# MATHEMATICS MAGAZINE

Vol. 53, No. 4
September, 1980

WINNING AT TIC-TAC-TOE • THE THANKSGIVING EQUATION
WHAT CAN BE INTEGRATED • DO-IT-YOURSELF TILINGS

MATHEMATICS MAGAZINE

Volume 53, Number 4, September 1980
(ISSN—0025-570X)



**COVER:** Three dimensional tic-tac-toe has a first player win strategy! Judicious removal of branches from the game tree reduced the problem to a feasible computer check of the remaining foliage (see p.202).

## ARTICLES

195 Integration in Finite Terms: The Liouville Theory, *by Toni Kasper.*

202 Qubic: $4\times4\times4$ Tic-Tac-Toe, *by Oren Patashnik.*

## NOTES

217 Fourier's Seventeen Lines Problem, *by Barbara Turner.*

219 On the Enumeration of Cryptograms, *by Solomon W. Golomb.*

222 The Square Root of a $2\times2$ Matrix, *by Bernard W. Levinger.*

224 Will It Tile? Try the Conway Criterion!, *by Doris Schattschneider.*

233 Nice Cubic Polynomials for Curve Sketching, *by Tom Bruggeman and Tom Gush.*

235 The Tree Planting Problem on a Sphere, *by Stephen J. Ruberg.*

237 Cooking a Turkey, *by John Ruebush and Robert Fisk.*

239 A Coin Tossing Game, *by James C. Frauenthal and Andrew B. Miller.*

## PROBLEMS

244 Proposals Number 1101–1106.

245 Quickies Number Q665.

245 Solutions to Problems 1069–1072, 1074–1078.

251 Answers to Quickies.

## REVIEWS

252 Reviews of recent books and expository articles.

## NEWS AND LETTERS

255 Lester R. Ford, Carl B. Allendoerfer, and George Pólya Awards; Comments on Recent Issues.

## 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.

New manuscripts should be sent to: Doris Schattschneider, Editor-Elect, Mathematics Magazine, Department of Mathematics, Moravian College, Bethlehem, Pennsylvania 18018. 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.

## ABOUT OUR AUTHORS

**Toni Kasper** ("Integration in Finite Terms: The Liouville Theory") received a Ph.D. from Columbia University in 1976 and is currently an Associate Professor of Mathematics at Manhattan Community College. He became interested in the origins of calculus while a graduate student at UCLA and later was encouraged by Herbert Clemens at Columbia University to read Liouville's original papers. These papers make possible a deeper understanding of the function concept and lead directly to many issues of current interest.

**Oren Patashnik** ("Qubic: $4\times4\times4$ Tic-Tac-Toe") received his B.S. in Computer Science and Mathematics from Yale University in 1976. He then worked with experimental psychologists for four years—one year at Yale and three years at Bell Laboratories in Murray Hill, N.J. He is currently in the Computer Science Ph.D. program at Stanford University. Patashnik started playing Qubic at age 10. While taking an Artificial Intelligence course in his sophomore year at Yale, he became convinced that the first player could win at Qubic under optimal play. He set out to prove this for his senior project at Yale and finished the proof explained here a full year after he graduated.

**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 $18 per year. Members of the Mathematical Association of America or of Mu Alpha Theta may subscribe at special reduced rates. Colleges and university mathematics departments may purchase bulk subscriptions (5 or more copies to a single address) for distribution to undergraduate students.

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

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



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

ARTICLES

# Integration in Finite Terms: The Liouville Theory

*The search for elementary antiderivatives leads from classical analysis through modern algebra to contemporary research in computer algorithms.*

TONI KASPER
*City University of New York*
*New York, NY 10019*

It is sometimes said that the problem of indefinite integration is that of finding a function whose derivative is some given function. So worded, this description is a bit vague, if not misleading, since it ignores the fact that we usually want the derivative to have some specific form. Continuing the ancient Greek tradition which accepted as legitimate only those curves constructible with straightedge and compass (the so-called geometric curves), Descartes favored functions having algebraic expression over "mechanical curves," that is, those representable only in transcendental terms. Sharing Descartes' predilection for algebraic functions, Newton asserted that a quantity like $1/(x-a)$ could not be integrated since to do so would involve a transcendental quantity, the logarithm. For Newton, therefore, the integration could not be done since it is impossible to perform in strictly algebraic terms.

When possible, Newton avoided nonalgebraic forms by resorting to infinite series. The sacrifice of finite expression was no great loss to him in exchange for averting the still not acceptable transcendental quantities. Leibniz, on the other hand, did not share the prevailing general prejudice against nonalgebraic functions; his discomfiture was with nonfinite expression, so he readily admitted transcendental entities into the calculus, enlarging the repertoire of integrals that could be given in closed form.

We see that the question of whether a given function can be integrated depends on the functions one has available, and the allowable mode of expression. To state the problem of indefinite integration precisely, therefore, requires that we restrict both the class of functions and the mode of expression to be used. If we suppose, then, that $f(x)$ belongs to some special category of functions, we may ask whether its integral also belongs to the class, or can be expressed—according to some prescribed mode—in terms of functions which are members of that class.

As mathematicians became more experienced with the new functions they encountered, acceptance of them followed, and the function concept broadened. In addition, Leibniz' preference for finite expression prevailed. By the 19th century the problem of indefinite integration took the following now classical form: *to determine whether or not a given elementary function has an elementary integral and, if so, to calculate it*. We propose to give an account of the progress made by mathematicians towards solving the problem of finite elementary integration. We will present an overview tracing from the roots of the problem to its final resolution, with implications for some frequently encountered applications.

## Liouville's Theorem: Integration of Algebraic Functions

The credit for establishing integration in finite elementary terms as a mathematical discipline belongs to Joseph Liouville (1809–1882), who created the theory in a series of papers published between 1833 and 1841. Having considered the question of when an algebraic function has an algebraic integral [**1**], Liouville then dealt with the problem of when an algebraic function has an *elementary* integral [**2**]. To treat this question he developed, in 1834, what is now called Liouville's Theorem: *if $y$ is an algebraic function of $x$, and $\int y\,dx$ is elementary, then* $\int y\,dx = t + A\log u + B\log v + \cdots + C\log w$, *where $A, B, \ldots, C$ are constants, and $t, u, v, \ldots, w$ are algebraic functions of $x$.* It is this theorem, and the generalizations it inspired, that provided the basis of all future work on the problem of indefinite integration, and it laid the foundation on which the final resolution came to rest.

As an application of this result, Liouville was able to settle an old question concerning integrals of the form $\int R(x, \sqrt{P}\,)dx$, were $R$ is rational in $x$ and $P$, and $P$ is a third or fourth degree polynomial in $x$. One of the earliest examples of this type of integral arose in connection with attempts to rectify the ellipse, and for that reason such forms are called **elliptic integrals.** These occurred in many applications of the calculus, and attempts to express them as a finite combination of the known elementary functions often failed, compelling investigators (like Euler, for example) to use infinite series to evaluate them [**14**]. By the 18th century it was suspected that, in general, elliptic integrals cannot be represented by finite elementary expressions. In a demonstration based on his 1834 theorem, Liouville was able to show that such is indeed the case, furnishing mathematics with its first case of a proven nonelementary integral.

To make matters clear requires a closer look at what Liouville means by an elementary function. His notion includes the familiar simple forms known to the beginning student, namely, polynomials, rational functions, algebraic functions, the exponential and logarithmic functions, and the trigonometric functions. With the introduction of imaginary numbers, the trigonometric (and hyperbolic) functions can be defined in terms of exponentials and logarithms, so Liouville omits the former as a special class, admitting into the discussion only algebraic, exponential, and logarithmic quantities. Liouville's notion of elementary function is considerably broader, however, than these examples suggest. He begins by defining what he calls a **finite function,** this being a quantity given by an equation (or system of equations) which is written by subjecting the variables to a finite number of algebraic, exponential, or logarithmic operations. Two examples of such functions are provided by the following equations:

$$e^x y^5 - y + \log(\log x) = 0 \tag{1}$$

$$xy - e^y = 0. \tag{2}$$

The function $y$ defined by (1) enters the equation algebraically (which is how we describe a quantity subjected to only algebraic operations, i.e., addition, subtraction, multiplication, division, and the taking of roots); this is an example of what Liouville means by an **explicit finite function,** and what we now call an **elementary function.** The quantity given by (2), on the other hand, enters the equation transcendentally (meaning that it is acted upon by an exponential or logarithm), and it represents what Liouville refers to as an **implicit finite function.** While Liouville was able to prove in 1834 that elliptic integrals generally are not explicit finite functions, it was not until 1923 that Ritt showed [**12**] that such integrals do not even represent implicit finite functions; in other words, they are not finite functions at all, but entities of some higher transcendental order.

To some extent Liouville's use of the word "explicit" can be misleading. He does not mean that the equation can be solved explicitly for $y$, but that $y$ is an algebraic function of the other quantities in the equation. In fact, since algebraic theory has established that $y^5 - y - x = 0$ has no roots that are explicit algebraic functions of the coefficients present in the equation, we know for certain that it is impossible to solve (1) for $y$.

Since an elementary function is one that satisfies an algebraic relation, we see that "algebraic" is the fundamental property. As the reader may recall, the statement that $y$ is an algebraic function of quantities $x_1, x_2, \ldots, x_k$ means $y$ and the $x_i$ satisfy an equation of the form

$$P_0(x_1,\ldots,x_k)y^n + P_1(x_1,\ldots,x_k)y^{n-1} + \cdots + P_n(x_1,\ldots,x_k) = 0.$$

The left member of the equation may be taken to be an irreducible polynomial in $y$ whose coefficients, the $P_j$, are themselves polynomials in $x$ with constant coefficients. Now, in precise terms of Liouville's definition, $y$ is an **explicit finite function of x** if $y$ can be expressed as an algebraic function of quantities $u, u_1, \ldots, u_k$ according to the following scheme:

(1) $u$ is an algebraic function of $x$.

(2) $u_1$ is an exponential or logarithm of an algebraic function of $x$; that is, $u_1$ is of the form $e^u$ or $\log u$. The term $u_1$ is called a **monomial of the first kind.**

With $u$ and $u_1$ we form a **transcendental function of the first kind**, this being an algebraic function of $x$ and first order monomials like $u_1$.

(3) $u_2$ is an exponential or logarithm of a first order transcendental function. The term $u_2$ is called a **monomial of the second kind.**

Now, with terms like $u, u_1$, and $u_2$, we can construct a **transcendental function of the second kind,** which is an algebraic function of $x$ and the first and second order monomials.

The scheme continues, building a hierarchy of $n$th order monomials (or, more simply, "$n$-monomials") and their $n$th order transcendental functions, however far one wishes to go. Then $F$ is called an **explicit finite function of order $n$** (for short, a function of order $n$) if $F$ is expressible as an algebraic function of $n$-monomials (and, possibly, monomials of lower order), so that the order of $F$ is the highest order present among the monomials used to express $F$. Furthermore, if another function $G$ is an algebraic combination of $F$ and certain monomials, then $G$ is an algebraic function of all the monomials involved, and hence is an explicit finite function also. In other words, an algebraic function of monomials and an explicit finite function is itself an explicit finite function. As a simple example, consider the function $G$ defined by the equation $FG^5 - G - F^2e^x = 0$, where $F$ is in turn defined by the relation $F^7 + F - \log(\log x) = 0$. Here, $F$ is an algebraic function of the monomial $\log(\log x)$, and $G$ is an algebraic function of $F$ and the monomial $e^x$. Therefore, $G$ is an algebraic combination of both monomials, and is thus an explicit finite function.

Liouville recognized that this manner of classifying transcendental functions involves complications and subtleties. For one thing, it is difficult, in many cases, to determine the actual order of an explicit finite function. Secondly, even when we know the precise order $n$, there is uncertainty as to how many $n$-monomials are required (that is, the minimum number) to represent the function.

To illustrate the nature of the first problem, we note that the monomial $\log(xe^x)$ looks like a function of order 2 but, when written in the equivalent form $x + \log x$, has the appearance of a first order function. Similarly, the monomial $e^{\log x^2}$ looks like a second order function but, when written as $x^2$, is seen to be an algebraic function. Although Liouville himself did not specify an order for algebraic functions per se, being content with commencing the ordering at $n = 1$, it is quite clear, however, that he did consider functions of the first kind to possess a higher order than strictly algebraic functions.

Thus, a function expressed a given way in terms of monomials, and therefore appearing to have a certain order, could be capable of representation by another form having an apparently lower order. For Liouville's classification scheme to serve the purposes he intended, we must take for the order of an explicit finite function the *smallest* order required to represent the particular function at hand. With this approach the order is a definite integer, although it is not always easy to see readily what that number is. How do we know that a given function $F$, being presented one way as an algebraic combination of monomials, cannot be written in an alternate form employing monomials all of lower order than the highest order used in the given expression for $F$? Moreover, functions like $x^x$ and $x^\alpha$ (where $\alpha$ is an imaginary or irrational real number) are not even written in terms of monomials; how do we determine the order of functions like these, or that they are explicit finite functions in the first place? Although Liouville had no regular procedure for resolving the question of transcendental order, he did try to suggest, by treating several cases, how one might proceed in specific instances [3, pp. 86–104]. For example, by writing $x^\alpha$ as $e^{\alpha \log x}$, Liouville shows that the order of $x^\alpha$ is at most 2. He then shows that $x^\alpha$ cannot be represented by any first order function. Having already shown that $x^\alpha$ is not algebraic, it follows that it is of order 2 exactly.

To clarify the second problem connected with Liouville's scheme, that of determining not the order but the minimum number of monomials of that order required to represent the function, consider $F(x)=e^{x^2}$. Now $F$ is certainly of order 1 since it cannot be represented by an algebraic function, as Liouville proved when he showed that $e^p$ is never algebraic for any algebraic function $p$ [3, p. 69]. But $F$ can also be written as $e^{-x}e^{x^2+x}$, which is likewise an algebraic combination of first order monomials. The important difference between these two expressions for $F$ is that the second employs two first order monomials, while the first form uses just one. As this example shows, Liouville's arrangement allows an $n$th order explicit finite function to be expressed in various ways, some forms being more economical in $n$-monomials than others. To state, therefore, that $F$ is an explicit finite function of order $n$ means exactly—and no more than—the following:

(1) $F$ satisfies an algebraic equation (denoted by * for the sake of brevity) whose coefficients are polynomials in $x$ and monomials (in $x$).

(2) An $n$-monomial appears in * (along with, possibly, monomials of lower order).

(3) There is no way to express $F$ using monomials all of which have lower order than $n$.

As already indicated, these stipulations, although restrictive, do not determine the minimum number of $n$-monomials necessary to express $F$. However, Liouville's investigations do not depend on actually knowing this least number, but only on the consequences of assuming (which is always permissible) that the function in question is being represented by a form using the required minimum.

## Liouville's General Theorem: Integration of Elementary Functions

Liouville's theorem received its first generalization the following year, 1835, by Liouville himself. By defining a certain type of elementary function in algebraic terms of several variables, Liouville was able to extend the theory from the integration of algebraic functions to a special class of elementary functions. To be specific, Liouville's general theorem states that *if $y$ and $z$ are functions of $x$ whose derivatives, $dy/dx$ and $dz/dx$, are each algebraic functions of $x,y$, and $z$, and if $P$ is an algebraic function of $x$, $y$, and $z$ such that $\int P\,dx$ is a finite function, then $\int P\,dx = t + A\log u + B\log v + \cdots + C\log w$, where $A,B,\ldots,C$ are constants, and $t,u,v,\ldots,w$ are algebraic functions of $x$, $y$, and $z$.* Liouville points out that if $F$ and the two derivatives are not merely algebraic but rational in $x$, $y$, and $z$, then so are the functions $t,u,v,\ldots,w$. He uses this result to demonstrate that, if $y$ is algebraic in $x$, and $\int e^x y\,dx$ is elementary, then the integral can be expressed as $e^x(\alpha+\beta y+\gamma y^2+\cdots+\lambda y^{n-1})+\text{constant}$, where $\alpha,\beta,\gamma,\ldots,\lambda$ are rational functions of $x$ that can always be calculated when they exist. In other words, we can always determine, under the given conditions, if $\int e^x y\,dx$ is elementary. As an application, Liouville shows that both $\int (e^x/x)dx$ and $\int[\sin\alpha x/(1+\alpha^2)]d\alpha$, the latter regarded as a function of the positive variable $x$, are nonelementary. Finally, Liouville proves that it is always possible to determine, for algebraic functions $P,Q,\ldots,T$ and nonconstant algebraic functions $p,q,\ldots,t$ whether or not the integral $\int(Pe^p+Qe^q+\cdots+Te^t)dx$ is elementary, and to obtain the integral when it is.

During the rest of the 19th century very little was done in direct continuation of Liouville's work. Then, at the beginning of the 20th century, activity resumed. Beginning in 1906, the Russian mathematician D. D. Mordukhai-Boltovskoi (1876–1952) started writing on the Liouville theory, and contributed much to it. Between 1923 and 1927 Joseph Fels Ritt published his early discussions on the topic (and related material), and in 1936 Gino Loria gave a brief account of Liouville's work emphasizing his integration theory.

## Ostrowski's Generalization: The Method of Field Extensions

The next major addition to the Liouville theory came in 1946 when A. Ostrowski broadened Liouville's general theorem (of 1835) and extended it to the wider class of meromorphic functions (single-valued and analytic, except possibly for poles) in regions of the complex plane **[11]**. What is most important here is that, while previous treatments had been based essentially on Liouville's technique, Ostrowski achieved his generalization by developing a new idea, the so-called method of field extensions, which permits a very precise and general statement of the theorem, while simplifying the proof. Ostrowski's technique is based on the notion of a **differential field** (Ritt's term), which is an (algebraic) field equipped with a mapping into itself that obeys the addition and multiplication rules of differentiation. Even though Ostrowski was concerned with the analytic properties of the functions belonging to the field, his method of field extensions provided the germ of the algebraic approach that evolved when subsequent investigators extracted the algebraic ingredients of his treatment to furnish an even simpler, more general exposition of the subject, and in terms of which the problem of indefinite integration was eventually solved.

## Ritt's Formulation: Extension to Many-valued Functions

In 1948, Joseph Fels Ritt (1893–1951) published what has come to be called the classical account of integration in finite terms **[13]**. In this work, the author summarized the theory as of that date, and modified the presentation somewhat to accommodate the many-valued nature of elementary functions. Without getting bogged down in the details, an elementary function can be regarded as an algebraic function of one or more variables; that is, it is a root of an irreducible polynomial having coefficients in some field. The multi-valued character of elementary functions arises from the fact that polynomials generally have more than one root. Ritt achieved his extension to this case by the technique of analytic continuation along curves on a Riemann surface (a series of sheets lying one above the other) of the function, a procedure that permits a many-valued function, with a suitable restriction of the domain, to be treated as single-valued. Like his predecessors, Ritt relied, for the most part, on analytic considerations.

While Ritt's approach takes care of some of the details ignored in previous works, the subject can be treated from an algebraic point of view that makes it unnecessary to deal with such matters, i.e., either the analytic or multi-valued character of the functions. As indicated above, an elementary function, say $y$, satisfies an algebraic equation whose coefficients belong to some field $K$. All the algebraic properties of $y$ can be derived from the equation by studying $y$ as an element of $K(y)$, the algebraic extension obtained by adjoining $y$ to $K$, and there is really no need to consider the function's analytic properties as such. (As a matter of interest, Liouville's papers in the 1830's and 40's are the first important works dealing with the algebraic characteristics of elementary functions, while Risch has provided a modern discussion **[19]**.) As for the many-valued feature, it is sufficient to treat just one of the roots of the associated algebraic equation since any two roots, say $y_1$ and $y_2$, have basically the same behavior, this in the sense that their respective extension fields are isomorphic (with $y_1$ corresponding to $y_2$, and the elements of $K$ to themselves). A simple example is furnished by the algebraic equation $t^2(1-x^2)(1-c^2x^2)-1=0$. We adjoin any one of the roots $t$ to $K=R$, the field of rational functions), forming $R(t)$, an algebraic extension of $R$. We then study $t$ as an element of the so-called algebraic function field $R(t)$ without the necessity of resorting to a Riemann surface for $t$. Moreover, the algebraic properties of $t$ are shared by any other root of the given equation. Incidentally, $R(t)$ is called an "elliptic function field" because it is generated by the integrand of an elliptic integral, in this case the elliptic integral of the first kind.

Ritt's monograph also brought the subject up to date: it contained a bibliography and summary of the important developments up to that time, and simplified the presentation. Moreover, although his fundamental approach was still analytic, he stimulated an algebraic perspective, especially by promoting Ostrowski's method of field extensions. The character of Ritt's part in the algebraic formulation of analytic subjects can be glimpsed in the preface to E. R. Kolchin's *Differential Algebra and Algebraic Groups* (Academic Press, 1973):

> ...algebra...historically grew out of a study of algebraic equations with numerical coefficients. In much the same way, differential algebra sprang from the classical study of algebraic differential equations with coefficients that are meromorphic functions in a region of some complex space... It is noteworthy that a subject so substantial as differential algebra owes its existence to one person. J. F. Ritt (1893–1951) was not only its founding father, but also its principal prophet and practitioner. [As of this date] the majority of the main results, and the deepest ones, are due to him, and despite a new look, the main lines of the subject today are the same as in 1951. It had already become clear then that differential algebra is pure algebra, and although Ritt's life blood was classical analysis, in his second book on the subject [*Differential Algebra*, AMS Colloq. Publ., 33, 1950] he made a great effort to meet the algebraist half way.

## Resolution of the Problem: The Algebraic Formulation

The theory of integration in finite terms, created by Liouville in the early 1800's and summarized by Ritt in 1948, has experienced renewed interest in recent times, specifically in the work of Rosenlicht and Risch.

In 1968, Maxwell Rosenlicht published the first purely algebraic exposition of Liouville's 1835 theorem and its generalization by Ostrowski **[15]**. Rosenlicht's presentation follows Ostrowski (and Ritt) in the use of the differential field concept, the mapping which Rosenlicht calls a **derivation**. Furthermore, exponentials and logarithms are defined only in terms of the algebraic properties of their images (derivatives) under the derivation. Thus, if $u$ and $v$ are elements of the differential field in question, and if $u'$ and $v'$ are their images, respectively, then we call $u$ a logarithm of $v$ (or $v$ an exponential of $u$) if $u'=v'/v$, with $v\neq 0$. Rosenlicht's statement of Liouville's theorem, presented below, marks a major change in style in that it is written solely in terms of field elements and their images: unlike earlier versions, no mention is made of integrals or logarithms per se. Thus we have, in Rosenlicht's rendition, a considerably more abstract formulation, with differentiation supplanted by the more general idea of a mapping, and the specific nature of the functions replaced by membership of elements in a field. Rosenlicht's abstract generalization of the classical Liouville result says that *if $\alpha$ belongs to some differential field $F$ of characteristic* 0, *and if the equation $y'=\alpha$ has a solution in some elementary extension field of $F$ having the same subfield of constants, then there are constants $c_1,\dots,c_n$ in $F$ and elements $u_1,\dots,u_n$, $v$ in $F$ such that $\alpha=\sum_{i=1}^{n}c_i(u_i')/(u_i)+v'$.* As an application, Rosenlicht establishes the nonelementary character of the classic integrals $\int e^{z^2}dz$; $\int(e^z/z)dz$; $\int e^{e^z}dz$; $\int(1/\log z)dz$; $\int \log\log z\,dz$; $\int[(\sin z)/z]dz$.

Whereas Rosenlicht gave an algebraic proof of Liouville's theorem on functions with elementary integrals, R. H. Risch has actually furnished an algorithm for the theorem. By his own account, Risch was introduced to the subject of finite integration by Ritt's 1948 monograph. In a 1967 paper (published in 1969 as **[20]**), Risch presents an algorithm for that special class of elementary functions expressible without using irrational operations. In other words, the function must be constructed solely by means of rational operations, exponents, and logarithms: the algorithm is inapplicable if the exponents and logarithms can be replaced by adjoining constants and performing algebraic operations. Then, in **[18]** and **[19]**, algebraic operations are allowed, and Risch shows that the general problem of finite elementary integration reduces to a decidable question in the theory of algebraic functions. Although the complete account of Risch's algorithm—for deciding when an elementary function has an elementary integral, and obtaining it when it exists—has not yet been published, the author did describe (in 1970) some of the techniques and ideas involved **[21]**; the procedure as a whole results from combining the contents of **[18]**, **[19]**, and **[21]**. Risch has indicated that, whereas the algebraic case follows easily along the lines of **[21]**, the general case is a more complicated affair to carry out, and a simpler approach is desirable (one which might be found in the realm of algebraic geometry).

Today, a number of writers have published material on the topic of finite integration (and related questions), several incorporating aspects of Risch's result (see **[27]**, for example). Perhaps the greatest interest—because of the algorithmic nature of the solution—is among those in computer science. Risch makes the interesting suggestion that some features of his algorithm are suitable for presentation to calculus students. No calculus text at present provides this material, an omission that not only leaves the story of finite elementary integration incomplete, but deprives the calculus student of some valuable insights.

**References**


[1] Joseph Liouville, Mémoire sur la détermination des Intégrales dont la valeur est algébrique, J. Ecole Polytechnique, vol. 14, cahier 22, pp. 124–193, Paris. . . . . . . . . . 1833

[2] ______, Mémoire sur les Transcendantes Elliptiques de première et de seconde espèce considérées comme fonctions de leur amplitude, J. Ecole Polytechnique, vol. 14, pp. 37–83, Paris. . . . . . . . . . 1834

[3] ______, Mémoire sur la classification des transcendantes et sur l'impossibilité d'exprimer les racines de certaines équations en fonction finie explicite des coefficients, J. Math. Pures Appl., vol. 2, pp. 56–104, Paris. . . . . . . . . . 1837

[4] ______, Suite du Mémoire sur la classification des transcendantes et sur l'impossibilité d'exprimer les racines de certaines équations en fonction finie explicite des coefficients, ibid., vol. 3, pp. 523–546, Paris. . . . . . . . . . 1838

[5] ______, Sur les Transcendantes Elliptiques de première et de seconde espèce considérées comme fonctions de leur module, ibid., vol. 5, pp. 441–464, Paris. . . . . . . . . . 1840

[6] D. D. Mordukhai-Boltovskoi, Researches on the integration in finite terms of differential equations of the first order, Communications de la société mathématique de Kharkov, X, pp. 34–64, 231–269 (Russian). . . . . . . . . . 1906–09

[7] ______, On the Integration in Finite Terms of Linear Differential Equations, Warsaw, (Russian). . . . 1910

[8] ______, On the Integration of Transcendental Functions, Warsaw, (Russian). . . . . . . . . . 1913

[9] ______, Sur la résolution des équations différentielles du premier ordre en forme finie, Rend. Circ. Mat. Palermo, LXI, pp. 49–72. . . . . . . . . . 1937

[10] G. H. Hardy, The Integration of Functions of a Single Variable, 2nd ed., Cambridge Univ. Tracts in Mathematics and Mathematical Physics, no. 2, Cambridge, England. . . . . . . . . . 1916

[11] A. Ostrowski, Sur l'intégrabilité élémentaire de quelques classes d'expressions, Comment. Math. Helv., vol. 18, pp. 283–308. . . . . . . . . . 1946

[12] J. F. Ritt, On the integrals of elementary functions, Trans. Amer. Math. Soc., vol. 25, pp. 211–222. . . 1923

[13] ______, Integration in Finite Terms: Liouville's Theory of Elementary Models, Columbia Univ. Press, New York. . . . . . . . . . 1948

[14] Morris Kline, Mathematical Thought from Ancient to Modern Times, Oxford Univ. Press, pp. 411–422, New York. . . . . . . . . . 1972

[15] Maxwell Rosenlicht, Liouville's theorem on functions with elementary integrals, Pacific J. Math., vol. 24, no. 1, pp. 153–161. . . . . . . . . . 1968

[16] ______, Integration in finite terms, Amer. Math. Monthly, vol. 79, no. 9, pp. 963–972, November. . . 1972

[17] Robert H. Risch, On Real Elementary Functions, SDC document SP-2801/001/00, 22 May. . . . . . 1967

[18] ______, On the Integration of Elementary Functions which are Built Up Using Algebraic Operations, SDC document SP-2801/002/00, 26 June. . . . . . . . . . 1968

[19] ______, Further Results on Elementary Functions, IBM RC 2402 (#11698), 11 March. . . . . . . . . 1969

[20] ______, The problem of integration in finite terms, Trans. Amer. Math. Soc., vol. 139, pp. 167–189. . . 1969

[21] ______, The solution of the problem of integration in finite terms, Bull. Amer. Math. Soc., vol. 76, pp. 605–608. . . . . . . . . . 1970

[22] ______, Implicitly elementary integrals, Proc. Amer. Math. Soc., vol. 57, no. 1, pp. 68–90, May. . . . . 1976

[23] ______, Algebraic properties of the elementary functions of analysis, Amer. J. Math., vol. 101, no. 4, pp. 743–759, August. . . . . . . . . . 1979

[24] Michael Singer, Functions satisfying elementary relations, Berkeley dissertation. . . . . . . . . . 1974

[25] M. Rosenlicht and M. Singer, On Elementary, Generalized Elementary, and Liouvillian Extension Fields, Contributions to Algebra, Hyman Bass, Phyllis J. Cassidy, and Jerald Kovacic (Editors), Academic Press, pp. 329–342, New York. . . . . . . . . . 1977

[26] Michihiko Matsuda, Liouville's theorem on a transcendental equation $\log y = y/x$, J. Math. Kyoto Univ., vol. 16, no. 3, pp. 545–554. . . . . . . . . . 1976

[27] F. Baldassarri and B. Dwork, On second order linear differential equations with algebraic solutions, Amer. J. Math., vol. 101, no. 1, pp. 42–76, February. . . . . . . . . . 1979

# Qubic: 4×4×4 Tic-Tac-Toe

***Pruning the game tree of three-dimensional tic-tac-toe makes possible a computer-aided proof that the first player can always win.***


**Oren Patashnik**
*Bell Laboratories*
*Murray Hill, NJ 07974*

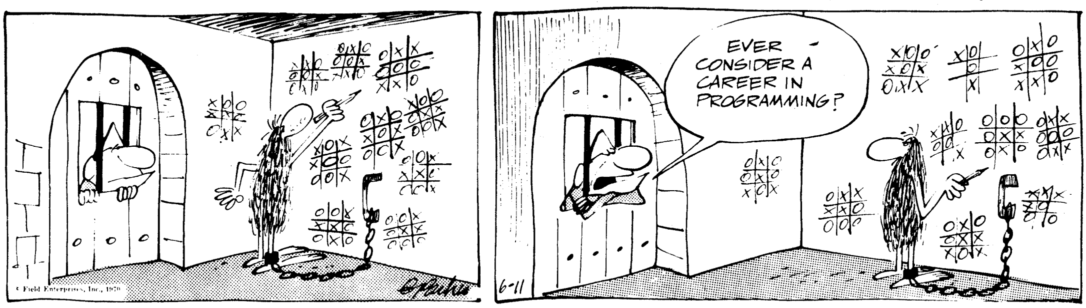

The computer is a powerful new tool for the mathematician. Its sheer size and speed make accessible many problems previously inaccessible (or at least unaccessed). The four-color theorem is a well-known example. In solving this problem Appel, Haken, and Koch **[1]**, **[2]**, **[3]** combined one hundred years of previous mathematical research with large high-speed computers to obtain a solution involving an intricate man-machine interaction. In this paper, we examine the problem of determining the outcome of 4×4×4 tic-tac-toe under optimal play. Not only is the problem itself interesting, but—as with the four-color theorem—so is the method of solution, which combines mathematics, human game-playing skill, and 1500 hours of computer time. We look first at the problem's mathematical background, then at the computer-aided solution, and finally at the solution's implications.

