Six Problems of Gian-Carlo Rota in Lattice Theory and Universal Algebra

JOSEPH P. S. KUNG
Department of Mathematics, University of North Texas, Denton, TX 76203, U.S.A.

and

CATHERINE YAN
Department of Mathematics, Texas A & M University, College Station, TX 77843, U.S.A.

> The algebraic structure sooner or later comes to dominate, whether or not it is recognized when a subject is born. Algebra dictates the analysis.
>
> Gian-Carlo Rota [33]

1. Algebraic structures and identities

This issue of *Algebra Universalis* is dedicated to the memory of Gian-Carlo Rota 1932–1999. Rota began his research career in analysis in the 1950's, but changed his focus to combinatorics in the 1960's. His work precipitated a revolution in combinatorics. We shall not repeat this well-known story. Instead, we will describe six research ideas of Rota in lattice theory and universal algebra which have not received adequate exposition or exposure. These problems come from Rota's own papers (particularly [30, 31, 32, 33]), his lectures at M. I. T. and elsewhere, and personal discussions with the authors.

Beyond specific problems, ideas from universal algebra lie at the heart of Rota's work. For example, a motivation for Rota's change of focus was his recognition of the central role which identities play in analysis and probability theory. At the risk of exaggeration, a risk that Rota was always willing to take, most mathematicians regard identities, at best, as necessary evils, that is, tricks, or things to be disposed of by tricks. To correct this, one of Rota's programs is to study identities at a fundamental level. The most natural environment for studying identities is, of course, universal algebra. The key result here is Garrett Birkhoff's theorem on free algebras. Philosophically, Birkhoff's theorem says that there are free structures associated with every set of identities and the best way to study identities is to describe the free structures. In addition, free algebras are universal objects in a suitable category. In Rota's conception of mathematics, constructing and studying the "right" free or universal object is the key to unveiling the algebraic structure underlying a subject.

The best example of how universal algebra influenced Rota's work is his study of Baxter algebras. The *Baxter identity* for a linear operator P is

$$P(x(Py)) + P(y(Px)) = qP(xy) + (Px)(Py),$$

where q is a constant. A *Baxter algebra* is an algebra with a linear operator satisfying the Baxter identity. In a *tour de force* of universal algebra, the theory of symmetric functions, and combinatorics, Rota constructed the free Baxter algebra. The free Baxter algebra provides a common structure underlying identities in probability theory, integration by parts, symmetric functions, q-integration and q-series. Rota's own account of his work and the unsolved problems in this area can be found in [29].

2. Linear lattices

In the early history of lattice theory, two classes of lattices held center stage. One is the class of distributive lattices, whose study is partly motivated by propositional logic. The natural models are collections of subsets closed under unions and intersections. The other is the class of modular lattices. Their study is motivated by order relations among congruence relations of algebraic structures. More specifically, lattices of normal subgroups of a group, ideals of a ring, subspaces of vector spaces, and submodules of a module are modular lattices. In actuality, as Birkhoff and M. L. Dubreil-Jacotin observed, all these lattices are more than modular: they are *linear lattices*, that is, they can be represented by lattices of equivalence relations which commute under composition of relations. [1]

2.1. Algebraic characterization of linear lattices

Linear lattices are modular, but there are modular lattices which cannot be represented as linear lattices. A fundamental problem is to characterize linear lattices by identities. In 1945, Schützenberger [34] found an identity satisfied by certain modular lattices which is equivalent to Desargues' theorem. Shortly after that Jónsson [19] proved that every linear lattice satisfies a variant of Schützenberger's identity, now known as the *Arguesian law*. The following simpler equivalent form of the Arguesian law was found by Haiman [13]:

$$a_1 \wedge \{a_2 \vee [(b_1 \vee b_2) \wedge (c_1 \vee c_2)]\} \leq b_1 \vee \{(a_2 \vee b_2) \wedge [((b_1 \vee c_1) \wedge (b_2 \vee c_2)) \vee ((a_1 \vee c_1) \wedge (a_2 \vee c_2))]\}.$$

[1] The normal usage is to call such lattices *type-I lattices*. We follow Rota's preference for his own, perhaps more "catchy", terminology.

Lattices satisfying the Arguesian law are called *Arguesian lattices.* Linear lattices are Arguesian, but the converse is not true. In [14], Haiman constructed a family of Arguesian lattices which cannot be represented as linear lattices. This construction also implies that there does not exist a finite set of lattice identities or universal Horn sentences characterizing linear lattices. Nevertheless, linear lattices have a simple and elegant proof theory [13] along the lines of Gentzen's system of natural deduction for the predicate calculus. Specifically, there is a set of deduction rules such that for every lattice identity, either it has a formal proof in the deduction system (and hence is true in all linear lattices), or an (infinite) counterexample to it exists and can be explicitly constructed in terms of the deduction rules. The question remains whether this proof theory gives a decision procedure for the theory of linear lattices.

