ACTA ARITHMETICA
116.2 (2005)

Unique range sets and uniqueness polynomials in positive characteristic II

by

TA THI HOAI AN (Taipei), JULIE TZU-YUEH WANG (Taipei) and PIT-MANN WONG (Notre Dame, IN)

1. Introduction. Let $\mathbf{K}$ be an algebraically closed field of characteristic $p \geq 0$, complete with respect to a non-archimedean absolute value. Let $\mathcal{M}^*(\mathbf{K})$ be the set of non-constant meromorphic functions defined on $\mathbf{K}$ and $\mathcal{F}$ be a non-empty subset of $\mathcal{M}^*(\mathbf{K})$. For $f \in \mathcal{F}$ and a set S in the range of f define

$$E(f,S) = \bigcup_{a \in S} \{(z,m) \in \mathbf{K} \times \mathbb{Z}^+ : f(z) = a \text{ with multiplicity } m\}.$$

Two functions f and g of $\mathcal{F}$ are said to *share* S, counting multiplicity, if $E(f,S) = E(g,S)$. A set S is called a *unique range set*, counting multiplicity, for $\mathcal{F}$, if the condition $E(f,S) = E(g,S)$ for $f, g \in \mathcal{F}$ implies that $f \equiv g$. A polynomial P defined over $\mathbf{K}$ is called a *uniqueness polynomial* for $\mathcal{F}$ if the condition $P(f) = P(g)$ for $f, g \in \mathcal{F}$ implies that $f \equiv g$; P is called a *strong uniqueness polynomial* if the condition $P(f) = cP(g)$ for $f, g \in \mathcal{F}$ and some non-zero constant c implies that $c = 1$ and $f \equiv g$.

In [1] we showed, in the case of positive characteristic, that a special family of polynomials are strong uniqueness polynomials for non-archimedean meromorphic functions. This was accomplished by explicitly constructing, for the curves in $\mathbf{P}^2$ associated to the special family, regular 1-form(s) of Wronskian type. It then follows from the non-archimedean uniformization theorem that these curves are non-archimedean hyperbolic, i.e., there is no non-constant non-archimedean analytic map into the curves. In dealing with more general forms of polynomials than those considered in [1] we are unable to explicitly construct regular 1-form(s), i.e., regular sections of the canonical bundle $\mathcal{K}_C$, on the associated curves; however, we are able to construct explicitly regular m-fold symmetric product of 1-form(s), i.e., regular sections of powers of the canonical bundle $\mathcal{K}_C^m$, and this still implies that

2000 *Mathematics Subject Classification*: Primary 30D35; Secondary 11J97, 11S80.

the associated curves are non-archimedean hyperbolic by the Berkovich Picard Theorem. Locally, on an open neighborhood (U, t) of a smooth point of a curve with local coordinate (uniformization parameter), a regular 1-form may be expressed as $a(t)dt$ where $a(t)$ is a regular function on U; analogously, a regular m-fold symmetric product of 1-form(s) is locally expressed as $a(t)dt^{\otimes m}$. Geometrically this means that, even though we cannot take a root to get a regular 1-form on the curve C ($a(t)^{1/m}$ is not necessarily single-valued), this can be done in an appropriate branched cover.

In Section 3, we treat the case when the characteristic p of the ground field (the ground field $\mathbf{K}$ is assumed to be algebraically closed complete with respect to a non-archimedean absolute value) is zero, and the case when $p > 0$ and p does not divide the degree of the polynomial P. In these cases, we are able to give a complete classification without any extra assumption on the multiplicities of $P'(X) = 0$ as in [9]. We note that the proof for this case involves only the construction of regular 1-forms. This result is recorded as Theorem 1 below. We also note that this line of argument can apply to the complex case (cf. [2]).

In Section 4, we treat the case where $p > 0$ and p divides the degree of the polynomial P. For this, we need to construct regular products of 1-forms. Unfortunately, we are unable to give a complete classification for this case. However, one can see from the statement of Theorem 2 (and the remarks after the theorem) that our results are indeed very sharp. Another result in this section concerns the unique range set problem for non-archimedean entire functions. If $p = 0$ or if p does not divide the cardinality $|S|$ of a finite set $S \subset \mathbf{K}$, it is well known that S is a unique range set for non-archimedean entire functions if and only if S is affinely rigid (cf. [5] and [8]). This characterization is false if p divides $|S|$ (cf. [4] and [8]). However, using Theorem 2, we are able to offer a precise classification for most cases.

Throughout this paper we will let $P(X)$ be a polynomial of degree n in $\mathbf{K}[X]$. We will use l to denote the number of distinct roots of $P'(X)$, and we will denote those roots by $\alpha_1, \ldots, \alpha_l$. We will use $m_1, \ldots, m_l$ to denote the multiplicities of the roots in P'. Thus,

$$P'(X) = a(X - \alpha_1)^{m_1} \cdots (X - \alpha_l)^{m_l},$$

where a is some non-zero constant. We will continually assume what we call

Hypothesis I:

$$P(\alpha_i) \neq P(\alpha_j) \qquad \text{whenever } i \neq j.$$

In other words, P is injective on the roots of P'.

Without loss of generality, we assume that we have listed the α_i so that the m_i are non-increasing. We note that Hypothesis I is a generic condition, and one can see later from our arguments that it makes the computation easier.

We now define three special cases of $P(X)$ as above:

(1A) $l = 1$ and the multiplicity of $X - \alpha_1$ in $P(X) - P(\alpha_1)$ is $\geq m_1$.
(1B) $l = 2, \min\{m_1, m_2\} = 1$, and the multiplicity of $X - \alpha_i$ in $P(X) - P(\alpha_i)$ is $m_i + 1$ for $i = 1, 2$.
(1C) $n = 4, l = 3$, and there exists a permutation ϕ of $\{1, 2, 3\}$ such that $\phi(i) \neq i$ for $i = 1, 2, 3$ and there exists a root w of $w^2 + w + 1 = 0$ such that

$$w = \frac{P(\alpha_i)}{P(\alpha_{\phi(i)})} \qquad \text{for } i = 1, 2, 3.$$

The main results of this article are:

THEOREM 1. *Let $P(X)$ be a polynomial as above satisfying Hypothesis* I. *Assume $p = 0$, or $p > 0$ and $p \nmid n$. Let S be the zero set of P and assume S is affinely rigid. Then*:

(I) *Either $P(X)$ belongs to* (1A) *or* (1B) *above, or $P(X)$ is a uniqueness polynomial for $\mathcal{M}^*(\mathbf{K})$.*
(II) *Either $P(X)$ belongs to* (1A), (1B) *or* (1C) *above, or $P(X)$ is a strong uniqueness polynomial for $\mathcal{M}^*(\mathbf{K})$.*

This result (and its proof) is similar, but a little more complicated than the corresponding result in the complex case (see [2]).

The situation is more complicated when $p \mid n$, and we require some additional notation. We use μ_i to denote the multiplicity of $X - \alpha_i$ in $P(X) - P(\alpha_i)$. We define $b_{i,j}$ by writing

$$P(X) - P(\alpha_i) = \sum_{j=\mu_i}^{n} b_{i,j}(X - \alpha_i)^j.$$

We then define the homogeneous forms $A_{i,\mu_i}(X, Y, Z)$ by

$$\begin{aligned} A_{i,\mu_i}(X,Y,Z) = b_{i,\mu_i} Z &\left[\frac{(X-\alpha_i Z)^{\mu_i} - (Y-\alpha_i Z)^{\mu_i}}{X-Y}\right] \\ &+ b_{i,\mu_i+1}\left[\frac{(X-\alpha_i Z)^{\mu_i+1} - (Y-\alpha_i Z)^{\mu_i+1}}{X-Y}\right]. \end{aligned}$$

Let $m = 1 + \sum_{i=1}^{l} m_i$. When $c \neq 0, 1$ and $m_1 = \cdots = m_l = 1$, for a fixed permutation ϕ of $\{1, \ldots, l\}$ such that $\phi(i) \neq i$ we define the homogeneous forms $B_{i,m}(X, Y, Z)$ by

$$B_{i,m}(X,Y,Z) = \sum_{j=2}^{m} [b_{i,j}(X - \alpha_i Z)^j - c b_{\phi(i),j}(Y - \alpha_{\phi(i)} Z)^j] Z^{m-j}.$$

We then let

$$B(i,m) := B_{i,m}(X,Y,1).$$

We are now ready to state the following theorem:

THEOREM 2. *Let $P(X)$ be a polynomial as above satisfying Hypothesis* I *and such that $p\,|\,n$. Let S be the zero set of $P(X)$ and assume that S is affinely rigid. Let m_i be arranged in non-increasing order. Then*

(I) $P(X)$ *is a uniqueness polynomial for* $\mathcal{M}^*(\mathbf{K})$ *if* (A), (B), *or* (C) *holds, where*:

  (A) $l \geq 3$;

  (B) $l = 2$ *and either*:

    (1) $m_2 \geq 2$, *or*

    (2) $m_2 = 1$ *and either*:

      (a) $\mu_1 \leq m_1$, *or*

      (b) $\mu_1 = m_1 + 1$ *and either*:

        (i) $(m_1 + 2) \nmid n$, *or*

        (ii) $(m_1 + 2)\,|\,n$, $A_{1,m_1}(X,Y,1)$ *is not a factor of* $[P(X) - P(Y)]/(X - Y)$;

  (C) $l = 1$ *and* (1), (2) *or* (3) *holds, where*:

    (1) $\mu_1 \leq m_1 - 1$,

    (2) $\mu_1 = m_1$ *and either*:

      (a) $(m_1 + 1) \nmid n$, *or*

      (b) $(m_1 + 1)\,|\,n$, $p \geq 5$, *and* $A_{1,m_1}(X,Y,1)$ *is not factor of* $[P(X) - P(Y)]/(X - Y)$,

    (3) $\mu_1 = m_1 + 1$, *and either*:

      (a) $u = 2$, $p \geq 5$, *and* $A_{1,m_1+1}(X,Y,1)$ *is not a factor of* $P(X) - P(Y)$, *or*

      (b) $u \geq 3$ *and* $m_1 \geq 2$, *except when* $(m_1,p) = (2,2)$, *or* $(u,m_1,p) = (3,2,5)$, *or* $(3,3,3)$, *where u is defined by writing* $P(X) - P(\alpha_1) = b_{1,m_1+1}(X - \alpha_1)^{m_1+1} + b_{1,m_1+u}(X - \alpha_1)^{m_1+u} + \cdots$ *with* $b_{1,m_1+u} \neq 0$.

(II) *If* $P(X)$ *is a uniqueness polynomial for* $\mathcal{M}^*(\mathbf{K})$ *then it is also a strong uniqueness polynomial for* $\mathcal{M}(\mathbf{K})$ *except in the following cases*:

  (A) $l = 3$, $m_1 = m_2 = m_3 = 1$, $3\,|\,n - 1$, $4\,|\,n$, *there exists a permutation* ϕ *of* $\{1,2,3\}$ *such that* $\phi(i) \neq i$ *for* $i = 1,2,3$, *and there exists a root w of* $w^2 + w + 1 = 0$ *such that*

$$w = \frac{P(\alpha_i)}{P(\alpha_{\phi(i)})} \quad \textit{for } i = 1,2,3,$$

and such that $B(1,4) = B(2,4) = B(3,4)$ *and it is not a factor of* $P(X) - wP(Y)$;

(B) $l = 2$, $m_1 = m_2 = 1$, $3 \mid n$ *and there exists a constant* c *different from* $0, 1$, *and* -1 *such that for some* i, j *with* $\{i, j\} = \{1, 2\}$, *we have* $P(\alpha_i) = cP(\alpha_j)$ *and* $B(i, 3)$ *is a factor of* $P(X) - cP(Y)$;

(C) $l = 2$, $m_1 = m_2 = 1$, n *is odd*, $3 \mid n$, $P(\alpha_1) = -P(\alpha_2)$, $B(1,3) = B(2,3)$, *and* $B(1,3)/(X+Y-\alpha_1-\alpha_2)$ *is a factor of* $P(X)+P(Y)$.

REMARK 1. The condition we find here is very sharp since A_{1,μ_1} (in (I)), $B_{1,4}$, $B_{1,3}$ (in (II.A) and (II.B)) or $B_{1,3}/(X + Y - \alpha_1 Z - \alpha_2 Z)$ (in (II.C)) do define irreducible curves of genus 0 and degree larger than one.

REMARK 2. If we assume that $p \geq 7$ and $m_1 \geq 2$ when $l = 1$, then the conditions in Theorem 2 are necessary and sufficient.

Let $\mathcal{A}^*(\mathbf{K})$ be the set of non-constant entire functions. It is well known that a polynomial is a strong uniqueness polynomial for $\mathcal{A}^*(\mathbf{K})$ if and only if its zero set is a unique range set of $\mathcal{A}^*(\mathbf{K})$. Let S be the set of zeros of $P(X)$. Suppose that b_{1,p^r} and b_{1,p^r-1} in the expansion of $P(X) - P(\alpha_1)$ are both non-zero. Similarly to [6], we consider the two-variable polynomial of degree $p^r - 1$

$$\begin{aligned}\mathcal{F}_{p^r-1}(X, Y) &:= A_{1,p^r-1}(X, Y, 1)\\ &= b_{1,p^r}(X - Y)^{p^r-1} + b_{1,p^r-1}\,\frac{(X - \alpha_1)^{p^r-1} - (Y - \alpha_1)^{p^r-1}}{X - Y}.\end{aligned}$$

For each s_j in S let $t_{j,1}, \ldots, t_{j,p^r-1}$ be the $p^r - 1$ solutions in t of the equation $\mathcal{F}_{p^r-1}(t, s_j) = 0$. Then define

$$T_{\mathcal{F}_{p^r-1}}(S) = \{t_{1,1}, \ldots, t_{1,p^r-1}, t_{2,1}, \ldots, t_{n,p^r-1}\}.$$

We say S is *preserved by a Frobenius transformation* $\mathcal{F}_{p^r-1}$ if $T_{\mathcal{F}_{p^r-1}}(S) = (p^r - 1)S$.

