Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

1. Gröbner basis
2. Buchberger's criterion
3. Modules

Gröbner basis

We call the definition.

Definition. Let $>$ be a global monomial order and $I \subset K[x_1, \dots, x_n]$ an ideal. The **lead term ideal** of I is the ideal generated by the lead terms of elements of I:

$$\mathrm{Lt}(I) = (\{\mathrm{Lt}(f) \mid f \in I\}).$$

Elements $f_1, \dots, f_r \in I$ are a **Gröbner basis** of I if

$$\mathrm{Lt}(I) = (\mathrm{Lt}(f_1), \dots, \mathrm{Lt}(f_r)).$$

Proposition. *Let $f_1, \dots, f_r \in I$ be a Gröbner basis of I and $f \in K[x_1, \dots, x_n]$. Consider the remainder h of f divided by $f_1, \dots, f_r$. Then*

$$f \in I \iff h = 0.$$

Macaulay's theorem

Theorem. *Let $f_1, \ldots, f_r$ be a Gröbner basis of an ideal $I \subset K[x_1, \ldots, x_n]$ with respect to a global monomial order. Then the monomials $\{x^\alpha \mid x^\alpha \notin \mathrm{Lt}(I)$ represent a K-vector space basis for $K[x_1, \ldots, x_n]/I$.*

Proof. Let $\overline{f}$ be an element of $K[x_1, \ldots, x_n]/I$ and $f \in K[x_1, \ldots, x_n]$ a representative. Then the remainder h of f divided by $f_1, \ldots, f_r$ represents the same element: $\overline{f} = \overline{h}$. Since $\mathrm{Lt}(I) = (\mathrm{Lt}(f_1, \ldots, \mathrm{Lt}(f_r))$, the remainder h is a linear combination of the $x^\alpha \notin \mathrm{Lt}(I)$ by condition 2b). So the $\overline{x^\alpha}$ with $x^\alpha \notin \mathrm{Lt}(I)$ span $K[x_1, \ldots, x_n]/I$ as an K-vector space. They are linearly independent by the proposition. □

Example of a division

Consider $f_1 = x^2y - y^3$, $f_2 = x^3 \in K[x, y]$ and $>_{\text{lex}}$. Then

$$\text{Lt}(f_1) = x^2y \text{ and } \text{Lt}(f_2) = x^3.$$

We divide $f = x^3y$ by f_1, f_2:

$$f = x\,\text{Lt}(f_1) + 0\,\text{Lt}(f_2) + 0, \text{ hence}$$
$$f^{(1)} = f - (xf_1 + 0f_2 + 0) = xy^3.$$

In the second step we obtain

$$xy^3 = 0\,\text{Lt}(f_1) + 0\,\text{Lt}(f_2) + xy^3, \text{ hence}$$
$$f^{(2)} = f^{(1)} - (0f_1 + 0f_2 + xy^3) = 0.$$

The final result is

$$f = xf_1 + 0f_2 + xy^3.$$

Same example in a different order

We consider $f_1 = x^2y - y^3$, $f_2 = x^3 \in K[x,y]$ and $>_{\mathrm{lex}}$ with lead terms $\mathrm{Lt}(f_1) = x^2y$ and $\mathrm{Lt}(f_2) = x^3$ as before.

If we divide $f = x^3y$ by x^3, $x^2y - y^3$ we obtain

$$f = y\,\mathrm{Lt}(x^3) + 0\,\mathrm{Lt}(x^2y - y^3)) + 0, \text{ hence}$$
$$f^{(0)} = x^3y - (y(x^3) + 0(x^2y - y^3) + 0) = 0$$

and the final result is $\quad f = yf_2 + 0f_1 + 0. \quad$ Thus

Warning: The remainder of the division by polynomials $f_1, \ldots, f_r$ can depend on the order of $f_1, \ldots, f_r$!
This does not happen if $f_1, \ldots, f_r$ is a Gröbner basis.

Warning

The remainder of the division by polynomials $f_1, \ldots, f_r$ can depend on the order of $f_1, \ldots, f_r$! The reason is that the condition 2a) depends very much on the order.

Theorem. *Let $>$ be a global monomial order on $K[x_1, \ldots, x_n]$, $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ non-zero polynomials. For every $f \in K[x_1, \ldots, x_n]$ there exist uniquely determined $g_1, \ldots, g_r \in K[x_1, \ldots, x_n]$ and a unique remainder $h \in K[x_1, \ldots, x_n]$ satisfying*

1) $f = g_1 f_1 + \ldots + g_r f_r + h$

2a) *No term of $g_j \operatorname{Lt}(f_j)$ is divisible by a lead term $\operatorname{Lt}(f_i)$ for some $i < j$.*

2b) *No term of h is divisible by a lead term $\operatorname{Lt}(f_j)$.*

Buchberger's Criterion

Let $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ be poynomials. How to compute a Gröbner basis for $I = (f_1, \ldots, f_r)$?

