Solving Systems of Algebraic Equations by Using Gröbner Bases

Michael Kalkbrener
Research Institute for Symbolic Computation (RISC)
Johannes Kepler Universität Linz, Austria

Abstract

In this paper we give an explicit description of an algorithm for finding all solutions of a system of algebraic equations which is solvable and has finitely many solutions. This algorithm is an improved version of a method which was deviced by B. Buchberger. By a theorem proven in this paper, gcd-computations occuring in Buchberger's method can be avoided in our algorithm.

1 Introduction

The method of Gröbner bases was introduced by B. Buchberger in his 1965 Ph.D.thesis. This work is accessible in [1]. His method, as its central objective, solves the simplification problem for polynomial ideals and, on this basis, gives easy solutions to a large number of other algorithmic problems.

In the present paper we use Gröbner bases for the solution of systems of algebraic equations. In particular, we deal with the following problem:

Given: *F, a finite set of polynomials in the indeterminates $x_1, \ldots, x_n$ over a field K such that F is solvable and has finitely many solutions. (A solution of F is an element b of $\bar{K}^n$ such that $f(b) = 0$ for all $f \in F$, where $\bar{K}$ is the algebraic closure of K.)*

Find: *all solutions of the system F.*

A first algorithm for reducing this multivariate problem to a univariate one by using Gröbner bases appears in [1].

A second algorithm (see [2], Method 6.10) makes use of the fact that if the purely lexicographical ordering is used every Gröbner basis G of a zero-dimensional ideal I consists of finitely many polynomials

$$\begin{array}{rcl} G_{1,1} & \in & K[x_1], \\ G_{2,1} & \in & K[x_1, x_2], \\ \cdots & & \cdots \\ G_{2,car_2} & \in & K[x_1, x_2], \\ \cdots & & \cdots \\ G_{n,1} & \in & K[x_1, \ldots, x_n], \\ \cdots & & \cdots \\ G_{n,car_n} & \in & K[x_1, \ldots, x_n], \end{array}$$

where $car_2 \geq 1, \ldots, car_n \geq 1$, and the i-th elimination ideal of I is the ideal generated by $\{G_{1,1}, G_{2,1}, \ldots, G_{i,car_i}\}$ (see [4]). Method 6.10 finds a solution $(b_1, \ldots, b_i, c)$ of the $i+1$-th elimination ideal by adjoining a zero c of the polynomial

$$gcd(G_{i+1,1}(b_1, \ldots, b_i, x_{i+1}), \ldots, G_{i+1,car_{i+1}}(b_1, \ldots, b_i, x_{i+1}))$$

to the solution $(b_1, \ldots, b_i)$ of the i-th elimination ideal.

In this paper we prove a theorem which states that there exists a $d \in \bar{K}$ and an $r \in \{1, \ldots, car_{i+1}\}$ such that

$$d \cdot G_{i+1,r}(b_1, \ldots, b_i, x_{i+1}) = gcd(G_{i+1,1}(b_1, \ldots, b_i, x_{i+1}), \ldots, G_{i+1,car_{i+1}}(b_1, \ldots, b_i, x_{i+1}))$$

and that the polynomial $G_{i+1,r}$ can be easily found by a test for zero in an extension field of K. Therefore, this theorem leads to an improved version of Method 6.10, in which the gcd-computation is avoided.

In section 2 we introduce a few definitions. In section 3 a specification of the problem and the explicit descriptions of the algorithm in [2] and of our improved version are given. Furthermore, the theorem on which our method is based is presented. In section 4 we prove this theorem.

2 Definitions

Throughout the paper K denotes an arbitrary field and $\bar{K}$ the algebraic closure of K.

Let n be a natural number. By $K[x_1, \ldots, x_n]$ we denote the ring of all polynomials over K in n indeterminates.

Let f be an element of $K[x_1, \ldots, x_n]$ and r an element of $\{1, \ldots, n\}$.

