A Simple Algorithm to Compute Comprehensive Gröbner Bases Using Gröbner Bases

Akira Suzuki
Kobe University
Rokkodaicho 1-1, Nada
Kobe, Japan
sakira@kobe-u.ac.jp

Yosuke Sato
Tokyo University of Science
Kagurazaka 1-3, Shinjuku
Tokyo, Japan
ysato@rs.kagu.tus.ac.jp

ABSTRACT

We introduce a simple algorithm to compute comprehensive Gröbner bases. It requires only computations of reduced Gröbner bases in polynomial rings over ground fields. It is so simple that we can easily implement it on any computer algebra system that has a routine to compute reduced Gröbner bases. Our implementations on several computer algebra systems show that it is also sufficiently fast comparing with other existing algorithms.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms

General Terms

Algorithms

Keywords

Gröbner basis, Gröbner system, comprehensive Gröbner basis

1. INTRODUCTION

In 1992, the concepts of comprehensive Gröbner bases and comprehensive Gröbner systems together with their algorithms are introduced by Weispfenning [10].
In recent years, several improvements have been done by Weispfenning (CCGB [11]), Montes (DISPGB [5, 6]) and Suzuki-Sato (ACGB [8, 9]). All the algorithms introduced by them, however, essentially require S-polynomial computations and monomial reductions with polynomials in a polynomial ring over a coefficient field $K(\bar{A})$ of rational functions together with complicated conditions of parameters so called case distinctions, where K is a ground field and $\bar{A}$ are parameters. This fact makes it hard to implement their algorithms on computer algebra systems even if they have a routine to compute Gröbner bases in a polynomial ring over $K(\bar{A})$.

ISSAC'06, July 9–12, 2006, Genova, Italy.

In this paper, we introduce simple algorithms to compute comprehensive Gröbner systems and comprehensive Gröbner bases. One of the most important properties of our algorithms which does not hold in others is that we do not require case distinctions to be pairwise disjoint, i.e. parameter spaces of two branches may not be disjoint. Though this fact looks a serious disadvantage, abandonment of pairwise disjointness enables us to avoid taking care of disequations of case distinctions. It also enables us to merge equations of case distinctions into the computation of Gröbner bases in polynomial rings of over the ground field K. Our algorithms require only computations of Gröbner bases in polynomial rings over a ground field. They are so simple that we can easily implement them on any computer algebra system that can compute Gröbner bases in polynomial rings over K. Actually, we implemented them on several computer algebra systems such as Risa/Asir, Singular and Maple. Through our computation experiment, we checked our program is sufficiently fast comparing with other existing implementations such as CGB of [10, 3] and DISPGB of [6], when we do not have so many parameters. One of the main reasons is that Gröbner bases computations in polynomial rings over a ground field K are generally much faster than their computations in polynomial rings over a rational function field $K(\bar{A})$.

Our plan is as follows. In Section 2, we describe our algorithm to compute comprehensive Gröbner systems. In Section 3, we describe our device to compute faithful comprehensive Gröbner systems which leads us to an algorithm to compute comprehensive Gröbner bases. In Section 4, we give some benchmark data in comparison with other existing implementations.

2. COMPREHENSIVE GRÖBNER SYSTEMS

Let us begin with giving several notations and definitions we use throughout the rest of the paper.

K and L denote fields such that L is an algebraic closure of K. $\bar{X}$ and $\bar{A}$ denote finite sets of variables such that $\bar{X} \cap \bar{A} = \emptyset$ and m denotes the cardinality of $\bar{A}$. $T(\bar{X})$, $T(\bar{A})$ and $T(\bar{X}, \bar{A})$ denote the sets of terms of $\bar{X}$, $\bar{A}$ and $\bar{X} \cup \bar{A}$ respectively. $<_{\bar{X},\bar{A}}$ denotes a term order on $T(\bar{X}, \bar{A})$ such that $\bar{X} \gg \bar{A}$, i.e. any term in $T(\bar{X})$ is greater than any term in $T(\bar{A})$, $<_{\bar{X}}$ denotes its restriction on $T(\bar{X})$.

For a polynomial $f \in K[\bar{X}, \bar{A}]$, regarding $K[\bar{X}, \bar{A}]$ as a polynomial ring $(K[\bar{A}])[\bar{X}]$ over the coefficient ring $K[\bar{A}]$, a *head coefficient of f under $\bar{A}$* (denoted by $hc_{\bar{A}}(f)$), a *head*

term of f under $\bar{A}$ (denoted by $ht_{\bar{A}}(f)$) and a *head monomial of f under $\bar{A}$* (denoted by $hm_{\bar{A}}(f)$) are the head coefficient, the head term and the head monomial of f with respect to $<_{\bar{X}}$ respectively. Notice that we have $hm_{\bar{A}}(f) = hc_{\bar{A}}(f) \cdot ht_{\bar{A}}(f)$ for each $f \in K[\bar{X}, \bar{A}]$.

For arbitrary $\bar{a} \in L^m$, we can define the canonical specialization homomorphism $\sigma_{\bar{a}} \colon K[\bar{A}] \to L$ induced by $\bar{a}$, and we can naturally extend it to $\sigma_{\bar{a}} \colon (K[\bar{A}])[\bar{X}] \to L[\bar{X}]$. For $f_1, \ldots, f_k \in K[\bar{A}]$, $V(f_1, \ldots, f_k) \subseteq L^m$ denotes the affine variety of $f_1, \ldots, f_k$, i.e.

$$V(f_1, \ldots, f_k) = \{\bar{a} \in L^m \ : \ f_1(\bar{a}) = \cdots = f_k(\bar{a}) = 0\}.$$

In a similar fashion, for $F \subseteq K[\bar{A}]$, we let $V(F) = \{\bar{a} \in L^m : f(\bar{a}) = 0 \quad (\forall f \in F)\}$.

