数理解析研究所講究録
第 1809 巻 2012 年 205-212

Homogenized modular algorithms for Gröbner bases

YUJI KOBAYASHI

Department of Information Science, Toho University,
Funabashi 274-8510, Japan

1 Introduction

Gröbner bases and the Buchberger algorithm (Buchberger [3]) are now central techniques in Computational Algebra ([2]). One of serious problems is the intermediate swell of the size of the coefficients of polynomials during computation of Gröbner bases (Ebert [4]).

To avoid this, the modular algorithm is considered to be useful (Winkler [5]). Choosing a suitable prime p compute a Gröbner basis $\overline{G}$ over the field $\mathbb{Z}_p=\mathbb{Z}/(p)$, then reconstruct a system G over $\mathbb{Z}$ from $\overline{G}$. If p is large enough and lucky, G is a correct Gröbner basis. But there is no effective way to check that p is lucky and large enough beforehand.

Let H be a finite set of polynomials in $\mathbb{Z}[X]=\mathbb{Z}[X_1, \ldots, X_n]$ and let p be a prime number. For a polynomial f in $\mathbb{Z}[X]$, f_p denotes the polynomial on $\mathbb{Z}_p[X]$ induced from f. Moreover, define $H_p=\{f_p|f\in H\}$. Let $>$ be a term order on $\mathbb{Z}[X]$ and $\overline{G}$ be the Gröbner basis obtained by the Buchberger algorithm from H_p on $\mathbb{Z}_p[X]$. Let G be a set of polynomial in $\mathbb{Z}[X]$ such that $G_p=\overline{G}$.

To see that G is a Gröbner basis we check that (i) every S-polynomial of G is reduced to 0 modulo G. If this is checked, then G is a Gröbner basis of 'some' ideal of $\mathbb{Z}[X]$. To see that G is a Gröbner basis of the ideal $I(H)$ generated by H, we check that (ii) every $h\in H$ is reduced to 0 modulo G. If this is checked, $I(H)\subset I(G)$ holds. Here, if the converse inclusion $G\subset I(H)$ is satisfied, G is a correct Gröbner basis for H.

Arnold [1] proved that if H is homogeneous, the converse inclusion holds if the conditions (i) and (ii) above are checked. If H is not homogeneous, we homogenize it to ${}^{h}G$, and complete it to G' by the modular algorithm, and then ahomogenizing it we obtain the Gröbner basis $G={}^{a}G'$ of $I(H)$. In this note we examine these steps precisely.

2 Compatible orders and weights

A *quasi-order* $\geq$ on a set A is a reflexive, transitive and comparable relation on A. For $a, b\in A$ we write $x\sim y$ if $x\geq y$ and $y\geq x$, and $x>y$ if $x\geq y$ and

$(x \not\succ y)$.

A quasi-order $\geq$ on A is *well-founded* if there is no infinite decreasing sequence $a_1 > a_2 > \dots$, or equivalently, any nonempty subset of A has a minimal element. A well-founded order is a *well-order.*

Let $X = \{X_1, X_2, ..., X_r\}$ be a finite set of symbols (variables). Let $M(X)$ be the set of (monic) monomials, that is, $M(X)$ is the free abelian monoid generated by X. Any element x in $M(X)$ is written as

$$x = X_1^{e_1} X_2^{e_2} \cdots X_r^{e_r} \tag{1}$$

with $e_i \in \mathbb{N} = \{0, 1, 2, \dots\}$, in particular, 1 denotes the identity element (the empty monomial). For another $y = X_1^{f_1} X_2^{f_2} \cdots X_r^{f_r} \in M(X)$, we have

$$xy = X_1^{e_1+f_1} X_2^{e_2+f_2} \cdots X_r^{e_r+f_r}.$$

From now on we consider only (quasi-)orders on $M(X)$.

A quasi-order on $M(X)$ is *compatible*, if

$$x \geq y \;\Rightarrow\; sxt \geq syt$$

for any $x, y, s, t \in M(X)$. It is *positive* (resp. *non-negative*), if

$$x > 1 \text{ (resp. } x \geq 1)$$

for any $x \, (\neq 1) \in M(X)$.