## Mathematical background

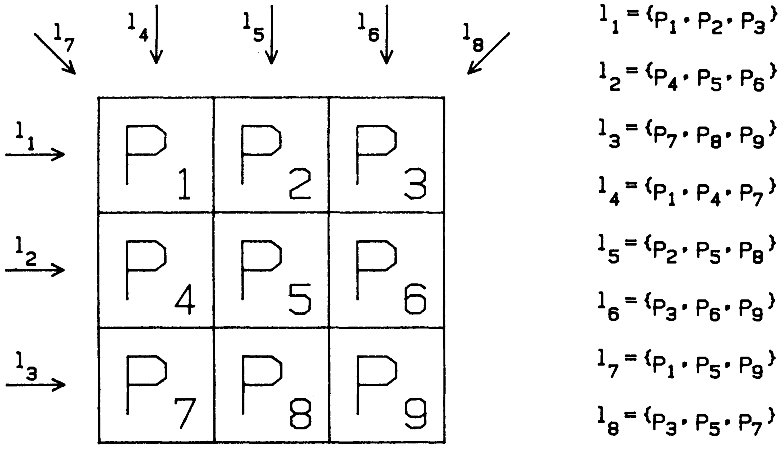
The familiar two-dimensional 3×3 tic-tac-toe has been played for a long time; in fact, we don't know its origins. One needn't play very long, though, to see that each player can force a draw if he or she plays properly. A more interesting version of tic-tac-toe is played in three dimensions on a 4×4×4 cube. (This game is marketed by Parker Brothers as Qubic; henceforth we refer to it as such.) Before examining Qubic, we discuss $q$-player positional games in general, 2-player $k^n$ tic-tac-toe games in particular.

A ***q*-player positional** game consists of a set $P$ of points (the board); a set $L$ of lines (the winning combinations), each a subset of $P$; and $q$ players who take turns choosing unchosen points from $P$ (i.e., moving) until either: (a) a player has chosen all the points in any line (that player wins), or (b) all the points in $P$ are chosen (the players draw). For example, regular tic-tac-toe for two players has nine points and eight lines, as shown in Figure 1. For a given

THE WIZARD OF ID by Brant parker and Johnny hart




THE WIZARD OF ID, by permission of Johnny Hart and Field Enterprises, Inc.




**The nine points and eight lines of $3^2$ tic-tac-toe.**

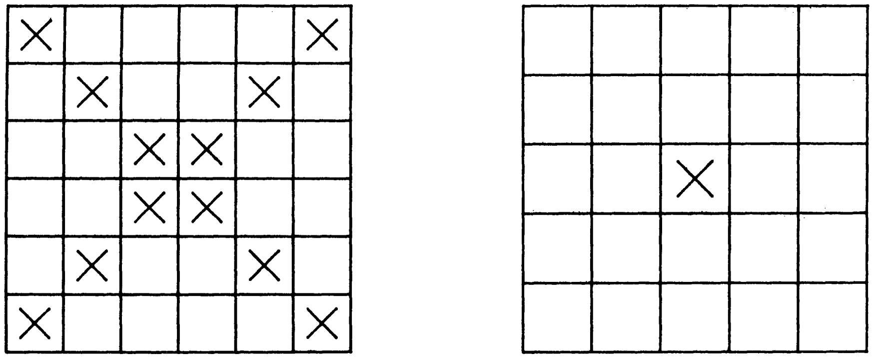
FIGURE 1

$q$-player positional game, our main problem of interest, known as the **strategy problem**, is: under optimal play, is the game a draw, and if not, which player wins? We restrict the strategy problem, however. Positional games with one player are trivial (the one player can always win if $L$ is nonempty, except in certain ethnic jokes), and positional games with three or more players are too complicated for analysis (it's not clear, for example, how the rules should handle coalitions). Accordingly, for the rest of this paper, we consider only 2-player positional games.

From game theory **[5]** we know that for any finite 2-player perfect information game, either the first player can force a win, the second player can force a win, or each player can force a draw. Furthermore, for positional games the second player can't force a win, as the following argument shows. Suppose the second player *can* force a win; that is, suppose the second player has a strategy $S$ that allows him to win no matter what the first player does. (Think of $S$ as an oracle that tells the second player which point to choose, given the first player's choice.) The first player can then "steal" strategy $S$ by choosing his first point at random and thereafter (a) following $S$, or (b) choosing another random point if $S$ dictates he choose the already chosen random point. In a positional game, having an extra point can't possibly harm the first player, since it neither hinders the first player nor helps the second player in forming a line. (There is one apparent exception: having an extra point may leave no unchosen point to choose at the game's end—that is, it may prevent the first player from choosing the last point when the board is full. In this case, however, this last point must be the first player's random point; the first player must *already* have won, then.) Thus by following $S$ the first player can always win, contradicting the assumption that the second player can always win. Therefore, the second player can't force a win in any positional game. Hence, for a given positional game, the strategy problem boils down to: can the first player force a win or can the second player force a draw?

The $k^n$ tic-tac-toe games (henceforth referred to as the **$k^n$-games**) form a subclass of the positional games (see Gardner **[10]** and Berlekamp, Conway, and Guy **[4]** for discussions of tic-tac-toe and related games). We can view a game in this subclass as an $n$-dimensional hypercube with $k$ cells on an edge, whose points $P$ are the centers of these cells and whose lines $L$ are the sets of $k$ collinear points. Regular tic-tac-toe (FIGURE 1) is the $3^2$-game and Qubic is the $4^3$-game.

For any $k^n$-game, the number $|P|$ of points is $k^n$, and the number $|L|$ of lines is $[(k+2)^n - k^n]/2$. The expression for the number of points is obvious; the expression for the number of lines is elegantly proved by Moser **[13]** as follows. Consider a $k^n$ hypercube $H$ whose lines we



**The points marked X are the strongest points in their respective games. In the $5^2$-game there are $(3^n-1)/2=4$ lines containing the strongest point. In the $6^2$-game there are $2^n-1=3$ lines containing each strongest point.**

FIGURE 2

want to count. Embed $H$ in a $(k+2)^n$ hypercube $H'$ so that $H'$ has a layer of cells on each side of $H$ and let $S$ be the shell of points in $H'$ surrounding $H$. The points in $S$ are those in $H'$ that are not in $H$, so there are $(k+2)^n-k^n$ points in $S$. For any line $l$ in $H$, its unique extension $l'$ to $H'$ (the only $l'$ in $H'$ containing all the points of $l$) contains exactly two points of $S$, one at either end of $l'$. Furthermore, for any point in $S$, exactly one line of $H$ extends to it (this requires a little thought). Hence, the lines of $H$ must number half the points of $S$, or $[(k+2)^n-k^n]/2$, as claimed. (Technically this expression for the number of lines fails for the $1^n$-games if $n>1$. We can, however, revise our definition of a line to include a notion of direction, making the expression valid; we avoid the details of this revision since they aren't crucial.)

Our last property, given without proof, concerns a **strongest-point**—one contained in the most lines (see FIGURE 2). How many lines, denoted by SPL (strongest-point lines), contain such a point? If $k$ is odd, there is a single strongest point; it is in the center of the hypercube. In this case

$$\mathrm{SPL}=(3^n-1)/2 \quad \text{if } k \text{ is odd.}$$

If $k$ is even, each point in a main diagonal is a strongest point (a main diagonal is a line containing opposite corner points of the hypercube). There are $2^{n-1}$ main diagonals; they are pairwise disjoint, so there are $k2^{n-1}$ strongest points. For each

$$\mathrm{SPL}=2^n-1 \quad \text{if } k \text{ is even.}$$

We can now consider the strategy problem for the $k^n$-games, summarized in TABLE 1. We divide the $k^n$-games into three classes. Class 1 consists of those games for which draws are impossible even under nonoptimal play; that is, no draw position exists. This means that the first player can always force a win in these games, since, as we saw earlier, the second player can't. Class 2 consists of those games for which a draw position exists but for which the first player can nevertheless force a win. Class 3 consists of those games for which the second player can force a draw. Thus, under optimal play, games in classes 1 and 2 are first-player wins, and games in class 3 are draws.

In a 1963 paper, Hales and Jewett **[11]** show, using Hall's well-known marriage theorem **[12]**, that the second player can force a draw if $k \geqslant 2\times\mathrm{SPL}$; that is, if

$$k \geqslant 3^n-1 \quad \text{if } k \text{ is odd,}$$

or

$$k \geqslant 2^{n+1}-2 \quad \text{if } k \text{ is even.}$$

Thus, these $k^n$-games belong to class 3 (draws). (Their argument uses the following pairing strategy: there exists a set of mutually exclusive pairs of points such that a player can't win

| Number of points in a line $k=$ | $2^k=$ | $n=1$ class | $n=1$ points / lines / strongest-point lines | $n=2$ class | $n=2$ points / lines / strongest-point lines | $n=3$ class | $n=3$ points / lines / strongest-point lines | $n=4$ class | $n=4$ points / lines / strongest-point lines | $n=5$ class | $n=5$ points / lines / strongest-point lines |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 1 | 1 / 1 / 1 | 1 | 1 / 4 / 4 | 1 | 1 / 13 / 13 | 1 | 1 / 40 / 40 | 1 | 1 / 121 / 121 |
| 2 | 4 | 3 | 2 / 1 / 1 | 1 | 4 / 6 / 3 | 1 | 8 / 28 / 7 | 1 | 16 / 120 / 15 | 1 | 32 / 496 / 31 |
| 3 | 8 | 3 | 3 / 1 / 1 | 3 (tic tac toe) | 9 / 8 / 4 | 1 | 27 / 49 / 13 | 1 | 81 / 272 / 40 | 1 | 243 / 1441 / 121 |
| 4 | 16 | 3 | 4 / 1 / 1 | 3 | 16 / 10 / 3 | 2, 3 (Qubic) | 64 / 76 / 7 | 2, 3 | 256 / 520 / 15 | 1, 2, 3 | 1024 / 3376 / 31 |
| 5 | 32 | 3 | 5 / 1 / 1 | 3 | 25 / 12 / 4 | 2, 3 | 125 / 109 / 13 | 2, 3 | 625 / 888 / 40 | 2, 3 | 3125 / 6841 / 121 |
| 6 | 64 | 3 | 6 / 1 / 1 | 3 | 36 / 14 / 3 | 2, 3 | 216 / 148 / 7 | 2, 3 | 1296 / 1400 / 15 | 2, 3 | 7776 / 12496 / 31 |
| 7 | 128 | 3 | 7 / 1 / 1 | 3 | 49 / 16 / 4 | 2, 3 | 343 / 193 / 13 | 2, 3 | 2401 / 2080 / 40 | 2, 3 | 16807 / 21121 / 121 |
| 8 | 256 | 3 | 8 / 1 / 1 | 3 | 64 / 18 / 3 | 3 | 512 / 244 / 7 | 2, 3 | 4096 / 2952 / 15 | 2, 3 | 32768 / 33616 / 31 |
| 9 | 512 | 3 | 9 / 1 / 1 | 3 | 81 / 20 / 4 | 3 | 729 / 301 / 13 | 2, 3 | 6561 / 4040 / 40 | 2, 3 | 59049 / 51001 / 121 |
| 10 | 1024 | 3 | 10 / 1 / 1 | 3 | 100 / 22 / 3 | 3 | 1000 / 364 / 7 | 2, 3 | 10000 / 5368 / 15 | 2, 3 | 100000 / 74416 / 31 |
| 11 | 2048 | 3 | 11 / 1 / 1 | 3 | 121 / 24 / 4 | 3 | 1331 / 433 / 13 | 2, 3 | 14641 / 6960 / 40 | 2, 3 | 161051 / 105121 / 121 |
| 12 | 4096 | 3 | 12 / 1 / 1 | 3 | 144 / 26 / 3 | 3 | 1728 / 508 / 7 | 2, 3 | 20736 / 8840 / 15 | 2, 3 | 248832 / 144496 / 31 |
| 13 | 8192 | 3 | 13 / 1 / 1 | 3 | 169 / 28 / 4 | 3 | 2197 / 589 / 13 | 2, 3 | 28561 / 11032 / 40 | 2, 3 | 371293 / 194041 / 121 |
| 14 | 16384 | 3 | 14 / 1 / 1 | 3 | 196 / 30 / 3 | 3 | 2744 / 676 / 7 | 3 | 38416 / 13560 / 15 | 2, 3 | 537824 / 255376 / 31 |
| 15 | 32768 | 3 | 15 / 1 / 1 | 3 | 225 / 32 / 4 | 3 | 3375 / 769 / 13 | 3 | 50625 / 16448 / 40 | 2, 3 | 759375 / 330241 / 121 |

**A summary of the strategy problem for the $k^n$-games, for small $k$ and $n$. For each game, the table gives the classes of which the game is possibly a member (the games in the outlined area are unsolved—they are possibly members of both classes 2 and 3). The table also gives for each game, top to bottom, the number of points, the number of lines, and the number of strongest-point lines.**

TABLE 1

unless he chooses both points of some pair; the second player prevents the first player from winning by choosing one point of a pair any time the first player chooses the other.)

Erdős and Selfridge [8] improve the Hales and Jewett result by showing (but not with a pairing strategy) that the second player can force a draw if $\mathrm{SPL}+|L|<2^k$; that is, if

$$(3^n-1)/2+\left[(k+2)^n-k^n\right]/2<2^k \quad \text{if } k \text{ is odd,}$$

or

$$2^n-1+\left[(k+2)^n-k^n\right]/2<2^k \quad \text{if } k \text{ is even.}$$

Hales and Jewett also show that, given a $k$, there exists an $n_k$ such that whenever $n \geqslant n_k$ the $k^n$-game has no draw position; these $k^n$-games are thus in class 1 (wins). (They don't specify values for $n_k$; however, we know that the minimum $n_k=k$ for $k=1,2,3$, but the minimum $n_4 \neq 4$.)

Paul [18] adds to another Hales and Jewett result to show that whenever $k \geqslant n+1$, a draw position exists; these $k^n$-games, then, belong either to class 2 (wins) or class 3 (draws). Paul improves this result for $n \geqslant 4$, showing that a draw position exists if $k \geqslant n$. (For a complete discussion of draw position existence and related issues, see [15], [16], [17], [18].)

These results support several conjectures:

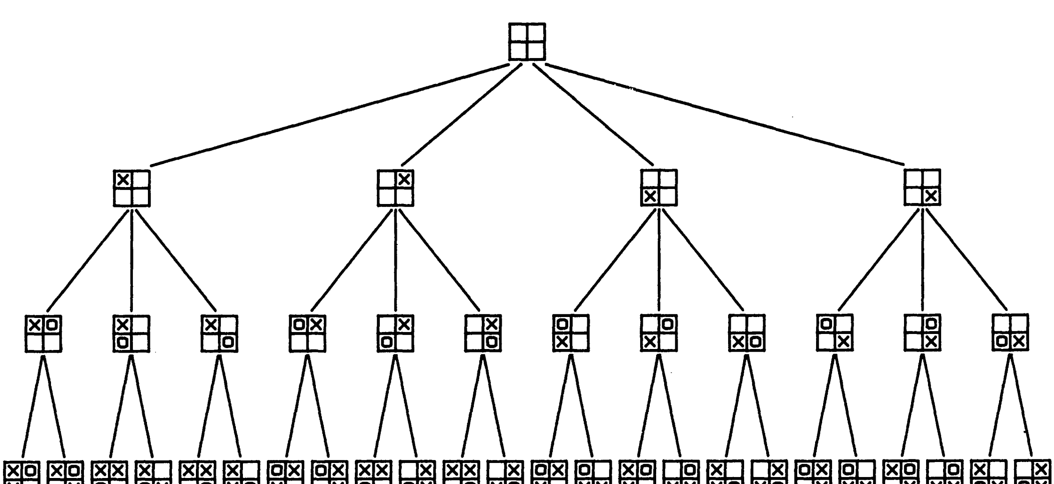
1. Hales and Jewett [11] conjecture that the second player can force a draw, because a pairing strategy exists, whenever there are at least twice as many points as lines (i.e., $k \geqslant 2/(2^{1/n}-1)$). (Proving this reduces to showing that a certain ratio, namely the number of lines in a subset of $L$ divided by the number of points aggregately contained in this subset, is a maximum when this subset is $L$ itself. Upon close inspection this ratio conjecture is very compelling, not only when a pairing strategy exists, but for any $k^n$-game.)
2. A modification of Gammill's conjecture [9] predicts that the second player can force a draw if and only if there are more points than lines (i.e., $k > 2/(3^{1/n}-1)$).
3. Citrenbaum [6] conjectures that the second player can force a draw if and only if there are more points in a line than there are dimensions (i.e., $k > n$).
4. A modification of conjecture 3 predicts that the second player can force a draw if and only if a draw position exists (i.e., it predicts that class 2 is empty).

These conjectures are consistent with all the information in TABLE 1, but differ on the strategy problem for the smallest unsolved member of the $k^n$-games, the $4^3$-game, Qubic: conjecture 2 predicts the first player can force a win; conjectures 3 and 4 predict the second player can force a draw. (Conjecture 1 makes no prediction for Qubic.) The next section describes my solution to the strategy problem for Qubic.

### Computer-aided solution to Qubic

The program I eventually used to solve the Qubic strategy problem evolved from an attempt to analytically prove Qubic a first-player win, which I "knew" was true from years of playing the game. Unable to find a purely analytic proof, I had to resort to a brute-force search, requiring a computer.

A brute-force search is based on a game tree, discussion of which demands some terminology. An ***r*-position** (sometimes just **position**) is an enumeration of the points of $P$ each player has



**The complete game tree for the $2^2$-game.**

FIGURE 3

chosen after $r$ total moves. An $r$-position is at **level $r$** of the game tree. A **terminal position** is one for which the game has ended. A **game tree** is a representation of all positions reachable, subject to a given set of restrictions, from the 0-position (no points chosen). Thus, a path from the 0-position to a terminal position in the game tree represents a single game. A **brute-force search** (sometimes just **search**) of a game tree, then, is an examination of every position of the game tree.

This terminology applies to a general game tree. Next, we discuss three specific game trees: a complete game tree and two successive refinements of it.

A **complete game tree** is a representation of all positions reachable from the 0-position, subject to no restrictions (except of course that points be chosen legally). FIGURE 3 shows the complete game tree for the $2^2$-game. A **naive brute-force search** is specifically a brute-force search of a complete game tree. (Abstractly, this entails examining all legally possible games.)

Using a naive brute-force search to determine the identity and location of the terminal positions in the complete game tree solves the strategy problem; that is, it tells us whether the first player can force a win or the second player can force a draw. A naive brute-force search for Qubic, however, becomes exponentially unreasonable. For example, after three total moves there are $64 \times 63 \times 62 = 249,984$ 3-positions in the complete game tree. Thus, I needed to refine the complete game tree, making the resulting search reasonable.

Although it's not clear that I made the brute-force search of Qubic reasonable (ten and a half months of brute forcing hardly seems reasonable), I *did* substantially reduce the size of the game tree. For example, instead of a quarter million 3-positions, my new game tree had only seven. I employed two processes to accomplish this reduction, corresponding to our two refinements of the complete game tree:

1. I restricted the set of first-player moves that the search examined (for a given position) to a single "winning" move (henceforth referred to as a **first-player move**).
2. I eliminated any position equivalent to one previously examined.

**FIGURE 4 shows a first player game tree for the $2^2$-game. There are only three terminal positions instead of the 24 for the complete game tree in FIGURE 3. Switching any two points leaves the set of lines unchanged in the $2^2$-game; thus, any such switch can't change the outcome of any game. FIGURE 5 shows the result of switching $p_2$ and $p_4$. FIGURE 6 shows a distinct-position tree for the $2^2$-game. Compare it to the trees in FIGURES 3 and 4.**

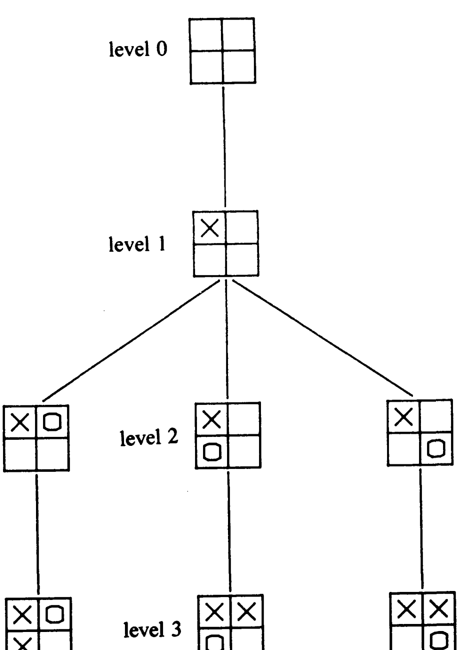



FIGURE 4

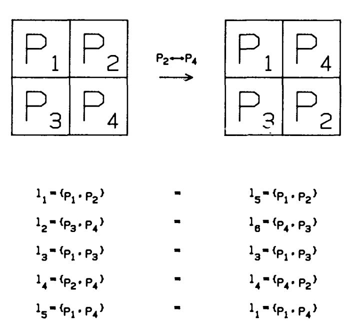



FIGURE 5

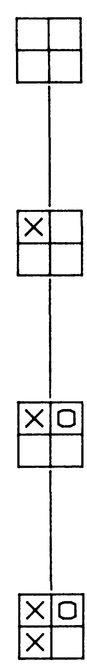


FIGURE 6

Process 1 followed from my belief that Qubic was a first-player win. I didn't need to search the complete game tree— I wasn't interested in how poorly the first player could play; I was interested only in his optimal play. Hence, to prove Qubic a first-player win, I needed only find a game tree, all of whose terminal positions were first-player wins, that placed no restrictions on the second-player moves. Thus, no matter what the second player did, the first player would win. This game tree, henceforth referred to as a **first-player game tree**, is our first refinement of the complete game tree. FIGURE 4 shows a first-player game tree for the $2^2$-game. Process 1 reduced the number of 3-positions from 24 in the complete game tree to three in the first-player game tree. For Qubic this reduction was from 249,984 3-positions in the complete game tree to $1\times 63\times 1=63$ in the first-player game tree.

Process 2 involved recognizing equivalent positions. Intuitively, the first two positions on level 2 in FIGURE 4 are equivalent—they are mere reflections of each other. Further reflection reveals that these positions are equivalent to the third position on level 2. To see this, consider the following. Since *any* two points constitute a line in the $2^2$-game, switching two points (or in fact any permutation of the points) leaves the set of lines unchanged (FIGURE 5 illustrates this, switching points $p_2$ and $p_4$). Thus, such a switch can't change the outcome of any game. Since the third position on level 2 is just a $p_2$—$p_4$ switch of the first position, it must be equivalent to the first (and therefore to the second). In fact, any one-to-one mapping of the set of four points onto

**FIGURE 7 shows two unintuitive automorphisms for Qubic. Identify the points by ordered triples: $X_1$ in the top position is $(1,1,1)$; $O_3$ is $(2,3,4)$. The left automorphism switches coordinate-value 2 with coordinate-value 3. The right automorphism switches 1 with 2, and 3 with 4. Thus the automorphisms map $X_1$ from $(1,1,1)$ to $(1,1,1)$ and $(2,2,2)$ respectively. They map $O_3$ from $(2,3,4)$ to $(3,2,4)$ and $(1,4,3)$ respectively.**

**FIGURE 8 shows the two distinct 1-positions for Qubic. On the first player's first move, the 16 points marked X are equivalent to each other—these are the strongest points for Qubic (compare this to FIGURE 2). The remaining 48 points are equivalent to each other. Thus, the first player has a choice of just two distinct moves, yielding only two distinct 1-positions for Qubic. (Of course, Qubic's distinct-position tree contains only the strong one.)**

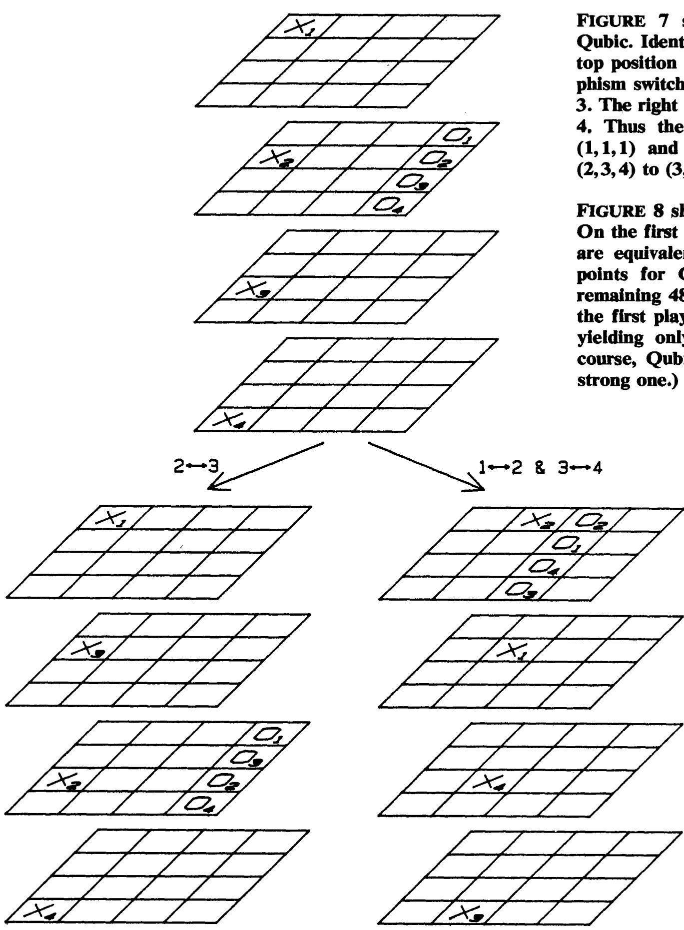



FIGURE 7

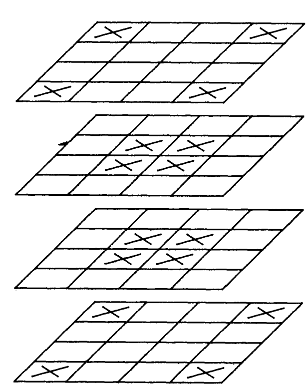


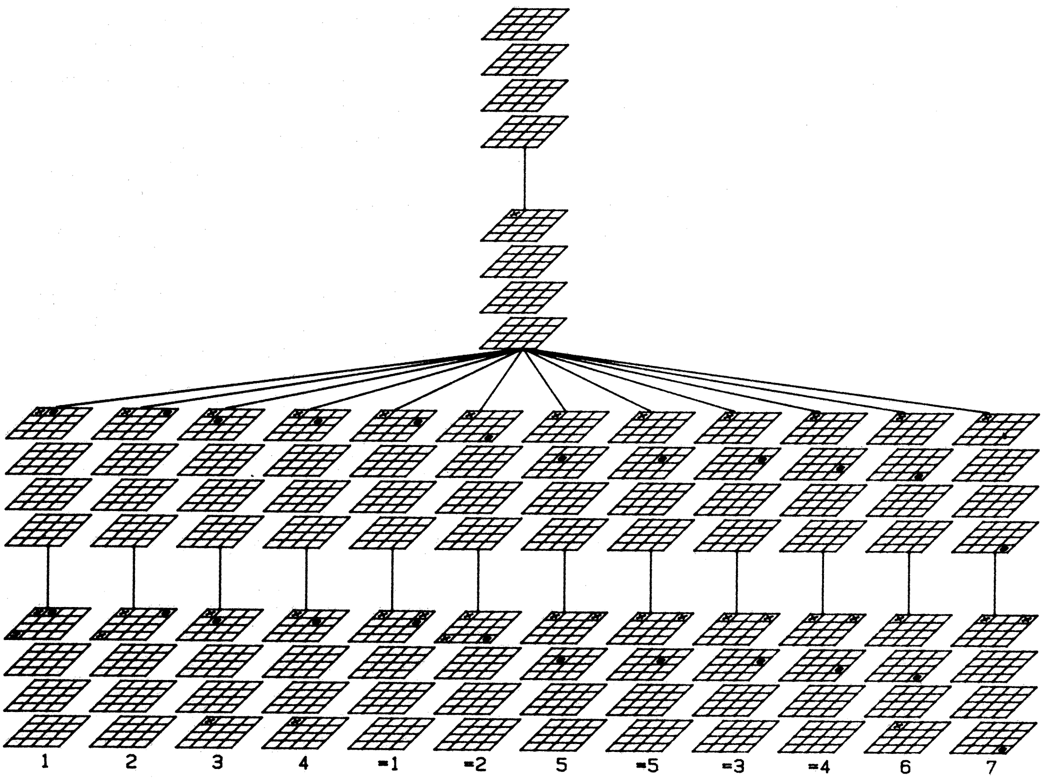
FIGURE 8

itself preserves the set of six lines, so there are $4! = 24$ transformations, or automorphisms, for the $2^2$-game.

