Some Applications of Commutative and Non-Commutative Gröbner Bases

Rafał Abłamowicz*
rablamowicz@tntech.edu

AGACSE 2008, Leipzig, Germany, August 17–19, 2008

*Department of Mathematics, Tennessee Technological University, Cookeville, TN 38505

Abstract: Gröbner bases in polynomial rings over a field have numerous applications in geometry, applied mathematics, and engineering. Non commutative Gröbner bases in Grassmann and Clifford (geometric) algebras are less known but have a potential to be very useful in practical applications of these algebras. We show a few standard applications of commutative Gröbner bases in the theory of symmetric functions, finite group invariants, as well as in some problems in engineering including finding polynomial equations of equidistant curves and surfaces. We show how these bases are computed in Grassmann and Clifford algebras.

Keywords: Gröbner basis, elimination ideal, envelope, Grassmann algebra, Clifford algebra, left ideal, PBW ring, monomial order

Topics

I. Gröbner basis theory in polynomial rings

II. PBW rings and algebras

III. G-algebras and GR-algebras

IV. Gröbner bases in Grassmann and Clifford algebras

V. Computational differences and similarities when computing Gröbner bases in $k[x_1, \ldots, x_n]$, and Grassmann and Clifford algebras

VI. Final Comments

I. Gröbner basis theory in polynomial rings (Cox *et al.*)

Definition 1. *Let k-field, $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$*

$$\mathbf{V}(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n \,|\, f_i(a_1, \ldots, a_n) = 0\}$$

for all $1 \leq i \leq s$. We call $\mathbf{V}(f_1, \ldots, f_s)$ the **affine variety** *defined by $f_1, \ldots, f_s$.*

Example 1. *Examples of some varieties:*

- $\mathbf{V}(x^2 + y^2 - 1) \subset \mathbb{R}^2$ *(circle)*
- $\mathbf{V}(y - x^2, z - x^3) \subset \mathbb{R}^3$ *(twisted cubic)*
- $\mathbf{V}(x + y + z + w, x - 2y + z - 3w) \subset \mathbb{R}^4$ *(linear variety)*

Lemma 1. *If $V, W \subset k^n$ are affine varieties, then so are $V \cup W$ and $V \cap W$.*

Definition 2. *A subset $I \subset k[x_1, \ldots, x_n]$ is an* **ideal** *if it satisfies:*

(i) $0 \in I$,

(ii) If $f, g \in I$, then $f + g \in I$,

(iii) If $f \in I$ and $h \in k[x_1, \ldots, x_n]$, then $hf \in I$.

Definition 3. *Let* $f_1, \ldots, f_s$ *be polynomials in* $k[x_1, \ldots, x_n]$. *Then we set*

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \,:\, h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \right\}$$

Lemma 2. *Let* $f_1, \ldots, f_s$ *be polynomials in* $k[x_1, \ldots, x_n]$. *Then* $\langle f_1, \ldots, f_s \rangle$ *is an ideal of* $k[x_1, \ldots, x_n]$. *We call* $\langle f_1, \ldots, f_s \rangle$ *the* **ideal generated by** $f_1, \ldots, f_s$

Definition 4. *We say that ideal* I *is* **finitely generated** *if there exist* $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ *such that* $I = \langle f_1, \ldots, f_s \rangle$. *We say that* $f_1, \ldots, f_s$ *are a* **basis** *of* I.

Proposition 1. *If* $f_1, \ldots, f_s$ *and* $g_1, \ldots, g_t$ *are bases of the same ideal in* $k[x_1, \ldots, x_n]$, *so that* $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, *then* $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$.

Definition 5. *Let* $V \subset k^n$ *be an affine variety. Then we set*

$$\mathbf{I}(V) = \{ f \in k[x_1, \ldots, x_n] \,:\, f(a_1, \ldots, a_n) = 0 \}$$

for all $(a_1, \ldots, a_n) \in V$.

Lemma 3. *If* $V \subset k^n$ *is an affine variety, then* $\mathbf{I}(V) \subset k[x_1, \ldots, x_n]$ *is an ideal. We call* $\mathbf{I}(V)$ *the* **ideal of** V.

Note that $\langle f_1, \ldots, f_s \rangle \subset \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ although equality need not occur, for example, $\langle x^2, y^2 \rangle \subsetneq \mathbf{I}(\mathbf{V}(x^2, y^2))$.

Definition 6. *A* **monomial ordering** *on* $k[x_1,\ldots,x_n]$ *is any relation* $>$ *on* $\mathbb{Z}^n_{\geq 0} = \{(\alpha_1,\ldots,\alpha_n)\,|\,\alpha_i \in \mathbb{Z}_{\geq 0}\}$, *or equivalently, any relation on the set of monomials* x^α, $\alpha \in \mathbb{Z}^n_{\geq 0}$, *satisfying:*

(i) $>$ *is a total ordering on* $\mathbb{Z}^n_{\geq 0}$ *(for any* $\alpha,\beta \in \mathbb{Z}^n_{\geq 0}$, $\alpha > \beta, \alpha = \beta$ *or* $\beta > \alpha$*)*

(ii) If $\alpha > \beta$ *and* $\gamma \in \mathbb{Z}^n_{\geq 0}$, *then* $\alpha + \gamma > \beta + \gamma$.

(iii) $>$ *is a well-ordering on* $\mathbb{Z}^n_{\geq 0}$ *(every nonempty subset has smallest element)*

- **Lexicographic Order**: $\alpha >_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the left-most nonzero entry is positive.
- **Graded Reverse Lex Order**: $\alpha >_{grevlex} \beta$ if either $|\alpha| > |\beta|$, or $|\alpha| = |\beta|$ and in $\alpha - \beta \in \mathbb{Z}^n$ the right-most nonzero entry is negative.
- **Graded Inverse Lex Order**: $\alpha >_{ginvlex} \beta$ if either $|\alpha| > |\beta|$, or $|\alpha| = |\beta|$ and in $\alpha - \beta \in \mathbb{Z}^n$ the right-most nonzero entry is positive. (NC case)
- **Elimination Order**: Separate all n variables into two (or more) disjoint lists L_1, L_2 of lengths n_1, n_2. Then, $(\alpha_1,\alpha_2) >_{lexdeg} (\beta_1,\beta_2)$, where length$(\alpha_1)$ = length$(\beta_1) = n_1$, length(α_2) = length$(\beta_2) = n_2$, if $\alpha_1 >_{grevlex} \beta_1$ with ties broken by $\alpha_2 >_{grevlex} \beta_2$.

General Division Algorithm in $k[x_1, \ldots, x_n]$**.** *Fix a monomial order* $>$ *on* $\mathbb{Z}^n_{\geq 0}$*, and let* $F = (f_1, \ldots, f_s)$ *be an ordered* s*-tuple of polynomials. Then every* $f \in k[x_1, \ldots, x_n]$ *can be written as*

$$f = a_1 f_1 + \cdots a_s f_s + r, \tag{1}$$

where $a_i, r \in k[x_1, \ldots, x_n]$ *and either* $r = 0$ *or* r *is a linear combination, with coefficients in* k*, of monomials, none of which is divisible by any of* $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_s)$*. We call* r *a* **remainder** *of* f *on division by* F*. Furthermore, if* $a_i f_i \neq 0$*, then we have* $\mathrm{multideg}(f) \geq \mathrm{multideg}(a_i f_i)$.

Remark. *The remainder* r *in (1) is not unique as it depends on the order of polynomials in* F *and on the monomial order. For example, let* $f = xy^3 + 1, f_1 = xy + 1, f_2 = y^2 - y$*. Then, in* $lex(x, y)$ *order, one gets*

$$f = y^2 \cdot f_1 + (-1) \cdot f_2 + (-y + 1) \text{ when dividing by } (f_1, f_2) \tag{2}$$

$$f = (xy + x) \cdot f_1 + (1) \cdot f_2 + 0 \text{ when dividing by } (f_2, f_1) \tag{3}$$

Thus, (3) shows that $f \in \langle f_1, f_2 \rangle \subset k[x_1, \ldots, x_n]$ *while (2) fails to give zero remainder, when dividing by the ideal basis, and seems to imply that* $f \notin \langle f_1, f_2 \rangle$*. This shortcoming of the Division Algorithm disappears when we divide polynomials by a Gröbner basis.*

Definition 7. *An ideal* $I \subset k[x_1, \ldots, x_n]$ *is a* **monomial ideal** *if there is a subset* $A \subset \mathbb{Z}^n_{\geq 0}$ *(possibly infinite) such that* I *consists of all polynomials which are finite sums of the form* $\sum_{\alpha \in A} h_\alpha x^\alpha$*, where* $h_\alpha \in k[x_1, \ldots, x_n]$*. In this case we write* $I = \langle x^\alpha : \alpha \in A \rangle$*.*

Dickson's Lemma. *Every monomial ideal* $I \subset k[x_1, \ldots, x_n]$ *has a finite basis.*

