MATHEMATICS MAGAZINE

Vol. 50, No. 1
January, 1977
CODEN: MAMGA8

GREEK VARIABLES • WARING'S PROBLEM

TRUTH IN LENDING • VOTING BLOCS

MATHEMATICS MAGAZINE

Volume 50, Number 1, January 1977

COVER: Artist's conception of the ultimate mathematician, a machine that "never talks nonsense and never tells lies". Developments in mathematical logic, reported on pp. 5–11, have made possible this considerable improvement on the proverbial tribe of a thousand monkeys sitting at a thousand typewriters.

ARTICLES

NOTES

PROBLEMS

NEWS AND LETTERS

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

Paul Halmos ("Logic from A to G") moved to the University of California (Santa Barbara) in 1976. About his earlier history he writes as follows. "My professional life was spent mainly at Chicago, Michigan, and Indiana, but in bits and pieces around the world. My training and publications make me an analyst, but my heart has always been in the algebraic way of looking at things. My interest in logic started when I was an undergraduate philosophy major at Illinois, and tried to read *Principia Mathematica*. More than twenty years later I tried to make algebra out of all the logic I knew, but Gödel's theorem resisted the attempt."

Charles Small ("Waring's Problem") received his Ph.D. from Columbia University in 1969, and has taught at Queen's University, Kingston, Ontario, since 1970. His interest in Waring's problem is an outgrowth of a chronic obsession with the natural numbers — an addiction he shares with most mathematicians. In addition to writing the present survey article, this addiction led him to write for the *American Mathematical Monthly* an article on the analogous (and easier) question mod n. He is also the co-author of books on the Brauer group, and homological methods in commutative rings.

Oskar Itzinger ("The South American Game") studied in mathematical psychology, logic and statistics at the University of Vienna and obtained his Ph.D. in 1973. Since then he has been Assistant Professor at the Institute for Advanced Studies, Vienna, Division for Applied Mathematics. In the course of collecting material for a book on Nim-type games Professor Itzinger discovered a larger class of games which may be solved by new approaches of which the method presented here is just one simple example.

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. College 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, Suite 310, 1225 Connecticut Avenue, N.W., Washington, D.C. 20036. Back issues may be purchased, when in print, from P. and H. Bliss Co., Middletown, CT 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.

Logic from A to G

A sketch for a mathematician's mechanical helper, flippantly annotated by a working mathematician.

PAUL R. HALMOS
University of Calfornia, Santa Barbara

What logic is and is not

Originally "logic" meant the same as "the laws of thought" and logicians studied the subject in the hope that they could discover better ways of thinking and surer ways of avoiding error than their forefathers knew, and in the hope that they could teach these arts to all mankind. Experience has shown, however, that this is a wild-goose chase. A normal healthy human being has built in him all the "laws of thought" anybody has ever invented, and there is nothing that logicians can teach him about thinking and avoiding error. This is not to say that he knows *how* he thinks and it is not to say that he never makes errors. The situation is analogous to the walking equipment all normal healthy human beings are born with. I don't know how I walk, but I do it. Sometimes I stumble. The laws of walking might be of interest to physiologists and physicists; all I want to do is to keep on walking.

The subject of mathematical logic, which is the subject of this paper, makes no pretense about discovering and teaching the laws of thought. It is called *mathematical* logic for two reasons. One reason is that it is concerned with the kind of activity that mathematicians engage in when they prove things. Mathematical logic studies the nature of a proof and tries to forecast in a general way all possible types of things that mathematicians ever will prove, and all that they never can. Another reason for calling the subject *mathematical* logic is that it itself is a part of mathematics. It attacks its subject in a mathematical way and proves things exactly the same way as do the other parts of mathematics whose methods it is concerned with. The situation is like that of a factory that makes machines whose purpose is to make machines. A worker at such an establishment is no different from a worker at any other machine factory, except perhaps that he understands a little better what makes machines in general work as they do (and a little less well how any particular machine works).

The history of logic, like the history of most subjects, developed all in the wrong order. If I told it to you straight, you'd get completely confused. I propose to tell you a little bit of the history of logic in the "right" order, that is, in the order in which it *should* have happened.

First Boole and propositions

According to my version of history it all begins with George Boole about 100 years ago. Boole's contribution was a systematic study of the innocuous little words that we all use every day to tie propositions together, the so-called propositional connectives. These connectives are, in English,

and, or, not, implies, and *if-and-only-if.*

It is convenient to have abbreviations for these words. The customary mathematical symbols used to abbreviate them are

$$\&, \vee, \neg, \Rightarrow, \quad \text{and} \quad \Leftrightarrow.$$

Thus, for example, if P and Q are propositions, then so also is $P \& Q$. If P says "the sun's shining" and Q says "it's hot", then $P \& Q$ says "the sun's shining and it's hot".

Next Peano and numbers

The next figure in our revised history is the 19th-century Italian mathematician Peano who studied the foundations of arithmetic. He studied, in particular, the properties of the basic numbers *zero* and *one*, the basic operations of *addition* and *multiplication*, and the basic relation of *equality*. The symbols for these things are, of course, known to everybody: they are

$$0, 1, +, \times, \quad \text{and} \quad =.$$

Thus, for example, the popular proposition that "two and two make four" can be written in the unabbreviated form

$$(1+1)+(1+1)=1+(1+(1+1)).$$

Then Aristotle and a quantifier

Immediately after Peano comes Aristotle, who lived well over 2000 years ago, and to whom we are indebted for the first analysis of the crucial words *all* and *some*. (Incidentally, we have now also reached the beginning of the alphabet: the "A" in "Logic from A to G" is, of course, Aristotle.) The abbreviations are $\forall$ and $\exists$. To illustrate the use of these symbols, consider a well-known sentence such as "He who hesitates is lost". In pedantic mathematese this can be said as follows: "For all X, if X hesitates, then X is lost". Using $H(X)$ and $L(X)$ as abbreviations for "X hesitates" and "X is lost", we may write

$$(\forall X)(H(X) \Rightarrow L(X)).$$

If we doubt this assertion, if, that is, we are inclined to believe it quite likely that hesitation is possible without subsequent perdition, we may express our skepticism in the form

$$(\exists X)(H(X) \;\&\; (\neg L(X)).$$

Finally Frege and many quantifiers

An essential part of such Aristotelean abbreviations is the use of auxiliary symbols such as the "X" above; symbols such as that play the role of pronouns in the language of logic. Recall that, in the example, "X" took the place of "he". Symbols used in this way are called *individual variables*, and the next historical figure to be mentioned is the first one to face them courageously. His name is Frege, and he too lived in the 19th century. His role for us today is to emphasize that *one* variable, that is one pronoun, is much too meager equipment for most scientific and mathematical purposes. Thus, for instance, if we want to express the very modest assertion that there are more than two numbers, that is, that there exist at least three different ones, we would do it this way:

$$(\exists X)(\exists Y)(\exists Z)(\neg(X=Y) \;\&\; \neg(Y=Z) \;\&\; \neg(X=Z)).$$

For this purpose, pretty clearly, we need at least three variables. To say that there are more than ten numbers, we need at least eleven variables. To do any non-trivial amount of mathematics, we need an (at least potentially) infinite supply of variables. An efficient way of getting such a supply (since ordinary alphabets are much too finite) is to use one letter, say "X", and one extra symbol, say a dash $'$, and then use in the role of variables the symbols

$$X,\ X',\ X'',\ X''',\ X'''',\ \text{etc.}$$

In addition to all the symbols I have mentioned so far, there are two others that I have already used, and compulsive honesty now forces me to adjoin them to the list. The symbols I mean are the *left parenthesis* and *right parenthesis* denoted, of course, by

$$($$

and

$$).$$

How many symbols?

It turns out that a considerably large body of mathematics, namely, all arithmetic, can be expressed by means of the symbols I have listed so far. (Thus, for instance, Euler's celebrated theorem that every positive integer is the sum of four squares can be written as follows:

$$(\forall X)(\exists X')(\exists X'')(\exists X''')(\exists X'''')(X=(X'\times X')+((X''\times X'')+((X'''\times X''')+(X''''\times X''''))))).)$$

In fact certain savings can be made; some symbols are naturally and easily definable in terms of others. Our list can easily be cut down to an even dozen, namely to

$$\&\ \neg\ +\ \times\ 0\ 1\ \exists\ X\ '\ =\ (\ \ ).$$

To recapture $\vee$ observe that $P \vee Q$ is the same as $\neg(\neg P\ \&\ \neg Q)$. To recapture $\Rightarrow$ observe that $P \Rightarrow Q$ is the same as $\neg P \vee Q$. To get $\forall$ note that $(\forall X)P(X)$ is the same as $\neg(\exists X)(\neg P(X))$. In words: to say that everybody hates spinach is the same as to deny that there is somebody who loves it. There is some technical advantage in such abbreviations, but there's no sense in tying ourselves down. Whenever convenient I'll still use $\vee$ and $\Rightarrow$ and $\forall$, and I'll even use Y, Z, U, V, and such, as variables. The proper way to interpret these irregularities is clear by now: replace $\vee$, $\Rightarrow$, $\forall$, and the like by their definitions, and replace Y, Z, U, V, and such, by X', X'', X''', X'''', etc.

It might be fun to make a couple of side observations here. One of them is that what we are doing for elementary arithmetic can just as well be done for *all* extant mathematics. The technical machinery, that is the symbolism and the rules governing it, doesn't even get more complicated: the only difference is that we have to think a little harder. Since that is clearly undesirable, I am going to stick to elementary arithmetic. The second observation is that there is nothing magic about the number twelve. A dozen symbols are adequate for arithmetic, and in fact for all mathematics (though we might have to find a different dozen for that). A little care and stinginess, however, can easily reduce the dozen to still fewer, and the best possible result that you would hope for in your wildest dreams is true, namely, that two symbols are enough. A complete exposition of all mathematics written with, say, the dots and dashes of the Morse code wouldn't make particularly thrilling reading, but in principle it is perfectly feasible.

The mechanical mathematician

Let us now set about designing the mechanical mathematician to end all mathematicians. The virtues of this imaginary machine are purely conceptual; it will not be claimed that there is any practical advantage in building it. It will never replace the live mathematician.

The first step is to build into the machine a typewriter ribbon, a dozen typewriter keys (one bearing each one of the dozen basic symbols), and a potentially infinitely long piece of typing paper. The idea is that when a certain crucial button is pushed the machine is to start printing, and to print one after another all things that it could conceivably ever print. One way to program this would be to arrange the dozen symbols in an arbitrary order (call it alphabetical), and then to direct the machine to print the first twelve symbols ("letters") of the alphabet, then to print the 144 two-letter "words", next the 1728 three-letter "words", and so on *ad infinitum*. A machine so designed would print a lot of nonsense (for example

$$= \; = \; = \; (\,(\,(\,0 \; + \; '\,),$$

and it would print a lot of lies (for example

$$(\exists X)((0 \times X) = 1)),$$

but it would also, sooner or later, get around to printing all arithmetical statements.

Insist on grammar

In order to make the machine more like a flesh-and-blood mathematician, the next thing we must do is to arrange matters so that the output of the machine, while possibly false, should never be arrant nonsense. This is in principle quite easy. There is no point in listing here all the restrictions to which the machine must be subjected, but let us look at a few samples. First, teach the machine some "grammar". Let us say that a ***noun*** is any sequence of symbols built up from 0's and 1's by successively sandwiching $+$'s and $\times$'s between them and separating the results by the appropriate parentheses. Examples:

$$0,$$

$$1+1,$$

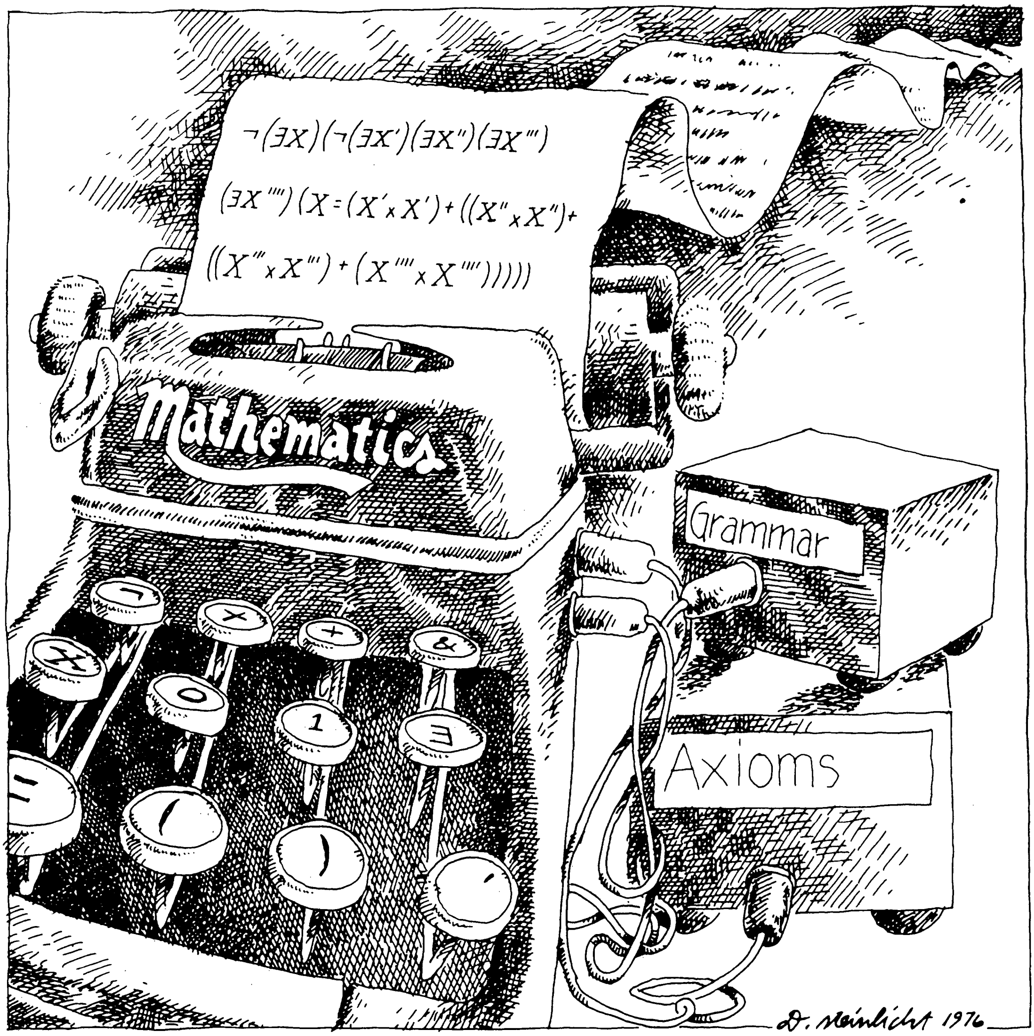
$$((1+1)\times(1+(1+(1+1))))$$

are nouns in this sense. Let us, similarly, say that a *pronoun* is anything obtained from X by successively appending dashes. Thus the pronouns are

$$X,\ X',\ X'',\ X''', \text{ etc.}$$

To go on in the same spirit, a *substantive* shall be a string of nouns and pronouns put together by means of addition and multiplication (and the auxiliary use of parentheses) the same way as nouns were originally put together from 0's and 1's. It is not at all difficult to design the machine so that it is able to recognize a substantive when it sees one. Once that is done, we can direct the machine as follows: "Start printing substantives (in some systematic order). After printing one, print an equal sign and then print another substantive. Learn to recognize the strings you have printed in this manner (substantive, equal, substantive), and call each such string a *clause*." Our machine can now print sensible clauses, and recognize them as such. It is just one step from here to teach the machine to print (and to recognize) compound *phrases*. The idea is to put clauses together by suitably restricted use of the logical operators *or*, *not*, and *some*. A machine that prints only phrases is thus within conceptual reach. Such a machine might still print incomplete phrases (for example $X = 0$) and lies (for example $1 = 0$), but it will no longer print gibberish.

The incidental mention of "incomplete phrases" suggests another look at what we want the mechanical mathematician to do. An incomplete phrase, in the sense I want that expression to have now, is something like "he is lost". The natural reaction upon seeing or hearing those words is to ask "Who is lost?" Similarly, "$X = 0$" should evoke the reaction "What is X?". Phrases with "dangling pronouns" like the "he" in "he is lost" and like the "X" in "$X = 0$" are the ones I mean to call incomplete here. A phrase that has no such dangling pronouns shall be called a *sentence*. The next step in perfecting the mechanical mathematician is to teach it to recognize a sentence when it sees one, and



to instill in it an inhibition that permits it to print complete sentences only (that is, no incomplete phrases). Now if the button is pushed, the machine will start printing sensible sentences. It will never present the machine operator with "$X = 0$". It might say something uninteresting (for example $(\exists X)(X = 0)$) or false (for example $(\forall X)(X = 0)$), but at any rate it will always say something.

Establish the axioms

The machine now knows how to talk; the next step is to teach it how to prove things. Neither the machine nor its flesh-and-blood prototype, however, can prove something from nothing. A live mathematician has his axioms; the machine must have built into it certain sentences that it is instructed to start from. Let us call those sentences *axioms.* Once again I shall not define here exactly which sentences are to be the axioms of arithmetic, but I shall indicate some examples. (The complete definition of "axiom" for elementary arithmetic is not even very long or complicated. This is just not the time and place to get technical.) Very well then: the machine might be taught that whenever P and Q are sentences, then the sentence

(A) $$P \Rightarrow (P \vee Q)$$

shall be printed in red ink. The idea, of course, is that every such sentence is to be regarded as an axiom. Similarly, we might say that if $P(X)$ and $Q(X)$ are phrases (containing the dangling pronoun "X", but no other), then the sentence

$$(B) \qquad (\exists X)(P(X) \vee Q(X)) \Rightarrow (\exists X)P(X) \vee (\exists X)Q(X)$$

shall be printed in red. Final sample: a sentence such as

$$(C) \qquad (\forall X)(\forall Y)(X + Y = Y + X)$$

might be an axiom of elementary arithmetic. (Interpretive examples: (A) If it's hot, then either the sun's shining or else it's hot or both. (B) If somebody likes either spinach or broccoli, then either somebody likes spinach or somebody likes broccoli. (C) $2+3=3+2$.)

The main point is this: in some sensible and systematic manner a certain collection of sentences is singled out from among all the sentences that the machine can print, and the machine is directed to print those special sentences in red. The red sentences are called the axioms for the machine.

Program the procedure

I said before that nobody can prove something from nothing, and, for that reason, I endowed the mechanical mathematician with some starting sentences. But it is just as true that nobody can prove something *with* nothing. The machine can print black and red sentences, and, if the axioms were chosen in accordance with the wishes of a reasonable being, the red sentences (the axioms) will be true. The machine might nevertheless still print a lot of false stuff, and it still has no means of producing new true sentences out of old ones.

The process of educating the machine has now reached its final step. In that step the machine must learn to recognize certain patterns of sentences and is rewarded by being permitted to use more red ink. The total list of such *rules of procedure* is not long, and the list of two examples from among them, that I propose actually to give, is even shorter. Possible rule number one: if P is a red sentence, and if $P \Rightarrow Q$ is a red sentence, then print Q in red. (Interpretation: if "The sun's shining" is an axiom or has already been proved, and if the same is true of "If the sun's shining, then it's hot", then we may consider to have proved "It's hot".) Possible rule number two: if an incomplete phrase $P(X)$ containing the dangling pronoun "X" (and no others) is such that the sentence $P(0)$ is red ($P(0)$ is the sentence obtained from $P(X)$ by substituting 0 for X), then print the sentence $(\exists X)P(X)$ in red. (Interpretation: if we substitute 0 for X in "$1+X=1$", we obtain "$1+0=1$". If this sentence is an axiom or has already been proved, then we may consider to have proved "$1+X=1$ for some X".)

With the last modification we can now rest on our laurels. We may if we wish change the internal design of the machine so that it no longer deigns to print anything but red sentences. When the button is pushed, the machine starts printing axioms, and, by means of the rules of procedure, it goes on to print *theorems* that it can "derive" from the axioms. It can do this in some systematic (say, alphabetic) order.

The millennium is come; the mechanical mathematician is complete. Push one button and sit back. One after another the theorems of elementary arithmetic will appear on the tape. If you wait long enough, sooner or later you will see all theorems pass before your eyes. The machine never talks nonsense, and the machine never tells lies. If you find the machine somewhat boring, possibly repetitious, and much much too slow for your merely human patience, that is not its fault.

Are there contradictions?

We have incorporated into the machine all that we ourselves, its builders, know about elementary arithmetic. The internal workings of the machine *are* elementary arithmetic. The external theory of the machine, its design and its structural properties, are part of another discipline often called *metamathematics* (or, in this case, metaarithmetic). The following question is typical of the ones that can be asked in metamathematics: "Will the machine ever print both a sentence P and its negation $\neg P$?" Should it ever do so, we would probably express our displeasure at this state of affairs by saying that elementary arithmetic is inconsistent. Fortunately this is not so: arithmetic is consistent. The proof of consistency depends on a very sophisticated, definitely non-elementary study of the structure of the "machine" we've been describing. The study is "non-elementary" in several senses of the word. In the most precise technical sense the fact is that the proof that the machine is consistent is not one of the theorems that the machine itself is able to prove. To say it again: the machine will never contradict itself, but it is not able to prove that it won't.

Can everything be proved?

Another interesting metamathematical question is this: "Is the machine complete, in the sense that it either proves or disproves every sentence of elementary arithmetic?" I've already told you the answer to this question, but the point will bear repetition. As the machine now stands, everything it prints it proves. If I am interested in a particular arithmetical sentence, I may write that sentence on a piece of paper and then, after setting the machine into operation, compare each successive output of the machine with my prepared slip. If the slip says P and if, at some stage, the machine also says P, I retire victorious: my P is proved. If the slip says P, and if, at some stage, the machine says $\neg P$, I retire in ignominy: my P is disproved. Isn't there, however, a third possibility? Couldn't it happen that the machine will never print P and neither will it ever print $\neg P$? Couldn't it happen that the machine will never decide the P versus $\neg P$ controversy? It could, and it does, and we have thereby reached the end of the alphabet. G is for Gödel, the brilliant twentieth-century logician. In the early 1930's Gödel proved, by a delicate and ingenious analysis of the arithmetic machine, that there are sentences (many of them) that the machine never decides. His proof is quite explicit: he gives a complete set of directions for writing down an undecidable sentence. The proof that the sentence obtained by following his directions is undecidable depends on a detailed examination of those very directions themselves. There is nothing wrong, there is no paradox, and it all hangs together. The fact that no one has ever bothered actually to write down Gödel's undecidable sentence is, once again, the fault of human impatience and the brevity of human life.

I said when I raised the question of completeness that I had already answered it. Indeed, consider a sentence (written out formally in the dozen formal symbols of arithmetic) that says that arithmetic is consistent. It is not at all clear that the apparently meager formal apparatus of arithmetic is capable of expressing such a sentence; it is one of Gödel's accomplishments to have shown that it is capable of doing so. If we take that for granted, and if we call one such sentence P, then what we know is that P is not provable in elementary arithmetic. What about $\neg P$? Well, clearly, $\neg P$ cannot be provable either. Reason: everything that is provable is true, as we already know from our earlier thoughts on the subject. (This depends on the fact that arithmetic is consistent.) The sentence $\neg P$ is certainly *not* true. (Recall that $\neg P$ denies the consistency of arithmetic.) Conclusion: neither P nor $\neg P$ is provable. (Note: of the two, P is the one that is true.)

There is more

That is the end of the road, for us, for now. It is by no means the end of the road for mathematical logic. What I've been reporting to you happened in the 1930's, and science has not stood still since then. Gödel himself has contributed several other striking results to our knowledge of formal logic. Many others have taken up the field and opened up unexpected applications and complications. Who, for instance, could have expected formal mathematical logic to turn out to be one of the most important tools in the design of honest-to-goodness circuits-and-printouts electronic computing machines? Mathematical logic is alive and well; much remains to be done; it'll be a long time before anyone can describe mathematical logic from A to Z.

