Spaces as Distributive Lattices

Thierry Coquand

Trieste, August 2008

Axiom of Choice

$\{0,1\}^{\mathbb{N}} \rightarrow [0,1]$

$(b_n) \longmapsto \Sigma b_n/2^n$

This is a surjective map, but it has *no* continuous section

Unfortunately, the fact that it is surjective is not constructively valid

Axiom of Choice

$\{-1,0,1\}^{\mathbb{N}} \to [-1,1]$

$(b_n) \longmapsto \Sigma b_n/2^n$

This is a surjective map, but it has *no* continuous section

This time, the fact that it is onto is constructively valid

Completeness Theorem

"If something can be stated simply, it has a simple proof"

$$\forall z.inv(1 - uz) \wedge \forall z.inv(1 - vz) \quad \rightarrow \quad \forall z.inv(1 - (u + v)z)$$

Topology in algebra

There are a lot of examples of use of *topology* in algebra

Zariski spectrum of a ring, the space of valuations, the notion of scheme, ...

Problem: the existence of the elements of these spaces is usually proved using Zorn's Lemma. How can we represent them computationally?

Topology in algebra

In constructive mathematics, it is possible to keep these rich topological intuitions by defining a (formal) space to be a *distributive lattice*

The elements of this lattice have to be thought of as basic open of the space. We are going to present two examples: the Zariski spectrum of a ring and the space of valuations of a field.

Distributive lattice

A distributive lattice can be thought of as a logical approximation of rings: we replace $+$ by $\vee$ and $\times$ by $\wedge$

We have a duality between $\vee$ and $\wedge$ which is invisible in the theory of rings

We think of the elements U of the lattice as basic open of a topological space

Points

What should be a point? We represent it as a predicate $\alpha(U)$ meaning that the point is in U. We should have

$$\alpha(1), \qquad \neg\alpha(0)$$

$$\alpha(U_1 \vee U_2) \rightarrow \alpha(U_1) \vee \alpha(U_2)$$

$$\alpha(U_1 \wedge U_2) \leftrightarrow \alpha(U_1) \vee \alpha(U_2)$$

Classically we can think of α as a lattice map $L \rightarrow \mathbf{2}$ where $\mathbf{2}$ is the two element lattice

A point is similar to the complement of a prime ideal

We write $Sp(L)$ the space of points of L

Points

The topology is in general non separated and we have an order on points

$\alpha_1 \leqslant \alpha_2$ iff $\alpha_1(U) \leqslant \alpha_2(U)$ for all U

The *Krull dimension* n of a lattice is the length of maximal proper chain $\alpha_0 < \cdots < \alpha_n$

Morphisms

Any lattice map $\psi : L_1 \rightarrow L_2$ defines (by composition) a continuous map $\psi^* : Sp(L_2) \rightarrow Sp(L_1)$

Proposition: *The map ψ^* is surjective iff the map ψ is injective*

This can easily proved using Zorn's Lemma. We understand this result as the fact that we can express the surjectivity of a map in an algebraic way

An example of this situation will be provided by the *center* map in algebraic geometry

Zariski spectrum

Fundamental object in abstract algebra, usually defined as a set of prime ideals of a ring R with the basic open

$$D(a) = \{\mathfrak{p} \mid a \notin \mathfrak{p}\}$$

This is a *spectral space*

The compact open form a distributive lattice. They are exactly the finite union $D(a_1) \vee \cdots \vee D(a_n)$

Zariski spectrum

However, even if the ring R is given concretely (discrete) it may be difficult to show effectively the existence of *one* prime ideal

For instance if N is a very large integer, to give a prime ideal of $\mathbb{Z}/N\mathbb{Z}$ is to give a prime factor of N

Often, what matters is not *one* particular prime ideals, but the collection of *all* prime ideals.

Zariski spectrum

Zariski spectrum is best seen as a point-free space (cf. Menger, 1940, de Bruijn 1967)

A. Joyal (1972) definition of the Zariski spectrum

We consider the distributive lattice defined by the generators $D(a),\ a \in R$ (seen as formal symbols) and the relations

$$D(0) = 0 \qquad D(1) = 1 \qquad D(ab) = D(a) \wedge D(b) \qquad D(a+b) \leqslant D(a) \vee D(b)$$

Zariski spectrum

In general we define a *support* of R to be a distributive lattice L with a map $D : R \to L$ satisfying the relations

$$D(0) = 0 \qquad D(1) = 1 \qquad D(ab) = D(a) \wedge D(b) \qquad D(a+b) \leqslant D(a) \vee D(b)$$

Intuitively $D(f)$ is the "open set" over which the function f is $\neq 0$

We can distinguish between the properties of an arbitrary support and the properties of the *universal* support, the Zariski lattice $\mathsf{Zar}(R)$

