ on its domain of infinity are true for other maps on their domains of infinity. In our theorem, Böttcher's coordinates establish that there exist continuous paths γ_1 and γ_2 in $\mathbb{C}$ that, under R, behave in much the same way that the real and imaginary axes behave under $z \mapsto z^n$. That is, we saw that q_c maps the real line into the real line; now we are saying that $R(z)$ maps γ_1 into γ_1. Further, one can prove that those paths, γ_1 and γ_2, stay within a bounded distance of the real and imaginary axes, respectively [**1**, Theorem 7]. Using those paths, we can make arguments about the boundedness of the real or imaginary parts similar to those made for $z \mapsto z^n$ above.

Therefore, if n is even, we have the same result that we had for q_c. When n is odd, the fact that the imaginary axis is closed under iteration by z^n changes the result a bit and causes $U(R) \neq K(R)$. Therefore, even though the filled Julia set for $z^3 - i$ in FIGURE 4 seems to resemble the filled Julia set for $z^2 - 1$ in FIGURE 2, $U(z^3 - i) \neq K(z^3 - i)$ while $U(z^2 - 1) = K(z^2 - 1)$. The difference comes from the existence of a curve γ that has bounded distance from the imaginary axis and is closed under iteration by $z^3 - i$, while no such curve exists for q_{-1}.

Conclusion

In this paper, we have seen that there really is a significant amount of information being conveyed in the real and imaginary parts of the iterates of some families of rational maps. For the well-known family $q_c(z) = z^2 + c$, the set $U(q_c)$ is actually equal to the filled Julia set for q_c; meanwhile, even though the contour plots for $V(q_c)$ look very much like the contour plots for $U(q_c)$, the set $K(q_c)$ is a proper subset of $V(q_c)$. When we extend to rational maps of the form $R(z) = z^n + P(z)/Q(z)$ where $n \geq 2$, we still see images of $K(R)$ inside both contour plots for $U(R)$ and for $V(R)$. A new surprise, though, is that when n is odd, $U(R)$ is not equal to $K(R)$. Otherwise, the behavior of $U(R)$, $V(R)$, and $K(R)$ is similar to what occurs with the much simpler case, q_c, even though the images are much more intricate.

Other questions present themselves: What can a collection of surface projections (perhaps even these surface projections) tell us visually about a complex function besides its Julia set? Is there another projection besides the real and imaginary parts that tell us something about the dynamics of these functions? What other functions have interesting properties when studied in this manner? Finally, are there any other images hidden in these surfaces? We already found a perturbed rat; who knows what else lurks out there!

Acknowledgments Some images in this paper were made with *FracTool,* available from http://jimrolf.com/java/fractTool/fractTool.html; others were made with *FractalStream,* available from http://www.math.cornell.edu/~noonan/fstream.html.

REFERENCES

1. J. Barnes, C. Curry, L. Schaubroeck, Real and imaginary parts of polynomial iterates, *New York J. Math.* **16** (2010) 749–761.
2. P. Blanchard, F. Cilinger, D. Cuzzocreo, R. Devaney, D. Look, E. Russell, Checkerboard Julia sets for rational maps, *Int. J. Bifur. Chaos* **23** No. 2 (2013) 13.
3. P. Blanchard, R. Devaney, A. Garijo, E. Russell, A generalized version of the McMullen domain, *Int. J. Bifur. Chaos* **18** (2008) 2309–2318.
4. R. V. Churchill, J. W. Brown, *Complex Variables and Applications*. Fifth edition. McGraw-Hill Press, New York, 1990.
5. R. Devaney, *A First Course in Chaotic Dynamical Systems*. Westview Press, Boulder, 1992.
6. R. Devaney, *An Introduction to Chaotic Dynamical Systems*. Second edition. Westview Press, Boulder, 2003.
7. S. Lang, *Complex Analysis*. Third edition. Spring-Verlag, New York, 1993.
8. J. Milnor, *Dynamics in One Complex Variable*. Third edition. Princeton Univ. Press, Princeton, 2006.
9. C. McMullen, *Automorphisms of Rational Maps*. Vol. 1, Holomorphic Functions and Moduli. Math. Sci. Res. Inst. Publ. 10. Springer, New York, 1988.
10. J. Stewart. *Calculus: Early Transcendentals*. Seventh edition. Brooks/Cole, Belmont, CA, 2012.

Summary. Functions from the complex plane to itself are difficult to visualize; we consider the real and imaginary projections. In this paper, we explore the connections between the graphs of the real and imaginary parts of various complex functions and their corresponding filled Julia sets. We begin by examining the family of complex quadratic functions. We then expand our results to a broader collection of rational maps, including functions whose Julia sets form a Cantor set of simple closed curves, checkerboards, and a perturbed rat.

JULIA A. BARNES (MR Author ID: 613418) received her Ph.D. in mathematics from the University of North Carolina at Chapel Hill in 1996 and is now a professor of mathematics at Western Carolina University. Her mathematical interests include complex dynamical systems, ergodic theory, organizing math treasure hunts, and developing hands-on teaching ideas. She is also an associate director for Project NExT and enjoys hiking in her spare time.

CLINTON P. CURRY (MR Author ID: 845521) received his Ph.D from the University of Alabama at Birmingham in 2009, specializing in the fields of complex dynamical systems and topology. After teaching a few years, he left the academic fold to pursue his interest in computer programming at Google. His other interests include playing guitar and vintage calculators.

ELIZABETH D. RUSSELL (MR Author ID: 854956) received her Ph.D. in mathematics from Boston University in 2009 where she specialized in complex dynamics, chaos, and fractals. Since then, she has held positions at the United States Military Academy, Western New England University, and with the United States government. In her spare time, she enjoys competitive and social ballroom dance.

LISBETH E. SCHAUBROECK (MR Author ID: 663310) earned her Ph.D. at the University of North Carolina at Chapel Hill in 1998 and is now a professor of mathematical sciences at the United States Air Force Academy in Colorado Springs. Her professional interests include complex variables, undergraduate knot theory, and mentoring new faculty members. She and her husband enjoy bowling and are learning archery along with their two sons.

Many More Names of (7, 3, 1)

EZRA BROWN
Virginia Polytechnic Institute and State University
Blacksburg, VA 24061-0123
ezbrown@math.vt.edu

Combinatorial designs are collections of subsets of a finite set that satisfy specified conditions, usually involving regularity or symmetry. As the scope of the 984-page *Handbook of Combinatorial Designs* [**7**] suggests, this field of study is vast and far reaching. Here is a picture of the very first design to appear in "Opening the Door," the first of the *Handbook*'s 109 chapters:

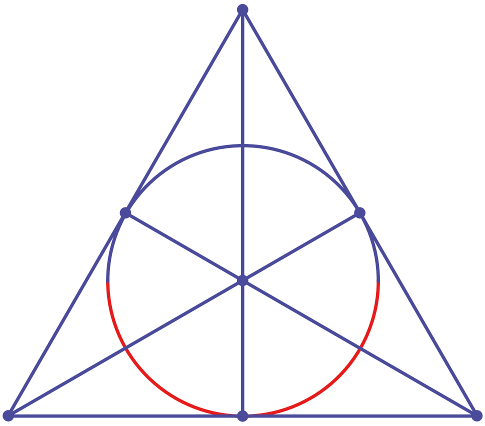


Figure 1 The design that opens the door

This design, which we call the (7, 3, 1) design, makes appearances in many areas of mathematics. It seems to turn up again and again in unexpected places. An earlier paper in this MAGAZINE [**4**] described (7, 3, 1)'s appearance in a number of different areas, including finite projective planes, as the Fano plane (FIGURE 1); graph theory, as the Heawood graph and the doubly regular round-robin tournament of order 7; topology, as an arrangement of six mutually adjacent hexagons on the torus; $(-1, 1)$ matrices, as a skew-Hadamard matrix of order 8; and algebraic number theory, as the splitting field of the polynomial $(x^2 - 2)(x^2 - 3)(x^2 - 5)$.

In this paper, we show how (7, 3, 1) makes appearances in three areas, namely (1) Hamming's error-correcting codes, (2) Singer designs and difference sets based on n-dimensional finite projective geometries, and (3) normed algebras.

We begin with an overview of block designs, including two descriptions of (7, 3, 1). We then describe certain binary error-correcting codes called Hamming codes, in which (7, 3, 1) makes three different appearances. Next, we expand the treatment of Hamming codes from binary codes to codes over all finite fields $\mathbb{F}_q$, where q is an odd prime. Then, we describe generalizations of the block design structure of (7, 3, 1) to

Math. Mag. **88** (2015) 103–120. doi:10.4169/math.mag.88.2.103. © Mathematical Association of America
MSC: Primary 05B05, Secondary 11R52; 17A35; 94B05.

the so-called Singer designs in the finite projective geometries $PG(n, q)$, as well as the Singer difference sets associated with these designs.

We continue with a fascinating connection between (7, 3, 1) and two number systems—the real algebras of dimensions 8 and 16, called the octonions and the sedenions, respectively. These superficially resemble the complex numbers, and mathematicians were led to these systems by asking questions about sums of squares. It turns out that (7, 3, 1) has two distinct connections with the octonions and makes 15 appearances within the sedenions.

But first, let's talk about block designs in general and (7, 3, 1) in particular.

Block designs

Let v, b, r, k, and λ be positive integers, with $v > k$. A *balanced incomplete block design* (or BIBD) with parameters v, b, r, k, and λ is an collection of b subsets (or *blocks*) of a v-element set V of elements such that each block contains k points, each element in V appears in exactly r blocks, and each pair of elements appears together in exactly λ blocks.

The parameters are not independent, for they satisfy the two equalities $bk = vr$ and $r(k - 1) = \lambda(v - 1)$; let's see why this is so. First, there are two ways to count the number of pairs $\{B, x\}$ such that the block B contains the element x. Each of the b blocks contains k elements, making bk pairs in all, and each of the v elements appears in r blocks, making vr pairs in all. It follows that

$$bk = vr.$$

Next, fix an element x. There are two ways to count the number of pairs $\{B, y\}$ such that x and y appear together in a block B. The element x is contained in r blocks, and each such block contains $k - 1$ other elements; also, the element x appears with another element y in λ blocks, and there are $v - 1$ elements $y \neq x$ in all. It follows that

$$r(k - 1) = \lambda(v - 1).$$

Thus, the parameters v, k and λ are enough to specify a block design and so we may speak of a (v, k, λ) design.

The two equalities are necessary for the existence of a BIBD with the given parameters. Clearly, there cannot be a (v, k, λ) design if r and b are not integers. But even if r and b are integers and the two equalities are satisfied, it happens that some combinations of parameters (v, k, λ) do not describe any designs. There are deep reasons that, for example, no designs with parameters (22, 7, 2) and (43, 7, 1) exist.

A BIBD is called *symmetric* if $v = b$, and so $r = k$; in this paper, *all of the designs we will consider are symmetric*. A (7, 3, 1) design consists of seven three-element subsets of $V = \{1, 2, 3, 4, 5, 6, 7\}$ such that each element is in three blocks and each pair of elements is together in a unique block. Since $v = b = 7$ and $r = k = 3$, this design is symmetric, and we can describe its blocks in two ways: (a) as $\mathcal{D}$, the seven translates mod 7 of the triple $D_1 = \{1, 2, 4\}$, and (b) as $\mathcal{H}$, the triples $\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}, \{2, 5, 7\}, \{3, 4, 7\}$, and $\{3, 5, 6\}$. FIGURE 2 shows both $\mathcal{D}$ and $\mathcal{H}$.

The block designs $\mathcal{D}$ and $\mathcal{H}$ are called *isomorphic* if there is a bijection of the set of points of $\mathcal{D}$ onto the set of points of $\mathcal{H}$ that induces a bijection of the blocks of $\mathcal{D}$ onto the blocks of $\mathcal{H}$. It happens that any two designs with parameters (7, 3, 1) are isomorphic, and so we speak of *the* (7, 3, 1) design.

And now, let's talk about error-correcting codes and their connections with (7, 3, 1).

D_1 :	{1, 2, 4}	H_1 :	{1, 2, 3}
D_2 :	{2, 3, 5}	H_2 :	{1, 4, 5}
D_3 :	{3, 4, 6}	H_3 :	{1, 6, 7}
D_4 :	{4, 5, 7}	H_4 :	{2, 4, 6}
D_5 :	{5, 6, 1}	H_5 :	{2, 5, 7}
D_6 :	{6, 7, 2}	H_6 :	{3, 4, 7}
D_7 :	{7, 1, 3}	H_7 :	{3, 5, 6}
(a)	The design $\mathcal{D}$	(b)	The design $\mathcal{H}$

Figure 2 (7, 3, 1) as (a) differences mod 7 and as (b) three-bit strings

Binary Hamming codes

Let's begin with two parties, Alice and Bob, who want to communicate with each other. Alice is sending a message to Bob. The message is expressed in some way as a sequence of strings of characters or *codewords*, which are sent to a receiver, one at a time. Errors can happen in the process, so the string Bob receives may fail to be a codeword. They can stop there, or they may try to correct the error. In every case we will consider, Alice will build some extra information into each codeword, and we will describe how this is done. Bob will use the extra information to test a string for an error and—if there is an error—to replace the bad string with the "closest" codeword (in the sense we'll describe). We are not concerned with the process by which the original message is translated into codewords or vice versa. For this paper, at least, we are only concerned with Alice sending one codeword at a time to Bob, possibly with some characters changed by error, and then with Bob trying to reconstruct the original codeword.

Mathematical schemes to deal with such errors first appeared in the 1940s in the work of several researchers, including Claude Shannon, Richard Hamming, and Marcel Golay. These researchers saw the need for something that would automatically detect and correct errors in signal transmissions across channels that were noisy and hence were likely to produce such errors. Their work led to a new branch of mathematics called *coding theory*—specifically, the study of error-detecting and error-correcting codes. They modeled these signals as sets of m-long strings called *blocks*, to be taken from a fixed alphabet of size q; a particular set $\mathcal{C}$ of such blocks, or *codewords*, is called a *q-ary code of length m*.

If q is a prime number, then $\mathcal{C}$ is called *linear* provided the codewords of $\mathcal{C}$ form a subspace of the m-dimensional vector space of $(\mathbb{Z}/q\mathbb{Z})^m$, the m-dimensional vector space over the field of integers mod q. A basis for such a linear code is called a *generating set* for the code. In this paper, *all of the codes we look at are linear codes.*

To *detect* errors means to determine that a codeword was incorrectly received; to *correct* errors means to determine the right codeword in case it *was* incorrectly received. Just how this correction happens will vary from code to code.

The fact that d errors in transmission change d characters in a block gives rise to the idea of distance between blocks. If v and w are n-blocks, then the *(Hamming) distance* $D(v, w)$ is the number of positions in which v and w differ. Thus, $D(11001, 10101) = 2$ and $D(1102002, 2011012) = 5$. If Alice sends the block v and Bob receives the block w, then $D(v, w)$ errors occurred while sending v. The *Hamming sphere of radius d* about an n-block w, denoted $S(w, d)$, is the set of all n-blocks whose Hamming distance from w is at most d. Finally, the *(Hamming) weight* of a codeword is the number of nonzero characters.

It follows that if the words in a code are all "far apart" in the Hamming distance sense, then we can detect errors. Even better, if we assume that only a few errors are received, then we can sometimes change the received block to the correct codeword. Let us now look at an example of an error-correction scheme.

A simple example of a binary code of length 3 consists of only two codewords, 000 and 111. If Bob receives 010, then it is most likely that Alice sent 000 and so the intended message was **0**; this is the *triplication* or *majority-vote* code. Effectively, a three-bit codeword consists of one "message bit" sent three times. More generally, a codeword of length n contains a certain number k of *message bits*, and the other $n-k$ *check bits* are used for error detection and correction. Such a code is called an (n, k) code: the triplication code is a (3, 1) code.

We have presented k as the number of message bits, but it can be defined more clearly as the dimension of the subspace consisting of the codewords. This makes sense only for linear codes—but in this paper, as previously mentioned, we are only concerned with linear codes.

The *minimum distance* of a code is the smallest distance between its codewords; this minimum distance determines the code's error detection and correction features. For example, a code with minimum distance five will detect up to four errors and correct up to two. You can show that a code with minimum distance d will detect up to $d-1$ errors and correct up to $\lfloor (d-1)/2 \rfloor$ errors. We see that if the Hamming spheres $S(w, d)$ of radius d about all codewords w are pairwise disjoint, then the code can correct up to d errors. Maximum efficiency in an (n, k) d-error correcting code $\mathcal{C}$ occurs when every string of length n is either a codeword or at a distance of at most d from a unique codeword—equivalently, when the Hamming spheres of radius d about all codewords partition the set of all n-blocks. This is a rare event, and a code with this property is called *perfect*. In this paper, *all of the codes we look at are perfect codes*.

Hamming's first error-correcting scheme was a perfect one-error correcting code of length seven with four message bits, three check bits, and minimum distance 3; hence, it could correct all errors in which a single bit was received incorrectly. Golay extended Hamming's work and constructed a family of $(2^n - 1, 2^n - 1 - n)$ linear binary perfect one-error correcting codes of minimum distance 3 for all $n \geq 2$. These are now known as the binary Hamming codes, and they include both Hamming's original (7, 4) code and the (3, 1) triplication code. The notation $H(m, k)$ refers to a linear binary perfect one-error correcting code of length m and dimension k.

$H(7, 4)$, Hamming's first code—the perfect single-error correcting code of length 7—was described in 1948 in [**17**, p. 418], as follows:

> Let a block of seven [binary] symbols be $X_1, X_2, \ldots, X_7$. Of these, X_3, X_5, X_6, and X_7 are the message symbols and chosen arbitrarily by the source. The other three are redundant and calculated as follows:
>
> $$X_4 \text{ is chosen to make } \alpha = X_4 + X_5 + X_6 + X_7 \text{ even}$$
> $$X_2 \text{ is chosen to make } \beta = X_2 + X_3 + X_6 + X_7 \text{ even}$$
> $$X_1 \text{ is chosen to make } \gamma = X_1 + X_3 + X_5 + X_7 \text{ even.}$$
>
> When a block of seven is received, α, β and γ are calculated and if even, called zero, if odd, called one. The binary number $\alpha\beta\gamma$ then gives the subscript of the X_i that is incorrect (if **0**, there was no error).

Now, this procedure determines α, β and γ mod 2 in the following way. Suppose exactly one of the seven bits, say X_j, is incorrect. Since $\alpha = X_4 + X_5 + X_6 + X_7$ adds up the X_i whose high bit equals 1, it follows that $\alpha = 1$ if and only if $j = 4, 5, 6$ or 7, that is, if the high bit of X_j is 1. Similarly, $\beta = X_2 + X_3 + X_6 + X_7$ adds up the X_j whose middle bit equals 1, so it follows that $\beta = 1$ if and only if $j = 2, 3, 6$ or 7, i.e., if the middle bit of X_j is 1. Finally, $\gamma = X_1 + X_3 + X_5 + X_7$ adds up the X_j whose low bit equals 1, and so $\gamma = 1$ if and only if $j = 1, 3, 5$ or 7, i.e., if the low bit of X_j is 1. Thus, X_j affects those, and only those, of α, β, and γ whose sum contains X_j.

Another way to describe the decoding procedure is that if $X = (X_1, \dots, X_7)$ is a seven-bit string, then compute $v = P \cdot X^t$, where

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

P is constructed in such a way that if the vector v is identical to the ith column of P, then X_i is the incorrect bit, and if $v = \mathbf{0}$, then there is no error.

The free choices for the four message symbols shows that there are 16 codewords, and the condition that $P \cdot v^t = \mathbf{0}$ (when v is a codeword) means that the vector v is in the (right) null space of the matrix P. Thus, the 16 codewords are closed under both addition and scalar multiplication by 0 and 1. In short, the codewords form a four-dimensional subspace of $(\mathbb{Z}/2\mathbb{Z})^7$ and we see that the above code is a linear code. More generally, if $\mathcal{C}$ is a linear code that is the null space of a matrix Q, then we call Q the *parity check matrix* for the code.

Hamming's scheme, then, takes every seven-long binary string with a single error and corrects that error, producing the corrected seven-bit codeword—whence the name "binary single error-correcting code of length 7." Since this code has length 7 and dimension 4, we call it the binary Hamming code $H(7, 4)$. The smallest binary Hamming code is $H(3, 1)$, the so-called triplication code: Each bit is sent three times, and the parity-check matrix is $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$.

(7, 3, 1) and the original Hamming code. The parity-check matrix P has another interesting feature. Write $P = [P_1, \dots, P_7]$—thus, P_i is the ith column of P—and consider the set C_i of columns of P whose dot products with P_i equal zero:

Do the C_i on the left in FIGURE 3 look familiar? They should. In fact, they are a rearrangement of the blocks $H_1, \dots, H_7$ in the right-hand column of FIGURE 2, and we have another way to produce the (7, 3, 1) design. This is also our first example of a *Singer design*, a topic we'll talk about in a later section.

i	P_i	binary C_i	decimal C_i
1	001	{010, 100, 110}	{2, 4, 6}
2	010	{001, 100, 101}	{1, 4, 5}
3	011	{011, 100, 111}	{3, 4, 7}
4	100	{001, 010, 011}	{1, 2, 3}
5	101	{010, 101, 111}	{2, 5, 7}
6	110	{001, 110, 111}	{1, 6, 7}
7	111	{011, 101, 110}	{3, 5, 6}

i	B_i	$\{j : B_{i,j} = 1\}$
1	1110000	{1, 2, 3}
2	1001100	{1, 4, 5}
3	1000011	{1, 6, 7}
4	0101010	{2, 4, 6}
5	0100101	{2, 5, 7}
6	0011001	{3, 4, 7}
7	0010110	{3, 5, 6}

Figure 3 The Singer (7, 3, 1) design (left) and the seven codewords of weight 3 (right)

(7, 3, 1), Hamming, and the three-circle Venn diagram. A second appearance of (7, 3, 1) in this code is in the table on the right side of FIGURE 3. This table comes from the seven codewords of weight 3. The blocks $B_i = B_{i,1} \dots B_{i,7}$ are the codewords, the points j are the integers $1, \dots, 7$, and $j \in B_i$ if and only if $B_{i,j} = 1$—another (7, 3, 1) design.

Finally, Hamming's system of three congruences (mod 2) has a nice pictorial interpretation, as follows. Draw the usual three-circle Venn diagram for three sets. Next, associate the region that is in all three sets with X_7, associate the regions that are in exactly two of the sets with X_3, X_5, and X_6, and associate the regions that are in exactly one of the sets with X_1, X_2, and X_4. We see that each region of the diagram is associated with exactly one of the X_i, and each X_i appears exactly once.

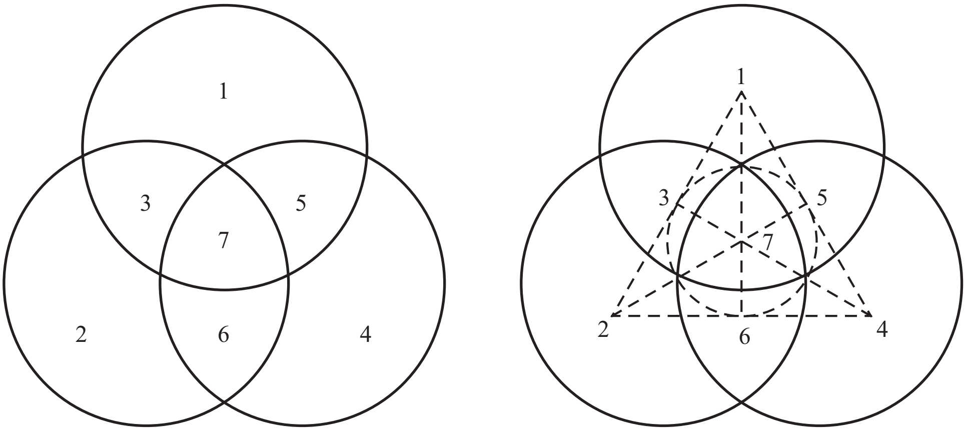


Figure 4 The three-circle Venn diagram (left) with another instance of (7, 3, 1) (right)

Hamming's scheme can be realized by placing X_i in its corresponding region, then the number of 1s in each of the circles must be even. Pictorially, if exactly one X_i is switched from x to $1 - x$, then it will be the value in the region contained in exactly those circles with an odd number of 1s. As a bonus, this picture also shows us one more appearance of (7, 3, 1) (on the right-hand side of FIGURE 4), and so the Hamming (7, 4) code gives us three different views of (7, 3, 1)!

