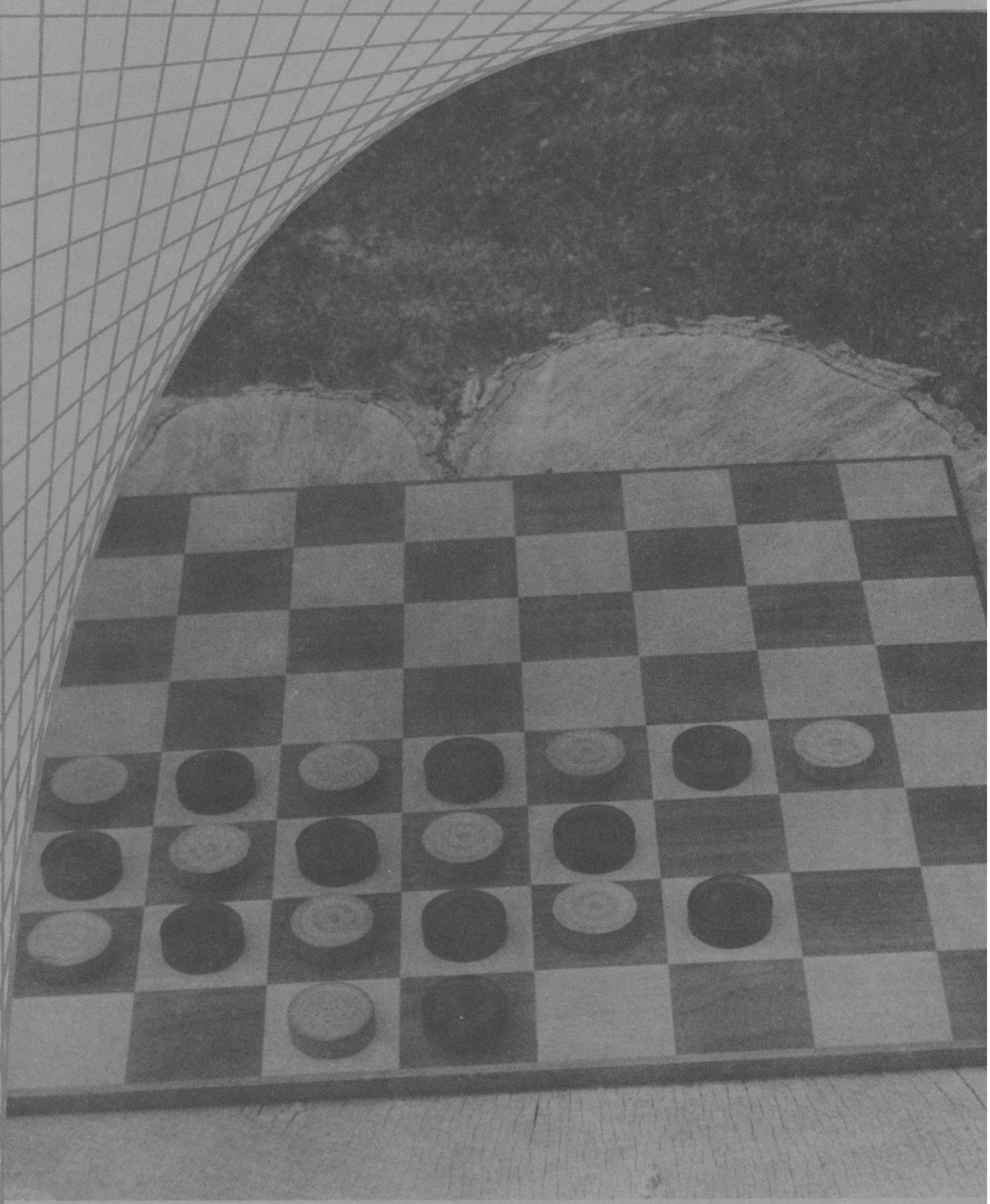
MATHEMATICS MAGAZINE



Vol 52, No. 4
September, 1979

FOUNDATION CRISES • GEOMETRIC GAMES

NEGATIVE BASES • 3D CHECKER JUMPING

MATHEMATICS MAGAZINE

Volume 52, Number 4, September 1979
(ISSN—0025-570X)

ARTICLES

NOTES

PROBLEMS

REVIEWS

NEWS AND LETTERS

COVER: How far above the center line can you get a checker by vertical and horizontal jumps, removing jumped checkers as you go? If this problem has you stumped, turn to page 227 where it is solved both in two and three dimensions.

EDITORIAL POLICY

Mathematics Magazine is a journal of collegiate mathematics designed to enrich undergraduate study of the mathematical sciences. The *Magazine* should be an inviting, informal journal emphasizing good mathematical exposition of interest to undergraduate students. Manuscripts accepted for publication in the *Magazine* should be written in a clear and lively expository style. The *Magazine* is not a research journal, so papers written in the terse "theorem-proof-corollary-remark" style will ordinarily be unsuitable for publication. Articles printed in the *Magazine* should be of a quality and level that makes it realistic for teachers to use them to supplement their regular courses. The editors especially invite manuscripts that provide insight into applications and history of mathematics. We welcome other informal contributions, for example, brief notes, mathematical games, graphics and humor.

Editorial correspondence should be sent to: Mathematics Magazine, Department of Mathematics, St. Olaf College, Northfield, Minnesota 55057. Manuscripts should be prepared in a style consistent with the format of *Mathematics Magazine*. They should be typewritten and double spaced on $8\frac{1}{2}$ by 11 paper. Authors should submit the original and one copy and keep one copy as protection against possible loss. Illustrations should be carefully prepared on separate sheets of paper in black ink, the original without lettering and two copies with lettering added; the printers will insert printed letters on the illustration in the appropriate locations.

Authors planning to submit manuscripts may find it helpful to obtain the more detailed statement of guidelines available from the editorial office.

ABOUT OUR AUTHORS

William H. Ruckle ("Geometric Games of Search and Ambush") has been a Professor of Mathematics at Clemson University since 1969. During the academic year 1975–76 he was Guest Professor of Mathematics at the J. W. Goethe University, Frankfurt am Main, West Germany, associated with the group of G. Koethe and J. Weidmann. His interest in game theory dates from 1969 when he began to study games of search and ambush motivated by the "hunter and bird" problem.

Ernst Snapper ("The Three Crises in Mathematics: Logicism, Intuitionism and Formalism") studied at the University of Amsterdam in Holland and received his Princeton Ph.D. in 1941 under J. H. M. Wedderburn. He was an NSF postdoctoral fellow at Harvard and has lectured at numerous summer institutes. He is presently Professor of Mathematics at Dartmouth College. His publications are in algebra, geometry and algebraic geometry and he is the co-author with Professor Robert J. Troyer of Metric Affine Geometry (Academic Press). His present interest is the philosophy of mathematics.

Rodney T. Hansen and Leonard G. Swanson ("Unitary Divisors") worked together at Montana State University where Professor Hansen has taught for the past eleven years. Hansen's interest in unitary divisors stems from his work in number theory and current interest in arithmetic function convolution theory. Leonard G. Swanson has been an Associate Professor of Mathematics at Portland State University for the past thirteen years, and was a visiting Professor at Montana State University during the 1977–78 academic year. His interest in number theory grew out of his interest in Fourier series and their applications in number theory.

BUSINESS INFORMATION. Mathematics Magazine is published by the Mathematical Association of America at Washington, D.C., five times a year in January, March, May, September, and November. Ordinary subscriptions are $12 per year. Members of the Mathematical Association of America or of Mu Alpha Theta may subscribe at special reduced rates. Colleges and university mathematics departments may purchase bulk subscriptions (5 or more copies to a single address) for distribution to undergraduate students.

Subscription correspondence and notice of change of address should be sent to A. B. Willcox, Executive Director, Mathematical Association of America, 1529 Eighteenth Street, N.W., Washington, D.C. 20036. Back issues may be purchased, when in print, from P. and H. Bliss Co., Middletown, Connecticut 06457.

Advertising correspondence should be addressed to Raoul Hailpern, Mathematical Association of America, SUNY at Buffalo, Buffalo, New York 14214.

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

ARTICLES

Geometric Games of Search and Ambush

A mathematical theory of hide and seek, developing strategies for both players.

WILLIAM H. RUCKLE
Clemson University
Clemson, SC 29631

The Hunter and Bird Game

Consider the following problem concerning a hunter, a bird and a field. The bird wants to fly from one side of the field to the other. The hunter wants to wait somewhere within the field and shoot the bird if it comes within range. The problem is to determine the best policy for both the bird and the hunter and the result of following this best policy.

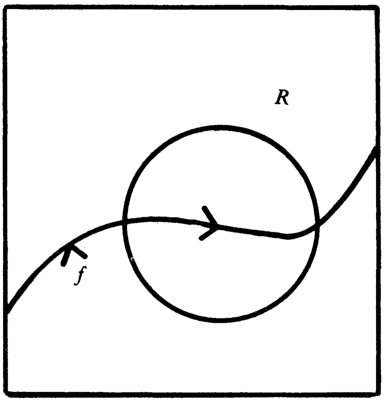
The precise statement of this problem depends upon the shape of the field, the capabilities of the bird and the hunter, and the meaning of the term "best policy." Assume the field is a square one unit long and one unit wide so that it can be realized as the unit square

$$L=\{(x,y)\colon 0\leqslant x\leqslant 1;\ 0\leqslant y\leqslant 1\}.$$

Assume the bird can choose as its path across the field the graph $\hat{f}$ of a function f from the unit interval into itself. This function f must be chosen from a set $\mathfrak{B}$ of paths available to the bird. The bird does not know where the hunter will wait, nor can it see him during the course of its flight. Therefore, the bird may as well choose its path at the beginning and stick to it. The hunter can stand at any point of the field. If the bird's path f comes to within the range r of his gun, he will shoot it. Otherwise, the bird will elude him and reach the other side of the field. The hunter cannot see the bird until it is within range, and he is not allowed to move after he has chosen his position. The hunter knows the set $\mathfrak{B}$ of paths available to the bird, and the bird knows the range r of the hunter's gun. Two reenactments of this encounter, one advantageous to the hunter, and one to the bird are illustrated in FIGURES 1 and 2.

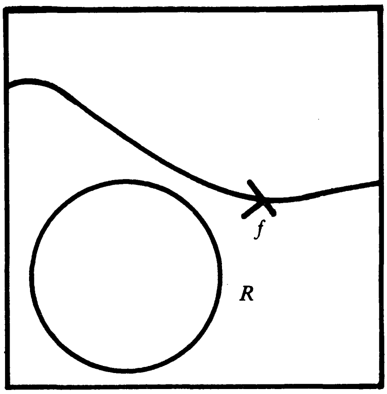
One way of defining the term "best policy" is by means of game theory. In order to do this, I must use the concept of a finite probability measure, a notion often described in courses on mathematical models or finite mathematics.

Let $\mathfrak{R}$ consist of all subsets of L which are the intersection of L with a circle of radius r. The encounter between the bird and the hunter can now be described as the following two person, zero-sum game: the bird chooses a function f from $\mathfrak{B}$; the hunter chooses a set R from $\mathfrak{R}$; the hunter then receives a payoff $F(R,f)$ given by the formula



Hunter and Bird Game: Hunter wins.

FIGURE 1



Hunter and Bird Game: Bird wins.

FIGURE 2

$$F(R,f)=\begin{cases}1 \text{ if } R\cap\hat{f}\neq\varnothing\\ 0 \text{ if } R\cap\hat{f}=\varnothing.\end{cases}\tag{1}$$

This game is called a zero-sum game because any gain by the hunter is assumed to result in an equal loss by the bird. (Some good references on two-person games are the books of Gale [**3**], Dresher [**1**], and Owen [**6**].)

A **solution** for a game consists of:

(a) a number v called the **value** of the game;

(b) a probability measure ρ on $\mathfrak{R}$ such that

$$\int_{\mathfrak{R}} F(R,f)\,d\rho(R)\geqslant v \qquad \text{for all } f \text{ in } \mathfrak{B};\tag{2}$$

(c) a probability measure β on $\mathfrak{B}$ such that

$$\int_{\mathfrak{B}} F(R,f)\,d\beta(f)\leqslant v \qquad \text{for all } R \text{ in } \mathfrak{R}.\tag{3}$$

The probability measure ρ is called an **optimal strategy** for the hunter, and the probability measure β is called an **optimal strategy** for the bird. What do these inequalities mean, and why are the measures ρ and β called optimal? The integral in inequality (2) is equal to the average of the payoff function $F(R,f)$ with respect to the measure ρ. Thus, if the hunter chooses his strategy according to the strategy ρ, he can expect on the average to shoot the bird with probability at least v no matter what the bird does since (2) holds for all f in $\mathfrak{B}$. Similarly, if the bird chooses his path according to strategy β, he can expect on the average to elude the hunter with probability at least $1-v$ no matter what the hunter does. This means that ρ and β are the most prudent strategies for hunter and bird, respectively. That is why they are called optimal. Von Neumann and Morgenstern in [**11**] argue forcefully that the strategies called "optimal" are indeed the best policies.

The problem of solving the above game may seem inhumanly difficult because it involves the determination of probability measures on infinite sets of geometric objects, i.e., $\mathfrak{R}$ a set of circles and $\mathfrak{B}$ a set of functions (or equivalently graphs of functions). This is what I thought when I first considered it. However, I was wrong. The solution is, in fact, quite easy. In order to approach the general solution, consider two special cases for specific values of r.

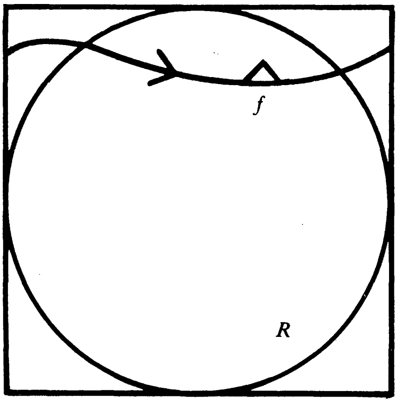
Case I. $r\geqslant 1/2$. In this case the bird does not have a chance. The hunter places himself in the middle of the field; the bird will come within his range with probability one (see FIGURE 3).

Here the value of the game to the hunter is $v=1$. An optimal strategy for the hunter is the probability measure ρ which has the value one on every subset $\mathbb{S}$ of $\mathfrak{R}$ which contains the circle whose center coincides with the center of L and whose radius is r and which has value zero on every subset of $\mathfrak{R}$ which does not contain this circle. All strategies are optimal for the bird.

Case II. $1/4 \leqslant r < 1/2$. Assume that $\mathfrak{B}$ the set of paths available to the bird contains among other things the functions f_1 and f_2 given by

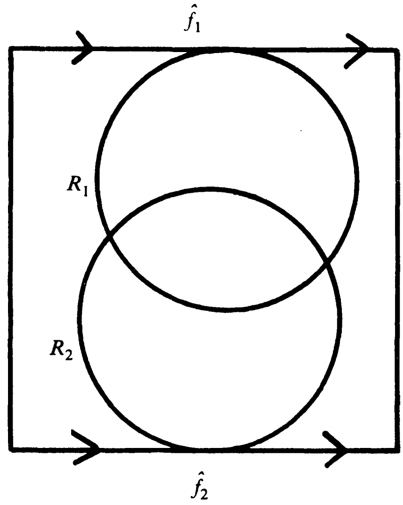
$$f_1(x)=1 \qquad f_2(x)=0 \qquad 0 \leqslant x \leqslant 1.$$

No circle R in $\mathfrak{R}$ intersects both f_1 and f_2. Thus, if the bird chooses one of the paths f_1 or f_2 with probability $1/2$, he will escape the hunter with probability at least $1/2$. This means that the value of the game to the hunter can be no more than $1/2$. On the other hand, suppose that the hunter chooses with probability $1/2$ one of the circles R_1 or R_2 where R_1 has center $(1/2, 1-r)$, R_2 has center $(1/2, r)$ and both circles have radius r. These two circles completely cover the vertical line $x=1/2$ through which the bird must pass. Therefore, the hunter will shoot the bird with probability at least $1/2$ (see FIGURE 4). The value of the game in this case is thus $1/2$. An optimal strategy for the bird is the probability measure β which is 0 for every subset of $\mathfrak{B}$ which contains neither f_1 nor f_2, $1/2$ for every subset of $\mathfrak{B}$ which contains one of these functions and 1 for every subset of $\mathfrak{B}$ which contains both of these functions. An optimal strategy for the hunter is the probability measure ρ which is 0 for every subset of $\mathfrak{R}$ which contains neither R_1 nor R_2, $1/2$ for every subset of $\mathfrak{R}$ which contains one of these circles and 1 for every subset which contains both circles.



The Hunter and Bird Game for $r \geqslant 1/2$. The Hunter always wins.

FIGURE 3



The Hunter and Bird Game with $r=5/16$. Optimal strategy for hunter: Choose one of the discs; for the bird: Choose one of the Paths.

FIGURE 4

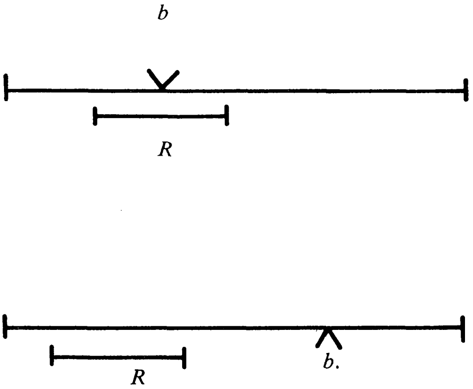
The solution of Case II of the Hunter and Bird Game contains all the elements of the solution in the most general case. This case, in fact, reduces to the children's game of guessing which hand holds the coin or pebble. For the bird's task, in fact, is simply to guess which side of the field the hunter is watching and fly straight across the other side.

In the optimal strategy for the hunter, the requirement that the center of his ambush be placed on the vertical line $x=1/2$ is not essential. The same optimal strategy for the hunter is possible on any vertical line through L. Moreover, the significant quality of the hunter's ambush set is not that it is a disc of radius r, but that its intersection with the vertical line through L is a closed interval of length $2r$. This is a consequence of the fact that the optimal strategy for the bird can be expressed entirely in terms of straight line paths.

Consequently, the Hunter and Bird Game can be reduced to the following one-dimensional game which I shall call the **Point Catcher Game** (see FIGURE 5): The player called Blue chooses a point b in the unit interval $I=[0,1]$ while the player called Red chooses a closed subinterval R of length d. If $b \in R$, then Red receives a payoff of 1 while if $b \in R$, Red receives 0.

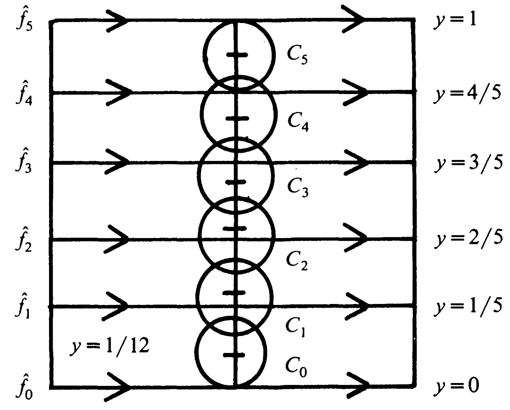
To solve the Point Catcher Game, we extrapolate from Case II of the Hunter and Bird Game. Suppose n is a positive integer such that $1/(n+1) \leqslant d < 1/n$. (Of course if $d=1$ the solution is obvious.) No subinterval B contains more than one of the $n+1$ points k/n; $k=0,1,\ldots,n$ since the distance between two adjacent points is $1/n$ which is greater than d. Thus if Blue chooses one of the point k/n with probability $1/(n+1)$, he will be caught with probability at most $1/(n+1)$. This means that the value of the Point Catcher Game is no greater than $1/(n+1)$. On the other hand, let Red choose with probability $1/(n+1)$ one of the intervals $R_k=[k/(n+1),(k+1)/(n+1)]$ $(k=0,1,\ldots,n)$ with probability $1/(n+1)$. Since these intervals cover I, any point b chosen by Blue must fall into one of them. Thus Red can expect to catch b with probability at least $1/(n+1)$. Therefore, the value of the game is $1/(n+1)$ and optimal strategies for Red and Blue are those described above. The conclusion above is summarized in the following theorem.

THEOREM 1. *The value of the Point Catcher Game is* $1/(n+1)$ *where* $1/(n+1) \leqslant d < 1/n$. *An optimal strategy for Red is to choose with probability* $1/(n+1)$ *one of the intervals* $[k/(n+1),(k+1)/(n+1)]$ $(k=0,\ldots,n)$. *An optimal strategy for Blue is to choose with probability* $1/(n+1)$ *one of the points* k/n: $k-0,1,\ldots,n$.



Two enactments of the Point Catcher Game.

FIGURE 5



The Hunter and Bird Game with $r=1/12$.

FIGURE 6

The Hunter and Bird Game is not exactly the same as the Point Catcher Game because the pure strategies for both Hunter and Bird differ from those of Red and Blue respectively. The encounters between bird and hunter described in FIGURES 1 and 2, for instance, do not have correspondents in the Point Catcher Game. Nevertheless, the solutions of the two games and the reasoning used to obtain them are analogous. The argument preceding Theorem 1 can be modified by picking a vertical line in L arbitrarily and relabeling the objects involved to obtain the following result, illustrated in FIGURE 6.

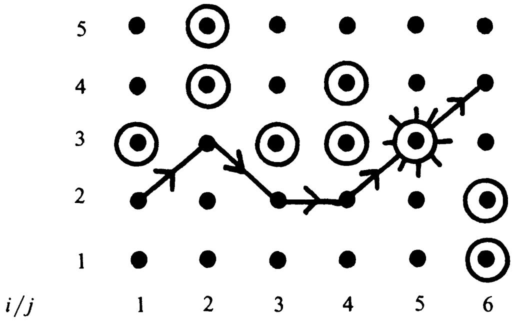
THEOREM 2. *Suppose* $\mathcal{B}$ *contains all constant paths and* $1/(n+1) \leqslant 2r < 1/n$. *The value of the Hunter and Bird Game is* $1/(n+1)$. *An optimal strategy for the hunter is the finite probability distribution* ρ *for which* $\rho(\{C_k\}) = 1/(k+1)$ *where* C_k *is the circle with center* $(1/2,(2k+1)/2(n+1))$ *and radius* r, $(k=0,\ldots,n)$. *An optimal strategy for the bird is the finite probability distribution* β *for which* $\beta(\{f_k\}) = 1/(k+1)$ *where* $f_k(x)=n/k$, $(k=0,1,\ldots,n)$.

The optimal strategy for the hunter is not unique because the centers of the circles involved in the optimal strategy can lie on any vertical line through L. Moreover, if $2r$ is strictly greater than $1/(n+1)$ the y-coordinate of the center of C_k need not be precisely at $k/(n+1)$. (Try to calculate how much play is possible.) The optimal strategy for the bird is not unique either: Try to find alternatives.

Games on a Rectangular Lattice

Before I learned that the Hunter and Bird Game has such an easy solution, I studied finite approximations of the continuous game in order to obtain a rough idea of what to expect in the continuous game. For a finite approximation of the Hunter and Bird game, let L be a rectangular array of points having m rows and n columns; thus, $L=\{(i,j) : i=1,2,\dots,n;\ j=1,2,\dots,m\}$. Let $\mathfrak{F}$ denote the collection of all functions f from $\{1,2,\dots,n\}$ into $\{1,2,\dots,m\}$. Each f in $\mathfrak{F}$ may be identified with its graph $\hat{f}=\{(i,f(i)) : i=1,2,\dots,m\}$ and thus interpreted as a path from the first column of L to the last column which does not double back on itself. The set $\mathfrak{R}$ of strategies available to Red will be a subcollection of the set $\mathfrak{S}$ of all subsets of L. The set $\mathfrak{B}$ of strategies available to Blue will be subset of $\mathfrak{F}$. Thus Blue can be thought of as traveling from one side of L to another, either attempting to avoid obstacles placed in L by Red or seeking objects in L hidden by Red.

This situation is illustrated in FIGURE 7. The lattice L has five rows and six columns. Red has chosen the set $\mathfrak{R}=\{(1,3),(2,4),(2,5),(3,3),(4,3),(5,3),(6,1),(6,2)\}$ and Blue has chosen the function $f(1)=2$, $f(2)=3$, $f(3)=2$, $f(4)=2$, $f(5)=3$, $f(6)=4$, which can be identified with the set $\{(1,2),(2,3),(4,2),(5,3),(6,4)\}$. At the point $(5,3)$ there is a meeting between f and R which can represent either a successful ambush of Blue by Red or Blue finding one of Red's hidden objects.



An enactment of a finite ambush game.

FIGURE 7

Geometric games played on a finite lattice L will always have a solution because of the Minimax Theorem of von Neumann [**11**]. In principle, this solution can be found by methods of linear programming. However, except for the most elementary examples of finite geometric games, the sets $\mathfrak{B}$ and $\mathfrak{R}$ will be too large for linear programming to be practical. (The geometric games discussed in this section are "ambush" type games. Additional finite games of this type are described in [**8**].)

For f in $\mathfrak{B}$ and R in $\mathfrak{R}$ define $\langle f,R\rangle'$ by

$$\langle f,R\rangle'=\begin{cases}1 \text{ if } (i,f(i))\in\mathfrak{R} \text{ for no } i\\ 0 \text{ if } (i,f(i))\in\mathfrak{R} \text{ for some } i.\end{cases}$$

You can interpret $\langle f,R\rangle'$ as the probability that Blue avoids Red if Blue takes path f and Red occupies the set R. The quantity $\{f,R\}'$ defined as $1-\langle f,R\rangle'$ is the probability that Blue locates at least one of Red's positions. Two basic formulas involving $\langle,\rangle'$ and $\{,\}'$ are

$$\langle f, R \cup S \rangle' = \langle f, R \rangle' \langle f, S \rangle'$$

and

$$\{f, R \cap S\}' = \langle f, R \rangle' \langle f, S \rangle'.$$

You can verify these formulas by using the definitions of $\langle , \rangle'$ and $\{,\}'$ and the fact that the functions take on only the values 0 and 1.

A mixed strategy for Blue may be regarded as a probability measure β and $\mathfrak{B}$ and a mixed strategy for Red as a probability measure ρ on $\mathfrak{R}$. For mixed strategies β and ρ we define $\langle , \rangle''$ and $\langle , \rangle$ by means of the formulas

$$\langle \beta, R \rangle'' = \beta\{f \in \mathfrak{B} : (i, f(i)) \notin R \text{ for all } i\}$$

and

$$\langle \beta, \rho \rangle = \sum_{R \in \mathfrak{R}} \langle \beta, R \rangle'' \rho(\{R\}).$$

The quantity $\langle \beta, R \rangle''$ can be interpreted as the conditional probability that Blue avoids Red's ambush given that Red uses the ambush set (pure strategy) R. Similarly $\langle \beta, \rho \rangle$ can be interpreted as the (unconditional) probability that Blue avoids Red's ambush if Blue uses the mixed strategy β and Red uses the mixed strategy ρ. If β_f is the probability measure on $\mathfrak{B}$ defined by $\beta_f(\mathfrak{A}) = 1$ for $f \in \mathfrak{A}$ and 0 for $f \notin \mathfrak{A}$, and if ρ_R is the probability measure on $\mathfrak{R}$ defined, similarly, by $\rho_R(\mathcal{C}) = 1$ for $R \in \mathcal{C}$ and 0 for $R \notin \mathcal{C}$, then $\langle \beta_f, R \rangle'' = \langle f, R \rangle'$ and $\langle \beta, \rho_R \rangle = \langle \beta, R \rangle''$ for every mixed strategy β for Blue. This means that $\langle , \rangle''$ can be considered as an extension of $\langle , \rangle'$ and $\langle , \rangle$ as an extension of $\langle , \rangle''$. So hereafter we shall drop the primes and write $\langle f, R \rangle$, and $\langle \beta, R \rangle$ instead of $\langle f, R \rangle'$ and $\langle \beta, R \rangle''$, respectively. The definition of $\{,\}$ is extended to mixed strategies by analogous formulas and can be interpreted in terms of Blue locating at least one of Red's positions.

One of the easiest finite ambush games takes place when $\mathfrak{B} = \mathfrak{F}$ and $\mathfrak{R}$ consists of all subsets of L which have no more than k members. The payoff to Blue if Blue plays f in $\mathfrak{B}$ and Red plays R in $\mathfrak{R}$ is $\langle f, R \rangle$. I shall refer to this game as the **Simple Ambush Game** (SAG). If $k \geqslant m$ where m is the number of rows in L, it is obvious that the value of SAG is 0 and that an optimal pure strategy for Red is any set which contains an entire column.

In order to solve SAG, consider the mixed strategy $\rho^{(i,k)}$ for Red defined by

$$\rho^{(i,k)}(R) = \begin{cases} \binom{m}{k}^{-1} & \text{if } R \text{ is one of the } \binom{m}{k} \text{ sets} \\ & \text{having all of its } k \text{ elements} \\ & \text{in the } i\text{th column} \\ 0 & \text{otherwise.} \end{cases} \tag{4}$$

The following theorem reiterates the common sense conclusion that Red can expect to do best in SAG when he places his ambush in a single column.

THEOREM 3. *The value of* SAG *when $k < m$ is equal to $1 - k/m$. A mixed strategy β for Blue is optimal if and only if $\beta\{f\colon f(i) = j\} = 1/m$ for every pair (i,j). Each strategy $\rho^{(i,k)}$ is optimal for Red.*

Proof. Let R be an arbitrary set in $\mathfrak{R}$, and let β be a mixed strategy for Blue satisfying the recommended criterion. Since

$$\{f\colon (i, f(i)) \in R \quad \text{for some } i\} = \bigcup_{(i,j) \in R} \{f\colon f(i) = j\},$$

it follows that the value v of the game satisfies

$$v \geqslant \langle \beta, R \rangle = 1 - \beta\{f\colon (i, f(i)) \in R \quad \text{for some } i\}$$
$$= 1 - \sum_{(i,j) \in R} \beta\{f\colon f(i) = j\} = 1 - k/m.$$

Next suppose f in $\mathfrak{B}$ is arbitrary and $\rho^{(i,k)}$ is given by (4). Let $\mathfrak{D}$ consist of all subsets of the ith column having exactly k elements. There are $\binom{m}{k}$ such sets and each pair (i,j) is in $\binom{m-1}{k-1}$ of them. Thus $\langle f,A\rangle=0$ for $\binom{m-1}{k-1}$ of the sets A in $\mathfrak{D}$ and $\langle f,A\rangle=1$ for the rest. This implies

$$v\leqslant\langle f,\rho^{(i,k)}\rangle=\binom{m}{k}^{-1}\sum_{A\in\mathfrak{D}}\langle f,A\rangle$$

$$=\left[\binom{m}{k}-\binom{m-1}{k-1}\right]\Big/\binom{m}{k}=1-k/m.$$

This proves that the value of the SAG is $1-k/m$ and that the strategies above are optimal.

There are many strategies for Blue which satisfy the criterion of Theorem 3. The simplest is that which gives each of the constant paths f_i (defined by $f_i(j)=i$ for each j) probability $1/m$ and all other paths probability 0. (Choose a row at random and go straight across.) Another is the "completely random" or "wiggly" measure β_* which assigns each f in $\mathfrak{F}$ the same probability, namely m^{-n}.

Even though the solution of SAG is exactly what you would expect by intuition and not terribly hard to obtain, it has a far reaching implication which drastically reduces the variety we can expect to find among finite ambush games. Let C denote the collection of all constant paths. As a generalization of SAG consider the game SAG($\mathfrak{B}$) for which $\mathfrak{R}$ consists of all subsets of L having k or fewer points, $\mathfrak{B}$ is any subset of $\mathfrak{F}$ which contains C and the payoff to Blue is $\langle f,R\rangle$ if Blue plays f in $\mathfrak{B}$ and Red plays $R\in\mathfrak{R}$. The measure β whose value for each $\{f_i\}$ is $1/m$ satisfies the criterion of Theorem 3 so that $\langle\beta,R\rangle\geqslant 1-k/m$ for each R in $\mathfrak{R}$. This means that the value of SAG($\mathfrak{B}$) is at least $1-k/m$. However, Red can use a strategy $\rho^{(i,k)}$ to prevent Blue from obtaining more than $1-k/m$. This proves the following corollary.

COROLLARY 1. *The value v of* SAG($\mathfrak{B}$) *is* $1-k/m$. *An optimal strategy for Blue is the measure β whose value for each $\{f_i\}$ is $1/m$. Each $\rho^{(i,k)}$ is optimal for Red.*

Corollary 1 has the following significance: If Red has no restriction on the set he can choose other than the total number of points it contains, then Blue cannot improve his position in the game by augmenting his capabilities beyond straight line paths. In view of the realistic assumption that Blue will possess the capability to move in straight line paths, it follows that in order to contrive finite ambush games substantively different from SAG, we must place a restriction on the way in which Red can deploy his ambush points.

Consider now a game which differs from SAG in that $\mathfrak{R}$ consists of all subsets of L which have no more than k members and no more than $c\leqslant k$ points in each column. The set $\mathfrak{B}$ of admissible pure strategies for Blue is still taken to be $\mathfrak{F}$ and the payoff to Blue remains $\langle f,R\rangle$ when Red plays R in $\mathfrak{R}$ and Blue plays f in $\mathfrak{F}$. If $c\geqslant m$ where m is the number of rows in L, the value of the game is 0. However, so long as $c<m$, the value of the game will be positive even when $k>m$. I shall call this game the **Column Restricted Ambush Game** (CRAG).

For each pair of integers k and c, there are unique integers p and q such that $k=pc+q$ and $0\leqslant q<c$. Let ρ_0 be the strategy for Red which says: choose $p+1$ columns arbitrarily, say $b_1,\ldots,b_p,b_{p+1}$; then select c points at random in each column $b_1,\ldots,b_p$ and q points at random in column b_{p+1}. For each ambush set A, $\rho_0(A)$ will equal $\left\{\binom{m}{c}^p\binom{m}{q}\right\}^{-1}$. It can be shown, using a series of inequalities which you may find tedious, that in CRAG the strategy ρ_0 is optimal for Red while the wiggly strategy β_* is optimal for Blue. The complete proof of the following theorem is contained in [8].

THEOREM 4. *The value of* CRAG *is* $(1-c/m)^p(1-q/m)$. *The wiggly strategy β_* is optimal for Blue. The strategy ρ_0 described above is optimal for Red.*

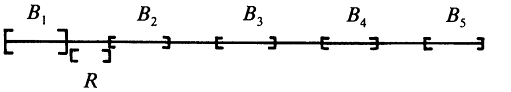
EXAMPLE. "Tactical Use of Mines": The Blue navy is planning to send a battleship through a narrow strait. If the battleship passes through the strait without striking a mine, the Red forces expect to suffer 20,000 casualties. It requires 40 mines placed directly across the strait to ensure that a ship will be hit. The Red navy has 121 mines available and a light plane that can carry 12 mines per flight. However, it is impossible for the plane to return to exactly the same line where it dropped the mines previously. The situation is approximated by a lattice of 4,000 points arranged in 40 rows and 100 columns. Red can occupy a set consisting of no more than 12 points in each column. Commodore Rong argues that Red should place 11 mines at random in each of 11 columns. The probability that Blue will not be hit is then $(1-11/40)^{11} \approx .0291$ so the expected number of casualties for Red will be 582. However, Admiral Wright, who knows Theorem 4, overrules the commodore and points out that 12 mines in 10 columns plus one in a 13th reduces the probability of Blue's passing to $(1-12/40)^{10}(1-1/40) \approx .0275$ which will lead to 550 expected casualties an improvement of 5.5%. (In this example Blue has 40^{100} pure strategies while Red has even more. The impossibility of solving such a game by the techniques of linear programming ought to be obvious.)