As is well known as a variant of Dickson's lemma (see [2]), a non-negative compatible quasi-order on $M(X)$ is well-founded.

A *weight function* (simply a *weight*) ω is a homomorphism from $M(X)$ to the additive group $\mathbb{R}$ of real numbers. The weight ω is determined by the values $\omega(X_i)$ of $X_i \in X$. In fact, for $x \in M(X)$ in (1) we have

$$\omega(x) = e_1\omega(X_1) + e_2\omega(X_2) + \cdots + e_r\omega(X_r).$$

The set of weights on $M(X)$ forms an $\mathbb{R}$-space of dimension d.

A weight ω is *positive* (resp. *non-negative*), if

$$\omega(X_i) > 0 \;\; (\text{resp. } \omega(X_i) \geq 0)$$

for every i. It is *rational* (resp. *integral*), if

$$\omega(X_i) \in \mathbb{Q} \;\; (\text{resp. } \omega(X_i) \in \mathbb{Z})$$

for every i. The degree function deg is a typical positive integral weight.

For a weight ω, the associated quasi-order $\geq_\omega$ is defined by

$$x \geq_\omega y \;\Leftrightarrow\; \omega(x) \geq \omega(y)$$

for $x, y \in M(X)$.

For a weight ω on $M(X)$, $\geq_\omega$ is a compatible quasi-order on $M(X)$. If ω is positive (resp. non-negative), so is $\geq_\omega$ and it is well-founded.

A weight ω is $\geq$-*monotone* (simply *monotone*), if

$$x \geq y \Rightarrow \omega(x) \geq \omega(y),$$

or equivalently,

$$\omega(x) > \omega(y) \Rightarrow x > y$$

for $x, y \in M(X)$.

3 Gröbner bases

Let K be a field and let $K[X]$ be the polynomial ring in $X_1, X_2, \ldots, X_r$ over K. A compatible positive order on $M(X)$ is called a *term order*, and we fix a term order $\geq$ in this section.

For a polynomial

$$f = \sum_{x \in M(X)} k_x \cdot x \quad (k \in K) \tag{2}$$

in $K[X]$, the maximal x such that $k_x \neq 0$ is the *leading monomial* of f denoted by $\mathrm{lt}(f)$, here k_x is the *leading coefficient* denoted by $\mathrm{lc}(f)$ and $k_x \cdot x = \mathrm{lc}(f) \cdot \mathrm{lm}(f)$ is the *leading term* denoted by $\mathrm{lt}(f)$. We set $\mathrm{rt}(f) = f - \mathrm{lt}(f)$. For a subset G of $K[X]$, set

$$\mathrm{lm}(G) = \{\mathrm{lm}(g) \mid g \in G\}.$$

We extend $\geq$ to the quasi-order $\geq$ on $M(X)$ as follows. First,

(i) $f > 0$

for any nonzero $f \in K[X]$, and

(ii) $f \geq g$ if $\mathrm{lm}(f) > \mathrm{lm}(g)$ or $\big(\mathrm{lm}(f) = \mathrm{lm}(g)$ and $\mathrm{rt}(f) \geq \mathrm{rt}(g)\big)$

for any nonzero $f, g \in K[X]$.

Let $G \subset K[X]$. If some term of $f \in K[X]$ is divided by $\mathrm{lm}(g)$ for some $g \in G$, f is *G-reducible*, otherwise, f is *G-irreducible*. Let $\mathrm{Red}(G)$ (resp. $\mathrm{Irr}(G)$) denote the set of G-reducible (resp. G-irreducible) monomials. Clearly,

$$\mathrm{Red}(G) = \mathrm{lm}(G) \cdot M(X), \ \mathrm{Irr}(G) = M(X) \setminus \mathrm{Red}(G).$$

For $f \in K[X]$, if some term $k \cdot x\,(k \in K \setminus \{0\}, x \in M(X))$ of f is G-reducible; $x = x' \cdot \mathrm{lm}(g)$ for some $x' \in K[X]$ and $g \in G$, then we can *rewrite* f to

$$f' = f - k \cdot x' \left(\mathrm{lm}(g) - \frac{\mathrm{rt}(g)}{lc(g)}\right) = f - \frac{k}{\mathrm{lc}(g)} \cdot x'g.$$

In this situation we write as

$$f \to_G f'.$$

The reflexive transitive closure of the relation $\to_G$ is denoted by $\to_G^*$. If $f \to_G^* f'$ for $f, f' \in K[X]$, we say that f is *reduced* to f' modulo G.

