On the existence of order functions

Ruud Pellikaan *

Appeared in:

Abstract
The notions of well-behaving sequences and order functions is fundamental in
the elementary treatment of geometric Goppa codes. The existence of order
functions is proved with the theory of Gröbner bases.

Keywords: Geometric Goppa codes, algebraic geometry codes, Gröbner bases,
order function, weight function, discrete valuation.

AMS classification: 94B25

1 Introduction

In the papers [5, 6, 7, 11, 12] a method is given to treat geometric Goppa
codes without algebraic geometry, that is to say that the parameters \([n, k, d]\)
and the decoding of these codes up to half the (designed) minimum distance
can be done without the theory of algebraic curves over finite fields [25], or
equivalently the theory of function fields of one variable over finite fields [24],
in particular without the theorem of Riemann-Roch. In their treatment the
notion of a well-behaving sequence is fundamental. In this paper a method is
given to prove the existence of well-behaving sequences or, in the terminology
of this paper, the existence of order or weight functions using the theory of
Gröbner bases [1, 2].

*Department of Mathematics and Computing Science, Technical University of Eind-
hoven, P.O. Box 513, 5600 MB Eindhoven, The Netherlands.
Let $\mathcal{X}$ be an algebraic curve defined over the finite field $\mathbb{F}_q$. The genus of the curve $\mathcal{X}$ is denoted by $g$. The function field of rational functions on $\mathcal{X}$ that are defined over $\mathbb{F}_q$ is denoted by $\mathbb{F}_q(\mathcal{X})$. The principal divisor of a nonzero rational function $f$ is denoted by $(f)$. Let $P_1, \ldots, P_n$ be $n$ distinct rational points of $\mathcal{X}$. Let $D = P_1 + \cdots + P_n$. Let $G$ be a divisor which has disjoint support with the support of $D$. The vector space $L(G)$ is defined by

$$L(G) = \{ f \in \mathbb{F}_q(\mathcal{X}) | f = 0 \text{ or } (f) \geq -G \}.$$ 

The index of speciality $i(G)$ of a divisor $G$ is a nonnegative integer which is zero if $\deg(G) > 2g - 2$. Then

$$\dim(L(G)) = \deg(G) + 1 - g + i(G),$$

by the Theorem of Riemann-Roch. Consider the evaluation map

$$ev : L(G) \longrightarrow \mathbb{F}_q^n$$

defined by $ev(f) = (f(P_1), \ldots, f(P_n))$. The code $C_L(D, G)$ is by definition the image of $L(G)$ under this evaluation map. The dual $C_\Omega(D, G)$ of the code $C_L(D, G)$ can also be defined by a residue map of differential forms. Both these codes have the property that

$$k + d \geq n + 1 - g,$$

where $k$ is the dimension and $d$ is the minimum distance of the code.

If $P$ is a rational point of $\mathcal{X}$ that is not in the support of $D$, and $G = mP$, then $C_L(D, G)$ is called a one point geometric Goppa code. For a fixed $P$ two sequences of codes $(C_L(D, mP)|m \in \mathbb{N}_0)$ and $(C_\Omega(D, mP)|m \in \mathbb{N}_0)$ are obtained. The nonnegative integer $m$ is called a (Weierstrass) gap at $P$ if $L(mP) = L((m - 1)P)$ and a nongap otherwise. The integer $m$ is a nongap if and only if there exists a rational function $f$ with poles only at $P$ and pole order $m$. So 0 is a nongap and the sum of two nongaps is again a nongap. Hence the nongaps form a (numerical) semigroup. The number of gaps is equal to the genus $g$, and the largest gap is at most $2g - 1$. Let $(\rho_l|l \in \mathbb{N})$ be the sequence of nongaps in increasing order. Then $\rho_l = l + g - 1$ for all $l > g$.

The rational functions on $\mathcal{X}$ that have only a pole at $P$ form a ring $K_\infty(P)$ and the function

$$\rho : K_\infty(P) \rightarrow \mathbb{N}_0 \cup \{-\infty\},$$
where $\rho(f) = -v_P(f)$ and $v_P$ is the discrete valuation at $P$, will be the prime example of a weight function in the terminology of this paper. The map $\rho$ was denoted by $\deg$ in [21]. The image of the map $\rho$ is exactly the set of nongaps at $P$ and for every $l$ there exists a function $f_l \in K_\infty(P)$ such that $\rho(f_l) = \rho_l$. In this way a basis $(f_l| l \in \mathbb{N})$ of $K_\infty(P)$ over $\mathbb{F}_q$ is obtained. Let $L(l)$ be the vector space generated by $f_1, \ldots, f_l$, or equivalently $L(l) = \{ f \in K_\infty(P) | \rho(f) \leq \rho_l \}$. Let $l(i,j)$ be the smallest positive integer $l$ such that $f_i f_j \in L(l)$. Then the function $l(i,j)$ is strictly increasing in both arguments, since

$$\rho_i + \rho_j = \rho_{l(i,j)}$$

and $\rho_i$ is strictly increasing with $i$.

The same can be done on the level of words in $\mathbb{F}_q^n$ after applying the evaluation map. Denote the coordinatewise multiplication of $a$ and $b$ in $\mathbb{F}_q^n$ by $a \ast b$. So $a \ast b = (a_1 b_1, \ldots, a_n b_n)$. Then $\mathbb{F}_q^n$ becomes an $\mathbb{F}_q$-algebra. The evaluation map can be extended to a map

$$ev : K_\infty(P) \longrightarrow \mathbb{F}_q^n.$$ 

Notice that $ev(fg) = ev(f) \ast ev(g)$, so this map $ev$ is a morphism of $\mathbb{F}_q$-algebras. Let $f_l = ev(f_l)$. The basis $h_1, \ldots, h_n$ is obtained from this sequence by deleting superfluous elements as follows. The vector $h_1$ is the first nonzero element of the sequence $(f_l| l \in \mathbb{N})$. Suppose that $h_1, \ldots, h_{l+1}$ are defined for $l < n$, then $h_{l+1}$ is the first element of the sequence $(f_l| l \in \mathbb{N})$ which is not in the vector space generated by $h_1, \ldots, h_l$. The evaluation map is surjective, so the finite sequence $(f_l| l \in \mathbb{N})$ generates $\mathbb{F}_q^n$ as a vector space. Therefore indeed a basis $h_1, \ldots, h_n$ is obtained.