Definition 1. Let F be a subset of $K[\bar{X}, \bar{A}]$, $\mathcal{A}_1, \ldots, \mathcal{A}_l$ be algebraically constructible subsets of L^m and $G_1, \ldots, G_l$ be subsets of $K[\bar{X}, \bar{A}]$. Let $\mathcal{S}$ be a subset of L^m such that $\mathcal{S} \subseteq \mathcal{A}_1 \cup \cdots \cup \mathcal{A}_l$. A finite set $\mathcal{G} = \{(\mathcal{A}_1, G_1), \ldots, (\mathcal{A}_l, G_l)\}$ of pairs is called a *comprehensive Gröbner system on $\mathcal{S}$ for F* if $\sigma_{\bar{a}}[G_i]$ is a Gröbner basis of the ideal $\langle \sigma_{\bar{a}}[F] \rangle$ in $L[\bar{X}]$ for each $i = 1, \ldots, l$ and $\bar{a} \in \mathcal{A}_i$. Each $(\mathcal{A}_i, G_i)$ is called a *segment* of $\mathcal{G}$. We simply say $\mathcal{G}$ is a *comprehensive Gröbner system for F* if $\mathcal{S} = L^m$.

In this paper, we use only an algebraically constructible set that has a form $V(f_1, \ldots, f_k) \setminus V(g_1, \ldots, g_l) \subseteq L^m$.

Definition 2. Let $S_1, \ldots, S_l$ and $T_1, \ldots, T_l$ be finite subsets of $K[\bar{A}]$. A finite set $\mathcal{G} = \{(S_1, T_1, G_1), \ldots, (S_l, T_l, G_l)\}$ of triples is also called a *comprehensive Gröbner system* on S for F, if $\{(V(S_1) \setminus V(T_1), G_1), \ldots, (V(S_l) \setminus V(T_l), G_l)\}$ is a comprehensive Gröbner system on S for F. Each (S_i, T_i, G_i) is also called a *segment* of $\mathcal{G}$.

The following lemma which is an easy consequence of [4, Theorem 3.1] plays an important role for our algorithms.

LEMMA 2.1. *Let $G = \{g_1, \ldots, g_l\}$ be a Gröbner basis of an ideal $\langle F \rangle$ in $K[\bar{X}, \bar{A}]$ with respect to $<_{\bar{X},\bar{A}}$. For any $\bar{a} \in L^m$, let $\{g_{n_1}, \ldots, g_{n_k}\}$ be the set of all polynomials g of G such that $\sigma_{\bar{a}}(hc_{\bar{A}}(g)) \neq 0$. Then, $\{\sigma_{\bar{a}}(g_{n_1}), \ldots, \sigma_{\bar{a}}(g_{n_k})\}$ is a Gröbner basis of the ideal $\langle \sigma_{\bar{a}}[F] \rangle$ in $L[\bar{X}]$ with respect to $<_{\bar{X}}$ if and only if $\sigma_{\bar{a}}(g)$ is reducible to 0 modulo $\{\sigma_{\bar{a}}(g_{n_1}), \ldots, \sigma_{\bar{a}}(g_{n_k})\}$ for every g in G.*

The next lemma is the direct consequence.

LEMMA 2.2. *Let G be a Gröbner basis of an ideal $\langle F \rangle$ in $K[\bar{X}, \bar{A}]$ with respect to $<_{\bar{X},\bar{A}}$. If $\sigma_{\bar{a}}(hc_{\bar{A}}(g)) \neq 0$ for each $g \in G \setminus G \cap K[\bar{A}]$, then $\sigma_{\bar{a}}[G]$ is a Gröbner basis of $\langle \sigma_{\bar{a}}[F] \rangle$ in $L[\bar{X}]$ with respect to $<_{\bar{X}}$ for any $\bar{a} \in V(G \cap K[\bar{A}])$*

Let F be a subset of polynomials in $K[\bar{X}, \bar{A}]$. Let G be the reduced Gröbner basis of $\langle F \rangle$ in $K[\bar{X}, \bar{A}]$ and $\{h_1, \ldots, h_l\} = \{hc_{\bar{A}}(g) : g \in G \setminus K[\bar{A}]\} \subseteq K[\bar{A}]$, then the pair $(L^m \setminus (V(h_1) \cup \cdots \cup V(h_l)), G)$ forms a segment of comprehensive Gröbner system for F, i.e. $\sigma_{\bar{a}}[G]$ is a Gröbner basis of $\langle \sigma_{\bar{a}}[F] \rangle$ in $L[\bar{X}]$ for each $\bar{a} \in L^m \setminus (V(h_1) \cup \cdots \cup V(h_l))$. Thus, in order to get a comprehensive Gröbner system for F, we need to get Gröbner bases for each specialization on $V(h_1) \cup \cdots \cup V(h_l) = V(\mathrm{lcm}\{h_1, \ldots, h_l\})$.

In order to handle specializations on each $V(h_i)$, we can use Lemma 2.2 for $F \cup \{h_i\}$ again. Notice that $h_i \notin \langle F \rangle$ since $h_i = hc_{\bar{A}}(g)$ for some $g \in G \setminus K[\bar{A}]$ and G is reduced. Indeed, if we compute the reduced Gröbner basis G_1 of $\langle F \cup \{h_i\} \rangle$ and $\{h'_1, \ldots, h'_{l'}\} = \{hc_{\bar{A}}(g) : g \in G_1 \setminus K[\bar{A}]\}$, then $\sigma_{\bar{a}}[G_1]$ is a Gröbner basis of $\langle \sigma_{\bar{a}}[F \cup \{h_i\}] \rangle = \langle \sigma_{\bar{a}}[F] \rangle$ in $L[\bar{X}]$ for any $\bar{a} \in V(h_i) \setminus (V(h'_1) \cup \cdots \cup V(h'_{l'}))$. So, if we can continue this process, we will finally get a comprehensive Gröbner system for F.

