Bull. Korean Math. Soc. **34** (1997), No. 4, pp. 595–601

APPLICATION OF GRÖBNER BASES TO SOME RATIONAL CURVES

YOUNG HYUN CHO AND JAE MYUNG CHUNG

ABSTRACT. Let C_d be the rational curve of degree d in $\mathbb{P}^3_k$ given parametrically by $X_0 = u^d$, $X_1 = u^{d-1}t$, $X_2 = ut^{d-1}$, $X_3 = t^d$ $(d \geq 4)$. Then the defining ideal of C_d can be minimally generated by d polynomials $F_1, F_2, \ldots, F_d$ such that $\deg F_1 = 2$, $\deg F_2 = \cdots = \deg F_d = d-1$ and C_d is a set-theoretically complete intersection on $F_2 = X_1^{d-1} - X_2X_0^{d-2}$ for every field k of characteristic $p > 0$. For the proofs we will use the notion of Gröbner basis.

1. Introduction

One of the classical old problems in algebraic geometry is whether every connected projective curve in $\mathbb{P}^3_k$ is a set-theoretic complete intersection. For any $d \geq 4$, let C_d be the rational curve of degree d in $\mathbb{P}^3_k$ given parametrically by $X_0 = u^d$, $X_1 = u^{d-1}t$, $X_2 = ut^{d-1}$, $X_3 = t^d$. If k is an algebraically closed field of characteristic $p > 0$, then in [3] it was shown that C_d is a set-theoretically complete intersections in $\mathbb{P}^3_k$ for any $d \geq 4$. But even for $d = 4$, it is not known whether the rational quartic curve C_4 is a set-theoretic complete intersection in characteristic zero field.

The main results in this article are the followings. The defining ideal of C_d can be minimally generated by d polynomials $F_1, F_2, \ldots, F_d$ such that $\deg F_1 = 2$, and $\deg F_2 = \cdots = \deg F_d = d-1$ for any $d \geq 4$. Next we show that C_d is a set-theoretic complete intersection on $F_2 = X_1^{d-1} - X_2X_0^{d-2}$ for every field k of characteristic $p > 0$, and this fact is a generalization of Proposition 1.5 in [5]. For the proofs, we

Received February 3, 1997.

1991 Mathematics Subject Classification: 13C14, 13D02.

Key words and phrases: Gröbner bases, Rational curves, Set-theoretic complete intersection.

This research is partially supported by the S. N. U.-Daewoo Program in 1994.

use the notion of Gröbner bases of ideals in polynomial rings. Applying Buchberger's algorithm to the defining ideal of the corresponding affine curve E_d given parametrically by $Y_1 = s$, $Y_2 = s^{d-1}$, $Y_3 = s^d$, we get the Gröbner basis of the defining ideal of E_d. Then by Proposition 2.2, we find the Gröbner basis of the defining ideal of C_d, and this set consists of minimal equations defining C_d in Theorem 3.3.

2. Gröbner Bases

In this section we introduce the notion of Gröbner bases and those properties which are needed in next sections. For the main reference you may see [2].

Let S be a polynomial ring $k[X_1, \ldots, X_n]$ over a field k and A be the set of monomials in S. We give the reverse lexicographic order to A as follows: for two monomials $m = X_1^{a_1}X_2^{a_2}\cdots X_n^{a_n}$ and $n = X_1^{b_1}X_2^{b_2}\cdots X_n^{b_n}$ we write $m > n$ iff $\deg m > \deg n$ or $\deg m = \deg n$ and $a_i < b_i$ for the last index i with $a_i \neq b_i$.

$>$ is a monomial order and for any $f \in S$ we define the initial term of f, written $\text{in}(f)$, to be the greatest term of f with respect to the order $>$. For an ideal $I \subset S$, we define $\text{in}(I)$ to be the monomial ideal generated by the elements $\text{in}(f)$ for all $f \in I$.

For an ideal $I \subset k[X_1, \ldots, X_n]$, a set of polynomials $\{f_1, \ldots, f_r\} \subset I$ is called a Gröbner basis for I if $\text{in}(I)$ is generated by $\text{in}(f_1), \ldots, \text{in}(f_r)$. It can be easily checked that if $\{f_1, \ldots, f_r\} \subset I$ is a Gröbner basis of I then $I = (f_1, \ldots, f_r)$.