The easiest way to discover a new lead term of $(f_1, \ldots, f_r)$ is to consider a difference where the lead terms cancel. Consider the monomial $m_{ij} = \gcd(\mathrm{Lt}(f_i), \mathrm{Lt}(f_j))$ and the S-**polynomial**

$$S(f_i, f_j) := \frac{\mathrm{Lt}(f_i)}{m_{ij}} f_j - \frac{\mathrm{Lt}(f_j)}{m_{ij}} f_i.$$

The lead term in this difference cancels, so we might discover a new lead term of I.

Theorem. *Let $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ be polynomials and $>$ be a global monomial order. $f_1, \ldots, f_r$ is a Gröbner basis for $(f_1, \ldots, f_r)$ if and only if for each pair i, j the remainder of $S(f_i, f_j)$ divided by $f_1, \ldots, f_r$ is zero.*

Buchberger's algorithm

Algorithm.
Input. A global monomial order and polynomials $f_1, \dots, f_r$.
Output. A Gröbner basis $f_1, \dots, f_s$ for $(f_1, \dots, f_r)$.

1. Initialize $s = r$ and $L = \{f_1, \dots, f_r\}$
2. for all i, j with $1 \leq i < j \leq s$ do
   compute the remainder h of $S(f_i, f_j)$;
   if $h \neq 0$ then
   $f_{s+1} = h$; $L = L \cup \{f_{s+1}\}$; $s = s + 1$;
3. return L.

The algorithm terminates since monomial ideals are finitely generated.

Example

Consider $f_1 = x^3$, $f_2 = x^2y - y^3 \in K[x, y]$ and $>_{\text{lex}}$. Then

$$\text{Lt}(f_1) = x^3, \text{Lt}(f_2) = x^2y$$

$m_{12} = x^2$ and $S(f_1, f_2) = xf_2 - yf_1 = -xy^3 = 0f_1 + 0f_2 - xy^3$ has a non-zero remainder. Thus

$$f_3 = -xy^3.$$

$m_{13} = x$ and $S(f_1, f_3) = x^2f_3 - (-y^3)f_1 = 0.$
$m_{23} = xy$ and $S(f_2, f_3) = xf_3 - (-y^2)f_2 = -y^5$. Thus

$$f_4 = -y^5$$

The S-polynomials $S(f_1, f_4)$ and $S(f_3, f_4)$ are zero. $m_{24} = y$ and $S(f_2, f_4) = x^2f_4 - (-y^4)f_2 = -y^7 = 0f_1 + 0f_2 + 0f_3 + y^2f_4 + 0.$

So $f_1, \dots, f_4$ is a Gröbner basis.

Example: 3×3-minors of a 3×5-matrix

Consider the ideal $I \subset K[x_1, \ldots, z_5]$ generated by the 3 minors of the matrix

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ y_1 & y_2 & y_3 & y_4 & y_5 \\ z_1 & z_2 & z_3 & z_4 & z_5 \end{pmatrix}$$

and $>_{\text{lex}}$. There are $10 = \binom{5}{3}$ minors. To check that they form a Gröbner basis we have to check $45 = \binom{10}{2}$ S-pairs. Changing slightly the focus in Buchberger's criterion one can get away with 15 tests only.

We are going to explain how this works next.

Definition. Let $I, J \subset R$ be ideals in a ring. Then the **colon ideal** is

$$I : J = \{r \in R \mid rJ \subset I\}.$$

part 2

A second version of Buchberger's criterion

Notation. Let $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ be polynomials. We define $r-1$ monomial ideals as follows

$$M_j = (\mathrm{Lt}(f_1, \ldots, \mathrm{Lt}(f_{j-1})) : \mathrm{Lt}(f_j)$$

for $j = 2, \ldots, r$.
For each minimal generator $x^\alpha \in M_j$ the multiple $x^\alpha f_j$ is an expression not allowed in the division theorem by condition 2a).

Theorem. *With notation as above, $f_1, \ldots, f_r$ is a Gröbner basis for $(f_1, \ldots, f_r)$ if and only if for each $j = 2, \ldots, r$ and each minimal generator x^α of M_j the remainder of $x^\alpha f_j$ divided by $f_1, \ldots, f_r$ is zero.*

Example: 3×3-minors of a 3×5-matrix, 2

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 \\ y_1 & y_2 & y_3 & y_4 & y_5 \\ z_1 & z_2 & z_3 & z_4 & z_5 \end{pmatrix}$$

j	$\mathrm{Lt}(f_j)$	M_j
1	$x_1 y_2 z_3$	0
2	$x_1 y_2 z_4$	(z_3)
3	$x_1 y_3 z_4$	(y_2)
4	$x_2 y_3 z_4$	(x_1)
5	$x_1 y_2 z_5$	(z_3, z_4)
6	$x_1 y_3 z_5$	(y_2, z_4)
7	$x_2 y_3 z_5$	(x_1, z_4)
8	$x_1 y_4 z_5$	(y_2, y_3)
9	$x_2 y_4 z_5$	(x_1, y_3)
10	$x_3 y_4 z_5$	(x_1, x_2)

$$0 = \det \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \\ z_1 & z_2 & z_3 & z_4 \end{pmatrix}$$

$$\Longrightarrow \; z_3 f_2 = z_4 f_1 + z_2 f_3 - z_1 f_4 + 0.$$

Similarly, all other remainders are zero.