We denote the *degree of* f in the variable x_r by $deg(f, r)$. For a non-constant f, there is a first s such that $f \in K[x_1, \ldots, x_s]$. Considering f as a polynomial in x_s, we denote the *leading coefficient* by $lc(f)$.

Let H be a finite subset of $K[x_1, \ldots, x_n]$ and I an ideal in $K[x_1, \ldots, x_n]$.

By $Ideal(H)$ we denote the *ideal generated by* H. The set

$$V(I) = \{\, a \in \bar{K}^n \mid f(a) = 0 \text{ for all } f \in I \,\}$$

is called the *variety of* I. We denote the *radical of* I by $\sqrt{I}$ and the set $I \cap K[x_1, \ldots, x_r]$ by $I_{/x_r}$.

Let n be greater than 1 and b an element of $\bar{K}^{n-1}$.

By $I(b, x_n)$ we denote the set

$$\{\, h(b, x_n) \in K(b)[x_n] \mid h \in I \,\}.$$

By Hilbert's basis theorem, we can choose a finite subset $F = \{f_1, \ldots, f_m\}$ of $K[x_1, \ldots, x_n]$ such that $Ideal(F) = I$. Clearly,

$$I(b, x_n) = Ideal(\{f_1(b, x_n), \ldots, f_m(b, x_n)\}),$$

where the ideal on the right-hand side is formed in $K(b)[x_n]$.

For h, an element of $K(b)[x_n]$, the following conditions are equivalent:

1. $h = gcd(\{f_1(b, x_n), \ldots, f_m(b, x_n)\})$,
2. $I(b, x_n) = Ideal(\{h\})$ and h is normed.

We denote the uniquely determined $h \in K(b)[x_n]$ which satiesfies these conditions by $gcd(I, b)$.

Throughout the paper we fix the "purely lexicographical ordering" of the power products of $x_1, \ldots, x_n$. We denote it by $\ll$. Furthermore, we assume

$$x_1 \ll x_2 \ll \ldots \ll x_n.$$

We refer to [2] for the definitions of *LeadingPowerProduct, SPolynomial, Gröbner basis,* and *reduced Gröbner basis.*

Let G be a reduced Gröbner basis.

Let $G_{r,1}, \ldots, G_{r,car_r}$ be the polynomials in G that belong to $K[x_1, \ldots, x_r]$ but not to $K[x_1, \ldots, x_{r-1}]$. We suppose the order chosen in such a way that

$$LeadingPowerProduct(G_{r,j}) \ll LeadingPowerProduct(G_{r,k}) \text{ for } j < k.$$

3 Solving Systems of Algebraic Equations by Using Gröbner Bases

Throughout the following sections n is a natural number greater than 1.

In this paper we want to solve the following problem:

Given: F, a finite subset of $K[x_1, \ldots, x_n]$ such that I is zero-dimensional, where $I := Ideal(F)$.

Find: $V(I)$.

In [2] B. Buchberger presents the following algorithm for this problem:

Algorithm 1

input: F, a finite subset of $K[x_1, \ldots, x_n]$ such that I is a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, where $I := Ideal(F)$.

output: X_n, a finite subset of $\bar{K}^n$ such that $X_n = V(I)$.

G:=GB(F), where $GB(F)$ is the uniquely determined reduced Gröbner basis such that $Ideal(GB(F)) = Ideal(F)$.

Comment: It is proven in [4] that $Ideal(G) \cap K[x_1, \ldots, x_r] = Ideal(G \cap K[x_1, \ldots, x_r])$ (for $r = 1, \ldots, n$), where the ideal on the right-hand side is formed in $K[x_1, \ldots, x_r]$. Therefore, the polynomials in G have their variables "separated". G contains exactly one polynomial in $K[x_1]$ (actually, it is the polynomial in $Ideal(G) \cap K[x_1]$ with smallest degree). According to the definition in section 2 we denote it by $G_{1,1}$.