The earliest Hamming codes were designed to correct errors in messages encoded as bit strings, and the underlying arithmetic was done in the two-element field. In the next section, we extend the results of this section to correct errors in messages where the arithmetic is performed in a finite field $\mathbb{F}_q$, where q is an odd prime.

q-ary Hamming codes

Let q be a prime. A *q-ary code of length m* is a collection of strings of length m over an alphabet of q elements. Since q is a prime, we may take these elements to be the finite field $\mathbb{F}_q = \{0, 1, \dots, q - 1\}$. As we have seen, if a code can correct up to d errors in messages of length n, then every string of length n is at a Hamming distance at most d from a codeword and so is contained within a sphere $S(w, d)$ of Hamming radius d about some codeword w.

We now show how to construct q-ary Hamming codes—that is, q-ary perfect one-error correcting codes—so we consider the Hamming spheres of radius 1. If w is a codeword of length n, then there are n positions where a single error can occur, and for each position, there are $(q-1)$ possible errors. Thus, for q-ary codes, the sphere $S(w, 1)$ contains the codeword w together with all $n(q-1)$ strings with exactly one error. It follows that if a q-ary code $\mathcal{C}$ corrects all single errors, then the spheres of radius 1 about every codeword in $\mathcal{C}$ are pairwise disjoint. Hence, the set of all q^n q-ary strings of length n contains the union of these spheres. If such a code $\mathcal{C}$ is perfect, then every such string belongs to one of these spheres. Hence, if $\mathcal{C}$ is perfect and contains W codewords, then we see that

$$W = \frac{q^n}{1+n(q-1)}.$$

The right-hand side is called the *Hamming* or *sphere-packing* bound, and a single-error correcting code is perfect exactly when the Hamming bound is attained.

For a Hamming code of length n, we see that $W(1+n(q-1)) = q^n$; since q is a prime, this means that $1+n(q-1)$ must be a power of q. Thus, $1+n(q-1) = q^k$ for some positive integer k; we solve this for n and see that $n = \frac{q^k-1}{q-1}$, and so the code contains q^{n-k} codewords. It follows that we may encode all q-ary messages of length $n-k$ in a way that corrects each error pattern involving a single incorrect character. In short, a codeword contains $n-k$ message digits and k so-called parity-check digits.

Thus, if a perfect q-ary Hamming code exists, then its length is necessarily equal to $n = \frac{q^k-1}{q-1}$ for some k. Now, we know that "necessary" does not mean "sufficient." But in fact, q-ary Hamming codes of length n having $n-k$ message digits do exist for all n and k, and we now show how to construct such $\left(\frac{q^k-1}{q-1}, \frac{q^k-1}{q-1} - k\right)$ codes. These are linear codes, as they are realized as $n-k$-dimensional subspaces of an n-dimensional vector space $\mathbb{F}_q^n$ over $\mathbb{F}_q$.

Let Q be a $k \times m$ matrix over $\mathbb{F}_q$ such that for fixed k, (1) no two columns of Q are linearly dependent, and (2) for the given k, m is as large as possible. Condition (1) states that no two columns of Q are multiples of each other. Now, each nonzero column vector v has $q-1$ nonzero scalar multiples, so (1) implies that we may choose at most one of these. We collect one vector from each set of $q-1$ nonzero multiples of a given vector until we cannot proceed further. Since there are q^k-1 nonzero vectors of length k and since these are partitioned into sets of $q-1$ nonzero multiples of a single vector, this means that we will have at least $(q^k-1)/(q-1)$ columns. But every nonzero vector is a multiple of exactly one of the vectors we have chosen, so the desired maximum number m of columns is equal to $(q^k-1)/(q-1)$. Sounds familiar, doesn't it? Indeed it is. The value of m we seek is precisely the number n from the preceding several paragraphs.

To encode a message string, we mimic what is done for the binary Hamming codes, with slight variations. Let q, n and k be as above, and let Q be a $k \times n$ matrix constructed as follows. Let the first k columns of the parity-check matrix be the identity matrix I_k of order k; these k positions will determine the parity digits. The other $n-k$ columns represent the message digits: Placed in increasing numerical order, they are the base-q representations of the non-powers of q between 1 and q^k-1 whose most significant digit is a 1. One can check that Q has the properties (1) and (2) mentioned in the previous paragraph.

For the Hamming q-ary code of dimension $n-k$, the parity-check matrix will have k rows and n columns. That is, a q-ary string of length n contains $n-k$ message digits and k parity digits. In all, the parity-check matrix has $(q^k-1)/(q-1)$ columns. Thus, a ternary Hamming code of length $(3^4-1)/(3-1) = 40$ will have four parity positions and 36 message positions. A base-5 Hamming code of length $(5^3-1)/(5-1) = 31$ has five parity positions and 26 message positions.

Let's illustrate this with the ternary Hamming code of length $13 = (3^3 - 1)/(3 - 1)$. The parity-check matrix T for this code is given by

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

To encode the message $(m_4, m_5, m_6, m_7, m_8, m_9, m_{10}, m_{11}, m_{12}, m_{13})$, determine the values of c_1, c_2 and c_3 so as to make the vector $(c_1, c_2, c_3, m_4, m_5, m_6, m_7, m_8, m_9, m_{10}, m_{11}, m_{12}, m_{13})$ an element of the right null space of T. That is, pick c_1, c_2 and c_3 to satisfy the congruences

$$c_1 + m_6 + m_7 + m_8 + m_9 + m_{10} + m_{11} + m_{12} + m_{13} \equiv 0 \pmod 3,$$

$$c_2 + m_4 + m_5 + m_8 + m_9 + m_{10} + 2m_{11} + 2m_{12} + 2m_{13} \equiv 0 \pmod 3, \text{ and}$$

$$c_3 + m_4 + 2m_5 + m_6 + 2m_7 + m_9 + 2m_{10} + m_{12} + 2m_{13} \equiv 0 \pmod 3.$$

For example, applying this procedure to the message $(1, 1, 2, 1, 0, 0, 1, 2, 1, 1)$ yields $c_1 = 1, c_2 = 2$, and $c_3 = 0$, and so the associated codeword is $(1, 2, 0, 1, 1, 2, 1, 0, 0, 1, 2, 1, 1)$.

More generally, let v^t denote the transpose of v. For a message $(x_{k+1}, \ldots, x_n)$ of length $n - k = \frac{q^k-1}{q-1} - k$, we determine k check digits $c_1, \ldots, c_k$ such that $T \cdot (c_1, \ldots, c_k, x_{k+1}, \ldots, x_n)^t$ is the zero vector of length n.

To decode a message v, calculate $w = T \cdot v^t$. If $w = \mathbf{0}$, then v is a codeword. If not, then for some nonzero integer a mod q and some positive integer j, $w = aT_j$. To correct the error, subtract a (mod q) from the jth component of P_j.

To see how this works, let's look at an example with the ternary Hamming code of length 13. Suppose we receive the string $z = (2, 2, 0, 0, 0, 1, 0, 0, 2, 1, 1, 2, 0)$. We compute $w = T \cdot z^t = (0, 2, 1)$ mod 3; this is nonzero, so there was an error in transmission. Assuming that there was an error in only one character, we see that $w = (0, 1, 2) \equiv 2T_5$ mod 3. In the above decoding scheme, this means that $a = 2$, so we subtract 2 (mod 3) from the fifth component of z. The result is the vector

$$v = (2, 2, 0, 0, 0-2, 1, 0, 0, 2, 1, 1, 2, 0) \equiv (2, 2, 0, 0, 1, 1, 0, 0, 2, 1, 1, 2, 0) \bmod 3.$$

Sure enough, $T \cdot v^t \equiv (0, 0, 0)$ mod 3—as claimed.

Finally, we need to show that the above code has minimum distance three. As in the binary case, ours is a linear code, so the minimum distance between codewords is equal to the minimum weight of a nonzero codeword. Let's prove this now.

Note that the parity-check matrix T of our Hamming q-ary code of dimension $n - k$ has k rows and n columns. By construction, the columns of T are nonzero and pairwise linearly independent. Thus, there are no codewords of weights 1 or 2, so the minimum weight of a nonzero codeword is at least 3. But columns T_{k-1}, T_k and T_{k+1} are linearly dependent because $T_{k-1} + T_k - T_{k+1} = \mathbf{0}$. Hence, the $n - k$-long vector v with $v_{k-1} = v_k = 1$ and $v_{k+1} = -1$ and zeros everywhere else is a codeword of weight 3—as claimed.

Now, you might wonder about the usefulness of q-ary codes for $q \geq 3$. Wonder no more: Ternary error-correcting codes have made their way into the world of card magic. Chapter Q (for Queen) of Colm Mulcahy's recent book [**8**]—a great read, by the way—includes a variety of card tricks that use the ternary (4, 2) Hamming code with parity-check matrix

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

Does this matrix T have a block-design connection, similar to that enjoyed by Hamming's parity-check matrix T? Indeed it does. If T_i the ith column of T and D_i is the set of columns of T whose dot products with D_i equal zero, here's what we get:

i	T_i	ternary D_i	columns j for $T_j \in D_i$
1	100	{010, 001, 011, 012}	{2, 3, 4, 5}
2	010	{100, 001, 101, 102}	{1, 3, 6, 7}
3	001	{100, 010, 110, 120}	{1, 2, 8, 11}
4	011	{100, 012, 112, 121}	{1, 5, 10, 12}
5	012	{100, 011, 111, 122}	{1, 4, 9, 13}
6	101	{010, 102, 112, 122}	{2, 7, 10, 13}
7	102	{010, 101, 111, 121}	{2, 6, 9, 12}
8	110	{001, 120, 121, 122}	{3, 11, 12, 13}
9	111	{012, 102, 111, 120}	{5, 7, 9, 11}
10	112	{011, 101, 112, 120}	{4, 6, 10, 11}
11	120	{001, 110, 111, 112}	{3, 8, 9, 10}
12	121	{011, 102, 110, 121}	{4, 7, 8, 12}
13	122	{012, 101, 110, 122}	{5, 6, 8, 13}

Figure 5 The Singer (13, 4, 1) design

You can verify that in FIGURE 5, the D_i are the blocks of a (13, 4, 1) design on the columns of T, and this is no accident. In the next section, we explore this connection between parity-check matrices for q-ary Hamming codes and certain block designs. These block designs arise in the context of finite projective geometries over $\mathbb{F}_q$, and R. C. Bose describes them in his 1939 landmark paper on combinatorial designs [**3**]. Let's look at these designs now.

Singer designs

Let n be a positive integer, and let $U_n = \{(x_0, x_1, \ldots, x_n) : x_i \in \mathbb{F}_q\} - \{(0, \ldots, 0)\}$ be the set of all nonzero $(n + 1)$-tuples with elements in the field $\mathbb{F}_q$. Define an equivalence relation $\sim$ on U_n by $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ provided there exists a nonzero constant λ such that $x_i = \lambda y_i$ for all i. We define the n-dimensional projective space $PG(n, q)$ over $\mathbb{F}_q$ to be the set of all $\sim$-equivalence classes in U_n.

A point of $PG(n, q)$ is an equivalence class of $(n + 1)$-tuples. For an example, consider the space $PG(3, 5)$ of dimension 3 over the five-element field. The nonzero scalar multiples of $p = (1, 4, 3, 3)$ are p itself, $2p = (2, 3, 1, 1)$, $3p = (3, 2, 4, 4)$, and $4p = (4, 1, 2, 2)$, and so in $PG(3, 5)$, p represents the class of its nonzero multiples. (The same letter refers to both the element and its equivalence class—the key is to remember that scalar multiples represent the same class.) The lattice of subspaces of $PG(n, q)$ corresponds to the lattice of subspaces of $\mathbb{F}_q^{n+1}$.

There are $q^{n+1} - 1$ nonzero vectors in $\mathbb{F}_q^{n+1}$, and each nonzero vector is in a $\sim$-equivalence class containing $q - 1$ scalar multiples. Hence, $PG(n, q)$ contains $(q^{n+1} - 1)/(q - 1)$ elements, which are the points.

In [**3**], R. C. Bose proved the following theorem about an interesting class of block designs, now known as *Singer designs* after their discoverer James Singer, who first described them in [**18**].

Bose's Theorem. *The points and $(n-1)$-dimensional subspaces of $PG(n,q)$ are the points and blocks, respectively, of a*

$$\left(\frac{q^{n+1}-1}{q-1}, \frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}\right)$$

symmetric balanced incomplete block design.

To see why this is so, we first review some linear algebra. Let H be a d-dimensional subspace of an n-dimensional vector space. The *(right) null space* $H^{\perp}$ of H is the set of vectors v for which $Hv = \mathbf{0}$—left null spaces are defined analogously—and the *nullity* of H is the dimension of $H^{\perp}$. The rank-nullity theorem tells us that the dimension of $H^{\perp}$ is equal to $n-d$. Thus, if B is an n-dimensional subspace of $\mathbb{F}_q^{n+1}$, then by the rank-nullity theorem, $B^{\perp}$ has dimension 1.

Now, let K be a d-dimensional subspace of $PG(n,q)$. Then K corresponds to a $d+1$-dimensional subspace of $\mathbb{F}_q^{n+1}$, so its null space has dimension $n+1-(d+1) = n-d$. Projectively, this null space corresponds to an $n-d-1$-dimensional subspace of $PG(n,q)$. In particular, if K is an $(n-1)$-dimensional subspace of $PG(n,q)$, then its null space has dimension $n-(n-1)-1 = 0$. In short, the null space of an $(n-1)$-dimensional subspace of $PG(n,q)$ is a point, and it follows that distinct $(n-1)$-dimensional subspaces have distinct null spaces. Hence, the points and the $(n-1)$-dimensional subspaces—let's call the latter *blocks*—are in one-to-one correspondence, and there are $v = (q^{n+1}-1)/(q-1)$ of each.

Let B be the block whose null space is the point $(a_0, \ldots, a_n)$. Then every element $w = (x_0, \ldots, x_n) \in B$ satisfies $\sum_{i=0}^{n} a_i x_i = 0$; without loss of generality, suppose $a_0 \neq 0$. Then each of the $q^n - 1$ nonzero choices of $x_1, \ldots, x_n$ determines a unique value of x_0. However, since the $q-1$ scalar multiples of a solution vector w are considered the same, we divide out by that quantity and see that a block contains $k = (q^n-1)/(q-1)$ points. A similar argument shows that every point is contained in k blocks.

Finally, two blocks are either equal or intersect in an $(n-2)$-dimensional subspace of $PG(n,q)$, and repeating the above argument shows that the intersection of distinct blocks has $\lambda = (q^{n-1}-1)/(q-1)$ points, and each pair of distinct points belongs to λ blocks.

In short, the collection of subspaces of dimension $n-1$ in $PG(n,q)$ forms a symmetric (v,k,λ) block design whose elements are the points of $PG(n,q)$, and this completes the proof of Bose's theorem. These are called Singer designs, for reasons that will be made clear in the next section.

We now make a connection between Hamming codes and Singer designs, and the connection is this.

Theorem (The Hamming–Singer Connection). *Let q be a prime and let n be a positive integer, and let P be the parity-check matrix for the q-ary Hamming code with $n+1$ parity-check digits. Then*

- *The null spaces of the columns of P form a symmetric block design with the columns as points and the null spaces as blocks.*
- *This design contains $v = (q^{n+1}-1)/(q-1)$ points and the same number of blocks.*
- *Each block contains $k = (q^n-1)/(q-1)$ points, and each point is in the same number of blocks.*

- *Each pair of points belongs to $\lambda = (q^{n-1} - 1)/(q - 1)$ blocks together. In other words:*
- *The columns of a parity-check matrix of a Hamming*

$$\left(\frac{q^{n+1} - 1}{q - 1}, \frac{q^{n+1} - 1}{q - 1} - (n + 1)\right)$$

code are the points of a (v, k, λ) Singer design with v, k, and λ as above.

The fact that the columns of P are pairwise linearly independent guarantees that those columns can be viewed as the points of $PG(n, q)$; the Hamming–Singer connection then follows from previous reasoning. In particular, we see that for $n = q = 2$, we have $v = 7, k = 3$ and $\lambda = 1$, and so the Singer (7, 3, 1) design is another name for (7, 3, 1). See FIGURE 3).

Singer difference sets in *PG*(*n, q*)

James Singer (1906–1976) graduated from Cornell in 1926 and received a Ph.D. from Princeton in 1931 with a dissertation in topology directed by the eminent topologist J. W. Alexander. He was on the mathematics faculty of Brooklyn College from 1936 to 1974 and by all accounts was an influential and beloved teacher. He became interested in finite projective geometry, and in his 1938 paper [**18**], Singer proved the following theorem.

Singer's Theorem. *Let D be an $(n - 1)$-dimensional subspace of $PG(n, q)$. Then there is a bijective transformation carrying the $v = (q^{n+1} - 1)/(q - 1)$ points of $PG(n, q)$ onto the integers $\{0, 1, \dots, v - 1\}$ in such a way that the resulting integers corresponding to the $k = (q^n - 1)/(q - 1)$ points of D have the following property. Namely, every nonzero integer mod v can be expresses as the difference between distinct elements of D in exactly $\lambda = (q^{n-1} - 1)/(q - 1)$ ways.*

In short, Singer proved that with v, k and λ as above, each block of a Singer (v, k, λ) design is what he called a *difference set*. More generally, if v, k and λ are positive integers, then a (v, k, λ) *difference set* is a k-element subset $D = \{d_1, \dots, d_k\}$ of $\{1, 2, \dots, v\}$ such that every nonzero integer (mod v) can be expressed as a difference $d_i - d_j$ of the elements of D in exactly λ ways. Later, researchers expanded the definition to arbitrary finite groups, in which a (v, k, λ) difference set in a v-element group G is a k-element subset D of G such that every nonidentity element of G can be expressed in exactly λ ways as a product ab^{-1} of elements of D.

We began the 2002 paper [**4**] by showing that the subset $Q_7 = \{1, 2, 4\}$ of $\mathbb{Z}$ mod 7 is a (7, 3, 1) difference set. For, in $\mathbb{Z}$ mod 7, $1 = 2 - 1, 2 = 4 - 2, 3 = 4 - 1, 4 = 1 - 4, 5 = 2 - 4$, and $6 = 1 - 2$. Thus, Q_7 is a (7, 3, 1) difference set. We then showed that (a) if $p = 4n + 3$ is a prime, then the set Q_p of nonzero squares mod p is a $(4n + 3, 2n + 1, n + 1)$ difference set and (b) if D is a (v, k, λ) difference set, then the v translates $D + i = \{x + i \bmod v \mid x \in D\}$ form a symmetric (v, k, λ) block design. In particular, the seven translates of Q_7 mod 7 are the blocks $D_1, \dots, D_7$ in the left-hand column of FIGURE 2. Similarly, each of the nonzero integers mod 11 can be represented in exactly two ways as a difference of distinct elements of $Q_{11} = \{1, 3, 4, 5, 9\}$, and the 11 translates $Q_{11} + i$ mod 11 form a symmetric (11, 5, 2) block design.

A symmetric design on $V = \{0, \dots, v - 1\}$ is called *cyclic* if the v blocks are the v translates $D + i$ mod v of some fixed block D. Singer's next theorem tells us in such a design, every block is a difference set.

Theorem. *Let $\mathcal{B} = \{B_0, B_1, \ldots, B_{v-1}\}$ be the blocks of a cyclic (v, k, λ) design on the set of points $V = \{0, 1, \ldots, v-1\}$, Then each block B_i is a (v, k, λ) difference set.*

Let's prove this.

To simplify the proof, we assume that $0 \in B_0$. Thus, $B_0 = \{x_1, \ldots, x_{k-1}, 0\}$ for some $x_i \in V$, $1 \leq k-1$, $x_i \neq 0$. We show that B_0 is a (v, k, λ) difference set. Since the design is symmetric, each point is in k blocks and there are v blocks in all. Since the design is cyclic, we see that $B_j = \{x_1 + j, \ldots, x_{k-1} + j, j\}$ for $0 \leq j \leq v-1$.

Now, let d be any nonzero element of V. Then d and 0 are in exactly λ blocks together—that is, for λ values of j, $d, 0 \in B_j$. A block has no repeated elements, so if $d, 0 \in B_j$, then $d = x_r + j$ and $0 = x_s + j$ for distinct $x_r, x_s \in B_0$. Thus, $d = d - 0 = x_r - x_s$ for exactly λ pairs (x_r, x_s) of distinct elements of B_0. Since d was arbitrary, it follows that every nonzero number mod v can be expressed as a difference of elements of B_0 in exactly λ ways. In short, B_0 is a (v, k, λ) difference set.

Thus, if $a, b \in B_j$, then $a = x_r + j$, $b = x_s + j$ for $x_r, x_s \in B_0$, and so $a - b = x_r + j - (x_s - j) = x_r - x_s$. Hence, the differences of elements in B_j are the same as the differences of elements in B_0, and so each block B_j is a (v, k, λ) difference set—as claimed.

More generalization is possible. In fact, there is a way to make the Singer block designs contained in $PG(n, q)$ into cyclic designs. Proving this is tedious, so we will not pursue it. For a proof, see [**20**, pp. 79–82].

We now explore a fascinating connection (7, 3, 1) has with a number system that superficially resembles the complex numbers and to which mathematicians were led by asking questions about sums of squares.

Sums of squares, the octonions, and the sedenions

Squares and their sums have fascinated the mathematical world for millennia, beginning with the Pythagorean theorem. Euclid gives a proof of the Pythagorean theorem in Book I, Proposition 47 of The Elements. Book X, Proposition 29, Lemma 1 gives a general formula for triples (x, y, z) of integers such that $x^2 + y^2 = z^2$. In modern notation, if a and b are relatively prime integers of opposite parity, set $x = a^2 - b^2$, $y = 2ab$, and $z = a^2 + b^2$; then $x^2 + y^2 = z^2$.

Several hundred years later, Diophantus (*ca.* 250 CE) made an observation in the solution to Problem III.22 of his *Arithmetica*, an observation that implicitly contains the identity

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2,$$

which gives the product of two sums of two squares as a sum of two squares. Diophantus does not supply a proof, but almost a millennium later, Leonardo of Pisa (1175–1240) includes this two-squares identity—with proof—in his *Liber quadratorum* (The Book of Squares).

In 1748, Euler proved the four square identity, namely that the product of two sums of four squares is again a sum of four squares, showing that if $a_1, \ldots, a_4$ and $b_1, \ldots, b_4$ are numbers, then

$$\begin{aligned}
&(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\
&\quad = (a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4)^2 + (a_1b_2 + a_2b_1 + a_3b_4 - a_4b_3)^2 \\
&\qquad + (a_1b_3 - a_2b_4 + a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 + a_4b_1)^2.
\end{aligned}$$

Lagrange used this identity in his 1770 proof that every positive integer can be written as a sum of four squares of integers. The identities of Diophantus and Euler raised the question, “Are there other identities like this?”

One such identity for sums of eight squares was first found by the Danish mathematician Ferdinand Degen in 1818 . The eight-squares identity states that if $a_0, \dots, a_7$ and $b_0, \dots, b_7$ are numbers, then

$$\begin{aligned}
&(a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2)\\
&\quad \times (b_0^2 + b_1^2 + b_2^2 + b_3^2 + b_4^2 + b_5^2 + b_6^2 + b_7^2)\\
&\quad = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7)^2\\
&\qquad + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 + a_4b_5 - a_5b_4 - a_6b_7 + a_7b_6)^2\\
&\qquad + (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1 + a_4b_6 + a_5b_7 - a_6b_4 - a_7b_5)^2\\
&\qquad + (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0 + a_4b_7 - a_5b_6 + a_6b_5 - a_7b_4)^2\\
&\qquad + (a_0b_4 - a_1b_5 - a_2b_6 - a_3b_7 + a_4b_0 + a_5b_1 + a_6b_2 + a_7b_3)^2\\
&\qquad + (a_0b_5 + a_1b_4 - a_2b_7 + a_3b_6 - a_4b_1 + a_5b_0 - a_6b_3 + a_7b_2)^2\\
&\qquad + (a_0b_6 + a_1b_7 + a_2b_4 - a_3b_5 - a_4b_2 + a_5b_3 + a_6b_0 - a_7b_1)^2\\
&\qquad + (a_0b_7 - a_1b_6 - a_2b_5 + a_3b_4 - a_4b_3 - a_5b_2 + a_6b_1 + a_7b_0)^2.
\end{aligned}$$

At this point, mathematicians were quite hopeful that other, perhaps infinitely many, sums-of-squares identities exist. Let’s rephrase the question “Are there other identities like this?” as follows. For which positive integers n does there exist an identity of the form

$$(x_1^2 + \cdots + x_n^2)(y_1^2 + \cdots + y_n^2) = z_1^2 + \cdots + z_n^2, \qquad \text{where } z_k = \sum_{i,j=1}^{n} A_{ijk} x_i y_j,$$

and the A_{ijk} are constants independent of the values of the x_i and the y_j?

