TEN MATHEMATICS PROBLEMS I WILL NEVER SOLVE

by Gian-Carlo Rota Department of Mathematics
MIT room 2-351 77 Massachusetts Avenue
Cambridge MA0219-4307

Invited address at the joint meeting of the American Mathematical Society and the Mexican Mathematical Society, Oaxaca, Mexico, December 6, 1997.

If we scan the mathematical literature since the turn of the century, we will be surprised to realize how few mathematicians have published lists of problems.To the best of my knowledge, the last invitation a mathematician to draw such a list was extended at the International Congress of 1950, which took place in Cambridge, Massachusetts. Von Nemann was unanimously chosen by the Organizing Committee of the Congress to give a lecture bearing the title "Problems of Mathematics"(or something to that effect), and at first he accepted the invitation. However, as the time of delivery of his address drew near, von Neumann began to have second thoughts. At the last moment, he changed his mind, and despite the printed announcement, he delivered instead a rather dry one hour lecture on -would you believe it? -the theory of self adjoint operators in Hilbert space. I learned this bit of history when I stumbled upon a copy of the draft of von Neumann's lecture-never published -which I found among my late friend Stan Ulam's papers.

The reason for this reluctance to draw lists of mathematical problems needs hardly be stated. Hilbert's address at the first International Congress of 1900 has scared everyone away from ever attempting anything even vaguely pretending to emulate Hilbert.

What, then, are you to expect in the next forty-five minutes? Shall I follow in von Neumann's footsteps and trap you into listening to a lecture that has been misleadingly advertised? Well, almost, but not quite. Let us briefly reflect on the Philosophy of mathematical problems.

Mathematicians love to state mathematical problems in what might be called "one-shot" version.Is the Riemann hypothesis true? Are there any cardinal numbers between aleph-not and aleph? Is e^{π} irrational? My late friend Garrett Birkhoff used to make fun of such of shot statements of problems by repeating his own deliberately ludicrous variant:"Is every regular function normal?"

One-shot statements of problems are fun to listen to. However, such statements conceal more than they disclose. They are a symptom of a disease that affects all mathematicians:erasing one's footsteps-to quote my colleague Jim Munkres. Behind every one-shot statement there always lurks a theory, either a theory in the making or a theory that has reached a crucial turning point, elegantly if elliptically summarized in the rhetoric of the problem. Such a background of theory is hidden behind the deceptive simplicity of a statement of the form "is A really equal to B?". Without the tacit presupposition of theory, the statement of a mathematics problem would be no more interesting than any of those logical puzzles that were once the core of IQ. tests, in a bygone age whose ending we do not regret.

I might as well lay my cards on the table. The problems I am about to state belong to the worst kind. They are meant to foreshadow theories that do not at present exist, and that might never be come into being. I have been piling them in my for the last forty years. I feel I should have worked on them when I was younger instead of wasting my time as I did. I thank you for giving me this opportunity to discharge my feelings of guilt upon you.

I will begin by stating problems that seem to make some sense, and gradually fade into flakiness.

Problem one. The basis conjecture.

Let V be a vector space of dimension n over an arbitrary field, and let $B_1,\ B_2,\ \cdots$, B_n be n bases of the vector space V. These bases need not be disjoint or distinct. Is it possible to construct an n by n matrix in which the entries in the i-th row are precisely the elements of the basis B_i and which in addition has the property that every column is a basis?

The conjecture has been proved by Marini for $n = 2, 3, 4, 6, 8$ and by Art Drisko for $n = p + 1$, where p is a prime. It is probably true for all even integers n.

Behind this conjecture lurk certain identities from invariant theory, which remain unproved, and which must be passed over in silence. As a matter of fact, one can rattle off several other conjectures on linear dependence of vectors and tensors, all of them suggested by as yet unproved identities in invariant theory. I would feel crushed if the basis conjecture were to be settled by methods other than some new insight in the algebra of invariant theory.

Problem two. The critical problem. You have heard the statement of the four color conjecture for planar graphs. Hadwiger generalized it to an n-color problem U follows:

A graph is n-colorable if and only if its lattice of contractions does not contain the lattice of contractions of the complete n graph as a minor.

Hadwiger's conjecture was settled a few years ago by Robertson and Seymour. There is a catch, however, in their proof: it assumes the truth of the four-color conjecture.

A conjecture similar to the four-color conjecture was Mated by Tutte for flows in graph; it is still open. These and a host of other similar conjectures are special instances of a problem that Crapo and I formulated in 1970.

