Constructive Homological Algebra

jww Henri Lombardi and Claude Quitté

Monastir, December 16, 2009

Linear algebra over a ring

Linear algebra $=$ solving linear system of equations

$AX = 0$ homogeneous case

Over a field the situation is well understood

We want to generate all solutions: find L such that $AL = 0$ and such that $AX = 0$ iff X can be written LY

The ring is *coherent* if we can solve, in this sense, such homogenenous systems

Linear algebra over a ring

Important examples of coherent rings

polynomial rings $k[X_1, \ldots, X_n]$ via Gröbner bases

Valuation domain: we have $x|y$ or $y|x$

Prüfer domain: has a simple first order description (Ducos, Lombardi, Quitté, Salou) non Noetherian version of Dedekind domain

Linear algebra over a ring

$AX = B$ general case

If we can also decide this: *strongly discrete ring*

It is enough to decide membership to finitely generated ideal $\langle a_1, \ldots, a_n \rangle$

Linear algebra over a ring

Important examples of strongly discrete coherent rings

polynomial rings $k[X_1, \ldots, X_n]$ via Gröbner bases (other proof: Hilbert, Seidenberg)

Valuation/Prüfer domain with a decidable divisibility relation

Resolutions

Let R be *coherent*

Let $I = \langle a_1, \ldots, a_p \rangle$ be a finitely generated ideal

We have a surjective map $R^p \to I \to 0$

The kernel of this map is finitely generated: this is precisely what coherent means, so we can describe the relations between the generators

$$R^q \to R^p \to I \to 0$$

Resolutions

In the same way, the relations *between the relations* can be finitely generated

$R^l \rightarrow R^q \rightarrow R^p \rightarrow I \rightarrow 0$

In general we can in this way define a stream of free modules $F_0,\ F_1,\ F_2,\ \dots$ and an exact sequence

$0 \leftarrow I \leftarrow F_0 \leftarrow F_1 \leftarrow F_2 \leftarrow \dots$

Resolutions

More generally we work with *finitely presented module*

$R^n \xrightarrow{u} R^l \to M \to 0$

Concretely it given by a $n \times l$ matrix representing the map u

We can in the same way compute the free resolutions of this module

$0 \leftarrow M \leftarrow F_0 \leftarrow F_1 \leftarrow F_2 \leftarrow \ldots$

Thus we can work with only concrete objects: sequence of matrices

Finite Free Resolutions

$$0 \leftarrow I \leftarrow F_0 \leftarrow F_1 \leftarrow F_2 \leftarrow \cdots \leftarrow F_m \leftarrow 0$$

In the case $m = 0$: we have $F_0 = R$ or $F_0 = 0 = I$ (otherwise $1 = 0$ in R)

The ideal I is principal.

For $m = 1$? For $m = 2$?

Hilbert Syzygies Theorem: for $R = k[X_1, \ldots, X_n]$ for any ideal we have a sequence that stops at a stage $\leqslant n$

Finite Free Resolutions

The maps $F_{i-1} \leftarrow F_i$ are concrete objects: matrices with values in the ring R

We write $F_i = R^{p_i}$ and the map is a $p_i \times p_{i-1}$ matrix

To give a finite free resolution: logically simple statements

$A_i A_{i-1} = 0$

$A_i X = 0$ iff there exists Y such that $X = A_{i-1} Y$

If the ring is coherent strongly exact the second condition is also decidable

Finite Free Resolutions

Northcott *Finite free resolutions*, Cambridge University Press, 1976

Eagon and Northcott *On the Buchsbaum-Eisenbud theory of finite free resolutions*, J. Reine Angew. Math. 262/263 (1973), 205-219

Concrete and nicely presented ("beautifully self-contained treatment"): explicit manipulation of matrices over a ring

Use several notations with indexes over finite sets

Not completely elementary: some arguments use localisation at arbitrary prime ideals, or at arbitrary minimal prime ideals