The question was answered in 1898 by Adolph Hurwitz, who proved that such an identity exists for $n = 1, 2, 4, 8$—and for no other positive integers. He showed that each sums-of-squares identity led to an n-dimensional *normed algebra*. Now a normed algebra $\mathbb{A}$ is an n-dimensional vector space over the real numbers $\mathbb{R}$ that has two special features, namely (1) a vector multiplication that distributes over vector addition, and (2) a mapping $N : \mathbb{A} \to \mathbb{R}$ such that $N(uv) = N(u)N(v)$ for all $u, v \in \mathbb{A}$. These algebras are the real numbers $\mathbb{R}$ ($n = 1$), the complex numbers $\mathbb{C}$ ($n = 2$), Hamilton’s *quaternions* $\mathbb{H}$ ($n = 4$), and the *octonions* $\mathbb{O}$ ($n = 8$). The latter is a beautiful algebraic system with a multiplication table that reveals itself as another aspect of (7, 3, 1). We will explore the octonions below, and then we will construct the analogous 16-dimensional algebra known as the *sedenions* and see just why it is not a normed algebra.

One square is easy: Because multiplication of real numbers is commutative and associative, we see that $a^2b^2 = (ab)^2$ for all real numbers a and b. As for two squares, Diophantus (*ca.* 250 CE) had an answer. Problem III.22 of his *Arithmetica* implicitly contains the identity

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2,$$

which gives the product of two sums of two squares as a sum of two squares. As mentioned above, the normed algebras associated with the one-square and two-square identities will turn out to be the real numbers $\mathbb{R}$ and the complex numbers $\mathbb{C}$, respectively.

In fact, multiplication of complex numbers reflects the two-squares identity as follows. Let $z = a + bi$ and define $N(z) = a^2 + b^2$; if $w = c + di$, then $N(w) = c^2 + d^2$, and we see that $zw = ac - bd + (ad + bc)i$. Finally, we see that

$$N(zw) = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)(c^2 + d^2) = N(z)N(w),$$

by the two-squares identity.

As for the associated normed algebra associated with the four-squares identity, that is one of the great stories in mathematics, and it came about in the following way.

During the early 1840s, William R. Hamilton was searching for a way to multiply ordered triples of real numbers, analogous to multiplication of complex numbers viewed as ordered pairs. He searched a long time and failed to find such a multiplication, but working through these unsuccessful attempts led him to one of the famous "aha!" moments in the history of mathematics. On the morning of October 16, 1843, that moment came to Hamilton while he was taking a walk. He realized in a flash of insight that the solution he sought was a multiplication of quadruples, not triples, and then, as he described in an 1865 letter to his son Archibald [**13**], "Nor could I resist the impulse—unphilosophical as it may have been—to cut with a knife on a stone of Brougham Bridge, as we passed it, the fundamental formula with the symbols, i, j, k; namely,

$$i^2 = j^2 = k^2 = ijk = -1,$$

which contains the Solution of the Problem, but of course, as an inscription, has long since mouldered away."

Hamilton gave the name *quaternions* to the resulting algebra $\mathbb{H}$ generated by 1, i, j and k; the multiplication table for the units 1, i, j and k is as follows:

$*$	**1**	**i**	**j**	**k**
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

A quaternion is an expression of the form $x_1 + x_2i + x_3j + x_4k$, where the x_n are real numbers. It is easy to see how to add these expressions term-by-term, and Hamilton's new multiplication table shows us how to multiply them. One multiplies two quaternions by using the distributive law, Hamilton's table, and the fact that $xi = ix, xj = jx$, and $xk = kx$ for all real numbers x. Hamilton showed that this multiplication is associative; however, the table shows that $ij = k = -ji$ and so multiplication is not commutative. We can define a norm on $\mathbb{H}$ by $N(x_1 + x_2i + x_3j + x_4k) = x_1^2 + x_2^2 + x_3^2 + x_4^2$, and because of the four-square identity, it follows that $N(x)N(y) = N(xy)$ for all $x, y \in \mathbb{H}$. Therefore, $\mathbb{H}$ is a four-dimensional normed algebra—that is, $\mathbb{R}^4$ equipped with a multiplication—and because of that, we can show that $\mathbb{H}$ is a *division ring*, which means that every nonzero element of $\mathbb{H}$ has a multiplicative inverse. Here's how.

We first define the *conjugate* $\overline{x}$ of a quaternion x by $\overline{x_1 + x_2i + x_3j + x_4k} = x_1 - x_2i - x_3j - x_4k$. Another routine calculation shows that

$$x\overline{x} = (x_1 + x_2i + x_3j + x_4k)(x_1 - x_2i - x_3j - x_4k) = x_1^2 + x_2^2 + x_3^2 + x_4^2 = N(x).$$

Now, if $x \neq 0$, then $N(x)$ is a positive real number, and it follows that

$$x \cdot \frac{\overline{x}}{N(x)} = \frac{N(x)}{N(x)} = 1.$$

Hence, x has a multiplicative inverse, and so $\mathbb{H}$ is a division algebra. Since, at that time, the only known division rings were fields, $\mathbb{H}$ was the first example of a noncommutative division ring. This unique status of $\mathbb{H}$ would last only a couple of months.

What happened next was that, the very next day, Hamilton mailed the good news about the quaternions to his friend and fellow mathematician John T. Graves. Two months later, Graves sent him a letter in which he described a multiplication on $\mathbb{R}^8$; we now call this algebra the *octonions* $\mathbb{O}$. Hamilton's quaternion multiplication uses three units $\{i, j, k\}$, each of whose squares is equal to -1. Graves' multiplication on $\mathbb{O}$ uses seven units $\{o_1, \dots, o_7\}$ whose products come from the following multiplication table:

*	**1**	$\mathbf{o_1}$	$\mathbf{o_2}$	$\mathbf{o_3}$	$\mathbf{o_4}$	$\mathbf{o_5}$	$\mathbf{o_6}$	$\mathbf{o_7}$
1	1	o_1	o_2	o_3	o_4	o_5	o_6	o_7
$\mathbf{o_1}$	o_1	-1	o_4	o_7	$-o_2$	o_6	$-o_5$	$-o_3$
$\mathbf{o_2}$	o_2	$-o_4$	-1	o_5	o_1	$-o_3$	o_7	$-o_6$
$\mathbf{o_3}$	o_3	$-o_7$	$-o_5$	-1	o_6	o_2	$-o_4$	o_1
$\mathbf{o_4}$	o_4	o_2	$-o_1$	$-o_6$	-1	o_7	o_3	$-o_5$
$\mathbf{o_5}$	o_5	$-o_6$	o_3	$-o_2$	$-o_7$	-1	o_1	o_4
$\mathbf{o_6}$	o_6	o_5	$-o_7$	o_4	$-o_3$	$-o_1$	-1	o_2
$\mathbf{o_7}$	o_7	o_3	o_6	$-o_1$	o_5	$-o_4$	$-o_2$	-1

Better yet, this multiplication came equipped with a norm, namely

$$N(a_0 + a_1 o_1 + \cdots + a_7 o_7) = a_0^2 + a_1^2 + \cdots + a_7^2.$$

This norm satisfies $N(ab) = N(a)N(b)$ because of Graves' other bit of news, namely his rediscovery of the eight-squares identity,

$$\begin{aligned}
&(a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2) \\
&\quad \times (b_0^2 + b_1^2 + b_2^2 + b_3^2 + b_4^2 + b_5^2 + b_6^2 + b_7^2) \\
&\quad = (a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3 - a_4b_4 - a_5b_5 - a_6b_6 - a_7b_7)^2 \\
&\qquad + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2 + a_4b_5 - a_5b_4 - a_6b_7 + a_7b_6)^2 \\
&\qquad + (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1 + a_4b_6 + a_5b_7 - a_6b_4 - a_7b_5)^2 \\
&\qquad + (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0 + a_4b_7 - a_5b_6 + a_6b_5 - a_7b_4)^2 \\
&\qquad + (a_0b_4 - a_1b_5 - a_2b_6 - a_3b_7 + a_4b_0 + a_5b_1 + a_6b_2 + a_7b_3)^2 \\
&\qquad + (a_0b_5 + a_1b_4 - a_2b_7 + a_3b_6 - a_4b_1 + a_5b_0 - a_6b_3 + a_7b_2)^2 \\
&\qquad + (a_0b_6 + a_1b_7 + a_2b_4 - a_3b_5 - a_4b_2 + a_5b_3 + a_6b_0 - a_7b_1)^2 \\
&\qquad + (a_0b_7 - a_1b_6 - a_2b_5 + a_3b_4 - a_4b_3 - a_5b_2 + a_6b_1 + a_7b_0)^2.
\end{aligned}$$

As we have seen, the eight-squares identity was first found by the Danish mathematician Ferdinand Degen in 1818, but there is no evidence that Degen constructed the associated multiplication on $\mathbb{R}^8$. Arthur Cayley independently rediscovered that identity when he constructed the eight-dimensional normed algebra $\mathbb{O}$ in 1845, and both he and Graves used the same method to produce their versions of $\mathbb{O}$. Their method was to mimic the constructions of $\mathbb{C}$ and $\mathbb{H}$ as two-dimensional vector spaces over $\mathbb{R}$ and $\mathbb{C}$, respectively, with multiplication described by a formula similar to multiplication of complex numbers.

This method should bear the names of both Cayley and Graves. Unfortunately, Cayley's work was published first, and his method was later generalized by the American mathematician L. E. Dickson in such papers as [**10**]. As a result, we call this method the *Cayley–Dickson* construction.

Because $\mathbb{O}$ is a normed algebra, by previous reasoning we see that $\mathbb{O}$ is also a division ring, and the table tells us that multiplication in $\mathbb{O}$ is noncommutative. It is also nonassociative, for $o_1(o_2o_3) = o_1o_5 = o_6$, whereas $(o_1o_2)o_3 = o_4o_3 = -o_6$.

The construction of this multiplication table seems quite mysterious; however, if we look more closely, we notice that

$$\begin{aligned}
o_1o_2 &= o_4 = -o_2o_1,\\
o_2o_3 &= o_5 = -o_3o_2,\\
o_3o_4 &= o_6 = -o_4o_3,\\
o_4o_5 &= o_7 = -o_5o_4,\\
o_5o_6 &= o_1 = -o_6o_5,\\
o_6o_7 &= o_2 = -o_7o_6, \text{ and}\\
o_7o_1 &= o_3 = -o_1o_7.
\end{aligned}$$

And now we see it. For distinct $a, b \in \{1, \dots, 7\}$, $o_ao_b = \pm o_c$, where $\{a, b, c\}$ is one of the seven blocks D_i in the mod 7 (7, 3, 1) block design. The sign is determined by cyclically ordering the blocks as follows: $(1, 2, 4)$, $(2, 3, 5)$, $(3, 4, 6)$, $(4, 5, 7)$, $(5, 6, 1)$, $(6, 7, 2)$, and $(7, 1, 3)$. Then $o_ao_b = o_c$ or $o_ao_b = -o_c$ according as a does or does not directly precede b in the unique ordered block containing a and b. Thus, 6 precedes 1 in the block $(5, 6, 1)$, so $o_6o_1 = o_5$; 6 does not directly precede 4 in $(3, 4, 6)$, so $o_6o_4 = -o_3$. (We note that these designated orderings on the blocks of (7, 3, 1) arise as a direct result of Graves' method of constructing $\mathbb{O}$.) And that is why "the multiplication rule for the octonion units" is another name of (7, 3, 1).

But there is more: the octonion algebra has the following structural feature:

1. The octonion algebra $\mathbb{O}$ contains seven complex subalgebras $\mathbb{C}_n = \mathbb{R}\langle o_n\rangle$ and seven quaternion subalgebras $\mathbb{H}_n = \mathbb{R}\langle o_t, o_u, o_v\rangle$, where $\{t, u, v\}$ is a block in (7, 3, 1).
2. Each $\mathbb{H}_n$ contains three of the $\mathbb{C}_k$ and each $\mathbb{C}_k$ is contained in three of the $\mathbb{H}_n$.
3. Each pair $\{\mathbb{C}_k, \mathbb{C}_m\}$ is contained in a unique $\mathbb{H}_n$ together.

In short, $\mathbb{O}$ contains a (7, 3, 1) block design, with the seven quaternion subalgebras as blocks and the seven complex subalgebras as points—another name of (7, 3, 1).

Well, can we do this again and get a 16-squares identity? We applied the Cayley–Dickson construction to the complex numbers to get the quaternions, and the resulting algebra was no longer commutative. We applied Cayley–Dickson to the quaternions to get the octonions and there was a connection with (7, 3, 1), but the resulting algebra was no longer associative. It is natural, therefore, to ask what happens when we apply Cayley–Dickson to the octonions? The answer is that we can do this, and the result is a 16-dimensional real algebra $\mathbb{S}$ called the *sedenions*. The multiplication on $\mathbb{S}$ uses 15 units $\{s_1, \dots, s_{15}\}$ whose products come from the multiplication table described in FIGURE 6.

$*$	$\mathbf{1}$	$\mathbf{s_1}$	$\mathbf{s_2}$	$\mathbf{s_3}$	$\mathbf{s_4}$	$\mathbf{s_5}$	$\mathbf{s_6}$	$\mathbf{s_7}$	$\mathbf{s_8}$	$\mathbf{s_9}$	$\mathbf{s_{10}}$	$\mathbf{s_{11}}$	$\mathbf{s_{12}}$	$\mathbf{s_{13}}$	$\mathbf{s_{14}}$	$\mathbf{s_{15}}$
$\mathbf{1}$	1	s_1	s_2	s_3	s_4	s_5	s_6	s_7	s_8	s_9	s_{10}	s_{11}	s_{12}	s_{13}	s_{14}	s_{15}
$\mathbf{s_1}$	s_1	-1	s_3	$-s_2$	$-s_5$	$-s_4$	$-s_7$	s_6	s_9	$-s_8$	$-s_{11}$	s_{10}	$-s_{13}$	s_{12}	s_{15}	$-s_{14}$
$\mathbf{s_2}$	s_2	$-s_3$	-1	s_1	s_6	$-s_7$	s_4	$-s_5$	s_{10}	s_{11}	$-s_8$	$-s_9$	$-s_{14}$	$-s_{15}$	s_{12}	s_{13}
$\mathbf{s_3}$	s_3	s_2	$-s_1$	-1	s_7	$-s_6$	s_5	$-s_4$	s_{11}	$-s_{10}$	s_9	$-s_8$	$-s_{15}$	s_{14}	$1s_{13}$	s_{12}
$\mathbf{s_4}$	s_4	$-s_5$	$-s_6$	$-s_7$	-1	s_1	s_2	s_3	s_{12}	s_{13}	s_{14}	s_{15}	$-s_8$	$-s_9$	$-s_{10}$	$-s_{11}$
$\mathbf{s_5}$	s_5	s_4	$-s_7$	s_6	$-s_1$	-1	$-s_3$	s_2	s_{13}	$-s_{12}$	s_{15}	$-s_{14}$	s_9	$-s_8$	s_{11}	$-s_{10}$
$\mathbf{s_6}$	s_6	s_7	s_4	$-s_5$	$-s_2$	s_3	-1	$-s_1$	s_{14}	$-s_{15}$	$-s_{12}$	s_{13}	s_{10}	$-s_{11}$	$-s_8$	s_9
$\mathbf{s_7}$	s_7	$-s_6$	s_5	s_4	$-s_3$	$-s_2$	s_1	-1	s_{15}	s_{14}	$-s_{13}$	$-s_{12}$	s_{11}	s_{10}	$-s_9$	$-s_8$
$\mathbf{s_8}$	s_8	$-s_9$	$-s_{10}$	$-s_{11}$	$-s_{12}$	$-s_{13}$	$-s_{14}$	$-s_{15}$	-1	s_1	s_2	s_3	s_4	s_5	s_6	s_7
$\mathbf{s_9}$	s_9	s_8	$-s_{11}$	s_{10}	$-s_{13}$	s_{12}	s_{15}	$-s_{14}$	$-s_1$	-1	$-s_3$	s_2	$-s_5$	s_4	s_7	$-s_6$
$\mathbf{s_{10}}$	s_{10}	s_{11}	s_8	$-s_9$	$-s_{14}$	$-s_{15}$	s_{12}	s_{13}	$-s_2$	s_3	-1	$-s_1$	$-s_6$	$-s_7$	s_4	s_5
$\mathbf{s_{11}}$	s_{11}	$-s_{10}$	s_9	s_8	$-s_{15}$	s_{14}	$-s_{13}$	s_{12}	$-s_3$	$-s_2$	$-s_1$	-1	$-s_7$	s_6	$-s_5$	s_4
$\mathbf{s_{12}}$	s_{12}	s_{13}	s_{14}	s_{15}	s_8	$-s_9$	$-s_{10}$	$-s_{11}$	$-s_4$	s_5	s_6	s_7	-1	$-s_1$	$-s_2$	$-s_3$
$\mathbf{s_{13}}$	s_{13}	$-s_{12}$	s_{15}	$-s_{14}$	s_9	s_8	s_{11}	$-s_{10}$	$-s_5$	$-s_4$	s_7	$-s_6$	s_1	-1	s_3	$-s_2$
$\mathbf{s_{14}}$	s_{14}	$-s_{15}$	$-s_{12}$	s_{13}	s_{10}	$-s_{11}$	s_8	s_9	$-s_6$	$-s_7$	$-s_4$	s_5	s_2	$-s_3$	-1	s_1
$\mathbf{s_{15}}$	s_{15}	s_{14}	$-s_{13}$	$-s_{12}$	s_{11}	s_{10}	$-s_9$	s_8	$-s_7$	s_6	$-s_5$	$-s_4$	s_3	s_2	$-s_1$	-1

Figure 6 The sedenions

It happens that there are 15 eight-dimensional subalgebras of $\mathbb{S}$, each isomorphic to the octonions, and for each of these, the multiplication tables are generated by 15 isomorphic copies of (7, 3, 1). One obtains the overall multiplication by adjusting the tables of the 15 octonions to achieve consistency of the products from one octonion subalgebra to the next. There are also 35 four-dimensional subalgebras of $\mathbb{S}$, each isomorphic to the quaternions, and 15 two-dimensional subalgebras of $\mathbb{S}$, each isomorphic to the complex numbers. And there is another design hidden within this set of subalgebras. Namely, the 15 complex subalgebras (points) and the 35 quaternionic subalgebras (blocks) form a (15, 35, 7, 3, 1) block design.

However, the string of normed algebras—that is, algebras with sums-of-squares identities—stops with $\mathbb{O}$. The reason is that $\mathbb{S}$ contains pairs of nonzero elements whose product equals zero, and this prevents $\mathbb{S}$ from being a normed algebra. Indeed, suppose there were a norm N on $\mathbb{S}$. From the table we see that

$$(s_5 + s_9)(s_7 - s_{11}) = s_5s_7 + s_9s_7 - s_5s_{11} - s_9s_{11} = 0.$$

Thus, $0 = N(0) = N((s_5 + s_9)(s_7 - s_{11})) = N(s_5 + s_9)N(s_7 - s_{11})$, so one of $N(s_5 + s_9)$, $N(s_7 - s_{11})$ must be 0. But this implies that either $s_5 = -s_9$ or $s_7 = s_{11}$, neither of which holds. Hence, the sedenions are not a normed algebra. Finally, the Cayley–Dickson operation on $\mathbb{S}$ won't produce a normed algebra, as the resulting 32-dimensional algebra would contain 31 copies of $\mathbb{S}$. Thus, there are no more real normed algebras to be produced by the Cayley–Dickson construction, and so—according to L. E. Dickson's modification of Hurwitz' original proof [**10**]—there are no real normed algebras beyond the octonions.

And with that, our journey through more of the many names of (7, 3, 1) is done.

REFERENCES

1. J. C. Baez, The octonions, *Bull. Amer. Math. Soc.* **39** (2002) 145–205, see also http://math.ucr.edu/home/baez/octonions/oct.pdf.
2. T. Beth, D. Jungnickel, H. Lenz, *Design Theory*. Second edition. Cambridge Univ. Press, Cambridge, 1999.
3. R. C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugenics* **9** (1939) 353–399.
4. E. Brown, The many names of (7, 3, 1), *Math. Mag.* **75** (2002) 83–94.
5. E. Brown, N. Loehr, Why is PSL(2, 7) ≅ GL(3, 2)?, *Amer. Math. Monthly* **116** no. 8 (October 2009) 727–731.
6. E. Brown, K. Mellinger, Kirkman's Schoolgirls wearing hats and walking through fields of numbers, *Math. Mag.* **82** (2009) 3–15.
7. *Handbook of Combinatorial Designs*. Second edition. Ed. by C. J. Colbourn and J. H. Dinitz. Chapman and Hall/CRC, Boca Raton FL, 2007.
8. C. Mulcahy, *Mathematical Card Magic: Fifty-Two New Effects*. A K Peters/CRC, Boca Raton FL, 2013.
9. J. H. Conway, D. A. Smith, *On Quaternions and Octonions*. A K Peters, Natick MA, 2003.
10. L. E. Dickson, On quaternions and their generalizations and the history of the eight square theorem, *Annals of Math.* second series, **20** (1919) 155–171.
11. R. Guy, The unity of combinatorics, *Combinatorics Advances*. Edited by C. J. Colbourn and E. S. Mahmoodian. Kluwer Academic Publishers, Dordrecht, The Netherlands. 1995, pp. 129–159.
12. M. Hall, Jr., *Combinatorial Theory*. Second edition. John Wiley & Sons, New York, 1986.
13. William R. Hamilton, Letter from Sir W. R. Hamilton to Rev. Archibald H. Hamilton, August 5, 1865.
14. T. P. Kirkman, On a problem in combinations, *Camb. Dublin Math. J.* **2** (1847) 191–204.
15. T. P. Kirkman, Query 6, *Lady's and Gentlemen's Diary* (1850) p. 48.
16. T. P. Kirkman, Note on an unanswered prize question, *Camb. Dublin Math. J.* **5** (1850) 255–262.
17. C. E. Shannon, A mathematical theory of communication, *Bell System Tech. J.* **27** (1948) 379–423, 623–656.
18. J. Singer, A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.* **43** (1938) 377–385.
19. T. M. Thompson, *From Error-Correcting Codes through Sphere Packings to Simple Groups*. Carus Mathematical Monograph No. 21. Mathematical Association of America, Washington, DC, 1983.
20. W. D. Wallis, *Introduction to Combinatorial Designs*. Second edition. Chapman and Hall/CRC, Boca Raton FL, 2007.
21. W. S. B. Woolhouse, Prize question 1733, *Lady's and Gentleman's Diary*, 1844.

Summary. The (7, 3, 1) block design is an object that shows up in many areas of mathematics. In fact, (7, 3, 1) seems to appear again and again in unexpected places. A 2002 paper described (7, 3, 1)'s connection with such areas as graph theory, number theory, topology, round-robin tournaments, and algebraic number fields.

In this paper, we show how (7, 3, 1) makes appearances in the areas of error-correcting codes, n-dimensional finite projective geometries, difference sets, normed algebras, and the three-circle Venn diagram.

EZRA (BUD) BROWN (MR Author ID: 222489) grew up in New Orleans and has degrees from Rice University and Louisiana State University. He has been at Virginia Tech since 1969, where he is currently Alumni Distinguished Professor of Mathematics. His research interests include number theory and combinatorics. In graduate school, he first met the (7, 3, 1) block design, and the design continues to amaze him with its many and varied mathematical connections. He is a frequent contributor to the MAA journals.

In his spare time, Bud enjoys singing (from opera to rock and roll), playing jazz piano, and solving word puzzles. He and his wife, Jo, enjoy kayaking, bicycling, and birding. He occasionally bakes biscuits for his students, and he once won a karaoke contest.

Rationalizing Denominators

ALLAN BERELE
Department of Mathematics,
DePaul University, Chicago, IL 60614
aberele@condor.depaul.edu

STEFAN CATOIU
Department of Mathematics,
DePaul University, Chicago, IL 60614
scatoiu@condor.depaul.edu

A standard topic in algebra is rationalizing denominators. Given a fraction in which the denominator involves radicals, we want to find an equivalent fraction whose denominator is an integer. The two cases most commonly covered are those in which the denominator is a monomial, such as

$$\frac{1}{\sqrt{3}}=\frac{1}{\sqrt{3}}\times\frac{\sqrt{3}}{\sqrt{3}}=\frac{\sqrt{3}}{3},$$

and ones in which the denominator is the sum or difference of two square roots, or one square root and one integer, such as

$$\frac{1}{\sqrt{5}-\sqrt{3}}=\frac{1}{\sqrt{5}-\sqrt{3}}\times\frac{\sqrt{5}+\sqrt{3}}{\sqrt{5}+\sqrt{3}}=\frac{\sqrt{5}+\sqrt{3}}{5-3}=\frac{\sqrt{5}+\sqrt{3}}{2}.$$

In the pre-calculator era it would have been obvious why we rationalize denominators: A rationalized fraction such as $(\sqrt{5}+\sqrt{3})/2$ would have been much easier to compute than the unrationalized fraction $1/(\sqrt{5}-\sqrt{3})$. Although this is no longer an issue, it is still useful to be able to put radical fractions in a canonical form (and not just to make it easier to check the student's answer with the one in the solutions manual!). For example, from a more advanced point of view, rationalizing denominators is relevant to understanding why the field of linear functions

$$\mathbb{Q}(\alpha)=\left\{\frac{x+y\cdot\alpha}{s+t\cdot\alpha}: x,y,s,t\in\mathbb{Q},\ (s,t)\neq(0,0)\right\},$$

where α is a root of an irreducible polynomial x^2+bx+c with $b,c\in\mathbb{Q}$, coincides with the ring of linear polynomials $\mathbb{Q}[\alpha]=\{x+y\cdot\alpha : x,y\in\mathbb{Q}\}$ (the product of two such polynomials will again be linear because $\alpha^2=-c-b\alpha$).

