Proc. Univ. of Houston
Lattice Theory Conf..Houston, 1973

The Valuation Ring of a Distributive Lattice

by

Gian-Carlo Rota
Massachusetts Institute of Technology

Contents

1. Introduction

Traditionally, the algebraic properties of Boolean algebras are reduced to those of Boolean rings by a well-known construction. A Boolean ring, however, has the double disadvantage of having torsion, and of not being applicable to the richer domain of distributive lattices. In this paper we describe another construction, or functor, called the valuation ring, which associates to every distributive lattice L a torsionless ring $V(L)$ generated by idempotents. The lattice L can be recovered by giving a suitable order structure to the valuation ring $V(L)$, and thus the entire theory of distributive lattices is reduced to that of a simple class of rings. For example, the representation theory of distributive lattices is subsumed to that of valuation rings, where standard methods of commutative algebra apply.

The applications and further development of the present techniques lie in at least three directions.

First, the valuation ring turns out to be a very simple way of functorially associating a ring to a simplicial complex; we surmise that simplicial homology will benefit from this association.

Second, the theory of pseudo-Boolean functions and programming of Hammer and Rudeanu can be seen to be an informal use of valuation rings; this theory can gain from the rigorous foundation provided by the present ideas.

Third, the notion of quantifier on a Boolean algebra can be transferred to the valuation ring, where it becomes a linear averaging operator; in this way, problems in first-order logic can be translated into problems about commuting sets of averaging operators on commutative rings. The resulting linearization of logic is probably the most promising outcome of the present investigations.

The method of presentation is deliberately informal and discursive. Some of the proofs are barely sketched; we hope to give a thorough presentation elsewhere.

2. The Valuation Ring. The theory of distributive lattices is richer than the better known theory of Boolean algebras; nevertheless it has had an abnormal development, for a variety of reasons of which we shall recall two. First, Stone's representation theorem of 1936 for distributive lattices closely imitated his representation theorem for Boolean algebras, and as a consequence turned out to be too contrived (I have yet to find a person who can state the entire theorem from memory.) Second, a strange prejudice circulated among mathematicians, to the effect that distributive lattices are just Boolean algebra's weak sisters.

More recently, the picture seems to have brightened. The definitive representation theorem for distributive lattices has been proved by H. A. Priestley; it extends at long last to all distributive lattices the duality "distributive lattice - partially ordered sets", first noticed by Birkhoff for finite lattices. Strangely, Nachbin's theory of ordered topological spaces had been available since 1950, but nobody before Priestley had had the idea of taking a totally disconnected ordered topological space as the structure space for distributive lattices.

The second prejudice was more difficult to overcome; it paralleled the criticism of similar prejudices in other branches of mathematics. To stay on comparatively familiar ground, consider what happened in combinatorics. Here, it became clear a short while ago that the notion of set would have to be supplemented by a more pliable notion, which Knuth has called multiset. A multiset is simply a set where every element is assigned a multiplicity, positive negative or zero. Aside from the fact that multisets are found plentifully in nature, they offer a decisive advantage over sets: they form a torsionless ring, where addition and multiplication are defined "elementwise" (Indeed, multisets are functions from a set to the integers.) Sets, on the other hand, have a more rigid algebraic structure: they form a Boolean algebra, or at best a distributive lattice. But it turns out that even for the study of Boolean operations on sets it is preferable to work with the ring of multisets, as was first noted by Whitney; unfortunately, his suggestion went unheeded until recently.

It is this idea that I put forth a few years ago in my paper in the Rado Festschrift (It seems that publishing an idea in a Festschrift is the quickest way to have it forgotten.)

Given a distributive lattice L, can we associate to L a ring V(L) such that, if the lattice L were to be a lattice of sets, then V(L) would "automatically" turn out to be isomorphic to the ring of multisets over the same set?

Such a ring V(L) is easily constructed as follows. To begin with, construct an intermediate ring F(L) consisting of all formal linear combinations of elements of L. Addition is defined formally, and multiplication in two steps: if x and y are elements of L, set $x\,y = x \wedge y$, then extend by bilinearity.

Now, the main fact about the ring F(L) is that the submodule J generated by elements of the form

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

is an ideal! The verification is easy. For any $z \in L$, we must show that the element

$$z(x + y - x \wedge y - x \vee y) \qquad (*)$$

belongs to J. Expanding this expression we find it equals

$$z \wedge x + z \wedge y - z \wedge (x \wedge y) - z \wedge (x \vee y).$$

We now use various identities satisfied in distributive lattices. The third term equals

$$z \wedge (x \wedge y) = (z \wedge x) \wedge (z \wedge y)$$

using commutative, associative and idempotent laws for the meet operation $\wedge$. The fourth term is simplified by the distributive law:

$$z \wedge (x \vee y) = (z \wedge x) \vee (z \wedge y) . \qquad (**)$$

Making all these substitutions, we find that (*) equals

$$z \wedge x + z \wedge y - (z \wedge x) \wedge (z \wedge y) - (z \wedge x) \vee (z \wedge y),$$

which clearly belongs to the submodule J, thereby completing the proof that J is an ideal.

Now define the valuation ring of the distributive lattice L to be the quotient ring $V(L) = F(L)/J$.

Before proceeding any further, note the following amusing aside. To define the valuation ring, all we need is a set L, together with two binary operations $\wedge$ and $\vee$, say, such that, (a) the operation $\wedge$ is commutative, associative and idempotent, and (b) the distributive law (**) holds. Nothing else

is assumed of the operation $\vee$. Are these identities sufficient to define a distributive lattice?

Now, the construction of the valuation ring is (like every other "construction") a functor from the category of distributive lattices to the category of rings. Thus, every distributive-lattice concept should have an analog for a certain sub-category of rings. For example, an ideal in the lattice-theoretic sense, namely, a subset I of L closed under joins and such that $x \vee y \in I$ for $x \in I$ and $y \in L$, is, when considered as a subset of the valuation ring V(L), an ideal in V(L) in the ring-theoretic sense.

The problem therefore arises of how to recover the lattice L from the valuation ring V(L). Let us consider two special cases. First, suppose that L is the lattice of all subsets of a finite set S. Then the valuation ring V(L) is naturally isomorphic to a ring of multisets on the set S. This non-trivial fact validates our claim that the valuation ring is indeed the algebraic analog of the ring of multisets.