Definition 8. *Let* $I \subset k[x_1, \ldots, x_n]$ *be a nonzero ideal. Then,* $\mathsf{LT}(I)$ *is the set of leading terms of elements of* I *and* $\langle \mathsf{LT}(I) \rangle$ *is the ideal generated by the elements of* $\mathsf{LT}(I)$*.*

Proposition 2. *Let* $I \subset k[x_1, \ldots, x_n]$ *be an ideal.*

(i) $\langle \mathsf{LT}(I) \rangle$ *is a monomial ideal.*

(ii) There are finitely-many $g_1, \ldots, g_s \in I$ *such that*

$$\langle \mathsf{LT}(I) \rangle = \langle \mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_s) \rangle.$$

Hilbert Basis Theorem. *Every ideal* $I \subset k[x_1, \ldots, x_n]$ *has a finite generating set. That is,* $I = \langle g_1, \ldots, g_s \rangle$ *for some* $g_1, \ldots, g_s \in I$*.*

Definition 9. *Fix a monomial order. A finite subset* $G = \{g_1, \ldots, g_t\}$ *of an ideal* I *is said to be a* **Gröbner basis** *if*

$$\langle \mathsf{LT}(g_1), \ldots, \mathsf{LT}(g_t) \rangle = \langle \mathsf{LT}(I) \rangle. \tag{4}$$

As a consequence of Proposition 2 and Hilbert Basis Theorem we have

Corollary 1. *Fix a monomial order. Then every ideal* $I \subset k[x_1, \ldots, x_n]$ *other than* $\{0\}$ *has a Gröbner basis.*

Useful results (Cox *et al*):

Proposition 3. *If* $g_1, \ldots, g_t$ *is a Gröbner basis for* I *and* $f \in k[x_1, \ldots, x_n]$, *then* $f \in I$ *if and only if the remainder of* f *on division by* $g_1, \ldots, g_t$ *is zero.*

Proposition 4. *If* $g_1, \ldots, g_t$ *is a Gröbner basis for* I *and* $f \in k[x_1, \ldots, x_n]$, *then* f *can be written uniquely in the form* $f = g + r$ *where* $g \in I$ *and no term of* r *is divisible by any* $\mathsf{LT}(g_i)$.

When dividing f by a Gröbner basis, we denote the remainder as $r = \overline{f}^G$. Due to the uniqueness of r, one gets unique coset representatives for elements in the quotient ring $k[x_1, \ldots, x_n]/I$: The coset representative of $[f] \in k[x_1, \ldots, x_n]/I$ will be $\overline{f}^G$.

How to compute a Gröbner basis? How to check whether an ideal basis is a Gröbner basis?

Answer is provided by Buchberger's algorithm (and its modifications) that uses S-polynomials.

Definition 10. *The S-***polynomial** *of* $f_1, f_2 \in k[x_1, \ldots, x_n]$ *is defined as*

$$S(f_1, f_2) = \frac{x^\gamma}{\mathsf{LT}(f_1)} f_1 - \frac{x^\gamma}{\mathsf{LT}(f_2)} f_2, \tag{5}$$

where $x^\gamma = \mathrm{lcm}(\mathsf{LM}(f_1), \mathsf{LM}(f_2))$ *and* $\mathsf{LM}(f_i)$ *is the leading monomial of* f_i *w.r.t. some monomial order.*

Example 2. *Let* $f_1 = x^4 - 3xy, f_2 = x^2y - 2 \in k[x, y]$ *and* $lex(x, y)$ *order. Then,* $\mathsf{LT}(f_1) = x^4$, $\mathsf{LT}(f_2) = x^2y$ *and*

$$S(f_1, f_2) = \frac{x^4 y}{x^4} \cdot f_1 - \frac{x^4 y}{x^2 y} \cdot f_2 = y \cdot f_1 - x^2 \cdot f_2 = -3xy^2 + 2x^2 \in \langle f_1, f_2 \rangle.$$

Since $\mathsf{LT}(S(f_1, f_2))$ *divisible by neither* $\mathsf{LT}(f_1)$ *nor* $\mathsf{LT}(f_2)$*, or,* $\mathsf{LT}(S(f_1, f_2)) \notin \langle \mathsf{LT}(f_1), \mathsf{LT}(f_2) \rangle$*, we see that* f_1, f_2 *is not a Gröbner basis of* $\langle f_1, f_2 \rangle$*.*

Buchberger's Criterion. *A basis* $\{g_1, \ldots, g_t\} \subset I$ *is a Gröbner basis of* I *if an only if* $\overline{S(g_i, g_j)}^G = 0$ *for all* $i < j$.

Buchberger's algorithm for finding a Gröbner basis: If $F = \{f_1, \ldots, f_s\}$ fails because $\overline{S(f_i, f_j)}^G \neq 0$ for some $i < j$, then we add this remainder to F and try again.

Example 3. *Let* $F = \{f_1, f_2\}$ *as in Example 2. We know that* $\overline{S(f_1, f_2)}^F = -3xy^2 + 2x^2 = f_3$, *so we set* $F_1 = \{f_1, f_2, f_3\}$ *and compute:*

$$\overline{S(f_1, f_2)}^{F_1} = 0, \quad \overline{S(f_1, f_3)}^{F_1} = 0, \quad \overline{S(f_2, f_3)}^{F_1} = -4 + 3xy^3 = f_4,$$

so F_1 *is not a Gröbner basis yet. Adding* $F_2 = \{f_1, f_2, f_3, f_4\}$, *we compute*

$$\overline{S(f_1, f_4)}^{F_2} = 0, \quad \overline{S(f_2, f_3)}^{F_2} = 0, \quad \overline{S(f_2, f_4)}^{F_2} = -3y^2 + 2x = f_5,$$

so F_2 *is not a Gröbner basis yet. Adding* $F_3 = \{f_1, f_2, f_3, f_4, f_5\}$, *we compute again and find that* $\overline{S(f_i, f_j)}^{F_3} = 0$ *for all* $i < j$ *except* $\overline{S(f_4, f_5)}^{F_3} = 9y^5 - 8 = f_6$, *so that the Gröbner basis of* $I = \langle f_1, f_2 \rangle$ *finally is*

$$F_4 = \{x^4 - 3xy,\ x^2y - 2,\ -3xy^2 + 2x^2,\ 3xy^3 - 4,\ 2x - 3y^2,\ 9y^5 - 8\}.$$

since $\overline{S(f_i, f_j)}^{F_4} = 0$ *for all* $i < j$.

Buchberger's Algorithm. *Given* $\{f_1, \ldots, f_s\} \subset k[x_1, \ldots, x_n]$, *consider the algorithm which starts with* $F = \{f_1, \ldots, f_s\}$ *and then repeats the two steps*

- *(Compute Step) Compute* $\overline{S(f_i, f_j)}^F$ *for all* $f_i, f_j \in F$ *with* $i < j$,
- *(Augment step) Augment* F *by adding the nonzero* $\overline{S(f_i, f_j)}^F$ *until the Compute Step gives only zero remainders. The algorithm always terminates and the final value of* F *is a Gröbner basis of* $\langle f_1, \ldots, f_s \rangle$.

Comments

– Gröbner bases were introduced in 1965 by B. Buchberger and named by him in honor of W. Gröbner (1899-1980), Buchberger's thesis advisor.

– Gröbner bases gave rise to development of computer algebra systems like muMath, Maple, Mathematica, Reduce, AXIOM, Singular, CoCoCA, FGb, Macaulay, etc.

– Buchberger's Algorithm has been made more efficient, see Becker and Cox, Faugère, and references therein.

cont.

- Gröbner basis $F4$ computed above is too big: A standard way to reduce it is to replace any polynomial f_i with its remainder on division by $\{f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_t\}$, removing zero remainders, and for polynomials that are left, making their leading coefficient equal to 1. This produces a *reduced Gröbner basis*.
- In general, for a fixed monomial, order, any ideal in $k[x_1, \ldots, x_n]$ has a *unique* reduced Gröbner basis. For example, for the ideal in Example 3, the reduced Gröbner basis is

$$G_{red} = \{y^5 - \frac{8}{9}, x - \frac{3}{2}y^2\}$$

Some problems that can be solved using Gröbner bases:

- The ideal membership problem, i.e., does $f \in I = \langle f_1, \ldots, f_s \rangle$?
- Finding generators for the intersection of two ideals $I \cap J$.

cont.

- Solving systems of polynomial equations, e.g., intersecting surfaces and curves, finding closest point on curve to the given point, Lagrange multiplier problems (especially for several multipliers), etc. Solutions to these problems are based on the so called Extension Theory. (Cox)
- Finding equations for equidistant curves and surfaces to curves and surfaces defined in terms of polynomial equations, such as conic sections, Bézier cubics; finding syzygy relations among various sets of polynomials, for example, symmetric polynomials, finite group invariants, interpolating functions, etc. Solutions to these problems are based on the so called Elimination Theory. (Cox)
- Finding equidistant curves and surfaces as envelopes to families of curves and surfaces, respectively. (Cox *et al.*) (Abłamowicz and Liu)
- The implicitization problem, i.e., eliminating parameters and finding implicit forms for curves and surfaces.

cont.