Intersection Games on Intervals

The games treated in this section are played on the interval $I=[0,1]$. The collection $\mathfrak{B}$ and $\mathfrak{R}$ of pure strategies for Blue and Red respectively consist of subintervals. The solutions of such games can be generalized to games played upon arbitrary intervals by making a simple change of scale. More details about such games can be found in [7], [9], and [10].

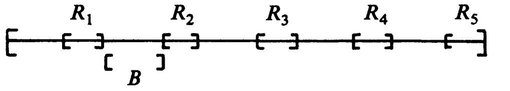
In the **Segment Catcher Game** (SCG), Blue chooses any closed subinterval $B \subseteq I$ of length at least b and Red chooses a closed subinterval R of length at most r. If $B \cap R$ is nonempty, Red receives one; otherwise, he receives 0. If $b=0$ the SCG reduces to the Point Catcher Game whose solution is given by Theorem 1. Clearly if $r+b \geqslant 1$, there is no contest for Red will always win. Suppose that $r+b<1$, and let $e=1/n-(1+1/n)b-r$. The mixed strategy for Blue in SCG analogous to his optimal strategy in the Point Catcher Game is to choose with probability $1/(n+1)$ one of the $n+1$ intervals $[p(r+b+e), b+p(r+b+e)]$ for $p=0,1,\ldots,n$. If Blue adopts this mixed strategy and Red plays the pure strategy $R=[t,t+q]$ where $q \leqslant r$ then, since the intervals from which Blue will choose are separated from each other by at least $r+e$, it follows that R will meet at most one of Blue's possible choices (see FIGURE 8). Therefore, R will meet Blue's choice with probability at most $1/(n+1)$.

The mixed strategy for Red in SCG which resembles his optimal strategy in the Point Catcher Game is to choose with probability $1/(n+1)$ one of the $n+1$ intervals $[(p+1)b+nr,(p+1)(b+r)] \cap I$, for $p=0,1,\ldots,n$. Assume Red adopts the suggested strategy and Blue plays the pure strategy $B=[t,t+q]$ where $q \geqslant b$. Since every point in I is no more than b units from one of the intervals which Red may choose, it follows that Red's choice will meet B with probability at least $1/(n+1)$ (see FIGURE 9). This argument remains valid when r or b (but not both) are zero; i.e., $\mathfrak{R}$ or $\mathfrak{B}$ consist of points. The solution of SCG is summarized in the following theorem.



The Segment Catcher Game with $r=2/27$ and $b=3/25$. An optimal strategy for Blue versus a pure strategy for Red. Here $n=4$, $e=7/270$.

FIGURE 8



The Segment Catcher Game with $r=1/27$ and $b=3/25$. An optimal strategy for Red versus a pure strategy for Blue.

FIGURE 9

THEOREM 5. *If $r+b<1$ the value v of* SCG *is $1/(1+n)$ where n is the largest integer such that $(n+1)b+nr<1$. Let $e=1/n-(1+1/n)b-r$. An optimal strategy for Blue is to choose with probability $1/(n+1)$ one of the $n+1$ intervals $[p(r+b+e), b+p(r+b+e)]$ for $p=0,1,\ldots,n$. An optimal strategy for Red is to choose with probability $1/(n+1)$ one of the $n+1$ intervals $[(p+1)b+pr,(p+1)(b+r)] \cap I$ for $p=0,1,\ldots,n$. (The last interval is $[(n+1)b+nr, r]$.)*

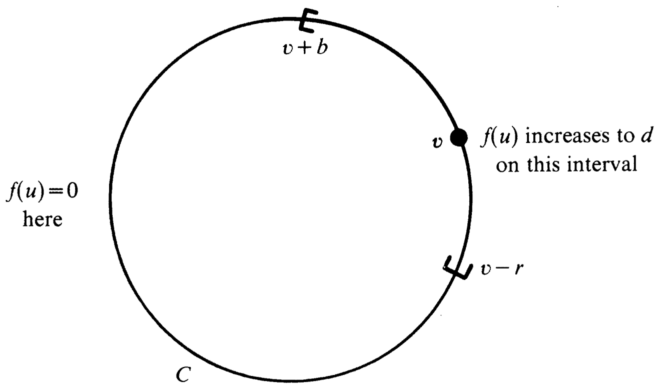
A more complicated game than SCG is the **Overlap Game** (OG). The collections $\mathfrak{R}$ and $\mathfrak{B}$ are the same as in SCG, but the payoff to Red is now the length of $B\cap R$. It is easy to solve a modified OG (COG) played on a circle C of unit circumference. Here $\mathfrak{R}$ and $\mathfrak{B}$ both consist of all closed arcs on C of length r and b, respectively. The payoff to Red is the length of the arc $R\cap B$, or 0 if $R\cap B=\varnothing$. An optimal strategy for Red is to choose a point u on C according to a uniform probability distribution and then occupy the arc $(u,u+r)$ where $u+r$ is the point on C that is r units from u measured counterclockwise along the circle. If Blue chooses the arc $(v,v+b)$, the payoff to Red is given by the formula

$$f(u)=\begin{cases}0 & \text{if } u\notin(v-r,v+b)\\ d(u-v+r) & \text{if } u\in(v-r,v-r+d)\\ d & \text{if } u\in(v-r+d,v+b-d)\\ d(v+b-u) & \text{if } u\in(v+b-d,v+b)\end{cases}$$

where d is the minimum of b and r (see FIGURE 10). Thus the expected payoff to Red is

$$\int_C f(u)\,du=\int_{v-r}^{v-r+d}d(u-v+r)\,du+\int_{v-r+d}^{v+b-d}d\,du+\int_{v+b-d}^{v+b}d(v+b-u)\,du$$
$$=db+dr-d^2=br.$$

If Blue uses the same strategy, he can hold Red's expected payoff to br by the same calculations. Therefore, the value of COG is br and the uniform distribution on C is optimal for both Red and Blue.



The Circular Overlap Game.

FIGURE 10

OG itself is not hard to solve when both r and b are unit fractions; say $r=1/m$ and $b=1/n$. The value of OG is then rb, just as in COG. An optimal strategy for Red is to occupy one of the intervals $[p/m,p+1/m]$, $p=0,1,\ldots,m-1$ with probability $1/m$. The analogous strategy is optimal for Blue. For if Red employs the strategy suggested and Blue selects the interval B, the expected payoff to Red will be

$$\sum_{p=1}^{m} l(B\cap[p/m,p+1/m])1/m=1/ml(B)=b/m=rb$$

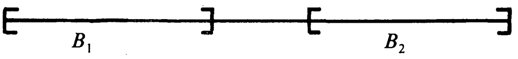
where $l(B)$ means the length of B. A similar calculation shows that Blue can hold Red to the same expected payoff if he uses the corresponding strategy.

It is the presence of end points on I which makes OG more complicated than COG. In order to describe the solution of OG, I shall introduce two possible strategies available to Red or Blue, namely the gap strategy and the lap strategy.

The **gap strategy** for Blue is described as follows. Let $g=1-b[1/b]$ and $s=g/([1/b]-1)$, where [ ] denotes the greatest integer function. Blue occupies one of the $[1/b]$ intervals $[k(b+s),k(b+s)+b]$ for $k=0,1,\ldots,([1/b]-1)$ with probability $1/[1/b]$. The last interval in the gap strategy is $[1-b,1]$. The **lap strategy** for Blue is described as follows: Let $t=(b[1/b]+b-1)/[1/b]=(b-g)/[1/b]$, and let Blue occupy one of the $[1/b]+1$ intervals $[k(b-t),k(b-t)+b]$ for $k=0,1,\ldots,[1/b]$. The last interval in the lap strategy is $[1-b,1]$, since $[1/b](b-t)=[1/b]b-b+g=1-b$.

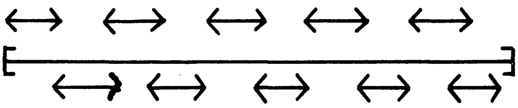
The gap strategy for Red is to occupy with probability $[1/r]^{-1}$ one of the $[1/r]$ intervals $[k(r+v),k(r+v)+r]$ for $k=1,2,\ldots,[1/r]$, where $v=(1-[1/r]r/([1/r]+1)$. The lap strategy for Red is to occupy with probability $([1/r]+1)^{-1}$ one of the $[1/r]+1$ intervals $[k(r-w),k(r-w)+r]$ for $k=0,1,\ldots,[1/r]$, where w is equal to $(r+r[1/r]-1)/[1/r]$.

Some examples of the gap and lap strategies are illustrated in FIGURES 11–14. The complete solution of OG requires four cases. Since the proof is rather tedious, we shall give only the proof of Case I, as a typical example. The complete argument can be found in [10].



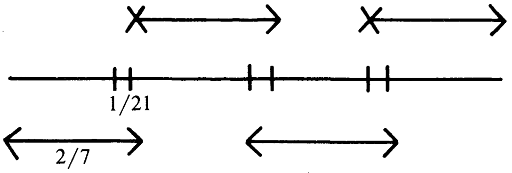
The gap strategy for Blue when $b=2/5$; occupy one of the intervals with probability 1/2. Here $s=g=1/5$.

FIGURE 11



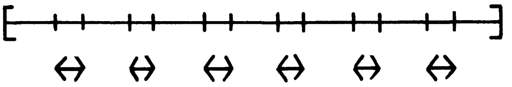
The gap strategy for Blue when $b=1/10$: occupy one interval with probability 1/10. Here $g=s=0$.

FIGURE 12



The lap strategy for Blue when $b=2/7$: occupy one interval with probability 1/4.

FIGURE 13



The antigap strategy for Red when $b=3/20$ and $r=1/20$: occupy one of the intervals with probability 1/6. Here g is 1/10 and $m=3$.

FIGURE 14

THEOREM 6. The solution of the Overlap Game.

I. *If $r\leqslant b$ and $b-r\geqslant 1-b[1/b]$ the value of* OG *is $r/[1/b]$. An optimal strategy for Blue is the gap strategy. An optimal strategy for Red is the* **antigap strategy** *of occupying with probability $1[1/b]$ one of the $[1/b]$ intervals $[kb-r,kb]$ for $k=1,2,\ldots,m$, or $[kb+g,kb+g+r]$ for $k=m+1,\ldots,[1/b]-1$. (Here m is any integer with $1<m<[1/b]$.)*

II. *If $r\leqslant b$ and $b-r<1-b[1/b]$ the value of* OG *is $(r+t)/(1+[1/b])$. An optimal strategy for Blue is the lap strategy. An optimal strategy for Red is the* **antilap strategy** *determined as follows: let $u=(r-t[1/b])/([1/b]+1)=(1-b[1/b]-b+r)/([1/b]+1)$ and occupy one of the $[1/b]$ intervals $[k(b+u)-r,k(b+u)]$ for $k=1,2,\ldots,[1/b]$ with probability $[1/b]^{-1}$.*

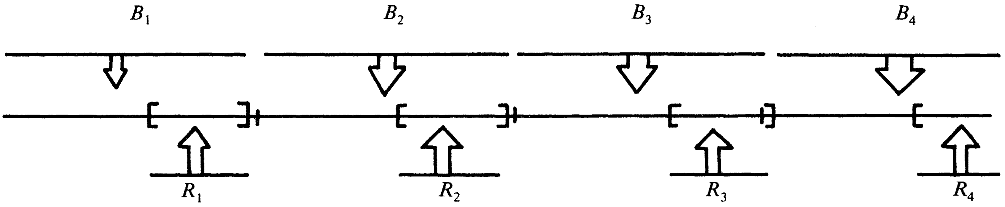
III. *If $r>b$ and $1-[1/r]r\leqslant b$ the value of* OG *is $(b-v)/[1/r]$. An optimal strategy for Red is the gap strategy. An optimal strategy for Blue is the antigap strategy described as follows: occupy with probability $([1/r]+1)^{-1}$ one of the $[1/r]+1$ intervals $[k(r-x),k(r-x)+b]$ for $k=0,1,\ldots,[1/r]$, where $x=[1/r]^{-1}(b-(1-[1/r]r))$.*

IV. *If $r>b$ and $d=1-[1/r]r>b$ the value of* OG *is $b/(1+[1/r])$. An optimal strategy for Red is the lap strategy. An optimal strategy for Blue is the following antilap strategy: occupy with probability $([1/r]+1)^{-1}$ one of the $(1+[1/r])$ intervals $[kr,kr+b]$ for $k=0,1,2,\ldots,m$ or $[kr+d-b,kr+d]$ for $k=m+1,\ldots,[1/r]$. (Here m is any integer with $0<m<[1/r]$.)*

Proof of Case I. Suppose in Case I Blue employs the gap strategy (interval) R. The largest expected payoff for Red occurs when R is entirely contained in one of the intervals comprising the gap strategy. Thus Red can expect at most $r/[1/b]$.

Suppose Red uses the antigap strategy and Blue plays a pure strategy B. Since B has length $b > r+g$, it will contain subintervals having total length at least r of two of the intervals comprising the antigap strategy. The worst possible case for Red occurs when B spans $[mb, mb+g]$, but even then B has intersection with $[mb-r, mb] \cup [mb+g, mb+g+a]$ of length at least r. Therefore, Red can expect at least $r/[1/b]$.

EXAMPLE. "Defense of a Line": The Red army has a single machine gun unit with which to defend a line 4100 yards long. The gun unit can control a circle of 400 yards diameter. The Blue army intends to penetrate the line along a front of 1000 yards. The payoff to Red is proportional to the length of the Blue line which comes within the range of his gun. This is an example of OG with $r = 4/41$, $b = 10/41$. Since $b - r = 6/41 \geqslant 1/41 = 1 - [1/b]$ this encounter is an example of Case I. By Theorem 6 its value is (proportional to) 16/41. An optimal strategy for Blue (see FIGURE 15) is to attempt penetration along one of the following four fronts with probability 1/4: 0 to 1000 yards; 1033 to 2033 yards; 2066 to 3066 yards; 3099 to 4099 yards. An optimal strategy for Red is to control with probability 1/4 one of the following fronts: 600 to 1000 yards; 1600 to 2000 yards; 2700 to 3100 yards; 3700 to 4100 yards. Here the m in the antigap strategy equals 3.



Defense of a Line. Blue advances along one of four fronts; Red defends one of four fronts.

FIGURE 15

Some More Geometric Games

Here are some more geometric games that can be solved with techniques similar to those treated in this article. The first three are on a rectangular lattice L, the fourth on a linear lattice, and the last three on the interval $[0,1]$.

1. Red chooses a subset R of L having at least k members and Blue chooses a path f in $\mathfrak{F}$. If Blue encounters any point of R he receives one, otherwise zero. Thus the payoff to Blue is $\{f, R\}$, defined in the middle section of this article.

2. This game is the same as the preceding one, except now the payoff to Blue is the number of members of R which he encounters.

3. Red chooses a subset R of L without restriction and Blue chooses any path f in $\mathfrak{F}$. If Blue finds Red, then Red receives 0. Otherwise he receives the number of points in R.

4. Red chooses a sequence of m consecutive integers between 1 and p; Blue chooses a sequence B of n consecutive integers between 1 and p. The payoff to Red is the number of integers in $R \cap B$.

5. Red chooses a subinterval R of $[0,1]$ having length at most r; Blue may choose an interval B of any length b and receive b if $R \cap B$ is empty and 0 otherwise.

6. Red and Blue choose points r and b respectively on a sphere S. If the distance from r to b measured linearly is less than a preassigned quantity, then Red receives 1; otherwise Red receives 0.

7. The solution to the previous game is relatively easy, yet the analogous game played on a unit disc appears to be much more difficult. Red chooses a point r on a disc D of unit radius and Blue chooses a point b in D. If $r-b \leqslant c$, then Red receives 1; otherwise he receives 0. [4] contains a beautiful solution to this problem when $c=1/2$.

In preparing this article I have benefited from the suggestions of Richard Beaudoin, William Park (Clemson undergraduate students), H. Kaneko (a Clemson graduate student) and two referees.

References

[1] Melvin Dresher, Games of Strategy—Theory and Application, Prentice-Hall, Englewoods Cliffs, N.J., 1961.

[2] W. Feller, An Introduction to Probability Theory and its Applications, Vol. I, John Wiley, New York, 1957.

[3] David Gale, The Theory of Linear Economic Models, McGraw-Hill, New York, Toronto, London, 1960.

[4] D. Gale and C. R. Glassey, Problem E 2469, Amer. Math. Monthly, 81 (1974) 405; solution by Roger Evans, Amer. Math. Monthly, 82 (1975) 521.

[5] P. R. Halmos, Measure Theory, D. Van Nostrand, New York, 1950.

[6] G. Owen, Game Theory, Saunders, Philadelphia, 1968.

[7] J. R. Reay and W. Ruckle, Ambushing random walks III—more continuous models, Clemson Univ. Technical Report #284.

[8] W. Ruckle, R. Fennell, P. T. Holmes, and C. Fennemore, Ambushing random walks I—finite models, Operations Res. 24 (1976) 314–324.

[9] W. Ruckle, Ambushing random walks II—continuous models, Clemson Univ. Technical Report #235; to appear in Operations Res.

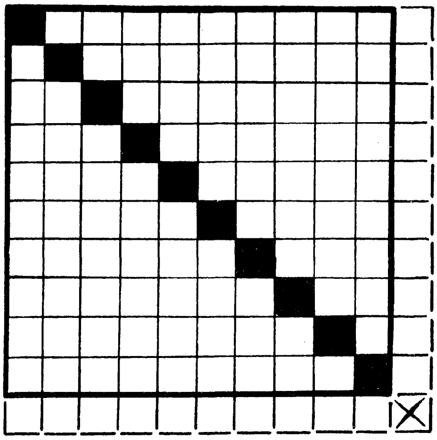
[10] W. Ruckle, Some examples of geometric games, Clemson Univ. Technical Report #273.

[11] J. von Neumann and O. Morgenstern, Games and Economic Behaviour, Princeton Univ. Press, Princeton, N.J., 1947.

Proofs Without Words: Combinatorial Identities

$$\binom{n}{2} = \tfrac{1}{2}(n^2-n) = \Sigma_{i=1}^{n-1} i$$

$$\binom{n+1}{2} = \binom{n}{2} + n$$



—James O. Chilaka
Laguardia C. College
City University of New York
Brooklyn, New York 11235

The Three Crises in Mathematics: Logicism, Intuitionism and Formalism

Crises in classical philosophy reveal doubts about mathematical and philosophical criteria for a satisfactory foundation for mathematics.

Ernst Snapper
Dartmouth College
Hanover, NH 03755

The three schools, mentioned in the title, all tried to give a firm foundation to mathematics. The three crises are the failures of these schools to complete their tasks. This article looks at these crises "through modern eyes," using whatever mathematics is available today and not just the mathematics which was available to the pioneers who created these schools. Hence, this article does not approach the three crises in a strictly historical way. This article also does not discuss the large volume of current, technical mathematics which has arisen out of the techniques introduced by the three schools in question. One reason is that such a discussion would take a book and not a short article. Another one is that all this technical mathematics has very little to do with the philosophy of mathematics, and in this article I want to stress those aspects of logicism, intuitionism, and formalism which show clearly that these schools are founded in philosophy.

Logicism

This school was started in about 1884 by the German philosopher, logician and mathematician, Gottlob Frege (1848–1925). The school was rediscovered about eighteen years later by Bertrand Russell. Other early logicists were Peano and Russell's coauthor of Principia Mathematica, A. N. Whitehead. The purpose of logicism was to show that classical mathematics is part of logic. If the logicists had been able to carry out their program successfully, such questions as "Why is classical mathematics free of contradictions?" would have become "Why is logic free of contradictions?". This latter question is one on which philosophers have at least a thorough handle and one may say in general that the successful completion of the logicists' program would have given classical mathematics a firm foundation in terms of logic.

Clearly, in order to carry out this program of the logicists, one must first, somehow, define what "classical mathematics" is and what "logic" is. Otherwise, what are we supposed to show is part of what? It is precisely at these two definitions that we want to look through modern eyes, imagining that the pioneers of logicism had all of present-day mathematics available to them. We begin with classical mathematics.

In order to carry out their program, Russell and Whitehead created *Principia Mathematica* **[10]** which was published in 1910. (The first volume of this classic can be bought for $3.45! Thank heaven, only modern books and not the classics have become too expensive for the average reader.) *Principia*, as we will refer to *Principia Mathematica*, may be considered as a formal set theory. Although the formalization was not entirely complete, Russell and Whitehead thought that it was and planned to use it to show that mathematics can be reduced to logic. They showed that all classical mathematics, known in their time, can be derived from set theory and hence from the axioms of *Principia*. Consequently, what remained to be done, was to show that all the axioms of *Principia* belong to logic.

Of course, instead of *Principia*, one can use any other formal set theory just as well. Since today the formal set theory developed by Zermelo and Fraenkel (ZF) is so much better known than *Principia*, we shall from now on refer to ZF instead of *Principia*. ZF has only nine axioms and, although several of them are actually axiom schemas, we shall refer to all of them as "axioms." The formulation of the logicists' program now becomes: Show that all nine axioms of ZF belong to logic.

This formulation of logicism is based on the thesis that classical mathematics can be defined as the set of theorems which can be proved within ZF. This definition of classical mathematics is far from perfect, as is discussed in [**12**]. However, the above formulation of logicism is satisfactory for the purpose of showing that this school was not able to carry out its program. We now turn to the definition of logic.

In order to understand logicism, it is very important to see clearly what the logicists meant by "logic." The reason is that, whatever they meant, they certainly meant more than classical logic. Nowadays, one can define classical logic as consisting of all those theorems which can be proven in first order languages (discussed below in the section on formalism) without the use of nonlogical axioms. We are hence restricting ourselves to first order logic and use the deduction rules and logical axioms of that logic. An example of such a theorem is the law of the excluded middle which says that, if p is a proposition, then either p or its negation $\neg p$ is true; in other words, the proposition $p \vee \neg p$ is always true where $\vee$ is the usual symbol for the inclusive "or."

If this definition of classical logic had also been the logicists' definition of logic, it would be a folly to think for even one second that all of ZF can be reduced to logic. However, the logicists' definition was more extensive. They had a general concept as to when a proposition belongs to logic, that is, when a proposition should be called a "logical proposition." They said: *A logical proposition is a proposition which has complete generality and is true in virtue of its form rather than its content.* Here, the word "proposition" is used as synonymous with "theorem."

For example, the above law of the excluded middle "$p \vee \neg p$" is a logical proposition. Namely, this law does not hold because of any special content of the proposition p; it does not matter whether p is a proposition of mathematics or physics or what have you. On the contrary, this law holds with "complete generality," that is, for any proposition p whatsoever. Why then does it hold? The logicists answer: "Because of its form." Here they mean by form "syntactical form," the form of $p \vee \neg p$ being given by the two connectives of everyday speech, the inclusive "or" and the negation "not" (denoted by $\vee$ and $\neg$, respectively).

On the one hand, it is not difficult to argue that all theorems of classical logic, as defined above, are logical propositions in the sense of logicism. On the other hand, there is no *a priori* reason to believe that there could not be logical propositions which lie outside of classical logic. This is why we said that the logicists' definition of logic is more extensive than the definition of classical logic. And now the logicists' task becomes clearer: It consists in showing that all nine axioms of ZF are logical propositions in the sense of logicism.

The only way to assess the success or failure of logicism in carrying out this task is by going through all nine axioms of ZF and determining for each of them whether it falls under the logicists' concept of a logical proposition. This would take a separate article and would be of interest only to readers who are thoroughly familiar with ZF. Hence, instead, we simply state that at least two of these axioms, namely, the axiom of infinity and the axiom of choice, cannot possibly be considered as logical propositions. For example, the axiom of infinity says that there exist infinite sets. Why do we accept this axiom as being true? The reason is that everyone is familiar with so many infinite sets, say, the set of the natural numbers or the set of points in Euclidean 3-space. Hence, we accept this axiom on grounds of our everyday experience with sets, and this clearly shows that we accept it in virtue of its content and not in virtue of its syntactical form. In general, when an axiom claims the existence of objects with which we are familiar on grounds of our common everyday experience, it is pretty certain that this axiom is not a logical proposition in the sense of logicism.

And here then is the first crisis in mathematics: Since at least two out of the nine axioms of ZF are not logical propositions in the sense of logicism, it is fair to say that this school failed by about 20% in its effort to give mathematics a firm foundation. However, logicism has been of the greatest importance for the development of modern mathematical logic. In fact, it was logicism which started mathematical logic in a serious way. The two quantifiers, the "for all" quantifier $\forall$ and the "there exists" quantifier $\exists$ were introduced into logic by Frege **[5]**, and the influence of *Principia* on the development of mathematical logic is history.

It is important to realize that logicism is founded in philosophy. For example, when the logicists tell us what they mean by a logical proposition (above), they use philosophical and not mathematical language. They have to use philosophical language for that purpose since mathematics simply cannot handle definitions of so wide a scope.

The philosophy of logicism is sometimes said to be based on the philosophical school called "realism." In medieval philosophy "realism" stood for the Platonic doctrine that abstract entities have an existence independent of the human mind. Mathematics is, of course, full of abstract entities such as numbers, functions, sets, etc., and according to Plato all such entities exist outside our mind. The mind can discover them but does not create them. This doctrine has the advantage that one can accept such a concept as "set" without worrying about how the mind can construct a set. According to realism, sets are there for us to discover, not to be constructed, and the same holds for all other abstract entities. In short, realism allows us to accept many more abstract entities in mathematics than a philosophy which had limited us to accepting only those entities the human mind can construct. Russell was a realist and accepted the abstract entities which occur in classical mathematics without questioning whether our own minds can construct them. This is the fundamental difference between logicism and intuitionism, since in intuitionism abstract entities are admitted only if they are man made.

Excellent expositions of logicism can be found in Russell's writing, for example **[9]**, **[10]** and **[11]**.

Intuitionism

This school was begun about 1908 by the Dutch mathematician, L. E. J. Brouwer (1881–1966). The intuitionists went about the foundations of mathematics in a radically different way from the logicists. The logicists never thought that there was anything wrong with classical mathematics; they simply wanted to show that classical mathematics is part of logic. The intuitionists, on the contrary, felt that there was plenty wrong with classical mathematics.

By 1908, several paradoxes had arisen in Cantor's set theory. Here, the word "paradox" is used as synonymous with "contradiction." Georg Cantor created set theory, starting around 1870, and he did his work "naively," meaning nonaxiomatically. Consequently, he formed sets with such abandon that he himself, Russell and others found several paradoxes within his theory. The logicists considered these paradoxes as common errors, caused by erring mathematicians and not by a faulty mathematics. The intuitionists, on the other hand, considered these paradoxes as clear indications that classical mathematics itself is far from perfect. They felt that mathematics had to be rebuilt from the bottom on up.

The "bottom," that is, the beginning of mathematics for the intuitionists, is their explanation of what the natural numbers $1,2,3,\ldots$ are. (Observe that we do not include the number zero among the natural numbers.) According to intuitionistic philosophy, all human beings have a primordial intuition for the natural numbers within them. This means in the first place that we have an immediate certainty as to what is meant by the number 1 and, secondly, that the mental process which goes into the formation of the number 1 can be repeated. When we do repeat it, we obtain the concept of the number 2; when we repeat it again, the concept of the number 3; in this way, human beings can construct any *finite* initial segment $1,2,\ldots,n$ for any natural number n. This mental construction of one natural number after the other would never have been possible if we did not have an awareness of time within us. "After" refers to time and Brouwer agrees with the philosopher Immanuel Kant (1724–1804) that human beings have an immediate awareness of time. Kant used the word "intuition" for "immediate awareness" and this is where the name "intuitionism" comes from. (See Chapter IV of [**4**] for more information about this intuitionistic concept of natural numbers.)

It is important to observe that the intuitionistic construction of natural numbers allows one to construct only arbitrarily long *finite* initial segments $1,2,\ldots,n$. It does not allow us to construct that whole closed set of all the natural numbers which is so familiar from classical mathematics. It is equally important to observe that this construction is both "inductive" and "effective." It is inductive in the sense that, if one wants to construct, say, the number 3, one has to go through all the mental steps of first constructing the 1, then the 2, and finally the 3; one cannot just grab the number 3 out of the sky. It is effective in the sense that, once the construction of a natural number has been finished, that natural number has been constructed in its entirety. It stands before us as a completely finished mental construct, ready for our study of it. When someone says, "I have finished the mental construction of the number 3," it is like a bricklayer saying, "I have finished that wall," which he can say only after he has laid every stone in place.

We now turn to the intuitionistic definition of mathematics. According to intuitionistic philosophy, mathematics should be defined as a mental activity and not as a set of theorems (as was done above in the section on logicism). It is the activity which consists in carrying out, one after the other, those mental constructions which are inductive and effective in the sense in which the intuitionistic construction of the natural numbers is inductive and effective. Intuitionism maintains that human beings are able to recognize whether a given mental construction has these two properties. We shall refer to a mental construction which has these two properties as a **construct** and hence the intuitionistic definition of mathematics says: *Mathematics is the mental activity which consists in carrying out constructs one after the other.*

A major consequence of this definition is that all of intuitionistic mathematics is effective or "constructive" as one usually says. We shall use the adjective "constructive" as synonymous with "effective" from now on. Namely, every construct is constructive, and intuitionistic mathematics is nothing but carrying out constructs over and over. For instance, if a real number

r occurs in an intuitionistic proof or theorem, it never occurs there merely on grounds of an existence proof. It occurs there because it has been constructed from top to bottom. This implies for example that each decimal place in the decimal expansion of r can in principle be computed. In short, all intuitionistic proofs, theorems, definitions, etc., are entirely constructive.

Another major consequence of the intuitionistic definition of mathematics is that mathematics cannot be reduced to any other science such as, for instance, logic. This definition comprises too many mental processes for such a reduction. And here, then, we see a radical difference between logicism and intuitionism. In fact, the intuitionistic attitude toward logic is precisely the opposite from the logicists' attitude: According to the intuitionists, whatever valid logical processes there are, they are all constructs; hence, the valid part of classical logic is part of mathematics! Any law of classical logic which is not composed of constructs is for the intuitionist a meaningless combination of words. It was, of course, shocking that the classical law of the excluded middle turned out to be such a meaningless combination of words. This implies that this law cannot be used indiscriminately in intuitionistic mathematics; it can often be used, but not always.

Once the intuitionistic definition of mathematics has been understood and accepted, all there remains to be done is to do mathematics the intuitionistic way. Indeed, the intuitionists have developed intuitionistic arithmetic, algebra, analysis, set theory, etc. However, in each of these branches of mathematics, there occur classical theorems which are not composed of constructs and, hence, are meaningless combinations of words for the intuitionists. Consequently, one cannot say that the intuitionists have reconstructed all of classical mathematics. This does not bother the intuitionists since whatever parts of classical mathematics they cannot obtain are meaningless for them anyway. Intuitionism does not have as its purpose the justification of classical mathematics. Its purpose is to give a valid definition of mathematics and then to "wait and see" what mathematics comes out of it. Whatever classical mathematics cannot be done intuitionistically simply is not mathematics for the intuitionist. We observe here another fundamental difference between logicism and intuitionism: The logicists wanted to justify all of classical mathematics. (An excellent introduction to the actual techniques of intuitionism is **[8]**.)

Let us now ask how successful the intuitionistic school has been in giving us a good foundation for mathematics, acceptable to the majority of mathematicians. Again, there is a sharp difference between the way this question has to be answered in the present case and in the case of logicism. Even hard-nosed logicists have to admit that their school so far has failed to give mathematics a firm foundation by about 20%. However, a hard-nosed intuitionist has every right in the world to claim that intuitionism has given mathematics an entirely satisfactory foundation. There is the meaningful definition of intuitionistic mathematics, discussed above; there is the intuitionistic philosophy which tells us why constructs can never give rise to contradictions and, hence, that intuitionistic mathematics is free of contradictions. In fact, not only this problem (of freedom from contradiction) but all other problems of a foundational nature as well receive perfectly satisfactory solutions in intuitionism.

Yet if one looks at intuitionism from the outside, namely, from the viewpoint of the classical mathematician, one has to say that intuitionism has failed to give mathematics an adequate foundation. In fact, the mathematical community has almost universally rejected intuitionism. Why has the mathematical community done this, in spite of the many very attractive features of intuitionism, some of which have just been mentioned?

One reason is that classical mathematicians flatly refuse to do away with the many beautiful theorems that are meaningless combinations of words for the intuitionists. An example is the Brouwer fixed point theorem of topology which the intuitionists reject because the fixed point cannot be constructed, but can only be shown to exist on grounds of an existence proof. This, by the way, is the same Brouwer who created intuitionism; he is equally famous for his work in (nonintuitionistic) topology.

A second reason comes from theorems which can be proven both classically and intuitionistically. It often happens that the classical proof of such a theorem is short, elegant, and devilishly clever, but not constructive. The intuitionists will of course reject such a proof and replace it by their own constructive proof of the same theorem. However, this constructive proof frequently turns out to be about ten times as long as the classical proof and often seems, at least to the classical mathematician, to have lost all of its elegance. An example is the fundamental theorem of algebra which in classical mathematics is proved in about half a page, but takes about ten pages of proof in intuitionistic mathematics. Again, classical mathematicians refuse to believe that their clever proofs are meaningless whenever such proofs are not constructive.

Finally, there are the theorems which hold in intuitionism but are false in classical mathematics. An example is the intuitionistic theorem which says that every real-valued function which is defined for *all* real numbers is continuous. This theorem is not as strange as it sounds since it depends on the intuitionistic concept of a function: A real-valued function f is defined in intuitionism for all real numbers only if, for every real number r whose intuitionistic construction has been completed, the real number $f(r)$ can be constructed. Any obviously discontinuous function a classical mathematician may mention does not satisfy this constructive criterion. Even so, theorems such as this one seem so far out to classical mathematicians that they reject any mathematics which accepts them.

These three reasons for the rejection of intuitionism by classical mathematicians are neither rational nor scientific. Nor are they pragmatic reasons, based on a conviction that classical mathematics is better for applications to physics or other sciences than is intuitionism. They are all emotional reasons, grounded in a deep sense as to what mathematics is all about. (If one of the readers knows of a truly scientific rejection of intuitionism, the author would be grateful to hear about it.) We now have the second crisis in mathematics in front of us: It consists in the failure of the intuitionistic school to make intuitionism acceptable to at least the majority of mathematicians.