The goal of this paper is to discuss techniques of rationalization for more complex denominators, such as ones with higher radicals or more terms. However useful rationalization may or may not be, it is always important to be curious and ask questions. How do we rationalize the denominator if it is neither a monomial nor a sum of square roots seems a natural such question. In the course of this paper we will present three different algorithms for rationalizing denominators, and accordingly, three different proofs that radical denominators can always be rationalized. Along the way to the answer we will explain some interesting ideas from linear algebra, symmetric function theory, field theory, and algebraic number theory. Interested readers can find more

Math. Mag. **88** (2015) 121–136. doi:10.4169/math.mag.88.2.121. © Mathematical Association of America
MSC: Primary 11R09, Secondary 12D05; 12E05; 12F05.

information on these topics in textbooks like the ones by Howie [**1**], Nicholson [**2**], Ribenboim [**3**], or Stillwell [**4**].

We are using 1 for all of the numerators for simplicity. In the sequel we will often omit the numerators altogether and simply focus on the denominators.

Binomial denominators

If the denominator of a fraction is the binomial $a - b$, we can rationalize it using the well-known factoring formula for a difference of two nth powers

$$(a-b)(a^{n-1}+a^{n-2}b+a^{n-3}b^2+\cdots+b^{n-1})=a^n-b^n, \tag{1}$$

provided both a and b are nth roots. For example, to rationalize the fraction

$$\frac{1}{\sqrt[3]{9}-\sqrt[3]{2}}$$

we would multiply numerator and denominator by

$$\sqrt[3]{9}^2+\sqrt[3]{9}\sqrt[3]{2}+\sqrt[3]{2}^2=3\sqrt[3]{3}+\sqrt[3]{18}+\sqrt[3]{4}$$

to get

$$\frac{3\sqrt[3]{3}+\sqrt[3]{18}+\sqrt[3]{4}}{9-2}=\frac{3\sqrt[3]{3}+\sqrt[3]{18}+\sqrt[3]{4}}{7}.$$

We can adapt (1) to deal with sums instead of differences by simply substituting in $-b$ for b, yielding

$$(a+b)(a^{n-1}-a^{n-2}b+a^{n-3}b^2-\cdots\pm b^{n-1})=a^n\pm b^n.$$

What if the denominator is a sum or difference of radicals with different degrees such as $\sqrt{3}-\sqrt[3]{5}$? There are two reasonable strategies we could employ in this case. One is to convert both to a common degree:

$$\sqrt{3}-\sqrt[3]{5}=3^{1/2}-5^{1/3}=3^{3/6}-5^{2/6}=\sqrt[6]{27}-\sqrt[6]{25}$$

and so we could multiply numerator and denominator by

$$\sqrt[6]{27}^5+\sqrt[6]{27}^4\sqrt[6]{25}+\sqrt[6]{27}^3\sqrt[6]{25}^2+\sqrt[6]{27}^2\sqrt[6]{25}^3+\sqrt[6]{27}\sqrt[6]{25}^4+\sqrt[6]{25}^5.$$

The second strategy is to deal with the radicals individually. To eliminate the square root we would multiply the numerator and denominator by $(\sqrt{3}+\sqrt[3]{5})$ which would turn the denominator into $3-\sqrt[3]{25}$. Then we could eliminate the cube root by multiplying the numerator and denominator by $9+3\sqrt[3]{25}+5\sqrt[3]{5}$.

Denominators with square roots

The above techniques will work for any fraction in which the denominator is a binomial. What if the denominator has three or more terms? We present a technique that will work for square roots. Say the denominator is a sum of three square roots, for example $\sqrt{2}+\sqrt{3}+\sqrt{11}$. Considering the first two grouped together, we multiply by $(\sqrt{2}+\sqrt{3})-\sqrt{11}$ to get

$$(\sqrt{2}+\sqrt{3})^2-\sqrt{11}^2=2+2\sqrt{6}+3-11=-6+2\sqrt{6}.$$

Although this does not rationalize the denominator in one fell swoop, it rewrites the fraction with a denominator having only one square root which we could then rationalize by mutiplying numerator and denominator by $-6-2\sqrt{6}$.

This technique can be adapted if the denominator is a sum of up to five square roots. The problem is that if we square a sum of two square roots, we get only one square root and if we square a sum of three we are left with three, but if we square a sum of four or more square roots we get more than we started with! There is a trick we can use to adapt our technique to any number of square roots: Instead of trying to reduce the number of radicals, we will reduce the number of prime factors. Let $\{p_1,\ldots,p_k\}$ be the set of primes which divide at least one of the radicals. Write the denominator as $A+B$, where B is the sum of all terms of the form $\sqrt{p_k a}$ and A is the sum of the other terms, or zero if there are none. Better yet: Write B as $C\sqrt{p_k}$, so the denominator is now $A+C\sqrt{p_k}$. Then if we multiply the numerator and denominator by $A-C\sqrt{p_k}$, the denominator becomes $A^2-C^2p_k$. Although $A^2-C^2p_k$ may well involve more square roots than the original denominator, these square roots will only have prime factors from the set $\{p_1,\ldots,p_{k-1}\}$. Repeating this procedure at most $k-1$ more times, all square roots will be eliminated.

Example 1. When rationalizing the denominator $2\sqrt{10}-3\sqrt{6}+\sqrt{15}$, the set of primes is $\{p_1=2, p_2=3, p_3=5\}$. We write the expression in standard form

$$2\sqrt{10}-3\sqrt{6}+\sqrt{15}=(-3\sqrt{6})+(2\sqrt{2}+\sqrt{3})\sqrt{5}=A_1+C_1\sqrt{5}$$

according to the last prime 5. Multiplication by the conjugate $A_1-C_1\sqrt{5}$ yields

$$(-3\sqrt{6})^2-(2\sqrt{2}+\sqrt{3})^2\cdot 5=54-(8+4\sqrt{6}+3)\cdot 5=-1-20\sqrt{6}$$

whose set of primes is $\{p_1=2, p_2=3\}$. We write the new denominator in standard form

$$-1-20\sqrt{6}=(-1)+(-20\sqrt{2})\sqrt{3}=A_2+C_2\sqrt{3}$$

according to the last prime 3. Multiplication by the conjugate $A_2-C_2\sqrt{3}$ yields

$$(-1)^2-(-20\sqrt{2})^2\cdot 3=1-2400=-2399.$$

The fraction is then rationalized as

$$\frac{1}{2\sqrt{10}-3\sqrt{6}+\sqrt{15}}=\frac{(A_1-C_1\sqrt{5})(A_2-C_2\sqrt{3})}{-2399}.$$

More on square roots

In this section we produce an exact formula for rationalizing any fraction whose denominator is a linear combination with rational coefficients of square roots of rational numbers. Equivalently, we rationalize denominators of the form

$$\sqrt{a_1}\pm\sqrt{a_2}\pm\cdots\pm\sqrt{a_n},$$

for $a_1, a_2, \dots, a_n$ integers and any fixed choices of signs ±. This will include the case in which a_1 is a perfect square.

The following example gives the motivation for the whole section.

Example 2. We start with the product expansion for $-6 + 2\sqrt{6}$ of Section 2:

$$(\sqrt{2}+\sqrt{3}+\sqrt{11})(\sqrt{2}+\sqrt{3}-\sqrt{11}) = (\sqrt{2}+\sqrt{3})^2 - \sqrt{11}^2 = -6+2\sqrt{6},$$

and come up with a similar expansion for $-6 - 2\sqrt{6}$:

$$(\sqrt{2}-\sqrt{3}+\sqrt{11})(\sqrt{2}-\sqrt{3}-\sqrt{11}) = (\sqrt{2}-\sqrt{3})^2 - \sqrt{11}^2 = -6-2\sqrt{6}.$$

Multiplication of the two makes the product

$$\begin{aligned}(\sqrt{2}+\sqrt{3}+\sqrt{11})(\sqrt{2}+\sqrt{3}-\sqrt{11})(\sqrt{2}-\sqrt{3}+\sqrt{11})(\sqrt{2}-\sqrt{3}-\sqrt{11})\\ = (-6+2\sqrt{6})(-6-2\sqrt{6}) = 36-24 = 12\end{aligned} \tag{2}$$

a rational number. In particular, the rationalization of $1/(\sqrt{2}+\sqrt{3}+\sqrt{11})$ is

$$\frac{1}{\sqrt{2}+\sqrt{3}+\sqrt{11}} = \frac{(\sqrt{2}+\sqrt{3}-\sqrt{11})(\sqrt{2}-\sqrt{3}+\sqrt{11})(\sqrt{2}-\sqrt{3}-\sqrt{11})}{12}.$$

The general case of a denominator that is a sum/difference of n square roots is done in a similar fashion. Consider the n variable polynomial f given by the product

$$f = \prod(x_1 \pm x_2 \pm \cdots \pm x_n)$$

and whose factors are determined by one of two choices of sign for the indeterminates $x_2, \dots, x_n$. Separating these two choices for the last variable x_n, we deduce

$$\begin{aligned} f &= \prod(x_1 \pm x_2 \pm \cdots \pm x_{n-1} + x_n) \times \prod(x_1 \pm x_2 \pm \cdots \pm x_{n-1} - x_n)\\ &= \prod(x_1 \pm x_2 \pm \cdots \pm x_{n-1} + x_n)(x_1 \pm x_2 \pm \cdots \pm x_{n-1} - x_n)\\ &= \prod\left((x_1 \pm x_2 \pm \cdots \pm x_{n-1})^2 - x_n^2\right).\end{aligned}$$

For instance, the product decomposition (2) of Example 2 corresponds to

$$f = \prod\left((\sqrt{2}\pm\sqrt{3})^2 - \sqrt{11}^2\right).$$

Back to generality, we observe that the degree of x_n in each monomial of f is even and, similarly, the same is true for $x_2, \dots, x_{n-1}$. By elimination, since f is homogenous of even degree 2^{n-1}, the same is true for x_1 as well. It follows that $f(x_1, \dots, x_n)$=$g(x_1^2, \dots, x_n^2)$, for some polynomial g in n indeterminates and with integer coefficients. In particular, by setting $x_i = \sqrt{a_i}$, for $i = 1, 2, \dots, n$, and a_i integers, we deduce that $f(\sqrt{a_1}, \dots, \sqrt{a_n}) = g(a_1, \dots, a_n)$ is an integer.

Let α, β be two polynomials with rational coefficients in variables radicals of rationals. Then α, β are *rational conjugates* if their product is a rational number r. This is equivalent to saying that the fraction $1/\alpha$ rationalizes as $1/\alpha = \beta/r$. We therefore proved the following theorem on the exact rationalization of the fraction $1/(\sqrt{a_1} \pm \sqrt{a_2} \pm \cdots \pm \sqrt{a_n})$.

Theorem 1. *Let $a_1, a_2, \ldots, a_n$ be positive integers. Then the product*

$$\prod(\sqrt{a_1} \pm \sqrt{a_2} \pm \cdots \pm \sqrt{a_n}),$$

taken upon all choices of sign ±, is an integer. In particular, the rational conjugate of any factor of the above product is the product of the remaining factors.

Polynomial denominators and the method of indeterminate coefficients

Geometric series and rational conjugates. Continuing with the idea of Section 1, the expansion that produced the formula of the nth partial sum of the geometric series

$$(1-x)(1+x+x^2+\cdots+x^{n-1}) = 1-x^n,$$

when evaluated at $x = \sqrt[n]{r}$, for r rational, makes the product

$$(1-\sqrt[n]{r})\left(1+\sqrt[n]{r}+(\sqrt[n]{r})^2+\cdots+(\sqrt[n]{r})^{n-1}\right) = 1-(\sqrt[n]{r})^n = 1-r$$

a rational number. In particular, the reciprocals of its two factors rationalize as

$$\frac{1}{1-\sqrt[n]{r}} = \frac{1+\sqrt[n]{r}+\cdots+(\sqrt[n]{r})^{n-1}}{1-r}$$

and

$$\frac{1}{1+\sqrt[n]{r}+\cdots+(\sqrt[n]{r})^{n-1}} = \frac{1-\sqrt[n]{r}}{1-r}.$$

The above two denominators are both polynomials with rational coefficients in variable $\sqrt[n]{r}$. This is what we call a *polynomial denominator*. Fractions with polynomial denominators will be the subject of this and the next section.

Since $(\sqrt[n]{r})^n = r$ is a rational number, powers greater than or equal to n of $\sqrt[n]{r}$ reduce to smaller powers. Then the most general polynomial denominator looks like

$$f(\sqrt[n]{r}) = a_0 + a_1\sqrt[n]{r} + a_2(\sqrt[n]{r})^2 + \cdots + a_{n-1}(\sqrt[n]{r})^{n-1},$$

for some rational numbers $a_0, a_1, \ldots, a_{n-1}, r$. Eventually multiplying by their common denominator, numbers $a_0, \ldots, a_{n-1}$ may be assumed integers. We shall see next that the reciprocal of any polynomial denominator is rationalizable to a polynomial denominator of the same kind, that is, for the same n and r.

Example 3. Suppose we are rationalizing the fraction $1/f$, for $f = 3-5\sqrt[3]{2}+\sqrt[3]{4}$. We look for a polynomial of the same form

$$g = a + b\sqrt[3]{2} + c\sqrt[3]{4}$$

that makes the product

$$\begin{aligned} fg &= (3-5\sqrt[3]{2}+\sqrt[3]{4})(a+b\sqrt[3]{2}+c\sqrt[3]{4}) \\ &= 3a + (3b-5a)\sqrt[3]{2} + (a-5b+3c)\sqrt[3]{4} + (b-5c)\sqrt[3]{8} + (c)\sqrt[3]{16} \\ &= 3a+2b-10c + (-5a+3b+2c)\sqrt[3]{2} + (a-5b+3c)\sqrt[3]{4} \end{aligned}$$

a rational number. This leads to a homogenous linear system

$$\begin{cases} a - 5b + 3c = 0 \\ -5a + 3b + 2c = 0 \end{cases}$$

of two equations in three unknowns having a nontrivial solution. Using one's favorite linear algebra method or software, one such solution is $a = 19/22, b = 17/22, c = 1$. This can be rescaled to integers as $a = 19, b = 17, c = 22$. Then $fg = 3a + 2b - 10c = 57 + 34 - 220 = -129$, and the desired rationalization is

$$\frac{1}{3 - 5\sqrt[3]{2} + \sqrt[3]{4}} = \frac{1}{f} = \frac{g}{fg} = \frac{19 + 17\sqrt[3]{2} + 22\sqrt[3]{4}}{-129}.$$

In general, given a polynomial denominator

$$f = a_0 + a_1\sqrt[n]{r} + a_2(\sqrt[n]{r})^2 + \cdots + a_{n-1}(\sqrt[n]{r})^{n-1},$$

we can construct a polynomial denominator of the same form

$$g = b_0 + b_1\sqrt[n]{r} + b_2(\sqrt[n]{r})^2 + \cdots + b_{n-1}(\sqrt[n]{r})^{n-1}$$

by requiring the product

$$\begin{aligned} fg = {} & a_0b_0 + (a_0b_1 + a_1b_0)\sqrt[n]{r} + (a_0b_2 + a_1b_1 + a_2b_0)(\sqrt[n]{r})^2 + \cdots \\ & + (a_0b_{n-1} + \cdots + a_{n-1}b_0)(\sqrt[n]{r})^{n-1} + (a_1b_{n-1} + \cdots + a_{n-1}b_1)r + \\ & (a_2b_{n-1} + \cdots + a_{n-1}b_2)r\sqrt[n]{r} + \cdots + a_{n-1}b_{n-1}r(\sqrt[n]{r})^{n-2} \end{aligned}$$

to be rational. This leads to zero coefficients for powers of $\sqrt[n]{r}$ that are not divisible by n. The resulting system of $n - 1$ homogenous linear equations in n unknowns $b_0, b_1, \ldots, b_{n-1}$ always has a nontrivial solution that can be rescaled to integers. This was the method of indeterminate coefficients for polynomial denominators.

This method can be adapted to work for linear combinations with rational coefficients of any order radicals of rational numbers. For example, given a denominator expression of the form

$$f = \sqrt{5} - 2\sqrt[5]{7},$$

we look for a rational conjugate g of the form

$$g = \sum_{i=0}^{1}\sum_{j=0}^{4} b_{ij}(\sqrt{5})^i(\sqrt[5]{7})^j.$$

The homogenous linear system implied by condition fg rational involves $2 \times 5 - 1 = 9$ equations in 10 unknowns that we leave as an exercise to the interested reader!

A rationalization formula for polynomial denominators

We have seen in the previous section that every polynomial denominator $f(\sqrt[n]{r})$ admits a rational conjugate $g(\sqrt[n]{r})$. In this section we produce the formula of g as a function of f. Looking at the two conjugates we have so far, $1 - \sqrt[n]{r}$ and $1 + \sqrt[n]{r} + \cdots + (\sqrt[n]{r})^{n-1}$, one is easy while the other is more complicated. In order to use this example to understand how rational conjugates can be computed, we have to go back to the original expansion that produced them. The roots of polynomial $x^n - 1$ are the nth complex roots of unity. They are given by

$$\omega_k = e^{2k\pi i/n} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad \text{for } k = 0, 1, \ldots, n-1.$$

$\omega = \omega_1$ is called a *primitive nth root of unity*, and $\omega_k = \omega^k$, for $k = 0, 1, \ldots, n-1$. Thus polynomial $x^n - 1$ factors as $x^n - 1 = (x-1)(x-\omega)\cdots(x-\omega^{n-1})$. Division of both sides by their constant coefficient $-1 = (-1)(-\omega)\cdots(-\omega^{n-1})$ and the fact that the reciprocals of all nth roots of unity are all nth roots of unity makes this factorization equivalent to

$$1 - x^n = (1-x)(1-\omega x)\cdots(1-\omega^{n-1}x).$$

When $x = \sqrt[n]{r}$, for r rational, and $f(x) = 1 - x$, this relation makes the product

$$f(\sqrt[n]{r})f(\omega\sqrt[n]{r})\cdots f(\omega^{n-1}\sqrt[n]{r}) = 1 - (\sqrt[n]{r})^n = 1 - r$$

a rational number. A rational conjugate of denominator $f(\sqrt[n]{r}) = 1 - \sqrt[n]{r}$ is then the product of the remaining factors

$$f(\omega\sqrt[n]{r})f(\omega^2\sqrt[n]{r})\cdots f(\omega^{n-1}\sqrt[n]{r}) = \prod_{j=1}^{n-1} f(\omega^j\sqrt[n]{r}).$$

We shall see that these formulas are true in general. The next theorem gives the formula for the rational conjugate of any polynomial denominator. This is equivalent to a rationalization formula for reciprocals of all polynomial denominators.

Theorem 2. *Consider the polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$ with rational coefficients, and let ω be a primitive nth root of* 1. *Then the polynomial*

$$P(x) := \prod_{j=0}^{n-1} f(\omega^j x)$$

of variable x is actually a polynomial over the rationals in variable x^n. In particular, the rationalization formula of $1/f(\sqrt[n]{r})$ *is*

$$\frac{1}{f(\sqrt[n]{r})} = \frac{\prod_{j=1}^{n-1} f(\omega^j\sqrt[n]{r})}{P(\sqrt[n]{r})}.$$

The proof of this theorem is given at the end of the next section. Until then, we further test it on two examples. The first one is easy, while the second gives the idea for the general proof.

Example 4. Consider the polynomial $f(x) = 1 + x + \cdots + x^{n-1} = (1-x^n)/(1-x)$, and compute the product

$$f(\sqrt[n]{r})f(\omega\sqrt[n]{r})\cdots f(\omega^{n-1}\sqrt[n]{r}) = \prod_{j=0}^{n-1}\frac{1-(\omega^j\sqrt[n]{r})^n}{1-\omega^j\sqrt[n]{r}} = \prod_{j=0}^{n-1}\frac{1-r}{1-\omega^j\sqrt[n]{r}}$$
$$= \frac{(1-r)^n}{\prod_{j=0}^{n-1}(1-\omega^j\sqrt[n]{r})} = \frac{(1-r)^n}{1-r} = (1-r)^{n-1}.$$

This being a rational number, Theorem 2 works for this particular f.

The method of proof used here reduces the result to the other known case, and based on this, it is not applicable to the general case proof. We need one more example.

Example 5. Suppose we are rationalizing the fraction of the last section

$$\frac{1}{3-5\sqrt[3]{2}+\sqrt[3]{4}}.$$

In this case, $f(x) = 3 - 5x + x^2$, $n = 3$, and ω is a primitive cubic root of unity. We compute the product

$$\begin{aligned}
f(\sqrt[3]{2})f(\omega\sqrt[3]{2})f(\omega^2\sqrt[3]{2}) &= (3-5\sqrt[3]{2}+\sqrt[3]{4})(3-5\omega\sqrt[3]{2}+\omega^2\sqrt[3]{4})(3-5\omega^2\sqrt[3]{2}+\omega^4\sqrt[3]{4})\\
&= 27 - 125\omega^3\cdot 2 + \omega^6\cdot 4 - 3^2\cdot 5(1+\omega+\omega^2)\sqrt[3]{2}\\
&\quad + 3^2(1+\omega^2+\omega^4)\sqrt[3]{4} + 3\cdot 5^2(1+\omega^2+\omega^4)\sqrt[3]{4}\\
&\quad + (3)(-5)(1)(\omega^5+\omega^4+\omega^2+\omega^4+\omega+\omega^2)\sqrt[3]{8}\\
&\quad + 3(\omega^2+\omega^4+\omega^6)\sqrt[3]{16} + 25(\omega^5+\omega^4+\omega^3)\sqrt[3]{16}\\
&\quad - 5(\omega^2+\omega^4+\omega^6)\sqrt[3]{32}
\end{aligned}$$

and note that all three-term parentheses vanish, based on $\omega^3 = 1$ and $1 + \omega + \omega^2 = 0$ and so the product reduces to the rational number $27 - 250 + 4 + 90 = -129$. A rational conjugate of $3 - 5\sqrt[3]{2} + \sqrt[3]{4}$ is then $(3 - 5\omega\sqrt[3]{2} + \omega^2\sqrt[3]{4})(3 - 5\omega^2\sqrt[3]{2} + \omega^4\sqrt[3]{4})$

$$\begin{aligned}
&= 9 - 15(\omega+\omega^2)\sqrt[3]{2} + [3(\omega^2+\omega^4)+25]\sqrt[3]{4} - 5(\omega^4+\omega^5)\sqrt[3]{8} + \sqrt[3]{16}\\
&= 9 - 15(-1)\sqrt[3]{2} + [3(-1)+25]\sqrt[3]{4} - 5(-1)2 + 2\sqrt[3]{2} = 19 + 17\sqrt[3]{2} + 22\sqrt[3]{4}.
\end{aligned}$$

The rationalization of the original fraction is the same as the one obtained earlier:

$$\frac{1}{3-5\sqrt[3]{2}+\sqrt[3]{4}} = \frac{19+17\sqrt[3]{2}+22\sqrt[3]{4}}{-129}. \tag{3}$$

In order to see how this miraculous vanishing process works and get a hint on how to proceed with the general proof, we replace numbers $1, \omega, \omega^2, \sqrt[3]{2}$ by variables y_1, y_2, y_3, x and redo the computation as follows:

$$\begin{aligned}
f(y_1x)f(y_2x)f(y_3x) &= (3-5y_1x+(y_1x)^2)(3-5y_2x+(y_2x)^2)(3-5y_3x+(y_3x)^2)\\
&= 27 - 125y_1y_2y_3x^3 + y_1^2y_2^2y_3^2x^6 - 3^2\cdot 5(y_1+y_2+y_3)x\\
&\quad + 3^2(y_1^2+y_2^2+y_3^2)x^2 + 3\cdot 5^2(y_1y_2+y_1y_3+y_2y_3)x^2\\
&\quad + (3)(-5)(1)(y_1^2y_2+y_1y_2^2+y_1^2y_3+y_1y_3^2+y_2^2y_3+y_2y_3^2)x^3\\
&\quad + 3(y_1^2y_2^2+y_1^2y_3^2+y_2^2y_3^2)x^4 + 25(y_1^2y_2y_3+y_1y_2^2y_3+y_1y_2y_3^2)x^4\\
&\quad - 5(y_1^2y_2^2y_3+y_1y_2^2y_3^2+y_1^2y_2y_3^2)x^5.
\end{aligned}$$

A polynomial $f(x_1, x_2, \ldots, x_n)$ is called *symmetric* if it remains invariant under any permutation of its indeterminates $x_1, x_2, \ldots, x_n$. This means

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n),$$

for any permutation σ of $\{1, \dots, n\}$. Basic properties of symmetric polynomials will be reviewed in the next section. For more, see [**2**], 4.5. On the last computation, the coefficients of powers of x are homogenous symmetric polynomials in $y_1, \dots, y_n$ of the same degree as the x-degree. When specializing to roots of unity, these coefficients become zero when their total y-degree is not a multiple of 3; and they turn into rational numbers, otherwise.