Let $S(l)$ be the vector space generated by $h_1, \ldots, h_l$. Let $\phi(i,j)$ be the the smallest positive integer such that $h_i \ast h_j \in S(l)$. The function $\phi(i,j)$ is strictly increasing for many values but not for all values of $i, j$. Well-behaving sequences in $\mathbb{F}_q^n$ are introduced in terms of the function $\phi(i,j)$ being increasing for certain values of $i$ and $j$ [5, 6]. In this paper the distinction between functions and words is emphasized and the notion of well-behaving is studied on the level of functions.

Now a more abstract point of view is taken. Let $R$ be an $\mathbb{F}_q$-algebra $R$, that is to say a commutative ring with a unit that has $\mathbb{F}_q$ as a unitary subring. Suppose that $R$ has a basis consisting of a well-behaving sequence together
with a surjective morphism \( \varphi : R \rightarrow \mathbb{F}_q^n \) of \( \mathbb{F}_q \)-algebras. In the following section a sketch will be given how this gives rise to a sequence of codes \( C(l) \) and a bound on the minimum distance of these codes following the ideas of [5, 6, 7, 11, 12, 13, 19, 20, 22, 23]. This was generalized to a bound on the generalized Hamming weights by [10].

In Section 3 the notion of an order function is defined. It is shown that the \( \mathbb{F} \)-algebra \( R \) has a basis consisting of a well-behaving sequence if and only if \( R \) has an order function. If \( R \) has an order function, then it is an integral domain. A stronger notion than an order function is a weight function. If \( R \) has a weight function, then the values of the weight function form a semigroup, and the bounds on the minimum distance of the codes \( C(l) \) can be formulated in terms of parameters of this semigroup. See [13].

What remains is to show the existence of well-behaving sequences in an elementary way. This is done in Sections 4 and 5.

## 2 A bound on the minimum distance

Let \( \mathbb{F} \) be a field. Let \( R \) be an \( \mathbb{F} \)-algebra. In this paper it is assumed that

\[
\varphi : R \longrightarrow \mathbb{F}_q^n,
\]

is a surjective morphism of \( \mathbb{F} \)-algebras.

**Example 2.1** **Affine \( \mathbb{F} \)-algebras.** Let the set \( \mathcal{P} \) consist of \( n \) distinct points \( P_1, \ldots, P_n \) in \( \mathbb{F}^m \), the affine space over \( \mathbb{F} \) of dimension \( m \). Consider the evaluation map

\[
ev_P : \mathbb{F}[X_1, \ldots, X_m] \longrightarrow \mathbb{F}^n,
\]

defined by \( ev_P(f) = (f(P_1), \ldots, f(P_n)) \). This is a morphism of \( \mathbb{F} \)-algebras from \( \mathbb{F}[X_1, \ldots, X_m] \) to \( \mathbb{F}^n \), since \( fg(P_i) = f(P_i)g(P_i) \) for all polynomials \( f \) and \( g \), and all \( i \). The map \( ev_P \) is surjective [3, 10].

Suppose that \( I \) is an ideal in the ring \( \mathbb{F}[X_1, \ldots, X_m] \). Let \( \mathcal{P} = \{P_1, \ldots, P_n\} \) be in the zerset of \( I \) with coordinates in \( \mathbb{F} \). So \( f(P_j) = 0 \) for all \( f \in I \) and all \( j = 1, \ldots, n \). Then the evaluation map induces a well-defined linear map

\[
ev_P : \mathbb{F}[X_1, \ldots, X_m]/I \longrightarrow \mathbb{F}^n,
\]

which is also a surjective morphism of \( \mathbb{F} \)-algebras.
Definition 2.2 Let \( (f_i|i \in \mathbb{N}) \) be a basis of \( R \) over \( F \). Let \( L(l) \) be the vector space generated by \( f_1, \ldots, f_l \). So for all \( f \in R \) there exists a positive integer \( l \in \mathbb{N}_0 \) such that \( f \in L(l) \). Let \( l(i, j) \) be the smallest nonnegative integer \( l \) such that \( f_i f_j \in L(l) \).

The sequence \( (f_i|i \in \mathbb{N}) \) is called well-behaving if \( l(i, j) \) is strictly increasing in both arguments, that is to say

\[
l(i, j) < l(i + 1, j)
\]

for all \( i, j \in \mathbb{N} \), by symmetry. See [5, 6], and [13, 19] for the similar notion of an error-correcting array.

Remark 2.3 The associativity of the triple product \( f_i f_j f_k \) implies the associativity of \( l(i, j) \), that is to say \( l(i, l(j, k)) = l(l(i, j), k) \).

Remark 2.4 If \( (f_i|i \in \mathbb{N}) \) is a well-behaving sequence, then \( l(i, j) \) is not zero for all \( i, j \in \mathbb{N} \). Because, if \( l(i, j) = 0 \) for \( i > 1 \), then \( 0 \leq l(i - 1, j) < l(i, j) = 0 \) which is a contradiction. By symmetry it is not possible that \( l(i, j) = 0 \) for \( j > 1 \). Suppose that \( l(1, 1) = 0 \). Then \( f_1 f_1 = 0 \), so \( f_1 f_1 f_3 = 0 \). So \( l(1, l(1, 3)) = 0 \). But if \( j = l(1, 3) \), then \( j > l(1, 2) > 0 \). So \( l(1, l(1, 3)) = l(1, j) > 0 \), which is a contradiction.

Definition 2.5 Let \( F = \mathbb{F}_q \). Let \( f_i = \varphi(f_i) \). Define the evaluation code \( E(l) \) and its dual \( C(l) \) by

\[
E(l) = \varphi(L(l)) = \langle f_1, \ldots, f_l \rangle,
C(l) = \{ c \in \mathbb{F}_q^n \mid c \cdot f_i = 0 \text{ for all } i \leq l \}.
\]

Definition 2.6 Define

\[
N(l) = \{ (i, j) \in \mathbb{N}^2 \mid l(i, j) = l + 1 \}.
\]

Let \( \nu(l) \) be the number of elements of \( N(l) \).

Proposition 2.7 If \( y \in C(l) \setminus C(l + 1) \), then \( \text{wt}(y) \geq \nu(l) \).