- The forward and the inverse kinematic problems in robotics. (Buchberger, Cox)
- Automatic geometric theorem proving. (Buchberger, Buchberger and Winkler, Cox)
- Expressing invariants of a finite group in terms of generating invariants. (Cox)
- Finding relations between polynomial functions, e.g., interpolating functions (syzygy relations).
- For many other applications, including integer programming, complex information systems, or algebraic coding theory see Buchberger and Winkler, Cox, Grabmeier
- See also bibliography on Gröbner bases at Johann Radon Institute for Computational and Applied Mathematics (RICAM).

Example 1: Equidistant curves to a parabola

- f_1 defines a parabola with a focus at $(0,p)$ where $|p|$ denotes the distance between the focus $F=(0,p)$ and the vertex $V=(0,0)$:

$$f_1 = 4py_0 - x_0^2 = 0 \tag{6}$$

- f_2 defines a circle of radius (offset) r centered at a point (x_0, y_0) on f_1

$$f_2 = (y-y_0)^2 + (x-x_0)^2 - r^2 = 0 \tag{7}$$

- f_3 gives a condition that point $P(x,y)$ lies on a line perpendicular to f_1 at (x_0,y_0) on f_1

$$f_3 = 2xp - 2x_0p + x_0y - x_0y_0 = 0 \tag{8}$$

- Study affine variety $\mathbf{V} = \mathbf{V}(I)$ where $I = \langle f_1, f_2, f_3 \rangle \subset \mathbb{R}[x_0, y_0, x, y, p, r]$
- Reduced Gröbner basis for I_2 for the lex order $y_0 > x_0 > x > y > p > r$:

$$I_2 = I \cap \mathbb{R}[x,y] = \langle g \rangle \quad \text{(second elimination ideal)}$$

- When is $\mathbf{V}(g)$ smooth? What are the singular points, if any, $p \in \mathbf{V}(g)$ where $(\nabla g)(p) = 0$?

Envelope with three singular points when $p = \frac{1}{3}$ and $r = \frac{3}{2} > r_{crit} = 2|p|$:

$$g = 83808y + 52812x^2 + 16900y^2 - 37248y^3 - 4896x^2y^2 - 34416x^4 - 17280x^4y \\ - 13824x^2y^3 + 9216y^4 + 5184x^4y^2 + 5184x^6 - 84681 + 6240x^2y$$

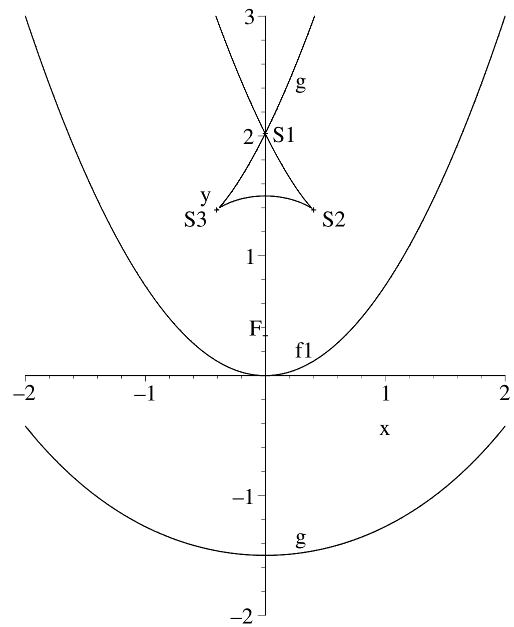

Fig. 3: Parabola with parallel lines and three singular points S_1, S_2, S_3

For a generic parabola $4py = x^2$:

- As the offset $r \to r_{crit} = 2|p|$, virtual singular point approaches variety g.
- No singular points when $0 < r < r_{crit}$, exactly one singular point when $r = r_{crit}$, and three singular points when $r > r_{crit} = 2|p|$.
- For the order $lex(y_0, x_0, x, y, r, p)$, reduced Gröbner basis for I has 14 polynomials with exactly one polynomial $g \in \mathbb{R}[x, y, r, p]$.
- Single polynomial $g \in \mathbb{R}[x, y, r, p]$ implicitly determines the envelope:

$$g = -2pr^2yx^2 + 8pr^2y^3 + 8p^2r^2y^2 - 32yp^3r^2 + 16p^4r^2 - 16y^4p^2 + 32y^3p^3 - 16p^4y^2 + 3r^2x^4 + 8p^2r^4 + 20p^2r^2x^2 - y^2x^4 + 10ypx^4 - x^6 - x^4p^2 + 8py^3x^2 - 32x^2y^2p^2 + 8x^2yp^3 - 3r^4x^2 + 2r^2x^2y^2 + r^6 - r^4y^2 - 8pr^4y$$

- Analysis of $\nabla g = 0$ gives exact coordinates of the singular points and the critical value of the offset $r_{crit} = 2|p|$ (see [2]).
- $r_{crit} = 2|p| = \frac{1}{\kappa_{max}} = \rho_{min}$ is parabola's *semi-latus rectum*

Example 2: Idempotent variety

Consider $C\ell_{2,0}$ with a monomial basis $1, \mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_{12} = \mathbf{e}_1 \wedge \mathbf{e}_2$. What is the most general idempotent $u = u^2 \in C\ell_{2,0}$? Let $u = x_0 + x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + x_{12}\mathbf{e}_{12}$. Then, the equation $u^2 = u$ yields:

$$\begin{aligned} p_1 &= x_0^2 + x_1^2 + x_2^2 - x_{12}^2 - x_0, & p_2 &= x_1(2x_0 - 1), \\ p_3 &= x_2(2x_0 - 1), & p_4 &= x_{12}(2x_0 - 1) \end{aligned} \tag{9}$$

The family of idempotents is an affine variety $\mathbf{V}(p_1, p_2, p_3, p_4)$. We solve the above system by finding a Gröbner basis G for the ideal $I\langle p_0, p_1, p_2, p_3\rangle \subset \mathbb{R}[x_0, x_1, x_2, x_{12}]$ for $lex(x_0, x_1, x_2, x_{12})$ order. G consists of seven polynomials:

$$\begin{aligned} g_1 &= x_{12}(4x_1^2 - 1 + 4x_2^2 - 4x_{12}^2), & g_2 &= x_2(4x_1^2 - 1 + 4x_2^2 - 4x_{12}^2), \\ g_3 &= x_1(4x_1^2 - 1 + 4x_2^2 - 4x_{12}^2), & g_4 &= x_{12}(2x_0 - 1), \\ g_5 &= x_2(2x_0 - 1), & g_6 &= x_1(2x_0 - 1), \\ g_7 &= x_0^2 + x_2^2 - x_{12}^2 + x_1^2 - x_0. \end{aligned} \tag{10}$$

Here $g_1, g_2, g_3 \in G_1 = G \cap \mathbb{R}[x_1, x_2, x_{12}]$ whereas $g_4, g_5, g_6, g_7 \in G_0 = G \subset \mathbb{R}[x_1, x_2, x_{12}]$. Thus, $\mathbf{V}(p_1, p_2, p_3, p_4) = \mathbf{V}(g_1, g_2, g_3, g_4, g_5, g_6, g_7)$. When $x_0 = \frac{1}{2}$, we get

$$u_{1,2} = \frac{1}{2} + x_{12}\mathbf{e}_{12} \pm \frac{1}{2}\sqrt{1 - 4x_2^2 + 4x_{12}^2}\,\mathbf{e}_1 + x_2\mathbf{e}_2, \quad 1 - 4x_2^2 + 4x_{12}^2 \geq 0. \tag{11}$$

cont. When $x_0 \neq 0$, we get trivial idempotents 0 and ± 1. Thus, $u_{1,2}$ in (11) are the only non-trivial idempotents in $C\ell_{2,0}$ and their variety is the hyperboloid $4x_1^2 + 4x_2^2 - 4x_{12}^2 = 1$. The primitive idempotents $\frac{1}{2}(1 \pm \mathbf{e}_1)$ and $\frac{1}{2}(1 \pm \mathbf{e}_2)$ belong to this variety when $x_{12} = x_2 = 0$ and $x_{12} = x_1 = 0$, respectively.

The above example can be generalized when searching for general elements in any Clifford or Grassmann algebra that satisfy certain relations.

