Groebner Basics

Talk given at the Special Semester
on Groebner Bases Linz 2006

Hans-Gert Gräbe,
Dept. Computer Science, Univ. Leipzig, Germany
`http://www.informatik.uni-leipzig.de/~graebe`

February 27, 2006

Notations

k a (computationally feasible) field

K/k alg. closed extension

$R = k[x_1, \ldots, x_n] = k[\mathbf{x}]$ the ring of polynomials over k

$\mathbb{A}^n := \{(a_1, \ldots, a_n) : a_i \in K\}$ the n-dim. *affine space*

$B = \{f_1, \ldots, f_s\} \subset S$ a (finite) system of polynomials

$V = V(B) := \{\mathbf{a} \in \mathbb{A}^n \ : \ f_i(\mathbf{a}) = 0 \ \forall\, i\}$
the set of common zeroes.
Such a set $V \subset \mathbb{A}^n$ is an *affine variety*.

$I = Id(B)$ the ideal generated by B.
We have $V(B) = V(Id(B))$.

Monomial $\mathbf{x}^\alpha = x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}, \quad \alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$

The set of terms

$$T = T(\mathbf{x}) = T(x_1, \ldots, x_n) = \{\mathbf{x}^\alpha \ : \ \alpha \in \mathbb{N}^n\}$$

is a semigroup with unit $1 = \mathbf{x}^0$, the *term monoid*.

A *polynomial* in $x_1, \ldots, x_n$ over k is a finite k-linear (i.e., $c_\alpha \in k$) combination of terms $f = \sum c_\alpha \mathbf{x}^\alpha$.

This representation is called *distributive* and can be computed with `expand` in most of the CAS.

It is unique, i.e., a *canonical representation*, if the coefficients are (representable and) represented in canonical form and the order of summands is fixed.

To fix that order one defines a total ordering $<$ on $T(\mathbf{x})$ that is additionally *monotone*

$$s < t \Rightarrow s \cdot u < t \cdot u \quad \text{for all } s, t, u \in T(\mathbf{x})$$

Such an ordering is called a *term ordering*.

Many sources require additionally that $<$ is a well ordering, i.e., the two equivalent conditions hold

(a) Each subset $M \subset T$ has a smallest element.
(b) All strictly descending chains $t_1 > t_2 > \ldots$ in T are finite.

We call such term orderings *Noetherian term orderings*.

Lexicographical ordering (lex) with $x_1 > x_2 > \ldots > x_n$

$$x_1^{a_1} x_2^{a_2} \cdot \ldots \cdot {x_n}^{a_n} >_{\text{lex}} x_1^{b_1} x_2^{b_2} \cdot \ldots \cdot {x_n}^{b_n}$$
$$\Leftrightarrow \begin{cases} a_1 > b_1 & \text{or} \\ a_1 = b_1 & \text{and } x_2^{a_2} \cdot \ldots \cdot {x_n}^{a_n} >_{\text{lex}} x_2^{b_2} \cdot \ldots \cdot {x_n}^{b_n} \end{cases}$$

Reverse lexicographical ordering (revlex) with $x_1 < x_2 < \ldots < x_n$

$$x_1^{a_1} \cdot \ldots \cdot {x_{n-1}}^{a_{n-1}} {x_n}^{a_n} >_{\text{revlex}} x_1^{b_1} \cdot \ldots \cdot {x_{n-1}}^{b_{n-1}} {x_n}^{b_n}$$
$$\Leftrightarrow \begin{cases} a_n < b_n & \text{or} \\ a_n = b_n & \text{and } x_1^{a_1} \cdot \ldots \cdot {x_{n-1}}^{a_{n-1}} >_{\text{revlex}} x_1^{b_1} \cdot \ldots \cdot {x_{n-1}}^{b_{n-1}} \end{cases}$$

Degree ordering (wrt. the standard grading)

$$x_1^{a_1} \cdot \ldots \cdot {x_n}^{a_n} >_{\text{deg}xxx} x_1^{b_1} \cdot \ldots \cdot {x_n}^{b_n}$$
$$\Leftrightarrow \begin{cases} \text{deg}(\mathbf{a}) > \text{deg}(\mathbf{b}) & \text{or} \\ \text{deg}(\mathbf{a}) = \text{deg}(\mathbf{b}) & \text{and } x_1^{a_1} \cdot \ldots \cdot {x_n}^{a_n} >_{\text{xxx}} x_1^{b_1} \cdot \ldots \cdot {x_n}^{b_n} \end{cases}$$

xxx is another term ordering, the *tie-breaking* ordering.