Let P be a finite ranked partially ordered set having a minimum and a maximum element, whose Moebius function is$\mu(x, y)$. The polynomial

$$_{x \in P}\mu(0, x)\lambda^{r(x)}$$

is called the characteristic polynomial of the partially ordered set P. The chromatic polynomial of a graph is a special case of the characteristic polynomial, when P is taken to be the lattice of contractions of the graph.

The critical problem asks for the explanation of the location of the roots of the characteristic polynomial in terms of the absence of certain forbidden configurations, or "obstructions", in the partially ordered set P.

Much work has been done since 1970 on the critical problem, especially in the special case of arrangements of hyper planes; an impressive two hundred page survey has recently been published by J. P. S. kung. Sometimes in the seventies, kelly and I rashly conjectured a relationship between the critical problem and the zeros of zeta functions in algebraic geometry; a recent paper of Anders Bjorner bears out the truth of this conjecture. Richard Stanley's beautiful theory of supersolvable lattices singles out a remarkable class of partially ordered sets for which the critical problem can be explicitly solved, but attempts to go beyond Stanley have not gotten very far. Some brave recent spadework by Bruce Sagan may believe this statement.

Despite all the effort, everyone feels that the right ideas to deal with the critical problem are still in the wings. When and how such ideas will come into being is anybody's guess.

Problem three. The Titchmarsh convolution theorem.

It may seem strange that a problem in classical analysis should come right after a problem in combinatorics, but we will see that the two are related in a strange way. I copy the statement of the Titchmarsh convolution theorem from Titchmarsh's old book on the Fourier integral:

"Let $f(x)$ and $k(x)$ be real valued integrable functions on the interval $(0, \gamma)$,and let

$$\int_0^x f(y)k(x-y)dy = 0$$

for almost all x in(0,γ). Then f(x)=0 for almost all x in(0,α), and k(x)=0 for almost all x in(0,β),where $\alpha + \beta = \gamma$."

Titrehmarsh's proof of this seemingly elementary statement uses heavy complex variable machinery. No elementary proof of this theorem has ever been given, to the best of my knowledge. A consequence of Titchmarsh's theorem is the fact that the ring of continuous real functions $f(x)$, defined for $x \geq 0$, is an integral domain, when convolution is taken as multiplication. There is a purported "elementary proof" of this latter statement due to Mikusinski and Ryll-Nardzewski, but I find their proof to be neither elementary nor convincing. The basic idea is still missing. Allow me to digress on the importance of this theorem, from two different points of view.

Part of the difficulty of this theorem is due to the fact that we miss is an understanding of the algebra of integration by parts. Denote by J the definite integral operator, that is

$$Jf(x) = \int_0^x f(y)dy$$

The linear operator J satisfies the integration by parts identity

$$JfJ_g = J(fJ_g) + J(_gJf)$$

Iteration of this identity gives the shuffle identities

$$J(f_1J(f_2J\cdots(Jf_n)\cdots))J(g_1J(g_2J\cdots(Jg_k)\cdots) = (h_1J(h_2J\cdots(Jh_n{+}k)\cdots)$$

where the sum ranges over all sequences $h_1,\ h_2,\ \cdots,\ h_{n+k}$which are shuffles of the sequences $f_1, f_2,\ \cdots, f_n$ and $g_1,\ g_2,\ \cdots,\ g_k$.

Whereas algebraists have devoted a lot of attention to derivations, the algebraic theory of the indefinite integral has been strangely neglected.

The shuffle identities are only the tip of an iceberg of algebra and combinatorics, as yet unexplored. The profound work of Kuo Tsai Chen bears witness to the importance of the algebra of the indefinite integral. Jack Milnor once told me that he consider's K. T. Chen's work to be some of the most important and most neglected mathematics of the latter half of this century. However, not even his opinion has so far made a dent into the uncontrollable forces of fashion and fad.

As long as the algebraic structure is not faced up to, there is little hope for an understanding of the Titchmarsh convolution theorem.