The successive elimination can, then, be carried out by the following process:

$X_1 := \{ c \mid c \in \bar{K}$ and $G_{1,1}(c) = 0 \}$
for $r := 1$ *to* $n - 1$ *do*
  $X_{r+1} := \emptyset$
  for all $b \in X_r$ *do*
    $H := \{ G_{r+1,s}(b, x_{r+1}) \mid s \in \{1, \ldots, car_{r+1}\} \}$
    q:= greatest common divisor of the polynomials in H
    $X_{r+1} := X_{r+1} \cup \{ (b, c) \mid c \in \bar{K}$ and $q(c) = 0 \}$

Upon termination, X_n will contain all the solutions.

The improved version of this algorithm is based on the following new theorem which we prove in the next section.

Theorem 1 *Let l be an element of $\{2, \ldots, n\}$, I a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, G the reduced Gröbner basis in $K[x_1, \ldots, x_n]$ such that $Ideal(G) = I$, and $b \in V(I_{/x_{l-1}})$.*
Then there exists a $d \in \bar{K}$ such that

$$d \cdot G_{l,min_b}(b, x_l) = gcd(\{G_{l,1}(b, x_l), \ldots, G_{l,car_l}(b, x_l)\}),$$

where min_b denotes the minimum of the set

$$\{ r \mid r \in \{1, \ldots, car_l\} \text{ and } lc(G_{l,r})(b) \neq 0 \}.$$

Therefore, we can replace the instructions

$H := \{ G_{r+1,s}(b, x_{r+1}) \mid s \in \{1, \ldots, car_{r+1}\} \}$
q:= greatest common divisor of the polynomials in H

in Algorithm 1 by the instruction

$q := G_{r+1,min_b}(b, x_{r+1})$

and obtain the following algorithm:

Algorithm 2

input: F, a finite subset of $K[x_1, \ldots, x_n]$ such that I is a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, where $I := Ideal(F)$.

output: X_n, a finite subset of $\bar{K}^n$ such that $X_n = V(I)$.

$G := GB(F)$
$X_1 := \{ c \mid c \in \bar{K} \text{ and } G_{1,1}(c) = 0 \}$
for $r := 1$ *to* $n-1$ *do*
  $X_{r+1} := \emptyset$
  for all $b \in X_r$ *do*
    $q := G_{r+1,min_b}(b, x_{r+1})$
    $X_{r+1} := X_{r+1} \cup \{ (b, c) \mid c \in \bar{K} \text{ and } q(c) = 0 \}$

Note that for computing min_b, where $b \in V(I_{/x_{r-1}})$, one has to check only whether

$$\begin{aligned} (lc(G_{r,1}))(b) &= 0, \\ (lc(G_{r,2}))(b) &= 0, \\ \ldots &\; . \; . \end{aligned}$$

till the first s is found such that

$$(lc(G_{r,s}))(b) \neq 0.$$

4 Proof of Theorem 1

For proving Theorem 1 we first show a stronger result for reduced Gröbner bases of zero-dimensional primary ideals:

Theorem 2 *Let l be an element of $\{2, \ldots, n\}$, Q a zero-dimensional primary ideal in $K[x_1, \ldots, x_n]$, and G the reduced Gröbner basis in $K[x_1, \ldots, x_n]$ such that $Ideal(G) = Q$. Then*

$$G_{l,1}(b, x_l) = \ldots = G_{l,car_l - 1}(b, x_l) = 0 \tag{1}$$

for all $b \in V(Q_{/x_{l-1}})$.

Proof:

We first show that (1) holds for some $b \in V(Q_{/x_{l-1}})$:

We assume, to the contrary, that

$$\text{for every } b \in V(Q_{/x_{l-1}}) \\ \text{there exists an } r \in \{1, \ldots, car_l - 1\} \text{ with } G_{l,r}(b, x_l) \neq 0. \tag{2}$$

In this proof we denote $(G \cap K[x_1, \ldots, x_l]) \setminus \{G_{l,car_l}\}$ by F.
Let $f_1, f_2 \in F$.
By Method 6.9 in [2], there exists a natural number s such that

$$LeadingPowerProduct(G_{l,car_l}) = x_l^s.$$

Therefore,
$$deg(f_1, l) < deg(G_{l,car_l}, l) \text{ and } deg(f_2, l) < deg(G_{l,car_l}, l).$$