But now take an ordered set P, and let L=L(P) be the lattice of decreasing subsets of P; a subset D of P is decreasing, if $x \in D$ and $y \leq x$ imply that $y \in D$ (decreasing sets are also called order-ideals, but we prefer the former

term, recently introduced by Priestley.) Lattice operations are unions and intersections of sets. Then it can be shown that V(L) is isomorphic as a ring to V(B), where B is the Boolean algebra of subsets of P generated by decreasing sets. If P is a finite set, then B is the Boolean algebra of all subsets of P.

In order to strengthen the structure of the valuation ring V(L) we must impose some order structure. We shall do it in the simplest way. A valuation ring V(L) will be a torsionless commutative ring generated by idempotents, with a distinguished sublattice L of idempotents, such that L generates the ring. In other words, L will be a subset of idempotents closed under products and under the operation $x,y \to x+y-xy$. A morphism of valuation rings ϕ: $V(L) \to V(L')$ is a ring homomorphism which maps L into L'. Every valuation ring V(L) is the valuation ring of the set L considered as a distributive lattice, and the two will be identified.

An element

$$x = \sum_{e \in L} n(e)e \quad , \quad n(e) \geq 0$$

is called monotonic. Monotonic elements are closed under sums

and products, in other words they form a cone or semiring. It is possible to characterize a valuation ring in terms of this semiring C, as follows.

A commutative ring R with identity will be called a valuation ring if it is endowed with a distinguished subset, or cone, C, closed under sums and products, and forming a distributive lattice, such that:

(a) The lattice operations in C are compatible with sums and products, that is $f + (g \wedge h) = (f + g) \wedge (f + h)$ similarly with $\vee$, for f,g and h in C, as well as all other identities satisfied in a lattice-ordered commutative ring which can be written without using subtraction;

(b) Every element of C is a (finite) sum of idempotents belonging to C;

(c) Every element of R is the difference of two elements of C.

This intrinsic characterization suggests the extension of the present theory to rings not generated by idempotents; such an extension might give an extension of classical predicate logic (see below.)

The category of valuation rings is equivalent to the category of distributive lattices. It has a generator, namely, the valuation ring of the two-element lattice; we

shall see that this fact can be used to obtain a representation theorem for valuation rings. Actually, more is true, but neither category theorists nor first-order logicians have yet invented a precise way of saying it, though the appropriate term was introduced long ago by Birkhoff: the two categories (or first-order theories) are cryptomorphic. In other words, to every fact about one there "naturally" corresponds a fact about the other. The algebraic structure of a valuation ring is richer than that of a ring. It turns out that the linear functional

$$\varepsilon\Big(\sum_{e\in L} n(e)e\Big) = \sum_{e\in L} n(e)$$

is an augmentation of the ring, that is, it is a ring homomorphism. Setting

$$f \vee g = \varepsilon(g)f + \varepsilon(f)g - fg, \quad f, g \in \mathbf{V(L)}$$

defines a second ring operation on V(L); actually, the same definition works for all augmented algebras.

If L has a minimal element z and a maximal element u, then u acts as an identity and z as an integral (Sweedler) in V(L); that is,

$$fz = \varepsilon(f)z, \quad f \in L.$$

In the $\vee$-ring, the roles of u and z are reversed. From now on, we shall assume all valuation rings endowed with u and z, and morphisms to preserve u and z.

The operation of complementation in a valuation ring R is defined as

$$\tau(f) = \varepsilon(f)(u + z) - f, \quad f \in R,$$

so that in particular

$$\tau(z) = u, \ \tau(u) = z, \ \tau(x) = u + z - x$$

if x is a positive idempotent. Note that the complementation τ is idempotent. Indeed

$$\tau^2(f) = \varepsilon(\tau(f))(u + z) - \tau f =$$

$$= \varepsilon(\varepsilon(f)(u + z) - f)(u + z) - \varepsilon(f)(u + z) + f =$$

$$= (2\,\varepsilon(f) - \varepsilon(f))(u + z) - \varepsilon(f)(u + z) + f = f,$$

as desired. As a further check that the complement τ is indeed a strengthening of the classical lattice-theoretic complement, suppose $R = V(L)$, and let x' be the complement

of x in L. Then check that $\tau(x) = x'$. Which identities in distributive lattices carry over to valuation rings? The answer is not hard to guess: all those identities where each variable occurs only once, that is, linearly. For example, the de Morgan law

$$(x \vee y)' = x' \wedge y'$$

carries over to the identity

$$\tau(f \vee g) = \tau(f)\tau(g),$$

but the distributive law

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

does not, because the variable x occurs twice, or non-linearly, on the right side. It does if one of the entries is idempotent, however.

One of the more interesting identities that carry over to the valuation ring is the inclusion-exclusion principle. It was in fact this identity that originally motivated my definition of the valuation ring. Recall that in the

valuation ring, for positive idempotents $x_1, x_2, \ldots, x_n$, one shows that

$$x_1 \vee x_2 \vee \ldots \vee x_n = x_1 + \ldots + x_n - x_1x_2 - x_1x_3 - \ldots -$$

$$-x_{n-1}x_n + x_1x_2x_3 + \ldots - \ldots + \ldots \pm x_1x_2\ldots x_n.$$

For arbitrary elements $f_1, f_2, \ldots, f_n$ one finds

$$f_1 \vee f_2 \vee \ldots \vee f_n = \sum_{i=1}^{n} (-1)^{n-i+1} \sum_{\sigma} \varepsilon(f_{\sigma 1} f_{\sigma 2} \ldots f_{\sigma i}) f_{\sigma(i+1)}$$

$$f_{\sigma(i+2)} \cdots f_{\sigma n},$$

where the inner sum ranges over all shuffles σ of the indices $1, 2, \ldots, n$. This identity is valid more generally in any augmented algebra.

3. Canonical Idempotents

Let S be a subset of the monotonic cone of $V(L)$, then the subring generated by S is of the form $V(L')$, where L' is a sublattice of L. Furthermore, if S is finite-dimensional, so is $V(L')$.

