Parametric Gröbner bases
Geometry & applications

Andreas Bøgh Poulsen *201805425*

AARHUS UNIVERSITET
INSTITUT FOR MATEMATIK

Supervisor: Niels Lauritzen

Contents

Introduction

1 Preliminaries

This project will assume familiarity with ring theory, multivariate polynomials over fields. A familiarity with Gröbner bases will be beneficial, but we will introduce the necesary notations and definitions. Let R be a Noetherian, commutative ring and $X = (x_1, x_2, \dots, x_n)$ be an ordered collection of symbols. We denote the ring of polynomials in these variables $R[X]$. Given two (disjoint) sets of variables X and Y, we will use $R[X, Y]$ to mean $R[X \cup Y]$, which is isomorphic to $R[X][Y]$. A monomial is a product of variables and a term is a monomial times a coefficient. We denote a monomial as X^v for some $v \in \mathbb{N}^n$.

1.1 · Definition (Monomial order, leading term). A *monomial order* is a total order $<$ on the set of monomials satisfying that $u < v \implies wu < wv$.

Given a monomial order $<$ and a polynomial $f \in R[X]$, the *leading term* of f is the term with the largest monomial w.r.t. $<$ and is denoted by $\mathrm{lt}_<(f)$. If $\mathrm{lt}_<(f) = a \cdot m$ for some monomial m and $a \in R$, then we denote $\mathrm{lm}_<(f) = m$ and $\mathrm{lc}_<(f) = a$. If $<$ is clear from context, it will be omitted.

These definitions naturally extend to sets of polynomials, so given a set of polynomials $F \subset k[X]$, we denote $\mathrm{lm}_<(F) := \{\mathrm{lm}_<(f) \mid f \in F\}$. The above definitions work over a general ring (and we will use that), for from here, we'll work over a field k. With this, we can give the definition of a Gröbner basis.

1.2 · Definition (Gröbner basis). Let $G \subset k[X]$ be a finite set of polynomials and $<$ be a monomial order. We say G is a *Gröbner basis* if $\langle \mathrm{lt}_<(G) \rangle = \langle \mathrm{lt}_<(\langle G \rangle) \rangle$.

2 Definitions and initial results

The purpose of this project is to study parametric Gröbner bases, so let's introduce those. The bare concept is rather simple.

2.1 · Definition (Parametric Gröbner basis). Let k, k_1 be fields, U and X be collections of variables and $F \subset k[X, U]$ be a finite set of polynomials. A *parametric Gröbner basis* is a finite set of polynomials $G \subset k[X, U]$ such that $\sigma(G)$ is a Gröbner basis of $\langle \sigma(F) \rangle$ for any ring homomorphism $\sigma : k[U] \to k_1$.

We call such a $\sigma : k[U] \to k_1$ a *specialization*. By the linearity of σ, all such ring homomorphisms can be characterized by their image of U. Thus, we can identify $\{\sigma : k[U] \to k_1 \mid \sigma \text{ is a ring hom.}\}$ with the affine space k_1^m when U has m elements. For $\alpha \in k_1^m$ we'll denote the corresponding map

$$\sigma_\alpha(u_i) = \alpha_i \quad \text{for } u_i \in U$$

extended linearly.

When we work with these parametric Gröbner bases, it will be more convenient to have a bit more information attached to them, namely which elements are required for which σ. Since σ is described by an $\alpha \in k_1^m$, we can restrict them using subsets of k_1^m.

2.2 · Definition (Vanishing sets & algebraic sets). Let E be a finite subset of $k[X]$. Then the *vanishing set* of E is $V(E) := \{v \in k^n \mid e(v) = 0 \ \ \forall e \in E\}$.

An *algebraic set* is a set of the form $V(E) \setminus V(N)$ for two finite subsets E and N of $k[X]$.