The above idea leads us to the following algorithms. We assume the algorithm `ReducedGröbnerBasis` $(F, <)$ outputs the reduced Gröbner basis of $\langle F \rangle$ with respect to the term order $<$.

Algorithm `CGSMain`

Input: F: a finite subset of $K[\bar{X}, \bar{A}]$
Output: $\mathcal{H}$: a finite set of pairs (h, G) of a polynomial and a Gröbner basis in $K[\bar{X}, \bar{A}]$.

```
begin
G := ReducedGröbnerBasis(F, <_{X̄,Ā});
if 1 ∈ G then
  H := {(1, F)};
else
  {h_1, ..., h_l} := {hc_Ā(g) : g ∈ G \ K[Ā]};
  h := lcm{h_1, ..., h_l};      (where lcm∅ = 1)
  H := {(h, G)} ∪
       CGSMain(G ∪ {h_1}) ∪ ··· ∪ CGSMain(G ∪ {h_l});
end if
return H;
end.
```

THEOREM 2.3. *The algorithm `CGSMain` terminates for any input F of a finite subset of $K[\bar{X}, \bar{A}]$. If $\mathcal{H}$ is the output of `CGSMain`(F), then $\{(G \cap K[\bar{A}], \{h\}, G \setminus K[\bar{A}]) : (h, G) \in \mathcal{H}\}$ forms a comprehensive Gröbner system on $V(\langle F \rangle \cap K[\bar{A}])$ for F.*

PROOF. First we show the termination. We suppose that `CGSMain`(F) does not terminate, then there exists an infinite sequence $F_0, F_1, F_2, \ldots$ such that $F_0 = F$ and `CGSMain`(F_{n+1}) is called in `CGSMain` (F_n) for each $n = 0, 1, 2, \ldots$ by König's Lemma. Notice that $F_{n+1} = F_n \cup \{h_n\}$ for some $h_n \in K[\bar{A}]$ such that $h_n \notin \langle F_n \rangle$ as we explained above. Hence, we have $\langle F_n \rangle \subsetneq \langle F_{n+1} \rangle$ for each n, which contradicts to the fact $K[\bar{X}, \bar{A}]$ is a noetherian ring.

We next show that, if $(h, G) \in \mathcal{G}$, then the triple $(G \cap K[\bar{A}], h, G \setminus K[\bar{A}])$ forms a segment of a comprehensive Gröbner system for F, i.e. $\sigma_{\bar{a}}[G \setminus K[\bar{A}]]$ is a Gröbner basis of $\langle \sigma_{\bar{a}}[F] \rangle$ for each $\bar{a} \in V(G \cap K[\bar{A}]) \setminus V(h)$. Let $\bar{a}$ be an arbitrary element of $V(G \cap K[\bar{A}]) \setminus V(h)$. By the algorithm, G is the reduced Gröbner basis of the ideal $\langle F \cup S \rangle$ with respect to $<_{\bar{X},\bar{A}}$ for some finite set $S \subseteq K[\bar{A}]$. Since $<_{\bar{X},\bar{A}}$ satisfies $\bar{A} \ll \bar{X}$, we have $\langle G \cap K[\bar{A}] \rangle = \langle F \cup S \rangle \cap K[\bar{A}]$ in $K[\bar{A}]$, so we may assume $S = G \cap K[\bar{A}]$. Then, $\sigma_{\bar{a}}[G]$ is a Gröbner basis of $\langle \sigma_{\bar{a}}[F \cup S] \rangle$ by Lemma 2.2 since the assumption $h(\bar{a}) \neq 0$ implies $h_i(\bar{a}) \neq 0$ for each $i = 1, \ldots, l$. The fact $\bar{a} \in V(G \cap K[\bar{A}])$ implies $\sigma_{\bar{a}}[G] \setminus \{0\} = \sigma_{\bar{a}}[G \setminus K[\bar{A}]] \setminus \{0\}$ and $\sigma_{\bar{a}}[F \cup S] \setminus \{0\} = \sigma_{\bar{a}}[F] \setminus \{0\}$, from which it follows that $\sigma_{\bar{a}}[G \setminus K[\bar{A}]]$ is a Gröbner basis of $\langle \sigma_{\bar{a}}[F] \rangle$.

To conclude the proof, we need show that the conditions in $\mathcal{H}$ covers the entire $V(\langle F \rangle \cap K[\bar{A}])$, i.e.

$$V(\langle F \rangle \cap K[\bar{A}]) \subseteq \bigcup_{(h,G) \in \mathcal{H}} V(G \cap K[\bar{A}]) \setminus V(h).$$

We actually show the equation:

$$V(\langle F \rangle \cap K[\bar{A}]) = \bigcup_{(h,G) \in \mathcal{H}} V(G \cap K[\bar{A}]) \setminus V(h).$$

Notice that the following equation always holds.

$$V(\langle G\rangle \cap K[\bar{A}]) =$$
$$(V(\langle G\rangle \cap K[\bar{A}]) \setminus V(h)) \cup \bigcup_{i=1,\ldots,l} V(\langle G \cup \{h_i\}\rangle \cap K[\bar{A}]),$$

from which, the above equation follows by the induction on the well-founded tree of the algorithm. □

Algorithm CGS

Input: F : a finite subset of $K[\bar{X}, \bar{A}]$
Output: $\mathcal{G}$: a finite set of triples which forms a comprehensive Gröbner system for F.

```
begin
H := CGSMain(F);
G_0 := ReducedGröbnerBasis(F, <_{X̄,Ā});
if G_0 ∩ K[Ā] = ∅ then
  G := ∅;
else
  G := {(∅, G_0 ∩ K[Ā], {1})};
end if;
for each (h, G) ∈ H do
  G := G ∪ {(G ∩ K[Ā], {h}, G \ K[Ā])};
end for;
return G;
end.
```