Widespread used are the *degree lexicographic* (deg-lex) and the *degree reverse lexicographic* (deg-revlex) term orderings.

The lexicographic and all degree orderings are Noetherian.

The pure revlex ordering is not Noetherian, since

$$x_1 > x_1^2 > x_1^3 > \ldots$$

is an infinitely strictly descending chain of terms.

A term ordering $(T(\mathbf{x}), >)$ *is Noetherian iff*
(c) $m > 1$ *for all* $m \in T, m \neq 1$*.*

Characterization of Term Orderings

$\widetilde{T} = \{\mathbf{x}^\alpha \ : \ \alpha \in \mathbb{Z}^n\}$ is the set of *generalized terms*. A term ordering $<$ can be extended to $\widetilde{T}$.

$<$ is characterized by its *positivity cone*

$$C_+ = \left\{\mathbf{x}^\alpha \in \widetilde{T} \ : \ \mathbf{x}^\alpha > 1\right\}$$

This cone is a half space supported by a (uniquely defined) linear functional $w \in (\mathbb{Z}^n)^* \cong \mathbb{R}^n$. We say that w is the *weight vector* of $<$ and $<$ *refines* w.
w is uniquely determined by the row vector

$$(w(x_1), \ldots, w(x_n)).$$

We write shortly $w(\mathbf{x}^\alpha) = w(\alpha)$.

Theorem (Characterization of Term Orderings)
A term ordering can be described by a sequence of weight vectors $w_1, w_2, \ldots, w_k \in \mathbb{R}^n$ *such that for* $\mathbf{x}^\alpha \in \widetilde{T}$

$$\mathbf{x}^\alpha > 1 \Leftrightarrow \exists j < k : w_i(\alpha) = 0 \text{ for } i \leq j \text{ and } w_{j+1}(\alpha) > 0$$

w_1 is uniquely defined, w_j only upto multiples of w_i, $i < j$.

Hence any term ordering can be given as *matrix term ordering* where the weights of the variables wrt. w_i are the entries of row i of the *weight matrix*.

A term order is Noetherian iff the first non zero entry in each column of the weight matrix is positive.

Weight Matrices for the Standard Term Orderings

$>_{\text{lex}}$: $\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & 1 \end{pmatrix}$

$>_{\text{deglex}}$: $\begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ & & \dots & & \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$

$>_{\text{revlex}}$: $\begin{pmatrix} 0 & \dots & 0 & -1 \\ 0 & \dots & -1 & 0 \\ & & \dots & \\ -1 & \dots & 0 & 0 \end{pmatrix}$

$>_{\text{degrevlex}}$: $\begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 0 & 0 & \dots & 0 & -1 \\ 0 & 0 & \dots & -1 & 0 \\ & & \dots & & \\ 0 & -1 & \dots & 0 & 0 \end{pmatrix}$

Given a **finite** set $\mathbf{\Sigma} \subset \widetilde{T} \setminus \{1\}$ consider the set

$$W_{\mathbf{\Sigma}} = \{w \in \mathbb{R}^n \ : \ \forall \mathbf{x}^\alpha \in \mathbf{\Sigma} \ w(\alpha) > 0\}$$
$$= \bigcap_{\mathbf{x}^\alpha \in \mathbf{\Sigma}} \{w \in \mathbb{R}^n \ : \ w(\alpha) > 0\}$$

This is the set of all weight vectors w such that for all refinements $<$ of w the terms from $\mathbf{\Sigma}$ are positive. As a finite intersection of open halfspaces this set is either empty or an open cone and hence n-dimensional. The closure of that cone is dual to the cone spanned by the $\mathbf{x}^\alpha \in \mathbf{\Sigma}$ in $\mathbb{Z}^n$.

For $\mathbf{\Sigma} = \{x_1, \ldots, x_n\}$ we get exactly the cone of Noetherian term orderings. Since $w = (11 \ldots 1)$ is in the interior part of that cone all refinements of w are Noetherian.