2.3 · Definition (Gröbner system). Let A be an algebraic set and $F, G \subset k[X, U]$ be finite sets. Then (A, G) is called a *segment of a Gröbner system for F* if $\sigma_\alpha(G)$ is a Gröbner basis of $\langle \sigma_\alpha(F) \rangle$ for all $\alpha \in A$. A set $\{(A_1, G_1), \dots, (A_t, G_t)\}$ is called a *Gröbner system* if each (A_i, G_i) is a segment of a Gröbner system. A Gröbner system $\{(A_1, G_1, \dots, (A_t, G_t))\}$ is called *comprehensive*, if $\bigcup_{i=1}^t A_i = k_1^{|U|}$. We also say a Gröbner system is *comprehensive on $L \subset k_1^{|U|}$* if $\bigcup_{i=1}^t A_i = L$.

We will sometimes call a triple (E, N, G) for a segment of a Gröbner system. By this we mean that $(V(E) \setminus V(N), G)$ is a segment of a Gröbner system.

2.4 · Example. *Let $X = \{x, y\}$ and $U = \{u\}$ and consider the polynomials $f(x, y, u) = ux^2 + x$ and $g(x, y, u) = xy + 1$. When $u \neq 0$, a Gröbner basis of $\langle f, g \rangle$ could be $(y - u, ux + 1)$, whatever u may be.* TODO

Skriv om Kalkbrener

2.5 · Definition (Leading coefficient w.r.t. variables). Let $f \in k[U][X]$. Then the leading term of f is denoted $\mathrm{lt}_U(f)$, the leading coefficient is $\mathrm{lc}_U(f)$ and the leading monomial is $\mathrm{lm}_U(f)$. These notations are also used when $f \in k[X, U]$, just viewing f as a polynomial in $k[U][X]$.

Note that $\mathrm{lc}_U(f) \in k[U]$, i.e. the leading term is a polynomial in $k[U]$ times a monomial in X.

From this point, we assume that the monomial order on $k[X, U]$ satisfies $X^{v_1} > U^{v_2}$ for all $v_1 \in \mathbb{N}^{|X|}$ and $v_2 \in \mathbb{N}^{|U|}$. This monomial order restricts to a monomial order on $k[X]$, denoted by $<_X$. Note that this assumption is not too restrictive, as we're usually only interested in a certain monomial order on the variables, since the parameters will be specialized away anyway. Thus for a given monomial order $<_X$, we can construct a suitable monomial order on $k[X, U]$, by using $<_X$ and breaking ties with any monomial order on $k[U]$.

2.1 A useful criterion

In this section we will prove a criterion to decide when a Gröbner basis G of an ideal $\langle F \rangle$ maps to a Gröbner basis $\sigma(G)$ if the ideal $\langle \sigma(F) \rangle$. This is theorem 3.1 in [1].

2.6 · Lemma. *Let G be a Gröbner basis of an ideal $\langle F\rangle$ w.r.t. $<$, let $\sigma : k[U] \to k_1$ be a specialization and set $G_\sigma = \{\sigma(g) \in G \mid \sigma(\mathrm{lc}_U(g)) \neq 0\} = \{g_1, g_2, \dots, g_l\} \subset k_1[X]$. Then G_σ is a Gröbner basis of the ideal $\langle\sigma(F)\rangle$ w.r.t. $<_X$ if and only if $\sigma(g)$ is reducible to 0 modulo G_σ for every $g \in G$.*

Proof. First, we prove " $\Longrightarrow$ ": Suppose G_σ is a Gröbner basis of $\langle\sigma(F)\rangle$. Since σ is linear and every element of $\langle F\rangle$ is a linear combination of elements in F, we have $\langle\sigma(F)\rangle = \sigma(\langle F\rangle)$. Since $g \in F$ for every $g \in G$, $\sigma(g) \in \langle\sigma(F)\rangle$, thus $\sigma(g)$ reduces to 0 modulo G_σ.