Example 3: Distance to ellipse

Find a point (or points) on ellipse $f_1 = \frac{x^2}{a^2} + \frac{y^2}{b^2} - 1$ that minimizes distance from the ellipse to a given point $P = (x_0, y_0), x_0 \neq 0$, not on the ellipse. Thus, one needs first to find points Q on the ellipse such that a line T tangent to the ellipse at Q is orthogonal to the vector $\overrightarrow{QP}$. Let $f_2 = a^2 y(x - x_0) - b^2 x(y - y_0)$. Then, the condition $f_2 = 0$ assures that the vector $\overrightarrow{QP} \perp T$. Let $x_0 = 4, y_0 = \frac{3}{2}, a = 2, b = 1$. Thus, we must to solve a system of equations

$$f_1 = 4y^2 + x^2 - 4 = 0 \quad \text{and} \quad f_2 = 6yx - 32y + 3x = 0 \tag{12}$$

for x and y.

cont. We find the reduced Gröbner basis for the ideal $I = \langle f_1, f_2 \rangle$ that defines $V = \mathbf{V}(f_1, f_2)$ for $lex(x, y$ order. The basis contains two polynomials

$$
\begin{aligned}
g_1 &= -18y^3 + 9 - 9y^2 + 12x - 110y, \\
g_2 &= -9 - 36y + 229y^2 + 36y^3 + 36y^4
\end{aligned} \tag{13}
$$

Observe that g_2 belongs to $I_2 = I \cap \mathbb{R}[y]$. Observe also that the leading coefficient in g_1 w.r.t. $lex(x, y)$ is 12, hence by the Extension Theorem (Cox), every partial solution to the system $\{g_1 = 0, g_2 = 0\}$ on the variety $\mathbf{V}(g_2)$ can be extended to a complete solution of (12) on the variety V. Since polynomial g_2 is of degree 4, it's solutions are expressible in radicals. When approximated, two real values of y are $y_1 = 0.2811025120$ and $y_2 = -0.1354474035$. Each of the exact values of y, when substituted into equation $g_1 = 0$ yields exact value of x. Thus, we have two points Q on the ellipse whose approximate coordinates are $Q_1 = (1.919355494, 0.2811025085)$ and $Q_2 = (-1.981569077, -0.1354473991)$. Checking the distances, one finds $||\overrightarrow{Q_1P}|| = 2.411388118 < ||\overrightarrow{Q_2P}|| = 6.201117385$, or, that the point Q_1 is closest to the given point P.

cont. In the purely symbolic case when a, b, x_0, y_0 remain unassigned, the above process returns a two-polynomial reduced Gröbner basis for I :

$$G = [a^4y^4 - a^4y^2b^2 + 2a^2y^2b^4 - 2a^2b^2y^4 + a^2y^2x_0^2b^2 + 2a^2b^2y^3y_0 - 2a^2yb^4y_0 - b^6y_0^2 - 2y^3y_0b^4 - y^2b^6 + 2yb^6y_0 + y^4b^4 + y^2y_0^2b^4, a^2b^4y_0 - b^6y_0 - a^2b^2y^2y_0 + b^4y^2y_0 + a^4yb^2 - 2a^2yb^4 + yb^6 - a^2x_0^2yb^2 - a^4y^3 + 2a^2b^2y^3 - b^4y^3 + x_0b^4xy_0] \quad (14)$$

where the first polynomial is of degree 4 in y and is, in principle, solvable with radicals. The second polynomial is again of degree 1 in the variable x. Thus, in general, this problem is solvable in radicals.

Definition 11 (Cox). *Let $G \subset \mathsf{GL}(n,k)$, $\mathsf{char}\, k = 0$, be a finite matrix group. A polynomial $f(\mathbf{x}) \in k[x_1,\ldots,x_n]$ is* **invariant under** *G if $f(\mathbf{x}) = f(A\mathbf{x})$ for all $A \in G$.* The set of all invariant polynomials is denoted $k[x_1,\ldots,x_n]^G$.*

It is easy to show that $k[x_1,\ldots,x_n]^G$ is a subring of $k[x_1,\ldots,x_n]$. It is referred to as the **ring of invariants** of the finite group G.

Theorem 1 (Noether). *Given a finite matrix group $G \subset \mathsf{GL}(n,k)$, we have*

$$k[x_1,\ldots,x_n]^G = k[R_G(x^\beta) : |\beta| \le |G|].$$

In particular, $k[x_1,\ldots,x_n]^G$ is generated by finitely many homogeneous invariants.

Here, R_G denotes the **Reynolds operator** of G. Gröbner basis algorithm is used to express any G-invariant polynomial $f \in k[x_1,\ldots,x_n]^G = k[f_1,\ldots,f_m]$ in terms of $f_1,\ldots,f_m$, using this next result.

*Here, $\mathbf{x}$ is the column vector $[x_1\ x_2\ \cdots\ x_n]^T$.

Proposition 5. *Let $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ are given. Fix a monomial order in $k[x, \ldots, x_n, y_1, \ldots, y_m]$ where any monomial involving one of $x_1, \ldots, x_n$ is greater than all monomials in $k[y_1, \ldots, y_m]$. Let G be a Gröbner basis of the ideal $\langle f_1 - y_1, \ldots, f_m - y_m \rangle \subset k[x, \ldots, x_n, y_1, \ldots, y_m]$. Given $f \in k[x_1, \ldots, x_n]$, let $g = \overline{f}^G$ be the remainder of f on division by G. Then: (i) $f \in k[f_1, \ldots, f_m]$ if and only if $g \in k[y_1, \ldots, y_m]$. (ii) If $f \in k[f_1, \ldots, f_m]$, then $f = g(f_1, \ldots, f_m)$ is an expression of f as a polynomial in $f_1, \ldots, f_m$.*

Thus, this result tells us how to determine whether $f \in k[f_1, \ldots, f_m]$ and if so, how to express it in terms of the generating polynomials. In particular, this result allows one to determine whether a polynomial f is G-invariant, that is, whether $f \in k[x_1, \ldots, x_n]^G = k[f_1, \ldots, f_m]$.

Example 4: Symmetric polynomials

Let G be the symmetric group S_3. Let

$$\sigma_1 = x_1 + x_2 + x_3, \quad \sigma_2 = x_1x_2 + x_1x_3 + x_2x_3, \quad \text{and} \quad \sigma_3 = x_1x_2x_3$$

be the *elementary symmetric polynomials* in x_1, x_2, x_3. (Sturmfels) A Gröbner basis F for the ideal $I = \langle \sigma_1 - y_1, \sigma_2 - y_2, \sigma_3 - y_3 \rangle$ in $lex(x_1, x_2, x_3, y_1, y_2, y_3)$ order is

$$F = [x_3^3 - x_3^2 y_1 + y_2 x_3 - y_3,\ x_2^2 + x_2 x_3 - x_2 y_1 + x_3^2 - x_3 y_1 + y_2,\ x_1 + x_2 + x_3 - y_1]$$

cont. Let

$$f = x_1^2x_2 + x_1x_2^2 + 3x_1x_2x_3 + x_1^2x_3 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2 - x_1^2x_2^2x_3^2.$$

It can be checked directly that $f(\mathbf{x}) = f(\sigma\mathbf{x})$, $\forall\sigma \in S_3$. That is, f is invariant under S_3 and $f \in k[x_1, x_2, x_3]^{S_3}$. Reducing f modulo F gives $g = \overline{f}^F = y_1y_2 - y_3^2 \in k[y_1, y_2, y_3]$. Thus, by part (i) of the above Proposition, we see again that f is symmetric. Furthermore, from part (ii) we get that $f = \sigma_1\sigma_2 - \sigma_3^2$.

For more examples on finite group generators and finding the so called *syzygy relations* (or, *syzygies*), see (Cox, Sturmfels). For a small Maple package related to finite group invariants as well as generators (relations) of syzygy ideals, see `SP` package.

Example 5: Rodrigues matrix

Recall that the trigonometric form of a quaternion $a = a_0 + \mathbf{a} \in \mathbb{H}$ is $a = \|a\|(\cos\alpha + \mathbf{u}\sin\alpha)$, where $\mathbf{u} = \mathbf{a}/|\mathbf{a}|$, $|\mathbf{a}|^2 = {a_1}^2 + {a_2}^2 + {a_3}^2$ and α is determined by $\cos\alpha = a_0/\|a\|$, $\sin\alpha = |\mathbf{a}|/\|a\|, 0 \le \alpha < \pi$. Then, any quaternion can be written as

$$a = \|a\|(\cos\alpha + |\mathbf{a}|^{-1}(a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k})\sin\alpha). \tag{15}$$

cont.