Regular elements and ideals

a is *regular*: if $ax = 0$ then $x = 0$

$a_1, \dots, a_n$ define a regular ideal: if $a_1 x = \cdots = a_n x = 0$ then $x = 0$

property 1: *if* $\langle a, a_1, \dots, a_n \rangle$ *and* $\langle b, a_1, \dots, a_n \rangle$ *are regular then so is* $\langle ab, a_1, \dots, a_n \rangle$

Corollary: *if* $\langle a_1, \dots, a_n \rangle$ *is regular then so is* $\langle a_1^l, \dots, a_n^l \rangle$

Regular elements and ideals

property 2: *if* $\langle a_1, \dots, a_n \rangle$ *is regular and we have* $x = y$ *in each* $R[1/a_1], \dots, R[1/a_n]$ *then* $x = y$ *in* R

Corollary: *if* $\langle a_1, \dots, a_n \rangle$ *is regular and* J *is regular in each* $R[1/a_1], \dots, R[1/a_n]$ *then* J *is regular in* R

"New" kind of glueing property (usually one assumes $1 = \langle a_1, \dots, a_n \rangle$)

Matrices and regular ideals

If we have a $p \times q$ matrics A, and $I \subseteq I_p,\ J \subseteq I_q$ with $|I| = |J| = n$ we write $A^{(n)}(I, J)$ for the determinant of the corresponding extracted $n \times n$ matrix

The *determinantal ideal* $\Delta_n(A)$ of order n is the ideal generated by all $A^{(n)}(I, J)$

In particular $\Delta_0(A) = R$ and $A(\emptyset, \emptyset) = 1$

Matrices and regular ideals

Lemma: (McCoy) *Let* $R^p \xrightarrow{u} R^q$ *be represented by a* $p \times q$ *matrix* A *then* u *is injective iff the ideal* $\Delta_p(A)$ *is regular*

Proof: we show that if $xA(I, J) = 0$ whenever $|I| = |J| = l + 1$ then $xA(I, J) = 0$ whenever $|I| = |J| = l$

We have $xA(I, J) = 0$ whenever $|I| = |J| = p + 1$

We apply this until we have $x = xA(\emptyset, \emptyset) = 0$.

Formal proof? (I think the argument does not assume $p \leqslant q$)

Regular sequences

$u_1, \ldots, u_m$ is a *regular sequence* iff

u_1 is regular

u_2 is regular mod. u_1

u_3 is regular mod. u_1, u_2

$\ldots$

u_m is regular mod. $u_1, \ldots, u_{m-1}$

Grade

$Gr(a_1, \ldots, a_n) \geqslant 2$ iff the ideal $\langle a_1, \ldots, a_n \rangle$ contains a regular sequence u_1, u_2, in the *Noetherian* case

In general iff

$a_1, \ldots, a_n$ is regular and

$a_1, \ldots, a_n$ is regular modulo $a_1X_1 + \cdots + a_nX_n$

This implies

$\forall i \ j. a_ib_j = a_jb_i$

$\leftrightarrow \quad \exists x. \ \ x \ (a_1, \ldots, a_n) = (b_1, \ldots, b_n)$

Original Goal

To understand the results of Auslander, Buchsbaum, Serre on *regular rings*

Local rings at a non singular point: Noetherian and the maximal ideal is generated by a regular sequence

These rings have a nice structure: *integral domain* and *unique factorization domain*

Homological characterization: Noetherian and *finite global dimension* which means that we have n such that any (finitely generated ideal) have a finite free resolution of length $\leqslant n$

Constructive version of these results? Corresponding algorithms?

Euler characteristic

If I has a finite free resolution

$$0 \leftarrow I \leftarrow F_0 \leftarrow F_1 \leftarrow \cdots \leftarrow F_n \leftarrow 0$$

where F_i is R^{p_i} we define the Euler characteristic to be

$$p_0 - p_1 + p_2 - \dots$$

Constructive version

The constructive core consists in two results that have elementary statements and proofs, and have nothing to do with Noetherianity