THEOREM 2.4. *Let F be a finite subset of $K[\bar{X}, \bar{A}]$. Then the output of* CGS(F) *forms a comprehensive Gröbner system for F.*

PROOF. In Theorem 2.3, we have already shown that $\{(G\cap K[\bar{A}], \{h\}, G\setminus K[\bar{A}]) : (h, G) \in \mathcal{G}\}\setminus\{(\emptyset, G_0\cap K[\bar{A}], \{1\})\}$ forms a comprehensive Gröbner system on $V(\langle F\rangle \cap K[\bar{A}])$ for F. Notice that $V(\langle F\rangle \cap K[\bar{A}]) = V(G_0 \cap K[\bar{A}])$. So, if $G_0 \cap K[\bar{A}] = \emptyset$, then $V(\langle F\rangle \cap K[\bar{A}]) = L^m$ and we are done. If $G_0 \cap K[\bar{A}] \neq \emptyset$, then $1 \in \langle \sigma_{\bar{a}}[F]\rangle$ for each $\bar{a} \in L^m \setminus V(\langle F\rangle \cap K[\bar{A}])$. So, $\{(\emptyset, G_0 \cap K[\bar{A}], \{1\})\}$ forms a comprehensive Gröbner system on $L^m \setminus V(\langle F\rangle \cap K[\bar{A}])$ for F. □

Notice that parameter spaces of segments of a Gröbner system produced by the algorithm CGSMain may not be disjoint, i.e. $(V(G \cap K[\bar{A}]) \setminus V(h)) \cap (V(G' \cap K[\bar{A}]) \setminus V(h'))$ could be non-empty for distinct elements (G, h) and (G', h') of $\mathcal{H}$. Though this fact seems to be a serious disadvantage of our algorithm, it enables us to avoid producing unnecessary disequations. In CGSMain, as soon as we get a disequation, namely h, a segment (h, G) is determined, and we do not use the disequation $h \neq 0$ in the following computation. So, in our algorithm, we do not have to take care of disequations, which makes our algorithm extremely simple. In CGSMain, we do not even check if $V(\langle G\rangle \cap K[\bar{A}]) \setminus V(h) = \emptyset$. Of course, we can check it after the algorithm terminates and omit it from the segments in case it is empty. We can also make the constructible sets of segments pairwise disjoint. We can apply a standard technique of Gröbner bases, where we only need computations of Gröbner bases in polynomial rings over K. We can also make a Gröbner system reduced, i.e., a specialized Gröbner basis with any element of the constructible set of the segment is a reduced Gröbner basis. After the termination of CGSMain, what we have to do is only monomial reductions in a polynomial ring $K(\bar{A})[\bar{X}]$. Since a head coefficient of each polynomial does not vanish by a specialization with any element of the constructible set of the segment, we can apply monomial reductions of $K(\bar{A})[\bar{X}]$.

There are several ways to optimize the algorithm. The easiest one is using $\{h'_1, \ldots, h'_k\}$ instead of $\{h_1, \ldots, h_l\}$ where $\{h'_1, \ldots, h'_k\}$ is a set of factors of the square free part of $h_1 \cdots h_l$. We can also detect a redundant recursive call, i.e. we can check if $V(h_i)$ is included in the union of all constructible sets that are computed so far. Another interesting optimization is using known results of stabilities of Gröbner bases under specializations. For example, if $G \cap K[\bar{A}]$ is a zero-dimensional radical ideal, then we do not need continue the computation anymore since $(V(G \cap K[\bar{A}]), G)$ is a segment of a Gröbner system for F. (See [4, Theorem 3.2] or [1, Theorem 2].) We can also use primary ideal decomposition of the ideal $\langle G \cap K[\bar{A}]\rangle$ in order to make parameter spaces more fine. All the above optimization methods are included in our implementation on Risa/Asir.

3. COMPREHENSIVE GRÖBNER BASES

A comprehensive Gröbner system $\{(s_1, t_1, G_1), \ldots, (s_l, t_l, G_l)\}$ for F is called *faithful* if $G_i \subseteq \langle F\rangle$ for each $i = 1, \ldots, l$. We can modify the algorithm CGSMain to compute a faithful comprehensive Gröbner system. The key idea is introducing a new auxiliary variable U besides $\bar{X}$ and $\bar{A}$. Let $<_{U,\bar{X},\bar{A}}$ be a term order of $T(U, \bar{X}, \bar{A})$ extending $<_{\bar{X},\bar{A}}$ such that $U \gg \bar{X} \gg \bar{A}$, and let $<_{U,\bar{X}}$ be its restriction on $T(U, \bar{X})$. As in the previous section, for each $f \in K[U, \bar{X}, \bar{A}]$, $hc_{\bar{A}}(f)$, $ht_{\bar{A}}(f)$ and $hm_{\bar{A}}(f)$ denote the head coefficient, the head term and the head monomial of f with respect to $<_{U,\bar{X}}$ as a polynomial of $(K[\bar{A}])[U, \bar{X}]$. We also use $hc(f)$, $ht(f)$ and $hm(f)$ to denote the head coefficient, the head term and the head monomial of f with respect to $<_{U,\bar{X},\bar{A}}$ as a polynomial of $K[\bar{A}, U, \bar{X}]$. We define homomorphisms σ^0 and σ^1 from $K[U, \bar{X}, \bar{A}]$ to $K[\bar{X}, \bar{A}]$ as a specialization of U with 0 and 1 respectively, i.e. $\sigma^0(f(U, \bar{X}, \bar{A})) = f(0, \bar{X}, \bar{A})$ and $\sigma^1(f(U, \bar{X}, \bar{A})) = f(1, \bar{X}, \bar{A})$. For a polynomial $f \in K[U, \bar{X}, \bar{A}]$ and a set $S \subseteq K[U, \bar{X}, \bar{A}]$, $f \cdot S$ denotes the set $\{f \cdot s : s \in S\} \subseteq K[U, \bar{X}, \bar{A}]$. With these notations, we have the following lemmas.

