Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today's topic is constructive ideal and module theory.

1. Intersection of ideals
2. Syzygies
3. $I : J$
4. Elimination and kernels of ring homomorphisms
5. Homomorphism between finitely presented modules

Intersection of ideals

Let $I, J \subset S = K[x_1, \dots, x_n]$ be ideals. We want to compute their intersection.

Algorithm.

Input. $f_1, \dots, f_r$ generators of the ideal I,
$g_1, \dots, g_s$ generators of the ideal J.

Output. Generators of the ideal $I \cap J$.

1. Form the matrix
$$\varphi = \begin{pmatrix} 1 & f_1 & \dots & f_r & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 & g_1 & \dots & g_s \end{pmatrix}$$
2. Compute the syzgy matrix $\psi = (h_{ij})$ whose columns generate the kernel
$$\ker(\varphi : S^{r+s+1} \to S^2).$$
3. Return the entries of the first row
$$h_{11}, h_{12}, \dots, h_{1t}$$
of the $(r + s + 1) \times t$-matrix ψ.

Proof of correctness

The equation

$$\begin{pmatrix} 1 & f_1 & \dots & f_r & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 & g_1 & \dots & g_s \end{pmatrix} \begin{pmatrix} h_{1j} \\ h_{2j} \\ \vdots \\ h_{(r+s+1),j} \end{pmatrix} = 0$$

shows that h_{1j} is both a linear combination of the f_i's and the g_i's. Hence $h_{1j} \in I \cap J$. Conversely, if $h \in I \cap J$, then

$$h = h_1 f_1 + \ldots + h_r f_r = h'_1 g_1 + \ldots + h'_s g_s$$

for suitable h_i and h'_j. Hence the vector

$$(h, -h_1, \ldots, -h_r, -h'_1, \ldots, h'_s)^t \in \ker(\varphi).$$

Since the kernel is generated by the columns of ψ we obtain that h is a linear combination of $h_{11}, h_{12}, \ldots, h_{1t}$. □

Computation of syzygies

Let $S = K[x_1, \ldots, x_n]$ be the polynomial ring and $F = S^s$ be a free S-module.

Algorithm.

Input. Vectors $f_1, \ldots, f_r \in F$

Output. A matrix $\psi \in S^{r \times t}$ whose columns generate the kernel of the S-module homomorphism

$$\varphi : S^r \to F, e_i \mapsto f_i.$$

1. Choose a monomial order on F and compute a Gröbner basis $f_1, \ldots, f_r, f_{r+1}, \ldots, f_{r'}$ of $(f_1, \ldots, f_r)$, while keeping track of the Buchberger test syzgies $G^{(i,\alpha)}$.
2. Sort the $G^{(i,\alpha)}$ such that the test syzygies which produced new GB elements come first.

Computation of syzygies

3. The matrix with columns $G^{(i,\alpha)}$ has now shape

$$\psi' = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \text{ with } C = \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$

   a $(r'-r) \times (r'-r)$ upper triangular square matrix 1's on the diagonal. Return

$$\psi = B - AC^{-1}D.$$

Note that one can compute C^{-1} by applying row operations to the matrix $(E|C)$ to obtain $(C'|E)$. The inverse matrix $C' = C^{-1}$ has entries in S.

Proof of correctness

ψ' is a $r' \times (r' - r + t)$-matrix whose columns generate the kernel of the map

$$\varphi' : S^{r'} \to F, e_i \mapsto f_i$$

since the $G^{(i,\alpha)}$ form a Gröbner basis of $\ker(\varphi')$. Multiplying

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \text{ with } \begin{pmatrix} E_{r'-r} & -C^{-1}D \\ 0 & E_t \end{pmatrix}$$

yields

$$\widetilde{\psi}' = \begin{pmatrix} A & B - AC^{-1}D \\ C & 0 \end{pmatrix}$$

whose columns still generate $\ker(\varphi')$. Elements of $\ker(\varphi)$ correspond to elements of $\ker(\varphi')$ of shape

$$(h_1, \ldots, h_r, 0 \ldots, 0)^t.$$

Such an element is a linear combination of the last t columns of $\widetilde{\psi}'$ because of the upper triangular shape of C. Thus the columns of $\psi = B - AC^{-1}D$ generate $\ker(\varphi)$. □

$I : J$

Algorithm.

Input. $f_1, \dots, f_r$ generators of the ideal I,
$g_1, \dots, g_s$ generators of the ideal J.

