ON THE EQUATIONS DEFINING PROJECTIVE MONOMIAL CURVES

MARGHERITA BARILE[1]
Dipartimento di Matematica, Università degli Studi di Bari, Via Orabona 4
70125 Bari (ITALY)

MARCEL MORALES
Université de Grenoble I, Institut Fourier, Laboratoire de Mathématiques
associé au CNRS, URA 188, B.P.74, 38402 Saint-Martin D'Hères Cedex,
and IUFM de Lyon, 5 rue Anselme, 69317 Lyon Cedex (FRANCE)

Let K be an algebraically closed field, let $R = K[X_0, X_1, X_2, X_3]$. A projective monomial curve is a subvariety C of $\mathbf{P}^3_K$ parametrized by

$$X_0 = u^d,\ X_1 = t^d,\ X_2 = t^{a_1}u^{b_1},\ X_3 = t^{a_2}u^{b_2},$$

where d, a_1, a_2, b_1, b_2 are all nonnegative integers, and $a_1 + b_1 = a_2 + b_2 = d$. Without loss of generality we may assume that $d > a_1 > a_2 > 0$. Let I be the defining ideal of C.

1 Characteristic zero

Moh [1] showed that for $\operatorname{char} K > 0$ the curve C can always be defined by two binomial equations. The next result is a generalization to the case where $\operatorname{char} K = 0$. In the proof we shall explicitely use the arguments developed in [1]. We refer to this paper for more details.

[1]Supported by an Institutional Fellowship from the Commission of the European Communities, Contract ERBCHBG CT 94-0540.

Proposition 1.1. *The curve C is defined set-theoretically by 3 binomial equations.*

PROOF. Let $q = \gcd(a_1, b_1, d)$, and set

$$f = X_2^{d/q} - X_1^{a_1/q} X_0^{b_1/q}$$

Then

$$I \cap K[X_0, X_1, X_2] = (f)$$

Let p be a positive prime number, $p \neq \operatorname{char} K$. Let

$$g = \gcd(d, a_1), \qquad e = \gcd(g, a_2), \qquad g^* = \frac{g}{e}.$$

There are positive integers l_0, l_1, l_2, m such that

$$g^* p^m a_2 = l_1 d + l_2 a_1 \quad \text{and} \quad g^* p^m = l_0 + l_1 + l_2.$$

Let

$$f_1 = X_3^{g^* p m} - X_1^{l_1} X_2^{l_2} X_0^{l_0}.$$

Let $\bar{p}$ be a positive prime number, $\bar{p} \neq \operatorname{char} K$ and $p \neq \bar{p}$. Re-apply the above construction with respect to $\bar{p}$, and obtain a polynomial

$$f_2 = X_3^{g^* \bar{p} m} - X_1^{\bar{l}_1} X_2^{\bar{l}_2} X_0^{\bar{l}_0},$$

where the notation is self-defining. We show that

$$C = V(f, f_1, f_2).$$

Since $f, f_1, f_2 \in I$, one inclusion is trivial. For the opposite inclusion let $h = M_1 - M_2$ be a binomial generator of I, where

$$M_1 = X_0^{\alpha_0} X_1^{\alpha_1} X_2^{\alpha_2} X_3^{\alpha_3} \quad \text{and} \quad M_1 = X_0^{\beta_0} X_1^{\beta_1} X_2^{\beta_2} X_3^{\beta_3}.$$

Then

$$d\alpha_0 + a_1\alpha_2 + a_2\alpha_3 = d\beta_0 + a_1\beta_2 + a_2\beta_3,$$

whence

$$a_2\alpha_3 \equiv a_2\beta_3 \pmod{g}$$

and

$$\frac{a_2}{e}\alpha_3 \equiv \frac{a_2}{e}\beta_3 \pmod{g^*}$$

and finally

$$\alpha_3 \equiv \beta_3 \pmod{g^*},$$

because $\gcd(a_2/e, g^*) = 1$. Therefore there are some nonnegative integers s, t such that

$$\alpha_3 = sg^* + c \qquad \text{and} \qquad \beta_3 = tg^* + c.$$

Thus we can write

$$h = X_3^c (X_0^{\alpha_0} X_1^{\alpha_1} X_2^{\alpha_2} X_3^{sg^*} - X_0^{\beta_0} X_1^{\beta_1} X_2^{\beta_2} X_3^{tg^*}),$$

