Infinite objects in constructive mathematics

Thierry Coquand

Mar. 20, 2005

Krull dimension

Let L be a distributive lattice. The theory of prime filters of L is the theory $T(X)$

$X(a \vee b) \to [X(a) \vee X(b)]$

$X(a \wedge b) \leftrightarrow [X(a) \wedge X(b)]$

$X(1) \qquad \neg X(0)$

One can show: $X(a_1) \vee \cdots \vee X(a_k)$ is provable iff $a_1 \vee \cdots \vee a_k = 1$

Quite simple Nullstellensatz

Krull dimension

It is convenient to have the topological intuition from Stone duality: the models form a space Spec(L) where the basic open are precisely the elements of a of L

$X \in D(a) \leftrightarrow X(a)$

In this case, the basic open $D(a)$ are precisely the compact open subsets of this space Spec(L)

Krull dimension

One considers now the theory T_C of *chain* of prime filters $T(X_0, \ldots, X_n)$ saying that each X_i is a prime filter and that we have $X_{i+1} \subseteq X_i$

$$X_{i+1}(a) \to X_i(a)$$

To say that L is of Krull dimension $< n$ is to say that we cannot have a proper chain; this means that for any $a_1, \ldots, a_n$ we have

$$T_C \vdash X_0(a_1) \wedge \cdots \wedge X_{n-1}(a_n) \ \to \ X_1(a_1) \vee \cdots \vee X_n(a_n)$$

Some results on constructive theory of Krull dimension for rings and lattices were obtained by Joyal and Espanol (1981)

Krull dimension

By looking systematically for a notion of Nullstellensatz identities for the theory T_C one obtains the following new characterisation

Theorem L is of Krull dimension $< n$ iff for any $a_1, \ldots, a_n$ there exists $x_1, \ldots, x_n$ such that

$$a_1 \wedge x_1 = 0,\ a_2 \wedge x_2 \leq a_1 \vee x_1,\ \ \ldots,\ a_n \wedge x_n \leq a_{n-1} \vee x_{n-1},\ 1 = a_n \vee x_n$$

For instance L is of Krull dimension 0 iff any element has a complement iff L is a Boolean algebra

Krull dimension

One gets a nicer characterisation by working in the cHa of ideals

Dimension 0: $a \vee \neg a = 1$ (classical logic)

Dimension 1: $a \vee (a \to (b \vee \neg b)) = 1$

Dimension 2: $a \vee (a \to (b \vee (b \to (c \vee \neg c)))) = 1$

Intermediate logic?? Are finitely generated algebras finite?

Krull dimension

A finite distributive lattice L is the lattice of downward closed set of a finite poset, which can be identified with Spec(L)

The Krull dimension is exactly the height of the Hasse diagram associated to the poset Spec(L)

For Kripke model, we have a way to express as formulae the height of the associated poset

Boundary

Analysing this definition suggests to introduce the following notion: if $a \in L$ let the boundary of a be the ideal $B_a = a \vee \neg a = \{x \vee y \mid x \leq a,\ y \wedge a = 0\}$

"Geometrically" this definition corresponds to the topological boundary of $D(a)$

We get then the following inductive definition:

Definition: Kdim$(L) < 0$ iff $1 =_L 0$ and Kdim$(L) < n+1$ iff for any $a \in L$ we have Kdim$(L/B_a) < n$

Boundary

We can transpose this definition to rings: if $a \in R$ let the boundary of a be the ideal B_a generated by a and all elements x such that ax is nilpotent

Definition: Kdim$(R) < 0$ iff $1 =_L 0$ and Kdim$(R) < n+1$ iff for any $a \in R$ we have Kdim$(R/B_a) < n$

Boundary

Unfolding this definition, we get the following Nullstellensatz

Theorem: Kdim$(R) < n$ iff for any $a_1, \ldots, a_n$ there exists $k_1, \ldots, k_n$ and $u_1, \ldots, u_n$ such that

$$a_1^{k_1}(a_2^{k_2}(\ldots a_n^{k_n}(1 - a_n u_n) \cdots - a_2 u_2) - a_1 u_1) = 0$$

We have yet another example of a reduction of a Π_1^1 statement to a Σ_1^0 statement

Using this characterisation, one can give a simple constructive proof of Kdim$(\mathbb{Q}[X_1, \ldots, X_n]) = n$

A simple example

A basic result in algebra is the following.

Theorem: *A finitely generated projective module over a local ring R is free*

Projective module: a direct factor of a free module

Local ring: has only one maximal ideal

These conditions can be expressed more concretely to get something first-order

A simple example

Only one maximal ideal: this should be the set of elements that are *not* invertible

We replace this by the following simpler (logically) definition:

R is local iff

$Inv(x+y) \to [Inv(x) \vee Inv(y)]$ for all x, y iff

$Inv(x) \vee Inv(1-x)$ for all x

where $Inv(x)$ means that x is invertible

A simple example

A finitely generated projective module can be represented by an idempotent matrix

It is represented by an *idempotent matrix* F, since M is a direct factor of some R^n

The elements of M are the vector FX for $X \in R^n$

A simple example

In this way we can simplify the abstract statement to a statement about idempotent matrix F over a local ring.