COROLLARY 1. *Let* $P(X)$ *be a polynomial as above satisfying Hypothesis* I *and such that* $p \mid n$. *Let* S *be the zero set of* $P(X)$.

(I) *In cases* (A) *and* (B) *below*, S *is a unique range set for* $\mathcal{A}^*(\mathbf{K})$ *if and only if* S *is affinely rigid*:

(A) $l \geq 2$;

(B) $l = 1$, *and either*

(1) $\mu_1 \leq m_1 - 1$, *or*

(2) $\mu_1 = m_1$, *and either*

(a) $(m_1 + 1) \nmid n$, *or*

(b) $(m_1 + 1) \mid n$ *and* $p \geq 5$,

(3) $\mu_1 = m_1 + 1 \geq 3$, *and either*

(a) $b_{1,m_1+2} = 0$ *and* $p \geq 7$, *or*

(b) $b_{1,m_1+2} \neq 0$ *and* $m_1 + 2$ *is not a power of* p, *and* $p \geq 5$.

(II) *When* $l = 1$, $\mu_1 = m_1 + 1 \geq 3$, $p \geq 7$, $b_{1,p^r} \neq 0$, *and* $m_1 + 2 = p^r$ *for some* $r \geq 1$, S *is a unique range set for* $\mathcal{A}^*(\mathbf{K})$ *if and only if* S *is affinely rigid and* S *is not preserved by the Frobenius transformation* $\mathcal{F}_{p^r-1}(X, Y)$.

2. Symmetric products of regular differential forms. The starting point of [1] is the theorem of Berkovich that a projective irreducible algebraic curve defined over a complete non-archimedean field $\mathbf{K}$ is hyperbolic if and only if it is of positive genus (cf. [3] and [7]). This means simply that there is no non-constant analytic map from $\mathbf{K}$ into an irreducible projective algebraic curve R defined over $\mathbf{K}$ if and only if there is a regular 1-form (an element of $H^0(R, \mathcal{K}_R)$, where $\mathcal{K}_R$ is the canonical sheaf of R) on R which is not identically zero. Since $H^0(R, \mathcal{K}_R^m)$, $m \geq 1$, is trivial if and only if R is a rational curve, this again means that there is no non-constant analytic map from $\mathbf{K}$ into R if and only if there is a regular m-fold symmetric product of 1-form(s) (an element of $H^0(R, \mathcal{K}_R^m)$) on R.

For our purpose, we will need to consider plane curves which may have singularities. We now explain what we mean by a regular m-fold symmetric product of 1-forms. Let R be a plane curve defined by a homogeneous polynomial $R(X, Y, Z) = 0$ over $\mathbf{K}$ and let $\mathfrak{p}$ be a point of R. Let $[X]$, $[Y]$, $[Z]$ be the residue classes of X, Y, Z respectively in the coordinate ring of R. Every 1-form of R can be represented as $Q([X], [Y], [Z])d[X]$, where $Q([X], [Y], [Z])$ is a rational function in $[X]$, $[Y]$, $[Z]$. To check the regularity of a differential form, we will have to check it on each of the local parametrizations. To be more precise, $[X]$, $[Y]$, $[Z]$ can be analytically parametrized at a point $\mathfrak{p} \in R$ by

$$\varphi = (\varphi_0, \varphi_1, \varphi_2) : \Delta_\varepsilon = \{t \in \mathbf{K} \mid |t|_\nu < \varepsilon\} \to R, \qquad \varphi(0) = \mathfrak{p}.$$

The order of a polynomial $Q([X], [Y], [Z])$ (a rational function, or a differential form) in $[X]$, $[Y]$, $[Z]$ with respect to a local parametrization φ at $\mathfrak{p}$ is defined by

$$\mathrm{ord}_{\mathfrak{p},\varphi}\, Q([X], [Y], [Z]) := \mathrm{ord}_t\ Q(\varphi_0, \varphi_1, \varphi_2).$$

Clearly, this definition is independent of the choice of the representing classes of $[X]$, $[Y]$, $[Z]$. For simplicity of notation, we write $\mathrm{ord}_{\mathfrak{p},\varphi}\, Q(X, Y, Z)$ for $\mathrm{ord}_{\mathfrak{p},\varphi}\, Q([X], [Y], [Z])$, where φ is a local parametrization of the curve at $\mathfrak{p}$. A differential form ω in $[X]$, $[Y]$, $[Z]$ is regular at $\mathfrak{p}$ if $\mathrm{ord}_{\mathfrak{p},\varphi}\, \omega \geq 0$ for every analytic parametrization φ at $\mathfrak{p}$.

We deduce

Theorem 3. *Let R be an irreducible projective plane curve defined over $(\mathbf{K}, |\ |_\nu)$. The curve R admits a non-trivial global regular m-fold symmetric product of 1-forms if and only if R is non-archimedean hyperbolic.*

3. Proof of Theorem 1. From now on we consider a polynomial P of the form

$$P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0.$$

Its derivative may be expressed as

$$P'(X) = a(X-\alpha_1)^{m_1} \cdots (X-\alpha_l)^{m_l},$$

where $a \neq 0$ and $\alpha_1, \ldots, \alpha_l$ are the *distinct* roots of P' and $m_i \geq 1$. We assume that P satisfies Hypothesis I, i.e.,

$$P(\alpha_i) \neq P(\alpha_j) \quad \text{for all } 1 \leq i \neq j \leq l. \tag{3.0.1}$$

We denote by μ_i the multiplicity of $X - \alpha_i$ in $P(X) - P(\alpha_i)$. Therefore,

$$P(X) - P(\alpha_i) = *(X-\alpha_i)^{\mu_i} + \cdots + *(X-\alpha_i)^{m_i+1} + \cdots + *(X-\alpha_i)^n. \tag{3.0.2}$$

Here, we use $*$ to indicate a non-zero element in $\mathbf{K}$. We will use this notation throughout the paper. Note that $\mu_i \leq m_i + 1$ and that equality holds if the characteristic of $\mathbf{K}$ is zero.

Let $F(X,Y,Z)$ be the homogenization of the polynomial of two variables

$$\frac{P(X) - P(Y)}{X - Y} = \sum_{k=1}^{n} a_k \sum_{j=0}^{k-1} X^{k-1-j} Y^j,$$

so that

$$F(X,Y,Z) = \sum_{k=1}^{n} \sum_{j=0}^{k-1} a_k X^{k-1-j} Y^j Z^{n-k} = Z^n \, \frac{P(X/Z) - P(Y/Z)}{X - Y}. \tag{3.0.3}$$

Denote by C the curve defined by $F(X,Y,Z) = 0$. Similarly, let $F_c(X,Y,Z)$ be the homogenization of the polynomial $P(X) - cP(Y)$ for $c \neq 0, 1$, and denote by C_c the curve defined by $F_c(X,Y,Z) = 0$. If f and g are non-archimedean meromorphic functions such that $P(f) = P(g)$ or $P(f) = cP(g)$, then $\phi = (f, g, 1)$ is a non-archimedean analytic map into C or C_c respectively. Our purpose is to construct respectively on C and each C_c, $c \neq 0, 1$, a regular 1-form or a regular product of 1-forms which is non-trivial on each of its components. Then Theorem 3 implies that f and g have to be constant, i.e., $P(X)$ is a strong uniqueness polynomial.

3.1. *On the curve* $[F(X,Y,Z) = 0]$. We may express the polynomial $F(X,Y,Z)$ as a polynomial in $X - \alpha_i Z$ and $Y - \alpha_i Z$:

$$F(X,Y,Z) = *\left[\frac{(X-\alpha_i Z)^{\mu_i} - (Y-\alpha_i Z)^{\mu_i}}{X-Y}\right] Z^{n-\mu_i} + *\left[\frac{(X-\alpha_i Z)^{w_i} - (Y-\alpha_i Z)^{w_i}}{X-Y}\right] Z^{n-w_i} + \cdots + *\left[\frac{(X-\alpha_i Z)^{n} - (Y-\alpha_i Z)^{n}}{X-Y}\right], \tag{3.1.1}$$

where w_i is the degree of the second non-vanishing term in (3.0.2).

From (3.1.1), and the fact that $F(\varphi_0, \varphi_1, \varphi_2) = 0$ for any analytic parametrization $\varphi = (\varphi_0, \varphi_1, \varphi_2)$ at $\mathfrak{p}_i = (\alpha_i, \alpha_i, 1)$, it is easily seen that

$$\operatorname{ord}_{\mathfrak{p}_i,\varphi}(X - \alpha_i Z) = \operatorname{ord}_{\mathfrak{p}_i,\varphi}(Y - \alpha_i Z), \tag{3.1.2}$$

hence

$$\operatorname{ord}_{\mathfrak{p}_i,\varphi}(X - Y) = \operatorname{ord}_{\mathfrak{p}_i}(X - \alpha_i Z - (Y - \alpha_i Z)) \geq \operatorname{ord}_{\mathfrak{p}_i,\varphi}(X - \alpha_i Z) \tag{3.1.3}$$

and

$$\operatorname{ord}_{\mathfrak{p}_i,\varphi}((X - \alpha_i Z)^{\mu_i - 1} + \cdots + (Y - \alpha_i Z)^{\mu_i - 1}) \geq (w_i - 1) \operatorname{ord}_{\mathfrak{p}_i,\varphi}(X - \alpha_i Z). \tag{3.1.4}$$

By Euler's Theorem the condition $F(X,Y,Z) = 0$ is equivalent to

$$X \frac{\partial F}{\partial X} + Y \frac{\partial F}{\partial Y} + Z \frac{\partial F}{\partial Z} = 0.$$

The (Zariski) tangent space of C is defined by the equations $F(X,Y,Z) = 0$ and

$$dX \frac{\partial F}{\partial X} + dY \frac{\partial F}{\partial Y} + dZ \frac{\partial F}{\partial Z} = 0.$$

Then by Cramer's rule

$$\gamma := \frac{W(X,Y)}{\frac{\partial F}{\partial Z}} = \frac{W(Y,Z)}{\frac{\partial F}{\partial X}} = \frac{W(Z,X)}{\frac{\partial F}{\partial Y}} \tag{3.1.5}$$

is a well defined rational 1-form on $\pi^{-1}(C)$ ($\pi : \mathbf{K}^3 \setminus \{0\} \to \mathbf{P}^2$ is the usual projection), where

$$W(X,Y) = \begin{vmatrix} X & Y \\ dX & dY \end{vmatrix}, \quad W(Y,Z) = \begin{vmatrix} Y & Z \\ dY & dZ \end{vmatrix}, \quad W(Z,X) = \begin{vmatrix} Z & X \\ dZ & dX \end{vmatrix}$$

are the Wronskians.

LEMMA 1. *Let P be a polynomial satisfying Hypothesis* I *and m_i be arranged in non-increasing order. Then any irreducible component of C admits a non-trivial regular* 1*-form in the following cases*:

(i) $l \geq 3$, *or* $l = 2$ *and* $m_2 \geq 2$;
(ii) $p > 0$, $l = 2$, $m_2 = 1$, $\mu_1 \leq m_1$, *and the curve C has no linear components*;
(iii) $p > 0$, $l = 1$, $\mu_1 \leq m_1 - 1$, *and the curve C has no linear components.*

Proof. Differentiating and restricting to the curve $C = [F(X,Y,Z) = 0]$ yields

$$\frac{\partial F}{\partial X}(X,Y,Z) = \frac{aZ^{n-1-\sum_{i=1}^{l} m_i}\prod_{i=1}^{l}(X-\alpha_i Z)^{m_i}}{X-Y},$$
$$\frac{\partial F}{\partial Y}(X,Y,Z) = \frac{-aZ^{n-1-\sum_{i=1}^{l} m_i}\prod_{i=1}^{l}(Y-\alpha_i Z)^{m_i}}{X-Y}.$$

By (3.1.5) and canceling out the common factors, we get the following rational 1-form:

$$\eta = \frac{W(Y,Z)}{\prod_{i=1}^{l}(X-\alpha_i Z)^{m_i}} = \frac{-W(X,Z)}{\prod_{i=1}^{l}(Y-\alpha_i Z)^{m_i}}, \tag{3.1.6}$$

well defined on $\pi^{-1}(C)$. Observe that η does not have any pole along $[Z=0]$ (because, as the line $Z=0$ is not an irreducible component of C, this would mean that $X=Y=0$ as well). On the finite part of C (i.e., $Z \neq 0$) the only possible poles of η (on $\pi^{-1}(C)$) are the pull-back of the set $\{(\alpha_i,\alpha_j,1) \in C \mid 1 \le i,j \le l\}$ and Hypothesis I implies that $\alpha_i = \alpha_j$. Let $m = 1 + \sum_{i=1}^{l} m_i$ and

$$\omega := \frac{(X-Y)^{m-3}}{\prod_{i=1}^{l}(X-\alpha_i Z)^{m_i}}\, W(Y,Z) = (X-Y)^{m-3}\eta,$$

which is well defined on the curve C and has a possible pole at $\mathfrak{p}_i = (\alpha_i,\alpha_i,1)$, $1 \le i \le l$, along C. Moreover, one can see from (3.1.3) that for each $j = 1,\dots,l$,

$$\operatorname{ord}_{\mathfrak{p}_j,\varphi}\omega \ge (m-3-m_j)\operatorname{ord}_{\mathfrak{p}_j,\varphi}(X-\alpha_j Z) = \Big(\Big(\sum_{i\neq j}^{l} m_i\Big)-2\Big)\operatorname{ord}_{\mathfrak{p}_j,\varphi}(X-\alpha_j Z),$$

which is ≥ 0 if $l \ge 3$ or $l = 2$ and $m_2 \ge 2$. Therefore, ω is a regular 1-form on C in these cases. It is easy to see that $X-Y$ is not a factor of $F(X,Y,Z)$. This completes the proof of (i).

