Subalgebra Analogue to H-Bases for Ideals

28th August, 2018

- The concept of Groebner bases, introduced by Buchberger in 1965, has become an important ingredient for the treatment of various problems in computational algebra. All approaches related to Groebner bases are fundamentally tied to monomial orderings, which lead to asymmetry among the variables of interest.

[1]F. S. Macaulay, The algebraic theory of modular systems, Cambridge Tracts in Math and Math. Physics, no. 19, Cambridge University Press (1916)

[2]H.M. Möller and T. Sauer, H-bases for polynomial interpolation and system solving, Advances in Computational Mathematics 12, 335-362 (2000)

- The concept of Groebner bases, introduced by Buchberger in 1965, has become an important ingredient for the treatment of various problems in computational algebra. All approaches related to Groebner bases are fundamentally tied to monomial orderings, which lead to asymmetry among the variables of interest.
- On the other hand, the concept of H-bases for ideals[1], introduced long ago by Macaulay, is based solely on homogeneous terms of a polynomial. These bases have many applications too[2].

[1] F. S. Macaulay, The algebraic theory of modular systems, Cambridge Tracts in Math and Math. Physics, no. 19, Cambridge University Press (1916)

[2] H.M. Möller and T. Sauer, H-bases for polynomial interpolation and system solving, Advances in Computational Mathematics 12, 335-362 (2000)

- Since the properties and applications of Sagbi bases are typically similar to standard Groebner bases results, it is natural to probe the concept of Subalgebra bases which may be based solely on homogeneous terms of a polynomial.

- Since the properties and applications of Sagbi bases are typically similar to standard Groebner bases results, it is natural to probe the concept of Subalgebra bases which may be based solely on homogeneous terms of a polynomial.
- In this paper we present the analogue to H-bases for ideals, we call them SH-bases.We present their connection to the Sagbi basis concept, characterize SH-basis and show how to construct them.

Notation

We consider polynomials in n variables $x_1, \ldots, x_n$ with coefficients from a field K. For short, we write

$$\mathcal{P} := K[x_1, \ldots, x_n].$$

Notation

We consider polynomials in n variables $x_1, \ldots, x_n$ with coefficients from a field K. For short, we write

$$\mathcal{P} := K[x_1, \ldots, x_n].$$

If G is a subset of $K[x_1, \ldots, x_n]$ (not necessarily finite), then the subalgebra of $\mathcal{P}$ generated by G is $K[G]$.

Let Γ denote an ordered monoid, i.e., an abelian semigroup under an operation $+$, equipped with a total ordering $>$ such that, for all $\alpha, \beta, \gamma \in \Gamma$,

$$\alpha > \beta \Longrightarrow \alpha + \gamma > \beta + \gamma.$$

Let Γ denote an ordered monoid, i.e., an abelian semigroup under an operation $+$, equipped with a total ordering $>$ such that, for all $\alpha, \beta, \gamma \in \Gamma$,

$$\alpha > \beta \Longrightarrow \alpha + \gamma > \beta + \gamma.$$

A direct sum

$$\mathcal{P} := \bigoplus_{\gamma \in \Gamma} \mathcal{P}_{\gamma}^{(\Gamma)}$$

is called grading (induced by Γ) or briefly a Γ-grading if for all $\alpha, \beta \in \Gamma$

$$f \in \mathcal{P}_{\alpha}^{(\Gamma)}, g \in \mathcal{P}_{\beta}^{(\Gamma)} \Longrightarrow f \cdot g \in \mathcal{P}_{\alpha+\beta}^{(\Gamma)}$$

Since the decomposition above is a direct sum, each polynomial $f \neq 0$ has a unique representation

$$f = \sum_{i=1}^{s} f_{\gamma_i}, \qquad 0 \neq f_{\gamma_i} \in \mathcal{P}_{\gamma_i}^{(\Gamma)}.$$

Since the decomposition above is a direct sum, each polynomial $f \neq 0$ has a unique representation

$$f = \sum_{i=1}^{s} f_{\gamma_i}, \quad 0 \neq f_{\gamma_i} \in \mathcal{P}_{\gamma_i}^{(\Gamma)}.$$

Assuming that $\gamma_1 > \gamma_2 > \ldots > \gamma_s$, the Γ-homogeneous term f_{γ_1} is called the maximal part of f, denoted by $M^{(\Gamma)}(f) := f_{\gamma_1}$, and $f - M^{(\Gamma)}(f)$ is called the d-reductum of f. For $G \subset \mathcal{P}$, $M^{(\Gamma)}(G) := \{ M^{(\Gamma)}(g) \,|\, g \in G \}$.