Let us now take a different point of view on the Titchmarsh convolution theorem. The algebra of integable functions on the half line under convolution can be viewed as a continuous analog of the algebra of formal power series. But what is the algebra of formal power series, ”really”? We know that this algebra is isomorphic to a subalgebra of the algebra of infinite triangular matrices. But the algebra of triangular matrices may be generalized by replacing the linear order of the integers by an arbitrary partial order; one then obtains a generalization of the algebra of triangular matrices that is called the incidence algebra of a partially ordered set. A certain subalgebra of the incidence algebra of an arbitrary partially ordered set can be singled out as the analog of the algebra of formal power series for partially ordered sets; it is called the reduced incidence algebra. The reduced incidence algebra plays for partially ordered sets a role similar to the group algebra of a group. A thorough exposition of these ideas has recently been given in an excellent book by Spiegel and O'Donnell.

The algebra of integrable function under convolution is the reduced incidence algebra when the partially ordered set is the positive semiaxis endowed with its natural order.

By such analogical reasoning, we eventually realize what the underlying problem is: it is that of developing for incidence algebras something similar to harmonic analysis. The theory of the Laplace transform is a step, but only the first step, in this direction.

Allow me to digress with a personal anecdote. Several years ago I gave a lecture at McMaster University, in which I mentioned these ideas. After the lecture, Banaschewski took me aside and told me: ”Look here, your problem is neither new nor easy. I happen to know that Witt worked on it for half his life, and never published a word on it!”

Problem four. A unified theory of special functions.

On hearing this problem, one thinks back to all previous occasions when the same problem was stated at various times in history, all the way to Gauss and Riemann, and more recently to Truesdell and the British and Dutch schools. At the present time, the problem is viewed as that of finding a unifined approach that will give the identities satisfied by both hypergeometric and q-hypergeometric functions. I would not bring up this problem, if I did not have what is informally known as "an axe to grind".

Lately, q-analogs have come into high fashion. They have been ennobled by the name "quantum groups", even though they are neither quantum nor groups. Thirty years ago, those half dozen of us who worked on q-analogs were looked at with deep suspicion. More than sixty years ago, the Reverend F. H. Jackson, who was at that time probably the only person working on q-analogs, stormed out of the lecture room when someone made an unpleasant comment about q-analogs, and never finished his lecture on the q-analog of the gamma function.

The idea is to develop the q-analog of integration by parts. Operators performing this task are called Baxter operators; they are linear operators P denned on a commutative algebra which for fixed q satisfy the identity

$$P(xPy) + P(yPx) = qP(xy) + (Px)(Py)$$

For$q = 0$, one obtains the identity that characterizes integration by parts, as we have seen. To obtain the q-analog of an ordinary linear differential equation with pollynomial coefficients, one rewrites the differential equation as an equivalent integral equation, using the indefinite integral operator J in place of derivatives, and then one replaces the indefinite integral by a Baxter operator. When this process is performed on the differential equation for the exponential function, one obtains as a q-analog the celebrated Spitzer formula of probability theory. Atkinson used the same principle device to find the q-analogs of the trigonometric functions.

Identities among symmetric functions can be coded into identities holding for Baxter operators, as a matter of fact in 1968 I constructed the "free" Baxter operator in terms of the algebra of symmetric functions. Pierre Cartier read my paper and found my construction to be too indirect, so he proceeded to prove the q-analogs of the shuffle identities satisfied by the indefinite integral, in a paper published in one of the first volumes of "Advances in Mathematics".

It is likely that q-analogs of the differential equations satisfied by hypergeometric functions can be stated in terms of Baxter operators, using the analogical device described above that starts with the indefinite integral. If this conjecture were to be true, we would have a unified theory of hypergeometric and q-hypergeometric functions based upon the algebra of Baxter operators.

You may ask why I have never undertaken the task of verifying this conjecture. To give you an honest answer, let me recall an episode from Don Quixote. In the third chapter of part one, Don Quixote builds his helmet out of cardboard. He then tests it with his sword, and the helmet is smashed to bits. Whereupon, Don Quixote proceeds to put together an identical helmet, but this time he decides not to test it, or, as Cervantes writes, ″lo dio′ por bueno″. We behave like Don Quixote when we refuse to try out an idea, ″la damos por Buena″ for fear that our idea might not work.

Problem five. Set functions on convex bodies.

The cat is out of the bag: I have mentioned the algebra of symmetric functions, and it would be easy to rattle off five more problems dealing exclusively with symmetric functions. I will resist this temptation, but not completely. Allow me to digress again with a silly historical anecdote

When Beethoven had just arrived in Vienna as a young man, he made his living playing the piano for those who could afford to hire him. One of these persons was an Austrian prince who would summon Beethoven late in the evening and ask him to play Bach partitas into the wee hours of the night. One evening Beethoven felt tired, and when the prince mentioned the name ″Bach″ he snapped back: ″This is not Bach, this is ′eine Stroemung′″.