Rota has pointed out that one could determine whether linear lattices form an equational class without an explicit set of identities characterizing them by using a theorem of Birkhoff. This theorem states that a category of algebraic systems can be defined by identities if and only if it is closed under products, subalgebras and homomorphic images. It is easy to verify that the class of linear lattices is closed under products and subalgebras. Hence, one need only prove closure under homomorphic images. However, this seems difficult and the only known partial result is the following theorem of Herrmann [17]: Every homomorphic image of a finite length lattice represented by a lattice of subspaces of a vector space can again be so represented.

2.2. Structure of free linear lattices

Another theorem of Birkhoff asserts that a category of algebraic systems is endowed with free algebras if and only if it is closed under products and subalgebras. It follows that free linear lattices on any set of generators exist. The problem then arises of describing the structure of the free linear lattice generated by a given poset. There are two questions which are of particular interest: describe the free linear lattices generated by three disjoint chains, and the free linear lattice with n (mutually incomparable) generators.

It is known that the free linear lattice (or modular lattice) generated by two finite chains $\hat{1} = a_0 > a_1 > \cdots > a_k = \hat{0}$, $\hat{1} = b_n > \cdots > b_1 > b_0 = \hat{0}$ is finite and distributive. In fact, it is isomorphic to the Young lattice $Y(k, n)$, the lattice of order ideals of the product partially ordered set $[k] \times [n]$ of two chains, one having length k and the other having length n. It is also known that the free linear lattice with three generators has exactly twenty-eight elements. These elements describe explicitly all the projective invariants of three subspaces of a projective space in general position. On the other hand, free linear lattices with four or more generators and free linear lattices generated by three or more chains are infinite and complicated. Thus the free linear lattice generated by three chains or the free linear lattice on four generators are crucial examples for study, as they are the smallest "generic" linear lattices which are not finite. The second example would also shed light on the fundamental properties of linear varieties in projective spaces.

The free linear lattice on n generators is intimately related to the ring of invariants of a set of n subspaces in general position in projective spaces. Gelfand has conjectured that the free linear lattices in four generators is decidable. If true, this conjecture would distinguish the class of linear lattices from that of modular lattices, for it is proved by Freese [8] and Herrmann [16] that the free modular lattices with four or more generators have an undecidable word problem. A thorough study of representations of free linear lattices in vector spaces was carried out by Gelfand and Ponomarev in [9] and [10]. It should be possible to translate their constructions using lattice-theoretic language to linear lattices. Such an extension will shed light on rings of invariants and may lead to a solution to Gelfand's conjecture.

2.3. Linear lattices and synthetic projective geometry

A major application of linear lattices is to synthetic projective geometry. This is done by regarding joins and meets as algebraic renderings of spans and intersections of subspaces [2, 5, 12]. It is very likely that many invariant properties of subspaces of vector spaces should be expressible as identities holding in linear lattices or modular lattices. Hawrylycz and Rota conjectured that for any theorem holding in *all* projective geometries, a closely related identity, with spans and intersections replaced by joins and meets, will hold in linear lattices. A first step in this program is to check whether one can get valid lattice identities for the classical theorems in projective geometry, such as the theorems of Desargues, Pappus, Bricard, and Fontené, and their higher dimensional generalizations (see [15] for descriptions of these theorems). The lattice identity equivalent to Desargues' theorem is the Arguesian law. Hawrylycz [15] went a step further and constructed a class of identities holding in Grassmann-Cayley algebras which correspond to classical theorems of projective geometry. Mainetti and Yan [21, 22] then developed a systematic method to translate a subfamily of Hawrylycz's identities into lattice identities valid in linear lattices. As Yan showed in [37], these methods also translate all the Hawrylycz identities into valid lattice identities among congruence varieties of Abelian groups.

The method of Mainetti and Yan can in fact be used to translate any identity holding in Grassmann-Cayley algebras into a lattice identity, which may or may not hold for all linear lattices. The key condition used by Hawrylycz is that his identities are "multilinear" in vectors or covectors. Such multilinearity properties are also used essentially in the proof of Mainetti and Yan that their translations of the subfamily of Hawrylycz's identities holds in linear lattices. Thus, multilinearity seems to be a natural condition ensuring that the translated lattice identity holds for linear lattices. Supporting this view is the following example. The identity in Grassmann-Cayley algebras corresponding to Pappus' theorem is:

$$\begin{aligned}&((b \vee c') \wedge (b' \vee c)) \vee ((c \vee a') \wedge (c' \vee a)) \vee ((a \vee b') \wedge (a' \vee b))\\ &\quad = ((c \vee b') \wedge (c' \vee b)) \vee ((a \vee b) \wedge (a' \vee c)) \vee ((a \vee b') \wedge (a' \vee c'))\end{aligned}$$