Theorem 2 (Meister). *Let a and r be quaternions with non-zero vector parts where $\|a\| = 1$, so $a = \cos\alpha + \mathbf{u}\sin\alpha$ where $\mathbf{u}$ is a unit vector. Then, the norm and the scalar part of the quaternion $r' = ara^{-1}$ equal those of r, that is, $\|r'\| = \|r\|$ and $\mathrm{Re}(r') = \mathrm{Re}(r)$. The vector component $\mathbf{r}' = \mathrm{Im}(r')$ gives a vector $\mathbf{r}' \in \mathbb{R}^3$ resulting from a finite rotation of the vector $\mathbf{r} = \mathrm{Im}(r)$ by the angle 2α counter-clockwise about the axis $\mathbf{u}$ determined by a.*

Let $a = a_0 + \mathbf{a}$, $b = b_0 + \mathbf{b} \in \mathbb{H}$. Let $\mathbf{v}_a$, $\mathbf{v}_b$, and $\mathbf{v}_{ab}$ be vectors in $\mathbb{R}^4$ whose coordinates equal those of $a, b, ab \in \mathbb{H}$. (Meister)

Then, the vector representation of the product ab is

$$ab \mapsto \mathbf{v}_{ab} = G_1(a)\mathbf{v}_b = G_2(b)\mathbf{v}_a \tag{16}$$

where

$$G_1(a) = \begin{bmatrix} a_0 & -\mathbf{a}^T \\ \mathbf{a} & a_0 I + K(\mathbf{a}) \end{bmatrix}, \quad G_2(b) = \begin{bmatrix} b_0 & -\mathbf{b}^T \\ \mathbf{b} & a_0 I - K(\mathbf{b}) \end{bmatrix}, \tag{17}$$

and

$$K(\mathbf{a}) = \begin{bmatrix} 0 & -a_3 & a_2 \\ a_3 & 0 & -a_1 \\ -a_2 & a_1 & 0 \end{bmatrix}, \quad K(\mathbf{b}) = \begin{bmatrix} 0 & -b_3 & b_2 \\ b_3 & 0 & -b_1 \\ -b_2 & b_1 & 0 \end{bmatrix}, \tag{18}$$

cont. are skew-symmetric matrices determined by the vector parts $\mathbf{a}$ and $\mathbf{b}$ of the quaternions a and b, respectively. For properties of matrices $G_1(a)$ and $G_2(b)$ see (Meister). Theorem 2 implies that mapping $r \mapsto r' = ara^{-1}$, $\|a\| = 1$, gives the rotation $\mathbf{r} \mapsto \mathbf{r}'$ in $\mathbb{R}^3$. Using 4×4 matrices, it can be written as:

$$\mathbf{v}_r \mapsto \mathbf{v}'_r = G_1(a)G_2(a^{-1})\mathbf{v}_r = G_1(a){G_2}^T(a)\mathbf{v}_r \tag{19}$$

where

$$G_1(a){G_2}^T(a) = \begin{bmatrix} 1 & 0 \\ 0 & \underbrace{(2{a_0}^2 - 1)I + 2\mathbf{a}\mathbf{a}^T + 2a_0 K(\mathbf{a})}_{R(a)} \end{bmatrix} \tag{20}$$

The 3×3 matrix $R(a)$ in the product $G_1(a){G_2}^T(a)$ is the well-known **Rodrigues matrix** of rotation. (Goldstein, Meister) The Rodrigues matrix has this form in terms of the components of a :

$$R(a) = \begin{bmatrix} a_0^2 + a_1^2 - a_2^2 - a_3^2 & 2a_1a_2 - 2a_0a_3 & 2a_1a_3 + 2a_0a_2 \\ 2a_1a_2 + 2a_0a_3 & a_0^2 - a_1^2 + a_2^2 - a_3^2 & 2a_2a_3 - 2a_0a_1 \\ 2a_1a_3 - 2a_0a_2 & 2a_2a_3 + 2a_0a_1 & a_0^2 - a_1^2 - a_2^2 + a_3^2 \end{bmatrix} \tag{21}$$

cont. Entries of $R(a)$ are homogeneous polynomials of degree 2 in $\mathbb{R}[a_0, a_1, a_2, a_3]$. Separating the scalar and the vector parts of the quaternion r in the $4D$ representation (19), we get

$$\mathrm{Re}(r') = \mathrm{Re}(r), \quad \mathrm{Im}(r') = \boxed{\mathbf{r}' = R(a)\mathbf{r}} = R(a)\,\mathrm{Im}(r) \tag{22}$$

The first relation shows that the scalar part of r remains unchanged, while the vector part $\mathbf{r}'$ of r' is a result of rotation of the vector part $\mathbf{r}$ of r about the axis $\mathbf{a} = a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ and the angle of counter-clockwise rotation is 2α. Observe that

$$\det R(a) = \|a\|^6 \quad \text{and} \quad R(a)^T R(a) = \|a\|^4 I.$$

Thus, the Rodrigues matrix $R(a)$ gives a rotation if and only if $\|a\| = 1$.

Problem: Find the rotation axis $\mathbf{a}$ and the rotation angle 2α by expressing (a_0, a_1, a_2, a_3) in terms of the entries of an orthogonal matrix M of determinant 1. For that purpose, use Gröbner basis and the theory of elimination. (Cox)

cont. Let $M = (m_{ij})$ be an orthogonal 3×3 matrix so $M^T M = I$. This one constraint gives us six polynomial constraints on the entries of M :

$$c_1 = m_{11}^2 + m_{21}^2 + m_{31}^2 - 1,\ c_2 = m_{12}^2 + m_{22}^2 + m_{32}^2 - 1,\ c_3 = m_{13}^2 + m_{23}^2 + m_{33}^2 - 1,$$
$$c_4 = m_{11}m_{12} + m_{21}m_{22} + m_{31}m_{32},\ c_5 = m_{11}m_{13} + m_{21}m_{23} + m_{31}m_{33},$$
$$c_6 = m_{12}m_{13} + m_{22}m_{23} + m_{32}m_{33}$$

We add one more constraint, namely, that $\det M = 1$:

$$c_7 = m_{11}m_{22}m_{33} - m_{11}m_{23}m_{32} - m_{21}m_{12}m_{33} + \\ m_{21}m_{13}m_{32} + m_{31}m_{12}m_{23} - m_{31}m_{13}m_{22} - 1$$

A Gröbner basis G_J for the syzygy ideal $J = \langle c_1, c_2, \ldots, c_7 \rangle$ with respect to $lex(m_{11}, m_{12}, \ldots, m_{33})$ contains 20 polynomials. This means that the seven constraint polynomials are not algebraically independent. Define nine polynomials $f_k \in \mathbb{R}[a_0, a_1, a_2, a_3, m_{ij}]$

$$[f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8, f_9] = [m_{ij} - R(a)_{ij}] \tag{23}$$

Our goal is to express the four parameters a_0, a_1, a_2, a_3 in terms of the nine matrix entries m_{ij} that are subject to the seven constraint relations $c_s = 0$, $1 \leq s \leq 7$. This should be possible up to a sign since for any rotation in $\mathbb{R}^3$ given by an orthogonal matrix M, $\det M = 1$, there are two unit quaternions a and $-a$ that such that $R(a) = R(-a) = M$.

cont. We compute a Gröbner basis G_I for the ideal $I = \langle f_1, \ldots, f_9, c_1, \ldots, c_7 \rangle$ for $lex(a_0, a_1, a_2, a_3, m_{11}, m_{12}, \ldots, m_{33})$ order. G_I contains 50 polynomials of which 20 polynomials are in $\mathbb{R}[m_{ij}]$: Thus, they provide a basis G_J for the syzygy ideal J. We need to solve the remaining 30 polynomial relations for a_0, a_1, a_2, a_3, so we divide them into a set S_l of 20 polynomials that are linear in a_0, a_1, a_2, a_3, and a set S_{nl} of 10 polynomials that are non-linear in a_0, a_1, a_2, a_3. The first four polynomials in S_{nl} are:

$$
\begin{aligned}
{a_0}^2 &= \frac{1}{4}(1 + m_{11} + m_{22} + m_{33}), \qquad & {a_1}^2 &= \frac{1}{4}(1 + m_{11} - m_{22} - m_{33}), \\
{a_2}^2 &= \frac{1}{4}(1 - m_{11} + m_{22} - m_{33}), \qquad & {a_3}^2 &= \frac{1}{4}(1 - m_{11} - m_{22} + m_{33}),
\end{aligned}
\tag{24}
$$

which easily shows that $\|a\| = 1$, the quaternion a defined by the orthogonal matrix M is a unit quaternion.

cont. The remaining six polynomials in S_{nl} are:

$$a_0a_1 = \frac{1}{4}(m_{32} - m_{23}), \quad a_0a_2 = \frac{1}{4}(m_{13} - m_{31}), \quad a_1a_2 = \frac{1}{4}(m_{12} + m_{21}),$$
$$a_0a_3 = \frac{1}{4}(m_{21} - m_{12}), \quad a_1a_3 = \frac{1}{4}(m_{13} + m_{31}), \quad a_2a_3 = \frac{1}{4}(m_{23} + m_{32}), \quad (25)$$

The remaining 20 polynomials from S_l are linear in a_0, a_1, a_2, a_3. Let A be the coefficient matrix of that linear homogeneous system. Matrix A is 20×4 but it can be easily reduced to 14×4 by analyzing its submatrices and normal forms of their determinants modulo the Gröbner basis G_J. It can be shown that this symbolic matrix is of rank 3. That is, there is always a one-parameter family of solutions. Once that one-parameter family of solutions is found, two unit quaternions $\pm a$ such that $R(\pm a) = M$ can be found from remaining 10 nonlinear equations.