Proof. See [5, 6, 7, 10, 11, 12, 13, 19, 20, 22, 23].
Definition 2.8
\[ d_{\text{ORD}}(l) = \min\{\nu(l') \mid l' \geq l\}, \]
\[ d_{\text{ORD},\varphi}(l) = \min\{\nu(l') \mid l' \geq l, C(l') \neq C(l' + 1)\}, \]
If \( R \) is an affine algebra of the form \( \mathbb{F}[X_1, \ldots, X_m]/I \) and \( \varphi \) is the evaluation map \( ev_{\mathcal{P}} \) of the set \( \mathcal{P} \) of \( n \) points in \( \mathbb{F}^m \), then \( d_{\text{ORD},\varphi} \) is denoted by \( d_{\text{ORD},\mathcal{P}} \).

**Theorem 2.9** The numbers \( d_{\text{ORD}}(l) \) and \( d_{\text{ORD},\varphi}(l) \) are lower bounds for the minimum distance of \( C(l) \):
\[ d(C(l)) \geq d_{\text{ORD},\varphi}(l) \geq d_{\text{ORD}}(l). \]

**Proof.** The theorem is a direct consequence of Definition 2.8 and Proposition 2.7.

**Remark 2.10** The notation \( d_{\text{ORD}} \) refers to the order function associated to the well-behaving sequence as will be done in the next section. This bound was called the Feng-Rao bound in [13] and denoted by \( d_{\text{FR}} \).

The set \( N(l) \) and the numbers \( \nu(l) \) and \( d_{\text{ORD}} \) do not depend on the map \( \varphi \), or in case \( R \) is an affine algebra and \( \varphi \) is the evaluation map \( ev_{\mathcal{P}} \), on the choice of the set \( \mathcal{P} \).

If \( \mathcal{P} \subseteq \mathcal{P}' \), then \( d_{\text{ORD,}\mathcal{P}} \geq d_{\text{ORD,}\mathcal{P}'} \). So, the number \( d_{\text{ORD,}\mathcal{P}} \) depends on the choice of the set of points. Hence in many examples an improvement of the order bound \( d_{\text{ORD}} \) is obtained. In particular for the Reed-Muller codes the bound \( d_{\text{ORD}} \) is very weak whereas \( d_{\text{ORD,}\mathcal{P}} \) is tight. See [10, 11, 12].

**Example 2.11** Let \( R = \mathbb{F}_q[X] \). Let \( f_i = X^{i-1} \). Then \( (f_i \mid i \in \mathbb{N}) \) is a well-behaving sequence of \( R \) and \( l(i, j) = i + j - 1 \). Let \( \alpha \) be a primitive element of \( \mathbb{F}_q \). Let \( n = q - 1 \). Let \( \varphi : R \to \mathbb{F}_q^n \) be the evaluation map defined by \( \varphi(f) = (f(\alpha^0), f(\alpha^1), \ldots, f(\alpha^{n-1})) \). Then \( C(l) \) is a Reed-Solomon code. The sequence \( \alpha^0, \alpha^1, \ldots, \alpha^{l-1} \) is a defining set of the cyclic code \( C(l) \) and \( d_{\text{ORD}}(l) = l + 1 \) is the BCH bound.

**Example 2.12** Let \( I \) be the ideal in \( \mathbb{F}[X, Y] \) generated by \( X^3 + Y^2 + Y \).

Let \( R = \mathbb{F}[X, Y]/(X^3 + Y^2 + Y) \). Let \( f_1 = 1, f_{2i} = X^i \) and \( f_{2i+1} = X^{i-1}Y \) for \( i \in \mathbb{N} \). Then \( (f_i \mid i \in \mathbb{N}) \) is a well-behaving sequence of \( R \), and \( l(1, 1) = 1, l(1, 2) = l(2, 1) = 2 \) and \( l(i, j) = i + j \) for all \( i, j > 1 \). Furthermore \( \nu(1) = 2 \) and \( \nu(l) = l \) for all \( l > 1 \). So \( d_{\text{ORD}}(l) = \nu(l) \).
Remark 2.13 It is possible to give a version of these ideas on the level of words in $F_n^q$ without any reference to the functions. See [5, 6, 11, 12, 13, 19, 20, 22, 23]. Let $h_1, \ldots, h_n$ be a basis of $F_n^q$. Let $S(l)$ be the vector space generated by $h_1, \ldots, h_l$. Let $C_r$ be the dual of the code $S(r)$. Let $\phi(i, j)$ be the smallest positive integer such that $h_i \ast h_j \in S(l)$. The pair $(i, j)$ is called well-behaving if $\phi(i', j') < \phi(i, j)$ for all $i', j'$ such that $i' \leq i, j' \leq j$ and $(i', j') \neq (i, j)$. Define

$$N_{WB}(l) = \{(i, j) | \phi(i, j) = l + 1 \text{ and } (i, j) \text{ is well-behaving}\}.$$  

Let $\nu_{WB}(l)$ be the number of elements of $N_{WB}(l)$. Define

$$d_{WB}(r) = \min \{|\nu_{WB}(r')| r \leq r' < n\}.$$  

Then $d_{WB}(r)$ is a lower bound on the minimum distance of $C_r$.

Let the basis $h_1, \ldots, h_n$ be obtained by deleting superfluous elements of the sequence $(f_l | l \in \mathbb{N})$, where $(f_l | l \in \mathbb{N})$ is a well-behaving sequence of an $F_q$-algebra $R$ with surjective map $\varphi$ and $f_l = \varphi(f_l)$. If the dimension of $C(l)$ is $k$, $r = n - k$ and $C(l) \neq C(l + 1)$, then $d_{WB}(r) \geq d_{ORD, \varphi}(l)$.

3 Order, degree and weight functions

Consider the following definitions from [10, 11, 12].

Definition 3.1 An order function on an $F$-algebra $R$ is a function

$$\rho : R \rightarrow \mathbb{N}_0 \cup \{-\infty\},$$

such that the following conditions hold

(O.0) $\rho(f) = -\infty$ if and only if $f = 0$
(O.1) $\rho(\lambda f) = \rho(f)$ for all nonzero $\lambda \in F$
(O.2) $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$
and equality holds when $\rho(f) < \rho(g)$.
(O.3) If $\rho(f) < \rho(g)$ and $h \neq 0$, then $\rho(fh) < \rho(gh)$
(O.4) If $\rho(f) = \rho(g)$, then there exists a nonzero $\lambda \in F$ such that $\rho(f - \lambda g) < \rho(g)$.

for all $f, g, h \in R$. Here $-\infty < n$ for all $n \in \mathbb{N}_0$.  