From this and the definition of the S-polynomial we obtain
$$deg(SPolynomial(f_1, f_2), l) \leq \max\{deg(f_1, l), deg(f_2, l)\} < deg(G_{l,car_l}, l).$$

Thus, $SPolynomial(f_1, f_2)$ reduces to zero modulo F. By Theorem 6.2 in [2],
$$F \textit{ is a Gröbner basis.} \tag{3}$$

Obviously,
$$F \textit{ is reduced.} \tag{4}$$

$G \cap K[x_1, \ldots, x_{l-1}]$ is a reduced Gröbner basis because $SPolynomial(g_1, g_2)$ reduces to zero modulo $G \cap K[x_1, \ldots, x_{l-1}]$ for all $g_1, g_2 \in G \cap K[x_1, \ldots, x_{l-1}]$. By Lemma 6.8 in [2],
$$Ideal(G \cap K[x_1, \ldots, x_{l-1}]) = Q_{/x_{l-1}}.$$

Thus, by Method 6.9 in [2],
$$V(Q_{/x_{l-1}}) \textit{ is finite.} \tag{5}$$

Let $(c_1, \ldots, c_l) \in V(Ideal(F))$. Then
$$f(c_1, \ldots, c_{l-1}) = 0 \text{ for every } f \in G \cap K[x_1, \ldots, x_{l-1}].$$

So, by Lemma 6.8 in [2],
$$(c_1, \ldots, c_{l-1}) \in V(Q_{/x_{l-1}}).$$

From assumption (2) we know that there exists an $r \in \{1, \ldots, car_l - 1\}$ with
$$G_{l,r}(c_1, \ldots, c_{l-1}, x_l) \neq 0.$$

Thus,
$$\{\, a \mid a \in \bar{K} \text{ and } (c_1, \ldots, c_{l-1}, a) \in V(Ideal(F)) \,\} \text{ is finite.}$$

By this fact and (5),
$$V(Ideal(F)) \textit{ is finite.} \tag{6}$$

Thus, by (3), (4), and (6), F is a reduced Gröbner basis and $V(Ideal(F))$ is finite.

On the other hand, there exists no polynomial f in F such that
$$LeadingPowerProduct(f) \in K[x_l].$$

This is a contradiction to Method 6.9 in [2].

Thus, in contrast to assumption (2), there exists a $b' \in V(Q_{/x_{l-1}})$ with
$$G_{l,1}(b', x_l) = \ldots = G_{l,car_l-1}(b', x_l) = 0.$$

From this we now deduce that (1) holds for all $b \in V(Q_{/x_{l-1}})$*:*

Let $b'' \in V(Q_{/x_{l-1}})$.

It is easy to prove that $Q_{/x_{l-1}}$ is a zero-dimensional primary ideal in $K[x_1, \ldots, x_{l-1}]$. Hence,

$$\sqrt{Q_{/x_{l-1}}} \text{ is a zero-dimensional prime ideal.}$$

Let $k \in \{1, \ldots, car_{l-1}\}$.

We write $G_{l,k}$ in the form

$$p_j(x_1, \ldots, x_{l-1})x_l^j + \ldots + p_0(x_1, \ldots, x_{l-1}),$$

where $j := deg(G_{l,k}, l)$. As

$$V(Q_{/x_{l-1}}) = V(\sqrt{Q_{/x_{l-1}}})$$

(see [5], section 131, p. 167), b' and b'' are elements of $V(\sqrt{Q_{/x_{l-1}}})$. Thus,

$$p_s(b') = 0 \text{ iff } p_s \in \sqrt{Q_{/x_{l-1}}} \text{ iff } p_s(b'') = 0 \text{ for all } s \in \{0, \ldots, j\}$$

(see [5], section 129, p. 162). Hence,

$$G_{l,1}(b'', x_l) = \ldots = G_{l,car_l-1}(b'', x_l) = 0. \bullet$$

Corollary 1 is an easy consequence of the previous theorem.