For (ii), suppose that the multiplicity μ_1 of $X-\alpha_1$ in $P(X)-P(\alpha_1)$ is no greater than m_1; then μ_1 is divisible by p and can be written as $\mu_1 = p^a b$ with $a,b \ge 1$, $p \nmid b$. Consider the form

$$\omega := \frac{W(Y,Z)(X-Y)^{p^a-1}((X-\alpha_1 Z)^{b-1}+\dots+(Y-\alpha_1 Z)^{b-1})^{p^a}}{(X-\alpha_1 Z)^{p^a b}(X-\alpha_2 Z)},$$

which is well defined on $\mathbf{P}^2$. Since $m_1 \ge p^a b$ we can write ω as a product of η and a polynomial:

$$\omega = (X-Y)^{p^a-1}((X-\alpha_1 Z)^{b-1}+\dots+(Y-\alpha_1 Z)^{b-1})^{p^a}(X-\alpha_1 Z)^{m_1-p^a b}\eta,$$

hence the poles of ω are poles of η. By (3.1.4), $(\alpha_1,\alpha_1,1)$ is not a pole of ω and, by (3.1.3), $(\alpha_2,\alpha_2,1)$ is not a pole of ω either. Thus ω is regular on C.

If the curve C has no linear components, then ω is a non-trivial regular 1-form on every component of C.

We now consider case (iii), where $l = 1$ and $\mu_1 \leq m_1 - 1$. Similarly, we may write $\mu_1 = p^a b$ with $a, b \geq 1$, $p \nmid b$. Let $w_1 - 1$ be the degree of the second term in (3.1.1). If $w_1 \neq m_1 + 1$, then w_1 is divisible by p, hence $w_1 - \mu_1 \geq 2$. If $w_1 = m_1 + 1$, then we also have $w_1 - \mu_1 \geq 2$ since $\mu_1 \leq m_1 - 1$. We infer from (3.1.4) that

$$\begin{aligned}\omega &:= \frac{W(Y,Z)(X-Y)^{p^a-1}((X-\alpha_1 Z)^{b-1} + \cdots + (Y-\alpha_1 Z)^{b-1})^{p^a}}{(X-\alpha_1 Z)^{\mu_1+1}} \\ &= (X-Y)^{p^a-1}((X-\alpha_1 Z)^{b-1} + \cdots + (Y-\alpha_1 Z)^{b-1})^{p^a}(X-\alpha_1 Z)^{m_1-\mu_1-1}\eta\end{aligned}$$

is regular on the curve C. Moreover, it is non-trivial on every component of C if C has no linear components. ∎

3.2. *On the curve* $[F_c(X,Y,Z) = 0], c \neq 0, 1$. We shall establish the results of Section 3.1 on the curve $[F_c(X,Y,Z) = 0]$.

As in the previous subsection, we see that

$$\gamma := \frac{W(Y,Z)}{\frac{\partial F_c}{\partial X}} = \frac{W(Z,X)}{\frac{\partial F_c}{\partial Y}} = \frac{W(X,Y)}{\frac{\partial F_c}{\partial Z}}$$

is a well defined rational 1-form on $\pi^{-1}(C_c)$ ($\pi : \mathbf{K}^3 \setminus \{0\} \to \mathbf{P}^2$ is the usual projection). Differentiation yields on $C_c = [F_c(X,Y,Z) = 0]$:

$$\frac{\partial F_c}{\partial X}(X,Y,Z) = aZ^{n-1-\sum_{i=1}^{l} m_i} \prod_{i=1}^{l} (X - \alpha_i Z)^{m_i},$$

$$\frac{\partial F_c}{\partial Y}(X,Y,Z) = -caZ^{n-1-\sum_{i=1}^{l} m_i} \prod_{i=1}^{l} (Y - \alpha_i Z)^{m_i}.$$

Consider the rational 1-form (well defined on $\pi^{-1}(C_c)$)

$$\eta := \frac{W(Y,Z)}{(X-\alpha_1 Z)^{m_1} \cdots (X-\alpha_l Z)^{m_l}} \equiv \frac{W(Z,X)}{-c(Y-\alpha_1 Z)^{m_1} \cdots (Y-\alpha_l Z)^{m_l}}. \tag{3.2.1}$$

We see again that there are no poles along $[Z = 0] \cap \pi^{-1}(C_c)$. Let

$$l_0 := \#\{(i,j) \mid P(\alpha_i) = cP(\alpha_j)\}.$$

Since $P(X)$ satisfies Hypothesis I, it is easy to see that $0 \leq l_0 \leq l$, and $l_0 = l$ if and only if there exists a permutation ϕ of $\{1, \ldots, l\}$ such that $(\alpha_i, \alpha_{\phi(i)}, 1) \in C_c$ for any $i = 1, \ldots, l$, i.e.,

$$\frac{P(\alpha_1)}{P(\alpha_{\phi(1)})} = \frac{P(\alpha_2)}{P(\alpha_{\phi(2)})} = \cdots = \frac{P(\alpha_l)}{P(\alpha_{\phi(l)})} = c.$$

Therefore, η has at most l_0 possible poles at $(\alpha_i, \alpha_j, 1)$ with $P(\alpha_i) = cP(\alpha_j)$ along the curve C_c. For simplicity of notation, in what follows ϕ *will always be a permutation of* $(1, \dots, l)$ *such that* $\phi(i) = j$ *if* $P(\alpha_i) = cP(\alpha_j)$.

We shall need the following:

PROPOSITION 1. *Let P be a polynomial satisfying Hypothesis* I, *and ϕ be a permutation of $\{1, \dots, l\}$ such that $\phi(i) = j$ if $P(\alpha_i) = cP(\alpha_j)$. If there exists $1 \leq i \leq l$ such that $|m_i - m_{\phi(i)}| \geq 2$, then every irreducible component of C_c admits a non-trivial regular* 1*-form.*

Proof. Without loss of generality, we may assume that $m_i - m_{\phi(i)} \geq 2$. Let

$$\omega := \frac{W(Y, Z)(Y - \alpha_{\phi(i)} Z)^{m_i - 2}}{(X - \alpha_i Z)^{m_i}},$$

which is well defined on $\mathbf{P}^2$. By (3.2.1), along the curve C_c, ω has only possible poles at $(\alpha_i, \alpha_j, 1)$, $j \neq i$. Since P satisfies Hypothesis I, from the definition of the permutation ϕ we see that if $P(\alpha_i) \neq cP(\alpha_{\phi(i)})$ then $(\alpha_i, \alpha_j, 1) \notin C_c$ for each $j \neq i$. Therefore, ω is regular on the curve C_c. Otherwise, from the relation

$$\begin{aligned} &\frac{W(Y, Z)(Y - \alpha_{\phi(i)} Z)^{m_i - 2}}{(X - \alpha_i Z)^{m_i}} \\ &\qquad = (Y - \alpha_{\phi(i)} Z)^{m_i - m_{\phi(i)} - 2} \, \frac{W(Y, Z)(Y - \alpha_{\phi(i)} Z)^{m_{\phi(i)}}}{(X - \alpha_i Z)^{m_i}} \end{aligned}$$

and $m_i - m_{\phi(i)} \geq 2$, we see that a pole of ω is also a pole of

$$\frac{W(Y, Z)(Y - \alpha_{\phi(i)} Z)^{m_{\phi(i)}}}{(X - \alpha_i Z)^{m_i}},$$

which is however regular on C_c by (3.2.1) and Hypothesis I. It is easy to see that C_c has no factor of the form $aY - bZ$, hence $W(Y, Z) \not\equiv 0$. This implies that ω is non-trivial on any component of C_c. ∎

REMARK. A similar result was obtained in [9] using the truncated second main theorem for rational functions of [10] and [11]. The proof above using the construction of a regular 1-form is much simpler.

Let $\mathfrak{p}_i = (\alpha_i, \alpha_{\phi(i)}, 1)$ and $\mathfrak{p}_j = (\alpha_j, \alpha_{\phi(j)}, 1)$ be distinct points in $\mathbf{P}^2$. Let L_{ij} be the linear form defined as follows:

$$L_{ij} := (Y - \alpha_{\phi(j)} Z) - \frac{\alpha_{\phi(i)} - \alpha_{\phi(j)}}{\alpha_i - \alpha_j} \, (X - \alpha_j Z). \tag{3.2.2}$$

In other words, $[L_{ij} = 0]$ is the line passing through $\mathfrak{p}_i$ and $\mathfrak{p}_j$. Thus L_{ij} is also equal to

$$(Y - \alpha_{\phi(i)} Z) - \frac{\alpha_{\phi(i)} - \alpha_{\phi(j)}}{\alpha_i - \alpha_j} \, (X - \alpha_i Z).$$

It is clear from the definition that

$$(3.2.3)\quad \operatorname{ord}_{\mathfrak{p}_i,\varphi} L_{ij} \geq \min\{\operatorname{ord}_{\mathfrak{p}_i,\varphi}(X-\alpha_i Z), \operatorname{ord}_{\mathfrak{p}_i,\varphi}(Y-\alpha_{\phi(i)} Z)\}$$

and

$$(3.2.4)\quad \operatorname{ord}_{\mathfrak{p}_j,\varphi} L_{ij} \geq \min\{\operatorname{ord}_{\mathfrak{p}_j,\varphi}(X-\alpha_j Z), \operatorname{ord}_{\mathfrak{p}_j,\varphi}(Y-\alpha_{\phi(j)} Z)\}.$$

LEMMA 2. *Let P be a polynomial satisfying Hypothesis* I *and m_i be arranged in non-increasing order. If the curve C_c has no linear factor then any irreducible component of C_c admits a non-trivial regular* 1*-form except in the following cases*:

(i) $l = l_0 = 3$ *and* $m_1 = m_2 = m_3 = 1$;
(ii) $l = 2$ *and* $m_1 = m_2 = 1$ *and* $l_0 = 1, 2$;
(iii) $l = 1$ *and* $m_1 = 1$.

Proof. If $l = 1$, it is clear that η has no pole on $\pi^{-1}(C_c)$. Therefore

$$\omega := \frac{W(Y,Z)}{(X-\alpha_1 Z)^2} = (X-\alpha_1 Z)^{m_1-2}\eta$$

is well defined and regular on C_c if $m_1 \geq 2$. It is easy to see that $[X - \alpha_1 Z = 0]$ is not a component of C_c, thus ω is non-trivial on any irreducible component of C_c.

We now assume that $l \geq 2$. If $m_2 \geq 2$ then $m_1 + m_2 - 2 \geq m_1 \geq m_i$ for $1 \leq i \leq l$. The only possible poles of the 1-form

$$\omega := \frac{W(Y,Z)L_{12}^{m_1+m_2-2}}{(X-\alpha_1 Z)^{m_1}(X-\alpha_2 Z)^{m_2}}$$

on the curve C_c are $\mathfrak{p}_i = (\alpha_i, \alpha_{\phi(i)}, 1)$, $i = 1, 2$. If $\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z) \leq \operatorname{ord}_{\mathfrak{p}_1,\varphi}(Y-\alpha_{\phi(1)} Z)$ then $\operatorname{ord}_{\mathfrak{p}_1,\varphi} L_{12} = \operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)$. Therefore, as $m_1 + m_2 - 2 \geq m_1$, ω is regular at $\mathfrak{p}_1$. If $\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z) > \operatorname{ord}_{\mathfrak{p}_1,\varphi}(Y-\alpha_{\phi(1)} Z)$ then $\operatorname{ord}_{\mathfrak{p}_1,\varphi} L_{12} = \operatorname{ord}_{\mathfrak{p}_1,\varphi}(Y-\alpha_{\phi(1)} Z)$. By (3.2.1), on $\pi^{-1}(C_c)$ we have

$$\frac{W(Y,Z)(Y-\alpha_{\phi(1)}Z)^{m_{\phi(1)}}}{(X-\alpha_1 Z)^{m_1}} \equiv \frac{W(Z,X)(X-\alpha_2 Z)^{m_2}\cdots(X-\alpha_l Z)^{m_l}}{-c(Y-\alpha_{\phi(2)}Z)^{m_{\phi(2)}}\cdots(Y-\alpha_{\phi(l)}Z)^{m_{\phi(l)}}},$$

which is regular at $\pi^{-1}(\mathfrak{p}_1)$. The regularity of ω follows from this because $m_1+m_2-2 \geq m_{\phi(1)}$ and $\operatorname{ord}_{\mathfrak{p}_1,\varphi} L_{12} = \operatorname{ord}_{\mathfrak{p}_1}(Y-\alpha_{\phi(1)}Z)$. The regularity of ω at $\mathfrak{p}_2$ is similarly established. Therefore ω is regular on C_c and is non-trivial on any component of C_c provided that it has no linear component.