PP-Ideals and Monoid Ideals. Dickson's Lemma

An ideal $I \subset R$ is a *PP-ideal*, iff

$$f = \sum c_\alpha \mathbf{x}^\alpha \in I \Rightarrow \forall\, \alpha \;\; (c_\alpha \neq 0 \Rightarrow \mathbf{x}^\alpha \in I)\,.$$

The set Σ of all $\mathbf{x}^\alpha \in I$ form a *monoid ideal*, i.e., a subset of T with

$$\Sigma \cdot T := \{\mathbf{x}^\alpha \cdot \mathbf{x}^\beta \,:\, \mathbf{x}^\alpha \in \Sigma,\, \mathbf{x}^\beta \in T\} \subset \Sigma.$$

A subset $\Sigma_0 = \{\mathbf{x}^{a_1}, \ldots, \mathbf{x}^{a_m}\}$ of a monoid ideal Σ is a *basis*, if $\Sigma_0 \cdot T = \Sigma$, and a *minimal basis*, if additionally Σ_0 is minimal wrt. inclusion and that property.

A monomial ideal $\Sigma \subset T$ has a uniquely determined minimal basis $Gen(\Sigma)$.

This minimal basis contains exactly the minimal wrt. term divisibility $\mathbf{x}^\alpha \in \Sigma$, i.e., with the property

$$\mathbf{x}^\beta \in \Sigma, x^\beta \,|\, \mathbf{x}^\alpha \;\Rightarrow\; x^\beta = \mathbf{x}^\alpha.$$

Theorem (Dickson's Lemma)
Each monomial ideal $\Sigma \subset T$ has a finite basis.

This theorem holds for term monoids with finitely many variables.

Normal Forms

Fix a representation $0 \neq f(\mathbf{x}) = \sum_{i=0}^{N} c_i \mathbf{x}^{\alpha_i} \in R$ with $\mathbf{x}^{\alpha_i} > \mathbf{x}^{\alpha_j}$ for $i < j$ and all $c_i \neq 0$.

We denote

the term set $T(f) := \{\mathbf{x}^\alpha : c_\alpha \neq 0\}$,
the leading term $lt(f) := \mathbf{x}^{\alpha_0}$,
the leading coefficient $lc(f) := c_0$,
the leading monomial $lm(f) := lc(f) \cdot lt(f)$,
the reductum $red(f) := f - lm(f)$.

Main idea: Substitute larger terms by smaller ones, i.e., convert polynomial relations $f \in R$ into (algebraic) substitution rules

$$lt(f) \mapsto -lc(f)^{-1}\, red(f).$$

Example:

$$B_1 = \{f_1 = x^2 + xy + y^2, f_2 = xz + yz, f_3 = y^3 - z^3\}$$

yields the rule system (wrt. $<_{lex}$)

$$x^2 \mapsto -xy - y^2,\ xz \mapsto -yz,\ y^3 \mapsto z^3.$$

If we apply these rules in the given order to the polynomial

$$g = x^2y^2 + x^2z^2 + y^2z^2,$$

we get step by step

$$\begin{aligned}
g &\mapsto x^2z^2 - xy^3 - y^4 + y^2z^2 \\
&\mapsto -xy^3 - xyz^2 - y^4 \\
&\mapsto -xyz^2 - xz^3 - y^4 \\
&\mapsto -xz^3 - y^4 + y^2z^2 \\
&\mapsto -y^4 + y^2z^2 + yz^3 \\
&\mapsto y^2z^2
\end{aligned}$$

For $B = \{f_1, \dots, f_m\} \subset R \setminus \{0\}$ define

$$\Sigma(B) := \{x^\alpha \ : \ \exists\, f \in B : lt(f) \,|\, x^\alpha\}$$

Each term from $\Sigma(B)$ can be reduced applying one of the rules obtained from B by smaller terms. $t \in \Sigma(B)$ is called *non standard term* and $t \in T(X) \setminus \Sigma(B)$ is called *standard term*.

$Lt(B)$ denotes the PP-ideal generated by $\Sigma(B)$.

NF(f:polynomial, B:basis):polynomial

Input: Polynomial $f \in R$, finite set $B \subset R$.