The statement of this theorem, for a fixed size of F is first-order and geometric.

The statement in this new form suggest the algorithm form of the proof: given F of size n we should construct $X_1, \ldots, X_k$ with $k \leq n$ such that $FX_1, \ldots, FX_k$ is a basis of the image of F

The only "subprogram" we can use is given by

$\forall x. Inv(x) \vee Inv(1-x)$

A simple example

The concrete version is:

Theorem: *If F is an idempotent square matrix over a local ring R then F is similar to a matrix of the form*

$$\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$$

We can effectively build an invertible P such that PFP^{-1} is of this form

A simple example

We have a first-order classical derivation, that we can transform by proof-theoretic methods (Friedman's translation) to a constructive first-order derivation

We know a priori that the proof should have a simple form and can only use the disjunction $Inv(x) \vee Inv(1-x)$

It may be that the proof, as a first-order proof function of the size of the matrix, is not uniform in the size (but this is not likely)

Serre's splitting-off theorem

1958 (J.P. Serre) theorem of existence of free summands in projective modules (which represents fiber bundles over the *maximal* spectrum of a ring)

1964 (O. Forster) bounds on the number of generators of a module, in term of the *prime* spectrum of a ring

1967 R. Swan refines Forster's result for *maximal* spectrum

All these results were about *Noetherian* rings

What about nonNoetherian rings??

Serre's splitting-off theorem

Breakthrough in 1984

Heitmann obtained a nonNoetherian version of Forster's theorem, and some nonNoetherian version of Serre's and Swan's theorem (which does not generalise these theorems however)

In 2004: simple constructive proofs of these results (that can be thought of as algorithms)

As a side product, we got an improvement of Heitman's results, and a nonNoetherian generalisation of Serre and Swan's theorems

Serre's splitting-off theorem

Serre (1958) represents algebraically the notion of a vector bundle

Example: tangent bundle of a manifold, on S^1 and S^2

When is a vector bundle trivial?? A necessary condition is that it admits a non vanishing section

Example: tangent bundle over S^2 is not trivial

Serre's splitting-off theorem

Heuristically, if the dimension of each fibers is big w.r.t. the dimension of the base space, one can find a non vanishing section

Serre obtained a purely algebraic version of this result

If X is a simplical complex, and we have a fiber bundle $E(x),\ x \in X$, we find a nowhere vanishing continuous section $s(x) \in E(x)$ by defining it stepwise on simplices of higher and higher dimension

The key fact is that if we have a continuous function on the boundary of $[0,1]^n$ to S^n we can extend it to $[0,1]^n$ (i.e. $\pi_k(\mathsf{S}^n) = 0$ if $k < n$)

Algebraic formulation

The base space is represented by the *maximal spectrum* $\mathrm{Max}(R)$ of a (commutative) ring R, with the Zariski topology

The vector bundle is represented by a *module* M over R

Serre's splitting-off theorem

Intuitively: R ring of functions over Max(R) and M represents the module of *sections* of the fiber bundle

We consider only finitely generated modules over R

Serre shows that the vector bundles correspond exactly to the *projective* modules over M

The points x of Max(R) are maximal ideals, and the vector space fiber at x is the module M/xM over the field R/x. Its dimension is written $r_x(M)$

If $s \in M$ we can write $s(x)$ the equivalence class of s in M/xM and $M(x)$ for M/xM

Serre's splitting-off theorem

Serre considers the dimension jdim(R) which is the Krull dimension of Max(R) (as a subspace of Spec(R))

Assume that R is *Noetherian* and jdim$(R) < k$

Theorem: (Serre, 1958) If $k \leq r_x(M)$ for all $x \in$ Max(R) then there exists a non vanishing section $s \in M$, i.e. an element $s \in M$ such that $s(x) \neq 0$ for all $x \in$ Max(R)

We give a first-order formulation of a non Noetherian version of this statement, which becomes a schema of theorems in the first-order theory of commutative rings

Swan's theorem

Assume that R is *Noetherian* and jdim$(R) = d$

Theorem: (Swan, 1967) Assume that $r_x(M) = r$ for all $x \in \mathrm{Max}(R)$ then M can be generated by $r + d$ elements

(Interestingly the concrete version of the this and Serre's theorem are almost the same)

Can this be generalised to the nonNoetherian cases?

For instance Vascancelos and Wiegand, 1978, obtained the bound $r(d + 1)$ for the number of generators in the nonNoetherian cases

Concrete version

How to represent concretely a finitely generated projective module M?