Symmetric polynomials and roots of unity

The last example highlighted a possible proof of Theorem 2 using symmetric polynomials and roots of unity. Before proceeding with such a proof, let's review some basic properties of symmetric polynomials and their specialization to roots of unity.

Viète's relations. French mathematician François Viète (1540–1603) observed in the late 1500's that if a degree n equation

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

written in its equivalent monic form

$$x^n + \frac{a_1}{a_0}x^{n-1} + \cdots + \frac{a_{n-1}}{a_0}x + \frac{a_n}{a_0} = 0$$

has n roots $y_1, y_2, \dots, y_n$, counting multiplicities, then the equation factors as

$$(x - y_1)(x - y_2) \cdots (x - y_n) = 0.$$

By expanding and collecting similar x-terms, this becomes

$$x^n - (y_1 + y_2 + \cdots + y_n)x^{n-1} + (y_1y_2 + \cdots + y_{n-1}y_n)x^{n-2} + \cdots + (-1)^n y_1y_2 \cdots y_n = 0.$$

Coefficient identification with the earlier monic equation yields what we now call Viète's relations or the relations between roots and coefficients of the given equation:

$$\begin{cases} e_1 = y_1 + y_2 + \cdots + y_n = -\dfrac{a_1}{a_0} \\ e_2 = \displaystyle\sum_{1 \le i < j \le n} y_iy_j = \dfrac{a_2}{a_0} \\ \qquad\qquad \vdots \\ e_n = y_1y_2 \cdots y_n = (-1)^n \dfrac{a_n}{a_0}. \end{cases}$$

The polynomials $e_1, \dots, e_n$ are called the elementary symmetric polynomials in the variables $y_1, \dots, y_n$. Note that e_i is the sum of all distinct products of i of the variables. When applied to the equation $x^n - 1 = 0$ whose roots are $1, \omega, \omega^2, \dots, \omega^{n-1}$, Viète's relations yield

$$e_j(1, \omega, \dots, \omega^{n-1}) = \begin{cases} 0, & \text{if } 1 \le j < n \\ (-1)^{n-1}, & \text{if } j = n. \end{cases}$$

Newton's relations. The subject of symmetric polynomials was considered in the late 1600's by English mathematician Isaac Newton (1642–1727) who looked at the polynomials

$$p_k = y_1^k + y_2^k + \cdots + y_n^k, \quad \text{for } k \geq 0.$$

He showed that $p_0 = n$, $p_1 = y_1 + y_2 + \cdots + y_n = e_1$, and $p_2 = y_1^2 + y_2^2 + \cdots + y_n^2 = (y_1 + y_2 + \cdots + y_n)^2 - 2(y_1 y_2 + \cdots + y_{n-1} y_n) = e_1^2 - 2e_2$, and so on, he gave the expressions of p_k, for small values of k. He also gave the recursive formulas

$$p_k = \begin{cases} e_1 p_{k-1} - e_2 p_{k-2} + \cdots + (-1)^{k-2} e_{k-1} p_1 + (-1)^{k-1} k e_k, & \text{if } k < n, \\ e_1 p_{k-1} - e_2 p_{k-2} + \cdots + (-1)^{n-1} e_n p_{k-n}, & \text{if } k \geq n, \end{cases}$$

better known as Newton's relations. In particular, all these can be used to show p_k is a polynomial in $e_1, \dots, e_n$ with integer coefficients. See [**2**], 4.5, Theorem 5.

Example 6. Suppose we want to compute the polynomial $p_4 = y_1^4 + y_2^4 + y_3^4$ for the cubic equation

$$2x^3 - 4x^2 + 2x + 3 = 0$$

with roots y_1, y_2, y_3, without actually solving the equation. Viète's relations imply that

$$\begin{aligned} e_1 &= y_1 + y_2 + y_3 = -\frac{-4}{2} = 2, \\ e_2 &= y_1 y_2 + y_1 y_3 + y_2 y_3 = \frac{2}{2} = 1, \\ e_3 &= y_1 y_2 y_3 = -\frac{3}{2}. \end{aligned}$$

We clearly have $p_0 = 3$, $p_1 = e_1 = 2$, and by Newton's relations

$$\begin{aligned} p_2 &= e_1 p_1 - 2e_2 = 4 - 2 = 2, \\ p_3 &= e_1 p_2 - e_2 p_1 + e_3 p_0 = 2 \cdot 2 - 1 \cdot 2 - \frac{3}{2} \cdot 3 = -\frac{5}{2}, \\ p_4 &= e_1 p_3 - e_2 p_2 + e_3 p_1 = 2 \cdot (-\frac{5}{2}) - 1 \cdot 2 + -\frac{3}{2} \cdot 2 = -10. \end{aligned}$$

The subject of symmetric polynomials today has a fundamental theorem which states that "every symmetric polynomial in $y_1, \dots, y_n$, say with rational coefficients, can be written as a polynomial with rational coefficients in $e_1, \dots, e_n$, the elementary symmetric polynomials." See [**2**], 4.5, Theorem 4.

Proof of Theorem 2. Let f be a general polynomial in variable x with rational coefficients. As we have seen in a previous example, in order to understand the nature of the cancellations leading to the proof that $\prod_{j=0}^{n-1} f(\omega^j \sqrt[n]{r})$ is a rational number, we better consider the polynomial

$$P(x; y_1, y_2, \dots, y_n) := \prod_{j=1}^{n} f(y_j x) = b_0 + b_1 x + \cdots + b_m x^m.$$

This is symmetric in $y_1, \dots, y_n$ and so are its coefficients b_j. The fundamental theorem of symmetric polynomials makes $b_j(y_1, \dots, y_n) = c_j(e_1, \dots, e_n)$, for some polynomial c_j in n indeterminates over the rationals. Moreover, by the definition of P, the y-degree of each monomial in P is equal to its x-degree, so the polynomials $b_j(y_1, \ldots, y_n)$ are homogenous of degree j. As we shall see later on, specialization of variables $y_1, \ldots, y_n$ to roots of unity $1, \omega, \ldots, \omega^{n-1}$ makes $e_1 = \cdots = e_{n-1} = 0$. It then makes sense to consider polynomials $d_j(e_n) = c_j(0, \ldots, 0, e_n)$ obtained from $b_j(y_1, \ldots, y_n) = c_j(e_1, \ldots, e_n)$ by sending variables $e_1, \ldots, e_{n-1}$ to zero. Since this assignment amounts to cancellation of monomials in a homogenous polynomial, $d_j(e_n)$ must be homogenous of degree j in $y_1, \ldots, y_n$, hence it is a monomial in e_n. In particular, $d_j(e_n) = 0$ whenever j is not a multiple of n.

Back to proving Theorem 2, we have

$$\begin{aligned} P(x) &= \prod_{i=0}^{n-1} f(\omega^i x) = P(x; 1, \omega, \ldots, \omega^{n-1}) = \sum_{j=0}^{m} b_j(1, \omega, \ldots, \omega^{n-1}) x^j \\ &= \sum_{j=0}^{m} c_j(e_1(1, \omega, \ldots, \omega^{n-1}), \ldots, e_n(1, \omega, \ldots, \omega^{n-1})) x^j \\ &= \sum_{j=0}^{m} c_j(0, \ldots, 0, (-1)^{n-1}) x^j = \sum_{j=0}^{m} d_j((-1)^{n-1}) x^j. \end{aligned}$$

By the comments at the end of previous paragraph, the last expression is a polynomial in x^n with rational coefficients. ■

Galois theory point of view

In its wider sense, Galois theory is the abstract theory of field extensions. It was invented around 1830 by French mathematician Evariste Galois (1811–1832) who did not live to see the fruits of his discovery. Shortly after his theory saw the light of day around 1840, it was employed to solve the famous construction problems of antiquity: trisection of the angle, duplication of the cube, squaring the circle, and the classification of constructible regular polygons. These were the longest lasting open problems in the history of mathematics. For more on these, see [**1**] or [**4**].

One basic principle of Galois theory is that "the product of all *conjugates* of a polynomial with *messy* coefficients is a polynomial in the same variables but with *nicer* coefficients." Our previous sections on square roots and the rationalization formula are based on this principle, and for this reason they should be considered as Galois theory regardless of the techniques we employed in there. Here are a couple of more Galois theory results that are useful when rationalizing denominators.

Reciprocals of algebraic numbers are rationalizable. Let α be a nonzero complex number that satisfies a polynomial equation with rational coefficients

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_m\alpha^m = 0,$$

where $a_m \neq 0$. Such number α is called an *algebraic number*. Eventually dividing by the nonzero term of smallest degree, we may assume that $a_0 = 1$. Further division by α makes the equation equivalent to

$$\frac{1}{\alpha} = -a_1 - a_2\alpha - \cdots - a_m\alpha^{m-1}. \tag{4}$$

This is the rationalization of $1/\alpha$. In other words, the rational conjugate of α is a polynomial in α of degree $m - 1$. Since in the original equation one can solve for α^m

as a linear combination of smaller powers of α, the set $\mathbf{Q}[\alpha]$ of all polynomials in α with rational coefficients is actually the set of all such polynomials of degree at most $m-1$. In particular, if α is a sum of radicals, α^{-1} can be expressed as a sum of radicals.

Example 7. Let $\alpha = \sqrt{2}+\sqrt{3}$. Passing $\sqrt{2}$ to the other side and squaring makes $\alpha^2 - 2\alpha\sqrt{2}+2 = 3$. Then $\sqrt{2} = (\alpha^2-1)/(2\alpha)$ and further squaring yields $2 = (\alpha^4 - 2\alpha^2+1)/(4\alpha^2)$. By clearing the denominator $4\alpha^2$, α satisfies the equation

$$1 - 10\alpha^2 + \alpha^4 = 0,$$

and consequently,

$$\frac{1}{\alpha} = 10\alpha - \alpha^3.$$

Checking that $10\alpha - \alpha^3 = \sqrt{3}-\sqrt{2}$ is an easy exercise left to the reader.

Radical expressions are algebraic. Let f be any polynomial of single variable over the rationals, and let α be an algebraic number. Then $f(\alpha)$ is an algebraic number, and in particular, $1/f(\alpha)$ is rationalizable by (4). Indeed, the powers of $f(\alpha)$ form an infinite subset

$$\{1, f(\alpha), f^2(\alpha), f^3(\alpha), \ldots\}$$

of the finite dimensional $\mathbf{Q}$-vector space $\mathbf{Q}[\alpha]$ which must be linearly dependent, say

$$b_0 + b_1 f(\alpha) + \cdots + b_s f^s(\alpha) = 0,$$

for some nonzero rational numbers $b_0, \ldots, b_s$. This makes $f(\alpha)$ an algebraic number.

In particular, since $\sqrt[n]{r}$ is algebraic, the reciprocal of any polynomial denominator

$$f(\sqrt[n]{r}) = a_0 + a_1(\sqrt[n]{r}) + a_2(\sqrt[n]{r})^2 + \cdots + a_{n-1}(\sqrt[n]{r})^{n-1},$$

for $r, a_0, a_1, \ldots, a_{n-1}$ rational numbers, is rationalizable.

Example 8. Let $f = 3 - 5\sqrt[3]{2} + \sqrt[3]{4}$ be the polynomial denominator studied before. We simplify its square

$$f^2 = 9 + 25\sqrt[3]{4} + \sqrt[3]{16} - 30\sqrt[3]{2} + 6\sqrt[3]{4} - 10\sqrt[3]{8} = -11 - 28\sqrt[3]{2} + 31\sqrt[3]{4},$$

and its cube

$$f^3 = f^2 \cdot f = (-11 - 28\sqrt[3]{2} + 31\sqrt[3]{4})(3 - 5\sqrt[3]{2} + \sqrt[3]{4}) = -399 + 33\sqrt[3]{2} + 222\sqrt[3]{4}.$$

By linear algebra, the four elements $1, f, f^2, f^3$ of the three-dimensional $\mathbf{Q}$-vector space $\mathbf{Q}[\sqrt[3]{2}]$ of standard basis $1, \sqrt[3]{2}, \sqrt[3]{4}$ must be linearly dependent. A nontrivial linear dependence relation

$$c_0 + c_1 f + c_2 f^2 + c_3 f^3 = 0$$

can be obtained either by ad hoc methods or by row reducing the augmented matrix

$$\left[\begin{array}{cccc|c} 1 & 3 & -11 & -399 & 0 \\ 0 & -5 & -28 & 33 & 0 \\ 0 & 1 & 31 & 222 & 0 \end{array}\right]$$

whose columns are the coordinate vectors of 1, f, f^2, f^3 relative to the standard basis. This matrix row reduces to

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & -129 & 0 \\ 0 & 1 & 0 & -57 & 0 \\ 0 & 0 & 1 & 9 & 0 \end{array}\right]$$

which corresponds to the system

$$\begin{cases} c_0 \qquad\qquad -129c_3 = 0, \\ \qquad c_1 \qquad\quad -57c_3 = 0, \\ \qquad\qquad c_2 \quad +9c_3 = 0. \end{cases}$$

Setting the independent variable $c_3 = 1$ yields unique values $c_0 = 129$, $c_1 = 57$, and $c_2 = -9$. Therefore, f satisfies the polynomial equation

$$129 + 57f - 9f^2 + f^3 = 0.$$

Division by $129f$ and solving for the first term gives the rationalization of $1/f$, by (4):

$$\frac{1}{f} = \frac{57 - 9f + f^2}{-129}.$$

The numerator of the last fraction is $57 - 9(3 - 5\sqrt[3]{2} + \sqrt[3]{4}) + (-11 - 28\sqrt[3]{2} + 31\sqrt[3]{4}) = 19 + 17\sqrt[3]{2} + 22\sqrt[3]{4}$. This method then produced the same rationalization (3) as the previous two methods of Examples 3 and 5.

For any complex number α, the set $\mathbf{Q}[\alpha]$ of all polynomials in α with rational coefficients is the smallest subring of $\mathbf{C}$ that contains both $\mathbf{Q}$ and α. The field of fractions $P(\alpha)/Q(\alpha)$ of elements of $\mathbf{Q}[\alpha]$ with nonzero denominator is denoted by $\mathbf{Q}(\alpha)$. This is the smallest subfield of $\mathbf{C}$ that contains both $\mathbf{Q}$ and α. We have seen that when α is algebraic, reciprocals of polynomials in α are rationalizable to polynomials in α, so $\mathbf{Q}[\alpha] = \mathbf{Q}(\alpha)$. See [**1**], 3.2, for this result over a general field.

Reciprocals of all radical expressions are rationalizable. Galois theory can be used to prove much more general results. One of these is the following.

Theorem 3. *The reciprocal of any radical expression over* **Q** *is rationalizable.*

This includes more complicated denominators like

$$3\sqrt{2} + \sqrt[3]{5} \text{ or } 1 + \sqrt[3]{\sqrt{2} + \sqrt{3}}.$$

The idea behind the proof is to view the radical expression as an iterated laying of new radicals on top of old ones, and attach to this process a chain rule of radical field extensions, starting with the rationals. Each time a new radical appears in the expression, we make a new larger field that is a simple radical extension of the old field. For example, the radical expression $3\sqrt{2} + \sqrt[3]{5}$ induces a tower of radical field extensions

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{2}, \sqrt[3]{5}),$$

and the expression $1 + \sqrt[3]{\sqrt{2} + \sqrt{3}}$ induces the tower

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt{2}, \sqrt{3}) \subset \mathbf{Q}(\sqrt{2}, \sqrt{3}, \sqrt[3]{\sqrt{2} + \sqrt{3}}).$$

In general, each radical expression α gives rise to a tower

$$\mathbf{Q} = F_0 \subset F_1 \subset \cdots \subset F_m$$

of simple radical field extensions $F_j \subset F_{j+1} = F_j(\sqrt[n]{t})$, for $t \in F_j$, such that $\alpha \in F_m$. Since each simple radical extension is finite dimensional over the smaller field (finite extension) and towering makes dimensions multiply up, the field extension $F_n \supset \mathbf{Q}$ is finite, hence algebraic. For this, see [**1**], 3.1. In particular, α is an algebraic number so by (4), its reciprocal is rationalizable and its rational conjugate is a polynomial in α.

A general method of finding rational conjugates. The towering process outlined above can be used as an iterated method of finding a polynomial equation with rational coefficients satisfied by a general radical expression α. By (4), this produces the rationalization of $1/\alpha$. To understand how this works, we use the same two examples we had before.

Example 9. Suppose $\alpha = 3\sqrt{2} + \sqrt[3]{5}$. We solve for the radical of the largest field extension

$$\alpha - 3\sqrt{2} = \sqrt[3]{5}$$

and cube both sides. The resulting expression, $(\alpha - 3\sqrt{2})^3 = 5$, expands to

$$\alpha^3 - 9\alpha^2\sqrt{2} + 54\alpha - 54\sqrt{2} = 5,$$

which is a polynomial equation in α with coefficients in the next smaller field $\mathbf{Q}(\sqrt{2})$. We continue by solving for the radical of this field extension

$$\frac{\alpha^3 + 54\alpha - 5}{9\alpha^2 + 54} = \sqrt{2}$$

and squaring both sides makes the result equivalent to a polynomial equation

$$(\alpha^3 + 54\alpha - 5)^2 - 2(9\alpha^2 + 54)^2 = 0.$$

This in turn yields the rationalization of $1/\alpha$, by (4).

Example 10. Suppose $\alpha = 1 + \sqrt[3]{\sqrt{2} + \sqrt{3}}$. Separating the radical of the last field extension, we have

$$\alpha - 1 = \sqrt[3]{\sqrt{2} + \sqrt{3}}$$

and cubing yields

$$(\alpha - 1)^3 = \sqrt{2} + \sqrt{3}.$$

Separating the radical of the next smaller extension makes $(\alpha - 1)^3 - \sqrt{2} = \sqrt{3}$, and squaring makes

$$(\alpha - 1)^6 - 2(\alpha - 1)^3\sqrt{2} + 2 = 3.$$

We further solve for the next radical

$$\frac{(\alpha - 1)^6 - 1}{2(\alpha - 1)^3} = \sqrt{2}$$

and squaring on both sides produces an equivalent polynomial equation

$$[(\alpha - 1)^6 - 1]^2 - 8(\alpha - 1)^6 = 0$$

satisfied by α over $\mathbf{Q}$. As usual, this will give the rationalization of $1/\alpha$, by (4).

Final remarks and conclusion

We end our essay on rationalizing denominators with three closing remarks and a summary of the methods.

A more general rationalization algorithm using prime numbers. It is not hard to modify the number theoretical algorithm to rationalize the denominator when it is a linear combination of square roots so that it can handle any sums/differences of higher order radicals of integers. Indeed, iterating the following four steps produces the desired rationalization.

1. Without loss of generality, all roots are nth roots.
2. Let p be a prime number occurring as a factor in some roots.
3. Write the denominator as $f = a_0 + a_1 p^{1/n} + \cdots + a_{n-1} p^{(n-1)/n}$, where each a_i is a sum/difference of radicals with no factors of p in its radicals.
4. Use the rationalization formula of Theorem 2 with the same polynomial P to get a fraction whose denominator $P(p^{1/n})$ is a radical expression with fewer prime numbers as factors in all its radicals.

Proof of the indeterminate coefficients method. The general method of indeterminate coefficients outlined previously is a consequence of Galois theory. Indeed, any finite sum/difference $f = \sum_i (\pm \sqrt[n_i]{a_i})$ of radicals of integers lives in the field $\mathbf{Q}(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \ldots)$ generated over $\mathbf{Q}$ by the individual summands, and so does $1/f$. As all radicals of integers are algebraic, the field they generate over $\mathbf{Q}$ equals the ring they generate over $\mathbf{Q}$. Then $1/f$ belongs to the polynomial ring $\mathbf{Q}[\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \ldots]$. In particular, it is a linear combination of monomials in variables $\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \ldots$, with appropriate degree bounds.

Rationalizing denominators and the norm of a field extension. The rationalization formulas for polynomial denominators or denominators that are sums of square roots are related to the notion of norm of a finite field extension. If f is an element of a finite field extension $L \supseteq K$ of basis $\mathcal{B} = \{x_1, \ldots, x_n\}$, then the *norm* of f is the number (element of K)

$$N_{L/K}(f) := \det(M),$$

where M is the matrix relative to $\mathcal{B}$ of the K-linear map $m_f : L \to L$ defined by $m_f(x) = fx$.

Example 11. If $f = 3 - 5\sqrt[3]{2} + \sqrt[3]{4}$ is an element of $\mathbf{Q}(\sqrt[3]{2}) \supset \mathbf{Q}$ of $\mathbf{Q}$-basis $\mathcal{B} = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$, then

$$\begin{aligned} m_f(1) &= 3 - 5\sqrt[3]{2} + \sqrt[3]{4}, \\ m_f(\sqrt[3]{2}) &= 2 + 3\sqrt[3]{2} - 5\sqrt[3]{4}, \\ m_f(\sqrt[3]{4}) &= -10 + 2\sqrt[3]{2} + 3\sqrt[3]{4}. \end{aligned}$$

Consequently,

$$M = \begin{bmatrix} 3 & 2 & -10 \\ -5 & 3 & 2 \\ 1 & -5 & 3 \end{bmatrix}$$

and

$$N_{\mathbf{Q}(\sqrt[3]{2})/\mathbf{Q}}(f) = \begin{vmatrix} 3 & 2 & -10 \\ -5 & 3 & 2 \\ 1 & -5 & 3 \end{vmatrix} = 27 - 250 + 4 + 30 + 30 + 30 = -129.$$

This is exactly the rationalized denominator of $1/f$ in (3), or the product of all conjugates of f by cubic roots of unity computed in Example 5.

Computing the norm $N_{\mathbf{Q}(\sqrt{2},\sqrt{5},\sqrt{11})/\mathbf{Q}}(f)$ for $f = \sqrt{2} + \sqrt{3} + \sqrt{11}$ of Example 2 is the last exercise left to the reader. For more on norms in field extensions, see [**1**], 8.3. For more on norms in ring extensions, see [**3**], 12.2.

Conclusion. We have presented three techniques to rationalize any denominator which is a sum of roots, and each gives a proof that any such denominator can indeed be rationalized. One can rationalize using prime factors; one can use indeterminate coefficients; or one can find a polynomial satisfied by the denominator.

Acknowledgment We would like to thank the referees for their support, careful reading, and generous suggestions for improvement.

REFERENCES

1. J. Howie, *Fields and Galois Theory*. Springer Undergraduate Mathematics Series, Springer-Verlag, London, 2006.
2. W. K. Nicholson, *Introduction to Abstract Algebra*. Third edition. John Wiley & Sons, Hoboken, NJ, 2007.
3. P. Ribenboim, *Classical Theory of Algebraic Numbers*. Springer-Verlag, New York, 2001.
4. J. Stillwell, *Elements of Algebra: Geometry, Numbers, Equations*. UTM, Springer-Verlag, New York, 2003.

Summary. We present several techniques for rationalizing the denominators of fractions which involve radical expressions of rational numbers. Our algorithms are based on prime numbers, indeterminate coefficients, symmetric polynomials, and Galois theory.

ALLAN BERELE (MR Author ID: 35020) received his Ph.D. from the University of Chicago under the direction of I. N. Herstein, with A. Regev of the Weizmann Institute as his unofficial adviser which is why his main interest is rings with polynomial identities.

STEFAN CATOIU (MR Author ID: 632038) received his Ph.D. from the University of Wisconsin-Madison under the direction of Donald S. Passman. His research interests include enveloping algebras, generalized and quantum differentiation, number theory, geometry, and elementary mathematics.