where a, b, c, a', b', c' are vectors in a Grassmann-Cayley algebra of dimension 3. This identity is not multilinear in the vectors a, b, c or the vectors a', b', c'. As expected, the Mainetti-Yan translation fails to create a identity valid in linear lattices. This is consistent with the fact that Pappus' theorem does not hold in projective geometries over skew fields. (Identities which do not hold in all linear lattices are also interesting, for such identities define natural varieties of linear lattices.) Currently, the simplest open problem is to find a valid linear lattice identity corresponding to Bricard's theorem, which is about incidence relations of lines in a projective plane. The Grassmann-Cayley algebra identity corresponding to Bricard's theorem is multilinear. A lattice version holding for congruence varieties of Abelian groups is given in [37].

2.4. Commuting equivalence relations and information theory

Two equivalence relations on a set are said to be *independent* when every equivalence class of the first has non-empty intersection with every equivalence class of the second. This notion of independence originated in information theory, and has the following intuitive interpretation. In the problem of searching for an unknown element, an equivalence relation can be viewed as a question, whose answer will tell which equivalence class the unknown element belongs to. Two equivalence relations are independent when the answer to one question gives no information on the possible answer to the other question. Pairs of equivalence relations occurring in algebra are seldom independent. Instead, they often commute, that is, they are isomorphic to disjoint sums of independent equivalence relations on disjoint sets. It would be interesting to find an information-theoretic interpretation of two commuting equivalence relations. Another open problem is to generalize the notion of two equivalence relations commuting to three or more equivalence relations.

2.5. Ferrers relations

In the theory of partitions of a number, a partition $\lambda_1 + \lambda_2 + \ldots + \lambda_r = n$, $\lambda_1 \geq \lambda_2 \geq \ldots \lambda_r > 0$ of a number n is represented as a Ferrers diagram consisting rows with $\lambda_1, \lambda_2, \ldots, \lambda_r$ boxes. Ferrers diagrams motivate the following definition. Let R be a binary relation on the set S. For an element a in S, let $R(a)$ be the set $\{b \in S : (a, b) \in R\}$. The relation R is a *Ferrers relation* if there is an linear ordering of S such that $R(a) \subseteq R(b)$ whenever $a \leq b$. Is there a simple algebraic characterization of Ferrers relations? Are there natural examples? Is there an information-theoretic interpretation?

3. Lattices and the foundations of probability theory

In the words of Rota, classical probability can be considered a game played on two lattices defined on a sample space: the Boolean σ-algebra of events and the lattice of Boolean σ-subalgebras. The lattice Σ of all (Boolean) σ-subalgebras of a Boolean algebra is one of the most interesting objects in lattice theory. For example, it has been proved that the class of σ-subalgebras satisfies no lattice identities other than the trivial ones and that every lattice can be embedded in a lattice of σ-subalgebras. On the other hand, by imposing suitable conditions on the Boolean algebra or its σ-subalgebras, one can obtain many classes of lattices as subclasses of the class of lattices of σ-subalgebras. Examples of such classes are the partition lattices, the modular lattices, the linear lattices, and their stochastic analogs. Understanding the structure of lattices of Boolean σ-subalgebras would greatly enhance our knowledge of the interplay between lattice theory and probability.

3.1. Algebraic and stochastic independence

The lattice of all Boolean σ-subalgebras of a Boolean algebra is a natural generalization of the lattice of equivalence relations on a set; in fact, the two notions coincide in the case of finite Boolean algebras. The notion of independence can be extended to Boolean σ-subalgebras. Two Boolean σ-subalgebras B and C are *algebraically independent* if for all non-zero elements $b \in B$ and $c \in C$,

$$b \wedge c \neq \hat{0}.$$

A strengthening of algebraic independence is stochastic independence. Given a probability measure P, two σ-subalgebras B and C are *stochastically independent* if, for elements $b \in B$ and $c \in C$,

$$P(b \wedge c) = P(b)P(c)$$

Banach proved the following theorem for a sequence of algebraically independent σ-subalgebras (B_i) of a lattice B of σ-subalgebras. Let P_i be a probability measure on B_i. Then there exists a probability measure P on B such that the the σ-subalgebras B_i in the sequence are stochastically independent, and the restriction P to the σ-subalgebra B_i equals P_i for all indices i. A definition of algebraic commutativity for a pair of Boolean σ-subalgebras was proposed and an analog of the Banach's theorem for a pair of σ-subalgebras was proved in [36]. However, two questions are still open. (1) Extend the definition of algebraic and stochastic commutativity to sequences of σ-subalgebras. (2) Find an analog of Banach's theorem for sequences of commuting σ-subalgebras.