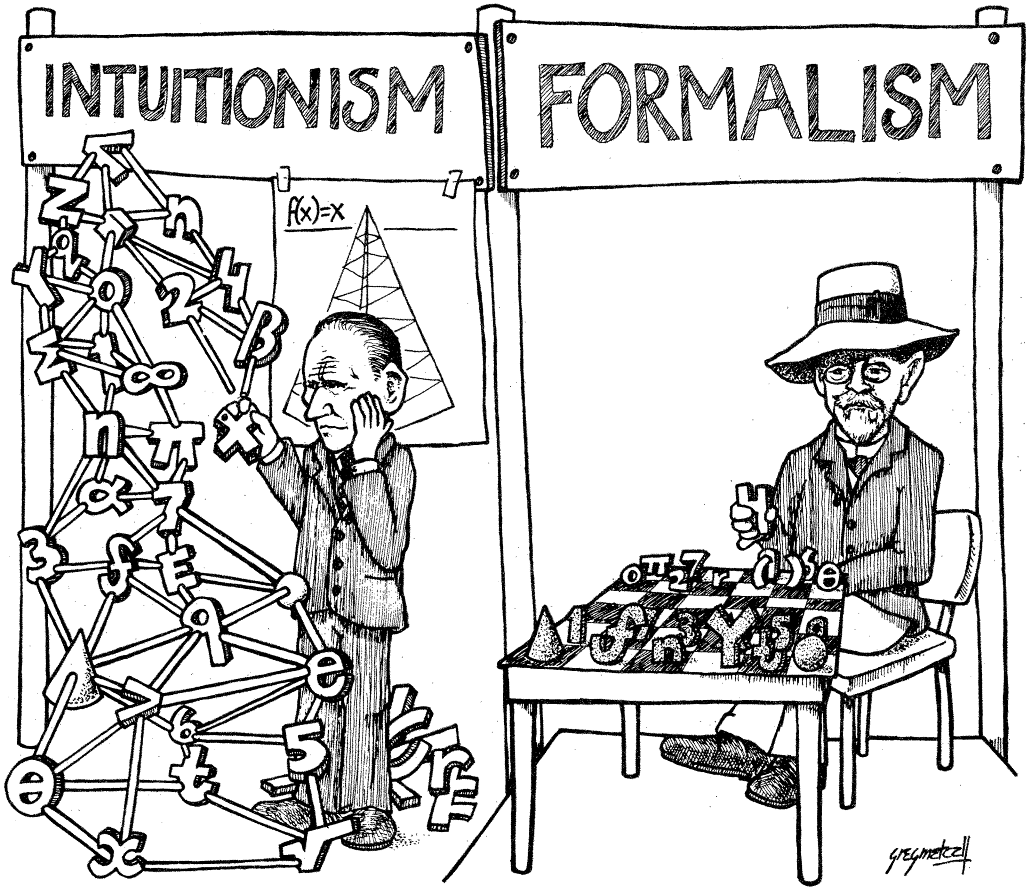
It is important to realize that, like logicism, intuitionism is rooted in philosophy. When, for instance, the intuitionists state their definition of mathematics, given earlier, they use strictly philosophical and not mathematical language. It would, in fact, be quite impossible for them to use mathematics for such a definition. The mental activity which is mathematics can be defined in philosophical terms but this definition must, by necessity, use some terms which do not belong to the activity it is trying to define.

Just as logicism is related to realism, intuitionism is related to the philosophy called "conceptualism." This is the philosophy which maintains that abstract entities exist only insofar as they are constructed by the human mind. This is very much the attitude of intuitionism which holds that the abstract entities which occur in mathematics, whether sequences or order-relations or what have you, are all mental constructions. This is precisely why one does not find in intuitionism the staggering collection of abstract entities which occur in classical mathematics and hence in logicism. The contrast between logicism and intuitionism is very similar to the contrast between realism and conceptualism.

A very good way to get into intuitionism is by studying **[8]**, Chapter IV of **[4]**, **[2]** and **[13]**, in this order.

Formalism

This school was created in about 1910 by the German mathematician David Hilbert (1862–1943). True, one might say that there were already formalists in the nineteenth century since Frege argued against them in the second volume of his *Grundgesetze der Arithmetik* (see the book by Geach and Black under **[5]**, pages 182–233); the first volume of the *Grundgesetze* appeared in 1893 and the second one in 1903. Nevertheless, the modern concept of formalism, which includes finitary reasoning, must be credited to Hilbert. Since modern books and courses in mathematical logic usually deal with formalism, this school is much better known today than either logicism or intuitionism. We will hence discuss only the highlights of formalism and begin by asking, "What is it that we formalize when we formalize something?"



The answer is that we formalize some given *axiomatized* theory. One should guard against confusing axiomatization and formalization. Euclid axiomatized geometry in about 300 B.C., but formalization started only about 2200 years later with the logicists and formalists. Examples of axiomatized theories are Euclidean plane geometry with the usual Euclidean axioms, arithmetic with the Peano axioms, ZF with its nine axioms, etc. The next question is: "How do we formalize a given axiomatized theory?"

Suppose then that some axiomatized theory T is given. Restricting ourselves to first order logic, "to formalize T" means to choose an appropriate first order language for T. The vocabulary of a first order language consists of five items, four of which are always the same and are not dependent on the given theory T. These four items are the following: (1) A list of denumerably many variables—who can talk about mathematics without using variables? (2) Symbols for the connectives of everyday speech, say $\neg$ for "not," $\wedge$ for "and," $\vee$ for the inclusive "or," $\rightarrow$ for "if then," and $\leftrightarrow$ for "if and only if"—who can talk about anything at all without using connectives? (3) The equality sign $=$; again, no one can talk about mathematics without using this sign. (4) The two quantifiers, the "for all" quantifier $\forall$ and the "there exist" quantifier $\exists$; the first one is used to say such things as "*all* complex numbers have a square root," the second one to say things like "*there exist* irrational numbers." One can do without some of the above symbols, but there is no reason to go into that. Instead, we turn to the fifth item.

Since T is an axiomatized theory, it has so called "undefined terms." One has to choose an appropriate symbol for every undefined term of T and these symbols make up the fifth item. For instance, among the undefined terms of plane Euclidean geometry, occur "point," "line," and "incidence," and for each one of them an appropriate symbol must be entered into the vocabulary of the first order language. Among the undefined terms of arithmetic occur "zero," "addition," and "multiplication," and the symbols one chooses for them are of course 0, +, and ×, respectively. The easiest theory of all to formalize is ZF since this theory has only one undefined term, namely, the membership relation. One chooses, of course, the usual symbol $\in$ for that relation. These symbols, one for each undefined term of the axiomatized theory T, are often called the "parameters" of the first order language and hence the parameters make up the fifth item.

Since the parameters are the only symbols in the vocabulary of a first order language which depend on the given axiomatized theory T, one formalizes T simply by choosing these parameters. Once this choice has been made, the whole theory T has been completely formalized. One can now express in the resulting first order language L not only all axioms, definitions, and theorems of T, but more! One can also express in L all axioms of classical logic and, consequently, also all proofs one uses to prove theorems of T. In short, one can now proceed entirely within L, that is, entirely "formally."

But now a third question presents itself: "Why in the world would anyone want to formalize a given axiomatized theory?" After all, Euclid never saw a need to formalize his axiomatized geometry. It is important to ask this question, since even the great Peano had mistaken ideas about the real purpose of formalization. He published one of his most important discoveries in differential equations in a formalized language (very similar to a first order language) with the result that nobody read it until some charitable soul translated the article into common German.

Let us now try to answer the third question. If mathematicians do technical research in a certain branch of mathematics, say, plane Euclidean geometry, they are interested in discovering and proving the important theorems of the branch of mathematics. For that kind of technical work, formalization is usually not only no help but a definite hindrance. If, however, one asks such foundational questions as, for instance, "Why is this branch of mathematics free of contradictions?", then formalization is not just a help but an absolute necessity.

It was really Hilbert's stroke of genius to understand that formalization is the proper technique to tackle such foundational questions. What he taught us can be put roughly as follows. Suppose that T is an axiomatized theory which has been formalized in terms of the first order language L. This language has such a precise syntax that it itself can be studied as a *mathematical* object. One can ask for instance: "Can one possibly run into contradictions if one proceeds entirely formally within L, using only the axioms of T and those of classical logic, all of which have been expressed in L?" If one can prove mathematically that the answer to this question is "no," one has there a mathematical proof that the theory T is free of contradictions!

This is basically what the famous "Hilbert program" was all about. The idea was to formalize the various branches of mathematics and then to prove *mathematically* that each one of them is free of contradictions. In fact if, by means of this technique, the formalists could have just shown that ZF is free of contradictions, they would thereby already have shown that all of classical mathematics is free of contradictions, since classical mathematics can be done axiomatically in terms of the nine axioms of ZF. In short, the formalists tried to create a mathematical technique by means of which one could prove that mathematics is free of contradictions. This was the original purpose of formalism.

It is interesting to observe that both logicists and formalists formalized the various branches of mathematics, but for entirely different reasons. The logicists wanted to use such a formalization to show that the branch of mathematics in question belongs to logic; the formalists wanted to use it to prove mathematically that that branch is free of contradictions. Since both schools "formalized," they are sometimes confused.

Did the formalists complete their program successfully? No! In 1931, Kurt Gödel showed in [6] that formalization cannot be considered as a mathematical technique by means of which one can prove that mathematics is free of contradictions. The theorem in that paper which rang the death bell for the Hilbert program concerns axiomatized theories which are free of contradictions and whose axioms are strong enough so that arithmetic can be done in terms of them. Examples of theories whose axioms are that strong are, of course, Peano arithmetic and ZF. Suppose now that T is such a theory and that T has been formalized by means of the first order language L. Then Gödel's theorem says, in nontechnical language, "No sentence of L which can be interpreted as asserting that T is free of contradictions can be proven formally within the language L."Although the interpretation of this theorem is somewhat controversial, most mathematicians have concluded from it that the Hilbert program cannot be carried out: Mathematics is not able to prove its own freedom of contradictions. Here, then, is the third crisis in mathematics.

Of course, the tremendous importance of the formalist school for present-day mathematics is well known. It was in this school that modern mathematical logic and its various offshoots, such as model theory, recursive function theory, etc., really came into bloom.

Formalism, as logicism and intuitionism, is founded in philosophy, but the philosophical roots of formalism are somewhat more hidden than those of the other two schools. One can find them, though, by reflecting a little on the Hilbert program.

Let again T be an axiomatized theory which has been formalized in terms of the first order language L. In carrying out Hilbert's program, one has to talk about the language L as one object, and while doing this, one is not talking within that safe language L itself. On the contrary, one is talking about L in ordinary, everyday language, be it English or French or what have you. While using our natural language and not the formal language L, there is of course every danger that contradictions, in fact, any kind of error, may slip in. Hilbert said that the way to avoid this danger is by making absolutely certain that, while one is talking in one's natural language about L, one uses only reasonings which are absolutely safe and beyond any kind of suspicion. He called such reasonings "finitary reasonings," but had, of course, to give a definition of them. The most explicit definition of finitary reasoning known to the author was given by the French formalist Herbrand ([7], the footnote on page 622). It says, if we replace "intuitionistic" by "finitary":

> By a finitary argument we understand an argument satisfying the following conditions: In it we never consider anything but a given finite number of objects and of functions; these functions are well defined, their definition allowing the computation of their values in a univocal way; we never state that an object exists without giving the means of constructing it; we never consider the totality of all the objects x of an infinite collection; and when we say that an argument (or a theorem) is true for all these x, we mean that, for each x taken by itself, it is possible to repeat the general argument in question, which should be considered to be merely the prototype of these particular arguments.

Observe that this definition uses philosophical and not mathematical language. Even so, no one can claim to understand the Hilbert program without an understanding of what finitary reasoning amounts to. The philosophical roots of formalism come out into the open when the formalists define what they mean by finitary reasoning.

We have already compared logicism with realism, and intuitionism with conceptualism. The philosophy which is closest to formalism is "nominalism." This is the philosophy which claims that abstract entities have no existence of any kind, neither outside the human mind as maintained by realism, nor as mental constructions within the human mind as maintained by conceptualism. For nominalism, abstract entities are mere vocal utterances or written lines, mere names. This is where the word "nominalism" comes from, since in Latin *nominalis* means "belonging to a name." Similarly, when formalists try to prove that a certain axiomatized theory T is free of contradictions, they do not study the abstract entities which occur in T but, instead, study that first order language L which was used to formalize T. That is, they study how one can form sentences in L by the proper use of the vocabulary of L; how certain of these sentences can be proven by the proper use of those special sentences of L which were singled out as axioms; and, in particular, they try to show that no sentence of L can be proven and disproven at the same time, since they would thereby have established that the original theory T is free of contradictions. The important point is that this whole study of L is a strictly syntactical study, since no meanings or abstract entities are associated with the sentences of L. This language is investigated by considering the sentences of L as meaningless expressions which are manipulated according to explicit, syntactical rules, just as the pieces of a chess game are meaningless figures which are pushed around according to the rules of the game. For the strict formalist "to do mathematics" is "to manipulate the meaningless symbols of a first order language according to explicit, syntactical rules." Hence, the strict formalist does not work with abstract entities, such as infinite series or cardinals, but only with their meaningless names which are the appropriate expressions in a first order language. Both formalists and nominalists avoid the direct use of abstract entities, and this is why formalism should be compared with nominalism.

The fact that logicism, intuitionism, and formalism correspond to realism, conceptualism, and nominalism, respectively, was brought to light in Quine's article, "On What There Is" (**[1]**, pages 183–196). Formalism can be learned from any modern book in mathematical logic, for instance **[3]**.

Epilogue

Where do the three crises in mathematics leave us? They leave us without a firm foundation for mathematics. After Gödel's paper **[6]** appeared in 1931, mathematicians on the whole threw up their hands in frustration and turned away from the philosophy of mathematics. Nevertheless, the influence of the three schools discussed in this article has remained strong, since they have given us much new and beautiful mathematics. This mathematics concerns mainly set theory, intuitionism and its various constructivist modifications, and mathematical logic with its many offshoots. However, although this kind of mathematics is often referred to as "foundations of mathematics," one cannot claim to be advancing the philosophy of mathematics just because one is working in one of these areas. Modern mathematical logic, set theory, and intuitionism with its modifications are nowadays technical branches of mathematics, just as algebra or analysis, and unless we return directly to the philosophy of mathematics, we cannot expect to find a firm foundation for our science. It is evident that such a foundation is not necessary for technical mathematical research, but there are still those among us who yearn for it. The author believes that the key to the foundations of mathematics lies hidden somewhere among the philosophical roots of logicism, intuitionism, and formalism and this is why he has uncovered these roots, three times over.

Excellent literature on the foundations of mathematics is contained in **[1]** and **[7]**.

References

[1] P. Benacerraf and H. Putnam, Philosophy of Mathematics, Prentice-Hall, 1964.

[2] M. Dummett, Elements of Intuitionism, Clarendon Press, Oxford, England, 1977.

[3] H. B. Enderton, A Mathematical Introduction to Logic, Academic Press, 1972.

[4] A. A. Fraenkel, Y. Bar-Hillel, and A. Levy, Foundations of Set Theory, North-Holland, Amsterdam, Netherlands, 1973.

[5] G. Frege, Begriffschrift, in Translations from the Philosophical Writings of Gottlob Frege by P. Geach and M. Black, Basil Blackwell, Oxford, England, 1970. Also in [7] pp. 1–82.

[6] K. Gödel, On formally undecidable propositions of Principia Mathematica and related systems, in [7] pp. 596–616.

[7] J. van Heijenoort, From Frege to Gödel, Harvard Univ. Press, Cambridge. Available in paperback.

[8] A. Heyting, Intuitionism, An Introduction, North-Holland, Amsterdam, Netherlands, 1966.

[9] B. Russell, Principles of Mathematics, 1st ed. (1903) W. W. Norton, New York. Available in paperback.

[10] B. Russell and A. N. Whitehead, Principia Mathematicia, 1st ed. (1910) Cambridge Univ. Press, Cambridge, England. Available in paperback.

[11] B. Russell, Introduction to Mathematical Philosophy, Simon and Schuster, New York, 1920. Available in paperback.

[12] E. Snapper, What is mathematics?, Amer. Math. Monthly, no. 7, 86 (1979) 551–557.

[13] A. S. Troelstra, Choice Sequences, Oxford Univ. Press, Oxford, England, 1977.

Unitary Divisors

A novel definition of divisibility produces interesting contrasts with classical theory.

RODNEY T. HANSEN
Montana State University
Bozeman, MT 59717

LEONARD G. SWANSON
Portland State University
Portland, OR 97207

One of the oldest and most studied branches of mathematics is number theory. Its problems have been instrumental in the development of many topics in mathematics that now appear to be unrelated to number theory—topics in the areas of complex variables, measure theory, and combinatorics to name just a few. An examination of the literature seems to indicate that almost anyone classified as a mathematician has at one time or another worked on at least one problem in number theory. Perhaps the long interest in number theory of so many people can be attributed to two major factors. First, number theory deals mainly with the basic building blocks of mathematics, the integers—things we have all worked with since we were children. Second, it is possible for a person to study the subject— and arrive at unsolved (unsolvable?) problems— without the extensive background required in so many other areas of mathematics.

This paper attempts to illustrate both these attractions of number theory by exploring the concept of a unitary divisor—a relatively new concept in number theory. Unitary divisors are not mentioned in the *Mathematics Dictionary* [**2**] and of fifty-six number theory textbooks examined, only three include unitary divisors. Examples of unitary divisors are given in TABLE 1 and can be used to gain understanding of that which follows. There are strong similarities between properties of divisors and unitary divisors. On the other hand, many properties and associated concepts crumble upon attempted formulation. (For example, endeavors to define a unitary prime and a unitary common multiple cause all sorts of existence problems.) Information on the properties of (ordinary) divisibility and related concepts can be found in Long [**3**].

In this paper we shall define unitary divisors and examine their basic properties, define related concepts including unitary gcd and unitarily relatively prime integers, look at a few of the applications of unitary divisors, and mention some open questions which involve unitary divisors.

Definitions and Basic Properties

Let Z^+ denote the positive integers and suppose d, $n \in Z^+$. We define d to be a **unitary divisor** of n provided:

(1) d is a divisor of n, (denoted by $d|n$), and

(2) the greatest common divisor of d and n/d equals 1, (denoted by $(d,n/d)=1$).

We shall write $d|^*n$ to denote the fact that d is a unitary divisor of n.

An examination of TABLE 1 leads to the following easily proven results about unitary divisibility. If p_i are distinct primes and $n=\Pi p_i$, then all of the divisors of n are unitary divisors. Conversely, any number for which all the divisors are unitary divisors must be either a single prime or a product of distinct primes. If n is a power of a prime, then 1 and n are the only unitary divisors of n. Conversely, if 1 and $n>1$ are the only unitary divisors of n, then n is either a prime or a power of a prime.

Certain elementary properties of divisibility carry over at once to unitary divisibility. It is easy to see that for every positive integer n: $n|^*n$ and $1|^*n$; if $d|^*n$, then $(n/d)|^*n$; if $d|^*n$, then $d\leqslant n$; if $d|^*n$ and $n|^*d$, then $n=d$. Additional properties of divisibility have analogs with respect to unitary divisibility. For example, unitary divisibility is a transitive relation on Z^+. That is, if $a|^*b$ and $b|^*c$, then $a|^*c$. This follows since $a|^*b$ yields $a|b$ and $(a,b/a)=1$ while $b|^*c$ gives $b|c$ and $(b,c/b)=1$. Now $a|b$ implies $b=au$ for some $u\in Z^+$ and $c=bv$ for some $v\in Z^+$ since $b|c$. Then, $(a,c/a)=(a,bv/a)=(a,auv/a)=(a,uv)$. Now, $(a,u)=(a,b/a)=1$ and $1=(b,c/b)=(b,v)=(au,v)$, which implies $(a,v)=1$. It follows that $(a,uv)=1$ and hence $(a,c/a)=1$. Since $a|b$ and $b|c$, we also have $a|c$, and thus $a|^*c$. It is also the case that unitary divisibility has a cancellation property in the sense that if $ad|^*an$, then $d|^*n$. By definition, $ad|^*an$ implies $ad|an$ and $(ad,an/ad)=1$; which implies $d|n$ and $(ad,n/d)=1$ so that $d|n$ and $(d,n/d)=1$. We also know that if p is a prime and $p|^*ab$, then either $p|^*a$ or $p|^*b$. This is true since $p|^*ab$ means that p appears exactly once as a factor of ab, so appears exactly once as either a factor of a or else b. Thus, $p|^*a$ or $p|^*b$.

Certain standard results dealing with sums and products of divisors of positive integers have neat analogs for unitary divisors. Wall [1] has determined the formulas for both the number and

		Number of	Sum of
n	Unitary Divisors	Unitary Divisors	Unitary Divisors
4	1,4	2	5
6	1,2,3,6	4	12
8	1,8	2	9
9	1,9	2	10
10	1,2,5,10	4	18
12	1,3,4,12	4	20
14	1,2,7,14	4	24
15	1,3,5,15	4	24
16	1,16	2	17
18	1,2,9,18	4	30
20	1,4,5,20	4	30
21	1,3,7,21	4	32
22	1,2,11,22	4	36
24	1,3,8,24	4	36
25	1,25	2	26
26	1,2,13,26	4	42
27	1,27	2	28
28	1,4,7,28	4	40
30	1,2,3,5,6,10,15,30	8	72
32	1,32	2	33
33	1,3,11,33	4	48
34	1,2,17,34	4	54
35	1,5,7,35	4	48
36	1,4,9,36	4	50
38	1,2,19,38	4	60
39	1,3,13,39	4	56
40	1,5,8,40	4	54

TABLE 1

the sum of the unitary divisors of any positive integer n. If $\omega(n)$ is the number of distinct prime divisors of $n>1$ and $\omega(1)=0$, then $\Sigma_{d|*n}1=2^{\omega(n)}$. This can be proved by a direct application of the Binomial Theorem. If $\Pi_{i=1}^{r}p_i^{a_i}$ is the prime decomposition of n, it follows at once from the formula $\Sigma_{d|n}d=\Pi_{i=1}^{r}(1+p_i+p_i^2+\cdots+p_i^{a_i})$ that the sum of the unitary divisors of n is given by $\Sigma_{d|*n}d=\Pi_{i=1}^{r}(1+p_i^{a_i})=\Pi_{i=1}^{\omega(n)}(1+p_i^{a_i})$. If k is any positive integer, this last result generalizes to $\Sigma_{d|*n}d^k=\Pi_{i=1}^{\omega(n)}(1+p_i^{ka_i})$. It is also the case that $\Sigma_{d|*n}d^k=\Sigma_{d|*n^k}d$. As for products, the argument that shows that $\Pi_{d|n}d=n^{\tau(n)/2}$, where $\tau(n)$ is the number of divisors of n, can be modified to show that $\Pi_{d|*n}d=n^{\tau^*(n)/2}$, where $\tau^*(n)$ is the number of unitary divisors of n. If k is any positive integer, this last result generalizes to $\Pi_{d|*n}d^k=n^{k\tau^*(n)/2}$.

Several important properties of divisibility do not extend to unitary divisibility. The most disappointing is the failure of the linear property of divisibility which states that if $d|n$ and $d|m$, then $d|(nx+my)$ for all integers x and y. TABLE 1 shows that $2|^*6$ and $2|^*10$ while $2\nmid{}^*16$. Another divisibility property that fails to extend to unitary divisibility is the multiplicative property which states that if $d|n$, then $ad|an$ for any non-zero integer a. TABLE 1 shows that $2|^*6$ while $3\cdot 2\nmid{}^*3\cdot 6$. It is interesting that unitary divisibility has a cancellation property, but it fails to have the multiplicative property.

Other extensions of ideas associated with divisibility may occur to the reader—for example, the idea of perfect number. A positive integer n is called a **perfect number** if the sum of the divisors of n is $2n$. We define a positive integer n to be a **unitary perfect number** if the sum of all the unitary divisors of n is $2n$. One can see that 6 is unitary perfect as well as perfect. The number 28 is perfect, but it is not unitary perfect.

Greatest Common Unitary Divisor and Least Common Unitary Multiple

If a and b are integers, the **greatest common divisor (gcd)** of a and b is defined to be the number $d=(a,b)$ which has the following properties: (1) $d\geqslant 0$; (2) $d|a$ and $d|b$; and (3) if $e|a$ and $e|b$, then $e|d$. The standard proofs that this number d exists and is unique for any two integers a and b rest on the fact that divisibility has a linear property—a property that unitary divisibility does not possess. Thus, if we are to define a greatest common unitary divisor, we must take a different approach.

Let a and b be positive integers with prime decompositions given by $a=\Pi_{i=1}^{t}p_i^{a_i}$ and $b=\Pi_{i=1}^{t}p_i^{b_i}$ with $a_i,b_i\geqslant 0$, (for all i) where t is the number of distinct prime factors of ab. Define the number d by $d=\Pi_{i=1}^{t}p_i^{d_i}$, where $d_i=a_i$ if $a_i=b_i$ and $d_i=0$ if $a_i\neq b_i$. Thus, we define the **greatest common unitary divisor (gcud)** of a and b to be the number d and we write $(a,b)^*=d$. It is not difficult to show that the gcud of two positive integers a and b can then also be characterized as the number d which satisfies the properties: (1) $d\geqslant 1$; (2) $d|^*a$ and $d|^*b$; (3) if $e|^*a$ and $e|^*b$, then $e|^*d$. An examination of TABLE 1 shows, for example, that $(15,35)^*=5$ and $(4,16)^*=1$; and the last equality suggests another definition. If $(a,b)^*=1$, we shall say that a and b are **unitarily relatively prime**. Note that $(4,16)^*=1$ while $(4,16)=4$. On the other hand, if $(a,b)=1$, we must also have $(a,b)^*=1$. In general, we have $(a,b)^*\leqslant(a,b)$. Using the prime decomposition notation introduced in the definition of the gcud, we note, that if $a_i=b_i$, then $d_i=\min(a_i,b_i)$; while if $a_i\neq b_i$, then $d_i=0\leqslant\min(a_i,b_i)$. Thus, $d_i\leqslant\min(a_i,b_i)$ for all i, and we have

$$(a,b)^*=\prod_{i=1}^{t}p_i^{d_i}\leqslant\prod_{i=1}^{t}p_i^{\min(a_i,b_i)}=(a,b).$$

As for when the two are equal, we will have $(a,b)^*=(a,b)=1$ iff a and b contain no common prime factors. We will have $(a,b)^*=(a,b)\neq 1$ iff a and b contain common prime factors, each of which is raised to the same power in both a and b. For example, $(28,36)=4=(28,36)^*$ and $(10,30)=10=(10,30)^*$.

Certain properties of the gcd extend to the gcud. It is clear that $(1,a)^*=(a,1)^*=1$ and that we still have the symmetric property $(a,b)^*=(b,a)^*$. The associative property $(a,(b,c)^*)^*=((a,b)^*,c)^*$ also holds. If we let $(a,(b,c)^*)^*=p_1^{d_1}\cdots p_r^{d_r}$, then each $p_i^{d_i}$ must appear as a factor of

a, b, and c, and only that d_i power of p_i can appear in each of a, b, and c. This forces $((a,b)^*,c)^*=p_1^{d_1}\cdots p_r^{d_r}$ and the associative property is established.

It is also true that if $a|^*b$ and $c|^*b$ and $(a,c)^*=1$, then $ac|^*b$, as the following shows. Let $a=\Pi_{i=1}^{t}p_i^{a_i}, b=\Pi_{i=1}^{t}p_i^{b_i}$, and $c=\Pi_{i=1}^{t}p_i^{c_i}$, where $a_i,b_i,c_i\geqslant 0$ and t is the number of distinct prime factors of abc. Note that $(a,c)^*=1$ says that for all i, either $a_i\neq c_i$ or $a_i=c_i=0$. Now, $a|^*b$ implies that each $p_i^{a_i}$ must be a factor of b and $c|^*b$ implies that each $p_i^{c_i}$ must be a factor of b and further $p_i^{b_i}=p_i^{a_i}$ or $p_i^{b_i}=p_i^{c_i}$. However, $a_i\neq c_i$ forces $a_i=0$ or $c_i=0$. Thus, if $a_i\neq 0$, $c_i=0$ and if $c_i\neq 0$, $a_i=0$, so if $p_i^{a_i+c_i}$ is a factor of ac, $p_i^{a_i+c_i}$ must be $p_i^{a_i}$, $p_i^{c_i}$, or 1. Each factor of this type will appear in b, and hence $ac|^*b$.

Another property of the gcd that extends properly to the gcud is that if $a|^*bc$ and $(a,b)=1$, then $a|^*c$. Note that we have $(a,b)=1$ and not $(a,b)^*=1$, since the property fails if $(a,b)=1$ is replaced by $(a,b)^*=1$. Since $(a,b)=1$, we know that a and b have no common prime factors. However, $a|^*bc$, so the prime powers in a must appear exactly in bc and must therefore be in c and we have $a|^*c$.

Certain well known properties of the gcd fail to extend to the gcud. If $(a,b)=1$ and $(a,c)=1$, then $(a,bc)=1$. This property fails to extend to the gcud since $(36,10)^*=1$ and $(36,14)^*=1$ while $(36,140)^*=4$. The gcd has a distributive property: $(ka,kb)=|k|(a,b)$. The gcud does not have this distributive property as is shown by $3(2,6)^*=3\cdot 2\neq 2=(6,18)^*$.

The concept of least common multiple (lcm) presents some unexpected problems. If a and b are nonzero integers, their **least common multiple** m, denoted $[a,b]=m$, is the number which satisfies: (1) $m\geqslant 1$; (2) $a|m$ and $b|m$; and (3) if $a|n$ and $b|n$, then $m|n$. For nonzero integers a and b, the gcd and lcm are related by $[a,b]=|ab|/(a,b)$. An attempt to define least common unitary multiple in a similar manner leads one to the discovery that a common unitary multiple may not exist for two numbers—let alone a least one! Consider 8 and 20. The unitary divisors of 8 are 1 and 8; the unitary divisors of 20 are 1, 4, 5, and 20. Now, 8 is a unitary divisor of numbers of the form $n=2^3\cdot p_1^{a_1}\cdots p_r^{a_r}, p_i\neq 2$, for all i. However, no number of this form will have 20 as a unitary divisor. Thus, 8 and 20 do not have a common unitary multiple if we go about things in the conventional way. We are therefore led to the following as one way to define a least common unitary multiple: If a and b are positive integers, the **least common unitary multiple (lcum)** of a and b is $[a,b]^*=ab/(a,b)^*$. One can quickly observe that $[a,b]^*=[b,a]^*$; $[a,b]^*=ab$ if and only if $(a,b)^*=1$; and $[a,b]^*=[a,b]$ if and only if $(a,b)^*=(a,b)$.

Applications

One application we want to look at is an extension of Euler's Theorem. We first need the definition of the **Euler ϕ function:** If $n\in Z^+$, then $\phi(n)$ is the number of positive integers not exceeding n which are relatively prime to n. A general discussion of the Euler ϕ function can be found in the paper by Avital and Hansen [4]. Euler's Theorem states that if $(a,n)=1$, then $a^{\phi(n)}\equiv 1 \pmod{n}$. A seemingly elementary application of Euler's Theorem suggested by Avital for inclusion in [4] is that each positive integer a less than 10 when raised to the fifth power is congruent to a modulo 10. That is, $a^5\equiv a \pmod{10}$ or $a^{\phi(10)+1}\equiv a \pmod{10}$ for each a, independent of any relative primality (or other type) condition. Why? No answer could be found. Recent work by Osborn [5], Livingston and Livingston [6], and Hansen [7] have explored this and related questions. To pursue this matter, let us consider the first few powers of $0,1,2,\ldots,n-1 \pmod{n}$ for n equal to 4, 6, 9, and 10. These are given in TABLE 2. Note that for $n=6$ and $n=10$ the integers of the top row are repeated in the same order in certain subsequent rows. (This we indicate by the arrows.) For $n=4$, the number 2 causes problems; for $n=9$, the number 3 causes problems. (Note that each is a non-unitary divisor of the given n.) Observe that both 6 and 10 are products of distinct primes and hence each divisor of 6 or 10 is also a unitary divisor. These observations lead to the following result—a corollary to Euler's Theorem.

THEOREM A. *If $(a,n)=1$ or a is a unitary divisor of n, then there exists a positive integer $k\leqslant n$ such that $a^k\equiv a \pmod{n}$.*

$n=4$

a	0	1	2	3
a^2	0	1	0	1
a^3	0	1	0	3
a^4	0	1	0	1

$n=6$

a	0	1	2	3	4	5	
a^2	0	1	4	3	4	1	
a^3	0	1	2	3	4	5	←
a^4	0	1	4	3	4	1	
a^5	0	1	2	3	4	5	←
a^6	0	1	4	3	4	1	

$n=9$

a	0	1	2	3	4	5	6	7	8
a^2	0	1	4	0	7	7	1	4	1
a^3	0	1	8	0	1	8	6	1	8
a^4	0	1	7	0	4	4	1	7	1
a^5	0	1	5	0	7	2	6	4	8
a^6	0	1	1	0	1	1	1	1	1
a^7	0	1	2	0	4	5	6	7	8
a^8	0	1	4	0	7	7	1	4	1
a^9	0	1	8	0	1	8	6	1	8

$n=10$

a	0	1	2	3	4	5	6	7	8	9	
a^2	0	1	4	9	6	5	6	9	4	1	
a^3	0	1	8	7	4	5	6	3	2	9	
a^4	0	1	6	1	6	5	6	1	6	1	
a^5	0	1	2	3	4	5	6	7	8	9	←
a^6	0	1	4	9	6	5	6	9	4	1	
a^7	0	1	8	7	4	5	6	3	2	9	
a^8	0	1	6	1	6	5	6	1	6	1	
a^9	0	1	2	3	4	5	6	7	8	9	←
a^{10}	0	1	4	9	6	5	6	9	4	1	

In certain cases, marked by arrows, a certain power of any number less than *n* (mod *n*) yields the original number again (see text).

TABLE 2

Proof. If $n=1$, the result is immediate. If $n>1$ and $(a,n)=1$, the congruence follows from Euler's Theorem with $k=\phi(n)+1$. If $n>1$, $a>1$, and $a|^*n$, then consider $a^x\equiv a \pmod{n}$. It follows that $a^{x-1}\equiv 1 \pmod{n/(a,n)}\equiv 1 \pmod{n/a}$. Since $(a,n/a)=1$, $a^{\phi(n/a)}\equiv 1 \pmod{n/a}$ and so $a^{\phi(n/a)+1}\equiv a \pmod{n}$, where $\phi(n/a)+1\leqslant n$. Thus, in this case we let $k=\phi(n/a)+1$.

Now, let us answer the question posed by Avital and prove an extension of Euler's Theorem. That $a^5\equiv a \pmod{10}$ for all integers a such that $0\leqslant a\leqslant 9$ follows from A since each divisor of 10 is a unitary divisor. The extension of Euler's Theorem follows.

THEOREM B. *If n is expressible as a product of distinct primes, then* $a^{\phi(n)+1}\equiv a \pmod{n}$ *for all integers a such that* $0\leqslant a<n$.

Proof. If $a=0$, the result is clear. Now consider the case $a>0$. Since every divisor of n is a unitary divisor, the proof of Theorem A assures that if $(a,n)=1$, then $a^{\phi(n)+1}\equiv a \pmod{n}$; and that if a is a unitary divisor of n, then $a^{\phi(n/a)}\equiv 1 \pmod{n/a}$. Hence $a^{\phi(n)/\phi(a)}\equiv 1 \pmod{n/a}$ implies $a^{\phi(n)}\equiv 1 \pmod{n/a}$, which yields $a^{\phi(n)+1}\equiv a \pmod{n}$.