It remains to consider the case $m_2 = 1$. Then $p \neq 2$ and $m_i = 1$ for any $i = 2, \ldots, l$. By Proposition 1, we only need to consider the cases $m_1 = 1$ and $m_1 = 2$. First, we suppose that $m_1 = 2$. Since $p \neq 2$, $\mu_1 = m_1 + 1 = 3$. Similarly, we have $\mu_{\phi(1)} = m_{\phi(1)} + 1 = 2$, since $\phi(1) \neq 1$ and $m_i = 1$ for any

$i = 2, \dots, l$. Let

$$\omega := \frac{W(Y,Z)L_{12}}{(X-\alpha_1 Z)^2(X-\alpha_2 Z)},$$

which is well defined in $\mathbf{P}^2$ and the only possible poles on the curve C_c are $\mathfrak{p}_1 = (\alpha_1, \alpha_{\phi(1)}, 1)$ and $\mathfrak{p}_2 = (\alpha_2, \alpha_{\phi(2)}, 1)$. If $\mathfrak{p}_i \notin C_c$ then, on the curve C_c, ω is regular at this point. If $\mathfrak{p}_1 \in C_c$ then from the expression of $F_c(X,Y,Z) = 0$ at $\mathfrak{p}_1$ we see readily that

$$3\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z) = 2\operatorname{ord}_{\mathfrak{p}_1,\varphi}(Y-\alpha_{\phi(1)}Z) > 0.$$

Hence,

$$2 \le \operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z) < \operatorname{ord}_{\mathfrak{p}_1,\varphi}(Y-\alpha_{\phi(1)}Z)$$

and

$$\operatorname{ord}_{\mathfrak{p}_1,\varphi} L_{12} = \operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z).$$

We infer that

$$\begin{aligned}\operatorname{ord}_{\mathfrak{p}_1,\varphi} \omega &= \operatorname{ord}_{\mathfrak{p}_1,\varphi} W(Y,Z) + \operatorname{ord}_{\mathfrak{p}_1,\varphi} L_{12} - 2\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)\\ &\ge \operatorname{ord}_{\mathfrak{p}_1,\varphi}(Y-\alpha_{\phi(1)}Z) - \operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z) - 1 \ge 0.\end{aligned}$$

Similarly, if $\mathfrak{p}_2 \in C_c$ then

$$2\operatorname{ord}_{\mathfrak{p}_2,\varphi}(X-\alpha_2 Z) = (m_{\phi(2)}+1)\operatorname{ord}_{\mathfrak{p}_2,\varphi}(Y-\alpha_{\phi(2)}Z) > 0,$$

where $m_{\phi(2)} = 1, 2$. If $m_{\phi(2)} = 1$ then we have $\operatorname{ord}_{\mathfrak{p}_2,\varphi}(Y-\alpha_{\phi(2)}Z) = \operatorname{ord}_{\mathfrak{p}_2,\varphi}(X-\alpha_2 Z)$ and ω is clearly regular at $\mathfrak{p}_2$. If $m_{\phi(2)} = 2$ then $3\operatorname{ord}_{\mathfrak{p}_2,\varphi}(Y-\alpha_{\phi(2)}Z) = 2\operatorname{ord}_{\mathfrak{p}_2,\varphi}(X-\alpha_2 Z) > 0$ and ω is also regular at $\mathfrak{p}_2$. Finally, we consider the case $m_1 = 1$. If $l_0 \le l-2$ then we may assume that $(\alpha_1, \alpha_j, 1)$ and $(\alpha_2, \alpha_j, 1)$ are not in C_c for any $1 \le j \le l$. This implies that the 1-form

$$\omega := \frac{W(Y,Z)}{(X-\alpha_1 Z)(X-\alpha_2 Z)}$$

is regular on C_c by (3.2.1). If $l_0 = l-1$, we may assume that $(\alpha_1, \alpha_j, 1) \notin C_c$ for any $1 \le j \le l$ and $(\alpha_i, \alpha_{\phi(i)}, 1) \in C_c$ for $2 \le i \le l$. Suppose that $l \ge 3$; then

$$\omega := \frac{W(Y,Z)L_{23}}{(X-\alpha_1 Z)(X-\alpha_2 Z)(X-\alpha_3 Z)}$$

is well defined and regular on C_c. If $l_0 = l$, we need $l \ge 4$, and

$$\omega := \frac{W(Y,Z)L_{12}L_{34}}{(X-\alpha_1 Z)(X-\alpha_2 Z)(X-\alpha_3 Z)(X-\alpha_4 Z)}$$

is regular on C_c. Since C_c has no linear component, the restriction of ω to any of its components is non-trivial by construction. ∎

Remark. In [9], there is another exceptional case: $n = 5$, $l = l_0 = 2$, $m_1 = m_2 = 2$ and $\mu_i = m_i + 1$. This case actually can be eliminated since $X + Y - \alpha_1 Z - \alpha_2 Z$ is a linear factor of C_c, which means that S is not affine rigid.

3.3. *Proof of Theorem 1.* The curve in the following lemma is one of the exceptional cases in our results.

LEMMA 3. *Let λ_1, λ_2 be non-zero constants and b be a positive integer. Let*

$$A(X,Y,Z) \\ = \lambda_1\left[\frac{(X-\alpha Z)^b-(Y-\alpha Z)^b}{X-Y}\right]Z+\lambda_2\left[\frac{(X-\alpha Z)^{b+1}-(Y-\alpha Z)^{b+1}}{X-Y}\right].$$

Then $[A(X,Y,Z)=0]$ is an irreducible curve of genus 0.

Proof. Without loss of generality, we may assume that $\alpha=0$ by taking a linear transformation. Then

$$A(X,Y,Z)=\lambda_1\left[\frac{X^b-Y^b}{X-Y}\right]Z+\lambda_2\left[\frac{X^{b+1}-Y^{b+1}}{X-Y}\right].$$

If $A(X,Y,Z)$ is reducible, then $b\geq 2$ and it can only be factored as

$$A(X,Y,Z)=[H_j(X,Y)Z+H_{j+1}(X,Y)]G_{b-1-j}(X,Y),$$

where H_j, H_{j+1} and G_{b-1-j} are homogeneous polynomials in X and Y of degree j, $j+1$, $b-j-1$ respectively. From the expression of $A(X,Y,Z)$, we have

$$G_{b-1-j}(X,Y)\,\Bigg|\,\left[\frac{X^{b+1}-Y^{b+1}}{X-Y}\right] \quad\text{and}\quad G_{b-1-j}(X,Y)\,\Bigg|\,\left[\frac{X^b-Y^b}{X-Y}\right].$$

Since $\gcd(b,b+1)=1$, this is impossible unless $G_{b-1-j}(X,Y)$ is constant. Therefore, this curve is irreducible.

It is clear that this curve has only one multiple point $(0,0,1)$ of multiplicity $b-1$. The deficiency is

$$\delta_A=\frac{(\deg A-1)(\deg A-2)}{2}-\frac{(b-1)(b-2)}{2}=0.$$

Therefore the genus is 0. ∎

We are now in a position to prove Theorem 1. As indicated at the beginning of this section, $P(X)$ is a uniqueness polynomial for meromorphic functions if the curve C admits a regular 1-form non-trivial on each of its components; and $P(X)$ is a strong uniqueness polynomial for meromorphic functions if the curve C and each C_c, $c\neq 0,1$, admit a regular 1-form non-trivial on each of their components. Therefore by Lemma 1, $P(X)$ is a uniqueness polynomial if its zero set S is affinely rigid except when (i) $l=1$ and $\mu_1=m_1$, (ii) $l=1$ and $\mu_1=m_1+1$, or (iii) $l=2$, $\min\{m_1,m_2\}=m_2=1$ and $\mu_i=m_i+1$ for $i=1,2$. Since $p\nmid n$, $n=(\sum_{i=1}^{l}m_i)+1$. Therefore, $n=m_1+1$ in cases (i), (ii), and $n=m_1+2$ in case (iii). Hence, one can easily see that the curve C in case (i) is defined by

$$F(X,Y,Z) = *\left[\frac{(X-\alpha_1 Z)^{m_1} - (Y-\alpha_1 Z)^{m_1}}{X-Y}\right]Z + *\left[\frac{(X-\alpha_1 Z)^{m_1+1} - (Y-\alpha_1 Z)^{m_1+1}}{X-Y}\right].$$

Therefore, C is irreducible and its genus is 0 by Lemma 3.

In case (ii), the curve C is defined by

$$F(X,Y,Z) = *\left[\frac{(X-\alpha_1 Z)^{m_1+1} - (Y-\alpha_1 Z)^{m_1+1}}{X-Y}\right],$$

which can be factorized into linear components. Therefore S is not affinely rigid.

In case (iii), the curve C is defined by

$$F(X,Y,Z) = *\left[\frac{(X-\alpha_1 Z)^{m_1+1} - (Y-\alpha_1 Z)^{m_1+1}}{X-Y}\right]Z + *\left[\frac{(X-\alpha_1 Z)^{m_1+2} - (Y-\alpha_1 Z)^{m_1+2}}{X-Y}\right].$$

Therefore, C is irreducible and its genus is 0 by Lemma 3.

Similarly, by Lemmas 1 and 2, $P(X)$ is a strong uniqueness polynomial if its zero set S is affinely rigid except for cases (i)–(iii) above and (iv) $l = l_0 = 3$ and $m_1 = m_2 = m_3 = 1$. We have checked that $P(X)$ is not a uniqueness polynomial in the cases (i)–(iii). For case (iv), we have $n = 4$, and

$$\frac{P(\alpha_1)}{P(\alpha_{\phi(1)})} = \frac{P(\alpha_2)}{P(\alpha_{\phi(2)})} = \frac{P(\alpha_3)}{P(\alpha_{\phi(3)})} = w,$$

where $\{\phi(1), \phi(2), \phi(3)\} = \{1,2,3\}$ and $\phi(i) \neq i$, $i = 1,2,3$, and $w^2 + w + 1 = 0$. One checks easily that the curve $C_w = [F_w(X,Y,Z) = 0]$ is irreducible and has genus 0. Therefore, $P(X)$ is not a strong uniqueness polynomial in this case. This completes the proof of the theorem. ■

4. Proof of Theorem 2. The situation is more complicated if $n = \deg P(X)$ is divisible by $p > 0$ due to the fact that the curves C and C_c may have singularities at infinity in this case. We are unable to find regular 1-forms, but, as we shall show, there exist products of 1-forms (i.e., sections of $\mathcal{K}_C^m$ and $\mathcal{K}_{C_c}^m$) which are regular and non-trivial on C and on each C_c, $c \neq 0, 1$. In the following we set

$$m = 1 + \sum_{i=1}^{l} m_i. \tag{4.0.1}$$

If n is divisible by p then m is clearly the largest exponent in $P(X)$ not divisible by p.

4.1. *On the curve* $[F(X,Y,Z)=0]$. Let $F(X,Y,Z)$ and all the other notation be the same as previously defined.

LEMMA 4. *Suppose that* $p>0$ *and* $p\,|\,n$. *Let* $\gcd(n,m)=d$ *and* ξ_d^j, $0\le j\le d-1$, *be the primitive roots of* $X^d=1$. *Then the only possible poles of the differential form*

$$\zeta := \frac{W(Y,Z)}{Z(X-\alpha_1 Z)^{m_1}\cdots(X-\alpha_l Z)^{m_l}}$$

on $\pi^{-1}(C)$ *are the pull-backs of* $\mathfrak{p}_i=(\alpha_i,\alpha_i,1)$, $1\le i\le l$, *and* $\mathfrak{q}_j=(\xi_d^j,1,0)$, $0\le j\le d-1$.

Proof. Since $p\,|\,n$, we have

$$\frac{\partial F}{\partial Z}(X,Y,Z)=a_m(n-m)Z^{n-m-1}\Big(\sum_{i=0}^{m-1}X^{m-1-i}Y^i+ZH_{m-2}\Big), \tag{4.1.1}$$

where H_{m-2} is a homogeneous polynomial of degree $m-2$ in X,Y,Z. Restricting $\partial F/\partial X$ and $\partial F/\partial Y$ to the curve $C=[F(X,Y,Z)=0]$ yields

$$\begin{aligned}\frac{\partial F}{\partial X}(X,Y,Z)&=\frac{ma_mZ^{n-m}\prod_{i=1}^{l}(X-\alpha_iZ)^{m_i}}{X-Y},\\ \frac{\partial F}{\partial Y}(X,Y,Z)&=\frac{-ma_mZ^{n-m}\prod_{i=1}^{l}(Y-\alpha_iZ)^{m_i}}{X-Y}.\end{aligned}$$

Together with (4.1.1) and (3.1.5), we have

$$\begin{aligned}\zeta&=\frac{W(Y,Z)}{Z(X-\alpha_1Z)^{m_1}\cdots(X-\alpha_lZ)^{m_l}}\\ &\equiv-\frac{W(Z,X)}{Z(Y-\alpha_1Z)^{m_1}\dots(Y-\alpha_lZ)^{m_l}}\\ &\equiv-\frac{W(X,Y)}{(X-Y)(X^{m-1}+X^{m-2}Y+\cdots+Y^{m-1}+ZH_{m-2})},\end{aligned} \tag{4.1.2}$$

which is a rational 1-form on $\pi^{-1}(C)$. Similarly to the proof of Lemma 1, one can easily verify that the only possible poles of ζ on $\pi^{-1}(C)$ are the pull-backs of $\mathfrak{p}_i=(\alpha_i,\alpha_i,1)$, $1\le i\le l$, and $(x,1,0)$ with $x^n=1$ and $x^m=1$. For the latter case, it is easy to see that ξ_d^j, $0\le j\le d-1$, are the only solutions satisfying $x^n=1$ and $x^m=1$. Therefore, the pull-backs of $\mathfrak{q}_j=(\xi_d^j,1,0)$, $0\le j\le d-1$, are the only possible poles of ζ along $\pi^{-1}(C)\cap[Z=0]$. ∎

Suppose that $*(X-\alpha_iZ)^v$ appears in the expression of (3.0.2), and suppose that there is a term $*(X-\alpha_iZ)^{v_1}$ following it. Let $A_{i,v-1}Z^{n-v}$ be the sum of the terms in (3.1.1) up to degree $v-1$ in X and Y, i.e.,

$$A_{i,v-1} = *\left[\frac{(X-\alpha_i Z)^{\mu_i}-(Y-\alpha_i Z)^{\mu_i}}{X-Y}\right]Z^{v-\mu_i}+\cdots + *\left[\frac{(X-\alpha_i Z)^{v}-(Y-\alpha_i Z)^{v}}{X-Y}\right]. \tag{4.1.3}$$

We have the following estimates on its order at $\mathfrak{p}_i$, which is a point of C by (3.1.1), and $\mathfrak{q}_j$.