And so it is with the algebra of symmetric functions. It was once a ″Bach″ which has presently turned into ″eine Stroemung″.

Another field that has recently come into high fashion is the geometry of convex sets. A chapter of this theory deals with the assignment of set functions to convex bodies, that is, numerical functions defined on convex bodies which enjoy suitable continuity properties, and which are invariant under the group of Euclidean motions.

I will use a device that was effectively employed by one my undergraduate teachers, Professor Bochner. In the classroom, he would prefix the statement of a theorem by the words: ″Subject to technical assumptions, the following is true″; without, of course, ever revealing what his technical assumptions were. I have never had the ″chutzpah″ to imitate

Professor Bochner, until this moment.

The conjecture is the following:

"Subject to technical assumptions", every invariant set function defined on convex bodies is associated to a symmetric function. Linear set functions, that is, finitely additive measures, are known to be associated with the elementary symmetric functions: they are the "intrinsic volumes". Little is known about non additive set functions. Beifang Chen and I have proved a rudimentary version of his conjecture, but our technical assumptions are preposterous.

Problem six. Set functions of polynomial type.

A quadratic set function may be defined as follows. *Consider a bimeasureβ, that is, a function $\beta(A, B)$ defined on pairs A, B of subsets of a set S, taking real values, which is a finitely additive measure in the variable A when B is held fixed, and similarly for B. Set $(A) = \beta(A, A)$ to obtain what may be rightfully called a quadratic set function.*

When we compare this definition of a quadratic set function with the definition of a quadratic form, we notice a deficiency. Quadratic forms may be defined without recourse to the associated bilinear form. We have, however, no intrinsic definition of quadratic set function, let alone a way of associating a bimeasure to a quadratic set function. The same may be said about cubic set functions, etc.; more generally, we lack an intrinsic definition of a set function of polynomial type.

What is at stake is the possibility of expansion of an "arbitrary" set function into a Volterra type series, where the second term might be a measure, the third term a quadratic set function, etc.; much as one does with non linear operators.

This problem is not new, as Pesi Masani dutifully informed me one day while giving me a strange look. It was stated by Norbert Wiener. Let me tell you another little story.

In the old days, what is now the Notices of the American Mathematical Society was a small pamphlet, published on the occasion of every meeting of the Society, and containing largely the abstracts of the papers to be presented at each meeting, with a strange twist. Members of the Society were allowed to present papers "by title". All they needed to do was send in an abstract, and all these abstracts would be published after light refereeing. Masani guided me to an obscure such abstract by Norbert Wiener, in which this problem is stated. No paper of Wiener ever followed the abstract; however, Brockway McMillan, a student of Wiener's, took a modest first step in his thesis, published in the Annals of Mathematics but systematically ignored.

I cannot help but tell you another of my little stories. In the fifties, Marston Morse, having completed his beautiful theory of the calculus of variations in the large, began to work on an entirely different theory, namely, the theory of bimeasures. I believe he was the one who introduced the term. Once more, the forces of fad and fashion prevailed, and few mathematicians, if any, read the impressive sequence of papers on the subject that Morse and Trbansue were assiduously publishing. Morse felt hurt by this neglect, and whenever anyone wrote to him on any subject, he would get by return mail a package, containing the complete set of reprints of the work of Morse and Transue. I did see the stack of reprints lying on the desk of at least one of my colleagues at MIT in the late fifties.

Problem seven. Intrinsic volumes on lattices of subspaces.

Let us begin with a Mickey Mouse version, which Dan klain and I have worked out in our book on geometric probability. A subset S of a partially ordered set P is said to be an order ideal when it has the following property: if an element x of P belongs to S, and if $y \leq x$, then the element y also belongs to S. The union and intersection of order ideals is an order ideal. If the partially ordered set P is the family of all subsets of a finite set, then an order ideal of P is ordinarily called a simplicial complex. The problem is that of finding all measures on the family of simplicial complexes which are invariant under permutations of the underlying set. These are easily found. Set $\mu_k(S)$ to be the number of subsets with k elements contained in the simplicial complex S. Every invariant measure is a linear combination of the measures μ_k. Remarkably, the measure μ_k is associated to the k-th elementary symmetric function.

Observe the following amusing consequence. The alternating sum $\mu_1(S) - \mu_2(S) + \ldots$ equals the Euler characteristic of the simplicial complex S.