Definition 3.2 Let $R$ be an $F$-algebra. A weight function on $R$ is an order function on $R$ that satisfies furthermore

\[(O.5)\quad \rho(fg) = \rho(f) + \rho(g)\]

for all $f, g \in R$. Here $-\infty + n = -\infty$ for all $n \in \mathbb{N}_0$.

If $\rho$ is a weight function and $\rho(f)$ is divisible by an integer $d > 1$ for all $f \in R$, then $\rho(f)/d$ is again a weight function. Hence we may assume that the greatest common divisor of the integers $\rho(f)$ with $0 \neq f \in R$ is 1.

Definition 3.3 A degree function on $R$ is a map that satisfies conditions $(O.0)$, $(O.1)$, $(O.2)$ and $(O.5)$.

It is clear that condition $(O.3)$ is a consequence of $(O.5)$.

Example 3.4 The standard example of an $F$-algebra $R$ with a degree function $\rho$ is obtained by taking $R = F[X_1, \ldots, X_m]$ and $\rho(f) = \deg(f)$, the degree of $f \in R$. It is a weight function if and only if $m = 1$.

Theorem 3.5 Let $R$ be an $F$-algebra. Let $(f_i| i \in \mathbb{N})$ be a well-behaving sequence of $R$. Let $(\rho_i| i \in \mathbb{N})$ be a strictly increasing sequence of nonnegative integers. Define $\rho(0) = -\infty$, and $\rho(f) = \rho_i$ if $l$ is the smallest positive integer such that $f \in L_l$ for a nonzero $f \in R$. Then $\rho$ is an order function on $R$. If moreover $\rho_{\iota(fg)} = \rho_i + \rho_j$, then $\rho$ is a weight function.

Proof. Conditions $(O.0)$, $(O.1)$, $(O.2)$ and $(O.4)$ are a direct consequence of the definitions.

With every nonzero element $f \in R$ the unique positive integer $\iota(f)$ is associated such that $f \in L(\iota(f))$ and $f \not\in L(\iota(f) - 1)$. So $\rho(f) = \rho_{\iota(f)}$.

Let $f$ and $g$ be nonzero elements of $R$. Then

$$f = \sum_{i \leq \iota(f)} \lambda_i f_i, \quad g = \sum_{j \leq \iota(g)} \nu_j f_j \quad \text{and} \quad fg = \sum_{l \leq \iota(fg)} \mu_l f_l,$$

with $\lambda_{\iota(f)} \neq 0$, $\nu_{\iota(g)} \neq 0$ and $\mu_{\iota(fg)} \neq 0$. There exist $\mu_{ij} \in F$ such that

$$f_i f_j = \sum_{l \leq \iota(i,j)} \mu_{ij} f_l$$
and $\mu_{ijl(i,j)} \neq 0$, by definition of $l(i, j)$. So

$$
\mu_l = \sum_{l(i,j)=l} \lambda_i \nu_j \mu_{ijl}.
$$

The function $l(i, j)$ is strictly increasing in both arguments, by assumption. So $l(i, j) < l(\nu(f), \nu(g))$ if $i < \nu(f)$ or $j < \nu(g)$. Furthermore, if $i = \nu(f)$ and $j = \nu(g)$, then

$$
\lambda_i \nu_j \mu_{ijl(i,j)} \neq 0.
$$

This element is therefore equal to $\mu_{\nu(fg)}$. So $\nu(fg) = l(\nu(f), \nu(g))$. Hence $\rho(fg) = \rho(\nu(f), \nu(g))$ and (O.3) holds, since $l(i, j)$ is strictly increasing. Therefore $\rho$ is an order function.

If moreover $\rho_{i(j,i)} = \rho_i + \rho_j$, then

$$
\rho(fg) = \rho(\nu(fg)) = \rho(\nu(f), \nu(g)) = \rho(f) + \rho(g).
$$

Therefore $\rho$ is a weight function.  \qed

**Lemma 3.6** Let $\rho$ be an order function on $R$. Then:

1) If $\rho(f) = \rho(g)$, then $\rho(fh) = \rho(gh)$ for all $h \in R$.

2) $\rho(1) \leq \rho(f)$ for all nonzero elements $f \in R$.

3) $\mathbb{F} = \{f \in R \mid \rho(f) \leq \rho(1)\}$.

4) If $\rho(f) = \rho(g)$, then there exists a unique nonzero $\lambda \in \mathbb{F}$ such that $\rho(f - \lambda g) < \rho(g)$

**Proof.**

1) If $\rho(f) = \rho(g)$, then there exists a nonzero $\lambda \in \mathbb{F}$ such that $\rho(f - \lambda g) < \rho(g)$, by (O.4). So $\rho(fh - \lambda gh) < \rho(gh)$, by (O.3). Now $fh = (fh - \lambda gh) + \lambda gh$. Hence $\rho(fh) = \rho(\lambda gh) = \rho(gh)$, by (O.2) and (O.1), respectively.

2) Suppose that $f$ is a nonzero element of $R$ such that $\rho(f) < \rho(1)$. Then $\rho(1) > \rho(f) > \rho(f^2) > \cdots$ is a strictly decreasing sequence, by (O.3), but this contradicts the fact that $\mathbb{N}_0 \cup \{-\infty\}$ is a well-order. Hence $\rho(1) \leq \rho(f)$ for all nonzero elements $f$ in $R$.

3) It is clear that $\mathbb{F}$ is a subset of $\{f \in R \mid \rho(f) \leq \rho(1)\}$, by (O.0) and (O.1) If $f$ is nonzero and $\rho(f) \leq \rho(1)$, then $\rho(f) = \rho(1)$, by 1). So there exists a nonzero $\lambda \in \mathbb{F}$ such that $\rho(f - \lambda) < \rho(1)$, by (O.4). Hence $f - \lambda = 0$ and $f \in \mathbb{F}$.