It is represented by an *idempotent matrix* F, since M is a direct factor of some R^n

The elements of M are the vector FX for $X \in R^n$

Concrete version

How to represent $k \leq r_x(M)$ for all $x \in \mathrm{Max}(R)$?

$1 = \Delta_k(F)$ where $\Delta_k(F)$ is the ideal generated by all the minors of F of order k

Indeed for each $x \in \mathrm{Max}(R)$ the matrix F should be of rank $\geq k$ over the field R/xR

Thus the ideal generated by $\Delta_k(F)$ is not included in x

This means $1 = \Delta_k(F)$

Concrete version

Serre's theorem becomes for a Noetherian ring R such that jdim$(R) < k$

Theorem: If F is an idempotent matrix and $1 = \Delta_k(F)$ then there exists $X \in R^n$ such that FX is *unimodular*

A vector $(a_i) \in R^n$ is *unimodular* iff there exists $u_i \in R$ such that $\Sigma u_i a_i = 1$

Unimodular vector: for each $x \in Max(R)$ at least one component does not belong to x (the ideal generated by the a_i is contained in *no* ideal maximal)

Concrete version

Indeed we want $s \in M$ such that $s(x) \neq 0$ for all $x \in \mathrm{Max}(R)$

This means: we want $X \in R^n$ such that $FX = (a_i)$ is not 0 modulo x, for any $x \in \mathrm{Max}(R)$

This means that the ideal generated by (a_i) is not included in x for any $x \in \mathrm{Max}(R)$

This is equivalent to: 1 belongs to the ideal generated by (a_i)

Heitmann dimension

For the hypotheses *Noetherian* Heitmann discovered in 1984 that it is probably not necessary

Interestingly the heart of the matter for eliminating the Noetherian hypotheses is directly connected to our inductive definition of dimension

This is presented by Heitmann as a trivial, but crucial, remark similar to the fact that to quotient a ring by a boundary ideal reduces the dimension

Heitmann dimension

Heitmann in his argument uses a refinement of Krull dimension (to talk about maximal spectrum) which can be formulated in a *first-order way*

The intersection of all maximal ideals (Jacobson radical) is the set $J(R)$ of elements $a \in R$ such that $1 - ax$ invertible for all x

We redefine the boundary H_a of a as the ideal generated by a and the set of elements x such that $ax \in J(R)$

Definition: $\mathrm{Hdim}(L) < 0$ iff $1 =_L 0$ and $\mathrm{Hdim}(L) < n+1$ iff for any $a \in L$ we have $\mathrm{Hdim}(L/H_a) < n$

Heitmann dimension

The statement $\mathrm{Hdim}(R) < n$ is expressed by a *first-order* formula which is *prenex*

Its logical complexity increases with n

$\mathrm{Hdim}(R) < 1$ means that for any a there exists x such that $a(1-ax) \in J(R)$

$\mathrm{Hdim}(R) < 2$ means that for any a we have $\mathrm{Hdim}(R/H_a) < 1$ which means that for any b there exists y such that $b(1-by) \in J(R/H_a)$, which means that for any z there exists t, u we have $a(t(1-zb(1-by)) - ua) \in J(R)$

$\forall a, b. \exists y. \forall z. \exists t, u \forall v \exists w. \ldots$

Heitmann dimension

The schema of first-order theorems we prove is

Theorem: If Hdim$(R) < k$ then given a $m \times n$ rectangular matrix F such that $\Delta_k(F) = 1$ there exists $X \in R^n$ such that FX is unimodular

The proof was obtained by looking at the case of a 3×2 matrix with $k = 2$, which is formulated by a purely first-order statement

The proof in this special case generalises directly

Heitmann dimension

The statement has the form

$A \to (t = 0 \to \exists x.u = 0)$

where A is prenex

We know *a priori* that if it is provable, it is provable intuitionistically

Heitmann dimension

This theorem generalises also Swan's theorem: we get as a corollary that if a f.g. module M is locally generated by r elements over a ring R such that $\mathrm{Hdim}(R) = d$ then R is generated by $d + r$ elements, as in Swan's theorem

Heitmann dimension

Using this, L. Ducos could obtain a nonNoetherian version of Bass cancellation theorem

Theorem: If Hdim$(R) < n$ and P, Q, N are finitely generated projective modules such that P is of rank $\geq n$ and $P \oplus N \simeq Q \oplus N$ then $P \simeq Q$

Where the method may not work

Statement in algebra of the form $R\ Noetherian \vdash \ldots$

Regular Element Theorem: *if R Noetherian* and if

$$a_1 x = \cdots = a_n x = 0 \rightarrow x = 0$$

then there exists $u \in <a_1, \ldots, a_n>$ such that $ux = 0 \rightarrow x = 0$

Conclusion

One can make sense in constructive mathematics of relatively recent results of commutative algebra

The statements and proofs get simpler for this example

Conclusion

Quite simple considerations on the logical complexity of the statements in algebra seem already to be useful; for instance, the fact that the *elements* of a ring are "simpler" than the *prime ideals*

Using relatively simple Nullstellensatz theorems one can reduce the logical complexity of statements and guess a priori an expected complexity for the proof

Can one apply proof theoretic techniques for proofs that use a Noetherian hypotheses?