Hence $f_1, \ldots, f_{10}$ is a Gröbner basis.

Modules

For our proof of Buchberger's criterion we need the concept of modules and division with remainder in free modules.

Definition. Let R be a ring. An R-**module** M is an abelian group together with an operation

$$R \times M \to M, (a, m) \mapsto am$$

satisfying the usual associativity and distributivity laws:

$$a(bm) = (ab)m \quad \forall a, b \in R \; \forall m \in M$$

$$1m = m \quad \forall m \in M$$

$$(a + b)m = am + bm \quad \forall a, b \in R \; \forall m \in M$$

$$a(m + n) = am + an \quad \forall a \in R \; \forall m, n \in M$$

For a field K a K-module is simply a K-vector space.

Examples of modules

R is an R-module.

A free module is module of the form $F = R^r$. It has basis vectors $e_j = (0, \ldots, 1, \ldots, 0)^t$ with 1 in the j-th position. An element of F is simply a column vector

$$(a_1, \ldots, a_r)^t = \sum a_j e_j$$

with entries in R.

A submodule $N \subset M$ of a module M is a subgroup N satisfying

$$n \in N \Rightarrow an \in N \quad \forall a \in R \, \forall n \in N.$$

Thus an ideal I is a submodule of R.

If $f_1, \ldots f_r \in M$ then

$$(f_1 \ldots, f_r) = \{g_1 f_1 + \ldots + g_r f_r \mid g_j \in R\}$$

is a submodule of M.

Homomorphism

An R-**module homomorphism** $\varphi\colon M \to N$ is a group homomorphism satisfying additionally $\varphi(am) = a\varphi(m)$.

$\ker\varphi$ is a submodule of M and $\mathrm{im}(\varphi)$ is a submodule of N.

To say that a module is generated by elements $f_1, \dots, f_r \in M$ is equivalent to say that

$$\varphi : F = R^r \to M, e_j \mapsto f_j$$

defines a surjective R-module homomorphism.

Definition. A **syzygy** between elements $f_1, \dots, f_r \in M$ is an element $(g_1, \dots, g_r)^t \in F = R^r$ satisfying $\sum g_j f_j = 0$.
In other words, it is an element of $\ker\varphi$ where $\varphi : F = R^r \to M$ is defined by $e_j \mapsto f_j$.

Quotient modules

Let $N \subset M$ be a submodule. Then

$$f \equiv g \mod N :\Leftrightarrow f - g \in N$$

defines an equivalence relation on M with equivalence classes

$$f + N = \{f + h \mid h \in N\}.$$

The set of equivalence classes

$$M/N = \{f + N \mid f \in M\} \subset 2^M$$

carries a unique R-module structure such that

$$\pi \colon M \to M/N, f \mapsto f + N$$

becomes an R-module homomorphism.

Homomorphism theorem

Theorem. *Let* $\varphi\colon M \to N$ *be an* R*-module homomorphism. Then*

$$\operatorname{im}(\varphi) \cong M/\ker(\varphi).$$

Proof. $f + \ker(\varphi) \mapsto \varphi(f)$ is a well-defined isomorphism.

For $\varphi\colon M \to N$ we define the **cokernel** of φ as

$$\operatorname{coker}(\varphi) = N/\operatorname{im}(\varphi).$$

Finitely presented modules

Definition. An R-module M is **finitely generated** if there exists a surjection

$$\varphi : R^r \to M$$

M is **finitely presentable**, if one can choose the surjection $\varphi : R^r \to M$ such that the syzygy module $\ker(\varphi)$ is finitely generated as well. In that case we obtain a sequence

$$R^s \xrightarrow{\varphi_1} R^r \xrightarrow{\varphi} M \longrightarrow 0$$

with $\mathrm{im}(\varphi_1) = \ker(\varphi)$ and $M \cong \mathrm{coker}(\varphi_1)$. Such sequence is called a **finite presentation** of M.

Since a homomorphism $R^s \to R^r$ between free modules can be described by $r \times s$-matrices with entries in R we can simply specify a finitely presented module via a matrix φ_1.

Tasks of constructive module theory

Not so easy are the following tasks: Given two finitely presented modules

$$R^s \xrightarrow{\varphi_1} R^r \longrightarrow M \longrightarrow 0$$

and

$$R^\ell \xrightarrow{\psi_1} R^k \longrightarrow N \longrightarrow 0\ ,$$

1. decide whether M and N are isomorphic,
2. compute the R-module $\mathrm{Hom}(M, N)$ of all R-module homomorphisms.

We will approach these questions in case of $R = K[x_1, \ldots, x_n]$ using Gröbner basis for submodules of free modules.

part 4