Zariski spectrum

For an arbitrary support we have $D(a^2) = D(a)$ and $D(a^n) = D(a)$ if $n \geqslant 1$

We have $D(a, b) = D(a + b, ab)$

If $D(ab) = 0$ then $D(a + b) = D(a, b)$

For the Zariski lattice, all elements can be written on the form

$$D(a_1, \ldots, a_n) = D(a_1) \vee \cdots \vee D(a_n)$$

$D(a) \leqslant D(b_1, \ldots, b_m)$ if a is in the radical of the ideal generated by $b_1, \ldots, b_m$

Nullstellensatz

Theorem: $D(a_1) \wedge \cdots \wedge D(a_n) \leqslant D(b_1, \ldots, b_m)$ *holds iff the product* $a_1 \ldots a_n$ *is in the radical of the ideal generated by* $b_1, \ldots, b_m$

This is also known as the *formal* version of the Nullstellensatz. This can be seen as a *cut-elimination* result: any proof can be reduced to a direct proof

If R polynomial ring over $\mathbb{Q}$, $D(p)$ can be thought of as the complement of the set of zeros of p (in some algebraic closure).

Nullstellensatz

The proof of the Nullstellensatz is an explicit construction of the Zariski spectrum (by opposition to a purely abstract universal characterisation)

We consider the (distributive) lattice of *radicals* of finitely generated ideal and we define $D(a)$ to be $\sqrt{< a >}$

Notice that in the general the lattice of ideals of a ring is *not* distributive

Zariski spectrum

This definition is purely algebraic: we manipulate only rings and lattices, $R \longmapsto$ Zar(R) is a functorial construction

Even if R is discrete (we have an algorithm to decide the equality in R), the lattice Zar(R) does not need to be discrete

Counter-example with Kripke model: $\mathbb{Z} \to \mathbb{Z}[1/2]$ is injective but Zar$(\mathbb{Z}) \to$ Zar$(\mathbb{Z}[1/2])$ is not

Zariski spectrum

Any element of the Zariski lattice is of the form $D(a_1, \ldots, a_n)$. We have seen that $D(a, b) = D(a + b)$ if $D(ab) = 0$

In general we cannot write $D(a_1, \ldots, a_n)$ as $D(a)$ for *one* element a

We can ask: what is the least number m such that *any* element of Zar(R) can be written on the form $D(a_1, \ldots, a_m)$. An answer is given by the following version of *Kronecker's Theorem*: this holds if Kdim $R < m$

Sheaf over lattices

If L is a distributive lattice, a *presheaf of rings* over L is a family $\mathcal{F}(U)$ of rings for each element U of L with a map $\mathcal{F}(U) \to \mathcal{F}(V),\ x \longmapsto x|V$ whenever $V \leqslant U$

We require furthermore $x|U = x$ for $x \in \mathcal{F}(U)$ and $(x|V)|W = x|W$ whenever $W \leqslant V \leqslant U$

Sheaf over lattices

We say that $\mathcal{F}$ is a *sheaf* iff

(1) whenever $U = U_1 \vee U_2$ and $x_i \in \mathcal{F}(U_i)$ and $x_1|U_1 \wedge U_2 = x_2|U_1 \wedge U_2$ then there exists one and only one x in $\mathcal{F}(U)$ such that $x|U_i = x_i$

(2) $\mathcal{F}(0)$ is the trivial ring 0

If $\mathcal{F}$ is a sheaf over a lattice L and U is an element of L then $\mathcal{F}$ defines a sheaf by restriction on the lattice $\downarrow U$

Structure sheaf

To simplify we assume that R is an integral domain

Lemma: *If* $D(b) \leqslant D(a_1, \dots, a_n)$ *in* $\mathsf{Zar}(R)$ *then we have*

$$R[1/a_1] \cap \cdots \cap R[1/a_n] \subseteq R[1/b]$$

Structure sheaf

Any element of Zar(R) can be written $D(b_1, \ldots, b_m) = D(b_1) \vee \cdots \vee D(b_m)$

We define the *structure sheaf* $\mathcal{O}$ on Zar(R) by

$$\mathcal{O}(D(b_1, \ldots, b_m)) = R[1/b_1] \cap \cdots \cap R[1/b_m]$$

This is well-defined by the previous Lemma

An example of a local-global principle

Classically the point of the space $\mathsf{Zar}(R)$ are the prime ideals of R and the fiber of the sheaf $\mathcal{O}$ at a point $\mathfrak{p}$ is the localisation $R_{\mathfrak{p}}$

One intuition is that we have a continuous family of local rings $R_{\mathfrak{p}}$, and any element of R defines a global section of this family

We can see $R[1/a]$ for $\mathfrak{p}$ in $D(a)$ as an "approximation" of $R_{\mathfrak{p}}$ and indeed $R_{\mathfrak{p}}$ can be defined as the inductive limit of all $R[1/a]$ for $\mathfrak{p}$ in $D(a)$