Is there a general metatheorem allowing to guess when a Noetherian assumption can be eliminated?

Example: Kronecker's theorem

Kronecker in section 10 of

Grundzüge einer arithmetischen Theorie der algebraischen Grössen.
J. reine angew. Math. 92, 1-123 (1882)

proves a theorem which is now stated in the following way

An algebraic variety in $\mathbb{C}^n$ *is the intersection of* $n+1$ *hypersurfaces*

If we look at the own statement of (direct followers of) Kronecker we find something close to the formal statement that for any $g_1, \ldots, g_{n+2} \in \mathbb{Q}[x_1, \ldots, x_n]$ there exists $f_1, \ldots, f_{n+1}$ such that

$$[X(g_1) \wedge \cdots \wedge X(g_{n+2})] \leftrightarrow [X(f_1) \wedge \cdots \wedge X(f_{n+1})]$$

Example: Kronecker's theorem

Thus the formal approach should be closer here to the original statement of Kronecker

One works with the system of equations and provability rather than with the solutions in $\mathbb{C}^n$

The meaning of Kronecker's theorem

For Kronecker, the solutions were purely *formal*, like in the present explanation of infinite objects as theories

When is $f = 0$ a consequence of $g_0 = \cdots = g_m = 0$?

How to deduce consequences? We have two principles

If we have $A = 0,\ B = 0$ we have also $rA + sB = 0$

If we have $A^2 = 0$ we have $A = 0$

This is exactly to say that f belongs to the radical of the ideal generated by $g_0, \ldots, g_m$

Boundary

The argument of Kronecker, which uses elimination theory, was simplified (?) later by van der Waerden

Theorem: *If a ring* R *is* Noetherian *and such that* Kdim$(R) \leq n$ *then any f.g. ideal is radically generated by at most* $n+1$ *elements*

General abstract argument, but uses Noetherianity

Boundary

It turns out that one can prove directly by using the inductive definition of Krull dimension

Theorem: *If* $\mathrm{Kdim}(R) \leq n$ *then any f.g. ideal is radically generated by at most* $n+1$ *elements*

This result is due to Heitmann (1984)

Using our definitions, we get a direct elementary proof

This can be expected *a priori* by completeness (and cannot be guessed if one uses a formulation with prime ideals)

Boundary

This argument can be instantiated in the case of $R = \mathbb{Q}[x_1, \ldots, x_n]$ gives an algorithm for the following problem:

Given $n+2$ polynomials g_1, g_2, $\ldots$, g_{n+2} in n indeterminates with rational coefficients, construct $n+1$ polynomials f_1, f_2, $\ldots$, f_{n+1} in the same indeterminates with rational coefficients that are zero mod g_1, g_2, $\ldots$, g_{n+2} and have the property that, for each i, some power of g_i is zero mod f_1, f_2, $\ldots$, f_{n+1}

Furthermore the solution, though inspired by "ideal" methods, uses only methods that Kronecker would have accepted

References

Th.C., H. Lombardi, M.-F. Roy
An elementary characterisation of Krull dimension
to appear (2005)

Th.C.
Sur un théorème de Kronecker concernant les variétés algébriques
C.R.Acad.Sci., Paris, Ser I 338 (2004), Pages 291-294

Th. C., H. Lombardi, C. Quitté
Generating non-Noetherian modules constructively
Manuscripta Mathematica, 1115, 513-520 (2004)

L. Ducos
Théorèmes de Forster-Swan et Bass. Preprint (2004)

References

R. Heitmann "Generating non-Noetherian modules efficiently"
Michigan Math. J. 31 (1984), 167-180

O. Forster "Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring"
Math.Z. 84 1964, 80-87

J.-P. Serre "Modules projectifs et espaces fibrés à fibre vectorielle"
Séminaire P. Dubreil, Année 1957/1958

R.G.Swan "The Number of Generators of a Module"
Math.Z. 102 (1967), 318-322

References

Coste M., Lombardi H., Roy M.F.
"Dynamical method in algebra: Effective Nullstellensätze"
J.P.A.A. 155 (2001)

L. Ducos, H. Lombardi, C. Quitté and M. Salou.
Théorie algorithmique des anneaux arithmétiques, de Prüfer et de Dedekind.
Journal of Algebra 281, (2004), 604-650.