Now to the real problem. Let the partially ordered set P be the partially ordered set of all subspaces of a finite dimensional Hilbert space over the reals. We want all real valued finitely additive measures on the order ideals of P that are invariant under the action of the orthogonal group. The difficulty lies in the choice of a suitable subfamily of order ideals, one that will give the "right" measures. The invariant measures on Grassmanians provide one such invariant measure, when suitably nom1alized, but not even the definition of the Euler characteristic as an invariant measure is obvious in this context.

This problem is related to the two preceding problems, in a way that is not fully understood at present.

Problem eight. Confluent symmetric functions.

Two cautions: first, the problem I am about to state may sound like an obvious one, one that should have been worked out a long time ago; what is surprising is that no one seems to have considered it. Second, the title of this problem is a misnomer: the functions in question are not symmetric. I stumbled upon this problem while rereading Aitken's marvelous little book "Determinants and Matrices", which is the all time bestseller among linear algebra textbooks.

Recall the definition of the Schur functions, which Aitken and the British mathematicians of the time called "bialternant". I follow Aitken's notation, which respects the old Scottish custom of avoiding all subscripts.

A typical Schur function is the following quotient of two determinants:

$$|arrayccccc1\alpha^a\alpha^b\alpha^c\alpha^d l\beta^a\beta^b\beta^c\beta^d 1\gamma^a\gamma^b\gamma^c\gamma^d 1\delta^a\delta^b\delta^c\delta^d\epsilon^a\epsilon^b\epsilon^c\epsilon^d$$

This is a typical example of a cong1lent "symmetric" function. Neither the algebra nor the combinatorics of these functions has been studied, to the best of my knowledge.

Once more, I cannot help running of on a tangent. The notion of "confluence" occurs in a great many mathematical circumstances, for example in Birkhoff-Hermite interpolation and, originally, in the confluent hypergeometric functions. It is a major concern of algebraic geometers. It is probably unrealistic to expect that this idea will ever be understood within a single theory. Having built up my "chutzpah" by stating eight problems, allow me to call your attention to a proposal I made in 1972. Substantial work has been done on this proposal by Philip Hirschhorn, Louise Raphael and Steve Roman, and most recently by Luis Verde Star.

Let us take the vector space of polynomials of one real variable, to a fix our ideas. Define a linear functional ϵ_a to be the evaluation of a polynomial $p(x)$ at the point $x = \alpha$, that is, $\epsilon_a(p(x)) = p(\alpha)$, and define the product of two such linear functionals as

$$\epsilon_a\epsilon_b = \epsilon_a - \epsilon_b a - b$$

This Product is associative, and it easy to see that $(\epsilon_a)^2(p(x)) = p'(a)$. Thus, the algebra of the epsilons includes both differences and derivatives, all evaluated without taking limits. Can this algebra be generalized?

Problem nine. Invariants of four subspaces.

I met Gelfand for the first time in Oxford in 1973, when he received an honorary degree, and for the second time in the seventies, when he received an honorary degree from Harvard. During the Soviet era, he was allowed out of the Soviet Union only when he was to receive an honorary degree. When I met him for the second time in Cambridge, I was flattered that he remembered our first meeting. He took me aside and explained to me why it is important to study the structure consisting of four subspaces of a vector space V. Every linear operator T on V can be coded into four subspaces: roughly speaking, these are the x-axis, the y-axis, the diagonal $x = y$ and the graph $y = Tx$. Thus, all invariants of matrices, for example, the Segre invariants, are encoded in the invariant theory of four subspaces. It must be added that the invariant theory of four subspaces is more general than the invariant theory of operators.

The problem is that of explicitly describing the lattice of subspaces generated by four subspaces in general position. I like this way of stating the problem, because it makes clear that a good part of the problem consists of giving an explicit sense to the word ”explicitly”. The lattice generated by four subspaces in general position is infinite, but nevertheless it should be ”explicitly” described in some sense or other. No one, to my knowledge, has undertaken the nitty-gritty task of doing explicit computations of the elements of this lattice. The algebraic generators of the ring of invariants of four subspaces have been computed by Howe and Huang, and their explicit computation further supports this conjecture.

Certain elements of this lattice would describe, in a geometric sense, the special positions of the four spaces that in the algebraic theory of invariants are described by the vanishing of a concomitant.

Problem ten. Profinite combinatorics. To state this problem, I need even more chutpah, because I will be extrapolating on the basis of a single example.