4) Let $\rho(f) = \rho(g)$. The existence of $\lambda$ is assured by (O.4). Suppose that $\rho(f - \lambda g) < \rho(f)$ and $\rho(f - \mu g) < \rho(f)$ for nonzero $\lambda, \mu \in \mathbb{F}$. Let
\[ u = f - \lambda g \quad \text{and} \quad v = f - \mu g. \] Then \((\mu - \lambda)f = \mu u - \lambda v.\) So \(\rho((\mu - \lambda)f) \leq \max\{\rho(u), \rho(v)\} < \rho(f)\) by (O.2). If \(\mu \neq \lambda\), then \(\rho((\mu - \lambda)f) = \rho(f)\), by (O.1), which is a contradiction. Hence \(\mu = \lambda\). \hfill \Box

**Proposition 3.7** If there exists an order function on \(R\), then \(R\) is an integral domain.

**Proof.** Suppose that \(fg = 0\) for some nonzero \(f, g \in R\). We may assume that \(\rho(f) \leq \rho(g)\). So \(\rho(f^2) \leq \rho(fg) = \rho(0) = -\infty\). So \(\rho(f^2) = -\infty, and f^2 = 0\). Now \(f \neq 0\), hence \(\rho(1) \leq \rho(f)\), by Lemma 3.6. So \(\rho(f) \leq \rho(f^2) = \rho(0) = -\infty\). Hence \(f = 0\), which is a contradiction. Therefore \(R\) has no zero divisors. \hfill \Box

**Example 3.8** The \(\mathbb{F}\)-algebra \(R = \mathbb{F}[X_1, X_2]/(X_1X_2 - 1)\) is an integral domain. Denote the coset of \(X_i\) modulo the ideal \((X_1X_2 - 1)\) by \(x_i\). If \(\rho\) is an order function on \(R\), then \(\rho(1) \leq \rho(x_1)\), so \(\rho(x_2) \leq \rho(x_1x_2) = \rho(1)\), hence \(\rho(x_2) = \rho(1)\) and in the same way we get \(\rho(x_1) = \rho(1)\). Therefore \(\rho(f) \leq \rho(1)\) for all \(f \in R\). Hence \(\mathbb{F} = R\) by Lemma 3.6, which is a contradiction since \(x_1 \notin \mathbb{F}\). So not every integral domain has an order function. \hfill \Box

**Proposition 3.9** Let \(R\) be an \(\mathbb{F}\) algebra with order function \(\rho\). Then there exists a well-behaving sequence \((f_i | i \in \mathbb{N})\) of \(R\).

**Proof.** Let \((\rho_i | i \in \mathbb{N})\) be the increasing sequence of all nonnegative integers that appear as the order \(\rho(f)\) of a nonzero element \(f \in R\). By definition there exists an \(f_i \in R\) such that \(\rho(f_i) = \rho_i\) for all \(i \in \mathbb{N}\). So \(\rho(f_i) < \rho(f_{i+1})\) for all \(i\), and for all nonzero \(f \in R\) there exists an \(i\) with \(\rho(f) = \rho(f_i)\), by definition. The fact that \(\{f_i | i \in \mathbb{N}\}\) is a basis is proved by induction and Lemma 3.6 (4). That the function \(l(i, j)\) is strictly increasing is a consequence of (O.3). \hfill \Box

**Remark 3.10** In a sense the theory of algebraic curves is reversed. In the classical way one first has to show, among other things, that the curve is irreducible, and than one computes a well-behaving sequence of the \(\mathbb{F}\)-algebra \(K_\infty(P)\). In the new approach one starts to show that an \(\mathbb{F}\)-algebra \(R\) has an order function, or equivalently a well-behaving sequence, and one gets as a consequence that \(R\) is an integral domain.
4 On the existence of order and weight functions

The notion of a well-behaving sequence is well known in the theory of Gröbner bases [1, 2].

**Definition 4.1** Let $R = \mathbb{F}[X_1, \ldots, X_m]$. Suppose that $\prec$ is a total order on the set of monomials in the variables $X_1, \ldots, X_m$ such that for all monomials $M_1, M_2$, and $M$ the following holds

(R.1) If $M \neq 1$, then $1 \prec M$,
(R.2) If $M_1 \prec M_2$, then $MM_1 \prec MM_2$.

Then $\prec$ is called a reduction, term or admissible order on the monomials.

The multi-index notation is used for monomials. That means $X^{\alpha} = \prod_{i=1}^{m} X_i^{\alpha_i}$ if $\alpha = (\alpha_1, \ldots, \alpha_m)$. The degree of a monomial and of its exponent is defined by

$$\deg(X^\alpha) = \deg(\alpha) = \sum_{i=1}^{m} \alpha_i.$$ 

Giving a reduction order on monomials in $m$ variables is the same as giving a total order on $\mathbb{N}_0^m$ such that, for all $\alpha_1, \alpha_2$, and $\alpha$ in $\mathbb{N}_0^m$, the following holds

(E.1) If $\alpha \neq 0$, then $0 \prec \alpha$,
(E.2) If $\alpha_1 \prec \alpha_2$, then $\alpha + \alpha_1 \prec \alpha + \alpha_2$.

We use $\prec$ both for monomials and exponents.

**Example 4.2** The lexicographic order $\prec_L$ is defined by

$\alpha \prec_L \beta$ if and only if $\alpha_1 = \beta_1, \ldots, \alpha_{l-1} = \beta_{l-1}$ and $\alpha_l < \beta_l$ for some $l$, $1 \leq l \leq m$.

The lexicographic order is a reduction order that is not isomorphic with $\mathbb{N}$ with its ordinary order $\prec$.

**Remark 4.3** Let $\prec$ be a reduction order that is isomorphic with $\mathbb{N}$ with its ordinary order $\prec$. Then the monomials can be listed by the sequence $(M_l| l \in \mathbb{N})$ such that $M_l \prec M_{l+1}$ for all $l$. Furthermore for all $i, j$ there exists an $l(i, j)$ such that $M_i M_j = M_{l(i, j)}$. The function $l(i, j)$ is strictly increasing, since $\prec$ is a reduction order. So $(M_l| l \in \mathbb{N})$ is a well-behaving sequence of $R = \mathbb{F}[X_1, \ldots, X_m]$. Hence $R$ has an order function by Theorem 3.5.
Example 4.4 Let \( w = (w_1, \ldots, w_m) \) be an \( m \)-tuple of positive integers called *weights*. The *weighted degree* of \( \alpha \in \mathbb{N}_0^m \) and the corresponding monomial \( X^\alpha \) is defined by

\[
\text{wdeg}(X^\alpha) = \text{wdeg}(\alpha) = \sum_{i=1}^{m} \alpha_i w_i,
\]

and of a nonzero polynomial \( F = \sum \lambda_\alpha X^\alpha \) by

\[
\text{wdeg}(F) = \max \{ \text{wdeg}(X^\alpha) \mid \lambda_\alpha \neq 0 \}.
\]

This gives a degree function \( \text{wdeg} \) on the ring \( \mathbb{F}[X_1, \ldots, X_m] \). The *weighted graded lexicographic order* \( \preceq_w \) on \( \mathbb{N}_0^m \) is defined by

\[
\alpha \preceq_w \beta \text{ if and only if } \text{wdeg}(\alpha) < \text{wdeg}(\beta) \text{ or } \text{wdeg}(\alpha) = \text{wdeg}(\beta) \text{ and } \alpha \prec_L \beta,
\]

and similarly for the monomials. This is indeed a reduction order that is isomorphic with \( \mathbb{N} \). Hence \( \mathbb{F}[X_1, \ldots, X_m] \) has an order function by Remark 4.3 which will be denoted by \( \omega \).