3.2. Lattices of commuting σ-subalgebras

The concept of commuting equivalence relations also has a stochastic analog. The σ-subalgebras B and C are *stochastically commuting* if, for all pairs of random variables X and Y measurable with respect to the σ-subalgebras B and C respectively, the following equality holds between conditional expectations:

$$E(X|B \cap C)E(Y|B \cap C) = E(XY|B \cap C),$$

or, equivalently, the conditional expectation operators E_B and E_C commute, that is, $E_B \circ E_C = E_C \circ E_B$. In [36], Yan characterized the structure of a pair of non-atomic stochastically commuting σ-subalgebras, thus, obtaining the probabilistic analog of Dubreil-Jacotin's theorem for commuting equivalence relations.

A stochastic analog of a linear lattice is a sublattice of the lattice of σ-subalgebras in which any two elements are stochastically commuting. It is natural to ask what lattice identities are valid in lattices of (algebraically or stochastically) commuting σ-subalgebras. In particular, do the Arguesian law and its higher dimensional generalizations hold in lattices of commuting σ-subalgebras? It is not known whether these two classes of lattices can be defined by a set of identities. A promising approach to this problem is to to develop a proof theory for such lattices, extending Haiman's proof theory for linear lattices. We expect to have a syntactic set of deduction rules which is complete, in the sense that every valid theorem in the theory of lattices of commuting σ-subalgebras is provable by the deduction rules. Such a proof theory should lead to an algebraic characterization of lattices of commuting σ-subalgebras. Finally, it would be interesting to find necessary and sufficient conditions for a lattice of commuting σ-subalgebras to be a linear lattice.

3.3. Lattices of σ-subalgebras associated with stochastic processes

The *σ-subalgebra of the random variable* X is the smallest σ-subalgebra relative to which X is measurable. Two random variables are *conditionally independent* if their σ-subalgebras are stochastically commuting. Rota has conjectured that Gaussian processes are "typical" in the following sense: any sufficiently large family of conditionally independent random variables can be made simultaneously Gaussian.

The lattice of σ-subalgebras *associated with* a stochastic process is the sublattice generated by the σ-subalgebras of all the random variables belonging to the stochastic process in the lattice of all σ-subalgebras of the sample space. For example, the lattice of σ-subalgebras associated with a martingale is isomorphic to a linearly ordered set and this fact plays an essential role in the study of martingales. Since linearly ordered σ-algebras stochastically commute, lattices of σ-subalgebras associated with martingales are stochastically commuting.

Another example is the following Gaussian process. Let $X_1, X_2, \ldots, X_n$ be n independent random variables with the standard normal distribution and consider the Gaussian process

$$\{\sum_{i=1}^{n} a_i X_i : (a_1, a_2, \ldots, a_n) \in \mathbf{R}^n\}.$$

Then the lattice associated with the Gaussian process is isomorphic to the lattice of subspaces of $\mathbf{R^n}$ under the bijection: a subspace W corresponds to the σ-subalgebra $X(W)$ generated by the random variables $\sum a_i X_i$, $(a_1, a_2, \ldots, a_n) \in W$. Moreover, the σ-subalgebras $X(W)$ commute stochastically. However, in contrast to martingales, the lattice structure had remained marginal in the study of these Gaussian processes.

It would be interesting to find other natural examples of stochastic processes whose associated lattices of σ-subalgebras are stochastically commuting. In addition, one may also try to establish connections between probabilistic properties of a stochastic process and algebraic properties of its associated lattice of σ-subalgebras. Specifically, intriguing problems are to find interpretations of the distributive axiom, the modular axiom, and the Arguesian law for stochastic processes.

4. Continuous geometries, quantum probability, and profinite combinatorics

A *continuous geometry* is a complemented, modular, irreducible, order complete topological lattice not satisfying a chain condition. Continuous geometry was discovered by von Neumann while trying to find a probabilistic setting for quantum mechanics [25]. These geometries are continuous analogs of lattices of subspaces of projective spaces. In particular, they have dimension functions which take all values in the interval $[0, 1]$. Von Neumann constructed a non-commutative ring from a continuous geometry. This ring shares many properties with rings of random variables. In particular, there is an analog of probability distributions for continuous geometries.

4.1. Continuous geometries and lattices of commuting σ-subalgebras

The theory of continuous geometry is very suggestive for the theory of lattices of commuting σ-subalgebras, since there is strong evidence that the lattices of commuting σ-subalgebras can also be equipped with a "continuous" dimension function. In particular, there should be a similar axiomatization for the theory of lattice of commuting σ-subalgebras. In addition, if a dimension function can be defined, lattices of commuting σ-subalgebras, especially the ones arising naturally, make better models for invariant theory and the study of linear varieties in projective spaces.