There are two major examples of gradings. The first one is grading by degrees,

There are two major examples of gradings. The first one is grading by degrees,

$$\mathcal{P}_d^{(\Gamma)} = \{p \in \mathcal{P} \,|\, p \text{ homogenous of degree } d\} \quad \forall\, d \in \mathbb{N}.$$

Here, $\Gamma = \mathbb{N}$ with the natural total ordering. This grading is called the H-grading because of the homogeneous polynomials. Therefore we also write H in place of this Γ.

There are two major examples of gradings. The first one is grading by degrees,

$$\mathcal{P}_d^{(\Gamma)} = \{p \in \mathcal{P} \,|\, p \text{ homogenous of degree } d\} \quad \forall\, d \in \mathbb{N}.$$

Here, $\Gamma = \mathbb{N}$ with the natural total ordering. This grading is called the H-grading because of the homogeneous polynomials. Therefore we also write H in place of this Γ. The space of all polynomials of degree at most d can now be written as

$$\mathcal{P}_d := \bigoplus_{k=0}^{d} \mathcal{P}_k^{(H)}.$$

There are two major examples of gradings. The first one is grading by degrees,

$$\mathcal{P}_d^{(\Gamma)} = \{p \in \mathcal{P} \,|\, p \text{ homogenous of degree } d\} \quad \forall\, d \in \mathbb{N}.$$

Here, $\Gamma = \mathbb{N}$ with the natural total ordering. This grading is called the H-grading because of the homogeneous polynomials. Therefore we also write H in place of this Γ. The space of all polynomials of degree at most d can now be written as

$$\mathcal{P}_d := \bigoplus_{k=0}^{d} \mathcal{P}_k^{(H)}.$$

The maximal part of a polynomial $f \neq 0$ is its homogeneous form of highest degree, $M^{(H)}(f)$. For simplicity, let $M^{(H)}(0) := 0$.

Definition

A subset G of $\mathcal{P}$ is called **SH- basis** of the subalgebra $\mathcal{A}$ of $\mathcal{P}$ if, for all $0 \neq f \in \mathcal{A}$, there exist G-monomials G^{α_i} and $c_i \in K$, $i = 1, \ldots, p$ such that

$$f = \sum_{i=1}^{p} c_i G^{\alpha_i} \quad \text{and} \quad \max_{i=1}^{p}\{\deg(G^{\alpha_i})\} = \deg(f)$$

The representation for f is also called its SH-representation with respect to G.

Definition

Let $f \in \mathcal{P}$ and $G \subset \mathcal{P}$. We say f d-reduces to $\widetilde{f}$ with respect to G if

$$\widetilde{f} = f - \sum_{i=1}^{m} c_i G^{\alpha_i}, \quad \deg(\widetilde{f}) < \deg(f),$$

holds with G-monomials G^{α_i} satisfying $\deg(G^{\alpha_1}) \leq \deg(f)$, $i = 1, \ldots, m$. In this case we write

$$f \to_G \widetilde{f}.$$

By $\to_{G,*}$ we denote the transitive closure of the binary relation $\to_G$[3].

[3] $f \to_{G,*} h$ if we apply d-reduction iteratively such as $f \to_G h_1 \to_G h_2 \ldots \to_G h$, where h cannot be d-reduced any further with respect to G.

Algorithm 1

Input: Let G and f be subset and polynomial respectively in $\mathcal{P}$.
Output: $h \in \mathcal{P}$ such that $f \rightarrow_{G,*} h$.

1: $h := f$.
2: while $(h \neq 0$ and $G_h = \{\sum_i c_i G^{\alpha_i} \mid M^{(H)}(\sum_i c_i G^{\alpha_i}) = M^{(H)}(h)\} \neq \emptyset)$
3: (a) choose $\sum_i c_i G^{\alpha_i} \in G_h$.
(b) $h := h - \sum_i c_i G^{\alpha_i}$ and continue at 2.