Let $M = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}$. Then, the above process gives $a_0 = a_0, a_1 = a_0, a_2 = 0, a_3 = 0$, and $a_0 = \pm\frac{1}{2}\sqrt{2}$ so one unit quaternion is:

$$a = \frac{1}{2}\sqrt{2} + \frac{1}{2}\sqrt{2}\mathbf{i} = a_0 + \mathbf{a}, \cos\alpha = \frac{1}{2}\sqrt{2}, \sin\alpha = |\mathbf{a}| = \frac{1}{2}\sqrt{2}.$$

cont. The Rodrigues matrix gives $R(\pm a) = M$, $\alpha = \frac{1}{4}\pi$, so the rotation angle is $2\alpha = \frac{1}{2}\pi$, and the rotation axis $\mathbf{u}$ is just $\mathbf{i}$, as expected.

For another example, consider the following orthogonal matrix:

$$M = \begin{bmatrix} 0 & \frac{\sqrt{210}-5\sqrt{14}}{35} & \frac{-2\sqrt{35}-5\sqrt{21}}{35} \\ \frac{\sqrt{210}+5\sqrt{14}}{35} & \frac{11}{35} & \frac{-7\sqrt{6}+5\sqrt{10}}{35} \\ \frac{-2\sqrt{35}+5\sqrt{21}}{35} & \frac{-7\sqrt{6}-5\sqrt{10}}{35} & \frac{4}{35} \end{bmatrix}$$

with $\det M = 1$. Then, solution to the linear system is $a_0 = a_0$, $a_1 = \frac{-\sqrt{10}}{5}a_0$, $a_2 = \frac{-\sqrt{21}}{5}a_0$, $a_3 = \frac{\sqrt{14}}{5}a_0$. Upon substitution into the non-linear equations we find $a_0 = \pm\frac{\sqrt{70}}{14}$ which eventually gives $a = \frac{\sqrt{70}}{14} + (-\frac{\sqrt{7}}{7}\mathbf{i} - \frac{\sqrt{30}}{10}\mathbf{j} + \frac{\sqrt{5}}{5}\mathbf{k})$, $\cos\alpha = \frac{\sqrt{70}}{14}$, $\sin\alpha = |\mathbf{a}| = \frac{3\sqrt{14}}{14}$. It can be verified again that $R(\pm a) = M$ and $\alpha \approx 0.9302740142$ rad.

II. PBW rings and algebras (Bueso *et al.*)

- Let k be a field and let $T = T_n = k\langle x_1, \ldots, x_n \rangle$ be a free associative k-algebra, e.g., a tensor k-algebra on a free k-module V with basis $X = \{x_1, \ldots, x_n\}$. T can be thought of as the polynomial ring over k in non-commuting variables X with **monomials**

$$\mathrm{Mon}(T) = \{x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_n}^{\alpha_n} \,|\, 1 \leq i_1, i_2, \ldots, i_n, \alpha_k \geq 0\}$$

  spanning it as a k-vector space. Distinguish **standard monomials**:

$$\mathrm{Mon}_S(T) \ni x^\alpha = x_{i_1}^{\alpha_1} x_{i_2}^{\alpha_2} \cdots x_{i_n}^{\alpha_n} \mapsto (\alpha_1, \alpha_1, \ldots, \alpha_n) = \alpha \in \mathbb{N}^n$$

  where $1 \leq i_1 < i_2 < \cdots < i_n$ and $\alpha_k \in \mathbb{N}$ and the map is a bijection.

- Any finitely generated associative k-algebra is a quotient T_n/I, for some n and a proper two-sided ideal $I \subset T_n$. (Rotman)

- If the set of standard monomials (modulo I) forms a k-basis of an algebra $A = T/I$, we say that A has a **Poincaré-Birkhoff-Witt (PBW) basis in the variables** X.

- An abstract associative algebra A has a **PBW basis** if there exists an isomorphism of k-algebras $A \cong T/I$ such that T/I has a PBW basis. For example, $k[x_1, x_2, \ldots, x_n]$ does have a PBW basis while $k\langle x_1, x_2, \ldots, x_n\rangle$ does not.

- Generalization of the definition of PBW algebras to left PBW rings (together with admissible orders) can be found in Bueso *et al.*

Definition 12. *Let R be a ring containing a division ring k and let $x^\alpha = x_1^{\alpha_1} \ldots, x_n^{\alpha_n}$ be a* **standard term** *where $x_1, \ldots, x_n \in R$. The ring R is said to be* **left polynomial** *over k if the set $\{x^\alpha; \alpha \in \mathbb{N}^n\}$ is a basis of R as a left k-vectors pace. Then, every $f \in R$ has a* **standard representation** $f = \sum_{\alpha \in \mathbb{N}^n} c_\alpha x^\alpha$.

Definition 13. *An* **admissible** *order on $(\mathbb{N}^n, +)$ is a total order $\preceq$ satisfying the following two conditions:*

- $0 \prec \alpha$, $\forall \alpha \in \mathbb{N}^n$, *and*
- $\alpha + \gamma \prec \beta + \gamma$, $\forall \alpha, \beta, \gamma \in \mathbb{N}^n$ *with* $\alpha \prec \beta$.

For $0 \neq f \in R$, *let* $\exp(f) = \max_{\preceq}\{\alpha \in \mathbb{N}^n, c_\alpha \neq 0\}$ *for an admissible order* $\preceq$.

Definition 14. *A ring R which is left-polynomial over k in $x_1, \ldots, x_n$ is called a left* **Poincaré-Birkhoff-Witt ring** *(left PBW ring) if there exists an admissible order $\preceq$ on $(\mathbb{N}^n, +)$ that satisfies the following conditions:*

- $\forall\, 1 \leq i < j \leq n$, $\exists\, q_{ij} \in k \setminus \{0\}$ *s.t.* $\exp(x_j x_i - q_{ji} x_i x_j) \prec \epsilon_i + \epsilon_j$ *where* $\epsilon_i = (0, \ldots, 1, \ldots, 0) \in \mathbb{N}^n$.

- $\forall\, 1 \leq i \leq n$ *and* $\forall\, a \in k \setminus \{0\}$, $\exists\, q_{ja} \in k \setminus \{0\}$ *s.t.* $\exp(x_j a - q_{ja} x_j) \prec \epsilon_j$.

Let $p_{ji} = x_j x_i - q_{ji} x_i x_j$ *for* $1 \leq i < j \leq n$, *and* $p_{ja} = x_j a - q_{ja} x_j$ *for* $1 \leq i \leq n$ *and* $a \in k \setminus \{0\}$. *We denote the left PBW ring R as*

$$R = k\{x_1, \ldots, x_n;\, Q, Q', \prec\}$$

where

$$Q = \{x_j x_i = q_{ji} x_i x_j + p_{ji};\, 1 \leq i < j \leq n\}$$

and

$$Q' = \{x_j a = q_{ja} x_j + p_{ja};\, 1 \leq j \leq n,\, a \in k^*\}$$

Definition 15. *A left PBW ring R is called a* **PBW algebra** *if k is a commutative field and if $x_j a = a x_j$ for every $a \in k$ and $1 \leq j \leq n$.*

Lemma 4. *(Bueso et al.) Any left PBW ring is a domain.*

Hilbert Basis Theorem. *Every left PBW ring is left noetherian.*

Examples of PBW rings and algebras

- Commutative polynomial ring $k[x_1, \ldots, x_n]$: For every admissible order $\preceq$ on $\mathbb{N}^n$, we have

$$k[x_1, \ldots, x_n] = k\{x_1, \ldots, x_n;\ x_i x_j = x_j x_i,\ \preceq\}$$

  is a PBW algebra.

- Let g be a finite-dimensional Lie k-algebra with k basis $\{x_1, \ldots, x_n\}$. Let $\mathcal{U}(\mathrm{g})$ be its enveloping algebra. By the Poincaré-Birkhoff-Witt theorem, $\mathcal{U}(\mathrm{g})$ is left polynomial in $x_1, \ldots, x_n$, and it is noetherian (Bueso *et al.*). In general, $\mathcal{U}(\mathrm{g}) = T(\mathrm{g})/I$, where $T(\mathrm{g})$ is the tensor algebra over the linear space of g and I is a two-sided ideal generated by $x \otimes y - y \otimes x - [x, y]$, $\forall x, y \in \mathrm{g}$. Therefore, $\mathcal{U}(\mathrm{g})$ is a PBW algebra and

$$\mathcal{U}(\mathrm{g}) = k\{x_1, \ldots, x_n;\ x_i x_j = x_j x_i + [x_j, x_i],\ \preceq_{deglex}\}$$

- Let $\mathbf{q}$ be a multiplicatively anti-symmetric $n \times n$ matrix over k, i.e., $q_{i,j} \neq 0$ and $q_{i,j} = q_{j,i}^{-1}$ for all $1 \leq i, j \leq n$. The (multiparameter) n-**dimensional quantum space** $k_{\mathbf{q}}[x_1, \ldots, x_n]$ associated to $\mathbf{q}$ is the quotient of the free k-algebra $k\langle x_1, \ldots, x_n \rangle$ by the two-sided ideal associated to the relations $Q = \{x_j x_i = q_{ji} x_i x_j, j > i\}$. Let $\preceq$ be any admissible order on $\mathbb{N}^n$. Then

$$\mathcal{O}_{\mathbf{q}}(k^n) = k\{x_1, \ldots, x_n;\, Q, \preceq\}$$

  is a PBW algebra.