Let I be an ideal of $K[X]$. A finite set $G \subset K[X]$ is a *Gröbner basis* of I, if
(i) $G \subset I$, and
(ii) every $f \in I$ is reduced to 0 modulo G.
The condition (ii) is equivalent to the inclusion $\mathrm{lm}(I) \subset \mathrm{Red}(G)$.

G is *reduced*, if any $g \in G$ is $(G \setminus \{g\})$-irreducible. G is *monic*, if every $f \in G$ is monic, that is $\mathrm{lc}(f) = 1$. Any ideal in $K[X]$ has a unique monic reduced Gröbner basis (if the order $\geq$ is fixed).

Lemma 3.1. *Let I be an ideal, and for $x \in \mathrm{lm}(I)$ choose one f_x in I such that $\mathrm{lm}(f_x) = x$. Then, $\{f_x\}_{x \in \mathrm{lm}(I)}$ is a K-linear base of I. If is G a Gröbner basis of I, then $\{f_x\}_{x \in \mathrm{Red}(G)}$ is a K-linear base of I.*

Suppose that K is the quotient field of an integral domain R. Let P be a maximal ideal of R and let ρ_P be the canonical surjection from R to the quotient $\overline{R} = R/P$. The homomorphism ρ_P extends to the homomorphism ρ: $R[X] \to \overline{R}[X]$.

Proposition 3.2. *With the situation above, suppose that a subset G of $R[X]$ is a Gröbner basis of an ideal I of $K[X]$. If $lc(G)$ is out of P, then $G_P = \rho_P(G)$ is a Gröbner basis of the ideal $I_P = \rho_P(I \cap R[X])$ in $R_P[X]$.*

4 Homogeneous ideals

Let ω be a weight on $M(X)$ and let $v \in \mathbb{R}$. A polynomial $f \in K[X]$ is *ω-homogeneous* (we simply say homogeneous) of weight v, if all the monomials in f have the same weight v. In this case v is the *weight* of f and we write $\omega(f) = v$. Any polynomial f is decomposed as a sum of the homogeneous polynomials;

$$f = \sum_{v \in \mathbb{R}} f[v],$$

where $f[v]$ is homogeneous with weight v.

For a subset H of $K[X]$, $H[v]$ denotes the set of homogeneous elements with weight v. H is *homogeneous*, if every element of it is homogeneous, that is, $H = \cup_{v \in \mathbb{R}} H[v]$. An ideal of $K[X]$ is *homogeneous* if it is generated by homogeneous polynomials. If I is a homogeneous ideal, then any element in I is a sum of homogeneous elements of I. Thus, $I[v]$ is the set of homogeneous elements of I of weight v. A homogeneous ideal I has a homogeneous Gröbner basis. In fact, a reduced Gröbner basis of I is homogeneous.

If ω is positive, then the set $M(X)[v]$ of monomials with a given weight $v \in \mathbb{R}$ is finite. If I is a homogeneous ideal, then for $x \in \mathrm{lm}(I)$, f_x can be chosen from $I[v]$ such that $\mathrm{lm}(f_x) = x$. By this observation together with Lemma 3.1, we have

Lemma 4.1. *Let ω be a positive weight on $M(X)$ and I be a homogeneous ideal of $K[X]$. Then, $I[v]$ is a finite dimensional K-space with base $\{f_x | x \in \mathrm{lm}(I)[v]\}$, and $\dim_K I[v] = |\mathrm{lm}(I)[v]|$. If G is a Gröbner basis of I, then $\dim_K I[v] = |\mathrm{Red}(G)[v]|$*

From here in this section R is a principal ideal domain, K is its quotient field, p is a prime element of R, and ρ_p denotes the canonical surjection from R to $R_p = R/(p)$ as well as the canonical surjection from $R[X]$ to $R_p[X]$. For an ideal I of $K[X]$, I_p denotes the ideal $\rho_p(I \cap R[X])$ of $R_p[X]$. If J is an ideal of $R[X]$, then $J_p = \rho_p(J)$.