Another area of application of unitary divisors is the theory of arithmetic functions. The basic reference in this area is Wall [1]. An **arithmetic function** is a mapping whose domain is Z^+ and whose range is in the complex numbers. (The range may be generalized to other algebraic structures.) If f and g are arithmetic functions, the **Dirichlet product** $f\circ g$ is defined by $(f\circ g)(n)=\Sigma_{d|n}f(d)g(n/d)$. If we replace $d|n$ by $d|^*n$ in the last definition, we have the definition of the **unitary product** $f*g$ given by $(f*g)(n)=\Sigma_{d|^*n}f(d)g(n/d)$. If we let A denote the set of all arithmetic functions and $(f+g)(n)=f(n)+g(n)$ for all $f,g\in A$, it is not difficult to prove that $(A,+,\circ)$ and $(A,+,*)$ are commutative rings with identities. The function $\varepsilon(n)$ defined as 1 if $n=1$ and 0 if $n>1$ is the identity with respect to both $\circ$ and $*$. $(A,+,*)$ can be used in the construction of creatures called Harrison primes. (See [1] for a careful development.)

Of major interest in arithmetic function theory is the development of inversion formulae. With respect to the Dirichlet product, we have the classical Möbius inversion formula which states that $f(n)=\Sigma_{d|n}g(d)$ if and only if $g(n)=\Sigma_{d|n}f(d)\mu(n/d)$, where μ is the **Möbius function** defined by

$$\mu(n)=\begin{cases}1 & \text{if } n=1\\ (-1)^k & \text{if } n=p_1^{a_1}\cdots p_k^{a_k} \text{ and } a_1=a_2=\cdots=a_k=1\\ 0 & \text{otherwise.}\end{cases}$$

If we let $\eta(n)=1$ for all $n\in Z^+$, then the Möbius inversion formula can be stated as $f=g\circ\eta$ if and only if $g=f\circ\mu$. A similar result can be proved for the unitary product where the roll of the Möbius function μ is played by $\alpha(n)=(-1)^{\omega(n)}$, where $\omega(n)$ is the number of distinct prime divisors of n if $n>1$ and $\omega(1)=0$. We then have an inversion formula for unitary multiplication given by $f=g*\eta$ if and only if $g=f*\alpha$.

For more on arithmetic function theory, the reader may wish to consult the papers by Cohen [8], [9], McCarthy [10], and Rao [11].

Open Questions

We close by listing a few unsolved problems involving unitary divisors. One of the places to look for questions is the attempt to find unitary divisor analogs of division type properties. For example, we have defined unitary perfect numbers as the analog of perfect numbers. It is known [1] that 6; 60; 90; 87,360; and 146,361,946,186,458,562,560,000 are the first five unitary perfect numbers. Are there any other unitary perfect numbers? Is there any sort of relationship between perfect numbers and unitary perfect numbers? Here is another example. Is there any meaningful way to define a unitary prime and if so, can one get a decomposition theorem in terms of unitary primes? And finally, do any of the classical summation and product formulae have analogs when $d|n$ is replaced by $d|^*n$ or when they are modified in some other way? We know that $\Sigma_{d|n}\phi(d)=n$, where ϕ is the Euler function. Is there a neat way to express $\Sigma_{d|^*n}\phi(d)$? If we define $\phi^*(n)$ to be the number of positive integers not exceeding n which are unitarily relatively prime to n, is there a neat representation for $\Sigma_{d|^*n}\phi^*(d)$? Is there any sort of analog for

$$\phi(n)=\Sigma_{d|n}\mu(d)\frac{n}{d}$$

where any of several modifications are introduced?

We stop with these few open questions. Perhaps the real fun is finding the questions. The classical division properties and associated formulae involving the classical arithmetic functions, as well as the general theory of arithmetic functions, provide fruitful ground for continued investigation.

This paper was written while the second author was on sabbatical leave at Montana State University.

References

[1] C. R. Wall, Selected Topics in Elementary Number Theory, U of South Carolina Press, Columbia, S. C., 1974.

[2] Glen James and Robert James, Mathematics Dictionary, Third Edition, D. Van Nostrand, Princeton, N.J., 1968.

[3] C. T. Long, Elementary Introduction to Number Theory, Second Edition, D. C. Heath, Lexington, MA, 1972.

[4] S. Avital and R. Hansen, Euler's ϕ-function, A function satisfying many properties and having many uses, to appear in Internat. J. Math. Education Sci. and Tech.

[5] R. Osborn, A "Good" Generalization of the Euler-Fermat Theorem, this MAGAZINE, Vol. 47, No. 1 (1974) 28–31.

[6] A. E. Livingston and M. L. Livingston, The congruence $a^{r+s}\equiv a^r$ (mod m), Amer. Math. Monthly, Vol. 85, No. 2 (1978) 97–100.

[7] R. Hansen, Extension of the Euler-Fermat theorem, Bull. of Number Theory, 2:5 (1977) 1–4.

[8] E. Cohen, Arithmetic functions associated with the unitary divisors of an integer, Math. Z., Vol. 74 (1960) 66–80.

[9] ———, Unitary products of arithmetical functions, Acta. Arith., Vol. 7 (1961) 29–38.

[10] P. McCarthy, Some more remarks on arithmetical identities, Portugal. Math., Vol. 21 (1962) 45–57.

[11] K. Rao, On the unitary analogues of certain totients, Monatsh Math., Vol. 70 (1966) 149–154.

notes

Mathematical Foundations of Constitutional Law

STEPHEN A. KENTON
Eastern Connecticut State College
Willimantic, CT 06226

In a recent article [2], Felix Browder stressed the relevance of mathematics "as the ultimate and transparent form of all human knowledge and practice," as opposed to its conception in terms of social utility or as a body of research. This conception of mathematics "as the science of significant form" and a unifying cultural force in western civilization has been previously treated in a classic work by Morris Kline [10]. Kline stresses that a distinctive characteristic of mathematics is its deductive form and totally rational spirit. It is our thesis that Western law is explicitly modeled on these principles which underlie mathematics. It can be said that "...law is truth in action...it is the only weapon man has fashioned whose force rests solely on the sanctity of reason." [13] The purpose of this note is to discuss constitutional law as an example of the essential nature and cultural role of mathematics in our society. We will draw an analogy between three problems in mathematics and constitutional law: consistency, completeness and the extent of the use of logic. The analogies are used to gain insights into legal problems, not as starting points for the formal logical analysis of a system which we view as mirroring mathematics in a cultural and largely non-technical sense. This perception of law is intended to bring light to one facet of a complex social institution.

The deductive technique of organizing knowledge was formalized by Euclid over two thousand years ago. The Euclidean model is composed of *undefined terms, definitions, axioms* ("truths" giving properties of these terms and wherein no axiom should be provable from the other axioms), *theorems,* and *proofs* of these theorems using certain predetermined rules of logic. This system has been used as a model in almost every area of our culture. For example, in "A Discourse on Method," Descartes extended Euclid's method to all philosophical inquiries. As a result of Newton's Law of Universal Gravitation and subsequent work in mathematical physics, succeeding scholars attempted to copy his technique of mathematical inquiry in the eighteenth century study of such diverse areas as ethics, poetry, political science and economics.

The writings of Plato are fundamental to many areas of our culture, in particular to the theory of law. For Plato, while law and justice are equivalent, "laws can be derived only from reason..." [5], a position consistent with his view that the appreciation of the nature of justice demands the study of mathematics to develop the reasoning capacity. It is to Aristotle that we give credit for "the first example of the use of a precise scientific method in the exploration of legal propositions." [3] Aristotelian logic is the basis of the constitutional form of government, notwithstanding Plato's refusal to deduce laws from an existing constitution [5].

The codification of law and its basis in the *jus naturale* (natural law) as the foundation for all subsequent law may be attributed to Cicero upon whose writings much of our present law rests. According to legal scholar Carl Joachim Friedrich, "when the fathers of the American [and State] constitutions proclaimed that their constitutions were establishing governments of laws and not of men, they merely restated what Cicero had already formulated..." [5] The continuation of Cicero's legal tradition may be found in Aquinas who saw law as a rational system based on theological foundations [3]. As in mathematics, the constitutional system is based on the idea of accepted truths limiting the nature of further laws (theorems).

The use of mathematical technique in the law was clearly stated in the seventeenth century by John Locke:

> I doubt not, but from self-evident propositions, by necessary consequences, as uncontestable as those in mathematics, the measures of right and wrong might be made out, to anyone that will apply himself with the same indifferency and attention to the one as he does to the other of these sciences. [3]

Locke enumerated the axioms of his system, among which are that each man has the right to property and the right to share in political responsibility, and that the government rests on the consent of the governed; further, the sovereign power is in trust to the people and the people have the right to overthrow their government if this trust is broken [11]. It is no accident that in writing the Declaration of Independence Thomas Jefferson not only used Locke's method of deriving necessary consequences from self-evident truths, but also used many of his principles as the starting points of his own arguments. In a letter to John Trumbull, Jefferson wrote, "I consider...[Bacon, Locke and Newton] as the three greatest men that have ever lived without any exception, and as having laid the foundation of those superstructures which have been raised in the Physical and Moral sciences..." [1]

The form of the Declaration is Euclidean in nature, starting with a list of axioms and concluding in a proof based on these axioms. A list would include "equal," "liberty," "happiness," "just," "natural" and "men" among the undefined terms; "rights," "government" and "powers" among the terms defined elsewhere; "all men are created equal," "all men are endowed by their creator with inalienable rights," and "government derives its power from the consent of the governed" among the axioms; and "overthrow the government" as the *only* theorem, with the remainder of the document a proof of this theorem. The interpretation of certain undefined terms, such as "men" and "equal" (as in "all men are created equal"), has led to many important debates, especially with respect to the issue of slavery in the nineteenth century. Though a historian might view the axioms of the Declaration as basic normative claims employing terms with a defined meaning, one can add a further dimension to the understanding of the document by the perception of the axioms as an explicit attempt by Jefferson to carry out Locke's previously quoted plan of deriving necessary consequences "from self-evident propositions." The rules of inference would be those employed in the philosophical discourse of the 18th century as opposed to the more formal rules of logical analysis advocated by the 19th century philosophers of analytical jurisprudence.

The Declaration of Independence and the Constitution are the culmination of centuries of legal thought and support our thesis that American law is founded on the form and spirit of mathematics. The legal developments of the nineteenth century continued this tradition in the work of John Austin (1790-1895), the founder of analytical jurisprudence. This is the notion of law as established fact subject to scientific treatment and orderly classification, as a science built upon the mathematical model. The philosophy was to find the concepts and principles common to all legal systems. It attempted to reduce a large number of legal concepts to a basic few that were not themselves further analyzable. It is a study of what law is as opposed to what an individual or group thinks it ought to be. Austin's thoughts on undefined terms could certainly have been written by Euclid:

> Many legal concepts are complex and derivative, capable of reduction to simpler notions of which they are composed. Soon this process ends as we discover those fundamental terms whose meaning cannot be elucidated by other legal terms without circularity, and are therefore capable of enlightening definition only, if at all, in terms from outside the law. [4]

The Scandinavian School of legal philosophy holds that "basic legal terms stand for no kind of entities, empirical or non empirical; rather, they are fictions or imaginary ideas." These notions lead to legal positivism where no reference need be made to natural justice (cf. Locke) in the definition of law or the determination of the validity of any law.

Although the law uses mathematics as a model, it is rife with logical problems. The theorists of analytical jurisprudence attempted to show that law should be viewed as a perfect imitation of the mathematical form. They felt that many legal problems would disappear under the rigorous analysis engendered by this outlook. However, mathematics has problems of both a philosophical and logical nature (see **[6]**, for example). In spite of Cantor's belief that only certain formal criteria need be met, his set theory led to logical problems which he could not resolve. It is to be expected that law, which is only an approximation of the mathematical method, would be confronted with some analogous problems.

Just as the 18th century moral philosophers tried to extend formal mathematical analysis to their studies, so did the 19th century followers of John Austin attempt the same program. In both centuries, the results were disappointing. Though we have seen that many political scientists saw law as an extension of mathematics into their field, the analogies between mathematics and law which we draw are used to gain an insight into legal problems, not as a technique to rationalize formal analysis (as the followers of John Austin's theories of analytical jurisprudence hoped).

Consistency. The American constitution is a system of positive law which is the product of many centuries of legal argument. In structuring this constitutional system, it is necessary to determine the logical legitimacy of legislative laws; i.e., are new laws consistent with respect to basic laws? (A set of propositions is **consistent** when no contradiction can be derived from the joint assertion of the propositions in the set.) Though it is now largely accepted that the courts have this review function, it took almost a hundred years for this to be accomplished, as noted in **[9]**: "For more than half a century after *Marbury* vs. *Madison*, Congress and the President continued to consider themselves at least the equals of the judiciary in determining the constitutionality of legislation." However, it is known that a majority of the influential members of the Constitutional Convention declared, directly or indirectly for judicial control **[12]**. Our present attitude toward the courts is most precisely stated by Alexander Hamilton:

> The interpretation of the laws is the proper and peculiar province of the courts. A constitution...must be regarded by the judges as a fundamental law. It must belong to the judges to ascertain...the meaning of any particular act proceeding from the legislative body. If there should happen to be an irreconcilable variance between the two...the Constitution ought to be preferred to the statute, the intention of the people to the intention of their agents. [7]

That this separation of powers was intended may be seen by reading the early state constitutions, such as that of Virginia adopted June 29, 1776 **[14]**.

The problem of consistency in the set of precedents (accepted law) is directly related to attaching meaning to words. This point is spoken to most directly by Nizer:

> It is an ancient rule of construction that when two articles appear to be in conflict, they should be so interpreted as to give meaning to each. It is not to be assumed that the drafters...simply didn't know what they were doing and created [inconsistent] bylaws. **[13]**

With respect to consistency, the law requires that certain words not have the connotations of common parlance, but instead be thought of as legalistic concepts. For example, in a recent case, a student's parents sued the San Francisco Board of Education for not fulfilling its *duty* to educate their son (Cal. Sup. Ct. No. 643312). The Court of Appeals upheld the dismissal of the suit, saying that though the duty of the Board was to educate, the only question before the court was the *duty of care*, a legalistic concept which essentially says that the legal responsibility of the Board was the physical safety of its students. Words such as 'duty' "do not have the straightforward connexion with counterparts in the world of fact which most ordinary words have and to which we appeal in our definition of ordinary words...though we speak of men having duties,...the word 'duty' does not...describe anything as ordinary words do." **[8]**

Perhaps the greatest strength of the American judicial system is the flexibility of the Constitution. With the passage of time, the culture changes and the accepted meanings of undefined terms are often modified, a situation not possible in mathematics wherein undefined terms take their properties from the axioms (though, in practice, undefined terms have many interpretations, such as "line" in the different models of both Euclidean and non-Euclidean geometries). Rather than this being a weakness, as would be true in mathematics, these flexible interpretations allow the constitutional system to remain appropriate in changing times. For example, a Supreme Court decision in the 1890's held that segregated schools were allowed since it was possible to have "separate but equal" facilities. In 1954, the Court reversed itself saying that"separate" by its very nature means "unequal." The culturally motivated reinterpretation of the word "equal" was important in justifying the complex moral and empirical judgements in the case.

Limits of Logic. As distinguished from the purely deductive approach of analytical jurisprudence, O. W. Holmes, Jr., viewed the law as part of a historical and cultural tradition. While the followers of John Austin would hesitate to include the abstract notion of justice in their deliberations, it is evident that this ideal may make itself felt in judicial deliberations that are seemingly well defined by existing laws. Louis Nizer, a lawyer whose philosophy is in the tradition of Holmes, writes of one of his cases: "But there is no other way of winning this case than by drawing the factual history into the dispute and insisting that the legal question is not the sole determinative factor... Our cause is just. That is our strength..." **[13]** A recent example is the celebrated trial of Patricia Hearst. The opposing attorneys argued the admissibility of evidence of Miss Hearst's actions for the months *after* the bank robbery for which she was being tried. Judging from the statements of several jurors, it is unlikely the defendant would have been convicted had the prosecution not been allowed to present the case in this large perspective.

The notion of justice in law is complex. The writing of Hamilton in The Federalist Papers indicate that justice should be incorporated in the law by the drafters, while the courts should be interpreters of the law. The advocates of "judicial restraint" declare that the courts have gone beyond their proper role and are occasionally usurping the legislative function. Such decisions as Brown vs. Board of Education, "one man—one vote" in state legislatures, and the 1973 abortion decision are often viewed as lack of judicial restraint, while more liberal members of the legal community see the court decisions as proper judicial review. The problem may be viewed as the degree (if any) that courts allow themselves to interpret laws in light of past history and present culture.

Completeness. A system is **complete** if any properly written statement may be proved either true or false. It is reasonable to assume that the intention of the founders of the Constitution was to formulate a complete system. Their method of doing this was to give the states the power to formulate any rules not covered by the federal constitution. However, even with the overlay of state constitutions, the legal system is far from complete. As in mathematics, where a finite complete system encompassing number theory is impossible, the possibility of creating *independent* statements has been realized in law. For example, the Alien and Sedition Acts of World War I were determined to be independent of the Constitution even though their effect on the society was at least as great as any of the constitutional amendments. In "The Power Broker," the source of the power of Robert Moses was shown to be his ability to write independent laws which, in some ways, made him more powerful than the governor of New York.

Thus, although the law is fashioned as a deductive system, it is necessary to view it in its full historical and cultural framework as only an approximation of the mathematical method, and to see its supposed inconsistencies and flexible interpretations of undefined terms as the strengths that bring the system closer to the ideal of Justice. We see the contention that mathematics and law are closely connected is not the assertion that the analytical techniques of mathematics should be favored in understanding the law. Rather, it is the use of mathematics as the "form of all human knowledge" and as "a unifying cultural force in western civilization."

References

[1] J. P. Boyd, The Papers of Thomas Jefferson, Vol. 14, Princeton Univ. Press, Princeton, N.J., 1958.
[2] F. Browder, The Relevance of Mathematics, Amer. Math. Monthly, 83 (1976) 249–254.
[3] H. Cairns, Legal Philosophy from Plato to Hegel, Johns Hopkins Press, Baltimore, 1949.
[4] Encyclopedia of Philosophy, Analytical Jurisprudence, Vol. 1, pp. 109–110.
[5] C. J. Friedrich, The Philosophy of Law in Historical Perspective, Univ. of Chicago Press, Chicago, 1958.
[6] K. Godel, What is Cantor's Continuum Problem, Amer. Math. Monthly, 54 (1947) 515–525.
[7] A. Hamilton, The Federalist, #78.
[8] H. Hart, Definition and Theory in Jurisprudence, Oxford Univ. Press, London, 1959.
[9] Kelly & Harbison, The American Constitution, Third Ed., Norton&Co., New York, 1963.
[10] M. Kline, Mathematics in Western Culture, Oxford Univ. Press, New York, 1953.
[11] J. Locke, The Second Treatise of Civil Government and a Letter Concerning Toleration, Ed. J. Gough, Oxford Univ. Press, New York, 1946.
[12] R. G. McCloskey, Essays in Constitutional Law, Alfred A. Knopf, New York, 1957.
[13] L. Nizer, My Life in Court, Doubleday, Garden City, New York, 1961.
[14] C. B. Swisher, The Growth of Constitutional Power in the United States, Univ. of Chicago Press, Chicago, 1946.

Checker Jumping in Three Dimensions

EUGENE LEVINE
Adelphi University
Garden City, NY 11530

IRA J. PAPICK
University of Missouri
Columbia, MO 65211

In this paper we will introduce a variation of a most interesting checker jumping problem due to John Conway. Conway's original problem appears in *Mathematical Gems II* by Ross Honsberger [1] (also, see [2] for a discussion of this problem). We will briefly discuss this original version, as it contains the essential ideas in our three dimensional analogue.

As the interested reader will undoubtedly observe, there are many other amusing variations not considered in this article. It is our main intention to expose one possibility, and leave other directions open to the reader.

We now proceed to discuss Conway's original problem. For our checkerboard we shall take the infinite plane with the squares determined by the lattice lines. The x-axis, serving as the fold in the board, will have special significance.

By starting below the fold with any arrangement of checker pieces, the object is to advance as far above the fold as possible by only using vertical and horizontal checker jumps (no diagonal jumps). As in regular checkers, the piece that has been jumped is removed from the board. It is easy to see that reaching levels one and two above the x-axis presents no difficulties. With a bit of patience, it is possible to discover initial configurations which will put pieces in the third and fourth levels. FIGURE 1 indicates a basic arrangement to attain level three, which enters into later considerations.

FIGURE 2 provides an arrangement which achieves a level of four above the fold (see [1] for details). Actually, our interest in this configuration is the fact that it can be used to place

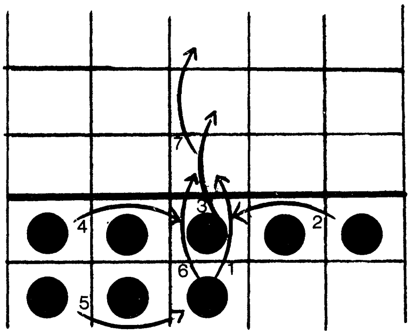


FIGURE 1.

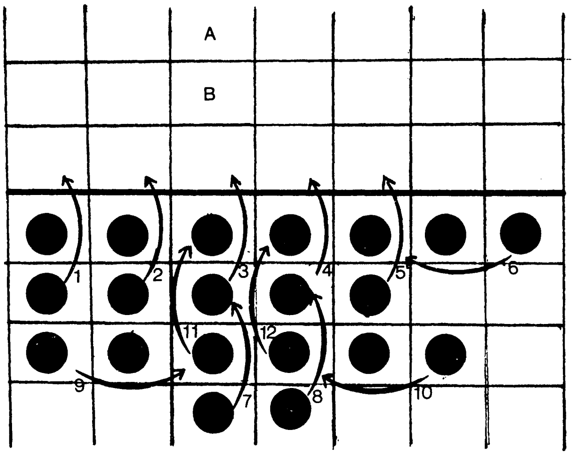


FIGURE 2.

checker pieces in squares A and B. (It is, of course, immediate from this result that level four can be attained.) It is perhaps appropriate to mention that twenty pieces is the fewest number which can be used to reach level four. (Note: Only the first twelve of the necessary moves are indicated in FIGURE 2. The reader should have no difficulty from there.)

The striking feature of Conway's problem is that no matter what initial configuration is chosen, *level five can never be achieved.* The proof of this is provided in [1], and in the following section we will adapt Conway's techniques to our variation.

The three dimensional analogue of Conway's problem requires essentially the same methods as the two dimensional problem. The interesting aspects of the three dimensional case are to show by construction that level seven can be attained, and then to apply ideas in [1] to show that this is best possible.

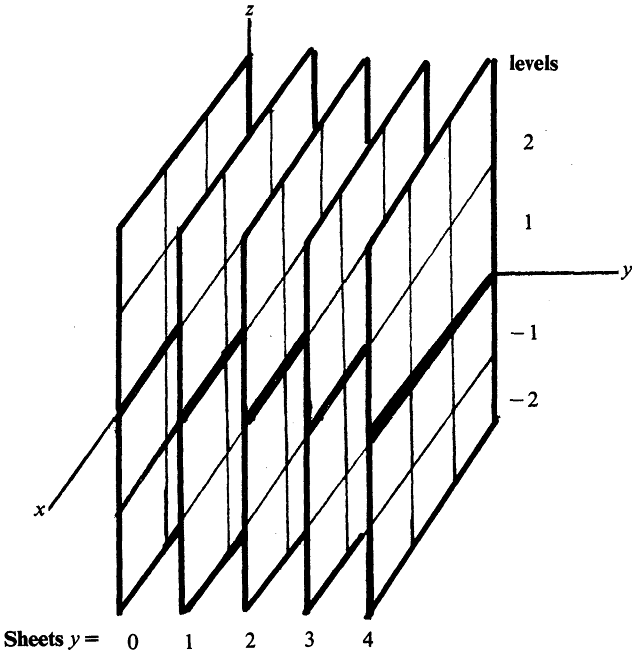
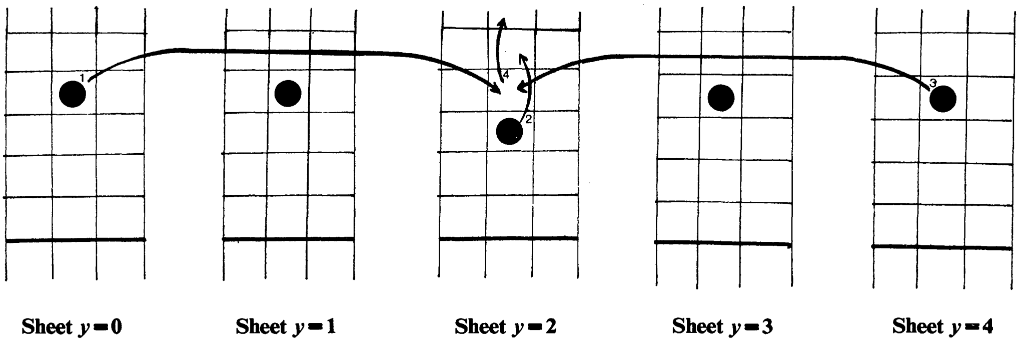


FIGURE 3.



A sequence of jumps beginning at level four that achieves level six.

FIGURE 4.

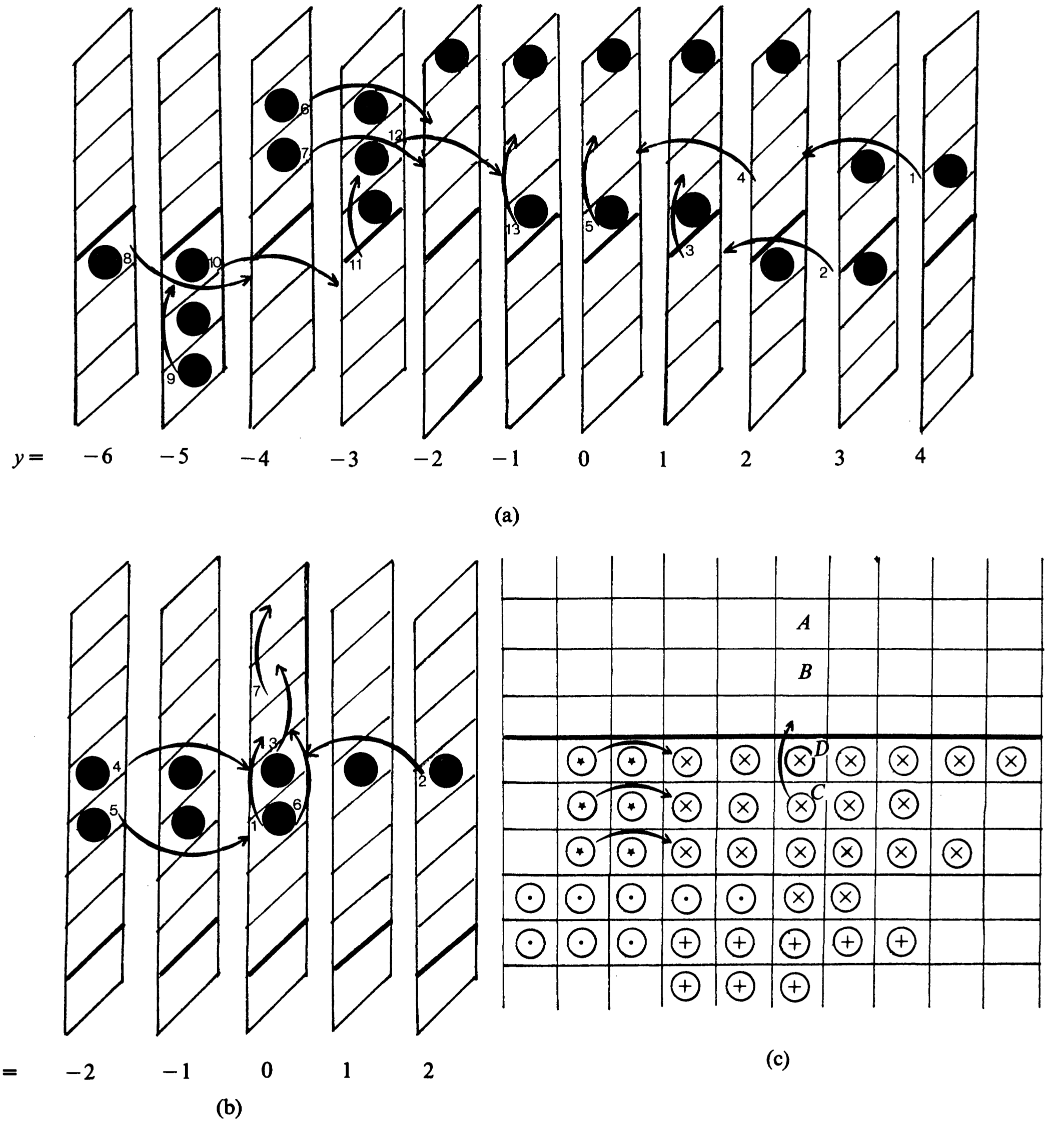
For ease of depicting three dimensional checker positions, our three dimensional checkerboard will consist of the planes $y=n$ for each integer n. In each of these planes, the x-axis will serve as the fold line (see FIGURE 3). As in Conway's original problem, our three-dimensional problem begins by positioning checkers below the folds of any number of sheets of the three dimensional board with any arrangement of checker pieces. The object is, in a finite number of moves, to advance as far as possible above any fold (i.e., in the positive z direction) by only using vertical and horizontal checker jumps on each sheet, and by using horizontal jumps from sheet to sheet.

It is immediate from Conway's problem [1] that we can reach the first four levels of any sheet by entirely restricting our initial configurations to that sheet. Levels five and six present no major obstacles, given the added degree of freedom (see FIGURE 4). However, the attainment of level seven is not obvious and requires a lengthy series of moves. As a first step in reaching level seven, we present a diagram (FIGURE 5a) consisting of parallel columns from different sheets and a sequence of moves which enables us to obtain a three-dimensional analogue of FIGURE 1. If we can construct the configuration of FIGURE 5a, then we can put a piece in level seven, as shown in FIGURE 5b. Since the subconfigurations in all planes, except possibly in $y=-3$ and $y=2$, are easily obtained (or are found in [1]), we need only show how to achieve the subconfigurations in planes $y=-3$ and $y=2$. This is done in FIGURE 5c.

To show that a piece cannot reach level eight of any sheet, it suffices on the sheet corresponding to the plane $y=0$ to take an arbitrary square P on level eight, and show that it is impossible to get there from any initial configuration below the folds. We give each box on each sheet a weight of x^n, where x is a positive number to be determined and n is the number of boxes in the shortest route to P by walking parallel to the axes (see FIGURE 6). The box P is assigned weight $x^0=1$. The **weight** of any position (relative to P) is then defined to be the sum of the corresponding weights assigned to the occupied boxes. We shall choose x so that the weight of any position either remains the same or is diminished no matter how many jumps are made with the pieces of that position.

To find such an x, an analysis of the different types of jumps is required. In general there are three types of jumps: (1) advancing closer to P, (2) retreating farther from P, (3) maintaining the same distance from P. These three types of jumps can occur on individual sheets as well as in the process of moving from one sheet to another. (See FIGURE 7 for a presentation of the different types of jumps occurring on a particular sheet. Similar diagrams are easily constructed to depict movement between sheets.)

In a jump of type 1 we gain the weight of x^n while losing the weights x^{n+1} and x^{n+2}. Thus, we may express the change as $x^n-(x^{n+1}+x^{n+2})=x^n(1-x-x^2)$. As for a jump of type 2 we may express the corresponding change in weight as $x^{n+2}-(x^{n+1}+x^n)=x^n(x^2-x-1)$. Finally, the change in weight for a move of type 3 is given by $x^n-(x^{n-1}+x^n)=-x^{n-1}$.



The sequence of moves in (a) leads to configuration (b), which yields a checker at level seven. Most planes in (a) are easy to achieve, except for $y=-3$ and $y=2$. To achieve $y=-3$, we use configuration (c), as follows: Using only the checkers of the form ⊗ we place two pieces at squares A and B. (see FIGURE 2 for the detailed moves). Then, using only the checkers of the form ⊕, we place a piece in square C (see FIGURE 1). After making three jumps with checkers ⊛ as indicated, the checkers depicted by ⊙ can be moved in the manner of FIGURE 1. Combining the outcome with the remaining checkers of the form ⊛ we place a piece in square D. To obtain the desired column in the plane $y=2$, the arrangement (c) can again be used by simply removing all checkers of the form ⊕.

FIGURE 5.

As in [**1**], our choice for x is that value which enables a jump of type 1 to not change the total weight of a given position. Thus, it suffices to take x to be the positive root of $1-x-x^2=0$. Note that $0<x<1$. By using the fact that x is positive and $x^2=1-x$, it is straightforward to verify that moves of type 2 and 3 reduce the weight of the original position. Hence, the weight of a given position will either remain unchanged or decrease in value after a finite number of moves has occurred. (See [**1**] for a similar analysis.)

To complete this variation of Conway's problem, we shall compute the value of the sum of the weights of aii squares *below* the folds of all sheets. Adding together the sums of the geometric

x^4	x^3	x^2	x	x^2	x^3
x^5	x^4	x^3	x^2	x^3	x^4
x^6	x^5	x^4	x^3	x^4	x^5
x^7	x^6	x^5	x^4	x^5	x^6
x^8	x^7	x^6	x^5	x^6	x^7
x^9	x^8	x^7	x^6	x^7	x^8
x^{10}	x^9	x^8	x^7	x^8	x^9
x^{11}	x^{10}	x^9	x^8	x^9	x^{10}
x^{12}	x^{11}	x^{10}	x^9	x^{10}	x^{11}

Sheet $y=-1$

x^3	x^2	x	P	x	x^2
x^4	x^3	x^2	x	x^2	x^3
x^5	x^4	x^3	x^2	x^3	x^4
x^6	x^5	x^4	x^3	x^4	x^5
x^7	x^6	x^5	x^4	x^5	x^6
x^8	x^7	x^6	x^5	x^6	x^7
x^9	x^8	x^7	x^6	x^7	x^8
x^{10}	x^9	x^8	x^7	x^8	x^9
x^{11}	x^{10}	x^9	x^8	x^9	x^{10}

Sheet $y=0$

x^4	x^3	x^2	x	x^2	x^3
x^5	x^4	x^3	x^2	x^3	x^4
x^6	x^5	x^4	x^3	x^4	x^5
x^7	x^6	x^5	x^4	x^5	x^6
x^8	x^7	x^6	x^5	x^6	x^7
x^9	x^8	x^7	x^6	x^7	x^8
x^{10}	x^9	x^8	x^7	x^8	x^9
x^{11}	x^{10}	x^9	x^8	x^9	x^{10}
x^{12}	x^{11}	x^{10}	x^9	x^{10}	x^{11}

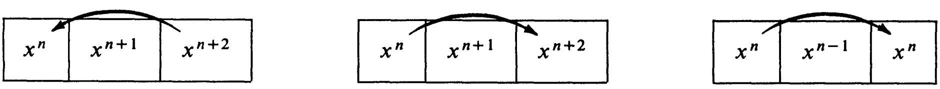
Sheet $y=1$

FIGURE 6.

series in each column below the folds, and using the fact that $1-x=x^2$, we obtain the following value:

$$V=\frac{x^8}{1-x}+\frac{4x^9}{1-x}+\frac{8x^{10}}{1-x}+\cdots+\frac{4jx^{8+j}}{1-x}+\cdots$$
$$=\frac{x^8}{1-x}+\frac{4x^9}{1-x}(1+2x+3x^2+\cdots)=\frac{x^8}{1-x}+\frac{4x^9}{(1-x)^3}$$
$$=x^6+4x^3=x^3(x^3+4)=(2x-1)(2x+3)=4x^2+4x-3=4-4x+4x-3=1.$$

Hence, since we are only allowed a finite number of moves, the weight of an initial position P must be (strictly) less than 1. Thus, it is impossible to culminate with a piece on square P, for this would yield a final position of weight 1 or greater.