Output. Generators of the ideal $I : J$.

1. Form the $s \times (rs+1)$-matrix

$$\varphi = \begin{pmatrix} g_1 & f_1 & \dots & f_r & & & & & & 0 \\ g_2 & & & & f_1 & \dots & f_r & & & \\ \vdots & & & & & & \ddots & & & \\ g_s & 0 & & & & & & f_1 & \dots & f_r \end{pmatrix}.$$

2. Compute the syzgy matrix $\psi = (h_{ij})$ whose columns generate the kernel

$$\ker(\varphi : S^{rs+1} \to S^s).$$

3. Return the entries of the first row $h_{11}, h_{12}, \dots, h_{1t}$ of the $(rs+1) \times t$-matrix ψ.

□

Elimination

Given an ideal $I \subset K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ we want to compute $I \cap K[y_1, \ldots, y_m]$. This can be done by computing a GB with respect to $>_{lex}$. However this computes the whole flag of elimination ideals. Using a product order is often cheaper.

Definition. Let $>_1$ be a global monomial order on $K[x_1, \ldots, x_n]$ and $>_2$ a global monomial order on $K[y_1, \ldots, y_m]$. Then the **product order** ($>_{12}$) **on** $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ is defined by

$$x^\alpha y^\beta >_{12} x^{\alpha'} y^{\beta'} \text{ iff } x^\alpha >_1 x^{\alpha'} \text{ or}$$
$$x^\alpha = x^{\alpha'} \text{ and } y^\beta >_2 y^{\beta'}.$$

This order has the key property that

$$\mathrm{Lt}(f) \in K[y_1, \ldots, y_m] \implies f \in K[y_1, \ldots, y_m]$$

holds.

Elimination

Algorithm.
Input. $f_1, \dots, f_r$ generators of an ideal
$I \subset K[x_1, \dots, x_n, y_1, \dots, y_m]$.
Output. A Gröbner basis of $I \cap K[y_1, \dots, y_m]$.

1. Compute a Gröbner basis $f_1 \dots, f_{r'}$ of $(f_1, \dots, f_r)$ with respect to a product order.
2. Return all Gröbner basis elements f_j with

$$\mathrm{Lt}(f_j) \in K[y_1, \dots, y_m].$$

Proof. An element $f \in K[y_1, \dots, y_m]$ lies in I iff the remainder under division by $f_1 \dots, f_{r'}$ is zero. This division involves only the Gröbner basis elements which we return. $\square$

Kernel of a ring homomorphism

Let $\varphi : K[y_1, \ldots, y_m] \to K[x_1, \ldots, x_n]/I, y_i \mapsto \overline{g}_i$ be a substitution homomorphism. We want to compute $\ker(\varphi)$.

Algorithm.

Input. $f_1, \ldots, f_r$ generators of the ideal I

$g_1, \ldots, g_m$ representatives of the $\overline{g}_i$.

Output. A Gröbner basis of $\ker(\varphi)$.

1. Consider the ideal J generated by $f_1, \ldots, f_r$ and $y_1 - g_1, \ldots, y_m - g_m$ in $K[x_1, \ldots, x_n, y_1, \ldots, y_m]$
2. Compute a Gröbner basis of J with respect to a product order and return the Gröbner basis elements with lead terms in $K[y_1, \ldots, y_m]$.

Proof. Let $F \in K[y_1, \ldots, y_m]$ be an element of the kernel, i.e.,

$$F(g_1, \ldots, g_m) \in I \iff F \in J \subset K[x_1, \ldots, x_n, y_1, \ldots, y_m].$$

Thus $\ker(\varphi) = J \cap K[y_1, \ldots, y_m]$ and a Gröbner basis is obtained by computing a GB of J with respect to $>_{12}$. □

Geometric interpretation

Suppose $K[x_1,\ldots,x_n]/I = K[A]$ is the coordinate ring of an algebraic set $A \subset \mathbb{A}^n$ and $(\overline{g}_1,\ldots,\overline{g}_r)$ are the components of a morphism

$$\phi : A \to \mathbb{A}^m.$$

Then the kernel J of $\varphi : K[y_1,\ldots,y_m] \to K[x_1,\ldots,x_n]/I$ is a radical ideal.

