Computational methods in algebraic geometry
Gröbner bases and Syzygies

Hans Schönemann

hannes@mathematik.uni-kl.de

FB Mathematik

University of Kaiserslautern

Motivation

- solving the ideal membership problem for polynomial rings
- computing the Hilbert function, dimension, etc. for ideal in polynomial rings
- ”solving” of polynomial equations

Rings and Ideals

A none empty set with 2 operations (R,+,*) is a Ring, if

- (R,+) is an abelian group (+ is commutative,associative,it exists a neutral element 0, for each element a exist an inverse element $-a$)
- (R,*) is a semigroup (it exists a neutral element 1,* is associative)
- Distribitivityät: $a * (b + c) = a * b + a * c$, $(b + c) * a = b * a + c * a$

Examples:

- $(Z, +, *)$ the integers
- $(Q, +, *)$ the rationals
- $(Q[x], +, *)$ polynomials over the rationals
- $(Q[x, dx], +, *)$ differetial operators in x and dx over the rationals

Rings and Ideals

An Ideal is a (none empty) subset of a ring R with

- $\forall a, b \in I : a + b \in I$
- $\forall a \in I, b \in R : a * b \in I$ (right ideal)
  or
  $\forall a \in I, b \in R : b * a \in I$ (left ideal)

Examples:

- all even numbers in Z
- all polynomials in x without absolute term (in $Q[x]$)
- (0) and R are ideals in every ring $(R, +, *)$

Ideals in Polynomial Rings

We work over a field K (a field $(K, +, *)$ is a ring, $(K \setminus \{0\}, *)$ is an abelian group).
Consider the polynomial ring $R = K[x_1, \ldots, x_n]$.
If $T \subset R$ is any subset, all linear combinations $g_1 f_1 + \ldots + g_r f_r$, with $g_1, \ldots .g_r \in R$ and $f_r \in T$, form an ideal $\langle T \rangle$ of R, called the ideal **generated by** T. We also say that T is a **set of generators** for the ideal.
Hilbert's Basis Theorem Every ideal of the polynomial ring $K[x_1, \ldots, x_n]$ has a finite set of generators.

The Geometry-Algebra Dictionary

Algebraic Sets I

The **affine** n**-space** over K is the set

$$\mathbb{A}^n(K) = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in K\}.$$

Definition. If $T \subset R$ is any set of polynomials, its **vanishing locus** in $\mathbb{A}^n(K)$ is the set

$$V(T) = \{p \in \mathbb{A}^n(K) \mid f(p) = 0 \mathrm{forall} f \in T\}.$$

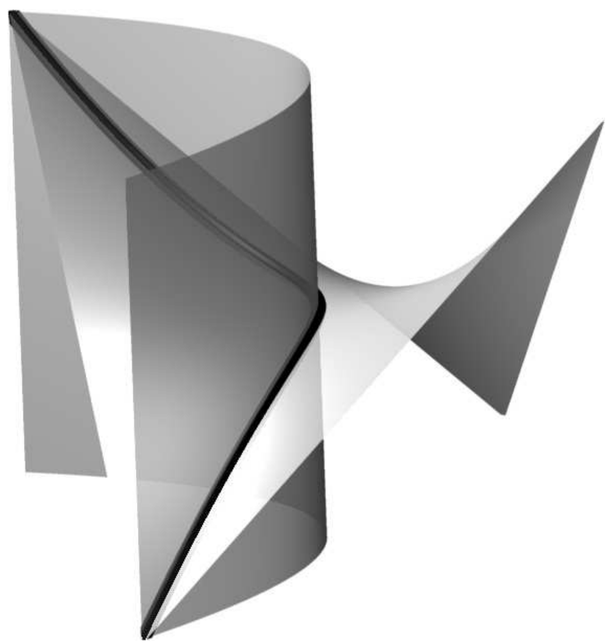
Every such set is called an **affine algebraic set.**
The vanishing locus of a subset $T \subset R$ coincides with that of the ideal $\langle T \rangle$ generated by T. So every algebraic set in $\mathbb{A}^n(K)$ is of type $V(I)$ for some ideal I of R. By Hilbert's basis theorem, it is the vanishing locus of a set of finitely many polynomials.

The Geometry-Algebra Dictionary

Algebraic Sets II

The vanishing locus of a single non-constant polynomial is called a **hypersurface** of $\mathbb{A}^n(K)$. According to our definitions, every algebraic set is the intersection of finitely many hypersurfaces.