Lemma 5. *We have*

(i) $\mathrm{ord}_{\mathfrak{p}_i,\varphi}(A_{i,v-1}) \ge v\,\mathrm{ord}_{\mathfrak{p}_i,\varphi}(X-\alpha_i Z)$;
(ii) $\mathrm{ord}_{\mathfrak{p}_r,\varphi}(A_{i,m-1}) \ge (p-1)\,\mathrm{ord}_{\mathfrak{p}_r,\varphi}(X-\alpha_r Z)$ *for* $1 \le r \le l$;
(iii) $p \mid -m\,\mathrm{ord}_{\mathfrak{q}_j,\varphi} Z + \mathrm{ord}_{\mathfrak{q}_j,\varphi}((X-Y)A_{i,m-1})$ *for* $0 \le j \le d-1$.

Proof. We first note that from (3.1.1), $\mathfrak{p}_i = (\alpha_i, \alpha_i, 1)$, $i = 1, \ldots, l$, and $\mathfrak{q}_j$, $0 \le j \le d-1$, are points of C. Moreover, (3.1.1) implies

$$\mathrm{ord}_{\mathfrak{p}_i,\varphi}(A_{i,v-1}) \ge (v_1-1)\,\mathrm{ord}_{\mathfrak{p}_i,\varphi}(X-\alpha_i Z) \ge v\,\mathrm{ord}_{\mathfrak{p}_i,\varphi}(X-\alpha_i Z).$$

This proves (i).

Since m is the largest exponent in $P(X)$ not divisible by p and n is divisible by p, we may write

$$F(X,Y,Z) = A_{i,m-1}Z^{n-m} + (X-Y)^{p-1}H(X,Y,Z),$$

where $H(X,Y,Z)$ is the homogeneous polynomial of degree $n-p$. Since $\mathfrak{p}_r = (\alpha_r, \alpha_r, 1) \in C$, this equation implies that $\mathfrak{p}_r \in [A_{i,m-1}(X,Y,Z) = 0]$ and

$$\mathrm{ord}_{\mathfrak{p}_r,\varphi}(A_{i,m-1}) \ge (p-1)\,\mathrm{ord}_{\mathfrak{p}_r,\varphi}(X-Y) \ge (p-1)\,\mathrm{ord}_{\mathfrak{p}_r,\varphi}(X-\alpha_r Z).$$

This gives (ii).

Since $(X-Y)F(X,Y,Z) - (X-Y)A_{i,m-1}Z^{n-m}$ is a pth power, for $\mathfrak{q}_j \in C$, $j = 0, \ldots, d-1$, we have

$$p \mid (n-m)\,\mathrm{ord}_{\mathfrak{q}_j,\varphi} Z + \mathrm{ord}_{\mathfrak{q}_j,\varphi}((X-Y)A_{i,m-1}),$$

which is equivalent to

$$p \mid -m\,\mathrm{ord}_{\mathfrak{q}_j,\varphi} Z + \mathrm{ord}_{\mathfrak{q}_j,\varphi}((X-Y)A_{i,m-1})$$

since n is divisible by p. This shows (iii). ∎

Lemma 6. *Let $P(X)$ be a polynomial of degree n satisfying Hypothesis* I. *Let m_i be arranged in non-increasing order. Assume that $p > 0$ and $p \mid n$. If the curve C has no linear components then any irreducible component of C admits a non-trivial regular product of* 1*-forms, i.e., elements of $H^0(C, \mathrm{sym}^i \mathcal{K}_C)$, in the following cases*:

(i) $l \ge 3$; $l = 2$ *and* $m_2 \ge 2$; $l = 2$ *and* $m_2 = 1$, *and* $\mu_1 \le m_1$; *or* $l = 1$ *and* $\mu_1 \le m_1 - 1$;
(ii) $l = 2$, $m_2 = 1$, $\mu_1 = m_1 + 1$ *and either*

(a) $(m_1+2)\nmid n$, *or*
(b) $(m_1+2)\,|\,n$ *and* A_{1,m_1+1} *is not a factor of* $F(X,Y,Z)$;

(iii) $l=1$ *and* $\mu_1=m_1$ *and either*

(a) $(m_1+1)\nmid n$, *or*
(b) $(m_1+1)\,|\,n$, $p\geq 5$, *and* A_{1,m_1} *is a factor of* $F(X,Y,Z)$;

(iv) $l=1$, $\mu_1=m_1+1$, *and either*

(a) $u=2$, $p\geq 5$, *and* A_{1,m_1+1} *is not a factor of* $F(X,Y,Z)$, *or*
(b) $u\geq 3$, *and* $m_1\geq 2$, *except when* $(m_1,p)=(2,2)$ *or* $(u,m_1,p)=(3,2,5),(3,3,3)$, *where* u *is defined by the expansion* $P(X)=P(\alpha_1)+*(X-\alpha_1)^{m_1+1}+*(X-\alpha_1)^{m_1+u}+$ *higher order terms.*

Proof. Part (i) is already covered by Lemma 1. The proof for the other cases is more involved as regards the verification of regularity of products of 1-forms; to shorten the proof we will omit some arguments that have been done in the proof of Lemma 1.

Let $m=1+\sum_{i=1}^{l}m_i$. For case (ii), we have $m=m_1+2$, $\mu_1=m_1+1$, $\mu_2=2$, and hence $p\nmid m_1+2$, $p\nmid m_1+1$, and $p\neq 2$. Moreover,

$$A_{1,m_1+1}=*Z\left[\frac{(X-\alpha_1Z)^{m_1+1}-(Y-\alpha_1Z)^{m_1+1}}{X-Y}\right]+*\left[\frac{(X-\alpha_1Z)^{m_1+2}-(Y-\alpha_1Z)^{m_1+2}}{X-Y}\right],$$

which defines an irreducible curve of genus 0 by Lemma 3. Let $e=3$ if the degree of the non-vanishing term after the degree m_1+2 in the expression of (3.0.2) is m_1+3, and $e=4$ otherwise. Take

$$\omega=\left(\frac{W(Y,Z)}{Z(X-\alpha_1Z)^{m_1}(X-\alpha_2Z)}\right)^{m_1+e}((X-Y)A_{1,m_1+1}Z^{e-2})^{m_1},$$

which is well defined on $\mathbf{P}^2$. On the curve C, ω has possible poles only at $\mathfrak{p}_j=(\alpha_j,\alpha_j,1)$, $j=1,2$, and $\mathfrak{q}_j=(\xi_d^j,1,0)$, $0\leq j\leq d-1$, with $d=\gcd(n,m_1+2)$ and ξ_d a primitive root of $X^d=1$. It is clear that ω is regular at $\mathfrak{p}_1$ since Lemma 5(i) implies that

$$\operatorname{ord}_{\mathfrak{p}_1,\varphi}A_{1,m_1+1}\geq(m_1+e-1)\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1Z).$$

By Lemma 5(ii), $\operatorname{ord}_{\mathfrak{p}_2,\varphi}A_{1,m_1+1}\geq(p-1)\operatorname{ord}_{\mathfrak{p}_2,\varphi}(X-\alpha_2Z)$, hence

$$\operatorname{ord}_{\mathfrak{p}_2,\varphi}\omega\geq(m_1p-m_1-e)\operatorname{ord}_{\mathfrak{p}_2,\varphi}(X-\alpha_2Z)\geq m_1(p-1)-4\geq 0$$

as $p\geq 3$ or $p=3$ and $m_1\geq 2$. We note that if $p=3$, then $m_1\neq 1$ since $p\nmid m_1+2$. Therefore, this shows that ω is regular at $\mathfrak{p}_2$. For the points at infinity $\mathfrak{q}_j$, $j=0,\ldots,d-1$, observe that

$$\operatorname{ord}_{\mathfrak{q}_j,\varphi}(A_{1,m_1+1}(X-Y))+\operatorname{ord}_{\mathfrak{q}_j,\varphi}Z\geq 3, \tag{4.1.4}$$

for if $\operatorname{ord}_{\mathfrak{q}_j,\varphi} A_{1,m_1+1}(X-Y) = \operatorname{ord}_{\mathfrak{q}_j,\varphi} Z = 1$ then Lemma 5(iii) implies $m-1 = m_1+1$ is divisible by p, which is impossible. Similarly if $m_1 = 1$ and $\operatorname{ord}_{\mathfrak{q}_j,\varphi} Z = 1$ then Lemma 5(iii) implies that $-3+\operatorname{ord}_{\mathfrak{q}_j,\varphi} A_{1,m_1+1}(X-Y)$ is divisible by p, hence $\operatorname{ord}_{\mathfrak{q}_j,\varphi} A_{1,m_1+1}(X-Y) \geq 3$. Therefore, we get

$$\text{(4.1.5)} \qquad \operatorname{ord}_{\mathfrak{q}_j,\varphi}(A_{1,m_1+1}(X-Y)) + 2\operatorname{ord}_{\mathfrak{q}_j,\varphi} Z \geq 5 \quad \text{ if } m_1 = 1.$$

Moreover, if $m_1 = 1$ then we may take $e = 4$ since the degree of the non-vanishing term following the degree 3 term cannot be 4; otherwise p would be 2. In this case we get

$$\begin{aligned}\operatorname{ord}_{\mathfrak{q}_j,\varphi} \omega &\geq -(m_1+e) + m_1 \operatorname{ord}_{\mathfrak{q}_j,\varphi}(A_{1,m_1+1}(X-Y)) + m_1(e-2)\operatorname{ord}_{\mathfrak{q}_j,\varphi} Z \\ &\geq m_1[\operatorname{ord}_{\mathfrak{q}_j,\varphi}(A_{1,m_1+1}(X-Y)) + (e-2)\operatorname{ord}_{\mathfrak{q}_j,\varphi} Z - 1] - e.\end{aligned}$$

By (4.1.4) this implies that $\operatorname{ord}_{\mathfrak{q}_j,\varphi} \omega \geq 2m_1 - 4$, which is non-negative if $m_1 \geq 2$. If $m_1 = 1$, then $e = 4$ and the preceding inequality implies that

$$\operatorname{ord}_{\mathfrak{q}_j,\varphi} \omega \geq \operatorname{ord}_{\mathfrak{q}_j,\varphi}(A_{1,m_1+1}(X-Y)) + 2\operatorname{ord}_{\mathfrak{q}_j,\varphi} Z - 5,$$

which is also non-negative by (4.1.5). This concludes the proof that ω is regular on C. We also need to check if ω is non-trivial on every component of C. For this, we will have to check if $[A_{1,m_1+1} = 0]$ is a component of C since it is an irreducible curve of genus 0. Suppose that $(m_1+2) \nmid n$ and $A_{1,m_1+1} \mid F(X,Y,Z)$. Then $(X-Y)A_{1,m_1+1} \mid (X-Y)F(X,Y,Z)$ and we see, by evaluating at $Z=0$, that $(X^{m_1+2} - Y^{m_1+2}) \mid (X^n - Y^n)$. Let ξ be a primitive root of $X^{m_1+2} = 1$ in $\mathbf{K}$. If $(X^{m_1+2} - Y^{m_1+2}) \mid (X^n - Y^n)$ then $(\xi, 1)$ is also a solution of $X^n - Y^n$ and so $1 = \xi^n$, which is impossible if $(m_1+2) \nmid n$. The proof breaks down if $(m_1+2) \mid n$ so it is necessary to assume, in this case, that A_{1,m_1+1} is not a factor of $F(X,Y,Z)$.

For (iii), we have $l = 1$ and $\mu_1 = m_1 = m-1$. Then m_1 is divisible by p and can be written as $m_1 = p^a b$ with $a, b \geq 1$. If $\gcd(n,m) = 1$, then

$$\omega := \frac{W(Y,Z)(X-Y)^{p^a-1}((X-\alpha_1 Z)^{b-1} + \cdots + (Y-\alpha_1 Z)^{b-1})^{p^a}}{Z(X-\alpha_1 Z)^{m_1}}$$

is regular and non-trivial on any component of C if it has no linear components.