4.2. Quantum probability

Von Neumann obtained quantum probability from "classical" probability by relaxing the condition that conditional expectation operators commute. He also introduced hyperfinite factors, which are algebras whose elements provide quantum analogs called *observables* of random variables. The lattice which plays the role of the Boolean σ-algebra of events in ordinary probability is the lattice of all closed subspaces of a hyperfinite factor. Such lattices were called *quantum lattices* by Rota. Quantum lattices are not necessarily distributive, but they are always complemented and modular. In fact, they can be realized as complemented lattices of stochastically commuting σ-subalgebras. A quantum lattice is also endowed with a function called the *trace* which satisfies many but not all properties of probability measures.

The problem of deriving the algebra of observables from the (modular) lattice structure of quantum mechanics was thought to be intractable, even by von Neumann. However, with the extra knowledge that the quantum lattice is a lattice of stochastically commuting σ-subalgebras, a derivation of the algebra of observables from the quantum lattice structure now seems feasible. If the theory of lattices of stochastically commuting σ-subalgebras captures the fundamental properties of observables, then the next step is to develop a new logic for quantum mechanics. Rota and his coauthors have made several steps in this direction in [6,7].

4.3. Profinite combinatorics

Von Neumann [24] (see also [3], p. 237) observed that there is a natural embedding of projective geometries over a finite field of order q which doubles the rank. This embedding

$$\mathrm{PG}(2^{\mathrm{m}},\mathrm{q}) \to \mathrm{PG}(2^{\mathrm{m}},\mathrm{q}) \times \mathrm{PG}(2^{\mathrm{m}},\mathrm{q}) \to \mathrm{PG}(2^{\mathrm{m}+1},\mathrm{q})$$

is given by

$$a \mapsto (a,a) \mapsto (a,0) \vee (0,a).$$

Taking the profinite limit of the directed system

$$\mathrm{PG}(1,\mathrm{q}) \to \mathrm{PG}(2,\mathrm{q}) \to \mathrm{PG}(4,\mathrm{q}) \to \ldots \to \mathrm{PG}(2^{\mathrm{m}},\mathrm{q}) \to \mathrm{PG}(2^{\mathrm{m}+1},\mathrm{q}) \to \ldots,$$

one obtains the *continuous geometry* CG(q) *over the finite field of order q* in which there are subspaces of "dimension" r for every real number r in the unit interval $[0,1]$.

In [11], Goldman and Rota proved finite q-identities by giving bijections between objects (such as subspaces, bases, and linear transformations) defined on finite vector or projective spaces. Rota suggested that infinite q-series identities can be given natural bijective proofs using the continuous geometries CG(q). He also suggested that there is a q-analog of the Poisson process on CG(q).

Together with the interpretation of the Riemann zeta function by a critical problem on profinite cyclic groups [1], the continuous geometries CG(q) are motivating examples for Rota's conception of a new subject: *profinite combinatorics*. Rota was just beginning to write down his ideas on this subject at the time of his death. All we have are the fragments of his vision in [32].

5. Expansions of set functions

This is the sixth problem in Rota's list [31]. This problem originated in an abstract [35] of Norbert Weiner, in which the possibility of finding a "Volterra" or power series expansion for set functions was discussed. McMillan [23] responded to this idea by proving an analogue for a general class of functions of a theorem of S. Bernstein, that if the differences of a function $F(x)$ are all non-negative on the unit interval $[0,1]$, then $F(x)$ can be represented as a power series

$$F(x) = \sum_{n=0}^{\infty} F^{(n)}(0)x^n/n!$$

on $[0,1)$. This class of functions includes functions defined on a suitable ring of subsets of the form

$$F(A) = f_0 + \int_A f_1 d\mu + \int_A \int_A f_2 d\mu d\mu + \ldots$$

In his proof, McMillan developed a theory of finite differences for the functions he studied. The subject then lay dormant. In this section, we present a brief exposition based on several informal discussions with Rota.

Let $\mathcal{C}$ be a *ring* of sets, that is, a collection of sets closed under finite unions and intersections. An *n-ary set function* is a function defined from the n-fold cartesian product $\mathcal{C} \times \mathcal{C} \times \ldots \times \mathcal{C}$ to a commutative ring R. A unary set function will be called a set function. A set function v is a *valuation* v if for all subsets A and B in $\mathcal{C}$,

$$v(A) + v(B) = v(A \cup B) + v(A \cap B)$$

and

$$v(\emptyset) = 0.$$

A n-ary set function w is an *n-ary valuation* v if for every index i and every fixed sequence $A_1, A_2, \ldots, A_{i-1}, A_{i+1} \ldots, A_n$ of subsets from $\mathcal{C}$, the "marginal" function

$$A \mapsto w(A_1, A_2, \ldots, A_{i-1}, A, A_{i+1} \ldots, A_n)$$

is a valuation. Just as valuations are set function analogues of linear functions, n-ary valuations are analogues of multilinear functions.