Waring's Problem

Survey of an almost-solved problem starting from a casual "and so on" of a 1770 "meditation" on algebra.

CHARLES SMALL
Queens University

What follows is a non-scholarly survey of the history of Waring's problem. Although a few easy things are proved along the way, the paper is mostly concerned with telling stories — in other words, quoting many beautiful theorems without proof. The proofs, for the most part, involve hard-core analysis, and are difficult. Anyone wishing to pursue the subject should examine chapters 20 and 21 of Hardy and Wright [**4**] and then [**1**] and [**2**]. Ellison's paper [**2**] provides a much more scholarly and detailed version of the story, with many proofs and an extensive bibliography; the present informal version should serve a useful role as an introduction to [**1**] and [**2**].

Waring's problem began with Edward Waring, who published a book entitled *Meditationes Algebraicae* in 1770, in which, among other things, the following remarkable assertion occurs: "Every number is the sum of 4 squares; every number is the sum of 9 cubes; every number is the sum of 19 biquadrates (4th powers); and so on." (Here, and throughout, number means natural number, possibly 0.)

The assertion for squares is much older: it is hinted in Diophantus (roughly third century A.D.) and stated explicitly by Bachet in 1621. Fermat claimed to have a proof in 1641, but in 1770 when Waring's book appeared, the 4-squares theorem was a well-known "fact" for which no proof was known. It was proved later in the same year by Lagrange, to the chagrin of Euler, who had tried unsuccessfully to find a proof.

There have been many other proofs for the 4-squares theorem since Lagrange; here's one that is particularly short and sweet. Suppose that we are given a number n which we want to write as a sum of four squares. Clearly, we can throw out any squares that divide n: if $n = x^2n'$ and $n' = a^2+b^2+c^2+d^2$ then $n = (xa)^2+(xb)^2+(xc)^2+(xd)^2$. Thus we may assume that $n = p_1 \cdots p_s$ is a product of distinct primes p_i. Then, by the Chinese Remainder Theorem, we know that Z_n breaks up as the corresponding direct product $Z_{p_1} \times \cdots \times Z_{p_s}$ of finite fields. Now in each Z_{p_i}, -1 is a sum of two squares. (In fact it's easy to prove, more generally, that in any finite field every element is a sum of two squares.) Thus -1 is a sum of two squares in Z_n, so we can find integers c, d, m such that $-1 = c^2 + d^2 - mn$.

Power	*Integer*	*Minimal Expression as sum of kth powers*	*Number of kth powers required*
2	7	$7 = 2^2 + 3\cdot 1^2$	$1+3=4$
3	23	$23 = 2\cdot 2^3 + 7\cdot 1^3$	$2+7=9$
4	79	$79 = 4\cdot 2^4 + 15\cdot 1^4$	$4+15=19$
5	223	$223 = 6\cdot 2^5 + 31\cdot 1^5$	$6+31=37$

WARING'S PROBLEM concerns efficient ways of expressing integers as sums of *k*th powers. When $k = 2$ it can always be done with four squares (including 0 if necessary); when $k = 3$ it requires 9 cubes, when $k = 4$ it requires at least 19 biquadrates (or fourth powers), and when $k = 5$ it requires 37 fifth powers. The sequences 7, 23, 79, 223, ... and 4, 9, 19, 37, ... form a pattern discovered by Euler: the number of *k*th powers needed to express the $(k-1)$st number in the first sequence is given by the corresponding number in the second sequence.

Now consider the matrix $A = \begin{pmatrix} n & c+di \\ c-di & m \end{pmatrix}$ over $Z[i]$, where $i = \sqrt{-1}$. Then $\det A = 1$ and $n > 0$. Under these conditions it can be shown (we indicate one method in the next paragraph) that $A = BB^*$ for some 2×2 matrix B over $Z[i]$, where * denotes conjugate transpose. The upper left entry in BB^* yields the desired expression for n:

$$\begin{pmatrix} n & - \\ - & - \end{pmatrix} = \begin{pmatrix} x+yi & z+wi \\ - & - \end{pmatrix} \begin{pmatrix} x-yi & - \\ z-wi & - \end{pmatrix}.$$

In other words, $n = x^2 + y^2 + w^2 + z^2$, a sum of 4 squares.

We can be sure that $A = BB^*$ for some 2×2 complex matrix B for well-known reasons ([**3**], §72): A represents a positive transformation. But we really need a matrix B over $Z[i]$. We can get it by a proof using induction on $c^2 + d^2$. This crucial observation is due to George Bergman, and it is what makes this proof work so nicely.

The assertions for cubes and biquadrates, and the implied assertions for higher powers, originate with Waring. The first question, no doubt, is what those implied assertions are: what does Waring's phrase "and so on" ("*& sic deinceps*") mean? One might observe that $2 \cdot 4 + 1 = 9$ and $2 \cdot 9 + 1 = 19$ and wonder if Waring meant to assert that for each k, every number is a sum of $s(k)$ kth powers, where $s(k)$ is the appropriate term in the sequence defined by $s(2) = 4$, $s(n+1) = 2s(n) + 1$. It turns out, as we shall see below, that there is a better candidate for such a sequence in which the next term after 19 is 37 rather than 39. But the most likely interpretation of what Waring had in mind is something weaker than this.

Let us define $g(k)$ to be the smallest r such that every number is the sum of r kth powers, and put $g(k) = \infty$ if no such r exists. Thus Lagrange's theorem is that $g(2) \leqq 4$ (and therefore $g(2) = 4$, since 7 is not a sum of three squares). In this language, the interpretation of Waring's assertion has usually been: $g(2) = 4$, $g(3) = 9$, $g(4) = 19$, and $g(k) < \infty$ for all k. Waring's problem, then, is to prove that $g(k) < \infty$ for all k, and then to compute $g(k)$.

Of course the general problem is much harder than the case $k = 2$ considered above. Indeed, it is one of those nasty gems, like Fermat's Last Theorem, which begins with a simply-stated assertion about natural numbers, and leads quickly into deep water. One difference between the two is that Fermat's Last Theorem is still a problem whereas Waring's problem is mostly a theorem: Fermat's conjecture that $x^n + y^n = z^n$ has no solution in positive integers when $n > 2$ remains unproved, while Waring's problem, at least in its original form, is 99% solved.

To get a feeling for the solution, let's look for numbers that cannot be written as sums of just a few kth powers. In other words, we're looking for lower bounds for $g(k)$. (Since we don't know, *a priori*, whether $g(k)$ is finite, it seems prudent to begin by seeking *lower* bounds!) The first obvious choice is $n = 2^k - 1$; clearly n requires n kth powers; hence $g(k) \geqq 2^k - 1$. A trick found by Euler will let us do better:

Divide 3^k by 2^k, writing the result as Euclid taught us: $3^k = q \cdot 2^k + r$, $0 \leqq r < 2^k$. Now consider $n = q \cdot 2^k - 1$. Since $n < q \cdot 2^k \leqq 3^k$, we can use only 1^k and 2^k to write n as a sum of kth powers; and since $n < q \cdot 2^k$ we can use only $(q-1)$ 2^k's; the difference has to be made up with 1's. Thus $n = (q-1) \cdot 2^k + (2^k - 1) \cdot 1^k$ is a minimal decomposition of n as a sum of kth powers; the number of kth powers involved is $q - 1 + 2^k - 1 = q + 2^k - 2$, which we will call $\bar{g}(k)$. Thus $q \cdot 2^k - 1$ is not the

r	*Largest known integer requiring r cubes*
9	$239 = 2 \cdot 4^3 + 4 \cdot 3^3 + 3 \cdot 1^3$
8	$454 = 7^3 + 4 \cdot 3^3 + 3 \cdot 1^3$
7	$8042 = 16^3 + 12^3 + 2 \cdot 10^3 + 6^3 + 2 \cdot 1^3$

NINE CUBES SUFFICE to solve Waring's problem for $k = 3$: every integer can be expressed as a sum of at most 9 cubes. Dickson proved that 239 is the largest number requiring as many as nine cubes. Numerical evidence going back to Jacobi suggests that 454 is the largest number requiring eight cubes, and that 8042 is the largest requiring seven cubes.

k	2	3	4	5	6	7	8	9	...
q	2	3	5	7	11	17	25	38	...
$\bar{g}(k)$	4	9	19	37	73	143	279	548	...
$g(k)$	4	9	19?	37	73	143	279	548	...
$G(k)$	4	$\geqq 4$, $\leqq 7$	16	$\geqq 6$, $\leqq 23$	$\geqq 9$, $\leqq 36$	$\geqq 8$, $\leqq 137$	$\geqq 32$, $\leqq 163$	$\geqq 13$, $\leqq 190$	...

Waring's problem deals with the representation of integers as sums of kth powers. In this table, $g(k)$ is the smallest number with the property that every number is the sum of $g(k)$ kth powers. Euler found a simple lower bound for $g(k)$, called $\bar{g}(k)$, given by the formula $\bar{g}(k) = q + 2^k - 2$ where $q = [(3/2)^k]$. This table indicates that for small $k \neq 4$ Euler's bound is in fact the correct value for $g(k)$; that it might be correct for all values of k is a major unsolved problem known as the "Ideal Waring Theorem". The final line in this table reflects the relative lack of knowledge concerning the related number $G(k)$, which is defined as the smallest number such that every sufficiently large number is the sum of $G(k)$ kth powers.

TABLE 1

sum of fewer than $\bar{g}(k)$ kth powers, so that $g(k) \geqq \bar{g}(k)$ for all k.

This result takes on some life if we tabulate (in TABLE 1) some values of $\bar{g}$. To do this it is convenient to express q as $[(3/2)^k]$, and then use $\bar{g}(k) = q + 2^k - 2$. Euler's procedure shows that 7 $(= 2 \cdot 2^2 - 1)$ requires 4 squares, 23 $(= 3 \cdot 2^3 - 1)$ requires 9 cubes, 79 $(= 5 \cdot 2^4 - 1)$ requires 19 biquadrates, ... And Euler knew the procedure, in general, by 1772.

The general theorem — that $g(k)$ is finite for all k — was proved in 1909 by Hilbert. By that time it had been shown that $g(3) = 9$ (Wieferich, 1909), that $g(4) \leqq 53$ (Liouville, 1859), and that $g(k)$ was finite for $k = 5$, 6, 7, 8, and 10.

Hilbert's proof is extremely complicated. The essential ingredient is a fantastic identity that had been conjectured by Hurwitz:

$$(X_1^2 + X_2^2 + \cdots + X_n^2)^k = \sum_{j=1}^{M} \lambda_j (a_{1j}X_1 + \cdots + a_{nj}X_n)^{2k}.$$

The assertion here is that for each n and k there exist positive rational numbers λ_j and integers a_{ij} (where $1 \leqq i \leqq n$, $1 \leqq j \leqq M$, and $M = (2k+n)!/(2k)!(n-1)!$) making the identity in the indeterminates $X_1, \ldots, X_n$ true. Hilbert proved the existence of such identities by estimating huge multiple integrals associated with certain convex bodies; in the original paper, a 25-fold integral is evaluated. The proof has since been simplified, but it remains an *existence* proof for the numbers $g(k)$, and sheds no light on their actual value.

Once Hilbert's theorem is known, the problem "reduces" to computation of $g(k)$. The general question was taken up by Hardy and Littlewood, in a long series of papers published in the 1920's under the title "On Some Problems of Partitio Numerorum" I, II, ..., VIII. "Partitio Numerorum" has since become additive number theory, in approximately the same sense that "analysis situs" has become topology. Additive number theory is now a vast and flourishing subject, which grew from Waring's problem and generalizations of it. Hardy and Littlewood developed a powerful analytic method for handling such questions, and they used it to give an entirely different proof of Hilbert's theorem. Their proof was no easier than Hilbert's, but it did offer some hope of leading to actual computation of the values of $g(k)$.

The Hardy-Littlewood method was improved in many important respects by Vinogradov, and the method which evolved from their combined work is still a dominant force in additive number theory. The Russians call it the Hardy-Littlewood-Vinogradov method, but elsewhere it is usually known as the "circle method", because it involves integrating a complicated function around a circle in the complex plane. The circle is divided into "major arcs" and "minor arcs" whose precise identification depends on the particular aspect of the problem being considered. Because the integrand behaves in a complicated way near the contour of integration, delicate analysis is required to estimate the integrals on those arcs.

The Hardy-Littlewood-Vinogradov method was sufficiently refined by about 1935 to allow Dickson to determine $g(k)$ for nearly all k. Recall the definition of q, r and $\bar{g}(k)$: $3^k = q \cdot 2^k + r$, $0 \leqq r < 2^k$, $q = [(3/2)^k]$, $\bar{g}(k) = q + 2^k - 2$. Let us call k **good** if $q + r \leqq 2^k$ and **bad** otherwise. What Dickson showed was this: *If k is good and not equal to* 4, *then* $g(k) = \bar{g}(k)$. *If k is bad then* $g(k) = \bar{g}(k) + q' - t$ *where* $q' = [(4/3)^k]$ *and* $t = 1$ *if* $2^k < qq' + q + q'$, *and* 0 *otherwise.* (Since $2^k \leqq qq' + q + q'$, t can equal 0 only in case $2^k = qq' + q + q'$.) This determines $g(k)$ completely, except for $k = 4$.

It is, of course, a matter of simple arithmetic to determine if a given k is good or not. In particular, the reader can check that all $k \leqq 9$ are good, so that if we leave aside $k = 4$ we can add $g(k)$ to our previous table (see the fourth line of TABLE 1). A computer study in 1964 showed that all $k \leqq 200{,}000$ are good, and a difficult theorem due to Mahler (1957) shows that at most finitely many k are bad; it is not known whether *any* bad k actually exist. This is certainly a tantalizing state of affairs: the conjecture that all k are good is a simple-looking assertion about the natural numbers that is (except for $k = 4$) equivalent to the so-called "ideal Waring theorem", namely, the assertion that the rather trivial lower bound $\bar{g}(k)$ found by Euler in 1772 is actually the correct value of $g(k)$ for all k.

To be perfectly accurate we should note that Dickson was not the only person involved in the proof of this key result. Dickson proved it in 1935 for $k \geqq 7$, aside from a few cases that were filled in during the 1940's by various people (including Dickson). For $k = 6$ it is due to Pillai (1940), and for $k = 5$ to Chen (1964). For $k = 3$ and $k = 2$ it is, as we have seen, classical and pre-classical, respectively. For $k = 4$ Euler's construction yields, as we have seen, $19 = \bar{g}(4) \leqq g(4)$. The upper bounds have decreased over the years, the best known currently being $g(4) \leqq 22$ (H. E. Thomas, 1974). There is little doubt that further computation will show $g(4) = 19$. It has been, since 1940, literally a matter of computation; for Auluck proved in that year that all numbers greater than $c = 10^{10^{88.39}}$ are sums of 19 biquadrates!

The theorem of Dickson *et al* solves Waring's problem in its original form (except for the ambiguity about $g(4)$ and the question of whether any bad numbers exist). However, there is another aspect which opens a whole new range of problems; in fact it is an essential part of the method of proof in the Hardy-Littlewood-Vinogradov-Dickson solution of Waring's problem.

To describe it, let us go back to the case of cubes. Recall that Wieferich, in 1909, had proved that $g(3) = 9$. In the same year, Landau observed that by tracing through Wieferich's arguments very carefully it was possible to prove more: only finitely many numbers actually required 9 cubes because all sufficiently large numbers are sums of 8 cubes. Back in 1851, Jacobi had tabulated for us all numbers up to 12,000, writing each as a sum of as few cubes as possible. He found, in that range, exactly 2 numbers that require 9 cubes (23 and 239), 15 numbers that require 8 cubes (the largest is 454), and 121 that require 7 cubes (the three largest are 5306, 5818 and 8042). On the basis of the increasingly large gaps between these numbers (5306, 5818, 8042, and 12,000, where he stopped) Jacobi concluded that it was very likely that all numbers greater than 8042 are sums of 6 cubes or fewer. In fact, numbers requiring 6 cubes become sparse toward the end of Jacobi's table, and he almost permits himself to conjecture that all sufficiently large numbers are sums of 5 cubes.

These observations suggest a general definition: let $G(k)$ denote the smallest r such that every sufficiently large number (i.e., every number with perhaps finitely many exceptions) is a sum of r kth powers. Then $G(k) \leqq g(k)$ for all k; and $G(2) \geqq 4$ since $7+8n$ is never a sum of 3 squares for any n (because 7 is not a sum of 3 squares mod 8). Therefore $G(2)=g(2)=4$.

The Hardy-Littlewood-Vinogradov proof leads to upper bounds for $G(k)$. If one finds such an upper bound, $\bar{G}(k)$, and if it is less than or equal to the lower bound $\bar{g}(k)$ for $g(k)$, one can use it to compute $g(k)$, by extracting from the proof a specific n_0 such that all $n > n_0$ are sums of $\bar{G}(k)$ kth powers. This is in fact how $g(k)$ is determined. For $k=4$, the appropriate n_0 was Auluck's number c; it is now known that every number less than 10^{140} or greater than $10^{1408.3}$ is a sum of 19 biquadrates, but the gap is still too large, as yet, to permit complete calculations.

Jacobi's conjecture for cubes — that $G(3) \leqq 6$, or perhaps even $G(3) \leqq 5$ — remains unproved; the best that is known is a theorem of Linnik (1942), according to which $G(3) \leqq 7$. As mentioned above, Landau had proved $G(3) \leqq 8$ in 1909; and Dickson showed in 1939 that in fact 23 and 239 are the only numbers that require 9 cubes. In the other direction, we know that $G(3) \geqq 4$ because of a striking result due to Maillet and Hurwitz: $G(k) \geqq k+1$ for all $k>1$. The proof, which is elegant and astonishingly easy, can be found in Hardy and Wright [**4**, Chapter 21.6]. (The special case $G(3) \geqq 4$ can also be proved by working mod 9.)

Only a little more is known about $G(k)$ in the direction of explicit lower or upper bounds for specific k although there are many asymptotic theorems comparing $G(k)$ with known functions for large k. We have mentioned $G(2)=4$ and $4 \leqq G(3) \leqq 7$. For biquadrates, we can show that $G(4) \geqq 16$. To begin, we note that 15 requires 15 biquadrates mod 16, so that $G(4) \geqq 15$. Using this it is easy to show that if n requires 16 biquadrates so does $16n$. Since 31 requires 16 biquadrates, this implies $G(4) \geqq 16$. In fact Davenport showed in 1939 that $G(4)=16$, and $G(2)$ and $G(4)$ are the *only* values of $G(k)$ known exactly.

Finally, let us mention briefly some generalizations. The most obvious, perhaps, is to ask Waring's question in other rings or fields: is every element which is a sum of kth powers a sum of g kth powers for some g depending only on k? There is a substantial literature on such questions, for example in algebraic number fields and their rings of integers; see e.g., [**5**].

Another possibility is to remain in the natural numbers and generalize the question: given an interesting subset S of numbers, is every number (respectively, every sufficiently large number) a sum of r elements of S, for some bound r depending only on S? For example if S is the set of kth powers, the appropriate r is $g(k)$ (respectively, $G(k)$). The question in this generality is the province of additive number theory, and the literature on it is vast (see, for example, the bibliography of [**6**]: 28 dense pages, single-spaced!).

One interesting choice for S is the set of primes; this leads to Goldbach's problem. Another is the set of values of some fixed integer polynomial, more general than X^k. We close with a rather special case, where there is a particularly striking theorem (quoted incorrectly in [**2**]).

Suppose we have a sequence $2 \leqq n_0 \leqq n_1 \leqq n_2 \leqq \cdots$ and we ask: is there, for each j, a bound $r=r(j)$ with the property that every sufficiently large number can be written in the form $x_j^{n_0}+x_{j+1}^{n_1}+\cdots+x_{j+r}^{n_r}$? (If all $n_j=k$, the appropriate bound is $G(k)-1$.) The answer was announced without proof by Freĭman in 1949, and proved by Scourfield in 1960: such bounds r_j exist if and only if $\Sigma\, 1/n_i$ diverges! The "only if" is relatively easy; the "if" uses the full Hardy-Littlewood-Vinogradov machine.

References

[1] H. Davenport, Analytic Methods for Diophantine Equations and Diophantine Inequalities, University of Michigan, Ann Arbor Publishers, 1962.

[2] W. J. Ellison, Waring's problem, Amer. Math. Monthly, 78 (1971) 10–36.

[3] P. R. Halmos, Finite-Dimensional Vector Spaces, second ed., Van Nostrand, 1958.

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

[5] J.-R. Joly, Sommes de puissances d-ièmes dans un anneau commutatif, Acta Arith., 17 (1970) 37–114.

[6] H.-H. Ostmann, Additive Zahlentheorie (two volumes), Springer Ergebnisse, Berlin, 1956.

The South American Game

A formal Boolean manipulation solves a Nim-like game played on the map of South America.

Oskar Itzinger
Institute for Advanced Studies, Vienna

In his 1971 book *Your Move* [**5**], David Silverman introduced a coloring game played on the map of South America. Two players (call them A and B) take turns coloring (with just one color) the 13 countries under the following restriction: each player may color only a country that has no common frontiers with a previously colored country. The last player who can color a country is the winner.

Silverman offers a trivial strategy for this game that insures that the first player, A, can always win. On his first move A should color Brazil because Brazil borders on 10 other countries: only Chile and Ecuador do not border on Brazil. No matter which country B colors, A can color the remaining one and win because Chile and Ecuador have no common frontier.

In addition to this obvious solution Silverman puts forward the following question: Do there exist countries other than Brazil with the property that if A chooses such a country on his first move then he wins regardless of B's answer? Silverman argues that there do exist such countries, but opines that to determine all of them would require the aid of a computer. In this paper we will develop a method to answer Silverman's question without excessive computation. Our method applies quite generally to a large class of games, of which Silverman's South America contest is but one colorful example.

TacTix-type games

The first step in our analysis of Silverman's problem is to recognize that his South American game is not so much related to traditional coloring problems as it is to games like Nim and TacTix. In Nim, players take turns removing stones from one or more piles according to certain specific rules. TacTix is a two-dimensional variation of Nim introduced some 30 years ago by the Danish scientist Piet Hein. Usually, TacTix is played on an n-by-n-array of counters. A move consists in removing one or more counters that are adjacent along rows or columns. The player who takes the last counter wins.

There exists a *reductio-ad-absurdum* proof that TacTix can be won by the player making the first move if n is odd, and by the player making the second move if n is even. (Obviously, a draw is impossible.) Various restrictions on TacTix and corresponding results are sketched in Epstein [**3**] and Gardner [**4**].