Now for a polynomial f in S, we denote ${}^h f$ for the homogeneous polynomial $X_0^{\deg f} f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0})$ in $k[X_0, \ldots, X_n]$. Also for any ideal $I \subset S$, ${}^h I$ will denote the homogeneous ideal generated by the forms ${}^h f$ with $f \in I$.

In [6], we can find the following well-known facts.

PROPOSITION 2.1. (1) *If $I(V)$ is the defining ideal of an affine variety V in $\mathbb{A}_k^n$, then the defining ideal of its projective closure in $\mathbb{P}_k^n$ is ${}^h I(V)$.*
(2) *For an ideal $I \subset S$, ${}^h \text{rad}\, I = \text{rad}\, {}^h I$.*

We give a monomial order to the set of monomials in $k[X_0, \ldots, X_n]$ as follows: for any monomial $m = X_0^{a_0}X_1^{a_1}\cdots X_n^{a_n}$, we rewrite m as

$X_1^{a_1} \cdots X_n^{a_n} X_0^{a_0}$. Then we apply the reverse lexicographic order with respect to the changed order of variables. From this setting of order, we can check that $\mathrm{in}(f) = \mathrm{in}({}^h f)$ for any $f \in S$.

PROPOSITION 2.2. (1) *If $\{f_1, \ldots, f_r\}$ is a Gröbner basis of the ideal $I \subset S$, then $\{{}^h f_1, \ldots, {}^h f_r\}$ is a Gröbner basis of the ideal ${}^h I$.*

(2) *If $\{f_1, \ldots, f_r\}$ is a Gröbner basis of the ideal $(f_1, \ldots, f_r)$ and $rad(f_1, \ldots, f_r) = I$ then ${}^h I = rad({}^h f_1, \ldots, {}^h f_r)$.*

Proof. Refer [5]. □

3. Minimal set of defining equations of C_d

Let C_d be the rational curve of degree d in $\mathbb{P}_k^3$ given parametrically by $X_0 = u^d$, $X_1 = u^{d-1}t$, $X_2 = ut^{d-1}$, $X_3 = t^d$. Take the standard affine open set $X_0 \neq 0$ and put $Y_1 = X_1/X_0$, $Y_2 = X_2/X_0$, $Y_3 = X_3/X_0$. Then C_d is the projective closure of the affine curve $E_d : Y_1 = s$, $Y_2 = s^{d-1}$, $Y_3 = s^d$.

The defining ideals of general affine curves of the form $Y_1 = s^\alpha$, $Y_2 = s^\beta$, $Y_3 = s^\gamma$ have been completely described by Herzog in [4]. By using the Theorem 3.8 in [4], we can calculate that $Y_1Y_2 - Y_3$ and $Y_1^{d-1} - Y_2$ are generators of $I(E_d)$. Our aim is to find the Gröbner basis of $I(E_d)$ and to calculate this we will use Buchberger's algorithm.

PROPOSITION 3.1 ([2]). *Let $S = k[X_1, \ldots, X_n]$ with a monomial order and $g_1, \ldots, g_t$ be nonzero elements of S. For each pair of indices i, j we define $m_{ij} = in(g_i)/GCD(in(g_i), in(g_j))$. GCD denotes the greatest common divisor. Next we choose a standard expression*

$$\begin{aligned} S(g_i, g_j) &\equiv m_{ji}g_i - m_{ij}g_j \\ (*) \qquad &= \sum_{\mu=1}^{t} f_\mu^{(ij)} g_\mu + h_{ij} \end{aligned}$$

for $m_{ji}g_i - m_{ij}g_j$ with respecto to $g_1, \ldots, g_t$. Then the elements $g_1, \ldots, g_t$ form a Gröbner basis iff $h_{ij} = 0$ for all i and j.

Here a standard expression (*) is an expression satisfying the condition that none of the terms of h_{ij} is in $(in(g_1), \ldots, in(g_t))$ and $in(S(g_i, g_j)) \geq in(f_\mu^{(ij)} g_\mu)$ for every μ.