Example 4.5 Let \( I \) be the ideal in \( \mathbb{F}[X,Y] \) generated by a polynomial of the form

\[
X^a + Y^b + G(X,Y)
\]

with \( \deg(G) < \min\{a, b\} \) and \( \gcd(a, b) = 1 \). So it is of type I according to [5], see also [15]. Let \( R = \mathbb{F}[X,Y]/I \). Denote the cosets of \( X \) and \( Y \) modulo \( I \) by \( x \) and \( y \), respectively. Then \( x^a = -y^b - g(x,y) \). So \( x^a \) is a linear combination of elements of the form \( x^\alpha y^\beta \) with \( 0 \leq \alpha < a \), since \( \deg(G) < b \). By recursion one shows that the set

\[
\{ x^\alpha y^\beta \mid 0 \leq \alpha < a \}
\]

is a basis for \( R \). Using the properties of order functions one shows that \( \rho(x) = b \) and \( \rho(y) = a \) if there exists a weight function \( \rho \) on \( R \) such that \( \gcd(\rho(x), \rho(y)) = 1 \).

In the following it is shown that indeed such a weight function exists.

Proposition 4.6 Let \( I \) be the ideal in \( \mathbb{F}[X,Y] \) generated by a polynomial of the form \( X^a + Y^b + G(X,Y) \) with \( \deg(G) < \min\{a, b\} \) and \( \gcd(a, b) = 1 \). Let \( R = \mathbb{F}[X,Y]/I \). Then there exists a weight function \( \rho \) on \( R \). The ring \( R \) is an integral domain, \( I \) is a prime ideal and \( X^a + Y^b + G(X,Y) \) is absolutely irreducible.
Proof. See also [5, 15]. A generalization of this proposition will be given in Theorem 5.11 and Proposition 5.12. Consider the total weighted degree lexicographic order \( <_w \) on the monomials in \( X \) and \( Y \) with respect to the weights \( \text{wdeg}(X) = b \) and \( \text{wdeg}(Y) = a \). This weight function is injective on the set \( \{ X^\alpha Y^\beta | 0 \leq \alpha < a \} \), since \( \gcd(a, b) = 1 \). Let \( f_1, f_2, \ldots \) be an enumeration of the elements \( x^\alpha y^\beta \) of the basis of \( R \), and let \( \rho_1, \rho_2, \ldots \) be an enumeration of the nonnegative integers of the form \( \alpha b + \beta a \) with \( 0 \leq \alpha < a \), in such a way that \( \rho_i < \rho_{i+1} \) and \( f_i = x^\alpha y^\beta \) if \( \rho_i = \alpha b + \beta a \) and \( 0 \leq \alpha < a \), for all \( i \).

It is proved by induction that \( \rho_{l(i,j)} = \rho_i + \rho_j \). The induction is with respect to the well-order \( <_w \) on \( \mathbb{N}^2 \). Now \( f_1 = 1 \) and \( \rho_1 = 0 \). So \( l(1, 1) = 1 \) and the start of the induction is satisfied. Suppose that the claim is proved for all \( (i', j') <_w (i, j) \). Let \( f_i = x^\alpha y^\beta \), \( \rho_i = \alpha b + \beta a \) with \( 0 \leq \alpha < a \).

Let \( f_j = x^\gamma y^\delta \), \( \rho_j = \gamma b + \delta a \) with \( 0 \leq \gamma < a \). Then \( f_i f_j = x^{\alpha+\gamma} y^{\beta+\delta} \) and \( \rho_i + \rho_j = (\alpha + \gamma)b + (\beta + \delta)a \).

If \( \alpha + \gamma < a \), then \( f_i f_j \) is a basis element. So \( f_{l(i,j)} = f_i f_j \) and \( \rho_{l(i,j)} = \rho_i + \rho_j \).

If \( \alpha + \gamma \geq a \), then \( \alpha + \gamma = a + \epsilon \) with \( 0 \leq \epsilon < a \). So

\[
\rho_i + \rho_j = (\alpha + \gamma)b + (\beta + \delta)a = eb + (b + \beta + \delta)a
\]

and

\[
f_i f_j = -x^\epsilon y^{b+\beta+\delta} - x^\epsilon g(x, y).
\]

The term \( x^\epsilon y^{b+\beta+\delta} \) is a basis element \( f_l \). We may assume by induction that \( x^\epsilon g(x, y) \in L(l - 1) \), since \( \deg(G) < \min\{a, b\} \). So \( l = l(i, j) \) and \( \rho_l = eb + (b + \beta + \delta)a = \rho_i + \rho_j \).

So in both cases \( f_i f_j \in L(l) \setminus L(l - 1) \), where \( l = l(i, j) \) and \( \rho_l = \rho_i + \rho_j \). Therefore \( l(i, j) < l(i + 1, j) \).

Hence there exists a weight function \( \rho \) on \( R \) such that \( \rho(x^\alpha y^\beta) = \alpha b + \beta a \), by Theorem 3.5. So \( R \) is an integral domain by Proposition 3.7 and \( I \) is a prime ideal. These results still hold after extending the field \( \mathbb{F} \) to its algebraic closure. Therefore \( X^a + Y^b + G(X, Y) \) is absolutely irreducible. \( \square \)

5 Gröbner bases and weight functions

Definition 5.1 Let \( \mathbb{F} \) be a field. Let \( R = \mathbb{F}[X_1, \ldots, X_m] \). The set of monomials in \( X_1, \ldots, X_m \) will be denoted by \( \mathcal{M} \). Let \( < \) be a reduction order on \( \mathcal{M} \).
If $F = \sum \lambda_{\alpha} X^\alpha$, then $\{X^\alpha | \lambda_{\alpha} \neq 0\}$ is called the *support* of $F$ and is denoted by $\text{supp}(F)$. The support is finite and $\prec$ is a total order, so $\text{supp}(F)$ has a largest element that is called the *leading monomial* of $F$ and is denoted by $\text{lm}(F)$. If $X^\alpha$ is the leading monomial of $F$, then $\lambda_{\alpha} X^\alpha$ is called the *leading term* of $F$ and is denoted by $\text{lt}(F)$, and $\lambda_{\alpha}$ is called the *leading coefficient* of $F$.