Output: Polynomial $f' \in R$ with $f \equiv f' \pmod{B}$ and $f' = 0$ or $lt(f') \notin \Sigma(B)$.

while $(f \neq 0)$ **and** $(M := \{b \in B : lt(b) \,|\, lt(f)\} \neq \emptyset)$ **do**

 choose $b \in M$

 $f := f - \frac{lm(f)}{lm(b)} b$

return f

The algorithm terminates for Noetherian term orderings.

The result (and the time) of a normal form computation may depend on the *reduction path*.

Since $f \equiv NF(f, B)$ (mod B) this gives a first half answer to the ideal membership problem

$$\boxed{\textit{If } NF(f,B) = 0 \textit{ then } f \in Id(B).}$$

The algorithm can be refined to an Extended Division Algorithm.

$$
\begin{aligned}
g \mapsto g_1 &= g - y^2 f_1 &&= x^2z^2 - xy^3 - y^4 + y^2z^2 \\
\mapsto g_2 &= g_1 - z^2 f_1 &&= -xy^3 - xyz^2 - y^4 \\
\mapsto g_3 &= g_2 + x\, f_3 &&= -xyz^2 - xz^3 - y^4 \\
\mapsto g_4 &= g_3 + y\, z\, f_2 &&= -xz^3 - y^4 + y^2z^2 \\
\mapsto g_5 &= g_4 + z^2 f_2 &&= -y^4 + y^2z^2 + yz^3 \\
\mapsto g_6 &= g_5 + y\, f_3 &&= y^2z^2 = g'
\end{aligned}
$$

yields $g = (y^2+z^2)f_1+(-y\,z-z^2)f_2+(-x+y)f_3+g'$.

NFwithRelations(f:polynomial, B:basis):
(polynomial, vector of polynomials)

Input: Polynomial $f \in R$, finite set $B = \{b_1, \ldots, b_m\} \subset R$

Output: Polynomial $f' \in R$ with $f' = 0$ or $lt(f') \notin \Sigma(B)$
and vector $v = (v_1, \ldots, v_m)$ with $f = \sum_i v_i\, b_i + f'$.

for $i = 1, \ldots, m$ **do** $v_i := 0$
while ($f \neq 0$) **and** ($M := \{b \in B : lt(b) \,|\, lt(f)\} \neq \emptyset$) **do**
  choose $b_i \in M$
  $f := f - \frac{lm(f)}{lm(b_i)} b_i$
  $v_i := v_i + \frac{lm(f)}{lm(b_i)}$
return (f, v)

This representation v has a special property; it avoids large intermediate terms.

For a finite set $B = \{b_1, \ldots, b_m\} \subset R$ *and a polynomial* $f \in R$ *the algorithm* **NFwithRelations** *returns after a finite number of steps a representation*

$$f = v_1\, b_1 + \ldots + v_m\, b_m + r$$

with $v_1, \ldots, v_m, r \in R$ *and* $r = 0$ *or* $lt(r) \notin \Sigma(B)$ *and* $lt(f) \geq lt(v_i)\, lt(b_i)$ *for all* i*.*

NF can be applied recursively to terms in $red(f)$, too. This yields a presentation $f \equiv \sum r_\alpha \mathbf{x}^\alpha \pmod{B}$ as linear combination of standard terms.

TNF(f:polynomial, B:basis):polynomial

Input: Polynomial $f \in R$, finite set $B \subset R$

Output: Polynomial $f' \in R$ with $f \equiv f' \pmod{Id(B)}$ and $f' = 0$ or $T(f') \cap \Sigma(B) = \emptyset$

`f:=NF(f,B)`

`if` $f = 0$ **`then return`** f

`else return` $lm(f) + TNF(red(f), B)$

The algorithm terminates for Noetherian term orderings.

$f \in B$ with $lt(f) \notin Gen(\Sigma(B))$ can be reduced by other base elements. Iterated application yields a result similar to the triangulation of a matrix within the Gauss algorithm.

Interreduce(B:basis):basis

Input: Basis $B = \{b_1, \ldots, b_m\} \subset R$

Output: Basis B' with $Id(B) = Id(B')$ and $|B'| = |Gen(\Sigma(B'))|$

while exists $f \in B,\ lt(f) \notin Gen(\Sigma(B))$ **do**

  $B = B - \{f\}$

  $f' = NF(f, B)$

  if $f' \neq 0$ **then** $B = B \cup \{f'\}$

return B

Interreduce terminates if $(T, <)$ is a Noetherian term ordering. Note that the `while` loop terminates due to Dickson's lemma. Noetherianity is required only for termination of **NF**, since $\Sigma(B)$ increases with every new $f' \neq 0$.