Now let L be a finite distributive lattice, and let P be the set of join-irreducibles of L, that is, of those elements $p \in L$ such that if $p = x \vee y$, then either $p = x$ or $p = y$. Clearly every element of L is the unique irredundant join of join-irreducibles. It is technically preferable not to consider z as a join-irreducible. The join-irreducibles are linearly independent. The Möbius function $\mu(p,q)$ is the integer-valued function on P such that

$$\mu(p,p) = 1$$

$$\mu(p,q) = 0 \quad \text{if } p \not\leq q$$

$$\sum_{p \leq q \leq r} \mu(p,q) = 0 \quad \text{for } p < r.$$

Now set

$$e(p) = \sum_{q \in P} \mu(q,p)q.$$

It can be shown that the $e(p)$ and z are a set of linearly independent

orthogonal idempotents spanning V(L), and that every $x \in L$ is a linear combination of the e(p) and z with coefficients 0 or 1; these properties uniquely characterize the e(p). We shall call them the canonical idempotents. If L is a sublattice of L', then the canonical idempotents of L are sums of those of L', so we may define the canonical idempotents of an arbitrary distributive lattice L as the union of all canonical idempotents of finite sublattices of L. Every linearly independent subset of orthogonal idempotents is then a subset of the set of idempotents of a finite sublattice of L.

The canonical idempotents can be used to derive criteria for the following: when is an $f \in V(L)$ actually a member of the lattice L, that is, expressible by joins and meets of join-irreducibles? In other words, when is a linear combination

$$f = \sum_{p \in P} c(p)p$$

actually expressible by the two lattice operations alone? This question is particularly important for free valuation rings (v. below). We shall answer it in two ways.

Expressing f in terms of the canonical idempotents we have

$$f = \sum_{p} a(p)e(p)$$

for some coefficients a, which can be computed in terms of the coefficients **c** .

Now $f \in L$ if and only if

(a) $a(p) = 0$ or 1 for all $p \in P$,

(b) if $a(p) = 1$ and $q \leq p$, then $a(q) = 1$.

In other words, the p for which $a(p) = 1$ form a decreasing set of the set P of join-irreducibles. Since

$$a(q) = \sum_{p \geq q} c(p)$$

this condition can be translated into one in terms of the c-coefficients, which gives the following necessary and sufficient condition for $f \in L$: there exists a <u>decreasing subset</u> A (= lower order-ideal: if $p \in A$ and $q \leq p$ then $q \in A$) of join-irreducibles such that

$$(*) \qquad c(q) = \sum_{p \in A} \mu(q,p).$$

For a free valuation ring (v. below) this condition has an elegant topological formulation. The problem whose solution

we have just outlined can be restated in purely combinatorial terms: when can a linear combination of idempotents be built up by using only product $x\,y$ and the operation $x + y - x\,y = x \vee y$? There is at least one case when the Möbius function can be explicitly computed and thus the solution can be restated more explicitly, that is the free valuation ring on an ordered set Q. Let Q be a set of commuting idempotents subject to identities $p\,q = p$, which define a partial order $p \leq q$. The monotonic cone generated by sums and products in Q defines the structure of a valuation ring $V(L)$, where L is the distributive lattice freely generated by the ordered set Q. Note that Q is not the set P of **join**-irreducibles of L; the set P is the set of all distinct products of elements of Q, thus, P is isomorphic to the distributive lattice of **increasing** sets of Q (order ideals). The Möbius function of P is calculated by the classical inclusion-exclusion principle, and the canonical idempotents are given by the formulas

$$e(\prod_{p\in S} p) = \sum_{B} (-1)^{|B|} \prod_{p\in B} p \quad , \quad S \subseteq Q$$

for every antichain S of Q, the sum ranging over every superset B of S.

Using the canonical idempotents, we can define an order relation in $V(L)$. For any monotonic f, the subring generated by f is of the form $V(L")$ for a finite $L"$. Since every $g \in V(L)$ is of the form $g = f-h$ with monotonic f and h, it follows that $g \in V(L')$ for some finite L'. Hence

$$g = \sum_{p \in P} a(p)e(p) ,$$

where P is the set of meet-irreducibles of L', and $e(p)$ the canonical idempotents. Say $g \geq 0$ if $a(p) \geq 0$ for all p. It can be shown that this is an order relation which makes $V(L)$ into a lattice-ordered ring. Note that this is a different order relation from the one defined by the monotonic cone.

The canonical idempotents can be used to systematically solve systems of Boolean equations in a distributive lattice. In fact the notion of pseudo-Boolean function of Hammer and Rudeanu is seen to be a special case of the valuation ring, and much of their theory can be extended to the present context.

4. Representation

If L is finite, then for $x \in L$ we have

$$x = \sum_{p \leq x} e(p) ,$$

and in this way we obtain a representation of every $x \in L$ as the indicator function (characteristic function) of a decreasing subset of the set P of join-irreducibles. The monotonic cone of $V(L)$ is thus represented as the cone of non-increasing functions on P, and $V(L)$ is represented as the ring generated by the indicator functions of increasing subsets of P. We thus obtain a very simple proof of Birkhoff's theorem.

We can extend this result to arbitrary valuation rings. Define $P(L)$ as the set of all prime ideals of the ring $V(L)$ generated by all canonical idempotents. Given any two prime ideals $a,b \in P(L)$, such that $a \not\geq b$ and $a \not\leq b$, we can find two orthogonal idempotents $e,f \in E(L)$ such that $e \in a$ and $f \in b$; now take a finite-dimensional sublattice L' for which $V(L')$ contains both e and f as canonical idempotents; it is then easy to find an increasing element p and a decreasing set q such that $e\,p = e$ and $f\,q = f$.

Now use the canonical idempotents, together with u and z, to define a compact totally order disconnected topology on the ordered set P(L). This topology, in view of the above remarks, enjoys the following property: given a,b not comparable, we can find an increasing clopen set p and a decreasing clopen set q such that a ε p and b ε q. Such a space is called totally order disconnected.

One thus gets the following representation theorem: every valuation ring is isomorphic to the ring generated by the (monotonic) cone of integer-valued non-increasing continuous functions on a totally order-disconnected compact space. This representation theorem is easier than the direct representation theorems for lattices, even for Boolean algebras.

Restated in categorical terms, the preceding argument can be made to prove the following. Consider the category Dis of distributive lattices having maximal element u and minimal element z, where morphisms are lattice-homomorphisms preserving u and z, as well as the category Val of valuation rings,where morphisms are ring homomorphisms preserving u and z and the monotonic cone; finally, the category Mon of all rings of continuous integer functions on totally order disconnected compact spaces, endowed with the monotonic cone of

all non-increasing functions, and morphisms consisting of all ring homomorphisms preserving the monotonic cone. The three categories are equivalent. (Note that in the category Mon the integral z requires special care.) By this equivalence, a host of questions relating to Boolean algebras and distributive lattices can be simplified.