Corollary 1 *Let l be an element of $\{2, \ldots, n\}$, Q a zero-dimensional primary ideal in $K[x_1, \ldots, x_n]$.*

Then there exists an $f \in Q_{/x_l}$ such that

$$f \in K[x_1, \ldots, x_l] \backslash K[x_1, \ldots, x_{l-1}], \ lc(f) = 1, \text{ and } gcd(Q_{/x_l}, b) = f(b, x_l) \text{ for all } b \in V(Q_{/x_{l-1}}).$$

Proof: Let G be the reduced Gröbner basis in $K[x_1, \ldots, x_n]$ such that

$$Ideal(G) = Q.$$

By definition,

$$G_{l,car_l} \in K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}].$$

We have proven that

$$lc(G_{l,car_l}) = 1.$$

Furthermore, by Lemma 6.8 in [2] and Theorem 2,

$$gcd(Q_{/x_l}, b) = gcd(\{G_{1,1}(b_1), \ldots, G_{l,car_l}(b, x_l)\}) = G_{l,car_l}(b, x_l) \text{ for all } b \in V(Q_{/x_{l-1}}). \bullet$$

A generalization of Corollary 1 is the next theorem.

Theorem 3 *Let l be an element of $\{2, \ldots, n\}$, I a zero-dimensional ideal in $K[x_1, \ldots, x_n]$, and $b \in V(I_{/x_{l-1}})$.*

Then there exists an $f \in I_{/x_l}$ such that

$$f \in K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}], \ (lc(f))(b) \neq 0, \text{ and } gcd(I_{/x_l}, b) = f(b, x_l).$$

Before we give a proof of Theorem 3 we show the following lemma, which is required in this proof.

Lemma 1 *Let m be a natural number, J a zero-dimensional ideal in $K[x_1, \ldots, x_m]$, and*

$$J = Q_1 \cap \ldots \cap Q_r$$

a reduced primary decomposition of J. Then

$$V(Q_s) \cap V(Q_{s'}) = \emptyset \textit{ for } s \neq s'.$$

Proof: We assume that there exists a

$$b \in V(Q_s) \cap V(Q_{s'}) \text{ for some } s, s' \in \{1, \ldots, r\}.$$

As $V(Q_s) = V(\sqrt{Q_s})$ and $V(Q_{s'}) = V(\sqrt{Q_{s'}})$,

$$b \in V(\sqrt{Q_s}) \cap V(\sqrt{Q_{s'}}).$$

As $\sqrt{Q_s}$ and $\sqrt{Q_{s'}}$ are zero-dimensional, b is a generic zero of $\sqrt{Q_s}$ and $\sqrt{Q_{s'}}$.

Let $f \in K[x_1, \ldots, x_m]$. From

$$f \in \sqrt{Q_s} \quad \text{iff} \quad f(b) = 0 \quad \text{iff} \quad f \in \sqrt{Q_{s'}}$$

we obtain

$$\sqrt{Q_s} = \sqrt{Q_{s'}}.$$

Hence,

$$s = s',$$

because we assumed the primary decomposition to be reduced. •

Proof of Theorem 3:

Let $Q_1, \ldots, Q_r$ be zero-dimensional primary ideals in $K[x_1, \ldots, x_n]$ such that $I_{/x_l} = Q_{1/x_l} \cap \ldots \cap Q_{r/x_l}$ is a reduced primary decomposition of $I_{/x_l}$. From

$$I_{/x_{l-1}} = Q_{1/x_{l-1}} \cap \ldots \cap Q_{r/x_{l-1}},$$

we have

$$V(I_{/x_{l-1}}) = V(Q_{1/x_{l-1}}) \cup \ldots \cup V(Q_{r/x_{l-1}}).$$

Without loss of generality, we assume that the primary ideals $Q_1, \ldots, Q_r$ are ordered in such a way that there exists an $s \in \{1, \ldots, r\}$ with

$$b \in V(Q_{1/x_{l-1}}), \ldots, b \in V(Q_{s/x_{l-1}}), b \notin V(Q_{s+1/x_{l-1}}), \ldots, b \notin V(Q_{r/x_{l-1}}).$$