Formally, TacTix is a two-person, zero-sum game with perfect information and a finite number of strategies. This game is, therefore, strictly determined. Like other similar games, TacTix may be represented as a game played on a graph. Counters in the initial configuration are represented by nodes of a graph. If two counters i and j are adjacent in the initial configuration then in the

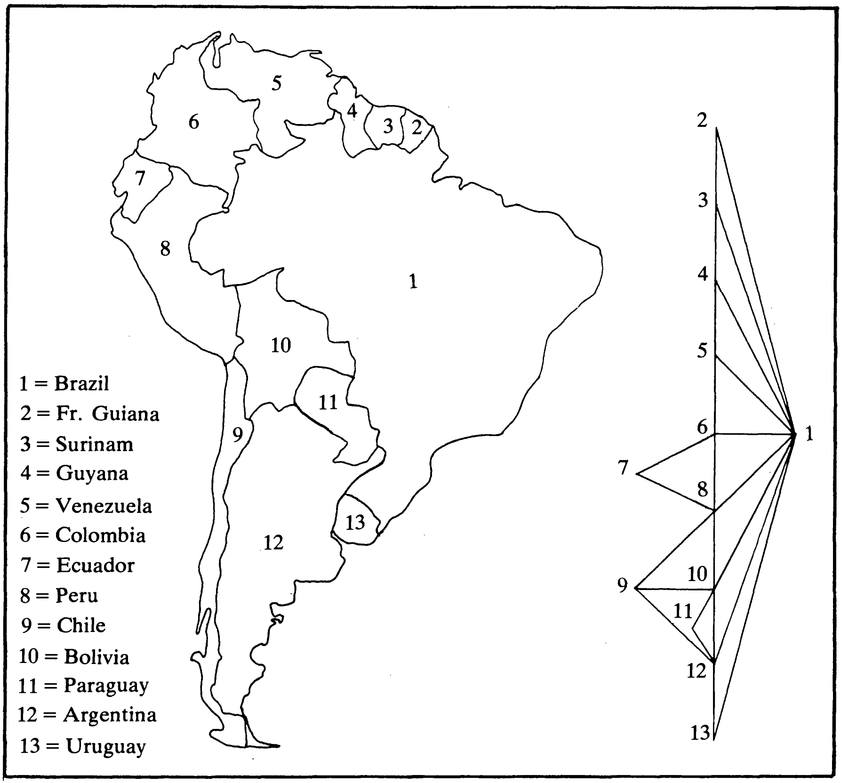


FIGURE 1

corresponding graph there is an arc between the nodes representing i and j. Then each TacTix game may be represented by the adjacency matrix $A = [a_{ij}]$ of the corresponding graph: $a_{ij} = 1$ if and only if nodes i and j are adjacent and 0 otherwise.

Traditionally, TacTix is played on a square or a rectangular board. But any appropriate adjacency matrix could be used as the blueprint for a TacTix-type game graph — provided only that the graph is connected and simple (i.e., contains no parallel arcs or self-loops). We will call such non-rectangular TacTix games **irregular,** and the rectangular ones **regular.** Of course, the rules for any given irregular TacTix-type game have to specify in a precise way how the counters (or, equivalently, the nodes of the corresponding graph) may be removed. The analysis of an irregular game may be very difficult, and hence, it may be hard to state the general strategy for playing that game. In the sequel we will discuss a certain class of irregular TacTix-type games — including David Silverman's South American game — for which it is possible to give a general method for analyzing every game in that class.

The South American game

To illustrate, we will carry out our analysis of irregular TacTix-type games in the context of Silverman's South American game. But first we must show that the South American game is, indeed, an irregular TacTix-type game. To see this we transform the map of South America into a simple graph G as in FIGURE 1. Then the rules of the coloring game amount to this TacTix-type rule: each player removes, in his turn, one node together with all nodes adjacent to it. The player who removes the last node from the graph is the winner.

By a **solution** to this game we will mean a sequence of moves (countries) that correspond to a legal play of the game. For example, if A colors Brazil (node 1) first, (thereby removing all nodes from the game graph except for Ecuador (node 7) and Chile (node 9)), and if B responds with Chile, and A finishes with Ecuador as his winning move, then the sequence Brazil, Chile, Ecuador (i.e., 1, 9, 7) is a solution to the South American game. What we wish to do is to discover *all* solutions to the game.

We begin with two basic facts that are crucial for our method: Given any solution, then (a) countries in that solution are pairwise not adjacent, and (b) each country not in that solution is adjacent to at least one country in that solution. If we interpret countries as nodes of G then we see that (a) is the graph-theoretic concept of an **internally stable set** of nodes whereas (b) is the graph-theoretic concept of an **externally stable set** of nodes. Moreover, each subset of the nodes of any simple symmetric graph which satisfies conditions (a) and (b) is called a **kernel** of that graph. (See [**1**] for an exposition of graph-theoretic concepts.)

It is clear that each solution of the South American problem interpreted in terms of G is a kernel of G, and conversely: A sequence of countries is a solution of the South American problem if and only if the corresponding set of nodes is a kernel of G.

Our next step is to determine the set of all kernels of G. For this purpose we will use the following result from graph theory: *A subset of the nodes of a simple graph is a kernel of that graph if and only if this subset is a maximal internally stable set.* (In terms of our game, all this says is that any maximal sequence of countries no two of which are adjacent will be a solution.) The reason why this characterization is useful is that there exists an effective algorithm (based on Boolean arithmetic) for obtaining all maximal internally stable sets of a given graph; see e.g., Deo [**2**; p. 170].

The algorithm goes like this: Let ϕ denote a formal sum $\Sigma\, ij$ where each pair i, j represents a pair of adjacent nodes of the graph. Now interpret sum and product as in a Boolean algebra, and use the laws of Boolean arithmetic to express the complement ϕ' as a sum of products of complements of nodes. The maximal internally stable sets of the graph are in a one-to-one correspondence with the terms of ϕ' written in this form: each term corresponds to the set of nodes not appearing in the particular term. Implementation of this algorithm yields the following set Π of maximal internally stable sets (i.e., kernels) of G:

(2, 4, 7, 9, 11, 13)	(2, 4, 6, 12)	(2, 5, 8, 11, 13)	(3, 5, 7, 12)
(2, 4, 7, 12)	(2, 4, 6, 10, 13)	(2, 5, 8, 12)	(3, 5, 8, 12)
(2, 4, 7, 10, 13)	(2, 5, 7, 12)	(3, 6, 12)	(3, 5, 7, 10, 13)
(2, 4, 8, 11, 13)	(2, 5, 7, 9, 11, 13)	(3, 6, 9, 11, 13)	(3, 5, 8, 11, 13)
(2, 4, 8, 12)	(2, 5, 7, 10, 13)	(3, 6, 10, 13)	(1, 7, 9)
(2, 4, 6, 9, 11, 13)		(3, 5, 7, 9, 11, 13)	

Let us inspect for a moment the set Π. We know that any solution of the South American game includes moves of both players. Therefore, it is trivial that an odd number of admissibly colored countries yields a win for A. Furthermore, we see that there are indeed elements with an odd number of nodes in Π (Silverman knew that: his solution is the element $(1,7,9) \in \Pi$) as well as elements with an even number of nodes. Since the smallest elements of Π consist of 3 nodes, and the largest elements of Π include 6 nodes, we can see that a solution is a winning solution for A if and only if the number of countries in that solution is either 3 or 5, while a solution is a winning solution for B if and only if the number of countries in that solution is either 4 or 6.

Now that we have found a method which, in a quite simple way, provides the set of all solutions of the South American game, we can address Silverman's problem proper: to determine all countries which have the property that if A chooses any of them on his first move, he will win regardless of the answers of B. To formalize this problem, we will define a node j in the game graph G as a **winning node for A** if and only if (a) there exists a solution for A in which the node (country) j is chosen by A on his first move, and (b) independent of countermoves of B, A chooses the last country. We will now show, in answer to Silverman's question, that *the winning nodes for* A *in the South American game are Brazil, Surinam and Bolivia.*

	Solutions leading to a win for A		Solutions leading to a win for B	
j	L_3^j	L_5^j	L_4^j	L_6^j
$j=1$	1, 7, 9	—	—	—
$j=2$	—	2, 4, 6, 10, 13	2, 4, 6, 12	2, 4, 6, 9, 11, 13
	—	2, 4, 7, 10, 13	2, 4, 7, 12	2, 4, 7, 9, 11, 13
	—	2, 4, 8, 11, 13	2, 4, 8, 12	—
	—	2, 5, 7, 10, 13	2, 5, 7, 12	2, 5, 7, 9, 11, 13
	—	2, 5, 8, 11, 13	2, 5, 8, 12	—
$j=3$	—	3, 5, 7, 10, 13	3, 5, 7, 12	3, 5, 7, 9, 11, 13
	—	3, 5, 8, 11, 13	3, 5, 8, 12	—
	3, 6, 12	3, 6, 9, 11, 13	3, 6, 10, 13	—
$j=4$	—	4, 2, 6, 10, 13	4, 2, 6, 12	4, 2, 6, 9, 11, 13
	—	4, 2, 7, 10, 13	4, 2, 7, 12	4, 2, 7, 9, 11, 13
	—	4, 2, 8, 11, 13	4, 2, 8, 12	—
$j=5$	—	5, 2, 7, 10, 13	5, 2, 7, 12	5, 2, 7, 9, 11, 13
	—	5, 2, 8, 11, 13	5, 2, 8, 12	—
	—	5, 3, 7, 10, 13	5, 3, 7, 12	5, 3, 7, 9, 11, 13
	—	5, 3, 8, 11, 13	5, 3, 8, 12	—
$j=6$	6, 3, 12	6, 3, 9, 11, 13	6, 3, 10, 13	—
	—	6, 2, 4, 10, 13	6, 2, 4, 12	6, 2, 4, 9, 11, 13
$j=7$	7, 1, 9	—	—	—
	—	7, 2, 4, 10, 13	7, 2, 4, 12	7, 2, 4, 9, 11, 13
	—	7, 2, 5, 10, 13	7, 2, 5, 12	7, 2, 5, 9, 11, 13
	—	7, 3, 5, 10, 13	7, 3, 5, 12	7, 3, 5, 9, 11, 13
$j=8$	—	8, 2, 4, 11, 13	8, 2, 4, 12	—
	—	8, 2, 5, 11, 13	8, 2, 5, 12	—
	—	8, 3, 5, 11, 13	8, 3, 5, 12	—
$j=9$	9, 1, 7	—	—	—
	—	9, 3, 6, 11, 13	—	9, 2, 5, 7, 11, 13
	—	—	—	9, 2, 4, 6, 11, 13
	—	—	—	9, 2, 4, 7, 11, 13
	—	—	—	9, 3, 5, 7, 11, 13
$j=10$	—	10, 3, 5, 7, 13	10, 3, 6, 13	—
	—	10, 2, 4, 6, 13	—	—
	—	10, 2, 4, 7, 13	—	—
	—	10, 2, 5, 7, 13	—	—
$j=11$	—	11, 2, 4, 8, 13	—	11, 2, 4, 6, 9, 13
	—	11, 2, 5, 8, 13	—	11, 2, 4, 7, 9, 13
	—	11, 3, 5, 8, 13	—	11, 2, 5, 7, 9, 13
	—	11, 3, 6, 9, 13	—	11, 3, 5, 7, 9, 13
$j=12$	12, 3, 6	—	12, 2, 4, 6	—
	—	—	12, 2, 4, 7	—
	—	—	12, 2, 4, 8	—
	—	—	12, 2, 5, 7	—
	—	—	12, 2, 5, 8	—
	—	—	12, 3, 5, 7	—
	—	—	12, 3, 5, 8	—
$j=13$	—	13, 3, 6, 9, 11	13, 3, 6, 10	—
	—	13, 2, 4, 6, 10	—	13, 2, 4, 6, 9, 11
	—	13, 2, 4, 7, 10	—	13, 2, 4, 7, 9, 11
	—	13, 2, 4, 8, 11	—	13, 2, 5, 7, 9, 11
	—	13, 2, 5, 7, 10	—	13, 3, 5, 7, 9, 11
	—	13, 2, 5, 8, 11	—	—
	—	13, 3, 5, 7, 10	—	—
	—	13, 3, 5, 8, 11	—	—

FIGURE 2

Suppose that A starts a play with the coloring of an arbitrary node j. A's choice induces some subfamily of the set Π, namely the family of all solutions that contain the node j. This subfamily, L^j, can be decomposed according to the length of the solutions:

$$L^j = L^j_3 \cup L^j_5 \cup L^j_4 \cup L^j_6,$$

where L^j_u ($u = 3,4,5,6$; $j = 1,\ldots,13$) may be empty for some u and j. The partitions of Π in the respective L^j_u's can be found in FIGURE 2.

Suppose $j = 1$. An inspection of FIGURE 2 shows that the families L^1_4, L^1_5 and L^1_6 are all empty — that is, there are no solutions for B which include the node $j = 1$, and there is no solution for A which includes the node $j = 1$ *and* consists of 5 nodes. The family L^1_3 of solutions for A has only one member. Therefore, B has to answer with a node in that member, and loses. It follows that $j = 1$ is a winning node for A. (Since $j = 1$ represents Brazil, this is the solution given by Silverman.)

Now suppose, for a given opening move j, that there exists at least one node which is an element of some solution for B but not an element of any solution for A. Then B may answer A's first move with such an element and win. This is what happens for the opening nodes $j = 2,4,5,7,8,9,11,12$ (see FIGURE 2). (For instance, if A opens with 2, then B can respond with 9 and win.) It follows at once that none of these eight nodes is a winning node for A.

There remain the cases $j = 3,6,10,13$ for which B is unable to force a win by his response to A's opening move. Suppose that A starts a given play with any of these nodes. B answers A's j ($j = 3,6,10,13$) with an appropriate node that is included in some solution for B. The ordered pair ⟨first move of A, answer of B⟩ determines a certain subset of kernels which are solutions of A. From the nodes of this subset A has to choose a further move. Now, the resulting ordered triple specifies in turn a subfamily of solutions for B. According to the maximality condition, B wins if there exists some node in the later subfamily which is not an element of any further solution for A; otherwise, A wins.

We leave it to the reader to verify by means of FIGURE 2 that B wins if A starts with $j = 6$ or $j = 13$. (For instance, if A opens with $j = 6$, B can respond with $j = 13$, and can win regardless of A's response.) However, A wins if his first move is $j = 3$, or $j = 10$. Therefore, Surinam ($j = 3$) and Bolivia ($j = 10$) are, in addition to Brazil, winning countries for A.

Variations and extensions

Games like Nim and TacTix are often played in the so-called ***misère*** form in which the definition of winner and loser are reversed. In a misère game, each player attempts to force his opponent to take the last stone. A straightforward application of the preceding methods can be used to show that Argentina is the unique winning opening move for the *misère* version of this game.

This example points to an interesting but as yet open question: Under what conditions is the set K of nodes that win both the standard and misère versions of an irregular TacTix-type game non-empty?

We mentioned above that the South America problem is a member of a restricted class of the irregular TacTix-type games. This restriction is caused only by the rules of the game not by the nature of the graph underlying the game. It follows that the kernel method can be applied to any TacTix-type game with suitable rules: It provides an effective algorithm for the complete analysis of such games. The interested reader may want to use it to analyze a coloring game on the map of Africa or Europe.

References

[1] C. Berge, Graphs and Hypergraphs, North Holland, Amsterdam, 1973.

[2] N. Deo, Graph Theory with Applications to Engineering and Computer Science, Prentice-Hall, Englewood Cliffs, New Jersey, 1974.

[3] R. Epstein, The Theory of Gambling and Statistical Logic, Academic Press, New York, 1967.

[4] M. Gardner, Cram, crosscram and quadraphage: new games having elusive winning strategies. Mathematical games, Scientific American, February 1974, pp. 106–108.

[5] D. Silverman, Your Move, McGraw-Hill, New York, 1971.

NOTES

The Power of Voting Blocs: An Example

PHILIP D. STRAFFIN JR.
Beloit College

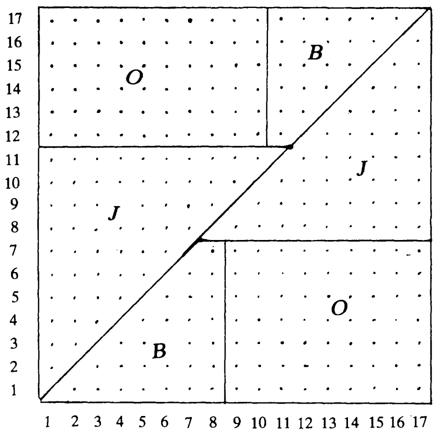
How does one measure power in a voting situation? A mathematical power index proposed by Lloyd Shapley and Martin Shubik in [3] has found wide favor among mathematicians and social scientists. In this note, I wish to use this index and some elementary game theory to analyze a particular voting situation, illustrative of a class of voting problems.

The Shapley-Shubik power index is calculated as follows. Assume that voters one by one join a coalition in support of a proposal. The voter who, upon joining the coalition, changes the coalition from a losing coalition into a winning coalition is called **pivotal.** A voter's Shapley-Shubik power index is simply his probability of being pivotal, assuming in the absence of other information that all orders of coalition formation are equally likely. The Shapley-Shubik index is thus intuitively pleasing, and easy to calculate at least in simple cases. It is also supported by an elegant axiomatic characterization (see [1]). The problem to which I wish to apply the index concerns the distribution of power in the county government of Rock County, Wisconsin.

Rock County, in southern Wisconsin, is dominated by the two cities of Janesville (population 46,000) and Beloit (population 36,000). There is often considerable rivalry between the two cities. The remainder of the county consists of small towns and rural areas. The county is governed by a Board of County Supervisors consisting of 40 members, elected from districts roughly equal in population. 11 supervisors are from the city of Beloit, 14 are from Janesville, 15 from town and rural areas. Historically, the supervisors from each city have been quite independent of one another in philosophy and voting behavior. Bloc voting by the supervisors from Beloit, or from Janesville, has not developed. I do not know about the situation in Janesville, but in Beloit there has been considerable unhappiness among city officials over this lack of cohesiveness. Surely Beloit would wield more influence if its delegation would agree to vote as a bloc.

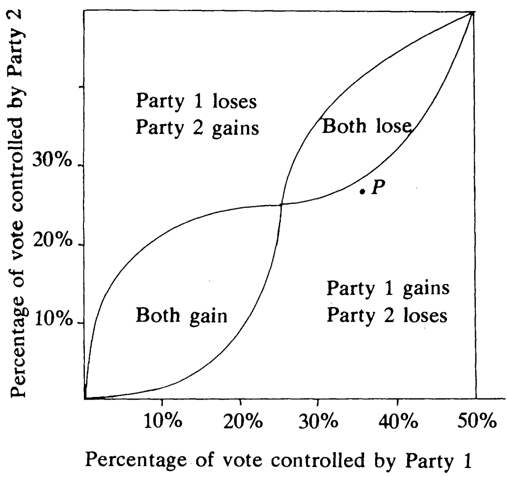
We can analyze this situation by using the Shapley-Shubik power index to calculate the total power of Beloit's eleven supervisors if they vote independently, and if they organize as a bloc. In the first case, each supervisor will have 1/40 of the total power, and Beloit's eleven together will have 11/40 or $27\frac{1}{2}\%$. In the second case, there are effectively 30 voters: 29 independent supervisors, and the Beloit bloc casting 11 votes. Since 21 votes are needed to pass a measure, Beloit will pivot if it joins a coalition 11th through 21st, i.e., 11/30 of the time. Beloit will have 11/30 or $36\frac{1}{2}\%$ of the power, a considerable increase. Janesville's supervisors, who had $14/40 = 35\%$ of the power before Beloit organized, would have $14/29 \cdot 19/30 = 30\frac{1}{2}\%$ of the power after Beloit organizes.

The problem with this scenario is, of course, that if Beloit's supervisors organized as a bloc, there would be considerable pressure for Janesville's supervisors to organize also. If that happened, we would have a game of 17 voters: 15 casting a single vote, Beloit casting 11, and Janesville casting 14. We can compute the Shapley-Shubik power indices for this game by counting the lattice points in the regions labeled B, J and O in FIGURE 1. A point (x, y) in this figure represents a voting coalition whose xth member in order of joining is Beloit and whose yth member is Janesville. The regions B, J, O represent points where Beloit, Janesville or others, repectively, are pivotal. This figure shows that



The Shapley-Shubik power index if Beloit and Janesville vote as blocs.

FIGURE 1



Gain or loss of power if both parties adopt bloc voting. Beloit–Janesville status is at point *P*.

FIGURE 2

Janesville pivots 100/272 of the time, for 37% of the power, while Beloit pivots 49/272 of the time for 18% of the power. In other words, if Janesville also organizes, Beloit is considerably worse off than it was at the status quo.

We can picture these results as a two-person, non-constant-sum game between Beloit and Janesville, with payoffs given by the total power of each city's supervisors:

		Janesville	
		$\bar{J}$ doesn't organize	J organizes
Beloit	$\bar{B}$ doesn't organize	$27\frac{1}{2}$ 35	20 52
	B organizes	$36\frac{1}{2}$ $30\frac{1}{2}$	18 37

Notice that Janesville will prefer to organize regardless of what Beloit does, and that once Janesville organizes, Beloit is actually better off *not* organizing. The game has a unique stable equilibrium outcome at $\bar{B}J$, with Beloit at a serious disadvantage. As long as the game remains at status quo $\bar{B}\bar{J}$, Beloit should be very happy not to rock the boat.

In practice, the difference between payoffs 20 vs. 18 for Beloit, or 35 vs. 37 for Janesville, is probably not perceivable. Hence it might be better to model the game qualitatively as:

		Janesville	
		$\bar{J}$	J
Beloit	$\bar{B}$	2 2	1 3
	B	3 1	1 2

where we assign higher numbers to preferred outcomes.

The natural equilibrium of this game is at BJ with Beloit at a serious disadvantage. However, it is within Beloit's power to encourage the status quo at $\bar{B}\bar{J}$ by (1) not organizing as long as Janesville doesn't, and (2) guaranteeing to organize if Janesville should. On the other hand, if the outcome should move to BJ, there is no way for Beloit to move it back to $\bar{B}\bar{J}$ — the change would be irreversible. Perhaps Beloit's supervisors are being canny in their uncooperative behavior, instead of just stubbornly independent. In any case, their independence may be serving Beloit well.

Similar situations arise frequently in other settings, for instance in political systems with two major parties and a number of minor parties, or in a corporation with two large stockholders and many small ones. If we assume that the number of minor parties is very large, with each one casting few votes, we can use analytic techniques on the problem, as is done elegantly by Shapley in [**2**]. Shapley shows that whether parties will gain or lose by voting as a bloc depends in a sophisticated way on the percentages of total votes controlled by each party. The results are shown in FIGURE 2. If Party 1 is Janesville, and Party 2 Beloit, the example of this paper is located at point P in the figure.

References

[1] R. D. Luce and H. Raiffa, Games and Decisions, Wiley, New York, 1957.

[2] L. S. Shapley, Values of Large Games, III: A Corporation with Two Large Stockholders, RM–2650–PR, The Rand Corporation, Santa Monica, 1961.

[3] L. S. Shapley and M. Shubik, A method for evaluating the distribution of power in a committee system, American Political Science Review, 48 (1954) 787–792.

[4] P. D. Straffin, Power Indices in Politics, MAA Modules in Applied Mathematics, Cornell University, Ithaca, 1976.

Compact and Connected Spaces

RICHARD JOHNSONBAUGH

Chicago State University

Various results in topology that make use of the concepts of compactness or connectedness may be unified by a formulation of the following sort: If $\mathcal{U}$ is a certain type of open cover of a space X, then X itself is a member of $\mathcal{U}$. For example, if f is a real-valued continuous function on X let $\mathcal{U}$ be the collection of open sets U of X such that f(U) is bounded. If X is compact we may easily show that X itself is in $\mathcal{U}$, thus concluding that f is bounded on X. Or again, for a real-valued continuous function f which is never zero on X let $\mathcal{U}$ be the collection of open sets of X on which f has constant sign. For a connected space X the intermediate value theorem is equivalent to the statement that X is a member of $\mathcal{U}$. Further examples of this approach may be obtained by thinking through, in the light of our definitions, the somewhat similar proofs usually given for compactness and for connectedness of a closed interval in the real line.

In this note we will show how compact and connected spaces may be developed in parallel ways in terms of covers. This leads to an efficient characterization of spaces that are simultaneously compact and connected.

We begin with compactness. If f is a real-valued continuous function on a compact space X and $\mathcal{U}$ is the collection of open subsets of X on which f is bounded, then $\mathcal{U}$ is, as we have already noted, an open cover of X. This particular open cover $\mathcal{U}$ has the property that if $U, V \in \mathcal{U}$, then $U \cup V \in \mathcal{U}$. In this case we say that $\mathcal{U}$ is **strongly finitely additive.** If we use compactness to produce a finite subcover $\{U_1, \ldots, U_n\}$ of $\mathcal{U}$, then f is bounded on $U_1 \cup \cdots \cup U_n = X$; thus $X \in \mathcal{U}$. This behavior characterizes compact spaces: *A space X is compact if and only if every strongly finitely additive open cover of X contains X.* A similar result appears in [**1**, p. 2].