A variant of the representation theorem replaces prime ideals by morphisms of V(L) into the valuation ring of the two-element distributive lattice. Another variant uses the representation in the finite case and constructs the space P(L) as a categorical limit. This last is perhaps the most satisfactory, though least familiar approach, since it exhibits totally order disconnected spaces as pro-finite ordered sets.

5. Homology

Let P be a finite ordered set. It is well-known that one can associate to P the homology groups of the simplicial complex $\Sigma(P)$ whose faces are all the linearly ordered subsets of P, ordered by inclusion. If P is already a simplicial complex, one obtains ordinary simplicial homology. If P has a unique minimal element z, then the homology of P is trivial. More generally, the rank of the zero-th homology group $H_0(\Sigma(P))$ equals the number of connected components in the Hasse diagram of the ordered set P, but an interpretation of the homology of P in terms of the order of P has not been given.

Now, we can associate to P the valuation ring of the distributive lattice of its decreasing sets, by a (contravariant) functor. This leads to the suspicion that the homology of an ordered set may be defined in an algebraic way by means of the associated valuation ring. It turns out in fact that the Koszul complex construction gives a resolution which is closely related to the simplicial homology of $\Sigma(P)$. Because the technique is not familiar, we briefly describe it here.

Suppose the valuation ring $V(L)$, with set P of join-irreducibles, acts on a module M. The most important case

occurs when M is a module of integer- or real-valued functions on a set S, and the action is obtained by associating to every $p \in P$ the indicator function of a subset of S, followed by ordinary multiplication. In plain words, the ordered set P is "represented" by a family of subsets of S, where inclusion of subsets is isomorphic to the order of P. The homology of P thus should be a measure of the complexity of a system of sets, relative to unions and intersections. Note that different modules M can give rise to essentially distinct homologies for the same ordered set P.

For simplicity denote the action of P on M by $(p,m) \to pm$, and list the elements of P, say $p_1, p_2, \ldots, p_n$. Choose anticommutative variables $e_1, \ldots, e_n$ generating an exterior algebra: $e_i e_j = - e_j e_i$. (Note: these are not members of $V(L)$.) Let $E_k(M)$ be the module of all linear combinations of elements of degree k, with coefficients in M, that is, of linear combinations of elements of the form

$$m\,(e_{i_1} e_{i_2} \ldots e_{i_k}), \quad 0 \leq k \leq n, \quad m \in M.$$

Define the boundary operator ∂ of such an element by

$$\partial(m\, e_{i_1} e_{i_2} \ldots e_{i_k}) =$$

$$= p_{i_1} m(e_{i_2} \dots e_{i_k}) - p_{i_2} m(e_{i_1} e_{i_3} \dots e_{i_k}) + \dots -$$

$$- \dots + (-1)^{k-1} p_{i_k} m(e_{i_1} e_{i_2} \dots e_{i_{k-1}}) .$$

This is well defined in view of the anticommutativity of the e_i. It is easily verified that $\partial^2 = 0$, so that we obtain a complex associating a **resolution to P and M .**

Our claim is that simplicial homology of an ordered set P can be obtained from the Koszul complex of P considered **as a subset of the valuation ring.**

The following questions may be worth investigating:

(a) Starting with the valuation ring of an infinite distributive lattice L , is it possible to define its homology by approximation by finite sublattices, whose valuation ring is a subring of the valuation ring of L ? This might simplify the process of simplicial approximation.

(b) In the finite ordered set P , the submodules M_k generated by $p_1 - p_2 + \dots + (-1)^{k-1} p_k$ $(p_1 \geq p_2 \geq \dots \geq p_k)$ generate all of the valuation ring. **Each of these** alternating sums is the indicator of a subset of P; thus we obtain a sequence of increasingly complex subsets of P , whose union is the family of all subsets of P . It is

inevitable to conjecture that the dimensions of M_k/M_{k-1} should be related to the Betti numbers of P. This filtration provides a measure of the complexity of a subset of P, which can in turn be used for the study of Boolean functions (see below.)

(c) The Koszul resolution may be expressed in terms of the canonical idempotents, instead of the join-irreducibles. In this way, one obtains an expression for the boundary in terms of the Mobius function. Is it possible in this way to relate the homology to the Mobius function? Judging by the example of geometric lattices, it should be.

(d) It is an open question to construct free resolutions for the valuation ring. Taking the elements of P as generators, one has the relations

$$p\ q = \sum_{r \in P} c(r)r$$

for suitable coefficients $c(r)$, easily computed in terms of the Mobius function of P. But these relations are not independent, considered as a module over $V(L)$. What are their dependencies? The question is not trivial even in the case of a valuation ring freely generated by an ordered set Q, as considered above, where the only relations are of the

form pq = p. These relations are not independent; a smaller generating set is obtained by taking only those where q covers p; but even these are not always independent. The question of a free resolution is worth investigating, if only because of the possible connection with the characteristic polynomial of the ordered set P , which, as has been observed, shares some of the properties of the Hilbert polynomial.

In terms of the canonical idempotents, a set of relations is given by the orthogonality relations. However, these are seldom independent; their dependencies depend on linear relations satisfied by the Mobius function.

6. Propositional Calculus

Classical propositional logic is equivalent to the study of the free valuation ring V(L) generated by a sequence of idempotents $x_1, x_2, \ldots$. The elements of this ring will be called Boolean polynomials. The axiomatic of propositional logic amount to an axiomatic for rings generated by idempotents. The constants u and z in the ring V(L) correspond to the propositional constants for truth and falsehood. The implication $p \supset q$ for idempotent p and q turns out to equal $u - p + p\,q$, and the deduction theorem states that if p,q are idempotents and $p \geq q$, then $p \supset q = u$. Verifying that a statement is a tautology amounts to showing that it equals u.

The present context leads to a re-examination of some of the concepts of classical logic, and we shall consider a few by way of example.

Suppose $f, g \in V(L)$ are not idempotents. Is it possible to give a meaning to "f implies g"? For monotonic (or even non-negative) f and g, the natural extension is $f \leq g$.