An **automorphism**, then, is a one-to-one mapping of the set of points onto itself that preserves the set of lines. Two positions are **equivalent** if they are automorphic images of each other; one of these positions is **redundant**. We call a first-player game tree with redundant positions removed a first-player distinct-position game tree, **distinct-position tree** for short. This game tree is our second refinement of the complete game tree. FIGURE 6 shows a distinct-position tree for the $2^2$-game.

For Qubic, it turns out, there are 192 automorphisms, proved by Silver **[20]**. Just as some of the 24 automorphisms for the $2^2$-game are unintuitive, so are most of Qubic's 192 automorphisms. In fact, only 48 are ordinary rotations or reflections of the cube; the remaining 144 are combinations of these 48 with at least one of the two automorphisms shown in FIGURE 7. These 192 automorphisms yield only two distinct 1-positions, as indicated in FIGURE 8.

These automorphisms also yield only $1 \times 12 = 12$ 2-positions in the distinct-position tree for Qubic. Thus, I reduced the number of 2-positions in Qubic's three specific game trees from $64 \times 63 = 4032$ in the complete game tree, to $1 \times 63 = 63$ in the first-player game tree, to $1 \times 12 = 12$ in the distinct-position tree. It seems, then, there should be $1 \times 12 \times 1 = 12$ 3-positions in Qubic's distinct-position tree. However, by judiciously choosing the first-player moves for the twelve 2-positions, combining processes 1 and 2, I rendered five of these twelve redundant; this completed the reduction of the 249,984 3-positions in the complete game tree to the seven 3-positions in the distinct-position tree. FIGURE 9 shows the top four levels of my distinct-position tree for Qubic.




**Levels 0, 1, 2, and 3 of Qubic's distinct-position tree. There are only seven distinct 3-positions, reduced from twelve 2-positions by judiciously choosing first-player moves for these twelve positions.**

FIGURE 9

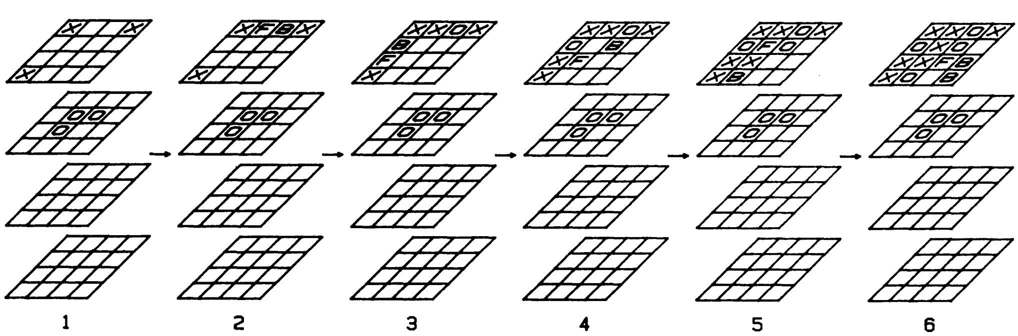
My problem, then, was reduced to finding a distinct-position tree for Qubic—a game tree, all of whose terminal positions were first-player wins, that made no restrictions on second-player moves, that restricted the first player to a single move for each position, and that contained no redundant positions. The only nonalgorithmic step in constructing such a tree was in finding the first-player moves. The rest—generating all possible second-player moves, removing redundant positions, and bookkeeping—was purely mechanical.

Initially I had planned to use a set of programmed heuristics to generate these first-player moves. ("Heuristics" comes from the Greek, *εὑρίσκειν*, to find **[14]**.) For several weeks I experimented with heuristics based on, for example, the number of lines and planes each player controlled. Unfortunately, the best set of heuristics I could find generated some moves worse than those I, as an experienced human player, could generate. Although finding a good set of heuristics would have been an interesting Artificial Intelligence problem, it didn't seem fruitful for proving Qubic a first-player win. I therefore had to abandon having my program make all the first-player moves—I had to make some of the first-player moves myself. We call these **strategic** moves.

My program was very good (perfect), however, at making certain first-player moves: at blocking a second-player three-in-a-row, and at finding a forced sequence (explained shortly) if one existed. These two types of moves, called **tactical** moves, comprised all but 2929 (the strategic moves) of the more than one million first-player moves made in the search. Thus, the most promising approach to proving Qubic a first-player win had my program making the tactical first-player moves, at which programs tend to be good, and had me making the strategic first-player moves, at which experienced humans tend to be good. (Incidentally, chess too shows these differing strengths of humans and computer programs. The human advantage in strategy is currently great enough to overcome the computer advantage in tactics: experts and masters, strategists, still beat the best programs, tacticians. Though the day of computer supremacy (in chess) is approaching, it seems this supremacy will arise not through strategic ("smart") programs, but through "smart" programmers using brute-force tactics.)

The two processes (choosing a single first-player move and eliminating redundant positions) kept the distinct-position tree small at the top levels (through level 5); they did not, however, change Qubic's exponential nature. In fact, the 192 automorphisms were virtually useless in reducing the tree size below level 5. Hence, to prevent this approach, too, from blowing up, I needed a third process—one to limit the search at lower levels of the tree.

Employing the forced-sequence search, alluded to above, was that process. A **forced sequence** is a sequence of moves from a given position, in which Player O must continually block Player X's three-in-a-row until at some move he or she must simultaneously block two such threes-in-a-



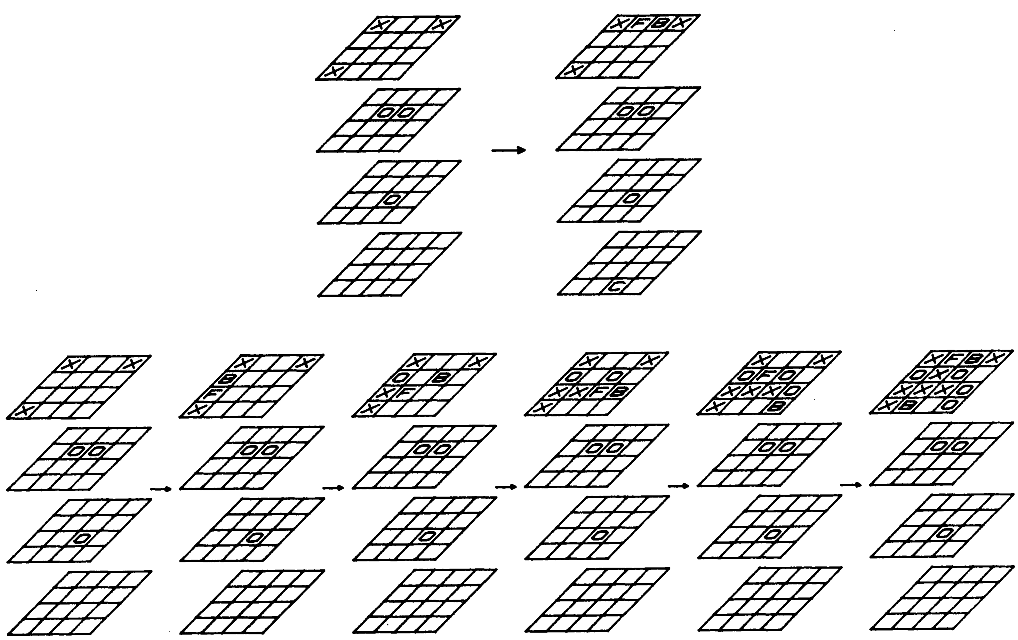

**A typical Qubic forced sequence. Player X's moves at *F* from each position continually force Player O to block at *B*, until Player O must block two threes-in-a-row in position 6; since this is impossible, Player O loses.**

FIGURE 10

row; this is impossible, so Player X wins. FIGURE 10 gives a typical example. (Note that a forced-sequence search is part of the overall search of the distinct-position tree.) A complication in finding a forced sequence may arise, however: Player O's block (of Player X's three-in-a-row) may give Player O a three-in-a-row, forcing Player X to block, typically ending the potential forced sequence. FIGURE 11 shows one such complication and its solution by reordering moves.

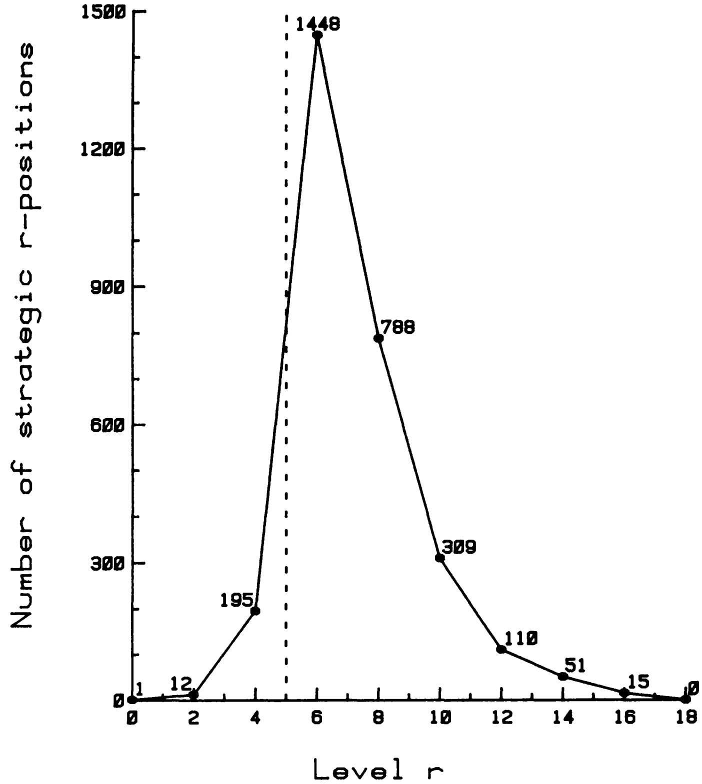
A forced-sequence search such as one shown in FIGURE 10 or 11 was very quick—such a search took a second or two of computer time. Some forced-sequence searches, however, took much longer, especially those for positions from which a forced sequence didn't exist. In fact, since the forced-sequence search had to find a forced sequence from a given position if one existed, to show that one did not exist from a given position, it had to examine *all* possible forced sequences. We saw that a naive brute-force search for Qubic (which examined the complete game tree) blew up because it had to examine *all* possible positions. Why, then, didn't the forced-sequence search blow up for some positions?

The answer has two parts. (Keep in mind that the forced-sequence search *was* at times precariously close to blowing up.) First: we saw that the naive brute-force search became a reasonable search when we refined the complete game tree to a first-player game tree; that is, we restricted one of the players (the first player in that case) to a single move for each position. For the forced-sequence search, the corresponding restriction was *implicit*; Player O being forced was implicitly restricted to a single move—to block the three-in-a-row or lose immediately. Thus the forced-sequence search, too, was reasonable. Second: the forced-sequence search was reasonable only if it was given a reasonable position from which to search; the positions from which it searched were reasonable because my strategic moves were good. The forced-sequence search, we saw, typically took only a second or two; however, for a few positions, it searched as long as half an hour. Hence, had my strategic moves been even slightly worse, the forced-sequence search would have blown up for a few positions.



**Complications arise in some forced sequences. In the top sequence, if Player X tries to win as in FIGURE 10, Player O's first block at *B* produces three-in-a-row, forcing Player X to block at *C*, ending the potential forced sequence. Player X can avoid this by reordering moves as in the bottom sequence.**

FIGURE 11




**The distribution of the 2929 strategic $r$-positions in Qubic's distinct-position tree. (A strategic $r$-position is one from which I made a strategic move.) Level 6 contained almost half; there were no strategic positions below level 16, eight moves by each player. The forced-sequence search took effect after the dotted line.**

FIGURE 12

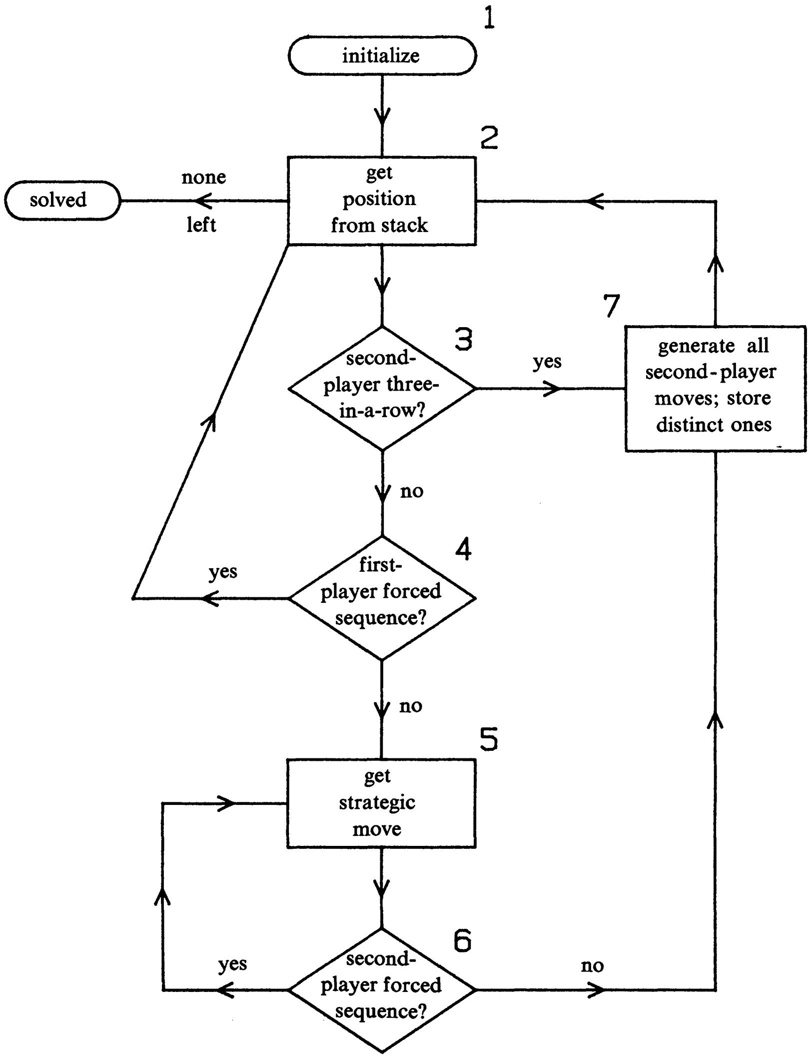
This explains why the forced-sequence search itself didn't blow up. It does not explain why the forced-sequence search kept the overall search of the distinct-position tree from blowing up below level 5. Very simply, the overall search didn't blow up below level 5 because most positions (roughly 98% of them) from which it was the first player's turn to move yielded a forced sequence (rendering further search from those positions unnecessary). To see this, consider an arbitrary $r$-position from which it was the first player's turn to move (that is, $r$ was even). It consisted of $r/2$ first-player points, which were chosen to be good, and $r/2$ second-player points, which were arbitrary and therefore likely to be lousy. Such an arbitrary $r$-position was therefore likely to yield a first-player forced sequence. Thus, positions terminated rapidly at lower levels of the distinct-position tree, keeping its search from blowing up.

FIGURE 12 shows Qubic's exponential nature. Since a forced sequence could exist after three moves by each player (as was the case in FIGURE 10), the forced-sequence search took effect after the dotted line (level 5). The jump between level 4 and level 6 would have been astronomical (instead of just enormous) had I not used the forced-sequence search.

My program, then, used the following algorithm (outlined in FIGURE 13) to construct and search the distinct-position tree for Qubic:

Step 1. Initialize: put the 0-position into the tree and onto the stack of unexamined positions. Go to step 2.

Step 2. Get the next unexamined position from the stack. If none, terminate the algorithm, the game is solved; otherwise go to step 3 (start examining).




**A flowchart for the Qubic algorithm.**

FIGURE 13

Step 3. Check for a second-player three-in-a-row (step 6 insures at most one). If one exists, go to step 7; otherwise go to step 4.

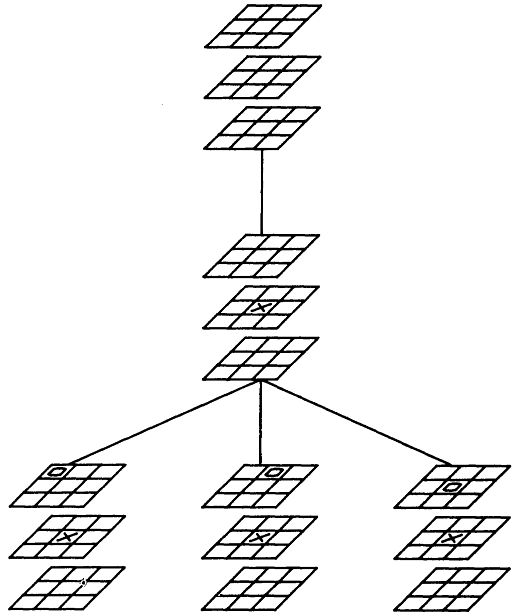
Step 4. Check for a first-player forced sequence. If one exists, add its positions to the tree and go back to step 2; otherwise go to step 5.

Step 5. Get a strategic move and go to step 6.

Step 6. Check for a second-player forced sequence. If one exists, complain and go back to step 5; otherwise go to step 7.

Step 7. Block a second-player three-in-a-row if one exists. Generate all possible second player moves and resulting positions. Remove redundant positions. Put the distinct positions into the tree and onto the unexamined-position stack. Go back to step 2.

To show the algorithm's simplicity, we use it to prove the trivial $3^3$-game a first-player win. (Of course, we must change "three-in-a-row" to "two-in-a-row" for the $3^3$-game.) FIGURE 14 gives the first three levels of the distinct-position tree we construct for this game.

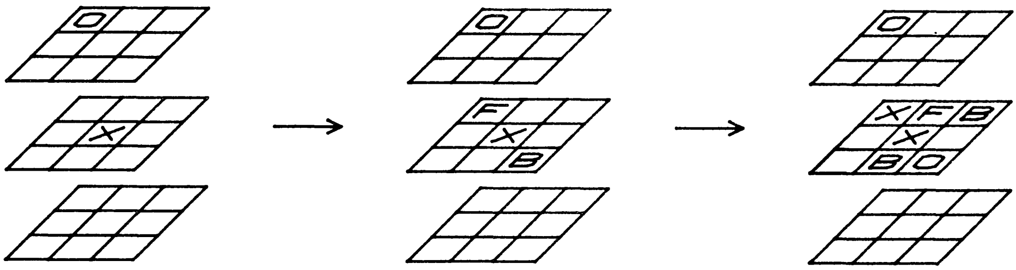


**Levels 0, 1, and 2 of the distinct-position tree for the $3^3$-game. Each position at level 2 yields a first-player forced sequence, so the $3^3$-game is a first-player win.**

FIGURE 14

1. Step 1—Put the 0-position into the tree and onto the unexamined-position stack.
2. Step 2—Get it from the stack.
3. Step 3—No second-player two-in-a-row.
4. Step 4—No first-player forced sequence.
5. Step 5—Get a strategic move. We know from the mathematical background section of the paper that the only strongest point for this game is the center point, so we choose it as our first (and only) strategic move.
6. Step 6—No second-player forced sequence.
7. Step 7—No second-player two-in-a-row. Generate all possible second-player moves and resulting positions. Remove redundant positions. Only three are distinct; put them into the tree and onto the stack.
8. Step 2—Get the first of these three from the stack.
9. Step 3—No second-player two-in-a-row exists.
10. Step 4—A first-player forced sequence exists (see FIGURE 15). Put its positions into the tree.
11. Step 2—Get the second of three from the stack.
12. Step 3—No second-player two-in-a-row exists.
13. Step 4—A first-player forced sequence exists, as before. Put its positions into the tree.
14. Step 2—Get the last of three from the stack.
15. Step 3—No second-player two-in-a-row exists.
16. Step 4—The same first-player forced sequence exists. Put its positions into the tree.
17. Step 2—The stack is empty; we have proved the $3^3$-game a first-player win.

Proving the $3^3$-game a first-player win, as above, would have taken a few seconds of computer time. Proving Qubic took a bit longer, about 1500 computer hours on the Yale




**A first-player forced sequence for the first 2-position in the distinct-position tree for the $3^3$-game; the other two 2-positions yield the same forced sequence.**

FIGURE 15

Computer Science Department PDP10, about half of which were wasted—occasionally I chose a bad strategic move and had to backtrack; more frequent mishaps ranged from memory parity errors (hardware problems) to tape-drive malfunctions (hardware problems). Even 750 unwasted computer hours, however, overestimates the time required to solve the problem by more than an order of magnitude. Had I known in advance it would have taken so long, I would have made my program faster by, for example, writing it in a lower level language instead of in Algol. Furthermore, the set of 2929 strategic moves I produced was not minimal. Given the hours I was generally allowed to use the machine (midnight to 8 A.M.—but far from complaining, I thoroughly appreciate the access to the machine at all), and my usual physical state (tired—I had to write an alarm into my program to wake me up for the strategic moves), I know that a better choice of strategic moves would slightly reduce 2929. Of my solution:

> 'twas much deeper than a well, and wider than a church door;
> 'twas more than enough, but it served. [**19**]

## Implications

The Qubic solution completes one more cell of TABLE 1: Qubic is the first known member of class 2, a $k^n$-game for which a draw position exists but for which the first player can nevertheless force a win; this disproves conjecture 4. This result also disproves conjecture 3—it shows that there exist first-player win $k^n$-games with $k>n$. The Qubic solution doesn't settle conjectures 1 or 2, although it supports conjecture 2. The strategy problem for the general $k^n$-game is still unsolved.

These are the solved problem's implications. The implications of the method of solution also merit discussion.

Why believe such a computer-aided result? After all, no one can possibly hand-check ten magnetic tapes of positions (body-check, maybe); no one can possibly prove that the 23 pages of Algol were correct, that the entire operating system was correct, and that the hardware functioned properly.

In an interesting, very readable, and highly recommended paper, DeMillo, Lipton, and Perlis [7] argue that a mathematical proof withstands a social process. The proof is believed, in successive stages, by the mathematician who discovered it, by colleagues, by journal reviewers, and finally by the general mathematical community. At each stage, the proof passes a test, gradually gaining acceptance.

The corresponding test for a computer proof such as mine (or Appel, Haken, and Koch's four-color theorem proof) is independent verification. For my proof, I gave Ken Thompson of Bell Laboratories a file of my 2929 strategic positions and moves. His *C* language program took "only" 50 hours on an Interdata 8/32 to verify the first-player win. In theory, his program did exactly what mine did, except that his program took the strategic moves from a file rather than from a human. In practice, his program was very different; it did, however, prove the same result.

Such verifications, in fact, may have advantages over verifications of some mathematical proofs. If a mathematician makes a subtle error in constructing a proof, a second mathematician is likely to miss the subtlety in inspecting the proof—the second mathematician's line of thinking is partly constrained by the first mathematician's line of thinking. However, two programmers working independently will be less likely to make identical errors in writing their programs. That is, one proof construction together with its dependent inspection is more error prone than two independent proof constructions.

Furthermore, certain mathematical proofs are inherently more error prone than their computer counterparts, regardless of verification. A 100-page existence proof for a certain group will much likelier contain an error than will an instance of the group, which the program finds after hours of searching. Thus, there are problems for which a computer proof seems preferred.

Finally, combining the respective strengths of humans and computers, fully exploiting the resources of both, may be the most (perhaps the only) feasible approach for solving certain problems; respective human and computer limitations may render approaches relying on either alone insufficient. The four-color theorem and the strategy problem for Qubic were two such problems. There will likely be others. The computer will remain an important mathematical tool.

**Acknowledgements**

I am deeply indebted to S. C. Eisenstat and the Yale Computer Science Department for allowing me to complete this project. At commercial rates, ten cents per kilo-core-second, the project would have cost me about fifty million dollars. I am also very grateful to K. Thompson for verifying my proof, and to E. R. Berlekamp, M. Gardner, R. L. Graham, J. B. Kruskal, and A. M. Odlyzko for their assistance and general encouragement in making the result known. Finally, I thank all those whose comments on earlier drafts greatly improved this paper.

**References**

[1] K. Appel and W. Haken, The solution of the four-color-map problem, Sci. Amer., 237, 4(Oct. 1977)108–121.
[2] ______, Every planar map is four colorable, Part I: Discharging, Illinois J. Math., 21(1977)429–490.
[3] K. Appel, W. Haken, and J. Koch, Every planar map is four colorable, Part II: Reducibility, Illinois J. Math., 21(1977)491–567.
[4] E. R. Berlekamp, J. H. Conway, and R. K. Guy, Winning Ways, Academic Press, Chapter 22 (to appear).
[5] D. Blackwell and M. A. Girshick, Theory of Games and Statistical Decisions, Wiley, New York, 1954, p. 21.
[6] R. L. Citrenbaum, Efficient Representations of Optimal Solutions for a Class of Games, Doctoral Dissertation, Case Western Reserve University, Univ. Microfilms International, 1970, pp. 116–7.
[7] R. A. DeMillo, R. J. Lipton, and A. J. Perlis, Social processes and proofs of theorems and programs, Comm. ACM., 22(1979)271–280.
[8] P. Erdős and J. L. Selfridge, On a combinatorial game, J. Combin. Theory Ser. A, 14(1973)298–301.
[9] R. C. Gammill, An examination of tic-tac-toe like games, AFIPS Confer. Proc., 43(1974)349–355.
[10] M. Gardner, The Scientific American Book of Mathematical Puzzles and Diversions, Simon & Schuster, New York, 1959, pp. 37–46.
[11] A. W. Hales and R. I. Jewett, On regularity and positional games, Trans. Amer. Math. Soc., 106(1963)222–229.
[12] P. Hall, On representatives of subsets, J. London Math. Soc., 10(1935)26–30.
[13] L. Moser, Solution to problem E 773 [1947, 281], Amer. Math. Monthly, 55(1948)99.
[14] Oxford English Dictionary, Oxford Univ. Press, New York, 1971.
[15] J. L. Paul, The $q$-regularity of lattice points in $R^n$, Bull. Amer. Math. Soc., 81(1975)492–494.
[16] ______, Addendum, The $q$-regularity of lattice points in $R^n$, Bull. Amer. Math. Soc., 81(1975)1136.
[17] ______, Tic-tac-toe in $n$-dimensions, this MAGAZINE, 51(1978)45–49.
[18] ______, Partitioning the lattice points in $R^n$, J. Combin. Th. Ser. A, 26(1979)238–248.
[19] W. Shakespeare, Romeo and Juliet, III. i. 97–98.
[20] R. Silver, The group of automorphisms of the game of 3-dimensional ticktacktoe, Amer. Math. Monthly, 74(1967)247–254.