Groebner Bases – Definition and Motivation

The same idea can be applied to any $f \in Id(B)$ with $lt(f) \notin \Sigma(B)$. The idea of the Groebner algorithm is to scan $I = Id(B)$ systematically for such elements.

Given an ideal I, start from $B = \emptyset$ and in every step enlarge B with an element $0 \neq f \in I$ with $lt(f) \notin \Sigma(B)$ as long as possible. We obtain a strictly increasing chain

$$\Sigma_0 \subset \Sigma_1 \subset \dots$$

of monomial ideals that must be finite by Dickson's lemma. Eventually we get a basis G with $\Sigma(G) = \Sigma(I)$.

> *A subset $G \subset I$ of an ideal I is called* Groebner basis *of I if $\Sigma(G) = \Sigma(I)$.*

Groebner Bases – First Properties

G is a subset of I but not required to generate I.

Theorem:
A Groebner $G \subset I$ of an ideal I generates I.

As an immediate corollary we obtain

Theorem (Hilbert's Basissatz)
Every ideal $I \subset R$ has a finite basis.

Indeed, we proved (not constructively so far) the existence of finite Groebner bases for every such ideal.

Further properties are

For a Groebner basis $G \subset I$ we have

$$f \in I \;\Leftrightarrow\; NF(f,G) = 0.$$

For a Groebner basis G and a polynomial $f \in R$ the total normal form $TNF(f,G)$ is uniquely determined and does not depend on the reduction path.

S-Polynomials

For $0 \neq f, g \in R$ we define the *S-Polynomial* of (f, g)

$$S(f,g) := \frac{m}{lm(f)} f - \frac{m}{lm(g)} g = \frac{m}{lm(f)} red(f) - \frac{m}{lm(g)} red(g),$$

where $m = \text{lcm}(lt(f), lt(g)$.

Due to cancellation of highest terms we have $S(f,g) = 0$ or $lt(S(f,g)) < m$.

Characterization of Groebner Bases

The following condition for $G \subset I$ are equivalent:

1. *G is a Groebner basis, i.e., $\Sigma(I) = \Sigma(G)$.*

2. *For all $f \in I$ and all reduction strategies we have $NF(f,G) = 0$.*

2'. *For all $f \in I$ exists a reduction strategy with $NF(f,G) = 0$.*

3. *For all pairs $g_1, g_2 \in G$ and all reduction strategies we have $NF(S(g_1,g_2),G) = 0$.*

3'. *For all pairs $g_1, g_2 \in G$ exists a reduction strategy with $NF(S(g_1,g_2),G) = 0$.*

4. *All* $f \in I$ *have a representation*

$$f = \sum_{g \in G} h_g\, g \quad \textit{with} \quad \forall\, g\ (lt(f) \geq lt(h_g\, g)).$$

5. *The standard terms* $N(G) := T(X) \setminus \Sigma(G)$ *are* k-*linearly independent* $\pmod{I}$.

5'. *The standard terms* $N(G)$ *form a* k-*linear basis of the factor ring* R/I, *i.e., all* $f \in R$ *have a unique* k-*linear representation*

$$f \equiv \sum_{m \in N(G)} c_m m \pmod{I}$$

mit $c_m \in k$.

GBasis(B:basis):basis

Input: finite set $B = \{f_1, \ldots, f_m\} \subset R$.

Output: a Groebner basis G of $I = Id(B)$.

G:=B;

$P := \{(f_i, f_j) \mid 1 \leq i < j \leq m\}$;

While $P \neq \emptyset$ do

  Choose $p \in P$; $P := P \setminus \{p\}$;

  $f := NF(S(p), G)$

  if $f \neq 0$ then

    $P := P \cup \{(g, f) \mid g \in G\}$;

    $G := G \cup \{f\}$;

return G;

GBasis *is Buchberger's algorithm. It terminates in a finite number of steps for any Noetherian term ordering.*

The result may contain more elements than necessary.

If G *is a Groebner basis of* I *and* $G' \subset G$ *a subset with* $Gen(\Sigma(G)) = \{lt(g) : g \in G'\}$ *then* G' *is a Groebner basis of* I*, too.*
Such a Groebner basis is called minimal.