Next, we prove "$\Longleftarrow$": Assume that $\sigma(g)$ is reducible to 0 modulo G_σ for every $g \in G$ and let $f \in \langle F\rangle$ such that $\sigma(f) \neq 0$. It's enough to show that there exists a $g \in \langle F\rangle$ such that $\mathrm{lm}_U(g) \mid \mathrm{lm}_U(\sigma(f))$ and $\sigma(\mathrm{lc}_U(g)) \neq 0$. Indeed, if that is the case, then $\mathrm{lt}(\sigma(g))$ □

2.2 Computing Gröbner systems

We will use lemma **??** in a slightly different formulation:

2.7 · Lemma. *Let $G = \{g_1, g_2, \dots, g_k\}$ be a Gröbner basis of an ideal $\langle F\rangle$ in $k[X, U]$ w.r.t $<$ and let $\alpha \in k_1^m$. If $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for each $g \in G \setminus (G \cap k[U])$, then $\sigma_\alpha(G)$ is a Gröbner basis of $\langle\sigma_\alpha(F)\rangle$.*

Proof. Let $G_\alpha = \{\sigma_\alpha(g) \mid \sigma_\alpha(\mathrm{lc}_U(g)) \neq 0\}$. If there is any $g \in G$, such that $\sigma_\alpha(g) \in k_1 \setminus \{0\}$, then $g \in G \cap k[U]$ since $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for all $g \in G \setminus K[U]$. Furthermore, since $g \in \langle F\rangle$, we get that $\langle\sigma_\alpha(F)\rangle = k_1[X]$ and $\sigma_\alpha(G)$ is a Gröbner basis.

If there is no such g, then $\alpha \in V(G \cap k[U])$. Take any $g \in G$. If $\sigma_\alpha(g) \in G_\alpha$, then $\mathrm{lt}(\sigma_\alpha(g)) = a \cdot \mathrm{lm}_U(g)$ for some $a \in k_1$ since $X^{\nu_1} > U^{\nu_2}$. Thus the monomial of its leading term is preserved by σ_α, so $\sigma_\alpha(g)$ is reducible to 0 modulo G_α, since it's leading term is divisible by its own leading term.

On the other hand, if $\sigma_\alpha(g) \notin G_\alpha$, then we must have $g \in G \cap k[U]$. Since $\alpha \in V(G \cap k[U])$ then $\sigma_\alpha(g) = 0$, so is immediately reducible to zero. Thus $\sigma_\alpha(G)$ is a Gröbner basis of $\langle\sigma_\alpha(F)\rangle$ by lemma **??**. □

With lemma **??** in mind, we can start constructing Gröbner systems. Let G be a reduced Gröbner basis of an ideal $\langle F\rangle \subset k[X, U]$, and let $H = \{\mathrm{lc}_U(g) \mid g \in G \setminus k[U]\}$. Then $\left(k_1^m \setminus \bigcup_{h \in H} V(h), G\right)$ is a segment of a Gröbner system. Thus, to make a Gröbner system, we need to find segments covering $\bigcup_{h \in H} V(h) = V(\mathrm{lcm}(H))$.

If we take G to be a reduced Gröbner basis, then $h \notin \langle F\rangle$ for any $h \in H$ since then the corresponding leading term would be divisible by a leading term in G. This is not allowed when G is reduced. Hence, we can find a Gröbner basis G_1 of $F \cup \{h\}$, which will then form a segment $(V(h) \setminus \bigcup_{h_1 \in H_1} V(h_1), G_1)$ where $H_1 = \{\mathrm{lc}_U(g) \mid g \in G_1\}$. Since $k[X, U]$ is Noetherian, this will eventually stop, forming a Gröbner system.