# Fourier's Seventeen Lines Problem

BARBARA TURNER
*California State University*
*Long Beach, CA 90840*

Geometric combinatorial problems involving points and lines are known for their challenging and difficult properties. One such problem which was posed by Joseph Fourier may be neatly solved by using triangular numbers. In his outstanding biography of this great mathematical physicist, John Herivel, [**1**, p.244] relates that Fourier, at age twenty (1788), in a letter to his friend and teacher, C. L. Bonard, sent the following teaser: "Here is a little problem of a rather singular nature: it occurred to me in connection with certain propositions in Euclid we discussed on several occasions. Arrange 17 lines in the same plane so that they give 101 points of intersection. It is to be assumed that the lines extend to infinity, and that no point of intersection belongs to more than two lines." Fourier suggests analyzing the problem by considering the general case.

The large number of lines (17) makes the problem interesting and the construction not immediately apparent. Herivel, in a note to the letter [**1**, p. 246], states: "The data given by Fourier leads to an impossible 35 pairs of parallel lines. If 101 were an error for 131, the answer would be 5 pairs of parallel lines and 7 other lines." However, if more than 2 lines are allowed in a family of parallel lines, there is a solution to Fourier's problem as originally stated: for example, arrange the lines in 3 families of parallel lines, containing 5,5, and 6 lines respectively, with one other line (FIGURE 1a).

As Fourier suggests, one should be concerned with the general situation. The maximum number of points of intersection, given $n$ lines, occurs when each line intersects every other line and no point of intersection belongs to more than two lines. Thus, the $n$th line has $(n-1)$ points of intersection. If that line is removed, then any other line must have $(n-2)$ points of intersection with the remaining lines, etc. Hence, the maximum number of points of intersection for $n$ lines is

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

For 17 lines, the maximum is 136.

Consequently, if the number of points of intersection is not to be a maximum, some lines must be parallel (since Fourier stipulates that no point of intersection can belong to more than two lines). Let $j$ be the number of lines that have parallel mates. These can be arranged into $k$ mutually exclusive families of parallel lines, containing $j_1, j_2, \ldots, j_k$ lines respectively, where $j_1+j_2+\cdots+j_k=j$. Then the number $m$ of points of intersection is the total of those from the parallel part plus the others. Thus,

$$m=j_1j_2+(j_1+j_2)j_3+\cdots+(j_1+\cdots+j_{k-1})j_k+\frac{(n-1)n}{2}-\frac{(j-1)j}{2}.$$

Recalling that $j=j_1+j_2+\cdots+j_k$, and simplifying, we obtain

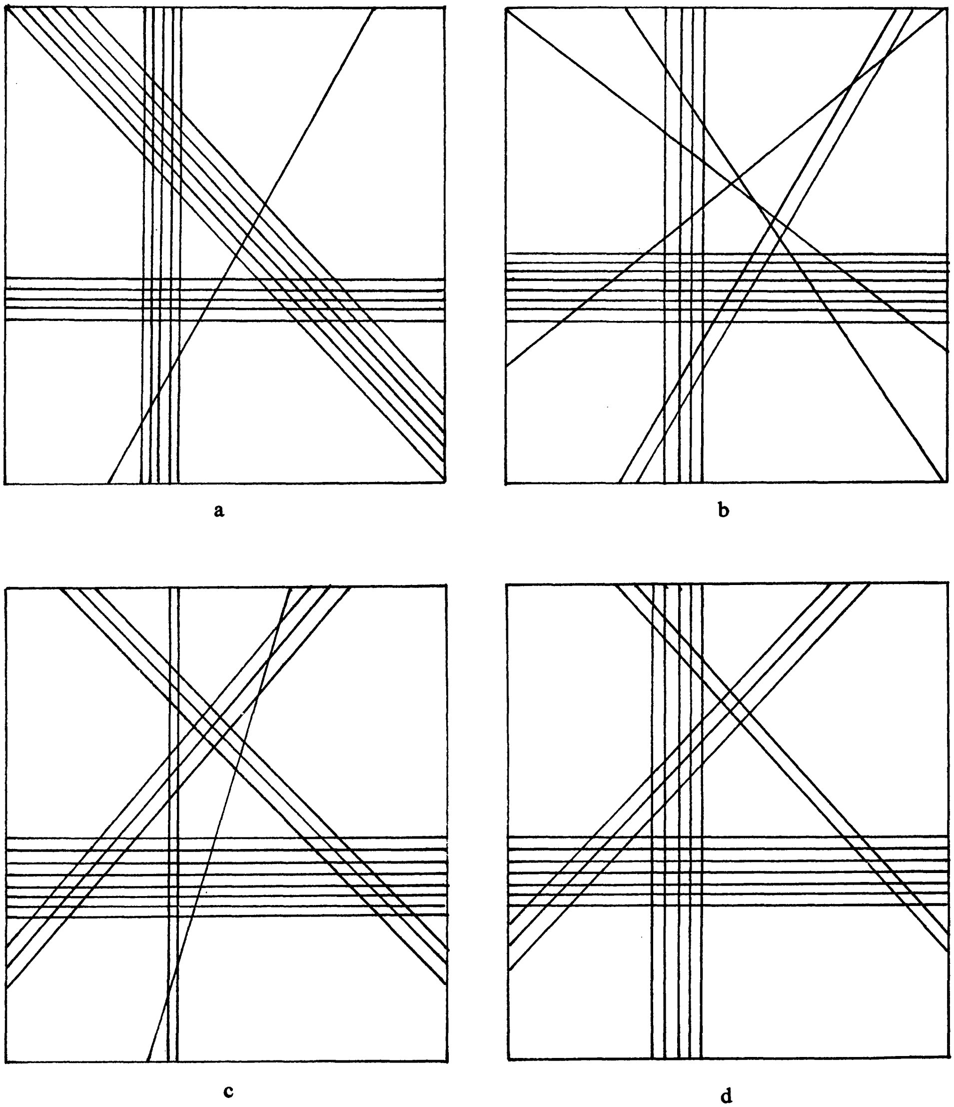
$$\frac{(n-1)n}{2}-m=\frac{(j_1-1)j_1}{2}+\frac{(j_2-1)j_2}{2}+\cdots+\frac{(j_k-1)j_k}{2}. \tag{1}$$

Thus a necessary condition for the solution of Fourier's general problem is that the difference between the maximum number of points of intersection, $(n-1)n/2$, and the desired number of points, $m$, is a sum of triangular numbers. The triangular numbers $(j_i-1)j_i/2$ in (1) have the following geometrical significance: when $j_i$ lines become parallel, this reduces the total number of points of intersection by $(j_i-1)j_i/2$.

Thus Fourier's problem, with $n=17$ and $m=101$, reduces from equation (1) to finding all integers $j_1, j_2, \ldots, j_k$ such that

$$\frac{(j_1-1)j_1}{2}+\frac{(j_2-1)j_2}{2}+\cdots+\frac{(j_k-1)j_k}{2}=35$$

and $j_1+j_2+\cdots+j_k \leqslant 17$.



The four solutions of Fourier's problem.

FIGURE 1.

It is easy to see that there are no solutions using only one or two families of parallel lines, since 35 is neither a triangular number nor the sum of two triangular numbers. By exhausting the possibilities among the triangular numbers less than 35, namely 1, 3, 6, 10, 15, 21, and 28 (corresponding to families of $j_i$ parallel lines where $j_i = 2, 3, 4, 5, 6, 7$, and 8 respectively), one finds that *there are exactly four solutions to Fourier's problem.* There are two solutions using 3 families of parallel lines. In addition to the solution given in FIGURE 1a, one can use 3 families of parallel lines, with 2, 4, and 8 lines respectively, and 3 other lines (FIGURE 1b). There are also two solutions involving 4 families of parallel lines. One solution uses families of 2, 3, 3, and 8 parallel lines, with one other line (FIGURE 1c), while the other uses families of 2, 3, 5 and 7 parallel lines (FIGURE 1d). Note that this last solution is the only one which does not require the addition of any nonparallel lines.

**Reference**

[1] J. Herivel, Joseph Fourier, The Man and The Physicist, Clarendon Press, Oxford, 1975.

# On the Enumeration of Cryptograms

SOLOMON W. GOLOMB
*University of Southern California*
*Los Angeles, CA 90007*

By a **cryptogram** we will mean a **substitution cipher**, which replaces each letter of the alphabet in the plaintext by a specific letter of the alphabet in the coded text. Thus the encipherment is specified by a particular permutation of the alphabet, which is applied consistently throughout the plaintext to produce the cryptogram. Decipherment is accomplished by applying the inverse permutation.

We adopt the convention (widely used in cryptography) that the "normalized cryptogram" for a given plaintext message is accomplished by replacing the first letter of the plaintext, everywhere it appears in the message, by "A", replacing the next distinct letter of the plaintext by "B", and so on. If $p$ is any plaintext message, and $c$ is a cryptogram of $p$, then both $c$ and $p$ have the same normalized cryptogram $n$. Thus, one cryptogram for MISSISSIPPI is PLVVLVVLSSL, obtained by the "Caesar cipher," which replaces each letter by the letter three positions later in the alphabet. However, applying the algorithm for obtaining the "normalized cryptogram" to either MISSISSIPPI or to PLVVLVVLSSL yields ABCCBCCBDDB. The question to be explored in this note is: How many different normal cryptograms can conceivably result from plaintext messages (sensible or not) of length $n$?

If the plaintext message consists of a single letter, its normalized cryptogram must be A. If the plaintext message consists of two letters, the normalized cryptogram may be AA or AB. For three-letter messages, the possible cryptograms are AAA, AAB, ABA, ABB, and ABC. If we let $b(n)$ denote the number of distinct normalized cryptograms of length $n$, then the sequence $b(n)$ begins $1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, \ldots$.

Suppose we let $S(n,k)$ denote the number of distinct normalized cryptograms of length $n$ in which exactly $k$ distinct letters appear. Thus $S(5,3) = 25$, with the distinct patterns being AAABC, AABAC, AABBC, AABCA, AABCB, AABCC, ABAAC, ABABC, ABACA, ABACB, ABACC, ABBAC, ABBBC, ABBCA, ABBCB, ABBCC, ABCAA, ABCAB, ABCAC, ABCBA, ABCBB, ABCBC, ABCCA, ABCCB, ABCCC. The numbers $S(n,k)$ are known [1] as the **Stirling numbers of the second kind.** For $1 \leqslant k \leqslant n \leqslant 10$, these are shown in TABLE 1. The sum of $S(n,k)$

TABLE 1

| $n \backslash k$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | $B(n)$ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | | | | | | | | | | 1 |
| 2 | 1 | 1 | | | | | | | | | 2 |
| 3 | 1 | 3 | 1 | | | | | | | | 5 |
| 4 | 1 | 7 | 6 | 1 | | | | | | | 15 |
| 5 | 1 | 15 | 25 | 10 | 1 | | | | | | 52 |
| 6 | 1 | 31 | 90 | 65 | 15 | 1 | | | | | 203 |
| 7 | 1 | 63 | 301 | 350 | 140 | 21 | 1 | | | | 877 |
| 8 | 1 | 127 | 966 | 1701 | 1050 | 266 | 28 | 1 | | | 4140 |
| 9 | 1 | 255 | 3025 | 7770 | 6951 | 2646 | 462 | 36 | 1 | | 21147 |
| 10 | 1 | 511 | 9330 | 34105 | 42525 | 22827 | 5880 | 750 | 45 | 1 | 115975 |

**The Stirling numbers of the second kind, $S(n,k)$, whose row sums are the Bell numbers $B(n)$.**

for $k$ from 1 to $n$ yields the values $B(n)$, which are known [1] as the **Bell numbers.** These are the same as the numbers $b(n)$, which count the number of distinct cryptogram patterns of length $n$, provided that $n \leqslant 26$. For $n > 26$, patterns using more than 26 distinct letters are counted in $B(n)$, but cannot occur in cryptograms based on a 26-letter alphabet. If we let $b_q(n)$ denote the number of distinct normalized cryptograms which are $n$ letters long and based on a $q$-symbol alphabet, then clearly

$$b_q(n) = \sum_{j=1}^{\min(n,q)} S(n,j). \tag{1}$$

Thus $b_q(n) = B(n)$ if and only if $q \geqslant n$.

To prove these assertions, it suffices to show that the Stirling numbers of the second kind, $S(n,k)$, do indeed count the number of cryptogram patterns on messages of length $n$ in which $k$ distinct symbols occur. The formula (1) for $b_q(n)$ then clearly follows, and we may regard $B(n) = \sum_{k=1}^{n} S(n,k)$ as the *definition* of the Bell numbers.

The Stirling number of the second kind, $S(n,k)$, is most conveniently defined [2] as the number of ways of partitioning a set of $n$ distinct objects into $k$ nonempty subsets. For the cryptogram enumeration problem, the $n$ distinct objects are the $n$ positions in the message; and two positions are put in the same subset if and only if they are occupied by the same letter of the alphabet. Thus $S(n,k)$ is the number of distinct cryptograms of length $n$ in which $k$ distinct letters occur.

It is known ([1], [2]) that $S(n,k)$ is given explicitly by

$$S(n,k) = \frac{1}{k!} \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n, \tag{2}$$

and satisfies the recursion $S(n+1,k) = kS(n,k) + S(n,k-1)$.

Cryptogram patterns inspire several intriguing word puzzles. From $S(5,4) = 10$, there are ten patterns for 5-letter English words containing four distinct letters. Examples of these ten patterns are: OOZED, EVERY, TASTE, SPOTS, WEEDS, NEVER, SERVE, SPOON, THERE, SHALL. The reader may find it entertaining to attempt to construct similar sets of words for other values of $S(n,k)$. Of the twenty-five patterns previously listed for $S(5,3) = 25$, nineteen correspond to words listed in a collegiate-size English dictionary. The three patterns containing triple letters, AAABC, ABBBC, and ABCCC, can be "decoded" into such comic-strip standbys as EEECK, PSSST, and WHEEE. The three remaining patterns, AABBC, AABCC, and ABBCC, each containing two double-letter pairs, are harder to interpret as English.

Cryptograms for amateur puzzlists frequently preserve the spaces between words from the plaintext. This suggests the problem of enumerating the cryptogram patterns containing spaces. (We assume that in such a cryptogram, neither the first nor the last position is a space, and that two spaces are never consecutive.) The number of ways to designate spaces in a message of length $n$ is then easily shown to be $f_n$, the $n$th term of the Fibonacci sequence, where $f_1=1, f_2=1$, and $f_n=f_{n-1}+f_{n-2}$ for $n>2$. Indeed, there can be no spaces in messages of length 1 or length 2 under our rules (hence $f_1=f_2=1$, corresponding to the no-space patterns of these lengths), and the number of patterns allowing spaces for length $n$, $n>2$, is the sum of the two previous cases, as is seen by considering whether the $(n-1)$st position in the message is to be a letter (which can be completed in $f_{n-1}$ ways) or a space (which can be completed in $f_{n-2}$ ways).

The number of ways that exactly $r$ spaces can occur in a message of length $n$ is clearly $\binom{n-r-1}{r}$, in view of the restrictions on the placing of the spaces. It is also well known (see [3]) that

$$\sum_{r=0}^{[(n-1)/2]}\binom{n-r-1}{r}=f_n. \tag{3}$$

If the message of length $n$ contains $r$ spaces, then it contains $n-r$ letters, which fall into $b_q(n-r)$ cryptogram patterns in which spaces are ignored. Thus, the total number of cryptogram patterns of length $n$, formed from a $q$-symbol alphabet, and allowing spaces to appear (where *space* is not counted in the alphabet size) is

$$m_q(n)=\sum_{r=0}^{[(n-1)/2]}\binom{n-r-1}{r}b_q(n-r). \tag{4}$$

If we assume that the alphabet contains an unlimited number of symbols, the number of distinguishable cryptograms of length $n$, allowing spaces to appear, is

$$M(n)=\sum_{r=0}^{[(n-1)/2]}\binom{n-r-1}{r}B(n-r). \tag{5}$$

The sequence $M(n)$ begins: $1,2,7,25,102,456,2219,11640,65364,390646,\ldots$. The patterns corresponding to $M(4)=25$ are:

| | | | | |
|---|---|---|---|---|
| AAAA, | AAAB, | AABA, | AABB, | AABC, |
| ABAA, | ABAB, | ABAC, | ABBA, | ABBB, |
| ABBC, | ABCA, | ABCB, | ABCC, | ABCD, |
| AA A, | AA B, | AB A, | AB B, | AB C, |
| A AA, | A AB, | A BA, | A BB, | A BC. |

Finally, we note that John Riordan has observed (in [4]) that the Bell numbers also count the number of inequivalent "rhyme schemes" in a verse of $n$ lines. The convention here (as with cryptograms) is to denote the rhyme sound at the end of the first line by $a$. If the second line rhymes with the first, it too is identified by $a$, otherwise by $b$; etc. This is clearly isomorphic to the cryptogram enumeration problem, except that the number of possible rhyme sounds is a much larger "alphabet" than the 26 letters of cryptograms. The fourteen-line Elizabethan (or Shakespearean) sonnet has the rhyme scheme *abab cdcd efef gg*. The Petrarchan sonnet, also fourteen lines, has the rhyme scheme *abbaabba* for the first eight lines (the "octet"), but any of a number of schemes, such as *cdecde*, or *cdcede*, or *cddece*, for the concluding six lines (the "sestet"). (If we drop the normalization convention of using the letters of the alphabet (in order) to represent the new rhyme sounds as they appear, then "*cdcede*" can be represented instead as "sestet.")

This research was supported in part by the United States Army under Grant No. DAAG 29-76-G-0190.

**References**

[1] J. Riordan, An Introduction to Combinatorial Analysis, Wiley, New York, 1958, pp. 34–49.
[2] C. L. Liu, Introduction to Combinatorial Mathematics, McGraw-Hill, New York, 1968, pp. 38–40.
[3] H. S. M. Coxeter, Regular Polytopes, Pitman, New York, 1948, p. 31.
[4] J. Riordan, A Budget of Rhyme Scheme Counts, Ann. New York Acad. Sci., vol. 319, Second International Conference on Combinatorial Mathematics (1979) 455–465.

# The Square Root of a $2 \times 2$ Matrix

**Bernard W. Levinger**
*Colorado State University*
*Fort Collins, CO 80523*

A basic heuristic principle in linear algebra is that all computations are possible for $2 \times 2$ matrices. Thus one can compute inverses, eigenvalues, and eigenvectors by manageable formulas. The purpose of this note is to give a simple formula for the square root of a $2 \times 2$ matrix as an application of the Cayley-Hamilton theorem.

The standard procedure for computing the square root of an $n \times n$ matrix $A$ is to diagonalize $A$, that is, to find an invertible matrix $P$ such that $P^{-1}AP = D$ is diagonal. In general, the matrix $D$ will have $2^n$ distinct square roots which are obtained by taking the square roots of the diagonal elements of $D$ with all possible choices of plus and minus signs. (The diagonal elements of $D$ are the eigenvalues of $A$ and the columns of $P$ are the corresponding eigenvectors of $A$.) If $D^{1/2}$ is any square root of $D$, it follows that $C = PD^{1/2}P^{-1}$ is a square root of $A$, that is, $C^2 = A$. If $A$ has multiple eigenvalues, it can happen that there are fewer than $2^n$ square roots, no square roots, or infinitely many square roots, depending on the Jordan normal form of $A$.

For a $2 \times 2$ matrix, it is possible to perform the above procedure by formula. Since the characteristic equation of $A$ is quadratic, one can solve for the eigenvalues of $A$ and hence $D$, $P$ and $D^{1/2}$ can be given explicitly. However, the computation can get quite messy, as the following example shows:

Let $A$ be the $2 \times 2$ matrix $\left(\begin{smallmatrix} 1 & 2 \\ 3 & 4 \end{smallmatrix}\right)$. The characteristic equation of $A$ is $\det(A - \lambda I) = \left|\begin{smallmatrix} 1-\lambda & 2 \\ 3 & 4-\lambda \end{smallmatrix}\right| = (4 - 5\lambda + \lambda^2) - 6 = \lambda^2 - 5\lambda - 2 = 0$, and the eigenvalues are $\lambda^{\pm} = \frac{1}{2}(5 \pm \sqrt{33})$. It is a little complicated to find the eigenvectors

$$x^+ = \begin{pmatrix} 4 \\ 3 + \sqrt{33} \end{pmatrix}, \qquad x^- = \begin{pmatrix} 4 \\ 3 - \sqrt{33} \end{pmatrix},$$

from which it follows that

$$P = \begin{pmatrix} 4 & 4 \\ 3 + \sqrt{33} & 3 - \sqrt{33} \end{pmatrix}, \qquad P^{-1} = \frac{1}{8\sqrt{33}} \begin{pmatrix} \sqrt{33} - 3 & 4 \\ \sqrt{33} + 3 & -4 \end{pmatrix}.$$

One can verify that $AP = PD$ or $A = PDP^{-1}$ where

$$D = \frac{1}{2} \begin{pmatrix} 5 + \sqrt{33} & 0 \\ 0 & 5 - \sqrt{33} \end{pmatrix}.$$

Let us choose

$$D^{1/2} = \frac{1}{2} \begin{pmatrix} \sqrt{10 + 2\sqrt{33}} & 0 \\ 0 & \sqrt{10 - 2\sqrt{33}} \end{pmatrix},$$

so $C = PD^{1/2}P^{-1}$ equals

$$\frac{1}{16\sqrt{33}} \begin{pmatrix} 4 & 4 \\ 3 + \sqrt{33} & 3 - \sqrt{33} \end{pmatrix} \begin{pmatrix} \sqrt{10 + 2\sqrt{33}} & 0 \\ 0 & \sqrt{10 - 2\sqrt{33}} \end{pmatrix} \begin{pmatrix} \sqrt{33} - 3 & 4 \\ \sqrt{33} + 3 & -4 \end{pmatrix}.$$

It takes considerable patience to compute

$$C = \frac{1}{4\sqrt{33}} \begin{pmatrix} \sqrt{33}\,\alpha - 3\bar{\alpha} & 4\bar{\alpha} \\ 6\bar{\alpha} & \sqrt{33}\,\alpha + 3\bar{\alpha} \end{pmatrix}$$

where $\alpha = \sqrt{10 + 2\sqrt{33}} + \sqrt{10 - 2\sqrt{33}}$ and $\bar{\alpha}$ is its complex conjugate, and even more to verify that $C^2 = A$.

The point of this example is to show that the standard method is too complicated. However, there is an easier way which works in the $2\times 2$ case. The Cayley-Hamilton theorem states that any matrix satisfies its characteristic equation. Thus, if $C$ is a $2\times 2$ matrix, then

$$C^2-(\operatorname{Tr} C)C+(\det C)I=0. \tag{1}$$

(Here $\operatorname{Tr} C$, the trace of $C$, is the sum of the diagonal elements.) If $C^2=A$, then $\det C=(\det A)^{1/2}$, so

$$(\operatorname{Tr} C)C=A+(\det A)^{1/2}I. \tag{2}$$

We can solve for $(\operatorname{Tr} C)$ by taking traces on both sides of (2)

$$(\operatorname{Tr} C)^2=\operatorname{Tr} A+2(\det A)^{1/2}. \tag{3}$$

This allows us to solve for $C$.

Let $A=\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then $\operatorname{Tr} A=a+d$ and $\det A=ad-bc$. We write $\Delta=(\det A)^{1/2}=\sqrt{ad-bc}$ and get $\operatorname{Tr} C=\sqrt{a+d\pm 2\Delta}$. If $a+d\neq \pm 2\Delta$, then (2) and (3) yield two square roots of $A$

$$C^{\pm}=(a+d\pm 2\Delta)^{-1/2}\begin{pmatrix} a\pm\Delta & b \\ c & d\pm\Delta \end{pmatrix}. \tag{4}$$

(Two additional square roots are $-C^{\pm}$ which gives four square roots in the general case.)

Thus in our example, $A=\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $\Delta=\sqrt{-2}$, (4) yields

$$C^{\pm}=(5\pm 2\sqrt{-2}\,)^{-1/2}\begin{pmatrix} 1\pm\sqrt{-2} & 2 \\ 3 & 4\pm\sqrt{-2} \end{pmatrix}.$$

(It is easy to check that $(C^{\pm})^2=A$, but it takes quite a bit of complex arithmetic to verify that $C^{+}$ agrees with $PD^{1/2}P^{-1}$.) (4) is a general formula for the square root of a $2\times 2$ matrix. The only thing that can go wrong is that $a+d\pm 2\Delta$ might vanish. This occurs precisely when $A$ has a repeated eigenvalue. (If the eigenvalues of $A$ are $\lambda_1$, $\lambda_2$, then $\lambda_1+\lambda_2=a+d$ and $\lambda_1\lambda_2=\det A=\Delta^2$. By the arithmetic-geometric mean inequality, $\frac{1}{2}|\lambda_1+\lambda_2|\geqslant\sqrt{|\lambda_1\lambda_2|}$ with equality only when $\lambda_1=\lambda_2$.) In this case our formula may or may not give a complete picture. There are three possibilities:

1. $a+d=0=\Delta$. Here (4) is worthless. $A$ has the double eigenvalue 0 and, if $A\neq 0$, $A$ has no square root. For, suppose $C^2=A$. By (3), $\operatorname{Tr} C=0$ and, by (2), $A=0$. It is not hard to find matrices which satisfy condition 1, for instance $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right)$. They are the square roots of the zero matrix (considered in case 3, below).
2. $0\neq a+d=\pm 2\Delta$ and $b\neq 0$ or $c\neq 0$. Here formula (4) gives complete information, but $A$ has only two square roots. $\lambda=(a+d)/2$ is a double eigenvalue of $A$ and $A$ is similar to $\left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$. For instance, if $A=\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, then $C^{+}=\frac{1}{2}\left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right)=\left(\begin{smallmatrix} 1 & 1/2 \\ 0 & 1 \end{smallmatrix}\right)$ is a square root of $A$, whereas $C^{-}$ makes no sense.
3. $0\neq a+d=\pm 2\Delta$ and $b=c=0$. Here $A=aI$. Here formula (4) breaks down. We obtain only two square roots of $A$, $a^{1/2}I$, from the formula, whereas there are actually infinitely many. Observe that if $C=\left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, then

$$C^2=\begin{pmatrix} \alpha^2+\beta\gamma & \beta(\alpha+\delta) \\ \gamma(\alpha+\delta) & \delta^2+\beta\gamma \end{pmatrix},$$

so that $C^2=aI$ whenever $\alpha+\delta=0$ and $\alpha^2+\beta\gamma=a$. There are infinitely many solutions of these equations for each value of $\alpha$. Thus $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 1/2 & 1 \\ 3/4 & -1/2 \end{smallmatrix}\right)$ are all square roots of $I=\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

One may also ask under what conditions the square roots of a real matrix are real. From (4), a sufficient condition in the general case is that $\Delta$ be real and $a+d>0$. This means that

$a+d>0$ and $\det A>0$. Since $|a+d|>2|\Delta|$, this condition is also necessary. However, when $A=aI$, one can find real square roots even when $a<0$. For instance, $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 5 \\ -1/5 & 0 \end{pmatrix}$ are square roots of $-I=\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Finally, we ask if there are possibilities of generalizing (4). The same method can be used to give an expression for an $n$th root of $A$, but it leads to an $n$th order polynomial equation for $\operatorname{Tr} C$ which must be solved to calculate $C$. This is not very attractive. To extend the method to higher order matrices appears to be much more difficult, because the characteristic equation of $C$ involves higher symmetric functions of the eigenvalues of $C$ in addition to the trace and determinant. Thus one would have to solve several equations in several variables. However, this just again serves to support our initial assertion that $\mathbb{C}^2$ is the best of all possible worlds.

# Will It Tile? Try the Conway Criterion!

**Doris Schattschneider**
*Moravian College*
*Bethlehem, PA 18018*

Several years ago Martin Gardner described a discovery by John H. Conway that proved very useful in determining which polyominoes (stuck-together squares) might pave the plane. Gardner [5] describes Conway's sufficient condition for a tile to pave the plane as follows:

> We examine a given [tile] to see if its perimeter can be divided into six parts, *a*, *b*, *c*, *d*, *e* and *f*, that meet the following requirements: (1) Two opposite edges, *a* and *d*, are 'parallel' in the sense that they are congruent and in the same orientation. (2) Each of the other four edges, *b*, *c*, *e* and *f*, is centro-symmetric; that is, they are unaltered by a 180° rotation around the midpoint. ...Any of the six edges may be empty (nonexistent).

The polyomino tile A in Figure 1 illustrates this. It turns out that this criterion applies even to tiles which are not polygons.