For a given sequence $f_1, \ldots, f_2$ of Boolean polynomials, not necessarily idempotent, one can define the information of the sequence to be the sublattice L' of L generated by the sequence (with or without taking complements). The complexity of the sequence can then be described by finding a

resolution of the set of generators of L', that is the join-irreducibles of L', in the sense of generators and relations. The relations describe, in an intuitive way, the various ways of proving a subset of the f_i from another subset, and the relations between relations give a meaning to the notion "two proofs are equivalent." The Koszul complex built on P or directly on the f_i also gives information on the complexity of Boolean functions. Thus, the study of complexity of Boolean polynomials can be reduced to techniques of commutative algebra.

The duality of classical logic is preserved in the valuation ring: interchanging joins and meets simply interchanges the roles of u and z, and u becomes the integral, whereas z is the unit.

The canonical idempotents of the free valuation ring can be explicitly computed. Any subset A of generators defines a join-irreducible

$$x_A = \prod_{x \in A} x ,$$

and gives for the canonical idempotents $e(A)$ the formula

$$e(A) = \sum_{B \neq \phi} \mu(A,B) x_B .$$

If A is the set $x_1, x_2, \ldots, x_n$, then this can be rewritten as

$$e(A) = x_1 x_2 \ldots x_n \, (u - x_{n+1}) \, (u - x_{n+2}) \ldots \, .$$

When is a Boolean polynomial a Boolean function? This question can be interpreted in two ways, according as one admits just meets and joins, or complementation as well. Every Boolean polynomial can be uniquely written as a linear combination of canonical idempotents; it is a Boolean function (including complementation) if **every coefficient** in such an expression is 0 or 1. It is a Boolean function, expressed by **joins** and meets only, if and only if the coefficients which equal 1 form a decreasing **set of P .**

Suppose now that a Boolean polynomial f is given in the form

$$(*) \qquad f = \sum_A c(A) x_A \, ,$$

where A ranges over a finite set of idempotents. What conditions must the numerical coefficients c(A) satisfy, in order that f be a Boolean function built up out of joins and meets (but not complements)? An elegant answer can be given using the notion of Euler characteristic of a simplicial complex, namely, a

family of sets closed under the operation of taking subsets. If Σ is a finite such simplicial complex, and A a member, or "face" of Σ, then the relative simplicial complex (Σ,A) consists of those faces of Σ which contain the face A; let $\chi(\Sigma,A)$ denote the Euler characteristic of the relative simplicial complex (Σ,A). The answer to our question is: a Boolean polynomial (*) is a lattice polynomial if and only if

$$c(A) + 1 = -\chi(\Sigma,A)$$

for some simplicial complex Σ of subsets of the set of **join-irreducibles**; A ranges through the faces of Σ, and $c(A) = 0$ otherwise.

Now consider the representation of a Boolean polynomial f in terms of joins, meets and complements $\bar{x} = u-x$. In terms of the canonical idempotents a necessary and sufficient condition is that

$$f = \sum_A c(A)e(A) + u \sum_A (|c(A)|-c(A))/2 ,$$

with $c(A) = \pm 1$. Again, this can be turned into a condition in terms of the **generators** x_i, but we shall not do so. The representation in terms of joins, meets and complements is not unique, as is well-known, and the theory of prime implicants

can be developed along present lines. So can the classical theory of Boolean equations.

A (propositional) theory is an ideal in the free valuation ring, generated by Boolean functions, that is, by members of L ; in this case the quotient is again a valuation ring, in general not free; again, the complexity of the axiom system can be investigated by generators and relations, or by finding a suitable basis for the axioms in the valuation ring. Finding the canonical idempotents explicitly amounts to solving the decision problem for the theory. We shall illustrate the simplicity of the use of the valuation ring by an example from combinatorics.

Recall that a geometry on a finite set S is a family of n-subsets called bases such that if $(a_1,\ldots,a_n)$ and $(b_1,\ldots,b_n)$ are bases, then for some i , both $(b_i,a_2,\ldots,a_n)$ and $(a_1,b_1,\ldots,\hat{b}_i,\ldots,b_n)$ are bases. A fundamental problem is that of deciding which statements about bases follows from this axiom.

Now one can restate the axiom as an identity in the valuation ring generated by idempotents $(a_1,\ldots,a_n)$ which take the value 1 if the a_i form a basis, and 0 otherwise. The basis axiom then turns into a linear identity, which, simplified by the inclusion-exclusion principle, is

$$(a_1,\ldots,a_n)(b_1,\ldots,b_n) = (b_1,a_2,\ldots,a_n)(a_1,b_2,\ldots,b_n)\vee$$

$$\vee(b_2,a_2,\ldots,a_n)(b_1,a_1,b_3,\ldots,b_n)\vee \ldots \vee(b_n,a_2,\ldots,a_n)$$

$$(b_1,b_2,\ldots,a_1) = \sum_{i=1}^{n} (b_i,a_2,\ldots a_n)\ (a_1,b_1,\ldots,\hat{b}_i,\ldots,b_n) -$$

$$- \sum_{i<j} (b_i,a_2,\ldots,a_n)(b_j,a_2,\ldots,a_n)(a_1,\ldots,\hat{b}_i,\ldots b_n)$$
$$(a_1,\ldots\hat{b}_j,\ldots b_n) + \ldots \quad .$$

This identity can be analyzed by Young's method of standard tableaux. In this way, a decision procedure can be found for combinatorial geometry, and the powerful techniques of representations of the symmetric group can be brought to bear on the problem.

7. Averaging Operators

An averaging operator on a valuation ring $V(L)$ is a linear operator A such that

(1) $A\,u = u$, $A\,z = z$.

(2) $A(fAg) = Af\,Ag$.

(3) If f is in the monotonic cone, so is Af.

Sometimes these operators go by the name of Reynolds operators. In probability, they are called conditional expectations. We shall investigate the structure of averaging operators. To this end, it is convenient to consider valuation rings with coefficients in an arbitrary commutative ring R with identity subject to conditions to be specified later, and written $V(L,R)$.

The range of an averaging operator A is a valuation ring of the form $V(L')$, where L' is a sublattice of L. For every $x \in L$ we have

$$(*) \quad A\,x = \sum_{e \in P} c(x,e)e \quad , \quad c(x,e) \in R \ ,$$

where P is the set of canonical idempotents of L' other than z, and the sum is finite. We shall characterize an averaging operator by properties of the coefficients $c(x,e)$.