MAA100
MATHEMATICAL ASSOCIATION OF AMERICA
CELEBRATING A CENTURY OF ADVANCING MATHEMATICS

From the Files of Past MAGAZINE Editors
Paul Zorn 1996–2000

Paul Zorn on a memorable article during his tenure as editor of the MAGAZINE: "One of my very, very favorite pieces was an article by Vic Klee, a combination of geometry and set theory." V. Klee, J. R. Reay, A surprising but easily proved geometric decomposition theorem, *Math. Mag.* **71** no. 1 (1998) 3–11.

NOTES

Revelations and Generalizations of the Nine Card Problem

BREEANNE BAKER SWART
Department of Mathematics and Computer Science
The Citadel, The Military College of South Carolina
Charleston, SC 29409
breeanne.swart@citadel.edu

BRITTANY SHELTON
Albright College
Reading, PA 19612
bshelton@albright.edu

Want to see a card trick? Grab a deck of cards; we'll wait. The trick you are about to perform is known as the nine card problem and is credited to magician Jim Steinmeyer [**3**]. The authors first saw this trick performed by Justin Flom on The Ellen Degeneres Show.

Now that you have a deck of cards, pull out any nine cards. Suppose they are A♣2♦3♠4♥5♣6♦7♠8♥9♣ in this order. Stack (without reshuffling) the cards so that they are face down with the ace of clubs on the top and the nine of clubs on the bottom. Spell out the name of the card that started third from the left, "three of spades." That is,

1. Starting with the top card, spell out "three" by placing one card on the table for each letter. Each new card goes on top of the previous ones. Then place the stack of cards on the table at the bottom of the stack in your hand. The order of the cards is now 6♦7♠8♥9♣5♣4♥3♠2♦A♣ from top to bottom.
2. Do the same for "of." The order of the cards should be 8♥9♣5♣4♥3♠2♦A♣7♠6♦.
3. Repeat for "spades," and the order should be A♣7♠6♦2♦3♠4♥5♣9♣8♥.

To complete the trick, spell out "Ellen." Here's the kicker: Flip over the last card placed on the table to reveal 3♠!

You are now an amateur magician! To see this trick performed by a professional magician, watch Flom's performance at

http://www.ellentv.com/2013/01/04/card-trick-from-home/.

To add to the performance, audience members, each of whom had a different set of nine cards, performed the trick and "should have" revealed the card he or she spelled—"should have" because not all audience members were successful! In this paper, we use permutations to prove this claim and to generalize the trick.

An explanation of how this trick works as well as suggested ways to spice up its performance can be found in [**2**], where Mulcahy also includes an exercise for the

Math. Mag. **88** (2015) 137–143. doi:10.4169/math.mag.88.2.137. © Mathematical Association of America
MSC: Primary 05A05, Secondary 00A08.

reader to prove that the only card whose position is determinable is the third card from the left in a hand of nine cards.

Analysis of the trick

Call the card that starts in the third position from the left the flip card. A simple observation of the position of the flip card after each spelling helps to explain why the trick always works. After one spelling, the flip card will be in the third position from the bottom because when the face-value of every possible card is spelled out, it has at least three letters. The second spelling moves the flip card to the fifth position from the bottom, which is also the fifth position from the top, because "of" has two letters. After the third spelling, the flip card remains in the middle of the stack because each of the four suits has at least five letters. Thus, when the top five cards are placed on the table, the last card to be put on the table is the flip card.

The nine card problem can also be explained using permutations. Before doing so, we introduce some terminology to transition from card tricks to mathematics.

Definition 1. *A* shuffle of length *k is the act of placing k cards in reverse order at the bottom of the pile.*

For example, FIGURE 1 shows the original arrangement of a hand of nine cards and the arrangement of the cards after a shuffle of length three.

Each shuffle in the trick is associated to a word, and the length of the shuffle is the number of letters in this word. For example, the shuffle illustrated in Figure 1 is the shuffle associated to the word "ace." It is also the shuffle associated to "two," "six," and "ten" because these words all contain three letters. With this in mind, we construct equivalence classes that partition the set of possible words associated to shuffles. The equivalence classes for the set of possible first shuffles are {ace, two, six, ten}, {four, five, nine, jack, king}, and {three, seven, eight, queen}. There is a single equivalence class for the second shuffle, namely {of}. The equivalence classes for the set of possible third shuffles are {clubs}, {spades, hearts}, and {diamonds}.

Permutations of $[9] = \{1, 2, \ldots, 9\}$ can be used to describe the arrangements of the cards after each possible shuffle. The identity permutation, $12 \cdots 9$, represents the original arrangement of the cards in hand. Define the permutation $w = w_1 w_2 \cdots w_9$ representing the position of the cards after a shuffle by $w_i = j$ if the card originally in position j ends up in position i after the shuffle.

Observe that the shuffle illustrated in FIGURE 1 takes the original arrangement of ace, 2, 3, ..., 9 to the arrangement 4, 5, ..., 9, 3, 2, ace. Thus, the permutation 456789321 represents the arrangement of the cards after the shuffle associated to the

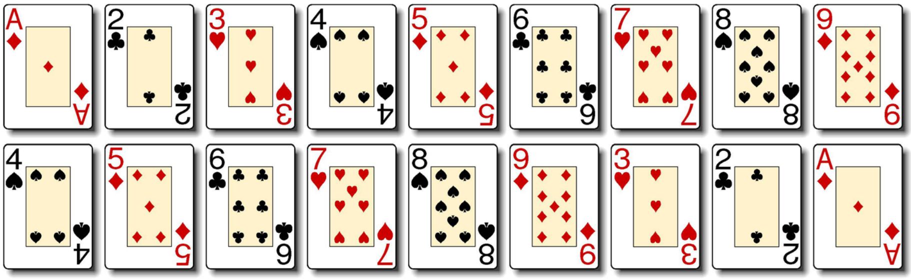


Figure 1 The bottom row shows the rearrangement of the cards in the top row after a shuffle of length three.

equivalence class {ace, two, six, ten}. The shuffles associated to {four, five, nine, jack, king}, {three, seven, eight, queen}, {of}, {clubs}, {spades, hearts}, and {diamonds} correspond to the permutations 567894321, 678954321, 345678921, 678954321, 789654321, and 987654321, respectively.

Successive shuffles can then be represented by composing permutations. The composition of permutation f with permutation g, $f \circ g$, represents the position of each card after shuffles f and g. Keeping in the spirit of composition of functions, we multiply these permutations from right to left. For example, the trick with ace of spades as the flip card is represented by the permutation $456789321 \cdot 345678921 \cdot 789654321 = 154239876$.

Since the card that starts in the third position needs to end in the fifth position for the magic trick to work, this card is not invariant under successive shuffles. In terms of permutations, this means that the permutations representing possible outcomes of the trick have 3 in the fifth position. Thus, neither 3 nor 5 is a fixed point in any of these permutations. However, since 3 is in the same position in each of these permutations, we call it a pseudo fixed point.

Definition 2. *Call $i \in [9]$ a* pseudo fixed point *if each permutation representing the arrangement of the cards after spelling out the name of a card contains i in the same position.*

Using this terminology, we can prove that the card trick always works.

Lemma 1. *For the nine card problem, 3 is the only pseudo fixed point.*

Proof. Notice that each of the permutations that represents a possible first shuffle is of the form $a_1a_2a_3a_4a_5a_6321$. Similarly, each permutation that represents a possible third shuffle is of the form $b_1b_2b_3b_454321$. Because "of" is represented by 345678921, it follows that

$$a_1a_2a_3a_4a_5a_6321 \cdot 345678921 \cdot b_1b_2b_3b_454321$$

represents the outcome of the trick with any first and third shuffles. The resulting permutation has 3 in the fifth position. Thus, 3 is a pseudo fixed point. Because each of the other positions of the resulting permutation depends on the a_i and b_j, the 3 in position 5 is the only pseudo fixed point. ■

In terms of the card trick, this says that the flip card, the card that starts in the third position, will always be in the fifth position after the third shuffle. Furthermore, the flip card is the only card whose position after all three shuffles is determinable.

Generalizations of the nine card problem

How does the trick change if the words associated to the shuffles are changed? Suppose we spelled out "math for life" instead of the name of a card. The corresponding permutation, 217653498, does not have 3 in position 5. This demonstrates that altering the lengths of the words associated to the shuffles can alter the pseudo fixed points.

First generalization Let's create a new trick by altering the lower bounds on the lengths of the first and third shuffles. Denote the lower bound on the length of the ith shuffle by l_i for $i \in \{1, 3\}$ and the fixed length of the second shuffle by l_2. In the nine card problem, $l_1 = 3$, $l_2 = 2$, and $l_3 = 5$. To further generalize the nine card problem, suppose n cards are held. Now permutations of $[n]$ will be used to represent the arrangement of the cards after each shuffle.

There is a necessary upper bound of n on the length of a shuffle because there are not enough cards to complete a longer shuffle. Furthermore, $l_i > 0$ for all i, otherwise there is no shuffle. Because shuffles of length $n-1$ and n are represented by the same permutation, we do not need to consider the case where $l_i = n$ for any i. Thus, l_1, l_2, and l_3 have values between 1 and $n-1$, inclusive.

The following propositions consider what conditions on the shuffle lengths are required to produce a pseudo fixed point. They also describe the pseudo fixed points in the permutations representing the final positions of the cards.

Proposition 1. *If there exists a pseudo fixed point when three shuffles are performed on n cards, then* $l_1 + l_2 + l_3 \geq n + 1$.

Proof. Suppose $l_1 + l_2 + l_3 \leq n$. After the first shuffle, 1 through l_1 will be in the rightmost l_1 positions in reverse numerical order. Since $l_1 + l_2 + l_3 \leq n$, it follows that $l_2 < n - l_1$. Thus, none of 1 through l_1 are in the leftmost l_2 positions. So after the second shuffle, 1 through l_1 will be in positions $n - l_2 - l_1 + 1$ through $n - l_2$ in reverse numerical order since the leftmost l_2 cards will move to the rightmost positions. Since l_3 is only a lower bound for the number of cards moved, after the third shuffle, the numbers in the $n - l_3$ leftmost positions are unknown. Positions $n - l_3 + 1$ through n contain the numbers from positions 1 through l_3 after the second shuffle, which depend on the length of the first shuffle. Therefore, the number in each position after the third shuffle cannot be determined and there are no pseudo fixed points.

Thus, for there to be a pseudo fixed point, $l_1 + l_2 + l_3 \geq n + 1$. ■

The conditions in Proposition 1 are both necessary and sufficient to determine the existence of a pseudo fixed point, as shown in Proposition 2.

Proposition 2. *If three shuffles are performed on n cards such that* $l_1 + l_2 + l_3 = n + s$, $s \geq 1$, *then the number of pseudo fixed points and their positions depend on the relationship between* l_1, l_2, l_3, *and* s. TABLE 1 *provides the five possible cases for the relationships between these variables, the resulting pseudo fixed points, and their positions.*

TABLE 1: This table summarizes the pseudo fixed points and their positions for the generalized nine card problem.

	$\min\{l_1, l_3, s\}$	Additional Restriction	Pseudo fixed points	Respective positions
1	l_1	$l_2 \leq n - l_1$	$1, 2, \ldots, l_1$	$l_2 + 1, l_2 + 2, \ldots, l_2 + l_1$
2	l_1	$l_2 > n - l_1$	$1, 2, \ldots, l_1$	$l_2 + 1, l_2 + 2, \ldots, n,$ $l_2, l_2 - 1, \ldots, n - l_1 + 1$
3	l_3	$l_3 > n - l_2$	$1, 2, \ldots, l_3$	$l_2 + 1, l_2 + 2, \ldots, n,$ $l_2, l_2 - 1, \ldots, n - l_3 + 1$
4	l_3	$l_3 \leq n - l_2$	$l_1 - s + 1, l_1 - s + 2,$ $\ldots, n - l_2$	$n - l_3 + 1, \ldots,$ $n - 1, n$
5	s		$l_1 - s + 1, \ldots, l_1$	$l_1 + l_2 - s + 1, \ldots, l_1 + l_2$

Since the same methodology is used to prove each of the five cases, we provide only the proof of case 1. To challenge yourself, try proving cases 2 through 5, then compare to the proofs provided in the supplement [**4**]. Although case 5 does not have an additional condition, the proof still has the same structure as the others.

Proof. Case 1: Suppose $l_2 \leq n - l_1$ and $\min\{l_1, l_3, s\} = l_1$. The permutation after the first shuffle is

$$a_1 a_2 \cdots a_{n-l_1} l_1 \cdots 21$$

where $a_1, \ldots, a_{n-l_1}$ are the numbers $l_1 + 1, \ldots, n$. Since l_1 is only a lower bound for the length of the first shuffle, the arrangement of $l_1 + 1$ through n depends on the actual length of the shuffle performed. The second shuffle moves a_1 through a_{l_2}, the l_2 leftmost numbers after the first shuffle, to the rightmost positions. Furthermore, now 1 through l_1 will be in positions $n - l_2$ through $n - l_1 - l_2$, respectively. Therefore, the permutation after two shuffles is

$$a_{l_2+1} \cdots a_{n-l_1} l_1 \cdots 21 a_{l_2} \cdots a_2 a_1.$$

The third shuffle then moves a_{l_2+1} through a_{n-l_1}, 1 through l_1, and a_{l_2} through $a_{l_2-(s-l_1)+1}$, the leftmost l_3 numbers after the second shuffle, to the rightmost positions. Thus, the permutation after three shuffles is

$$c_1 c_2 \cdots c_{n-l_3} a_{l_2-(s-l_1)+1} \cdots a_{l_2} 12 \cdots l_1 a_{n-l_1} \cdots a_{l_2+1}$$

where c_1 through c_{n-l_3} depend on the actual length of the shuffle performed. Therefore, 1 through l_1 are pseudo fixed points and will occur in positions $n - (l_3 - s) - l_1 + 1$ through $n - (l_3 - s)$, respectively, or $l_2 + 1$ through $l_1 + l_2$, respectively. ■

The trick cannot have more than l_1 pseudo fixed points because the cards in the first $n - l_1$ positions are unknown after the first shuffle. Similarly, since the cards in the first $n - l_3$ positions of the arrangement after the third shuffle are unknown, the trick cannot have more than l_3 pseudo fixed points.

Furthermore, a trick cannot have more than $s = n - (l_1 + l_2 + l_3)$ pseudo fixed points because the cards must work their way through the hand and return to the bottom of the stack throughout the three shuffles, which will not occur unless the shuffles have total length more than n.

Corollary 1. *If three shuffles are performed on n cards such that* $l_1 + l_2 + l_3 = n + s$, $s \geq 1$, *there will be* $\min\{l_1, l_3, s\}$ *pseudo fixed points.*

Second generalization The second shuffle in the nine card problem has a fixed length of two. To further generalize, let's consider what happens if the length of the second shuffle can vary just as the first and third shuffles vary. Pseudo fixed points can still occur; however, the conditions that guarantee pseudo fixed points will be different.

Again, $l_i > 0$ for all i and the length of every shuffle has an upper bound of n.

For this generalization, we do not consider the case where $l_i = n - 1$ for any i because the results are the same as when $l_i = n$. Thus, l_1, l_2, and l_3 have values 1 through $n - 2$ inclusive and n.

In order to guarantee that the position of at least one card is determinable, the shuffles must be sufficiently long enough to cycle the cards through the stack. Specifically, $\min\{l_1, l_3\} + l_2$ must be at least $n + 1$ as shown in Proposition 3.

Proposition 3. *If there exists a pseudo fixed point when three shuffles are performed on n cards, then* $\min\{l_1, l_3\} + l_2 \geq n + 1$.

Proof. Suppose $\min\{l_1, l_3\} + l_2 \leq n$. If $\min\{l_1, l_3\} = l_1$, then $l_1 + l_2 \leq n$. The first shuffle will move the leftmost l_1 numbers to the rightmost positions, and the permutation after one shuffle is

$$a_1 a_2 \cdots a_{n-l_1} l_1 \cdots 21$$

where $a_1, \ldots, a_{n-l_1}$ are the numbers $l_1 + 1, \ldots, n$ in an unknown order. Since their order is unknown, $l_1 + 1$ through n cannot be pseudo fixed points.

Since $l_1 + l_2 \leq n$, it follows that $l_2 \leq n - l_1$, and so a_1 , $a_2, \ldots, a_{l_2}$ are moved to the rightmost l_2 positions in reverse order. However, since l_2 is only a lower bound for the length of the second shuffle, 1 through l_1 may or may not be moved to reverse order by the second shuffle. Thus, the positions of 1 through l_1 are also unknown after the second shuffle. So there will not be any pseudo fixed points.

Similarly, if $\min\{l_1, l_3\} = l_3$, then $l_3 + l_2 \leq n$ and no numbers have a determinable position in the permutation representing the composition of the second and third shuffles. Therefore, if a pseudo fixed point exists, then $\min\{l_1, l_3\} + l_2 \geq n + 1$. ■

In addition, the difference between the sum of the lower bounds on two consecutive shuffles (first and second or second and third) and the number of cards determines the number of pseudo fixed points.

Proposition 4. *If* $\min\{l_1, l_3\} + l_2 \geq n + 1$, *then there are* $s = \min\{l_1, l_3\} + l_2 - n$ *pseudo fixed points. Furthermore,* $\min\{l_1, l_3\} - s + 1$ *through* $\min\{l_1, l_3\}$ *are the pseudo fixed points, and they occur in positions* l_2 *through* $l_2 - s + 1$, *respectively.*

Proof. Suppose $\min\{l_1, l_3\} + l_2 \geq n + 1$. Let $s = \min\{l_1, l_3\} + l_2 - n \geq 1$.

The first shuffle moves the leftmost l_1 numbers to the rightmost positions, and the permutation after one shuffle is

$$a_1 a_2 \cdots a_{n-l_1} l_1 \cdots 21$$

where $a_1, \ldots, a_{n-l_1}$ are the numbers $l_1 + 1, \ldots, n$ in an unknown order.

The second shuffle moves the leftmost l_2 numbers to the rightmost positions. Therefore, the permutation after two shuffles is

$$b_1 b_2 \cdots b_{n-l_2} (n - l_2 + 1) \cdots l_1 a_{n-l_1} \cdots a_2 a_1$$

where $b_1, \ldots, b_{n-l_2}$ are $1, \ldots, n - l_2$ in an unknown order.

The third shuffle moves the leftmost l_3 numbers to the rightmost positions. The minimum of l_1 and l_3 determines which numbers are in these l_3 leftmost positions.

Case 1: If $\min\{l_1, l_3\} = l_1$, then $n - l_2 + 1 = l_1 - s + 1$ and $n - l_2 + s = l_1 \leq l_3$. In this case, the leftmost l_3 numbers include b_1 through b_{n-l_2}, $n - l_2 + 1 = l_1 - s + 1$ through l_1, and a_{n-l_1} through a_{n-l_3+1}. Therefore, the permutation after three shuffles is

$$c_1 c_2 \cdots c_{n-l_3} a_{n-l_3+1} \cdots a_{n-l_1} l_1 \cdots (l_1 - s + 1) b_{n-l_2} \cdots b_2 b_1$$

where $c_1, \ldots, c_{n-l_3}$ depend on the actual length of the third shuffle. Thus, $l_1 - s + 1$ through l_1 are pseudo fixed points and occur in positions l_2 through $l_2 - s + 1$, respectively.

Case 2: If $\min\{l_1, l_3\} = l_3$, then $n - l_2 = l_3 - s$. In this case, the leftmost l_3 numbers include b_1 through b_{n-l_2} and $n - l_2 + 1$ through l_3. Therefore, the permutation after three shuffles is

$$c_1 c_2 \cdots c_{n-l_3} l_3 \cdots (n - l_2 + 1) b_{n-l_2} \cdots b_2 b_1$$

where $c_1, \ldots, c_{n-l_3}$ are $l_3 + 1, \ldots, n$ in an unknown order. Thus, $n - l_2 + 1 = l_3 - s + 1$ through l_3 are pseudo fixed points and occur in positions l_2 through $l_2 - s + 1$, respectively. ■

Conclusion

The pseudo fixed points in the permutation associated to the final positions of the cards represent the cards whose positions are determinable after three shuffles. Since 3 is not the only pseudo fixed point in the generalized tricks, the flip card does not have to be the third card from the left. This opens the door to a whole new set of card tricks that you can perform to impress your friends and colleagues.

With the above propositions in hand, we can now return to the exercise posed by Mulcahy in [**2**], which is to show that with n cards, if the card starting in position s always finishes in position t when the words associated to the three shuffles are the three words in the name of a playing card, then $n = 9$, $s = 3$, and $t = 5$. Lemma 1 proves that when nine cards are used, $n = 9$, then necessarily $s = 3$ and $t = 5$.

However, nine is not the only value of n for which the position of a flip card is determinable. By Proposition 1, the number of cards n must be at most nine in order to have a pseudo fixed point because $n < l_1 + l_2 + l_3 = 10$. Since the longest shuffle is of length eight (the shuffle associated to "diamonds"), there must be at least eight cards in hand. Any other construction of such a trick must have $n = 8$. By Proposition 2 Case 5, when $n = 8$, then 2 and 3 are pseudo fixed points that appear in positions 4 and 5, respectively. Thus, $n = 9$, $s = 3$, $t = 5$ is not the only construction of the trick!

REFERENCES

1. ”Card trick from home!,” Jan. 4, 2013. Produced by Ellen Degeneres. Perf. Ellen Degeneres and Justin Flom. *The Ellen Degeneres Show.* WAD Productions, Inc. Television.
2. C. Mulcahy, Card Colm (2009), `http://www.maa.org/community/maa-columns/past-columns-card-colm/esteem-synergism.`
3. J. Steinmeyer, The nine card problem, *MAGIC* (May 1993) 56–57.
4. B. B. Swart, B. Shelton, Revelations and generalizations of the nine card problem, *Math. Mag.* **88** no. 2 (2015), `www.maa.org/mathmag/supplements.`

Summary. The nine card problem is a magic trick performed by shuffling nine playing cards according to a set of rules. The magic is that a particular card will always reappear. The success of this trick can be easily explained by considering the lengths of the words in the names of playing cards, which define the shuffling rules. In this paper, we use permutations to prove that the trick will always work. We then use this methodology to generalize the trick to any number of cards with shuffles according to different rules.

BREEANNE BAKER SWART (MR Author ID: 1093737) is an assistant professor of mathematics at The Citadel in Charleston, SC. She received her Ph.D. from Lehigh University under the direction of Garth Isaak. Her research interests include graph theory, combinatorics, and number theory.

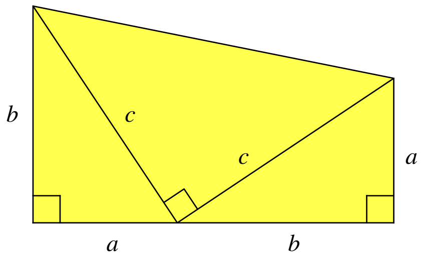
BRITTANY SHELTON (MR Author ID: 960329) is an assistant professor of mathematics at Albright College. She earned a B.S. from Montclair State University and a Ph.D. from Lehigh University. Her mathematical interests include algebraic and enumerative combinatorics. She has recently developed an interest in incorporating magic tricks, including this one, into the classroom.

Proof Without Words: President Garfield and the Cauchy–Schwarz Inequality

CLAUDI ALSINA
Universitat Politècnica de Catalunya
Barcelona, Spain
claudio.alsina@upc.edu

ROGER B. NELSEN
Lewis & Clark College
Portland, OR
nelsen@lclark.edu

It is well known (see, for example, [1]) that James A. Garfield, the twentieth President of the United States, published a proof of the Pythagorean theorem in 1876, five years before he became President. His proof is based on the yellow trapezoid below, and proceeds by computing its area in two different ways.

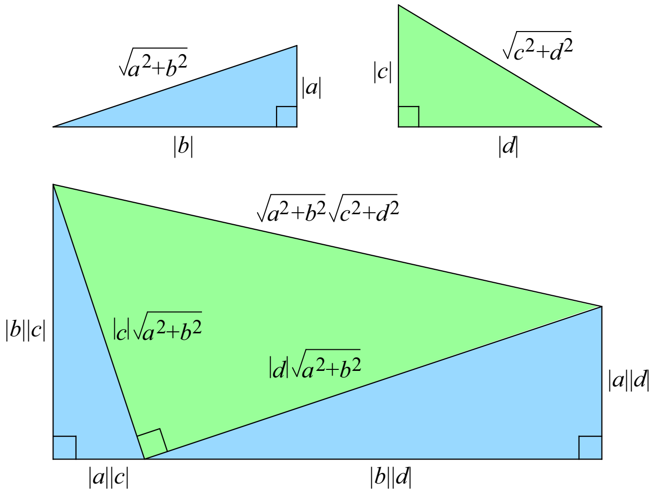


Although there is absolutely no evidence that he did so, Garfield could have used another trapezoid consisting of three right triangles to prove wordlessly the two-dimensional version of the Cauchy–Schwarz inequality.