In my own investigations of tiling problems, I found this test an excellent one, yet it became apparent that certain tiles could fit this description and still fail to pave the plane. Tile B in Figure 1 is such an example. Clearly what is wrong is that the edges $a$ and $d$, which are congruent and parallel as required, cannot interlock with each other to fulfill the intention of that requirement. The somewhat ambiguous term "parallel" in Gardner's description seems to be the source of the problem. The use of this term might actually suggest that the endpoints of the edges $a$ and $d$ must form a parallelogram (Göbel's version in [6] actually states this); in fact, paving tiles can have these endpoints collinear. Tile C in Figure 1 is of this type; here the

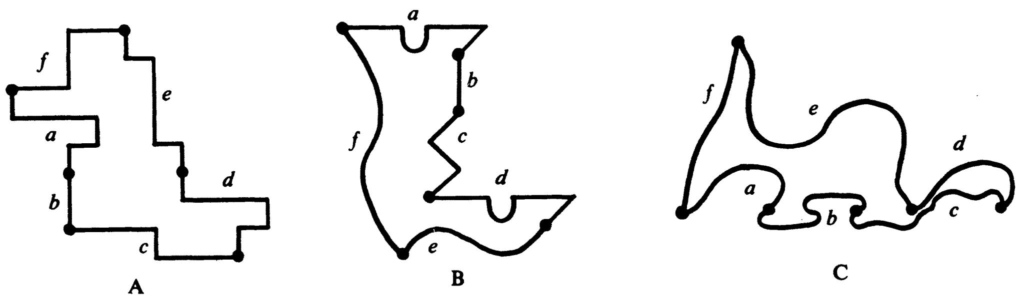



Figure 1

segments $a$ and $d$ are congruent by a *translation* (the usual definition of "parallel" in transformation geometry) along the line containing all four endpoints of $a$ and $d$.

In searching for a reformulation of the Conway Criterion that would remove these ambiguities, and explain how it works, I found that although the Conway test is by no means necessary for a tile to pave the plane, it actually characterizes those tiles which pave the plane "nicely" using only half-turns (180° rotations). This note presents my reformulation of the test (approved by John H. Conway) and focuses on why and how the criterion works. (R. Bantegnie states a similar version in [1].)

Throughout, a **tile** (noun) will be a closed topological disk in the plane with its boundary a simple closed curve. To **tile** (verb) or **pave** the plane with a tile T is to cover the plane with congruent images of T, without gaps of overlaps (except for boundaries), forming a jigsaw puzzle of infinite size called a **tiling by T**. If two points $v_i$, $v_j$ are on the boundary of a tile, we will denote by $\widehat{v_iv_j}$ that portion of the boundary which connects $v_i$ to $v_j$ and call $\widehat{v_iv_j}$ a **boundary segment**.

CONWAY CRITERION (CC). *A tile* T *can pave the plane by half-turns if there are six consecutive points* $v_1,\dots,v_6$, *at least three distinct, on the boundary of* T (*consecutive in the sense of traveling a cycle around the boundary*) *which satisfy the following conditions*:

(i) $\widehat{v_1v_2}$ *is congruent to* $\widehat{v_5v_4}$ *by a translation* $\tau$ *in which* $\tau(v_1)=v_5$ *and* $\tau(v_2)=v_4$.

(ii) $\widehat{v_2v_3}, \widehat{v_3v_4}, \widehat{v_5v_6}, \widehat{v_6v_1}$ *are centro-symmetric.*

*The* $v_i$ *are vertices of a tiling by* T *which is generated by half-turns about the midpoints of the centro-symmetric segments* (*and perhaps about some of the* $v_i$).

A tile which satisfies the two conditions of the Conway Criterion will be called a CC tile, and the tiling generated by the specified half-turns its CC tiling. Note that any CC tile will also satisfy the two conditions in Gardners's description, but by labeling vertices, rather than segments on the boundary, we can clarify the way in which the "parallel" segments must match. If the vertices (black dots) of the three tiles in FIGURE 1 are labeled consecutively, beginning with $v_1, v_2$ as endpoints of the boundary segment $a$, it is easily seen that tile B is not a CC tile, while tiles A and C are.

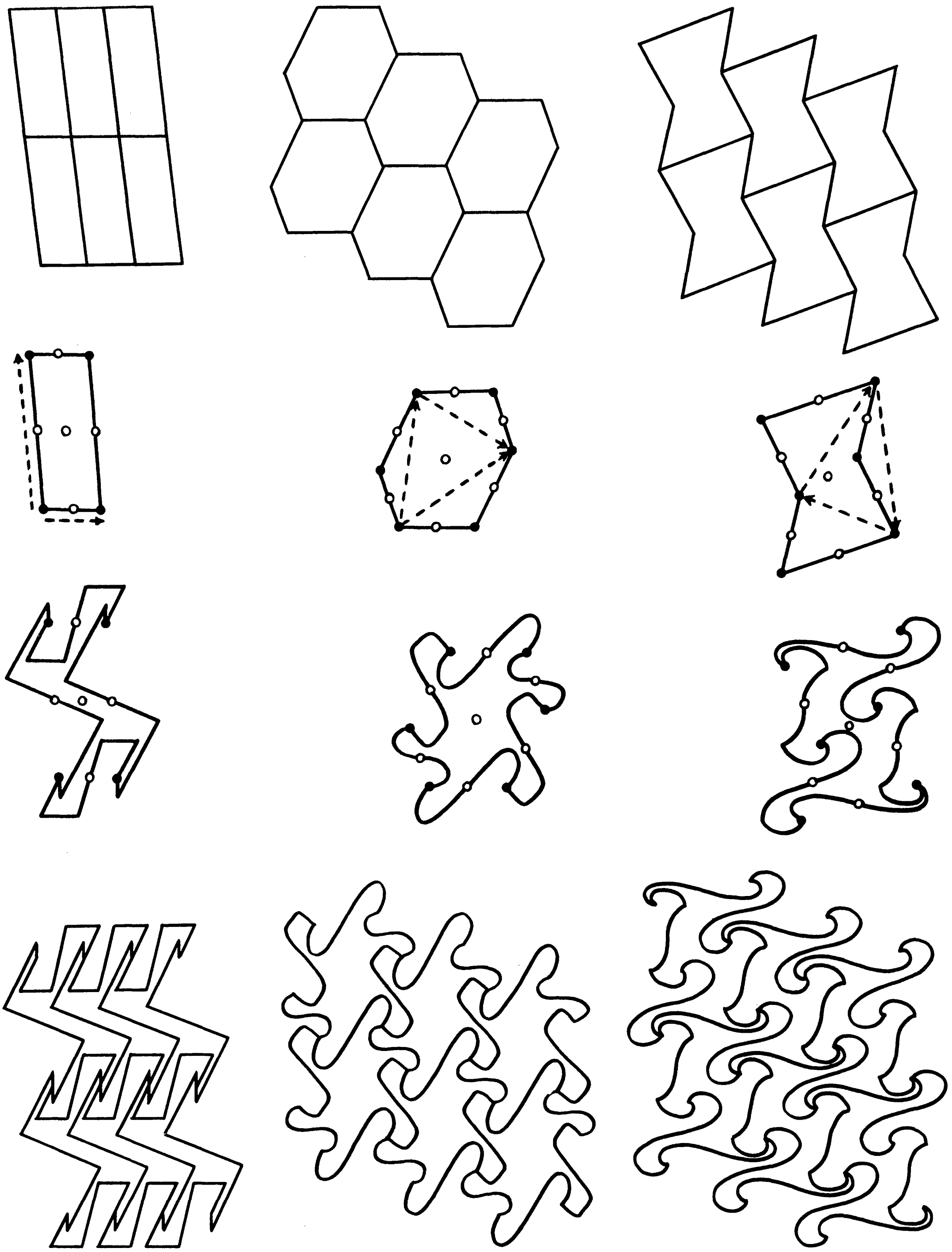
To explain why the criterion is sufficient, we begin by describing arbitrary tiles which pave the plane in the simplest manner. Such tiles are just translated in two directions, laid in parallel rows. The boundary of such tiles must be composed of matching pairs of "opposite" segments which interlock when the tile is translated. There can be only two pairs or three pairs of opposite matching boundary segments if we take the ends of the segments to be vertices of the tiling (i.e., a point in the tiling where at least three tiles meet). Coxeter proves this for convex polygon tiles **[4]**; Niven gives an even more general proof in **[10]**. Both proofs remain valid for arbitrary tiles if the term "vertex of a tile" is defined to be a point on the boundary which is a vertex of the associated tiling. Thus, the only tiles which pave the plane by successive translations in two directions are generalizations of parallelograms or par-hexagons (a convex or nonconvex hexagon with opposite sides equal and parallel).

Either a parallelogram tile or a par-hexagon tile can. also fill the plane by successive half-turns. This is because these tiles and their edges are centro-symmetric figures. The following facts are at work **[2]**:

($H+H$): the sum (composite) of two half-turns about points $x$ and $y$, respectively, is a translation whose vector is $2\overrightarrow{xy}$.

($T+H$): a translation $\tau$ followed by a half-turn about a point $y$ is equivalent to a half-turn about a point $x$ located so that the vector associated to $\tau$ is $2\overrightarrow{xy}$.

The next two observations are illustrated in FIGURE 2. Property ($H+H$) implies that a half-turn about a midpoint of an edge of one of these tiles combined with a half-turn about the center of the tile creates the translation which matches that edge to its opposite parallel edge, and moves

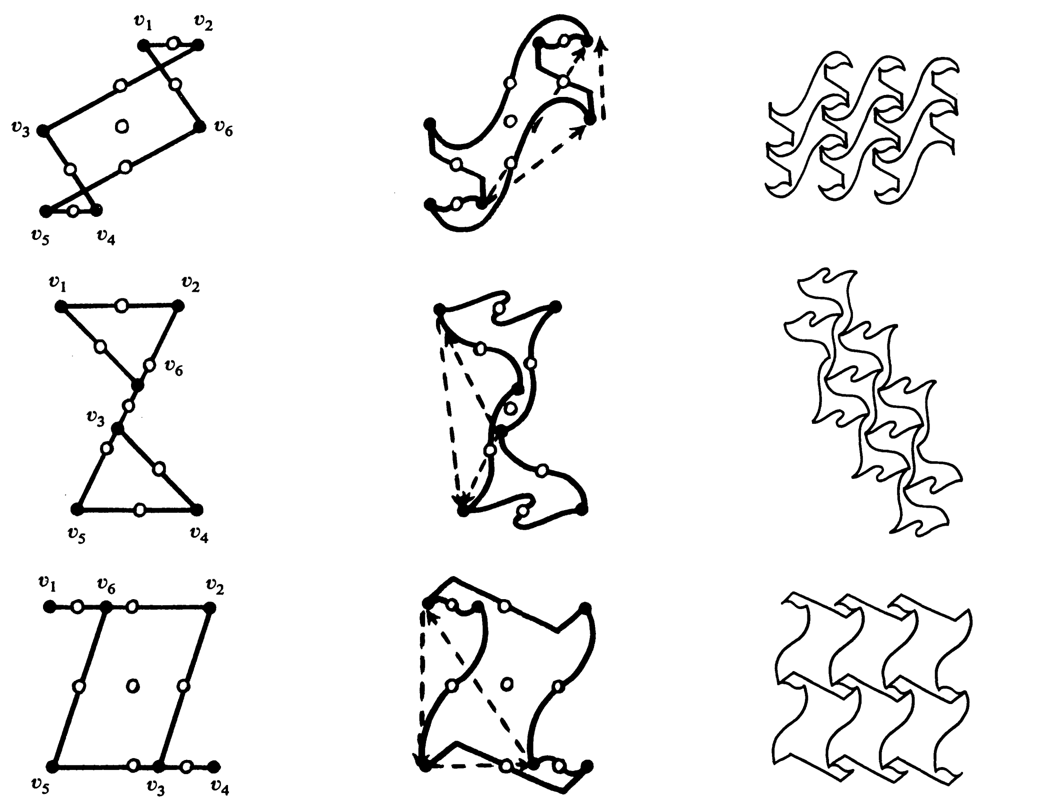


**Familiar tilings of the plane by parallelograms and par-hexagons. These polygons have opposite pairs of sides which match by translations (dotted vectors); each of these translations is the sum of two half-turns whose centers are located at midpoints of sides and at the center of the polygon (small circles). Replacing pairs of opposite edges of the polygons with congruent centro-symmetric segments produces $p2$ unit tiles which pave the plane using the same half-turns and translations.**

FIGURE 2

the tile to an adjacent tile. Properties $(H+H)$ and $(T+H)$ together imply that all sums of these successive half-turns will yield translations and half-turns which leave the tiling invariant. This is because the half-turn centers that are used to generate the tiling form a parallelogram lattice with edges of the parallelograms parallel to and one-half the length of the translation vectors which generate the tiling. If pairs of opposite edges of a parallelogram or par-hexagon are replaced by pairs of congruent boundary segments that are centro-symmetric, then this crucial placement of half-turn centers is preserved, and so a more general tile is created which can pave the plane by half-turns in the same manner. This description characterizes ***p*2 unit tiles**. The name "$p2$" refers to the type of symmetry group (generated by half-turns) which acts transitively on the tiles in the associated tiling **[12]**; the word "unit" refers to the fact that the translation subgroup of this group also acts transitively on the tiles of this tiling. FIGURE 3 shows that it is sometimes possible to create a $p2$ unit tile from a par-hexagon whose boundary is not a simple closed curve. You try to choose centro-symmetric boundary segments which join consecutive vertices so as to eliminate intersections.

We can now show why any CC tile paves the plane by half-turns as specified in the criterion. If such a tile is a $p2$ unit tile, in which case (i) is satisfied for opposite pairs of boundary segments and (ii) is satisfied by all boundary segments, it certainly tiles in this manner. For any other CC tile T, it is sufficient to show that a single half-turn about the midpoint of one of the centro-symmetric segments in (ii) creates a $p2$ unit tile $\bar{\mathrm{T}}$ whose associated tiling is generated by the half-turns specified in the criterion. By its construction, we at least know that $\bar{\mathrm{T}}$ is a centro-symmetric tile.




**Even a re-entrant or 'degenerate' par-hexagon whose boundary is not a simple closed curve may possibly give rise to a *p*2 unit tile. Vertices of the par-hexagons are labeled consecutively.**

FIGURE 3

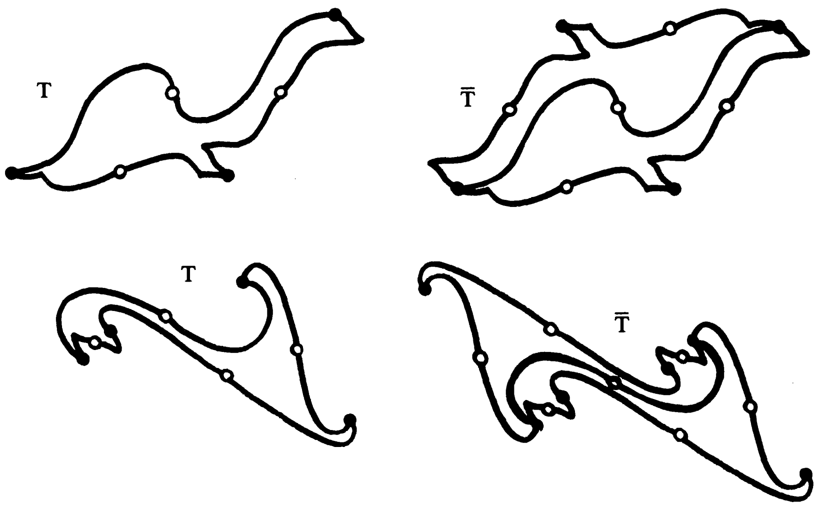



FIGURE 4

If on the one hand T is a CC tile with $v_1 = v_2$ (and $v_4 = v_5$), then the boundary of T consists of three or four centro-symmetric boundary segments. It seems obvious (see FIGURE 4) that the new tile $\overline{\mathrm{T}}$ is a $p2$ unit tile. In the first case, $\overline{\mathrm{T}}$ is a generalized parallelogram and in the second, a generalized par-hexagon. Actually, some elementary facts of geometry guarantee that the midpoints of the centro-symmetric boundary segments of $\overline{\mathrm{T}}$ form the correct parallelogram lattice required of a $p2$ unit tile. It is an easy exercise in analytic geometry to prove the following:

(1) If $p,q,r$ are three distinct points in the plane, and $m_1,m_2$ are the midpoints of the line segments $pq$ and $qr$, then $m_1m_2$ is parallel to $pr$ and $m_1m_2$ is one-half the length of $pr$.
(2) If $p,q,r,s$ are four distinct points in the plane, not all collinear, then the midpoints of the line segments $pq,qr,rs,sp$ form a parallelogram.

A proof of (2) for the case when no three of the four points are collinear appears in [3]. Note that both (1) and (2) remain true if the phrase "midpoints of the line segments" is replaced by "midpoints of the centro-symmetric boundary segments," since these midpoints are, in fact, the same points. Although the parallelogram of midpoints in (2) may be degenerate, collapsed on a line segment, this cannot occur in our case since the points $p,q,r,s$ are the vertices $v_i$ on a simple closed curve, the boundary of T. Thus in both cases T indeed tiles by half-turns about the midpoints of its centro-symmetric boundary segments.

If on the other hand T is a CC tile with $v_1 \neq v_2$ (and $v_4 \neq v_5$), then the segments $\widehat{v_1v_2}$ and $\widehat{v_5v_4}$

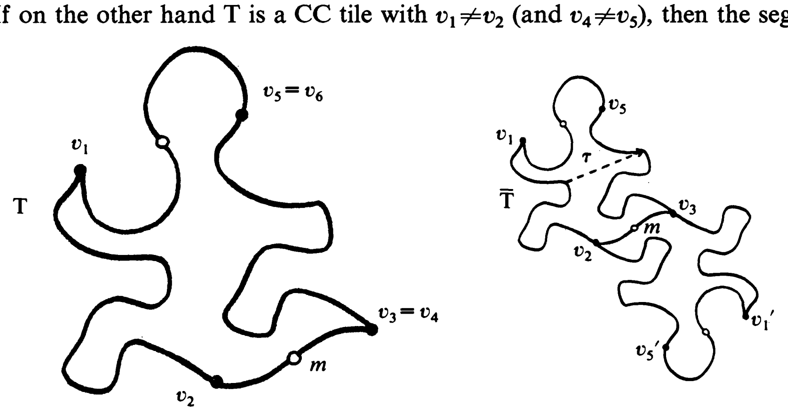



FIGURE 5

are congruent by the translation $\tau$, and two, three or four centro-symmetric boundary segments complete the boundary of T. Relabeling vertices if necessary, we may assume that we have chosen the midpoint $m$ of $\widehat{v_2v_3}$ about which to half-turn T to create $\overline{\mathrm{T}}$. To prove $\overline{\mathrm{T}}$ is the desired $p2$ unit tile, four different cases must be considered, determined by the number and location of distinct vertices of T (relative to $\widehat{v_2v_3}$). We prove one case below (FIGURE 5) and leave the remaining similar arguments to the reader (FIGURE 6).

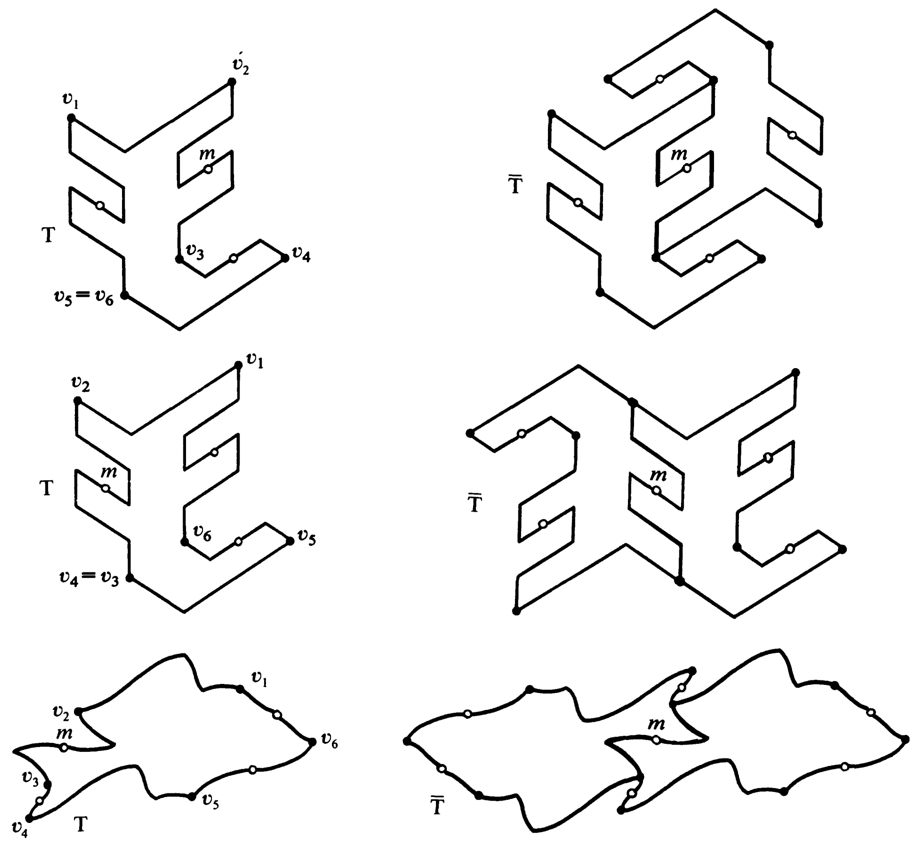



FIGURE 6

When T has two centro-symmetric boundary segments which join $\widehat{v_1v_2}$ and $\widehat{v_4v_5}$, then $v_3 = v_4$ and we can label $v_5 = v_6$. Denote by $h_m$ the half-turn about $m$, and let $v_1'$ and $v_5'$ be the images of $v_1$ and $v_5$ by $h_m$. Since $\tau(v_2) = v_4 = v_3$, property (T+H) implies that the sum of $\tau$ followed by $h_m$ is a half-turn about $v_2$. This shows that the boundary segment $\widehat{v_1v_2v_5}'$ of $\overline{\mathrm{T}}$ is centro-symmetric about $v_2$. Since $\overline{\mathrm{T}}$ is centro-symmetric, and has two pairs of "opposite" centro-symmetric boundary segments (namely $\widehat{v_1v_5}$ and $\widehat{v_5'v_1'}$ and $\widehat{v_1v_2v_5'}$ and $\widehat{v_5v_3v_1'}$), $\overline{\mathrm{T}}$ is a $p2$ unit tile which paves by half-turns about the midpoints of $\widehat{v_1v_5}$, $\widehat{v_2v_3}$, and the vertex $v_2$ of T.

We now turn to the converse and ask which tiles must be CC tiles? Since a CC tile T or its double tile $\overline{\mathrm{T}}$ is a $p2$ unit tile, our earlier remarks show that the half-turns which generate its CC tiling leave that tiling invariant. It is also possible for a tile to pave by half-turns in a "sloppy" way. For example, the tiling by triangles in FIGURE 7 can be continued (randomly shifting rows) to insure that although each triangle half-turns into each of its neighbors, none of these half-turns leaves the tiling invariant.

The Conway Criterion actually characterizes those tiles which pave "nicely" by half-turns: *If a tile* T *paves the plane by half-turns which leave the tiling invariant, then T is a CC tile.* If a tile

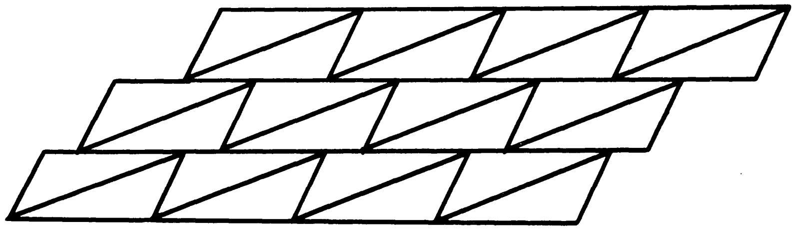


FIGURE 7

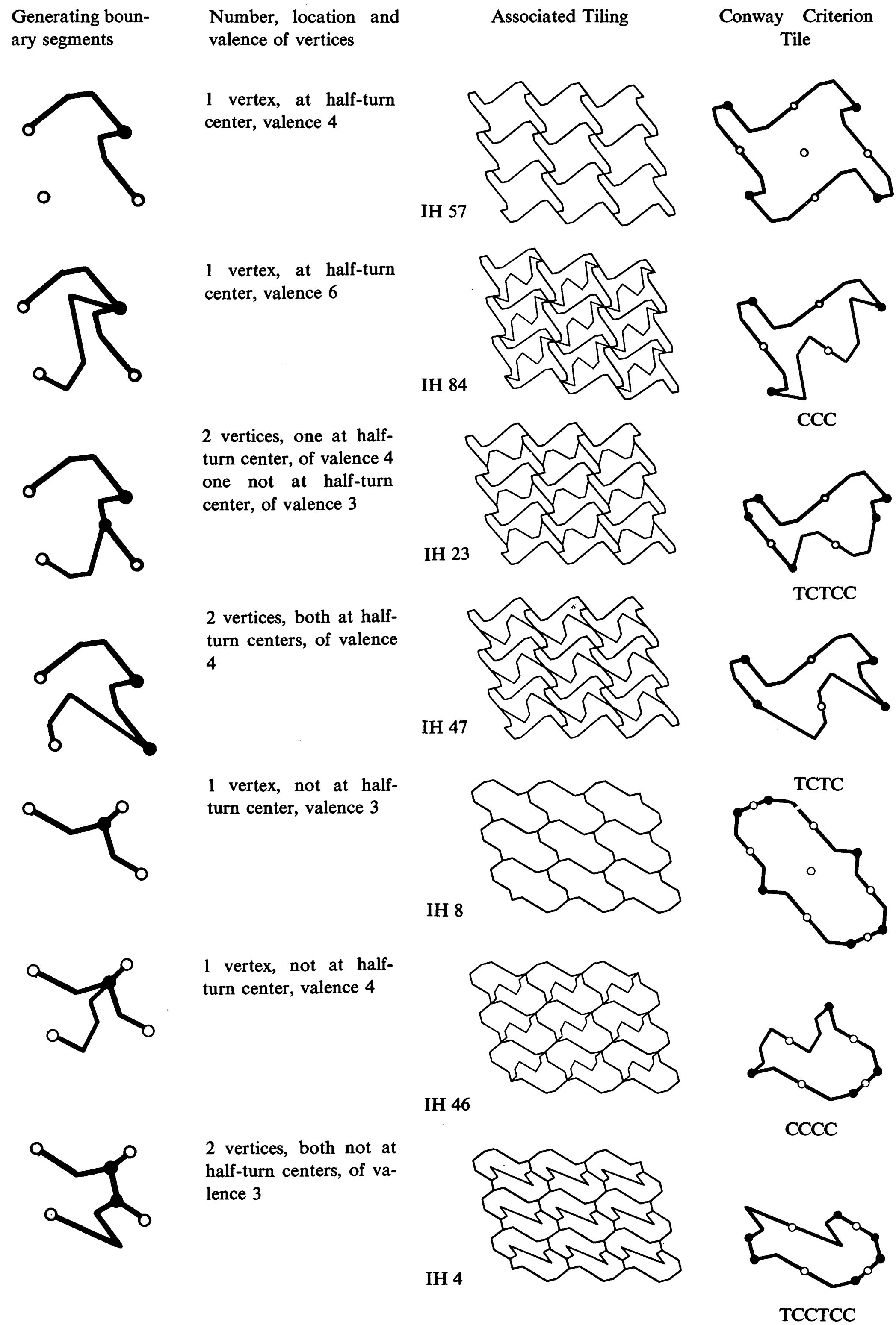
paves by such half-turns, then these motions generate a subgroup of the symmetry group of the tiling which acts transitively on the tiles. Tiles which have $p2$ isohedral tilings (a $p2$ symmetry group acts transitively on the tiles) are shown in [7] and [8]; the results there verify our statement above. Since details are missing in these references, we offer a constructive proof which also shows how, by hand or by using computer graphics equipment, $p2$ isohedral tilings can be created.

If T is a tile which paves by half-turns, then the centers of these half-turns must be located on the boundary of T (a point about which T half-turns into an adjacent copy of T) or at the "center" of T (a point about which T half-turns onto itself). If the half-turns must leave the tiling invariant, then three half-turns about noncollinear centers will generate the whole tiling; these centers are carried into a lattice of half-turn centers for the whole tiling. To show that T must be a CC tile, we create tilings by such a tile T, then examine all of the "distinct" ways in which this can be done.

Beginning with three noncollinear half-turn centers, properties $(H+H)$ and $(T+H)$ imply that the sum of these three half-turns creates a fourth half-turn whose center completes a parallelogram of half-turn centers. Joining three or all of these centers with curves creates connected segments which, when acted on by the group $G$ generated by these half-turns, form a planar network enclosing tiles. We will call these arbitrary curves chosen to connect the half-turn centers **generating boundary segments**. In choosing the generating boundary segments, care must be taken so that the resulting tiling will be one for which the group $G$ acts transitively on the tiles. In this way, we create a tiling by a single tile T which paves the plane "nicely" by half-turns. A little thoughtful experimentation easily yields all the distinct ways in which generating boundary segments can connect the half-turn centers in the desired manner. If we classify generating boundary segments according to the location of vertices of the associated tiling (relative to the half-turn centers) and the valences of these vertices, then there are just seven distinct types (FIGURE 8). The choice for the shapes of the generating boundary segments is limitless. All of the types of $p2$ isohedral tilings listed in [7] are accounted for in this scheme and, in addition, it is clear that each of the 7 types of tiles created satisfies Conway's Criterion.