Since $A\, e = e$ for $e \in P$ we infer that if $x \wedge e = z$, then $A\, x \wedge e = z$, or, as we shall say, the support of Ax contains the support of x. Furthermore, we infer

$$(1) \quad c(x \wedge e, e) = c(x, e) .$$

$$(2) \quad c(e, e) = 1 , \quad e \in P .$$

From the fact that A is linear, or $A(x \vee y) + A(xy) = Ax + Ay$ we add the property

$$(3) \quad c(x \wedge y, e) + c(x \vee y, e) = c(x, e) + c(y, e), \quad x, y \in L,$$

in other words, for fixed e the function c is a valuation on the lattice L. Finally, we have that $A\, z = z$, so

$$(4) \quad c(z, e) = 0$$

and $A\, u = u$, whence

$$c(u, e) = 1 .$$

When the lattice L' is finite, and when P is the set of canonical idempotents of L', conditions (1) - (4) on the coefficients c define a unique averaging operator.

When L' is not finite, the right side of (*) is not well-defined; to handle this case, we introduce a seemingly special class of averaging operators. For every finite sublattice π of L', let A_π be an averaging operator whose range is the valuation ring $V(\pi)$, considered as a subring of $V(L)$. If σ is a sublattice of π, we assume that

$$(**) \qquad A_\sigma A_\pi = A_\sigma ,$$

in other words, the operators A_π form a martingale as π runs through all finite sublattices of L'. Now set, for $x \in L$

$$(***) \qquad A\,x = \lim_{\pi} A_\pi\, x$$

where the limit on the right side means the following: for every $x \in L$ there is a sufficiently large sublattice π of L' such that $A_\pi x = A\,x$, and $A_\sigma x = x$ for all sublattices σ of : L' containing π. We shall say that such an averaging operator is obtained by finite approximation.

Condition (**) implies a condition on the coefficients c, derived as follows. Writing

$$A_\sigma x = \sum_{e \in P} c(x,e)e; \quad A_\pi x = \sum_{f \in Q} c(x,f)f,$$

where P and Q are the sets of canonical idempotents of σ and π, we find

$$A_\sigma A_\pi x = \sum_e \sum_f c(x,f)c(f,e)e =$$

$$= \sum_e c(x,e)e \quad ,$$

and hence

$$\sum_f c(x,f)c(f,e) = c(x,e) \ .$$

Since σ is a sublattice of π, each canonical idempotent of π is contained in a unique canonical idempotent of σ, and the preceding sum simplifies to

$$\sum_{f \leq e} c(x,f)c(f,e) = c(x,e) \ .$$

Replacing x by xf_o for a fixed canonical idempotent f_o of σ, this gives

$$\sum_{f \leq e} c(xf_o,f)c(f,e) = c(xf_o,e).$$

But $c(xf_o,f) = 0$ unless $f = f_o$, and this sum simplifies to

$$c(xf_o,f_o)c(f_o,e) = c(xf_o,e) \ ,$$

which in turn can be restated in more elegant form as

$$(5) \qquad c(x,ef)c(f,e) = c(xf,e) \ .$$

This is the condition for a cocycle in homology. Finally, consider the limit condition (***). If A x is given by the right side of (*), and if f is any canonical idempotent of L', then

$$A(xf) = fAx = \sum_e c(x,e)ef = \sum_e c(x,ef)\ ef$$

and thus we have that $c(x,e) = c(x,f)$ for any $f \leq e$; in other words, we require:(6) for every $x \in L$ and every canonical idempotent e of L' such that

$$A\ x = \sum_e c(x,e)e \qquad \text{with } c(x,e) \neq 0$$

one has $c(x,e) = c(x,f)$ for every canonical idempotent f of L' contained in e.

This last condition puts a strong restriction on the sublattice L'. For suppose $f \leq x$; then $c(x,f) = 1$ by (1)

and hence $c(x,e) = 1$; thus, if $c(x,e) \neq 1$, then no $f \leq e$ is contained in x. Again, if $f\,x = z$, then $c(x,f) = 0$ by (4); thus, if $c(x,e) \neq 0$, then any canonical idempotent f such that f meets e also meets x, that is, $f \wedge x \neq z$. We conclude that there is a maximal $f \in L'$ contained in x, call it $\forall_x$, and a minimal $e \in L'$ containing x, call it $\exists_x$. The (non-linear !) operators on L

$$x \to \forall_x, \qquad x \to \exists_x$$

are quantifiers (universal and existential) in the sense of Halmos, and the sublattice L' must be relatively complete in L.

We thus find that on the right side of (*) one term always is $c(x, \forall x)\,\forall x$, with $c(x, \forall x) = 1$; of the remaining terms, $c(x,e) \neq 0$ only if $e \leq \exists x$. A function $c(x,e)$ defined for $x \in L$ and for all non-zero canonical idempotents $e \in L'$, satisfying condition (1) - (6) is called a fibering of L' by L. We have shown that every averaging operator obtained by finite approximation determines a fibering; conversely, every fibering determines an averaging operator, assuming that L' is relatively complete in L.

Any further statement about the existence of a fibering for a given pair L and L' depends on more delicate measure-theoretic questions. If L and L' are Boolean algebras, the existence of a "universal" fibering can be e established, but this requires a previous classification of subalgebras of a Boolean algebra (Maharam), and cannot be undertaken here. The case of interest in predicate logic is worked out below.

8. Quantifiers.

Every relatively complete Boolean subalgebra L' of a Boolean algebra L defines two quantifiers, the existential quantifier

$$\exists x = \inf \{y: y \geq x , y \in L'\}$$

and the universal quantifier

$$\forall x = \sup \{y: y \leq x, y \in L'\}$$

We have seen that every non-trivial averaging operator on the valuation ring $V(L,R)$ defines two such quantifiers. Is it possible to reverse the process? In other words, given L and L', we wish to construct an averaging operator:

$$A x = \sum_e c(x,e)e$$

where e ranges over the canonical idempotents of L', with the following properties:

(a) for $x \in L$, the support of x, that is, $\Sigma\{e: c(x,e)\neq 0\}$, is the idempotent $\exists x$

(b) for $x \in L$, the idempotent $\forall x$ coincides with $\Sigma\{e: c(x,e) = 1\}$.