LEMMA 3.1. *Let F and S be subsets of $K[\bar{X}, \bar{A}]$. For any $g \in \langle (U \cdot F) \cup ((U-1) \cdot S)\rangle_{K[U,\bar{X},\bar{A}]}$, $\sigma^0(g) \in \langle S\rangle_{K[\bar{X},\bar{A}]}$ and $\sigma^1(g) \in \langle F\rangle_{K[\bar{X},\bar{A}]}$.*

PROOF. Since $g \in \langle (U \cdot F) \cup ((U-1) \cdot S)\rangle_{K[U,\bar{X},\bar{A}]}$, there exists $f_1, \ldots, f_i \in F$, $s_1, \ldots, s_j \in S$ and $h_1, \ldots, h_{i+j} \in K[U, \bar{X}, \bar{A}]$ such that
$g = Uf_1h_1 + \cdots + Uf_ih_i + (U-1)s_1h_{i+1} + \cdots + (U-1)s_jh_{i+j}$.
By specializing U with 0 and 1,
$\sigma^0(g) = -(s_1\sigma^0(h_{i+1}) + \cdots + s_j\sigma^0(h_{i+j}))$ and
$\sigma^1(g) = f_1\sigma^1(h_1) + \cdots + f_i\sigma^1(h_i)$.
Since $\sigma^0(h_{i+1}), \ldots, \sigma^0(h_{i+j}), \sigma^1(h_1), \ldots, \sigma^1(h_i) \in K[\bar{X}, \bar{A}]$, $\sigma^0(g) \in \langle S\rangle_{K[\bar{X},\bar{A}]}$ and $\sigma^1(g) \in \langle F\rangle_{K[\bar{X},\bar{A}]}$. □

LEMMA 3.2. *Let F be a finite subset of $K[\bar{X}, \bar{A}]$. Let S be a finite subset of $K[\bar{A}]$ such that $V(S) \subseteq V(\langle F\rangle \cap K[\bar{A}])$. Let G be the reduced Gröbner basis of the ideal $\langle (U \cdot F) \cup ((U-1) \cdot S)\rangle$ in $K[U, \bar{X}, \bar{A}]$ with respect to $<_{U,\bar{X},\bar{A}}$. Let $\{h_1, \ldots, h_l\} = \{hc_{\bar{A}}(g) : g \in G'\} \subseteq K[\bar{A}]$, where $G' = \{g \in G : ht(g) \notin T(\bar{X}, \bar{A}), hc_{\bar{X},\bar{A}}(g) \notin K[\bar{A}]\}$. Then $\sigma_{\bar{a}}[\sigma^1[G]]$ is a Gröbner basis of $\langle \sigma_{\bar{a}}[F]\rangle$ in $L[\bar{X}]$ for each $\bar{a} \in V(S)$ such that $h_1(\bar{a}) \neq 0, \ldots, h_l(\bar{a}) \neq 0$.*

PROOF. Before going into the proof, first notice that $ht(g) \notin T(\bar{X}, \bar{A})$ is equivalent to that $ht(g)$ includes the variable U and $hc_{\bar{X},\bar{A}}(g) \notin K[\bar{A}]$ is equivalent to that $hc_{\bar{X},\bar{A}}(g)$ includes at least one variable of $\bar{X}$.

Notice that *any* polynomial of G has a linear form of U, i.e. the degree of U is at most 1, because of the definition of our term order. Let g be denoted as $g = U \cdot g^U + g_U$ for $g^U, g_U \in K[\bar{X}, \bar{A}]$, where $g^U = \sigma^1(g) - \sigma^0(g)$ and $g_U = \sigma^0(g)$. We have the following.

CLAIM 1. *For each $g \in G$, $g_U \in \langle S \rangle_{K[\bar{X},\bar{A}]}$ and $\sigma_{\bar{a}}(g_U) = 0$. Furthermore if $g \notin G'$, then $\sigma_{\bar{a}}(g) = 0$.*

PROOF OF CLAIM. By Lemma 3.1, $g_U = \sigma^0(g) \in \langle S \rangle_{K[\bar{X},\bar{A}]}$. By our assumption $\bar{a} \in V(S)$, $\sigma_{\bar{a}}(g_U) = 0$ follows. Let $g \in G \setminus G'$. Then $ht(g) \in T(\bar{X}, \bar{A})$ or $hc_{\bar{X},\bar{A}}(g) \in K[\bar{A}]$. For the first case, $g = g_U \in \langle S \rangle_{K[\bar{X},\bar{A}]}$, it follows that $\sigma_{\bar{a}}(g) = \sigma_{\bar{a}}(g_U) = 0$. If $ht(g) \notin T(\bar{X}, \bar{A})$ and $hc_{\bar{X},\bar{A}}(g) \in K[\bar{A}]$, then $g^U = hc_{\bar{X},\bar{A}}(g) \in K[\bar{A}]$. By Lemma 3.1, $g^U = \sigma^1(g) - \sigma^0(g) \in \langle F \cup S \rangle_{K[\bar{X},\bar{A}]}$. Hence, $g^U \in \langle F \cup S \rangle \cap K[\bar{A}]$. By our assumption that $V(S) \subseteq V(\langle F \rangle \cap K[\bar{A}])$, $\bar{a} \in V(\langle F \rangle \cap K[\bar{A}])$. It follows that $\sigma_{\bar{a}}(g^U) = 0$. Together with the fact $\sigma_{\bar{a}}(g_U) = 0$ shown in the above, we have $\sigma_{\bar{a}}(g) = 0$. □

Since $\sigma^1[G]$ is clearly a basis of the ideal $\langle F \rangle$ in $K[\bar{X}, \bar{A}]$, $\sigma_{\bar{a}}[\sigma^1[G]]$ is a basis of the ideal $\langle \sigma_{\bar{a}}[F] \rangle$ in $L[\bar{X}]$. It suffices to show that $\sigma_{\bar{a}}[\sigma^1[G]]$ is a Gröbner basis. Let $h = \mathrm{lcm}\{h_1, \ldots, h_l\}$ and $\bar{a}$ be an arbitrary element of $V(S) \setminus V(h)$. By the definition of h, $h_i(\bar{a}) \neq 0$ for each $i = 1, \ldots, l$ that is $hc_{\bar{A}}(g)(\bar{a}) \neq 0$ for each $g \in G'$.