- There are constructive methods to obtain new (left) PBW rings as **Ore extensions** of a given (left) PBW ring. For example, skew polynomial Ore algebras and rings of differential operators are particular instances of the so called **iterated Ore extensions**. (Bueso *et al.*)

- The n-th Weyl algebra $\mathbb{A}_n(k)$ is a PBW algebra.

- Let R be a (left) PBW ring containing a division ring k as defined above. The multivariable division algorithm in R, the normal form of a polynomial f in R w.r.t. to a set F, the Gröbner bases in left-, and two-sided ideals are discussed at length in (Bueso *et al.*)

III. G-algebras and GR-algebras (Levandovskyy)

Definition 16. *Let $\prec$ be a total well-ordering on $\mathbb{N}^n$.*

1. Let A be an algebra with PBW basis and $\prec_A$ be an ordering on A induced by $\prec$. Then $\prec_A$ is a **monomial ordering** *on A if the following conditions hold $\forall \alpha, \beta, \gamma \in \mathbb{N}^n$:*

- *If $x^\alpha \neq 0, x^\beta \neq 0,$ then $\alpha \prec \beta \Rightarrow x^\alpha \prec x^\beta$,*
- *If $x^\alpha \prec x^\beta, x^{\alpha+\gamma} \neq 0$ and $x^{\beta+\gamma} \neq 0$ then $x^{\alpha+\gamma} \prec x^{\beta+\gamma}$.*

2. Any $f \in A \setminus \{0\}$ can be written uniquely as $f = cx^\alpha + f'$, with $c \in k^*$ and $x^{\alpha'} \prec_A x^\alpha$ for any non-zero term $c'x^{\alpha'}$ of f'. Define $\mathrm{lm}(f) = x^\alpha$ *as the* **leading monomial** *of f, and* $\mathrm{lc}(f) = c$ *as the* **leading coefficient** *of f.*

Constructing a G-algebra

Definition 17. *Let I be a two-sided ideal of $T = k\langle x_1, x_2, \ldots, x_n\rangle$ generated by the elements:*

$$x_j x_i - c_{ij} x_i x_j - d_{ij}, \quad 1 \le i < j \le n, \quad c_{ij} \in k^*, \quad d_{ij} \in T. \tag{26}$$

*A k-algebra $A = T/I = k\langle x_1, x_2, \ldots, x_n \mid x_j x_i = c_{ij} x_i x_j + d_{ij}, \forall 1 \le i < j \le n\rangle$ is called a G-**algebra in** n **variables**, if the following conditions hold:*

- **Ordering condition**: *There exists a monomial well-ordering $\prec$ on T such that* $\mathrm{lm}(d_{ij}) \prec x_i x_j, \forall 1 \le i < j \le n$.

- **Non-degeneracy condition**: $\forall 1 \le i < j < k \le n$, *define polynomials*

  $$NDC_{ijk} = c_{ik} c_{jk} \cdot d_{ij} x_k - x_k d_{ij} + c_{jk} \cdot x_j d_{ik} - c_{ij} \cdot d_{ik} x_j + d_{jk} x_i - c_{ij} c_{ik} \cdot x_i d_{jk}$$

  The condition is satisfied if all NDC_{ijk} reduce to 0 w.r.t. the relations (26).

Note: $NDC_{ijk} = x_k(x_j x_i) - (x_k x_j) x_i$.

Some important properties of G-algebras

Theorem 3 (Apel, Levandovskyy). *Let A be a G-algebra in n variables.*

- *A has a PBW basis $\{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \mid \alpha_k \in \mathbb{N}\}$.*
- *A is left and right Noetherian.*
- *A is an integral domain.*
- *A has a left and a right noetherian quotient ring.*

Definition 18 (Levandovskyy). *Let B be a G-algebra and $I \subset B$ be a proper nonzero two-sided ideal. Then the quotient algebra B/I is called a* **GR-algebra** *(***Gröbner-ready algebra***)*

Examples of G-algebras

- Quasi-commutative polynomial rings, for example, the quantum plane $\mathbb{C}_q[x, y] = \mathbb{C}[x, y]/I_q$, $0 \neq q \in \mathbb{C}$ where I_q is generated by $yx - q \cdot xy$. It is a noetherian domain a basis of which (as a vector space over $\mathbb{C}$, is given by the elements $x^i y^j$, where i, j are positive integers. Then, generalizations to quantum spaces $k_q[x_1, x_2, \ldots, x_n] = k\langle x_1, x_2, \ldots, x_n\rangle/I_q$ where I_q is a two-sided ideal generated by the relations $x_j x_i - q x_i x_j$ for $1 \leq i < j \leq n$. (Bueso *et al.*)

- Universal enveloping algebras of finite dimensional Lie algebras. (Apel, Levandovskyy)

- Positive (negative) parts of quantized enveloping algebras (Klimyk and Schmüdgen)

- Weyl algebras and their quantizations, Smith algebras, some diffusion algebras (Isaev *et al.*).

- For more examples see Levandovskyy.

- Computations with G- and GR-algebras can be performed with `Plural` .

Examples of GR-algebras (Levandovskyy)

- All G-algebras.
- $\boxed{\text{Grassmann algebras } \bigwedge V,}$ $\boxed{\text{Clifford algebras } C\ell(Q)}$ (Q may be degenerate)
- Finite dimensional associative algebras given by structure constants (Drozd and Kirichenko)
- Skew polynomial rings
- Universal enveloping algebras of finite dimensional Lie algebras

See Levandovskyy (2006) for definitions and computations of left Gröbner bases in G- and GR-algebras as well as two-sided Gröbner bases using `Plural`.

G- and GR-algebras in `Plural`

- G-algebras are defined using `ring` command extended to non-commutative variables.

- GR-algebra is defined as a quotient of a G-algebra modulo a two-sided ideal I. It is of the type `qring`, for example, `qring Q = twostd(I)`.

- There are various special-purpose libraries for pre-defined algebras. In particular, `clifford.lib` for Clifford algebras $C\ell(Q)$ and `nctools.lib` for non-commutative algebras including Grassmann algebra.

- In Grassmann algebra, a monomial order $<$ is **admissible** if:

  (1) $m > 1$ for every monomial m in the Grassmann basis;

  (2) If $m_2 > m_1$ then $m_l \wedge m_2 \wedge m_r > m_l \wedge m_1 \wedge m_r$ for all monomials m_1, m_2, m_l, and m_r as long as $m_l \wedge m_2 \wedge m_r \neq 0$ and $m_l \wedge m_1 \wedge m_r \neq 0$.

  The only admissible orders are: `Lex`, `InvLex`, `Deg[Lex]`, and `Deg[InvLex]`.

IV. Gröbner bases in Grassmann and Clifford algebras

Computed with `SINGULAR:PLURAL` and the `TNB` package that computes GLB and GLIB bases of Stokes. (Stokes) A Maple package `SINGULARPLURALlink` provides an interface between Maple and `SINGULAR:PLURAL`.

Example 6 Consider polynomials $f_1 = \mathbf{e}_5 \wedge \mathbf{e}_6 - \mathbf{e}_2 \wedge \mathbf{e}_3$ and $f_2 = \mathbf{e}_4 \wedge \mathbf{e}_5 - \mathbf{e}_1 \wedge \mathbf{e}_3$ in $\bigwedge V_6$ where $\dim_{\mathbb{R}} V = 6$. The Gröbner basis for the ideal $I = \langle f_1, f_2 \rangle$ in `Deg[Lex]` order returned by `Plural` and `TNB` is

$$\{\mathbf{e}_{145}, \mathbf{e}_{245} + \mathbf{e}_{156}, \mathbf{e}_{256}, \mathbf{e}_{345}, \mathbf{e}_{356}, \mathbf{e}_{13} - \mathbf{e}_{45}, \mathbf{e}_{23} - \mathbf{e}_{56}\} \tag{27}$$

See also (Stokes).

Example 7 Take $C\ell_{2,0} \cong \mathrm{Mat}(2, \mathbb{R})$ and a primitive idempotent $f = \frac{1}{2}(1 + \mathbf{e}_1)$. Let $S = C\ell_{2,0} f = \mathrm{span}_{\mathbb{R}}\{f, \mathbf{e}_2 f\}$ be a spinor ideal. Then a Gröbner basis for S is $h = 1 + \mathbf{e}_1$. Note that $h = 2f$ is an almost idempotent.