Type 1 **Type 2** **Type 3**

FIGURE 7.

The imaginative reader will have perceived numerous possibilities for other variations of Conway's problem. Not only could one analyze the general n-dimensional case, but by allowing various different types of moves (e.g., the standard diagonal jump in checkers), the two dimensional case becomes very interesting. We end with this problem in mind, that is, to analyze Conway's 2-dimensional problem with the additional freedom of the standard diagonal jump in checkers. In solving this problem, a different weighting technique may be advantageous. However, the main difficulty will undoubtedly lie in constructing "best" positions as opposed to proving their optimality.

References

[1] R. Honsberger, Mathematical Gems II, The Mathematical Association of America, 1976.

[2] M. Gardner, Mathematical games, Scientific American, 238 (February, 1978) 27.

Lattice Points and Pick's Theorem

ANDY C. F. LIU
University of Alberta
Edmonton, Canada T6G 2G1

Pick's theorem [**6**] has duly received much attention in recent years, with the discovery of several elegant proofs. In this paper we give a new elementary proof and show that Pick's Theorem is topologically equivalent to the famous formula of Euler.

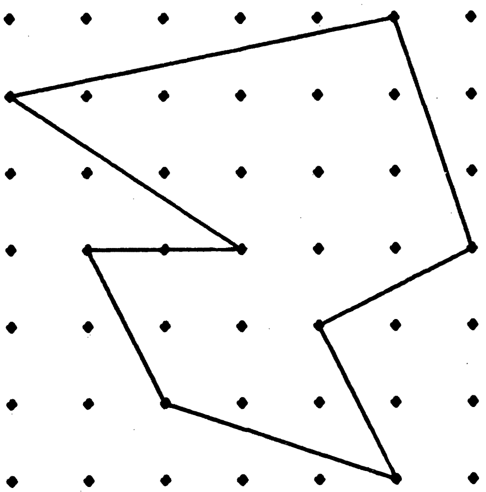
We remind the reader that in the Euclidean plane a lattice point is one whose coordinates are both integers, and a lattice polygon is one with lattice points as vertices. The area of lattice polygons is the subject of Pick's Theorem (see FIGURE 1): *The area A of a simple lattice polygon is given by $A = I + B/2 - 1$, where I and B denote respectively the numbers of interior and boundary lattice points of the polygon.*

All existing proofs of Pick's Theorem depend in important ways on primitive triangles, those lattice triangles with no interior lattice points and only three boundary lattice points (the vertices). It is easy to see that a lattice polygon can be decomposed into primitive triangles. Moreover, the following three propositions are all equivalent:

(1) Pick's Theorem: in a simple lattice polygon, $A = I + B/2 - 1$.
(2) The area of a primitive triangle is $1/2$.
(3) In a decomposition of a simple lattice polygon into primitive triangles, the number N of primitive triangles is given by $N = 2I + B - 2$.

For (3) implies (2), see [**2**], [**4**] or [**5**]; for (2) implies (1), see [**8**]. To see that (1) implies (3), apply (1) to a primitive triangle ($I = 0$ and $B = 3$) to obtain (2); it follows that $N = A/(\frac{1}{2}) = 2I + B - 2$.

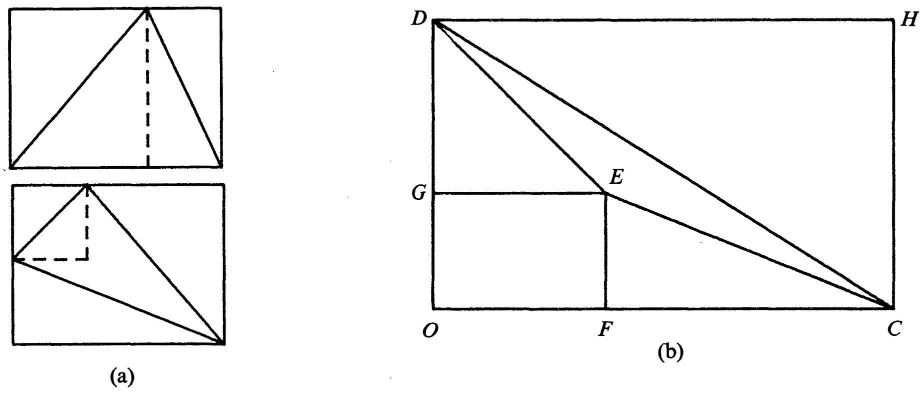
In view of this result, Pick's Theorem may be proved by establishing either (2) or (3); [**5**] and [**8**] use the former approach, [**2**] and [**4**] use the latter. Our proof shall be of (2). Inasmuch as Pick's Theorem is a statement about lattice points, they play a much more significant role in our proof than in any other proof of Pick's Theorem.



A=I+B/2−1=15+9/2−1=37/2.

FIGURE 1

To establish (2), let CDE be a primitive triangle and let $OCHD$ be the smallest lattice rectangle containing CDE. Since this rectangle is minimal, each of the four sides must pass through a vertex of the triangle, and the pigeon-hole principle forces the figures to share at least one vertex. Furthermore, unless a side of the triangle is actually a diagonal of the rectangle, the triangle will contain a lattice point in contradiction to its primitive character (see FIGURE 2a). Therefore we may assume that CD is a diagonal of the rectangle, as in FIGURE 2b.



(a)

(b)

FIGURE 2

Proceeding on this assumption, drop perpendiculars EF and EG to OC and OD, respectively. (E may coincide with F, G, or O.) Let O be the origin and OC and OD axes of a coordinate system. Let p and q be the x-coordinates of F and C respectively and let r and s be the y-coordinates of G and D respectively.

If $I(R)$ denotes the number of interior lattice points of a polygon R, then $I(OCHD) = (q-1)(s-1)$. Since CD contains no lattice points other than C and $D, I(OCD) = I(OCHD)/2 = (q-1)(s-1)/2$. Similarly, $I(CEF) = (q-p-1)(r-1)/2$ and $I(DEG) = (p-1)(s-r-1)/2$. Since CDE contains no interior lattice points, $I(OCD) - I(CEF) - (DEG) = pr$, the number of lattice points in $OFEG$ excluding those on OF or OG. This last equation simplifies to $qs - ps - qr = 1$. Finally, if $A(R)$ denotes the area of a polygon R,

$$\begin{aligned} A(CDE) &= A(OCD) - A(CEF) - A(DEG) - A(OFEG) \\ &= qs/2 - (q-p)r/2 - p(s-r)/2 - pr \\ &= (qs - ps - qr)/2 = 1/2. \end{aligned}$$

This completes the proof of (2), hence of Pick's Theorem too.

The relation $N = 2I + B - 2$ of (3) is recognized by several authors (see **[1]** and **[2]**) to hold in a more general topological setting. We shall now show that it is equivalent to the famous formula of Euler. It follows then that Pick's Theorem is topologically equivalent to Euler's Formula as well.

A **triangulation** (see FIGURE 3a) is a partition of a simple polygon into non-overlapping triangles which connect along entire sides. (FIGURE 3b does not represent a triangulation because triangles ABC and AEF connect along AF which is not an entire side of triangle ABC.) A triangulation can be accomplished in an unlimited number of ways. Around the outside of the figure occur sides which border only a single triangle; those occurring inside separate exactly two triangles of the triangulation. A triangulation generally introduces vertices of the partitioning triangles in the interior of the polygon and also on its sides.

Suppose we denote the number of triangles by N, the total number of edges in the triangulation by E, the number of vertices introduced in the interior by I, and the total number of vertices around the boundary by B. Then there are B sides of the triangles around the boundary, each bordering a single triangle, and $E - B$ edges inside the polygon, each bordering the two triangles it separates. Consequently, the $3N$ sides of the N triangles include each of the

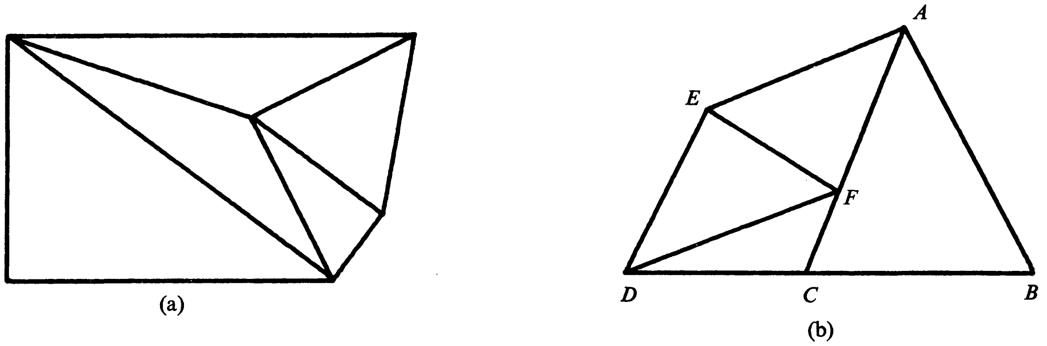


FIGURE 3

$E-B$ inner edges twice and each of the B outer edges just one, so we have $3N=2(E-B)+B=2E-B$.

If v, f, and e denote respectively the numbers of vertices, regions and edges of a simple planar map, Euler's Formula states that $v+f-e=2$. We shall now show that the following statements are equivalent:

(3) In a triangulation, $N=2I+B-2$.
(4) In a triangulation, $E=3I+2B-3$.
(5) Euler's formula: In a simple planar map, $v+f-e=2$.

For (5) implies (3), see [2]; for (3) implies (4), apply the formula $3N=2E-B$ to (3). To show that (4) implies (5), we argue as follows:

Inside every finite region of the simple planar map, introduce a new vertex and join it to all vertices of the region. This gives rise to a triangulation or a topological equivalent of it. As indicated above, let us denote the total number of vertices in this triangulation by $I+B$. Since there are v original vertices in the planar map and $f-1$ finite regions each of which yields a new vertex, $I+B=v+f-1$. Every triangle in the triangulation is bounded by one original edge of the planar map and two new edges. On the other hand, every new edge is a side of two triangles. Therefore, twice the number of new edges would count each triangle twice, showing that the number of new edges is equal to the number of triangles, which is N. Altogether, the total number of edges is $E=e+N$. Now, from (4) and the relation $3N=2E-B$ (proved above for every triangulation), we have

$$\begin{aligned} v+f-e &= (I+B+1)-(E-N) \\ &= I+B+1-(E+B)/3 \\ &= I+B+1-(I+B-1)=2, \end{aligned}$$

so the proof is completed.

As mentioned before, Gaskell, Klamkin and Watson [2] and Honsberger [4] proved Pick's Theorem by establishing (3), but only the former proof is topological. In proving Pick's Theorem, Funkenbusch [1] established (4) directly, but then appealed to Euler's Formula instead of deriving it.

The generalization of Pick's Theorem to higher dimensions may prove difficult (see [3], [5] and [7]). For further references, see [2] and [3].

The author thanks the referee and Murray S. Klamkin for suggestions which improved the presentation of the paper.

References

[1] W. W. Funkenbusch, From Euler's formula to Pick's formula using an edge theorem, Amer. Math. Monthly, 81 (1974) 647–648.

[2] R. W. Gaskell, M. S. Klamkin, and P. Watson, Triangulations and Pick's Theorem, this MAGAZINE, 49 (1976) 35–37.

[3] J. Hammer, Unsolved problems concerning lattice points, Fearon-Pitman, Belmont, Calif., 1977, pp. 12–19 and 44–49.

[4] R. Honsberger, Ingenuity in Mathematics, New Mathematical Library, vol. 23, MAA, 1970, pp. 27–31.

[5] I. Niven and H. S. Zuckerman, Lattice points and polygonal area, Amer. Math. Monthly, 74 (1967) 1195–1200.

[6] G. Pick, Geometrisches zur Zahlenlehre, Ztschr. d. Vereines 'Lotos', Prague, 1899.

[7] J. E. Reeves, On the volume of lattice polyhedra, Proc. London Math. Soc., (3) 7 (1957) 378–395.

[8] A. M. Yaglom and I. M. Yaglom, Challenging Mathematical Problems with Elementary Solutions, Volume 2, Holden-Day, San Francisco, 1964, pp. 62–66.

Snapping and Shaky Antiprisms

WALTER WUNDERLICH
Technical University
Vienna, Austria

In his interesting article [1] Michael Goldberg recently presented a number of interesting examples of multi-stable polyhedra. A polyhedron of this kind has the remarkable property of possessing two or more distinct forms with the same development, i.e., with the same faces in equal arrangement; the difference consists only in the corresponding dihedral angles along the edges. If two forms are not too different, a model made of rigid plates which are hinged at their edges may "snap" from one position to the other with a slight temporary elastic strain. If the two positions coincide, the structure is called "shaky". Theoretically, it would allow only an infinitesimal deformation, but in fact a corresponding model is not at all stable and shows a perceptible but limited mobility.

After mentioning the author's snapping octahedra [2], Goldberg suggested generalizing those triangular antiprisms by replacing the base triangles by other rigid polygons situated in parallel planes. In what follows we describe how to construct correctly such models having n-gons as bases.

Let $A_1A_2\ldots A_n (n \geqslant 3)$ be an arbitrary (not necessarily simple) rigid n-gon in the plane $z = h - s \geqslant 0$, h and s being numerical constants. By applying a screw motion about the z-axis, composed of a turn with angle 2σ and a translation of length $2s$, the polygon is transferred into a new position $A_1'A_2'\ldots A_n'$ in the plane $z' = h + s$. The coordinates x_i, y_i of any vertex A_i change to

$$x_i' = x_i \cos 2\sigma - y_i \sin 2\sigma, \quad y_i' = x_i \sin 2\sigma + y_i \cos 2\sigma. \tag{1}$$

The plane of symmetry of the chord A_iA_i', i.e., the plane which is perpendicular to and bisecting the segment A_iA_i', is defined by

$$(x - x_i)^2 + (y - y_i)^2 + (z - h + s)^2 = (x - x_i')^2 + (y - y_i')^2 + (z - h - s)^2$$

The intersections $b_i (i = 1, 2, \ldots, n)$ of these planes with a suitable plane which we call the base plane are the sides of a polygon $B_1B_2\ldots B_n (B_iB_{i+1} = b_i$, where $B_{n+1} = B_1)$. This n-gon may serve as base of a snapping polyhedron, provided the quantities σ and s are sufficiently small. The additional edges, connecting each point A_i with B_i and B_{i+1}, conserve their lengths when A_i passes to A_i', as $d(A_i, b_i) = d(A_i', b_i)$ where $d(X, Y)$ means the distance from X to Y.

If in particular we use the base plane $z=0$, the equation of the line b_i reads, after introduction of the expressions (1) and application of some well-known formulas of trigonometry, as follows:

$$-(x_i\sin\sigma+y_i\cos\sigma)x+(x_i\cos\sigma-y_i\sin\sigma)y=sh/\sin\sigma. \tag{3}$$

To arrive at a simple graphical construction, we apply to the orthogonal projection of A_i onto the base plane a rotation with angle $90°+\sigma$ about the origin O. The obtained point A_i^* has the coordinates

$$x_i^*=-x_i\sin\sigma-y_i\cos\sigma,\ y_i^*=x_i\cos\sigma-y_i\sin\sigma. \tag{4}$$

Hence equation (3) is equivalent to

$$x_i^*x+y_i^*y=sh/\sin\sigma=r^2, \tag{5}$$

and this relation means that b_i is the polar line of A_i^* with respect to a circle with radius r and center O. The corresponding construction is shown in FIGURE 1 and applied in FIGURE 2 to a quadrangle ($n=4$).

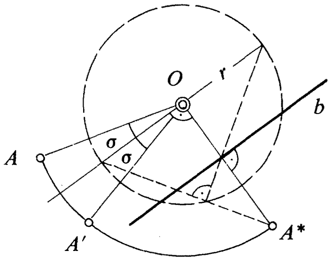


FIGURE 1

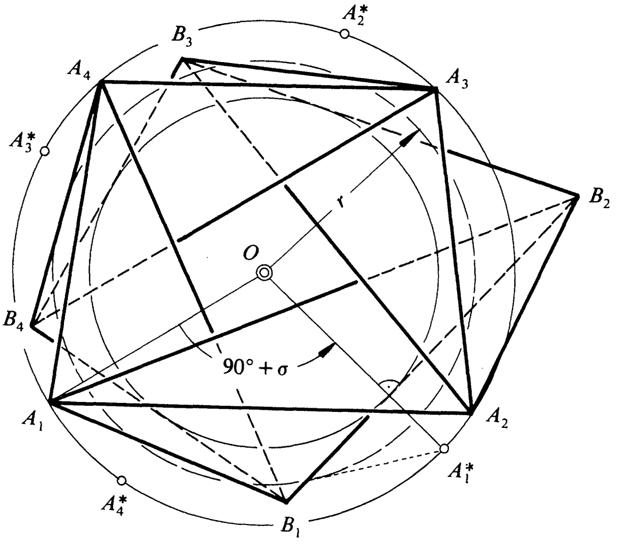


FIGURE 2

Having found a fitting pair of end faces $A_1A_2\ldots A_n$ and $B_1B_2\ldots B_n$ by means of the rule of FIGURE 1, the median height h of the snapping antiprism might still be changed within a certain range, as the construction depends only on r and σ; thus a prescribed value of h will be obtained by taking $s=r^2\sin\sigma/h$.

In the case $h=s$ the first form of the antiprism is collapsed into a plane. The limit case $\sigma=s=0$ with $\lim(s/\sigma)=c\neq 0$ leads to coinciding positions and therefore to shaky antiprisms. The construction of FIGURE 1, to be performed with a circle of radius $r=ch$, is applicable without difficulty. Due to the polarity the ray OB_i will be parallel to $A_{i-1}A_i$.

If, as in FIGURE 2, the polygon $A_1A_2\ldots A_n$ is inscribed in a circle centered on the z-axis, the base polygon $B_1B_2\ldots B_n$ will be circumscribed about a circle of the same kind and vice versa. (In FIGURE 2, where the (removed) upper face is a trapezoid, the base is a kite.) Consequently snapping and shaky antiprisms with similar or congruent end faces with coaxial circumcircles—as the triangular specimen in [2]—exist only if the polygons are regular.

References

[1] M. Goldberg, Unstable polyhedral structures, this MAGAZINE, 51 (1978) 165–170.

[2] W. Wunderlich, Starre, kippende, wackelige und bewegliche Achtflache, Elem. Math., 20 (1965) 25–32.

A Second Look at Descartes' Rule of Signs

Daniel S. Drucker
Wayne State University
Detroit, MI 48202

Let us begin with a question. Does the equation

$$7x^{11}+3x^8-13x^7-22x^6+5x^5-4x^4+x^3+8x^2=0$$

have any nonreal roots? The best conventional approach to this question is the following indirect line of reasoning based on Descartes' rule of signs:

1. Since x^2 is the largest power of x which is a factor of the left side of the equation, zero occurs exactly twice as a root.
2. By Descartes' rule, the number of positive roots is no greater than the number of variations of sign in the coefficients. (Actually, Descartes' rule says more: The difference between the number of variations of sign and the number of positive roots is an *even* nonnegative integer.) Reading from left to right, the signs of the coefficients are $++--+-++$, so there are 4 changes of sign, thus at most 4 positive roots.
3. By substituting $-x$ for x, we obtain the equation
$$-7x^{11}+3x^8+13x^7-22x^6-5x^5-4x^4-x^3+8x^2=0.$$
Every positive root of this equation is a negative root of the original equation, and vice versa. The signs of the coefficients in this equation are $-++-----+$, so by Descartes' rule, this equation has at most 3 positive roots. It follows that the original equation has at most 3 negative roots.
4. Every real root is zero, positive, or negative, so the original equation has at most 9 real roots. Since the degree of the equation is 11, there is at least one conjugate pair of nonreal roots.

The point of this note is to present a little-known formulation of Descartes' rule of signs, based on the gaps between the terms of the polynomial, that provides an immediate answer to our opening question.

Our reformulation of Descartes' rule will be a formula for the number of nonreal roots of a real polynomial f. To derive the formula, we assign a nonnegative even integer called a measure to each gap between the terms of f. The sum of these measures will be less than or equal to the number of nonreal roots of f.

Let $f(x)=a_dx^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0$. A **gap** in f consists of two nonzero coefficients, say a_i and $a_j(i>j)$, such that $a_k=0$ whenever $i>k>j$. It is customary for a gap to be called a **permanence** when the signs of a_i and a_j agree, and a **variation** when the signs are different. We say that a gap is even (resp. odd) when the number of missing terms between a_ix^i and a_jx^j is even (resp. odd). (Note that this number is $i-j-1$, not $i-j$.)

The measure of an even gap is defined to be the number of missing terms, while the measure of an odd gap is taken to be one more than this number when the gap is a permanence, and one less than this number when the gap is a variation. For example, a gap of measure 0 consists of the nonzero coefficients of two consecutive powers of x, or of a variation with one missing term. The **measure** of f is the sum of the measures of all gaps in f. For practice, check that the gaps in the polynomial $x^{19}+x^{16}-x^{13}-x^9+x^8-x^7+x^6+x^5-x^3$ are an even permanence of measure 2, an even variation of measure 2, an odd permanence of measure 4, and various gaps of measure 0, including an odd variation. This polynomial has measure 8.

Let V denote the number of variations in f and let V^- denote the number of variations in the polynomial obtained by replacing x with $-x$ in each term of f. Also let p (resp. n) denote the number of positive (resp. negative) roots of f. Descartes' rule of signs says that $V-p$ and V^--n

are nonnegative even integers. Finally let M denote the measure of f. We will show that *the number of nonreal roots of f equals the sum of the nonnegative even integers M, $V-p$, and $V^- - n$.*

Suppose that zero occurs z times as a root of f. This means that the expression for f ends with the nonzero term $a_z x^z$. Since the degree d of f equals the number of roots of f, we see that the number of nonreal roots of f is $d-z-p-n$. Thus we need only show that $d-z=M+V+V^-$.

When there are no missing terms between $a_d x^d$ and $a_z x^z, d-z$ is just the number of gaps in f. In general, $d-z$ is the sum of the number g of gaps and the number m of terms missing from the gaps: $d-z=g+m$. Let V_0 and V_E denote, respectively, the numbers of odd and even variations, and, similarly, P_0 and P_E the numbers of odd and even permanences. Then it follows from the definition of M that $m=M+V_0-P_0$. Since every gap is a variation or a permanence, and every permanence is even or odd, $g=V+P_E+P_0$. Substituting these last two relations in the expression for $d-z$, we obtain:

$$d-z=g+m=V+P_E+P_0+M+V_0-P_0=M+V+V_0+P_E.$$

When x is replaced by $-x$ in the expression for f, only odd powers of f change their sign. It follows that odd variations and even permanences of f become variations of the new polynomial, whereas even variations and odd permanences become permanences. In particular, $V^-=V_0+P_E$. Hence $d-z=M+V+V^-$. As we noted above, this yields the desired formula: the total number of nonreal roots is just $M+(V-p)+(V^- - n)$. Since $V-p$ and $V^- - n$ are nonnegative integers, there are at least M nonreal roots, i.e., at least $M/2$ conjugate pairs of complex roots. For example, the polynomial $x^{19}+x^{16}-x^{13}-x^9+x^8-x^7+x^6+x^5-x^3$ mentioned earlier has measure 8 and therefore has at least 4 conjugate pairs of complex roots.

Any gap with positive measure guarantees the existence of nonreal roots. In particular, any gap with two or more missing terms ensures that there are nonreal roots. (In the case of a permanence, one missing term suffices.) This observation is enough to answer the question raised at the beginning of the paper.

Books on the theory of equations often prove that $V=p$ and $V^-=n$ for real polynomials whose roots are real. Our formula yields a sharper result: *The roots of a real polynomial are all real precisely when $V=p$, $V^-=n$, and $M=0$.* This is because the sum of the nonnegative integers M, $V-p$, and $V^- - n$ can equal zero only when each of the summands is zero. Notice, however, that the conditions $V=p$ and $V^-=n$ can be satisfied without M vanishing. For example, the polynomial x^8-2x^4+1 has roots ± 1 and $\pm i$, each occurring twice, so $p=n=2$. We find that $V=V^-=2$, but $M=4$. On the other hand, the polynomial x^2-x+1 has measure 0, but $V-p=2-0=2$. Thus the condition $M=0$ is independent of the conditions $V=p$ and $V^-=n$.

There are many applications of the extended Descartes' rule in undergraduate mathematics. One that I have found interesting and useful is the classification of characteristic values of 3×3 complex matrices. In general, a 3×3 matrix A has characteristic polynomial

$$f(x)=x^3-(\mathrm{tr}A)x^2+\tfrac{1}{2}\left[(\mathrm{tr}A)^2-\mathrm{tr}(A^2)\right]x-\det A.$$

A straightforward analysis of all possible cases yields a classification of the nature of the characteristic values of A, which are the roots of $f(x)$, in terms of the signs of $\mathrm{tr}A$, $\det A$, and $[(\mathrm{tr}A)^2-\mathrm{tr}(A^2)]$. In the common case in which A is a real symmetric matrix, all the characteristic values are real, so this classification yields the signature of the matrix; this information can be used, for example, to classify critical points of functions of three variables.

For discussion and proofs of Descartes' rule, see the references listed below.

References

[1] A. A. Albert, An inductive proof of Descartes' rule of signs, Amer. Math. Monthly, 50 (1943) 178–180.

[2] N. B. Conkwright, Introduction to the Theory of Equations, Ginn, Boston, 1941.

[3] L. E. Dickson, First Course in the Theory of Equations, Wiley, New York, 1922.

[4] C. C. MacDuffee, Theory of Equations, Wiley, New York, 1954.

[5] J. V. Uspensky, Theory of Equations, McGraw-Hill, New York, 1948.

An Inequality for Convex Lattice Polygons

PAUL R. SCOTT
University of Adelaide
South Australia.

A **lattice polygon** Π is a simple polygon whose vertices are points of the integral lattice. We let $b=b(\Pi)$ denote the number of lattice points on the boundary of Π, and $c=c(\Pi)$ the number of lattice points interior to Π. In 1900, Pick [1] proved that the area of Π is given by $A(\Pi)=\frac{1}{2}b+c-1$. More recently it has been shown [2] that if Π is convex and has at least one interior lattice point, then $b \leqslant 2c+7$. This inequality is best possible, as is shown by the lattice triangle with vertices $(0,0)$, $(3,0)$ and $(0,3)$.

A simple modification of the proof of [2] allows us to establish the following result: *If* Π *is a convex lattice polygon and every angle of* Π *is acute, then* $b \leqslant 2c+4$, *and this result is best possible.* Of course in this case Π is just an acute-angled triangle. The triangle in Figure 1 satisfies $b=2c+4$.

Of rather more interest is the case in which every angle of Π is obtuse. *If* Π *is a convex lattice polygon and every angle of* Π *is obtuse, then* $b \leqslant 2c$, *and this result is best possible.* The lattice octahedron in FIGURE 2 with $b=8$ and $c=4$ shows that the inequality cannot be improved.

Let P be a lattice point on the boundary of Π. Since the angle at P is obtuse (or straight), the unit circle with centre P passes through at least one lattice point interior to Π. Hence, with each lattice point on the boundary of Π, we can associate an interior lattice point which is distant 1 from it.

The theorem will be established if we can show that each lattice point interior to Π is at a unit distance from not more than two lattice points on the boundary. Suppose that P,Q,R are three boundary lattice points at a unit distance from the interior lattice point I. Since the unit circle with center I passes through only four lattice points, two points, P,R say, must lie at opposite ends of a diameter. Let us take I to be the lattice point $(0,0)$, P to be $(0,1)$, and R to be $(0,-1)$; denote by H the half-plane $x \geqslant 0$.

By suitably reflecting Π we may assume that there exist parallel support lines to $\Pi \cap H$ at P,R which have non-negative slope. Hence there exist $h \geqslant 0, k>0$ such that $\Pi \cap H$ is supported

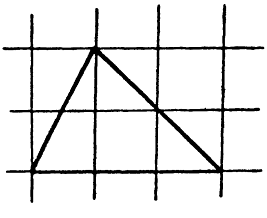


FIGURE 1

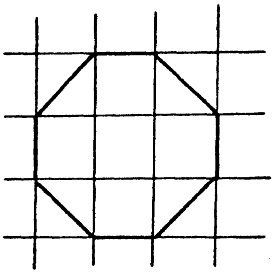


FIGURE 2

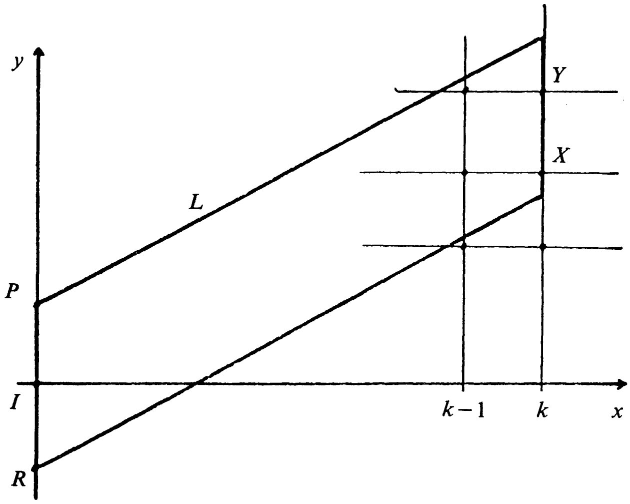


FIGURE 3

by the sides of the parallelogram L determined by the lines $x=0, x=k, y=hx\pm 1$. Clearly $\Pi\cap H \subset L$.

The parallelogram L in FIGURE 3 contains at most three of the lattice points on $x=k$. Further, since the angle of L at $(k, hk+1)$ is not obtuse, this point cannot be a vertex of Π, even if it is a lattice point. Hence Π has at most two vertices on $x=k$. Suppose X is the only vertex of Π on $x=k$. We observe that any segment lying on $x=k-1$ which subtends a right angle at X has length at least 2. Since L meets $x=k-1$ in a segment of length 2, it follows that Π cannot have an obtuse angle at X. Hence Π must have exactly two vertices X, Y on $x=k$. If $h=0$, then L is a rectangle, and Π cannot have obtuse angles at the points $(k, \pm 1)$. We deduce that $h>0$. Let X be (k,j) and Y be $(k,j+1)$. But now since L contains no lattice points satisfying $x<k, y>j+1$, the angle of Π at Y cannot be obtuse.

In every case, then, we obtain a contradiction. It follows that each lattice point interior to Π can be at a unit distance from not more than two lattice points on the boundary, and $b\leqslant 2c$ as required.

References

[1] G. Pick, Geometrisches zur Zahlenlehre, Sitzungsber Lotos Prag., (2) 19 (1900) 311–319.

[2] P. R. Scott, On convex lattice polygons, Bull. Austral. Math. Soc., 15(1976) 395–399.

Negative Based Number Systems

WILLIAM J. GILBERT
University of Waterloo
Waterloo, Ontario, Canada N2L 3G1

R. JAMES GREEN, student
University of Toronto
Toronto, Ontario, Canada M5S 1A1

Many number systems, besides the decimal system, are used for arithmetical calculation. Computers, in their internal working, usually use the binary system or sometimes the base 16 hexadecimal system. The Babylonians used base 60 for their number notation and the remains of this system can still be seen in our division of the hour and minute into 60 parts. In fact, any integer larger than one can be used as a base for the positive numbers. However, what is not so well known is that all the numbers, both positive and negative, can be represented by means of a negative integral base [**1**], [**3**]. Besides its intrinsic interest, the study of such a system forces one to understand and reevaluate the properties of positive bases that one takes for granted.

The representation of numbers in a negative base is simplified because there is no need for a sign to be attached to each negative number; it is already built in. For example, $-326=(-10)^3+7(-10)^2+3(-10)+4$, so -326 is represented by 1734 in base -10. A computer using base -2 has even been built that exploits this fact [**4**]. As we shall show below, all integers may be uniquely represented in a negative base; in fact, this representation is "more unique" than with a positive base because, without signs, there is not the problem of $+0$ being equal to -0. We can add, subtract and multiply in a negative base, even though we may obtain an infinite series of carry digits. This problem, however, can be overcome in various ways. We shall also show how to divide by integers to obtain negative based expansions of fractions. As with decimals, certain fractions have two different periodic expansions.

There have been other systems proposed for representing both positive and negative numbers without using a sign as a prefix. These usually consist of allowing the digits used in the expansion to include negative numbers. Linderholm [2; p. 63] suggests that the symbols ᔭ,Ɛ,↊,I 0,1,2,3,4,5 be used in decimal expansions, where ᔭ stands for -4, etc. For example, ↊Ɛ4 represents $-200-30+4=-226$. This is rather similar to the Yoruba system of numeration used in part of Nigeria [6]. In general, both positive and negative numbers can be represented in a positive base b if the digits allowed are any b consecutive integers that contain -1, 0 and 1. If b is odd, then the digits can be chosen symmetrically about zero and this simplifies many calculations [5].

To formalize negative bases, we say that the integer N is expressed in the base b if it is written in the form $N=\Sigma_{k=0}^{m}a_kb^k$, where $0\leqslant a_k<|b|$. We denote this by $N=(a_ma_{m-1}\ldots a_1a_0)_b$. If b is ten, we omit the parentheses and subscript b to obtain the usual decimal expansion. Whether the base is positive or negative, the digits a_k in the expansion can be calculated in the usual way by setting $q_0=N$ and then repeatedly using the division algorithm $q_k=q_{k+1}b+a_k$, where $0\leqslant a_k<|b|$, until the quotient becomes zero. For example, let us convert 34 to negative decimal (base -10) and negative binary (base -2):

$$\begin{array}{rl@{\qquad}rl}
34= & (-3)(-10)+4 & 34= & (-17(-2)+0 \\
-3= & 1(-10)+7 & -17= & 9(-2)+1 \\
1= & 0(-10)+1 & 9= & (-4)(-2)+1 \\
 & & -4= & 2(-2)+0 \\
 & & 2= & (-1)(-2)+0 \\
 & & -1= & 1(-2)+1 \\
 & & 1= & 0(-2)+1
\end{array}$$

Hence, $34=(174)_{-10}$ and $34=(1100110)_{-2}$. We can check these calculations by expanding the numbers to obtain

$$(174)_{-10}=1(-10)^2+7(-10)+4=100-70+4=34$$

and

$$(1100110)_{-2}=(-2)^6+(-2)^5+(-2)^2+(-2)=64-32+4-2=34.$$

Some other examples of expansions in negative binary and negative decimal are given in TABLE 1.