We define $h_t \in Q_{1/x_l} \cap \ldots \cap Q_{t/x_l}$ such that $h_t \in K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}]$,
$h_t(b, x_l) = gcd(Q_{1/x_l} \cap \ldots \cap Q_{t/x_l}, b)$, and $lc(h_t) = 1$ for every $t \in \{1, \ldots, s\}$:

By Corollary 1, there exists an $f \in Q_{1/x_l}$ with

$$f \in K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}],\ lc(f) = 1,\ \text{and}\ f(b, x_l) = gcd(Q_{1/x_l}, b).$$

Set $h_1 := f$.

We assume that $t \in \{1, \ldots, s-1\}$ and that h_t is already defined.

Let $f \in Q_{t+1/x_l}$ such that

$$f \in K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}],\ lc(f) = 1,\ \text{and}\ f(b, x_l) = gcd(Q_{t+1/x_l}, b).$$

Set $h_{t+1} := h_t \cdot f$.

From

$$gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b) \in (Q_{1/x_l} \cap \ldots \cap Q_{t/x_l})(b, x_l) \text{ and}$$
$$gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b) \in Q_{t+1/x_l}(b, x_l)$$

we obtain

$$h_t(b, x_l) \text{ divides } gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b) \text{ and}$$
$$f(b, x_l) \text{ divides } gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b).$$

Assume that there exists a $c \in \bar{K}$ such that

$$h_t(b, c) = f(b, c) = 0.$$

From the fact that $h_t(b, x_l)$ divides every element of $(Q_{1/x_l} \cap \ldots \cap Q_{t/x_l})(b, x_l)$ and that $f(b, x_l)$ divides every element of $Q_{t+1/x_l}(b, x_l)$ we obtain

$$(b_1, \ldots, b_{l-1}, c) \in V(Q_{1/x_l} \cap \ldots \cap Q_{t/x_l}) \cap V(Q_{t+1/x_l}).$$

As

$$V(Q_{1/x_l}) \cup \ldots \cup V(Q_{t/x_l}) = V(Q_{1/x_l} \cap \ldots \cap Q_{t/x_l}),$$

we have a contradiction to Lemma 1.

Therefore, $h_t(b, x_l)$ and $f(b, x_l)$ are relatively prime. Thus,

$$h_{t+1}(b, x_l) \text{ divides } gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b).$$

Furthermore,

$$h_{t+1} \in K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}] \text{ and } lc(h_{t+1}) = 1.$$

From this and $h_{t+1}(b, x_l) \in (Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l})(b, x_l)$, it follows

$$h_{t+1}(b, x_l) = gcd(Q_{1/x_l} \cap \ldots \cap Q_{t+1/x_l}, b).$$

We define $q \in K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}]$ such that there exists an $e \in \bar{K}$ with $e \cdot q(b, x_l) = gcd(I_{/x_l}, b)$ and $deg(q, l) = deg(q(b, x_l), l)$:

We choose a $p_t \in Q_{t/x_{l-1}}$ for every $t \in \{s+1, \ldots, r\}$ such that

$$p_t(b) \neq 0.$$

This is always possible, because $b \notin V(Q_{t/x_{l-1}})$ for all $t \in \{s+1, \ldots, r\}$.

Set $q := p_{s+1} \cdot \ldots \cdot p_r \cdot h_s$.