Lemma 4.2. *Let ω be a positive weight on $M(X)$ and let I be a homogeneous ideal of $K[X]$. Then, for any $v \in \mathbb{R}$,*

$$\dim_K I[v] \geq \dim_{R_p} I_p[v].$$

Lemma 4.3. *Let ω be a positive weight on $M(X)$, and let I be a homogeneous ideal of $K[X]$. Let G be a (homogeneous) Gröbner basis of a homogeneous ideal L. Let $\overline{G}$ be a (homogeneous) Gröbner basis of a homogeneous ideal $\overline{J}$ of $R_p[X]$. If (i) $I \subset L$, (ii) $\mathrm{lm}(G) = \mathrm{lm}(\overline{G})$, and (iii) $\overline{J} \subset I_p (= \rho_p(I \cap R[X])$, then $I = L$ and G is a Gröbner basis of I.*

Corollary 4.4. *Let ω be a positive weight on $M(X)$, and let H be a homogeneous subset of $R[X]$. Let I (resp. J) be the ideal of $K[X]$ (resp. $R[X]$) generated by H. Let G be a (homogeneous) Gröbner basis of a homogeneous ideal L. Let $\overline{G}$ be a (homogeneous) Gröbner basis of a homogeneous ideal J_p of $R_p[X]$. If (i) $I \subset L$, and (ii) $\mathrm{lm}(G) = \mathrm{lm}(\overline{G})$, then $I = L$ and G is a Gröbner basis of I.*

5 Homogenization and ahomogenization

Let ω be a fixed non-negative integral weight on $M(X)$ with $\omega(X_i) = v_i$ for $i = 1, \ldots, r$. For $f \in K[X]$, let $\mathrm{m}_\omega(f)$ denote the maximum of the weights of the monomials appearing in f.

We introduce a new indeterminate X_0 and the weight ω_0 on $M(X_0, X) = M([X_0, X_1, \ldots, X_r]$ defined by $\omega_0(X_0) = 1$, and $\omega_0(X_i) = v_i$ for $i = 1, \ldots, r$. Let $K[X_0, X] = K[X_0, X_1, \ldots, X_r]$.

For $f \in K[X]$, define ${}^{\mathrm{h}}f \in K[X_0, X]$ by

$${}^{\mathrm{h}}f = X_0^t f(X_1 X_0^{-v_1}, \ldots, X_r X_0^{-v_r}),$$

where $t = \mathrm{m}_\omega(f)$. Then ${}^{\mathrm{h}}f$ is $\geq_0$-homogeneous. On the other hand for $f \in K[X_0, X]$, we define ${}^{\mathrm{a}}f \in K[X]$ by

$${}^{\mathrm{a}}f = f[1, X].$$

For a subset H of $K[X]$ (resp. $K[X_0, X]$), set

$${}^{\mathrm{h}}H = \{{}^{\mathrm{h}}f \mid f \in H\} \quad (\text{resp. } {}^{\mathrm{a}}H = \{{}^{\mathrm{a}}f \mid f \in H\}).$$

For an ideal I of $K[X]$, ${}^{\bar{\mathrm{h}}}I$ denotes the ideal of $K[X_0, X]$ generated by ${}^{\mathrm{h}}I$. Because the mapping sending $f \in K[X_0, X]$ to ${}^{\mathrm{a}}f \in K[X]$ is a homomorphism, ${}^{\mathrm{a}}I$ is an ideal of $K[X]$ for an ideal I of $K[X_0, X]$.