We have $\Gamma(D(a), \mathcal{O}) = R[1/a]$

Local-global principle

Let us consider a linear system $MX = A$ with M in $R^{n\times m}$ and X in $R^{m\times 1}$ and A in $R^{n\times 1}$

A local-global principle is that if in each $R_{\mathfrak{p}}$ the linear system $MX = A$ has a solution then it has a global solution

If $MX = A$ has a solution in $R_{\mathfrak{p}}$ then we find a such that $\mathfrak{p}$ in $D(a)$ and $MX = A$ has a solution in $R[1/a]$

By compactness we find a *finite* sequence $a_1, \dots, a_n$ such that $1 = D(a_1, \dots, a_n)$ and $MX = A$ has a solution in each $R[1/a_i]$

Local-global principle

The constructive expression of this local-global principle is thus

Proposition: *If we have $a_1, \ldots, a_n$ such that $1 = D(a_1, \ldots, a_n)$ and $MX = A$ has a solution in each $R[1/a_i]$ then the system $MX = A$ has a global solution in R*

The proof is simple: we have X_i, k_i such that $MX_i = a_i^{k_i} A$

We have $\Sigma u_i s_i^{k_i} = 1$ and so $X = \Sigma u_i X_i$ satisfies $MX = A$

Exactly like "partition of unity" in analysis

Local-global principle

Example: if M is in $R^{k\times l}$ matrix and $1 = \Delta_k(M)$ then $MX = A$

Indeed for each $k \times k$ minor δ of M, we have a solution of $MX = A$ in $R[1/\delta]$

Another local-global principal

If M is an idempotent matrix over a local ring we know that M is similar to a canonical projection matrix

Hence if M is an idempotent matrix over *any* ring R the matrix M is locally over any prime $\mathfrak{p}$ of R similar to a canonical projection matrix

Hence by compactness we should be able to find $a_1, \ldots, a_n$ such that $1 = D(a_1, \ldots, a_n)$ and M is similar to a canonical projection matrix over each $R[1/a_i]$

By completeness we expect to be able to find such a sequence $a_1, \ldots, a_n$ from M

Another local-global principle

Let M be in $R^{l \times l}$ and $C_1, \ldots, C_l$ be the vector column of M

Write $E_1, \ldots, E_l$ is the canonical basis of $R^{l \times 1}$

Define $C_i^0 = C_i$ and $C_i^1 = E_i - C_i$

The following argument gives a sequence: write $1 = det\ I_l = det(M + I_l - M)$ as a sum of 2^l elements that are the determinants d_σ of the matrix $C_1^{b_1}, \ldots, C_l^{b_l}$ where $\sigma = b_1, \ldots, b_l$ is a sequence of $0, 1$

Clearly over $R[1/d_\sigma]$ we have a basis of $Im\ M$ formed by the elements C_i for i such that $b_i = 0$ and a basis of $Im\ (I_l - M)$ formed by the elements $E_i - C_i$ for i such that $b_i = 1$

Finite local-global principle

A finitely presented module is given by a matrix M over a ring R

The n-*Fitting ideal* I_n is the ideal generated by the $n \times n$ minor of M

It can be shown that the module defined by M is *projective* iff $I_n^2 = I_n$ iff I_n is generated by an idempotent

Proposition: *If we have* $a_1, \ldots, a_m$ *such that* $1 = D(a_1, \ldots, a_m)$ *and* M *defines a projective module over* $R[1/a_i]$ *for all* i *then* M *defines a projective module over* R

Summary

We can describe topological space used in commutative algebra as *distributive lattices*

Distributive lattices can be described equationally

We can also define the notion of *sheaf* over a distributive lattice and express local-global principles

Space of valuation

Let L be a field, and R a subring of L

Another spectral space important in commutative algebra is the space Val(L, R) of *valuation rings* of L containing R

Such a ring is a subring $V \subseteq L$ containing R and such that if s in L and $s \neq 0$ then s is in V *or* $1/s$ is in V

We have always the solution $V = L$

Space of valuation

We define the lattice $\mathsf{Val}(L,R)$ as the universal solution of the problem $V_R : L \to \mathsf{Val}(L,R)$ with the conditions

$$V_R(r) = 1 \qquad (r \in R)$$

$$V_R(s_1) \wedge V_R(s_2) \leqslant V_R(s_1 s_2) \wedge V_R(s_1 + s_2)$$

$$1 = V_R(s) \vee V_R(1/s) \qquad (s \neq 0)$$

Space of valuation

In general we cannot simplify $V_R(s_1) \wedge \cdots \wedge V_R(s_l)$, but we have