Decimal	Negative Decimal	Negative Binary
-12	$(28)_{-10}$	$(110100)_{-2}$
-11	$(29)_{-10}$	$(110101)_{-2}$
-10	$(10)_{-10}$	$(1010)_{-2}$
-9	$(11)_{-10}$	$(1011)_{-2}$
-8	$(12)_{-10}$	$(1000)_{-2}$
-7	$(13)_{-10}$	$(1001)_{-2}$
-6	$(14)_{-10}$	$(1110)_{-2}$
-5	$(15)_{-10}$	$(1111)_{-2}$
-4	$(16)_{-10}$	$(1100)_{-2}$
-3	$(17)_{-10}$	$(1101)_{-2}$
-2	$(18)_{-10}$	$(10)_{-2}$
-1	$(19)_{-10}$	$(11)_{-2}$

Decimal	Negative Decimal	Negative Binary
0	$(0)_{-10}$	$(0)_{-2}$
1	$(1)_{-10}$	$(1)_{-2}$
2	$(2)_{-10}$	$(110)_{-2}$
3	$(3)_{-10}$	$(111)_{-2}$
4	$(4)_{-10}$	$(100)_{-2}$
5	$(5)_{-10}$	$(101)_{-2}$
6	$(6)_{-10}$	$(11010)_{-2}$
7	$(7)_{-10}$	$(11011)_{-2}$
8	$(8)_{-10}$	$(11000)_{-2}$
9	$(9)_{-10}$	$(11001)_{-2}$
10	$(190)_{-10}$	$(11110)_{-2}$
11	$(191)_{-10}$	$(11111)_{-2}$

Expansions in various bases.
TABLE 1

If the base is a negative integer less than minus one, say $b=-s$, then *every integer, positive or negative, can be expanded uniquely in base b*. To show the existence of the expansion, we have to prove that the algorithm for finding the digits a_k always terminates. The successive quotients in the algorithm are given by $q_{k+1}=(q_k-a_k)/(-s)$, where $0 \leqslant a_k < s$ and $a_k \equiv q_k (\text{mod } s)$. Now if $q_k > 0$ then $|q_{k+1}| \leqslant |q_k/s| < |q_k|$. If $q_k < 0$, then $|q_{k+1}| = |(-q_k+a_k)/s| < |q_k/s|+1 \leqslant |q_k|$, unless $q_k=-1$. In the case $q_k=-1$ we have $a_k=s-1$ and $q_{k+1}=1$; however $q_{k+2}=0$. Therefore, the sequence of the absolute values of the quotients, $|q_k|$, decreases until it eventually becomes zero; thus the algorithm always terminates. The uniqueness of the digits in the base b expansion of an integer can be proved as follows. If two expansions represent the same integer, by looking at congruences modulo $|b|$ it can be seen that their rightmost digits must be the same. Subtracting these digits from their representations, dividing by b, and then repeating the argument will show that in each position their digits are the same.

Since a number in a negative base has no sign prefix, how do we tell whether it is positive or negative? The answer is simple: it is positive if it contains an odd number of digits, not counting leading zeros, and negative otherwise. You can tell which of two numbers is larger by comparing the digits of the highest power of the base in which they differ. If they begin to differ in an even power of the base, then the larger is the one with the larger digit. However, if they begin to differ in an odd power of the base, the larger is the one with the smaller digit. For example, $(3326)_{-10} > (3354)_{-10}$ because they begin to differ in the first power of -10. Using this rule we see that $(3547)_{-10} > (3261)_{-10}$ and $(111)_{-2} > (1010)_{-2}$.

We can add, subtract and multiply numbers in negative bases in the usual way. However, the carry digits are more complicated. Since $s=(1\,\overline{s-1}\,0)_{-s}$, where the symbol $\overline{s-1}$ stands for the single digit with value $s-1$, instead of carrying 1 we have to carry $1\,\overline{s-1}$ and this affects the next two higher places. For example, $2=(110)_{-2}$, $10=(190)_{-10}$, $20=(180)_{-10}$, etc; hence, instead of carrying one in negative binary we carry 11, instead of carrying one or two in negative decimal we carry 19 or 18 respectively. The following sample calculations are all done in base -10. In subtraction, we can borrow 10 in one column by adding 1 to the next higher column. We have dropped the subscripts -10 for convenience, and displayed carry digits in smaller type.

$$\begin{array}{r} 204 \\ +107 \\ \hline 491 \\ \hline {\scriptstyle 19} \end{array} \qquad\qquad \begin{array}{r} 204 \\ \times\ 107 \\ \hline 19588 \\ 20400 \\ \hline 39988 \\ \hline \end{array} \qquad\qquad \begin{array}{r} {\scriptstyle 6\ 1} \\ \cancel{5}7 \\ -48 \\ \hline 29 \\ \hline \end{array}$$

However, it often happens that the carry digits accumulate and we obtain an infinite series of carry digits. Compare the following two additions in base -10.

$$\begin{array}{r} 55 \\ +\ 27 \\ \hline \ldots 00062 \\ \hline {\scriptstyle 19} \\ {\scriptstyle 19} \\ {\scriptstyle 19} \\ \cdot \\ \cdot \\ \cdot \end{array} \qquad\qquad \begin{array}{r} 19 \\ +\ 1 \\ \hline \ldots 00000 \\ \hline {\scriptstyle 19} \\ {\scriptstyle 19} \\ {\scriptstyle 19} \\ \cdot \\ \cdot \\ \cdot \end{array}$$

It is clear from the second example above that this situation will always happen whenever we can represent both positive and negative numbers; since $-1=(1\,\overline{s-1})_{-s}$, adding 1 to this must give zero with an infinite series of carry digits. However, even though there is an infinite number of carry digits, the correct answer is obtained in a finite number of steps. It can be shown that if we add two numbers with r or fewer digits, then their sum contains $r+2$ or fewer digits. We could therefore program a computer to perform this arithmetic and not worry about the possibility of an infinite series of carry digits. In doing the arithmetic by hand, one soon recognizes those combinations of digits that sum to zero.

So far we have just considered integers in negative bases. However, it is also possible to represent any real number in a negative base by using an infinite expansion of the form $\sum_{k=-\infty}^{m} a_k b^k$ where $0 \leqslant a_k < |b|$. For example, $\frac{3}{8}=1-\frac{1}{2}-\frac{1}{8}=(1.101)_{-2}$. Any rational number p/q can be converted into base b by repeating the following division algorithm.

$$\begin{gathered} p=aq+r_0 \\ br_0=a_{-1}q+r_{-1} \\ br_{-1}=a_{-2}q+r_{-2} \\ \vdots \end{gathered}$$

We then obtain $p/q=(a.a_{-1}a_{-2}\ldots)_b$. When the base b and the numbers p and q are positive, the remainders are chosen so that $0 \leqslant r_{-k-1} < q$; this will automatically force the numbers a_{-k} to lie in the required range $0 \leqslant a_{-k} < b$. However this choice of the remainders r_{-k-1} does not work for negative bases. We have to adjust the remainder so that a_{-k} is an allowable digit in the range $0 \leqslant a_{-k} < |b|$ and so that the subsequent remainders stay bounded. There is sometimes a choice, as the following two ways of converting $1/3$ to negative binary shows. (All the numbers shown are in base 10.)

$$\begin{array}{rl} 1=0\cdot3+1 & \\ \left.\begin{array}{r} 1(-2)=-2=0\cdot3-2 \\ (-2)(-2)=4=1\cdot3+1 \\ 1(-2)=-2=0\cdot3-2 \end{array}\right\} & \begin{array}{l}\text{algorithm}\\ \text{repeats}\end{array} \end{array} \qquad \begin{array}{rl} 1=1\cdot3-2 & \\ \left.\begin{array}{r} (-2)(-2)=4=1\cdot3+1 \\ 1(-2)=-2=0\cdot3-2 \\ (-2)(-2)=4=1\cdot3+1 \end{array}\right\} & \begin{array}{l}\text{algorithm}\\ \text{repeats}\end{array} \end{array}$$

Hence $1/3=(.010101\ldots)_{-2}=(1.101010\ldots)_{-2}$. Both these repeating expansions can be checked by converting them back to fractional form in the usual way. This shows that the representation is not unique; this fact is well known in positive bases where, for example, $.5=.4999\ldots$ in the decimal system.

How do we decide which remainder to use at each stage of the algorithm? The remainder r_{-k} must of course be congruent modulo q to br_{-k-1}. The algorithm must be carried out as follows: In division by the positive integer q in the negative base $b=-s$, the digits a_{-k} are chosen in the range $0 \leqslant a_{-k} \leqslant |b|$ so that the remainders r_{-k} lie in the range $-[sq/(s+1)] \leqslant r_{-k} \leqslant [q/(s+1)]$, where [ ] denotes the greatest integer function. If q is not a multiple of $s+1$, then this range includes exactly one number from each congruence class modulo q and, as there is no choice for r_{-k}, there is only one representation. However, if q is a multiple of $s+1$, then the ends of the range are congruent modulo q and there is sometimes a choice for the digits. For example, when we divide by 3 in negative binary, the remainders must lie in the range $-2 \leqslant r_{-k} \leqslant 1$ and, as the second line in the previous expansions of $1/3$ show, we sometimes have a choice between -2 and 1 for the remainder. We leave it to the reader to show that the numbers with two different expansions in base $-s$ are those of the form $(-s)^k(a+(1/(s+1)))$, where a and k are integers.

The proof that the algorithm for division by q yields the correct expansion follows by showing that the remainders r_{-k} remain bounded if and only if they are chosen to lie in the stated range. This is done by induction. The basis for the induction is established by finding some integer a for which $p=aq+r_0$, where $-sq/(s+1) \leqslant r_0 \leqslant q/(s+1)$. This is always possible because the range of r_0 includes a complete congruence system modulo q. For the induction step, we split the range of the remainder r_{-k} into four cases and consider each separately.

Firstly, if $r_{-k} > q/(s+1)$, say $r_{-k} = (q/(s+1)) + a$, then $br_{-k} = (-s)r_{-k}$ is negative and a_{-k-1} is taken to be zero in order to keep the size of the remainder as small as possible. Then $br_{-k-1} = b^2 r_{-k} = (s^2 q/(s+1)) + s^2 a$ and, to reduce the size of the remainder as much as possible, we take $a_{-k-2} = s-1$ so that $r_{-k-2} = br_{-k-1} - (s-1)q = (q/(s+1)) + s^2 a$. By induction it follows that $r_{-k-2m} = (q/(s+1)) + s^{2m} a$ which shows that the expansion $(a.a_{-1}a_{-2}\ldots)_b$ will not converge to p/q. Secondly, if $r_{-k} < -sq/(s+1)$, say $r_{-k} = -sq/(s+1) - a$, it can be shown similarly that $r_{-k-2m+1} = (q/(s+1)) + s^{2m-1} a$ and the expansion still will not converge. Thirdly, if $0 \leqslant r_{-k} \leqslant q/(s+1)$ then br_{-k} is negative and we choose $a_{-k-1} = 0$. This means that r_{-k-1} lies in the allowable range $-sq/(s+1) \leqslant r_{-k-1} \leqslant 0$. Finally, if $-sq/(s+1) \leqslant r_{-k} < 0$, it follows that $0 \leqslant br_{-k} \leqslant s^2 q/(s+1) = (s-1)q + (q/(s+1))$. Then br_{-k} lies in the union of the closed intervals $[uq - (sq/(s+1)), uq + (sq/(s+1))]$ as u runs from 0 to $s-1$. Hence, there exists an integer a_{-k-1} with $0 \leqslant a_{-k-1} < s$ such that $br_{-k} = a_{-k-1}q + r_{-k-1}$, where $-sq/(s+1) \leqslant r_{-k-1} \leqslant q/(s+1)$. Since r_{-k-1} lies in the allowable range, this completes the induction step and shows that the algorithm for division works.

Because there can be at most $q+1$ choices for each remainder r_{-k}, it is clear that a rational number p/q will always yield a repeating (or terminating) expansion in any negative base. Conversely, as in positive bases, it can be shown that repeating expansions correspond to rational numbers.

The reader should try doing various arithmetical calculations in negative bases and should then check his answers. Addition, multiplication and subtraction can be checked by converting to decimals, while periodic expansions can be checked by finding the rational form in the usual way. Another exercise is to devise a scheme for converting numbers from base s to base $-s$ and then to find π in negative decimal to a certain number of decimal places. Since π is irrational, it will not have a periodic expansion in any base. It is also interesting to look at the standard algorithm for extracting the square root of a number. In negative bases there should be two answers if the number contains an odd number of digits and no answer otherwise.

References

[1] D. E. Knuth, The Art of Computer Programming, Vol. 2, Seminumerical Algorithms, Addison-Wesley, Reading, Mass., 1969.

[2] C. E. Linderholm, Mathematics Made Difficult, World Publishing, New York, 1972.

[3] A. H. Nelson, Investigation to discovery with a negative base, Math. Teacher, 60 (1967) 723–726.

[4] Z. Pawlak, An electronic digital computer based on the "−2" system, Bull. Acad. Polon. Sci., Sér. Sci. Tech., 7 (1959) 713–721.

[5] C. E. Shannon, Symmetrical notation for numbers, Amer. Math. Monthly, 57 (1950) 90–93.

[6] C. Zaslavsky, Africa Counts, Prindle, Weber and Schmidt, Boston, 1973.

Orthogonality of Generalized Eigenvectors

MAURICE MACHOVER
St. John's University
Jamaica, NY 11439

It is a well-known result that eigenvectors corresponding to different eigenvalues of a selfadjoint matrix are orthogonal. Specifically, this means that if A is an $n \times n$ matrix with complex entries such that A is equal to its adjoint A^* (which is its conjugate transpose $\bar{A}^T$), then $Ax = \lambda x$ and $Ay = \mu y$, for $\lambda \neq \mu$, implies $\langle x,y \rangle \equiv \Sigma_{p=1}^{n} x_p \bar{y}_p = 0$. If A is not selfadjoint, then the eigenvalues of A^* are the solutions of $\det(A^*-\lambda I)=\det(\bar{A}^T-\lambda I)=\overline{\det}(A^T-\bar{\lambda}I)$ $=\overline{\det}(A-\bar{\lambda}I)=0$ and hence are the complex conjugates of those of A. In this case the orthogonality result for selfadjoint matrices may be generalized as follows: if x is an eigenvector for the pair $\{A,\lambda\}$ and y is an eigenvector for $\{A^*,\bar{\mu}\}$ with $\lambda\neq\mu$, then x and y are orthogonal. The usual proof for this generalization is $\lambda\langle x,y\rangle=\langle\lambda x,y\rangle=\langle Ax,y\rangle=\langle x,A^*y\rangle=\langle x,\bar{\mu}y\rangle=$ $\mu\langle x,y\rangle$, hence $\langle x,y\rangle=0$.

This generalization, however, does not take account of the fact that the theorem on the Jordan canonical form for a matrix tells us that there is a set of generalized eigenvectors associated with a nonselfadjoint matrix [1]. The basic idea behind the generalized eigenvector is that we have not just a single vector x such that $(A-\lambda I)x=0$, but a sequence of vectors $x_0=0,x_1,x_2,\dots,x_n$ such that $(A-\lambda I)x_i=x_{i-1}$. The reader who is familiar with the Jordan form will recognize that for each block in the Jordan form we obtain such a chain of generalized eigenvectors and that the length of the chain is just the size of the corresponding block. Let us be precise and establish our notation. If the distinct eigenvalues of A are $\lambda_1,\lambda_2,\dots,\lambda_p$, there is associated with each λ_j a set of C_j chains (one for each block involving λ_j) of generalized eigenvectors $\{x_{kl}^{(j)}\},k=1,2,\dots,C_j$, where the l denotes the position in the chain. Hence $l=$ $1,2,\dots,r_{jk}$, where r_{jk} is the length of the kth chain for λ_j (the size of the kth block for λ_j) and $(A-\lambda_jI)x_{kl}^{(j)}=x_{kl-1}^{(j)}$ for $2\leqslant l\leqslant r_{jk}$ and $(A-\lambda_jI)x_{k1}^{(j)}=0$. The second subscript is called the rank of the generalized eigenvector and denotes the lowest power of $A-\lambda_jI$ that must be used to annihilate it. (An ordinary or proper eigenvector has rank one.) The number and lengths of the chains for each λ_j are uniquely determined by A. Moreover, A^* has a similar set of chains $y_{kl}^{(j)}$ corresponding to each $\bar{\lambda}_j$. It turns out that the orthogonality relation may be extended to include all the generalized eigenvectors, though most textbooks on linear algebra do not mention this fact. An obvious, but involved, way of establishing it would be to perform a detailed comparison of the similarity transformations leading to the Jordan canonical forms for A and A^*. The following proof is shorter, involves no more than the use of the scalar product, and is more in the style of the usual proof given for ordinary eigenvectors.

THEOREM. *If x and y are generalized eigenvectors for $\{A,\lambda\}$ and $\{A^*,\bar{\mu}\}$, respectively, with $\lambda\neq\mu$, then x and y are orthogonal.*

Proof. The proof proceeds by induction on the rank of y. First let y have rank one, so that $(A^*)^ky=\bar{\mu}^ky$ for all positive integers k. Suppose x has rank m. Then

$$0=\langle(A-\lambda I)^mx,y\rangle=\Big\langle\sum_{j+k=m}(-1)^j\frac{m!}{j!k!}\lambda^jA^kx,y\Big\rangle=\sum_{j+k=m}(-1)^j\frac{m!}{j!k!}\lambda^j\langle A^kx,y\rangle$$
$$=\sum_{j+k=m}(-1)^j\frac{m!}{j!k!}\lambda^j\langle x,(A^*)^ky\rangle=\sum_{j+k=m}(-1)^j\frac{m!}{j!k!}\lambda^j\mu^k\langle x,y\rangle=(-1)^m(\lambda-\mu)^m\langle x,y\rangle,$$

so that $\langle x,y\rangle=0$. Next, assume the result holds if y has rank k. Suppose y has rank $k+1$ and x has rank m. Since $(A^*-\bar{\mu}I)y$ has rank k,

$$0=\langle(A-\lambda I)^{m-1}x,(A^*-\bar{\mu}I)y\rangle=\langle(A-\lambda I)^{m-1}x,(A^*-\bar{\lambda}I)y+(\bar{\lambda}-\bar{\mu})y\rangle$$
$$=\langle(A-\lambda I)^mx,y\rangle+(\lambda-\mu)\langle(A-\lambda I)^{m-1}x,y\rangle=(\lambda-\mu)\langle(A-\lambda I)^{m-1}x,y\rangle,$$

so that $\langle(A-\lambda I)^{m-1}x,y\rangle=0$. Starting now with $(A-\lambda I)^{m-2}x$ and using this last result, we repeat the process to get $0=\langle(A-\lambda I)^{m-2}x,\ (A^*-\bar{\mu}I)y\rangle=(\lambda-\mu)\langle(A-\lambda I)^{m-2}x,y\rangle$; hence $\langle(A-\lambda I)^{m-2}x,y\rangle=0$. By continuing this process for $m-2$ more steps we arrive at $\langle(A-\lambda I)^{m-m}x,y\rangle$ $=\langle x,y\rangle=0$.

Reference

[1] L. Brand, Matrices with specified eigenvalues and associated eigenvectors, proper or generalized, Amer. Math. Monthly, 74 (1967) 640–648.

Solution Spaces of Differential Equations

MYREN KROM
California State University
Sacramento, CA 95819

The solution space of a linear homogeneous differential equation is a vector space. Conversely, given a finite dimensional vector space of analytic functions, it is easy to construct (see below) a differential equation with the given vector space as its solution space. The theorem proved below gives two properties of a finite dimensional vector space of analytic functions, each of which is a necessary and sufficient condition for the corresponding differential equation to be a constant coefficient differential equation.

The solution space of the nth order linear homogeneous differential equation with analytic coefficients,

$$a_n(z)\frac{d^ny}{dz^n}+\cdots\cdot a_1(z)\frac{dy}{dz}+a_0(z)y=0,\text{ with } a_n(z)\not\equiv 0,$$

is an n-dimensional vector space of analytic functions [3, p. 194–196], [5, p. 114]. Conversely, if F is a finite dimensional vector space of analytic functions, we can find a differential equation which has F as its solution space by the following method.

First choose a basis $\{\phi_1,\phi_2,\ldots\phi_n\}$ for the vector space F. The Wronskian of these basis functions is an analytic function by construction and it is not identically zero [1, p. 34], [2, p. 91]. If we let $L[y]$ be the result of expanding the determinant

$$\begin{vmatrix} y & \phi_1 & \phi_2 & \cdots\cdots & \phi_n \\ y' & \phi_1' & \phi_2' & \cdots\cdots & \phi_n' \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ \cdot & & & & \\ y^{(n)} & \phi_1^{(n)} & & \cdots\cdots & \phi_n^{(n)} \end{vmatrix}$$

by the elements of the first column, then $L[y]=0$ is a linear differential equation with analytic coefficients. The coefficient of the term of highest order in this differential equation is the Wronskian of the chosen basis functions; this Wronskian is not zero. Therefore, the differential equation is of order n. By elementary properties of determinants each of the basis functions satisfies the differential equation; the n-dimensional solution space is F.

Example 1. Let F be the vector space with the basis $\{t,e^t\}$. We expand the determinant

$$\begin{vmatrix} y & t & e^t \\ y' & 1 & e^t \\ y'' & 0 & e^t \end{vmatrix}$$

by the elements of the first column to get $(t-1)y''-ty'+y=0$.

Example 2. Let F be the vector space with the basis $\{te^t,e^t\}$. We expand the determinant

$$\begin{vmatrix} y & te^t & e^t \\ y' & te^t+e^t & e^t \\ y'' & te^t+2e^t & e^t \end{vmatrix}$$

by the elements of the first column to get $y''-2y'+y=0$.

Example 3. Consider the constant coefficient differential equation

$$a_n\frac{d^ny}{dz^n}+\cdots a_1\frac{dy}{dz}+a_0y=0,\text{ with } a_n\neq 0.$$

A basis for the solution space F is given by

$$\{z^ke^{z\lambda_i}\}k=0,1,\ldots,m_i-1;i=1,\ldots,s$$

where $\lambda_1,\ldots,\lambda_s$ are the distinct roots of the characteristic equation

$$f(\lambda)=a_n\lambda^n+\cdots+a_1\lambda+a_0=0$$

and λ_i has multiplicity m_i [**4**, p. 89]. Note that F is closed under translation and differentiation.

Only for the last two of these three examples is the differential equation corresponding to the given vector space a constant coefficient differential equation. Those vector spaces for which the differential equation is a constant coefficient differential equation are characterized by either of the two properties in the following theorem.

THEOREM. *Let Ω be a domain in the complex plane. Let H be the vector space of all complex valued functions analytic in Ω. Let F be a finite dimensional subspace of H. Then the following are equivalent*:

(1) *F is the solution space of a linear homogeneous constant coefficient differential equation*;
(2) *F is closed under translations*;
(3) *F is closed under differentiation.*

Proof. (1) implies (2). If a function f is a solution of a linear homogeneous constant coefficient differential equation, then by the chain rule for differentiation any translate of f (i.e., $f(z+k)$ where k is a constant) must also be a solution of that differential equation.
(2) implies (3). Since F is closed under translations, for every function f in F and every positive integer n the translate $f(z+\frac{1}{n})$ is an element of F. Therefore, since F is a vector space, the difference quotient $n[f(z+\frac{1}{n})-f(z)]$ is also an element of F. The limit of this sequence of difference quotients is the derivative of f. This limit is an element of F because H is a topological vector space under the topology of uniform convergence on compact subsets of Ω [**6**, p. 238], [**7**, p. 373] and every finite-dimensional subspace of a topological vector space is closed [**7**, p. 152].
(3) implies (1). The proof of this part of the theorem is based on the following lemma. The assumptions here, and in the lemma, are (3), the dimension of F is n, and $p\in\Omega$.

LEMMA. *For every basis B for F and for every positive integer k such that $1\leqslant k\leqslant n$, there is a function in B with nonzero* kth *term in its Taylor series expansion about p.*

Proof. Suppose there is a basis B for F and a k such that $1\leqslant k\leqslant n$ and for every function in B the kth term in its Taylor series expansion about p is zero. Then every function in F would have zero as the kth term in its Taylor series expansion about p since every function in F can be expressed as a linear combination of the functions in the basis B. The kth term of the Taylor series for any function in F is a linear combination of the kth terms of the basis functions [**8**, p. 182]. It follows from this and the fact that F is closed under differentiation that the Taylor series expansion about p of each function in F terminates at least by the kth term. This is a contradiction because it implies that the functions in the basis B are all polynomials of degree at most $k-2$; hence, these functions can't span an n-dimensional vector space. This completes the proof of the lemma.

By use of the lemma and a familiar triangularization process [**9**, p. 89], we may assume $B=\{\phi_1,\phi_2,\ldots\phi_n\}$ where, for $1\leqslant k\leqslant n$, the first nonzero term in the Taylor series expansion about p of ϕ_k is the kth term. The function ϕ_n and its first $n-1$ derivatives form a linearly independent set and, hence, another basis B_1 for F. The nth derivative of ϕ_n is in F; it can then be expressed in terms of the new basis B_1. That is, there exist constants $\alpha_1,\alpha_2,\ldots,\alpha_n$ such that

$$\phi_n^{(n)}=\alpha_1\phi_n^{(n-1)}+\alpha_2\phi_n^{(n-2)}+\cdots+\alpha_n\phi_n.$$

Clearly ϕ_n is a solution of the following linear homogeneous differential equation with constant coefficients:

$$\frac{d^ny}{dz^n}-\alpha_1\frac{d^{n-1}y}{dz^{n-1}}-\alpha_2\frac{d^{n-2}y}{dz^{n-2}}-\cdots\cdot-\alpha_ny=0.$$

By differentiating both sides of this differential equation we see that the first $n-1$ derivatives of ϕ_n are also solutions. Since every element of the basis B_1 for the n-dimensional vector space F satisfies the nth order differential equation above, F is the solution space of that differential equation.

References

[1] G. Birkhoff, G. Rota, Ordinary Differential Equations, Blaisdell Publishing Company, Waltham, Massachusetts, 1969.

[2] M. Bocher, The theory of linear dependence, Ann. of Math., Second Series, Vol. 2 (1900) 81–96.

[3] G. Carrier, M. Krook, C. Pearson, Functions of a Complex Variable, McGraw-Hill Book Co., New York, 1966.

[4] E. Coddington, N. Levinson, Theory of Ordinary Differential Equations, McGraw-Hill Book Co., New York, 1955.

[5] R. Finney, D. Ostberg, R. Kuller, Elementary Differential Equations With Linear Algebra, Addison-Wesley Publishing Co., Reading, 1976.

[6] J. Horvath, Topological Vector Spaces and Distributions, Vol. 1, Addison-Wesley Publishing Co., Reading, 1966.

[7] G. Kothe, Topological Vector Spaces 1, Springer-Verlag, New York, 1969.

[8] E. Saff, A. Snider, Fundamentals of Complex Analysis for Mathematics, Science, and Engineering, Prentice-Hall, New Jersey, 1976.

[9] R. Thrall, L. Tornheim, Vector Spaces and Matrices, Dover Publications, New York, 1970.

A Number Field Without Any Integral Basis

HUGH M. EDGAR
San Jose State University
San Jose, CA 95192

If K is an algebraic number field, that is a field which forms a finite dimensional vector space over Q, then every algebraic integer (i.e., root of a monic polynomial with integral coefficients) living in K can be uniquely expressed as a Z-linear combination of a distinguished subset $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ of the integers of K, where $n=[K:Q]$ is the dimension of the vector space. Any such set is called an **integral basis** for K/Q. More generally, if K is an algebraic number field whose ring of integers $[K]$ forms a UFD (unique factorization domain) and if L is any n-dimensional extension field of K, then there exists a distinguished subset $\{\beta_1,\beta_2,\ldots,\beta_n\}\subseteq[L]$ such that every algebraic integer of L is uniquely expressible as a $[K]$-linear combination of $\beta_1,\beta_2,\ldots,\beta_n$. Any such set $\{\beta_1,\beta_2,\ldots,\beta_n\}$ is called a **relative integral basis** (RIB) for L/K.

MacKenzie and Scheuneman ([1]) proved that if $K=Q(\sqrt{-14})$ and $L=Q(\sqrt{-7},\sqrt{-14})$ then L/K has no RIB. From what has been said above, it is clear that in any such example K must be chosen so that $[K]$ is not a UFD. Since there are only nine imaginary quadratic fields K for which $[K]$ is a UFD, it is easy to arrange for $[K]$ not to be a UFD in this context. The case of real quadratic fields is more delicate since, for instance, it is still not known whether there are infinitely many real quadratic fields K for which $[K]$ is a UFD. The object of this article is to provide a simple concrete example of a pair of real algebraic number fields L and K for which $[L:K]=[K:Q]=2$ while the relative extension L/K has no RIB. The argument is patterned on that of MacKenzie and Scheuneman.

We want a real quadratic field $K=Q(\sqrt{n})$ for which $[K]$ is not a UFD. The factorizations $6=2\cdot 3=(4+\sqrt{10})(4-\sqrt{10})$ can be used to prove that if $n=10$ then $[K]=[Q(\sqrt{10})]$ is not a UFD (see for instance, [2] or [3]). Since $[K]=[Q(\sqrt{n})]$ is a UFD for all positive integers $n<10$ (see, for instance, [4], p. 100) our choice of $K=Q(\sqrt{10})$ is a natural one. We next define L to be $K(\sqrt{5})=Q(\sqrt{5},\sqrt{10})$.

We wish to show that $[L:K]=2$ and for this it suffices to prove that $\sqrt{5}\notin Q(\sqrt{10})$. If $\sqrt{5}\in Q(\sqrt{10})$ then $\sqrt{5}=a+b\sqrt{10}$ for suitable $a,\ b\in Q$ and so $5=a^2+10b^2+2ab\sqrt{10}$ which forces ab to be 0. Each of the equations $a=0$, $b=0$ leads to a contradiction and so $\sqrt{5}\notin Q(\sqrt{10})$ and hence $[L:K]=2$.

To prove that the fields L and K have the desired properties, we have to show only that L/K has no RIB. This we do in two steps: first we show that if L/K had a RIB of any kind, then $\{1,(1+\sqrt{5})/2\}$ must also be a RIB for L/K. Then we show that $\{1,(1+\sqrt{5})/2\}$ is *not* a RIB for L/K.

Much of our argument involves the $[K]$-ideal $P=(5,\sqrt{10})$ generated by the two elements 5 and $\sqrt{10}$. We begin by showing that P is not a principal $[K]$-ideal. We will show later that this fact will also provide another way of establishing that $[K]$ is not a UFD.

We start by showing that $P^2=(5,\sqrt{10})^2=(5)$, where (5) denotes the principal $[K]$-ideal generated by the element 5. According to the definition of multiplication of ideals, $(5,\sqrt{10})^2=(25,5\sqrt{10},5\sqrt{10},10)=(25,5\sqrt{10},10)$. Thus 25 and 10 both belong to $(5,\sqrt{10})^2$, hence their greatest common divisor, 5, belongs to $(5,\sqrt{10})^2$ and so $(5)\subseteq(5,\sqrt{10})^2$. Conversely, each of the three quantities 25, $5\sqrt{10}$ and 10 is obviously a $[K]$-multiple of 5 so $(5,\sqrt{10})^2\subseteq(5)$ and so $(5)=(5,\sqrt{10})^2$. Taking norms (the number $N(I)$ of residue classes of an ideal I in $[K]$) throughout this ideal equation we get $N((5))=|N(5)|=5^2=N((5,\sqrt{10})^2)=[N((5,\sqrt{10}))]^2$ so that $N((5,\sqrt{10}))=5$. If $(5,\sqrt{10})$ were a principal $[K]$-ideal it would be possible to write $(5,\sqrt{10})=(a+b\sqrt{10})$ for suitable $a,b\in Z$. Again taking norms throughout this ideal equation we get $N((5,\sqrt{10}))=5=N((a+b\sqrt{10}))=|N(a+b\sqrt{10})|=|a^2-10b^2|$, which requires $a^2-10b^2=\pm 5$. However, it is easy to show that these two Pellian equations are insoluble and so we have proved that $(5,\sqrt{10})$ is a nonprincipal $[K]$-ideal.

We will now show that if L/K has a RIB then $\{1,\ (1+\sqrt{5})/2\}$ is a RIB for L/K. (The numbers $(1\pm\sqrt{5})/2$ are in $[L]$ since they are the roots of x^2-x-1.) Let us assume that $\{\alpha,\beta\}$ forms a RIB for L/K. Then there must exist $a,\ b,\ c,\ d,\in[K]$ for which we have

$$a\alpha+b\beta=1,$$
$$c\alpha+d\beta=\frac{1+\sqrt{5}}{2}. \tag{1}$$

If we apply to each of these equations the K-automorphism of L which takes $\sqrt{5}$ onto $-\sqrt{5}$ we obtain the equations

$$a\bar{\alpha}+b\bar{\beta}=1,$$
$$c\bar{\alpha}+d\bar{\beta}=\frac{1-\sqrt{5}}{2}, \tag{2}$$

where $\bar{\alpha}$, $\bar{\beta}$ denote, respectively, the image of α, β under this automorphism. Combining (1) and (2) in matrix form gives

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix}\alpha & \bar{\alpha}\\ \beta & \bar{\beta}\end{pmatrix}=\begin{bmatrix} 1 & 1\\ \dfrac{1+\sqrt{5}}{2} & \dfrac{1-\sqrt{5}}{2}\end{bmatrix}. \tag{3}$$

We now take the square of the determinant of both sides of (3) and find that

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix}^2 \begin{vmatrix} \alpha & \bar{\alpha} \\ \beta & \bar{\beta} \end{vmatrix}^2 = \begin{vmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{vmatrix}^2 = 5 = \gamma^2\delta \tag{4}$$

where

$$\gamma = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \text{ and } \delta = \begin{vmatrix} \alpha & \bar{\alpha} \\ \beta & \bar{\beta} \end{vmatrix}^2.$$

Since a, b, c, $d \in [K]$ it follows that $\gamma \in [K]$. It is also known (see, for instance, [**5**], p. 64) that $\delta \in [K]$. Hence $(\gamma^2\delta) = (5) = (\gamma)^2(\delta) = (5, \sqrt{10}\,)^2 = P^2$ makes sense as an equation among $[K]$-ideals. We have already proved that $P = (5, \sqrt{10}\,)$ is a nonprincipal $[K]$-ideal. P is also a prime ideal since its norm is the rational integral prime 5. We now use the theorem which says that any $[K]$-ideal factors uniquely into a product of distinct prime $[K]$-ideals raised to appropriate positive integral powers. If $(\gamma) \neq (1)$ then (γ) must possess at least one prime ideal factor and from the equation $(5) = (\gamma)^2(\delta) = P^2$ we see that this forces $(\gamma) = P$. Since P is nonprincipal, it follows that $(\gamma) = (1)$ and so γ must be a unit of the ring $[K]$. Solving for α from (3) we get

$$\alpha = (\gamma^{-1}d)1 + (-b\gamma^{-1})\left(\frac{1+\sqrt{5}}{2}\right)$$

which shows that α is a $[K]$-linear combination of 1 and $(1+\sqrt{5}\,)/2$. Likewise β can be shown to be a $[K]$-linear combination of 1 and $(1+\sqrt{5}\,)/2$ and hence every element of the $[K]$-module generated by α and β can be so represented. However, α and β together generate all of $[L]$, by assumption, so we have shown that if any $\{\alpha,\beta\}$ form a RIB for L/K, then so also do $\{1,(1+\sqrt{5}\,)/2\}$.