Buchberger's Algorithm [2]: In the Proposition 3.1, let $(g_1, \ldots, g_t) = I$. Compute the remainders h_{ij} of $S(g_i, g_j)$. If all the $h_{ij} = 0$, then $\{g_1, \ldots, g_t\}$ form a Gröbner basis for I. If some $h_{ij} \neq 0$, then replace $g_1, \ldots, g_t$ with $g_1, \ldots g_t, h_{ij}$, and repeat the process. Since the ideal generated by the initial forms of $g_1, \ldots, g_t$, h_{ij} is strictly larger than the one generated by the initial forms of $g_1, \ldots, g_t$, this process must terminate after finitely many steps.

THEOREM 3.2. *The Gröbner Basis of $I(E_d) \subset k[Y_1, Y_2, Y_3]$ is $\{f_1 = Y_1Y_2 - Y_3, f_2 = Y_1^{d-1} - Y_2,\ f_3 = Y_1^{d-2}Y_3 - Y_2^2, \ldots, f_d = Y_2^{d-1} - Y_1Y_3^{d-2}\}$, for any $d \geq 4$.*

Proof. Again, we use the reverse lexicographic order to the set of monomials in $k[Y_1, Y_2, Y_3]$. $\text{in}(f_1) = Y_1Y_2$, $\text{in}(f_2) = Y_1^{d-1}$.

$$\begin{aligned} S(f_1, f_2) &= (Y_1^{d-1}/Y_1)(Y_1Y_2 - Y_3) - (Y_1Y_2/Y_1)(Y_1^{d-1} - Y_2) \\ &= -(Y_1^{d-2}Y_3 - Y_2^2). \end{aligned}$$

We can see $-(Y_1^{d-2}Y_3 - Y_2^2)$ is a remainder of an standard expression of $S(f_1, f_2)$. Set $f_3 \equiv -S(f_1, f_2)$ and add f_3 to $\{f_1, f_2\}$. Now,

$$\begin{aligned} S(f_1, f_3) &= (Y_1^{d-2}Y_3/Y_1)(Y_1Y_2 - Y_3) - (Y_1Y_2/Y_1)(Y_1^{d-2}Y_3 - Y_2^2) \\ &= -(Y_1^{d-3}Y_3^2 - Y_2^3). \end{aligned}$$

Again $-(Y_1^{d-3}Y_3^2 - Y_2^3)$ is a remainder of $S(f_1, f_3)$. Set $f_4 \equiv -S(f_1, f_3)$, and add f_4 to $\{f_1, f_2, f_3\}$. Repeating this way, we get

$$\begin{aligned} S(f_1, f_{d-1}) &= (Y_1^2Y_3^{d-3}/Y_1)(Y_1Y_2 - Y_3) - (Y_1Y_2/Y_1)(Y_1^2Y_3^{d-3} - Y_2^{d-2}) \\ &= Y_2^{d-1} - Y_1Y_3^{d-2}. \end{aligned}$$

Set $f_d = S(f_1, f_{d-1})$, then

$$\begin{aligned} S(f_1, f_d) &= (Y_2^{d-1}/Y_2)(Y_1Y_2 - Y_3) - (Y_1Y_2/Y_2)(Y_2^{d-1} - Y_1Y_3^{d-2}) \\ &= Y_3 f_{d-1}, \end{aligned}$$

hence the remainder is 0. Until now we found the set $\{f_1, \ldots, f_d\}$ and to claim that this set is a Gröbner basis of $I(E_d) = (f_1, f_2)$ we only need to check that the remainders of standard expressions of $S(f_i, f_j)$ are 0, for $2 \leq i < j \leq d$. For $j < d$,