On the other hand, for each $g \in G \setminus G'$, we have $\sigma_{\bar{a}}(g) = 0$ by the claim. Thus $\sigma_{\bar{a}}[G] \setminus \{0\} = \sigma_{\bar{a}}[G']$ is a Gröbner basis in $L[U, \bar{X}]$ by Lemma 2.1.

Notice also that $\sigma_{\bar{a}}(U \cdot g^U + g_U) = \sigma_{\bar{a}}(U \cdot g^U)$ for each $g \in G'$. So, $H = \{\sigma_{\bar{a}}(U \cdot g^U) : g \in G'\}$ is a Gröbner basis in $L[U, \bar{X}]$. Since any monomial reduction by H and any computation of S-polynomials by each pair among H is conservative under the homomorphism σ^1, $\{\sigma_{\bar{a}}(g^U) : g \in G'\} = \sigma^1[\sigma_{\bar{a}}[G']]$ is a Gröbner basis. It follows that $\sigma_{\bar{a}}[\sigma^1[G]]$ is a Gröbner basis in $L[\bar{X}]$. □

The above lemma leads us to have the following algorithm which outputs a faithful comprehensive Gröbner system on $V(S)$ for F.

Algorithm `CGBMain`

Input: F : a finite subset of $K[\bar{X}, \bar{A}]$
S : a finite subset of $K[\bar{A}]$
such that $V(S) \subseteq V(\langle F \rangle \cap K[\bar{A}])$.
Output: $\mathcal{G}$: a finite set of triples of polynomials which forms a faithful comprehensive Gröbner system on $V(S)$ for F.

```
begin
if 1 ∈ ⟨S⟩ then
  G := ∅;
else
  G := ReducedGröbnerBasis(
         (U · F) ∪ ((U − 1) · S), <_{U,X̄,Ā});
  {h_1, ..., h_l} := {hc_Ā(g) : g ∈ G,
         ht(g) ∉ T(X̄, Ā), hc_{X̄,Ā}(g) ∉ K[Ā]};
  h := lcm{h_1, ..., h_l};
  G := {(S, {h}, σ^1[G])} ∪
         CGBMain(F, S ∪ {h_1}) ∪ ··· ∪ CGBMain(F, S ∪ {h_l});
end if
return G;
end.
```

THEOREM 3.3. *Let $F \subseteq K[\bar{X}, \bar{A}]$ and $S \subseteq K[\bar{A}]$ be finite sets such that $V(S) \subseteq V(\langle F \rangle \cap K[\bar{A}])$. Then the algorithm* `CGBMain`(F, S) *terminates. The output of* `CGBMain`(F, S) *forms a faithful comprehensive Gröbner system on $V(S)$ for F.*

PROOF. In order to show the termination of the algorithm, it suffices to show that each h_i is not in the ideal $\langle S \rangle$ for each $i = 1, \ldots, l$ as in the proof of Theorem 2.3. By the construction of h_i, there exists $g \in G$ such that $h_i = hc_{\bar{A}}(g)$, $ht(g) \notin T(\bar{X}, \bar{A})$ and $hc_{\bar{X},\bar{A}}(g) \notin K[\bar{A}]$. Therefore g has the following form.

$$g = h_i U T + g',$$

where T is a term of $T(\bar{X})$ and $ht_{\bar{A}}(g) = UT$.
If $h_i \in \langle S \rangle$, then $h_i \cdot (U - 1) \in \langle G \rangle$. So, $ht(h_i \cdot (U - 1)) = ht(h_i U)$ must be reducible by G, which implies that g is reducible by G contradicting to the fact that G is a reduced Gröbner basis.

Let $\mathcal{G}$ be the output of `CGBMain`. Let $(S, \{h\}, \sigma^1[G]) \in \mathcal{G}$ be a triple produced before the recursive call of `CGBMain`. Note first that the condition $V(S) \subseteq V(\langle F \rangle \cap K[\bar{A}])$ always hold since S is always increasing. Let $\bar{a}$ be an arbitrary element of $V(S) \setminus V(h)$. By Lemma 3.2, $\sigma_{\bar{a}}[\sigma^1[G]]$ is a Gröbner basis of $\langle \sigma_{\bar{a}}[F] \rangle$ in $L[\bar{X}]$.

We can show $V(S) = \bigcup_{(S', \{h'\}, G') \in \mathcal{G}} V(S') \setminus V(h')$ by the exactly same proof as Theorem 2.3.

Faithfulness is an easy consequence of Lemma 3.1. □

In order to construct a faithful comprehensive Gröbner system for F, first compute a basis S of the elimination ideal $\langle F \rangle \cap K[\bar{A}]$, then apply `CGBMain`$(F, S)$ to get a faithful comprehensive Gröbner system $\mathcal{G}$ on $V(S)$ for F. What we have to do now is to take care of $L^m \setminus V(S)$. Notice that $\sigma_{\bar{a}}[S]$ includes a non-zero element of L for any $\bar{a} \in L^m \setminus V(S)$. So, $\langle \sigma_{\bar{a}}[F] \rangle = \langle 1 \rangle$. Therefore $\mathcal{G} \cup \{(\emptyset, S, S)\}$ forms a faithful comprehensive Gröbner system for F.

Now, it is clear that the following algorithm computes a comprehensive Gröbner basis for F. We assume the algorithm `Elim`(F) computes a basis of the elimination ideal $\langle F \rangle \cap K[\bar{A}]$.