If $1 < \gcd(n,m) = d < m$, we may write $m = m_0 d$ with $m_0 \geq 2$ and $d \geq 2$. Then $m-d-2 = (m_0-1)d - 2 \geq 0$. Let

$$\omega := \left(\frac{W(Y,Z)(X^d - Y^d)}{Z(X-\alpha_1 Z)^{m_1}}\right)^{m_1} A_{1,m_1}^{m_1-d-1}.$$

Since $\mu_1 = m_1$,

$$\begin{aligned}A_{1,m_1} = {}&{*}Z\left[\frac{(X-\alpha_1 Z)^{m_1} - (Y-\alpha_1 Z)^{m_1}}{X-Y}\right] \\ &+ *\left[\frac{(X-\alpha_1 Z)^{m_1+1} - (Y-\alpha_1 Z)^{m_1+1}}{X-Y}\right],\end{aligned}$$

which again defines an irreducible curve of genus 0. Similarly, ω has only a possible pole at $\mathfrak{p}_1$. Since m_1 is divisible by p, the degree of the term appearing after $(X-\alpha_1)^{m_1+1}$ in (3.0.2) is at least m_1+p. Note that such a term must exist since $p\nmid m$ and $p\,|\,n$. By Lemma 5(i) we see that

$$\operatorname{ord}_{\mathfrak{p}_1,\varphi} A_{1,m_1} \geq (m_1+p)\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z),$$

thus

$$\begin{aligned}\text{(4.1.6)}\quad \operatorname{ord}_{\mathfrak{p}_1,\varphi}\omega &\geq [(m_1-d-1)(m_1+p)-m_1(m_1-d)]\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)\\ &= [d(pm_0-m_0-p)-2p+1]\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z).\end{aligned}$$

If $p=2$ then since $p\nmid m_1+1$ we have $m_0\geq 3$ and $d\geq 3$. Thus, by (4.1.6), $\operatorname{ord}_{\mathfrak{p}_1,\varphi}\omega$ is non-negative. If $m_0\geq 3$ and $p\geq 3$ then, by (4.1.6), $\operatorname{ord}_{\mathfrak{p}_1,\varphi}\omega\geq 2(2p-3)-2p+1=2p-5$, which is positive. It remains to check the case $m_0=2$ and $p\geq 3$. Since $p\,|\,m-1$, if $m_0=2$ and $p\geq 5$ then $d\geq 3$, and (4.1.6) implies that $\operatorname{ord}_{\mathfrak{p}_1,\varphi}\omega$ is positive. Similarly, if $m_0=2$ and $p=3$, then d can only be 2 or greater than 5. The latter case still implies that $\operatorname{ord}_{\mathfrak{p}_1,\varphi}\omega$ is non-negative. Thus, the only remaining case to be checked is $m_0=2, p=3$ and $d=2$. In this case we have

$$\omega=\frac{W(Y,Z)(X^2-Y^2)}{Z(X-\alpha_1 Z)^3}.$$

The expansion of $F(X,Y,Z)$ at $\mathfrak{p}_1=(\alpha_1,\alpha_1,1)$ is given by

$$*(X-Y)^2+*\sum_{i=0}^{3}(X-\alpha_1 Z)^{3-i}(Y-\alpha_1 Z)^i+\text{ higher order terms},$$

which implies that

$$2\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-Y)=3\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z).$$

This means that $\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)\geq 2$ and that

$$\begin{aligned}\operatorname{ord}_{\mathfrak{p}_1,\varphi}\omega &\geq \operatorname{ord}_{\mathfrak{p}_1,\varphi}(X+Y)+\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-Y)-2\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)-1\\ &\geq \frac{1}{2}\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)-1\geq 0.\end{aligned}$$

Thus regularity is established in every case. Since $[A_{1,m_1}=0]$ is an irreducible curve of genus 0, we conclude that ω is non-trivial on any component of C provided that A_{1,m_1} is not a factor of $F(X,Y,Z)$. Moreover, as $m=m_1+1$ and $A_{1,m_1}=A_{1,m-1}$, we conclude as before that $A_{1,m-1}$ is not a factor of $F(X,Y,Z)$ if $m\nmid n$.

For (iii.b), we have $m\,|\,n$ and $\mu_1=m_1=m-1$. Assume that $p\geq 5$. Let m_1+u ($\geq m_1+2$) be the degree of the non-vanishing term next to $(X-\alpha_1)^m$ in the expansion of $P(X)$ in (3.0.2). Since $p\,|\,m_1$ and $p\geq 5$, we have $p\,|\,u$, $m_1 \geq 5$ and $u \geq 5$. Then

$$\omega := \left(\frac{W(Y,Z)}{Z(X-\alpha_1 Z)^{m_1}}\right)^{m_1+u} (A_{1,m_1}(X-Y))^{m_1} Z^{(u-2)(m_1-1)-2}$$

is regular at $\mathfrak{p}_1$. This follows easily from the inequalities

$$\begin{aligned}
&(u-2)(m_1-1)-2 \geq 0,\\
&\operatorname{ord}_{\mathfrak{p}_1,\varphi} A_{1,m_1} \geq (m_1+u-1)\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z),\\
&\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-Y) \geq \operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z).
\end{aligned}$$

At the points at infinity $\mathfrak{q}_j$, $j = 0,1,\ldots,m-1$, we have (as $u \geq 5$ and $m_1 \geq 5$)

$$\begin{aligned}
\operatorname{ord}_{\mathfrak{q}_j,\varphi}\,\omega &\geq ((u-2)(m_1-1)-2)\operatorname{ord}_{\mathfrak{q}_j,\varphi} Z\\
&\qquad + m_1 \operatorname{ord}_{\mathfrak{q}_j,\varphi}(A_{1,m_1}(X-Y)) - m_1 - u\\
&\geq (u-2)m_1 - u - u = (u-2)(m_1-2) - 4 \geq 0.
\end{aligned}$$

Since $[A_{1,m_1} = 0]$ is an irreducible curve of genus 0, ω is regular and non-trivial on any component of C only if A_{1,m_1} is not a factor of $F(X,Y,Z)$.

For (iv.a), we have $l = 1$, $\mu_1 = m_1 + 1 = m$ and $u = 2$, where $m_1 + u$ ($\geq m_1 + 2$) is the degree of the non-vanishing term following $(X-\alpha_1)^m$ in the expansion of $P(X)$ in (3.0.2). Similarly, in this case

$$\begin{aligned}
A_{1,m_1+1} = {*}Z&\left[\frac{(X-\alpha_1 Z)^{m_1+1} - (Y-\alpha_1 Z)^{m_1+1}}{X-Y}\right]\\
&+ {*}\left[\frac{(X-\alpha_1 Z)^{m_1+2} - (Y-\alpha_1 Z)^{m_1+2}}{X-Y}\right],
\end{aligned}$$

which gives an irreducible curve of genus 0. If $n = m_1+2$ then $F(X,Y,Z) = A_{1,m_1+1}$. Hence the curve C is irreducible and has genus 0. If $n \geq m_1 + 3$ then there is a non-vanishing term following $(X-\alpha_1)^{m_1+2}$ in the expansion of $P(X)$ in (3.0.2) with degree $v > m_1 + 2$. Since $p\,|\,m_1+2$ and $p\,|\,v$, we have $v \geq m_1+2+p$ and $\operatorname{ord}_{\mathfrak{p}_1,\varphi} A_{1,m_1+1} \geq (m_1+1+p)\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)$ by Lemma 5(i). Observe that the condition $p\,|\,m_1+2$ implies that $m_1 \geq p-2$, hence $m_1 \geq 3$ and $m_1 - 2 \geq p - 4 \geq 1$ if $p \geq 5$. From this, it is easy to see that $(m_1-2)(p-2) \geq 6$ if $p \geq 5$ and $(p,m_1) \neq (5,3)$. Take

$$\omega := \left(\frac{W(Y,Z)}{(X-\alpha_1 Z)^{m_1}}\right)^{m_1+1} A_{1,m_1+1}^{m_1-2}.$$

Then

$$\begin{aligned}
\operatorname{ord}_{\mathfrak{p}_1,\varphi}\,\omega &\geq [(m_1+1+p)(m_1-2) - m_1(m_1+1)]\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)\\
&= [(m_1-2)(p-2)-6]\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)
\end{aligned}$$

is non-negative if $p \geq 5$ and $(p,m_1) \neq (5,3)$. Therefore, ω is regular and non-trivial on any component of C if A_{1,m_1+1} is not factor of C. For the remaining case, i.e., $(p, m_1) = (5, 3)$, we take

$$\omega := \left(\frac{W(Y,Z)}{Z(X-\alpha_1 Z)^3}\right)^5 A_{1,4}(X-Y)((X-\alpha_1 Z)^4 - (Y-\alpha_1 Z)^4)Z,$$

which is well defined in $\mathbf{P}^2$ and can have poles only at $\mathfrak{p}_1$ and at $\mathfrak{q}_i$, the points at infinity. Let $\mathfrak{q}$ be one of the points $\mathfrak{q}_i$. By Lemma 5(i), we have

$$5 \mid \operatorname{ord}_{\mathfrak{q},\varphi} Z + \operatorname{ord}_{\mathfrak{q},\varphi}((X-\alpha_1 Z)^4 - (Y-\alpha_1 Z)^4),$$

and hence $\operatorname{ord}_{\mathfrak{q}} Z + \operatorname{ord}_{\mathfrak{q},\varphi}((X-\alpha_1 Z)^4 - (Y-\alpha_1 Z)^4) \geq 5$. Therefore, ω is regular at the points at infinity. At $\mathfrak{p}_1$, we see from the expansion of $F(X,Y,Z)$ in (3.1.1) that

$$\operatorname{ord}_{\mathfrak{p}_1,\varphi}((X-\alpha_1 Z)^4 - (Y-\alpha_1 Z)^4) \geq 5 \operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)$$

and $\operatorname{ord}_{\mathfrak{p}_1,\varphi}(A_{1,4}(X-Y)) \geq 10 \operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)$, hence ω is also regular at $\mathfrak{p}_1$.

For (iv.b), we have $l = 1$, $\mu_1 = m_1 + 1 = m$, and $u \geq 3$. We note that in this case $p \mid m_1 + u$ and we need to exclude the following cases: $m_1 = 2$ and $p = 2$; $(u, m_1) = (3, 2)$, which gives $p = 5$; and $(u, m_1) = (3, 3)$, which gives $p = 3$. The first two conditions and $p \mid m_1 + u$ imply that $u \geq 5$ if $m_1 = 2$. Take

$$\omega := \left(\frac{W(Y,Z)}{Z(X-\alpha_1 Z)^{m_1}}\right)^{m_1+u} (A_{1,m_1}(X-Y))^{m_1} Z^{(u-2)(m_1-1)-2},$$

where $A_{1,m_1}(X-Y) = (X-\alpha_1 Z)^{m_1+1} - (Y-\alpha_1 Z)^{m_1+1}$. The assumption implies that $m_1 \geq 3$ or $m_1 = 2$ and $u \geq 5$, hence $(u-2)(m_1-1)-2 \geq 0$. Since $\operatorname{ord}_{\mathfrak{p}_1,\varphi} A_{1,m_1} \geq (m_1+u-1)\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)$ and $\operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-Y) \geq \operatorname{ord}_{\mathfrak{p}_1,\varphi}(X-\alpha_1 Z)$, it is clear that ω is regular at $\mathfrak{p}_1$. Let $\mathfrak{q}$ be one of the poles at infinity. Then

$$\begin{aligned} \text{(4.1.7)} \quad \operatorname{ord}_{\mathfrak{q},\varphi}\omega &\geq ((u-2)m_1 - u)\operatorname{ord}_{\mathfrak{q},\varphi} Z + m_1 \operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) \\ &\quad - m_1 - u \\ &\geq (u-2)m_1 - u - u = (u-2)(m_1-2) - 4, \end{aligned}$$

which is non-negative except when $m_1 = 2$ or $(u, m_1) = (3,3), (3,4), (3,5), (4,3), (5,3)$. Since $p \mid u + m_1$ and $p \nmid m_1 + 1$, (u, m_1) cannot be $(5,3)$ nor $(3,5)$. Similarly, if $(u, m_1) = (3,3)$ then $p = 3$. This case is ruled out by our assumption. We are left with the cases: $(u, m_1) = (3,4), (4,3)$, or $m_1 = 2$. Since $p \mid m_1 + u$, the first two cases occur only when $p = 7$, and $u \geq p - 2$ if $m_1 = 2$. Moreover, since $(m_1, p) \neq (2, 5)$ we must have $p \geq 7$ if $m_1 = 2$. The inequality (4.1.7) becomes

$$\begin{aligned} &\text{(4.1.8)} \quad \operatorname{ord}_{\mathfrak{q},\varphi} Z + 4\operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) - 7 && \text{if } (u, m_1) = (3,4), \\ &\text{(4.1.9)} \quad 2\operatorname{ord}_{\mathfrak{q},\varphi} Z + 3\operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) - 7 && \text{if } (u, m_1) = (4,3), \\ &\text{(4.1.10)} \quad (p-6)(\operatorname{ord}_{\mathfrak{q},\varphi} Z - 1) + 2\operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) - 6 && \text{if } m_1 = 2, \end{aligned}$$

respectively. On the other hand, by Lemma 5(iii) we have

$$7 \mid \operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) - 5\operatorname{ord}_{\mathfrak{q},\varphi} Z \quad \text{if } (u,m_1)=(3,4), \tag{4.1.11}$$

$$7 \mid \operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) - 4\operatorname{ord}_{\mathfrak{q},\varphi} Z \quad \text{if } (u,m_1)=(4,3), \tag{4.1.12}$$

$$p \mid \operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) - 3\operatorname{ord}_{\mathfrak{q},\varphi} Z \quad \text{if } m_1=2. \tag{4.1.13}$$