Indeed,

$$\begin{aligned} F \in \mathrm{rad}(J) &\implies F^N \in J \text{ for some N} \\ &\implies \varphi(F^N) = 0 \\ &\implies (F(g_1,\ldots,g_m))^N \in I \\ &\implies F(g_1,\ldots,g_m) \in I \text{ because } I \text{ is a radical ideal} \\ &\implies F \in \ker(\varphi) = J. \end{aligned}$$

$B = V(J) \subset \mathbb{A}^m$ is the Zariski closure $B = \overline{\phi(A)}$ of the image $\phi(A)$.

Description of module homomorphisms

Let $\varphi : M \to N$ be a homomorphism between two finitely presented $R = K[x_1, \ldots, x_n]$-modules. Then φ can be lifted to a commutative diagram between the presentations

$$\begin{array}{ccccccc}
R^{r_1} & \xrightarrow{\phi} & R^{r_0} & \longrightarrow & M & \longrightarrow & 0 \\
\downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \varphi} & & \\
R^{s_1} & \xrightarrow{\psi} & R^{s_0} & \longrightarrow & N & \longrightarrow & 0.
\end{array}$$

Here M is a module with r_0 generators $m_1, \ldots, m_{r_0}$ which are the image of the basis $e_1, \ldots, e_{r_0}$ and the columns of the matrix ϕ generate the kernel $\ker(R^{r_0} \to M)$. Thus $M = \text{coker}(\phi)$. Similarly, $N = \text{coker}(\psi)$.

To obtain φ_0 we choose a preimage $f_i \in R^{s_0}$ of $\varphi(m_i)$ and define

$$\varphi_0 = (f_1 | \ldots | f_{r_0})$$

to be the $s_0 \times r_0$-matrix with column vectors f_i.

Description of module homomorphisms

Proposition. *A* $s_0 \times r_0$*-matrix* φ_0 *induces a well-defined R-module homomorphism* $\varphi : M \to N$ *if and only if* φ_0 *can be completed to a commutative diagram*

$$\begin{array}{ccc} R^{r_1} & \xrightarrow{\phi} & R^{r_0} \\ \Big\downarrow {\scriptstyle \exists\varphi_1} & & \Big\downarrow {\scriptstyle \varphi_0} \\ R^{s_1} & \xrightarrow{\psi} & R^{s_0} \end{array}$$

Proof. φ_0 induces a well-defined map $\varphi : M \to N$ iff the composition

$$\begin{array}{ccc} R^{r_1} \xrightarrow{\phi} & R^{r_0} & \\ & \Big\downarrow {\scriptstyle \varphi_0} & \\ & R^{s_0} & \longrightarrow N \end{array}$$

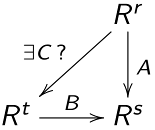
is zero. Since $R^{s_1} \xrightarrow{\psi} R^{s_0} \longrightarrow N \longrightarrow 0$

is exact at R^{s_0}, this is the case iff $\text{im}(\varphi_0 \circ \phi) \subset \text{im}(\psi)$

$\iff \exists\varphi_1$ with $\varphi_1 \circ \psi = \varphi_0 \circ \phi$, since R^{r_1} is free. $\square$

Lifting

Given two matrices A and B we want to decide whether A can be factor over B, i.e., whether there exists a matrix C with $A = BC$



If C exists then C is called a **lifting of A along B.**

Algorithm. Can A be factored over B?
Input. Matrices $A \in R^{s \times r}$ and $B \in R^{s \times t}$ over $R = K[x_1, \ldots, x_n]$.
Output. A boolean value, and in case of **true** a matrix $C \in R^{t \times r}$ such that $A = BC$.

1. Compute a Gröbner basis of the column vectors $a_1, \ldots, a_r$ of A.
2. Divide each column vector b_j of B by the Gröbner basis. If one of the remainders is non-zero return **false**.

Lifting

3. If all remainders are zero, express the b_i as a linear combination of the original generators $a_1, \ldots, a_r$ of the image $\mathrm{im}(A)$:

$$b_i = \sum_{j=1}^{r} c_{ij} a_j .$$

4. Return **true** and $C = (c_{ij})$.

Using this algorithm we can decide whether a matrix φ_0 induces a well-defined homomorphism $\varphi : M \to N$

$$\begin{array}{ccccccc}
R^{r_1} & \xrightarrow{\phi} & R^{r_0} & \longrightarrow & M & \longrightarrow & 0 \\
& \searrow & \downarrow \varphi_0 & & & & \\
R^{s_1} & \xrightarrow{\psi} & R^{s_0} & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

by computing a lifting φ_1 of $\varphi_0 \phi$ along ψ.