Algorithm `CGB`

Input: F : a finite subset of $K[\bar{X}, \bar{A}]$.
Output: G : a comprehensive Gröbner basis for F.

```
begin
S := Elim(F)
G := CGBMain(F, S);
G := S;
for each (S', T', G') ∈ G do
  G := G ∪ G';
end for;
return G;
end.
```

4. COMPUTATION EXAMPLES

We implemented our algorithms to compute comprehensive Gröbner systems for the case $K = \mathbb{Q}$ on Risa/Asir[1] [7], Singular[2] and Maple[3]. The implementation on Risa/Asir also contains reduced comprehensive Gröbner systems, comprehensive Gröbner bases and several optimizations which we described at the end of section 2. It can be obtained from the following web page[4]. In our computation experiments, in most cases, our implementations are faster than other existing implementations CGB and DISPGB. In this section, we give some of our computation examples together with data of computations with CGB and DISPGB.

EXAMPLE 1. *Under the lexicographic order such that $X > Y > Z$, compute a comprehensive Gröbner system (or a comprehensive Gröbner basis) for $F = \{X^3 - A, Y^4 - B, X + Y - Z\}$ where A and B are parameters. From this, we get the minimal polynomial of Z.*

From an input `acgs.rcgs([x^3-a,y^4-b,x+y-z],[x,y,z], 2);`, our program of Risa/Asir produces a comprehensive Gröbner system containing 7 segments. We show the corresponding case distinction and the minimal polynomial of Z for each segment.

```
  ((b)(a)(729*a^4-4096*b^3)(729*a^4+64*b^3)(16767
  *a^4+5632*b^3)!=0)
-z^12+4*a*z^9+3*b*z^8-6*a^2*z^6+48*b*a*z^5-3*b^2
*z^4+4*a^3*z^3+30*b*a^2*z^2+12*b^2*a*z-a^4+b^3

  ((a)!=0,b=0)
-z^12+4*a*z^9-6*a^2*z^6+4*a^3*z^3-a^4

  (b=0,a=0)
z^6

  ((b)!=0,a=0)
-z^12+3*b*z^8-3*b^2*z^4+b^3

  ((b)(a)!=0,729*a^4-4096*b^3=0)
-52488*a^2*z^11+46656*b*a*z^10-41472*b^2*z^9+216513
*a^3*z^8-34992*b*a^2*z^7+31104*b^2*a*z^6-1797120*
b^3*z^5+2803734*b*a^3*z^4-2649672*b^2*a^2*z^3+
3534912*b^3*a*z^2+5705216*b^4*z-272727*b^2*a^3

  ((b)(a)!=0,729*a^4+64*b^3=0)
-6561*a^2*z^10-2916*b*a*z^9-1944*b^2*z^8+39366*a^3
*z^7+39366*b*a^2*z^6+21384*b^2*a*z^5+16848*b^3*z^4
+205578*b*a^3*z^3+52731*b^2*a^2*z^2+41436*b^3*a*z
+6344*b^4

  ((b)(a)!=0,16767*a^4+5632*b^3=0)
-16767*z^12+67068*a*z^9+50301*b*z^8-100602*a^2*z^6+
804816*b*a*z^5-50301*b^2*z^4+67068*a^3*z^3+503010*
b*a^2*z^2+201204*b^2*a*z+22399*b^3
```

The following table includes timing data of this example. (OS Windows XP, CPU Pentium M 1.5GHz, Memory 1.0GB RAM)

'New' means our algorithm. 'reduce' means the output is a reduced comprehensive Gröbner system. 'opt' means that it uses several optimization technique some of which are discussed at the end of section 2. 'w/o opt' means that it does not use optimization technique except for the easiest case also described at the end of section 2. It could include not only redundant segments but also inconsistent segments. 'comp. G. basis.' means the algorithm `CGB` given in section 3, which also does not use optimization technique except for the easiest case. 'cases' means the number of segments in our algorithm and the number of case distinctions in others. We note that we get no answer for the examples below within 1 hour by `gsys` of Reduce with the option `off cgbgs;`.

System	Algorithm	time (sec.)	cases
Risa/Asir[5]	New (reduced, opt.)	0.4	7
Risa/Asir	New (w/o opt.,)	0.2	20
Risa/Asir	New (comp. G. basis)	0.6	—
Singular[6]	New (w/o opt.,)	0.2	20
Maple 9.5	New (w/o opt.,)	38.1	13
Maple 9.5	DISPGB Release 2.3	1240	3
Reduce[7]	CGB (gsys, on cgbgs)	2.6	8
Reduce	CGB (cgb, on cgbgs)	2.9	—

EXAMPLE 2. *Under the lexicographic term order such that $X > Y > Z$, compute a comprehensive Gröbner system (or a comprehensive Gröbner basis) for $F = \{X^4 - A, Y^5 - B, X + Y - Z\}$ where A and B are parameters.*

System	Algorithm	time (sec.)	cases
Risa/Asir	New (reduced, opt.)	22.8	15
Risa/Asir	New (w/o opt.,)	8.5	230
Risa/Asir	New (comp. G. basis)	135.4	—
Singular	New (w/o opt.,)	9.0	230
Maple 9.5	New (w/o opt.,)	—[8]	—
Maple 9.5	DISPGB	—[8]	—
Reduce	CGB	> 1 hour	—

EXAMPLE 3. *Let $f = ax_1^2 + by_1$ and $g = cy_2^2 + dx_2$. Under the lexicographic term order such that $x_1 > x_2 > y_1 > y_2 > s$, compute a comprehensive Gröbner system of*

$$\{f, g, (x_1 - x_2)^2 + (y_1 - y_2)^2 - s, \\ \partial f/\partial x_1 \cdot \partial g/\partial y_2 - \partial f/\partial y_1 \cdot \partial g/\partial x_2, \\ \partial f/\partial x_1 \cdot (y_1 - y_2) - \partial f/\partial y_1 \cdot (x_1 - x_2)\}$$

where a, b, c and d are parameters.