For $\operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) \geq 2$, (4.1.8) is non-negative. If $\operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) = 1$ then $\operatorname{ord}_{\mathfrak{q},\varphi} Z \geq 3$ by (4.1.11), hence (4.1.8) is non-negative. Similarly, if $\operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) \geq 2$ then (4.1.9) is non-negative; if $\operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) = 1$ then $\operatorname{ord}_{\mathfrak{q},\varphi} Z \geq 2$ by (4.1.12), hence (4.1.9) is non-negative. If $p > 7$ and $m_1 = 2$ it is easily checked that (4.1.10) is non-negative. If $p = 7$, then (4.1.13) implies that $\operatorname{ord}_{\mathfrak{q},\varphi} Z \geq 5$ if $\operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) = 1$, and $\operatorname{ord}_{\mathfrak{q},\varphi} Z \geq 3$ if $\operatorname{ord}_{\mathfrak{q},\varphi}(A_{1,m_1}(X-Y)) = 2$. Again we conclude that (4.1.10) is non-negative. Since the curve C has no linear factors, ω is regular and non-trivial on any component of C. This concludes the proof of the lemma. ■

4.2. *On the curve* $[F_c(X,Y,Z)=0]$, $c \neq 0,1$. We shall use the notation of Section 3, and recall that

$$P(X) - P(\alpha_i) = \sum_{j=\mu_i}^{n} b_{i,j}(X-\alpha_i)^j.$$

If $\mathfrak{p}_i = (\alpha_i, \alpha_{\phi(i)}, 1) \in C_c$, then we may write

$$F_c(X,Y,Z) = \sum_{j=\mu_i}^{n} b_{i,j} Z^{n-j}(X-\alpha_i Z)^j - c \sum_{j=\mu_{\phi(i)}}^{n} b_{\phi(i),j} Z^{n-j}(Y-\alpha_{\phi(i)} Z)^j. \tag{4.2.1}$$

Denote by $B_{i,m}$ the following sum:

$$B_{i,m}(X,Y,Z) = \sum_{j=\mu_i}^{m} b_{i,j} Z^{m-j}(X-\alpha_i Z)^j - c \sum_{j=\mu_{\phi(i)}}^{m} b_{\phi(i),j} Z^{m-j}(Y-\alpha_{\phi(i)} Z)^j.$$

If $p \mid n$, then $m = 1 + \sum_{i=1}^{l} m_i < n$, and so there exists an integer $u_i > m$ such that $b_{i,u_i} \neq 0$ or $b_{\phi(i),u_i} \neq 0$, and $b_{i,j} = b_{\phi(i),j} = 0$ for $m < j < u_i$. In other words, u_i is the degree in X and Y of the non-vanishing terms in (4.2.1) following $B_{i,m}$. Then, at $\mathfrak{p}_i$,

$$\operatorname{ord}_{\mathfrak{p}_i,\varphi} B_{i,m} \geq u_i \min\{\operatorname{ord}_{\mathfrak{p}_i,\varphi}(X-\alpha_i Z), \operatorname{ord}_{\mathfrak{p}_i,\varphi}(Y-\alpha_{\phi(i)} Z)\}; \tag{4.2.2}$$

and at $\mathfrak{q}_i = (x_i, 1, 0)$ such that $x_i^m = c$ and $x_i^n = c$, we have

$$p \mid \operatorname{ord}_{\mathfrak{q}_i,\varphi} B_{i,m} - m \operatorname{ord}_{\mathfrak{q}_i,\varphi} Z. \tag{4.2.3}$$

LEMMA 7. *Let P be a polynomial of degree n satisfying Hypothesis* I. *Assume that $p > 0$ and $p \mid n$. If the curve C_c has no linear components, then each component of C_c admits a non-trivial product of 1-forms in the following cases*:

(i) $l \geq 4$; $l = 2, 3$ *and* $\max\{m_i\} \geq 2$; *or* $l = 1$ *and* $m_1 \geq 2$;

(ii) $l = 3$, $m_1 = m_2 = m_3 = 1$, *and* $B_{1,4}$ *is not a factor of* $F_c(X, Y, Z)$ *if* $l_0 = l = 3$, $3 \mid n-1$, $4 \mid n$, *and* $B_{1,4} = B_{2,4} = B_{3,4}$;

(iii) $l = 2$, $m_1 = m_2 = 1$, $l_0 = 1$, *and* $B_{i,3}$ *is not a factor of* $F_c(X, Y, Z)$ *if* $3 \mid n$ *and* $(\alpha_i, \alpha_{\phi(i)}, 1) \in C_c$;

(iv) $l = 2$, $m_1 = m_2 = 1$, $l_0 = 2$ *and* $B_{1,3} = B_{2,3}$, *and* $B_{1,3}/(X + Y - (\alpha_1 + \alpha_2)Z)$ *is not a factor of* $F_c(X, Y, Z)$ *if* n *is odd*, *and* $3 \mid n$.

REMARK. In (ii), we let $\widetilde{P}_1(X) = P_0(X) - (P_0(\alpha_1) - cP_0(\alpha_{\phi(1)}))/(1-c)$, where $P(X) = \sum_{i=0}^{n} a_i X^i$ and $P_0(X) = \sum_{i=0}^{4} a_i X^i$. Then the sum $B_{1,4}$ is the homogenization of $\widetilde{P}_1(X) - c\widetilde{P}_1(Y)$, and $B_{1,4} = B_{2,4} = B_{3,4}$ is equivalent to the conditions that $\widetilde{P}_1(\alpha_i) = c\widetilde{P}_1(\alpha_{\phi(i)})$ for $i = 1, 2, 3$. These statements will be verified in the proof of the lemma.

Proof of Lemma 7. From Lemma 2, we already have (i), and (ii) in the case $l_0 < 3$. It remains to consider the cases (ii) for $l_0 = 3$, (iii), and (iv). We have

$$\frac{\partial F_c}{\partial X}(X, Y, Z) = m a_m Z^{n-m} \prod_{i=1}^{l} (X - \alpha_i Z)^{m_i},$$

$$\frac{\partial F_c}{\partial Y}(X, Y, Z) = -m c a_m Z^{n-m} \prod_{i=1}^{l} (Y - \alpha_i Z)^{m_i},$$

$$\frac{\partial F_c}{\partial Z}(X, Y, Z) = (n - m) a_m Z^{n-m-1} (X^m - cY^m + ZG_{m-1}),$$

where G_{m-1} is homogeneous polynomial of degree $m-1$. From these we get

$$\frac{W(Y, Z)}{Z \prod_{i=1}^{l} (X - \alpha_i Z)^{m_i}} \equiv \frac{W(Z, X)}{-cZ \prod_{i=1}^{l} (Y - \alpha_i Z)^{m_i}} \equiv \frac{W(X, Y)}{-(X^m - cY^m + ZG_{m-1})}.$$

This 1-form will be denoted by θ. We see that on the curve C_c, a point at infinity $\mathfrak{q}_i = (x_i, 1, 0)$ is a pole of θ only if $x_i^m = c$ and $x_i^n = c$.

We first consider the case $l = l_0 = 3$ and $m_1 = m_2 = m_3 = 1$. We have $m = 4$ and $p \neq 2, 3$ in this case. We note that if $p = 3$ and $l_0 = l = 3$ then $c = 1$, which is impossible. Moreover, the constant c is a solution of the equation $w^2 + w + 1 = 0$ and the only possible poles of θ are $\mathfrak{p}_i = (\alpha_i, \alpha_{\phi(i)}, 1)$, $i = 1, 2, 3$, and $\mathfrak{q}_j = (x_j, 1, 0)$ satisfying $x_j^4 = w$ and $x_j^n = w$. The solutions of $X^4 = w$ are $w, -w, w\xi, -w\xi$, where ξ is a primitive root of $X^4 = 1$. If $3 \nmid n-1$, none of these can be a solution of $X^n = w$, which implies that θ has no pole at infinity; if $3\,|\,n-1$ and $2\nmid n$, i.e., $\gcd(n,m)=1$, then $(w,1,0)$ is the only possible pole of θ at infinity; if $3\,|\,n-1$, $2\,|\,n$ and $4\nmid n$, then $(w,1,0)$ and $(-w,1,0)$ are the only two possible poles of θ at infinity; if $3\,|\,n-1$ and $4\,|\,n$, then it has four possible poles at infinity. For the first two cases, i.e., $3\nmid n-1$ or $3\,|\,n-1$ and $2\nmid n$, we may take

$$\omega = \frac{W(Y,Z)L_{12}L_{30}}{Z(X-\alpha_1 Z)(X-\alpha_2 Z)(X-\alpha_3 Z)},$$

where L_{30} is the line passing through $(\alpha_3,\alpha_{\phi(3)},1)$ and $(w,1,0)$. Similarly, ω is regular and is non-trivial on each component of C_c if C_c has no linear factor. For the other two cases, i.e., $3\,|\,n-1$, and $2\,|\,n$, we take

$$\omega = \left(\frac{W(Y,Z)L_{12}}{Z(X-\alpha_1 Z)(X-\alpha_2 Z)(X-\alpha_3 Z)}\right)^p B_{3,4}Z^{p-4},$$

which is regular at $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Since $m_3 = m_{\phi(3)} = 1$, we have $\operatorname{ord}_{\mathfrak{p}_3}(X-\alpha_3) = \operatorname{ord}_{\mathfrak{p}_3}(Y-\alpha_{\phi(3)})$. Hence inequality (4.2.2) and $u_i \geq p$ imply that ω is regular at $\mathfrak{p}_3$. At the point at infinity $\mathfrak{q} = (w,1,0)$,

$$\operatorname{ord}_{\mathfrak{q},\varphi}\omega \geq \operatorname{ord}_{\mathfrak{q},\varphi} B_{3,4} + (p-4)\operatorname{ord}_{\mathfrak{q},\varphi} Z - p. \tag{4.2.4}$$

By (4.2.3), $\operatorname{ord}_{\mathfrak{q},\varphi} B_{3,4} - 4\operatorname{ord}_{\mathfrak{q},\varphi} Z$ is divisible by p. Moreover, $\operatorname{ord}_{\mathfrak{q},\varphi} B_{3,4} + (p-4)\operatorname{ord}_{\mathfrak{q},\varphi} Z$ is greater than zero since $p \geq 5$. Hence, it is greater than p and this implies that the integer in (4.2.4) is not negative. Therefore ω is regular on C_c. To check that ω is non-trivial on each component of C_c we analyze further the sum $B_{i,4}$, $i=1,2,3$. We write $P(X) = P_0(X) + Q(X)$, where $P(X) = \sum_{j=0}^n a_j X^j$, $P_0(X) = \sum_{j=0}^4 a_j X^j$ and $Q(X) = \sum_{j=5}^n a_j X^j$. Then $P(X) - P(\alpha_i) = P_0(X) - P_0(\alpha_i) + Q(X) - Q(\alpha_i)$. The sum $B_{i,4}$ is the homogenization of $P_0(X) - P_0(\alpha_i) - c(P_0(Y) - P_0(\alpha_{\phi(i)}))$, since $p \geq 5$ and the degree of each term in $Q(X)$ is divisible by p. On the other hand, let

$$\widetilde{P}_i(X) := P_0(X) - \frac{P_0(\alpha_i) - cP_0(\alpha_{\phi(i)})}{1-c};$$

then $\widetilde{P}_i(X) - c\widetilde{P}_i(Y) = P_0(X) - P_0(\alpha_i) - c(P_0(Y) - P_0(\alpha_{\phi(i)}))$ and we see that $B_{i,4}$ is also the homogenization of $\widetilde{P}_i(X) - c\widetilde{P}_i(Y)$. Since $\deg P_0 = 4$ and $p \neq 2$, we see that each of the four points at infinity of $[B_{i,4}=0]$ has multiplicity one and so are non-singular points. At finite points, we see that the only possible singular points of $[B_{i,4}=0]$ are $(\alpha_j,\alpha_{\phi(j)},1)$, $j=1,2,3$, with multiplicity 2 since $\widetilde{P}_i'(X) = P'(X)$. Clearly, $\mathfrak{p}_i = (\alpha_i,\alpha_{\phi(i)},1) \in B_{i,4}$. If there exists one $j \neq i$ such that $(\alpha_j,\alpha_{\phi(j)},1) \notin [B_{i,4}=0]$, then it is easy to see that $[B_{i,4}=0]$ is irreducible and has genus at least 1. In this case, there exists a non-trivial regular 1-form on $[B_{i,4}=0]$, and ω is non-trivial on every component of C_c other than $[B_{i,4}=0]$. We now consider the case $\mathfrak{p}_j \in B_{i,4}$ for each $j \neq i$. Then $\widetilde{P}_i(\alpha_j) = c\widetilde{P}_i(\alpha_{\phi(j)})$, equivalently, $P_0(\alpha_j) - cP_0(\alpha_{\phi(j)}) =$

$P_0(\alpha_i) - cP_0(\alpha_{\phi(i)})$. Since $B_{i,4}$ is the homogenization of $P_0(X) - P_0(\alpha_i) - c(P_0(Y) - P_0(\alpha_{\phi(i)}))$, this implies that $B_{j,4} = B_{i,4}$. Therefore, in this case we have $B_{1,4} = B_{2,4} = B_{3,4}$, and $[B_{i,4} = 0]$ has three ordinary multiple points of multiplicity 2. If $[B_{i,4} = 0]$ is reducible, then Bézout's theorem implies that it consists of a line and a smooth irreducible curve of genus 1; if $[B_{i,4} = 0]$ is irreducible, then it is a curve of genus 0. The first case is certainly fine since C_c does not have a linear factor, and a component of genus 1 admits a non-trivial regular one form. Therefore, we only need to assume that $B_{i,4}$ is not a factor of $F_c(X, Y, Z)$ if $B_{1,4} = B_{2,4} = B_{3,4}$. However, if $B_{i,4}$ is a factor of $F_c(X, Y, Z)$, then we see that $(X^4 - wY^4) \mid (X^n - wY^n)$ by evaluating $B_{i,4}$ and $F_c(X, Y, Z)$ at $Z = 0$. Since $w^3 = 1$ and $3 \mid n - 1$, we have $w^n = 1$. This implies that $(X^4 - (wY)^4) \mid (X^n - (wY)^n)$, which, however, is impossible if $4 \nmid n$.