We shall solve this problem in a special case, which is strong enough to include the quantifiers of predicate logic. It will be simpler to describe the construction in set-theoretic language. Thus, we are given two sets S and T, and on S a Boolean algebra L' of subsets freely generated by elements $y_1, w_1, y_2, w_2, y_3, w_3, \ldots$ such that $y_i \wedge w_i = z$. We identify L' with the Boolean algebra of S-cylinder sets in the product $S \times T$. Now take a Boolean algebra of T-cylinder sets, freely generated by $z_1, z_2, \ldots$.

Set

$$x_i = y_i \vee (z_i \wedge w_i) = y_i + (z_i \wedge w_i) =$$

$$= y_i + t_i .$$

Now let L be the Boolean algebra of subsets of $S \times T$ generated by the x_i, y_i, and w_i. The quantifiers from L to L' can be explicitly described as follows:

(1) If x belongs to the Boolean subalgebra generated by the y_i and w_i, set $\forall x = x$ and $\exists x = x$;

(2) Set $\exists(x \vee y) = \exists x \vee \exists y$

and $\forall(x \wedge y) = \forall x \wedge \forall y$ for all $x,y \in L$;

(3) Set

$$\exists\, x_i = y_i + w_i,\ \exists\, y_i = y_i,$$

$$\exists\, (x_{i_1} x_{i_2} \ldots x_{i_n}) = (y_{i_1} + w_{i_1}) \ldots (y_{i_2} + w_{i_n}),$$

$$\forall x_i = y_i,\ \forall y_i = y_i,$$

$$\forall(x_{i_1} \vee \ldots \vee x_{i_n}) = y_{i_1} \vee \ldots \vee y_{i_n},$$

$$\exists\, \overline{x}_i = \overline{y}_i,$$

$$\forall\, \overline{x}_i = \overline{y_i + w_i}.$$

In view of the known properties of quantifiers (Halmos) this gives $\exists\, x$ for all x in L. We can now construct the averaging operator of L onto L', by choosing a suitable universal ring of coefficients.

Set

$$A\, x_i = y_i + c(x_i, w_i) w_i$$

where the coefficients c belong to an as yet unspecified ring. Define $A(x_{i_1} x_{i_2} \ldots x_{i_n})$ by induction, writing $A(x_1 \ldots x_n)$ for simplicity. Having defined $A(x_1 \ldots x_{n-1})$ we have

$$A(x_1 \ldots x_n) = A(x_1 \ldots x_{n-1}(y_n + t_n)) =$$

$$= y_n A(x_1 \ldots x_{n-1}) + A(x_1 \ldots x_{n-1} t_n) \quad ,$$

so we set

$$A(x_1 \ldots x_{n-1} t_n) = c(x_1 \ldots x_{n-1} x_n, w_1 \ldots w_n) w_1 \ldots w_n \ .$$

Let R be the commutative ring with identity generated by these values of c, together with conditions (1) - (6) of the preceding Section. Condition (6) is made specific by stating that

$$c(x_1 \ldots x_n , w_1 \ldots w_n f) = c(x_1 \ldots x_n, w_1 \ldots w_n)$$

for any idempotent f in the range of A. These conditions determine the values of c uniquely, and in fact make it a fibering of L by L'.

To simplify the computation of A x , write $\bar{x}_i = p_i + q_i$, where $p_i = \bar{y}_i - w_i + t_i$ is a cylinder set, and $q_i = w_i - t_i$. Then

$$A\,\bar{x}_i = p_i + c(\bar{x}_i, w_i)w_i \ ,$$

as is easily checked.

As an example of computation with the averaging operator A , let us verify that

$$A(x_1x_2) + A(x_1\bar{x}_2) = A(x_1) \ .$$

Now,

$$A(x_1\bar{x}_2) = y_1p_2 + c(x_1,w_1)p_2w_1 + c(\bar{x}_2,w_2)y_1w_2 +$$

$$+ c(x_1\bar{x}_2,w_1w_2)w_1w_2 \ ,$$

and

$$A(x_1x_2) = y_1y_2 + c(x,w_1)y_2w_1 + c(x_2,w_2)y_1w_2 +$$

$$+ c(x_1x_2,w_1w_2)w_1w_2 \ .$$

Adding,

$$A(x_1\bar{x}_2) + A(x_1x_2) = y_1(y_2+p_2) + c(x_1,w_1)(y_2+p_2)w_1 +$$

$$+ y_1w_2 + c(x_1,w_1w_2)w_1w_2 \quad ,$$

where we have used the additivity of e . But $y_2+p_2+w_2 = u$, and furthermore $c(x_1,w_1w_2) = c(x_1,w_1)$ by condition (6) in the definition of a fibering. Simplifying, the right side is seen to equal $y_1 + c(x_1,w_1)w_1$, as desired.

One retrieves the quantifiers from the averaging operator by the following algorithm:

(1) Write A x as the sum of multiples of disjoint idempotents,where the multiples are values of c;

(2) To get $\exists x$, replace by 1 all coefficients which are non-zero, and take the sum of the resulting idempotents;

(3) To get $\forall x$, replace by 0 all coefficients which do not equal 1, and take the sum of the remaining idempotents.

We shall informally illustrate the connection with the decision problem for the predicate calculus. Let $x_1,x_2,\ldots$ be **predicates in two individual variables:** $F_1(x,y),F_2(x,y),\ldots,$ and let the y_i and w_i be predicates in one individual variable, such as G(y). In order to analyze the validity or satisfiability of a formula in the predicate calculus quantified in the single variable x, and not necessarily in **prenex** normal form, reason as follows. Every predicate $F_i(x,y)$ can be decomposed into the disjoint sum of three predicates: $F_{i0}(x,y)$, corresponding to the set of x for which no y

exists for which $F_i(x,y)$ is true, $F_{i1}(x,y)$, corresponding to the set of x for which there exists some y such that $F_i(x,y)$ is true, and $F_{i2}(x,y)$, corresponding to the set of x for which $F_i(x,y)$ is true irrespective of y. Clearly $F_i(x,y) = F_{i0}(x,y) + F_{i1}(x,y) + F_{i2}(x,y)$. Now $F_{i1}(x,y)$ corresponds to t_i, and $F_{i2}(x,y)$ corresponds to y_i. We assign predicates $G_i(x)$ and $H_i(x) = F_{i2}(x,y)$ to t_i and y_i, so that we have

$$A\ F\ (x,y) = c(F, G_i)\ G_i\ (x) + H_i(x).$$

By this technique, and its extension to several variables, every formula of the predicate calculus is seen to be equivalent to a formula in a valuation ring endowed with commuting averaging operators. In other words, problems of first-order logic, such as the decision problem, can be shown to be equivalent to algebraic problems for valuation rings with averaging operators.