where the second factor belongs to I. For all positive integers q we set

$$h^{(q)} = M_1^q - M_2^q.$$

Then there is $\widetilde{h} \in (f)$ such that

$$h^{(p^m)} \equiv X_3^c \widetilde{h} \qquad (\text{mod } f_1).$$

Consequently

$$h^{(p^m)} \in (f, f_1).$$

Similarly one concludes that

$$h^{(\bar{p}^m)} \in (f, f_2).$$

Let P be a point in $\mathbf{P}_K^3$ such that $f(P) = f_1(P) = f_2(P) = 0$. We show that $h(P)$=0. Since h is an arbitrary generator of I, this will imply that $C \supseteq V(f, f_1, f_2)$ and complete the proof. It holds:

$$M_1^{p^m}(P) = M_2^{p^m}(P) \quad \text{and} \quad M_1^{\bar{p}^m}(P) = M_2^{\bar{p}^m}(P). \qquad (1)$$

Since p^m and $\bar{p}^m$ are relatively prime, there are integers λ, μ such that

$$\lambda p^m + \mu \bar{p}^m = 1.$$

It suffices to assume that $M_1(P)$ and $M_2(P)$ are non zero. In this case from (1) we deduce that

$$M_1(P) = M_1^{\lambda p^m + \mu \bar{p}^m}(P) = M_2^{\lambda p^m + \mu \bar{p}^m}(P) = M_2(P). \qquad \square$$

2 Positive characteristics

In this section we assume that $\operatorname{char} K > 0$. For the rest we refer to the notation introduced in Section 1. Moh showed that if $\operatorname{char} K = p$, then $C = V(f, f_1)$. We suppose that $\operatorname{char} K \neq p$ and show that the variety $V(f, f_1)$ always has p^m irreducible components, whose defining equations do not depend on $\operatorname{char} K$. We first show the claim in the localized ring $R' = R_{X_0 X_1 X_2}$. Let I' denote the image of I in R'. We need a preliminary result.

Lemma 2.1. *Let*

$$F = X_0^{u_0} X_1^{u_1} X_2^{u_2} X_3^{u_3} - X_0^{v_0} X_1^{v_1} X_2^{v_2}$$

be a binomial of I'. Suppose that $u_3 > 0$ is as small as possible. Then $u_3 = g^*$.

PROOF. The exponent u_3 is the smallest positive integer such that

$$\begin{aligned} u_1 d + u_2 a_1 + u_3 a_2 &= v_1 d + v_2 a_1 \\ u_0 d + u_2 b_1 + u_3 b_2 &= v_0 d + v_2 b_1 \end{aligned}$$

for certain nonnegative integers $u_0, u_1, u_2, v_0, v_1, v_2$. The preceding two conditions are equivalent to the following:

$$u_3 a_2 = w_1 d + w_2 a_1 \qquad (2)$$

$$u_3 b_2 = w_0 d + w_2 b_1 \qquad (3)$$

for some integers w_0, w_1, w_2. The smallest positive integer u_3 verifying (2) is

$$u_3 = \frac{\operatorname{scm}(g, a_2)}{a_2} = \frac{g a_2}{e a_2} = g^*.$$

On the other hand

$$\begin{aligned} g^* b_2 = g^*(d - a_2) &= g^* d - w_1 d - w_2 a_1 = (g^* - w_1) d - w_2 (d - b_1) \\ &= (g^* - w_1 - w_2) d + w_2 b_1, \end{aligned}$$

hence we can replace $w_0 = g^* - w_1 - w_2$ in equation (3), which shows that the system is solvable.

Fix a binomial F fulfilling the assumption of 2.1. Then it holds

Lemma 2.2. $I' = (f, F)R'$.