If one set all the variables equal to one variable X in a multilinear function, one obtains a constant multiple of a power of X. This motivates the following definition. A set function f is a *homogeneous set function of degree n* if there exists an n-ary valuation w such that for all subsets A in $\mathcal{C}$,

$$f(A) = w(A, A, \ldots, A).$$

Such an n-ary valuation satisfying equation is called an *underlying n-ary valuation* for the set function f. The n-ary valuation w is usually not uniquely determined by f.

For example, if v_1 and v_2 are valuations on a ring $\mathcal{C}$, then the product $A \mapsto v_1(A)v_2(A)$ is a *quadratic* or degree-2 homogeneous set function. If $\mathcal{F}$ is the ring of all subsets of a finite set and f is a quadratic homogeneous set function with underlying 2-valuation w, then by expanding $w(A, A)$, we have

$$f(A) = \sum_{\{a\} \subseteq A} f(\{a\}) + \sum_{\{a,b\} \subseteq A} [f(\{a, b\}) - f(\{a\}) - f(\{b\})].$$

In particular, a quadratic homogeneous set function on $\mathcal{F}$ is determined by its value on subsets of cardinality one or two. Similarly, a degree-i homogeneous set function on $\mathcal{F}$ is determined by its value on subsets of cardinality i or less. There is a continuous analog of part of this. The set function ϕ on the collection all measurable subsets of the real numbers given by

$$\phi(A) = \int \int_{A \times A} f(x, y) dx dy,$$

where $f(x, y)$ is an integrable function, is a quadratic set function on the ring of measurable subsets over the reals or an interval of the reals. However, not all quadratic set functions are of this form. Is there an analogue of the Radon-Nikodým theorem for quadratic homogeneous set functions and, more generally, higher degree homogeneous set functions?

A *polynomial* set function of degree n on a ring $\mathcal{C}$ is a finite sum of homogeneous set functions, all of degree at most n. As one would expect, every set function on a finite ring of subsets is polynomial. Indeed, if f is a set function on a finite ring $\mathcal{C}$, then f can be written as a finite sum

$$f = \theta_0 + \theta_1 + \theta_2 + \ldots,$$

where θ_i is a pure degree-i homogeneous set function of degree i. Here, a degree-i homogeneous set function θ is *pure* if $\theta(A) = 0$ for all sets A of cardinality less than i. The main problem, for set functions over collections of finite sets, is to find interesting examples of such expansions. We know only one such example. The principle of inclusion and exclusion can be regarded (although in a somewhat unnatural way) as a set function expansion. Needless to say, examples of polynomial set functions over other rings of subsets would also be of great interest. Rota suggested that one might find natural examples in geometric probability and the theory of convex sets (see [20]).

6. The generator field of a Boolean algebra

To define a measure on a Boolean algebra, one needs a field, usually the real numbers, where the measure takes its values. The generator field gives a way to construct a universal field of values for all measures on a given Boolean algebra using only the structure of the Boolean algebra.

Let $\mathcal{B}$ be a Boolean algebra. The *generator ring* $G_0(\mathcal{B})$ of $\mathcal{B}$ over the field F is the quotient ring $F[x_a : a \in \mathcal{B}]/\mathcal{I}$, where $F[x_a : a \in \mathcal{B}]$ is the ring of polynomials in the variables x_a, one for each element a of the Boolean algebra $\mathcal{B}$ and I is the ideal generated by the elements of the form

$$x_{a\vee b} + x_{a\wedge b} - x_a - x_b,$$

and $x_{\hat{0}}$, if $\mathcal{B}$ has a minimum $\hat{0}$. In particular,

$$(*) \qquad x_{a\vee b} = x_a + x_b - x_{a\wedge b} \quad \text{and} \quad \mathrm{x}_{\hat{0}} = 0$$

in $G_0(\mathcal{B})$. Note that we did not include the element $x_{a\wedge b} - x_a x_b$ in I and so $x_{a\wedge b}$ does not necessarily equal $x_a x_b$ in $G_0(\mathcal{B})$.

When $\mathcal{B}$ is an atomic Boolean algebra, then, by equation $(*)$ and the requirement that $x_{\hat{0}} = 0$, the generator ring $G_0(\mathcal{B})$ is isomorphic to the ring of polynomials $F[x_c]$, where c ranges over all the atoms of $\mathcal{B}$.

LEMMA (Rota). The generator ring $G_0(\mathcal{B})$ is an integral domain.