The case of several commuting quantifiers is technically more complex, but the idea is the same: one considers a Boolean algebra generated by disjoint parellelepipeds of a very special kind in an n-cube; the expression of quantifiers by averaging operator is akin to an Herband expansion,

but the linear structure of the valuation ring allows considerable simplifications. We hope to take up these matters elsewhere.

9. Logic and Probability.

In the present context, the algebra of real random variables on a probability space can be viewed as a close analog of a valuation ring, the only difference being that infinite sums of idempotents are allowed. In fact, the passage from predicate logic - i.e., a valuation ring with a set of commuting averaging operators - to probability is achieved by the following steps:

(1) Assign a probability measure μ to the canonical idempotents;

(2) Define an L-space norm on the valuation ring by setting

$$\left|\sum_{e} a(e)e\right| = \sum |a(e)|\mu(e) ;$$

(3) Complete the resulting normed linear space, thereby obtaining an L-space, representable as the space of all integrable functions.

(4) Represent every averaging operator as a conditional expectation operator (in the sense of probability.) Once the restriction that every element of the range be finite-valued is removed, one can show that a conditional expectation operator always exists.

The resulting structure is richer than that of a probability space, because it is endowed in addition with a monotonic **cone of non-decreasing functions.**

By this process certain questions of predicate logic can be seen to be analogous to questions in probability, and new questions in probability are suggested by the analogy - . For example, does the decision problem for averaging operators make sense? Problems of model theory, which can be rephrased and simplified in the context of valuation rings, have analogs for probability spaces. The intriguing possibility arises of handling the decision problem of predicate logic by the techniques of probability.

10. Acknowledgements.

It was L. Solomon who first introduced what we have called canonical idempotents, but his construction remained obscure for several years; he called it the Möbius algebra of an ordered set. A few years later, the present writer introduced the notion of valuation ring of a distributive lattice, quite unaware that it might be related (at least in the finite case) with Solomon's Möbius algebra. It was R. Davis who proved the isomorphism of the two structures; successively, C. Greene made the calculations with canonical idempotents obvious, and used them to systematically derive properties of the Möbius function. It must be pointed out however that the valuation ring is more general than the Möbius algebra, since it does not require any finiteness assumptions.

The valuation ring was later studied by Geissinger in a series of papers; to him is due the existence of an augmentation, the integral, and the elegant duality, which extends to all valuation rings the duality of Boolean algebras.

The representation of distributive lattices in terms of totally order disconnected spaces was recently discovered by Priestley; we have given here the valuation-ring version, which is slightly simpler and tells more. The notion of

quantifier on a Boolean algebra was introduced by Everett and Ulam and extensively studied by Halmos and others, but the precise connection with averaging operators seems to be new, though the analogy had been noted by Wright. Averaging operators on spaces of continuous functions have an extensive literature (Brainerd, Kelley, Wright); in the present context they have not been previously considered.

It seems astonishing that the use of the valuation ring as a technique of proof and as a decision procedure should not have been realized and exploited, even for the propositional calculus. We hope the present paper will contribute to correct this neglect.

The conjectured connection between the homology of an ordered set and the Koszul complex also seems to be new, and we hope its potential usefulness in studies of computational complexity will also be developed.

Bibliography

1. Adam, A., Truth functions, Akademiai Kiado, Budapest, 1968.
2. Birkhoff, G., Lattice Theory, 3rd ed., A.M.S., Providence, 1968.
3. Brainerd, B., On the structure of averaging operators, Journ. Math. Appl., 5 (1962), 347-377.
4. Cartan, H., and Eilenberg, S., Homological Algebra, Princeton University Press, Princeton, 1956.
5. Church, A., Introduction to Mathematical Logic, Princeton University Press, Princeton, 1956.
6. Davis, R., Order algebras, Bulletin A.M.S., 76 (1970), 83-87.
7. Grätzer, G., Lattice Theory, Freeman, San Francisco, 1971.
8. Geissinger, L., Valuations on distributive lattices I, II and III, to appear in Arkiv der Mathematik.
9. Greene, C., On the Möbius algebra of a partially ordered set, Advances in Math., 10 (1972), 177-187.
10. Halmos, P., Algebraic Logic, Chelsea, New York, 1962.
11. Hammer, P. and Rudeanu, S., Boolean Methods in Operations Research, Springer, New York, 1968.
12. Keimel, K., Algèbres commutatives engendrées par leur éléments idempotents, Can. J. Math., XXII (1970), 1071-1078.

13. Kelley, J. B., Averaging operators on $C_\infty(X)$, Illinois J. Math., 2 (1958), 214-223.

14. Priestley, H. A., Representation of distributive lattices, Bull. London Math. Soc. 2 (1970), 186-190.

15. Rasiowa, H. and Sikorski, R., The mathematics of metamathematics, Warsaw, 1963.

16. Rota, G.-C., On the representation of averaging operators, Rend. Padova, 30 (1960), 52-64.

17. Rota, G.-C., On the foundations of combinatorial theory I: Theory of Möbius functions, Zeit. für Wahr. 2(1964), 340-368.

18. Rota, G.-C., Reynolds operators, Proceedings of the Symposia in Applied Mathematics, Vol. XVI (1964), pages 70-83.

19. Rota, G.-C., On the combinatorics of the Euler characteristic, Studies in Pure Math., edited by L. Mirsky, Academic Press, London, 1971, pp. 221-233.

20. Solomon, L., The Burnside algebra of a finite group, J. Comb. Th. 2 (1967), 603-615.

21. Sweedler, M., Hopf Algebras, Benjamin, 1969.

22. Whitney, H., Characteristic functions and the algebra of logic, Annals of Math. 34 (1933), 404-414.

23. Wright, F. B., Generalized means, Trans. A.M.S., 98 (1961), 187-203.

24. Wright, F. B., Convergence of quantifiers and martingales, Illinois J. Math., 6(1962), 296-307.

December 7, 1973