Example 8 Take $C\ell_{3,1} \cong \mathrm{Mat}(4, \mathbb{R})$ and $f = \frac{1}{4}(1 + \mathbf{e}_1)(1 + \mathbf{e}_{34})$, a primitive idempotent. Let $S = C\ell_{3,1} f = \mathrm{span}_{\mathbb{R}}\{f, \mathbf{e}_2 f, \mathbf{e}_3 f, \mathbf{e}_{23} f\}$ be a spinor ideal. Then, `PLURAL` returns the following nilpotent polynomial g as a Gröbner basis for S :

$$g = \mathbf{e}_{13} + \mathbf{e}_{14} - \mathbf{e}_3 - \mathbf{e}_4 = -\mathbf{e}_3 f, \quad g^2 = 0, \quad f = -\mathbf{e}_3 g. \tag{28}$$

Due to the relations (28), we have $S = C\ell_{3,1} f = C\ell_{3,1} g$. That is, as expected, f and g differ by a unit.

Example 9 (Brachey) Let $f_1 = e_{56} - e_{23}, f_2 = e_{45} - e_{13} \in \bigwedge_6$ and use degree inverse lex order `Deg[InvLex]` on $\bigwedge_6$. After following Stokes' Algorithm (Stokes) and computing ten S-polynomials with a package `TNB` , one finds the following GLB basis for the left ideal $I = \langle f_1, f_2 \rangle$: $\{e_{56} - e_{23}, e_{45} - e_{13}, e_{1236}, e_{1234}, e_{136} - e_{234}\}$ whereas a GLIB basis for I is: $\{e_{56} - e_{23}, e_{45} - e_{13}, e_{236}, e_{136} - e_{234}, e_{235}, e_{135}, e_{134}\}$.

V. Computational differences and similarities when computing Gröbner bases in $k[x_1, \ldots, x_n]$, and Grassmann and Clifford algebras

- $k[x_1, x_2, \ldots, x_n]$ is a domain for any field k–in fact, it is UFD. In particular, it has no nonzero zero divisors. Grassmann algebras are never domains whereas most Clifford algebras $C\ell(Q)$ are not domains either as they possess nontrivial idempotents $e^2 = e$, $e \neq 0, 1$, and $e(e - 1) = 0$.

- Let $R = k[x_1, x_2, \ldots, x_n]$ and k be a field. Then, R is a noetherian ring. In particular, every ideal in R is finitely generated, equiv., R has ACC, equiv., R satisfies the maximum condition: Every non-empty family $\mathcal{F}$ of ideals in R has a maximal element. Any quotient ring $k[x_1, x_2, \ldots, x_n]/I$ where I is any ideal, is also noetherian.

- Grassmann algebras and superalgebras are left noetherian (Stokes).

cont.

- Left and right ideals in Grassmann and Clifford algebras do not coincide due to non-commutativity whereas they are identical in $k[x_1, \ldots, x_n]$.

- In commutative rings $k[x_1, x_2, \ldots, x_n]$, the division algorithm terminates due to noetherianness of the ring. Some non-commutative algebras are not noetherian (Mora), therefore, the division algorithm may not terminate in general. However, Grassmann algebra is left noetherian as it has no infinite ascending chain of ideals (Stokes).

- When reducing an S-polynomial $S(f_i, f_j) \in R = k[x_1, x_2, \ldots, x_n]$ modulo a finite set of polynomials F while computing a Gröbner basis, suppose $\overline{S(f_i, f_j)}^F = 0$. Then, $\overline{m \cdot S(f_i, f_j)}^F = 0$ for any monomial $m = x^\alpha \in R$. This is often not the case in Grassmann or Clifford algebra due the presence of non-zero zero divisors. This complicates computation of Gröbner bases in these algebras.

Importance of Grassmann algebras in:

- Affine and projective geometries,

- Automatic theorem proving and geometric reasoning: The vanishing of several ‘hypothesis’ polynomials implies the vanishing of one or more ‘conclusion’ polynomials in the ideal of consequences of the ‘hypothesis’ polynomials,

- Grassmann algebra is suitable for algorithmic treatment when treated as graded-commutative algebra of ‘exterior polynomials’: Generalization of Buchberger’s algorithm to Gröbner Left Bases (GLB) and Gröbner Left Ideal Basis (GLIB) by Stokes (1990)

- Obtaining Gröbner bases in Grassmann algebras is more complicated than in PBW algebras, which are domains, due an abundance of zero divisors. This leads to two types of Gröbner bases: Gröbner Left Bases (GLB) and Gröbner Left Ideal Bases (GLIB). Such dichotomy of bases does not exist in PBW algebras.

VI. Final Comments

- Non-commutative Gröbner bases in Grassmann algebras and the issue of ideal membership surface when analyzing systems of partial differential equations that arise in physics, i.e., in exterior differential systems (Hartley and Tuckey 1995 and references therein).

- Hartley and Tuckey (1995) provide another approach through the so called *saturating sets* to Gröbner bases in Grassmann and Clifford algebras in a REDUCE package called `XIDEAL`.

- Ability to compute Gröbner bases for one- and two-sided ideals in Grassmann and Clifford algebras allows for deciding on the ideal membership, computing bases for ideal intersections, sums, ideal quotients, etc. following the standard ideal treatment in a ring theory.

References

1. Abłamowicz, R.: `SINGULARPLURALlink` - An interface between Maple and `Singular:Plural`, 2008
2. Apel, J.: Gröbnerbasen in nichtkommutativen algebren und ihre anwendung. Dissertation, Universität Leipzig, 1988
3. Becker, T., and Weispfenning, V.: *Gröbner Bases*, Springer, 1993
4. Brachey, T.: *Gröbner Basis Algorithms for Grassmann Algebras in a Maple Package*, M.S. Thesis, Tennessee Technological University, 2008
5. Buchberger, B.: Gröbner base: an algorithmic method in polynomial ideal theory, in *Multidimensional Systems Theory*, N.K. Bose, ed., D. Reidel, 184–232, 1985
6. Buchberger, B.: Introduction to Gröbner bases, in Proc. Marktoberdorf Summer School 1995, Springer 1997
7. Buchberger, B., and Winkler, F.: *Gröbner Bases and Applications*, eds., Cambridge University Press, 1998
8. Bueso, José L., Gómez-Torrecillas, José, and Verschoren, A.: *Algorithmic Methods in Non-Commutative Algebra - Applications to Quantum Groups*, Kluwer, 2003

9. Cox, D.: Introduction to Gröbner bases, in *Proceedings of Symposia in Applied Mathematics*, Volume **53**: 1–24, 1998
10. Cox, D., Little, J., and O'Shea, D.: *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Springer, 2007
11. Drozd, Y., and Kirichenko, V.: *Finite Dimensional Algebras With an Appendix by Vlastimil Dlab*, Springer, 1994
12. Faugè, Jean-Charles: FGb, `http://fgbrs.lip6.fr/jcf/Software/FGb/`, 2008
13. Fearnly-Sander, D.: The idea of a diagram, in *Resolution of Equations in Algebraic Structures*, H. Ait-Kaçi and M. Nivat, eds., Academic Press, 1989
14. Grabmeier, J., Kaltofen, E., and Weispfenning, V.: Computer Algebra *Handbook*, eds. Springer, 2003
15. Gröbner Basis Bibliography at Johann Radon Institute for Computational and Applied Mathematics (RICAM), `www.ricam.oeaw.ac.at/Groebner-Bases-Bibliography/`, 2008
16. Hartley, D., and Tuckey, Ph.: Gröbner bases in Clifford and Grassmann Algebras, Preprint, 1995

17. Hayworth, A.: One sided non-commutative Gröbner bases with applications to computing Green's relations, arXiv:math.RA/9903033 v1 5 March 1999
18. Isaev, A., Pyatov, P., and Rittenberg, V.: Diffusion algebras. arXiv.math. QA/0103603, 2001
19. Klimyk, A., and Schmüdgen, K.: *Quantum Groups and Their Representations*, Springer, 1997
20. Levandovskyy, V.: PBW bases, non-degeneracy conditions and applications. In: Buchweitz, R.-O. and Lenzing, H. (eds.): *Proc. of the ICRA X conference, Toronto, Canada. AMS. Fields Institute Communications*, 229-246, 2005
21. Levandovskyy, V.: Manipulation within Clifford algebras in `Singular:Plural`, Private communication, 2006
22. Levandovskyy, V.: On Gröbner bases for non-commutative G-algebras. In Kredel, H. and Seiler, W.K. (eds.): *Proc. of the 8th Rhine Workshop on Computer Algebra*, 2002
23. Levandovskyy, V.: `Plural` , a non-commutative extension of `Singular` : Past, present and future. In: A. Iglesias, N. Takayama (eds.): *Proc. of International Congress on Mathematical Software*. LNCS 4151, Springer, 2006

24. Levandovskyy, V., and Schönemann, H.: `Plural` - a computer algebra system for non-commutative polynomial algebras, ISSAC'03, August 3–6, 2003

25. `Singular:Plural`: `www.singular.uni-kl.de/`, 2008

26. Mora, T.: *An introduction to commutative and non-commutative Gröbner bases*, *Theor. Comp. Sci.* **134**: 131–173, 1994

27. Rotman, J.: *Advanced Modern Algebra*, Prentice Hall, 2002

28. Stokes, T.: Gröbner bases in exterior algebra, *J. of Automated Reasoning* **6**: 233–250 (1990)