Proof. Suppose $p(x_a)q(x_a) = 0$ in $G_0(\mathcal{B})$. Then the set X of all the elements of $\mathcal{B}$ occurring as subscripts in $p(x_a)$ and $q(x_a)$ is finite. Hence, the Boolean subalgebra $\mathcal{B}_{\mathcal{X}}$ generated by X is finite. Since finite Boolean algebras are atomic and equation $(*)$ holds in $G_0(\mathcal{B})$, the subring generated by all the variables occurring in $p(x_a)$ and $q(x_a)$ is isomorphic to a polynomial ring. Since polynomial rings are integral domains, we conclude that $p(x_a) = 0$ or $q(x_a) = 0$.

The *generator field* $G(\mathcal{B})$ is defined to be the field of fractions of the integral domain $G_0(\mathcal{B})$. It is evident that G_0 is a functor from the category of Boolean algebras to the category of integral domains. Taking F to be the field of rational numbers, we obtain a field of characteristic zero defined intrinsically from the Boolean algebra.

One can go further using valuation rings [28]. Recall that if $\mathcal{L}$ is a distributive lattice and A a commutative ring, let $A[\mathcal{L}]$ be the ring of finite formal linear combinations $\sum a_i x_i$, where $a_i \in F$ and $x_i \in \mathcal{L}$ with multiplication given by $xy = x \wedge y$. By the distributivity axioms, the submodule I of $A[\mathcal{L}]$ generated by elements of the form

$$x + y - x \vee y - x \wedge y$$

is an ideal of $A[\mathcal{L}]$. The *valuation ring* $\mathrm{Val}(\mathcal{L}, \mathcal{A})$ (*over the base ring* A) is the quotient ring $A[\mathcal{L}]/\mathcal{I}$. Valuations on $\mathcal{L}$ correspond to linear functionals on its valuation ring. Taking the valuation ring $\mathrm{Val}(\mathcal{B}, \mathcal{G}(\mathcal{B}))$ with the generator field of $\mathcal{B}$ as the base field, one obtains the *universal valuation ring* for a Boolean algebra.

The theory of generator rings, generator fields, and universal valuation rings is totally undeveloped. A specific problem, which can be tackled independently of a theory, is to describe the generator field and universal valuation ring of the Boolean algebra of all Borel sets on the unit interval or the real line.

7. Straightening coefficients and Rota's basis conjecture

The straightening algorithm rewrites a bideterminant (which are products of determinants of matrices with generic variable entries) in the letter-place algebra as a unique linear combination of bideterminants which are "standard" [4,5]. This algorithm has been generalized [12]. A fundamental question in this area is the *problem of straightening coefficients:* given a bideterminant D and a standard bideterminant S, find a *direct* combinatorial way to compute the coefficient of S in the linear combination obtained from D by the straightening algorithm. A good answer for a generalized form of the straightening formula would resolve the vector space case of the following conjecture of Rota.

ROTA'S BASIS CONJECTURE. Let $\{x_1, x_2, \dots, x_n\}$, $\{y_1, y_2, \dots, y_n\}$, $\dots$, and $\{z_1, z_2, \dots, z_n\}$ be n bases in a rank-n matroid. Then, there exist n permutations $\alpha, \beta, \dots, \tau$ such that every column of the array

$$\begin{bmatrix} x_{\alpha(1)} & x_{\alpha(2)} & \cdots & x_{\alpha(n)} \\ y_{\beta(1)} & y_{\beta(2)} & \cdots & y_{\beta(n)} \\ \vdots & \vdots & \dots & \vdots \\ z_{\tau(1)} & z_{\tau(2)} & \cdots & z_{\tau(n)} \end{bmatrix}$$

is a basis of the matroid.

A discussion of this conjecture can be found in [18].

References

1. Alexander, K., Baclawski, K. and Rota, G.-C., *A stochastic interpretation of the Riemann zeta function,* Proc. Nat. Acad. Sci. U.S.A. *90*(1993), 697–699.

2. Barnabei, M., Brini, A. and Rota, G.-C., *On the exterior calculus of invariant theory,* J. Algebra, *96*(1985), 120–160.

3. Birkhoff, G., *Lattice Theory,* 3rd edn, Amer. Math. Soc., Providence R.I., 1967.

4. Désarmenien, J., Kung, J. P. S., and Rota, G.-C., *Invariant theory, Young bitableaux, and combinatorics,* Adv. Math., *27*(1978), 63–92.

5. Doubilet, P., Rota, G.-C. and Stein, J., *On the foundation of combinatorial theory. IX. Combinatorial methods in invariant theory,* Stud. Appl. Math., *53*(1976), 185–216.

6. Ellerman, D. P. and Rota, G.-C., *A measure theoretic approach to logical quantification,* Rend. Sem. Mat. Univ. Padova *59*(1978), 227–246.

7. Finberg, D., Mainetti, M. and Rota, G.-C., *The logic of commuting equivalence relations,* A. Ursini and P. Agliano, eds., Logic and Algebra (Pontignano, 1994), Marcel Dekker, New York, 1996, 69–96.