This gives us the ingredients for a simple algorithm for computing Gröbner systems, given below:

Algorithm 1: $\texttt{CGS}_{\texttt{simple}}$, an algorithm for computing comprehensive Gröbner systems on $V(E)$

INPUT: Two finite sets $F \subset k[X,U]$, $E \subset k[U]$

OUTPUT: A finite set of triples (A,N,G), each forming a segment of a comprehensive Gröbner system on $V(E)$.

if $\exists g \in E \cap (k \setminus \{0\})$ **then**
  return $\emptyset$;
else
  $G \leftarrow$ **groebner**(F);
  $H \leftarrow \{\mathrm{lc}_U(g) \mid g \in G \setminus k[U]\}$;
  $h \leftarrow \mathrm{lcm}(H)$;
  if $h = 1$ **then**
    return $\{(E,\{h\},F)\}$;
  else
    return $\{(E,\{h\},G)\} \cup \bigcup_{h' \in H} \texttt{CGS}_{\texttt{simple}}(G \cup \{h'\}, E \cup \{h'\})$
  end
end

However, this algorithm has a crucial law: if (E,N,G) is a triple returned by $\texttt{CGS}_{\texttt{simple}}$, then we don't necesarily have $G \subset \langle F \rangle$. This may or may not be a problem depending on the application. For some of the applications of this project, this is indeed a flaw. To fix this, we present an alternative algorithm, which will be extended to produce Gröbner segments, which are properly contained in $\langle F \rangle$. This algorithm depends on the following proposition.

2.8 · Proposition. *Let $F \subset k[X,U]$ and $S \subset k[U]$ be finite sets of polynomials and let G be the reduced Gröbner basis of $\langle F \cup S \rangle$. Then $(V(G \cap k[U]) \setminus V(h), G \setminus k[U])$ is a segment of a Gröbner system for both $\langle F \cup S \rangle$ and $\langle F \rangle$, where $h = \mathrm{lcm}\{\mathrm{lc}_U(g) \mid g \in G \setminus k[U]\}$.*

Proof. Let $h = \mathrm{lcm}\{\mathrm{lc}_U(g) \mid g \in G \setminus k[U]\}$ and let $\alpha \in V(G \cap k[U]) \setminus V(h)$. Since $X^{\nu_1} > U^{\nu_2}$, we have that $\langle G \cap k[U] \rangle = \langle F \cup S \rangle \cap k[U]$. Thus we can assume w.l.o.g. that $S = G \cap k[U]$.

Since $\alpha \notin V(h) = \bigcup_{g \in G \setminus k[U]} V(\mathrm{lc}_U(g))$, we have that $\sigma_\alpha(\mathrm{lc}_U(g)) \neq 0$ for each $g \in G \setminus k[U]$. Thus $\sigma_\alpha(G)$ is a Gröbner basis of $\langle \sigma_\alpha(F \cup S) \rangle$ by lemma ??.

Finally, since $\alpha \in V(G \cap k[U])$, we have that $\sigma_\alpha(G) = \sigma_\alpha(G \setminus k[U]) \cup \{0\}$, and since $S = G \cap k[U]$, we have $\sigma_\alpha(F \cup S) = \sigma_\alpha(F) \cup \{0\}$. Thus $\sigma_\alpha(G) = \sigma_\alpha(G \setminus k[U]) \cup \{0\}$ is a Gröbner basis of both $\langle \sigma_\alpha(F) \rangle$ and $\langle \sigma_\alpha(F \cup S) \rangle$. □

Armed with this proposition, we can compute Gröbner segments like this: we simply add leading terms to F until $\langle F \cup S \rangle = k[X,U]$ and compute the segment $(V(G \cup k[U]) \setminus V(h), G \setminus k[U])$ at every step along the way. This algorithm is a variation on the algorithm presented in [2].