Algorithm 1

Input: Let G and f be subset and polynomial respectively in $\mathcal{P}$.
Output: $h \in \mathcal{P}$ such that $f \to_{G,*} h$.

1: $h := f$.
2: while $(h \neq 0$ and $G_h = \{\sum_i c_i G^{\alpha_i} \mid M^{(H)}(\sum_i c_i G^{\alpha_i}) = M^{(H)}(h)\} \neq \emptyset)$
3: (a) choose $\sum_i c_i G^{\alpha_i} \in G_h$.
(b) $h := h - \sum_i c_i G^{\alpha_i}$ and continue at 2.

Remark:
We note that when step $2(b)$, has been performed, then $\deg(h)$ is strictly smaller than the $\deg(h - \sum_i c_i G^{\alpha_i})$ (by the choice of $\sum_i c_i G^{\alpha_i}$). This shows that the Algorithm 1 always terminate.

Characterization of SH-Basis

Theorem

Let $G \subset \mathcal{P}$ and $\mathcal{A}$ be a subalgebra of $\mathcal{P}$. Then the following conditions are equivalent:

i) G is an SH-basis of $\mathcal{A}$.

ii) $K[\{M^{(H)}(g) \mid g \in G\}] = K[\{M^{(H)}(f) \mid f \in \mathcal{A}\}]$.

iii) For all $f \in \mathcal{A}$, $f \to_{G,*} 0$.

SH-Bases and Sagbi Bases

We see an example of gradings that leads to the Sagbi basis concept. Here, $\Gamma = \mathbb{N}^n$ with componentwise addition and equipped with a total ordering, in addition, $\gamma \geq 0 \ \forall \gamma \in \Gamma$. For arbitrary $\gamma = (\gamma_1, \ldots, \gamma_n) \in \Gamma$, the space $\mathcal{P}_\gamma^{(\Gamma)}$ is a vector space of dimension 1, namely,

$$\mathcal{P}_\gamma^{(\Gamma)} = \{\, c \cdot x^{\gamma_1} \ldots x^{\gamma_n} \,|\, c \in K \,\}.$$

SH-Bases and Sagbi Bases

We see an example of gradings that leads to the Sagbi basis concept. Here, $\Gamma = \mathbb{N}^n$ with componentwise addition and equipped with a total ordering, in addition, $\gamma \geq 0 \ \forall \gamma \in \Gamma$. For arbitrary $\gamma = (\gamma_1, \ldots, \gamma_n) \in \Gamma$, the space $\mathcal{P}_\gamma^{(\Gamma)}$ is a vector space of dimension 1, namely,

$$\mathcal{P}_\gamma^{(\Gamma)} = \{\, c \cdot x^{\gamma_1} \ldots x^{\gamma_n} \,|\, c \in K \,\}.$$

The maximal part of a polynomial is now a product of a leading coefficient and a leading monomial, $M^{(\Gamma)}(f) = LC(f) \cdot LM(f)$, $LC(f) \in K, LM(f)$ a leading monomial.

If a monomial ordering is compatible with the semi-ordering by degrees,

$$\deg(x^\gamma) > \deg(x^\beta) \Longrightarrow \gamma > \beta, \quad \gamma, \beta \in \mathbb{N}^n$$

then any Sagbi-representation is an SH-representation, in other words, a Sagbi basis with respect to a degree compatible ordering is an SH-basis as well. The converse is false, as the following example shows.

Example

Let $f_1 = x^3 + x^2y$, $f_2 = y^3$, $f_3 = xy + y$ and $\mathcal{A} = K[f_1, f_2, f_3]$. Then f_1, f_2 and f_3 already constitute an SH-basis of $\mathcal{A}$. (This is consequence of previous theorem). If we order the monomials by degree lexicographical ordering then

$$K[\{M^{(H)}(f) \mid f \in \mathcal{A}\}] = K[x^3, y^3, xy, x^2y^4].$$

Example

Let $f_1 = x^3 + x^2y$, $f_2 = y^3$, $f_3 = xy + y$ and $\mathcal{A} = K[f_1, f_2, f_3]$. Then f_1, f_2 and f_3 already constitute an SH-basis of $\mathcal{A}$. (This is consequence of previous theorem). If we order the monomials by degree lexicographical ordering then

$$K[\{M^{(H)}(f) \mid f \in \mathcal{A}\}] = K[x^3, y^3, xy, x^2y^4].$$

Every Sagbi basis G with respect to this ordering contains at least four elements, for instance SINGULAR computes $G = \{g_1, g_2, g_2, g_4\}$ with

$$g_1 = x^3 + x^2y = f_1$$

$$g_2 = y^3 = f_2$$

$$g_3 = xy + y = f_3$$

$$g_4 = x^2y^4 - 3x^2y^3 - 3xy^3$$

Obviously, this Sagbi basis is an SH-basis as well.