In FIGURE 8 we have chosen to have the generating half-turn centers (small circles) form the same parallelogram for all seven cases. In addition, the first four tiles share some of the same boundary segments, and the last three tiles share some of the same boundary segments. This illustrates how the different types are related. Black dots on the generating boundary segments become vertices of the tile T and its tiling; all vertices of T and of its associated tiling are images of these by elements in the group $G$.

We close with some remarks on the nature of the Conway Criterion and an open question. Why is the test so useful? Its power in deciding if stuck-together squares, triangles and hexagons might tile is not too surprising, since boundaries of such tiles have a high probability of containing centro-symmetric segments. But it is a good first test to try on any tile since 10 of the 17 plane symmetry groups contain a subgroup generated by half-turns [12]. In analyzing the boundary of a tile, you look for centro-symmetric curves; those which are not line segments have characteristic zig-zag, stairstep, or $S$ shapes. FIGURE 9 shows that there may be several




**Creation of the seven distinct types of $p2$ isohedral tilings. The symbol next to each tiling is the classification number of Grünbaum and Shephard. The symbol under the five tiles which are not $p2$ unit tiles is that of Heesch and Kienzle.**

FIGURE 8

distinct ways of choosing the $v_i$ on the boundary of a tile to meet the Conway Criterion and each choice produces a different CC tiling. If a tile T fails the test, T may pave the plane with no half-turns, or a block of copies of T may form a CC tile. Gardner **[5]** discusses this, and **[7]**, **[8]**, and **[1]** provide useful diagrams and formulations of other criteria which suffice for a tile to pave the plane.

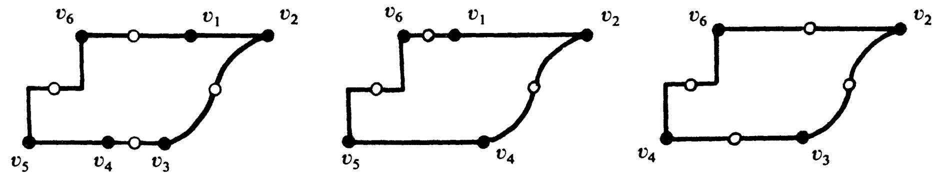



FIGURE 9

Creating tiles using the Conway Criterion (as I did for this note) can be great fun. Since all triangles and quadrilaterals are CC tiles, as are some pentagons and hexagons, new CC tiles can be created from them by altering their sides in an obvious way. This technique is described in **[11]**, but why it works is, unfortunately, not explained. P. A. MacMahon **[9]** also indicates many kinds of alterations of polygons, preserving the symmetries essential for tiling. The conditions of the Conway Criterion do not limit you to altering polygon tiles, however. You can choose shapes of (three to six) boundary segments and glue them together (creating vertices) to make a CC tile. The "polygon" of line segments connecting consecutive vertices may be reentrant (FIGURE 4), or even have all vertices but one collinear (FIGURE 1). If you choose some of the centro-symmetric boundary segments of a CC tile to be congruent, then the tile may have extra reflection or rotation symmetry, as will its associated tiling. The tiles shown in FIGURE 10 have associated tilings of type *pmg*, *cmm*, *p*4, respectively (see **[12]**).

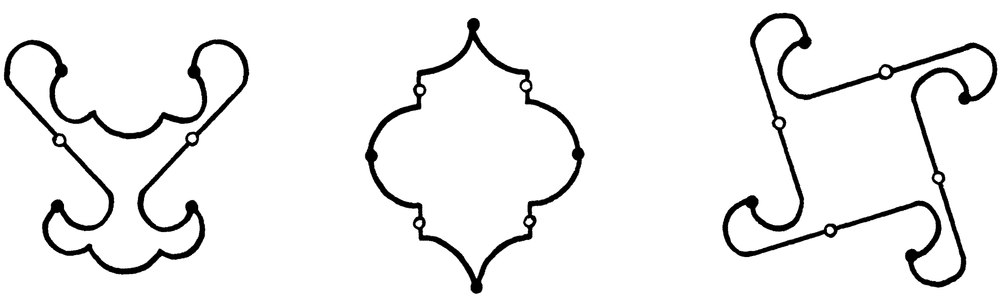


FIGURE 10

The Conway Criterion, and all other known criteria for testing whether or not a given tile paves the plane, is limited to tiles for which there is an associated **periodic** tiling (i.e., a group of translations acts transitively on some finite block of the tiling). There seems to be no hope for a test which decides if a given tile paves in any (haphazard) way at all, but perhaps the following question suggested by R. Bantegnie can be answered. If a tile T paves the plane by an application of successive half-turns (which need not be in the symmetry group of the finished tiling), must T be a CC tile? If not, must there exist a block of copies of T which is a CC tile?

**References**


[1] R. Bantegnie, Etalements Cristallographiques, Acta Math. Acad. Sci. Hungar., 30 (1977) 283–302.
[2] H. S. M. Coxeter, Introduction to Geometry, 2nd ed., Wiley, New York, 1969, pp. 41–42.
[3] H. S. M. Coxeter and S. L. Greitzer, Geometry Revisited, New Mathematical Library, no. 19, Math. Assoc. of Amer., 1967, p. 53.
[4] H. S. M. Coxeter, Twelve Geometric Essays, Southern Illinois Univ. Press, 1968, pp. 56–57.

[5] Martin Gardner, More about tiling the plane: the possibilities of polyominoes, polyiamonds, and polyhexes, Sci. Amer. (August 1975) 112–115.
[6] F. Göbel, Geometric Packing and Covering Problems, Packing and Covering In Combinatorics, A. Schrijver (Editor), Mathematical Centre, Amsterdam, 1979, pp. 179–199.
[7] Branko Grünbaum and G. C. Shephard, The eighty-one types of isohedral tilings in the plane, Math. Proc. Cambridge Philos. Soc., 82 (1977) 177–196.
[8] H. Heesch and O. Kienzle, Flächenschluss, Springer-Verlag, Berlin, 1963.
[9] P. A. MacMahon, New Mathematical Pastimes, Cambridge Univ. Press, 1930, p. 80ff. (To be reprinted in Percy Alexander MacMahon: Collected Papers, vol. 2, George E. Andrews (Editor), MIT Press.)
[10] Ivan Niven, Convex polygons that cannot tile the plane, Amer. Math. Monthly (December 1978) 785–792.
[11] E. R. Ranucci and J. L. Teeters, Creating Escher-Type Drawings, Creative Publications, Palo Alto, California, 1977, p. 83ff.
[12] Doris Schattschneider, The plane symmetry groups: their recognition and notation, Amer. Math. Monthly (June-July 1978) 439–450.

# Nice Cubic Polynomials for Curve Sketching

TOM BRUGGEMAN
*Xavier University*
*Cincinnati, OH 45207*

TOM GUSH
*SUNY at Stony Brook*
*Stony Brook, NY 11794*

The polynomials used in calculus texts to illustrate the applications of derivatives to curve sketching are, in spite of any student impressions to the contrary, reasonably nice polynomials. Most of their coefficients are integers, relatively small integers at that, and it is not unusual for the polynomials or even the derivatives to have an integer root. This is no mere coincidence. To simplify the sketching of a given polynomial, students are limited to such devices as a careful choice of origin, scale or coordinate system. Authors can use the additional device of careful selection of the polynomial. According to their taste, roots can be integers, rationals or even (cruelty!) irrationals. What if integer roots are chosen? When it comes time to find the point of inflection and relative extremes of cubic polynomials, the odds favor relative extremes at quadratic irrationals and points of inflection at rationals that are not integers.

It is the purpose of this note to use Pythagorean triplets to show how to construct cubic polynomials with integer coefficients whose roots are integers and whose first and second derivatives also have integer roots. We do not claim that this construction is original, but it is not such common knowledge that repeating it here will not be useful when it comes time to make up a calculus test.

We can suppose that the roots of the polynomial are 0, $a$, and $b$, since if one of the roots is not 0, a translation can make it so. Let

$$f(x)=x(x-a)(x-b)=x^3-(a+b)x^2+abx,$$

so

$$f'(x)=3x^2-2(a+b)x+ab \quad \text{and} \quad f''(x)=6x-2(a+b). \tag{1}$$

If

$$f'(x)=3(x-c)(x-d)=3x^2-3(c+d)x+3cd, \tag{2}$$

then comparing (1) and (2) gives

$$2(a+b)=3(c+d) \quad \text{and} \quad ab=3cd. \tag{3}$$

From the second equation, one of $a$ and $b$ is divisible by 3 and because of symmetry, we can suppose that it is $a$. From the first equation, $a+b$ is divisible by 3, and so $b$ is divisible by 3 also. Putting $a=3A$ and $b=3B$, (3) becomes

$$2(A+B)=c+d \quad \text{and} \quad 3AB=cd.$$

From the second equation, one of $c$ and $d$ is divisible by 3, and we can suppose that it is $c$. If $c=3C$, we have

$$2(A+B)=3C+d \quad \text{and} \quad AB=Cd. \tag{4}$$

Eliminating $A$ from (4) yields $2(Cd/B+B)=3C+d$, or

$$2B^2-(3C+d)B+2Cd=0. \tag{5}$$

If $B$ is to be an integer, the discriminant of the quadratic in (5) must be a perfect square:

$$(3C+d)^2-16Cd=H^2$$

which can be rearranged to

$$H^2+(4C)^2=(d-5C)^2.$$

We know how to find all of the Pythagorean triplets satisfying the above equation:

$$4C=2kst, \quad H=k(s^2-t^2), \quad d-5C=k(s^2+t^2) \tag{6}$$

for integers $s$, $t$ and any $k$. From (5), $B=(3C+d\pm H)/4$. Taking the plus sign (it turns out that choosing the minus sign gives the same result with $s$ and $t$ interchanged), (6) gives

$$\begin{aligned} B &= (3C+5C+k(s^2+t^2)+k(s^2-t^2))/4 \\ &= (4kst+2ks^2)/4. \end{aligned}$$

Putting $k=2r$ we get $B=rs(s+2t)$. From (6), $C=rst$ and $d=5rst+2r(s^2+t^2)=r(2s+t)(s+2t)$. Finally, substituting back we get

$$\begin{aligned} a &= 3rt(2s+t) \\ b &= 3rs(s+2t) \\ c &= 3rst \\ d &= r(2s+t)(s+2t). \end{aligned}$$

The root of the second derivative is

$$(a+b)/3=r(s^2+4st+t^2).$$

TABLE 1 gives some examples of these nice cubics; the list can be indefinitely extended.

| Polynomial | Roots of | | |
|---|---|---|---|
| $f$ | $f$ | $f'$ | $f''$ |
| $x^3-3x^2+4$ | $-1,2,2$ | $0,2$ | $1$ |
| $x^3-33x^2+216x$ | $0,9,24$ | $4,18$ | $11$ |
| $x^3-6x^2-135x$ | $-9,0,15$ | $-5,9$ | $2$ |
| $x^3-147x+286$ | $-13,2,11$ | $-7,7$ | $0$ |
| $x^3-3x^2-144x-140$ | $-10,-1,14$ | $-6,8$ | $1$ |
| $x^3-3x^2-144x+432$ | $-12,3,12$ | $-6,8$ | $1$ |

TABLE 1

The authors wish to express their gratitude to the referee for invaluable rewriting and to Dr. William Larkin for his interest in this problem.

# The Tree Planting Problem on a Sphere

STEPHEN J. RUBERG
*Miami University*
*Oxford, OH 45056*

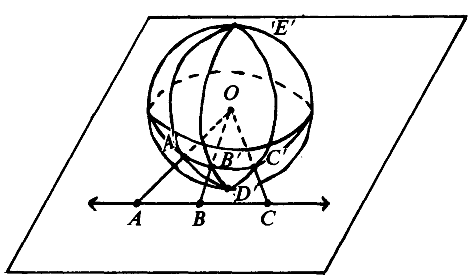
The tree planting problem has been a popular recreational pastime for many years. It has the following simple statement: How can $n$ points in the plane be arranged in rows, each containing exactly $k$ points, to produce a maximum number of rows? In the latter half of the 19th century, the famous mathematician J. J. Sylvester occupied much of his time with this question and related problems. Although this puzzle has been around for many years, only in some particular cases has limited progress been made, with virtually no progress toward a general solution. Even for small values of $k$ such as three and four, only a handful of results is known **[1]**.

Here we consider the tree planting question on a sphere, where a line is defined to be a great circle and trees are in a row if they lie on a single line. Thus, in general, two points determine a unique line. However, if the two points are the endpoints of a diameter of the sphere, henceforth called **antipodal points**, then there exists an infinite number of lines through the two points. Clearly, any two distinct lines intersect at exactly two antipodal points. We offer no complete solution but we do present some plausible conjectures.

Let us represent the points of a plane by a (gnomonic) projection to the center of a sphere tangent to the plane. Since any line in the plane will produce half a great circle on the sphere, the patterns of lines which are the solutions for the problem in the plane may be projected onto the sphere to help form the pattern of great circles which are the solutions there.

Obviously, for the spherical problem the case $k=2$ is trivial. Then $k=3$ and $n=3$ or 4, the values of $r$, the maximum number of rows, are one and two, respectively. To find the value of $r$ for $n=5$, we will begin by projecting a single line containing three points, $A$, $B$ and $C$, onto the sphere. Now by adding two antipodal points to the sphere, say $D'$ and $E'$, which are not in the great circle determined by $A'$, $B'$ and $C'$, three new rows are introduced (see Figure 1). These antipodal points form great circles with each point projected on the sphere. Hence, five points produce four rows.

This example illustrates certain important aspects of this projection procedure. First, the straight line containing three points is the solution to the problem in the plane. Second, the addition of antipodal points on the sphere is the *best* way to include these points in the pattern since they form a new row of three with every point already there. Consequently, there can be




**On a sphere five trees determine at most four rows of three trees each. The points and great circles are shown on the front of the sphere only for convenience.**

FIGURE 1

| $n$ | $p_n$ | $r_n$ | $n$ | $p_n$ | $r_n$ |
|---|---|---|---|---|---|
| 1 | 0 | 0 | 12 | 19 | 22 |
| 2 | 0 | 0 | 13 | 22* | 27 |
| 3 | 1 | 1 | 14 | 26* | 31 |
| 4 | 1 | 2 | 15 | 31* | 35* |
| 5 | 2 | 4 | 16 | 37 | 40* |
| 6 | 4 | 5 | 17 | 40* | 46* |
| 7 | 6 | 7 | 18 | 46* | 53 |
| 8 | 7 | 10 | 19 | 52* | 57* |
| 9 | 10 | 13 | 20 | 57* | 64* |
| 10 | 12 | 15 | 21 | | 71* |
| 11 | 16 | 19 | 22 | | 77* |

**Known values for the tree planting problem with some conjectures (marked with *).**

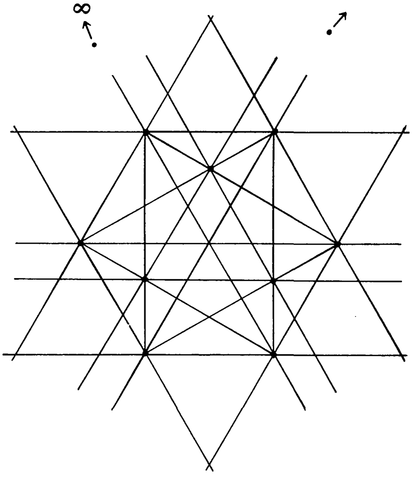
TABLE 1

no better solution to the problem on the sphere for $n=5$. That is, no better arrangement can be projected on the sphere, and no better choice for the additional two points can be made. It is important to note that no solution can contain two pairs of antipodal points since they would form an unacceptable row of four points. Since the plane is projected onto half the sphere, adding pairs of antipodal points will always work. Here no pair of points projected on the sphere would ever be antipodal.

To find the solution for $k=3$ and $n=6$, first project the pattern for the solution in the plane when $n=4$ $(r=1)$ onto the sphere. Adding two antipodal points to the sphere which do not lie in the great circles determined by the projected points results in four more rows of three. Thus, the solution on the sphere for $n=6$ is $r=5$.

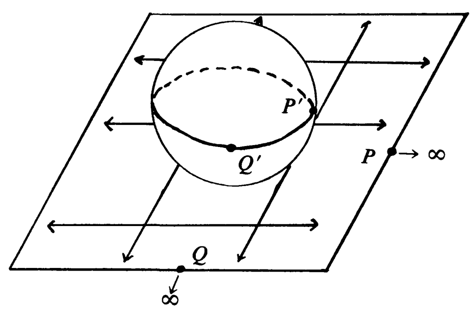
Since the solutions in the plane to the $k=3$ case have been determined for $n=3$ through 12 and $n=16$ [1], the solutions on the sphere can be determined for $n=3$ through 14 and $n=18$ using this projective approach. If $p_n$ denotes the solution in the plane for $n$ points, the solution $r_n$ for $n$ points on the sphere is $p_{n-2}+(n-2)$: the $p_{n-2}$ rows in the plane pattern form great circles on the sphere when projected, and the additional antipodal points (not lying in any of the great circles) form $(n-2)$ additional rows of three. Hence, $r_7=p_5+5=7$, $r_8=p_6+6=10$, etc.; see Table 1.

When $n=12$, the pattern for the solution in the plane involves ideal points (see Figure 2) [2]. Each ideal point of the plane is projected onto the equator of the sphere which becomes the projection of the ideal line (see Figure 3). For convenience, a projected ideal point will appear on only one side of the sphere in order to avoid its antipodal projection (see Figure 3). Thus, the projective procedure is applicable even in these situations.




**The tree planting problem with 12 trees (three of them "ideal") in the plane produces 19 rows; 12 with one ideal tree each, one with three ideal trees, and 6 ordinary.**

FIGURE 2




**The projection of ideal points onto the sphere.**

FIGURE 3

For $k=4$ the problem is somewhat trivial. Obviously when $n=4$, two pairs of antipodal points $ABCD$ which lie on the same great circle make an acceptable row of four. A fifth point $E$ does not increase the number of rows no matter where it is placed. However, when the sixth point $F$ is added as the antipodal point of $E$, two new rows are formed, namely $ACEF$ and $BDEF$. Once again, the addition of a seventh point $G$ does not create a new row. But an eighth point $H$ added as the antipodal point to $G$ produces three new rows—one with each pair of antipodal points. Proceeding in this fashion, we see that the $(2t+1)$th point does not increase $r_n$, while the $(2t+2)$th point added as the antipodal point of the $(2t+1)$th point provides $t$ new rows. Therefore, for $n=2m$ or $n=2m+1$, we conjecture that

$$r_n=\sum_{i=1}^{m-1} i=\frac{(m-1)m}{2}.$$

There is a host of conjectures for many values of $n$ for the plane problem. We have shown how the tree planting problem on the sphere (for $k=3$) can be reduced to that on the plane, in that any solution or conjectured solution in the plane can be projected onto the sphere to obtain corresponding results. The more creative reader might seek new solutions on the sphere and project them onto the plane to find improved results. In any case, the problem remains very perplexing with results for larger values of $k$ and $n$ virtually untouched.

I would like to thank Professor David Kullman of Miami University and the editors for their suggestions in revising this article.

**References**

[1] Stefan A. Burr, Branko Grünbaum and N. J. A. Sloane, The orchard problem, Geom. Dedicata, 2 (1974) 397–424.

[2] Martin Gardner, Mathematical games, Sci. Amer., 235 (August 1976) 102–109.

# Cooking a Turkey

**John Ruebush**
*University of Utah*
*Salt Lake City, UT 84105*

**Robert Fisk**
*Colorado School of Mines*
*Golden, CO 80401*

Many cookbooks provide a table of cooking time versus weight for roasting meats of various types. For roasting a turkey, the weight-time information in Table 1 is provided by the *Betty Crocker Cookbook* ([1], p. 442). We shall use some dimensional analysis and scale modeling to attempt to verify the cooking time entries in Table 1, assuming a cooking time of 3.25 hours for a 7-pound turkey.

| Ready-to-Cook Weight | Approximate Cooking Time | Internal Temperature |
|---|---|---|
| 6–8 pounds | 3 to $3\frac{1}{2}$ hours | 185° F |
| 8–12 pounds | $3\frac{1}{2}$ to $4\frac{1}{2}$ hours | 185° F |
| 12–16 pounds | $4\frac{1}{2}$ to $5\frac{1}{2}$ hours | 185° F |
| 16–20 pounds | $5\frac{1}{2}$ to $6\frac{1}{2}$ hours | 185° F |
| 20–24 pounds | $6\frac{1}{2}$ to 7 hours | 185° F |

Table 1

We start with the one-dimensional diffusion equation

$$\frac{\partial\theta}{\partial t}=\kappa\frac{\partial^2\theta}{\partial x^2}, \tag{1}$$

where $\theta(x,t)$ represents the temperature at any point $x$ and any instant $t$, assuming a homogeneous "turkey" with $\kappa$ the coefficient of thermal diffusivity. Let's assume the turkey is initially at room temperature $T_1$ and that the oven is at temperature $T_2$; we put the turkey in the oven at time $t=0$. Let $L$ be the length of the turkey. Then we have the boundary and initial conditions:

$$\begin{aligned} \theta(x,0)&=T_1, \quad 0<x<L,\\ \theta(0,t)&=T_2, \quad t>0, \\ \theta(L,t)&=T_2, \quad t>0. \end{aligned} \tag{2}$$

Next, we write (1) and (2) in a dimensionless form by letting (see **[2]**)

$$\xi=\frac{x}{L}, \quad \tau=\frac{\kappa t}{L^2}, \quad \phi=\frac{\theta-T_1}{T_2-T_1}. \tag{3}$$

First we find $\partial\theta/\partial t$ and $\partial^2\theta/\partial x^2$ in terms of $\xi$, $\tau$, and $\phi$. Since

$$\frac{\partial\theta}{\partial t}=\frac{d\theta}{d\phi}\cdot\frac{\partial\phi}{\partial\tau}\cdot\frac{d\tau}{dt}=(T_2-T_1)\cdot\frac{\partial\phi}{\partial\tau}\cdot\frac{\kappa}{L^2},$$

we have

$$\frac{\partial\theta}{\partial t}=\frac{(T_2-T_1)\kappa}{L^2}\frac{\partial\phi}{\partial\tau}. \tag{4}$$

Similarly, since

$$\frac{\partial\theta}{\partial x}=\frac{d\theta}{d\phi}\cdot\frac{\partial\phi}{\partial\xi}\cdot\frac{d\xi}{dx}=(T_2-T_1)\cdot\frac{\partial\phi}{\partial\xi}\cdot\frac{1}{L},$$

we obtain

$$\frac{\partial\theta}{\partial x}=\frac{T_2-T_1}{L}\frac{\partial\phi}{\partial\xi}.$$

Hence

$$\begin{aligned} \frac{\partial^2\theta}{\partial x^2}&=\frac{\partial}{\partial x}\left(\frac{T_2-T_1}{L}\cdot\frac{\partial\phi}{\partial\xi}\right)=\frac{T_2-T_1}{L}\cdot\frac{\partial}{\partial x}\left(\frac{\partial\phi}{\partial\xi}\right)\\ &=\frac{T_2-T_1}{L}\cdot\frac{\partial}{\partial\xi}\left(\frac{\partial\phi}{\partial\xi}\right)\cdot\frac{d\xi}{dx}=\frac{T_2-T_1}{L}\cdot\frac{\partial^2\phi}{\partial\xi^2}\cdot\frac{1}{L}\\ &=\frac{T_2-T_1}{L^2}\cdot\frac{\partial^2\phi}{\partial\xi^2}. \end{aligned} \tag{5}$$

Using (4) and (5) in (1) yields

$$\frac{\partial\phi}{\partial\tau}=\frac{\partial^2\phi}{\partial\xi^2}, \tag{6}$$

and using (3) in (2) gives

$$\begin{aligned} \phi(\xi,0)&=0, \quad 0<\xi<1,\\ \phi(0,\tau)&=1, \quad \tau>0,\\ \phi(1,\tau)&=1, \quad \tau>0. \end{aligned} \tag{7}$$

The importance of (6) is that the solution in the dimensionless form does not depend on what is being heated, and, in particular, does not depend on the size of the object being heated.

In the problem of roasting turkeys of different sizes, we wish to achieve the same internal temperature for each bird. This takes some time $\tau_0$ in the dimensionless form. We assume that turkeys of different sizes (weights) are geometrically similar objects and that they have the same thermal characteristics (i.e., $\kappa$ is the same for all turkeys). We also assume that the weight of a turkey is proportional to the cube of its length (see **[3]**):

$$W^{1/3}=kL. \tag{8}$$

Now, consider two turkeys, 1 and 2, which have weights $W_1$ and $W_2$, respectively. We assume that each is to be roasted until its temperature is $T$. In the nondimensionless form, this takes times $t_1$ and $t_2$, respectively, for each turkey. But, in the dimensionless form, $\tau_1$ equals $\tau_2$, so from (3),

$$\frac{\kappa t_1}{L_1^2}=\frac{\kappa t_2}{L_2^2}, \tag{9}$$

where $t_1$ and $t_2$ are the cooking times for the two turkeys and $L_1$ and $L_2$ are the lengths of the birds. Using (8) in (9) leads to

$$t_2=\left(\frac{W_2}{W_1}\right)^{2/3} t_1. \tag{10}$$

This says that cooking times aren't linear with weight ratios, but go as the $2/3$ power.

| Weight | Time |
|---|---|
| 10 pounds | 4.1 hours |
| 14 pounds | 5.2 hours |
| 18 pounds | 6.1 hours |
| 22 pounds | 7.0 hours |

TABLE 2

If we take $t_1=3.25$ hours for a 7-pound turkey, then we get the cooking times in TABLE 2, using (10) for turkeys of other weights. It is clear from this table that our simple model confirms the cooking table provided by Betty Crocker. It is interesting to observe that we avoided the solution of the heat equation in getting the cooking times.

**References**


[1] Betty Crocker's Cookbook, Bantam Books, New York, pp. 442.

[2] C. C. Lin and L. A. Segel, Mathematics Applied to Deterministic Problems in the Natural Sciences, Macmillan, New York, 1974, p. 195.

[3] J. Maynard Smith, Mathematical Ideas in Biology, Cambridge Univ. Press, London, 1968, pp. 2–13.


# A Coin Tossing Game


JAMES C. FRAUENTHAL
ANDREW B. MILLER
*SUNY at Stony Brook*
*Stony Brook, NY 11794*


Suppose that the first player (A) in a two-player game selects one of the four possible outcomes which occurs when a fair coin is tossed twice ($HH$, $HT$, $TH$ or $TT$, where $H$ stands for Heads and $T$ for Tails). The second player (B) then selects one of the three remaining two-toss sequences. A coin is then tossed repeatedly until the sequence chosen by one of the players occurs. The player whose sequence occurs first is the winner.

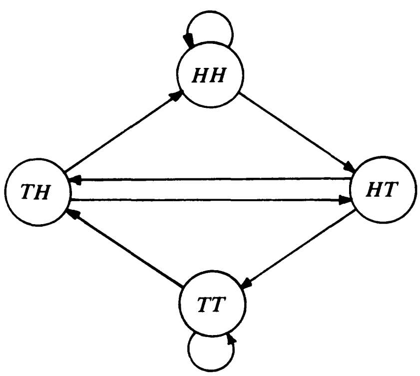
As an example, imagine that player A chooses the sequence $HH$ and that player B then selects $TH$. A coin is then tossed with the following results: $HTTTH$. On the fifth toss player B wins since the last two tosses yield the sequence $TH$. (Prior to the fifth toss neither player's chosen sequence had occurred, so it was necessary to keep tossing the coin.) Both players seem to have the same chance of winning this game, since both of the chosen two-toss sequences occur with the same frequency. However, as we will see, player B is three times as likely to win as is player A for the sequences selected in this example.

We begin by constructing a directed graph (digraph) to represent the game. The graph will have 4 vertices, one for $HH$, $HT$, $TH$, and $TT$. Suppose that at some point in the game the most recent two-toss sequence is $HH$; we think of the game as being at the vertex $HH$ in the graph. If the next toss is a tail, the game moves to the vertex $HT$, since now the most recent two-toss sequence is $HT$. This move (or transition) is represented by an edge directed from $HH$ to $HT$. If, instead, the next toss were another head, the game stays at the vertex $HH$; this kind of transition is represented by an edge (called a loop) which is directed from $HH$ to $HH$. These two edges directed away from $HH$ represent both possible outcomes for the situation when the game is at $HH$. The remainder of the digraph is constructed by drawing the pairs of directed edges which begin at each of the three remaining vertices $HT$, $TH$ and $TT$. The resulting directed graph is shown in FIGURE 1. Note that each vertex, in addition to having two outgoing edges, also has two incoming edges (where loops count as both outgoing and incoming edges): outgoing edges tell where the game can go on the subsequent toss of the coin, incoming edges tell where the game could have come from prior to the toss.