Example. The **twisted cubic curve** in $\mathbb{A}^3(\mathbb{R})$ is obtained by intersecting the hypersurfaces $V(y - x^2)$ and $V(xy - z)$:



The Geometry-Algebra Dictionary

Algebraic Sets III

Taking vanishing loci defines a map V which sends sets of polynomials to algebraic sets. We summarize the properties of V:

Proposition.

(i) The map V reverses inclusions: If $I \subset J$ are subsets of R, then $V(I) \supset V(J)$.

(ii) Affine space and the empty set are algebraic:

$$V(0) = \mathbb{A}^n(K). \quad V(1) = \emptyset.$$

(iii) The union of finitely many algebraic sets is algebraic: If $I_1, \ldots, I_s$ are ideals of R, then

$$\bigcup_{k=1}^{s} V(I_k) = V(\bigcap_{k=1}^{s} I_k).$$

The Geometry-Algebra Dictionary

Algebraic Sets IV

(iv) The intersection of any family of algebraic sets is algebraic: If $\{I_\lambda\}$ is a family of ideals of R, then

$$\bigcap_\lambda V(I_\lambda) = V\left(\sum_\lambda I_\lambda\right).$$

(v) A single point is algebraic: If $a_1, \ldots, a_n \in K$, then

$$V(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}.$$

Computational Problem Give an algorithm for computing ideal intersections.

Gröbner Bases

The key idea behind Gröbner bases is to reduce problems concerning arbitrary ideals in polynomial rings to problems concerning monomial ideals.

Monomial ordering

monomial ordering (term ordering) on $K[x_1, \ldots, x_n]$: a total ordering $<$ on $\{x^\alpha | \alpha \in \mathbf{N}^n\}$ with $x^\alpha < x^\beta$ implies $x^\gamma x^\alpha < x^\gamma x^\beta$ for any $\gamma \in \mathbf{N^n}$.
wellordering: 1 is the smallest monomial.
Let $a_1, \ldots, a_k$ be the rows of $A \in GL(n, \mathbf{R})$, then $x^\alpha < x^\beta$ if and only if there is an i with $a_j\alpha = a_j\beta$ for j < i and $a_i\alpha < a_i\beta$.
degree ordering: given by a matrix with coefficients of the first row either all positive or all negative.
$\mathbf{L(g)}$ leading monomial, $\mathbf{c(g)}$ the coefficient of L(g) in g, g = c(g)L(g) + smaller terms with respect to $<$.
elimination ordering for $x_{r+1}, \ldots, x_n$: $L(g) \in K[x_1, \ldots, x_r]$ implies $g \in K[x_1, \ldots, x_r]$).

What is a Gröbner basis?

- monomial ordering on $\{x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}\}$ is well–ordering

$x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n} > x_1^{\beta_1} \cdot \ldots \cdot x_n^{\beta_n}$ if

- lexicographical ordering: $\alpha_j = \beta_j$ if $j \leq k-1$ and $\alpha_k > \beta_k$
- degree-lexicographical ordering: $\sum \alpha_i > \sum \beta_i$ or $\sum \alpha_i = \sum \beta_i$ and $\alpha_j = \beta_j$ if $j \leq k-1$ and $\alpha_k > \beta_k$

- deg-lex: $y^3 + 5xy + y^2 + x + 3y + 1$
- lex: $xy + x + 77y^3 + y^2 + 3y + 1$

What is a Gröbner basis?

- $NF(x^3y + xy + z^2 \mid \{x^3 + z, z^2 - z\}) = xy - yz + z$
- $x^3y + xy + z^2 - y * (x^3 + z) = xy - yz + z^2$
- $xy - yz + z^2 - (z^2 - z) = xy - yz + z$
- normal form of f with respect to $G = \{f_1, \dots, f_k\}$:
  $NF(f||G)$
  $h := f$
  while $(\exists \text{monomial } m, L(h) = mL(f_i) \text{for some } i)$
  $h := h - \frac{c(h)}{c(f_i)} m f_i$
  return $(c(h)L(h) + NF(h - c(h)L(h) \mid G)$

Buchbergers Algorithm

input: S=$\{f_1, ...f_r\}$ polynomials in K$[x_1, ..., x_n]$, < well-ordering
L:={(f,g), f,g $\in$ S}
while L $\neq \emptyset$
    take (f,g) $\in$ L, L:=L $\setminus\{(f,g)\}$
    h:=NF(spoly(f,g) | S)
    if h$\neq$0
        L:=L$\cup\{(h,f)\forall f \in S\}$
        S:=S$\cup\{(h)\}$
    end
end
return S