To prove this, suppose that X is compact. Let $\mathcal{U}$ be a strongly finitely additive open cover of X. Then $\mathcal{U}$ contains a finite subcover $\mathcal{U}_f$. By finite additivity, $X = \cup \mathcal{U}_f \in \mathcal{U}$. Conversely, suppose that every strongly finitely additive open cover of X contains X. Let $\mathcal{U}$ be any open cover of X. Let $\mathcal{V}$ be the collection of open subsets V of X such that V can be covered by a finite subcollection of $\mathcal{U}$. Then $\mathcal{V}$ is a strongly finitely additive open cover of X. Thus $X \in \mathcal{V}$ and hence X is compact and our assertion is justified.

For connected spaces an analogous analysis based on the second example of the introduction suggests the following definition: a family $\mathcal{S}$ of sets is a **weakly infinitely additive** family if, whenever a subfamily $\{A_\alpha\}$ of $\mathcal{S}$ has non-void intersection, then $\cup A_\alpha \in \mathcal{S}$. A proof that a space is connected if and only if every weakly infinitely additive open cover of X contains X follows easily from generalizing this second example.

Finally, we combine these two ideas to obtain a characterization of compactness and connectedness jointly. We say that a family of sets $\mathcal{S}$ is **weakly finitely additive** if, whenever $A, B \in \mathcal{S}$ with $A \cap B$ non-void, we have $A \cup B \in \mathcal{S}$.

THEOREM. *A space X is compact and connected if and only if every weakly finitely additive open cover of X contains X.*

Proof. The sufficiency of the condition is a straightforward consequence of our previous remarks. So suppose that X is compact and connected. Let $\mathcal{U}$ be a weakly, finitely additive open cover of X. We may assume that each member of $\mathcal{U}$ is non-void. Since X is compact, there exists a finite subcover $\{U_1, \dots, U_n\}$ of $\mathcal{U}$. We argue by induction on n that $X \in \mathcal{U}$. The case $n = 1$ is obvious. Suppose the statement is true for $n-1$ and that we have a finite subcover $\{U_1, \dots, U_n\}$ of $\mathcal{U}$. Now U_1 meets U_i for some i, for otherwise $\{U_1, U_2 \cup \cdots \cup U_n\}$ would form a separation of the connected space X. We may assume $i = 2$. Since U_1 meets U_2, $U_1 \cup U_2 \in \mathcal{U}$. Thus $\{U_1 \cup U_2, U_3, \dots, U_n\}$ is a subcover of $\mathcal{U}$ containing $n-1$ sets. By induction $X \in \mathcal{U}$.

I wish to thank the editors, the referee, and Professor Michael Sullivan for their helpful suggestions concerning this note.

Reference

[1] K. Kuratowski, Topology, vol. II, Academic Press, New York, 1968.

A Nonparametric Model for Series Competitions

LOUIS G. VARGO
University of Missouri-Columbia

Imagine that two tennis players have decided to play a series of games to test their endurance as well as their skill. The first player to win 100 games wins the series. Each player knows nothing of the other's capabilities, so that neither they nor we can estimate the probabilities of game outcomes. They wish to know how many games they may expect to play and turn to us for advice. We may remember the recent paper by Groeneveld and Meeden [**1**] in which a shorter version (4 game wins decided the series) of such competitions was discussed. Their basic conclusion was that in the cases of baseball, hockey and basketball series, two game-outcome probability estimates are required in order to obtain satisfactory statistical agreement between the model and the historical data. Our tennis problem is different in two ways: the series is much longer and we have no data.

In [2] we find a treatment of the general n-games-to-win series, but again the model assumes an estimable probability of, say, player A winning the first game, and further, assumes that this probability holds for all following games. This model is not suited to answering the tennis question. For reference and comparison purposes however, we write their probability function. Let n be the number of wins required to win the series, p the probability of player A winning each game, and $q = 1 - p$. Then if the random variable X denotes the number of games in the completed series won by the series loser,

$$(1) \qquad P\{X = x\} = \binom{n+x-1}{x}(p^n q^x + q^n p^x), \quad \text{for} \quad x = 0, 1, 2, \ldots, (n-1).$$

Expression (1) can be obtained quite easily. If A wins the series, then A must win the last game. Thus there are $n + x - 1$ indeterminate game outcomes. The number of ways with distinct order that x of these games were won by B is $\binom{n+x-1}{x}$. Each of these ways (together with the final game) has a joint probability $p^n q^x$ of occurring since the game outcomes are assumed independent. Since each such series is different from all others, they are mutually exclusive events. Hence $\binom{n+x-1}{x} p^n q^x$ is the probability that B won x games when A won the series. To this must be added the probability that A won x games when B won the series: this is done in the second term of (1), in which the roles of A and B and of p and q are interchanged.

We should note, before we answer the tennis question, that taking $p = 1/2$ in (1) to solve the tennis problem is quite unjustified, for $p = 1/2$ is as strong an assumption as $p = 0$, and hardly more justified. In our nonparametric model we substitute for this equal-skill hypothesis the classic assumption that all distinct things of concern are equally likely to occur. The things of concern in this problem are series of games: more precisely they are sequences of wins and losses such that the number of wins is exactly n, the number of losses is less than n, and the last element in the sequence is a win. As argued above, there are $\binom{n+x-1}{x}$ distinct sequences having exactly x losses. In the nonparametric model we assume that each of these sequences is equally likely to occur. Since

$$\sum_{x=0}^{n-1} \binom{n+x-1}{x} = \binom{2n-1}{n},$$

the nonparametric probability function is

$$(2) \qquad P\{X = x\} = \binom{n+x-1}{x}\binom{2n-1}{n}^{-1}, \quad \text{for} \quad x = 0, 1, 2, \ldots, (n-1).$$

Since our derivation of function (2) makes no reference to player A or player B, but only to the series winner and loser, a second term is not required. For contrast we should note that the probability function obtained from (1) if we were to assume $p = q = 1/2$ is

$$P\{X = x\} = \binom{n+x-1}{x} 2^{-(n+x-1)} \quad \text{for} \quad x = 0, 1, 2, \ldots, (n-1).$$

In order to answer the tennis question we need the expectation of X:

$$E(X) = \sum_{x=0}^{n-1} xP\{X = x\} = \frac{(n-1)n}{n+1}.$$

The number of games they may expect to play is found by adding to the expected number of losses, $[E(X)]_{n=100} \doteq 98.0198$, the known number of wins, namely 100. Our answer to the tennis players is "198 games."

The expression for the variance of X is

$$V(X) = E(X^2) - [E(X)]^2 = \sum_{x=0}^{n-1} x^2 \binom{n+x-1}{x}\binom{2n-1}{n}^{-1} - [E(X)]^2$$

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

If the tennis players happen to be statistically receptive, we might include the information that our answer for the expected number of games carries a standard deviation of $[\sqrt{V(X)}]_{n=100} \doteq 1.38$ game.

Since $E(X) = (n^2 - n)/(n+1) = (n-2) + 2/(n+1)$, we see that for large values of n, $E(X) \doteq n - 2$. Similarly, $V(X) \doteq 2$ when n is large. Both of these approximations would have been quite accurate for the tennis problem.

We close by comparing our results with those of the parametric $p = q = 1/2$ model. The latter assumption of equal player skills entails a prediction of a 189-game tennis series. The standard deviation of this prediction is 7.86 games. These calculations involving the incomplete beta function were performed in **[2]**.

References

[1] R. A. Groeneveld and G. Meeden, Seven game series in sports, this MAGAZINE, 48 (1975) 187–192.

[2] V. R. R. Uppuluri and W. J. Blot, A Probability Distribution Arising in a Riff-Shuffle, in Random Counts in Scientific Work, vol. 1, Random Counts in Models and Structures, ed. by G. P. Patil, The Pennsylvania State University Press, University Park and London, 1970.

Quantification of Greek Variables in Calculus

TERRY A. MCKEE
Wright State University

Proofs involving limits typically require proving a statement beginning with $\forall\varepsilon$, i.e., showing something true for all positive numbers ε. Yet very often (for instance in proving continuity) it is sufficient to consider only ε from a sequence of positive numbers converging to zero. Similarly, proofs may involve asserting a statement beginning $\exists\delta$, i.e., asserting the existence of a positive number δ with a certain property. Yet very often this property will also be possessed by all positive numbers less than the exhibited δ.

In this paper we will investigate the frequent occurrence of these phenomena: being able to require less while showing $\forall\varepsilon\ldots$ and to conclude more from asserting $\exists\delta\ldots$. We will see that such phenomena result from the special way in which the quantifiers $\forall$ and $\exists$ tend to be used with Greek variables in calculus.

The ideas we want to discuss are logical in nature, and so we must begin by considering the language in which calculus is developed. The traditional (informal) logical language for calculus uses (Latin) variables such as x and y for real numbers and customary symbols for functions and relations (e.g., f and g for arbitrary functions with special symbols for addition, absolute value, less than, etc.). The logical symbols we will use are $\wedge$ (and), $\vee$ (or), $\neg$ (not), $\rightarrow$ (if, then), $\leftrightarrow$ (if and only if), and the quantifiers $\forall$ (for all) and $\exists$ (for some).

Greek variables such as ε and δ are customarily used in a topologically-motivated manner. Specifically, they are restricted to being positive reals and to occur only in the context $\ldots < \varepsilon$, where the inequality is preceded by a term involving only function symbols and (Latin) variables. For instance, the following are expressions of the statements that f is, respectively, continuous and uniformly continuous:

$$\forall x\, \forall \varepsilon\, \exists \delta\, \forall y[|x-y|<\delta \rightarrow |f(x)-f(y)|<\varepsilon] \tag{1}$$

$$\forall \varepsilon\, \exists \delta\, \forall x\, \forall y[|x-y|<\delta \rightarrow |f(x)-f(y)|<\varepsilon]. \tag{2}$$

Note that the logical symbols $\rightarrow$ and $\leftrightarrow$ can be eliminated by additional uses of $\wedge$, $\vee$, and $\neg$; i.e., $A \rightarrow B$ can be written as $\neg A \vee B$, and $A \leftrightarrow B$ as $(\neg A \vee B) \wedge (A \vee \neg B)$. We will say that a variable occurs **positively** (respectively, **negatively**) in an expression if and only if, after eliminating $\rightarrow$ and $\leftrightarrow$ from the expression, the variable is acted on by exactly an even (respectively, odd) number of negation symbols. For instance, ε occurs only positively and δ only negatively in the expressions (1) and (2). (A variable may occur several times in the same expression and so may occur both positively and negatively.)

We will call an occurrence of the quantifier $\forall$ (respectively, $\exists$) **privileged** in an expression when it is immediately followed by a Greek variable which occurs only positively (respectively, negatively) in the rest of the expression. Thus, each $\forall$ or $\exists$ immediately followed by ε or δ in (1) and (2) is privileged. (In fact, there is a sense in which quantifiers of Greek variables in calculus usually are privileged. The rather technical reason for this is shown in references **[2]** and **[3]** and Section 5 of the survey article **[1]**.) With a little practice, privileged quantifiers become quite easy to spot. We are calling them "privileged" because we will see that they enjoy nicer properties than other quantifiers.

The quantifiers "for arbitrarily small" and "for sufficiently small" are also frequently encountered in calculus. Although definable in terms of $\forall$ and $\exists$ (and $<$), these new quantifiers are frequently easier to use. Suppose $A(\varepsilon)$ is an expression in which ε occurs unquantified. By saying that $A(\varepsilon)$ is true **for arbitrarily small** ε, we will mean that for each positive real r there is some positive ε less than r such that $A(\varepsilon)$ is true; i.e., that $A(\varepsilon)$ is true (at least) for the elements of some sequence of positive reals converging to zero. By saying that $A(\varepsilon)$ is true **for sufficiently small** ε, we will mean that for some positive real r, $A(\varepsilon)$ is true for each positive ε less than r; i.e., that $A(\varepsilon)$ is true (at least) on some real interval of the form $(0, r)$. We can now state a substantial privilege enjoyed by privileged quantifiers.

THEOREM. *Each privileged quantifier $\forall$ can be equivalently replaced by "for arbitrarily small," and each privileged quantifier $\exists$ can be equivalently replaced by "for sufficiently small."*

For instance, expression (2) above can be rewritten: for arbitrarily small ε and for sufficiently small δ,

$$\forall x\, \forall y[|x-y|<\delta \rightarrow |f(x)-g(x)|<\varepsilon].$$

Thus, instead of showing something for each and every ε, we need only show it for, say, ε which are reciprocals of natural numbers. (And the δ produced can also be assumed to be a reciprocal of a natural number.) To prove the theorem, we need the following two lemmas.

LEMMA 1. *Suppose the variable ε occurs only positively in $A(\varepsilon)$ and that $A(\varepsilon)$ holds when ε assumes a particular positive real value r. Then $A(\varepsilon)$ will hold whenever ε assumes a real value greater than r.*

While a formal proof of this lemma could be an exercise in an introductory mathematical logic course, it is too delicate to give here. We can, however, sketch what such a proof would involve. First of all, the lemma is true for the simplest possible $A(\varepsilon)$ (i.e., for expressions of the form $\ldots < \varepsilon$) simply by transitivity of $<$. The proof builds inductively from this. For instance, the lemma's truth will follow for any combination of expressions (combined by $\wedge$ or $\vee$) from its truth in the constituent expressions. Also, the quantification of a variable (other than ε) will not change the lemma's truth. In this way, the lemma can be shown to hold for all expressions in which ε occurs only positively. The following "dual" form can be proved similarly.

LEMMA 2. *Suppose the variable ε occurs only negatively in $A(\varepsilon)$ and that $A(\varepsilon)$ holds when ε assumes a particular positive real value r. Then $A(\varepsilon)$ will hold whenever ε assumes a (positive) real value less than r.*

To finish the proof of the theorem, first note that "for all" immediately implies "for arbitrarily small." So suppose $A(\varepsilon)$ is true for arbitrarily small ε, where ε occurs only positively in $A(\varepsilon)$. To show $\forall\varepsilon A(\varepsilon)$, pick any positive real number r and observe that $A(\varepsilon)$'s truth for arbitrarily small ε insures $A(\varepsilon)$'s truth for some real less than r, and so by Lemma 1, for r. For the second half, observe that "for sufficiently small" immediately implies "for some." So suppose ε occurs only negatively in $A(\varepsilon)$ and that $A(\varepsilon)$ is true for some positive r. Then Lemma 2 implies $A(\varepsilon)$'s truth for all positive reals less than r, and so $A(\varepsilon)$ will be true for sufficiently small ε. This proves the theorem.

The following chain of implications shows the relationships which always hold among these four quantifiers:

$$\text{for all} \rightarrow \text{for sufficiently small} \rightarrow \text{for arbitrarily small} \rightarrow \text{for some.}$$

As the theorem shows, the first and third (and so the first three) are interchangeable for Greek variables occurring only positively, and (similarly) the last three are interchangeable for Greek variables occurring only negatively. This contributes to the common confusion of "for sufficiently small" with "for arbitrarily small" in calculus — privileged quantifiers can be replaced by either.

This chain of implications also suggests a very surprising aspect of the theorem — $\forall$ is being replaced by a quantifier more like $\exists$, and vice versa! This sense of reversal is heightened by considering the following distributive and "semidistributive" laws which are always true of $\forall$ and $\exists$ (whether privileged or not):

$$\forall\varepsilon[A(\varepsilon)\wedge B(\varepsilon)]\leftrightarrow\forall\varepsilon[A(\varepsilon)]\wedge\forall\varepsilon[B(\varepsilon)]$$

$$\forall\varepsilon[A(\varepsilon)\vee B(\varepsilon)]\leftarrow\forall\varepsilon[A(\varepsilon)]\vee\forall\varepsilon[B(\varepsilon)]$$

$$\exists\varepsilon[A(\varepsilon)\wedge B(\varepsilon)]\rightarrow\exists\varepsilon[A(\varepsilon)]\wedge\exists\varepsilon[B(\varepsilon)]$$

$$\exists\varepsilon[A(\varepsilon)\vee B(\varepsilon)]\leftrightarrow\exists\varepsilon[A(\varepsilon)]\vee\exists\varepsilon[B(\varepsilon)].$$

The quantifier "for arbitrarily small" can be seen to satisfy the last two laws, exactly the same laws as $\exists$, while "for sufficiently small" satisfies the first two, exactly as $\forall$. So the theorem allows replacement of a *privileged* quantifier $\forall$ by a quantifier behaving very much like $\exists$, and of a *privileged* quantifier $\exists$ by one behaving very much like $\forall$.

COROLLARY. *Privileged quantifiers distribute over both $\wedge$ and $\vee$.*

In other words, privileged quantifiers obey all four of the above laws with double arrows in each! To prove the distributivity of $\forall$ over $\vee$, first suppose $\forall\varepsilon[A(\varepsilon)\vee B(\varepsilon)]$ where the $\forall$ is privileged. Thus, $A(\varepsilon)\vee B(\varepsilon)$ is true for arbitrarily small ε. Since "for arbitrarily small" distributes over $\vee$ (just as $\exists$ does), we have that either $A(\varepsilon)$ holds for arbitrarily small ε or $B(\varepsilon)$ holds for arbitrarily small ε. Hence by the theorem, we have either $\forall\varepsilon A(\varepsilon)$ or $\forall\varepsilon B(\varepsilon)$, and so $\forall\varepsilon A(\varepsilon)\vee\forall\varepsilon B(\varepsilon)$ holds. The distributivity of $\exists$ over $\wedge$ follows similarly.

References

[1] J. A. Makowsky, Topological model theory, Proceedings of the CIME Meeting on Model Theory, Bressanone, Italy (1975), to appear.

[2] T. A. McKee, Sentences preserved between equivalent topological bases, Z. Math. Logik Grundlagen Math., 22 (1976) 79–84.

[3] M. Ziegler, A language for topological structures which satisfies a Lindström Theorem, Bull. Amer. Math. Soc., 82 (1976) 568–570.

Finding Truth in Lending

JOHN E. MORRILL
DePauw University

In 1968 the United States Congress passed and the President signed an act, ([**2**]), of which Title I has been generally called the Truth-in-Lending Law. Among the provisions of this part of the act is the requirement that the "costs" of certain installment loan contracts be described in terms of an "annual percentage rate". One intent of this regulation is to require creditors to provide a simple measure of the cost of a loan so that potential borrowers can have a reasonably easy way of comparing alternative loan opportunities. Finding the required annual percentage rate is not, in general, an easy problem; and the purpose of this note is to show that in some common loan situations, this rate may be found using a familiar algorithm often studied in elementary calculus — the Newton–Raphson Method.

The definition of the annual percentage rate can best be understood by considering the following simple model. There are more complex models which must be considered to answer all annual percentage rate questions, but the one we shall use is illustrative of very common kinds of installment loans, e.g., automobile loans and home mortgage loans. The notation which we use in this model is as follows:

A = the present value of a financial obligation to be repaid in equal installments,

R = the periodic installment payment made at the end of each payment period,

m = the number of payment periods in one year,

n = the total number of installment payments in the term of the loan contract, and

i = the annual percentage rate.

Now the model for the loan transaction is provided by the requirements of the Truth-in-Lending Law which state that each payment R is considered to consist of two portions. The first portion is an interest (or finance) payment in the amount of i/m of the unpaid loan balance or outstanding principal at the beginning of that mth of a year. The second portion, the remainder of R, is a partial repayment of the unpaid loan balance which then reduces that unpaid balance upon which interest is charged in the next payment interval. (For example, if $i = 18\%$ and $m = 12$, the interest charge each month would be $1\frac{1}{2}\%$ of the unpaid balance, and the remainder of the installment payment would be used to reduce the loan balance.) In the language of compound interest theory i is a nominal annual rate of interest, and i/m is the effective rate of interest per mth of a year.

One way to describe the relationship among the parameters of this model is through the following recursion relation: If A_t is the unpaid (principal) balance of the loan just after the tth payment has been made, then

$$(1)\qquad A_t - \left(R - \frac{i}{m}A_t\right) = A_{t+1}, \qquad t = 0, 1, 2, \ldots, n-1,$$

where $A_0 = A$, and $A_n = 0$, since the n payments of R are defined to completely discharge the loan obligation. The relation (1) leads directly to

$$(2)\qquad A\left(1+\frac{i}{m}\right)^n = R\left(1+\frac{i}{m}\right)^{n-1} + R\left(1+\frac{i}{m}\right)^{n-2} + \cdots + R;$$

and multiplying each side by $(1+i/m)^{-n}$, to

$$(3)\qquad A = R\left(1+\frac{i}{m}\right)^{-1} + R\left(1+\frac{i}{m}\right)^{-2} + \cdots + R\left(1+\frac{i}{m}\right)^{-n}.$$

Equation (3) is the familiar "equation of value" of compound interest theory which states that A is the present value of n payments of R made the end of each mth of a year at the (compound) interest rate i/m per mth of a year. Readers who wish to learn more about compound interest theory should see [**1**] or other texts on the mathematics of compound interest. Also in [**1**], pp. 277–278, the reader may find a list of articles which deal with the interest rate problem and other algorithms for finding the rate of interest.

The problem of finding the annual percentage rate in this model is then: Given A, R, m, and n; find i. We shall assume hereafter that $0 < A/R < n$, and hence $i > 0$, which is the situation in the "real world." From equation (2) we see that this problem is equivalent to solving an nth degree polynomial in i. This certainly suggests the use of an iterative technique such as the Newton–Raphson Method. Instead of attacking (2) or (3) directly however, we shall first simplify (3), by letting $v = (1+(i/m))^{-1}$, and thus transform (3) to $A = Rv + Rv^2 + \cdots + Rv^n$. Observing that the right hand member of this equation is a geometric series, and summing it, we have $R(v - v^{n+1})/(1-v) - A = 0$, which is of the form

$$f(v) \equiv v^{n+1} - \left(1+\frac{A}{R}\right) v + \frac{A}{R} = 0. \tag{4}$$

Hence, the problem of finding i is reduced to solving (4) for v in the interval (0, 1). (This follows because of the restriction that $i > 0$.) Analysis of $f'(v)$ and $f''(v)$ reveals, since $0 < A/R < n$, that $f(v)$ has the graph shown in Figure 1. That is, there is a minimum for f in (0, 1) at $v_{\min} = ((1+A/R)/(1+n))^{1/n}$, and a unique root of $f(v) = 0$ in the interval $(0, v_{\min})$. (That $f(v_{\min}) < 0$ is quickly seen by considering $f(0), f(1)$ and $f'(v)$.) To find this root we use the standard Newton–Raphson recursion relation $v_{i+1} = v_i - [f(v_i)/f'(v_i)]$ for $i = 0, 1, 2, \ldots$, with an initial "estimate" $v_0 = (A/R)/(1+A/R)$. It is easily shown that $v_0 < v_{\min}$; and therefore, because of the concavity of $f(v)$, the successive values $v_0, v_1, v_2, \ldots$ converge to the desired root of $f(v) = 0$. Other initial "estimates" could of course be used, but this is a particularly simple one. Finally, to obtain the annual percentage rate required by the Truth-in-Lending Law, we compute $i = m((1/v) - 1)$.