An order $\geq_0$ on $M(X_0, X)$ is defined as follows. For $x, y \in M(X_0, X)$

$$x \geq_0 y \;\Leftrightarrow\; \omega_0(x) > \omega_0(y) \text{ or } (\omega_0(x) = \omega_0(y) \text{ and } {}^{a}x \geq {}^{a}y).$$

If $\geq$ is positive (non-negative, well-founded, compatible) on $M(X)$, so is it on $M(X_0, X)$. If ω is monotone, $\geq_0$ is an extension of $\geq$, that is, $\geq_{0|M(X)} = \geq$.

Lemma 5.1. *(1)* ${}^{h}(f \cdot g) = {}^{h}f \cdot {}^{h}g$ *for* $f, g \in K[X]$.
(2) ${}^{ah}f = f$ *for any* $f \in K[X]$.
(3) ${}^{ah}H = H$ *and* ${}^{a\bar{h}}I = I$ *for a subset* H *of* $K[X]$ *and an ideal* I *of* $K[X]$,
(4) For any homogeneous $f \in K[X_0, X]$, $X_0^t \cdot {}^{ha}f = f$ *for some* $t \in \mathbb{N}$
(5) For any $f \in K[X]$ $\mathrm{lm}({}^{h}f) = X_0^t \cdot \mathrm{lm}(f)$ *for some* $t \in \mathbb{N}$. *If* ω *is monotone,* $\mathrm{lm}({}^{h}f) = \mathrm{lm}(f)$.
(6) For any homogeneous $f \in K[X_0, X]$, $X_0^t \cdot \mathrm{lm}({}^{a}f) = \mathrm{lm}(f)$ *for some* $t \in \mathbb{N}$.

Lemma 5.2. *(1) If* G *is a homogeneous Gröbner basis of a homogeneous ideal* I *of* $K[X_0, X]$, *then* ${}^{a}G$ *is a Gröbner basis of the ideal* ${}^{a}I$ *of* $K[X]$.
(2) Suppose that ω *is monotone. If* G *is a Gröbner basis of an ideal* I *of* $K[X]$, *then* ${}^{h}G$ *is a homogeneous Gröbner basis of* ${}^{\bar{h}}I$.

Hereafter in this section, K is the quotient field of a principal ideal domain R and p is a prime element of R.

Lemma 5.3. *Let* ω *be a compatible positive integral weight on* $M(X)$. *Let* H *be a subset of* $R[X]$, *and let* I *(resp.* J*) be the ideal of* $K[X]$ *(resp.* $R[X]$*) generated by* H. *Let* G *be a Gröbner basis of an ideal* L *of* $K[X]$. *Let* $\overline{G}$ *be a Gröbner basis of a homogeneous ideal* J_p *of* $R_p[X]$. *If (i)* $I \subset L$, *and (ii)* $\mathrm{lm}(G) = \mathrm{lm}(\overline{G})$, *and (iii)* ${}^{h}(f_p) \in ({}^{\bar{h}}I)_p$ *for all* $f \in J$, *then* $I = L$ *and* G *is a Gröbner basis of* I.

If the condition (iii) in the above Lemma is satisfied, p is called *lucky*, but there is no way to find p is lucky effectively. Next we work in the homogenized side.

Proposition 5.4. *Let* H *be a subset of* $K[X]$ *and let* I *be an ideal of* $K[X]$ *generated by* H. *Let* I' *(resp.* J'*) be the ideal of* $K[X_0.X]$ *(resp.* $R[X_0, X]$*) generated by* ${}^{h}H$. *Let* $\overline{G}$ *be a homogeneous Gröbner basis of* J'_p *and let* G *be a homogeneous Gröbner basis of a homogeneous ideal* L' *of* $K[X_0, X]$. *If* $I' \subset L'$, *and* $\mathrm{lm}(G) = \mathrm{lm}(\overline{G})$, *then* ${}^{a}G$ *is a Gröbner basis of* I. *Moreover, if* ω *is monotone,* ${}^{ha}G$ *is a Gröbner basis of* ${}^{\bar{h}}I$

6 Algorithms and examples

Let p be a odd prime and let $>$ be a term order on $M(X)$. For $f = a_n X^n + a_{n-1}X^{n-1} + \cdots a_1 X + a_0 \in \mathbb{Z}[X]$, let $||f||$ be the maximal norm of f, that is,

$$||f|| = \max\{|a_i| \mid i = 0, \ldots, n\}.$$

For $f \in \mathbb{Z}_p[X]$, let $g = \mathrm{re}(f)$ is a polynomial in $\mathbb{Z}[X]$ with minimal $||g||$ satisfying $g_p = c \cdot f$ with $c \in \mathbb{Z}_p$. For a set G of polynomials in $\mathbb{Z}_p[X]$, set $\mathrm{re}(G) = \{\mathrm{re}(f) \mid f \in G\}$. Let H be a finite subset of $\mathbb{Z}[X]$.