$$\begin{aligned} S(f_i, f_j) &= (Y_1^{d-j+1}Y_3^{j-2}/Y_1^{d-j+1}Y_3^{i-2})(Y_1^{d-i+1}Y_3^{i-2} - Y_2^{i-1}) \\ &\quad - (Y_1^{d-i+1}Y_3^{i-2}/Y_1^{d-j+1}Y_3^{i-2})(Y_1^{d-j+1}Y_3^{j-2} - Y_2^{j-1}) \\ &= Y_1^{j-i}Y_2^{j-1} - Y_2^{i-1}Y_3^{j-i} \\ &= Y_2^{i-1}(Y_1^{j-i}Y_2^{j-i} - Y_3^{j-i}) \\ &= Y_2^{i-1}(Y_1Y_2 - Y_3)G, \end{aligned}$$

for some $G \in k[Y_1, Y_2, Y_3]$. For $j = d$, since $\text{in}(f_i) = Y_1^{d-i+1}Y_3^{i-2}$ and $\text{in}(f_d) = Y_2^{d-1}$, $\text{GCD}(\text{in}(f_i), \text{in}(f_d)) = 1$. Hence remainders of standard expressions of $S(f_i, f_d) = 0$. □

THEOREM 3.3. *The Gröbner basis of* $I(C_d)$ *is* $\{F_1 = X_1X_2 - X_0X_3,$ $F_2 = X_1^{d-1} - X_0^{d-2}X_2,$ $F_3 = X_1^{d-2}X_3 - X_0^{d-3}X_2^2,$ $F_4 = X_1^{d-3}X_3^2 - X_0^{d-4}X_2^3, \ldots, F_d = X_2^{d-1} - X_1X_3^{d-2}\}$, *for any* $d \geq 4$. *Specially this set generates* $I(C_d)$ *minimally.*

Proof. Change the variables Y_i's in Theorem 3.2 to X_i's and then use Proposition 2.1(1) and Proposition 2.2(1). Minimality comes from comparing each terms of F_i's. □

COROLLARY 3.4. C_d *is not arithmetically Cohen-Macaulay for any* $d \geq 4$.

Proof. By [1], C_d is arithmetically Cohen-Macaulay iff the minimal number of generators of $I(C_d) \leq 3$. □

4. Set-theoretic complete intersection

In this section we will show that C_d is a set-theoretic complete intersection on $F_2 = X_1^{d-1} - X_0^{d-2}X_2$, for $\text{ch}\, k = p > 0$.

LEMMA 4.1. *Let p be a prime and $d \geq 4$. Choose $k > 0$ such that $p^k > (d-1)^2$. For $\ell = 1, \ldots, d-2$, write $\ell p^k = (d-1)\alpha_\ell + \beta_\ell$, where α_ℓ and β_ℓ are integers such that $\alpha_\ell \geq 0$ and $0 \leq \beta_\ell \leq d-2$. Then $\alpha_\ell + \beta_\ell \leq p^k$.*

Proof. $\alpha_\ell + \beta_\ell = \frac{\ell}{d-1}p^k - \frac{\beta_\ell}{d-1} + \beta_\ell \leq p^k(1 - \frac{1}{d-1}) + \beta_\ell \leq p^k - (\frac{p^k}{d-1} - \beta_\ell) \leq p^k - 1 \leq p^k$. □

THEOREM 4.2. *C_d is a set-theoretically complete intersection on $F_2 = X_1^{d-1} - X_0^{d-2}X_2$ if $\operatorname{ch} k = p > 0$.*

Proof. Let k be an integer such that $p^k > (d-1)^2$. Then,

$$(**) \quad \begin{aligned} &((X_1X_2 - X_3)^{p^k})^{d-1} \\ &= (X_1^{p^k}X_2^{p^k} - X_3^{p^k})^{d-1} \\ &= X_1^{p^k(d-1)}X_2^{p^k(d-1)} + (d-1)X_1^{p^k(d-2)}X_2^{p^k(d-2)}(-X_3)^{p^k} + \cdots + \\ &\quad (d-1)X_1^{p^k}X_2^{p^k}(-X_3)^{p^k(d-2)} + (-X_3)^{p^k(d-1)}. \end{aligned}$$