But now we can show that $\{1,(1+\sqrt{5}\,)/2\}$ does not form a RIB for L/K. If it did, then we may write

$$\sqrt{2} = A\cdot 1 + B\cdot\left(\frac{1+\sqrt{5}}{2}\right)$$

for suitable $A,B \in [K]$ since $\sqrt{2} = \sqrt{10}\,/\sqrt{5} \in [L]$. Then, applying the same K-automorphism of L as before, we obtain

$$-\sqrt{2} = A\cdot 1 + B\cdot\left(\frac{1-\sqrt{5}}{2}\right).$$

Hence $2\sqrt{2} = B\sqrt{5}$ so that $2^3 = 5B^2$ which is impossible. Hence $\{1,(1+\sqrt{5}\,)/2)$ cannot form a RIB for L/K and so we can conclude that L/K has no RIB whatsoever.

We close with some observations about where we are and how we got there. It is well known that the three conditions, that $[K]$ be a UFD, that $[K]$ be a PID (principal ideal domain) and that the class number, $h(K)$, be equal to one, are all equivalent whenever K is an algebraic number field. Hence, when we proved that $(5, \sqrt{10}\,)$ was a nonprincipal $[K]$-ideal we also had shown that $[K]$ was not a UFD and that $h(K) > 1$. A very pretty theorem of Mann ([**6**]) says that if $h(K) > 1$, then there must exist a quadratic extension L of K for which L/K has no RIB. So in some sense (existential!) we are guaranteed success once we know that $h(Q(\sqrt{10}\,)) > 1$, i.e., there must be a quadratic extension L of $Q(\sqrt{10}\,)$ for which $L/Q(\sqrt{10}\,)$ has no RIB. Our achievement has been to exhibit a concrete example of such an L.

We notice that the type of situation dealt with in this article provides us with a sort of noncommutative operation. The order in which things are done is important. If we adjoin $\sqrt{10}$ to Q first and then adjoin $\sqrt{5}$, we obtain $Q(\sqrt{5}\,,\sqrt{10}\,)/Q(\sqrt{10}\,)$ which has no RIB. If we reverse the order in which we make the adjunctions, we obtain $Q(\sqrt{5}\,,\sqrt{10}\,)/Q(\sqrt{5}\,)$ which has a RIB because $h(Q(\sqrt{5}\,)) = 1$ (see, for instance, [**4**], p. 100).

As Fujisaki ([**7**]) generalized the results of MacKenzie and Scheuneman, so also our single example can be replaced without too much additional effort by anything of the form

$Q(\sqrt{cp}, \sqrt{p})/Q(\sqrt{cp})$ where $p \equiv 5 (\text{mod } 8)$ is a prime and where $c \equiv 2 (\text{mod } 8)$, and is a square-free rational integer (see [**8**] and [**9**]).

Finally, for the definitive story on bicyclic biquadratic extensions of Q, we refer the reader to the recent paper of Bird and Parry ([**10**]).

References

[1] R. MacKenzie and J. Scheuneman, A number field without a relative integral basis, Amer. Math. Monthly, 78 (1971) 882–883.

[2] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 4th ed. (1960) reprinted with corrections, 1968, p. 211.

[3] H. Hancock, Foundations of the Theory of Algebraic Numbers, Volume 1, New York, Macmillan, 1931, p. 168.

[4] P. Samuel, Algebraic Theory of Numbers, Hermann, Paris, 1970.

[5] S. Lang, Algebraic Number Theory, Addison-Wesley, Reading, Mass., 1970.

[6] H. B. Mann, On integral bases, Proc. Amer. Math. Soc., 9 (1958) 167–172.

[7] G. Fujisaki, Some examples of number fields without relative integral bases, J. Fac. Sci. Univ. Tokyo, Sect. IA21 (1974) 92–95.

[8] H. M. Edgar, Notices Amer. Math. Soc., 24 (1977) Abstract 77T-A31, A-8.

[9] ———, Notices Amer. Math. Soc., 24 (1977), Abstract 746-A19, A-400.

[10] R. H. Bird and C. J. Parry, Integral bases for bicyclic biquadratic fields over quadratic subfields, Pacific J. Math., 66 (1976), No. 1, 29–36.

Orthonormal Matrices

Murray S. Klamkin
James R. Pounder
University of Alberta
Edmonton, Alberta, Canada T6G 2G1

It follows directly and elegantly from elementary matrix theory (or even geometrically) that if the row vectors of a real square matrix are orthonormal, then so also are the column vectors, and conversely. Here, we give an alternative elementary algebraic proof which, while not as elegant as the usual matrix proof, does provide an answer to a number of student queries over the years for an algebraic proof independent of matrices.

For a 2×2 matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we want to show that

$$\left.\begin{array}{r} a^2+b^2=1, \\ c^2+d^2=1, \\ ac+bd=0, \end{array}\right\} \Leftrightarrow \left\{\begin{array}{l} a^2+c^2=1, \\ b^2+d^2=1, \\ ab+cd=0. \end{array}\right.$$

The implications follow immediately from the identity

$$(a^2+b^2-1)^2+(c^2+d^2-1)^2+2(ac+bd)^2=(a^2+c^2-1)^2+(b^2+d^2-1)^2+2(ab+cd)^2. \quad (1)$$

More generally for the $n \times n$ matrix $A=[a_{rs}]$, we wish to show that

$$u_{rs} \equiv \sum_i a_{ir}a_{is} = \delta_{rs} \Leftrightarrow v_{rs} \equiv \sum_i a_{ri}a_{si} = \delta_{rs} \quad (r,s=1,2,\ldots,n),$$

where as usual $\delta_{rs}=1$ if $r=s$ and $\delta_{rs}=0$ if $r \neq s$.

The identity that we need, corresponding to (1), is that for an arbitrary $n\times n$ matrix $A=[a_{rs}]$ with $AA^T\equiv[u_{rs}], A^TA\equiv[v_{rs}]$,

$$\sum_{r,s}(u_{rs}-x\delta_{rs})^2\equiv\sum_{r,s}(v_{rs}-x\delta_{rs})^2. \qquad (2)$$

That (2) is an identity follows from

$$\sum_{r,s}u_{rs}^2=\sum_{r,s,i,j}a_{ir}a_{is}a_{jr}a_{js}=\sum_{r,s,i,j}a_{ri}a_{si}a_{rj}a_{sj}=\sum_{r,s}v_{rs}^2,$$

$$\sum_{r,s}u_{rs}\delta_{rs}=\sum_{r}u_{rr}=\sum_{i,r}a_{ir}^2=\sum_{r}v_{rr}=\sum_{r,s}v_{rs}\delta_{rs},$$

by interchange of the dummy indices.

Our desired result now follows immediately by letting $x=1$ in (2).

Calculating Surface Areas from a Blueprint

IRA ROSENHOLTZ
University of Wyoming
Laramie, WY 82071

The purpose of this paper is to present some techniques with which one can quickly calculate certain areas and surface areas. Our calculation is based on a formula of Georg Pick [1], and might reasonably be called "Variations on a Theme by Pick." His idea is this: Let P be a simple polygon in the plane, all of whose vertices are lattice points (that is, points having integer coordinates). Then the area A enclosed by P may be determined simply by counting the number I of lattice points interior to P and the number B of lattice points on P. The area is then given by $A=I+\frac{1}{2}B-1$. The problem of finding the area has been reduced to a counting problem! (See FIGURE 1.)

Very often a floor plan could be drawn (or superimposed) on graph paper or a grid so that its vertices are lattice points, and then Pick's Formula provides an efficient way of calculating the area—*if* the figure is a simple polygon. But what if it is not? The formula does not work on the non-simple polygon in FIGURE 2, for example.

Pick's Theorem applies to the simple polygon in FIGURE 1 (here $I=5$, $B=8$, and so $A=5+4-1=8$), but not to the polygon in FIGURE 2 which is not simple. In this case $I=0$, $B=5$, but $A=1\neq 0+5/2-1$.

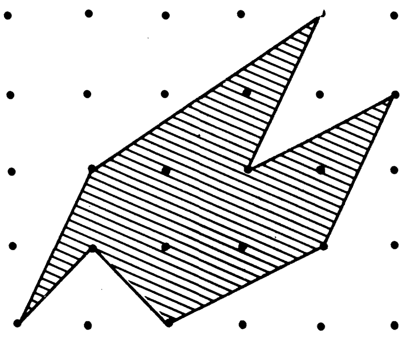


FIGURE 1.

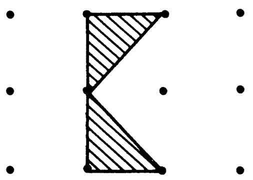
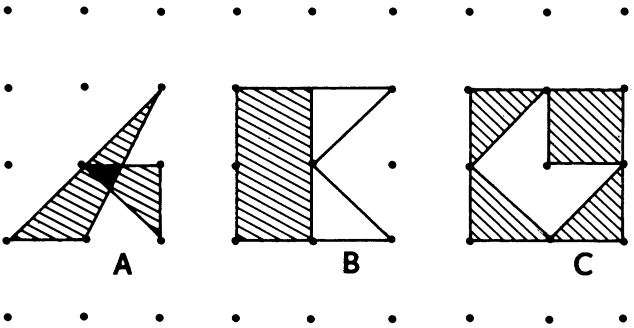


FIGURE 2.

Our immediate task is to generalize Pick's Formula to non-simple polygons. Later we shall indicate an extension to surface areas in 3-space, which will, for example, enable a person to quickly find the surface area of a complex polygonal roof.

Our first order of business is to specify exactly which figures we shall be considering. As before, we insist that our figure P be a polygonal figure in the plane having lattice point vertices, although it need not be a simple polygon plus its interior. Implicit in this is the assumption that if two edges of P intersect, their intersection is a vertex of each, and hence a lattice point. Furthermore, we assume that each point of P belongs to some non-degenerate triangle (plus its interior) which is contained in P (see FIGURE 3). We call this our "standing hypothesis"; it eliminates extraneous vertices and edges from entering our calculations. But they do not contribute anything to the area of P anyhow.



***A* and *B* are not acceptable figures (*A* doesn't have lattice point vertices and *B* has extraneous edges and vertices); *C* is acceptable.**

FIGURE 3.

Then, as we shall show, the area of P is given by the formula

$$A=I+\tfrac{1}{2}B-\chi(P)+\tfrac{1}{2}\chi(\partial P),$$

where I is the number of lattice points interior to P, ∂P represents the boundary of P, B is the number of lattice points on ∂P, and $\chi(F)$ denotes the Euler-characteristic of F, which may be calculated as the number of vertices of F, minus the number of edges of F, plus the number of faces of F. However, in practice it might save some time to use the fact that, for figures that concern us, $\chi(F)$ equals the number of (connected) components of F, minus the number of components of the complement of F in the plane, plus 1. (For example, for the polygon in FIGURE 2, $I=0$, $B=5$, $\chi(P)=1$, and $\chi(\partial P)=-1$; and $A=0+\frac{1}{2}\cdot 5-1+\frac{1}{2}(-1)=1$.) Notice that if P were a simple polygon with interior, then $\chi(P)=1$ and $\chi(\partial P)=0$, so our extension indeed reduces to the usual Pick Formula.

To outline a proof of this formula, we shall first assume (temporarily) that our figure can be triangulated into so-called "primitive triangles." These are the non-degenerate triangles whose vertices are its only lattice points. (We shall return to the question of triangulating the figure into primitive triangles shortly.) Observe that the area of a primitive triangle must be, by Pick's Formula, $A=0+\frac{1}{2}\cdot 3-1=\frac{1}{2}$. We now follow the clever argument given in [2].

Let P be our polygon, and assume that P can be triangulated into primitive triangles. Let D be the "double" of P—that is, D is formed by taking two copies of P and gluing them together along corresponding points of their boundaries. We let the letters V,E,F denote the number of vertices, edges, and faces (primitive triangles) respectively, and we use subscripts to specify which figure we refer to. (Thus V_D is the number of vertices in D, etc.) Then the following formulae are easily verified:

(1) $\chi_D = V_D - E_D + F_D$ (This is the definition.)

(2) $\chi_D = 2\chi_P - \chi_{\partial P}$

(3) $V_D = 2I + B$

(4) $2E_D = 3F_D$ (Our "standing hypothesis" guarantees that each edge of D is the common edge of exactly 2 faces of D.)

(5) $F_D = 2F_P$

(6) $A = \frac{1}{2}F_P$.

Thus,

$$\begin{aligned} F_D &= \chi_D - V_D + E_D && \text{by (1)} \\ &= (2\chi_P - \chi_{\partial P}) - V_D + E_D && \text{by (2)} \\ &= 2\chi_P - \chi_{\partial P} - (2I + B) + E_D && \text{by (3)} \\ &= 2\chi_P - \chi_{\partial P} - 2I - B + \tfrac{3}{2}F_D && \text{by (4).} \end{aligned}$$

Therefore,

$$\tfrac{1}{2}F_D = 2I + B - 2\chi_P + \chi_{\partial P},$$

and so

$$\begin{aligned} A &= \tfrac{1}{2}F_P && \text{by (6)} \\ &= \tfrac{1}{4}F_D && \text{by (5)} \\ &= I + \tfrac{1}{2}B - \chi_P + \tfrac{1}{2}\chi_{\partial P}, \end{aligned}$$

as claimed.

This completes our verification of the generalization of Pick's Formula to non-simple polygons, except for the detail of showing that the figure can be triangulated into primitive triangles. Most proofs of Pick's Formula devote little time to this detail (as well they might) because "everyone believes it" anyhow.

In order to triangulate the figure into primitive triangles, what we shall do is roughly as follows: First we locate a primitive triangle. Next, we remove it—very carefully—so that the remaining figure still satisfies our standing hypothesis. And then we use induction. But on what? The number of lattice points on the interior may have remained the same, and the number on the boundary may have actually increased! The answer is: We induct on the area! Finally, we must check that we really have a triangulation.

Step 1: If the figure is non-empty, there must be an edge (on the boundary) whose endpoints are two lattice points and having no other lattice points between them. Stand in the middle of this edge and look "inside." (Here we are using our "standing" hypothesis about the figure.) We must be able to see another lattice point in our figure, so we can locate a lattice triangle having our edge as one of its edges. Now using the convexity of this triangle, it is easy to locate a primitive triangle.

Step 2: We leave it to the reader to verify that it is possible to remove the primitive triangle from our figure in such a way that the remaining figure also satisfies our standing hypothesis. (There are 8 cases to consider!)

Step 3: Repeat steps 1 and 2 exactly $[2A]$ times, where $[2A]$ is the greatest integer in twice the area of the figure. At this point, there must be nothing left. For if anything were left, it would still satisfy the hypothesis, and would have some area—in fact area at least $\frac{1}{2}$; but this contradicts the fact that an area of $\frac{1}{2}$ was removed exactly $[2A]$ times.

Step 4: The primitive triangles we found really form a triangulation. Intersections like those in FIGURE 4 are impossible because the triangles are primitive. This completes the verification.

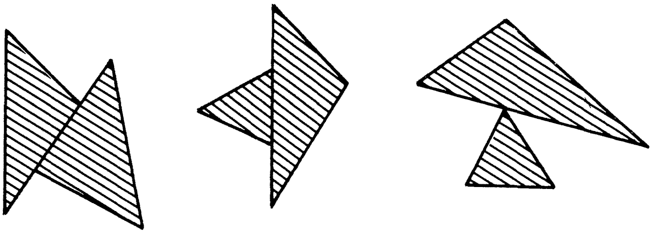


FIGURE 4.

For those who may feel a bit uncomfortable with Euler-characteristics, we now take a page from Reeve's book [3] and use a supplemental lattice to obtain another area formula in which Euler-characteristics do not appear. Again, we assume our standing hypothesis about P.

Let N be a positive integer. We call the set of all points (x,y) in the plane such that both Nx and Ny are integers the $1/N$-lattice. It follows from our generalization of Pick's Formula that the area of P is given by

$$A=\frac{1}{N^2}\left(I_N+\tfrac{1}{2}B_N-\chi(P)+\tfrac{1}{2}\chi(\partial P)\right),$$

where I_N and B_N denote the number of points of the $1/N$-lattice in the interior and boundary of P, respectively. (Note that since the Euler-characteristic is a topological invariant, it is unnecessary to use notation like $\chi(P_N)$, etc.) Of course, if M is another positive integer, then we get the corresponding equation for the area of P in terms of the $1/M$-lattice. Using both equations, we can eliminate $\chi(P)$ and $\chi(\partial P)$. We obtain

$$A=\frac{1}{N^2-M^2}\left\{(I_N-I_M)+\tfrac{1}{2}(B_N-B_M)\right\}.$$

Probably the easiest lattices to use in practice are the 1-lattice (the usual one) and the $1/2$-lattice. In this case, the formula, of course, becomes

$$A=\tfrac{1}{3}\left\{(I_2-I_1)+\tfrac{1}{2}(B_2-B_1)\right\}.$$

We now conclude with a little result which, when used in conjunction with the generalized Pick's Formula, will enable us to calculate the surface areas of lattice polygons in 3-space. The result is undoubtedly known, but an informal survey revealed that it is not "well-known." It resembles a "distance formula for areas." The distance formula in the plane enables one to calculate the length of a line segment in terms of the lengths of its projections onto the coordinate axes. Surprisingly, the corresponding result is true for areas!

Let T be any triangle in 3-space. Let A_{xy} denote the area of its projection onto the xy-plane. Define A_{yz} and A_{xz} similarly. Then the area of T is given by

$$A=\left\{A_{xy}{}^2+A_{yz}{}^2+A_{xz}{}^2\right\}^{\frac{1}{2}}.$$

To see this, it suffices to prove it under the assumption that T has a vertex at the origin. If $\vec{V}_1=(x_1,y_1,z_1)$ and $\vec{V}_2=(x_2,y_2,z_2)$ are the other two vertices, then

$$\begin{aligned}A&=\tfrac{1}{2}|\vec{V}_1\times\vec{V}_2|\\&=\left|\left(\tfrac{1}{2}\det\begin{pmatrix}y_1&z_1\\y_2&z_2\end{pmatrix},-\tfrac{1}{2}\det\begin{pmatrix}x_1&z_1\\x_2&z_2\end{pmatrix},\tfrac{1}{2}\det\begin{pmatrix}x_1&y_1\\x_2&y_2\end{pmatrix}\right)\right|\\&=\left\{A_{xy}^2+A_{yz}^2+A_{xz}^2\right\}^{1/2}.\end{aligned}$$

One word of caution: In using this to determine the surface area of a polygonal figure in 3-space, a person must exercise some care. For example, it would be nice to project the *entire* *figure* onto the coordinate planes, and use the general Pick's Formula with this one to determine its area. Unfortunately, an easy application of the equality part of Schwarz' inequality implies that this will work only if the entire figure lies on a collection of parallel planes (and their projections have disjoint interiors). So when using this formula, it is best to apply it piece-by-piece (or, at least, planar piece-by-planar piece).

(Parenthetically, this idea may be used to motivate the usual calculus formula for surface areas:

$$S=\int\int\sqrt{1+\left(\frac{\partial f}{\partial x}\right)^2+\left(\frac{\partial f}{\partial y}\right)^2}\;dx\,dy.$$

For, translating everything back to the origin for simplicity, the part of the tangent plane above the rectangle $[0,\Delta x]\times[0,\Delta y]$ is the parallelogram spanned by $(\Delta x, 0, \Delta x\partial f/\partial x)$ and $(0,\Delta y,\Delta y\partial f/\partial y)$. Then projecting is easy and we get $A_{xy}=\Delta x\,\Delta y$, $A_{yz}=\Delta x\,\Delta y\partial f/\partial x$, and $A_{xz}=\Delta x\,\Delta y\partial f/\partial y$. Thus

$$A=\Delta x\,\Delta y\sqrt{1+\left(\frac{\partial f}{\partial x}\right)^2+\left(\frac{\partial f}{\partial y}\right)^2}\;.)$$

References

[1] Georg Pick, Geometrisches zur Zahlenlehre, Lotos, Naturwissen Zeitschrift, Prague, 1899.

[2] R. W. Gaskell, M. S. Klamkin, and P. Watson, Triangulations and Pick's Theorem, this MAGAZINE, 49 (1976) 35–37.

[3] J. E. Reeve, On the volume of lattice polyhedra, Proc. London Math. Soc., 7 (1957) 378–395.

The Axioms of Set Theory

RICHARD CLEVELAND
California State University
Sacramento, CA 95819

G. Cantor while working one summer
Invented the transfinite number.
  It was such a find
  It affected his mind
And it often appeared in his slumber.

But Cantor knew well how to hustle,
And with very deep thoughts he could tussle.
  So without any fear he
  Established his theory—
Which was proved inconsistent by Russell.

Then Hilbert declared: "Cantor's system,
And transfinite numbers, I've missed 'em,"
  When along came a fellow
  Whose name is Zermelo
To give us some axioms—We'll list 'em:

1. *Extensionality*
We assume that our sets are extensional,
As opposed to their being intensional.
  So the name of the game
  Is that sets are the same
If they have the same members—that's
    sensible!

2. *Subsets*
By this postulate anyone may
Make a definite subset of A.
  Thus, the set of all x
  Of the opposite sex
Could be easily handled this way.

3. *Null Set*
We can't be assured of a full set,
Or even a reasonably dull set.
  It wouldn't be clear
  That there's any set here,
Unless we assume there's a null set.

4. *Pairing*
Only Euclid has seen Beauty bare,
But Zermelo was not unaware
  That his postulates need
  This additional seed
So that any two sets make a pair.

5. *Unions*
A mathematician named Taber
Was explaining this one to his neighbor:
  About how it lets
  One make unions of sets,
But does nothing for Organized Labor.

6. *Powers*
A mathematician named Bowers
Sat counting his subsets for hours.
  After two to the ten
  He started again,
Upon using the Axiom of Powers.

7. *Infinity*
We are told that the Axiom of Infinity
Is a lot like assuming a divinity:
  It allows us to bet
  That an infinite set
Can be found in most any vicinity.

8. *Regularity*
The postulate called Regularity
Adds naught to our theory but clarity.
  But there's no doubt about it
  If we were without it
We'd have sets of unusual parity.

9. *Choice*†
Zermelo had one more in store,
And this one we mustn't ignore:
  By which anyone may
  Take a messy array
And make it well-ordered once more.

Anyone who wants to give thanks'll
Have to wait until hearing from Fraenkel,
  Who added one more
  Just to even the score
And it helps out a lot, so be thankful!

10. *Replacement*
No matter how rapid his pace went,
The agonized look on his face meant
  He'd lost his composure
  Over a transitive closure
Without an appeal to Replacement.

Let's shout it, let's holler, let's bellow
Our praise for a jolly good fellow:
  For Fraenkel, of course,
  Gödel, Bernays, and Morse,
And last but not least for Zermelo!

Footnote

†The Axiom of Choice yields other possibilities:

There once was a maiden named Emma,
Who had a peculiar dilemma:
  She had so many beaus,
  That to choose, heaven knows,
She had to appeal to Zorn's Lemma.

PROBLEMS

DAN EUSTICE, Editor
LEROY F. MEYERS, Associate Editor
The Ohio State University

Proposals

To be considered for publication, solutions should be mailed before April 1, 1980.

1074. Suppose that all three roots of the cubic $x^3-px+q=0$ $(p>0, q>0)$ are real. Show that the numerically smallest root lies between q/p and $2q/p$. [*Chandrakant Raju, Indian Statistical Institute, New Delhi, India & R. Shantaram, University of Michigan-Flint.*]

1075. Counting from the right end, what is the 2500th digit of 10,000!? [*Philip M. Dunson, Battelle-Columbus Laboratories.*]

1076. Let $\mathcal{B}$ be an n-gon inscribed in a regular n-gon $\mathcal{C}$. Show that the vertices of $\mathcal{B}$ divide each side of $\mathcal{C}$ in the same ratio and sense if and only if $\mathcal{B}$ is regular. [*M. S. Klamkin, University of Alberta.*]

1077. Show that the number of integral-sided right triangles whose ratio of area to semi-perimeter is p^m, where p is a prime and m is a positive integer, is $m+1$ if $p=2$ and $2m+1$ if $p \neq 2$. [*Henry Klostergaard, California State University, Northridge.*]

1078. Describe as fully as possible the solutions of $xe^y+ye^x=0$. [*R. P. Boas, Northwestern University.*]

1079. Define $a_0=1$ and $a_{n+1}=(a_n-2)/a_n$ for $n \geqslant 0$.
(a) Show that the set $\{a_n\colon n=0,1,2,\ldots\}$ is unbounded.
(b) There exists a real number α such that $\{n\colon a_n \geqslant 1\}=\{[k\alpha]\colon k=0,1,2,\ldots\}$. Find α.
(c)* Find the closure of the set defined in part (a).
[*James Propp, student, Harvard University.*]

ASSISTANT EDITORS: DON BONAR, *Denison University;* WILLIAM A. MCWORTER, JR., *The Ohio State University. We invite readers to submit problems believed to be new. Proposals should be accompanied by solutions, when available, and by any information that will assist the editors. Solutions to published problems should be submitted on separate, signed sheets. An asterisk (*) will be placed by a problem to indicate that the proposer did not supply a solution. A problem submitted as a Quickie should be one that has an unexpected succinct solution. Readers desiring acknowledgement of their communications should include a self-addressed stamped card. Send all communications to this department to Dan Eustice, The Ohio State University, 231 W. 18th Ave., Columbus, Ohio 43210.*

Quickies

Solutions to Quickies appear at the conclusion of the Problems section.

Q662. Determine the maximum of

$$R=\frac{|z_1z_2+z_2z_3+z_3z_4+z_4z_5+z_5z_1|^3}{|z_1z_2z_3+z_2z_3z_4+z_3z_4z_5+z_4z_5z_1+z_5z_1z_2|^2}$$

where z_1, z_2, z_3, z_4, and z_5 are complex numbers of unit length. [*M. S. Klamkin, University of Alberta.*]

Solutions

Really Orthogonal **March 1978**

1035. A is a real $n\times n$ matrix. Do there exist orthogonal matrices B such that $A+B$ is real orthogonal? [*H. Kestelman, University College, London.*]

Solution I: Since there are $n+\binom{n}{2}=(n^2+n)/2$ conditions for an $n\times n$ matrix to be orthogonal, we have n^2+n conditions on B which has n^2 elements. Consequently, we do not expect to find solutions. In particular, let

$$A=\begin{pmatrix}2&1\\1&2\end{pmatrix},\qquad B=\begin{pmatrix}\cos\theta&\sin\theta\\-\sin\theta&\cos\theta\end{pmatrix}.$$

Then it would be necessary that $(2+\cos\theta,1+\sin\theta)$ and $(1-\sin\theta,2+\cos\theta)$ are orthogonal vectors or that $\cos\theta=-2$.

M. S. Klamkin
University of Alberta

Solution II: Suppose that A is also a real orthogonal matrix. [This was proposer's original formulation—Editor.] Then the problem is the same as that of finding an orthogonal matrix V such that $A+AV$ is orthogonal, i.e., $A(I+V)(I+V^T)A^T=I$, which is the same as $V^2+V+I=0$. No matrix with a real eigenvalue satisfies this: hence no solutions if n is odd. If n is even

$$M=\begin{pmatrix}\cos(2\pi/3)&-\sin(2\pi/3)\\ \sin(2\pi/3)&\cos(2\pi/3)\end{pmatrix}$$

satisfies this quadratic, and the complete solution is $V=W\operatorname{diag}(M,M,\dots,M)W^T$ where W is orthogonal and M occurs $\frac{1}{2}n$ times.

H. Kestelman
University College, London

Also solved by Daniel S. Freed and Peter W. Lindstrom.

Real Not Complex — March 1978

1036. If $a_1, a_2, \ldots, a_N$ are complex numbers such that $|a_N| > \Sigma_{k=0}^{N-1}|a_k|$, show that $\Sigma_{n=0}^{N} a_n \cos n\theta = 0$ has at least $2N$ solutions for $0 \leqslant \theta < 2\pi$. [*Joseph Silverman, Cambridge, Massachusetts.*]

Solution: The assertion is not correct as stated. Let $N=1$, $a_0 = i$, $a_1 = 2$. Then the hypothesis $|a_0| < |a_1|$ is satisfied, yet $2\cos\theta + i = 0$ has no real solutions.

The assertion of the problem is correct if the a_k are all required to be real. The function $F(\theta) = a_N \cos N\theta$ attains its extremes $\pm |a_N|$ at the $2N+1$ points $\theta_k = k\pi/N$, $k = 0, 1, \ldots, 2N$ in the interval $[0, 2\pi]$, whereas $f(\theta) = \Sigma_{n=0}^{N-1} a_n \cos n\theta$ satisfies $|f(\theta)| \leqslant \Sigma_{n=0}^{N-1}|a_n| < |a_N|$. Thus $F(\theta) + f(\theta)$ is alternately positive and negative at the points θ_k. By the intermediate value theorem $F(\theta) + f(\theta) = 0$ for at least one θ in each of the $2N$ intervals (θ_k, θ_{k+1}), $k = 0, 1, \ldots, 2N-1$.

Moreover, if $z = e^{i\theta}$, $F(\theta) + f(\theta) = 0$ if and only if $P(z) = \Sigma_{k=0}^{N} a_k (z^{N+k} + z^{N-k}) = 0$. Since $P(z)$ is a polynomial of degree $2N$, $P(z)$ has at most $2N$ distinct zeros. Thus, we conclude that $F(\theta) + f(\theta)$ has exactly $2N$ distinct zeros.

MICHAEL J. DIXON
California State University— Chico

Also solved (with real coefficients) by Richard Beigel, Robert L. Curry & John H. Mathews, Eli L. Isaacson, M. S. Klamkin (Canada), and the proposer.

Tangentially Equivalent — May 1978

1039. Sum the series $\sum\limits_{k=1}^{\infty} \dfrac{1}{k^2} \tan\dfrac{k\pi}{m} \tan\dfrac{k\pi}{n}$. [*M. B. Gregory & J. M. Metzger, University of North Dakota.*]

Solution I: If either m or n is even, the expression is not defined. Let, then, m and n be odd integers.

We will use contour integration to sum the series. Let

$$f(z) = \frac{\pi \tan\dfrac{\pi z}{m} \tan\dfrac{\pi z}{n} \cot \pi z}{z^2}.$$

The following facts are verified in the usual way:

1. f has a simple pole with residue $\tan(\dfrac{\pi k}{m} \tan\dfrac{\pi k}{n})/k^2$ at the nonzero integer k, or has a removable singularity at k if this value is 0.
2. f has a simple pole at 0 with residue π^2/mn.
3. f has a pole or a removable singularity at each member of the following two sets: $S = \{m(2s-1)/2\colon s \in Z\}$ and $T = \{n(2t-1)/2\colon t \in Z\}$.
4. If $w \in (S \backslash T) \cup (T \backslash S)$, then f has a removable singularity.
5. If $w \in S \cap T$, then $w = jq/2$ for some odd integer j, where q is the least common multiple of m and n. Then f has a simple pole with residue $-4mn/j^2q^2$ at w.

Now let C_n be the square with vertices $(\pm(n+\frac{1}{3}), \pm(n+\frac{1}{3}))$ and let I_n be its interior. On C_n, $|f(z)| \leqslant M|z|^{-2}$ for some M. By the residue theorem,

$$\oint_{C_n} f(z)\,dz = 2\pi i \left[\operatorname{Res}(f,0) + \sum_{k \in I_n \cap Z \backslash \{0\}} \operatorname{Res}(f,k) + \sum_{w \in S \cap T \cap I_n} \operatorname{Res}(f,w) \right].$$

Letting $n \to \infty$, we have

$$0 = \frac{\pi^2}{mn} + \sum_{2k=1}^{\infty} \frac{\tan\frac{\pi k}{m}\tan\frac{\pi k}{n}}{k^2} - 2\sum_{\substack{j=1\\ j \text{ odd}}}^{\infty} \frac{4mn}{j^2q^2}.$$

Thus,

$$\sum_{k=1}^{\infty} \frac{\tan\frac{\pi k}{m}\tan\frac{\pi k}{n}}{k^2} = \frac{\pi^2 mn}{2q^2} - \frac{\pi^2}{2mn} = \frac{\pi^2}{2}\left(\frac{mn}{q^2} - \frac{1}{mn}\right),$$

where q is the least common multiple of m and n.

PAUL ZWIER
Calvin College

Solution II: Since n is odd, the Fourier series of $U_n(t) = (-1)^{[nt]}$ on $[0,1]$ is

$$U_n(t) \sim \frac{1}{n} + \sum_{k=1}^{\infty} \frac{\sqrt{2}}{\pi k}\tan\frac{\pi k}{n}(\sqrt{2}\cos 2k\pi t).$$

Therefore, by Parseval's identity, we obtain

$$\int_0^1 U_n(t)\,U_m(t)\,dt = \frac{1}{mn} + \frac{2}{\pi^2}\sum_{k=1}^{\infty}\frac{1}{k^2}\tan\frac{\pi k}{m}\tan\frac{\pi k}{n}.$$

In Proposal #994 (this *Magazine*, vol. 51(1978) p. 130) it is established that $\int_0^1 U_n(t)U_m(t)\,dt = (m,n)^2/mn$, where m and n are odd and (m,n) is the greatest common divisor of m and n. Thus the desired sum is $\pi^2((m,n)^2 - 1)/2mn$.

M. B. GREGORY AND J. M. METZGER
University of North Dakota

Peter W. Lindstrom and J. M. Stark showed how to express the infinite sum as a finite sum where the number of terms depends upon the least common multiple of m and n.

Generalized Inverses — May 1978

1040. If A is an $m \times n$ matrix which is not invertible, show that there are infinitely many $n \times m$ matrices X satisfying $AXA = A$. [*H. Kestelman, University College, London.*]

Solution I: In the language of linear transformations, this problem can be stated as follows: Let V and W be non-zero vector spaces over an infinite field (the proposer forgot to mention this obvious requirement) and A be a non-invertible linear transformation from V into W. Show that there exist infinitely many linear transformations X from W into V such that $AXA = A$.

Of course we can assume $A \neq 0$. Otherwise any linear transformation from W into V will do.