It is possible that a subalgebra has a finite SH-basis, but no finite Sagbi basis, as the following example shows.

It is possible that a subalgebra has a finite SH-basis, but no finite Sagbi basis, as the following example shows.

Example

Let $G = \{f_1, f_2, f_3\} \subset K[x, y]$ where $f_1 = x + y$, $f_2 = xy$, $f_3 = xy^2$ and $\mathcal{A} = K[G]$. It is easy to see that G is an SH-basis of $\mathcal{A}$. However, the set $S = \{x + y, xy, xy^2, xy^3, xy^4, \ldots\} \subset \mathcal{A}$ is an infinite Sagbi basis for $\mathcal{A}$ with respect to a monomial ordering $x > y$.

Definition

Let $G = \{g_1, \ldots, g_s\}$ be a subset of $K[x_1, \ldots, x_n]$. We denote $AR((M^{(H)}(G))$, the ideal of algebraic relations between $M^{(H)}(g_i), i = 1, \ldots, s$ defined by:

Definition

Let $G = \{g_1, \ldots, g_s\}$ be a subset of $K[x_1, \ldots, x_n]$. We denote $AR((M^{(H)}(G))$, the ideal of algebraic relations between $M^{(H)}(g_i), i = 1, \ldots, s$ defined by:

$$AR((M^{(H)}(G)) = \{h \in K[y_1, \ldots, y_s] \,|\, h(M^{(H)}(g_1)), \ldots, M^{(H)}(g_s)) = 0\}$$

$AR((M^{(H)}(G))$ is an ideal in $K[y_1, \ldots, y_s]$.

SH-basis criterion

Theorem

Let $G = \{g_1, \ldots, g_s\}$ be a subset of $K[x_1, \ldots, x_n]$. Let $\mathcal{A} = K[G]$ and let $\{P_j(Y) \mid j \in J\}$ be a finite set of G-homogenous generators for $AR((M^{(H)}(G))$. Then the following conditions are equivalent:

i) G is an SH-basis of $\mathcal{A}$.

ii) For each $j \in J$, $P_j(G) = P_j(g_1, \ldots, g_s) \rightarrow_{G,*} 0$.

Algorithm 2

On the basis of above criterion, now we present an algorithm which computes SH-basis from a given set of generators. This algorithm is not necessarily terminating but does terminate, if and only if, the considered subalgebra has a finite SH-basis.

Algorithm 2

On the basis of above criterion, now we present an algorithm which computes SH-basis from a given set of generators. This algorithm is not necessarily terminating but does terminate, if and only if, the considered subalgebra has a finite SH-basis.

Input: A finite subset $G \subset \mathcal{P}$.
Output: SH-basis G.

1: Compute a generating set $\mathcal{S}$ for $AR(M^{(H)}(G))$.
2: For $P \in \mathcal{S}$
3: (a) $h \in \mathcal{P}$, such that $P(G) \rightarrow_{G,*} h$.
(b) If $h \neq 0$, set $G := G \cup \{h\}$ and continue at 1.

Remark:
We have implemented SH-basis construction algorithm in the computer algebra system SINGULAR[4]. Code can be download from mathcity.org/junaid.

[4] G-M. Greuel, G. Pfister and H. Schönemann, SINGULAR - A Computer Algebra System for Polynomial Computations, Free software under GNU General Public Licence (1990-to date)

Example 1

The subalgebra $\mathcal{A} \subset \mathcal{P}$ of symmetric polynomials is well known to be finitely generated by a set S which is a set of elementary symmetric polynomials in $\mathcal{P}$. The set S is an SH-basis of $\mathcal{A}$ as $AR(M^{(H)}(S)) = \{0\}$ i.e, there is no polynomial $0 \neq P(Y) \in K[y_1, \ldots, y_n]$ such that $P(S) = 0$.