(i) Compute the reduced Gröbner basis $\overline{G}$ of ${}^{\mathrm{h}}H_p$ in $\mathbb{Z}_p[X_0, X]$ with respect to $>_0$.
(ii) Compute $G_0 = \mathrm{re}(\overline{G})$.
(iii) Check if every S-polynomial reduced to 0 modulo G_0 in $\mathbb{Z}[X_0, X]$.
(iv) Check if every $h \in {}^{\mathrm{h}}H$ is reduced to 0 modulo G_0 in $\mathbb{Z}[X_0, X]$.
(v) Let $G = {}^{\mathrm{a}}G_0$.

If G_0 obtained in (ii) passes the tests (iii) and (iv), then G is a correct Gröbner basis of H.

Example 6.1. Let
$$H = \{X^2 + 2Y, XY + 1\}.$$
We consider the pure lexicographic order with $X > Y$. We have an S-polynomial $X - 2Y^2$, and reducing the system $H \cup \{X - 2Y^2\}$ we have a Gröbner basis
$$G = \{2Y^3 + 1, X - Y^2\}$$
of $I(H)$. On the other hand, homogenizing H, we have
$${}^{\mathrm{h}}H = \{X^2 + 2YZ, XY + Z^2\}.$$
Let $p = 5$, Completing ${}^{\mathrm{h}}H_p$ in $\mathbb{Z}_p[X, Y, Z]$, we have a Gröbner basis
$$\overline{G} = \{X^2 + 2YZ, XY + Z^2, XZ^2 + 3Y^2Z, 2Y^3Z + Z^4\}$$
of $I({}^{\mathrm{h}}H_p)$. From this we reconstruct a Gröbner basis
$$G' = \{X^2 + 2YZ, XY + Z^2, XZ^2 - 2Y^2Z, 2Y^3Z + Z^4\}$$
of $I({}^{\mathrm{h}}H)$ on $\mathbb{Z}[X, Y, Z]$. Then, ahomogenizing it we have a Gröbner basis
$${}^{\mathrm{a}}G' = \{X^2 + 2Y, XY + 1, X - 2Y^2, 2Y^3 + 1\}.$$
of $I(H)$. Then, reducing it we have $\{2Y^3 + 1, X - Y^2\} = G$.

As seen in the above example ${}^{\mathrm{a}}G'$ may not be reduced, though G' is reduced. Sometimes, G' can be very big compared with G. In these cases, our methods are not practical.

Example 6.2. Let
$$H = \{3X^2+5X^3-3Y^2, -4-4X^2+3XY+Y^3, 3+XY+5X^2Y+4Y^2-3XY^2\}.$$
The reduced Gröbner basis of H is $\{1\}$. However, the reduced Gröbner basis of ${}^{\mathrm{h}}H$ is very big with a polynomial which involves an integer with 1120 digits in decimal expression in its coefficients.

References

[1] E.A. Arnold, Modular algorithms for computing Gröbner bases, J. Symbolic Comp. **35** (2003), 403–419.

[2] T. Becker, V. Weispfenning, *Gröbner bases*, Springer, 1993.

[3] B. Buchberger, Gröbner-bases: an algorithmic method in polynomial ideal theory, In: Multidimensional Systems Theory (1985), 184–232.

[4] G.L. Elbert, Some comments on the modular approach to Gröbner-bases. ACM SIGSAM Bulletin **17**, (1983), 28–32.

[5] F. Winkler, A p-adic approach to the computation of Gröbner bases, J. Symbolic Comp. **6** (1987), 287- 304.