The game can now be understood in terms of the digraph. After each player has chosen a two-toss sequence and the coin has been tossed the initial two times, the game is at one of the four vertices. If this vertex corresponds to the choice of either of the players, the game is over; if not, the coin is tossed again and the result of the toss determines an outgoing edge. The vertex reached from this edge may be one of the players' sequences, and if it is, the game is over. If not, this process is repeated until the vertex which corresponds to the sequence chosen by one of the players is reached. At that point the game ends since the winner is determined.

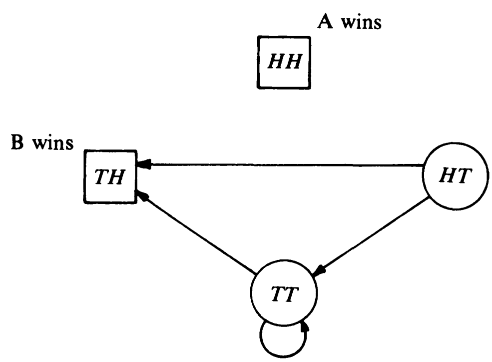
As explained thus far the digraph is useful for visualizing the progress of the game. The crucial observation for the purpose of analysis is that the outgoing edges from the vertices corresponding to the players' chosen sequences will never be used: once one of these vertices is reached, the game is over and no more coin tossing takes place. Hence, these outgoing edges may be removed from the graph.

Return now to the original example, which we will call Case I. The reduced digraph (omitting all outgoing edges from the vertices $HH$ and $TH$) is shown in FIGURE 2. This graph forms two disconnected pieces, in which the vertex chosen by player A ($HH$) cannot be reached from any of the other three vertices. Thus if the initial two tosses in this particular game are *not* $HH$, then player A can *never* win. Since two heads will occur in two tosses of a fair coin with probability $1/4$, player A's chance of winning is $1/4$; consequently, player B's chance is $3/4$. Thus, in this situation, player B's chance of winning is three times that of player A.




**Digraph for the two-toss game before players select vertices.**

FIGURE 1




**Digraph for Case I of the two-toss game in which player A chooses *HH* and player B chooses *TH*.**

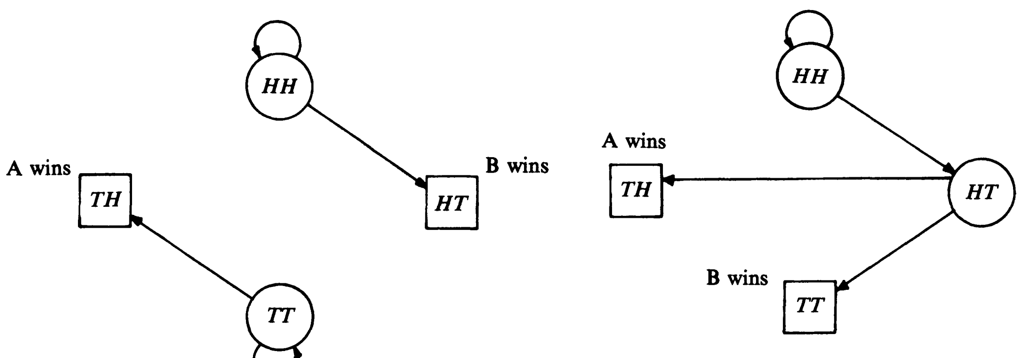
FIGURE 2

To complete the analysis of the two-toss game we should investigate the other three choices player A may make, and the corresponding proper responses for player B. Imagine that player A chooses the sequence $TT$; call this Case I′. It should be apparent (by interchanging $H$ and $T$), that player B should choose the sequence $HT$. In fact, throughout this paper, every pair of choices by the two players has a mirror-image choice formed by changing all $H$'s to $T$'s and vice versa. The mirror-image game submits to precisely the same analysis as the original game; consequently, only one of each pair will be discussed.

Another possible choice for player A is the sequence *TH*; call this Case II. Obviously, player B must not choose the sequence *HH* as this would put him at precisely the same disadvantage that player A was at in Case I. (In other words, the two players would each have taken the other's chosen sequence; but since we have already learned that *TH* beats *HH* three times out of four, this would be a foolish thing for player B to do.) Of the two other possible choices for player B, *HT* and *TT*, it makes no difference which one player B chooses, either choice will lead to a fair game (where both players' probability of winning is $1/2$). But the analysis is different depending upon whether player B chooses *HT* or *TT*, so we will discuss these two situations separately.

If player B chooses *HT*, the reduced digraph (formed by removing unusable edges from FIGURE 1), shown in FIGURE 3a, consists of two unconnected pieces. It is easily seen that if the first toss of the coin results in a head, player B must win, while if the first toss is a tail, player A must win. Hence both players have an equal chance of winning.

If instead player B chooses *TT* in response to player A's choice of *TH*, the digraph with the unusable edges deleted takes the form shown in FIGURE 3b. This time the digraph is not separated into two pieces, a condition which makes the analysis a bit harder. If the first two tosses yield *TH*, player A wins immediately; if they yield *TT*, player B wins immediately. Each of these outcomes occurs with a probability of $1/4$. If the first two tosses yield *HH*, the game must pass through the vertex *HT* before a winner can be determined. Thus, since half of all games end with a winner after the initial two tosses, half do not, and thus must pass through the vertex *HT* just before the game ends. But once the game is at *HT*, the winner is determined by the next toss, and since the coin is fair, player A wins half of all games which pass through vertex *HT*. In summary, player A wins all games which start at vertex *TH* and half of all games which start at either vertex *HH* or vertex *HT*; thus the probability that player A wins is $1/4 + (1/2)(1/4+1/4) = 1/2$. It therefore follows that if player B chooses *TT* in response to player A choosing *TH*, the game is fair. Further, since the choices *HT* and *TT* both lead to fair games (and the choice *HH* puts player B at the disadvantage) it is not possible for player B to gain the advantage by choosing his sequence second if player A chooses *TH*.




(a)
**Digraph for Case II of the two-toss game in which player A chooses *TH* and player B chooses *HT*.**

(b)
**Digraph for Case II of the two-toss game in which player A chooses *TH* and player B chooses *TT*.**

FIGURE 3

One final choice for the two-toss game remains: player A chooses the sequence *HT*. We call this Case II′ since it is the mirror-image of Case II. By analogy with Case II, player B can choose either *TH* or *HH* to make for a fair game. Once again, there is no choice available to player B which gives him an advantage. This completes the analysis of the two-toss game.

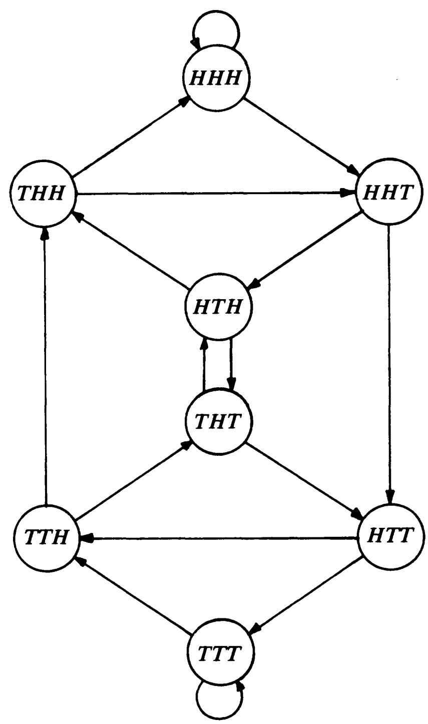
More interesting is the three-toss game, in which each player chooses one of the eight sequences which can occur when a coin is tossed three times. We begin the analysis with the directed graph for the complete three-toss game (FIGURE 4). There are now eight vertices corresponding with the eight three-toss sequences; as with the two-toss game, there are two outgoing and two incoming edges at each vertex.

The three-toss game turns out to be more interesting than the two-toss game because no matter which of the eight sequences player A chooses, player B can always choose a better one. TABLE 1 lists the eight choices player A can make, the corresponding best choice for player B and the probability that player B will win. We verify the results listed in TABLE 1 for Case III only. The methods employed for this case extend easily to Case IV, and Cases I and II are simple to analyze as their associated digraphs consist of two disconnected pieces. (As before, the primed cases are just mirror images of the unprimed cases, and need not be treated separately.)

In Case III, player A chooses the sequence *HTH* and player B chooses *HHT*. The digraph with the unusable edges deleted is shown in FIGURE 5. The probability of beginning at any one of the eight vertices is $1/8$. From each vertex player B has a certain conditional probability of winning. To find player B's probability of winning the game, it is necessary to multiply the sum of his conditional winning probabilities from each vertex by $1/8$.

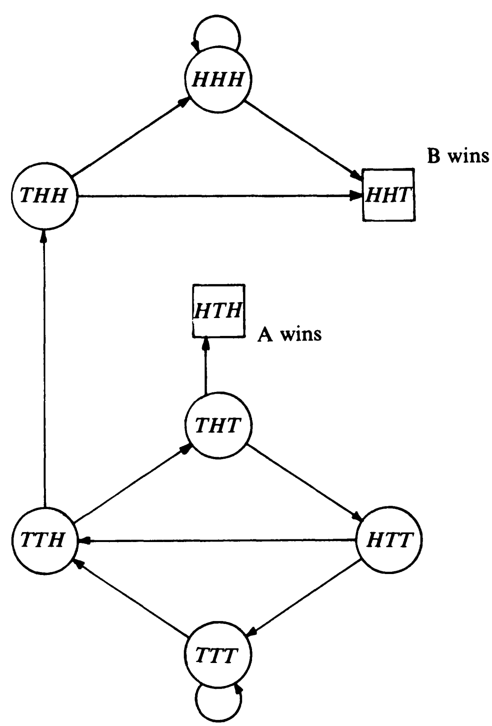
It is clear from FIGURE 5 that if the game begins at any of the vertices *HHT*, *THH* or *HHH*, player B must win, while if the game begins at vertex *HTH*, player B must lose. From any of the vertices, *TTH*, *TTT* and *HTT* the game must pass through the vertex *TTH* before either player can win. Therefore, the probability that player B wins if the game starts at the vertices *TTT* or *HTT* is the same as if the game starts at vertex *TTH*. It is convenient at this point to introduce a simple mathematical notation to keep track of these observations. Let

$$P(\mathrm{B}|HHH) = \text{Prob (B wins}|\text{game starts with sequence } HHH)$$




**Digraph for the three-toss game before players select vertices.**

FIGURE 4




**Digraph for Case III of the three-toss game in which player A chooses *HTH* and player B chooses *HHT*.**

FIGURE 5

| | Choices: | | Probability that |
|---|---|---|---|
| Case | Player A | Player B | Player B wins game |
| I | $HHH$ | $THH$ | |
| I′ | $TTT$ | $HTT$ | 7/8 |
| II | $HHT$ | $THH$ | |
| II′ | $TTH$ | $HTT$ | 3/4 |
| III | $HTH$ | $HHT$ | |
| III′ | $THT$ | $TTH$ | 2/3 |
| IV | $HTT$ | $HHT$ | |
| IV′ | $THH$ | $TTH$ | 2/3 |

**Three-toss games with Player B choosing the best strategy in response to Player A's choice.**

TABLE 1

and similarly for the other seven possible starting sequences. The observations just made can then be expressed as

$$P(\mathrm{B}|HHT)=P(\mathrm{B}|THH)=P(\mathrm{B}|HHH)=1,$$
$$P(\mathrm{B}|HTH)=0,$$
$$P(\mathrm{B}|TTH)=P(\mathrm{B}|TTT)=P(\mathrm{B}|HTT).$$

It is now apparent that there are really just two unknown quantities, $P(\mathrm{B}|THT)$ and $P(\mathrm{B}|TTH)$.

If the game is at the vertex $TTH$, after the next toss of the coin it will be at either $THT$ or $THH$ with equal probability (see FIGURE 5). Hence

$$P(\mathrm{B}|TTH)=\tfrac{1}{2}P(\mathrm{B}|THT)+\tfrac{1}{2}P(\mathrm{B}|THH);$$

analogously,

$$P(\mathrm{B}|THT)=\tfrac{1}{2}P(\mathrm{B}|HTT)+\tfrac{1}{2}P(\mathrm{B}|HTH).$$

Solving these leads to $P(\mathrm{B}|TTH)=2/3$ and $P(\mathrm{B}|THT)=1/3$. It therefore follows that

$$P(\mathrm{B\ wins})=\tfrac{1}{8}\left(1+1+1+0+\tfrac{2}{3}+\tfrac{2}{3}+\tfrac{2}{3}+\tfrac{1}{3}\right)=\tfrac{2}{3},$$

as reported in TABLE 1.

The coin-tossing game is compelling because it is unfair. In almost all cases the second player has a decided advantage over the first player, a fact which is not initially obvious. Although we have provided a reasonably complete analysis for numerous cases, a variety of questions remain which can be pursued by the interested reader.

The analysis could be reformulated as a Markov Chain. The transition matrix for the game prior to vertex selection by the two players (that is, the one which corresponds with the graphs in FIGURES 1 and 4) describes an ergodic Markov Chain. The process of vertex selection changes the transition matrix into one which describes an absorbing Markov Chain. Once the game is reformulated in this way, the ordinary methods for analyzing Markov Chains can be employed to calculate the winning probabilities for the two players. Using either the graphical or Markov Chain formulation, could one determine a method for deciding player B's optimal strategy in response to any choice made by player A?

The three-toss game could be extended to include a third player, C, who makes his choice after players A and B. Does the existence of this player affect player B's strategy?

One final remark seems worthwhile as it allows the vertex naming to be simplified. If the coin is imagined to have a zero on one side and a one on the other, then the various sequences can be interpreted as binary numbers. Thus, for example, if we let heads correspond with zero and tails correspond with one, for the three-toss game, $HHH \to 000 = 0$ (decimal), $HHT \to 001 = 1$ (decimal), $HTH \to 010 = 2$ (decimal), etc. Consequently, in an $n$-toss game, there will be a total of $2^n$ possible sequences which can be translated into the decimal integers $0, 1, \ldots, 2^n-1$. The main advantage of this translation is that it provides a natural ordering for the different sequences.

# PROBLEMS

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

## Proposals

*To be considered for publication, solutions should be mailed before March 1, 1981.*

**1101.** Can the plane be tiled with infinitely many convex regions such that every straight line meets only a finite number of the regions? [*Daniel B. Shapiro, The Ohio State University*.]

**1102.** Let $B$ and $B'$ be bilinear forms on a vector space $V$ over a field $F$. Suppose that for every $x$ and $y$ in $V$, $B(x,y)=0$ implies $B'(x,y)=0$. Prove that $B=cB'$ for some $c$ in $F$. [*Daniel B. Shapiro, The Ohio State University*.]

**1103.** For which positive integers does there exist a sequence of $n$ consecutive integers for which the $j$th integer, $1 \leqslant j \leqslant n$, has at least $j$ divisors, none of which divides any other member of the sequence? [*Hal Forsey, San Francisco State University*.]

**1104.** For $n$ equally spaced points on the unit circle, consider the $\binom{n}{3}$ triangles formed by choosing three points at a time as vertices.
(a) Find $S_n$, the sum of the areas of all these triangles.
(b) If $A_n$ denotes the average area of these triangles, determine limit $A_n$ as $n \to \infty$. [*Nick Franceschine, Sebastopol, California*.]

**1105.*** For $n$ points on the unit circle, consider the sum of the areas of the $\binom{n}{3}$ triangles formed by choosing three points at a time as vertices. Show that the sum is a maximum when the points are equally spaced. [*Peter Ørno, The Ohio State University*.]

**1106.** Let $p: N \to N$ be a permutation of the positive integers. Let $x = 0.a_1a_2\ldots$ be the decimal expansion (terminating, if possible) of $x$ in $(0,1)$ and define $p^*(x) = 0.a_{p(1)}a_{p(2)}\ldots$. Thus, each permutation $p$ induces a function $p^*: (0,1) \to (0,1)$. Characterize those permutations $p$ for which $p^*$ has at least one point of differentiability in $(0,1)$. [*Michael W. Ecker, Pennsylvania State University*.]

---

# Quickies

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

**Q665.** Many numbers which can be written as an alternating sequence of 0's and 1's are composite, for example

$$101010101 = 41 \times 271 \times 9091.$$

Of course, 101 is prime. Are there any others? [*Dan Moran, Michigan State University.*]

# Solutions

## Iterates **March 1979**

**1069.** Suppose $f: \mathbf{R} \to \mathbf{R}$ is continuous and for every rational $q$ there exists an $n$ with $f^n(q) = 0$ (the $n$th iterate of $f$). Prove or disprove: For every real number $t$ there is an $n$ such that $f^n(t) = 0$. [*F. David Hammer, University of California at Davis.*]

*Solution*: The following function shows that the statement is false. Let

$$f(x) = \begin{cases} \pi - 2|\pi - x| & \text{if} \quad |x - \pi| < \pi/2, \\ 0, & \text{elsewhere.} \end{cases}$$

Clearly $f(\pi) = \pi$ and thus $f^n(\pi) = \pi$ for every positive integer $n$. We also claim that $|x - \pi| \geqslant \pi/2^n$, for some positive integer $n$, implies $f^n(x) = 0$. For $n = 1$, $|x - \pi| \geqslant \pi/2$ implies $f(x) = 0$. Suppose that the claim holds for $n = k$. Then, if $\pi/2 \geqslant |x - \pi| \geqslant \pi/2^{k+1}$, we have $|f(x) - \pi| = 2|\pi - x| \geqslant \pi/2^k$. Thus $f^k(f(x)) = 0$ and hence $f^{k+1}(x) = 0$. This proves the claim and disproves the statement.

DONALD ELLIOTT & WILLIAM BOSCH
University of Northern Colorado

*Also solved by Michael W. Ecker, Edilio A. Escalona (Venezuela), C. S. Gardner, Jerrold W. Grossman, G. A. Heuer, Lars Kadison, Wayne McClish, James McKim & Stephen Snover, Adam Riese, Bill Scherer & John Strasen, Jonathan D. H. Smith (Germany), J. M. Stark, and the proposer.*

## Multinomial Trials **March 1979**

**1070.*** Let $p_1 + p_2 + \cdots + p_k = 1$ be a sum of $k \geqslant 2$ probabilities and let $M_n$, for $n = 1, 2, \ldots$, be the multinomial distribution based on these probabilities and $n$ trials. Event $A_n$ occurs if, during the $n$ trials, no possible outcome of the experiment occurs in two consecutive trials. Find the sum $\Sigma_{n=1}^{\infty} P(A_n)$. What are the convergence criteria for this sum to exist? [*Thomas E. Elsner & Joseph C. Hudson, General Motors Institute.*]

*Solution*: The series will be shown to converge for all possible values of the probability vector $(p_1, p_2, \ldots, p_k)$. A recursion formula will be derived for computing the summands $P(A_n)$. Also, this formula will be used to obtain the sum of the series.

There is no loss in generality to assume that $p_1, p_2, \ldots, p_k$ are all positive; otherwise, the problem would reduce to a similar one with smaller $k$. Let $p = \min\{p_1, p_2, \ldots, p_k\}$. Then

$$\begin{aligned}P(A_n) &= P(A_1 \cap A_2 \cap \cdots \cap A_n)\\ &= P(A_1)P(A_2|A_1)\cdots P(A_n|A_1 \cap A_2 \cap \cdots \cap A_{n-1})\\ &\leqslant 1\cdot(1-p)^{n-1}.\end{aligned}$$

Hence

$$\sum_{n=1}^{\infty} P(A_n) \leqslant \sum_{n=1}^{\infty} (1-p)^{n-1} = 1/p.$$

In the important special case where $p_1 = p_2 = \cdots = p_k = 1/k$, the above two inequalities become equalities with $p = 1/k$. For computing $P(A_n)$ in the general case, let $E_{i,j}$ denote the event that the $i$th class occurs on the $j$th trial. Then, for $1 \leqslant i \leqslant k$, $n \geqslant 2$,

$$\begin{aligned}P(E_{i,n} \cap A_n) &= P(E_{i,n} \cap E'_{i,n-1} \cap A_{n-1})\\ &= p_i P(E'_{i,n-1} \cap A_{n-1})\\ &= p_i P(A_{n-1}) - p_i P(E_{i,n-1} \cap A_{n-1}).\end{aligned} \tag{1}$$

Since $P(E_{i,1} \cap A_1) = p_i$ $(i = 1, 2, \ldots, k)$, $n-1$ successive substitutions of formula (1) into

$$P(A_n) = \sum_{i=1}^{k} P(E_{i,n} \cap A_n)$$

yield, for $n \geqslant 2$,

$$\begin{aligned}P(A_n) &= P(A_{n-1})\sum_{i=1}^{k} p_i - P(A_{n-2})\sum_{i=1}^{k} p_i^2 + P(A_{n-3})\sum_{i=1}^{k} p_i^3 - \cdots \pm P(A_1)\sum_{i=1}^{k} p_i^{n-1} \mp \sum_{i=1}^{k} p_i^n\\ &= \sum_{r=1}^{n}\left\{(-1)^{r-1}P(A_{n-r})\sum_{i=1}^{k} p_i^r\right\},\end{aligned} \tag{2}$$

where $P(A_0)$ is defined to be 1. This formula remains valid for the case $n=1$ because $P(A_1)=1$. Computation of $P(A_n)$ $(n = 2, 3, \ldots)$ can be carried out recursively using formula (2). Further,

$$\begin{aligned}\sum_{n=1}^{\infty} P(A_n) &= \sum_{n=1}^{\infty}\sum_{r=1}^{n}\left\{(-1)^{r-1}P(A_{n-r})\sum_{i=1}^{k} p_i^r\right\}\\ &= \sum_{i=1}^{k}\sum_{r=1}^{\infty}(-1)^{r-1}p_i^r\left\{\sum_{n=r}^{\infty} P(A_{n-r})\right\}\\ &= \left\{1 + \sum_{n=1}^{\infty} P(A_n)\right\}\sum_{i=1}^{k} p_i \sum_{r=1}^{\infty}(-p_i)^{r-1}\\ &= \left\{1 + \sum_{n=1}^{\infty} P(A_n)\right\}\sum_{i=1}^{k} p_i/(1+p_i).\end{aligned}$$

Interchange of the order of summation is permissible because $\sum_{r=1}^{\infty}(-p_i)^{r-1}$ $(i = 1, 2, \ldots, k)$ and $\sum_{n=1}^{\infty} P(A_n)$ are absolutely convergent series. Therefore,

$$\sum_{n=1}^{\infty} P(A_n) = s/(1-s), \text{ where } s = \sum_{i=1}^{k} p_i/(1+p_i).$$

B. R. JOHNSON
University of Victoria

*Also solved by Barry C. Arnold & Richard A. Groeneveld, W. W. Meyer, R. Shantaram, J. G. Wendel, and the proposers.*

## A Problem with Dice **March 1979**

**1071.** Player A rolls $n+1$ dice and keeps the highest $n$. Player B rolls $n$ dice. The higher total wins, with ties awarded to Player B.

(a) For $n=2$, show that Player A wins and find his probability of winning.

(b*) Find the smallest value of $n$ for which Player B wins. [*Joseph Browne, Onondaga Community College.*]

*Solution* (a): Let $X_1$, $X_2$, $X_3$, $Y_1$, and $Y_2$ be the outcome on rolling five dice and let $U=X_{(2)}+X_{(3)}$ and $V=Y_1+Y_2$, where $X_{(2)}$ and $X_{(3)}$ are the two largest among $X_1$, $X_2$, and $X_3$. By a straightforward counting of cases we obtain:

$$\begin{array}{ll} P(U=3 \text{ and } V=2)=(3/6^3)(1/6^2); & P(U=4 \text{ and } V\leqslant 3)=7(1+2)/6^5; \\ P(U=5 \text{ and } V\leqslant 4)=12(1+3+3)/6^5; & P(U=6 \text{ and } V\leqslant 5)=19\cdot 10/6^5; \\ P(U=7 \text{ and } V\leqslant 6)=27\cdot 15/6^5; & P(U=8 \text{ and } V\leqslant 7)=34\cdot 21/6^5; \\ P(U=9 \text{ and } V\leqslant 8)=36\cdot 26/6^5; & P(U=10 \text{ and } V\leqslant 9)=34\cdot 30/6^5; \\ P(U=11 \text{ and } V\leqslant 10)=27\cdot 33/6^5; & P(U=12 \text{ and } V\leqslant 11)=16\cdot 35/6^5. \end{array}$$

Upon adding these we have $P(U>V)=4812/7776=401/648\approx .6188$.

G. A. HEUER
Concordia College

*Also solved by Walter Bluger (Canada), Michael Goldberg, Michael Vowe (Switzerland), and the proposer. No solutions to part* (b) *were received. Bluger conjectures that Player* A *always wins and his probability of winning has a limiting value of about* .58 *as* $n\to\infty$. *See Problem* 1098, *this* MAGAZINE, 53 (1980) 180, *for a related problem.*

## A Tailored Polynomial **May 1979**

**1072.** The professor is preparing her final exam for calculus. She wants to include the problem: "Find the relative maxima, relative minima, and points of inflection of the following function." The function should be a polynomial $P(x)$ of degree 4 with three distinct relative extrema and two distinct points of inflection. In order to solve the problem, the students must be able to factor $P'(x)$ and $P''(x)$. But the typical calculus student in her class can factor a quadratic polynomial correctly only if its roots are integers between $-20$ and 20, and the student can factor a cubic polynomial only if it is $x$ times a quadratic which the student can factor. Help the professor find such a polynomial. [*Peter Ørno, The Ohio State University.*]

*Solution*: Let $P'(x)=ax(x-b)(x-c)$ and $P''(x)=a'(x-b')(x-c')$ where $b,c,b',c'$ are distinct integers between $-20$ and 20. Note that we may also assume none of these is 0, since 0 is already one of the extrema.

Differentiating $P'$ and setting it equal to $P''$, we obtain the system of equations

$$a'=3a$$
$$2(b+c)=3(b'+c')$$
$$bc=3b'c'.$$

From the last two equations we conclude that $3|b$ and $3|c$. Solving the two equations for $b'$, we get $b'=\left((b+c)\pm\sqrt{(b+c)^2-3bc}\,\right)/3$. Thus the expression $(b+c)^2-3bc=b^2-bc+c^2$ is a perfect square divisible by 9. Now let $b=3k$ and $c=3m$ where $k,m$ are distinct non-zero integers. Since $b,c\in[-18,18]$, we may take $k,m\in[-6,6]$. Write $b^2-bc+c^2=9(k^2-km+m^2)$. We must find $k,m$ so that $k^2-km+m^2$ is a perfect square. From the symmetry of the expression we may assume two cases: $0<k<m$ and $k<0<m$ with $|k|\leqslant|m|$. Checking these values we find exactly two solutions: $k=-3$, $m=5$ and $k=-5$, $m=3$.

So there are only two pairs: $b=-15$, $c=9$ or $b=-9$, $c=15$. From this we get

$$P'(x)=ax(x+15)(x-9) \text{ or } P'(x)=ax(x+9)(x-15).$$

Thus

$$P(x)=a\left(\frac{x^4}{4}+2x^3-\frac{135}{2}x^2\right)+c_0 \text{ or } P(x)=a\left(\frac{x^4}{4}-2x^3-\frac{135}{2}x^2\right)+c_1.$$

Hence, up to a constant term, there are just two monic polynomials with the specified requirements:

$$P(x)=x^4+8x^3-270x^2 \text{ or } P=x^4-8x^3-270x^2.$$

PROBLEM SOLVING GROUP
University of Hartford

*Also solved by Merrill Barnebey, Duane M. Broline, Glenn Clark, Clayton W. Dodge, Kay Dundas, Gail Eisner, Milton Eisner, Win Emmons, Daniel Eustace, Gordon Fisher, M. P. Gopal, Clifford H. Gordon, Tsai-Sheng Liu, Stephen R. Monson, Zane C. Motteler, Roger B. Nelsen, James G. Schmidt, Robert S. Stacy, J. M. Stark, Mary Kay Sullivan, James W. Uebelacker, University of Bern Problems Group (Switzerland), Western Maryland College Seminar, Dennis Wildfogel, Kenneth L. Yocom, and the proposer.*

**Smallest Root of a Cubic** **September 1979**

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

*Solution* I. In fact the desired root lies between $q/p$ and $3q/2p$. The graph of the cubic is symmetric about the inflection point at $(0,q)$, and has its relative minimum at $(\sqrt{p/3}, q-(2p/3)\sqrt{p/3})$. Its numerically smallest root $r$ occurs where the graph crosses the $x$-axis between these two points. (Because of the symmetry the negative root is farther from the origin.) The tangent to the graph at $(0,q)$ crosses the $x$-axis at $q/p$, and the chord from $(0,q)$ to the minimum point crosses the $x$-axis at $3q/2p$. Now, when $x>0$, $f''(x)>0$, so that $r$ must lie between $q/p$ and $3q/2p$.

G. A. HEUER
Concordia College

*Solution* II. Since the sum of the roots is zero and the product is negative, we must have two positive roots and one negative root. Call them $r$, $s$, and $-(r+s)$, where $0<r\leqslant s$.