Minimal and Reduced Groebner Bases

$Gen(\Sigma(I))$, hence $\{lt(g) : g \in G'\}$, is uniquely determined.

$$G'' = \{lt(g) - TNF(lt(g), G') : g \in G'\} \subset I$$

is called *the minimal reduced Groebner basis*. It is completely unique for a given ideal I and fixed term ordering.

A Criterion for Trivial Ideals

For $B \subset R$ are equivalent:

1. *$V_K(B) = \emptyset$, i.e., B has no common zeroes over an algebraically closed extension K of k.*
2. *$Id(B) = Id(1)$ is the unit ideal.*
3. *Any Groebner basis $G = GBasis(B)$ contains ac onstant polynomial.*
4. *$\{1\}$ is the minimal reduced Groener basis of $Id(B)$.*

Elimination Orders and the Elimination Theorem

$B \subset R = k[\mathbf{x}]$ is a finite set of polynomials, $\mathbf{x} = (x_1, \ldots, x_k, y_1, \ldots, y_m)$.

Goal: Compute a basis of the *elimination ideal*

$$I' = Id(B) \bigcap k[y_1, \ldots, y_m].$$

Solution: Choose a term ordering on $T(\mathbf{x})$ where a term containing a factor x_i is greater than all terms not containing such factors (elimination ordering). Any matrix term ordering refining the weight vector w with $w(x_i) = 1, w(y_j) = 0$ does (e.g., the lex ordering with $x_i > y_j$ for all (i, j)).

The Elimination Theorem

If $G = GBasis(B)$ *is a (min. reduced) Groebner basis of* B *wrt. an elimination ordering for* $x_1, \ldots, x_k, y_1, \ldots, y_m$ *then*

$$G' = \{g \in G \,:\, lt(g) \in T(y_1, \ldots, y_m)\}$$

is a (min. reduced) Groebner basis of the elimination ideal $I' = Id(B) \bigcap k[y_1, \ldots, y_m]$.

The lexicographic ordering is eliminating for any initial sequence of variables. Hence Groebner bases wrt. the lex. ordering are “triangular” and well suited to compute solution sets.

For $G = GBasis(B)$ a (min. reduced) lex. Groebner basis of $B \subset R = k[\mathbf{x}]$ with $x_1 > \cdots > x_n$ the subsets

$$G_i = \{g \in G : lt(g) \in T(x_i, \ldots, x_n)\}$$

are (min. reduced) Groebner bases of the elimination ideals $Id(B) \bigcap k[x_i, \ldots, x_n]$.
In particular, G_n contains the polynomial $g(x_n) \in I$ of smallest degree only in x_n, if such a polynomial exists and G is minimal and reduced.

Based on that observation we get an inductive way to compute the solutions of a polynomial system B:

> If $(x^0_{i+1}, \ldots, x^0_n)$ is a common zero of G_{i+1}, then $G_i \setminus G_{i+1}$ contains all polynomials required to determine x^0_i such that $(x^0_i, \ldots, x^0_n)$ is a common zero of G_i.

This requires to compute with algebraic numbers in an early stage. A better way (the Groebner factorizer) tries to factor intermediate polynomials $f = f_1 \cdot \ldots \cdot f_k$ to split the problem:

$$V(F \cup \{f\}) = \bigcup_k V(F \cup \{f_k\})$$

Independent Sets and Dimension

Dimension of an ideal $I \subset R$

$$\dim(R/I) = \max\Big(d : \exists \left(x_{i_1}, \ldots, x_{i_d}\right) \; I \bigcap k[x_{i_1}, \ldots, x_{i_d}] = \{0\}\Big).$$

A subset $x_{i_1}, \ldots, x_{i_d} \subset \mathbf{x}$ with $I \bigcap k[x_{i_1}, \ldots, x_{i_d}] = \{0\}$ is called an *independent set* modulo I.