As a concluding illustration, consider the practice of some financial instutions in advertising new car loan rates. Such an advertisement might state that the borrower would pay "$8 per $100 per year,"

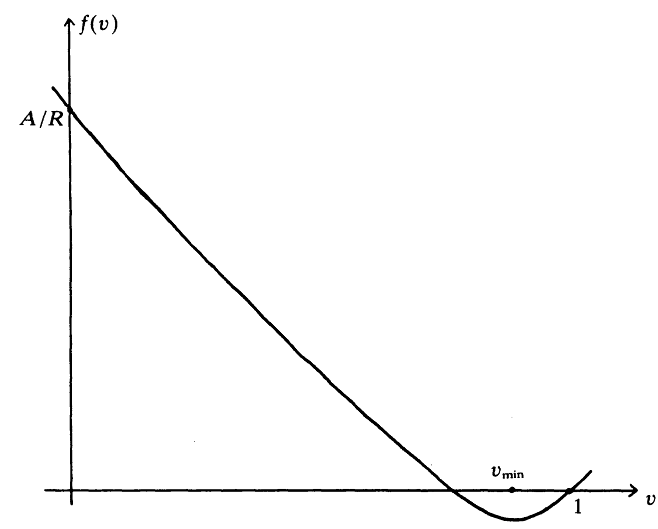


Figure 1

frequently touted as an 8% interest rate. However, what this means is that for each \$100 borrowed for one year, the borrower would repay \$108 per year divided into twelve equal monthly installments, i.e., \$9 per month. Since July 1, 1969 when the Truth-in-Lending Law became effective, the creditor has been required to state that the annual percentage rate (to two decimal places) for this transaction is 14.45%. This tells the borrower that he is paying an interest rate of about 1.2% each month on the unpaid principal balance.

References

[1] Marjorie Butcher, and Cecil Nesbitt, Mathematics of Compound Interest, Ulrich's Books, Ann Arbor, 1971.

[2] The Consumer Credit Protection Act, Public Law 90–321, 90th Congress, S·5, May 29, 1968.

Maximum Area Under Constraint

TUNG-PO LIN
California State University, Northridge

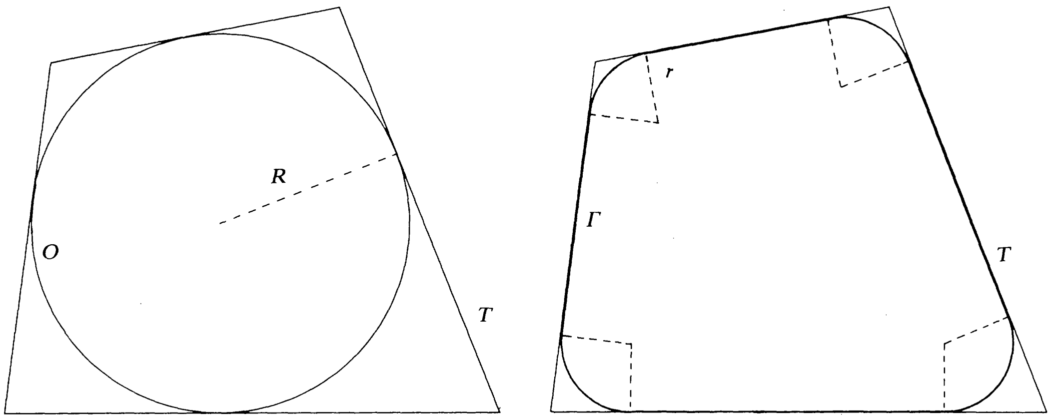
The time-honored isoperimetric problem can be given an interesting twist when additional constraints are imposed. For example, one may ask: (i) What is the maximum area of a simple closed curve contained in a given square, or triangle, when the perimeter of the curve is given? (ii) What is the maximum area-perimeter ratio of all simple closed curves contained in a given square, or triangle? Partial answers to these and related questions have appeared in the literature [**1–4**]. Recently, Garvin [**5**] asked the question (ii) above relative to an arbitrary triangular region. Scott [**6**] asked a similar question in the setting of a square lattice. In this note, we shall answer both questions completely under a more general constraint, namely, when the given region is a polygon T circumscribable on a circle. The methods used are elementary and the results are amazingly simple in terms of properly chosen parameters.

Let P be the perimeter of a polygon T circumscribable on a circle O with circumference C. In FIGURE 1(i); a quadrilateral is shown as an example. The radius R and the area S of the circle O are then given by $R = C/2\pi$ and $S = \pi(C/2\pi)^2 = C^2/4\pi$. When the polygon T is circumscribable on a circle, its area A can be computed easily as $A = RP/2 = CP/4\pi$; this is most easily seen by viewing the polygon as the union of triangles of altitude R whose bases are the sides of the polygon.

Suppose ρ is the perimeter of a simple closed curve Γ contained in the polygon T. If $\rho \leqq C$, then it is obvious that maximum area is attained when Γ assumes the shape of a circle whose radius is $\rho/2\pi$. In other words, when $0 < \rho \leqq C$, the optimal area of Γ satisfies $\alpha = \pi r^2 = \rho^2/4\pi$. Similarly, when $\rho \geqq P$, the maximum area of Γ is obviously equal to the area A of T. So in this case $\alpha = CP/4\pi$.

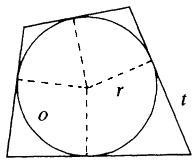
However, when $C < \rho < P$, the above conclusions are no longer valid. The optimal curve Γ will then consist of certain circular arcs together with a portion of the straight edges of the polygon T; see, for example, the heavy curve in FIGURE 1(ii). DeMar [**1**] proved that when T is a triangle, the curved portions of Γ are circular arcs of equal radii and are tangent to all straight edges. Similar arguments apply to any convex polygon.

When the given polygon T is circumscribable on a circle (e.g., triangles, squares, rhombi and many others) the formulae for the perimeter and area of the optimal curve Γ are easily obtained as follows: If we cut all the corners along the dotted lines as shown in FIGURE 1(ii), and put them together as shown in FIGURE 1(iii), we get a configuration t directly similar to that of FIGURE 1(i). Let the perimeter and area of the small polygon t be p and a respectively, and the radius, circumference, and area of the small circle o in t be r, c, s, respectively. The the perimeter ρ of the optimal curve Γ is $P - p + c$ while its area α is $A - a + s$. From the similarity of T (FIGURE 1(i)) and t (FIGURE 1(iii)) we have



(i) (ii)

In a polygon T circumscribable about a circle O (i), a simple closed curve Γ which encloses maximum area must consist of segments of the polygon joined by circular arcs of equal radii r which are tangent to the polygon (ii), in which case the "corners" fit together to form a polygon t similar to the original which is circumscribable about a small circle o of radius r (iii).



(iii)

FIGURE 1

$$p - c = (P - C)r/R = (p - C)r/(C/2\pi)$$

$$a - s = (A - S)r^2/R^2 = (CP/4\pi - C^2/4\pi)r^2/(C^2/4\pi^2) = \pi(P - C)r^2/C.$$

Thus $\rho = P - [(P - C)r/(C/2\pi)]$ and $\alpha = CP/4\pi - [\pi(P - C)r^2/C]$. By solving the perimeter equation for r,

(1) $$r = C(P - \rho)/2\pi(P - C),$$

and substituting this into the equation for area, we obtain the optimal relation between area and perimeter:

(2) $$\alpha = C(2P\rho - \rho^2 - CP)/4\pi(P - C).$$

These various bounds for the area enclosed by Γ are summarized in the following theorem and represented graphically in FIGURE 2.

THEOREM 1. *Let Γ be a simple closed curve of perimeter ρ contained in a polygon of perimeter P which is circumscribable on a circle of circumference C. The area enclosed by Γ is then bounded above by*

$$\alpha = \begin{cases} \rho^2/(4\pi) & \text{if } 0 < \rho \leqq C, \\ C(2P\rho - \rho^2 - CP)/4\pi(P - C) & \text{if } C < \rho \leqq P, \\ CP/(4\pi) & \text{if } P < \rho. \end{cases}$$

The square lattices in Scott's article [**6**] correspond to $P = 8$ and $C = 2\pi$ reducing the middle expression in α to $(16\rho - \rho^2 - 16\pi)/(16 - 4\pi)$. Silver has considered in [**4**] the more general case of oblique lattices.

In regard to question (ii) mentioned above, it is now easy to see from FIGURE 2 that α/ρ, which corresponds to the slope of the straight line joining the origin to a point in the shaded region, attains its maximum value at a point on the portion of the curve between $\rho = C$ and $\rho = P$. Since $d(\alpha/\rho)/d\rho = (\rho\alpha' - \alpha)/\rho^2$, the maximum value of α/ρ is achieved at a point on the curve where the

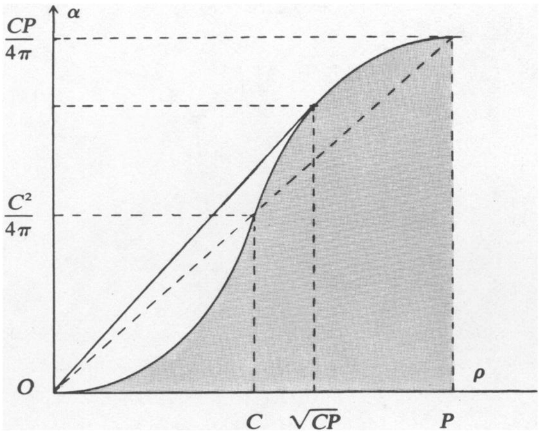


FIGURE 2

slope $\alpha' = d\alpha/d\rho$ of the curve coincides with the value α/ρ at that point. The slope of the curve $\alpha = \alpha(\rho)$ is easily found from Theorem 1 to be

$$\frac{d\alpha}{d\rho} = \begin{cases} \rho/2\pi & \text{if } 0<\rho \leqq C, \\ 2C(P-\rho)/4\pi(P-C) & \text{if } C<\rho \leqq P, \\ 0 & \text{if } P<\rho. \end{cases}$$

By comparing this formula with equation (1) and checking the other two cases directly, we see that it can be cast in the following extremely simple form: $d\alpha/d\rho = r$ for all ρ. Consequently, ***the maximum value of α/ρ occurs at a value of ρ such that $\alpha/\rho = r$.*** If we substitute into this equation the formulas (1) and (2) for r and α that hold whenever $C<\rho \leqq P$, we can obtain the following simple result: $\rho = \sqrt{CP}$. In words, the area-perimeter ratio of Γ attains its maximum when the perimeter of Γ is the geometric average of the perimeter of the polygon and the circumference of the incircle. The value of this maximum is found, by substitution of $\rho = \sqrt{CP}$ in the formula for α, to be $C\sqrt{P}/2\pi(\sqrt{P}+\sqrt{C})$. This is also, by virtue of the preceding discussion, the value of the radius of the corner arcs when α/ρ attains its maximum value. We summarize these results in the following formal statement.

THEOREM 2. *Let Γ be a simple closed curve of perimeter ρ and area α contained in a polygon of perimeter P which is circumscribable on a circle of circumference C. Then the maximum value of α/ρ is achieved when $\rho = \sqrt{CP}$, and this value is $C\sqrt{P}/2\pi(\sqrt{P}+\sqrt{C})$.*

This theorem solves the problem posed by Garvin [5] where he was concerned with triangular regions. For another special case, that of square regions, Bender [3] gave an upper bound for the area-perimeter ratio of $P/(8\sqrt{2}) \doteq 0.0884\ P$. (In Bender's article, $P = 4\sqrt{2}$.) By putting $C = \pi(P/4)$ (for the circumference of the circle inscribed in a square) into the bound given in Theorem 2, we obtain $P/[4(2+\sqrt{\pi})] \doteq 0.0663\ P$, thus confirming Scott's conjecture. (In his article $P = 8$.)

For a differential analytical proof of the result in Theorem 2 in a square region, see the solution to the "Free Plot Problem" by proposer Royes Salmon [2], which, incidentally, offers another explanation of why r is the maximum vlaue of α/ρ.

References

[1] R. F. DeMar, A simple approach to isoperimatric problems in the plane, this MAGAZINE, 48 (1975) 1–12.
[2] L. A. Graham, Ingenious Mathematical Problems and Methods, Dover, New York, 1959, pp. 29, 169–173.
[3] E. Bender, Area-perimeter relations for two dimensional lattices, Amer. Math. Monthly, 69 (1962) 742–744.
[4] M. Silver, On extreme figures admissible relative to rectuangular lattices, Pacific J. Math., 40 (1972) 451–457.
[5] A. D. Garvin, A note on DeMar's article and an epilogue, this MAGAZINE, 48 (1975) 219–221.
[6] P. R. Scott, An area-perimeter problem, Amer. Math. Monthly, 81 (1974) 884–885.

Hamiltonian Circuits: A Hierarchy of Examples

JAMES F. SMITH
Le Moyne College

MICHAEL J. QUINN
Gonzaga University

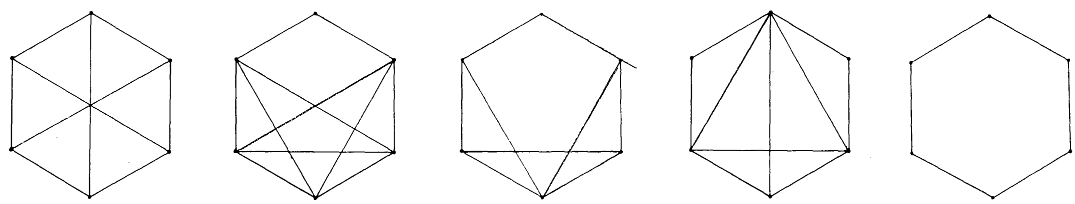
In a recent expository paper, Nash-Williams [1] lines up three sets of sufficient conditions for a graph G on n vertices ($n \geqq 3$) to be Hamiltonian, that is, to contain a closed path passing through each vertex exactly once. The conditions D, P, and C (stated below), due respectively to Dirac (1952) [2], Pósa (1962) [3], and Chvátal (1972) [4], are given in an order that is at once chronological and decreasing with respect to stringency. Both of these ordering criteria are maintained if we insert Ore's condition O (1960) [5] after that of Dirac: it is quite easy to see that $D \Rightarrow O \Rightarrow P \Rightarrow C$. (The implication $O \Rightarrow P$ is not as evident as the others; hence we offer a proof of it at the end of this note.) Our purpose here is to present a simple and convenient set of examples illustrating the strict improvement of each criterion over its predecessors.

Following Nash-Williams and recent convention, we use the term "graph" to mean "simple graph": we consider only graphs with no loops or multiple edges. Let $v(\xi)$ denote the valence (or degree) of a vertex ξ of G, and let $(v_1, v_2, \ldots, v_n)$, the n-tuple of valences of vertices of G arranged in nondecreasing order, denote the valence sequence (or degree spectrum) of G. Then the four conditions guaranteeing that a graph G on n vertices ($n \geqq 3$) be Hamiltonian are:

- D: For every vertex ξ, $v(\xi) \geqq n/2$.
- O: For every pair of nonadjacent vertices ξ and η, $v(\xi) + v(\eta) \geqq n$.
- P: For each $k < n/2$, $v_k \geqq k + 1$; however, when n is odd the last of these inequalities (which occurs for $k = (n-1)/2$) may be weakened to $v_k \geqq k$ and $v_{k+1} \geqq k + 1$.
- C: For each $k < n/2$, either $v_k \geqq k + 1$ or $v_{n-k} \geqq n - k$.

FIGURE 1 contains various Hamiltonian graphs on six vertices that illustrate the decreasing stringency of these four criteria. We include the six-cycle (i.e., the circuit graph on six vertices) among our Hamiltonian graphs as the standard example showing that none of these four criteria is necessary. We note that $n = 6$ is the smallest number of vertices for which such a unified set of examples can be devised. For $n = 5$, P and C are equivalent; for $n = 4$ or 3, all conditions are equivalent to the absence of vertices of valence less than 2.

Finally, we show, by a contrapositive argument, that $O \Rightarrow P$. Suppose that $v_k \leqq k$ for some $k < n/2$. Then G contains at least k vertices with valence k or less; we let $\xi_1, \ldots, \xi_k$ denote k such vertices. If any two of these are not adjacent, O fails. On the contrary, suppose that $\xi_1, \ldots, \xi_k$ are pairwise adjacent; then each of these vertices is adjacent to each of the other $k - 1$ of them, and



D, O, P, C | *O, P, C* | *P, C* | *C* | None

FIGURE 1

possibly to one additional vertex. There are at most k such additional vertices, which, along with $\xi_1, \ldots, \xi_k$, account for no more than $2k$ vertices of G. But $2k < n$, and therefore there is a vertex ξ' not adjacent to any of $\xi_1, \ldots, \xi_k$. Thus, $v(\xi') \leqq n-1-k$, and so O fails, since for any $i = 1, \ldots, k$, $v(\xi_i) + v(\xi') \leqq n-1$.

References

[1] C. St. J. A. Nash-Williams, Hamiltonian circuits, Studies in Graph Theory, vol. II, ed. D. R. Fulkerson, MAA Studies in Mathematics, vol. 12, 1975, pp. 301–360.

[2] G. A. Dirac, Some theorems on abstract graphs, Proc. London Math. Soc., 2 (1952) 69–81.

[3] L. Pósa, A theorem concerning Hamiltonian lines, Magyar Tud. Akad. Mat. Fiz. Oszt. Kozl., 7 (1962) 225–226.

[4] V. Chvátal, On Hamilton's ideals, J. Combinatorial Theory, Ser. B, 12 (1972) 163–168.

[5] O. Ore, Note on Hamilton circuits, Amer. Math. Monthly, 67 (1960) 55.

Equivalence of Extension Fields

Charles J. Parry

Virginia Polytechnic Institute and State University

David Perin

Center for Naval Analyses

It is obvious that one need adjoin only $\sqrt{2}$ to the rationals Q in order to find a field extension of the rationals in which both x^2-2 and x^2-8 have roots. In symbols, $Q(\sqrt{2}) = Q(\sqrt{8})$. A little experimentation soon suggests that in fact $Q(a^{1/2}) = Q(b^{1/2})$ whenever $b = ac^2$ for some c in Q. In fact it is not hard to show that $b = ac^2$ is a necessary and sufficient condition that $Q(a^{1/2}) = Q(b^{1/2})$.

Let us denote by $a^{1/n}$ any root of the polynomial $x^n - a$. If we try to extend the example of square roots to the general case we might conjecture that $Q(a^{1/n}) = Q(b^{1/n})$ if and only if $b = c^n a$ for some c in Q. However, since $Q(3^{1/3}) = Q(9^{1/3})$ but $9 \neq c^3 3$ for any $c \in Q$, we might modify our conjecture to something like the following: $Q(b^{1/n}) = Q(a^{1/n})$ if and only if $b = c^n a^i$ where i and n are relatively prime and $c \in Q$. However, further experimentation will reveal that even this conjecture is not quite right since the condition $b = c^n a^i$ is not necessary for the equality $Q(a^{1/n}) = Q(b^{1/n})$. For let $a = -3^2$, $b = -2^4 \cdot 3^2$ and $n = 8$. Now $b = 16a = (1+\sqrt{-1})^8 a$ so $b^{1/8} = a^{1/8} + \sqrt{-1}\, a^{1/8}$. Now $a^{4/8} = a^{1/2} = 3\sqrt{-1}$, so $a^{5/8} = 3\sqrt{-1}\, a^{1/8}$. Thus $b^{1/8} = a^{1/8} + \frac{1}{3} a^{5/8}$ so $Q(b^{1/8}) \subset Q(a^{1/8})$. But since $4a^{1/2} = b^{1/2}$ in the field $Q(b^{1/8})$ we may solve $b^{1/8} = a^{1/8} + \frac{1}{3} a^{5/8}$ for $a^{1/8}$ and thus $Q(a^{1/8}) \subset Q(b^{1/8})$. So in fact $Q(a^{1/8}) = Q(b^{1/8})$. However, $b \neq c^8 a^i$ for any integer i or any $c \in Q$.

We shall show below that a minor change in the modified conjecture does provide a necessary and sufficient condition. Our proof will be a direct one using only a careful study of polynomials of the form $x^n - a$ and their factors, an approach well known to beginning students of field theory. By way of comparison, advanced proofs using the Kummer theory of fields may be found in the literature (see [**2**, p. 171] or [**3**, p. 219]).

In everything that follows n will denote a positive integer greater than 1, k will denote a field of characteristic relatively prime to n, and ζ will denote a primitive nth root of unity in the algebraic closure of k. With these conventions we may now state our main result.

Theorem. *Let a and b be non-zero elements of k. Then $k(a^{1/n}) = k(b^{1/n})$ if and only if $b = a^i c^n$ for some c in $k(\zeta)$ and some integer i with $(i, n) = 1$.*

Proof. Let K denote $k(\zeta)$, and let m denote the degree of $K(a^{1/n})$ over K. Factor $X^n - a = \Pi_{i=1}^{s} g_i(X)$ as a product of monic irreducible polynomials in $K[X]$. When any root of $X^n - a$ is adjoined to K the same field $K(a^{1/n})$ is obtained. Thus each $g_i(X)$ has degree $[K(a^{1/n}): K] = m$ and so m divides n. Set $g(X) = g_1(X)$ and suppose $a^{1/n}$ and $\omega a^{1/n}$ are roots of $g(X)$ where ω is some nth root of unity in K. If $g(X) = X^m + a_1 X^{m-1} + \cdots + a_m$, then $h(X) = \omega^m g(X) - g(\omega X)$ is a polynomial in $K[X]$ of degree less than m which has $a^{1/n}$ as a root. Thus $h(X) \equiv 0$, so that $(\omega^m - \omega^{m-i})a_i = 0$ for each $i = 1, \ldots, m$. But $a_m \neq 0$ so $\omega^m - 1 = 0$ which says ω is an mth root of unity. Since (char k, n) = 1, $g(X)$ has m distinct roots and so they must be $\{\omega^i a^{1/n} \mid i = 1, 2, \ldots m\}$ where $\omega = \zeta^{n/m} = \zeta^s$ is a primitive mth root of unity. From above $0 = (\omega^m - \omega^{m-i})\ a_i = (1 - \omega^{m-i})\ a_i$, but if $i \neq m$ then $\omega^{m-i} \neq 1$, so that $a_i = 0$. Thus $g(X) = X^m + a_m$ has $a^{1/n}$ as a root which means $a^{m/n} = -a_m$ is in K. We shall use this fact later.

By hypothesis $b^{1/n} \in K(a^{1/n})$ so there exist elements $c_0, c_1, \ldots, c_{m-1}$ of K such that

(1) $$b^{1/n} = \sum_{i=0}^{m-1} c_i a^{i/n}.$$

If $m = 1$ then both $a^{1/n}$ and $b^{1/n}$ are elements of K so that $b = a(b^{1/n}a^{-1/n})^n$. Thus we may assume $m > 1$. Since $a^{1/n}$ and $\omega a^{1/n} = \zeta^s a^{1/n}$ are both roots of the irreducible polynomial $g(X) \in K[X]$, there is an automorphism of $K(a^{1/n})$ which fixes K and replaces $a^{1/n}$ with $\zeta^s a^{1/n}$ (see Theorem 5.I, [**1**, p. 183]). Applying this automorphism to equation (1) replaces $b^{1/n}$ with some root $\zeta^t b^{1/n}$ of $X^n - b$. Thus we obtain

(2) $$\zeta^t b^{1/n} = \sum_{i=0}^{m-1} c_i \zeta^{si} a^{i/n}.$$

Multiplying equation (1) by ζ^t and subtracting equation (2) we obtain

$$0 = \sum_{i=0}^{m-1} c_i (\zeta^t - \zeta^{si}) a^{i/n}.$$

But $1, a^{1/n}, \ldots, a^{m-1/n}$ form a basis for $K(a^{1/n})$ over K and so are linearly independent over K. Thus

(3) $$c_i (\zeta^t - \zeta^{si}) = 0$$

for $i = 0, 1, \ldots, m-1$. Since $b \neq 0$, not all c_i's are zero, so $\zeta^t - \zeta^{si} = 0$ for at least one i. Now $\zeta^t - \zeta^{si} = 0$ if and only if

(4) $$si \equiv t \pmod{n}.$$

Because $s = n/m$ congruence (4) will have at most one solution. (In fact, this solution will exist only if s divides t and then the solution is $i = t/s$.) Since we already have at least one solution this solution must be the only one. Thus there is exactly one i such that $\zeta^t - \zeta^{si} = 0$. It follows from equations (3) and (1) that $c_j = 0$ for $j \neq i$ and $b^{1/n} = c_i a^{i/n} = e a^{1/n}$; this implies $b = e^n a^i$.