Example for a Gröbner basis

ideal

$$\begin{array}{ccccccccc} x_1 & + & x_2 & + & x_3 & - & 1 & = & f_1 \\ x_1 & + & 2x_2 & - & x_3 & + & 2 & = & f_2 \end{array}$$

Groebner basis

$$\begin{array}{ccccccccc} x_1 & & & + & 3x_3 & - & 4 & = & g_1 \\ & & x_2 & - & 2x_3 & + & 3 & = & g_2 \end{array}$$

$NF(g_2|\{f_1, f_2\}) = g_2$ but $NF(g_2|\{g_1, g_2\}) = 0$

- Gröbner bases can be very complicated and their computation can take a lot of time.

Basic Properties of Gröbner bases

- ideal membership
  $f \in I$ iff NF(f,GB(I))=0
- elimination
  $<$ an elimination order for $y_1, \ldots, y_n$,
  $R = K[x_1, \ldots, x_r, y_1, \ldots, y_n]$. Then
  $GB(I) \cap K[x_1, \ldots, x_r] = GB(I \cap K[x_1, \ldots, x_r])$.
- Hilbert function
  H(I)=H(L(I))

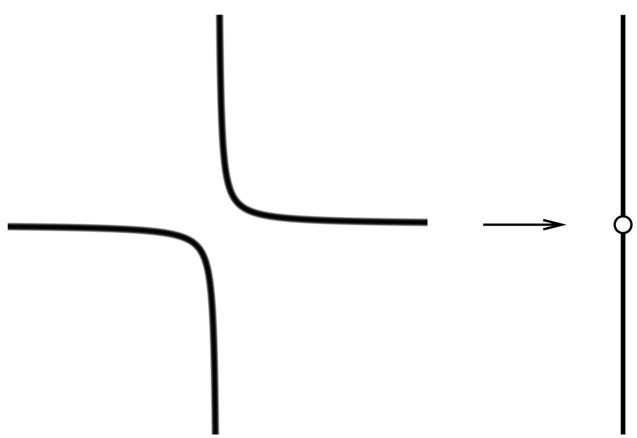
Leading ideal and dimension

- leading ideal: $L(I) = \langle \{L(f) | f \in I\} \rangle$
- The leading monomials of a Gröbner basis generate the leading ideal.
- Many invariants of the leading ideal can be computed combinatorically.
- The ideal and its leading ideal have many common properties.
- the dimension
- the Hilbert function
- $\{y^3 + x^2, x^2y - xy^2, x^4 + x^3\}$ is a Gröbner basis of $I =< y^3 + x^2, y^4 + xy^2 >$ therefore $L(I) =< y^3, x^2y, x^4 >$ and $dim_{\mathbb{C}} \mathbb{C}[x, y]/I = 8$

Geometry of Elimination

Definition. Let $A \subset \mathbb{A}^n(K)$ and $B \subset \mathbb{A}^m(K)$ be (nonempty) algebraic sets. A map $\varphi : A \to B$ is a **polynomial map**, or a **morphism**, if its components are polynomial functions on A. That is, there exist polynomials $f_1, \ldots, f_m \in R$ such that $\varphi(p) = (f_1(p), \ldots, f_m(p))$ for all $p \in A$.
The image of a morphism needs not be an algebraic set.

Example. Let $\pi : A^2(R) \to A^1(R),\ (a,b) \mapsto b$, be projection of the xy-plane onto the y-axis. Then π maps the hyperbola $C = V(xy-1)$ onto the punctured line $\pi(C) = A^1(R) \setminus \{0\}$ which is not an algebraic set.



Solving

```
ring  A=0,(x,y,z),lp;
ideal I=x2+y+z-1,
        x+y2+z-1,
        x+y+z2-1;

ideal J=groebner(I);
J;
J[1]=z6-4z4+4z3-z2          J[2]=2yz2+z4-z2
J[3]=y2-y-z2+z              J[4]=x+y+z2-1

triangL(J);
[1]:                        [2]:
   _[1]=z4-4z2+4z-1            _[1]=z2
   _[2]=2y+z2-1                _[2]=y2-y+z
   _[3]=2x+z2-1                _[3]=x+y-1
```

Monomial Orderings of Modules

In what follows, let F be R^s with its canonical basis $e_1, \ldots, e_s$.