$V_R(s) \wedge V_R(1/s) = V_R(s + s^{-1})$

$V_R((x+y)^{-1}) \leqslant V_R(1/x) \vee V_R(1/y)$

$1 = V_R(x^{-1}) \vee V_R((1-x)^{-1})$

Space of valuation

Theorem: $V_R(t_1) \wedge \cdots \wedge V_R(t_n) \leqslant V_R(s_1) \vee \cdots \vee V_R(s_m)$ *holds iff we have an equality of the form* $1 = \Sigma 1/s_i P_i(t_j, 1/s_i)$

This is a *cut-elimination* Theorem, proved by *algebraic* elimination of variables

Space of valuation

The main Lemma for this result is extracted from the classical proof of existence of valuation rings

Main Lemma: *If I is an ideal and we have two relations*

$$x^k = b_1 x^{k-1} + \cdots + b_0, \qquad 1 = a_l x^l + \cdots + a_0$$

with $a_0, \ldots, a_l$ in I then 1 is in I

This proved by induction on $k + l$

We can then apply this to the ideal $<1/s_1, \ldots, 1/s_k>$ of $R[1/s_1, \ldots, 1/s_k]$

Space of valuation

Special case: $1 = V_R(s/t_1) \vee \cdots \vee V_R(s/t_n)$ iff s is *integral* over the ideal I generated by $t_1, \ldots, t_n$ in $R[t_1, \ldots, t_n, s]$. This means that we have an equality

$$s^l = a_1 s^{l-1} + \cdots + a_l$$

where a_k is in I^k

Special case: $1 = V_R(s)$ iff $1/s$ is invertible in $R[1/s]$ iff s is integral over R

We get a constructive reading of the fact that the intersection of valuation rings containing R is the integral closure of R

Application: Dedekind Prague's Theorem

Theorem: *If* $(\Sigma a_i X^i)(\Sigma b_j X^j) = \Sigma c_k X^k$ *then each product* $a_i b_j$ *is* integral *over the coefficients* c_k

This generalises a famous result of Gauss: if all a_i, b_j are *rationals* and all c_k are *integers* then all products $a_i b_j$ are *integers*

This "may be considered as one of the most basic result in commutative algebra of the XIXth century ... It ended up as one exercise in Bourbaki, but here it is proved in a non constructive way" (Olaf Neumann)

This appears as an exercise in Bourbaki, Algebra, Chapter 7 (Diviseurs)

Application: Dedekind Prague's Theorem

We get a proof-theoretic reading of the non constructive argument. We take $L = \mathbb{Q}(a_0, \ldots, a_n, b_0, \ldots, b_m),\ R = \mathbb{Q}$ and we prove

$$1 = V(a_i b_j / c_0) \vee \cdots \vee V(a_i b_j / c_m)$$

This corresponds to the non constructive argument: prove this for an *arbitrary* valuation

Application: Dedekind Prague's Theorem

For $n = m = 2$ a proof certificate of $1 = V(a_0b_1/c_0) \vee \cdots \vee V(a_0b_1/c_4)$ is

$$(a_0b_1)^6 = p_1(a_0b_1)^5 + p_2(a_0b_1)^4 + p_3(a_0b_1)^3 + p_4(a_0b_1)^2 + p_5(a_0b_1) + p_6$$

where

$$p_1 = 3c_1, \quad p_2 = -3c_1^2 - 2c_0c_2, \quad p_3 = c_1^3 + 4c_0c_1c_2$$
$$p_4 = -c_0^2c_1c_3 - 2c_0c_1^2c_2 - c_0^2c_2^2 + 4c_0^3c_4$$
$$p_5 = c_0^2c_1^2c_3 + c_0^2c_1c_2^2 - 4c_0^3c_1c_4$$
$$p_6 = -c_0^3c_1c_2c_3 + c_0^4c_3^2 + c_0^3c_1^2c_4$$

Application: Dedekind Prague's Theorem

Constructively $L \to \mathsf{Val}_R(L)$ is seen as a (clever) system of notations which records polynomial identities

Classically $\mathsf{Val}_R(L)$ is seen as a set of points

Zariski spectrum and space of valuations

Given any domain R of field of fractions L we have a lattice map

ψ : $\mathsf{Zar}(R) \to \mathsf{Val}(L, R)$, $\qquad D(a) \longmapsto V(1/a)$ $(a \neq 0)$

This is the *center map*. It is *always* injective.

The (constructive) proof of this fact requires cut-elimination

Intuitively: the function f is $\neq 0$ iff $1/f$ is finite

Center map

The terminology comes from the study of points for algebraic curves

We look at the local ring at a point of the curve

If the point is not singular its local ring is a discrete valuation ring

If the point is singular there is a finite number of discrete valuation rings of center the maximal ideal defined by this point. In this case, it is possible to show directly the *existence* of these valuations.