System	Algorithm	time (sec.)	cases
Risa/Asir	New (reduced, opt.)	147.0	21
Risa/Asir	New (w/o opt.,)	7.9	1515
Singular	New (w/o opt.,)	11.0	1515
Maple 9.5	New (w/o opt.,)	> 1 hour	—
Maple 9.5	DISPGB	> 1 hour	—
Reduce	CGB	> 1 hour	—

EXAMPLE 4. *A same computation of example 3 with $f = x_1^2 + y_1^2 + a$ and $g = y_2 - bx_2^2 + c$.*

System	Algorithm	time (sec.)	cases
Risa/Asir	New (reduced, opt.)	10.1	19
Risa/Asir	New (w/o opt.,)	7.8	81
Singular	New (w/o opt.,)	5.9	81
Maple 9.5	New (w/o opt.,)	904.7	27
Maple 9.5	DISPGB	> 1 hour	—
Reduce	CGB (gsys, on cgbgs)	17.2	14

[1] `http://www.math.kobe-u.ac.jp/Asir/`
[2] `http://www.singular.uni-kl.de/`
[3] `http://www.maplesoft.com/`
[4] `http://kurt.scitec.kobe-u.ac.jp/~sakira/CGBusingGB/`
[5] Kobe Distribution, version 20051024
[6] version 3-0-1
[7] version 3.8
[8] the computation is aborted by an error of Maple.

EXAMPLE 5. *Let* $f = (x-a)^2 + by^2 + b$. *Under the lexicographic term order such that* $x > y > z > s$, *compute a comprehensive Gröbner system of*

$$\{f - z, x^2 + y^2 + z^2 - s, x + \partial f/\partial x \cdot z, y + \partial f/\partial y \cdot z\}$$

where a *and* b *are parameters.*

System	Algorithm	time (sec.)	cases
Risa/Asir	New (reduced, opt.)	49.4	42
Risa/Asir	New (w/o opt.,)	46.4	342
Singular	New (w/o opt.,)	19.9	342
Maple 9.5	New (w/o opt.,)	>1 hour	—
Maple 9.5	DISPGB	1787.0	7
Reduce	CGB (gsys, on cgbgs)	102.9	14

EXAMPLE 6. *A same computation as example 5 with* $f = (x-a)^2 + ay^2 + b$.

System	Algorithm	time (sec.)	cases
Risa/Asir	New (reduced, opt.)	95.3	23
Risa/Asir	New (w/o opt.,)	126.7	503
Singular	New (w/o opt.,)	149.0	503
Maple 9.5	New (w/o opt.,)	>1 hour	—
Maple 9.5	DISPGB	>1 hour	—
Reduce	CGB	>1 hour	—

5. CONCLUSIONS AND REMARKS

One of the most important properties of our algorithms which does not hold in other existing algorithms is that we allow the case distinction not to be pairwise disjoint. As we describe in the paper, this property enables us to work entirely in a polynomial ring over the ground field K and makes our algorithm simple. We do not have to take care of disequations. This fact makes our algorithms extremely fast even when we produce redundant segments. This phenomenon also occurs among our implementations. In example 2 and 3 of the section 4, though a large amount of redundant segments are computed in the computations of 'w/o opt', the computation time of them is much shorter than the computations of 'reduced, opt'. The major reason is that the computation cost to check whether a segment is redundant is generally very high. (The cost to make the comprehensive Gröbner system reduced is very small.)

In general, the depth of our algorithms, is proportional to the number of parameters. Therefore, when the number of parameters is very small, under an environment where we can use parallel computation with enough amount of cpu's, the computation time of a comprehensive Gröbner system or a comprehensive Gröbner basis is also proportional to the computation time of each Gröbner basis in case they are almost same.

It should be noted that our algorithm are not fast in case there are much more parameters than main variables. For example, if each member of F is linear with respect to the main variables and F includes much more parameters than the main variables, our algorithms are generally much slower than the other existing algorithm.

6. REFERENCES

[1] Becker, T. (1994). On gröbner bases under specialization. Applicable Algebra in Engineering, Communication and Computing, 5, 1–8.

[2] Becker, T. and Weispfenning, V. (1993). Gröbner Bases –A Computational Approach to Commutative Algebra–, Springer-Verlag.

[3] Dolzmann, A. and Sturm, T. (1997). Redlog: Computer algebra meets computer logic, ACM SIGSAM Bulletin, 31, 2, 2–9.

[4] Kalkbrener, K. (1997). On the stability of gröbner bases under specialization, J. Symb. Comp. 24, 1, 51–58.

[5] Montes, A. (2002). A new algorithm for discussing Gröbner basis with parameters, J. Symb. Comp. 33, 1-2, 183–208.

[6] Manubens, M. and Montes, A. (2005). Improving DISPGB Algorithm Using the Discriminant Ideal, J. Symb. Comp., A3L 2005 special issue, to appear

[7] Noro, M. and Takeshima, T. (1992). Risa/Asir – A Computer Algebra System. International Symposium on Symbolic and Algebraic Computation (ISSAC 92), Proceedings, 387–396.

[8] Suzuki, A. and Sato, Y. (2002). An Alternative approach to Comprehensive Gröbner Bases. International Symposium on Symbolic and Algebraic Computation (ISSAC 2002), Proceedings, 255–261.

[9] Suzuki, A. and Sato, Y. (2003). An Alternative approach to Comprehensive Gröbner Bases. J. Symb. Comp. 36/3-4, 649–667.

[10] Weispfenning, V. (1992). Comprehensive Gröbner bases, J. Symb. Comp. 14/1, 1–29.

[11] Weispfenning, V. (2003). Canonical Comprehensive Gröbner bases, J. Symb. Comp. 36, 669-683.