Theorem. *For real numbers a, b, c, and d,*

$$|ac+bd| \leqslant \sqrt{a^2+b^2}\sqrt{c^2+d^2}.$$

Proof.



$$|ac+bd| \leqslant |a|\,|c|+|b|\,|d| \leqslant \sqrt{a^2+b^2}\sqrt{c^2+d^2}. \qquad \blacksquare$$

Math. Mag. **88** (2015) 144–145. doi:10.4169/math.mag.88.2.144. © Mathematical Association of America
MSC: Primary 97H30; 26D15.

REFERENCE

1. H. Eves, *Great Moments in Mathematics* (*Before* 1650). Mathematical Association of America, Washington, 1980.

Summary. We prove wordlessly the Cauchy–Schwarz inequality (for $n = 2$) using a trapezoid partitioned into three right triangles.

CLAUDI ALSINA (MR Author ID: 25110) is professor of mathematics at Universitat Politècnica of Catalunya–Barcelona Tech.

ROGER B. NELSEN (MR Author ID: 237909) is professor emeritus at Lewis & Clark College, where he taught mathematics and statistics for forty years.

MAA100
MATHEMATICAL ASSOCIATION OF AMERICA
CELEBRATING A CENTURY OF ADVANCING MATHEMATICS

From the Files of Past MAGAZINE Editors J. Arthur Seebach and Lynn Arthur Steen 1976–1980

Lynn Steen's favorite articles in the MAGAZINE during his tenure as co-editor were by P. Halmos, Logic from A to G, *Math. Mag.* **50** no. 1 (1977) 5–11 and V. Klee, Some unsolved problems in plane geometry, *Math. Mag.* **52** no. 3 (1979) 131–145.

MAA100
MATHEMATICAL ASSOCIATION OF AMERICA
CELEBRATING A CENTURY OF ADVANCING MATHEMATICS

From the Files of Past MAGAZINE Editors J. Arthur Seebach and Lynn Arthur Steen 1976–1980

When Lynn Arthur Steen (LAS) and J. Arthur Seebach, Jr. (AS) were co-editors of the MAGAZINE, submissions were sent via post and were typewritten manuscripts. When an article was accepted, LAS and AS would mark changes on the typewritten manuscript and then LAS, AS, and the author would receive a typeset version. All would read the manuscript and look for corrections. Because corrections were coming from several different directions at the same time, sometimes they were mixed up, like the time the word "number" was used when "integer" would have been correct. One person said "insert 'whole before 'number'," another said "change 'number' to 'integer'," both changes were made resulting in "whole integer."

Mutually Tangent Spheres in *n*-Space

OWEN D. BYER
Eastern Mennonite University
Harrisonburg, VA 22802
byer@emu.edu

DEIRDRE L. SMELTZER
Eastern Mennonite University
Harrisonburg, VA 22802
smeltzed@emu.edu

It is well known that given three mutually tangent circles in the plane, the three points of tangency lie on a generalized circle (an actual circle or a line) that is orthogonal to the original three and tangent to the segments between the centers of any two of the circles (see FIGURE 1). In this note we extend the result to higher dimensions, using the term "generalized sphere" in n-dimensional space to refer to an actual sphere or an $(n-1)$-dimensional hyperplane.

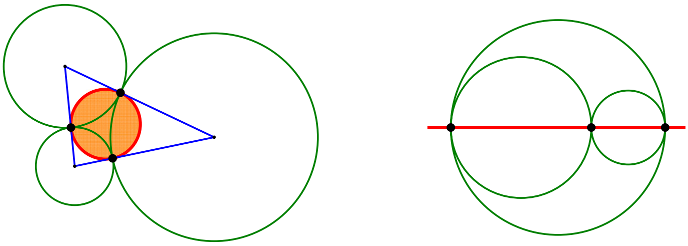


Figure 1 Two possible configurations of three mutually tangent circles

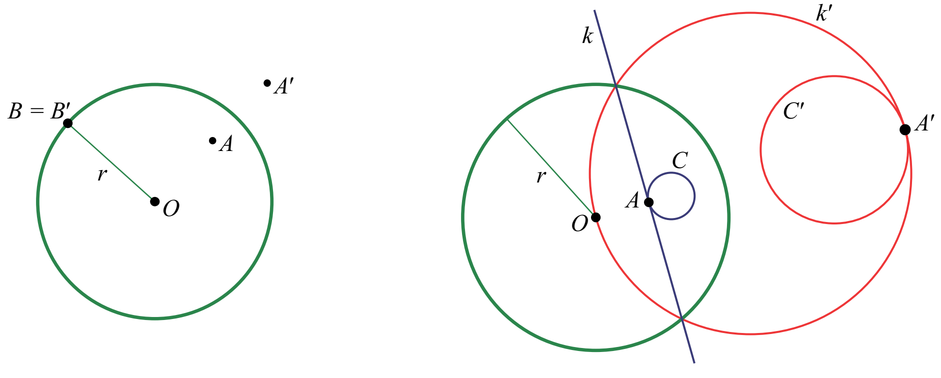
Theorem. *The points of tangency of $n+1$ mutually tangent spheres in n-dimensional space lie on a generalized sphere. This sphere is orthogonal to the other spheres and tangent to the segments joining their centers.*

To prove the statement, we employ the method of inversions, a powerful tool for proving statements involving tangency, collinearity, and cocyclicity. While inversions are most often considered with respect to a circle in a plane, the following definition is actually valid in n-dimensional space.

Definition. *Let O be a fixed point (center) and $r > 0$ a fixed number (radius). The inversion $I = I_{O,r}$ maps every point $A \neq O$ onto a point $A' = I(A)$ such that A is on the ray OA and $OA \cdot OA' = r^2$.*

A quick review of properties of inversions is in order. From the definition, we see that $I_{O,r}$ is a transformation of the points of any extended n-dimensional space (including the point at ∞, if we view O as being mapped to ∞). FIGURE 2(a) shows the images of points A and B under the inversion $I_{O,r}$ in the plane. More generally, we define the image of a set of points X as $I(X) = \{I(x) : x \in X\}$. The following properties regarding the images of special sets under inversion in n-space correspond to and are consequences of the results for inversion in a plane (some of which are illustrated in FIGURE 2(b)). Proofs for the 2-dimensional case can be found in [**1**], [**3**], or [**4**].

Math. Mag. **88** (2015) 146–150. doi:10.4169/math.mag.88.2.146. © Mathematical Association of America
MSC: Primary 51M04.



(a) (b)

Figure 2 Depictions of inversion with respect to a circle

- If Π is a hyperplane containing O, then $I(\Pi) = \Pi$.
- If Π is an $(n-1)$-dimensional hyperplane not containing O, then $I(\Pi) = \Pi'$ is a sphere containing O.
- If $\mathcal{S}$ is a sphere containing O, then $I(\mathcal{S}) = \mathcal{S}'$ is an $(n-1)$-dimensional hyperplane not containing O.
- If $\mathcal{S}$ is a sphere not containing O, then $I(\mathcal{S}) = \mathcal{S}'$ is a sphere not containing O.
- The measure of the angle between any two intersecting generalized spheres in n-space is invariant under inversion. In particular, points of tangency are preserved.

The above properties suggest that inversions blur the distinction between (hyper)planes and spheres. As such, an inversion can be used to transform a given configuration into one in which these objects are interchanged, often resulting in symmetry that makes statements easier to prove.

Proof of Theorem. It is not too hard to see that if the points of tangency are not distinct, then all the spheres meet at one common point and the result is trivial. The more interesting case is when there are $\binom{n+1}{2}$ distinct points of tangency, and that is the situation we now consider.

Let O be the point of tangency between two of the spheres, say $\mathcal{S}_1$ and $\mathcal{S}_2$, and consider an inversion $I_{O,r}$. Then $I(\mathcal{S}_1) = \mathcal{S}_1'$ and $I(\mathcal{S}_2) = \mathcal{S}_2'$ intersect only at $I(O)$, the point at ∞; thus $\mathcal{S}_1'$ and $\mathcal{S}_2'$ are parallel $(n-1)$-dimensional hyperplanes. Since the remaining spheres $\mathcal{S}_3, \ldots, \mathcal{S}_{n+1}$ are tangent to each other but do not contain O, their images, $\mathcal{S}_3', \ldots, \mathcal{S}_{n+1}'$ are tangent spheres that are also tangent to both of the parallel hyperplanes $\mathcal{S}_1'$ and $\mathcal{S}_2'$. Therefore, $\mathcal{S}_3', \ldots, \mathcal{S}_{n+1}'$ are congruent, mutually tangent spheres with centers $O_3, \ldots, O_{n+1}$ (as shown in FIGURE 3, for $n = 3$).

In n-dimensional Euclidean space, the set $\{\overrightarrow{O_3O_4}, \ldots, \overrightarrow{O_3O_{n+1}}\}$ spans a k-dimensional hyperplane $\mathcal{H}$, where $k \le n-2$. (Actually, the set forms a basis and $k = n-2$, but since we omit the proof that the vectors $\overrightarrow{O_3O_i}$ are linearly independent, we limit ourselves to the stated weaker result, which is sufficient.) Since $\overrightarrow{O_iO_j} = \overrightarrow{O_iO_3} + \overrightarrow{O_3O_j}$ for $3 \le j \le n+1$, $\mathcal{H}$ contains all lines $\overleftrightarrow{O_iO_j}$. Note that $\mathcal{H}$ lies in the $(n-1)$-dimensional hyperplane that is parallel to and equidistant from $\mathcal{S}_1'$ and $\mathcal{S}_2'$.

Let $M_{i,j}$ be the point of tangency of $\mathcal{S}_i'$ and $\mathcal{S}_j'$, $1 \le i < j \le n+1$. Then for $i \ge 3$, since $M_{i,j}$ is the midpoint of $\overline{O_iO_j}$, $M_{i,j} \in \mathcal{H}$. By definition, for $3 \le j \le n+1$, $M_{1,j}$ and $M_{2,j}$ are the points of tangency of $\mathcal{S}_j'$ with the hyperplanes $\mathcal{S}_1'$ and $\mathcal{S}_2'$, respectively. Since $\mathcal{S}_1'$ and $\mathcal{S}_2'$ are parallel hyperplanes orthogonal to each of the other $\mathcal{S}_j'$, we conclude that the points $M_{1,j}$, O_j, and $M_{2,j}$ are collinear (for $3 \le j \le n+1$) and the $n-1$ lines formed by these triples are parallel.

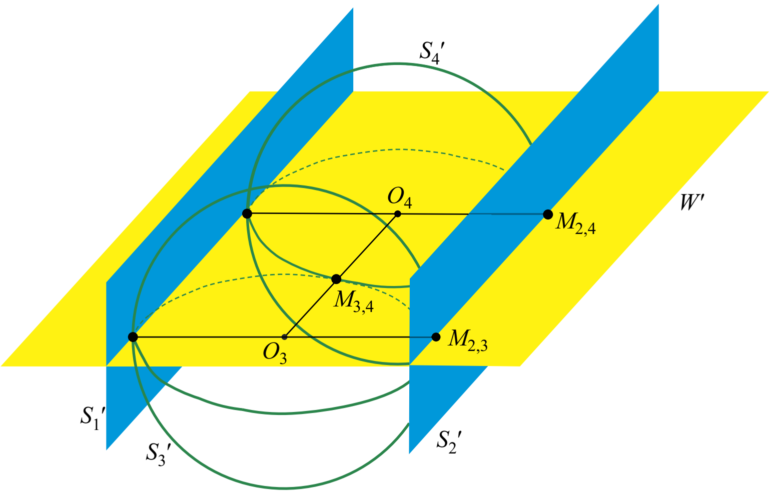


Figure 3 Inversive image of four tangent 3-spheres

Let $\mathcal{B}$ be a set of basis vectors for the subspace $\mathcal{H}$. Now form the span of $\mathcal{B} \cup \{\overrightarrow{M_{1,3}M_{2,3}}\}$. The result lies in an $(n-1)$-dimensional hyperplane $\mathcal{W}'$, containing each of the $\overleftrightarrow{M_{1,j}M_{2,j}}$ for $3 \leq j \leq n+1$ (since they are parallel) and therefore all of the mutual points of tangency of $\mathcal{S}_1', \mathcal{S}_2', \ldots, \mathcal{S}_{n+1}'$. Note that since $\mathcal{S}_1'$ and $\mathcal{S}_2'$ are parallel, they may be viewed as meeting at the point at ∞, a point which lies on all hyperplanes, including $\mathcal{W}'$.

Clearly $\mathcal{W}'$ is orthogonal to $\mathcal{S}_1'$ and $\mathcal{S}_2'$, because $\mathcal{W}'$ contains $\overleftrightarrow{M_{1,3}M_{2,3}}$, which is orthogonal to both $\mathcal{S}_1'$ and $\mathcal{S}_2'$. In addition, $\mathcal{W}'$ is orthogonal to sphere $\mathcal{S}_j'$ for $3 \leq j \leq n+1$, because $\mathcal{W}'$ passes through O_j, the center of $\mathcal{S}_j'$.

Therefore, $\mathcal{W}$, the preimage of $\mathcal{W}'$, is a generalized sphere containing all the points of tangency of the $\mathcal{S}_i$. Furthermore, since angle measures between intersecting spheres are preserved, $\mathcal{W}$ is orthogonal to each of the $\mathcal{S}_i$. Note that $\mathcal{W}$ is an $(n-1)$-dimensional hyperplane (rather than an actual sphere) if and only if the centers of the original spheres are co-hyperplanar.

It remains to show that $\mathcal{W}$ is tangent to each line passing through the centers of two of the original spheres. To this end, let $l_{i,j}$ be the line through the centers of the spheres $\mathcal{S}_i$ and $\mathcal{S}_j$. Note that $l_{i,j}$ is orthogonal to the two spheres. We consider two cases.

When $(i, j) \neq (1, 2)$, the image of $l_{i,j}$ is a circle orthogonal to $\mathcal{S}_i'$ and $\mathcal{S}_j'$ at $M_{i,j}$. Then, since $\mathcal{W}'$ is also orthogonal to $\mathcal{S}_i'$ and $\mathcal{S}_j'$ at $M_{i,j}$, $I(l_{i,j})$ is tangent to $\mathcal{W}'$ at $M_{i,j}$. Therefore, $l_{i,j}$ is tangent to $\mathcal{W}$.

For the second case, let l be the line through the centers of spheres $\mathcal{S}_1$ and $\mathcal{S}_2$. It contains O, the center of our inversion, so $I(l)$ is a line, which is orthogonal to $\mathcal{S}_1'$ and $\mathcal{S}_2'$. Since $\mathcal{W}'$ is also orthogonal to $\mathcal{S}_1'$ and $\mathcal{S}_2'$, and $I(l)$ does not lie in $\mathcal{W}'$ (else the points of l would be a subset of the sphere $\mathcal{W}$), we see that $I(l)$ and $\mathcal{W}'$ do not meet in Euclidean space. (They could be viewed as meeting at the point at ∞.) Therefore, l and $\mathcal{W}$ meet only at O, which means l is tangent to $\mathcal{W}$. ■

Perhaps the most recognizable instance of the theorem occurs when $n = 3$ and the four initial spheres have noncoplanar centers. Then,

$\mathcal{W}$ is a sphere orthogonal to each of the four given spheres, passing through their six points of mutual tangency. Moreover, $\mathcal{W}$ is the **midsphere** *of the tetrahedron whose*

vertices are the centers of the four spheres, because it is tangent to each edge of the tetrahedron. (See FIGURE 4.)

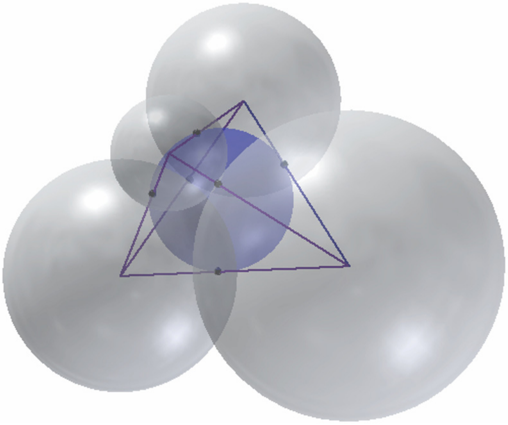


Figure 4 Configuration with $n = 3$

For Coxeter's ninetieth birthday, the Australian artist John Robinson presented him with a sculpture (called *Firmament*) consisting of five mutually tangent spheres made from wooden and steel balls. In [**2**], Coxeter discusses the construction of five mutually tangent spheres, stating and proving the following related result.

For each of five mutually tangent spheres, there is a sphere passing through the six points of mutual contact of the remaining four.

Our theorem shows that given *any* four mutually tangent spheres, their points of tangency lie on a generalized sphere; we do not assume the existence of a fifth sphere tangent to each of them. Thus Coxeter's result is an immediate corollary of our theorem.

The natural question is whether, given four mutually tangent spheres, there will always be a fifth sphere tangent to each of the four. Coxeter notes in his abstract that when the four are congruent, there will always be two such spheres; however, the assumption of congruence is not necessary. Indeed, examination of FIGURE 3 makes it clear that in the inversive image, two spheres can be found that are tangent to $\mathcal{S}_1'$, $\mathcal{S}_2'$, $\mathcal{S}_3'$, and $\mathcal{S}_4'$: these spheres, $\mathcal{S}_5'$ and $\mathcal{S}_6'$, are congruent to $\mathcal{S}_3'$ and $\mathcal{S}_4'$ and positioned between the planes $\mathcal{S}_1'$ and $\mathcal{S}_2'$, one above and one below $\mathcal{S}_3'$ and $\mathcal{S}_4'$. In the original configuration, the preimages of $\mathcal{S}_5'$ and $\mathcal{S}_6'$ will both be spheres tangent to $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, and $\mathcal{S}_4$.

Though we discovered our result prior to reading Coxeter's paper, in hindsight the existence of the fifth sphere tangent to the original four is just as interesting as, and ultimately equivalent to, the fact that there is a sphere passing through their six points of tangency. While it is curious that Coxeter did not make this connection, his theorem was part of a larger focus on five initial spheres and the collection of spheres passing through various subsets of their points of mutual tangency. In any case, both results are beautiful examples of the powerful use of inversion.

Acknowledgment The authors thank Esther Tian for her help in using Autodesk Inventor to create Figure 4.

REFERENCES

1. O. Byer, F. Lazebnik, D. L. Smeltzer, *Methods for Euclidean Geometry*. Mathematical Association of America, Washington, DC, 2010.
2. H. S. M. Coxeter, Five spheres in mutual contact, *J. Geom. Graph.* **4** no. 2 (2000) 109–114.

3. H. S. M. Coxeter, *Introduction to Geometry*. Second edition. John Wiley and Sons, New York, 1969.
4. N. A. Court, *Modern Pure Solid Geometry*. Second edition. Chelsea, New York, 1964.

Summary. In this note we prove that the points of tangency of $n+1$ mutually tangent spheres in n-dimensional space lie on a generalized sphere. Coxeter's observation that for each of five mutually tangent spheres there is a sphere passing through the six points of mutual contact of the remaining four is a corollary of this result in the $n = 3$ case.

DEIRDRE L. SMELTZER (MR Author ID: 647964) received her Ph.D. in mathematics from the University of Virginia. Following four years at the University of St. Thomas in St. Paul, MN, she accepted a faculty position at her alma mater, Eastern Mennonite University in 1998. Since that time, she has served at EMU in multiple roles: faculty member, chair of the Mathematical Sciences department, director of the Cross-cultural Programs, and currently as Undergraduate Academic Dean. Recent mathematical pursuits have been primarily in Euclidean geometry.

OWEN D. BYER (MR Author ID: 624239) received a Ph.D. in mathematics from the University of Delaware under the supervision of Felix Lazebnik. After teaching for three years at Northwestern College in Orange City, IA, he took a position at Eastern Mennonite University. He is now in his 17th year there and is chair of the Mathematical Sciences Department. He and Deirdre have collaborated on several mathematical projects, most notably the text *Methods in Euclidean Geometry*, published by MAA in 2010. Owen's favorite problems are in the Discrete Mathematics realm and he is an avid duplicate bridge player.

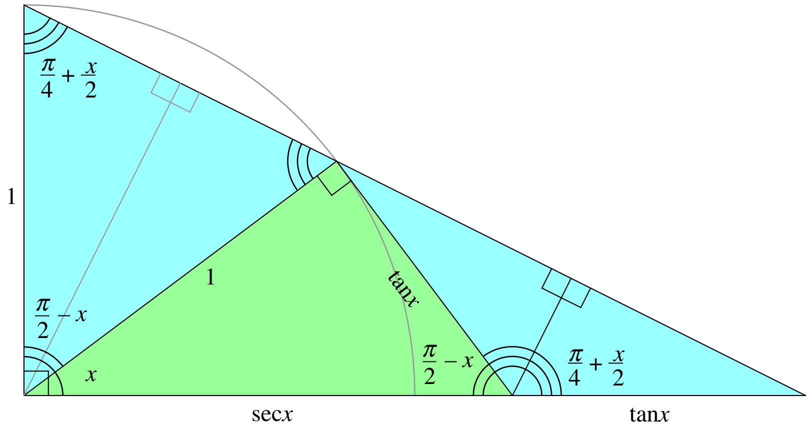
A	B	B	O	T	■	P	A	R	E	N	■	B	O	A
C	S	T	A	R	■	E	M	O	T	E	■	O	C	D
L	A	U	R	E	N	T	S	C	H	W	A	R	T	Z
■	■	■	S	E	A	R	■	S	N	E	E	Z	E	■
R	T	E	■	■	R	O	D	■	■	R	O	O	T	■
C	E	D	R	I	C	V	I	L	L	A	N	I	■	■
A	N	I	S	O	■	■	L	E	O	■	■	■	■	■
■	S	T	A	N	I	S	L	A	W	U	L	A	M	■
■	■	■	■	■	N	E	A	■	■	N	E	U	R	O
■	■	N	O	R	B	E	R	T	W	E	I	N	E	R
■	S	O	M	A	■	■	D	O	H	■	■	T	D	S
■	C	R	O	W	N	S	■	P	O	E	T	■	■	■
A	U	T	O	B	I	O	G	R	A	P	H	I	E	S
H	B	O	■	A	L	I	T	O	■	H	E	L	L	O
N	A	N	■	R	E	N	E	W	■	S	E	E	K	S

Proof Without Words: A Trigonometric Identity for sec x + tan x

ROGER B. NELSEN
Lewis & Clark College
Portland, OR
nelsen@lclark.edu

$$\sec x + \tan x = \tan\left(\frac{\pi}{4} + \frac{x}{2}\right)$$

Proof:



NOTE: Calculus students will recognize the expression $\sec x + \tan x$ since it appears in the indefinite integral of the secant of x. However, the first known formula for this integral, discovered in 1645, was

$$\int \sec x\, dx = \ln\left|\tan\left(\frac{\pi}{4} + \frac{x}{2}\right)\right| + C.$$

See [**1**] for details.

REFERENCE

1. V. F. Rickey, P. M. Tuchinsky, An application of geography to mathematics: History of the integral of the secant, *Math. Mag.* **53** (1980) 162–166.

Summary. We prove wordlessly the identity $\sec x + \tan x = \tan(\pi/4 + x/2)$.

ROGER B. NELSEN (MR Author ID: 237909) is a professor emeritus at Lewis & Clark College, where he taught mathematics and statistics for forty years.

Math. Mag. **88** (2015) 151. doi:10.4169/math.mag.88.2.151. © Mathematical Association of America
MSC: Primary 97G60

Unifying Two Proofs of Fermat's Little Theorem

MASSIMO GALUZZI
Dipartimento di Matematica
Università Statale di Milano
Via Saldini, 50 - 20133 Milano
galuzzim@gmail.com

Two interesting papers in this MAGAZINE [**2, 3**] have proposed unusual proofs of a famous result of Fermat.

Fermat's Little Theorem. *If $n \in \mathbb{N}$ and p is prime, then*

$$n^p - n \equiv 0 \pmod{p}.$$

It may be worthwhile to observe that the two proofs can be simplified and generalized with the help of a simple lemma. We begin with a definition.

Definition. Given a set S and a function $\varphi : S \to S$, we consider the iterates φ, $\varphi(\varphi)$, $\varphi(\varphi(\varphi))$, ... A point x is called *k-periodic* if

$$\underbrace{\varphi(\varphi(\cdots(\varphi}_{k \text{ times}}(x)))) = x,$$

where k is the number of iterations.

Lemma. *Let S be a set, and suppose that a family of functions $f_n : S \to S$, indexed by $n \geq 2$, has the following properties:*

- *For every n the function f_n has exactly n fixed points in S;*
- *For every n, m we have $f_n(f_m) = f_{nm}$.*

Then, given $n \geq 2$ and p prime, the number of p-periodic points of f_n is exactly $n^p - n$.