Constructive version

Theorem 1: *If I has a finite free resolution*

$$0 \leftarrow I \leftarrow F_0 \leftarrow F_1 \leftarrow \cdots \leftarrow F_n \leftarrow 0$$

and

(1) if the Euler characteristic is $\neq 1$ then $I = 0$

(2) if the Euler characteristic is 1 then I is regular

Constructive version

The part (2) is called Vasconcellos Theorem in Northcott's book

(1) is proved via localisation at arbitrary prime

(2) is proved via localisation at arbitrary minimal prime

Constructive version

Using a general technique of eliminations of prime and minimal prime we obtain an elementary and short proof of Theorem 1

In particular in the case $I = \langle a \rangle$, from a given finite free resolution of I we can decide

$a = 0$ or

a is regular

This explains: if the ring is regular then it is an integral domain (Serre)

Constructive version

Theorem 2: *If* $I = \langle a_1, \ldots, a_p \rangle$ *has a finite free resolution*

$$0 \leftarrow I \leftarrow F_0 \leftarrow F_1 \leftarrow \cdots \leftarrow F_n \leftarrow 0$$

of Euler characteristic 1 *then* $a_1, \ldots, a_p$ *have a gcd*

This time, this corresponds to a general algorithm

A particular case

Hilbert-Burch

$$0 \to R^2 \xrightarrow{M} R^3 \xrightarrow{(a_1\ a_2\ a_3)} I \to 0$$

where

$$M = \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \\ u_3 & v_3 \end{pmatrix}$$

A particular case

$$0 \to R^2 \xrightarrow{M} R^3 \xrightarrow{(a_1\ a_2\ a_3)} I \to 0$$

In this case we can show (for *any* ring):

the 2×2 minors of M: $\Delta_1, \Delta_2, \Delta_3$ form a regular ideal and furthermore whenever we have a family b_1, b_2, b_3 such that $b_i\Delta_j = b_j\Delta_i$ then there exists a (unique) b such that $b_1 = b\Delta_1,\ b_2 = b\Delta_2,\ b_3 = b\Delta_3$

This follows from $Gr(\Delta_1, \Delta_2, \Delta_3) \geqslant 2$

This corresponds to an *algorithm*. The existence of b is using the *exactness* of the sequence, which is expressed in a constructive way

A particular case

$$0 \to R^2 \xrightarrow{M} R^3 \xrightarrow{(a_1\ a_2\ a_3)} I \to 0$$

We have $a_1u_1+a_2u_2+a_3u_3 = a_1v_1+a_2v_2+a_3v_3 = 0$ and hence $a_i\Delta_j = a_j\Delta_i$

Hence we have a such that $a_1 = a\Delta_1,\ a_2 = a\Delta_2,\ a_3 = a\Delta_3$ and one can then show that a is the gcd of a_1, a_2, a_3

Future work

General case: multiplicative structure and Cayley determinant

$$0 \to F_n \xrightarrow{u_n} F_{n-1} \xrightarrow{u_{n-1}} \dots \xrightarrow{u_1} F_0 \to I \to 0$$

the map u_i is represented by the $p_i \times p_{i-1}$ matrix A_i

We define

$$q_n = p_n,\ q_{n-1} = p_{n-1} - q_n,\ \dots,\ q_0 = p_0 - q_1$$

Then $\Delta_{q_i}(A_i)$ is regular and $\Delta_{q_i+1}(A_i) = 0$

Future work

If $I \subseteq I_p$ we write I' the complement of I in I_p. We can then consider that the sequence corresponding to I, I' defines a permutation of I_l and we write $sgn(I, I')$ the signature of this permutation.

Theorem: *There exists a family $u_l(I)$ of elements of R with $I \subseteq I_{p_l}$ of cardinal q_l such that*

$$A_l(I, J) = sgn(I, I')u_{l+1}(I')u_l(J)$$

This is related to the notion of *Cayley determinant* of a complex of Euler characteristic 0 (simplest case $R^n \to R^n$)

Future work

non Noetherian theory of regular sequences: for instance if $u_0, u_1, \ldots, u_n$ is regular inside $\langle a_1, \ldots, a_n \rangle$ then $1 = 0$ in R

Noetherian case (Lionel Ducos): some results towards constructive equivalence between the usual definition of regular rings and the homological characterization