For (iii), we may assume that $\mathfrak{p}_1 = (\alpha_1, \alpha_2, 1) \in C_c$ and $(\alpha_2, \alpha_1, 1) \notin C_c$. Then the only possible poles of θ are $\mathfrak{p}_1$ and $\mathfrak{q} = (x, 1, 0)$ satisfying $x^3 = c$ and $x^n = c$. Suppose that $\xi^3 = c$; then $X^3 = c$ has three possible solutions ξ, $w\xi$ and $w^2\xi$, where $w^2 + w + 1 = 0$. Therefore, if $3 \nmid n$, θ has at most one pole (i.e., $\mathfrak{q}_0 = (\xi, 1, 0)$) at infinity. In this case, we take

$$\omega = \frac{W(Y, Z)L_{10}}{Z(X - \alpha_1 Z)(X - \alpha_2 Z)},$$

where L_{10} is a line passing through $\mathfrak{p}_1$ and $\mathfrak{q}_0$. If $3 \mid n$, then we take

$$\omega = \left(\frac{W(Y, Z)}{Z(X - \alpha_1 Z)(X - \alpha_2 Z)}\right)^p B_{1,3} Z^{p-3}.$$

One checks (by an argument analogous to the one given in the previous case) that ω is indeed regular on C_c and that $B_{1,3}$ defines an irreducible curve of genus 0. Therefore it is necessary to assume that $B_{1,3}$ is not a factor of $F_c(X, Y, Z)$.

For (iv), $l = l_0 = 2$ and $m_1 = m_2 = 1$ imply that $p \neq 2, 3$, $c = -1$, and θ has poles at infinity, say $(x, 1, 0)$, only if $x^3 = -1$ and $x^n = -1$. Obviously θ has no pole at infinity if n is even. If n is odd and $3 \nmid n$ then $(-1, 1, 0)$ is the only pole of θ at infinity. In this case, we take

$$\omega = \frac{W(Y, Z)L_{12}}{Z(X - \alpha_1 Z)(X - \alpha_2 Z)}.$$

Since the line $[L_{12} = X + Y - (\alpha_1 + \alpha_2)Z = 0]$ passes through the points $\mathfrak{p}_1 = (\alpha_1, \alpha_2, 1), \mathfrak{p}_2 = (\alpha_2, \alpha_1, 1)$ and $(1, -1, 0), \omega$ is regular at these points. If n is odd and $3 \mid n$ we claim that $B_{1,3} = B_{2,3}$. For simplicity, write

$$P'(X) = (X - \alpha_1)(X - \alpha_2)Q(X).$$

Then

$$P(X) - P(\alpha_1) = \left(\frac{\alpha_1 - \alpha_2}{2}(X-\alpha_1)^2 + \frac{1}{3}(X-\alpha_1)^3 + \cdots\right) R(X).$$

Here Q and R are polynomials. We deduce from this that

$$B_{1,3} = \frac{\alpha_1 - \alpha_2}{2}[(X-\alpha_1 Z)^2 - (Y-\alpha_2 Z)^2]Z + \frac{1}{3}[(X-\alpha_1 Z)^3 + (Y-\alpha_2 Z)^3],$$
$$B_{2,3} = \frac{\alpha_2 - \alpha_1}{2}[(X-\alpha_2 Z)^2 - (Y-\alpha_1 Z)^2]Z + \frac{1}{3}[(X-\alpha_2 Z)^3 + (Y-\alpha_1 Z)^3].$$

Clearly, $X + Y - (\alpha_1 + \alpha_2)Z$ is a linear factor of $B_{1,3}$ and $B_{2,3}$; moreover, it is easily seen that $B_{1,3} = B_{2,3}$ and $B_{1,3}/(X + Y - (\alpha_1 + \alpha_2)Z)$ is irreducible and defines a curve of genus 0. Thus

$$\omega = \left(\frac{W(Y,Z)}{Z(X-\alpha_1 Z)(X-\alpha_2 Z)}\right)^p B_{1,3} Z^{p-3}$$

is regular on C_c and is non-trivial on each component of C_c if $B_{1,3}/(X + Y - (\alpha_1 + \alpha_2)Z)$ is not a factor of $F_c(X,Y,Z)$. ■

4.3. *Proof of Theorem 2 and Corollary 1.* Theorem 2 follows directly from Lemmas 6 and 7.

We now prove the corollary. It is well known that if S is not affinely rigid, then $P(X)$ is not a strong uniqueness polynomial for $\mathcal{A}^*(\mathbf{K})$. From now on we suppose that S is affinely rigid. When $l \geq 3$, $P(X)$ is already a strong uniqueness polynomial for $\mathcal{M}^*(\mathbf{K})$ except when $l = l_0 = 3$, $m_1 = m_2 = m_3 = 1$, $3 \mid n-1$, $4 \mid n$, $B_{1,4} = B_{2,4} = B_{3,4}$, and $B_{1,4}$ is a factor of $F_c(X,Y,Z)$. We actually proved that in this case $[B_{1,4} = 0]$ is irreducible and of genus 0. From our proof of Lemma 7, we see that on the components of C_c other than $[B_{1,4} = 0]$, the product of 1-forms we constructed is regular and non-vanishing. Thus those components must be of positive genus. On the other hand, we have shown in the proof of Lemma 7 that $B_{1,4}(X,Y,1)$ can be written as $\widetilde{P}_1(X) - c\widetilde{P}_1(Y)$ with $\deg \widetilde{P}_1(X) = 4$. Since $p \neq 2$, $p \nmid 4$, $\widetilde{P}_1$ is a strong uniqueness polynomial for $\mathcal{A}^*(\mathbf{K})$ if and only if $\widetilde{P}_1(X) - c\widetilde{P}_1(Y)$ and $(\widetilde{P}_1(X) - \widetilde{P}_1(Y))/(X - Y)$ have no linear factors. Therefore, $B_{1,4}(X,Y,1) = 0$ cannot admit a solution consisting of a pair of non-constant non-archimedean entire functions. Therefore, $P(X)$ is a strong uniqueness polynomial for $\mathcal{A}^*(\mathbf{K})$ if $l \geq 3$. Moreover, this argument works analogously for cases (I.A), (I.B.1), and (I.B.2) since the polynomials $A_{1,m_1}(X,Y,1)$ (in Theorem 2(I.B.2.b.ii) and (I.C.2)) and $B_{1,3}(X,Y,1)$ (in Theorem 2(II.C)) do not admit any solution consisting of a pair of non-constant non-archimedean entire functions.

It now remains to consider the case when $l = 1$ and $\mu_1 = m_1 + 1$. Then

$$P(X) - P(\alpha_1) = b_{1,m_1+1}(X-\alpha_1)^{m_1+1} + b_{1,m_1+2}(X-\alpha_1)^{m_1+2} + \cdots.$$

If $b_{1,m_1+2} = 0$, then Theorem 2(I.C.3.b) implies that $P(X)$ is also a strong uniqueness polynomial for $\mathcal{A}^*(\mathbf{K})$ provided $m_1 \geq 2$ and $p \geq 7$. Therefore (I.B.3.a) holds. If $b_{1,m_1+2} \neq 0$, we let

$$P_0(X) = b_{1,m_1+1}(X - \alpha_1)^{m_1+1} + b_{1,m_1+2}(X - \alpha_1)^{m_1+2}.$$

Then as was shown in [1], the polynomial $P_0(X)$ is a strong uniqueness polynomial for $\mathcal{A}^*(\mathbf{K})$ if and only if $m_1 + 2 = p^r s$, $p \nmid s$, $s \geq 2$. We also note that in this case,

$$\frac{P_0(X) - P_0(Y)}{X - Y} = A_{1,m_1+1}(X, Y, 1).$$

Therefore, $A_{1,m_1+1}(X, Y, 1) = 0$ has no solutions in $\mathcal{A}^*(\mathbf{K}) \times \mathcal{A}^*(\mathbf{K})$ if m_1+2 is not a power of p. Hence, $P(X)$ is a strong uniqueness polynomial for $\mathcal{A}^*(\mathbf{K})$ in the case (I.B.3.b) by Theorem 2(I.C.3.a).

We now prove (II). We let $m_1 + 2 = p^r$ for some positive integer r. From Theorem 2(I.C.3.a) and the previous discussion, $P(X)$ is not a strong uniqueness polynomial for $\mathcal{A}^*(\mathbf{K})$ if and only if $F(X, Y, Z)$ is divisible by $A_{1,m_1+1} = A_{1,p^r-1}$. This condition is equivalent to $P(X) - P(Y)$ being divisible by

$$\begin{aligned} A_{1,p^r-1}(X, Y, 1) &= b_{1,p^r-1} \frac{(X - \alpha_1)^{p^r-1} - (Y - \alpha_1)^{p^r-1}}{X - Y} + b_{1,p^r}(X - Y)^{p^r-1} \\ &= \mathcal{F}_{p^r-1}(X, Y). \end{aligned}$$

If $P(X) - P(Y)$ is divisible by $\mathcal{F}_{p^r-1}(X, Y)$, then $(p^r - 1)S = T_{\mathcal{F}_{p^r-1}}(S)$ by the lemma stated at the end of this section, which was proved in [6] over $\mathbb{C}$, but its proof works for any field. On the other hand, if $(p^r-1)S = T_{\mathcal{F}_{p^r-1}}(S)$, one see easily that the points $\{(t_{ij}, s_i, 1) \mid 1 \leq i \leq n,\ 1 \leq j \leq p^r - 1\}$ are in the intersection of two curves defined by $P(X) - P(Y)$ and $\mathcal{F}_{p^r-1}(X, Y)$ and the sum of the relevant intersection multiplicities is $n(p^r - 1)$. Moreover, the curves have one extra intersection point $(1, 1, 0)$ at infinity, which implies they must have a common component by Bézout's theorem. Since $A_{1,m_1+1}(X, Y, Z)$ is irreducible, this implies that $\mathcal{F}_{p^r-1}(X, Y)$ is a factor of $P(X) - P(Y)$.

Lemma (cf. [6]). *Let $P(X) = (X - s_1) \cdots (X - s_n)$ be a monic polynomial with divisor of zeros S in $\mathbf{K}$. Let $R(x, y) = x^d + \cdots$ be a degree d polynomial in $\mathbf{K}[x, y]$ such that $R(x, y)$ divides $P(x) - bP(y)$ with some $b \neq 0$ in $\mathbf{K}$. Then*

$$[P(X)]^d = \prod_{i=1}^{n} R(x, s_i).$$

References

[1] T. T. H. An, J. T.-Y. Wang and P.-M. Wong, *Unique range sets and uniqueness polynomials in positive characteristic*, Acta Arith. 109 (2003), 259–280.

[2] —, —, —, *Strong uniqueness polynomials: the complex case*, Complex Var. Theory Appl. 49 (2004), 25–54.

[3] V. Berkovich, *Spectral Theory and Analytic Geometry over Non-Archimedean Fields*, Math. Surveys Monogr. 33, Amer. Math. Soc., Providence, RI, 1990.

[4] A. Boutabaa, W. Cherry and A. Escassut, *Unique range sets in positive characteristic*, Acta Arith. 103 (2002), 169–189.

[5] A. Boutabaa, A. Escassut and L. Haddad, *On uniqueness of p-adic entire functions*, Indag. Math. 8 (1997), 145–155.

[6] W. Cherry and J. T.-Y. Wang, *Uniqueness polynomials for entire functions*, Internat. J. Math. 13 (2002), 323–332.

[7] —, —, *Non-Archimedean analytic maps to algebraic curves*, in: Value Distribution Theory and Complex Dynamics, W. Cherry and C.-C. Yang (eds.), Contemp. Math. 303, Amer. Math. Soc., 2002, 7–36.

[8] W. Cherry and C.-C. Yang, *Uniqueness of non-archimedean entire functions sharing sets of values counting multiplicity*, Proc. Amer. Math. Soc. 127 (1999), 967–971.

[9] J. T.-Y. Wang, *Uniqueness polynomials and bi-unique range sets for rational functions and non-archimedean meromorphic functions*, Acta Arith. 104 (2002), 183–200.

[10] —, *The truncated second main theorem of function fields*, J. Number Theory 58 (1996), 139–157.

[11] —, *A note on Wronskians and ABC theorem in function fields of prime characteristic*, Manuscripta Math. 98 (1999), 255–264.

Institute of Mathematics
Academia Sinica
Nankang, Taipei 11529, Taiwan, R.O.C.
E-mail: tthan@math.sinica.edu.tw
jwang@math.sinica.edu.tw

Department of Mathematics
University of Notre Dame
Notre Dame, IN 46556, U.S.A.
E-mail: wong.2@nd.edu

Received on 16.6.2003
and in revised form on 14.9.2004 (4560)