By reversing the roles of a and b we obtain $a = d^n b^j$ for some $d \in K$ and some integer j. Thus $a = d^n e^{nj} a^{ij}$, or $a^{ij-1} = (d^{-1}e^{-j})^n$. Hence $a^{(ij-1)/n} = d^{-1}e^{-j}$ where $a^{(ij-1)/n}$ is an appropriately chosen nth root. If $ij - 1 = mq + r$ with $0 \leqq r < m$ then

$$a^{r/n} = d^{-1}e^{-j}a^{-mq/n} \in K$$

since e, d and $a^{m/n} = -a_m$ are elements of K. This means that $a^{1/n}$ is a root of $r(X) = X^r - a^{r/m} \in K[X]$. But $g(X) = X^m - a^{m/n}$ is the irreducible polynomial of $a^{1/n}$ over K, so $g(X)$ divides $r(X)$. Thus $r = 0$ and so $ij \equiv 1 \pmod{m}$ which implies $(i, m) = 1$.

We shall now show that i can be chosen so that $(i, n) = 1$. Let $p_1, \ldots, p_v$ be the distinct primes which divide n but do not divide m. The Chinese remainder theorem [**4**, p. 30] gives a solution less than n to the $v + 1$ congruences $X \equiv 1 \pmod{p_j}$, $j = 1, \ldots, v$, and $X \equiv i \pmod{m}$. Now $X = i + mu$ for some integer u and $(X, n) = 1$ since $(i, m) = 1$ and $X \equiv 1 \pmod{p_j}$ for $j = 1, \ldots, v$. Thus we obtain

$$b = e^n a^i = (e\,a^{-mu/n})^n a^{i+mu} = c^n a^x$$

with $c \in K$ and $(X, n) = 1$. This completes the proof of our theorem.

We now show why in the first example our simple original conjecture worked. We prove below that if n is a prime, then $Q(a^{1/n}) = Q(b^{1/n})$ if and only if $b = c^n a^i$. In the first example n was 2 and the only candidate for i is 1. Now, if $b = a^i e^n$ with $e \in K$ then for some integer j, $(ba^{-i})^{1/n} = \zeta^j e = c \in k(a^{1/n}) \cap K$. Thus $b = a^i c^n$ with $c \in k(a^{1/n}) \cap K$. This means that the element c of our theorem can actually be chosen in the field $k(a^{1/n}) \cap k(\zeta)$. In particular if $k(a^{1/n}) \cap K = k$ then c can actually be chosen in k, which is our original conjecture. When $n = p$ is prime and a has no pth root in k we shall show $X^p - a$ is irreducible over k. Thus $[k(a^{1/p})\colon k] = p$ and $[K\colon k] \leqq p - 1$ so $[k(a^{1/p}) \cap K\colon k]$ must be a divisor of p which is less than p; i.e., must be 1. Thus, $k(a^{1/p}) \cap K = k$ as desired. To show $X^p - a$ is irreducible suppose $f(X) \in k[X]$ divides $X^p - a$ with degree $f(X) = t$ where $1 \leqq t < p$. Now the roots of $f(X)$ are all of the form $\zeta^i a^{1/p}$ and so the constant term c of $f(X)$ has the form $\pm \eta a^{t/p}$ where $\eta^p = 1$. Now there are integers r and s such that $rt + sp = 1$. Thus

$$a^{1/p} = a^{tr/p} a^s = (\pm c/\eta)^r a^s$$

so $\eta^r a^{1/p} = \pm c^r a^s \in k$ contradicting that $X^p - a$ has no root in k. Thus $X^p - a$ is irreducible as required.

References

[1] I. N. Herstein, Topics in Algebra, Blaisdell, New York, 1964.

[2] G. J. Janusz, Algebraic Number Fields, Academic Press, New York, 1973.

[3] S. Lang, Algebra, Addison-Wesley, Reading, Mass., 1965.

[4] I. Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, Wiley, New York, 1972.

Riffling Casino Checks

MARTIN J. GARDNER

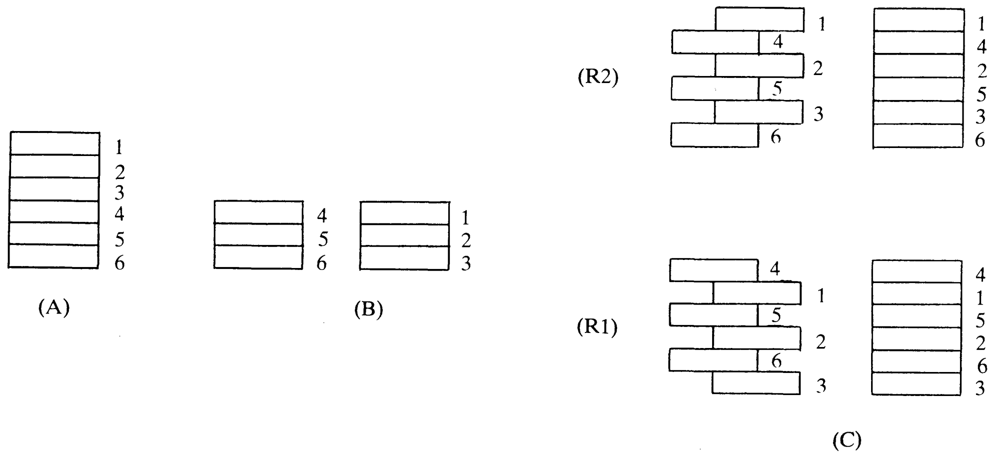
Univ. of Southampton Faculty of Medicine

C. A. MCMAHAN

Louisiana State University Medical Center

Casino checks are used in the place of cash on many gaming tables. These checks, sometimes referred to as chips, can be visualized as molded clay versions of silver dollars. Ordinarily, a check is about 10 grams in weight and slightly less than 4 centimeters in diameter. The ability to "riffle" casino checks perfectly is a skill learned by many dealers. It is an exercise used by dealers to improve their finger dexterity, enabling them to handle checks with precision and speed. These are basic requirements of an efficient, profitable organization. Thus dealers can be seen, during temporarily idle moments at the tables, performing these operations in many Las Vegas casinos.

The term riffling is used here to mean "cutting a stack of checks into two equal substacks, and then shuffling these two substacks so that they are perfectly interlaced". Riffling of checks is a one-handed operation, as compared to the more familiar two-handed riffling of cards. In FIGURE 1 the two possible riffles of a stack of six checks are shown schematically, each check being numbered with its position from the top of the original stack. Successively repeated riffling of the reconstituted stacks will eventually restore the checks to their original order. In this note we investigate several natural questions concerning the riffling operation: How many repeated riffles for coincidence with the



THE OPERATION OF RIFFLING: The original stack (A) is cut into 2 equal substacks (B). Then the two substacks are interlaced (C). If the right hand side substack is on the bottom, the resulting reconstituted stack is the R1 riffle; if the left hand side substack is on the bottom, the resulting stack is the R2 riffle.

FIGURE 1

original order are necessary for different stack sizes? How do riffles R1 and R2 compare? What can we say about the route of any particular check? Since the maximum size of a stack of checks that can conveniently be handled by a dealer is twenty — checks are usually stacked on casino tables in 20's — we will limit our investigation to stacks of even number size from 2 to 20.

Since riffling permutes the original stack of checks, our investigation will employ the language of permutation groups. If we consider a stack to contain $2n$ checks numbered from top to bottom as $1,2,3,4,\ldots,2n-1,2n$, then the rearrangement produced by riffle R1 can be represented as the permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & 2n-1 & 2n \\ n+1 & 1 & n+2 & 2 & \cdots & 2n & n \end{pmatrix},$$

and that produced by R2 as

$$\begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & 2n-1 & 2n \\ 1 & n+1 & 2 & n+2 & \cdots & n & 2n \end{pmatrix}.$$

The first row of each permutation gives the original order of the checks, and the second row gives the order of the reconstituted stack (again from top to bottom). When $n=3$ they can be seen to lead to the results shown in FIGURE 1. For this same example, writing the permutations in cyclic notation produces:

$$\text{for R1, } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix} = (1\ 4\ 2)(3\ 5\ 6);$$

$$\text{for R2, } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 5 & 3 & 6 \end{pmatrix} = (1)(2\ 4\ 5\ 3)(6).$$

The orders of these two permutations (given by the least common multiple of the numbers of elements in each constituent cycle) are 3 and 4, respectively, for R1 and R2. These figures give the number of repetitions of each riffling operation required before simultaneous return of all the checks to their original positions, and show that these are different for $n=3$.

FIGURE 2 gives the permutations describing the two riffling operations in cyclic notation and their orders, arrived at as above, for $n = 1, \ldots, 10$. For no value of n is the order the same for riffles R1 and R2, nor does either riffle show any consistent increasing order with increasing n. A closer study of the data in FIGURE 2 reveals, however, that the order of R2 for stack size $2n + 2$ is equal to the order of R1 for stack size $2n$. Moreover, the cycles of R2 with stack size $2n+2$ are given by adding 1 to all elements in each of the cycles of R1 with stack size $2n$ — then including cycles (1) and $(2n+2)$. Thus the R2 riffle can be treated as an R1 riffle with a dummy check on the top and bottom.

n	R1	Order	R2	Order
1	(1 2)	2	(1)(2)	1
2	(1 3 4 2)	4	(1)(2 3)(4)	2
3	(1 4 2)(3 5 6)	3	(1)(2 4 5 3)(6)	4
4	(1 5 7 8 4 2)(3 6)	6	(1)(2 5 3)(4 6 7)(8)	3
5	(1 6 3 7 9 10 5 8 4 2)	10	(1)(2 6 8 9 5 3)(4 7)(10)	6
6	(1 7 10 5 9 11 12 6 3 8 4 2)	12	(1)(2 7 4 8 10 11 6 9 5 3)(12)	10
7	(1 8 4 2)(3 9 12 6)(5 10)(7 11 13 14)	4	(1)(2 8 11 6 10 12 13 7 4 9 5 3)(14)	12
8	(1 9 13 15 16 8 4 2)(3 10 5 11 14 7 12 6)	8	(1)(2 9 5 3)(4 10 13 7)(6 11)(8 12 14 15)(16)	4
9	(1 10 5 12 6 3 11 15 17 18 9 14 7 13 16 8 4 2)	18	(1)(2 10 14 16 17 9 5 3)(4 11 6 12 15 8 13 7)(18)	8
10	(1 11 16 8 4 2)(3 12 6)(5 13 17 19 20 10)(7 14)(9 15 18)	6	(1)(2 11 6 13 7 4 12 16 18 19 10 15 8 14 17 9 5 3)(20)	18

Riffles R1 and R2 in cyclic notation and their orders for check stacks of size $2n$ ($n = 1, 2, \ldots, 10$)

FIGURE 2

Inspection of the constituent cycles makes it possible to trace the successive positions in the reconstituted stacks of a particular check following repeated identical riffles. Thus, for $n = 4$ with riffle R1, the check starting in position 3 moves to position 6 after one riffle and back to its original position 3 after a second riffle. Likewise, the check starting in position 6 moves to position 3 and then back to position 6: the checks in positions 3 and 6 continually interchange places. On the other hand, the check starting in position 1 moves through positions 2, 4, 8, 7, 5 before returning after 6 successive riffles to its original position 1. In fact, all the checks starting in these 6 numbered positions cycle among themselves in these positions during repeated riffles in this same sequence.

The positions before (P_i) and after (P_{i+1}) the ith R1 riffle are related by

$$P_{i+1} \equiv 2P_i \pmod{2n+1}, \qquad 1 \leqq P_i \leqq 2n.$$

Thus a check starting in position P_1 will move, after k successive R1 riffles, to position P_{k+1} given by $P_{k+1} \equiv 2^k P_1 \pmod{2n+1}$. Using the example at the end of the previous paragraph with $n = 4$ and $P_1 = 8$, we get $P_2 = 7$, $P_3 = 5$, $P_4 = 1$, $P_5 = 2$, $P_6 = 4$ and back to $P_7 = 8$; further riffles will produce only repetition of these positional changes. This recursion formula can therefore be used to generate the cycles shown in FIGURE 2.

If we require $P_{k+1} = P_1$ in the relation $P_{k+1} \equiv 2^k P_1 \pmod{2n+1}$, we obtain $0 \equiv (2^k - 1)P_1 \pmod{2n+1}$ for all values of $P_1 = 1, 2, \ldots, 2n$ as a condition for all checks to simultaneously return to their original position following successive R1 riffles. This condition can only be true if $2^k - 1$ is divisible by $2n + 1$. Thus the minimum number of R1 riffles required to return a stack of $2n$ checks to its original order is given by the smallest integer k such that $2^k - 1$ is divisible by $2n + 1$. This number is, of course, precisely the order of the permutation which we computed earlier as the least common multiple of the lengths of the constituent cycles.

For R2 riffles, the successive positions are related by $P_{i+1} \equiv 2P_i - 1 \pmod{2n-1}$, from which we can, as above, show that the minimum number of R2 riffles required to return a stack of $2n$ checks to its original order is given by the smallest integer k such that $2^k - 1$ is divisible by $2n - 1$.

It can be seen from the permutation orders listed in FIGURE 2 that for stack sizes of 6, 14 and 20 an R1 riffle produces the quickest return to the original position, while for other stack sizes an R2 riffle is preferable. The substantial differences in number of repeated riffles required for different stack sizes lead to unexpected riffling strategies. For instance, to restore a stack of 10 checks to their original order in a minimum number of riffles one should add 4 dummy checks on the top of the stack to give 14 checks, use 4 R1 riffles, and then remove the extra checks.

Riffling theory extends to repeated shuffling of a deck of 52 cards, and, in that context, the riffle R2 is referred to as the "Faro Out Shuffle" by magicians and (some) card players. It is described in detail by Marlo [**2**]; see also Feller [**1**], p. 335. With this method of shuffling the original order of a deck of 52 cards is reconstituted after only 8 shuffles — and hence its special interest. However, with riffle R1 (the "Faro In Shuffle") it takes 52 shuffles, and each card passes through every position before return.

This paper was written while M. J. Gardner held a visiting post at Louisiana State University Medical Center. We wish to acknowledge the helpful comments and suggestions of the editors and the referee.

References

[1] W. Feller, An Introduction to Probability Theory and Its Applications, vol. 1, Wiley, New York, 1950, Chapter 15.
[2] E. Marlo, Revolutionary Card Technique, Chicago, 1958, Chapters 6 and 7.
[3] S. Brent Morris, The Basic Mathematics of the Faro shuffle, Pi Mu Epsilon J., 6 (Spring 1975) 85–92.

The Indeterminate Form 0°

LOUIS M. ROTANDO
HENRY KORN
Westchester Community College

Consider the following limit problems often encountered in elementary calculus textbooks:

$$\lim_{x\to 0^+} (\sin x)^{\tan x} \qquad \lim_{x\to 0^+} (e^{x+1}-e)^x$$

$$\lim_{x\to 0^+} (\arctan x)^x \qquad \lim_{x\to 1^-} (1-x)^{\sinh(x-1)}.$$

In each of the above problems the limit is 1. Curiously enough the limit is also 1 for most similar problems typically included in the exercise sets devoted to indeterminate forms. Yet the limit process does not yield 1 for every example of the type 0°: G. C. Watson [**1**] discusses a generalization of the counterexample

$$\lim_{x\to 0^+} x^{a/\log x},$$

and conditions on f wherein $\lim_{x\to 0^+} x^{f(x)} = 1$ are investigated by L. J. Paige [**2**].

The purpose of this note is to further study of the indeterminate form 0° by looking at examples of the more general form

$$\lim_{x\to 0^+} f(x)^{g(x)}$$

in which f and g are real functions **analytic** at $x = 0$, that is, representable there by a Taylor series. In such cases we can show that the limit is 1.

THEOREM. *Suppose that f and g are nonzero real analytic functions at $x = 0$ for which $f(x) \geqq 0$ for all positive x sufficiently close to 0. If $\lim_{x\to 0^+} f(x) = \lim_{x\to 0^+} g(x) = 0$, then $\lim_{x\to 0^+} f(x)^{g(x)} = 1$.*

Proof. Applying L'Hospital's Rule, we have

$$\lim_{x\to 0^+} f(x)^{g(x)} = \exp\left[\lim_{x\to 0^+} \frac{\log f(x)}{1/g(x)}\right] = \exp\left[\lim_{x\to 0^+} \frac{f'(x)g^2(x)}{-f(x)g'(x)}\right]. \tag{1}$$

Since f and g are analytic and approach zero as x approaches zero, it follows by continuity that $f(0)=g(0)=0$, and in some neighborhood of $x=0$, f and g have the form

$$f(x) = x^m F(x), \qquad F(0)\neq 0$$

$$g(x) = x^n G(x), \qquad G(0)\neq 0$$

where m and n are positive integers, while F and G are analytic at $x=0$. Substituting these into (1) we obtain, after simplification,

$$\lim_{x\to 0^+} f(x)^{g(x)} = \exp\left[\lim_{x\to 0^+} \frac{x^n[xF'(x)+mF(x)]G^2(x)}{-F(x)[xG'(x)+nG(x)]}\right]. \tag{2}$$

The numerator $N(x)\equiv x^n[xF'(x)+mF(x)]G^2(x)$ as well as the denominator $D(x)\equiv -F(x)[xG'(x)+nG(x)]$ in this last limit are analytic at $x=0$. Since $D(0)\neq 0$, it follows from continuity at $x=0$ that $\lim_{x\to 0^+} D(x)\neq 0$, and therefore $\lim_{x\to 0^+}[N(x)/D(x)]=0$. Hence $\lim_{x\to 0^+} f(x)^{g(x)}=1$.

We note in conclusion that a simple linear transformation of variables will permit coverage of the case $\lim_{x\to a^+} f(x)^{g(x)}$. The theorem may also be easily modified to include the case $\lim_{x\to 0^-} f(x)^{g(x)}$ by requiring $f(x)\geqq 0$ for negative x sufficiently close to 0. Finally, if the restriction of "analytic" is weakened to "infinitely differentiable" at $x=0$ then the theorem would be false. A nice counterexample to illustrate this is given by letting $g(x)=x$ and

$$f(x) = \begin{cases} e^{-1/x^2} & \text{if } x\neq 0 \\ 0 & \text{if } x=0. \end{cases}$$

In this case the reader can easily verify that $\lim_{x\to 0^+} f(x)^{g(x)}=0$ and $\lim_{x\to 0^-} f(x)^{g(x)}=\infty$.

The author is indebted to the referee for several suggestions that led to substantial clarification of the proof.

References

[1] G. C. Watson, A note on indeterminate forms, Amer. Math. Monthly, 68 (1961) 490–492.
[2] L. J. Paige, A note on indeterminate forms, Amer. Math. Monthly, 61 (1954) 189–190.

Symmetries for Conditioned Ruin Problems

W. A. Beyer
M. S. Waterman
Los Alamos Scientific Laboratory

In this paper we discuss some interesting symmetries that arise in conditioning random walks on the integers with absorbing boundaries. These results are ancillary to a study done on conditional expected duration of walks used in a mathematical model of cancer tumors [**1**].

A tumor is an abnormal mass of tissue which is not inflammatory. A cancer tumor is thought of as arising from perhaps a single wayward cell which has lost the ability to control itself. At least this is a model for certain simple cases. The wayward cell starts reproducing without regard to the presence of other cells. Of course, the wayward cell may die before catastrophe overtakes the host organism. On the other hand, the single wayward cell may produce a family tree of descendants (called a clone) large enough to be noticeable to the host organism. In this case the descendents become a tumor. It is the tumor which is noticeable, and not the early cells that died without progeny. Our interest in the tumor growth is to estimate the expected time for the cancerous clone to reach tumor size from a single wayward cell, given that tumor size was reached.

Suppose each cell has probability $\lambda\,(0<\lambda<1)$ of dividing to produce two identical new cells and probability $\mu=1-\lambda$ of dying. We are interested in the process by which a single cell becomes, by this chance mechanism, a macroscopic clone of N cells. Although the natural model for this problem is a birth and death process with linear growth, we will employ the simpler model of classical gambler's ruin. The classical ruin problem concerns a random walk on $\{0,1,\dots,N\}$ where, if $0<r<N$, the probability of moving from r to $r-1$ is $\mu=1-\lambda$. The walk terminates when either absorbing state 0 or N is reached. If the initial state is z, where $0<z<N$, the duration of the walk will be the number of steps from z to absorption. The quantity in which we are interested is the conditional duration F_z of the walk, given that the walk terminates at N. For the cancer tumor problem, $z=1$.

Recently F. Stern [5] derived formulae for F_z and for E_z, the conditional duration of those walks terminating at 0. He also showed that $E_z=F_z$ when $2z=N$ and $0<\lambda<1$. S. M. Samuels [4] showed that, under these conditions, even more is true: the duration of the game and the absorption point are independent random variables. For a numerical example relevant to the cancer tumor model, let $z=1$, $N=10^4$, and $\lambda=.99$. Then, using Stern's formula with $r=.01/.99$,

$$F_z=\frac{(.99-.01)^{-1}}{1-r}\left[(10^4-1)(r-1)+2\cdot 10^4\left(\frac{r-r^{10^4}}{r^{10^4}-1}\right)\right]=10203.04\dots.$$

If the formula for F_z is used with $\lambda=.01$ and $\mu=.99$, it turns out that, again, $F_z=10203.04\dots$. We observed this symmetry in μ and λ from computer results for conditional expected duration before Stern's results appeared. That the conditional duration was equal for $\lambda=.99$ and $\lambda=.01$ seemed to us a surprising and paradoxical result. The purpose of this paper is to explain and generalize this phenomenon.

We begin with a random walk $\mathscr{W}$ on $\{0,1,\dots,N\}$ with absorbing barriers at 0 and N and for $0<r<N$, transition probabilities λ_r for $r\to r+1$ and $\mu_r=1-\lambda_r$ for $r\to r-1$. Our major result can be summarized as follows:

THEOREM. *Conditioning the random walk $\mathscr{W}$ on absorption at one of the barriers yields a new random walk of the same type. If the transition probabilities λ and μ of $\mathscr{W}$ are independent of position, transition probabilities of the conditioned walk depend on position and are symmetric in μ and λ.*

It follows from this theorem that when the transition probabilities of $\mathscr{W}$ are independent of position, any function of the transition probabilities of the conditioned walk is symmetric in μ and λ. For example, the expected duration of the conditioned walk is — as we noted earlier — symmetric in μ and λ. This result underlies the results of Stern and Samuels and will be discussed more fully later in this note. But before doing that we want to prove our theorem.