For $R' = k[x_{i_1}, \ldots, x_{i_d}]$ we have obviously

$$Lt(I) \bigcap R' = \{0\} \;\Rightarrow I \bigcap R' = \{0\}$$

$(x_{i_1}, \ldots, x_{i_d})$ is called a *strongly independent set* modulo I (and the term ordering) if $\Sigma(I) \cap T(x_{i_1}, \ldots, x_{i_d}) = \emptyset$

and

$$d' = \max\left(d : \exists \left(x_{i_1}, \ldots, x_{i_d}\right)\ \Sigma(I) \cap T(x_{i_1}, \ldots, x_{i_d}) = \emptyset\right)$$

the *strong dimension* of R/I. This is exactly $\dim(R/Lt(I))$.

By definition $d' \leq \dim(R/I)$.

For an ideal the dimension and the strong dimension coincide.

The proof uses a deformation argument that is of separate interest.

Groebner Weighted Deformations

Example:

$$B = \left\{x^2 + y + z - 3, x + y^2 + z - 3, x + y + z^2 - 3\right\}$$

There is a positive integer weight vector w such that $Lt_{\texttt{lex}}(Id(B))$ and $Lt_{<}(Id(B))$ coincide for any term ordering $<$ refining w.

Indeed, take $w = (4, 3, 1)$ for this example

$$yz^2 + 1/2z^4t - 2yt^2 - 5/2z^2t^3 + 3t^5$$
$$z^6 - 10z^4t^2 + 4z^3t^3 + 19z^2t^4 - 8zt^5 - 6t^6$$
$$x + yt + z^2t^2 - 3t^4$$
$$y^2 - yt^3 - z^2t^4 + zt^5$$

Existence of Groebner Weighted Deformations

$G = \left\{ \mathbf{x}^\alpha - \sum_{\mathbf{x}^\beta \in N} c_{\alpha\beta} \mathbf{x}^\beta : \mathbf{x}^\alpha \in Gen(\Sigma) \right\}$ *is a minimal reduced Groebner basis of the ideal* I*, with the set* $N = T \setminus \Sigma(I)$ *of standard terms. Then exists a positive integer weight vector* $w \in \mathbb{Z}_+$ *such that*

$$\forall \alpha,\ \beta\ \left(c_{\alpha\beta} \neq 0 \Rightarrow w(\alpha) > w(\beta) \right)$$

For all term orderings $<'$ *that refine* w*, we have* $\Sigma'(G) = \Sigma(G)$ *and* G *is a Groebner basis also wrt.* $<'$*.*

We define a family

$$G_t = \left\{ \mathbf{x}^\alpha - \sum_\beta c_{\alpha\beta}\mathbf{x}^\beta \cdot t^{w(\alpha)-w(\beta)} : \mathbf{x}^\alpha \in Gen(\Sigma) \right\}$$

of Groebner bases over the ring $R_t = k[t][x_1, \ldots, x_n]$ such that $G = G_1$ is the Groebner basis of the original ideal I and $G_0 = Lt(I)$ is the corresponding PP-ideal.

The set N of standard terms is not only a k-linear base of R/I but also a $k[t]$-free base of R_t/I_t. Hence the deformation $Spec\,(R_t/I_t)$ is flat over the base $Spec(k[t])$ and all fibers have the same dimension:

$$d' = \dim(R/Lt(I)) = \dim(R/I)$$

The Pair Criteria and Syzygies of $Lt(I)$

Main Syzygy Criterion

For $f, g \in R$ non trivial with relative prime leading terms we have always $NF(S(f,g), \{f,g\}) = 0$.

For more advanced criteria we fix some notation.

$G = \{f_1, \ldots, f_N\}$ is the base under consideration in a running Groebner basis computation. Further we assume all $lc(f_i) = 1$

Set $m_i = lt(f_i)$, $m_I = \mathrm{lcm}(m_i, i \in I)$ for a subset $I \subset \{1, \ldots, m\}$, $e_i \in R^N$ the i-th unit vector and $(1 \leq i < j \leq N)$

$$s_{ij} = \frac{m_{ij}}{m_i} e_i - \frac{m_{ij}}{m_i} e_j \in R^N$$

All the s_{ij} form a generating set for the first syzygy module $S_1 = Ker(\phi_1)$ of $Lt(G)$, i.e., the kernel of the map

$$\phi_1 : R^N \to R \quad \text{given by} \quad e_i \mapsto m_i$$

Hence two other criteria for G to be a Groebner basis are

6. For each $s \in S_1$ exists a reduction strategy such that $NF(s \cdot B, G) = 0$.

6'. For each $s \in S_1$ and every reduction strategy we have $NF(s \cdot B, G) = 0$.