Definition 5.2 The partial order $\leq_P$ on $\mathcal{M}$ is defined by $X^\alpha \leq_P X^\beta$ if and only if $\alpha_i \leq \beta_i$ for all $i = 1, \ldots, m$.

Definition 5.3 Let $\mathcal{B}$ be a finite subset of $R$. If $F, G \in R$, then $F$ *reduces* to $G$ with respect to $\mathcal{B}$ if there exists a monomial $X^\alpha$ in the support of $F$ with coefficient $\lambda_{\alpha}$, and an element $B \in \mathcal{B}$ such that $\text{lt}(B) = \mu_{\beta} X^\beta$, $\beta \leq_P \alpha$ and

$$G = F - \frac{\lambda_{\alpha}}{\mu_{\beta}} BX^{\alpha-\beta}.$$  

This is denoted by $F \rightarrow_B G$, or $F \rightarrow G$ for short. If $F = G$ or there is a sequence $G_1, \ldots, G_k$ such that $F = G_1$, $G = G_k$ and $G_i \rightarrow_B G_{i+1}$ for all $1 \leq i < k$, then this is denoted by $F \rightarrow^* \mathcal{B} G$.

The ideal generated by $\mathcal{B}$ is denoted by $(\mathcal{B})$. If $F \rightarrow^* \mathcal{B} 0$, then $F \in (\mathcal{B})$. A finite set $\mathcal{B}$ in $R$ is called a *Gröbner basis* if the converse holds as well; that is to say, if $F \rightarrow^* \mathcal{B} 0$ for all $F \in (\mathcal{B})$.

The following theorem characterizes Gröbner bases.

Theorem 5.4 Let $\mathcal{B}$ be a finite set in $R$. Then $\mathcal{B}$ is a Gröbner basis if and only if

$$\{\text{lm}(F) | F \in (\mathcal{B}), F \neq 0\} = \{\text{lm}(BM) | B \in \mathcal{B}, B \neq 0, M \in \mathcal{M}\}.$$  

Proof. See [1, 2].

Definition 5.5 The *footprint* or $\Delta$-set of a Gröbner basis $\mathcal{B}$ is defined by

$$\Delta(\mathcal{B}) = \mathcal{M} \setminus \{\text{lm}(BM) | B \in \mathcal{B}, B \neq 0, M \in \mathcal{M}\}.$$  

Corollary 5.6 If $\mathcal{B}$ is a Gröbner basis for the ideal $I$ in $R$, then the cosets modulo $I$ of the elements of the footprint $\Delta(\mathcal{B})$ form a basis of $R/I$.
Definition 5.7 Let $F_1$ and $F_2$ be nonzero polynomials. Let $M_i = \text{lcm}(F_i)$ and $\lambda_i = \text{lc}(F_i)$. Then there exist monomials $N_1$ and $N_2$ such that $M_i N_i = \text{lcm}(M_1, M_2)$ for $i = 1, 2$. The S-polynomial of $F_1$ and $F_2$ is defined as

$$S(F_1, F_2) = \lambda_2 N_1 F_1 - \lambda_1 N_2 F_2.$$ 

Another useful characterization of Gröbner bases is given by the following.

Proposition 5.8 Let $\mathcal{B}$ be a finite set in $R$. Then $\mathcal{B}$ is a Gröbner basis if and only if $S(B_1, B_2) \rightarrow^\bullet_\mathcal{B} 0$ for all $B_1, B_2 \in (\mathcal{B})$.

Proof. See [1, 2].

Remark 5.9 The theory of Gröbner bases can be developed for any $\mathbb{F}$-algebra with an order function.

Let $\preceq_w$ be the weighted graded lexicographic order on $\mathbb{F}[X_1, \ldots, X_m]$ with respect to the weights $(w_1, \ldots, w_m)$. Let $\omega$ be the associated order function. See Example 4.4.

Lemma 5.10 Let $\preceq_w$ be the weighted graded lexicographic order. Let $\mathcal{B}$ be a set of polynomials such that every element of $\mathcal{B}$ has exactly two monomials of highest weighted degree in its support. If $F \rightarrow^\bullet_\mathcal{B} G$ with respect to $\preceq_w$ and $F$ has exactly one monomial of highest weighted degree in its support, then $\text{wdeg}(F) = \text{wdeg}(G)$ and $G$ has exactly one monomial of highest weighted degree in its support.

Proof. By induction it is enough to show the lemma when $F \rightarrow_\mathcal{B} G$ and $F$ has exactly one monomial of highest weighted degree in its support. Let $F = F' + \lambda \alpha X^\alpha$ for some polynomial $F'$ such that $\text{wdeg}(F') < \text{wdeg}(F)$ and $\lambda X^\alpha$ is the leading term of $F$. Let $F \rightarrow_\mathcal{B} G$. Then $G = F - \mu MB$ for some $B \in \mathcal{B}$ and monomial $M$ such that $\text{lt}(\mu MB)$ is a nonzero term of $F$. So $\text{wdeg}(MB) \leq \text{wdeg}(F)$.

If $\text{wdeg}(MB) < \text{wdeg}(F)$, then $G = (F' - \mu MB) + \lambda \alpha X^\alpha$. So the weighted degree of $F' - \mu MB$ is strictly smaller than $\text{wdeg}(G)$, and $F$ and $G$ both have $X^\alpha$ as the unique monomial of highest weighted degree in their support.