Algorithm 2: $\mathrm{CGS}_{\mathrm{aux}}$, an auxiliary algorithm for computing Gröbner systems

INPUT: A finite set $F \subset k[X,U]$
OUTPUT: A finite set of tuples (h,G)
$G \leftarrow$ **groebner**(F);
$H \leftarrow \{\mathrm{lc}_U(g) \mid g \in G \setminus k[U]\}$;
$h \leftarrow \mathrm{lcm}(H)$;
if $h = 1$ **then**
    return $\{(h,G)\}$;
else
    return $\{(h,G)\} \cup \bigcup_{h' \in H} \mathrm{CGS}_{\mathrm{aux}}(G \cup \{h'\})$;
end

2.9 · Lemma. *Assume that $F \subset k[X,U]$ is a Gröbner basis, and let $\mathscr{H}$ be the result of $\mathrm{CGS}_{\mathrm{aux}}(F)$. If $(h,G) \in \mathscr{H}$, then $(V(G \cap k[U]) \setminus V(h), G \setminus k[U])$ is a Gröbner system. Furthermore,*

$$\{(V(G \cap k[U]) \setminus V(h), G \setminus k[U]) \mid (h,G) \in \mathscr{H}\}$$

is a comprehensive Gröbner system on $V(\langle F \rangle \cap k[U])$.

Proof. We first prove that $\mathrm{CGS}_{\mathrm{aux}}$ terminates on every input. Let F be the input to $\mathrm{CGS}_{\mathrm{aux}}$, let G be the reduced Gröbner basis of $\langle F \rangle$, and let $H = \{\mathrm{lc}_U(g) \mid g \in G \setminus k[U]\}$. Since G is reduced, $h \notin \langle F \rangle$ since then its leading term would be divisible by an element in G, but that is not the case. Indeed, since $h \in k[U]$, it cannot be reduced by any $g \in G \setminus k[U]$ (as $X^{\nu_1} > U^{\nu_2}$, so the leading terms of $G \setminus k[U]$ must contain a variable from X), and if it was reducible by a $p \in G \cap k[U]$, then that p would also reduce one of the elements of $G \setminus k[U]$. Thus $\langle F \rangle \subsetneq \langle F \cup h \rangle$. Since this is the case at every recursive call, the each successive call to $\mathrm{CGS}_{\mathrm{aux}}$ will have a strictly greater ideal. Since $k[X,U]$ is Noetherian, this must stop eventually.

Next, we prove that if $(h,G) \in \mathscr{H}$, then $(V(G \cap k[U]) \setminus V(h), G \setminus k[U])$ is a segment of a Gröbner system. If we let F be the original input to $\mathrm{CGS}_{\mathrm{aux}}$, then each such G is the reduced Gröbner basis of $\langle F \cup S \rangle$ where $S \subset k[U]$ is the set of recursively added leading coefficients. By proposition **??** $(V(G \cap k[U]) \setminus V(h), G \setminus k[U])$ is a segment of a Gröbner system.

Finally, we prove that $\bigcup_{(h,G) \in \mathscr{H}} V(G \cap k[U]) \setminus V(h) = V(\langle F \rangle \cap k[U])$. Note, that since $V(\mathrm{lcm}(H)) = \bigcup_{h \in H} V(h)$, we have the following:

$$\begin{aligned} V(\langle G \cap k[U] \rangle) &= (V(\langle G \cap k[U] \rangle) \setminus V(\mathrm{lcm}(H))) \cup \bigcup_{h \in H} V(h) \\ &= (V(\langle G \cap k[U] \rangle) \setminus V(\mathrm{lcm}(H))) \cup \bigcup_{h \in H} V(\langle G \cup \{h\} \rangle \cap k[U]). \end{aligned}$$

By induction, the recursive calls to $\mathrm{CGS}_{\mathrm{aux}}$ will compute Gröbner segments covering $\bigcup_{h \in H} V(\langle G \cup \{h\} \rangle \cap k[U])$. Jeg skal finde ud af hvordan jeg vil håndtere base-casen. Mit bud lige nu er, at er

Eller måske skal man kun bruge $k[U]\setminus k$, så konstanter bliver der. Der er nogle problemer med de der konstanter. $\square$

Finally, we can use the result of this lemma to compute a comprehensive Gröbner system.