Proof. If q_z is the probability of absorption at 0 for a walk starting at z, then $q_z=\lambda_z q_{z+1}+u_z q_{z-1}$ with $q_0=1$ and $q_N=0$. Parzen ([3], p. 233) gives the solution to this difference equation with these boundary conditions as

(1) $$q_z=\left(\sum_{i=z}^{N-1}\prod_{j=1}^{i}x_j\right)\Big/\left(\sum_{i=0}^{N-1}\prod_{j=1}^{i}x_j\right)$$

where $x_j = \mu_j/\lambda_j$ and, by convention, $\Pi_{j=1}^{0} x_j \equiv 1$. If p_z is the probability of absorption at N for a walk starting at z, the value of p_z may be obtained from (1) by interchanging λ_j and μ_j (thereby replacing x_j by x_j^{-1}) and replacing z by $N-z$:

$$p_z = \left(\sum_{i=0}^{z-1} \prod_{j=1}^{i} x_j\right) \Big/ \left(\sum_{i=0}^{N-1} \prod_{j=1}^{i} x_j\right).$$

Clearly $p_z + q_z = 1$. If $\lambda_z = \lambda$ and $\mu_z = \mu$ for $0 < z < N$, then we obtain the well-known formula (Feller [**2**], p. 345) that

$$q_z = \begin{cases} \dfrac{(\mu/\lambda)^N - (\mu/\lambda)^z}{(\mu/\lambda)^N - 1}, & \lambda \neq \mu, \\ 1 - z/N, & \lambda = \mu. \end{cases}$$

Let us now compute the probability of a left step conditioned on absorption at a given boundary, say at $z = n$. Let P denote the probability measure associated with $\mathcal{W}$, L the event of the first step left, B_N the event of absorption at N, and S_z the event of being at z for $0 < z < N$. Then

$$\begin{aligned} P(L \mid S_z \cap B_N) &= P(L \cap S_z \cap B_N)/P(S_z \cap B_N) \\ &= \mu_z \frac{P(S_{z-1} \cap B_N)}{p_z} = \mu_z \frac{p_{z-1}}{p_z} = \mu_z \left(\sum_{i=0}^{z-2} \prod_{j=1}^{i} x_j\right) \Big/ \left(\sum_{i=0}^{z-1} \prod_{j=0}^{i} x_j\right) \\ &= \mu_z \frac{1 + x_1 + x_1x_2 + \cdots + x_1x_2\cdots x_{z-2}}{1 + x_1 + x_1x_2 + \cdots + x_1x_2\cdots x_{z-1}}. \end{aligned} \tag{2}$$

To investigate whether this formula for $P(L \mid S_z \cap B_N)$ is symmetric in λ and μ, we replace x_j by x_j^{-1} and μ_z by $\lambda_z = \mu_z x_z^{-1}$ to obtain

$$\text{(3)} \quad \mu_z \left(\sum_{i=0}^{z-2} \prod_{j=i+1}^{z-1} x_j\right) \Big/ \left(\sum_{i=0}^{z-1} \prod_{j=i+1}^{z} x_j\right) = \mu_z \frac{x_1x_2\cdots x_{z-1} + x_2x_3\cdots x_{z-1} + x_3x_4\cdots x_{z-1} + \cdots + x_{z-1}}{x_1x_2\cdots x_z + x_2x_3\cdots x_z + x_3\cdots x_z + \cdots + x_z}.$$

In general, (2) and (3) will not have the same value unless x_j is independent of j. But if the x_j are independent of j, they will agree and have as a common value:

$$P(L \mid S_z \cap B_N) = \mu \frac{P_{z-1}}{P_z} = \begin{cases} \dfrac{\mu^z\lambda - \mu\lambda^z}{\mu^z - \lambda^z} & (\mu \neq \lambda) \\ \mu \dfrac{N-z+1}{N-z} & (\mu = \lambda) \end{cases}$$

A similar analysis for the first step right, R, leads to the formula

$$P(R \mid S_z \cap B_N) = \lambda \frac{p_{z-1}}{p_z} = \begin{cases} \dfrac{\mu^{z+1} - \lambda^{z+1}}{\mu^z - \lambda^z} & (\mu \neq \lambda) \\ \lambda \dfrac{N-z-1}{N-z} & (\mu = \lambda) \end{cases}$$

Therefore, in either case, the conditional transition probabilities for uniform x_j are symmetric in μ and λ. This completes the proof of the theorem.

In the remainder of the note, the transition probabilities λ, μ are independent of position. The formulae in the case of absorption at zero are

$$P(R \mid S_z \cap B_0) = \frac{\lambda^{N-z}\mu - \lambda\mu^{N-z}}{\lambda^{N-z} - \mu^{N-z}} \quad (\mu \neq \lambda)$$

$$P(L \mid S_z \cap B_0) = \frac{\lambda^{N-z+1} - \mu^{N-z+1}}{\lambda^{N-z} - \mu^{N-z}} \quad (\mu \neq \lambda).$$

(These formulae are derived by interchanging λ and μ, interchanging L and R, and replacing z by $N-z$. But λ is *still* the probability of a right step.) If we assume $\mu < \lambda$ and let $N \to \infty$, we obtain the probabilities conditioned on absorption at zero of a random walk on the nonnegative integers:

$$P(R \mid S_z \cap B_0) \to \mu \quad \text{and} \quad P(L \mid S_z \cap B_0) \to \lambda.$$

This yields a new random walk in which left and right probabilities are interchanged, a result noted by O'N. Waugh [**6**] who attributes it to D. G. Kendall.

Our theorem applies directly to the classical gambler's ruin problem, and it is in that context that we can relate our work to that of Samuels and Stern. In the ruin problem players A and B start with a and b dollars, respectively. They repeatedly toss a coin which has probability λ of heads, $0 < \lambda < 1$. A wins one dollar from B whenever heads occur, while B wins one dollar from A whenever tails occur. The game continues until one of the players has no money left. Samuels [**4**] showed that if $a = b$, the duration of the game is independent of who wins it. That is, if D is the duration of the game (i.e., the number of tosses in the game) and $W = 1$ or 0 according to whether A or B wins, then $P(D = d \mid W = 1) = P(D = d \mid W = 0)$ for all d. (Stern derives explicit expressions for the conditional expected duration, and notes symmetry if $a = b$).

Suppose now that our gamblers begin with equal fortunes $a = b$. We denote by $\bar{g}$ the reflection of a game history g obtained by interchanging heads and tails. This permits us to distinguish between a **symmetric** event, a set of game histories S for which $g \in S$ implies $\bar{g} \in S$, and an **antisymmetric** event in which $g \in S$ implies $\bar{g} \notin S$. (For example, the set of game histories for which $D = 10$ is a symmetric event, whereas the set of game histories in which A wins is an antisymmetric event.) With this terminology we can generalize Samuel's theorem in the following way: *In the classic gambler's ruin with equal initial fortunes, if E is a symmetric event and F is either of the antisymmetric events* "A wins" *or* "B wins", *then E and F are independent.* If E is the event "$D = d$" and F is the event "A wins", then one obtains Samuels' theorem that the duration of the game is independent of who wins.

To prove this denote by P_λ the probability measure for the games with probability λ of heads. Then since $P_\lambda(g) = P_\mu(\bar{g})$, one has $P_\lambda\{E \mid F\} = P_\mu\{\bar{E} \mid \bar{F}\} = P_\mu\{E \mid \sim F\}$. By the theorem, $P_\mu\{E \mid \sim F\} = P_\lambda\{E \mid \sim F\}$ and thus $P_\lambda\{E \mid F\} = P_\lambda\{E \mid \sim F\}$. Hence

$$\frac{P_\lambda\{E \cap F\}}{P_\lambda\{F\}} = \frac{P_\lambda\{E \cap \sim F\}}{P_\lambda\{\sim F\}} = \frac{P_\lambda\{E\} - P_\lambda\{E \cap F\}}{1 - P_\lambda\{F\}}.$$

This relation simplifies to the desired statement of independence: $P_\lambda\{E \cap F\} = P_\lambda\{E\}P_\lambda\{F\}$. (The case of $P_\lambda\{F\} = 0$ or $P_\lambda\{\sim F\} = 0$ can be handled separately.)

We are indebted to Dr. G. I. Bell for suggesting this problem and for discussions and to Professor S. M. Samuels for pointing out connections betweeen our results and other work. Work on this paper was performed under the auspices of the United States Energy Research and Development Administration.

References

[1] G. I. Bell, Models of carcinogenesis as an escape from mitotic inhibitors, Science, 192 (1976) 569–572.

[2] W. Feller, An Introduction to Probability Theory and its Applications, vol. I, 3rd ed., Wiley, New York, 1968.

[3] E. Parzen, Stochastic Processes, Holden-Day, San Francisco, 1962.

[4] S. M. Samuels, The classical ruin problem with equal initial fortunes, this MAGAZINE, 48 (1975) 286–288.

[5] F. Stern, Conditional expectation of the duration in the classical ruin problem, this MAGAZINE, 48 (1975) 200–203.

[6] W. O'N. Waugh, Conditioned Markov processes, Biometrika, 45 (1958) 241–249.

PROBLEMS

Dan Eustice, Editor
Leroy F. Meyers, Associate Editor
The Ohio State University

Proposals

To be considered for publication, solutions should be mailed before August 1, 1977.

1003. Let P and Q be two distinct points in the interior of a circular disk with neither point at the center. With the boundary of the disk acting as a mirror, a ray of light from point P determines, by the successive reflections from the boundary, a polygonal path in the disk. This path is dependent on the initial direction of the ray of light. Given a positive integer k, show that there is such a path with the kth reflection of the ray intersecting Q.

*With k, P and Q given, can the number of such distinct paths be determined? [*Richard Crandall, Boston, Massachusetts, and Peter Ørno, The Ohio State University.*]

1004. A river flows with a constant speed w. A motorboat cruises with a constant speed v with respect to the river, where $v > w$. If the path travelled by the boat is a square of side L with respect to the ground, the time of the traverse will vary with the orientation of the square. Determine the maximum and minimum time for the traverse. [*M. S. Klamkin, University of Alberta.*]

1005. Suppose f and g are differentiable functions for $x > 0$ and $f'(x) = -g(x)/x$ and $g'(x) = -f(x)/x$. Characterize all such f and g. [*Brian Hogan, Highline Community College, Midway, Washington.*]

1006. A simple closed curve in the plane encloses a region R of area A. There is a point P in the interior of R such that every line through P intersects R in a line segment of length d. Find the greatest lower and least upper bounds for A. Are there curves where these bounds are attained? [*G. A. Heuer, Concordia College, Moorhead, Minnesota.*]

1007.* It is known that given an integer n, $n \geqq 0$, there is a positive integer k, such that k occurs in exactly n distinct Pythagorean triples (x, y, z), $x < y < z$, $x^2 + y^2 = z^2$. For example, 2^{n+1} occurs in exactly n Pythagorean triples. For each n, determine $m_n = \min\{k : k$ occurs in exactly n Pythagorean triples$\}$. By inspection, $m_n = 1, 3, 5, 16$, and 12 for $n = 0, 1, 2, 3$, and 4, respectively. [*Thomas E. Elsner, General Motors Institute.*]

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.

Q643. Let $m < n$ be positive integers exactly one of which is even. Prove that the only integral value of x for which $(x^{2^n} - 1)/(x^{2^m} - 1)$ is a perfect square is zero. [*Erwin Just, Bronx Community College.*]

Q644. Let A be a nonzero matrix of rank one so that $A = ab^*$, where a and b denote column vectors and * denotes conjugate transpose. Show that A is Hermitian if and only if a is a scalar multiple of b. Given that A is Hermitian, show that A is positive semidefinite if and only if the inner product a^*b is positive. [*John Z. Hearon, National Institutes of Health.*]

Solutions

Maximum Area Triangle **November 1975**

955. For three line segments of unequal lengths a, b, and c drawn on a plane from a common point, characterize the proper angular positions such that the outer endpoints of the line segments define the maximum-area triangle. Show how to approximate the exact values of the angles for $a = 3$, $b = 4$, and $c = 5$. [*Charles F. White, Oxon Hill, Maryland.*]

Solution: The characterization of the location of the segments a, b, c is that they lie on the altitudes of the maximum area triangle, with the common point the intersection point of the altitudes.

To see this, place one segment, say a, on the positive x axis. The coordinates of the end point are $(a, 0)$. Then the coordinates of the other two points are $P_1: (b\cos\alpha_1, b\sin\alpha_1)$ and P_2: $(c\cos\alpha_2, c\sin\alpha_2)$ where α_1 and α_2 are the angles formed by the two segments b and c with the positive x-axis. (The common point is the origin and we may assume $\alpha_1 < \alpha_2$).

The area of the triangle can be found by evaluating the determinant

$$A = \frac{1}{2}\begin{vmatrix} a & 0 & 1 \\ b\cos\alpha_1 & b\sin\alpha_1 & 1 \\ c\cos\alpha_2 & c\sin\alpha_2 & 1 \end{vmatrix},$$

$$A = \frac{1}{2}\left[(ab\sin\alpha_1 - ac\sin\alpha_2) + bc\sin(\alpha_2 - \alpha_1)\right],$$

i.e., $A = f(\alpha_1, \alpha_2)$. Now for a possible extremum of A,

(1) $$f_{\alpha_1} = \tfrac{1}{2}(ab\cos\alpha_1 - bc\cos(\alpha_2 - \alpha_1)) = 0,$$

(2) $$f_{\alpha_2} = \tfrac{1}{2}(-ac\cos\alpha_2 + bc\cos(\alpha_2 - \alpha_1)) = 0.$$

Upon equating these we find

(3) $$b \cos \alpha_1 = c \cos \alpha_2$$

i.e., the x coordinates of the two endpoints P_1 and P_2 must be equal; that is, the segment a must be perpendicular to the side which is formed by the two points P_1 and P_2. Thus, a is coincident with the altitude. Then either P_1 is in quadrant 1 and P_2 is in quadrant 4 or P_1 is in quadrant 2 and P_2 is in quadrant 3, assuming $\alpha_1 < \alpha_2$. In the second case the usual test yields a relative maximum. It should be noted that the same argument with either segment b or c would yield the fact that b and c must also lie on the respective altitudes of the maximum area triangle.

For the case of $a = 5$, $b = 4$, $c = 3$, however, we shall proceed differently. Returning to (1) and using (3) we have $a \cos \alpha_1 = c \cos \alpha_2 \cos \alpha_1 + c \sin \alpha_2 \sin \alpha_1$; or $a \cos \alpha_1 - b \cos^2 \alpha_1 = c \sin \alpha_2 \sin \alpha_1$, or squaring,

$$a^2 \cos^2 \alpha_1 - 2ab \cos^3 \alpha_1 + b^2 \cos^4 \alpha_1 = c^2 \sin^2 \alpha_2 \sin^2 \alpha_1$$

$$= c^2 \left(1 - \frac{b^2}{c^2} \cos^2 \alpha_1\right)(1 - \cos^2 \alpha_1) = (c^2 - b^2 \cos^2 \alpha_1)(1 - \cos^2 \alpha_1)$$

$$= c^2 - b^2 \cos^2 \alpha_1 - c^2 \cos^2 \alpha_1 + b^2 \cos^4 \alpha_1$$

or $2ab \cos^3 \alpha_1 - (a^2 + b^2 + c^2) \cos^2 \alpha_1 + c^2 = 0$.

Using 3, 4, 5, we have $40 \cos^3 \alpha_1 - 50 \cos^2 \alpha_1 + 9 = 0$. This cubic in $\cos \alpha_1$ has approximate roots of $-.3724$, $.5791$, and 1.0432. The first yields a relative maximum with $\alpha_1 \doteq 111.86°$ and $\alpha_2 \doteq 240.23°$. The area is approximately 20.4858.

ROBERT S. FISK
Pacific Lutheran University

Editor's Comment. This problem is a special case of extremal problems on simplices. See Leon Gerber, *The orthocentric simplex as an extreme simplex*, Pacific Journal of Mathematics, 56 (1975), 97–111, and M. S. Klamkin, *An identity for simplexes and related inequalities*, Simon Stevin, 48 (1974–1975), 57–64.

Also solved by Martin Berman, Bern Problem Solving Group (Switzerland), Ragnar Dybvik (Norway), Leon Gerber, Michael Goldberg, M. S. Klamkin (Canada), Lew Kowarski, Larry A. Olson, C. C. Oursler, David E. Penney, Lawrence A. Ringenberg, J. M. Stark, Gene Zirkel, and the proposer.

Convergent and Periodic **November 1975**

958. Give direct proofs of the following two results:

a. If $\text{Re}(z_0) > 0$ and the sequence $\{z_n\}$ is defined for $n \geqq 1$ by

$$z_n = \frac{1}{2}\left(z_{n-1} + \frac{A}{z_{n-1}}\right),$$

where A is real and positive, then $\text{limit}_{n \to \infty} z_n = \sqrt{A}$.

b. Suppose $\{x_n\}$ is a real sequence defined for $n \geqq 1$ by

$$x_n = \frac{1}{2}\left(x_{n-1} - \frac{A}{x_{n-1}}\right),$$

where A is positive. Show that if p is a given integer greater than 1, then the initial term x_0 can be chosen so that $\{x_n\}$ is periodic with period p. (These results are contained implicitly in K. E. Hirst, *A square root algorithm giving periodic sequences*, J. London Math. Soc., (2) 6 (1972) 56–60.) [*Murray S. Klamkin, University of Waterloo.*]

Solution: a. If w is a complex number defined by

$$z_0=\sqrt{A}\,\frac{1+w}{1-w}$$

then

$$\mathrm{Re}(z_0)=\frac{z_0+\bar{z}_0}{2}=\frac{\sqrt{A}}{2}\left(\frac{1+w}{1-w}+\frac{1+\bar{w}}{1-\bar{w}}\right)=\sqrt{A}\,\frac{1-|w|^2}{|1-w|^2}.$$

The condition $\mathrm{Re}(z_0)>0$ is therefore equivalent to $|w|<1$. Now

$$z_1=\frac{1}{2}\left(\sqrt{A}\,\frac{1+w}{1-w}+\sqrt{A}\,\frac{1-w}{1+w}\right)=\sqrt{A}\,\frac{1+w^2}{1-w^2}.$$

Using repeatedly the relation

$$z_n=\frac{1}{2}\left(z_{n-1}+\frac{A}{z_{n-1}}\right),$$

we find in the same way

$$z_n=\sqrt{A}\,\frac{1+w^{2^n}}{1-w^{2^n}}.$$

Since $|w|<1$ it follows that $\lim_{n\to\infty} z_n=\sqrt{A}$.

Remark: If $\mathrm{Re}(z_0)<0$ one finds $\lim_{n\to\infty} z_n=-\sqrt{A}$.

b. Take $x_0=\sqrt{A}\cot(\pi/(2^p-1))$.
We will show that $x_n=\sqrt{A}\cot(\pi\cdot 2^n/(2^p-1))$ for $n\geqq 0$. This follows, by induction, from

$$x_{n+1}=\frac{\sqrt{A}}{2}\left[\cot\left(\frac{\pi\cdot 2^n}{2^p-1}\right)-\tan\left(\frac{\pi\cdot 2^n}{2^p-1}\right)\right]=\sqrt{A}\cot\left(\frac{\pi\cdot 2^{n+1}}{2^p-1}\right).$$

Hence

$$x_{n+p}=\sqrt{A}\cot\left(\frac{\pi\cdot 2^{n+p}}{2^p-1}\right)=\sqrt{A}\cot\left(\pi\cdot 2^n+\frac{\pi\cdot 2^n}{2^p-1}\right)=\sqrt{A}\cot\left(\frac{\pi\cdot 2^n}{2^p-1}\right)=x_n$$

and $\{x_n\}$ has period p.

L. van Hamme
Vrije Universiteit Brussel
Brussels, Belgium

Also solved by Bern Problem Solving Group (Switzerland), M. G. Greening (Australia), Leo Hämmerling (Germany), Edward T. H. Wang (Canada), and the proposer.

A Geometric Inequality **November 1975**

959. Let P be a point in the interior of the triangle ABC and let r_1, r_2, r_3 denote the distances from P to the sides of the triangle. Let R denote the circumradius of ABC. Show that

$$\sqrt{r_1}+\sqrt{r_2}+\sqrt{r_3}\leqq 3\sqrt{R/2},$$

with equality if and only if ABC is equilateral and P is the center of ABC. [*L. Carlitz, Duke University.*]

Solution I: If r_i is the distance from P to side a_i of ABC, then, using the facts that

$$a_1r_1 + a_2r_2 + a_3r_3 = 2\Delta \quad \text{and} \quad \Delta = a_1a_2a_3/4R$$

(Δ being the area of ABC) and applying Cauchy's inequality, we obtain

$$\begin{aligned}\sqrt{r_1}+\sqrt{r_2}+\sqrt{r_3} &= \sqrt{a_1r_1/a_1}+\sqrt{a_2r_2/a_2}+\sqrt{a_3r_3/a_3}\\ &\leqq (a_1r_1+a_2r_2+a_3r_3)^{1/2}\left(\frac{1}{a_1}+\frac{1}{a_2}+\frac{1}{a_3}\right)^{1/2}\\ &= \left(\frac{a_1a_2a_3}{2R}\right)^{1/2}\left(\frac{1}{a_1}+\frac{1}{a_2}+\frac{1}{a_3}\right)^{1/2}\\ &= \frac{1}{\sqrt{2R}}(a_2a_3+a_3a_1+a_1a_2)^{1/2}\\ &\leqq \frac{1}{\sqrt{2R}}(a_1^2+a_2^2+a_3^2)^{1/2},\end{aligned}$$

with equality if and only if

$$a_1^2r_1 = a_2^2r_2 = a_3^2r_3 \quad \text{and} \quad a_1 = a_2 = a_3,$$

i.e., if and only if ABC is equilateral and P is its center. But the polar inertia inequality implies that $a_1^2 + a_2^2 + a_3^2 \leqq 9R^2$, equality holding if and only if $a_1 = a_2 = a_3$. Hence

$$\sqrt{r_1}+\sqrt{r_2}+\sqrt{r_3} \leqq \frac{1}{\sqrt{2R}}\cdot 3R = 3\sqrt{R/2},$$

equality holding if and only if P is the center of the equilateral triangle ABC.

MARK KLEIMAN, student
Stuyvesant High School
New York, New York

Solution II (*generalization*): Let P be a point in an n-simplex $\mathcal{A}$ with inradius r and circumradius R. Let the distances of P from the vertices and faces of $\mathcal{A}$ be respectively d_i and e_i for $i \in \mathcal{I} = \{0, 1, \ldots, n\}$. Berkes [**1**] proved that

$$\left(\frac{1}{n+1}\sum d_i^p\right)^{1/p} \geqq nr \tag{1}$$

for $p = 1$. Since the left side is a power mean, which increases with p, the result follows for all $p \geqq 1$. In [**2**, Theorem 4.4] we proved (1) for $p \geqq 2/[1 + \log(n+1)]$ and also

$$\left(\frac{1}{n+1}\sum e_i^p\right)^{1/p} \leqq R/n \tag{2}$$

for $p \leqq 0$. The present problem is that of proving (2) for $n = 2$ and $p = 1/2$. We shall prove (2) for $p = 2/3$ and hence obtain:

THEOREM. *Inequality* (2) *is valid for all* $p \leqq 2/3$. *Equality holds if and only if P is the center of a regular simplex.* (*We conjecture that the best possible exponent exceeds* 2/3 *and approaches* 1 *as n increases.*)

Proof. Let h_i be the altitude to face i, V_i the n-dimensional volume of the n-simplex with vertex P and opposite face i, V the volume of the given simplex, and K_i the $(n-1)$-dimensional area of face i. Then

$$\sum \frac{e_i}{h_i} = \sum \frac{e_i K_i/(n+1)}{h_i K_i/(n+1)} = \sum \frac{V_i}{V} = 1.$$

Hence the problem becomes:

$$\text{maximize} \sum e_i^{2/3} \text{ subject to} \sum \frac{e_i}{h_i} = 1.$$

The method of Lagrange multipliers yields

$$\frac{2}{3} e_i^{-1/3} - \lambda h_i^{-1} = 0, \qquad i \in \mathcal{I}, \tag{3}$$

for the extreme point; it is easy to verify that this yields a maximum. Then

$$e_i = \left(\frac{2h_i}{3\lambda}\right)^3, \qquad 1 = \sum \frac{e_i}{h_i} = \left(\frac{2}{3\lambda}\right)^3 \sum h_i^2, \quad \text{and} \quad \lambda = \frac{2}{3}\left(\sum h_i^2\right)^{1/3}.$$

Multiplying (3) by $3e_i/(2(n+1))$ and summing, we get

$$\left[\frac{1}{n+1}\sum e_i^{2/3}\right]^{3/2} = \left[\frac{3\lambda}{2(n+1)}\right]^{3/2} = (n+1)^{-3/2}\left(\sum h_i^2\right)^{1/2}$$

for the extreme point. Since the last expression is independent of λ and e_i, we have

$$\left[(n+1)^{-1}\sum e_i^{2/3}\right]^{3/2} \leqq (n+1)^{-3/2}\left(\sum h_i^2\right)^{1/2} \tag{4}$$

for all points of $\mathcal{A}$.