The proof of this result follows from the facts: (1) If V is a vector space over an infinite field F and N is a proper subspace of V, i.e., $N \neq \{0\}$ and $N \neq V$, then N has infinitely many complementary subspaces in V. (2) If A is an injective linear transformation from vector space V into vector space W, and S is a complementary subspace of $A(V)$ in W, then there exists a linear transformation X from W into V such that $X(W) = V$, $AXA = A$, and the null space of X is S. To prove (1), let M be a complementary subspace of N in V with a basis $\mathfrak{B}$. Let $\beta \in \mathfrak{B}$ and $\alpha \neq 0$ in N. For each $c \in F$, the subspace M_c spanned by $\{c\alpha + \beta\} \cup \{\mathfrak{B} - \{\beta\}\}$ is a complementary subspace of N in V, and $M_c = M_{c'}$ if and only if $c = c'$. To prove (2), $W = A(V) \oplus S$. For each $x \in W$, $x = Av + s$ uniquely. The mapping X from W into V defined by $X(x) = v$ has the required properties.

For the proof of the pudding, let N be the null space of A. Since A is non-invertible, either $N \neq \{0\}$ or $N=\{0\}$ but $AV \neq W$. Suppose $N \neq \{0\}$. Then by (1), N has infinitely many complementary subspaces in V. For each complementary subspace M of N in V, A is injective on M. By (2), there exists a linear transformation X from W into $M \subset V$ such that $X(W)=M$ and $AXA=A$ on M. But if $\alpha \in V$, then $\alpha = n+m$, where $n \in N$, $m \in M$, and $AXA(\alpha)=AXA(m)$ $=Am=A\alpha$. Hence $AXA=A$ in V. Suppose $N=\{0\}$ and $AV \neq W$. By (1), AV has infinitely many complementary subspaces in W. Since A is injective on V, then by (2) for each complementary subspace S of AV there exists a linear transformation X from W to V such that $AXA=A$ and X has null space S.

Edward T. Wong
Oberlin College

Solution II: Let B be equivalent to A and suppose that $BXB=B$. Then $B=PAQ$ for some non-singular $m \times m$ matrix P and $n \times n$ matrix Q. Thus $PAQXPAQ=PAQ$ and since P and Q are non-singular $A(QXP)A=A$. Furthermore, $QXP=QYP$ if and only if $X=Y$. Therefore it suffices to take

$$A=\begin{pmatrix} I_{kk} & 0_{ks} \\ 0_{rk} & O_{rs} \end{pmatrix}. \quad \text{Let} \quad X=\begin{pmatrix} I_{kk} & B_{kr} \\ C_{sk} & D_{sr} \end{pmatrix}$$

where B, C and D are arbitrary matrices of the indicated size. A routine block multiplication shows that $AXA=A$. Also $k<\max(m,n)$ since A is singular. Thus at least one of B, C or D exists, which clearly gives infinitely many solutions provided the ground field is infinite.

P. K. Garlick
University of Michigan—Flint

Also solved by Wm. D. Bell (Canada), Ulrich Faigle (Germany), Eli L. Isaacson, Joel Levy, Peter W. Lindstrom, Lance Littlejohn, Scott Smith, and the proposer. Bell, Faigle and Levy pointed out that X is called a generalized inverse. References were provided to: C. R. Rao, Linear Statistical Inference and its Applications, 2nd ed., Wiley, 1973, pp. 24–27, and S. R. Searle, Linear Models, Wiley, 1971, chapter 1.

Divisible Differences **May 1978**

1041. For $0<m<n$, find $N(m,n)$, the minimum positive integer such that any subset of $\{1,2,\ldots,n\}$ of $N(m,n)$ elements contains numbers differing by m. [*Richard A. Gibbs, Fort Lewis College.*]

Solution: Arrange the integers $1,2,\ldots,n$ into m rows so that the ith row consists of the integers congruent to $i \pmod m$. The numbers in each row are in their natural order. Let V be the set of numbers in the odd-numbered columns. Each column has m elements save possibly the last which has t elements where $n=qm+t$, $0<t\leqslant m$. Counting V gives

$$\text{Card } V=\begin{cases} km+r, & \text{if } n=2km+r, \quad 0\leqslant r<m \\ (k+1)m, & \text{if } n=(2k+1)m+r, \quad 0\leqslant r<m. \end{cases}$$

We claim $N(n,m)=\text{Card } V+1$. Clearly no two elements of V differ by m. Let S be any subset of $1,2,\ldots,n$ maximal with respect to the property that no two elements of S differ by m. We have Card $S \geqslant$ Card V. We will establish our claim by showing Card $S \leqslant$ Card V. The set S can contain at most m numbers from any two adjacent columns, since otherwise two numbers would be from the same row. Thus Card $S \leqslant$ Card V.

S. F. Barger
Youngstown State University

Also solved by Richard Beigel, J. Binz (Switzerland), Stan Cohen & Joseph O'Rourke, Thomas Elsner, Nick Franceschine III, William E. Gould, Eli L. Isaacson, Peter W. Lindstrom, William M. McGovern, David L. Motte, Howard Pullman, Scott Smith, Vincent G. Sprague, J. M. Stark, and the proposer.

Sum of Two Squares — May 1978

1042. Prove that any integer which is the sum of the squares of two different, non-zero integers is divisible by a prime which is the sum of the squares of two different, non-zero integers. [*Henry Klostergaard, California State University, Northridge.*]

Solution: The proof depends on two well-known results given in many texts on elementary number theory:

(i) If $n=a^2+b^2$, where a and b are relatively prime integers with $ab>1$, then either n is a prime of the form $4k+1$, the product of such primes, or twice such a product. Thus, n has no factor of the form $4k+3$.

(ii) Every prime of the form $4k+1$ is the sum of the squares of two different integers.

We need only note further that if $(a,b)=d>1$, then $n=a^2+b^2$ gives $n'=(n/d)^2=(a/d)^2+(b/d)^2$ where a/d and b/d are relatively prime integers. By (i) and (ii), n' has at least one factor which is the sum of two different squares, and this factor is clearly a factor of n as required.

E. P. Starke
Plainfield, New Jersey

Also solved by Richard Beigel, Ulrich Faigle (Germany), P. K. Garlick, Dale T. Hoffman, M. S. Klamkin (Canada), Hugh Noland, Peter W. Lindstrom, Victor Pambuccian (Romania), Leonard Palmer, John Petro, Bob Prielipp, Sahib Singh, Scott Smith, J. M. Stark, Ernst Trost (Switzerland), Aleksandras Zujus, and the proposer. Some of the references supplied by the solvers were: *Burton, Elementary Number Theory, pp.* 264–265; *Griffin, Elementary Theory of Numbers, pp.* 159–164; *Niven & Zuckerman, An Introduction to the Theory of Numbers, pp.* 106–110; *Sierpinski, Elementary Theory of Numbers, p.* 362.

A Congruence — May 1978

1044. Let p be a prime and k a positive integer. The congruence relation $(x-a)(x-b)\equiv 0 \pmod{p^k}$ has the obvious solutions $x\equiv a \pmod{p^k}$ and $x\equiv b \pmod{p^k}$. When are these the only solutions? [*J. Metzger, University of North Dakota.*]

Solution: For $k=1$, the answer is "always" since the integers $(\bmod\, p)$ form a field. For $k\geqslant 2$, these are the only solutions iff $a\not\equiv b \pmod p$.

Proof. Suppose $a\equiv b$. Then $a=b+mp$ and direct computation shows that $a+np^{k-1}$ is a solution of the given congruence for $0\leqslant n<p$.

Conversely, if x satisfies the congruence, $x\not\equiv a,b \pmod{p^k}$, then neither $x-a$ nor $x-b$ is divisible by p^k, but their product is. Hence each must be divisible by p, so $a-b=(x-b)-(x-a)\equiv 0 \pmod p$.

Faith Morrison, student
Liberty High School
Bethlehem, Pennsylvania

Also solved by Anders Bager (Denmark), Richard Beigel, Michael W. Ecker, Thomas E. Elsner, Nick Franceschine III, Dale T. Hoffman, Eli L. Isaacson, Peter W. Lindstrom, Victor Pambuccian (Romania), John Petro, Reinhard Razen (Austria), Sahib Singh, Lawrence Somer, Vincent G. Sprague, Alan H. Stein, Ernst Trost (Switzerland), Aleksandras Zujus, and the proposer.

Absolute Perfect Squares — May 1978

1045. N is a perfect square if there exists a K such that $N=K^2$. Following T. N. Bhargava and P. H. Doyle, *On the Existence of Absolute Primes*, (47) 233–234, this Magazine, define

N to be an *absolute perfect square*, relative to a given base, if every permutation of the digits of N is a perfect square in that base. In base ten, 1, 4, and 9 are obviously absolute perfect squares. Show that these are the only ones. [*J. L. Murphy, California State College at San Bernardino.*]

Solution: A rapid check shows that no 2-digit square is absolute. A square n with three or more digits ends in 00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61, 64, 69, 76, 81, 84, 89 or 96. We now stipulate that n be an absolute square. The sequence above now shrinks to 00, 16, 44, 61, 69, 96, since the other endings do not tolerate permutation of digits. Putting some other digit of n at the last place or at the last place but one we shall get again one of the six permissible endings. The only case surviving this test is $n=444\ldots44$ (at least three digits). Since $\frac{1}{4}n=111\ldots11$ is not a square, ending as it does in 11, neither is n. Thus the only absolute squares (in base 10) are the single digit ones: (0), 1, 4, 9. Absolute squares with two or more digits exist in other bases. In base 7 we get $22=4^2$. In base 3 we get $11=2^2$ and $11111=102^2$. In base 7 again: $1111=26^2$. Clearly 11 is an absolute square in every base $b=n^2-1$. 10 is an absolute square iff the base is a square.

Anders Bager
Hjørring, Denmark

Also solved by Richard Beigel, Eli L. Isaacson, Allan Wm. Johnson Jr., Peter W. Lindstrom, Graham Lord (Canada), William McGovern, Victor Pambuccian (Romania), Bob Prielipp, Howard Pullman, Lawrence Somer, E. P. Starke, Aleksandras Zujus, and the proposer.

Decimal Divisibility — May 1978

1046. For an arbitrary positive integer k, consider the decimal integer h consisting of m copies of k followed by n zeros. Show that for each positive integer x, there exist an m, $m\neq 0$, and an n such that x divides h. [*Daniel J. Aulicino, Fiorello H. LaGuardia Community College.*]

Solution I: Consider the x numbers consisting of r copies of k $(1\leqslant r\leqslant x)$. If one of them is divisible by x, then the problem is solved; in the other case, by the pigeonhole principle, two of these numbers are in the same residue class modulo x, hence their difference (which is of the required form) is divisible by x.

Reinhard Razen
Loeben, Austria

Solution II: The following gives an explicit construction for n and m.

Denote the number consisting of m copies of k by k_m. Then it is necessary to find integers n and m for which x divides $10^n k_m$.

Write $x=2^r5^sy$ where $\gcd(y,10)=1$. Taking $n=\max(r,s)$, it suffices to find m for which y divides k_m.

If k contains p digits, then $k_m=k(1+10^p+10^{2p}+\cdots+10^{(m-1)p})=k(10^{mp}-1)/(10^p-1)$. It suffices to determine m so that $(10^p-1)y$ divides $10^{mp}-1=(10^p)^m-1$. Since $\gcd((10^p-1)y,10^p)=1$, Euler's theorem shows that $(10^p)^m-1\equiv 0 \pmod{(10^p-1)y}$ for $m=\phi((10^p-1)y)$, where ϕ is the Euler ϕ-function.

Eli L. Isaacson
New York University

Also solved by Richard Beigel, Michael Ecker, Nick Franceschine III, P. K. Garlick, George C. Harrison, Allan Wm. Johnson Jr., Peter W. Lindstrom, William McGovern, William Myers, Victor Pambuccian (Romania), Bob Prielipp, Lawrence Somer, Vincent G. Sprague, J. M. Stark and the proposer.

1047. Given an infinite sequence $A=\{a_n\}$ of positive integers, we define a family of sequences A_i, where $A_0=A$ and $A_i=\{b_r\}$ for $i=1,2,3,\ldots$, where b_r is the number of times that the rth lowest term of A_{i-1} occurs in A_{i-1}. For example, if $A=A_0=\{1,2,2,3,3,3,4,4,4,4,\ldots\}$, then $A_1=\{1,2,3,4,\ldots\}$ and $A_2=\{1,1,1,1,\ldots\}$.

(a) Find a non-decreasing sequence A such that the sequences A_i are all distinct.

(b)* Let $T=\{t_n\}$ be the unique non-decreasing sequence containing all the positive integers which has the property that $T_1=T_0$. Define $U=\{u_n\}$ and $V=\{v_n\}$ so that for all n, $u_n=t_{2n-1}$ and $v_n=t_{2n}$. Are the sequences U_i and V_i all distinct? [*James Propp, Great Neck, New York.*]

Solution: (a) It is easily seen that a non-decreasing sequence A for which consecutive elements differ by at most one is uniquely determined by its first element and by A_1. In fact, if a is the first element of A and $A_1=\{b_r\}$, then the first b_1 elements of A are a, the next b_2 elements are $a+1$, the next b_3 elements are $a+2$, and so on.

Therefore, defining the first element of A_i to be $i+1$ for $i\geqslant 0$ produces the following sequences:

$$A=A_0=\{1,1,2,2,3,3,4,4,4,5,5,5,6,6,6,7,7,7,7,8,8,8,8,\ldots\}$$
$$A_1=\{2,2,2,3,3,3,4,4,4,5,5,5,6,6,6,6,7,7,7,7,\ldots\}$$
$$A_2=\{3,3,3,3,4,4,4,4,5,5,5,5,6,6,6,6,7,7,7,7,\ldots\}$$
$$A_3=\{4,4,4,4,4,5,5,5,5,5,\ldots\}$$
$$A_4=\{5,5,5,5,5,5,\ldots\}$$
$$A_5=\{6,\ldots\}$$
$$A_6=\{7,\ldots\}$$
$$\vdots$$

Clearly, all these sequences are distinct.

ELI L. ISAACSON
New York University

Part (a) also solved by Jeffrey Shallit and the proposer.

Answers

Solutions to the Quickies which appear near the beginning of the Problems section.

Q662. Divide the denominator by $|z_1z_2z_3z_4z_5|$ and use $1/z=\bar{z}$ to obtain (with $z_6=z_1$) $R=|\Sigma z_iz_{i+1}|\leqslant\Sigma|z_iz_{i+1}|=5$. The idea of this problem is based on Problem E3528 of A. A. Bennett in the *American Mathematical Monthly,* 39 (1932) page 115.

REVIEWS

Paul J. Campbell, Editor
Beloit College

Pierre Malraison, Editor
Control Data Corp.

Assistant Editor: Eric S. Rosenthal, Princeton University. Articles and books are selected for this section to call attention to interesting mathematical exposition that occurs outside the mainstream of the mathematics literature. Some reviews of books are adapted from the Telegraphic Reviews in the American Mathematical Monthly.

Kolata, Gina Bari, *Isadore Singer and differential geometry,* Science 204 (1 June 1979) 933-934.

An interview with Singer, introducing both the man and his subject. Singer's exposition and research are influencing the rebirth of a physics-mathematics dialogue which is gaining much scientific recognition. This brief article offers a quick non-technical sketch of what's going on and why it's important.

Neuwirth, Lee, *The theory of knots,* Scientific American 240:6 (June 1979) 110-124, 202.

This is *Scientific American* at what it does best: top-flight graphics accompany excellent exposition to articulate the concepts of the homotopy group and the genus associated with a knot, together with the recent discovery of a relation between them.

Hellman, Martin E., *The mathematics of public-key cryptography,* Scientific American 241:2 (August 1979) 146-157, 198.

Description of two public-key encryption systems based on the well-known NP-complete problems: the knapsack problem (given a set of numbers and a sum to determine which of the numbers add up to the sum) and the factorization problem (given an integer, to find all its factors). Both methods rely on modular arithmetic to turn "smooth" functions into discontinuous ones, "introducing...confusion into the calculation of their inverses." Still, cryptography cannot yet guarantee the security of such systems.

Hersh, Reuben, *Some proposals for reviving the philosophy of mathematics,* Advances in Mathematics 31 (1979) 31-50.

Platonism, logicism, formalism, intuitionism--all sought an absolutely reliable foundation for mathematics, a guarantee of absolute certainty in mathematical truth. But the daily experience of mathematicians shows that mathematical truth is "fallible and corrigible." The author proposes that mathematical philosophy abandon a vain search for foundations and strive to account for mathematics as we experience it: the purposeful creation of mathematical objects which, once created, have well-determined properties independent of our knowledge of them. After all, why should mathematical truth be certain? or why should we expect it to be?

De Millo, Richard A., et al., *Social processes and proofs of theorems and programs*, Comm. ACM 22:5 (May 1979) 271-280.

If one were to make an analogy between mathematics and computer science, what would correspond to a theorem, or to its proof: the program? the algorithm? a formal verification of the program? The authors reject, on practical and philosophical grounds, the trend toward program verification; they abandon the search for absolute computational truth in favor of the goal of reliable software.

Anderson, Robert B., Proving Programs Correct, Wiley, 1979; viii + 184 pp, $8.95 (P).

"We believe that the proof that a program is correct should be a standard part of the programming process. Every program should be accompanied by a proof that it is correct." The author concentrates on the method of inductive assertions and the technique of structural induction; the book is suitable not only as a supplement for a second course in programming, but also for the general mathematical reader.

Robinson, Arthur L., *Tournament competition fuels computer chess*, Science 204 (29 June 1979) 1396-1398; erratum (20 July 1979) 262.

In the past 10 years computer chess has grown up: several current computer programs have ratings around 2000 on the U.S. Chess Federation scale, near the expert level. Controversy still persists as to which is the better strategy: to incorporate chess knowledge into the program, or to concentrate on fast full-width search of the game tree. The controversy has been fruitful for both chess and computer science: may it continue!

Okes, K.H., *Modelling the heating of a baby's milk bottle*, International J. Math. Educ. in Science and Technology 10:1 (1979) 125-136.

Splendid example of modelling: four models of increasing complexity, each compared against experimental results. Only elementary calculus is needed, plus an understanding of terminology and principles of heat transfer.

Steen, Lynn Arthur, *Unsolved problems in geometry*, Science News 115 (23 June 1979) 412-413.

A popular survey of a number of simple (to state) problems in a familiar geometric framework. Some are unsolved, others have yielded solutions (occasionally very simple) only after considerable time and work. Many of the problems were discussed in the May 1979 *Mathematics Magazine*; others will appear in November 1979.

Norton, Bernard J., *Karl Pearson and statistics: the social origins of scientific innovation*, Social Studies of Science 8 (1978) 3-34.

Pearson's interest in statistics was integrally linked with his devotion to eugenics. The paper explores his social views and philosophical thought and how they primed him to turn from mathematics to biometry and statistics when the occasion arose in the form of a new colleague in biology asking him for help.

Elliott, David, *Lagrange interpolation--decline and fall?* International J. Math. Educ. in Science and Technology 10:1 (1979) 1-12.

Brief and readable history, focusing on questions of uniform convergence and comparing Lagrange interpolation to cubic splines. Recent developments concern mean convergence.

Simon, Herbert A., *The uses of mathematics in the social sciences*, Mathematics and Computers in Simulation 20 (1978) 159-166.

A brief general survey, which indicates "how the status of fundamental measurement [e.g., cardinal vs. ordinal scale] in different social science fields determines the usefulness of different kinds of mathematics."

Diffie, Whitfield and Hellman, Martin E., *Privacy and authentication: an introduction to cryptography*, Proceedings IEEE 67 (March 1979) 397-427.

A "tutorial introduction" to contemporary cryptography and cryptanalysis, giving an overview of the state of the art and a guide to the literature.

Bruter, C.P., *The theory of catastrophes: some epistemological aspects*, Synthese 39 (1978) 293-315.

"Is the theory of catastrophes no more than a toy in the hands of gods, or does it rather appear as the expression of a divine form which allows us to play with it? Like the toys given to children to help them better know the world..."

Kolata, Gina Bari, *Institute idea divides mathematicians*, Science 205 (3 August 1979) 470-472.

Details conflict over whether 10% of NSF funds for mathematics should be devoted to a new research institute on a five-year trial basis.

Scarpelli, Anthony F., *1/f random tones: making music with fractals*, Personal Computing 3:7 (July 1979) 17-20.

Roughly speaking, a fractal is a pattern that no matter how clearly you look at it, or how much you magnify it, what you perceive still has the same pattern. In a somewhat confusing explanation the author investigates the novel idea of what a fractal would be in the realm of music.

Seebach, J. Arthur and Steen, Lynn Arthur (Eds.), Mathematics Magazine 50-Year Index, MAA, 1979; xxvi + 165 pp, $8 (P).

In addition to a key-word title index and an author index, the volume includes a delightful history of *Mathematics Magazine* by E.F. Beckenbach. Please note: this index volume will *not* be sent to subscribers automatically; like the recent *Eighty-Year Index* to the *Monthly* this index must be ordered separately. Remind your librarian!

Slowinski, David, *Searching for the 27th Mersenne prime*, J. Recreational Math. 11:4 (1978-79) 258-261.

Last October two high-school students, Curt Noll and Laura Nickel, discovered the 25th Mersenne prime. (Numbers of the form $2^p - 1$ are called Mersenne numbers and denoted M_p.) The discovery was national news--Walter Cronkite even read the story over CBS-TV. In February Noll and author Slowinski (independently) found that M_{23209} is the 26th Mersenne prime. In April Slowinski found the 27th, M_{44497}, using a Cray Computer. Walter, how'd you miss these?

Austing, Richard H., et al. (Eds.), *Curriculum '78: recommendations for the undergraduate program in computer science: a report of the ACM Curriculum Committee on Computer Science*, Communications ACM 22 (March 1979) 147-166.

The recommendations not only spell out a core curriculum and electives, but also specify requirements in mathematics.

Schaefer, Barbara Hirsch, Using the Mathematical Literature: A Practical Guide, Marcel Dekker, 1979; ix + 141 pp, $19.75.

Overview from a librarian's perspective of how the mathematical literature is organized and what the main source materials are. This volume complements *Use of Mathematical Literature* edited by A.R. Dorling (Butterworths, 1977) and *How to Find Out in Mathematics* (Second Revised Edition) by John E. Pemberton (Pergamon, 1969). All three should be displayed prominently in the mathematics section of every college library.

Deeter, C.R. and Hoffman, A.A.J., *Energy related mathematical models: annotated bibliography*, Energy Conversion 18 (1978) 189-227.

"A very small percentage of the descriptions of mathematical models contain any mention of accuracy or reliability analysis... The literature review reveals that there is almost no contact between the theoretical model builders and the 'real world' practitioners." The bibliography is organized according to validation and error analysis methods.

Swetz, Mark J. (Ed.), Socialist Mathematics Education, Burgundy Pr, 1979; xvi + 421 pp, $19.50; $12.50 (P).

Case studies for seven countries: USSR, East Germany, China, Hungary, Sweden, Tanzania, and Yugoslavia.

Committee on Prescience Education, Guidelines for the Preparation of Teachers of Mathematics, Second Edition, NCTM, 1979; 31 pp, $2.15 (P).

This revision includes updating (including reference to specific competencies in computer programming and in probability and statistics), removal of sexist language, and correlation to the standards of the National Council for Accreditation of Teacher Education.

Pearce, Peter, Structure in Nature as a Strategy for Design, MIT Pr, 1978; xvii + 245 pp, $45.

Hundreds and hundreds of photographs and illustrations of nature, polyhedra, and modular structures convey the architect author's conviction: that the structural designs that occur in nature are the proper source of inspiration for human structures. He has teamed with mathematician A.H. Schoen to enumerate "saddle polyhedra," which can be used to assemble infinite periodic structures.

Science and the citizen: superconducting supercomputer, Scientific American 240:6 (June 1979) 104, 109.

Relates progress to date on a computer based on Josephson function devices, which are fast and tiny superconducting switches.

Bergman, P.G., *Unitary field theories*, Physics Today 32:3 (March 1979) 44-51.

A summary of developments in field theory since Minkowski's observations on the geometric nature of space-time. Includes a concise description of how fibre bundles maneuver their way into theoretical physics. (Yes, Virginia, there is *applied* algebraic topology.)

Committee on the Teaching of Undergraduate Mathematics, College Mathematics: Suggestions on How to Teach It, MAA, 1979; x + 30 pp, free (P).

Copies of this excellent booklet were sent to all MAA members. Many nonmembers, such as most graduate teaching assistants, would also benefit from it; additional copies are available from the national headquarters.

NEWS & LETTERS

ALLENDOERFER, FORD, PÓLYA AWARDS

Authors of eight expository papers published in 1978 issues of journals of the Mathematical Association of America received awards at the 1979 August meeting of the Association at the University of Minnesota at Duluth. The 1978 awards, each in the amount of $100, are:

Carl B. Allendoerfer Awards:

Bruce Berndt (Dept. of Mathematics, University of Illinois, Urbana, IL 61801) for "Ramanujan's Notebooks," *Mathematics Magazine* 51 (1978) 147-164.

Doris Schattschneider (Dept. of Mathematics, Moravian College, Bethlehem, PA 18018) for "Tiling the Plane with Congruent Pentagons," *Mathematics Magazine* 51 (1978) 29-44.

Lester R. Ford Awards:

Bradley Efron, (Dept. of Statistics and Dept. of Preventive Medicine, Stanford University, Stanford, CA 94305) for "Controversies in the Foundations of Statistics,"*Amer. Math. Monthly* 85 (1978) 231-246.

Ned Glick, (Dept. of Mathematics and Dept. of Health Care and Epidemiology, University of British Columbia, Br. Columbia, Canada) for "Breaking Records and Breaking Boards,"*Amer. Math. Monthly* 85 (1978) 2-26.

Kenneth I. Gross (Dept. of Mathematics, University of North Carolina, Chapel Hill, NC 27514) for "On the Evolution of Noncommutative Harmonic Analysis,"*Amer. Math. Monthly* 85 (1978) 525-548.

J.B. Kruskal and Larry A. Shepp (Bell Laboratories, Murray Hill, NJ 07974) for "Computerized Tomography: The New Medical x-Ray Technology,"*Amer. Math. Monthly* 85 (1978) 420-439.

George Pólya Awards:

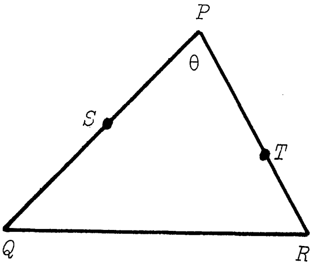
Richard L. Francis (Dept. of Mathematics, Southeast Missouri State University, Cape Girardeau, MO 63701) for "A Note on Angle Construction," *TYCMJ* 9 (1978) 75-80.

Richard Plagge (Dept. of Mathematics, Highline Community College, Midway, WA 98031) for "Fractions Without Quotients: Arithmetic of Repeating Decimals," *TYCMJ* 9 (1978) 11-15.

A QUICKIE REPAIR JOB

In Quickie 247 (this *Magazine*, 1959, pp. 285, 287), I asked for what values of x is $m^2 + n^2 - a^2 - b^2 \geq (mn-ab)x$ where $0 \leq a \leq m$ and $0 \leq b \leq n$? The published solution $x < 1$ is incorrect: it should be $x \leq 0$.

To see this consider a triangle PQR with $PQ = m$, $PR = n$, $PS = a$, $PT = b$:



If we let $x = 2 \cos \theta$, then the given inequality is equivalent to $QR \geq ST$. This will only be valid if QR is the longest side of the triangle. Since this must be true for arbitrary M and n, we must have $\theta \geq \pi/2$, not $\pi/6$ as stated.

Murray S. Klamkin
University of Alberta
Edmonton, Alberta
Canada T6G 2G1

1979 INTERNATIONAL MATHEMATICAL OLYMPIAD

The twenty-first International Mathematical Olympiad was held at Westfield College, London, on July 2-3, 1979. Twenty-two nations entered the competition, which consisted of the following six questions:

1. Let p and q be natural numbers such that

$$\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \dots - \frac{1}{1318} + \frac{1}{1319} .$$

Prove that p is divisible by 1979.
(W. Germany)

2. A prism with pentagons $A_1A_2A_3A_4A_5$ and $B_1B_2B_3B_4B_5$ as top and bottom faces is given. Each side of the two pentagons and each of the line-segments A_iB_j, for all $i, j = 1, \dots, 5$, is colored either red or green. Every triangle whose vertices are vertices of the prism and whose sides have all been colored has two sides of a different color. Show that all 10 sides of the top and bottom faces are the same color.
(Bulgaria)

3. Two circles in a plane intersect. Let A be one of the points of intersection. Starting simultaneously from A two points move with constant speeds, each point travelling along its own circle in the same sense. The two points return to A simultaneously after one revolution. Prove that there is a fixed point P in the plane such that, at any time, the distances from P to the moving points are equal. *(USSR)*

4. Given a plane π, a point P in this plane and a point Q not in π, find all points R in π such that the ratio $(QP + PR)/QR$ is a maximum.
(USA)

5. Find all real numbers a for which there exist non-negative real numbers x_1, x_2, x_3, x_4, x_5 satisfying the relations

$$\sum_{k=1}^{5} kx_k = a, \quad \sum_{k=1}^{5} k^3x_k = a^2, \quad \sum_{k=1}^{5} k^5x_k = a^3 .$$ *(Israel)*

6. Let A and E be opposite vertices of a regular octagon. A frog starts jumping at vertex A. From any vertex of the octagon except E, it may jump to either of the two adjacent vertices. When it reaches vertex E, the frog stops and stays there. Let a_n be the number of distinct paths of exactly n jumps ending at E. Prove that $a_{2n-1} = 0$,

$$a_{2n} = \frac{1}{\sqrt{2}}\,(x^{n-1} - y^{n-1}), \quad n = 1,2,3,\dots,$$

where $x = 2 + \sqrt{2}$ and $y = 2 - \sqrt{2}$.
(W. Germany)

Note: A path of n jumps is a sequence of vertices $(P_0, \dots, P_n)$ such that

i) $P_0 = A$, $P_n = E$;

ii) for every i, $0 \le i \le n - 1$, P_i is distinct from E;

iii) for every i, $0 \le i \le n - 1$, P_i and P_{i+1} are adjacent.

THE ROLE OF APPLICATIONS IN THE UNDERGRADUATE MATHEMATICS CURRICULUM

The National Research Council has just released its long-awaited report of the blue-ribbon Committee on the Role of Applications in the Undergraduate Mathematics Curriculum. Chaired by Peter Hilton, the Committee identified attitude (arrogance, scholasticism, suspicion) of mathematicians and fragmentation of mathematics as posing a threat of major proportions to the continued vitality of mathematics. The Committee recommends fourteen general changes in policy, attitude, and curriculum that stress increasing breadth of training (for both teachers and students), including an increase in the number of credits required for a mathematics major.

Copies of the 25 page report may be obtained from the Office of Mathematical Sciences, National Research Council, 2101 Constitution Avenue, Washington, D.C. 20418.

HOMOGENEOUS TILINGS BY REGULAR CONVEX POLYGONS

In their paper "Tilings by regular polygons" (this *Magazine*, 50 (1977) 227-247), B. Grünbaum and G.C. Shephard conjecture that there are 19 homogeneous edge-to-edge tilings by regular convex polygons. We have proved that there are actually 22 such tilings, of which 3 are 1-homogeneous, 13 are 2-homogeneous, 5 are 3-homogeneous and 1 is 4-homogeneous:

The 1-homogeneous tilings are the Archivedean tilings (3^6), (4^4) and (6^3) (p. 233, Fig. 7).

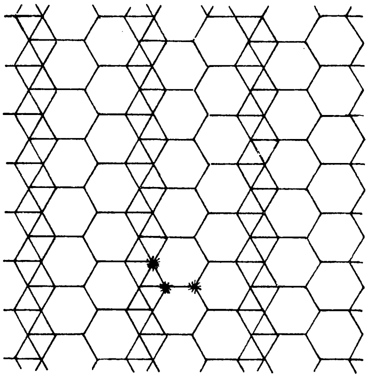
The thirteen 2-homogeneous tilings are the Archimedean tilings $(3^3.4^2)$, $(3^2.4.3.4)$, $(3.6.3.6)$, (3.12^2) and (4.8^2) (p. 233, Fig. 7); the 2-uniform tilings $(3^6; 3^2.6^2)$, $(3^4.6; 3^2.6^2)$, $(3^3.4^2; 4^4)_1$, and $(3^2.6^2; 3.6.3.6)$ (p. 235, Fig. 9); the 3-uniform tilings $(3^6; 3^2.6^2; 6^3)$ (p. 236, Fig. 10), $(3^4.6; 3^2.6^2; 6^3)$ and $(3^2.6^2; 3.6.3.6; 6\ )$ (Figures 1, 2 below); and the 4-uniform tiling $(3^6; 3^2.6^2; (6^3)^2)$ which exists in two mirror-symmetric forms (p. 236, Fig. 10).

The five 3-homogeneous tilings are the Archimedean tilings $(3.4.6.4)$ and $(4.6.12)$ (p. 233, Fig. 7); the 2-uniform tilings $(3.4.3.12; 3.12^2)$ and $(3.4^2.6; 3.6.3.6)_2$ (p. 235, Fig. 9); and the 3-uniform tiling $(3.4^2.6; 3.4.6.4; 4^4)$ (Figure 3 below).

The 4-homogeneous tiling is the 2-uniform tiling $(3.4.6.4; 4.6.12)$ (p. 235, Fig. 9).

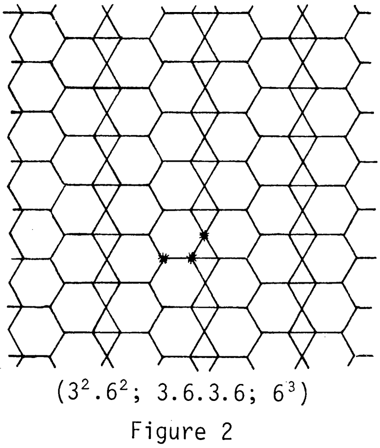
I. Debroey
Limburgs Universitair Centrum
Département WNF
Universitaire Campus
B-3610 Diepenbeek
Belgium

F. Landuyt
Université Libre de Bruxelles
Département de Mathématique
Campus Plaine - C.P. : 216
Boulevard du Triomphe
B-1050 Bruxelles
Belgium



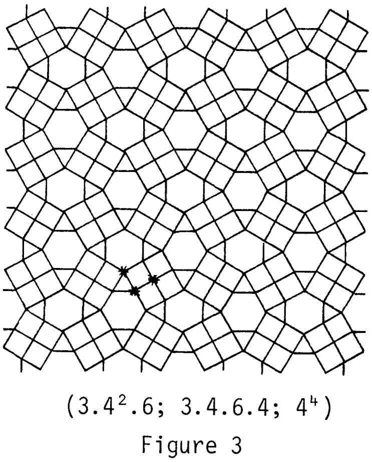
$(3^4.6; 3^2.6^2; 6^3)$

Figure 1



$(3^2.6^2; 3.6.3.6; 6^3)$

Figure 2



$(3.4^2.6; 3.4.6.4; 4^4)$

Figure 3

Three 3-uniform edge-to-edge tilings by regular convex polygons. One vertex of each orbit on the vertices is marked.

THE MATHEMATICAL ASSOCIATION OF AMERICA
1529 Eighteenth Street, N.W.
Washington, DC 20036

MATHEMATICS MAGAZINE VOL. 52, NO. 4 SEPTEMBER 1979