Cokern and image of an R-module homomorphism

Given a homomorphism $\varphi : M \to N$ represented by a matrix φ_0

$$\begin{array}{ccccccc} R^{r_1} & \xrightarrow{\phi} & R^{r_0} & \longrightarrow & M & \longrightarrow & 0 \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \varphi} & & \\ R^{s_1} & \xrightarrow{\psi} & R^{s_0} & \longrightarrow & N & \longrightarrow & 0 \end{array}$$

we will descibe presentations of coker(φ), im(φ) and ker(φ). We have presentations

$$R^{r_0} \oplus R^{s_1} \xrightarrow{(\varphi_0|\psi)} R^{s_0} \longrightarrow \operatorname{coker}(\varphi) \longrightarrow 0$$

and

$$R^{t_0} \oplus R^{r_1} \xrightarrow{(A|\phi)} R^{r_0} \longrightarrow \operatorname{im}(\varphi) \longrightarrow 0$$

where A is part of the syzygy matrix $\begin{pmatrix} A \\ B \end{pmatrix}$ of $(\varphi_0|\psi)$:

$$R^{t_0} \xrightarrow{\binom{A}{B}} R^{r_0} \oplus R^{s_1} \xrightarrow{(\varphi_0|\psi)} R^{s_0}.$$

Kernel of an R-module homomorphism

The computation of the presentation of $\ker(\varphi)$ takes more steps:

1. Compute the syzygy matrix $\begin{pmatrix} A \\ B \end{pmatrix}$ of $(\varphi_0|\psi)$:
$$R^{t_0} \xrightarrow{\binom{A}{B}} R^{r_0} \oplus R^{s_1} \xrightarrow{(\varphi_0|\psi)} R^{s_0}.$$
2. Compute the syzygy matrix $\begin{pmatrix} C \\ D \end{pmatrix}$ of $(A|\phi)$:
$$R^{t_1} \xrightarrow{\binom{C}{D}} R^{t_0} \oplus R^{r_1} \xrightarrow{(A|\phi)} R^{r_0}.$$
3. Then C is the presentation matrix of $\ker(\varphi)$:
$$R^{t_1} \xrightarrow{C} R^{t_0} \longrightarrow \ker(\varphi) \longrightarrow 0.$$

Proof of correctness

We have a commutative diagram

$$\begin{array}{ccccccc}
R^{t_1} & \xrightarrow{C} & R^{t_0} & \longrightarrow & \operatorname{coker}(C) & \longrightarrow & 0 \\
\Big\downarrow{\scriptstyle -D} & & \Big\downarrow{\scriptstyle A} & & \Big\downarrow{\scriptstyle \iota} & & \\
R^{r_1} & \xrightarrow{\phi} & R^{r_0} & \longrightarrow & M & \longrightarrow & 0 \\
\Big\downarrow{\scriptstyle \varphi_1} & & \Big\downarrow{\scriptstyle \varphi_0} & & \Big\downarrow{\scriptstyle \varphi} & & \\
R^{s_1} & \xrightarrow{\psi} & R^{s_0} & \longrightarrow & N & \longrightarrow & 0
\end{array}$$

The map ι induced by A maps into the $\ker(\varphi)$ because $\varphi_0 A$ induces the zero map as $\varphi_0 A = -\psi B$.
$\iota : \operatorname{coker}(C) \to \ker(\varphi)$ is surjective: An element of

$$f \in R^{r_0} \text{ maps to } 0 \in N \iff \varphi_0(f) \in \operatorname{im}(\psi).$$

Such element is of the form $f = Ag$ because $\begin{pmatrix} A \\ B \end{pmatrix}$ is the syzygy matrix of $(\varphi_0|\psi)$. This also shows that the description of $\operatorname{im}(\varphi) \cong \operatorname{coker}(A|\phi)$ above is correct.

Proof of correctness continued

$\iota : \mathrm{coker}(C) \to \ker(\varphi)$ is injective: An element

$$g \in R^{t_0} \text{ maps to } 0 \in M \iff Ag \in \mathrm{im}(\phi).$$

These elements are of the form Ch for some $h \in R^{t_1}$ because $\begin{pmatrix} C \\ D \end{pmatrix}$ is the syzygy matrix of $(A|\phi)$. Hence $g \mapsto 0 \in \mathrm{coker}(C)$.

We conclude that

$$\iota : \mathrm{coker}(C) \to \ker(\varphi)$$

is an isomorphism. □