Algorithm 3: CGS, an algorithm for computing a comprehensive Gröbner system

INPUT: $F \subset k[X, U]$ a finite set of polynomials

OUTPUT: A finite set of triples (E, N, G) forming a comprehensive Gröbner system

$\mathscr{H} \leftarrow \mathrm{CGS}_{\mathrm{aux}}(\mathrm{F})$;

$G_0 \leftarrow$ **groebner**(F);

$GS \leftarrow \emptyset$;

if $\exists g \in G_0 \cap k[U]$ **then**

  $GS \leftarrow \{(\emptyset, G_0 \cap k[U], \{1\})\}$;

end

for $(h, G) \in \mathscr{H}$ **do**

  $GS \leftarrow GS \cup \{(G \cap k[U], \{h\}, G \setminus k[U])\}$;

end

return GS;

Note that if $G \cap k[U] \neq \emptyset$, then $\{1\}$ is a Gröbner basis on $k_1^{|U|} \setminus V(G \cap k[U])$. Thus the algorithm computes a comprehensive Gröbner system.

3 Parametric Gröbner bases

We now move on to the problem of computing parametric Gröbner bases, which is the problem which Weispfenning tackled in his original article [3]. Recall the definition of parametric Gröbner bases from definition **??**

3.1 · Definition (Faithful Gröbner system). A Gröbner system $\{(A_1, G_1), \ldots, (A_t, G_t)\}$ of an ideal $\langle F \rangle$ is called *faithful* if $G_i \subset \langle F \rangle$ for all i.

3.2 · Corollary. *Let $\mathscr{G} = \{(A_1, G_1), \ldots, (A_t, G_t)\}$ be a comprehensive, faithful Gröbner system of an ideal $\langle F \rangle$. Then $\bigcup_{(A,G)\in\mathscr{G}} G$ is a parametric Gröbner basis.*

Proof. Let σ_α be a specialization. Since $\mathscr{G}$ was comprehensive, there is some l such that $\alpha \in A_l$. Then $\sigma_\alpha(G_l)$ is a Gröbner basis of $\langle \sigma_\alpha(F) \rangle$, so $\langle \mathrm{lt}(\sigma_\alpha(G_l)) \rangle = \langle \mathrm{lt}(\sigma_\alpha(\langle F \rangle)) \rangle$. Since for all i we have that $\langle \sigma_\alpha(G_i) \rangle \subset \langle \sigma_\alpha(F) \rangle$, we have that $\langle \mathrm{lt}(\sigma_\alpha(G_i)) \rangle = \langle \mathrm{lt}(\sigma_\alpha(\langle F \rangle)) \rangle$, so $\sum_{i=1}^{t} \langle \mathrm{lt}(\sigma_\alpha(G_i)) \rangle = \langle \sigma_\alpha(F) \rangle$, thus $\sigma_\alpha\left(\bigcup_{(A,G)\in\mathscr{G}} G\right)$ is a Gröbner basis for $\langle \sigma_\alpha(F) \rangle$. $\square$

The path to computing parametric Gröbner bases seem clear. We simply need to modify the segments of a comprehensive Gröbner system to be faithful, then we're done. While this is surpisingly easy to implement, proving that the way we do it works is a little more cumbersome.

We follow the path laid out by [2], and introduce a new variable t and extend the monomial order such that $t^n > X^{v_1} > U^{v_2}$ for all $n \in \mathbb{N}$ and vectors v_1, v_2. In the CGS algorithm we added leading coefficients h to a set $S \subset k[U]$, and computed reduced Gröbner bases of $\langle F \cup S \rangle$ to produce the segments. However, this "mixes up" the original ideal with the added leading coefficients. We need a way to seperate them. We do this by replacing $F \cup S$ with $t \cdot F \cup (1-t) \cdot S$. Here we use the convention, that for a polynomial a and a set of polynomials F, $a \cdot F := \{a \cdot f \mid f \in F\}$.