8. R. Freese, *Free modular lattices*, Trans. Amer. Math. Soc., *261*(1980), 81–91.

9. Gelfand, I. M. and Ponomarev, V. A., *Problems of linear algebra and classification of quadruples of subspaces in a finite-dimensional vector space,* Hilbert Space Operators and Operator Algebras (Proc. Internat. Conf., Tihany, 1970), Colloq. Math. Soc. János Bolyai, 5, North-Holland, Amsterdam, 1972, 163–237.

10. Gelfand, I. M. and Ponomarev, V. A., *Free modular lattices, and their representations,* Uspehi Mat. Nauk *29*(1974), 3–58.

11. Goldman, J. R. and Rota, G.-C., *On the foundations of combinatorial theory. IV. Finite vector spaces and Eulerian generating functions,* Stud. Appl. Math. *49*(1970), 239–258.

12. Grosshans, F. D., Rota, G.-C. and Stein, J. A., *Invariant Theory and Superalgebra,* Amer. Math. Soc., Providence RI, 1987.

13. Haiman, M., *Proof theory for linear lattices,* Adv. Math. *58*(1985), 209–242.

14. Haiman, M., *Arguesian lattices which are not type-1,* Algebra Universalis *28*(1991), 128—137.

15. Hawrylycz, M., *Arguesian identities in invariant theory,* Adv. Math. *122*(1996), 1–48.

16. C. Herrmann, *On the word problem for modular lattices with four generators*, Math. Ann. *265*(1983), 513–527.

17. C. Herrmann, *On the contraction of vectorial lattice representations*, Order *8*(1991), 275–281.

18. Huang, R. and Rota, G.-C., *On the relations of various conjectures on Latin squares and straightening coefficients,* Discrete Math. *128*(1994), 225–236.

19. Jónsson, B., *On the representation of lattices,* Math. Scand. *1*(1953), 193–206.

20. Klain, D. A. and Rota, G.-C., *Introduction to Geometric Probability,* Cambridge University Press, Cambridge, 1997.

21. Mainetti, M. and Yan, C. H., *Arguesian identities in linear lattices,* Adv. Math. *144*(1998), 50–93.

22. M. Mainetti and C. Yan, *Geometric identities in lattice theory*, J. Combin. Theory Ser. A, *91*(2000), 411–450.

23. McMillan, B., *Absolutely monotone functions,* Ann. of Math. *60*(1954), 467–501.

24. von Neumann, J., *Examples of continuous geometries,* Proc. Nat. Acad. Sci. *22*(1936), 101–108.

25. von Neumann, J., *Continuous Geometries,* Princeton University Press, Princeton NJ, 1960.

26. Rota, G.-C., *On the representation of averaging operators,* Rend. Sem. Mat. Univ. Padova, *30* (1960), 52–64.

27. Rota, G.-C., *On the foundations of combinatorial theory. I. Theory of Möbius functions,* Z. Wahrscheinlichkeittheorie und Verw. Gebiete, *2*(1964), 340–368.

28. Rota, G.-C., *On the combinatorics of the Euler characteristic,* Studies in Pure Mathematics (Papers presented to Richard Rado), Academic Press, London, 1971, 221-233.

29. Rota, G.-C., *Baxter operators, an introduction,* Gian-Carlo Rota on Combinatorics, J. P. S. Kung, ed., Birkhäuser, Boston and Basel, 1995, 504–512.

30. Rota, G.-C., *The many lives of lattice theory,* Notices Amer. Math. Soc. *44*(1997), 1440–1445.

31. Rota, G.-C., *Ten mathematics problems I will never solve,* DMV Mittellungen *2*(1998), 45–52.

32. Rota, G.-C., *Combinatorial snapshots,* Amer. Math. Soc. Colloquium Lectures, Baltimore MD, January 10–12, 1998.

33. Rota, G.-C., *Twelve problems in probability no one likes to bring up (The Fubini Lectures, Torino, Italy, June 3–5, 1998),* H. Crapo and D. Senato, eds., Algebraic Combinatoircs and Computer Science, a Tribute to Gian-Carlo Rota, Springer-Verlag Italia, Milano, 2001, 57–93.

34. Schützenberger, M.-P., *Sur certains axiomes de la théorie des structures,* C. R. Acad. Sci. Paris *221* (1945), 218–220.

35. Weiner, N., *Abstract 45-3-133,* Bull. Amer. Math. Soc. *45*(1939), 234.

36. Yan, C. H., *The theory of commuting Boolean algebras,* Ph. D. Thesis, Massachusetts Institute of Technology, Cambridge MA, 1997.

37. Yan, C. H. *Arguesian identities in the congruence varieties of Abelian groups,* Adv. Math. *150* (2000), 36–79.