Obviously, $q \in I_{/x_l}$. As

$$q(b, x_l) = p_{s+1}(b) \cdot \ldots \cdot p_r(b) \cdot gcd(Q_{1/x_l} \cap \ldots \cap Q_{s/x_l}, b) \text{ and } p_{s+1}(b) \cdot \ldots \cdot p_r(b) \in \bar{K} \setminus \{0\},$$

we know that

$$q(b, x_l) \text{ divides } gcd(Q_{1/x_l} \cap \ldots \cap Q_{s/x_l}, b).$$

From $h_s \in K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}]$ and $lc(h_s) = 1$ we obtain

$$deg(q, l) = deg(h_s, l) = deg(h_s(b, x_l), l) = deg(q(b, x_l), l). \tag{7}$$

As $I_{/x_l}$ is a subset of $Q_{1/x_l} \cap \ldots \cap Q_{s/x_l}$,

$$gcd(Q_{1/x_l} \cap \ldots \cap Q_{s/x_l}, b) \text{ divides } gcd(I_{/x_l}, b).$$

Thus,

$$q(b, x_l) \text{ divides } gcd(I_{/x_l}, b) \text{ and } q \in I_{/x_l}.$$

Hence, there exists an $e \in \bar{K}$ such that

$$e \cdot q(b, x_l) = gcd(I_{/x_l}, b). \tag{8}$$

From $q \in K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}]$, (7), and (8) we obtain that

$$e \cdot q \in K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}],\ lc(e \cdot q)(b) \neq 0,\ \text{and } (e \cdot q)(b, x_l) = gcd(I_{/x_l}, b). \quad \bullet$$

By means of this theorem it is relatively easy to prove Theorem 1:

Proof of Theorem 1: Let $q \in I_{/x_l}$ such that

$$q \in K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}],\ (lc(q))(b) \neq 0,\ \text{and } gcd(I_{/x_l}, b) = q(b, x_l).$$

We know that

$$g(b) = 0 \text{ for all } g \in G \cap K[x_1, \ldots, x_{l-1}],$$
$$q(b, x_l) \neq 0, \text{ and}$$
$$q \text{ reduces to zero modulo } G.$$

Thus, there exists an $f \in G \cap K[x_1, \ldots, x_l] \setminus K[x_1, \ldots, x_{l-1}]$ such that

$$f(b, x_l) \neq 0 \text{ and } deg(f, l) \leq deg(q, l).$$

Therefore,

$$deg(f(b, x_l), l) \leq deg(f, l) \leq deg(q, l) = deg(q(b, x_l), l).$$

As $q(b, x_l)$ divides $f(b, x_l)$, there exists an $e \in \bar{K}$ such that

$$e \cdot f(b, x_l) = q(b, x_l) = gcd(I_{/x_l}, b).$$

From

$$deg(f(b, x_l), l) = deg(q(b, x_l), l) = deg(q, l) \geq deg(f, l).$$

we obtain

$$lc(f)(b) \neq 0.$$

Thus,

$$deg(G_{l,min_b}(b, x_l), l) \leq deg(G_{l,min_b}, l) \leq deg(f, l) = deg(f(b, x_l), l).$$

On the other hand, $f(b, x_l)$ divides $G_{l,min_b}(b, x_l)$. Hence, there exists a $d \in \bar{K}$ such that

$$d \cdot G_{l,min_b}(b, x_l) = e \cdot f(b, x_l) = gcd(I_{/x_l}, b).$$

From Lemma 6.8 in [2],

$$d \cdot G_{l,min_b}(b, x_l) = gcd(\{G_{l,1}(b, x_l), \ldots, G_{l,car_l}(b, x_l)\}). \quad \bullet$$

In the case of two variables this result can be easily deduced from Lazard's structure theorem (see [3]).

Acknowledgement: I want to thank B. Roider. He suggested Theorem 1 might be true and stimulated me to prove this.

References

[1] B. Buchberger: *Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems*, Aequationes Math. 4/3, 374-383 (1970)

[2] B. Buchberger: *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*, in Recent Trends in Multidimensional Systems Theory, N.K. Bose (ed.), D. Reidel Publ. Comp. 184-232 (1985)

[3] D. Lazard: *Ideal Bases and Primary Decomposition: Case of Two Variables*, J. of Symbolic Computation 1, 261-270 (1985)

[4] W. Trinks: *Über B. Buchbergers Verfahren, Systeme algebraischer Gleichungen zu lösen*, J. of Number Theory 10/4, 475-488 (1978)

[5] B.L. van der Waerden: *Algebra II*, Springer-Verlag (1967)