In this way we can seperate the original ideal from the added polynomials by specializing away t. That is the content of this first lemma.

3.3 · Lemma. *Let $F, S \subset k[X,U]$ be finite sets and let $g \in \langle t \cdot F \cup (1-t) \cdot S \rangle_{k[t,X,U]}$. Then $g(0,X,U) \in \langle S \rangle_{k[X,U]}$ and $g(1,X,U) \in \langle F \rangle_{k[X,U]}$.*

Proof. By assumption, we can find $f_1, \dots, f_n \in F$, $s_1, \dots, s_m \in S$ and $q_1, \dots, q_n, p_1, \dots, p_m \in k[t,X,U]$ such that

$$g = \sum_{i=1}^{n} t\, q_i\, f_i + \sum_{j=1}^{m} (t-1) p_j\, s_j.$$

By linearity of the evaluation map, we get that

$$g(0,X,U) = \sum_{j=1}^{m} p_j(0,X,U)\, s_j(X,U) \in \langle S \rangle_{k[X,U]}$$

and

$$g(1,X,U) = \sum_{i=1}^{n} q_i(1,X,U)\, f_i(X,U) \in \langle F \rangle_{k[X,U]}.$$

We're going to need these two specializations a lot, so we'll give them names. Let $\sigma^0(f) = f(0,X,U)$ and $\sigma^1(f) = f(1,X,U)$. We also need that Gröbner bases are preserved under σ^1. While that is not true in general, the following is good enough for our uses.

3.4 · Lemma. *Let $F \subset k[X,U]$, $S \subset k[U]$ be finite sets with $V(S) \subset V(\langle F \rangle \cap k[U])$ and let G be the reduced Gröbner basis of $\langle t \cdot F \cup (1-t) \cdot S \rangle$. Let also*

$$H = \{\mathrm{lc}_U(g) \mid g \in G,\ \mathrm{lt}(g) \notin k[X,U],\ \mathrm{lc}_{X,U}(g) \notin k[U]\}.$$

Then $\sigma_\alpha(\sigma^1(G))$ is a Gröbner basis of $\langle \sigma_\alpha(F) \rangle$ for any $\alpha \in V(S) \setminus V(\mathrm{lcm}(H))$.

Proof. First note, that $\mathrm{lt}(g) \notin k[X,U]$ means that the leading term of g contains the variable t and since t dominates the other variables, this means that $g \in k[t,X,U] \setminus k[X,U]$. Also, any polynomial in G has degree at most 1 in t, again since t dominates the other variables. For any polynomial $g \in G$ we can therefor write $g = t\, g^t + g_t$ where $g_t = \sigma^0(g)$ and $g^t = \sigma^1(g) - \sigma^0(g)$.

References

[1] Michael Kalkbrener. ?On the Stability of Gröbner Bases Under Specializations? **in** *Journal of Symbolic Computation*: 24.1 (1997), **pages** 51–58. ISSN: 0747-7171. DOI: https://doi.org/10.1006/jsco.1997.0113. URL: https://www.sciencedirect.com/science/article/pii/S0747717197901139.

[2] Akira Suzuki **and** Yosuke Sato. ?A simple algorithm to compute comprehensive Gröbner bases using Gröbner bases? English. **in** Proceedings of the International Symposium on Symbolic and Algebraic Computation, ISSAC: Association for Computing Machinery (ACM), 2006, **pages** 326–331. ISBN: 1595932763. DOI: 10.1145/1145768.1145821.

[3] Volker Weispfenning. ?Comprehensive Gröbner bases? **in** *Journal of Symbolic Computation*: 14.1 (1992), **pages** 1–29. ISSN: 0747-7171. DOI: https://doi.org/10.1016/0747-7171(92)90023-W. URL: https://www.sciencedirect.com/science/article/pii/074771719290023W.