Proof. The number of fixed points of f_{n^p} is n^p, and we have to subtract the number of fixed points of f_n, which is n, to obtain the number of p-periodic points of f_n. ■

Assuming that such a family exists, we can now prove Fermat's little theorem.

Proof. We assume the existence of a family of functions as described in the lemma. Let n, p be as before.

The function f_n acts as a permutation on the fixed points of f_{n^p} so those that are not also fixed points of f_n must be in disjoint orbits of length p. The number of orbits of length p is given by

$$\frac{n^p - n}{p}.$$

Since this number is an integer, we conclude that p divides $n^p - n$. ■

Math. Mag. **88** (2015) 152–153. doi:10.4169/math.mag.88.2.152. © Mathematical Association of America
MSC: 11A25, 11B75

So everything depends on the existence of a family of functions with the properties given in the lemma. The papers mentioned at the beginning offer two possibilities, and the existence of these families allows us to conclude the proof.

In Levine's paper [**3**], the domain is $S = \mathbb{C}$ and the family of functions is given by $f_n(z) = z^n$, for $z \in \mathbb{C}$.

In Iga's paper [**2**], the domain is $S = [0, 1]$ and the family is given by

$$T_n(x) = \begin{cases} \{nx\} & \text{if } x \in [0, 1), \text{ and} \\ 1 & \text{if } x = 1, \end{cases}$$

where $x \in [0, 1]$ and $\{nx\}$ denotes the fractional part of nx.

Another family that has the properties described in the lemma consists of the Chebyshev polynomials. The main properties of these polynomials are described by Rivlin [**4**]. They are defined recursively by

$$\begin{aligned} T_0(x) &= 1, \\ T_1(x) &= x, \\ T_{n+1}(x) &= 2xT_n(x) - T_{n-1}(x). \end{aligned}$$

These polynomials satisfy the identity $T_n(T_m) = T_{nm}$, and when $n \geq 2$, the polynomial T_n has n fixed points in the domain $S = [-1, 1]$. So these polynomials may be used to obtain another proof of Fermat's little theorem.

The situation analyzed in the preceding lemma is similar to the one of Lemma 1 of [**1**], in which Fermat's little theorem is proved by counting certain necklaces. We are given a function $f : S \to S$, where S is a finite set (of objects), such that $f^{(p)}(x) = x$ for every x in S, where $f^{(p)}$ is the p-fold composition of f and p is a prime number.

It is proved that $|S| = |F| \bmod p$, where F is the set of fixed points of f. In this proof, the domain of f is different for each pair (n, p).

REFERENCES

1. P. G. Anderson, A. T. Benjamin, J. A. Rouse, Combinatorial proofs of Fermat's, Lucas's, and Wilson's theorems, *Amer. Math. Monthly* **112** (2005) 266–268. http://dx.doi.org/10.2307/30037444
2. K. Iga, A dynamical systems proof of Fermat's little theorem, *Math. Mag.* **76** (2003) 48–51, http://dx.doi.org/10.2307/3219132
3. L. Levine, Fermat's Little Theorem: A proof by function iteration, *Math. Mag.* **72** (1999) 308–309, http://dx.doi.org/10.2307/2691226
4. T. J. Rivlin, *The Chebyshev Polynomials*. Second edition. John Wiley, New York, 1990.

Summary. A new simple proof of Fermat's little theorem is given that generalizes the proofs given in this MAGAZINE by Levine (1999) and Iga (2003).

MASSIMO GALUZZI (MR Author ID: 243363) after retirement, became an adjunct professor of History of Mathematics at the Department of Mathematics at the Università Statale di Milano. He is the author of many articles about the mathematical contents of the work of, among others, Descartes, Newton, and Galois.

ACROSS

1. Monastery head
6. Shorthand for "("or")"
11. ___ constrictor
14. Type of algebra of continuous linear operators on a Hilbert space
15. Really ham it up
16. Neat freak's condition, possibly: Abbr.
17. * "A Mathematician Grappling with His Century" (1997/2001)
20. Cook a tuna steak, perhaps
21. Reason to say, "Gesundheit!"
22. Hwy.
25. Cuisenaire ___: colorful cylinder used in hands-on math activities with elementary-school students
27. Word that might come after square or cube
28. * "Theoreme Vivant" (2012) and "Birth of a Theorem" (2015)
33. Prefix meaning "not equal"
34. 20th-century geometer Moser, known for "Moser's Problem" about unit-length curves on the plane (which is still unsolved)
35. * "Adventures of a Mathematician" (1983)
42. Grant-giving org. whose chairperson is appointed by the POTUS
43. Prefix for science or surgeon
45. * "Ex-Prodigy: My Childhood and Youth" (1953) and "I am a Mathematician" (1956)
50. "Brave New World" drug
51. Homer Simpson's exclamation
52. Six-pt. scores in the NFL
53. Adorns a monarch
56. Quote attributed to Sophia Kovalevskaya: "It is impossible to be a mathematician without being a ___ in soul."
59. What all of the *starred clues* are
64. "Girls" home
65. Samuel who has been on the Supreme Court since 2006
66. Common basic programming output: "___ WORLD"
67. Output of dividing by 0 in C++
68. Subscribe to a journal or magazine again
69. David Sedaris book: "Squirrel ___ Chipmunk"

DOWN

1. Frequently injured knee part: Abbr.
2. Org. who voted in 2013 to allow gay members
3. A/C meas.
4. Scullers' needs
5. Connected graph with no cycles
6. Alexander ___, mid-19th century Russian chess player who popularized a symmetric, defensive opening
7. Org. headquartered in Providence, RI
8. Mythical birds
9. People: Prefix
10. Time of change
11. Dog breed also known as Russian wolfhound
12. Unit of digital information consisting of eight bits, or a group of eight musicians
13. Wood-shaping tool
18. D.E.A. agent
19. " ___ Flux": 2005 Charlize Theron film adapted from an MTV series
22. ___ Victor: record company that introduced the 45 RPM record in 1949
23. Place between ones and hundreds
24. Revise
26. Businessman William, founder of an American department store chain
29. Public-key cryptosystem: Abbr. (named for the surnames of the algorithm's inventors)
30. Charged particle
31. Meadow
32. Below the strike zone
36. "Mass ___ minor" J.S. Bach work
37. "Get it?"
38. College, in the U.K.
39. Marjorie ___ Browne: one of the first African-American women to receive a Ph.D. in Mathematics in the USA, from U. Michigan in 1949
40. Petunia Dursley, to Harry Potter
41. He's a horse, of course, of course
44. Some logical connectives
45. British mathematician Simon, student of John Conway and one of the co-authors of the "ATLAS of Finite Groups"
46. Herman Melville novel subtitled "A Narrative of Adventures in the South Seas"
47. Place to get oysters and steamers
48. The collection of elements of the form $a_{1,j}$ in the matrix A
49. "Hold your horses!"
50. Jacques Cousteau's equipment
54. It runs through Cairo
55. Phrase to wrap up a seminar talk: " ___ conclusion..."
57. Williams College athletes, based on an eponym of the school's original benefactor
58. "My country, 'tis of ___"
59. Luis von ___, Carnegie Mellon University Professor and founder of reCAPTCHA
60. Telecom. giant that merged with Bell Atlantic to form Verizon
61. ___ de France
62. Antlered animal
63. $\cdots$ _ _ _ $\cdots$

Math. Mag. **88** (2015) 154–155. doi:10.4169/math.mag.88.2.154. © Mathematical Association of America

Books for a Math Audience

BRENDAN W. SULLIVAN
Emmanuel College
Boston, MA 02115
sullivanb@emmanuel.edu

1	2	3	4	5	■	6	7	8	9	10	■	11	12	13
14					■	15					■	16		
17					18						19			
■	■	■	20				■	21						■
22	23	24	■	■	25		26	■	■	27				■
28			29	30				31	32				■	■
33					■	■	34			■	■	■	■	■
■	35				36	37				38	39	40	41	■
■	■	■	■	■	42			■	■	43				44
■	■	45	46	47				48	49					
■	50				■	■	51			■	■	52		
■	53				54	55	■	56		57	58	■	■	■
59							60					61	62	63
64			■	65					■	66				
67			■	68					■	69				

Clues start at left, on page 154. The Solution is on page 150.

Extra copies of the puzzle can be found at the Magazine's website, www.maa.org/mathmag/supplements.

MAA100
MATHEMATICAL ASSOCIATION OF AMERICA
CELEBRATING A CENTURY OF ADVANCING MATHEMATICS

From the Files of Past MAGAZINE Editors
J. Arthur Seebach and Lynn Arthur Steen 1976–1980

To highlight how technology has changed the way that editorial work is done: as editor of the MAGAZINE, Lynn Arthur Steen used to cut accepted manuscripts apart and paste them using rubber cement onto pages to indicate the layout of the articles for the printer.

PROBLEMS

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

PROPOSALS

To be considered for publication, solutions should be received by September 1, 2015.

1966. *Proposed by H. A. ShahAli, Tehran, Iran.*

Let n be a square-free natural number. Let S be an infinite set of integer quadruples (a, b, c, d) such that the sets $\{ad - bc : (a, b, c, d) \in S\}$ and $\{ac - nbd : (a, b, c, d) \in S\}$ are bounded. Prove that the set $\{a^2 - nb^2 : (a, b, c, d) \in S\}$ is bounded.

1967. *Proposed by Marcel Chirita, Bucharest, Romania.*

Let n be a positive integer. Determine all functions $f, g : \mathbb{R} \to \mathbb{R}$ with continuous derivatives f' and g' that satisfy the following conditions: For every real number x,

$$(f(x))^2 + (g(x))^2 = (f'(x))^2 + (g'(x))^2 \quad \text{and} \quad f(x) + g(x) = g'(x) - f'(x).$$

Moreover, the equation $f(x) = g(x)$ has $n + 1$ real roots with the smallest one being $x = 0$.

1968. *Proposed by George Apostolopoulos, Messolonghi, Greece.*

Let n be a positive integer. Prove that in any triangle ABC

Math. Mag. **88** (2015) 156–158. doi:10.4169/math.mag.88.2.156. © Mathematical Association of America

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.

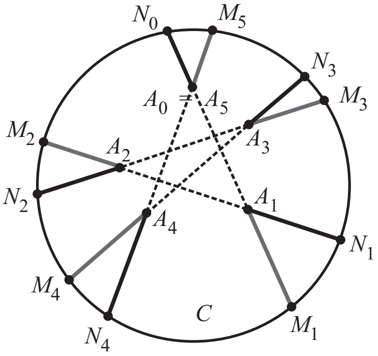
$$\frac{\cos^n\left(\frac{A}{2}\right)}{\sin^n\left(\frac{A}{2}\right)+\cos^n\left(\frac{A}{2}\right)}+\frac{\cos^n\left(\frac{B}{2}\right)}{\sin^n\left(\frac{B}{2}\right)+\cos^n\left(\frac{B}{2}\right)}+\frac{\cos^n\left(\frac{C}{2}\right)}{\sin^n\left(\frac{C}{2}\right)+\cos^n\left(\frac{C}{2}\right)}\le\frac{3s^{n/3}}{r^{n/3}+s^{n/3}},$$

where s and r denote the semiperimeter and the inradius of $\triangle ABC$, respectively.

1969. *Proposed by Omran Kouba, Higher Institute for Applied Sciences and Technology, Damascus, Syria.*

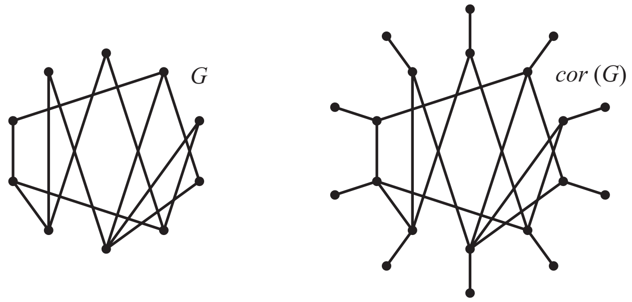
Let $n \geq 3$ be an integer, C be a circle, and $A_0, \dots, A_{n-1}, A_n$ (with $A_n = A_0$), be an equilateral polygon (not necessarily convex or nonintersecting) inside C; that is, $A_0A_1 = A_1A_2 = \cdots = A_{n-1}A_n$. For $0 \leq k < n$, the line A_kA_{k+1} intersects the circle C at two points; the one that belongs to the ray A_kA_{k+1} is denoted M_{k+1} and the other one is denoted by N_k. Prove that

$$\sum_{k=0}^{n-1} A_kN_k = \sum_{k=1}^{n} A_kM_k.$$



1970. *Proposed by Allen J. Schwenk, Western Michigan University, Kalamazoo, MI.*

A graph G has vertices $V(G) = \{v_1, v_2, \dots, v_n\}$ and edges $E(G) = \{e_1, e_2, \dots, e_m\}$. The *corona* of G, denoted by $cor(G)$, is the graph formed by adding n new vertices $w_1, w_2, \dots, w_n$ and n new edges v_iw_i for $1 \leq i \leq n$. A set of edges is called *independent* if no two edges share a vertex. Let b_i denote the number of independent edge-sets of size i. Prove that for any graph G and for each i with $0 \leq i < n/2$, the independent edge-sets of $cor(G)$ satisfy $b_i = b_{n-i}$.



Quickies

Q1049. *Proposed by Michael W. Botsko, Saint Vincent College, Latrobe, PA.*

Let f and g be real valued functions defined on $\mathbb{R}$ such that $f(x) \geq g(x)$ for all x. Suppose that $f(x+y) \geq f(x) + f(y)$ for all x and y, and that $g(-x) \geq -g(x)$ for all x. Prove or disprove that $f = g$.

Q1050. *Proposed by Ovidiu Furdui, Technical University of Cluj-Napoca, Cluj-Napoca, Romania.*

Calculate

$$\int_0^1 \int_0^1 xy(-1)^{\lfloor 1/x - 1/y \rfloor} dx dy,$$

where $\lfloor x \rfloor$ denotes the floor of x.

Answers

A1049. We prove that $f = g$. First note that $f(0) = f(0+0) \geq f(0) + f(0)$, so that $0 \geq f(0)$. Then note that

$$0 \geq f(0) = f(-x+x) \geq f(-x) + f(x) \geq g(-x) + f(x) \geq -g(x) + f(x).$$

Therefore, $g(x) \geq f(x)$ for all x, and because $f(x) \geq g(x)$ by assumption, it follows that $f = g$.

A1050. Let

$$I = \int_0^1 \int_0^1 xy(-1)^{\lfloor 1/x - 1/y \rfloor} dx dy.$$

By symmetry of the two variables, it follows that

$$I = \int_0^1 \int_0^1 xy(-1)^{\lfloor 1/y - 1/x \rfloor} dx dy.$$

If x is a real number that is not an integer, then $\lfloor x \rfloor + \lfloor -x \rfloor = -1$. It follows that $\lfloor 1/x - 1/y \rfloor = -1 - \lfloor 1/y - 1/x \rfloor$ for all $0 < x < 1$ and $0 < y < 1$, except for a set of measure zero. Thus

$$\begin{aligned} I &= \int_0^1 \int_0^1 xy(-1)^{\lfloor 1/y - 1/x \rfloor} dx dy = \int_0^1 \int_0^1 xy(-1)^{-1-\lfloor 1/x - 1/y \rfloor} dx dy \\ &= -\int_0^1 \int_0^1 xy(-1)^{-\lfloor 1/x - 1/y \rfloor} dx dy = -\int_0^1 \int_0^1 xy(-1)^{\lfloor 1/x - 1/y \rfloor} dx dy = -I. \end{aligned}$$

Therefore, $I = 0$.

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.

Harris, Michael, *Mathematics without Apologies: Portrait of a Problematic Vocation*, Princeton Univ. Press, 2015; xxii + 438 pp, \$29.95. ISBN 978-0-691-15423-7.

A unique feature of this book is a series of chapters, interleaved between essays, of monologue/dialogues about "How to Explain Number Theory at a Dinner Party." The series was inspired by a performing artist who had asked author Harris (Columbia Univ.): "What is it you do in number theory, anyway?" The series starts with the irrationality of $\sqrt{2}$ and gets to elliptic curves and the Birch–Swinnerton-Dyer conjecture (a Clay Millennium Problem). The series tries to answer what mathematicians do. But the main purpose of the book is to address the question: Why? *Why do mathematics at all?* What is the motivation of a pure mathematician, who is engaged in "one of the few remaining human activities not driven by commercial considerations"? Pure mathematicians describe their activities "in misleading terms... We promise Golden Geese [practical applications], immutable truths, ineffable beauty." But those are not really why we do mathematics. Harris's answer: *pleasure*—the pleasure of "figuring things out" through logical thinking (Daubechies), which can become a habit and even an addiction. Meanwhile, mathematicians make a Faustian bargain in those promises to society, including training students in financial mathematics, who go on to commit "crimes against humanity" (according to former French Premier Michel Rocard) and "organized crime" (Charles Ferguson, in *Predator Nation*). Harris, notable for his work on the Langlands conjectures, is very widely read and quotes ancient and contemporary sources *profusely*. The first essay goes on about how Harris acquired "charisma" (reputation), presumably setting forth his credentials for the ensuing discussions; and another goes into too much mathematical detail and terminology (for the general reader or even the nonspecialist mathematician) in describing a dream of his. Others analyze in depth mathematician Eric Frenkel's film *Rites of Love and Math* and the search for a "formula" for love, and Harris's hypothesis that Thomas Pynchon follows a "quadratic" style in his novels. There's much more; but with a chapter titled "Megaloprepeia," this erudite high-culture book is definitely not for those faint at heart in regard to any of literature, art, or philosophy.

Henle, Jim, *The Proof and the Pudding: What Mathematicians, Cooks, and You Have in Common*, Princeton Univ. Press, 2015; ix + 165 pp, \$26.95. ISBN 978-0-691-16486-1.

Who would think that mathematics and gastronomy have a lot in common? Well, author Henle warns at the outset: In this book, "there are no applications of math to cooking" (a welcome relief from the relentless onslaught of demand for "relevance"). The book does contain recipes (mostly by Henle), but "This isn't a cookbook." The point is that the attitudes and tools, the criteria for good work, and the satisfactions of mathematics and of cooking are similar. "But in both fields, the chief motivation is pleasure... fun." Both involve curiosity, experimentation, and solving problems. The book is "salted" with an average of more than one figure or cartoon per page, and the 25 chapters are "peppered" with recipes. Ah, but what math? Discrete mathematics, mostly discrete geometry, puzzles and games. What recipes? To learn about them, you will have to buy the book—and try them out.

Math. Mag. **88** (2015) 159–160, doi:10.4169/math.mag.88.2.159. © Mathematical Association of America

Csicsery, George, *Counting from Infinity: Yitang Zhang and the Twin Prime Conjecture*, Zala Films; 55-min. film with 38 mins. extra features, $149 with performance rights, $24.95 for home/personal use, plus $5 shipping. ISBN 978-0-098248-005-2. Order form at http://www.zalafilms.com/films/cfiflyer.pdf.

Wilkinson, Alec, The pursuit of beauty, *The New Yorker* (2 February 2015), http://www.newyorker.com/magazine/2015/02/02/pursuit-beauty.

Lin, Thomas, After prime proof, an unlikely star rises, *Quanta Magazine* (2 April 2015), https://www.quantamagazine.org/20150402-prime-proof-zhang-interview/.

In 2013 Yitang "Tom" Zhang (Univ. of New Hampshire), a relative unknown in mathematics, at the relatively "old" age of 58 surprised the world with a proof of the astonishing fact that there are infinitely many primes less than 70 million apart (a bound since lowered to 246). This film, article, and interview feature his biography, personality (he prefers solitude and a simple life), and character (determination, concentration). His story exhibits once again a compelling story that fulfills the popular stereotype: A lone eccentric mathematician, working in utter privacy and full obscurity, with extreme single-mindedness of purpose, emerges with a remarkable result—in his case, also the story of an immigrant outsider who makes good. Where's a film of similar accomplishment by someone counter to stereotype? Nevertheless, I thank George Csicsery for bringing Zhang and the mathematics to life in the film, which with extras includes interviews with number theorists Enrico Bombieri (Institute for Advanced Study), Terence Tao (UCLA), and others, particularly Kenneth Ribet (UC–Berkeley) discussing "smooth numbers," the ABC conjecture, and gaps between primes. (Thanks to Phil Straffin for his gift of the video.)

Suzuki, Jeff, *Constitutional Calculus: The Math of Justice and the Myth of Common Sense*, Johns Hopkins Univ. Press, 2015; ix + 280 pp, $34.95. ISBN 978-1-4214-1595-6.

A mathematician might regard the provisions of the U.S. Constitution as axioms of a legal system, and law developed since then as theorems in that system. This well-researched book, keyed to provisions in the Constitution and Bill of Rights and chock full of citations to court cases, examines and questions present-day practice in regard to the census, representation, apportionment, redistricting, the Electoral College, voting systems, policing, jury selection, the size of juries, "three strikes" laws, and the death penalty. Brought to bear is not so much mathematics as probability, including sampling, confidence intervals, Simpson's paradox, Bayes's formula, and Fisher's exact test, plus centrality measures from social network analysis. The book concludes with the author's recommendations for changes in current practice and institutions.

Parker, Matt, *Things to Make and Do in the Fourth Dimension: A Mathematician's Journey through Narcissistic Numbers, Optimal Dating Algorithms, at Least Two Kinds of Infinity, and More*, Farrar, Straus and Giroux, 2014; 454 pp, $28. ISBN 978-0-374-27565-5.

How many mathematicians do you know who are also stand-up comedians? Well, here is a prime example. No, it couldn't be a prime example: there is only one of him (though we learn from author Parker that 1 was a prime number through 1956, at least according to mathematician Derrick Lehmer). Anyway, this book is about fun mathematics, the kind that Parker asserts can win you free drinks (let me know if any of it works for you!). With an echo of Michael Harris above, Parker asserts that "the essence of mathematics is…the pursuit of pattern and logic for their own sake; it is sating our playful curiosity.… You can think of much of mathematics as being like train-spotting or stamp-collecting. Hmm, those may not be the two best examples I could have picked. I'm trying to sell this stuff to you." You can see where the humor can come in. And the book really is fun, with things to make and try, as it explores representations of numbers, slicing pizzas fairly (not as you would imagine), shapes of all kinds, flexagons, patterns in primes, knots (learn to tie your shoes the fast way!), graph theory, Bernoulli numbers, the zeta function, and indeed—not withstanding the title—just a couple of chapters about the fourth and higher dimensions. The hand-drawn figures are pleasantly informal. There are even instructions on how to build a computer out of dominos—not as easy as you think, since paths cannot cross and you need to build in calculated delays—and photos of an adder made out of 10,000 dominos ("possibly the most inefficient way ever to add 6 and 4"). My only complaint: I am too poor in British coins to do the 2-pence puzzles and the 25-pence and 50-pence geometrical constructions (hint to publisher: There may be a market for an Americanized edition).

MAA MATHFEST

August 5-8, 2015

Join us in Washington, D.C., for our Centennial Celebration.

2015 MAA Centennial Lecturers

Manjul Bhargava, Princeton University
Carlos Castillo-Chavez, Arizona State University
Jennifer Chayes, Microsoft Research
Ingrid Daubechies, Duke University
Erik Demaine, Massachusetts Institute of Technology
Karen Parshall, University of Virginia

Earle Raymond Hedrick Lecturer

Karen Smith, University of Michigan

Other Invited Lecturers

David Bressoud, Macalester College
(James R. C. Leitzel Lecture)

Noam Elkies, Harvard University
(Pi Mu Epsilon J. Sutherland Frame Lecture)

Joseph Gallian, University of Minnesota Duluth
(The Jean Bee Chan and Peter Stanek
Lecture for Students)

Jeffrey Lagarias, University of Michigan
(AMS-MAA Joint Invited Address)

Erica Walker, Columbia University
(AWM-MAA Etta Z. Falconer Lecture)

Terrence Blackman, The University of Denver
(NAM David Harold Blackwell Lecture)

"0394, part of Contrast Series"
Artwork and Photograph by
Erik Demaine and Martin Demaine

Mathematical sessions run Wednesday morning through Saturday evening (August 5–August 8)

Register Today
maa.org/mathfest

Joint Meeting with the Canadian Society for History and Philosophy of Mathematics and the British Society for the History of Mathematics.

MAA100
MATHEMATICAL ASSOCIATION OF AMERICA
CELEBRATING A CENTURY OF ADVANCING MATHEMATICS

MAA 100
MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth St., NW · Washington, DC 20036

CONTENTS

ARTICLES

NOTES

PROBLEMS AND SOLUTIONS

REVIEWS