Now $x^3-px+q=(x-r)(x-s)(x+r+s)$, so that $p=r^2+rs+s^2$ and $q=rs(r+s)$. Since $s^2\geqslant rs \geqslant r^2$, we have $s^2+rs-2r^2\geqslant 0$ and thus $2(s^2+rs+r^2)\leqslant 3(rs+s^2)$. From $rs+s^2<r^2+rs+s^2\leqslant (3/2)(rs+s^2)$, we get

$$\frac{rs(r+s)}{r^2+rs+s^2}<r\leqslant\frac{3}{2}\,\frac{rs(r+s)}{r^2+rs+s^2},$$

and so $q/p<r\leqslant 3q/2p$.

ROGER B. NELSEN
Lewis and Clark College

*Solution* III. We show that the numerically smallest positive root is in $(q/p, 3q/2p]$. Let $f(x)=x^3-px+q$. Since all roots are real, $4p^3-27q^2\geqslant 0$. By Descartes' rule of signs, $f(x)$ has one negative root. Now, $f(q/p)=(q/p)^3>0$, while

$$f(3q/2p)=27q^3/8p^3-q/2=q(27q^2-4p^3)/8p^3\leqslant 0.$$

Thus $f(x)$ has one root in $(q/p, 3q/2p]$ and one root at least as large as $3q/2p$. (Note: No doubt this result was a standard exercise back in those thrilling days of yesteryear when "Theory of Equations" was a regular part of undergraduate education.)

DUANE BROLINE
University of Evansville

*Also solved by Elizabeth Bator & Blair Spearman, Walter Bluger (Canada), W. J. Blundon (Canda), Paul Bracken (Canada), Santo Diano, Michael J. Dixon, Ragnar Dybvik (Norway), Milton P. Eisner, Stephen Eldridge (England), Thomas E. Elsner, Nick Franceschine III, Gordon Fisher, Lorraine L. Foster, Joel K. Haack, Lee O. Hagglund, University of Hartford Problem Solving Group, Robert Heller, Hans Kappus (Switzerland), Mark F. Kruelle, L. Kuipers (Switzerland), Kin Li, Ian McGee (Canada), Zane C. Motteler, Hugh Noland, P. J. Pedler, T. N. Robertson, B. K. Sachdeva, J. M. Stark, F. Màx Stein, M. Vowe (Switzerland), Yan-Loi Wong (Hong Kong), Imelda Yeung, Ken Yocum, and the proposers.*

**2500th Digit out of 35,660** **September 1979**

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

*Solution*: Let $n?$ denote the product of the integers from 1 to $n$, omitting multiples of 5. Then

$$\begin{aligned} 10{,}000! &= (10{,}000?)5^{2000}(2000!) \\ &= 5^{2499}(10{,}000?)(2000?)(400?)(80?)(16?)(3!) = 5^{2499}K, \text{ say.} \end{aligned}$$

There are no further factors of 5, and more than 2500 factors of 2, so the digit in question is the last nonzero digit; it will be the final digit of $K/2^{2499}$. Now $10? \equiv 6 \pmod{10}$, so 10,000?, 2000?, 400?, and 80? are all congruent to 6 (mod 10). Since $16? \equiv 4 \pmod{10}$ and $6^2 \equiv 6 \pmod{10}$, it follows that $K \equiv 4 \pmod{10}$. Since $K/2^{2499}$ is even, successive divisions of $K$ by 2 have final digits which cycle through $4,2,6,8,4,\ldots$. Now $2499 \equiv 3 \pmod 4$, thus the final digit of $K/2^{2499}$ is 8.

G. A. HEUER
Concordia College

*Also solved by Elizabeth Bator & Blair Spearman, Bill Bompart & Freddy Maynard & Edward Pettit & Gerald Thompson, Martha Cook & James Cross, Michael Dixon (Canada), Jordi Dou, Lorraine Foster, Raymond W. Freese & Chaman L. Sabharwal, Michael Gilpin & Betsy Hill, University of Hartford Problem Solving Group, Robert Patenaude, Seattle Pacific University Math Problems Seminar, Jeffrey Shallit, David Singmaster (England), Lawrence Somer, J. M. Stark, L. Van Hamme (Belgium), Michael Vowe (Switzerland), and the proposer. Bompart & Maynard & Pettit & Thompson, Freese & Sabharwal, Gilpin & Hill, and Shallit all used a computer to find the digit. Shallit provided all 35,660 digits. There were also several incorrect solutions.*

**Inscribed *n*-gons** **September 1979**

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

*Solution*: Let $A_i, B_i, i = 1,2,\ldots,n$, denote the vertices of a regular $n$-gon $\mathfrak{A}$ and the vertices of an inscribed $n$-gon $\mathfrak{B}$, respectively. Let $a$ be the length of each side of $\mathfrak{A}$. If $B_i$ divides $\overline{A_iA_{i+1}}$ into segments of lengths $c$ and $d$, then by the law of cosines, we deduce that

$$\overline{B_{i-1}B_i}^2 = c^2 + d^2 - 2cd\cos\theta = \text{constant, where } \theta = \frac{(k-2)\pi}{k}.$$

Thus $\Delta B_{i-1}A_iB_i \cong \Delta B_iA_{i+1}B_{i+1}$ and therefore angle $(B_{i-1}B_iB_{i+1}) = 180° - (180° - \theta) = \theta$. Hence the vertices $B_i$ form a regular $n$-gon.

Conversely, if $\mathfrak{B}$ is a regular $n$-gon, then angle $(B_{i-1}B_iB_{i+1}) = $ angle $(A_{i-1}A_iA_{i+1}) = \theta$. It follows that

$$\text{angle }(A_iB_iB_{i-1})+\text{angle }(A_iB_{i-1}B_i)=\text{angle }(A_iB_iB_{i-1})+\text{angle }(A_{i+1}B_iB_{i+1}),$$

and so angle $(A_iB_{i-1}B_i)=$ angle $(A_{i+1}B_iB_{i+1})$. Therefore, $\Delta B_{i-1}A_iB_i\cong\Delta B_iA_{i+1}B_{i+1}$. Thus $\overline{B_{i-1}A_i}=\overline{B_iA_{i+1}}$ and $\overline{A_iB_i}=\overline{A_{i+1}B_{i+1}}$. Therefore the vertices of $\mathfrak{B}$ divide each side of $\mathfrak{A}$ in the same ratio and sense.

IMELDA YEUNG, student
Oberlin College

*Also solved by Walter Bluger (Canada), Gordon Fisher, Joel K. Haack, L. Kuipers (Switzerland), Hubert J. Ludwig, Leroy F. Meyers, Seattle Pacific University Math Problems Seminar, Scott Smith, J. M. Stark, and the proposer.*

**Counting Pythagorean Triangles** **September 1979**

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

*Solution* I: Let the sides of the triangle be the integers $x, y$, and $z$. We require that

$$x^2+y^2=z^2 \quad\text{and}\quad xy=p^m(x+y+z). \tag{1}$$

Eliminate $z$ from these two equations to obtain

$$(x-2p^m)(y-2p^m)=2p^{2m}. \tag{2}$$

This means that $(x-2p^m)|2p^{2m}$. In addition, we do not allow $x-2p^m<0$. (If $x-2p^m=-p^j$ or $-2p^j$ for $0\leqslant j\leqslant m$, then $y\leqslant 0$; if $x-2p^m=-p^{m+j}$ or $-2p^{m+j}$ for $0<j\leqslant m$, then $x\leqslant 0$.)

If $p\neq 2$, the only pairs of $x$ and $y$ which satisfy (2) are given by

$$x-2p^m=p^s \quad\text{and}\quad y-2p^m=2p^{2m-s} \text{ for } 0\leqslant s\leqslant 2m. \tag{3}$$

This provides $2m+1$ solutions. Of course, $x$ and $y$ may be interchanged but this only yields triangles which are congruent to those given by (3).

For the case $p=2$, equation (2) becomes $(x-2^{m+1})(y-2^{m+1})=2^{2m+1}$. Thus $x-2^{m+1}|2^{2m+1}$ and so $x-2^{m+1}=2^j$, $y-2^{m+1}=2^{2m-j+1}$ for $0\leqslant j\leqslant m$ and so there are $m+1$ noncongruent solutions if $p=2$.

The number of triangles which satisfy (1) will equal the number of noncongruent solutions described above, namely $m+1$ if $p=2$ and $2m+1$ if $p\neq 2$.

PAUL BRACKEN, undergraduate
University of Toronto

*Solution* II: More generally, if the area to semi-perimeter ratio is $n=2^mp_1^{m_1}\cdots p_k^{m_k}$, where the $p_i$ are odd primes, then the number of triangles is $(m+1)(2m_1+1)\cdots(2m_k+1)$. Let $da$ and $db$ be the legs and $dc$ be the hypotenuse of the Pythagorean triangle where $(a,b,c)=1$. Then $n=dab/(a+b+c)$ and setting $a=2rs$, $b=r^2-s^2$ and $c=r^2+s^2$, where $(r,s)=1$, $r>s$ and $r-s$ is odd, we have $n/d=s(r-s)$. Let $f(k)$ denote the number of factors, $s$, of $k$ such that $(s,k/s)=1$ and $k/s$ is odd. Then clearly, $f(1)=f(2^m)=1$ and $f(p^m)=2$ if $p$ is an odd prime and $m>0$. Also, $f(k)$ is a multiplicative function and hence $F(n)=\Sigma\{f(n/d): d|n\}$, which is the number of solution triangles, is also multiplicative. It now follows that $F(n)=(m+1)(2m_1+1)\cdots(2m_k+1)$.

KEN YOCOM
South Dakota State University

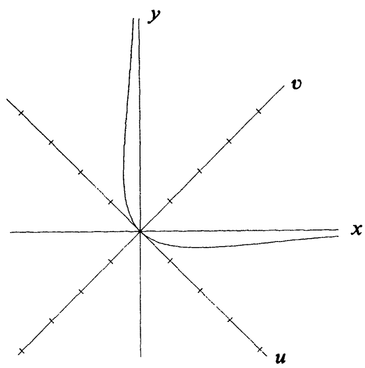
*Also solved by Bern Problem Solving Group (Switzerland), Walter Bluger (Canada), Martha Cook & James Cross, Robert S. Fisk, Lorraine L. Foster, Nick Franceschine III, P. K. Garlick, University of Hartford Problem Solving Group, L. Kuipers (Switzerland), Kin Li, Hugh Noland, Scott Smith, Lawrence Somer, J. M. Stark, Michael Vowe (Switzerland), and the proposer.*

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

*Solution:* The equation $xe^y + ye^x = 0$ is transformed into the equation $v = u(e^u - 1)/(e^u + 1)$ by the 45° rotation and dilation

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Using standard calculus techniques, we obtain the graph of $v$. The graph of $xe^y + ye^x = 0$ is then obtained by a $-45°$ rotation and contraction. (See figure.)




From the figure we see that every line $y = mx$ with $m < 0$ and $m \neq -1$ intersects the graph at (0,0) and one other point. If we substitute $y = mx$ into $xe^y + ye^x = 0$, we obtain $xe^x(e^{(m-1)x} + m) = 0$. Assuming $x \neq 0$, we have

$$x = \frac{\ln(-m)}{m-1} \quad \text{and} \quad y = \frac{m\ln(-m)}{m-1}.$$

If we also allow $m = -1$, the above equations provide a complete set of solutions in parametric form.

THE UNIVERSITY OF HARTFORD PROBLEM SOLVING GROUP

*Also solved by Elizabeth Bator & Blair Spearman, Walter Bluger (Canada), Milton & Gail Eisner, Gordon Fisher, Nick Franceschine III, Michael Goldberg, L. Kuipers (Switzerland), Roger Nelsen, University of New Orleans Problem Group, Hugh Noland, P. Ramankutty, B. K. Sachdeva, Simon A. Stricklen, Jr., Ken Yocum, and the proposer.*

# Answers

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

**Q665.** Let $N$ be such a number. Obviously, $N$ cannot end in 0. Therefore, $N = 101010\ldots0101$. Let $k$ be the number of 1's. If $k$ is even, the $N$ is divisible by 101. If $k$ is odd, multiply $N$ by 11 to obtain

$$11\,N = 111\ldots111 = 11\ldots11 \times 100\ldots001,$$

where the first factor in the product has $k$ digits and the second factor has $k+1$ digits. One of these two numbers is a factor of $N$. (Note that the proof is valid regardless of what base is used for the number system.)

# REVIEWS

**Paul J. Campbell, Editor**
*Beloit College*

**Pierre Malraison, Editor**
*Control Data Corp.*

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

MacLane, Saunders, *Mathematical models of space*, American Scientist 68:2 (March-April 1980) 184-191.

Excellent exposition which opens the reader's eyes to mathematical generalizations of the concept of space, including spaces without points.

Engel, Kenneth, *Shadows of the 4th dimension*, Science 80 (July/August 1980) 68-73.

A popular, gee-whiz account of Tom Banchoff's four-dimensional computer graphics, emphasizing views of Banchoff and Charles Strauss' award winning film *The Hypercube: Projections and Slices* and, for contrast, extracts from *Flatland*.

Berresford, G.C., et al., *Khachiyan's algorithm, Part I: A new solution to linear programming problems*, Byte 5 (August 1980) 198-208.

Explanation of Khachiyan's paper and analysis of the geometry of the algorithm.

Bernhard, Robert, *The Russian algorithm: A second look*, IEEE Spectrum 17 (May 1980) 56-57.

"It was too good to be true:" Tests of the new linear programming "ellipsoid algorithm" so far indicate that it will not replace the simplex method in practical computation.

Blum, L., et al., *Contribution to the ellipsoid algorithm*, Science 208 (20 June 1980) 1318-1319.

Refers to papers preceding Khachiyan's. (An impressive bibliography of material on the algorithm is available from Philip Wolfe, Mathematical Science Dept., IBM Watson Research Center, Yorktown Heights, NY 10598.)

Gardner, Martin, *Mathematical games: The capture of the monster: A mathematical group with a ridiculous number of elements*, Scientific American 242:6 (June 1980) 20-32, 186.

Introduction to group theory and the simple groups, occasioned by the recent success at constructing the "monster" simple group.

Kolata, Gina Bari, *Discovery by decree: A mathematics breakthrough is announced but details are not forthcoming*, Science 208 (25 April 1980) 377.

Robert L. Griess, Jr. (Institute for Advanced Study) announced on January 14 that he had constructed the conjectured sporadic simple group known as the "monster group," which has about $8 \times 10^{35}$ elements. Since then, however, he has refused to provide any details. Is he trying to milk his method before letting others in on it, or is he still checking his proof? We'll have to wait and see, says Kolata.

Kolata, Gina Bari, *New codes coming into use*, Science (16 May 1980) 694-695.

Description of industrial and military uses of the new "unbreakable" codes.

Kolata, Gina Bari, *Prior restraints on cryptography considered*, Science 208 (27 June 1980) 1442-1443.

The U.S. National Security Agency is trying to find a means to control publication of results in cryptography research, fearing that academics may publish instructions enabling anyone to make unbreakable codes. Should the latter occur, NSA mathematicians now working to break codes would no longer be needed.

Humphries, Jill, *Gödel's proof and the liar paradox*, Notre Dame J. Formal Logic 20:3 (July 1979) 535-544.

Argues that there is no relation except superficially, because Gödel's proof uses a constructive diagonal procedure.

Knuth, Donald E., *The letter S*, The Mathematical Intelligencer 2 (1980) 114-122.

A detailed account of the equations and algorithms involved in defining (and drawing) an aesthetically pleasing S. Knuth traces the mathematical problem to Francesco Torniello in 1517, and connects it with his current work on TEX and METAFONT.

*Computer typography*, Scientific American 242:6 (June 1980) 82, 85.

Describes Knuth's METAFONT language for designing typefaces and his TEX language for type composition, noting their special importance to printing mathematics.

Singmaster, David, *Notes on the "Magic Cube," 4th printing, Logical Games* (4509 Martinwood Dr., Haymarket, VA 22069), 1980; 36 pp, $4 (P).

Invented by the Hungarian artist E. Rubik, more than a million copies of the "magic cube" have been sold under various tradenames. This booklet explains, in language only mathematicians will understand, the group theoretic underpinnings and solutions of the puzzle.

Weinberg, Alvin M., *Energy policy and mathematics*, SIAM Review 22:2 (April 1980) 204-212.

"I have seen how elaborate predictions--e.g., with respect to the cost of nuclear energy--have turned out to be wrong by factors of 5 or more. ...Such estimates are uncertain, not only because the mathematical models on which estimates are based involve parameters whose values are uncertain, but also because the equations that describe the phenomena may have chaotic solutions and therefore may be inherently undecidable."

Berliner, Hans, *Computer backgammon,* Scientific American 242:6 (June 1980) 64-72, 186.

Description of the program BKG 9.8 that defeated the world champion in July 1979. The key to high-level play was the use of SNAC functions (for smoothness, nonlinearity and applications coefficients), each of which is a microstrategy that accents certain position features; it varies their coefficients in the polynomial function that evaluates the position. "It seems SNAC functions are the proper means of capturing the characteristic that human beings call judgment. They make it possible to respond to small changes in stimuli with small changes in behavior, and this is exactly what judgment (as opposed to logical deduction) is all about."

Coxeter, H.S.M., *The non-euclidean symmetry of Escher's picture "Circle Limit III,"* Leonardo 12 (1979) 19-25 + plate.

Escher's print, inspired in part by Coxeter, exhibits symmetries of the hyperbolic plane.

Field, J.V., *Kepler's star polyhedra,* Vistas in Astronomy 23 (1979) 109-141.

Examines and translates first published account of the star polyhedra.

Clapham, C.R.J., *When a fabric hangs together,* Bulletin London Math. Soc. 12 (1980) 162-164.

Answers a question of Grünbaum and Shephard in their article "Satins and Twills," in the May 1980 issue of this *Magazine*.

Fletcher, Colin R., *Rings of small order,* Mathematical Gazette 64 (March 1980) 9-22.

A delightful catalogue of all rings of order less than 8, which includes a surprising variety of structures.

Hewitt, Edwin and Hewitt, Robert E., *The Gibbs-Wilbraham phenomenon: An episode in Fourier analysis,* Archive for History of Exact Sci. 21 (1979) 129-160.

"We find forgotten pioneers. We encounter shocking disputes over priority. We study brilliant achievements, some never properly appreciated. We discover a remarkable series of blunders, which could hardly have arisen save through copying from predecessors without checking. In short, Gibbs' phenomenon and its history offer ample evidence that mathematics for all of its majesty and austere exactitude, is carried on by humans."

Lambert, Joseph B., et al., *Maya arithmetic,* American Scientist 68 (May-June 1980) 249-255.

"The elegance and simplicity of Maya arithmetic derives from its use of only two symbols. ...Essentially no memorization of multiplication tables is required, since two symbols can interact in only three ways." The authors present algorithms (devised 20 years ago by G.I. Sánchez) for multiplication and division in Maya vigesimal notation. It is pure speculation, however, that the Mayans used modifications of the algorithms taught to U.S. children. The question, "...have you ever tried to multiply with Roman numerals?", suggests the authors are not aware of alternative algorithms for the same mathematical operation. The public is fascinated by articles like this, and others will write them if mathematical educators and historians do not.

Randell, Brian, *An annotated bibliography on the origins of computers,* Annals of the History of Computers 1 (1979) 101-207.

Indexed collection of 750 annotated citations.

# NEWS & LETTERS

## NO 1980 INTERNATIONAL MATHEMATICAL OLYMPIAD

Traditionally in the September issue we publish the problems from the International Mathematical Olympiad. Unfortunately, there was no International Mathematical Olympiad this year, so we have no problems to offer in this issue. In 1981, the International Mathematical Olympiad is scheduled to be held in Washington, D.C.

## ALLENDOERFER, FORD, PÓLYA AWARDS

Authors of nine expository papers published in 1979 issues of journals of the Mathematical Association of America received awards at the 1980 August meeting of the Association at the University of Michigan. The 1980 awards, each in the amount of $100, are:

Carl B. Allendoerfer Awards:

Victor L. Klee, Jr. (Dept. of Mathematics, University of Washington, Seattle, WA 98195) for "Some Unsolved Problems in Plane Geometry," *Mathematics Magazine* 52 (1979) 131-145.

Ernst Snapper (Dept. of Mathematics, Dartmouth College, Hanover, NH 03755) for "The Three Crises in Mathematics: Logicism, Intuitionism and Formalism," *Mathematics Magazine* 52 (1979) 207-216.

Lester R. Ford Awards:

Robert Osserman (Dept. of Mathematics, Stanford University, Stanford, CA 94305) for "Bonnesen-Style Isoperimetric Inequalities," *American Mathematical Monthly* 86 (1979) 1-29.

Desmond Fearnley-Sander (Dept. of Mathematics, University of Tasmania, Hobart, Tasmania, Australia 7001) for "Hermann Grassman and the Creation of Linear Algebra," *American Mathematical Monthly* 86 (1979) 809-817.

David Gale (Dept. of Mathematics, University of California, Berkeley, CA 94720) for "The Game of Hex and the Brouwer Fixed Point Theorem," *American Mathematical Monthly* 86 (1979) 818-826.

Karel Hrbacek (Dept. of Mathematics, City College (CUNY), New York, NY 10031) for "Nonstandard Set Theory," *American Mathematical Monthly* 85 (1979) 659-677.

Cathleen S. Morawetz (Dept. of Mathematics, NYU-Courant, New York, NY 10012) for "Nonlinear Conservation Equations," *American Mathematical Monthly* 85 (1979) 284-287.

George Pólya Awards:

Hugh Ouellette (Dept. of Mathematics, Winona State University, Winona, MN 59987) and Gordon Bennett (Dept. of Mathematics, Western Montana College, Dillon, MT 59725) for "The Discovery of a Generalization," *Two-Year College Mathematics Journal* 10 (1979) 11-15.

Robert Nelson (Menlo School, Menlo Park, CA 94025) for "Pictures, Probability, and Paradox," *Two-Year College Mathematics Journal* 10 (1979) 182-190.

## THE WEIGHTED AVERAGE

The excellent note on "Magic Possibilities of the Weighted Average" by Ruma Falk and Maya Bar-Hillel (this *Magazine*, March 1980, pp. 106-107) can be looked at from the point of view of elementary probability and specifically as a variation of what has recently been called Simpson's Paradox. Such seemingly paradoxical problems have confused statisticians for years and a complete and simple solution appears to have been published only recently.

Let $P$ be a probability function (measure) and let $A$, $B$, $C$ be events. Throughout assume $P(A)$, $P(B)$, $P(C)$ are larger than zero. C.R. Blyth (in "On Simpson's Paradox and the Sure-Thing Principle," *J. Amer. Stat. Assoc.*, June 1972, pp. 364-366 and "Simpson's Paradox and Mutually Favorable Events," *J. Amer. Stat. Assoc.*, September 1973, p. 744) and K.L. Chung (in "On Mutually Favorable Events," *Annals Math. Stat.*, 13 (1942) pp. 338-349) have pointed out that it is possible to have

$$P(A|B) > P(A) \text{ and } P(A|C) > P(A)$$

but

$$P(A|BC) < P(A)$$

or

$$P(A|B\ C) < P(A).$$

Similarly it is possible to have

$$P(A|B) < P(A)$$

and both

$$P(A|BC) > P(A|C)$$

and

$$P(A|B\bar{C}) > P(A|\bar{C})$$

This is what is frequently called Simpson's Paradox. Blyth shows that this is equivalent to the possibility of having

$$P(A|B) < P(A|\bar{B})$$

and to have both

$$P(A|BC) > P(A|\bar{B}C)$$

and

$$P(A|B\bar{C}) > P(A|\bar{B}\bar{C}).$$

Our intuition initially goes wrong because we think of $P(A|B)$ as an average of $P(A|BC)$ and $P(A|B\bar{C})$, and of $P(A|\bar{B})$ = an average of $P(A|\bar{B}C)$ and $P(A|\bar{B}\bar{C})$.

What we have to realize is that these two averages may have different weightings. Falk and Bar-Hillel pointed out that we have to look at the weighted average:

$$P(A|B) = [P(C|B)] \cdot P(A|BC) +$$
$$[P(\bar{C}|B)] \cdot P(A|B\bar{C})$$
$$P(A|\bar{B}) = [P(C|\bar{B})]\ P(A|\bar{B}C) +$$
$$[P(\bar{C}|\bar{B})] \cdot P(A|\bar{B}\bar{C}).$$

Falk and Bar-Hillel's example is the possibility expressed in Blythe's version of Simpson's paradox. Let $A$ = the event of being admitted, $B$ = the event of being Female and $C$ = the event of being in the Painting Department. Then $P(A|BC) = .8 > P(A|\bar{B}C) = .4$ and $P(A|B\bar{C}) = .12 > P(A|\bar{B}\bar{C}) = .06$. Then using the intuitive but incorrect unweighted averages, we find that $P(A|B) = .188 < P(A|\bar{B}) = .366$.

Other interesting examples illustrating Simpson's paradox can be found in Chung's paper mentioned above. The paradox and solution can be explained using only elementary probability theory usually taught at the undergraduate level. I hope that more teachers will include these relatively new variations of Simpson's paradox in their undergraduate probability and statistics courses as these ideas become better known.

Robert Crouse
University of Connecticut
Storrs
Connecticut 06268

## FILLING A GAP

I would like to inform your readers that the gap described in P.D. Straffin's paper, "Periodic Points of Continuous Functions" (this *Magazine*, March 1978, pp, 99-105), has now been filled by me and a student of mine. Our result, "A Graph-theoretic Proof of Sharkovsky's Theorem on the Periodic Points of Continuous Functions," will appear in the *Pacific Journal of Mathematics*.

Chung-wu Ho
Southern Illinois University
Edwardsville
Illinois 62026

## EAST ARABIC NUMERALS

I have been enjoying reading informative articles in *Mathematics Magazine* for a long time. I noticed in your January 1979 issue on page 13, figure 5 a truly disturbing incorrect statement. Talking about East Arabic numerals in his article "The Evolution of Mathematics in Ancient China," Frank Swetz indicates that they are still in use in Turkey. As a matter of fact, they are not in use since the establishment of the new Republic of Turkey.

Murat M. Tanik
College Station
Texas 77840

PUBLICATIONS FROM

L'ENSEIGNEMENT MATHEMATIQUE

GENEVA

EM

## IMU Lectures

Series of Survey Lectures given under the sponsorship of the International Mathematical Union.

### L. HÖRMANDER:

*On the existence and the regularity of solutions of linear pseudo-differential equations.*
69 pages, 1971; 14 Swiss Francs.

### W.M. SCHMIDT:

*Approximation to algebraic numbers.*
70 pages, 1972; 16 Swiss Francs.

### J.L. LIONS:

*Sur le contrôle optimal de systèmes distribués.*
45 pages, 1973; 15 Swiss Francs.

### F. HIRZEBRUCH:

*Hilbert modular surfaces.*
103 pages, 1973; 28 Swiss Francs.

### D. MUMFORD:

*Stability of projective varieties.*
74 pages, 1977; 25 Swiss Francs.

### A.G. VITUSHKIN:

*On representation of functions by means of superpositions and related topics.*
68 pages, 1978; 23 Swiss Francs.

## Oeuvres Scientifiques de H. LEBESGUE

5 volumes, 2014 pages, 1972-73; 275 Swiss Francs for the 5 volumes set.

## Monographs Series

### A. WEIL:

*Essais historiques sur la théorie des nombre*
55 pages, 1975; 18 Swiss Francs.

### J. GUENOT et R. NARASIMHAN:

*Introduction à la théorie des surfaces Riemann.* 214 pages, 1976; 44 Swiss Francs

### TOPOLOGY AND ALGEBRA, Proceedings of a Colloquium in Honor of B. ECKMANN.

Lectures by J.F. Adams, M. André, A. Banyaga, R. Bieri, R. Bott, A. Dold, P.A. Griffiths, A. Haefliger, J.C. Hausmann, P. Hilton, F. Hirzebruch, M. Huber, I.M. James, M. Kervaire, M.A. Knus, H. Kraft, S. Mac Lane, W. Meier, J. Milnor and W. Thurston, G. Mislin, U. Stammbach, R. Strebel, U. Würgler, D. Zagier.
280 pages, 1978; 60 Swiss Francs.

### CONTRIBUTIONS TO ANALYSIS, Proceedings of a Symposium in Honor of A. PFLUGER.

Lectures by L.V. Ahlfors, H. Bauer, E. Bombieri, F.W. Gehring, W.K. Hayman, R. Kühnau, O. Lehto, B. Malgrange, R. Narasimhan.
106 pages, 1979; 29 Swiss Francs.

NEW:

### P. ERDÖS and R.L. GRAHAM:

*Old and new problems and results in combinatorial number theory.* Approx. 130 pages, 1980; 38 Swiss Francs.

EM

**20 % discount available on prepaid orders placed to**

L'Enseignement Mathématique, POB 124
CH-1211 Geneva 24, Switzerland

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

MATHEMATICS MAGAZINE VOL. 53, NO. 4, SEPTEMBER 1