It is enough to check (6.) for s in a base of S_1. Hence it is enough to test a subset of the s_{ij} that generates S_1.

To get a complete picture about such subsets we have to determine the relations between the s_{ij}, i.e., to compute the second syzygy module $S_2 = Ker(\phi_2)$ of $Lt(G)$ with

$$\phi_2 : R^{\binom{N}{2}} \to R^N \quad \text{given by} \quad e_{ij} \mapsto s_{ij}$$

A (not necessarily minimal) generating set of S_2 are the elements $(1 \leq i < j < k \leq N)$

$$s_{ijk} = \frac{m_{ijk}}{m_{ij}} e_{ij} - \frac{m_{ijk}}{m_{ik}} e_{ik} + \frac{m_{ijk}}{m_{ijk}} e_{jk}$$

The following strategy is usually applied if f_k enters into a partially computed GBasis $G = (f_i, 1 \leq i < k)$:

(1) Skip (j,k) if there is a $i < j$ with $m_{ijk} = m_{jk}$ (i.e., $m_i | m_{jk}$). The syzygy looks like [. . 1].

(2) Skip (i,k) if there is a $i < j$ with $m_{ijk} = m_{ik}$ (i.e., $m_j | m_{ik}$) **and** $m_{ijk} \neq m_{jk}$ (i.e., $m_i \not| m_{jk}$, hence (j,k) was not skipped in the first run). The syzygy looks like [. 1 $*$], where $*$ stands for a non-constant term.

(3) Scan the old pairs (i,j) and skip those with $m_{ijk} = m_{ij}$ (i.e., $m_k | m_{ij}$) **and** $m_{ijk} \neq m_{ik}$, $m_{ijk} \neq m_{jk}$ (i.e., $m_i \not| m_{jk}$, $m_j \not| m_{ik}$, hence neither (i,k) nor (j,k) was skipped in the first two runs). The syzygy looks like [1 $*$ $*$]

This is more or less the **Gebauer-Möller criterion** for useless pairs.

Multimodular and Trace Algorithms

Consider the ideal $I \subset \mathbb{Z}[\mathbf{x}]$ generated by $B = \{f_1, \ldots, f_m\}$ and its relation to $I_0 = I \cdot \mathbb{Q}[\mathbf{x}]$ and to $I_p = I \cdot \mathbb{Z}_p[\mathbf{x}]$ for different primes p.

For a proper definition of $\Sigma(I)$ we get $\Sigma = \Sigma(I) = \Sigma(I_0)$. We say that p is a *lucky prime* if $\Sigma(I_p) = \Sigma$.

Define $C_m = \gcd\,(lc(f) : f \in I,\ lt(f) = m)$ for $m \in \Sigma$.

p is lucky if $p \nmid C_m$ for all $m \in Gen(\Sigma)$.
Hence there are only finitely many unlucky primes.

Hilbert Series and Hilbert Driven GB Computation

$R = \oplus_d [R]_d$ is the decomposition of R in homogeneous components. A *H-module* is an R-module M with a similar decomposition $M = \oplus_d [M]_d$, $dim_k([M]_d)$ finite and $[M]_d = 0$ for $d \ll 0$.

In particular, any homogeneous ideal I and its factor ring R/I are H-modules.

Define the *Hilbert series* of M

$$H(M,t) = \sum_{d \in \mathbb{Z}} dim_k([M]_d)\, t^d$$

For $R = k[x_1, \ldots, x_n]$ we have $H(R, t) = \frac{1}{(1-x)^n}$.

The general computation exploits the relation (deg$(f) = d$)

$$H(R/(I + (f)), t) = H(R/I, t) - t^d H(R/(I : (f)), t)$$

Since $N(G) = T \setminus \Sigma(I)$ is a k-base of R/I we get

$$H(R/I, t) = H(R/Lt(I), t) = \sum_{d \in \mathbb{Z}} |[N(G)]_d| \; t^d$$

For homogeneous ideal in many cases the Hilbert series is known in advance. In this case the computation of S-polynomials in degree d can be terminated if $[Lt(\Sigma)]_d$ has the correct k-dimension. This version of Buchbergers algorithmus is called **Hilbert Driven Algorithm**.