Example 1

The subalgebra $\mathcal{A} \subset \mathcal{P}$ of symmetric polynomials is well known to be finitely generated by a set S which is a set of elementary symmetric polynomials in $\mathcal{P}$. The set S is an SH-basis of $\mathcal{A}$ as $AR(M^{(H)}(S)) = \{0\}$ i.e, there is no polynomial $0 \neq P(Y) \in K[y_1, \ldots, y_n]$ such that $P(S) = 0$.

Example 2

Let $G = \{ x + y + 1, x^2 + y^2 - x + 2, 2xy - y\}$ and $\mathcal{A} = \mathbb{Q}[G]$. The ideal $AR((M^{(H)}(G)) = AR(x + y, x^2 + y^2, xy)$ in $\mathbb{Q}[y_1, y_2, y_3]$ is generated by $P(Y) = y_1^2 - y_2 - y_3$. It is easy to see that the polynomial $P(G) = 3x + 3y - 1 \rightarrow_{G,*} 0$. This shows that G is an SH-basis of $\mathcal{A}$.

The next example shows that there are finitely generated algebras which do not admit a finite SH-basis.

The next example shows that there are finitely generated algebras which do not admit a finite SH-basis.

Example 3

Let $G = \{ g_1 = xz + y, g_2 = xyz, g_3 = xy^2z \}$ and $\mathcal{A} = \mathbb{Q}[G]$. Also we have $M^{(H)}(g_1) = xz, M^{(H)}(g_2) = xyz$ and $M^{(H)}(g_3) = xy^2z$.

The next example shows that there are finitely generated algebras which do not admit a finite SH-basis.

Example 3

Let $G = \{ g_1 = xz + y, g_2 = xyz, g_3 = xy^2z\}$ and $\mathcal{A} = \mathbb{Q}[G]$. Also we have $M^{(H)}(g_1) = xz, M^{(H)}(g_2) = xyz$ and $M^{(H)}(g_3) = xy^2z$. In first step, $G = \{ g_1 = xz + y, g_2 = xyz, g_3 = xy^2z\}$. It is evident that the ideal of relations $AR(M^{(H)}(G)) = AR(xz, xyz, xy^2z) \subset \mathbb{Q}[y_1, y_2, y_3]$ is generated by $P(Y) = y_1y_3 - y_2^2$. The polynomial $P(G) = (xz + y)(xy^2z) - (xyz)^2 = xy^3z \twoheadrightarrow_{G,*} 0$, so $G := G \cup \{g_4 = xy^3z\}$.

In second step, $G = \{ g_1 = xz + y, g_2 = xyz, g_3 = xy^2z, g_4 = xy^3z\}$. The polynomial $P(Y) = y_1y_4 - y_2y_3$ is one the generators of the ideal of relations $AR(M^{(H)}(G)) = AR(xz, xyz, xy^2z, xy^3z) \subset \mathbb{Q}[y_1, y_2, y_3, y_4]$. Here we note that the polynomial $P(G) = (xz + y)(xy^3z) - (xyz)(xy^3z) = xy^4z \twoheadrightarrow_{G,*} 0$, therefore we have $G := G \cup \{xy^4z\} = \{ g_1 = xz + y, g_2 = xyz, g_3 = xy^2z, g_4 = xy^3z, g_5 = xy^4z\}$.

In second step, $G = \{ g_1 = xz + y, g_2 = xyz, g_3 = xy^2z, g_4 = xy^3z\}$. The polynomial $P(Y) = y_1y_4 - y_2y_3$ is one the generators of the ideal of relations $AR(M^{(H)}(G)) = AR(xz, xyz, xy^2z, xy^3z) \subset \mathbb{Q}[y_1, y_2, y_3, y_4]$.
Here we note that the polynomial
$P(G) = (xz + y)(xy^3z) - (xyz)(xy^3z) = xy^4z \twoheadrightarrow_{G,*} 0$, therefore we have $G := G \cup \{xy^4z\} = \{ g_1 = xz + y, g_2 = xyz, g_3 = xy^2z, g_4 = xy^3z, g_5 = xy^4z\}$.
By induction, we get $G = \{xz + y, xyz, xy^2z, xy^3z, xy^4z, xy^5z, \ldots\}$ which implies that $\mathcal{A}$ have an infinite SH-basis.

Thank you!