Let G be the centroid and C the circumcenter of $\mathcal{A}$, and let A_iG_i, $i \in \mathcal{I}$, be the medians. Clearly $h_i \leqq A_iG_i$, $i \in \mathcal{I}$, with equality if and only if $\mathcal{A}$ is regular, in which case equality holds in (4) if and only if P is the center. Further, it is an immediate consequence of Lagrange's identity that

$$0 \leqq CG^2 = R^2 - (n+1)^{-1}\sum A_iG^2 = R^2 - n^2(n+1)^{-3}\sum A_iG_i^2,$$

with equality if and only if $C = G$, which holds if and only if $\mathcal{A}$ is regular. Thus

$$\left[(n+1)^{-1}\sum e_i^{2/3}\right]^{3/2} \leqq (n+1)^{-3/2}\left(\sum h_i^2\right)^{1/2}$$
$$\leqq (n+1)^{-3/2}\left(\sum A_iG_i^2\right)^{1/2} \leqq R/n.$$

References

[1] J. Berkes, Einfacher Beweis und Verallgemeinerung einer Dreiecksungleichung, Elem. Math., 22 (1967) 135–136.

[2] L. Gerber, The orthocentric simplex as an extreme simplex, Pacific J. Math., 56 (1975) 97–111.

LEON GERBER
St. John's University

Also solved by Gordon E. Bennett, Alex G. Ferrer (Mexico), Michael Goldberg, Leonard Goldstone, M. G. Greening (Australia), M. S. Klamkin (Canada), J. M. Stark, and the proposer.

Counting Squares and Cubes

November 1975

960. In a rectangle of dimensions a and b, lines parallel to the sides divide the interior into ab square unit areas. Through the interior of how many of these unit squares will a diagonal of the rectangle pass?

*Can the result be generalized to higher dimensions? [*Alan Wayne, Pasco-Hernando Community College, Florida.*]

Solution: As the diagonal can be represented by the set of ordered pairs (ak, bk), $0 \leqq k \leqq 1$, the number of squares it passes through is the number of points in the set which have at least one coordinate a non-zero integer. (We count each square when the diagonal has crossed it.) With g.c.d.$(a, b) = d$, both ak and bk are integers when $k = t/d$, $1 \leqq t < d$. The total number of squares passed through is therefore $a + b - d$.

Generalization. In Euclidean n-dimensional space, the number of unit cubes or hypercubes passed through by a diagonal from the origin to the point $(a_1, a_2, \ldots, a_n)$ is the number of n-tuples $(ka_1, ka_2, \ldots, ka_n)$, $0 < k \leqq 1$ containing one or more integer components. By the Inclusion-Exclusion Principle this number is

$$\sum_i d(a_i) - \sum_{i<j} d(a_i, a_j) + \sum_{i<j<k} d(a_i, a_j, a_k) - \cdots (-1)^{n+1} d(a_1, a_2, \ldots, a_n)$$

where $d(a, \ldots, z) = $ g.c.d.$(a, \ldots, z)$ and $d(a) = a$.

M. G. Greening
University of New South Wales
Australia

Also solved by Merrill Barnebey, Bern Problem Solving Group (Switzerland), George Berzsenyi, D. P. Choudhury (India), Steven R. Conrad, Clayton W. Dodge, Frank Eccles, Thomas E. Elsner, Donald C. Fuller, Leon Gerber, Richard A. Gibbs, Larry Godbold, Michael Goldberg, Mark Kleiman, Lew Kowarski, T. E. Moore, C. B. A. Peck, Gary D. Peterson, Benjamin L. Schwartz, Joseph Silverman, James W. Walker, and the proposer.

Geometric and Arithmetic

November 1975

961. The sequence $11^0, 11^1, 11^2, \ldots$ of integral powers of the number 11, reduced modulo 50, i.e., $1, 11, 21, 31, 41, 1, \ldots \pmod{50}$ is in both geometric and arithmetic progression. What is the law of formation for such a series? [*Erwin Schmid, Washington, D. C.*]

Solution: Let n be a positive integer and suppose that m is a divisor of $(n-1)^2$. Then for each $k = 1, 2, 3, \ldots$,

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

and consequently, for each $k = 0, 1, 2, \ldots$,

$$n^{k+1} - n^k \equiv n - 1 \pmod{m}.$$

Therefore, the geometric progression $n^0, n^1, n^2, n^3, \ldots \pmod{m}$ is also arithmetic $\pmod{m}$ with a common difference of $n - 1$.

In particular, if $n = 11$ and $m = 50$ (which is a divisor of $(11-1)^2$), the given example results.

George Berzsenyi
Lamar University

Also solved by D. P. Choudhury (India), Clayton W. Dodge, Thomas E. Elsner, Richard A. Gibbs, M. G. Greening (Australia), Reinaldo E. Giudici (Venezuela), Joseph Silverman, Kenneth M. Wilke, and the proposer.

963. Characterize convex quadrilaterals with sides a, b, c, and d such that

$$\begin{vmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{vmatrix} = 0.$$

[*Hüseyin Demir, Ankara, Turkey.*]

Solution: It is easy to show, by adding and subtracting rows and columns, that the given determinant equation is equivalent to

$$(a+c+b+d)(a+c-b-d)[(a-c)^2+(b-d)^2]=0.$$

Since we have a, b, c, and d all positive, then either

$$a+c=b+d, \quad \text{or} \quad a=c \quad \text{and} \quad b=d.$$

In the first case the quadrilateral can be circumscribed about a circle: in the second it is a parallelogram. The argument reverses to show that, if the quadrilateral either is a parallelogram or possesses an inscribed circle, then the determinant is zero.

CLAYTON W. DODGE
University of Maine at Orono

Also solved by Gerald Bergum, M. G. Greening (Australia), Daniel Mark Rosenblum, J. M. Stark, and the proposer.

Answers

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

Q643. We compute that $(x^{2^n}-1)/(x^{2^m}-1)=\Pi_{i=m}^{n-1}(1+x^{2^i})$ and refer to the latter product as $(*)$. Since the greatest common divisor of any two of the terms of $(*)$ is easily seen to be 2 if x is odd, and 1 if x is even, it follows that if x is even, then each term of $(*)$ is a perfect square; an impossibility unless $x=0$ because each term of $(*)$ exceeds a perfect square by 1. If x is odd, then $x^{2^k}+1\equiv 2 \pmod 4$ which guarantees that each term of $(*)$ is divisible by 2 and no higher power of 2. As a consequence $(*)$ is divisible by 2^{n-m} and no higher power of 2. Since $n-m$ is odd, 2^{n-m} is not a perfect square and this implies that $(*)$ is not a perfect square.

Q644. If $a=\alpha b$ with α a real scalar it is clear that $A=A^*$. Now assume $A=A^*$. Then, from $ab^*=ba^*$, we obtain $a(b^*b)=b(a^*b)$, which shows that a is a scalar multiple of b. From this last equality we have further that $(b^*a)(b^*b)=(b^*b)(a^*b)$ which shows a^*b to be real. Given that $a=\alpha b$ we have $x^*Ax=\alpha(x^*b)(b^*x)=\alpha|x^*b|^2$ which is nonnegative for all x if and only if $\alpha>0$. But $\alpha=(a^*b)/(b^*b)$.

NEWS & LETTERS

SUMMER SEMINAR ON MODELING

The North Central Section of the Mathematical Association of America will sponsor a seminar on Applications of Mathematics in Modeling Theory from June 20, 1977 to June 24, 1977 at Bemidji State University, Bemidji, Minnesota. Applications presented will in general be of such a nature that they could be used in the teaching of undergraduate classes. Speakers in attendance will come from St. Paul Fire and Marine Insurance, Minnesota Mutual Life Insurance, Control Data Corporation, Honeywell Corporation, and Mayo Clinic. Cost for room and board on the campus together with registration will be approximately seventy dollars.

Northern Minnesota has many beautiful resort areas so if you wish to bring the family and camp while attending the seminar, please contact Dr. Clayton Knoshaug of Bemidji State University. If you wish to attend and/or to present a paper, please contact Dr. Gerald Bergum, South Dakota State University, Brookings, South Dakota 57006. Two hours of credit can be earned.

CRYPTOLOGIA: A NEW JOURNAL

A new journal, *Cryptologia*, devoted to all aspects of cryptology is scheduled to begin publication at the end of 1976. This journal, to be published four times a year, will provide a forum for the exchange of ideas related to cryptology in the public sector. It will contain research papers, survey articles, personal accounts, reviews, educational notes, and problems. Some of the areas which will be discussed are mathematical, computational, literary, historical, political, military, mechanical and archeological aspects of cryptology. The first issue includes articles on cipher equipment, Beatrix Potter's journal cipher, statistical methods in cryptanalysis, cryptographic applications of permutation polynomials. The editors of *Cryptologia* are Cipher A. Deavours, Department of Mathematics, Kean College; David Kahn, Department of Journalism, New York University; and Brian J. Winkel, Department of Mathematics, Albion College. Subscription for four issues is $16.00; individual issues are available for $5.00 each. Further information may be obtained from: *Cryptologia*, Albion College, Albion, Michigan 49224.

THERE'S NOTHING NEW...

The content of "Groups of Singular Matrices" by Colonel Johnson, Jr. (this *Magazine*, Sept. 1976, pp. 205-207) is included in L. Mirsky, *An Introduction to Linear Algebra*, Oxford U. Pr., 1955, pp. 272-276.

Geoffrey A. Kandall
Hamden
Connecticut 06514

The result reported in Peter G. Sawtelle's "The Ubiquitous e" (this *Magazine*, Nov. 1976, pp. 244-245) was previously proved by A.J. Wise, "The Number of Arithmetic Operations Required to Evaluate an n by n Determinant", *The Mathematical Gazette*, 53 (1969) 174-176.

Peter A. Lindstrom
Genesee Comm. Coll.
Batavia
New York 14020

♀ REFEREES WANTED ♀

There once was a journal of math,
Which incurred one reader's wrath,
Of those who checked papers' details,
Ninety-six percent were males.

The names of seventy reviewers appear on page 264 of the November 1976 issue of *Mathematics Magazine*. At *least* sixty-seven of these names denote *males*. Assuming a name is a measure of the sex of the individual denoted, isn't the male-female ratio of your reviewing staff somewhat unrealistic? Surely, there are many more perspicacious female mathematicians than indicated by this representation.

H. MacKay
Portola Valley
California 94025

Editors' Note: As we stated on page 264 of the November 1976 issue, we are interested in hearing from mathematicians who are interested in refereeing for *Mathematics Magazine*. So far our response has been (apparently) one-hundred percent male. We are an equal opportunity employer, with positions still open.

NO CIRCLES

The letter of Mr. van der Pas (this *Magazine*, November 1976, p. 261) suggested to me that he may not be alone among readers who might enjoy being brought up-to-date on the consequences of Dan Pedoe's article, "The Most Elementary Theorem of Euclidean Geometry" (this *Magazine*, January 1976, pp. 40-42) and some of the interesting questions he raises therein. In the aftermath of Prof. Pedoe's article there have appeared a number of papers presenting simple "no-circle" proofs of Urquhart's Theorem, also some proving Pedoe's Two-Circle Theorem without using Rennie's Lemma. These proofs, by D. Eustice, K. Williams, and others, use only elementary geometry and/or trigonometry with a few easy computations. They appear in issues running from June to October 1976 of a new Canadian journal, *EUREKA*. Since this pleasant publication is not yet widely available, readers interested in coming to a somewhat fuller "full-circle" (or full "no-circle") understanding of these matters which were first raised by your presentation of Pedoe's article should write to: Léo Sauvé, Editor, *EUREKA*, Algonquin College, 281 Echo Drive, Ottawa, Ontario K1S 1N4.

Incidentally, Mr. van der Pas' letter contains an error. If a quadrangle $ABCD$ is symmetric about AC, $AB+BC=CD+DA$. If it is also convex it *does* contain an inscribed circle, contrary to van der Pas' statement.

Daniel Sokolowsky
Yellow Springs
Ohio 45387

MULTIPLICATIVE METRICS

"A Multiplicative Metric" (this *Magazine*, Sept. 1976, pp. 203-205), by Doris J. Schattschneider, refers to the property $d(ax,ay) = d(x,y)$ for a metric d. This property has been called by other authors "invariant." (See, for example, Kelley: *General Topology*, p. 210; other references are also given there.) Specifically, if G is a topological group, a metric d for G is called *left invariant* if $d(ax,ay) = d(x,y)$, *right invariant* if $d(xa,ya) = d(x,y)$, or *invariant* if $d(axb,ayb) = d(x,y)$ for all $a,b,x,y \in G$. Of course, if G is abelian, all of these definitions coincide. Another property discussed in this note, namely $d(x^{-1},y^{-1}) = d(x,y)$, is clearly satisfied by any invariant metric.

In Kelley, p. 210, it is shown that if there is a countable base for the neighborhood system of the identity e there exists a left invariant metric and a right invariant metric. (An invariant metric need not exist.) Let I denote the family of all neighborhoods of e which are invariant under inner automorphisms. Kelley shows that there exists an invariant metric for G if and only if I is a base for the neighborhood system of e and there is a countable base for the neighborhood system of e.

In Schattschneider's note, the multiplicative topological group $G = R - \{0\}$ is considered. It follows from the general theory above that there exists an invariant metric for G. The metric defined in this note is an example of such a metric. The question raised in the note about whether an invariant metric can be defined in higher dimensions is easily answered by the general theory. If we consider the multiplicative topological group G of n-tuples $(x_1,\ldots,x_n)$ with $x_i \neq 0$ for $i = 1,\ldots,n$, there is an invariant metric on G. An explicit example is given by the formula

$$d(x,y) = \sum_{i=1}^{n} \frac{|x_i - y_i|}{|x_i| + |y_i|}$$

where $x = (x_1,\ldots,x_n)$, $y = (y_1,\ldots,y_n)$.

Richard Johnsonbaugh
Chicago State Univ.
Chicago
Illinois 60628

You are quite right that the property $d(x,y) = d(x^{-1},y^{-1})$ can be obtained as a consequence of the invariance of the metric under the action of $G = R - \{0\}$ instead of by direct verification. However, it struck me that the properties of this metric were multiplicative analogies of the additive properties of the Euclidean metric on R, hence this was my mode of presentation.

By the way, an exercise in Bourbaki (*General Topology*, Part 2, Addison-Wesley, 1966, p. 236, Ex. 1) shows that such a metric satisfies the inequality $d(xy,1) \le d(x,1) + d(y,1)$. This comment was edited out of my manuscript.

My suggestion at the end of the paper to try to extend the given metric to high dimensions was stated in an extremely general way, and hence, your suggested metric on $G = \{(x_1,\ldots,x_n) \in R^n \mid x_i \neq 0, \text{ all } i\}$ is a reply to the suggestion. However, I intended (and wrote in an earlier version of the paper) an extension of the given metric to *all* of R^n. Your suggested metric on G easily extends to the invariant metric on R^n defined by: $\bar{d}(\bar{x},\bar{y}) = \Sigma d(x_i,y_i)$ with d my metric on R. An extension which would be nice but which may be difficult to authenticate is:

$$D(\bar{x},\bar{y}) = \begin{cases} \dfrac{|\bar{x}-\bar{y}|}{|\bar{x}|+|\bar{y}|}, & \text{if } \bar{x},\bar{y} \text{ are not both } \bar{0} \\ 0, & \text{if } \bar{x} = \bar{y} = \bar{0} \end{cases}$$

where $|\ |$ is the Euclidean vector length on R^n. Does this define a metric on R^n for $n > 1$?

Doris Schattschneider
Moravian College
Bethlehem
Pennsylvania 18018

1681 AND ALL THAT

I am writing you about a mistake in the article "Computers in Group Theory" by Joseph A. Gallian (this *Magazine*, March 1976, pp. 69-73). Gallian discussed some of the computer programs done by students at the University of Minnesota. A list was given for each of the integers in the interval 1678-1682 of the theorems which show that these integers are not the orders of simple groups.

Students at the University of Detroit found this article interesting and we ran similar programs. From our findings, theorem 2 *does* show that the integer 1681 is not the order of a simple group. But theorem 2 is not listed with 1681 in Gallian's article.

Theorem 2 states: An integer N is not the order of a simple group if for some prime p such that $p^2 | N$ and $p^3 \nmid N$, $N \le p^5$. This theorem shows that 1681 is not the order of a simple group. Let $N = 1681$. Since $1681 = 41^2$ let $p = 41$. So 41^2 divides 1681 and 41^3 does not divide 1681 and $1681 \le 41^5$. Thus the conditions of theorem 2 shows that 1681 is not the order of a simple group.

Victor Meyers, student
Connie Blockton, student
University of Detroit
Detroit
Michigan 48221

P.S. If you print my write-in, please send me a few copies (and a bill) so that I can show-off. Smile!

P.S.S. Please excuse the bacon grease on page one.

1976 PUTNAM EXAM

A-1. P is an interior point of the angle whose sides are the rays $\vec{OA}$ and $\vec{OB}$. Locate X on $\vec{OA}$ and Y on $\vec{OB}$ so that the line segment $\overline{XY}$ contains P and so that the product of distances $(PX)(PY)$ is a minimum.

A-2. Let $P(x, y) = x^2y + xy^2$ and $Q(x, y) = x^2 + xy + y^2$. For $n = 1, 2, 3, \ldots$, let $F_n(x, y) = (x + y)^n -$

$x^n - y^n$ and $G_n(x, y) = (x + y)^n + x^n + y^n$. One observes that $G_2 = 2Q$, $F_3 = 3P$, $G_4 = 2Q^2$, $F_5 = 5PQ$, $G_6 = 2Q^3 + 3P^2$. Prove that, in fact, for each n neither F_n or G_n is expressible as a polynomial in P and Q with integer coefficients.

A-3. Find all integral solutions of the equation

$$|p^r - q^s| = 1$$

where p and q are prime numbers and r and s are positive integers larger than unity. Prove that there are no other solutions.

A-4. Let r be a root of $P(x) = x^3 + ax^2 + bx - 1 = 0$ and $r + 1$ be a root of $y^3 + cy^2 + dy + 1 = 0$, where a, b, c, and d are integers. Also let $P(x)$ be irreducible over the rational numbers. Express another root s of $P(x) = 0$ as a function of r which does not explicitly involve a, b, c, or d.

A-5. In the (x, y)-plane, if R is the set of points inside and on a convex polygon, let $D(x, y)$ be the distance from (x, y) to the nearest point of R.

(a) Show that there exist constants a, b, and c, independent of R, such that

$$\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} e^{-D(x,\, y)}dx\, dy = a + bL + cA,$$

where L is the perimeter of R and A is the area of R.

(b) Find the values of a, b, and c.

A-6. Suppose $f(x)$ is a twice continuously differentiable real valued function defined for all real numbers x and satisfying $|f(x)| \le 1$ for all x and $(f(0))^2 + (f'(0))^2 = 4$. Prove that there exists a real number x_0 such that $f(x_0) + f''(x_0) = 0$.

B-1. Evaluate

$$\lim_{n \to \infty} \frac{1}{n}\sum_{k=1}^{n}\left(\left[\frac{2n}{k}\right] - 2\left[\frac{n}{k}\right]\right)$$

and express your answer in the form $\log a - b$, with a and b positive integers. (Here $[x]$ is defined to be the integer such that $[x] \le x < [x] + 1$ and $\log x$ is the logarithm of x to base e.)

B-2. Suppose that G is a group generated by elements A and B, that is, every element of G can be written as a finite "word"

$$A^{n_1}B^{n_2}A^{n_3}\ldots B^{n_k},$$

where $n_1, \ldots, n_k$ are any integers, and $A^0 = B^0 = 1$ as usual. Also, suppose that $A^4 = B^7 = ABA^{-1}B = 1$, $A^2 \neq 1$, and $B \neq 1$.

(a) How many elements of G are of the form C^2 with C in G?

(b) Write each such square as a word in A and B.

B-3. Suppose that we have n events $A_1, \ldots, A_n$, each of which has probability at least $1 - a$ of occurring, where $a < 1/4$. Further suppose that A_i and A_j are mutually independent if $|i - j| > 1$, although A_i and A_{i+1} may be dependent. Assume as known that the recurrence $u_{k+1} = u_k - au_{k-1}$, $u_0 = 1$, $u_1 = 1 - a$, defines positive real numbers u_k for $k = 0, 1, \ldots$. Show that the probability of all of $A_1, \ldots, A_n$ occurring is at least u_n.

B-4. For a point P on an ellipse, let d be the distance from the center of the ellipse to the line tangent to the ellipse at P. Prove that $(PF_1)(PF_2)d^2$ is constant as P varies on the ellipse, where PF_1 and PF_2 are the distances from P to the foci F_1 and F_2 of the ellipse.

B-5. Evaluate

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

B-6. As usual, let $\sigma(N)$ denote the sum of all the (positive integral) divisors of N. (Included among these divisors are 1 and N itself.) For example, if p is a prime, then $\sigma(p) = p + 1$. Motivated by the notion of a "perfect" number, a positive integer N is called "quasiperfect" if $\sigma(N) = 2N + 1$. Prove that every quasiperfect number is the square of an odd integer.

COUNT

Houghton Mifflin continues to offer the variety of mathematics texts that teachers count on to meet the diverse needs of students. Here are six new ones:

The Functions of Algebra and Trigonometry
Kenneth Bogart, Dartmouth College
About 500 pages / Instructor's Manual
Just published

Bogart's text is loaded with applications. Almost every topic is introduced and motivated by a word problem. Over 400 illustrations help clarify student understanding as does the informal but accurate style. Every algebraic computation used in calculus is stressed in the book.

"[Bogart] really makes the subject come alive." — D. W. Hall, Michigan State University.

Elementary Algebra by Example
William Brett and Michael Sentlowitz, both of Rockland Community College
About 500 pages / paper / Instructor's Manual / Just published

Brett and Sentlowitz use everyday situations to motivate algebraic concepts and techniques. The steps in solving problems are thoroughly explained in a conversational style. An arithmetic review, over 400 illustrations, numerous problems, glossary, plus chapter and cumulative self-tests further aid learning.

"From the student's standpoint, it might be exactly what they need in order to finally understand algebra. Approach is different and good." — J. L. Amburgey, College of DuPage

Statistics Step-by-Step
Howard B. Christensen, Brigham Young University
About 550 pages / paper / Instructor's Manual / Just published

Hundreds of students at Brigham Young University and at a community college have proven that *Statistics Step-by-Step* works. Christensen's sound pedagogy, generous use of illustrations, both verbal and visual, and step-by-step explanations make his text exceptionally clear. Complete solutions to over 200 problems appear in the text. Sample exams, solutions, and lecture hints for each unit appear in the Instructor's Manual.

Ken Wantling of Montgomery College says, *"The text is the best on explanations that I have seen, has a readable style, covers the appropriate topics for a beginner's statistics course and at an appropriate level."*

Introductory Statistics with Applications
Wayne W. Daniel, Georgia State University
About 450 pages / Instructor's Guide with Solutions / Study Guide / Just published

Daniels provides over 400 applied problems and a wealth of examples in his new elementary statistics text, emphasizing applications to the social and natural sciences and business. Difficult concepts such as sampling distributions and hypothesis testing are clearly explained.

THE MATHEMATICAL ASSOCIATION OF AMERICA
1225 Connecticut Avenue, N.W.
Washington, DC 20036

MATHEMATICS MAGAZINE VOL. 50, NO. 1, JANUARY 1977