PROOF. Let

$$G = X_0^{\alpha_0} X_1^{\alpha_1} X_2^{\alpha_2} X_3^{\alpha_3} - X_0^{\beta_0} X_1^{\beta_1} X_2^{\beta_2} \in I.$$

If $\alpha_3 = 0$, then $G \in (f)$. Suppose $\alpha_3 > 0$. In R' it holds:

$$\begin{aligned} G = & \frac{X_0^{\alpha_0} X_1^{\alpha_1} X_2^{\alpha_2} X_3^{\alpha_3 - g^*}}{X_0^{u_0} X_1^{u_1} X_2^{u_2}} F + \\ & \frac{1}{X_0^{u_0} X_1^{u_1} X_2^{u_2}} (X_0^{\alpha_0 + v_0} X_1^{\alpha_1 + v_1} X_2^{\alpha_2 + v_2} X_3^{\alpha_3 - g^*} - X_0^{\beta_0 + u_0} X_1^{\beta_1 + u_1} X_2^{\beta_2 + u_2}), \end{aligned}$$

where the binomial in brackets belongs to I, as it can be easily verified. The rest is induction. □

Let ω be a primitive p^m-th root of the unity. For all $i = 0, \dots, p^m - 1$ set

$$I_i = (f, F(X_0, X_1, X_2, \omega^i X_3)), \qquad I'_i = I_i R'.$$

Then

$$\bigcap_{i=0}^{p^m-1} I'_i = (f, F^{(p^m)})R',$$

where

$$F^{(p^m)} = X_0^{u_0 p^m} X_1^{u_1 p^m} X_2^{u_2 p^m} X_3^{g^* p^m} - X_0^{v_0 p^m} X_1^{v_1 p^m} X_2^{v_2 p^m}.$$

Lemma 2.3.

$$\bigcap_{i=0}^{p^m-1} I'_i = (f, f_1)R'.$$

Proof. Note that I_i is the image of (f, F) via the automorphism of R that is the identity on $K[X_0, X_1, X_2]$ and maps X_3 to $\omega^i X_3$. Since f and f_1 are mapped to themselves, the inclusion "$\supseteq$" is true. We prove "$\subseteq$". Note that

$$F^{(p^m)} = X_0^{u_0 p^m} X_1^{u_1 p^m} X_2^{u_2 p^m} f_1 + \\ X_0^{u_0 p^m + l_0} X_1^{u_1 p^m + l_1} X_2^{v_2 p^m} (X_2^{(u_2 - v_2)p^m + l_2} - X_0^{(v_0 - u_0)p^m - l_0} X_1^{(v_1 - u_1)p^m - l_1})$$

We prove that the monomial in brackets belongs to (f). To this end it suffices to show the following two numerical identities:

$$\begin{cases} \dfrac{(u_2 - v_2)p^m + l_2}{(v_1 - u_1)p^m - l_1} = \dfrac{d}{a_1} & (4) \\ \dfrac{(v_0 - u_0)p^m - l_0}{(v_1 - u_1)p^m - l_1} = \dfrac{d}{a_1} - 1 & (5) \end{cases}$$

Now, since f_1 and F are homogeneous elements of I, it holds:

$$\begin{aligned} g^* p^m &= l_0 + l_1 + l_2, & g^* p^m a_2 &= d l_1 + a_1 l_2; \\ g^* + u_2 + u_1 + u_0 &= v_2 + v_1 + v_0, & g^* a_2 + u_2 a_1 + u_1 d &= v_2 a_1 + v_1 d. \end{aligned}$$

From this (4) and (5) can easily be deduced. ☐

Proposition 2.4. *We have the following prime decomposition*

$$(f, f_1) = \bigcap_{i=0}^{p^m-1} I_i.$$

Proof. We have shown above that the claim holds for the images of the ideals in R'. This implies that I_i is an associated prime of I for all $i = 0, \dots, p^m - 1$. There remains to show that I has no other associated prime. Suppose that $\mathcal{P}$ is a prime ideal such that $(f, f_1) \subseteq \mathcal{P}$, and $X_0 X_1 X_2 \in \mathcal{P}$. Then $X_3 \in \mathcal{P}$, and two among X_0, X_1 and X_2 lie in $\mathcal{P}$. But then height $\mathcal{P} \geq 3$. Since (f, f_1) is of pure height 2, $\mathcal{P}$ is not an associated prime of I. ☐

In particular we have shown: the two binomial equations that in [1] define C for a certain positive characteristic are not valid in any other characteristic.

Acknowledgement

The first author is indebted to the Institut Fourier of the University of Grenoble for hospitality and support during the preparation of this note.

References

[1] [M] T. T. Moh, *Set-theoretic complete intersections*, Proc. Amer. Math. Soc. **94** (1985), pp. 217–220.