Definition. A **monomial** in F is a monomial in R times a basis vector of F, that is, an element of the form $x^\alpha e_i$. A **monomial order** on F may be defined in the same way as a monomial ordering on R. That is, it is a total order $>$ on the set of monomials in F satisfying

$$x^\alpha e_i > x^\beta e_j \implies x^\gamma x^\alpha e_i > x^\gamma x^\beta e_j \text{ for each} \gamma \in \mathbf{N}^n.$$

We require in addition that

$$x^\alpha e_i > x^\beta e_i \iff x^\alpha e_j > x^\beta e_j \,, \forall i, j = 1, \ldots, s.$$

Monomial Ordering of Modules

Important orderings:

- term over position

  ```
  ring R=....,(dp,c);
  ring R=....,(dp,C);
  ```

- position over term

  ```
  ring R=....,(c,dp);
  ring R=....,(C,dp);
  ```

Capital C sorts generators in ascending order, i.e., gen(1) < gen(2) < ....
A small c sorts in descending order, i.e., gen(1) > gen(2) > ....
Ordering, ..., C) is the default.

Gröbner Bases of Modules

Finally, given a monomial order on F, we define the **leading term**, the **leading coefficient**, the **leading monomial**, and the **tail** of an element of F as we did for a polynomial in R.
With this basic notation, the whole concept of Gröbner bases including its fundamental algorithms extend.

Syzygies

Definition
Let $I = \{g_1, \ldots, g_q\} \subseteq K[\underline{x}]^r$.
The module of syzygies syz(I) is

$$ker(K[\underline{x}]^q \to K[\underline{x}]^r), \sum w_i e_i \mapsto \sum w_i g_i$$

Lemma The module of syzygies of I is

$$(g_1(\underline{x}) - e_{r+1}, \ldots, g_q(\underline{y}) - e_{r+q}) \cap \{0\}^r \times K[\underline{x}]^q$$

in $K[x_1, \ldots, x_m]^q$.

```
ring R=0,(x,y,z),(c,dp);
ideal I=maxideal(1);
// the syzygies of the (x,y,z)
syz(I);
```

Computation of Syzygies

Let $f_1, ..., f_s$ be polynomials in R, $I = (f_1, ...f_s)$. Consider the following matrix, compute the Gröbner basis of the columns wrt. to an monomial ordering (position over term, smallest index first).

$$\begin{pmatrix} f_1 & \cdots & f_s \\ 1 & 0\ldots & 0 \\ \vdots & & \vdots \\ 0 & 0\ldots & 1 \end{pmatrix} \mapsto \begin{pmatrix} GB(I) & 0 \\ T & S \end{pmatrix}$$

where T is the transformation matrix of $f_1, ...f_s$ to $GB(I)$, and the columns of S are a generation set of the syzygies of $f_1, ...f_s$

Example Usage of Syzygies

Let $I = (f_1, ..f_r)$ and $J = (g_1, ..., g_s)$ be ideals in $K[x_1, ...x_n]$.
Let $(a_1, ...a_r, b_1...b_s)$ be a syzygy of $(f_1, ..f_r, g_1, ...g_s)$, i.e. $\sum a_i f_i + \sum b_j g_j = 0$.
Then $I \cap J$ is generated by $\sum a_i f_i$.

Summary of Operations with Ideals

- sum of ideals (intersection of algebraic sets)
- intersection of ideals (union of algebraic sets)
- elimination of variables (projection of algebraic sets)
- ideal quotient/saturation ("difference" of algebraic sets)
- Hilbert function
- dimension of the ideals (dimension of the algebraic set)
- solving
- syzygies

Algorithms for Gröbner bases

- Buchberger's algorithm (std)
- F4: Gauss wrt. a basis of all occuring monomials (mathicgb)
- consider the complexity of coefficients (slimgb)
- use leading terms of syzygies to avoid reductions to 0: F5 (sba)
- parallelization via chinese remainder theorem:
  - rational coefficients to Z/p (modstd)
  - algebraic extension to rational (ffmod)
  - rational functions to rational (nfmod)
- indirect methods:
  - change of ordering via FGLM (fglm)
  - use of a known Hilbert function (stdhilb)

Algorithms for Syzygies

- algorithms for Gröbner bases (syz(I,"std"), syz(I,"slimgb"))
- extend sba/F5 to compute the syzygies (planned)
- parallelization via chinese remainder theorem
- indirect methods:
  - Schreyer's algorithm: from a GB to a GB of the syzygies (sres)
  - combine Schreyer with minimizing: (lres)

Computational Problems

- worst case complexity cannot be improved: example is independend of the algorithm
- intermediate coefficient growth: intermediate coefficients are often much larger than the result
- F4/F5: very large matrices, very sparse: tend to fill up