Write $\ell p^k = (d-1)\alpha_\ell + \beta_\ell$, for $\ell = 1, \ldots, d-2$ and α_ℓ and β_ℓ are integers such that $\alpha_\ell \geq 0$, $0 \leq \beta_\ell \leq d-2$. Then

$$(**) \quad \begin{aligned} &= X_1^{(d-1)p^k}X_2^{(d-1)p^k} + (d-1)X_1^{(d-1)\alpha_{d-2}+\beta_{d-2}}X_2^{p^k(d-2)}(-X_3)^{p^k} \\ &\quad + \cdots + (d-1)X_1^{(d-1)\alpha_1+\beta_1}X_2^{p^k}(-X_3)^{(d-2)p^k} + (-X_3)^{(d-1)p^k} \\ &\equiv X_2^{dp^k} + (d-1)X_2^{\alpha_{d-2}}X_1^{\beta_{d-2}}X_2^{p^k(d-2)}(-X_3)^{p^k} + \cdots \\ &\quad + (d-1)X_2^{\alpha_1}X_1^{\beta_1}X_2^{p^k}(-X_3)^{(d-2)p^k} + (-X_3)^{(d-1)p^k} \\ &\quad \operatorname{mod}(X_1^{d-1} - X_2). \end{aligned}$$

Let the last polynomial to be g, and compute the degrees of each terms in g. The first term has degree dp^k and the last term has degree $(d-1)p^k$. The degrees of middle terms $= \alpha_\ell + \beta_\ell + p^k\ell + p^k(d-1-\ell) = p^kd + \alpha_\ell + \beta_\ell - p^k \leq p^kd$ by the Lemma 4.1, for $\ell = 1, \ldots, d-2$. Hence $\operatorname{in}(g) = X_2^{dp^k}$. Since $\operatorname{in}(X_1^{d-1} - X_2) = X_1^{d-1}$ and $\operatorname{GCD}(\operatorname{in}(g), \operatorname{in}(X_1^{d-1} - X_2)) = 1$, $\{X_1^{d-1} - X_2, g\}$ is a Gröbner basis of $(X_1^{d-1} - X_2, g)$.

On the other hand, because $(X_1X_2-X_3)^{(d-1)p^k} \equiv g \bmod(X_1^{d-1}-X_2)$ and $(X_1^{d-1}-X_2, X_1X_2-X_3)$ is a prime ideal we can easily check that $\mathrm{rad}(X_1^{d-1}-X_2, g) = (X_1^{d-1}-X_2, X_1X_2-X_3)$. Hence $I(C_d) = {}^hI(E_d) = {}^h(X_1^{d-1}-X_2, X_1X_2-X_3) = {}^h\mathrm{rad}(X_1^{d-1}-X_2, g)$. Now, since $\{X_1^{d-1}-X_2, g\}$ is a Gröbner basis of $(X_1^{d-1}-X_2, g)$, ${}^h\mathrm{rad}(X_1^{d-1}-X_2, g) = \mathrm{rad}({}^h(X_1^{d-1}-X_2), {}^hg)$ by Proposition 2.2(2).

Therefore $I(C_d) = \mathrm{rad}(X_1^{d-1}-X_0^{d-2}X_2, {}^hg)$, and this means that C_d is a set-theoretically complete intersection on F_2.

□

References

[1] H. Bresinsky, P. Schenzel and W. Vogel, *liasion, arithmetical Buchsbaum curves and monomial curves in* $\mathbb{P}^3$, J. Algebra **86** (1984), 283–301.

[2] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, G. T. M. Vol. **150** (Springer-Verlag New York 1995).

[3] R. Hartshorne, *Complete intersections in characteristic* $p > 0$, Amer. J. Math. **101** (1979), 380–383.

[4] J. Herzog, *Generators and relations of abelian semigroups and semigroup ring*, Man. Math. **3** (1970), 175–193.

[5] L. Robbiano and G. Valla, *Some curves in* $\mathbb{P}^3$ *are set-theoreti complete intersections*, Lecture Notes in Mathematics. Vol. **997** (Springer-Verlag, Berlin 1983), 391–399.

[6] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. **2** (Van Nostrand, Princeton 1960).

DEPARTMENT OF MATHEMATICS, COLLEGE OF NATURAL SCIENCES, SEOUL NATIONAL UNIVERSITY, SEOUL 151-742, KOREA