If $\text{wdeg}(MB) = \text{wdeg}(F)$, then the assumption is used that $B$ has exactly two monomials of highest weighted degree in its support. So there exist a polynomial $B'$, monomials $M_1$, $M_2$ and nonzero elements $\mu_1, \mu_2 \in \mathbb{F}_q$ such...
that $B = B' + \mu_1 M_1 + \mu_2 M_2$, $\text{wdeg}(B') < \text{wdeg}(M_1) = \text{wdeg}(M_2)$ and $M_1 \prec_w M_2$. Therefore the leading term of $\mu MB$ is $\mu_2 MM_2$ is equal to $\lambda_0 X^a$, since it is the only nonzero term of $F$ of weighted degree $\text{wdeg}(MB)$. So $G = (F' - \mu MB') - \mu_1 M M_1$ and the weighted degree of $F' - \mu MB'$ is strictly smaller than $\text{wdeg}(G) = \text{wdeg}(M M_1)$. Hence $\text{wdeg}(G) = \text{wdeg}(F)$ and $M M_1$ is the only monomial of highest weighted degree in the support of $G$. □

**Theorem 5.11** Let $I$ be an ideal in $\mathbb{F}[X_1, \ldots, X_m]$ with Gröbner bases $B$ with respect to $\prec_w$. Suppose that the elements of the footprint of $I$ have mutually distinct weighted degrees and that every element of $B$ has exactly two monomials of highest weighted degree in its support. Then there exists a weight function $\rho$ on $R = \mathbb{F}[X_1, \ldots, X_m]/I$ with the property that $\rho(f) = \text{wdeg}(F)$, where $f$ is the coset of $F$ modulo $I$, for all polynomials $F$ with support in $\Delta(I)$.

**Proof.** The condition on the footprint implies that there exists a sequence $F_1, F_2, \ldots$ enumerating the elements of the footprint such that $\text{wdeg}(F_i) < \text{wdeg}(F_{i+1})$ for all $i$. Let $f_i$ be the coset of $F_i$ modulo $I$. Then $f_1, f_2, \ldots$ is a basis of $R$ by Corollary 5.6. Let $\rho_i = \text{wdeg}(F_i)$. Then $\rho_i < \rho_{i+1}$ for all $i$. The product $f_if_j$ can be expressed as

$$f_if_j = \sum_{l \leq l(i,j)} \lambda_l f_l$$

with $\lambda_l \in \mathbb{F}$ for all $l$ and $\lambda_{l(i,j)} \neq 0$. So $F_i F_j - \sum_{l \leq l(i,j)} \lambda_l F_l \in I$. Hence

$$F_i F_j \leadsto_B \sum_{l \leq l(i,j)} \lambda_l F_l,$$

since $B$ is a Gröbner bases for $I$. Let $F = F_i F_j$ and $G = \sum_{l \leq l(i,j)} \lambda_l F_l$. Now $F$ satisfies the assumption of Lemma 5.10, since $F$ is a monomial. Hence

$$\rho_i + \rho_j = \text{wdeg}(F_i F_j) = \text{wdeg}(F) = \text{wdeg}(G) = \text{wdeg}(F_{l(i,j)}) = \rho_{l(i,j)}.$$

Theorem 3.5 implies that there exists a weight function $\rho$ on $R$ with the stated property. □
Proposition 5.12 Let $I$ be the ideal in $\mathbb{F}[X_1, \ldots, X_m]$ generated by

$$F_i = X_i^{a_i} + X_{i+1}^{b_i} + G_i$$

for $i = 1, \ldots, m - 1$,

where $G_i \in \mathbb{F}[X_1, \ldots, X_{i+1}]$, $\text{wdeg}(G_i) < a_1 \cdots a_ib_1 \cdots b_{m-1}$ and $\gcd(a_i, b_j) = 1$ for all $i \leq j$. Then the ring $R = \mathbb{F}[X_1, \ldots, X_m]/I$ has a weight function $\rho$.

Proof. This is a generalization of Proposition 4.6 and a consequence of Theorem 5.11.

Let $w_i = a_1 \cdots a_{i-1}b_i \cdots b_{m-1}$. Let $w = (w_1, \ldots, w_m)$. Let $\prec_w$ be the graded lexicographic order with respect to the weights $w$. Then

$$\text{wdeg}(X_i^{a_i}) = \text{wdeg}(X_{i+1}^{b_i}) = a_1 \cdots a_ib_1 \cdots b_{m-1} \geq \text{wdeg}(G_i).$$

So $X_i^{a_i}$ is the leading monomial of $F_i$ and $F_i$ has exactly two monomials in its support of the same highest weighted degree.

Let $B = \{F_1, \ldots, F_{m-1}\}$. Then the footprint of $B$ is equal to

$$\{X^a | 0 \leq a_i < a_i \text{ for all } 1 \leq i < m\}.$$  

The weighted degree of elements of this footprint are mutually distinct, since $\gcd(a_i, b_j) = 1$ for all $i \leq j$.

Consider the S-polynomial of $F_i$ and $F_j$

$$S(F_i, F_j) = X_i^{a_i}X_{i+1}^{b_i} + X_j^{a_j}G_i - X_i^{a_i}X_{i+1}^{b_j} + X_i^{a_i}G_j \rightarrow_F$$

$$-X_j^{b_j}X_{i+1}^{b_i} - G_iG_j - X_i^{a_i}X_{i+1}^{b_j} + X_i^{a_i}G_j \rightarrow_F 0.$$  

So $S(F_i, F_j) \rightarrow_B 0$ for all $F_i, F_j \in B$. Hence $B$ is a Gröbner basis for $I$ by Proposition 5.8. So the ring $R$ has a weight function by Theorem 5.11. □

Remark 5.13 Notice that it is essential that one assumes that the $G_i$ do not depend on $X_j$ for all $j > i + 1$. Take for instance $m = 3$, $a_1 = 3, b_1 = 5, a_2 = 5, b_2 = 2$ and $G_1 = X_2^3, G_2 = 0$, then $X_1^3 \in I = (X_1^3 + X_2^5 + X_3^2, X_2^3 + X_3^2)$, but $X_1 \notin I$.

The assumption "gcd($a_i, b_i$) = 1 for all $i" as in [4], instead of "gcd($a_i, b_j$) = 1 for all $i \leq j"", is not enough to guarantee the existence of an order function, and as a consequence that $I$ is a prime ideal. Take for example $m = 3$, $a_1 = b_2 = 2, a_2 = b_1 = 3$ and $G_1 = G_2 = 0$, then $I = (X_1^2 - X_2^3, X_2^3 - X_3^2)$ is not prime, since

$$(X_1 - X_3)(X_1 + X_3) = X_1^2 - X_3^2 = (X_1^2 - X_2^3) + (X_2^3 - X_3^2) \in I,$$

but $X_1 - X_3$ nor $X_1 + X_2$ is an element of $I$.  

17
This paper was submitted on August 1996. In the meantime it was found that Proposition 5.11 and its converse were shown by Miura [16, 17, 18]. In Matsumoto-Miura [14] this was done by the same Gröbner bases techniques as in this paper. A generalization of these results were obtained by Geil and the author in [8, 9].

References


